The Attempted Securitisation of Bitcoin and The Question of Money

Simon Butler

Doctor of Philosophy in Cyber Security

Royal Holloway, University of London

December 2022

Declaration of Authorship

I, Simon Butler, hereby declare that this thesis and the work presented in it is entirely my own. Where I have consulted the work of others, this is always clearly stated.

Signed: SButler

Date: 19/12/2022

Abstract

Money is the pivotal institution of society and yet, after more than 300 years, it remains a polarising and unresolved socio-economic issue, with deep implications for equality across the world. Bitcoin and cryptocurrencies have emerged as potential solutions to some of the old problems with money, but they are often dismissed and criticised. And a narrative has emerged that they are a security threat. This thesis uses the lens of securitisation theory to examine and explore this perceived threat.

Using document analysis, the speech acts of prominent figures and the extent to which cryptocurrencies are used in illicit activity are explored, revealing that cryptocurrencies are only used in a relatively small amount of crime. The thesis then considers the views of illicit users of cryptocurrencies and UK law enforcement officers. Analysis of scraped internet forum data shows that anonymity is not the main advantage of cryptocurrencies in illicit activity, as is commonly thought. And through the use of interview, the views of UK law enforcement officers reveal an ambivalence to cryptocurrencies as a technology. Finally, a case study of HullCoin, the world's first local cryptocurrency, shows that other forms of money do potentially have a valid role to play in the future of money.

With a focus on the economic sector of securitisation theory, this thesis concludes that there has been an attempted securitisation of cryptocurrencies, but this has not been accepted by some audiences. Illicit use is not a valid justification for claims that cryptocurrencies are a security threat, and the securitising speech acts are more likely an attempt to protect the established alliance, which draws wealth and power from the control of the supply of money. Bitcoin is money. The world could well benefit from reimaginations of this pivotal institution.

Table of Contents

Acknowledgements

I am grateful to many people for their support and participation in this thesis. The PhD experience has been incredibly hard but rewarding in equal measure, and I appreciate that I was given this life-changing opportunity by the EPSRC Centre for Doctoral Training in Cyber Security at Royal Holloway, University of London.

I am also particularly grateful to my supervisors. First, for being open-minded to this project when there was (and is) a lot of scepticism about cryptocurrencies. I am very appreciative of all the time they have taken over several years to read and provide feedback on my work. I have learnt a huge amount from them, and I think my thesis is much stronger as a result of all their guidance.

In terms of the research I conducted, much of the thesis would not have been possible without participation. So, thank you to the law enforcement officers and the HullCoin participants who gave time to talk to me about their thoughts and experiences. Similarly, I am very grateful to the Cambridge Cybercrime Centre for sharing their dataset with me and many other researchers.

And finally, and most significantly, to the person who supported me the most throughout.

List of Figures and Tables

1 Introduction

This thesis is a study of the extent to which Bitcoin and cryptocurrencies pose a security threat. There are several academic theories of security and in Section 1.3 the theoretical approach to this research is described and the meaning of 'security' is defined as it pertains to this work. At the outset, it would be useful to discuss the term 'cryptocurrency' since definitions and understanding can vary. Throughout this thesis 'cryptocurrencies' is used as an umbrella term for products and projects in this space, as described below, but the focus of this study is on the monetary aspects of cryptocurrencies. As such, Bitcoin specifically is of central interest as it was the first of its type and, even today, remains the overwhelmingly dominant cryptocurrency by market capitalisation.

The first of a new type of money, Bitcoin was released to the world as a whitepaper in 2008 and followed shortly thereafter by an open-source, working product that went live on 3 January 2009 (Nakamoto, 2008). Since the inception of Bitcoin, however, there has been a proliferation of thousands of other products and projects built using Bitcoin's underlying blockchain technology or in a similar vein. Collectively, all of these endeavours, and any virtual tokens or 'coins' associated with them, are commonly referred to as 'cryptocurrencies'. Terms preferred by others include crypto-assets and virtual currencies. Bitcoin was created as a money and several other cryptocurrency projects are also envisioned as monies, such as Litecoin or more privacy focussed offerings like Monero. But most cryptocurrency projects are not directly purposed as monies, and the tokens or coins associated with the project are instead designed as 'in-project' utility tokens. In this respect, the tokens are more akin to loyalty points that can be used for various purposes within any given ecosystem. Even today, there are relatively few tokens that are designed or fashioned as money like Bitcoin, as opposed to utility tokens.

It would be simpler if the analysis in this thesis was only of Bitcoin but that would be remiss – some of the other cryptocurrencies, particularly the other monetary ones, need to be included in this study as they are also important to consider. It could also even be that one day one of them supplants Bitcoin. That is not an issue for this thesis, for the arguments that are presented here about Bitcoin could also apply generally to another cryptocurrency should it ever emerge as the dominant monetary offering. The reader should, therefore, retain a degree of flexibility when it comes to the terminologies used in this study, although specific guidance or clarity will be given where necessary.

Today, there are several debates about Bitcoin and cryptocurrencies that remain as fresh as at any time since their creation. Some are concerned with whether cryptocurrencies can even be considered a form of money, or whether they are simply a scam (for example, Lo & Wang, 2014; Ammous, 2018; A. S. Hayes, 2018). And there is an unresolved question about whether society should even allow monies that are disintermediated from the state (see Bjerg, 2016; Dodd, 2017). These issues are fundamental philosophical questions of sociology that have deep roots in academic literature, which will be discussed further in Chapter 2. These debates and literatures also underpin another significant dispute about cryptocurrencies – the extent to which they are a threat to security and a tool for illicit activity. This is the primary debate that this thesis will contribute towards.

Cryptocurrencies raise important questions over the privacy of financial transactions – an area of particular conflict in relation to the security threat that alternative monies potentially pose. Especially since 9/11, the state has claimed a need to be able to monitor financial transactions in order to proactively, rather than reactively, investigate crime (Amoore & De Goede, 2005). The concern is that cryptocurrencies undermine this effort. For a long time though, there have been others who would like how they spend their money to remain private, for money to be beyond the control and potential abuse of the state (Hughes, 1993). This balance between security and liberty is an ongoing one that has been a feature of security dialogue for several decades (Neocleous, 2008).

Many years after Bitcoin launched, discussion about cryptocurrencies continues to be polarising; academic and popular debate remains divided on many of the issues mentioned, and whether they are a security threat remains a pivotal one. Much is made of the illicit usage of cryptocurrencies, and this appears to stand as a key justification for claims that cryptocurrencies are a security threat (Gloerich et al., 2018; Zamani et al., 2020; Kfir, 2020). This study aims to examine these claims. Who is claiming that cryptocurrencies are a threat and why? Is the use of cryptocurrencies for illicit activity significant? Is this the main reason why they are viewed as a security threat? And how do answers to these questions relate to some of the wider issues about Bitcoin, the state, and their relationship to money and security? The form of money has changed more in the last one hundred years than in the last one thousand, and money sits at the heart of society, both local and global. Whether Bitcoin and other cryptocurrencies are a security threat is, therefore, an important topic that requires greater research in order to contribute to these debates.

This chapter has five main sections. The first section begins by setting out the background context that is needed to understand the advent of cryptocurrencies. It outlines the longstanding problems in money and the ongoing tensions that exist between the state and others who desire more freedom, particularly in the use of cryptography. The research problem space is then summarised and the theoretical framework for the thesis is described. The research questions follow, before the final section concludes with a look at the chapter structure of the remainder of the thesis.

1.1 Context

Bitcoin did not appear in 2008 as an isolated invention – it has a long prehistory in both the development of money and cryptography. Advances in these areas, mainly since the mid-twentieth century, enabled the technological foundations for digital money and a societal drive amongst certain individuals to make it happen. This section will set out this historical background, as an important base for an understanding of these new forms of money.

1.1.1 An Old Problem

On 22 February 1797, French forces invaded Great Britain at the Battle of Fishguard. The incursion only lasted two days but the affair is most famously remembered as the ‘last invasion of Britain’ (Quinault, 1999) – the last time that foreign troops forcefully landed on British shores. There was, however, another outcome of the invasion that is, perhaps, not as well remembered. The news of French boots on British soil led to a run on the Bank of England, whose reserves had already been drained following several financial scares during war against Revolutionary France (1793 - 1802) (O'Brien & Palma, 2020). On Monday 27 February 1797, the Bank of England took action and suspended the conversion of paper notes into gold, a decision supported by the government of William Pitt the Younger and passed into law by Parliament on 3 May 1797 through the Bank Restriction Act (O'Brien & Palma, 2020). To some modern economic historians, the move was a success, avoiding insolvency of the Bank of England (O'Brien & Palma, 2020). But to others, writing at the time, it was an unqualified outrage (Cobbett, 1828). Whichever view you take, these events mark the genesis of a long struggle over the involvement of the state in (modern) money – a struggle arguably no more resolved now, more than 200 years later.

In 1815, William Cobbett, a prominent critic of government monetary policy (Roberts, 2017), published a book titled, *Paper Against Gold* (Cobbett, 1828). Printed in several editions, the book contains a collection of essays and writings spanning several years, including during Cobbett's incarceration for seditious libel over an article he published censuring the lashing of 'local militia' at Ely by German Legion Cavalry (1828: xvi). For this offence, Cobbett was sentenced to two years in prison and ordered to pay several thousand pounds to the King. For many years before his incarceration in 1810, Cobbett had argued against paper money and for a return to a gold standard. Letter 1, in *Paper Against Gold*, provides a rich, contemporaneous source which articulates the debates of that time over the form, function and control of money.

Why and how did banks (in this case, the Bank of England) come to be involved in money? For, as Cobbett wrote, 'some regard the Bank of England as being as old as the Church of England' (Cobbett, 1828: 7). Again, it was war against France that spurred King William III to pass an Act to raise funds that led to the origin of the Bank of England in 1694. The lenders of the money were incorporated into a company called, 'The Governor and Company of the Bank of England' (7). The Act enabled the Bank to issue notes, but only as promissory banknotes that could be redeemed for the ‘coin of the country’, namely gold and silver, ‘to the bearer and on demand’ – the latter phrase retained to this day. As Cobbett described, this redemption promise distinguished the Bank of England’s notes and, over time, led them to be viewed ‘as good as gold and silver’. Effectively, the Bank began on a gold standard and this promise to redeem held as long as faith in it existed and as long as the Bank did redeem the coin it held. But the crucial issue, that lies at the heart of the debate concerning the state and money, slowly emerged – the temptation to issue more notes than coin held in reserve.

Cobbett observed that for the first twenty years, the number of notes in circulation was very small and the increase in quantity very slow. The number of notes only appeared to grow come war in 1755, at which time the largest note was for 20 pounds, quickly followed by the appearance of 15 and 10-pound notes. The Government borrowed more money, which was now called the National Debt, with the interest paid through taxation ‘raised upon the people’ (10). The result was that ‘year after year we saw more of bank-notes and less of gold and silver’ (10). Soon, after Pitt’s War in 1793, notes were issued for five pounds, with all sums above this amount settled with notes – two and one-pound notes duly followed in 1797. Cobbett marked the month of February 1797 and the creation of the five-pound note as the moment that ‘suspicion asleep…became broad awake’, ‘as paper-money became completely predominant’ (5). The Bank Restriction Act and the refusal of the Bank of England to redeem paper for gold now laid bare an issue that the world has struggled with for hundreds of years – that money is invariably abused and misused by those in power. Paper money now enabled this abuse with an ease and scale not previously seen. This issue of state power in relation to the control of money is one that is central to this thesis, and one that we will continue to return to.

1.1.2 Money - A Brief History

For thousands of years, people have been using metal as a form of money. Coinage developed several hundred years BC (Davies, 2002: 63) and is still widely used to this day. Paper money has also been in use for a long time – since the seventh century in China but somewhat later in the UK having been first issued by the Bank of England as late as the seventeenth century (Fish and Whymark, 2015: 219). It was only in the twentieth century that we saw significant change in how we spend; credit cards, debit cards and automated electronic payments all arrived. As too did the internet and the subsequent boom in online commerce. The technological advancements have only gathered pace – mobile phones are in most people's pockets, along with banking and other apps. Indeed, 71 per cent of the world's population, or 5.9 billion, are forecast to be mobile subscribers by 2025 (Global System for Mobile communications Association, 2018). Society has become increasingly but unevenly digitised, and money is no exception.

For some time, though, there has been conflict about the form of money and the functioning of the international monetary system. The classical gold standard ended with World War I but was returned to by some after the war, before being dropped again due to deflationary pressures, as depression moved across the world in the 1920s and 1930s (Simmons, 1996: 410). After the Second World War, there was a growing recognition that the international monetary system needed attention and that failures in this area in the interwar period were at least in part to blame for political tensions in the world (Davies, 2002: 587). Economic policies were non-concordant with the 'impossible trinity' (Obstfeld, Shambaugh and Taylor, 2004: 75). This trinity is based on the Mundell-Fleming economic model, which shows that you cannot have effective monetary policy, fixed exchange rates and capital mobility all at once (Fan and Fan, 2002: 43). As a result, the Bretton Woods system emerged in 1944 and key amongst its features were the tying of currencies to gold and the establishment of the International Monetary Fund. The system fared well for a time but came to an end not long after the Nixon Shock of 1971 when the United States suspended the link of the dollar to gold for the final time (the UK dropped the gold standard in 1931). This brought about the end of *representative money* and ushered in the era of *fiat money*, which continues to the present day.

Representative money has a claim on a commodity such as gold, whereas fiat money is often referred to as a currency to distinguish it from other forms of money that are linked to commodities of 'real value'. The Bank of England describes fiat as 'money that is not convertible to gold or any other asset' (2019) – for example, a paper banknote. The implications of supply and demand in fiat currencies on national debt, inflation, inequality and price stability is an ongoing economic debate (see Dolmas et al., 2000; Albanesi, 2007; Binder, 2019; Ahmed et al., 2022). Fiat money is typically ‘backed’ by the government that issues it, often via a central bank and decreed through law. As such, governments can expand the supply of their currency with only self-imposed restriction. To some, this is seen as an advantage over the limitations of a gold standard, enabling the central bank to ‘smooth the functioning of the economy’ (Bank of England, 2019). To others though, the result is potential for greater currency devaluation - the US dollar lost 87 per cent of its purchasing power between 1957 and 2008 (Ferguson, 2008: 63). Austrian economists argue that fiat currencies lead to high inflation and, ultimately, crisis (Polleit, 2012). Whilst Bitcoin is similar to fiat in that it is not linked to a commodity, one of its key contrasting features to fiat is that it has a fixed total supply, which will be reached in approximately 2140 once all new Bitcoins have been mined. Whether gold, fiat or Bitcoin serves as the ‘better’ form of money is a common and ongoing debate, that will be returned to in more detail later in this thesis.

1.1.3 International Settlement

The modern financial system has also been shaped by the dominance of the US dollar as the international settlement currency. Not only is it the domestic currency of the largest economy in the world, but it has also become the dominant currency of international trade and even the reserve currency of the world, accounting for 70 per cent of foreign exchange reserve assets stored by central banks across the globe (usually in the form of bonds) (F. E. Martin et al., 2017).

This is relevant to the discussion of currencies because of the Triffin Dilemma, which describes the conflict that arises when a national currency is also used as an international reserve currency. As global trade rises, more dollars are demanded internationally, requiring ‘persistent deficits in the U.S. balance of payments’ – this jeopardises the dollar’s value, which is what the system itself is based on (Boughton, 2001: 926-927). Indeed, after the Global Financial Crisis of 2007-2008 the Governor of the People’s Bank of China called for reform of the international monetary system:

> The desirable goal of reforming the international monetary system, therefore, is to create an international reserve currency that is disconnected from individual nations and is able to remain stable in the long run, thus removing the inherent deficiencies caused by using credit-based national currencies. (Xiaochuan, 2009)

This is something that John Maynard Keynes had proposed at the Bretton Woods Conference in the 1940s with his supranational Bancor currency – but it was rejected (Sharpe, 2009: 128). The Chinese encouraged the IMF to promote and widen the use of their special drawing rights (SDRs), a unit of account basket of five major currencies, but almost ten years later in 2017, the Governor of the People's Bank of China was still calling for further reform and expanded use of SDRs (Xiaochuan, 2017). The dollar, to this day, retains its dominance on the international stage, but the world is not settled on this position.

The rise of cryptocurrencies has prompted central banks, including the Bank of England, to consider whether they should provide central bank digital currency (CBDC) (Carney, 2018: 11). Indeed, the People's Bank of China is reportedly close to launching such a currency (Huang, 2019). Facebook also announced their intention to launch a cryptocurrency called Libra, originally planned for early 2020 (Libra Association Members, 2019). Those plans were met with 'serious concerns' (Rappeport & Popper, 2019) and Facebook's head of blockchain projects faced scepticism in evidence given to the US Senate Banking Committee (Brandom, 2019). Facebook eventually abandoned its plans because of the opposition it faced. The fate, then, for cryptocurrencies is at best uncertain and as much a societal issue as an economic one. For centuries sociologists have considered the nature of money, who should control it and what form it should take. And these issues are geopolitical, as states compete over the advantages that control of money brings (Blandin et al., 2019: 54).

In relation to cryptocurrencies, central to the question of control is the issue of the disintermediation of banks and the state from money – Facebook did not aim to do either, but Bitcoin does both (Dodd, 2017: 37). Whilst Facebook stated they would not launch Libra without regulatory approval (Lee, 2019), Bitcoin has already been operational for over ten years. And the backdrop to the emergence of new forms of money has been one of growing geopolitical tension, as the prospect of a ‘new’ bipolar world order emerges. The US and China have been clashing and money will certainly play a part in whatever future unfolds as the two countries are intertwined financially, and geopolitically (The Economist, 2021). The US benefits from controlling the world’s reserve currency but China holds large amounts of US debt and any move away from the dollar would be complicated in terms of the value of its own reserves and the effects this move would have, such as on Chinese exports (Drezner, 2010: 393, 401). Nevertheless, much Western power lies in the dominant position of the dollar and there is concern about the risk that other forms of money could pose, be it from China, Facebook or cryptocurrencies. The emergence of new forms of money or global powers challenges the status quo and the existing advantages that Western powers currently enjoy. It is not likely that this position would be given up lightly. US Congressman Brad Sherman described this concern to the House Financial Services Committee, illustrating the tensions that exist over the control of money:

> An awful lot of our international power comes from the fact that the U.S. dollar is the standard unit of international finance and transactions… It is the announced purpose of the supporters of cryptocurrency to take that power away from us, to put us in a position where the most significant sanctions we have against Iran, for example, would become irrelevant. So whether it is to disempower our foreign policy, our tax collection enforcement or traditional law enforcement, the advantage of crypto over sovereign currency is solely to aid in the disempowerment of the United States and the rule of law. (Bambrough, 2019)

1.1.4 Advances in Cryptography

The modern-day shift from the use of coins and notes as long-held forms of money relied upon advances in telecommunications technology and cryptography. Key amongst the early advances was the invention of public-key cryptography (Diffie & Hellman, 1976). Up until this time, secure communication relied on symmetric cryptography, where parties shared a secret key. This type of system presents difficulty in how to establish the key between the sender and receiver. This was manageable for large organisations, such as the military, but not practical for a large, open system like the internet where two parties may not even know each other (Martin, 2012: 152). The Diffie-Hellman key exchange protocol changed this and enabled two strangers (on the internet) to securely establish a shared secret. Once the World Wide Web was created, the foundations were in place for the growth of the internet and applications such as internet commerce.

Prior to the arrival of the World Wide Web, there were several other significant inventions and events that are important context to cryptocurrencies. In 1976, the Data Encryption Standard (DES) algorithm was published following a call from the US National Bureau of Standards three years earlier. Of note is that there have been several criticisms of DES, principle among which is an unsubstantiated claim that the National Security Agency (NSA) influenced a reduction in key size to make exhaustive key search possible (Martin, 2012: 121). If this is the case, then this would be evidence of the state wanting to retain the ability to decrypt communications.

This is important as, in the decades since cryptography emerged into a more public setting, there has been an ongoing conflict between states and others over the control of cryptography (primarily for confidentiality purposes). This struggle intensified in the 1990s, a period now dubbed the ‘Crypto Wars’ (Moore and Rid, 2016: 8; Jarvis, 2021). In 1991, computer scientist and cryptographer Phil Zimmerman openly published free software called Pretty Good Privacy (PGP). The program could encrypt emails and files (for confidentiality) and it used public-key cryptography to provide other cryptographic security services. As a result, the US government investigated Zimmerman for several years on the grounds that he had broken export restrictions for cryptography (Openpgp.org, 2020). The Clipper chip was another manifestation of this time. These chips were designed by the US government and based on the idea of escrowing decryption keys so that the authorities could decrypt communications if needed (Karlstrøm, 2014: 29). The scheme was opposed and made irrelevant by the availability of software, such as PGP, which offered stronger security.

This struggle between the state and those that desire privacy through strong encryption has not ended. If anything, the conflict is as present as ever. In 2013, details of a government-run programme that targeted encrypted internet traffic were published in the media as a result of the Snowden leaks (Moore and Rid, 2016: 7). More recently Apple, the technology company, had a battle with US authorities who wanted a backdoor into the iPhone in order to access data connected to a terrorist incident (Kahney, 2019). These are difficult societal issues and the debates about the use of cryptography do not seem clearer, even after several decades of argument.

It is here that the issue of 'security' comes to the fore and the seemingly inescapable trade-off between the loss of liberty and the protection of society. Some, such as Neocleous (2008: 11), question whether there must be a conflict between liberty and security. This is an ancient question that speaks to the ideas of Hobbes and Rousseau as 'social contract theorists' (Steinberger, 2008: 596), where we accept some loss of liberty for a civil society. These theories and arguments are at the heart of the debate about encryption policy. The world events of 11 September 2001 shifted posture towards security, whilst the Snowden leaks moved sentiment back towards liberty. But there is debate about these issues and the question of the balance between liberty and security (Amoore & De Goede, 2005). This is important to this thesis, as these questions can be applied to the debates about cryptocurrencies. If the Crypto Wars were fought primarily over the confidentiality of information, then doubts about cryptocurrencies are similarly related to the contested use of cryptography. But here the conflict is over the use of cryptography in ensuring the integrity of financial transactions, as a means of achieving decentralised financial networks and self-sovereignty.

1.1.5 Cypherpunks and Digital Cash

In the 1990s, shortly after Phil Zimmerman released PGP, a group called the Cypherpunks was established. Eric Hughes, one of the founders, wrote a manifesto about the group's aims:

> We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money. (Hughes, 1993)

The reference to electronic money is important. Whilst tools for the confidentiality of information existed (PGP), a similarly capable system for electronic money did not – although it was a developing area. Hughes's manifesto also presented other key characteristics of the Cypherpunk ethos; namely to write code as an instantiation of their aims and to publish it for free, for use across the globe by all. The Cypherpunks also ran a mailing list, for discussion of their ideas and aims.

By the time of the Cypherpunk manifesto, there had been several advances in the field of cryptography on digital money. David Chaum's work was most notable; in 1981 he published a paper on untraceable electronic mail and, in 1983, a foundational paper for the concept of digital money describing a method for untraceable payments (Chaum, 1983). In the latter paper, he acknowledges the conflict between privacy and criminal use of payments. Interestingly, in 1989 Chaum started a company to create a digital currency, Digicash, which made the world's first cryptographic payment in 1994 (Moore and Rid, 2016: 13). It was perhaps too early for the growth of internet commerce, and it shut down a few years later. Throughout the 1990s, this parallel development in cryptographic research and real-world attempts at digital money continued. Research papers covered many topics which form the basis of the technology used in Bitcoin; proof-of work systems to counter denial-of-service, timestamping of documents, decentralised databases, and others. Digital currencies also came and went, such as Liberty Reserve and E-gold. E-gold was a prominent digital currency at the time with over 4 million accounts and over $5 million in transfers per day (United States District Court for the District of Columbia, 2008). But, like Liberty Reserve, it came into conflict with the state and charges were brought by the US government relating to money laundering. Defendants, in that case, were sentenced in November 2008 – the same month Satoshi Nakamoto released the Bitcoin whitepaper. Perhaps Satoshi was aware of the proceedings against E-gold and Liberty Reserve when he considered his own anonymity and the design of Bitcoin. Centralised money providers often met the same fate – they were shut down and the founders faced criminal charges.

1.1.6 Bitcoin – A New Money?

For some, the answer to many of the questions about the state control of money lies in a new type of non-state money, cryptocurrencies. The first and largest of these, Bitcoin, emerged after the Great Financial Crisis of 2007-08, with the system going live in January 2009. The result of a whitepaper released in 2008 by a pseudonymous Satoshi Nakamoto (Butler, 2019: 331), Bitcoin was designed as a decentralised money - with a fixed supply that stood it in stark contrast to fiat currencies. It has no single, centralised owner or entity that runs it; instead, it is a voluntary, global network based on the use of its open-source software. Crucially, in this way, it is disintermediated from the state and banks (Carney, 2018: 6-7).

Bitcoins are technically different from conventional fiat monies, which are essentially centrally controlled databases (plus some smaller amounts of physical cash), and they are created through a computational process called 'mining' (for detail, see Antonopoulos, 2017; also, Bjerg, 2016). Miners compete to process batches of transactions known as 'blocks' and the first to solve a 'puzzle' receives a reward of new Bitcoin. The blocks are then added to the previous record of blocks, hence the term blockchain. Bitcoin has been programmed so that just under 21 million Bitcoins will ever be produced (each Bitcoin can be divided into 100 million sub-units called Satoshis). The supply schedule to issue new Bitcoins is also fixed. The puzzle that miners solve is a Proof-of-Work algorithm that dynamically adjusts so that the puzzle is solved approximately every ten minutes. When Bitcoin launched, the reward was 50 Bitcoin per block and this schedule halves every 210,000 blocks (approximately every four years). The reward is currently 6.25 Bitcoin per block following the last halving in 2020. In this manner, the inflation rate decreases towards zero by approximately 2140. With a fixed total supply, Bitcoin is in effect deflationary, as users invariably lose access to some Bitcoins over time. This deflationary policy is a political statement aligned with the Austrian School of economic thought (which will be discussed in greater detail in Chapter 2) and establishes Bitcoin as hard money in contrast to the soft money of the state (A. Hayes, 2019). Whilst we do not know the identity of Satoshi Nakamoto, the roots of Bitcoin go back to the ‘Crypto Wars’ and the libertarian idealism of the Cypherpunks, who sought privacy in cyberspace and saw electronic money as part of that vision (Hughes, 1993).

Bitcoin has been controversial since its creation, drawing significant criticism from politicians, bankers, economists, investors and academics (Gloerich et al., 2018; Butler, 2019). Cryptocurrencies have been labelled a security threat in relation to crime (Butler, 2020: 136), scammers abound, and cryptocurrency services have suffered from cyber-attacks (Zamani et al., 2020). Securing the Bitcoin network via the Proof-of-Work algorithm consumes significant amounts of electricity and, in a decentralised system, achieving consensus for software development has proven difficult (Aste et al., 2017: 12-13). There is also discussion about whether the greater early supply of Bitcoin has resulted in a skewed wealth concentration (see Kondor et al., 2014; Schultze-Kraft, 2021). Others even question whether peer-to-peer communities are as free and open to all as envisioned (Nelms et al., 2018).

Economic commentators have argued that Bitcoin cannot even be considered money as it has no ‘value’ (as opposed to gold, which can be used for other purposes) (Yermack, 2013; Torpey, 2017). Ingham, a prominent sociologist, also dismisses cryptocurrencies, as they do ‘what money should not do: that is, introduce uncertainty into transactions’ (2020: 114). Cryptocurrencies are volatile; in 2021 Bitcoin surged to a new high before again falling more than 50 per cent in a matter of weeks. This may be due to immaturity as money, but others claim Bitcoin is far from the stable currency needed for a base money regime, nor is it demand elastic (Luther, 2020). Bitcoin’s supply does not change relative to demand and remains constant in response to the dynamically adjusted difficulty of the Proof-of-Work algorithm. It is worth noting, however, that cryptocurrencies can be designed with a variety of properties, including even a dynamic supply schedule (Ampleforth, 2021).

These many criticisms and questions are symptomatic of a struggle by monetary theorists to define even what Bitcoin is. Is it a commodity or fiat, or perhaps private fiat money or even synthetic commodity money (Luther, 2018)? In Section 2.1.2 in particular, Bitcoin is analysed philosophically to consider if it can be thought of as money. But for all these discussions, it may be a moot point whether Bitcoin is money or not; in practice, it is used across the world as such. Coinbase, a prominent cryptocurrency exchange, saw its customer base rise from 35 to 54 million in the six months before its stock market listing (2021). Demand and usage of cryptocurrencies continue to grow – Bitcoin alone settles in the region of 300,000 transactions and as much as $45 billion in Bitcoin is sent per day (Bitinfocharts.com, 2021).

Considering all the debates about the form and function of money that have persisted for centuries, one must wonder why attempts to improve it are met with such scepticism. Especially given that the traditional financial system is also viewed by many as structurally flawed. Henry Ford is frequently quoted as having said that if more people knew how the monetary system worked then there would be a revolution tomorrow (quoted in Ingham, 2020: 44). Or as Murray Rothbard put it, ‘the state is the organization of robbery systematized and writ large’ (1981: 66). Even a former Chair of the US Federal Deposit Insurance Corporation (FDIC) commented, in a nod to the Cantillon effect, ‘I do think the system’s rigged’ and it ‘favour[s] the wealthy’ (CNBC Television, 2019). Why then does Bitcoin receive such opposition? The critiques of Bitcoin and cryptocurrencies outlined provide some explanation but many of them ‘apply equally… to our current forms of conventional money’ (Bjerg, 2016: 69). For example, if Bitcoin is criticised as a largely speculative vehicle, what do we make of Forex markets where trade is 98 per cent speculative and volume dwarfs Bitcoin at over $2 trillion per day even as far back as 2000 (Lietaer, 2001: 314)? In this way, ‘Bitcoin is no more fake than more conventional forms of money’ (Bjerg, 2016: 68). If this is the case, then to what extent can a money be a security threat? Is it a question of illicit usage of that money or do the issues lie deeper, in our conception of money as a tool for society? These are some of the fundamental questions that this thesis will answer.

1.2 The Research Problem Space

The history of money is an intriguing subject, and there has been more change in the forms and ways we use money in recent years, especially since the internet, than in any other previous time. Money is central to the workings of society and core to issues of politics and security. It is against this backdrop that we have witnessed the emergence of cryptocurrencies. Despite claims that they are a security threat, which we will explore, their popularity continues to grow. It is hard to estimate the total number of global users but Coinbase reports that it alone serves 73 million verified users and 10,000 institutions from over 100 countries (2022).

Cryptocurrencies are supported by many different groups, from those that embrace their Cypherpunk roots, who believe in them as a new financial system, free from control by traditional actors, to those that are only interested in speculation. But there have been others, especially some in prominent public positions, who have denounced cryptocurrencies as a scam or criminal tool, remarks which are often reported by the media. Jamie Dimon, for example, the CEO of JP Morgan Chase, has gone as far as publicly calling anyone who buys Bitcoin stupid and has labelled it a fraud akin to the tulip bubble of the seventeenth century (Son & Levitt, 2017). Perhaps confusingly, Dimon also saw potential in the underlying blockchain technology, but not in Bitcoin, which he felt had marginal uses for criminal purposes and in troubled countries. In July 2018, Jerome Powell, the chairman of the US Federal Reserve, is reported to have said in evidence to the US Congress that ‘cryptocurrencies are great if you are trying to hide or launder money’ (Shi, 2018). And this criminal association has made many headlines over the years, such as this:

> FBI fears Bitcoin’s popularity with criminals. (Zetter, 2012)

More recently, the issue received even more attention when Facebook announced plans to launch its cryptocurrency, Libra. Following a briefing at the White House, *The New York Times* published this headline, quoting the US Treasury Secretary:

> Cryptocurrencies Pose National Security Threat, Mnuchin Says. (Rappeport & Popper, 2019)

It seems that the decades-old conflict between the state and those who want alternative systems that deliver greater freedom, privacy and ultimately less interference from the state based on cryptography continues. The narratives about cryptocurrencies will be examined in more detail specifically in Chapter 4, but security appears to be the foremost issue used in the state's objections to these new forms of money, rather than energy use or any of the other concerns mentioned. The security threat is, therefore, the focus of this thesis. What evidence is there that cryptocurrencies are the security threat that some claim? Is their use on the dark net for illicit activity a security risk? To what extent are they a concern to law enforcement officers? And are there other uses and benefits of cryptocurrencies that are being marginalised in this concern about security? These are gaps in knowledge that will be discussed further in Chapter 2 and refined as research questions to be addressed by the empirical chapters later in the thesis.

The context in this introduction has shown that we are approaching a crucial point in the evolution of money, at a time of increasing geopolitical instability, as new powers emerge and existing alliances are challenged. The role of money in this power dynamic can be seen clearly in the example of the sanctions applied to Russia in response to the invasion of Ukraine. The role of the US dollar as the reserve currency of the world is under increasing scrutiny, as debt across the world soars, and as cryptocurrencies have emerged as non-state monies. What part cryptocurrencies may play in the future of money remains to be seen. The conflict between the state and those that wish to use cryptographic tools continues, and cryptocurrencies are another aspect of this pressing and security-led issue. This thesis will explore this tension between those that wish to use cryptocurrencies and those that are concerned that they are a security threat. To find ways 'out of the impasse of security' (Neocleous, 2008: 185), we must research the extent to which they are a threat and examine the contested issues more deeply. Money is pivotal to society, and we must endeavour to ensure that debates on this topic are as well-informed as they can be.

1.3 The Theoretical Framework

The criminal use of cryptocurrencies concerns the use of a new form of digital money for cybercrime. In the UK, law enforcement categorises cybercrime as being cyber-dependent or cyber-enabled (HMIC, 2015). The former requires computing equipment, whereas the latter may be traditional crimes that can be enhanced by using computing technologies. As a result, there can be difficulty deciding where responsibility for cybercrime lies – is it with specialist cyber officers or a wider issue for all of law enforcement? This has become even more important as the world increasingly becomes digitalised. In the same way, there can also be difficulty placing cybercrime research within academic fields. Cyber security has perhaps traditionally been focussed primarily on technical research, predominantly from within maths and computer science departments. Here the issues are about cryptography, and computer or network security for example. But cybercrime research focuses on those who are committing the crimes, their methods and the financial and political aspects of this activity. This does not tend to lie as clearly within cyber security or a specific field, as it can easily relate to security studies, criminology, economics or many other areas.

This is a challenge for an interdisciplinary study such as this one. The influences, literature and pertinent theories cross many academic boundaries, so they do not lie neatly confined to an easily definable field. Subsequently, as the reading and research progressed throughout this study, my thoughts on where the work might sit shifted. In particular, two papers influenced me early on and shaped the direction of my research. The first was Dodd's 'The Social Life of Bitcoin' (2017). The perspective here is from economic sociology. Dodd looks at Bitcoin as a symptom of monetary plurality in the twenty-first century (36). Bitcoin is money and money has always been polarising, confusing, contradictory, and a topic surrounded by debate. I found that this perspective helped me make sense of the arguments that we see today around Bitcoin. Dodd provides us with a way of looking at Bitcoin and grounds us in the literature on money. Importantly, he also identifies the fact that it is Bitcoin that aims to disintermediate *both* the state and banks from money (37). The second influential paper was Moore and Rid's 'Cryptopolitik and the Darknet' (2016), which takes its perspective from security studies. Although the paper focuses on encryption policy more generally, the dilemmas they identify are relevant to cryptocurrencies as they are also based on the use of cryptography and involve friction with the state. Linking this work to Dodd's, roots us in questions of state power and security threats. As such, this study lies at the intersection of economic sociology and security studies. It was from security studies that I encountered securitisation theory, which emerged as a helpful theoretical lens to analyse the use of cryptocurrencies and the security threat claims about them.

1.3.1 Securitisation Theory

Securitisation theory emerged from the Copenhagen School in the 1990s (Stritzel, 2014) and was set out by Buzan, Waever and de Wilde as a (new) framework for analysis in security studies (1998). Their work takes a constructivist approach, which aligns with the philosophical worldview taken in this thesis (this is discussed in Chapter 3). Thus, understanding this theory is important in helping us to consider the security threat posed by cryptocurrencies. The theory examines security in five main sectors (military, political, economic, environmental and societal) and has been applied in security studies and international relations to a wide range of subjects, and in a wide variety of ways (Stritzel, 2014; M. B. Salter, 2008). There have been many empirical studies using securitisation theory but they have concentrated on 'migration, the environment and health' (Balzacq et al., 2016: 507). Interestingly, though, whilst there have been some applications of the theory to cyber security, 'the school's economic sector of security has almost been completely ignored' (Floyd, 2019: 173). Indeed, Balzacq's article reviewing the achievements and empirical research of securitisation theory does not even mention the economic sector (Balzacq et al., 2016; Floyd, 2019: 188). This study will, therefore, contribute to this under-researched sector of securitisation theory by applying the theory to the security debate about Bitcoin and cryptocurrencies.

In the context of international relations, securitisation theory presents but one conception of security, where 'security' has a specific meaning and definition. 'Security' means taking an issue beyond or above the normal rules of politics, presenting the issue 'as an existential threat, requiring emergency measures and justifying actions outside the normal bounds of political procedure' (23-24). 'Security is about survival' – of a referent object from the existential threat that the issue represents (Buzan et al., 1998: 21). Since the existential threat is specific to the circumstances being analysed, it is not a simple matter of threat to life; in the military sector the threat is normally thought of in relation to the state and in the political sector, sovereignty in terms of legitimacy or governing authority. But in the economic sector, the existential threat is ‘more difficult to pin down’ (22). What object’s survival is potentially threatened by the existence of cryptocurrencies?

Securitisation theory is useful here, with the ‘economic sector’ offering a widened conceptualisation of security beyond the ‘the old military and state-centered view of the traditionalists’ (Buzan et al., 1998: 1). In particular, the theory attempts to describe what can genuinely be considered a security threat in the economic sector. That is, which economic threats can be legitimately thought of as beyond the bounds of normal political procedure. This distinction is fundamental to this thesis; are cryptocurrencies a genuine security threat or is the narrative only a reflection of a less urgent issue of politicised economics? Furthermore, as securitisation cannot be imposed, the securitising actor needs to ‘argue one’s case’ – and if this case is not accepted then ‘we can talk only of a securitizing move, not of an object actually being securitised’ (25).

> Securitization studies aims to gain an increasingly precise understanding of who securitizes, on what issues (threats), for whom (referent objects), why, with what results, and, not least, under what conditions (i.e., what explains when securitization is successful). (Buzan, Waever and de Wilde, 1998: 32)

Securitisation theory, therefore, provides a helpful language and framework for discussing cryptocurrencies and for understanding whether the attention they receive is appropriate. That is, are cryptocurrencies receiving exceptional treatment and attention? For securitisation theorists, there is a price to pay for excessive treatment; it is de-democratising. Rather than an issue being left to market forces or even normal politics, securitisation leads to exceptional treatment such as the banning of cryptocurrencies. This is de-democratising in the sense that people are not being given the chance to decide for themselves about an issue or, as in the case of bans, being denied the opportunity to even use a technology such as cryptocurrencies. As a result, ‘security’ should not always be viewed as a good thing, and Waever argues that ‘it is better…to aim for desecuritization: the shifting of issues out of emergency mode and into the normal bargaining process of the political sphere’ (Buzan, Waever and de Wilde, 1998: 4). Should cryptocurrencies really be feared and be subject to special measures? Or after more than ten years in existence, should they be desecuritised (if a securitisation has taken place), with the focus shifting to other more pressing threats? The timeliness of a threat, therefore, is a relevant factor to consider.

Securitisation can also be constricting. With the form of money changing so much in the last fifty years, there is an argument for allowing ‘economic Darwinism’ to see if cryptocurrencies survive through value and use as a technology. But if the state intervenes, and in several countries cryptocurrencies have even been banned, then the constriction of securitisation can stifle technological development, marketplace growth, user adoption, and impact people who might find a genuine need for cryptocurrencies. For example, Bitcoin offers a faster and cheaper way to send funds globally than existing traditional finance (Butler, 2019: 332). In developed countries, citizens enjoy relatively stable currencies, accountable governments, and a reliable banking infrastructure – the same cannot be said for much of the world. There are, then, many who might benefit from what cryptocurrencies have to offer. As with the ‘War on Terror’, constriction can be negative for financial inclusion and more impactful on vulnerable members of society (Amoore and De Goede, 2005: 155-56). Tightening ‘Know-Your-Customer’ (KYC) regulations, for example, can make it harder for poorer groups to access finance, as they may not have passports or driving licences (155).

There is also another dimension of securitisation to explore. Through extraordinary means, the securitising actor claims protection of a referent object that is facing an existential threat. In the case of cryptocurrencies, though, what is the object? Who or what is being protected? The state, society, or its citizens perhaps? Cryptocurrencies are also interesting in that they can be counter-securitising. That is, some people use them to protect themselves *from* the state. There is an irony and paradox here. For some people, cryptocurrencies can offer protection from the financial mishandling of the economy by the state - there have been countless examples throughout history of currencies suffering hyperinflation causing great upheaval (Cagan, 1989: 179). Furthermore, during the Great Financial Crisis, for example, companies and individuals were even denied access to ‘their’ funds. Cryptocurrencies may offer a way for some people to have sovereignty for their money, free from interference by the state – the very organisation tasked with protecting them.

The use of securitisation theory, as shown, provides effective language and a coherent, central structure around which to discuss the debates about the use of cryptocurrencies and the security threat that they potentially pose. It also brings precision and clarity to the dialogue of cryptocurrencies, where much of the discussion currently lacks depth and rigour. This thesis, then, will uniquely apply the lens of securitisation theory to Bitcoin and cryptocurrencies to analyse and answer the many questions highlighted in this section. Have cryptocurrencies been 'securitised' – that is, has a representative of the state labelled them as a threat and, crucially, has the wider public accepted that they are a threat? If so, who has securitised them, what exactly is the threat, and what is it that is being protected? Cryptocurrencies are often presented as a security threat in the media but are they a pressing one, and to what extent is time an important factor in whether something even qualifies as a threat?

This study will, therefore, explore whether an attempted securitisation of cryptocurrencies has taken place. There will be an examination of how different actors are constructing cryptocurrencies as a security threat. There must be a discursive attempt by the state or representatives of the state to convince that an existential threat exists and the securitising actor, in a position of authority, achieves this through the 'security speech act' (Buzan et al., 1998: 40). With regards to the illicit usage narrative, the 'case' against cryptocurrencies needs examination – the headlines invariably state they are a threat, but any substantiation given must be scrutinised. This thesis will analyse this case to learn more about the threat that cryptocurrencies potentially pose.

Securitisation theory has been criticised for focussing too narrowly on the speech act and thus, through the many applications of it since it was introduced, has developed beyond this (Balzacq et al., 2016). The means of communication can include methods other than speech, such as imagery and even physical action (Kurylo, 2022). And four types of audiences have also been added to the theory: popular, elite, scientific and technocratic, where each of these 'settings explains variations in the form, content, and success of speech acts' (M. B. Salter, 2008: 322). Salter also argues that the state-centric model is insufficient for a complex, modern society and that other non-state actors can be included (2008: 324).

In the original framing of the theory, though, the discourse of politicians, government figures and other authority groups needs to be analysed and the 'analyst is obliged to question the success or failure of the securitizing speech act' (Buzan et al., 1998: 42). It may be that the headlines and media commentary referred to so far amounts only to a 'securitising move'; for to achieve securitisation an audience needs to accept it as such (1998: 25). If cryptocurrencies are indeed to some extent counter-securitising, then there is even a valid question about whether the state can ever be successful in securitising cryptocurrencies.

1.4 The Research Questions

The purpose of this study is to examine the potential securitisation of Bitcoin and cryptocurrencies. To this end, the central research question is:

> To what extent and for what reasons have the main western states or their representatives attempted to securitise Bitcoin and other cryptocurrencies?

An exploration of the following sub-questions will aid in answering the central question. These questions map to the four main empirical chapters of this thesis:

1. How are security-led narratives about the use of cryptocurrencies constructed and to what extent are they justified?

Research of this question explores the securitising speech acts of pertinent state actors regarding cryptocurrencies. This establishes what has been said about the security threat of cryptocurrencies and on what grounds. The second part of this question then aims to examine what has already been documented about the illicit use of cryptocurrencies in order to assess the validity of this threat in the speech acts.

2. What evidence is there that cryptocurrencies are actually useful for illicit activity?

Having established the grounds upon which cryptocurrencies are considered a threat and examined their illicit use specifically, research sub-question two then explores how useful cryptocurrencies are for illicit activity. This is done in a constructivist manner, by researching users of cryptocurrencies for illicit purposes to see if they find them as useful as the securitising speech acts suggest. This chapter also examines the properties of cryptocurrencies to provide a greater understanding of how they may or may not be useful in illicit activity.

3. To what extent do law enforcement opinions and experiences of cryptocurrencies support or contrast claims for their securitisation?

A similar approach is then taken to sub-question three by examining the views of law enforcement officers towards cryptocurrencies. This is important to see if they are behind the claim that cryptocurrencies are a security threat. This helps us understand whether cryptocurrencies need special treatment and must be moved out of ordinary politics to be handled with special measures, due to an existential threat that they potentially pose. Research questions two and three, therefore, capture the views of the two parties closest to and most knowledgeable of the illicit use of cryptocurrencies; the users themselves and those tasked with preventing illicit usage.

4. What prognosis is there for cryptocurrencies to play a valid role in money and society?

Research of the final sub-question moves the discussion beyond criminal usage to explore how cryptocurrencies can be a positive invention. This provides some balance but is also important if we are to consider whether cryptocurrencies are ‘more good than bad’. If this is the case, then perhaps there is an argument for the desecuritisation of cryptocurrencies. This chapter also returns the thesis to the core topic of money and further explores whether there are conceptions of money beyond state monopoly.

1.5 Chapter Structure

The purpose of this introduction was to root this thesis in the history of money and, in particular, within related debates about state money and power. Following this chapter, we move on to the literature review in Chapter 2. Here, we first examine the long history of scholarly debate about money to establish that there is a problem with the state's involvement in money. This is important as it highlights theoretical divides about money, which are intimately linked with the invention and subsequent deployment of Bitcoin. Trust emerges as a significant theme and, in the second part of Chapter 2, there is an exploration of the social science research that has been conducted on cryptocurrencies. This highlights how cryptocurrencies have been researched but crucially also then reveals the gaps in knowledge that this thesis aims to close.

Chapter 3 then sets out the methodology for the thesis. This includes my philosophical worldview, the approach taken to the theoretical framework and also the chosen strategies for inquiry. My background was fundamental to my motivation for and interest in this study and so this is discussed in detail as an exploration of my 'positionality', particularly concerning potential implications that this may have had on the research. The second half of Chapter 3 then presents the design for each of the empirical research strands which address the four research sub-questions.

The four empirical research chapters 4, 5, 6 and 7 then follow, as per the order of the sub-questions laid out in the previous section. The conclusion of the thesis is in Chapter 8. The first part reviews and discusses the findings of the empirical chapters. Section 8.2 then zooms out to consider the wider implications of the research in light of securitisation theory in the economic sector and the central research question. The remainder of the chapter summarises the contributions made to knowledge, theory, and methodology. Several recommendations are also made as to how we might move forward from the 'security impasse' that there appears to be regarding the use of cryptocurrencies. And finally, the thesis finishes with a look forward to the unanswered questions and future work that it is very much hoped other researchers may find cause to explore.

2 Literature Review: Money, Cryptocurrencies & Trust

Money is ‘the pivotal institution of modern capitalism’ (Ingham, 2004: 18). Yet, debates about the form of money, its politicisation, and even about what it is, have persisted for millennia (Ingham, 2020: 3). As much as money is an enabler of society, it has also been viewed as a perennial source of evil (Ferguson, 2008: 1-2). Should money be abolished altogether or could it be transformed to become a ‘means of improving society’ and achieving ‘monetary utopia’ (Dodd, 2012: 146-147)? Theory remains divided. However, amongst the many dualisms and conflicts, there is a common theme that emerges: the *problem* of the state’s involvement in money. In Chapter 1, the Bank Restriction Act of 1797 was identified as the genesis moment from which debate about (modern) money has been fought ever since. The severing of the conversion of paper money into gold broke trust in state money and laid bare once more a perennial issue – the debasing of money by those in power.

This literature review will be split into two broad parts. The first part examines the scholarly and theoretical history of modern money (from 1797 onwards). A great deal of this literature is from the late nineteenth and early twentieth centuries when monetary issues were prominent intellectual concerns. This literature is often more conceptual and philosophical, rather than having an empirical focus. But the arguments and theories examined still underpin modern thinking about money. Even though times and technologies have changed, there remains much to draw on from this literature, and their principles and arguments can be equally applied to modern monies, including cryptocurrencies. This theoretical literature on money is important to this thesis as Bitcoin was created as a new money, free from state control. But Bitcoin is questioned as even a form of money. This section will also, therefore, delve more deeply into this specific question to understand philosophically what money is, and whether Bitcoin meets this conception. Theory about money is important context, not just in terms of what it is but also in its relation to society. As such, this first part of the review highlights the important concepts, theories and controversies in money that underpin the analysis and framing of this thesis. Much of this section was published as an article in *Theory, Culture and Society*, titled, ‘The Philosophy of Bitcoin and the Question of Money’ (Butler, 2021).

The second part of the literature review will then move on to consider the recent body of academic work on cryptocurrencies that has emerged in the short period (in monetary terms) since Bitcoin went live as a system in 2009. Here, the focus is on more empirical and primarily sociological research, rather than purely economic or technical, as this thesis explores the usage of Bitcoin and cryptocurrencies and considers the security threat that they potentially pose. This research is more disparate than the first part of this review and concentrates on the studies of cryptocurrencies that have taken place, their methodologies, strengths and weaknesses. Some of the literature is drawn from work focussed on money, but there is also a large amount of cross-disciplinary work on cryptocurrencies. As such, it is not so easy to define the research in terms of schools of particular thought. It may be that cryptocurrencies are still a relatively new phenomenon and so the literature does not group together as clearly as the theoretical work on money. However, it is in this part of the literature review that the inconsistencies and unanswered questions in the existing research on cryptocurrencies are uncovered. The review closes with a summary of the research gaps that are identified from this analysis.

2.1 What is Money? The Fundamental Clash

Since 1797, there has been a tremendous development in economic thought. And this thinking is not the preserve of the field of economics, with a great deal of the advances and influence coming from wider areas within sociology. It is not possible, therefore, or necessary to discuss every aspect of this thought in this review. The intention instead, is to focus on some of the key clashes of position, as they relate most closely to Bitcoin and cryptocurrencies as new forms of money.

For centuries, the main divide amongst monetary scholars has been *commodity* versus *claim (credit)* theory. For commodity theorists, money emerged from barter, as an object to exchange with and value other commodities. Cows, salt and even shells were used as money (Menger, 1892: 239). However, precious metals soon became the commodity of choice, as they were durable and enabled division and reconstitution. Commodity theory expressed itself as metallism, where sound money is based on the scarcity of precious metals ‘with intrinsic value’, such as gold. This is also the classical view of money in economics, as merely a ‘medium of exchange’. Claim theorists, however, view money in an abstract sense as a ‘claim, or credit, measured by a money of account’ (Ingham, 2006: 260 and 2020: 9). Money is more than a technical device, with a ‘life and an importance’ of its own (Schumpeter, 1954: 265); or to Ingham, money is ‘a dynamic independent economic force’ (2020: 5).

Metallism, however, dominated the late seventeenth century and was advocated by the likes of John Locke, a key philosopher in the Age of Enlightenment (Ingham, 2020: 18). It was during this period that King William III of England passed the act to raise funds for war against France, leading to the formation of the Bank of England in 1694. The bank issued promissory paper notes, which could be redeemed for precious metal ‘to the bearer and on demand’. This was effectively still a metallist system, with the paper ‘representing’ the underlying precious metal. But, following further concern over revolutionary France, the Bank Restriction Act was passed in 1797 and the bank suspended the conversion of notes into gold (O’Brien & Palma, 2020). This was a watershed moment (as already discussed) - trust that paper could be exchanged for precious metal was broken, and it was the state that broke this trust. It was the breaking of the metallist link by the Bank Restriction Act that enraged the likes of William Cobbett and led to increased intellectual thought on the subject of monetary policy throughout the nineteenth century. Here, the British Currency School, including famous economists such as David Ricardo, supported metallism in opposition to the British Banking School who favoured credit for the stimulation of the economy (Ingham, 2020: 31).

Again, each school adopted a position opposite to the other. Ever since, debates have followed about commodity versus claim theory, the merits or otherwise of a gold standard, fiat currencies and various new, competing theories of ‘what to do’ with money. The problem with these debates is that they are often presented in this binary fashion as if the theories and logic of each are exclusive of the other and that one must be incorrect for the other to stand. But this is too restrictive for money, which varies greatly over time and societal sophistication. Thus, there are ways in which they are both right. Moreover, as will be shown below, while it is important to understand these debates, there are more pressing issues that need consideration, particularly in relation to cryptocurrencies, such as the state’s involvement in money.

2.1.1 Social Or State Money

Whilst commodity versus claim theory represents a broad clash of ideals with regard to what money is and its form, several schools of thought vary in their theoretical position about the role of the state in money. And this is the other key divide which underpins the consideration of Bitcoin and cryptocurrencies in this thesis. In short, should money be the preserve of the state, or can other forms of money have a role to play? The Bank Restriction Act highlighted a long-standing area of contention - that weakness in the form of money enables those in power to debase it, to their advantage. In the era of precious metals, coins were physically debased, and, with the advent of paper notes, the same effect was achieved by printing more notes than were backed by gold. As Adam Smith, the renowned classical economist, puts it in *The Wealth of Nations* of 1776:

> The avarice and injustice of princes and sovereign states, abusing the confidence of their subjects, have by degrees diminished the real quantity of metal… to pay their debts and to fulfil their engagements. [This is]… favourable to the debtor… ruinous to the creditor, and… sometimes produced a greater and more universal revolution in the fortunes of private persons, than could have been occasioned by a very great public calamity. (Smith, 2007: 25-26)

Despite protests, as exemplified by William Cobbett in Section 1.1.1, the state became increasingly involved in the creation and control of money following the establishment of the Bank of England, and paper money became widespread. Yet, if Smith notes that those in power abuse and misuse money, then it is right to consider the form of money and to question who should be responsible for this critical societal institution. It is notable that these are the same issues that William Cobbett questioned from his jail cell in 1810. It seems that money persists, even to this day, as a largely unresolved social phenomenon.

Even at the end of the nineteenth century, Carl Menger, an influential Austrian economist, claimed in *On the Origin of Money*, that there was still no satisfactory theory of money (1892: 240). Menger questioned the phenomenon of why we would accept a given commodity as money. He argued that ‘in the very nature of things’ there was a natural ‘degree of saleableness of commodities’ and that it was in the interest of rational man to accept the most saleable commodity as a means of exchange (1892: 242, 248). And at that time, precious metals were the medium of exchange as they were the most saleable commodities.

The other key concept Menger offered was that ‘money has not been generated by law [and] in its origin it is a social, and not a state-institution’ (1892: 255). This was an important theoretical distinction that stood in contrast to other schools of thought at that time. Indeed, Menger’s work served as the foundation for the Austrian School of economic thought, which argued that individual motivations lay at the heart of economic actions. In a period known as the *methodenstreit* (‘method dispute’), there was a fierce debate between Menger and the Austrian School and the opposing German Historical School. Among the members of the Historical School was Georg Friedrich Knapp who, in 1905, published a book called, *The State Theory of Money*. Here, Knapp argued the opposite to Menger - that ‘money is a creature of law’ and the ‘soul of currency is not in the material… but in the legal ordinances which regulate their use’ (Knapp, 1924: 1-2). This approach to money came to be known as Chartalism, a phrase coined in the book (87). In this vision of money, ‘monopoly of coercion’ over territory and money, based on control of the money of account, are essential elements of a state (Ingham, 2020: 32). The state decrees what is money and what can be used to pay taxes and debts, rather than the emergence of some commodity. This theory takes a very limited view of the sophistication of society – that state money should be accepted by the population even if it is of a poor form. But if those in power often abuse money, then why should people accept it if it is not to their benefit? If money is social in its origin, then it seems draconian, undemocratic even, to require coercion and decree to enforce the use of state money, rather than allowing choice based on the merits of one money over another.

By the early twentieth century, then, the thinking about money was divided into parallel strands of theory. On the one hand, was a split about whether money is a commodity or an abstract claim. And on the other, whether money was a social or state institution. Both these strands of theory are incredibly important to the consideration of Bitcoin and cryptocurrencies. If Bitcoin, for example, is neither state-backed nor tied to a commodity, then what is its 'value'? And what does value mean in any case? This is, after all, an argument that some have against Bitcoin as a money – that it is valueless. As such, it is important to examine this in some further detail.

2.1.2 The Philosophy of Money

The twentieth century was a crucial period for economic thought. Mixed amongst some of the theories already mentioned was a questioning of the relationship between money and 'value'. This relates to the two main theoretical divides; does a commodity bring value to money or is it a state decree? Karl Marx's labour theory of value provided an alternative conceptualisation, where commodity value could be determined by the labour hours needed to produce them – 'abstract human labour' (Lapavitsas, 2017: 222). This Marxist monetary theory had its roots in classical economics but theory evolved into a subjective theory of value, as seen by Menger and the Austrian School (von Mises, 1998: 3). Here the value of a good is not determined by its utility nor by the labour involved in its production, but as a determinant of the individuals who are buying and selling the item. The logic here helps explain the paradox of why an item can be less useful than another, yet more valuable. Again, it can be argued that there is a weakness in thinking that only one of these theories can be correct, rather than there being elements of each that are logical depending on the circumstances. It makes sense that the cost of production can be related to prices, but it also makes sense that there are forces at play on prices beyond this, such as the views of the buyer and seller. To fully understand and be open-minded about Bitcoin, we must think more broadly than the narrow constraints of individual theories.

In this light, it can be argued that Bitcoin has value through the costs involved in its production. Hayes, for example, shows that the marginal cost of production is related to prices and argues that Bitcoin has intrinsic value through the intangible computational labour expended in the mining process (2017; 2018). Or taking a subjective value approach, the market is indicating that there is certainly value to Bitcoin as many people are buying and selling it.

Questions about Bitcoin and cryptocurrencies in terms of value and utility are crucial to debates about their very existence. And so, these aspects must be given a thorough examination. To do this, I analysed Bitcoin using Georg Simmel's seminal book of 1900, *The Philosophy of Money*. Simmel was a leading German sociologist, and I found his work to be particularly insightful and useful for analysing the value and utility that Bitcoin may have as money. These are critical concepts for the remainder of the thesis.

Chapter One of The Philosophy of Money – 'Value and Money'

Value

That Bitcoin has no 'value' is an oft-used criticism in popular discourse, that speaks to commodity versus claim theory (K. Torpey, 2017). But does money need to have 'value'? And what is value anyway? In chapter one of *The Philosophy of Money*, Simmel notes that 'an object does not gain a new quality if we call it valuable; it is valued because of the qualities it has' (2004: 57). Value, therefore, is not a quality of an object, but a judgement of an object made by another (60). To those that say that Bitcoin has no value, they are correct – but then no object, including gold, has intrinsic value either. Value is a subjective assessment. Another simple way to think of this is that value is not fixed and inherently measurable, unlike an actual quality of an object, like weight. It is a unit of measurement, and like all our abstract measures – 'no one has ever seen an ounce or a foot or an hour' (Mitchell-Innes, 1914: 4). Whether the form of money is Bitcoin, gold or fiat, money has no intrinsic value and our practical notions of value only appear as one item is exchanged for another.

Utility and scarcity

Some claim Bitcoin has no utility, whilst proponents often cite its scarcity in contrast to fiat currencies (Butler, 2019: 332). Simmel describes scarcity as supply, a quantitative relationship between an object and the total available, but it is utility that ‘appears as the absolute part of economic values’ (2004: 88). Interestingly, for Simmel, utility is ‘the desire for the object’; it is not about *usefulness* but rather economic activity as a result of demand. In fact, Simmel observes that ‘we desire, and therefore value economically, all kinds of things that cannot be called useful or serviceable’. And so, if usefulness is all that is in demand, we must accept that it is demand that is the driver of economic activity (Simmel, 2004: 88-9). Furthermore then, we realise that not all useful objects are in demand. A tree in a remote forest has *uses* for fire or as a building material but, in that context, there is no demand for it, therefore no utility, and no economic activity. The claim, therefore, that Bitcoin has no utility is not valid according to Simmel. There is great demand for Bitcoin and so great utility, as it is driving the exchange of many objects and an enormous amount of economic transactions. This view aligns closely with the Austrian subjective theory of value. It seems quite clear then that our notions of value and utility must move beyond the narrow conceptions of money as a commodity. The views of the people involved with a system are just as important, if not more so than the materiality of any given money.

Chapter Two of The Philosophy of Money – ‘The Value of Money as a Substance’

Intrinsic Value

So does money need ‘intrinsic value’, achieved through some commodity, or ‘is it enough if money is simply a token’ (Simmel, 2004: 129)? Simmel concludes the latter (130), countering the argument that Bitcoin fails as money as it has no intrinsic value. As a simple explanation of Simmel’s logic, let us assume there are a total of ten eggs and ten dollars in the world. It follows that we can calculate a value for one egg i.e., one dollar, without the dollar requiring intrinsic value itself. Luther took Bitcoin’s existence to question Mises’ Regression Theorem, but this was refuted by Pickering (2019: 608) who argues that the theorem explains ‘the purchasing power of money using the subjective marginal utility theory of value’, not which commodities can emerge as money. Again, this is important, as the literature shows that too many academics are focussed on whether one theory is correct and the other wrong, rather than appreciating some of the value in each. There are times in societal development when commodity money made the most sense and other circumstances when credit theory monies work best.

For example, primitive economies began by using items of value for money but, Simmel argues, at that stage of an economy it would hardly be possible to do anything else. Who would accept a worthless piece of paper in exchange for something valuable like cattle? Money with value may have been a necessary starting point but society and money have evolved to move beyond needing this readily exchangeable value. Coins in a pocket do not have value because the metal can be used elsewhere (Simmel, 2004: 141). Even today, ‘metal money stands on an equal basis with paper money as a result of the growing psychological indifference to its value as metal’ (141). The substance of money is not important – depending on where society is in its evolutionary use of money. In this regard, fiat proves that something without intrinsic value can be money. Fiat does not have a link to precious metals and yet still functions as a medium of exchange. In the same way that it does not matter if a ruler to measure distance is made from plastic, wood or metal, ‘so the scale that money provides for the determination of values has nothing to do with the nature of its substance’ (Simmel, 2004: 146). And the movement from objects of value to ‘symbol’ money is a marker of cultural development (146). Indeed, for Simmel, the growth of intellectual ability in society and the development of abstract thought is characterised by the development of money closer and closer to a symbolic form, without intrinsic value (150). We must consider therefore whether Bitcoin represents an evolution in monetary sophistication. Has society moved forward to a point where existing monies are no longer the most appropriate form?

Furthermore, Simmel argues that even the most useful object has to give up its usefulness to function as money (151). That is, you cannot use gold for its other purposes when it is being used as money. This comes at a cost – if gold was no longer used as money, then there would be plenty for its other purposes. In this way, hoarding gold contributes to its value and makes it expensive for its other uses (154).

The argument that gold is a better form of money than Bitcoin as it has other uses, is not correct according to the philosophy of Simmel. Finally, there is an informal logical fallacy, *petitio principii*, in the argument. The premise that good money has other uses is assumed (whilst Simmel argues the opposite) and used in circular reasoning to declare that gold, therefore, is good money as it has value/other uses. Bitcoin and fiat pass the Simmel test for a pure money, gold does not. Having other uses does not make something a better money - according to Simmel, it makes it worse. If this is the case, then any persistent claims for a commodity such as gold to be the basis of money must surely now be discarded. Money should be of a token form – but it needs to be able to resist the abuse and misuse of those in power.

Money as a Symbol

Given, then, that gold is not the best form of money and that fiat passes the Simmel test, why would there be any need for Bitcoin? The problem, as noted earlier, lies in the state's misuse of money:

> Although, in principle, the exchange function of money could be accomplished by mere token money, no human power could provide a sufficient guarantee against possible misuse. The functions of exchange and reckoning obviously depend upon a limitation of the quantity of money, upon its 'scarcity'. (Simmel, 2004: 158)

Even though Simmel thought that pure token money was 'conceptually correct' (163), he did not think it was 'technically feasible' to detach money from a commodity like gold which limited supply, due to the propensity for misuse. Simmel may have been sceptical about 'discovering complete solutions to money's problems' (Dodd, 2012: 148) but he believed that 'the actual development of money suggests that [a pure token money] will be the final outcome' (Simmel, 2004: 163-4). The problem for Simmel, writing in 1900, was that 'no human power' would be sufficient guarantee to prevent misuse, which is why the power of the laws of nature governing the scarcity of gold was relied upon instead. Bitcoin, though, has shown that there are now other 'technically feasible' solutions – supply can be controlled by the power of code, preventing misuse by the state. Society, then, has evolved to a point that age-old problems in money can be solved effectively, without an outdated, ineffective and theoretically incorrect recourse to a commodity.

It is therefore scarcity or the control of *supply*, that is the real issue in money. This is supported by the writings of Simmel, and many of the other thinkers discussed in this thesis, through the numerous examples of state abuse of the supply. The literature shows that there has been a distraction and incorrect focus on whether money is of a physical or abstract form. And it is here that Bitcoin differs from fiat state money, even though both are pure token forms. Simmel, like others, makes the issue of abuse clear, here in reference to the Cantillon effect, where those who issue money benefit from spending money before prices have a chance to ‘catch up’:

> The numerator of the money fraction—the price of commodities—rises proportionately to the increased supply of money only after the large quantities of new money have already been spent by the government, which then finds itself confronted again with a reduced supply of money. The temptation then to make a new issue of money is generally irresistible, and the process begins all over again. I mention this only as an example of the numerous and frequently discussed failures of arbitrary issues of paper money, which present themselves as a temptation whenever money is not closely linked with a substance of a limited supply. (Simmel, 2004: 158-9)

This is where the core issue of money becomes political. When the money supply increases prices likely follow. But this is not instantaneous; ‘shocks, hypertrophy and stagnation’ occur because money is spread ‘in an uneven and inappropriate manner’ (160). And this is the fundamental issue with state money – how much new money is created and, crucially, who gets it. Simmel wrote that if everyone received an equal share of new money then ‘no one would gain any advantage’. But this is not what happens, and this is why Bitcoin has emerged, to use some of Simmel’s words, to protect ‘against political crises, party interests and government interference’. The conception of statists, then, is too pure, too utopian in thinking that the state can manage and distribute money best, and fairly. The evidence is to the contrary and aligns with the Austrian economic calculation problem. If the state cannot manage the fluctuations of an economy effectively, then it is also unlikely that it can manage the supply and distribution of new money effectively either. It is only logical, therefore, that new conceptions of money are developed and considered to better manage these functions for society.

The issue of money then is not about a clash of commodity theorists and claim theorists; as Ingham puts it, ‘the legacy of commodity theory and metallism’s misunderstandings of money should now be laid to rest’ (2020: 40). These debates are a distraction from what matters. Bitcoin is money, just as fiat and gold are. It has been necessary to argue extensively about why Bitcoin *is* money, not to say that we should use it as money, but to remove this area of debate from our remaining consideration of the money question, the political dimension. This, I argue, is where the money question solely relates to the information age and this point will be returned to in Chapter 8.

2.1.3 The Memorable Alliance

It was in the fifteenth and sixteenth centuries that our ‘distinctive capitalist monetary system’ first emerged (Ingham, 2020: 66). During this period, there had been an intensifying tension between sovereigns and the bourgeoisie over the control of money, financing for war and the settlement of debt by the state. And it was default by Charles II to London merchants that in time led to the ‘Glorious Revolution’ of 1688 and the crowning of the Dutch Prince of Orange as King William III (67). This was a key moment in the history of money, as the throne came with an agreement that established the Bank of England in 1694 as a mechanism to loan William money (for war). £1.2 million was loaned to the King, who promised to pay it back. The Bank then took that ‘promise’ as an asset on which it could then issue banknotes – in effect ‘doubling the creation of money’ – the King’s debt was now the National Debt (67). And it is this financing of the state by a small group of capitalists (here, the merchants who set up the Bank of England) that defines our modern states as ‘literally capitalist states’ (67). Ingham quotes Marx, further highlighting the problem of the state in money:

> As with the stroke of an enchanter's wand, [the public debt] endows barren money with the power of breeding and thus turns it into capital, without the necessity of its exposing itself to the troubles and risks inseparable from its employment in industry or even in usury. The state creditors actually give nothing away, for the sum lent is transformed into public bonds, easily negotiable, which go on functioning in their hands just as so much hard cash would. (Marx as quoted in Ingham, 2020: 68)

Our capitalist monetary system to this day is primarily concerned with this relationship that came to be in the seventeenth century between the three key parties at the heart of state money creation: the state/government, the central bank, and the private bankers. Ingham, a prominent modern sociologist, refers to this trio, and the ingrained relationship between them in modern capitalism, as the 'memorable alliance' (Ingham, 2020: 72). For all the parties involved, this has proven to be a very profitable business. The private bankers earn interest from the state through their privileged position, and the state and the central bank profit from seigniorage and enjoy access to endless funding (leading to a current parabolic increase in debt). The alliance eased the tensions of the fifteenth and sixteenth century, and the relationship continues to this day as the foundation of modern state money creation and control. But just because this is how money has been controlled for hundreds of years, does not mean that this is necessarily an efficient, fair or optimal method of doing so.

The theoretical positions, of commodity theory and metallism versus credit theory, and the Austrians versus the State theorists, provided the intellectual framework as the debates about money moved into the twentieth century. Here, war again rose to shape the course of monetary events and thinking. In 1914, at the outbreak of war, there was a repeat of the aftermath of the Battle of Fishguard some 117 years earlier, as panic led to a run on the banks and a suspension of convertibility. This also saw the first time that the Treasury issued money directly, rather than through the Bank of England (Ingham, 2020: 71). Significantly, the bankers were not happy with this issue of 'interest-free' money, and they 'insisted' that government debt should be funded by the private sector at a rate of interest, as was customary since the establishment of the Bank of England and the modern capitalist monetary system. They wanted the ‘memorable alliance’ of the state, the central bank and the banking system to remain the primary mechanism for the production of money (for discussion see Ingham, 2020: 65-85). This is merely a logical expression of self-interest. No entity that enjoys a privileged profit-making arrangement is likely to call for its end. Bitcoin, and other cryptocurrencies, represent issues of money outside the old alliance that would, amongst other things, challenge this money-making arrangement.

Metallists had fought for orthodoxy, as the gold standard came and went, but this was challenged by the likes of Keynes who had emerged as a leading economic thinker. In his 1923 work, *A Tract on Monetary Reform,* he famously claimed that ‘the gold standard is already a barbarous relic’ (Keynes, 1923: 172). Redeeming notes for gold was again under threat as global capitalism expanded. But even Keynes acknowledged that the consistent devaluation of money throughout history was not an accident and that there were two great forces behind it: the ‘impecuniosity of Governments and the superior political influence of the debtor class’ (Keynes, 1923: 9). The influence of the memorable alliance is clearly not to the advantage of everyone.

Yet, Keynes argued that the gold standard was old-fashioned and that it no longer gave stability, with a value that now depended on the United States’ Federal Reserve Board. Gold was no longer free from the dangers of a managed currency and the United States would not let its value fall in depreciation of its standard. We see here a seemingly inescapable paradox of money; that metal restricts spending, but without it, confidence in government money falters. Even Knapp, whose work introduced Chartalism, described paper money as a ‘degenerate’ and even ‘dangerous’ form (1924: 1-2). Keynes may have lost confidence in gold, but the age-old problems of money persisted:

> It is natural, after what we have experienced, that prudent people should desiderate a standard of value which is independent of Finance Ministers and State Banks. The present state of affairs has allowed to the ignorance and frivolity of statesmen an ample opportunity of bringing about ruinous consequences in the economic field. (Keynes, 1923: 169)

The memorable alliance has been at the heart of the capitalist system for centuries. And it has been a profitable alliance to be part of. It offers endless funding for governments and endless profits for banks. But the cost is a devaluation born by the rest of society. And the extent of the abuse and misuse of this privilege has resulted in a consistent history of economic disaster, which has had its theoretical detractors.

2.1.4 Fiat Money and the Austrian School

History shows that money *can* be a physical commodity (shells, stones or precious metals) or that it *can* be abstract (an IOU, a digital form or a bank note). Whilst debate is often about which form is 'best', the important point for discussion and analysis is the *impact* that those choices of the form of money have.

Dropping the gold standard in 1931 enabled a move from orthodoxy and a move from the scarcity constraints of precious metals. In the US, the 'great contraction' of the early 1930s saw 10,000 bank failures; consumers lost deposits, shareholders lost equity and a crash in banking deposits and loans ensued (Ferguson, 2008: 163). In an open letter to President Roosevelt in 1933, Keynes argued his heterodox position; that the 'public authority must be called in aid to create additional current incomes through the expenditure of borrowed or printed money' (Keynes, 1933). The state should step in when the consumer and business could or would not. Again, this seems a reasonable proposition, but the issue with this is that it relies on an assumption that the state can successfully intervene without misuse or unintended consequences. Regardless, these Keynesian economic thoughts became the foundation of Keynesianism, which dominated thinking in the middle of the twentieth century. Whilst not Chartalist in the sense of state money, Keynesianism did advocate for state intervention and state spending. In these ways, the Keynesian school of thought was opposed by the Austrians, who believed that central planning did not work and that the market was the best allocator of resources.

Keynes also criticised the Quantity Theory of Money, a long-contested economic theory most commonly associated with Fisher's 1911 equation of exchange, where prices levels are directly proportionate to the quantity of money in circulation:

> MV=pQ (where M = supply of money, V = the velocity of circulation of money, p = price and Q = quantity) (Fisher, 1922: 25)

Put another way, 'quantity theory' showed that an increase in the supply of money leads to an increase in prices, or inflation (ceteris paribus). Keynes argued that there was a mistaken belief 'that output and income can be raised by increasing the quantity of money… but this is like trying to get fat by buying a larger belt' (Keynes, 1933). The key was the 'volume of expenditure, which is the operative factor'. Keynes reiterated his support of managed currencies but believed that 'a profound change of methods' was necessary. The problem with Keynes's rationale though is that it isolates changes in demand from increases in the money supply and detaches any nominal increase in prices from any increase in the money supply. It may well be correct that an increase in the money supply would not, for example, increase the demand for food, but it does alter the purchasing power of existing money and thereby distorts notions of prices. These effects should not be discounted, and these changes are disadvantageous to those not in power.

The Bretton Woods system post-1944 worked well for a time as the world recovered after the war, enjoying growth and low unemployment. But questions over the new world order grew, with the French Minister of Finance famously describing the position of the US dollar as 'an exorbitant privilege' in 1965 (Ingham, 2020: 74). This was also a period of support for Keynesianism and the beliefs that governments can spend ahead of taxation and that this expenditure would raise the total amount spent in the economy (aggregate demand). The belief was that through monetary and fiscal policy, the business cycle can be smoothed and managed. Connected to this, is also the concept of the 'fiscal multiplier'. This can be defined as a measure of the 'short-term impact of discretionary fiscal policy on output'; or, more simply, as a measurement of the effect of a $1 change in spending or tax revenue on GDP (Batini et al., 2014). Importantly, with regard to Keynesianism, is the notion that a $1 spend by the government could return more than a $1 increase in GDP. Subsequently, multipliers are an important consideration in terms of fiscal policy design and the forecasting of the impacts that spending may have. (The fiscal multiplier is frequently attributed to a student of Keynes, even by Keynes himself in *The General Theory of Employment, Interest and Money* (Keynes, 1936), but others claim this is a myth and that Keynes actually introduced the multiplier in his 1921 work, *A Treatise on Probability* (Brady, 2020)).

The Bretton Woods international monetary system effectively concluded with the Nixon Shock of 1971, when the United States suspended the link of the dollar to gold. The end of representative money (with a claim on a commodity such as gold) ushered in the era of fiat money, which continues to the present day. Governments with fiat currencies have since been able to expand the supply of their money at their will. The result is the potential for greater currency devaluation – as a reminder, the US dollar lost 87 per cent of its purchasing power between 1957 and 2008 (Ferguson, 2008: 63) – and an explosion of national debt, which can be seen in Figure 1:

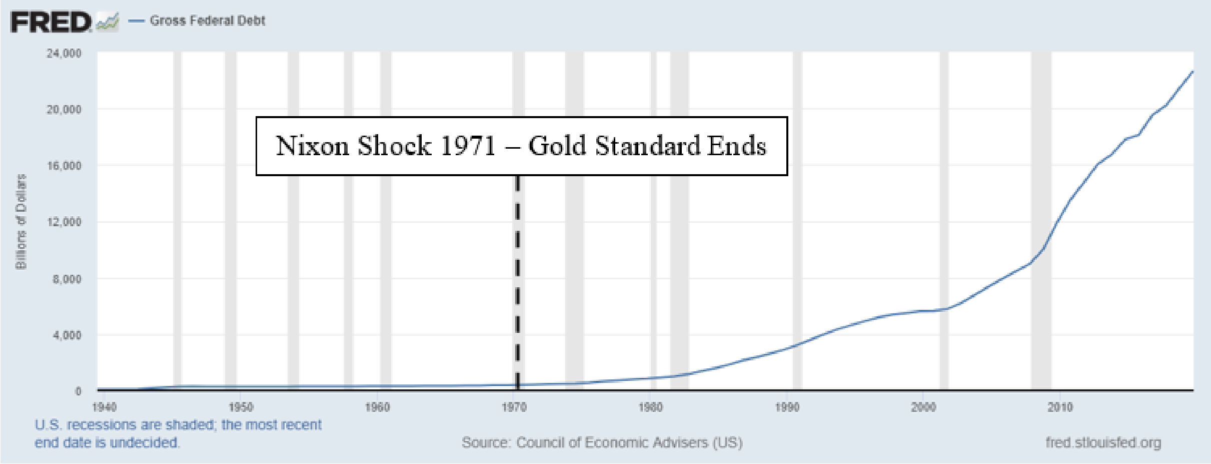


Figure 1: US Gross Federal Debt (Council of Economic Advisors, 2020)

There were, of course, objectors to Keynesianism and the new world order dominated by the US dollar. Prominent amongst these were generations of the Austrian School of economics of the twentieth century. Mises, in his 1920 work, *Economic Calculation in the Socialist Commonwealth,* wrote, in reference to socialists, that, 'economics… figures all too sparsely in the glamourous pictures painted by Utopians' (xvii). He defines socialism as where 'the means of production are the property of the community', rejecting it as 'the abolition of rational economy' (1 and 23). For Mises, central planning does not work, due to the 'problem of economic calculation' (38). The failure of socialist economies since appears to support his thesis.

> Every step that takes us away from private ownership of the means of production and from the use of money also takes us away from rational economics. (von Mises, 2012: 17)

Prior to this work, Mises had already published *The Theory of Money and Credit* in 1912 but an English version only appeared in 1934, a year after the New Deal in America had already begun and with it major works of Keynesian spending. In a preface to a 1952 edition, Mises noted that 'sound money [had given] way to progressively depreciating fiat money' and that 'all countries are today vexed by inflation and threatened by the gloomy prospect of a complete break-down of their currencies' (von Mises, 2009: 9). He also observed that:

> The great inflations of our age are… government made. They are the off-shoots of doctrines that ascribe to governments the magic power of creating wealth out of nothing and of making people happy by raising the 'national income'. (von Mises, 2009: 9)

Weber, too, in *Economy and Society*, had also warned that 'there is no denying that any inflation with the issue of paper money determined by financial needs of the state is in danger of causing debasement of the currency. Nobody, not even Knapp, would deny this' (1978: 192). Mises made no mistake in his intention to 'explode the basic inflationary fallacy that confused the thinking of authors and statesmen from the days of John Law down to those of Lord Keynes'. Indeed, Mises makes a mocking reference in what appears to be an oft erroneously interpreted quotation of Keynes; that, 'in the long run we are all dead'. This quotation from Keynes's *A Tract on Monetary Reform* is incorrectly taken to mean that Keynes cares only for the short term. That is, in reference to spending, we can spend today and should not worry about the longer-term impacts. This misses the context of the quotation, which is about quantity theory, where Keynes accepts that ‘in the long run’ a doubling of the money supply may double prices:

> But this long run is a misleading guide to current affairs. In the long run we are all dead. Economists set themselves too easy, too useless a task if in tempestuous seasons they can only tell us that when the storm is long past that the ocean is flat again. (Keynes, 1923: 80).

Keynes is arguing that even if increasing the money supply eventually raises prices, it may not do so for some time. Or, as he later describes, ‘there is a certain friction which prevents a moderate change in (money supply) from exercising its full proportionate effect on (price)’ (81). Rather than indicating a preference for the short-term, Keynes is advocating for early intervention. And perhaps this is where another flaw in the literature is revealed. That there is a widespread belief that Keynes argued there would be little consequence to intervention. It is not that Keynes thought there would be no consequences, but rather that in the meantime governments could be relied upon to successfully manage the economy and lessen the effects of economic downturns. These are very different propositions, and we would do well to focus more clearly on the impacts, and success, that any intervention may have because this really is the justification for intervention in the first place. If interventions are not successful, then outcomes would be better without them.

Whilst Keynes thought of the gold standard as a barbarous relic, Mises could see no other way, then or in the future, of ‘emancipating the monetary system from the changing influences of party politics and government interference’ (von Mises, 2009: 20). Both saw problems, but a solution to the question of money remained elusive. In *The Road to Serfdom*, Hayek, another prominent Austrian economist, wrote that ‘economic freedom… is the prerequisite of any other freedom’ (Hayek, 2005: 35). Published at the end of World War II in response to the rise of the Nazi Party, a national socialist party, Hayek argued that it was not a ‘wickedness’ of the German people that led to Nazism, but rather that this was a tragic consequence of the rise of central planning and the huge (state) power needed to further socialist ends. He saw democracy as an ‘obstacle to [the] suppression of freedom’ that central planning requires, out of which ‘arises the clash between planning and democracy’ (40). And this is the heart of the clash between the Austrian economists and the Keynesians; individual freedom and the ‘competitive system’ versus the directed actions of powerful, centralised planners. There is certainly a central paradox here, particularly in modern, Western societies; democracy, competition, and freedom to choose are encouraged – but only as long as this does not stray into the realm of money. Here, the argument is for state money, monopoly, suppression of choice, coercion, decree and the force of law. The clash and incompatibility of these positions is stark, and of course, relevant to discussion of cryptocurrencies.

The removal of the final vestiges of the gold standard in 1971, left the US in an increasingly dominant position, and demand for dollars enabled a growing deficit. In the UK, inflation soared and reached 26 per cent by 1976 (Ingham, 2020: 77). In the same year, Hayek wrote, in the *Denationalisation of Money*, of his ‘despair’ and ‘hopelessness’ in finding a political solution to inflation (Hayek, 1990: 13). And he saw ‘the age-old government monopoly of the issue of money’ as the chief cause of recurring depressions and high unemployment (14). Private industry, he believed, could provide the public with a choice of currencies in satisfaction of ‘the demand for the freedom of the issue of money’. And it was in this vein that Bitcoin emerged in 2008 as ‘an entirely novel form of money’ (Ingham, 2020: 111). But will or should states allow other entities to produce money? Hayek said that government should not stop ‘others from doing things they might do better’ (17). For Hayek as well, speaking in 1984, the question remained about how to challenge the state monopoly of money:

> I don’t believe we shall ever have a good money again before we take the thing out of the hands of government. That is, we can’t take it violently out of the hands of government. All we can do is by some sly roundabout way introduce something they can’t stop. (Quoted in Harvey & Branco-Illodo, 2020)

Keynesianism may have lost favour during this latest period of unrest and inflation, but not everyone shared the views of Hayek and the Austrian School as to their solution. Aligned with them, but taking a different approach, were the economists of the Chicago School. (Indeed, Hayek was even a professor at the University of Chicago in the 1950s and early 1960s.) Chief amongst the Chicago School was Milton Friedman, whose 1963 book with Anna Schwartz, *A Monetary History of the United States*, re-established the quantity theory of money as 'monetarism'. Whilst the supply of money is linked to inflation, Friedman argued that the 'Great Contraction' of 1929 to 1933 showed the importance of monetary policy, as the Federal Reserve had failed to provide sufficient liquidity to the banking system (Friedman, 1968: 3). Monetarism, then, aimed to control inflation through the use of monetary policy. This became the dominant government strategy and can be seen to this day in central bank targets for inflation. However, instead of a gold standard limiting the supply of money through natural scarcity, monetarism offered a looser restriction based on targets. Interestingly, Friedman called for monetary authorities to adopt a public policy 'of achieving a steady rate of growth in a specified monetary total… The precise rate of growth, like the precise monetary total, is less important than the adoption of some stated and known rate' (16). Today, this target has moved to inflation of prices, as defined by a basket of goods, such as the Consumer Price Index (CPI). But these are very different subjects of policy. Inflation of the money supply has morphed into an arbitrary and manipulatable definition of inflation of prices. And this illustrates the problem with the monetarist approach; it once again relies on those managing the system to do so in a controlled way, that does not lead to abuse and misuse. The literature shows us that this can in no way be guaranteed, as long as this management is in the 'hands of man'. We still lack a sufficient monetary theory.

2.1.5 Modern Money (Theory)

Governments across the world continue to build up debt through deficit spending, as expenditure exceeds income through taxation. The existing capitalist monetary system of endogenous and exogenous money enables this to happen. Endogeneity generally means that the supply of money is linked to demand, whilst exogenous money is not (Sieroń, 2019: 329). So economic transactions, such as a bank loan for a house purchase, that lead to an increase in the money supply are endogenous, whilst money created by an external body such as a central bank or a state is exogenous (A. Hayes, 2019: 10). There are no limits to either. And the literature does not appear to adequately challenge this status quo.

Furthermore, in the case of the UK Government, for example, it *owns* the bank that it owes money to. This raises the question of what I call *Schrödinger's debt*; if you borrow money but never have to pay it back, is it *really* a debt? The system of the memorable alliance contorts our conceptions of money. The ultimate expression of this thinking is Modern Monetary Theory (MMT). Chartalist in its origin, MMT places the state and state money at the centre of the monetary system. As the antithesis of orthodox economic thinking, MMT's most important concept 'is that the issuer of a currency faces no financial constraints' (Mitchell et al., 2019: 13). That is, a country can never become insolvent and can never run out of the money that it controls the supply of. In this way, MMT argues that it does not make sense to compare the finances of a state with a household. Government should not wait for tax revenue to spend - it must spend first. 'The cult of austerity', they argue, is based on outdated gold standard logic (14). These are bold, potentially dangerous assertions that demand scrutiny.

MMT is heavily influenced by the lesser-known work of Alfred Mitchell-Innes, an 'obscure functionary in Her Majesty's Foreign Service' who only wrote two articles about money in the early twentieth century (Wray, 2004). Yet, these two articles were sufficient to inspire L. Randall Wray (a prominent MMT theorist) to dedicate a whole volume to Mitchell-Innes's contribution to monetary theory. But Mitchell-Innes wrote in 'The Credit Theory of Money', one of the articles upon which MMT is partly based, that 'the issue of money is the burden and the taxation…the blessing' and that 'because we do not realize that the financial needs of a government do not differ from those of a private person… there can…be no question that the money of the American Government is depreciating' (1914: 6 and 10). This directly contradicts the MMT reasoning that a government's finances are nothing like a household and that the issuer of a currency faces no constraints. This is evidently not the case.

Mitchell-Innes is also clear that 'excessive indebtedness' causes a fall in the value of money and a 'general rise in prices' – a depreciation that has become 'more gradual and therefore more insidious' (6 and 11). The explosion of debt and now rising inflation across the world, particularly since the COVID-19 pandemic, are of great concern, as we see the misinterpretations of theory play out once more.

> The fact, however, is that the more government money there is in circulation, the poorer we are. Of all the principles which we may learn from the credit theory, none is more important than this, and until we have thoroughly digested it we are not in a position to enact sound currency laws. (Mitchell-Innes, 1914: 7)

There can be no mistake, from any theoretical tradition, that inflating the money supply makes us poorer. This is a critical perspective that appears to be lost in modern notions of money, and one that needs desperately to be reclaimed. For Mitchell-Innes, the gold standard was tantamount to a charade – redeeming paper for gold does not settle debt but merely changes ‘one form of obligation for another of an identical nature’ (1914: 10). The gold standard only *restrained* the creation of government money/debt but did nothing for repayment of any money or debt created. And without repayment, prices rise and the poorer we become. The greatest inflation in US history followed the end of the gold standard in 1971 (Mundell, 1999) and this was matched by the explosion of debt shown in Figure 1 (see Weber, 1978: 192; Middelkoop, 2016: 106).

The Great Financial Crisis of 2007-08 saw a culmination of this last 200 years of economic theory and policy. Monetarist criticism of the Fed’s role in the Great Contraction established the central bank as the lender of last resort. Orthodoxy called for restraint and prudence in financial policy, but this was opposed by others demanding more state spending as the solution to lows in the economic cycle. And quantitative easing (QE) emerged as a tool of economic policy. Whilst QE does not involve physically ‘printing’ money, it does involve the creation of money ‘by the tapping of the [central bank] keyboard’ (Ingham, 2020: 95). The divisions still run deep. And it is easier than ever to inflate the money supply out of control.

Some argue that our modern system, based on money creation primarily through bank-issued debt with interest, transfers wealth from the bulk of society to the top (Lietaer, 2001: 54; Bailey et al., 2021a: 9), producing an unstable monetary system and a society where the ‘future doesn’t matter’ (Lietaer, 2014). Selgin, too, in *The Theory of Free Banking*, wrote that ‘the outstanding monetary problem of our time is the failure of central banking to deliver the macroeconomic stability its adherents have promised’ (1988: xi). The evidence of this review seems to support these conclusions. In contrast, however, Ingham writes that ‘the ways in which money is currently produced and organized are by and large tried and tested’ and the result of ‘evolutionary selection’ (Ingham, 2020: 127).

Usury (charging interest for lending money), though, was condemned throughout much of history until only recently - now it is a systemic feature, concentrating wealth in a minority and driving inequality (Lietaer, 2001: 53). Research in economics also supports some of these negative assertions. Growing inflation is correlated with growing inequality (Albanesi, 2007) and excessive debt is related to lower growth (Reinhart & Rogoff, 2010). According to the IMF, there were 425 systemic banking, monetary and debt crises between 1970 and 2010 – ten per year (Lietaer et al., 2012: 10). This does not support the claim that governments can or have been successful in smoothing economic fluctuations. Monopolistic state money has proven to be far from a resilient, equitable system and, historically, societies with multiple currencies enjoyed greater stability and equality (Lietaer et al., 2012: 9). Perhaps, then, other currencies could be part of the solution to systemic volatility, rather than seen merely as a challenge to state monetary hegemony that leads to potential securitisation.

With an understanding of the long, divided history of money, and the competing theories and schools of thought on money, the second part of this review now explores the recent academic research on Bitcoin and cryptocurrencies. This is more empirical in nature compared to the previous part and enables us to examine the methods and designs that other researchers have employed in their studies of cryptocurrencies. The findings of this work are then layered onto the analysis of the scholarly theories of money, giving a fuller appreciation of Bitcoin and cryptocurrencies. This section will therefore inform the research design of this thesis and identify the research gaps that form the basis of the research questions, which were stated in Section 1.4.

2.2 The State, Trust and What We Know

2.2.1 The Role of the State

Ingham reduces the theoretical debate about money to his ‘money question’, which has two elements: ‘first, an adequate theory of money – what it is and how it is produced; and, second, the essential political dimension – who controls the production of money; how much; to what ends?’ (Ingham, 2020: 135). We have noted that, even after 300 years of discussion, disagreement persists over the first element. But it is the second element, the political dimension, that is of most relevance to the tensions and concerns about Bitcoin and cryptocurrencies - more specifically, the question of who should control the production of money. Should it be monopolised by the state, or can other entities have a role to play? Weber famously defined the state as ‘a human community that (successfully) claims the *monopoly of the legitimate use of force*’ (Weber, 1919). If the state is the ‘sole source of the right to use violence’, should it monopolise money too? Other theorists have taken this idea further to claim that modern states have also monopolised the legitimate means of movement, depriving people of the freedom to move (J. Torpey, 1998: 239). It seems that the modern state is keen on monopolising the production of money too. The theoretical divide, here, is Keynesianism/State theory versus the Austrian School. Whilst it has been shown that both sides acknowledge the problem of state involvement in money; the contention remains over what to do about it.

In Chapter 1, we explored the questions that exist over the use of cryptography in society and the battles of the Crypto Wars. And we can draw a direct parallel between the tension between the state and those that desire the freedom to use cryptography and the new tension that exists between the state and those that want to use cryptocurrencies. In fact, it is more than a parallel, rather it is an extension of those very same battles as Bitcoin finally delivered on the Cypherpunk vision of a digital money. Argument from the study of the use of cryptography can therefore be applied to Bitcoin, as cryptocurrencies are a subset of these technologies:

> Encryption policy is becoming a crucial test of the values of liberal democracy in the twenty-first century…Should the state limit and regulate the fast-growing use of cryptography? If so, how? (Moore & Rid, 2016: 7)

In the same way, should the state limit and regulate the fast-growing use of cryptocurrencies? And what might their reasons be for doing so? This is a crucial question, and one that goes to the heart of Moore and Rid's central, empirical question of whether 'cryptographic architectures encourage more illegitimate than legitimate behaviour?' (2016: 9). In this thesis, illegitimate and illicit are taken to generally mean unlawful. This is not precise, as an activity can be illegal in one jurisdiction and not another, but it is sufficient here for an indication of the types of activity that are discussed. There is no doubt that cryptocurrencies are used for illicit purposes, but there is also a great deal of lawful use as well. There is, therefore, a quantitative dimension, in the sense of scale and proportion of activity, to the consideration of the threat that cryptocurrencies pose. And if they are used for more legitimate than illegitimate activity, does that put the balance in their favour? Or is there more to consider than this quantitative relationship; in the political dimension, is there a threat posed by cryptocurrencies beyond their use for illicit activity?

It is here, in the political dimension, that a lot of contention lies. Not only in terms of 'who' can control money but also in terms of the political philosophy of Bitcoin. Bitcoin emerged after the Great Financial Crisis, with Satoshi Nakamoto famously inserting a message into the 'genesis block', the first block mined on the Bitcoin blockchain:

> The Times 03/Jan/2009 Chancellor on brink of second bailout for banks. (As quoted in Champagne, 2014)

Without drifting into the debate about 'technological determinism versus social shaping' (Schroeder, 2018: 18), 'Bitcoin can be seen as an act of social resistance' (Maddox et al., 2016: 65). Bitcoin challenges the soft money of the state through its fixed supply, as we have already seen, but the challenge goes deeper to issues of trust and politics.

In Dodd's *The Social Life of Bitcoin*, the author, refers to a YouTube video called 'The Declaration of Bitcoin's Independence', which states that 'Bitcoin is inherently anti-establishment, anti-system, and anti-state' (2017: 36). Whilst this view is pushed by some, there are others who express 'Bitcoin-related schadenfreude by recounting a list of Bitcoin flaws: the system's alleged vulnerability to hacking and fraud, its associations with criminality, and the uncertainties generated by price volatility' (36). It is here that we meet a familiar commentary regarding Bitcoin – that is, it is often difficult to know what it is about. To some it is anti-state, but then to others, it appears to be about something completely different. Research also adds to this confusion. For example, economists Yelowitz and Wilson analysed Google trends data to show that 'computer programming and illegal activity search terms are positively correlated with Bitcoin interest, whilst libertarian and investment terms are not' (2015: 1030). Yet Glaser et al. (2014) concluded that new users were interested in Bitcoin as an alternative investment rather than as a new method of transaction. Of course, there is a temporal dimension to consider in these varying conclusions, but we can be forgiven for finding it hard to understand what Bitcoin is or who it is for. Dodd though, offers us an explanation, from the perspective of economic sociology:

> Bitcoin is fascinating precisely because it demonstrates many of the contradictions and confusions that characterize money, and its relationship to law and the state, in general. Bitcoin is both a symptom of increasing monetary pluralism in the advanced capitalist societies, and an embodiment of monetary diversity in its own right. Like money itself, Bitcoin is multi-faceted, politically contested and sociologically rich in its functions and meanings. (Dodd, 2017: 36)

This helps make some sense of, or rationalise, the confusion and varying opinions surrounding Bitcoin. Money, more generally, is a contested topic; and so, therefore, is Bitcoin as (primarily) a new form of money. There are many ways that you can look at Bitcoin, whether that is from economics as an investment vehicle, computer science as a technology or sociology as a tool for society. In this thesis, the focus is the latter. Dodd also raises the point of monetary pluralism. As discussed earlier, the world is moving through a period of great transition with regard to the forms of money that society uses, and Bitcoin is another form that has emerged, alongside others that we are more familiar with: WeChat pay in China, PayPal, the Bristol Pound – all these have emerged since the arrival of the internet, along with many others. Pluralism is nothing new, nor are the debates about money which equally apply to Bitcoin.

Why though, has Bitcoin come in for much more scrutiny than other new forms of money? The answer for Dodd is that ‘Bitcoin expresses two forms of monetary disintermediation that are closely associated with this moment in the history of money, namely, its separation from banks and the state’ (Dodd, 2017: 37). Again, neither of these ideas are new; various proposals have been seen since the Great Depression aiming to disintermediate money from the banks and Hayek, in the 1970s, put forward other ideas to disintermediate the state from money (38). But Bitcoin does both. Banks are not needed to process the transactions, and the state cannot exercise monetary policy over Bitcoin as its policy is written into its code. Both of these objections lie in overt concerns that have been present in our society for some time. The banks had a significant role to play in the financial crisis of 2008 (referenced in the Bitcoin genesis block) and the increasing role of the state since 9/11 2001 has also been under increasing scrutiny (Amoore and De Goede, 2005; De Goede, 2012). There is invariably going to be tension if a new form of money challenges the profitable status quo of the memorable alliance. And this is where the literature falls short, in analysing this tension to better understand the true causes.

Many researchers from a variety of fields have tried to attribute the politics of Bitcoin to particular factions, such as libertarians, but this misses a point discussed in Simmel’s *The Philosophy of Money*. To an extent, it has been fair, given the indications we see in the genesis block and from Satoshi’s early writings, but from a philosophical perspective, this does not hold true. Bitcoin is not libertarian or right-wing because anyone *says* it is. Bitcoin has the technical properties it has and people from different leanings use it for those properties – it is a mistake to then transfer those political leanings back onto Bitcoin as ‘new’ properties. This may seem semantic, but it is important as it helps explain why there is such a variety of people and groupings, political or not, using Bitcoin. Users do not define the properties of the system; the system is what it is.

Having said this, ‘Bitcoin is arguably a social movement as much as it is a currency’ (Dodd, 2017: 40). And it is a social movement based on the properties of Bitcoin; that is, concerning the disintermediation of the banks and the state - properties which appeal to a wide variety of groupings, political or not. The banks have been seen by many as corrupt, profligate, and greedy (in terms of excessive fees) (Palframan, 2018), whilst the state has a proven history of being incapable of managing the money supply and, in recent years, of being increasingly invasive. There are simply many people from a host of social groupings that identify with these issues and therefore the ‘ideology’ of Bitcoin. Whether Bitcoin is better or not is only part of the argument; the fact is that people are *choosing* to use something else. In this way, Bitcoin and cryptocurrencies are also about identity. They enable people to aspire to and fulfil a variety of identities, such as being against state infrastructures and systems.

But underneath this layer, the real debate about cryptocurrencies is to do with their properties, as much as anything else. Which properties are of use to people (perceived usefulness), and which do certain parties (authorities) object to? It is here that we can return to the wider arguments of Moore and Rid regarding cryptography – ‘where should the line be drawn between desirable and undesirable properties of crypto systems?’ (2016: 9). What is the difference between good money and bad money? And, therefore, what is the difference between a good cryptocurrency and a bad one? For example, is a pseudonymous system like Bitcoin ‘acceptable’ whereas a completely private cryptocurrency is deemed bad? And similarly, when does one cryptocurrency represent a threat and another does not? Answers to these questions would help draw the lines for cryptocurrencies but it will only be possible to answer them once works such as this have been completed that aim to provide a greater understanding of the tension that exists, and the reasons for it.

The lessons from the debate about cryptography do not end here. Moore and Rid also argue that many view cryptography ‘as if it were a godlike force for good’ (2016: 29). There is certainly a danger with cryptocurrencies that there has been a similar positioning. Undoubtedly, many of them have been created without deep sociological consideration, resulting in a proliferation of cryptocurrencies appearing on the market with an array of varying properties. It is only a reactive endeavour, in works such as this, that we try to unpick their meaning and work out where the lines should be drawn in a functioning society, and evaluate whether there is even a need for cryptocurrencies. Before the internet, we lived in a world where transactions were far more untraceable than now, and the world functioned well enough. Perhaps economic Darwinism will determine our future payment systems, but a deeper understanding of what we want as a society would certainly help inform the debate about our future forms of money.

2.2.2 The Issue of Trust

Why do forms of money, or the people behind them, seek disintermediation? We have explored the reasons why Bitcoin may seek to disintermediate money from the banks and the state but in essence, this is an issue of trust. Trust in banks has weakened vis-a-vis the economic crash of 2008. Likewise, trust in the state has been weakened following the likes of the Snowden leaks and the many state failures of economic mismanagement. It is here that Bitcoin is different from any other form of money in that it tries to achieve its goals through technology – its code and the network of machines that process the transactions – solving the core problem of other forms of money that rely on a central authority for that trust (Dodd, 2017: 41). In this way, Bitcoin has four alluring features: it has a flat hierarchy with no central authority, technology solves longstanding mismanagement of money, there is no need to trust others (e.g. politicians or experts) and Bitcoin is ‘debt free money, just like gold’ (42).

Where the trust lies in a cryptocurrency remains an area of debate. Bashir, Strickland and Bohr recognise that trust has shifted away from the central ‘institution to other parts of the system, but trust remains the foundation of value for the system’ (2016: 350). And for Maurer, Nelms and Swartz, ‘Bitcoin combines a practical materialism with a politics of community and trust that puts the code front and center’ (2013: 263). To Hayes, who takes a science and technology studies approach, Bitcoin raises the prospect of the ‘governmentality of algorithms on society’ but disagrees that trust ‘has simply been transposed into machine code’ (2019: 3).

Rather, he argues that instead of ‘severing all ties with social relations’ that Bitcoin and others ‘foster more direct personal connections’ in peer-to-peer fashion instead of going through intermediaries. Interestingly, Hayes also proposes three ontologies for blockchains, including as ‘institutions in their own right’ (2019: 1). Whether the trust now resides in the code, or whether you view the blockchain as an institution that is now being trusted, the important point is that the trust has been disintermediated from where it was before and in a new way. The critical question for an advanced society with an advanced development of money, is where is trust best placed – that is, who or what will serve best in the management of the pivotal institution of money?

In fact, most of the social literature misses some of the more nuanced understanding of Bitcoin from a technical perspective. Whilst most writing focusses on the ‘trust in code’, one of the key ideologies of Bitcoin and a feature of the blockchain itself is that, by running a full node, you can calculate the state of the network *yourself*. That is, with Bitcoin as an example using an Unspent Transaction Output (UTXO) model, the idea is that a party running a full node can calculate the entire history of the blockchain themselves and can determine therefore whether transactions are valid. In this way, Bitcoin offers parties a way of trusting *themselves*, rather than another party; the mantra ‘don’t trust, verify’ is widely seen across Bitcoin reporting. (For most users, however, they will not run a full node and so do place trust elsewhere, including in any system itself.)

The issue of trust, then, is perhaps not entirely clear in the literature. Is trust about *whom* (or what) you, as a user, choose to place your trust in? Or is it about a greater sense of self-reliance, rather than trusting some third party? It may help, in the spirit of Simmel’s work, to conduct a small thought experiment. If in a military situation, we imagine that a drone is about to strike a target. Who would be preferred to have the final say on the execution of the attack? A human, who may be susceptible to many distractions but who can apply a subtlety of thought that might be required to avert a mistake, or a machine, which will execute as planned, without human fallibility (see Rid, 2016: 98 for similar discussion)? There is a technological paradox here and it seems self-evident that there will be those that would choose a human, just as there are those that would choose a machine. Distilling this further, who would you trust, man or machine? Or when it comes to the management of money, would you prefer to trust a government or the code of an independent monetary system? Similarly, it is unlikely that consensus could ever be reached on these questions, as they are about choice and preference rather than any particular answer being right or wrong. And if this is the case, then surely one solution is to allow choice and let people decide.

This question then becomes about mankind's relationship with technology. We have seen that Bitcoin has its roots in the Cypherpunk and libertarian movements, but it is possible and useful to look even further back at the emergence of cybernetics. Created by Norbert Weiner in his seminal book of 1948, *Cybernetics: Or Control and Communication in the Animal and the Machine*, this new field sparked a viewpoint and debate that is just as relevant today as it was then. Some were excited by the prospects of this new-found blending of man and machine, whilst others were equally disturbed by the potential downsides that this path may bring. As Rid describes in *Rise of the Machines*, 'optimism competed against pessimism, liberation against oppression, utopia against dystopia'(2016: 4). And so, it is with Bitcoin and its supply fixed in code; there are those that swear by its potential to change the world, just as there are those that proclaim it a scam and a disaster. Perhaps then, this is about viewpoints and different groups will have different perspectives. It is not necessarily about one being right and another wrong, merely that choices exist, and people will choose between them. Are there certain groups that are more pessimistic or optimistic than others or are we in a time where the human view of the benefits of technology is pushing us towards one 'side' or the other? These are interesting questions that speak to the concept of the 'governmentality of algorithms' (A. Hayes, 2019: 3).

For centuries, there has been a split view on technology and its benefits. Throughout history, we can see examples of groups that have embraced technology to the full, as well as those that feel the opposite. The Luddites in the early nineteenth century attacked machinery in response to threats to wages, modern-day Amish communities continue to resist the use of technology and the philosophy of the likes of Thoreau can be seen in Jamie Bartlett's '*Darknet*' as we meet an 'anarcho-primitivist' and a 'transhumanist' who come together in a clash of ideals (2014: 235). We see this unease in the present day in other areas as well – with Artificial

Intelligence (AI) and indeed with ‘tech giants’ and their centralisation and monolithic concentration of information and thereby wealth. As we debate these issues, so too do we debate cryptocurrencies. This brings us back to this issue of the human-technology relationship and some of the wider debates that we have seen around the nature of money. When is technology good for us and who gets to decide? How do we want society to look and operate and where does technology fit in? These are the questions we continue to return to when examining the nature of cryptocurrencies.

Bruce Schneier wrote a piece on his blog about the issue of blockchain and trust (2019). In it, he outlines that Bitcoin does not remove trust and that instead, the system shifts trust from people to institutions, as we saw above. As he points out, you still need to trust the ‘cryptography, the protocols, the software, the computers and the network’. This is true, and why the maxim of ‘don’t trust, verify’ needs to be taken at face value only. But the literature seems to miss the point that no conceivable monetary system can be trust-free, free of any risk from any humans or any technology.

> Honestly, cryptocurrencies are useless. They're only used by speculators looking for quick riches, people who don't like government-backed currencies, and criminals who want a black-market way to exchange money… Does the blockchain change the system of trust in any meaningful way, or just shift it around? Does it just try to replace trust with verification? Does it strengthen existing trust relationships, or try to go against them? How can trust be abused in the new system, and is this better or worse than the potential abuses in the old system? (Schneier, 2019)

It is exactly the whole premise of cryptocurrencies, in relation to trust, that they change the system and provide an alternative - people are then free to decide where the potential abuses might be worse and can choose accordingly. We need only look to the financial crisis of 2008 for proof that the existing system is not perfect either. The imagery of people queuing to withdraw money from banks is fresh in our minds - banks failed, and nation-states failed too, leaving creditors forced to accept reductions on money owed. The financial system is also aged and complicated, in a time of fast-moving technology, where payment is diversifying ‘rapidly – in both form and function’ (Nelms et al., 2018: 15). Banks struggle with legacy systems on a regular basis, as customers are frozen from their funds. In the UK, the Financial Conduct Authority reported a 187 per cent increase in technology outages, of which eighteen per cent related to cyber incidents (Financial Conduct Authority, 2018).

It is not just the banks that have issues – the whole transaction system is complicated and consists of many parties, with varying interests. Researchers have shown, for example, that making credit and debit card transactions is far from secure. Ali et al. conducted a study of online payments and showed that attackers can use online payment sites to guess and acquire all the security details needed to make card payments. Worryingly, of the 36 websites they contacted about the vulnerabilities, eight did not respond and, after four weeks of disclosure, 28 remained unchanged (Ali et al., 2017). And this is a system where every time you make a card payment you leave all the details needed for this kind of fraud with the retailer. UK Finance reported that ‘unauthorised financial fraud losses across payment cards, remote banking and cheques totalled £844.8 million in 2018, an increase of 16 per cent compared to 2017’ (UK Finance, 2019). This is not to say that there are no security threats with cryptocurrencies – there most certainly are: from user error, hacking of exchanges and even built-in system-level design features such as the 51 per cent mining attack (Bailey et al., 2021a: 4). The point though, is that the systems are different, with different advantages and disadvantages and in Schneier’s words, ‘is this better or worse than…in the old system’. That is the decision that users face, and a balanced comparison needs to be made. But perhaps cryptocurrencies can play a role as an alternative or even complementary monetary system, especially given the extent of the problems in the existing one.

Traditional systems do offer different properties that can be advantageous, such as the ability to ‘undo’ transactions. However, there are clearly many who feel that cryptocurrencies are something that they want to use and choose to use for many different reasons. Branding cryptocurrencies as useless is to discount that there are people who have assessed the alternatives and made a (rational) choice to use them. In this thesis, the aim is to move away from opinion to learn more about the views of actual users themselves – only they can describe why they have chosen to use cryptocurrencies. It is for any given user to decide whether a cryptocurrency is useful, whether it is to do with speed, cost, and anonymity or simply because they offer a model of trust that they prefer. The research of this thesis will add to the understanding of cryptocurrency usage, framed by the perspective of the economic sector of securitisation theory and the emergence of these new technologies as one of a growing reality of monetary plurality.

2.2.3 Legal Use of Cryptocurrencies

When this research project began in 2017, there was an overwhelming sense that the majority of research about cryptocurrencies was technical. Debates about how to scale blockchains in terms of the number of transactions they could process per second dominated the discussion, and this period was exemplified by the ‘blocksize war’ which resulted in a ‘hard fork’ of Bitcoin into two competing versions (BitMEX Research, 2021). This dominance continues to this day, with much less attention paid to other areas of research, and several academics have commented that more needs to be done from a social perspective (for example, Karlstrøm, 2014: 26; Bashir, Strickland and Bohr, 2016: 355; Abramova and Böhme, 2016; Alshamsi and Andras, 2019; Hayes, 2019). This also perhaps explains why sociological research is more disparate and harder to place into schools of thought or approaches. In the first part of this review, the theories and schools were easy to identify. But the recent research on cryptocurrencies is more of a loose collection of studies from a variety of disciplinary backgrounds. As such, the literature lacks a clear sense of approach or orientation. Perhaps this is something that can be improved as our conceptions of cryptocurrencies develop more, in a similar way that they have with money more widely.

However, given that money is *the* pivotal institution of society, there is a clear imbalance and a requirement for further research of a societal nature. This study aims to contribute toward balancing this lop-sided dominance of technical research through further exploration of some of the societal aspects of this topic. Money is of such great importance to how our world functions that it, arguably, has not been given the significance and gravity that it deserves.

Chapter 1 established that there has been concern about the criminal use of cryptocurrencies and that this has been the basis for the claim that they are a security threat. This will be examined later in more depth in Chapter 4. Chapter 1 also briefly discussed my interest in this topic and why I wanted to research cryptocurrencies (again, this aspect will be more fully discussed in the methodology in Chapter 3). My initial thoughts about the security threat of cryptocurrencies left me with an unanswered question: if blockchains leave a permanent record of transactions, why would this be preferable to cash, for example, as a way of conducting illicit transactions? To explore this paradox, I wanted to understand what motivates people to use cryptocurrencies. Several studies now exist that explore the use of cryptocurrencies and it is to this body of work that we now turn. Research examining the use of cryptocurrencies for legitimate purposes, such as for speculation or remittance, is first reviewed. As the illicit use of cryptocurrencies is of particular relevance to the question of security, research of the dark net is also explored. The dark net is a focus for the illicit use of cryptocurrencies as they host marketplaces where cryptocurrencies can be used to buy and sell illicit goods and services. Analysis of this work reveals the outstanding questions and gaps in the research space.

Bitcoin means different things to different people. This conclusion from one of the first surveys of Bitcoin users by Bashir, Strickland and Bohr (2016), is a simple one but it is also quite telling. In debates about the security threat of cryptocurrencies, there is often a tendency to oversimplify and make sweeping statements that allow for few possibilities – for example, the claim (that will be explored in due course) that cryptocurrencies are primarily a tool for illicit activity. The reality is that cryptocurrency usage and adoption are far more nuanced and varied. Of course, criminals are using them, but many use them for legitimate purposes too.

Bashir et al. conducted a web-based Bitcoin-user survey of US university students in April 2014. With backgrounds primarily in psychology and sociology, the researchers aimed to conduct an empirical study to provide a base for an under-researched subject. They invited 7,500 students to take part, achieving a 7% response rate of 520 people. This study is one of the first into the attitudes of people to cryptocurrencies and there are several findings. There was a clear political motivation in the adoption and attitudes toward Bitcoin, with libertarian ideology having a strong influence. Furthermore, novelty was a greater attraction of the currency than anonymity and there were also some interesting gender differences noted. This survey supports the data from another early study from 2014 of over 1,000 users, which showed that 95 per cent of respondents were male, with an average age of 33, and almost half identified as libertarian (Bohr and Bashir, 2014: 96).

Even though this work was a relatively early survey in Bitcoin’s history, it is significant that they found that novelty was a greater attraction than anonymity. The anonymity that cryptocurrencies afford is one of the main advantages that is often put forward by those claiming that they are an excellent criminal tool. To what extent then are cryptocurrencies anonymous and how much is this property a motivation for usage? This is an interesting area for further work, as it will help inform discussion about the usefulness of cryptocurrencies as a criminal tool and security threat.

The analysis of their survey findings was informed by wider research on currencies with a sociological and psychological focus. They compare the psychological perspective of money of Furnham, Wilson and Telford (2012) in terms of security, power, love and freedom. The idea of freedom is linked to the libertarian view, where the limited supply of Bitcoin translates to a loss of power to the state. This further ‘speaks to a longstanding concern, going back at least to the classical theory of Georg Simmel, on the relationship between monetary and social systems that allow for varying concentrations of political power’ (Bashir, Strickland and Bohr, 2016: 356). Do people use Bitcoin because it offers a new social order, where they do not have to rely on the state? This is certainly a possibility and ties in with ‘a long tradition of thought on monetary utopias that aim not for the abolition of money but its radical transformation as a means of improving society’ (Dodd, 2012). This view, from economic sociology, is a useful way of thinking about cryptocurrencies. Cryptocurrencies may be a new form of money, but the debate about them as money in many ways is not new, and merely adds to the already significant body of literature on monetary issues.

There are several limitations and opportunities for further research concerning this early study. First, in the world of cryptocurrencies, Bashir et al.'s research is already several years old. It is also significant that the survey took place prior to the explosion of interest and adoption in 2017. As usage has grown, it is possible that attitudes will have significantly changed and that this strong connection with libertarian ideology may not have such prominence as new users emerged. Similarly, as more legitimate users joined the system, the proportions and volumes of illicit use may also have changed. It would be interesting to explore the extent to which cryptocurrencies have been and are being used for illicit activity. Has this changed over time and how might that inform the security threat narrative of cryptocurrencies?

The Bashir, Strickland and Bohr 2016 survey also recognises the limitations of a sample of university students and suggests more work is needed to study wider groups of users to highlight different relationships with the technology. This could be achieved by surveying groups on social media sites such as Reddit or Twitter. Whilst the authors suggest looking beyond the university group they studied, there may be merit in seeing how attitudes have changed amongst that group post the 2017 boom. The use of survey as a method also needs consideration. Does this enable exploratory investigation and the depth that this thesis will require? Other methods, such as interviewing, may be better able to tease out a greater understanding of the motivations for the use of cryptocurrencies, particularly as they relate to illicit activity.

Other research has discussed the political and economic dimensions of Bitcoin. In an earlier study, Maurer, Nelms and Swartz (2013) investigated Bitcoin from a semiotics (communications research) perspective by studying the archived conversations of those involved in the system. This methodology was appropriate as Satoshi Nakamoto, in particular, only had an online presence. They showed that Bitcoin 'provides an alternative to currencies and payment systems that are seen to threaten users' privacy, limit personal liberty, and undermine the value of money through state and corporate oversight' (2013: 261). They also observed, in accordance with Simmel's views, that the real meaning of Bitcoin is below the surface level of its use as a currency; that is, as an 'index of much broader discussions over the nature of money' (263). Their choice of language alludes to the philosophical essence of what the furore surrounding Bitcoin as a new, private money is really about – it is not about transactions per second, it is about the fundamentals of our society, about how it should be run, where trust should be placed and crucially about how we abstract value in it.

By 2014, when Bitcoin had already been operational for five years, it had been noted that there was a lack of research into user adoption and that there had not been ‘any empirical research applying detailed interviews to gain rich knowledge’ about Bitcoin and cryptocurrencies (Baur et al., 2015: 64). This may be because Bitcoin was still a relatively niche market and topic of study. However, in an attempt to address this, Baur et al. conducted a series of 13 semi-structured interviews, which were then analysed using an open-coding qualitative research method (69). They applied the Technology Acceptance Model (TAM) theory to cryptocurrencies, where the perceived usefulness and ease of use are key determining factors in the adoption of new technologies. (TAM has since been adapted to cryptocurrencies in several further studies, such as by Abramova and Böhme, 2016; Mendoza-Tello et al., 2018; Roussou & Stiakakis, 2016 and Shahzad et al., 2018).

The interview results (again prior to the 2017 boom) show that there were ease of use concerns amongst participants and an agreement that the younger generation would be more suited to its usage. Whilst one merchant thought Bitcoin was as easy to implement as other offerings, and potentially more secure, price volatility was seen as the main threat (73). With regard to usefulness, there were several findings. Consumers thought that lower costs were a major reason for using Bitcoin, due to high credit card and overseas wiring fees. And again, anonymity was not viewed as an issue. It may be that these participants felt no need for any privacy in their transactions, but it would be very interesting to explore this dynamic amongst users who are engaging in more illicit activity.

Emerging economies may also find Bitcoin useful where traditional banking is not as accessible (74). For merchants, lower fees were also a factor as was the finality of payments - they strongly supported cryptocurrency and saw it as the future for payments (75). The overall conclusions for usefulness related mainly to lower fees and potential for international transactions. Only a small influence was given to greater anonymity. It is worth noting that there was no mention of libertarian or other such political motivation. Finally, the researchers note that the sample size is a limitation and that more research needs to be done.

This last point is worth some further discussion. Most of the research reviewed so far does not intentionally target a particular community or subset of users to identify the attitudes of that particular group. For example, the survey of university students did not aim to understand the view of students - students just happened to be the sample used. Researching selected communities about their usage or their attitudes towards cryptocurrencies would add to what is already known through a more detailed examination of the benefits that cryptocurrencies may bring. There are many different groups of users, be they speculators, savers, merchants, or those that use them illicitly to name a few, and each group will likely have a different perspective on why they use cryptocurrencies and the benefits that they offer for their purposes. It will only be through more directed research of these groups that we will be able to gain a deeper understanding of their respective perceptions.

Furthermore, this work will also enable comparison between groups, which will give a richer insight into how this perception of the utility value of cryptocurrencies changes across groupings. It will, of course, highlight individual community aspects, which too are valuable. For example, researchers conducted an online survey of users of the Bristol Pound, an alternative payment system for that community. This research was grounded in the literature on mobile money (for example of M-Pesa, a mobile phone payment system used in developing countries) and two strands of theory: sociological (where money allows ‘depersonalised and asocial…transfers’ or as a shaper of social relationships) and economic anthropology where the debate concerns how money practices have impacted socially and culturally (Ferreira, Perry and Subramanian, 2015: 1223). Whilst not a cryptocurrency, the survey showed some of the community benefits that might not have been seen from more general research:

> [The Bristol Pound payment system] supports people in making connections to other people, to their communities, to the places they move through, to their environment, and to what they consume. While these social and community bonds shape the kinds of interactions that become possible, feelings of trust

> also shape how users feel about the social and community bonds that they hold with their co-users. (Ferreira, Perry and Subramanian, 2015: 1232)

In this vein, there is a need for more specific research into community usage of cryptocurrencies to explore these social impacts. This also ties in with an economic sociological approach to cryptocurrencies, as there are many forms of money used in our societies today. Questions such as why a community might decide to choose a cryptocurrency over an alternative system such as used in Bristol (and several other towns and cities across the UK) would be interesting and a new area of research.

2.2.4 Further Legal Usage Studies

The studies above highlight the types of user enquiries that have been conducted and their findings. There are several other studies on users of cryptocurrencies, but it is not the purpose of a literature review to exhaustively cover them all in full detail. However, some deserve mention.

First, it is worth noting that several studies, drawing similar conclusions to varying degrees as so far seen, have been conducted with a geographical angle based primarily on the researchers' location: Presthus and O'Malley (2017) carried out a web survey of people in Oslo, nine Bitcoin users from forums in Malaysia were interviewed from an HCI perspective (Sas & Khairuddin, 2015), Tsanidis et al. (2015) looked at Bitcoin adoption in Greece and Shahzad et al. (2018) researched adoption of cryptocurrencies in mainland China through a questionnaire. These studies did not take a community or cultural perspective. They researched Bitcoin users who happened to be from the country of the researchers - in the same way that the earlier survey happened to study students. That is, the work was of a general nature and did not aim to highlight the particular views of that country or a particular group from within that nation. Wider research, beyond a geographic locality of the research team, is missing. As too is targeted research of specific communities for the very purpose of understanding the views of that specific group. This will be addressed in this thesis with research strands aimed at illicit users (across geographic boundaries), law enforcement officers with cryptocurrency experience and through a case-study of the HullCoin, a cryptocurrency designed for a particular community.

To conclude this short section, there have also been some studies looking at the experience of using cryptocurrencies, rather than why and for what purposes. For example, Gao, Clark and Lindqvist (2016) showed the barriers that exist for non-users of cryptocurrencies. Krombholz et al. (2016) conducted a large online survey of 990 Bitcoin users to examine their experiences with regard to security and privacy management. Similarly, a 2019 study looked at Bitcoin in comparison to credit cards from an HCI perspective, ‘bringing insight into the user experience of Bitcoin in terms of usability and security’ (Alshamsi and Andras: 98). Although this work also took in a small sample of university students, this time in the UK, part of the study involved practical work as participants conducted tasks on a Bitcoin wallet. Studies like this produce interesting results but they do not further our understanding of the motivation to use cryptocurrencies or of the security threat that they potentially pose. User experiences of Bitcoin wallets do not explore why certain groups or individuals want to use them.

2.2.5 The Dark Net

The usage of cryptocurrencies on the dark net is reportedly a key concern to law enforcement and governments, as already shown. As such, this issue takes a prominent position in the wider debate about the existence of cryptocurrencies and the threat that they pose. In this section, we will explore this specific location of research to understand what is known about the use of cryptocurrencies on the dark net, as this community of users is of great interest to any work that explores the security threat of cryptocurrencies. Most of this research does not address cryptocurrencies directly, but wider work in the area of the dark net must be examined, as it informs any future research intended with a focus on cryptocurrencies. There are also specific ethical and methodological considerations to this site of research which must be carefully considered.

Dark net markets are bad – this is the assumption that underpins much of the argument with regard to cryptocurrencies. Research does suggest that 'cryptomarkets' (dark net sites where illicit goods can be traded) will increase the volume of substances for sale, but the effect that has on harm is less clear cut; Aldridge, Stevens and Barratt argue, for instance, that drug quality and purchasing risk may be lower on the dark net due to feedback systems, price comparison, multiple-vendor choice and increased product information (even such as chemical test results) (Aldridge, Stevens and Barratt, 2018: 790). They also comment that the 'anonymity provided by hidden web services and use of cryptocurrencies for payment, should function to reduce possibilities for violent confrontation' (791).

This research raises what some may consider an uncomfortable reality that cryptocurrencies, at some level, may enable a *reduction* of harm in relation to drug-taking activity. Threats and physical violence are much lower on cryptomarkets compared to alternatives (Barratt, Ferris and Winstock, 2016: 24). This brings into question whether the debate about cryptocurrencies and the dark net is about cryptocurrencies or is it more about the underlying debate in society that has been long-running regarding policy as it appertains to illegal substances. Or put another way, is the issue of drugs and the dark net one of drugs or cryptocurrencies? Or is it even just about the mere existence of unregulated internet spaces? And in a similar warning as from De Goede regarding the war on terror, the authors note that:

> …policy makers will need to consider carefully how drug markets will innovate in response and pay particular attention to potential unintended consequences. As with off-line sales, it is unlikely that the on-line drug trade can be eradicated completely; cryptomarkets will, however, respond to regulation and enforcement in ways that have complex effects on both the harms and benefits. (Aldridge, Stevens and Barratt, 2018: 794)

The policy response to cryptocurrencies, especially in regard to the dark net, needs, therefore, some careful thought and is part of the wider, ongoing debate surrounding the dark net in general (Chertoff, 2017). This is even more important if you consider that the risk of arrest may also reduce when purchasing on the dark net – there were 391 arrests worldwide up to December 2016 (Aldridge, Stevens and Barratt, 2018:

792). This is a modest figure and should be borne in mind in relation to the findings of Kethineni, Cao and Dodge (2018), who conclude, in their work applying space transition theory to Bitcoin use on the dark net, that a lack of deterrence attracts criminals to the internet. As per the argument above concerning drug policy, is the problem with the dark net about cryptocurrencies or a failure of deterrence? In ‘space transition theory’, which explains the causation of crimes in cyberspace, lack of deterrence is one of the reasons that people can behave differently between the physical and online world (Jaishankar, 2007: 7). From a policy perspective then, should you target cryptocurrencies as an enabler or, taking a deterrence theory approach from criminology, decide that the problem is a failure in deterring criminals from the dark net? The important point to consider here is what effect targeting cryptocurrencies would have i.e., could people just use an alternate payment system? This line of thought will be returned to in Chapter 5, in particular when considering the threat of ransomware. Making a particular payment method more difficult to use may not necessarily do much for deterrence. A similar argument is made by Bancroft and Reid (2016: 508) with regard to dark net anonymity; they assert that although this topic receives much focus, it is not a precondition for online drugs selling as demonstrated by the fact that drug trading exists on the internet without attempts to hide identity. Authorities need to carefully consider what the problem is and be even more careful to consider the impact that any policy might have.

There is further merit to these thoughts provided by the research of Ladegaard (2018) who showed that after media coverage of police action on the dark net and after the life sentence given to the founder of the Silk Road, that trade on markets went up. Perhaps regular users remained undeterred by the arrest of a founder, but the author concludes that this adds to the growing literature that disputes whether punishment deters crime. If punishment does not adequately reduce dark net crime, would targeting cryptocurrencies prove to be a more useful policy response? What would deter people from the dark net? It has been noted by the research community that there is a lack of work assessing the effectiveness of strategies towards illicit markets (Holt, 2017: 5). This could be another interesting aspect to research either through the view of law enforcement officers or from the perspective of dark net market users.

The dark net has proven to be a popular area of research for academics from a multitude of disciplines, employing a variety of methodologies. A significant part of the literature focusses on the drugs dimension, in reflection of the status of this topic in wider society. Bancroft (2017), for example, scraped a dark net market forum as part of a qualitative study into the experiences of dark net users. The aim being to extend the debate about harm to show that it becomes ‘an active object rather than just a potential negative outcome to be avoided’ (3). Whilst the focus of the work was ‘on the breadth and depth of users’ orientations to risk and harm’ (7), it is interesting to note that this method of research delivers a greater understanding of the motivations and thoughts of the actual users of the dark net. Bancroft observed discussions where users felt ‘safer and less stigmatised’ (15) when purchasing on the dark net. He notes, however, that dark net markets are limited in their ability to reduce harm and that offline markets may be sufficient in many circumstances. Furthermore, there is inequality in using the dark net due to the resources and knowledge required to use it. This is an important thought as we consider the extent of these markets and the role that cryptocurrencies play within them. If they are difficult to use, does this make these markets a niche option, and thus is the fear in relation to cryptocurrencies overstated? This question will be explored in the empirical chapters.

There are several methodological observations by Bancroft from this qualitative approach that should be mentioned. The majority of the posts came from a minority of users – this needs consideration from the perspective of representation. The author tried to ask for permission to research the forum but received no answer and so decided to continue upon seeing no prohibiting rules. It is not stated, however, whether the research was conducted covertly or overtly. This is important as revealing the identity of the researcher could affect the information gathered and pose potential safety risks. Nvivo was used as a tool for analysing the information gathered and for testing hypotheses. And finally, ethics approval was sought at the university level.

Similar qualitative methods, as seen in this Bancroft study, may reveal more about trends and usage of cryptocurrencies than technical or statistical analysis of blockchain data alone. Social research into the use of cryptocurrencies on the dark net is limited at best and does not appear to have been the focus of work to date. A great deal of research seems to either be technical (descriptive research looking at volume and type of items for sale etc. – see Holt, 2017 and Dolliver and Kenney, 2016) or social with a focus on drugs and harm or the viewpoints of participants (e.g. Van Hout and Bingham, 2014). For example, Gharibshah et al. (2019) analysed the properties of threads on forums, but this type of technical research does not provide a deep understanding of the 'perceptions and thoughts of users' as qualitative methods might (Mirea et al., 2019: 106).

This fundamental difference in methodology, in terms of technical versus social, or quantitative versus qualitative, has also been commented on by Robert Gehl in his chapter in *Research Methods for Digital Humanities*. The chapter, 'Archives for the Dark Web: A Field Guide for Study', observes that work on the Dark Net is 'dominated by computer science and automated content analysis' and that more 'humanistic inquiry' is needed (Gehl, 2018). Gehl also raises some further limitations of existing work. First, there is more than one dark net; there are other systems as well as Tor that can be researched, such as Freenet, I2P and Zeronet. Second, much of the ethnographic work that has been conducted has focussed on dark net markets but there is much more that can be researched, such as forums and networking sites. Finally, web scraping archives from 2011-2015 (such as at www.gwern.net) are widely available for researchers and this has proven fertile ground (2018: 6). Whilst these archives are now several years old, they do not appear to have been researched in terms of what they tell us about cryptocurrencies at that time. Of particular interest would be the time around 2014, when ransomware payment methodology shifted from prepaid cards to cryptocurrencies. It would be interesting to see if there was much discussion about the choice of payment technology at this time. There is also a research gap covering the period after 2015 until the present day. This is particularly important with regard to cryptocurrencies as they became mainstream in 2017; what was known about them before that year has almost certainly now changed.

For example, to take this last point further, we have seen the connection between the Cypherpunk movement and both cryptocurrencies and the dark net. This is an important area to explore, as political viewpoints could be behind some of the motivations for using cryptocurrencies. Munksgaard et al. (2016) used topic modelling on a data-set from dark net crawls from 2011 to 2015 to show that there was a libertarian discourse on marketplace forums, including from the Silk Road founder (Dread Pirate Roberts), but it reduced following the shut-down of that platform. A research gap that exists is whether this libertarian discourse is conflated with the intentions of the creators of cryptocurrencies, in particular Bitcoin. Just because Dread Pirate Roberts set up the Silk Road with liberalist intentions, does not mean that cryptocurrencies were also set up with this intention, or any particular other. This will be a hard gap to close, as the creator of Bitcoin is anonymous and no longer active.

Similarly, Maddox et al. (2015) also showed this libertarian link and desire for ‘personal freedom’ in their ethnographic study of the Silk Road, where they conducted interviews with seventeen participants. They introduce the term ‘constructive activism’ to describe the way that users of the Silk Road built and engaged with a system that acts as their activism, as they cannot lobby in the real world due to their illicit activity (Maddox et al., 2015: 111). This has parallels to Van de Sande’s (2015) concept of ‘prefigurative politics’, where:

> According to a prefigurative reading of radical politics, the direct experimental actualization of a social and political alternative should be considered as an inherent part of activist practice itself. (van de Sande, 2015)

This is interesting and relevant to cryptocurrencies in several ways. As already discussed, it may be that these new systems are being used incidentally in liberalist activism, such as on the Silk Road. Whereas the intention of the designers was a prefigurative practice but for a different goal – that of sound money. But these goals are not the same. The point has been made that it is philosophically unsound to transpose the characteristics of a user onto the item being used. This appears to be a common oversight that researchers make and one that confuses the discussion about cryptocurrencies by thinking of them in terms of selected groups of users, rather than debating them as money in the monetary plurality that we now live. This returns us to the viewpoint of economic sociology; that cryptocurrencies are just another form of money that will be used by different groups with different transformative goals. We are, of course, interested in why different groups use cryptocurrencies but these reasons should not then be mixed up with the purpose of cryptocurrencies, which, in the first instance, is as a form of money. These conflations are very important to the narrative that surrounds cryptocurrencies, and therefore to the question of whether Bitcoin and others have been securitised, or whether there has been an attempted securitisation. And they are also important to the analysis of the justification given by those who may be making securitising speech acts.

2.3 The Research Gaps

It was necessary to split this review into two parts due to the nature of the debates about Bitcoin and cryptocurrencies but also due to the range of academic work that is relevant to them. Bitcoin was created as a new form of money with old problems in mind. The literature on money was, and is, therefore, key. This necessarily required a deep look into the theoretical and historical work in this field, as these are some of the richest but also most useful pieces of literature on this subject. Simmel’s work exemplifies this in its relevance and applicability to cryptocurrencies as new forms of money. As a whole though, this body of literature was too focused on the materiality of money, and not enough focus was given to the political dimension where the heart of tension about money, and cryptocurrencies, lies. However, the orientations, controversies and clashes in this literature were clear to see.

The second half of the review then focussed on the more recent, empirical work on cryptocurrencies since they were invented. This work is more disparate in the approaches taken as the research comes from a multitude of fields. This body of work is still exploratory, and many researchers have been investigating cryptocurrencies from a range of perspectives. This makes it hard to group the research or identify particular schools of thought, as could be done with the literature on money. This also likely reflects the inter-disciplinary nature of cryptocurrencies, as they have roots in computer science, as well as several disciplines within sociology; from economics to economic sociology, criminology, security studies and international affairs to name a few. The literature tended to focus on the use of cryptocurrencies, but often made the philosophical mistake of transferring those characteristics back onto them. This also misses the more leading importance of cryptocurrencies as money. The result is that the literature gives a conflated view of the issues, which need more research to achieve a deeper understanding and more sophisticated ways of thinking about cryptocurrencies beyond simpler concepts of use and intent. Critically, in terms of securitisation theory, these faults are integral to the narratives that surround cryptocurrencies. In Section 1.3.1, the importance of analysing the speech acts and the justifications that the object is a threat was highlighted. Yet, there is little of this in the literature. Generic, unsubstantiated claims against cryptocurrencies are often made in support of the narrative and these must be scrutinised in more detail.

In summary, there are several gaps and under-explored areas in the existing research that have been identified in the literature review:

1. First, there appears to be an axiomatic acceptance in the literature that cryptocurrencies are a threat. The narrative of the potentially securitising actors has not been examined thoroughly and there has not been enough academic research in the literature about the extent to which cryptocurrencies are used for illicit activity, certainly in comparison to existing methods. If the usage of cryptocurrencies is overwhelmingly illicit, then this may support claims that cryptocurrencies are primarily a criminal tool and therefore a security threat. More research is needed to better understand the ways that cryptocurrencies are potentially a threat and, importantly, to what extent.

2. Second, there has been a significant amount of research on cryptocurrency users, but this has all been done from a legal usage perspective. Given the apparent concern over the security threat that cryptocurrencies pose, there is a gap in the literature about the views of illicit users specifically. If there is concern that cryptocurrencies are a powerful criminal tool, then there needs to be research of this group to understand what properties of cryptocurrencies are useful, why they use them, and how they view them in comparison to traditional tools and methods. Researching the actual users of cryptocurrencies for illicit

purposes will provide answers to these questions, rather than basing judgement on the opinion of commentators or securitising actors.

3. Third, for all the claims that there are about the security threat of cryptocurrencies, there is also a gap in the literature examining this threat from the perspective of law enforcement officers. This is an important viewpoint to understand in terms of the justification of any securitising claims. This will help us understand if their experiences of cryptocurrencies are behind any securitising speech acts. It will be very informative to debates about the security threat of cryptocurrencies to learn the extent to which law enforcement officers view them as a threat and, again, in comparison to other tools and methodologies employed by criminals.

4. And finally, research on cryptocurrency users has focussed on individual views, or groups incidentally (such as students), where the view of the collective was not the object of research. There is insufficient academic research in the literature examining how cryptocurrencies may be useful at a community or civil level. This type of research has been done for the Bristol Pound, for example, but is lacking for cryptocurrencies. The focus to date has mainly been on the benefits that cryptocurrencies bring at an individual level, such as faster payments, but there needs to be a greater understanding of how cryptocurrencies could play a role for communities and whether they have something more legitimate to offer in money and society. The threats that cryptocurrencies pose are obviously crucial to the justification of any attempted securitisation, but these threats also need to be considered in contrast to the potential benefits that they offer as well.

These four research gaps and under-explored areas form the basis of the research questions and the main empirical chapters of this thesis. We now move on to the Methodology chapter where the methods for research of each of these gaps are discussed.

3 Methodology

This chapter sets out the research approach and design for this study. However, Chapter 2 provided much guidance for the researcher that is also drawn upon here. The advice and experience of researchers on the dark net is particularly important to this thesis due to the ethical considerations that this site of research demands. As such, the work of dark net researchers specifically contributes to the design of this study, and the ethics of this research is explored in detail in the sections to come.

The first half of the chapter is concerned with the research approach. It begins by explaining why the fundamental choice of a qualitative research design has been made. A short section then follows describing the position, here, to theoretical frameworks - highlighting that empiricism is the focus. These discussions aim to give the reader a sense of the underpinnings of this work. A broad treatment is then given to the strategies of inquiry that have been selected for the four empirical parts of this study. The research approach section then concludes with an in-depth consideration of positionality. The second half of the chapter establishes the rationale for each of the four strands of research through a detailed discussion of their research design. For each, there is an analysis of the most suitable data collection methods, the sample from which data is to be drawn and the data analysis methods that will be employed. Of note, ethics plays a prominent role in this study and so there is a thorough examination of ethical issues for each strand of research as well. Further discussion of positionality is also interwoven throughout.

Chapter 2 showed the extent of the interdisciplinary nature of cryptocurrencies. It also showed that whilst there is a great deal of academic research from a technical perspective, there has been a lack of research from a social science perspective. Further understanding of cryptocurrencies can be gleaned using other methodologies. It is for this reason that this thesis will take a social sciences approach to learn more about this important topic. There has been a growing call in the social science literature on cryptocurrencies to address the imbalance in the technical research (for example, Karlstrøm, 2014: 26; Bashir, Strickland and Bohr, 2016: 355; Abramova and Böhme, 2016; Alshamsi and Andras, 2019; Hayes, 2019; Bailey, Rettler and Warmke, 2021: 9). Some early research has been done but there remain gaps in knowledge, as highlighted in Chapter 2. Lessons and advice from these early studies have played a part in shaping the methodological choices made in this study.

It is worth remembering at this juncture the four strands that were identified in the theoretical framework for research. The first was the narrative of security threat concerning the illicit use of cryptocurrencies. The second was usage on the dark net as the primary focus of illicit activity, the third was that of the view of law enforcement, and the final area was community use (as not all cryptocurrency activity is illicit). We saw in Chapter 2 how these strands will provide a richer analysis of cryptocurrency usage. Examining the securitising speech acts and the extent to which cryptocurrencies are used for illicit activity will help us understand why they are viewed as a threat. Researching the dark net further will enhance our current view of this key area of illicit cryptocurrency usage and studying the view of law enforcement will reduce a knowledge gap. And finally, by focussing on a community, we will achieve a deeper understanding of social usage and the ways in which cryptocurrencies may have something to offer society. But it will be the combination of all these groupings and the analysis of the attitudes and motivations between them, and importantly the differences that there will inevitably be, that will be of greatest interest.

3.1 Research Approach

As has been indicated by the gaps within the literature, this study will employ a qualitative approach. The literature shows a strong call for more research of this type, due to the prominence of technical studies in the community of researchers working on cryptocurrencies. This is clearly not justification for this research approach on its own, and there are several reasons why a qualitative approach is most suitable for this study. The study of cryptocurrencies is relatively new and so this choice of research design is very appropriate as a means of exploring and contributing to the many debates outlined in Chapter 1. It will be useful, here, to include a definition of qualitative research, which will highlight why this approach is most suitable for exploratory work:

> Qualitative research is a means for exploring and understanding the meaning individuals or groups ascribe to a social or human problem. The process of research involves emerging questions and procedures, data typically collected in the participant's setting, data analysis inductively building from particulars to general themes, and the researcher making interpretations of the meaning of the data. (Creswell, 2009: 4)

The problem identified in Chapter 1 is that of money, its relationship to society and the security concerns that surround its usage. If we view cryptocurrencies from the perspective of securitisation theory, as described in the theoretical framework, then we can see that this is a societal problem regarding the institution of money. In terms of the debates about cryptocurrencies, there are research gaps in our knowledge of what different groups think about these issues and how they construct cryptocurrencies through security, and as a kind of security. To explore this, more needs to be learnt about the participants who use these systems. This learning then needs to be analysed to uncover meaning and themes that could otherwise be presumed. This is an inductive approach and is one reason why a quantitative approach is not suitable here. This research does not set out with preconceived theories about the attitudes and motivations of users of cryptocurrencies. One of the aims, then, is to research participants in their own settings, to learn more about them in their own words. The worldview that best aligns, therefore, with the philosophical perspective of this research is social constructivism:

> Social constructivists hold assumptions that individuals seek understanding of the world in which they live and work. Individuals develop subjective meanings of their experiences - meanings directed toward certain objects or things. These meanings are varied and multiple, leading the researcher to look for the complexity of views rather than narrowing meanings into a few categories or ideas. The goal of the research is to rely as much as possible on the participants' views of the situation being studied. (Creswell, 2009: 8)

A governing principle of this study is to contribute to the debates about this topic by focussing on the views of users of cryptocurrencies or those close to them. The opinions of those who commentate on cryptocurrencies are important, particularly from a securitisation perspective, and these views will be explored in Chapter 4. But the desire here is to look wider than just the ‘opinion’ of those removed from cryptocurrency usage, which often dominates the debate and the media headlines, and present a ‘specific version of social reality’ as constructed by the remaining three research groups (Bryman, 2012: 33).

If political and business leaders have constructed cryptocurrencies as a security threat, how does this compare to the constructions of law enforcement, to those who use them on the dark net or even to community use of these new forms of money? The social constructivist approach is also sympathetic to the lens of securitisation theory and also to the literature of economic sociology, where cryptocurrencies, as a form of money, are a complex subject that gives rise to a multitude of views. Bitcoin is a result of increasing ‘monetary pluralism…is multi-faceted, politically contested and sociologically rich in its functions and meanings’ (Dodd, 2017: 36). A constructivist approach motivates this research to explore different groups associated with cryptocurrencies, in order to learn more about what each thinks about these forms of money, and to add to the complexity of the view rather than narrow it. In this way, new ‘realities’ about the security threat that cryptocurrencies pose are discovered. And crucially, we are then able to ask whether these realities support an attempted securitisation, or whether they present a contrasting view and a counterargument for de-securitisation.

3.1.1 Theoretical Framework Approach

It is worth adding some specific detail about the approach taken to the use of a theoretical framework as outlined in Section 1.3. Two main sources shaped thinking towards the application of theory to this thesis. First, Bryman argues that theory provides ‘a framework within which social phenomena can be understood and the research findings can be interpreted’ (Bryman, 2012: 20). Research that does not have a theoretical basis ‘is often dismissed as naïve empiricism’ (2012: 22). The debate that arises here is whether theory should lead the empirical. The second influence comes from critical security studies where this argument is addressed and there is a call to the opposite – ‘to elevate the empirical above the theoretical’ (Salter and Mutlu, 2013: 43). Of note, is that the rationale in critical security studies is explained, in part, through a discussion of the use of securitisation theory as an example. The author contends that there has been an expectation that theory should be central to research but that this comes at a cost, by constricting analysis of specific security problems:

> Sometimes describing something without explaining it is enough to say something politically and intellectually important. Sometimes documenting that something exists or is said or done is enough to contribute to our understanding of what happens in security politics and practice. (Salter and Mutlu, 2013: 43)

This research draws on both positions to formulate an approach to the theoretical framework. Empiricism is the focus here, and theory has been applied only if it does not constrict. In fact, securitisation theory has been chosen because it provides a language and theoretical model to discuss cryptocurrencies as a security threat and to interpret the research data. In this vein, theory is seen as an important way of achieving a more ‘precise understanding’ of the issues (Buzan et al., 1998: 32), rather than a compulsion of discipline. The intention of this study is for the research topic and the data gathered to be the focus of the work, with the theory supplying a framework for analysis and discussion.

3.1.2 Strategies of Inquiry

There are many ways that research strategies of inquiry can be conceptualised and designed (Creswell, 2009: 11; Wolcott, 2012: 14; Bryman, 2012: 45; Salter and Mutlu, 2013: 19). The important point, though, is that the ‘researcher makes a conscious choice as to where to get the best view for the information desired’ (Wolcott, 2012: 14; also Corbetta, 2003: 233). As this study proposes four distinct strands of research, no single strategy is selected as a different design suits each.

The research design for each strand is discussed in detail in Section 3.2, however, it is possible to identify which of the designs offers the best view of the information being sought.

For the research of the security-led narratives about cryptocurrencies in Chapter 4, an archival approach has been chosen as the most appropriate strategy (Wolcott, 2012: 14). Ethnography is a fitting approach for researching illicit usage and the perspective of law enforcement in Chapters 5 and 6 – the former through participant observation and the latter by interviewing. For both groups, this study is interested in understanding their views. Due to ethical considerations, an observational approach without interaction is most suitable for research on the illicit usage of cryptocurrencies – this is examined in detail in the research design for this part of the empirical work. For law enforcement, learning directly from individuals closest to the usage of cryptocurrencies will provide the best information. And in Chapter 7, for the research of the legitimate role that cryptocurrencies could play in money and society, a case study approach is suitable as a specific user community has been identified to explore.

Finally, in terms of broad approach, it may be informative to explain why some of the other possible approaches have not been chosen. Phenomenology is associated most with ‘a detailed description of experiences’ (Creswell, 2009: 193). This study aims to understand more general attitudes and motivations rather than focus on individual experiences, so this approach is not suitable. Grounded theory aims to develop theories – this is also not an aim of this research. And Narrative research does not fit with the purpose of this study either as this work is not aiming to explore the individual ‘stories’ of participants.

The aim of this section has been to indicate the general direction for design as best suited to each of the four research strands. As noted, however, these choices are a guide, and the categorisations are not fixed. Flexibility was reserved to ensure that the methods selected were the most appropriate for the information sought.

3.1.3 The Researcher's Role

Academia favours the view that researchers are not 'detached observers' but rather that they are people who bring their own experiences, histories and even personalities to their work (S. Moser, 2008: 389-90). As such, the researcher should scrutinise the self in order to understand any potential impact on their research. There are two main areas of my background that have shaped my approach to this research. The first is a long-held interest in economics and finance. Some time ago, I studied Business Studies at A-level as well as an undergraduate degree in Management Studies. This interest led me to a role in financial services years later during the financial crisis of 2007-08. I saw first-hand the impact that such a crisis of the financial system can have. I remember the questions that were raised about how it came to be, who or what caused it and whether any individuals were to be held responsible. To an extent, these issues remain unanswered. During the crisis, savers were locked from their money and organisations, from charities to police forces, faced the prospect of losing money they had invested (Wintour & Gillan, 2008). The aftershock of the crisis lasted for many years and continues to this day. In 2011, as an example, Greek lenders saw the amounts they were owed cut in half as the debt was restructured (BBC News, 2015).

These incidents also raised some deeper questions about what money is and who owns or controls the balances someone or some organisation 'has'. It was amongst these times that Bitcoin was launched. It is this background of mine that led to my interest in these questions. And fresh memories of the crisis make me feel that these are important issues worthy of study. For this reason, this thesis is influenced by an economic perspective. These experiences also give me at least an understanding of why alternative currencies came to be or why people think they have value. The impact this has had on my approach to cryptocurrencies is to consider them seriously, without dismissing them due to the fervour and derision that often surrounds them.

The second, and primary, part of my background that impacts this research is my experience as a law enforcement officer. On first inspection, an outsider may think this would mean a bias *against* cryptocurrencies, as a former member of an agency of the state. However, the entire motivation for this study is to open-mindedly examine the issues and debates that are identified in Chapter 1. At the beginning of this research process, in 2017, the narratives surrounding cryptocurrencies appeared to be polarising, sometimes extreme in viewpoint, and, at times, unconvincing. This includes claims, for example, that they were popular with criminals or that they even cause death (Zetter, 2012: BBC News, 2018). It was scepticism of some of the claims, such as the extent of the use of cryptocurrencies in illicit activity, that motivated this inquiry. As a former investigator in the National Crime Agency, I have some experience in working on cases and gathering evidence. This included using the powers given by the state to investigate criminal activities. Contrary to popular belief, the processes in place for collecting information about individuals are very thorough, time-consuming, and take a long time to yield results.

Considering this, when I learnt about cryptocurrencies, I was confused by the claim that they were such a good tool for criminal activity. The idea of an immutable ledger that could be scrutinised by law enforcement at will, without the need to use the power of law to access information, seemed to me to be perhaps useful for policing and not so attractive for illicit use. If you are to carry out an illicit transaction, would you relish a system that leaves a public and permanent record? It was this paradox that served as the foundational motivation for this study. I became fascinated by the debate that exists about whether these new financial innovations are as good for criminal activity as some suggest. This certainly raises the danger of confirmation bias, but I am aware of this and consciously consider this point throughout this thesis in the interpretation of the findings.

Although I had scepticism about the headlines that I had seen, I embarked on this research with an open mind. That is, I did not set out on my research with an advocacy worldview, or with an agenda for reform. I would have been perfectly content if my research added to the security concerns about cryptocurrencies. Likewise, I had no notion of there being any social injustice issues related to this topic, but I am very aware of these issues now that I have delved deep into cryptocurrencies, especially with regard to the monetary aspects. So, whilst I began the research without much of an opinion about the security threat of cryptocurrencies, I certainly do have one now and this becomes clear in Chapter 8.

I should also add that since starting my research I have engaged with many cryptocurrency projects as a user, primarily as a learning experience. I also did a placement with a cryptocurrency project, as well as a fellowship where I ran a cryptocurrency-related start-up idea. Of note, for both of those experiences, I was paid in cryptocurrency, as it was the quickest, cheapest, and simplest option given that both roles had an international dimension. I do, therefore, have practical experience in using cryptocurrencies and believe that there are benefits to them.

My law enforcement background also impacts this study in other ways. Not only has it shaped my areas of interest, but it also affects how I approach this subject. When I have considered the choice of language, especially around illicit activity, I view the words illicit, illegal, and criminal in terms of UK law without, for example, taking any moral angle. That is to say, I use these terms as collective adjectives to enable discussion of cryptocurrency usage. Much is made of the use of cryptocurrencies for ‘criminal’ activity, particularly on the dark net. I have generally chosen to use the words illicit and illegal rather than criminal when discussing this topic as criminal is more of a loaded term with associated judgements. Criminal is still used, though, if it refers more specifically to convicted illegal activity. It is unavoidable to use these terms as this thesis specifically analyses the differences in the usage of cryptocurrencies for legal and illegal activity, as this is a key part of the securitising speech acts. But the use of these words is not intended as any comment on the activities that are described within. For example, marijuana use is legal in some jurisdictions, and many argue whether it should even be illegal. This study does not aim to address or take part in these debates but looks instead at the use of cryptocurrencies by different groups for different purposes.

My law enforcement experience also impacts my views on policing, the criminal justice system, and the deterrence of illegal activity. It has long been recognised in law enforcement that custodial sentencing should not be the only aspect of deterrence. Financial investigation is a standard part of cases, as the crown looks to take back the profits of criminal activity. It is also widely accepted by many that just ‘locking people up’ is not the sole answer to societal problems. I certainly left the NCA with questions about approaches to policing. Again, for this reason, I feel that these are complicated social issues that do not have simple answers. I take this same approach to cryptocurrencies. I think it is important to question why these systems have emerged, why some people choose to use them and to scrutinise any reaction to their existence and utilisation.

Other researchers have similar backgrounds, and it is worth reflecting on their experiences in terms of positionality. Belur (2014: 184) was a high-ranking ex-police officer who published a reflexive piece on the ‘impact of researcher characteristics such as gender, age, ethnicity and status on doing police research’. Status is important in this area of research and four types are identified: insider (a police officer), outsider (a researcher), inside-outsider (a civilian in police employment) and outsider-insider (ex-police officer) (2014: 187, 197). Like Belur, the author of this study is an outsider-insider. This is significant as Belur concludes that of all the characteristics that can affect police research, status as an outsider-insider was more important than all the others and affected every aspect of research. First, researching the police is typically difficult but outsider-insider status enables access. Second, this status affects the willingness of participants to engage. Belur found that some were more open as they felt that the researcher understood the realities of their work. And third, a shared background helped build relationships which affected the quality of response. Belur also shares some ethical recommendations. To maintain integrity, anonymity and confidentiality were ensured and findings were presented as constructive criticism. To avoid any deception, the researcher explained the aims of the study and stated their position as an ex-police officer.

Whilst not a conclusive experiment, it is also worth noting the work of Damsa and Ugelvik (Damsa & Ugelvik, 2017). The two researchers conducted independent research in the same Norwegian prison and analysed their findings to ‘reflect on researcher reflexivity and positionality’ (3). Both are white and middle-class, but Damsa is an older, male criminologist from Norway and Ugelvik a younger, female Romanian. They conclude that positionality did not have a significant impact on their research findings, although it did affect their experience of the research. My position as a former NCA officer certainly impacted trust and access in terms of the law enforcement research I was able to do. I also thought about the risk that my previous role might influence how critical I could be of my former employer. Similarly, I considered if there would be any issues criticising or using the words of former colleagues. I do not think that my former status affected the results of the research, and this is in part due to the research design which is discussed in detail for each strand in the next section, 3.2.

The desire for this study has always been to add to the debates about the existence of cryptocurrencies and the security threat they pose with rigorous academic research, regardless of which side of the discussion this may support. This presents an alternative view of the security threat of cryptocurrencies and one purpose, therefore, of this chapter is to enable the reader to make a judgement on the reliability and validity of this study by being clear about my approach and background (May and Pope, 1995: 110). The research design in the second half of this chapter also addresses further potential concerns. Sample selection is discussed, as are collection and analysis methods, as well as ethics. The aim of this is to ensure that the research has been conducted in an open and thorough inductive manner, with results that were determined by the material.

3.2 Research Design

The second half of this chapter describes where data will be collected from, what methods will be used and how the data will be analysed. As each of the four research strands was explored differently, they are considered in turn. Ethics is of particular importance to the research of illicit activity in Chapter 5, so each strand has an individual ethics subsection as well.

3.2.1 Chapter 4: The Security Narratives

As cryptocurrencies gained more mainstream interest in 2017 as I began my PhD, I became aware of striking headlines about cryptocurrencies. The narrative was often dominated by security concerns about the use of cryptocurrencies, and concern about their use on the dark net was a prominent fear. Here, ‘narrative’ is taken to mean securitising speech acts, rather than in the sense of a strategy of inquiry that aims to tell a story or give an account of someone’s personal experience (Bold, 2012). The analyst in securitisation theory aims to examine these speech acts to gain a clearer understanding of ‘who’ is claiming that something is a threat, on what grounds and to identify what it is that is threatened. As already discussed, my background drew me to the subject, and I was curious about how useful they would actually be for illicit activity. I began this strand as my first piece of research on cryptocurrencies, aimed at learning more about their illicit use. This work, therefore, was very exploratory as I delved into the topic for the first time.

3.2.1.1 Data Collection Method

As this first research step was exploratory, only one of the three main broad data-gathering techniques in qualitative research made sense – the use of documents (Corbetta, 2003: 204). Here, ‘documents’ generically means media of all kinds and the types of documents researched are discussed in the next section. At this early stage of research, it would not have been possible for me to have identified any participants to observe or to ask questions of. Also, as I wanted to explore the extent to which cryptocurrencies are used illicitly, the research and claims of others were of interest to me. I wanted to explore what others had already said or written about the threat of cryptocurrencies, but via the lens of securitisation theory and the speech act. Therefore, data-gathering through the use of open-source documents was selected as the most suitable technique. There would likely be enough documents, of varying types, in the public domain to be able to conduct a first-step exploratory analysis of the narrative surrounding cryptocurrencies as a security threat. This approach also did not require any special access or the permission of gatekeepers to view documents.

3.2.1.2 Sample Selection

There were two broad categories of documents that I was interested in researching. The first was media documents about the security threat that cryptocurrencies potentially posed, including reporting of what official figures had said about them. The securitising narrative that I had become aware of primarily concerned the threat posed by cryptocurrencies in facilitating illicit activity, but I was also interested in any other grounds that were given for any securitising speech acts. The media often reported on the comments of public officials. The purpose of the research was to understand what was being said about cryptocurrencies and to learn in what ways they considered cryptocurrencies a threat. Importantly, in terms of securitisation theory, was also the matter of 'who' was making the claims. This becomes an important consideration later in the thesis.

The documents were found through two main methods. Firstly, as an active researcher on the subject at the time, I was aware of major news headlines about cryptocurrencies that had a lot of public attention. I also found documents through internet search engines. Using 'Bitcoin' and 'Cryptocurrency' as the main search term, I combined them with 'crime terms' and the names and positions of key western officials from the memorable alliance. US officials were of particular interest due to the position of the US dollar. A variety of media outlets were searched, including some specific cryptocurrency news platforms. However, many articles were published by traditional media organisations in the US and the UK. Reporting from these larger, established outlets was preferred to ensure that the documents came from more reputable sources. The documents cited in Chapter 4 were chosen to reflect the views and comments of the key officials in relation to securitisation theory. In this way, they serve as a foundation for the rest of the thesis, not as a categorisation of every article published. A summary of the key document search terms is provided in Table 1:

Table 1: Document Search Terms

Cryptocurrency Terms	**Crime Terms**	**Key Officials**	**Media Outlets**
Bitcoin	Criminal	Fed Chairman	BBC
Cryptocurrency	Illicit	US Treasury	CNBC
	Money Laundering	US Banks	WSJ
	Dark net	UK Officials	Bloomberg
	Security Threat	Donald Trump	NY Times
	Drugs	Janet Yellen	Forbes
		Steven Mnuchin	Bloomberg
		Jamie Dimon	Financial Times
		Larry Fink	The Independent
		Mark Carney	The Guardian
			Wired
			Coindesk
			Bitcoin Magazine

The second broad category of document for data-gathering was official reporting. Here the goal was to gather information from reputable sources about the illicit use of cryptocurrencies. I was therefore interested in academic research, as well as official reporting from other organisations with an interest in the topic. Papers and reports were found during the literature review, using bibliographies and common academic repositories. This reporting came from a variety of sources, such as law enforcement agencies, blockchain intelligence companies and also other supranational organisations (UN, Europol for example). Again, as an exploratory piece of research, I wanted to get a broad understanding of the security threat of cryptocurrencies, rather than a piece of my own technical research about a specific threat such as ransomware. Only with a wider view can an assessment be made about the validity of the justification of any speech acts. There was already a great deal of reporting and research available, and the aim was to analyse this as a larger body, in order to gain an understanding of the fuller set of issues and also the scale of the illicit use of cryptocurrencies. The sample selection described was suitable for this purpose.

3.2.1.3 Data Analysis

Document analysis is a recognised qualitative technique for collecting and analysing existing research data (O'Leary, 2017: 496). For this strand, I followed O'Leary's eight-step process for interrogating texts (499). The majority of the documents were found online, and copies were saved into Mendeley, a programme that can be used for reference management and as a library for documents. Documents were then organised into relevant folders within the library. All downloads were taken from official websites of the original source to ensure authenticity. Each source was considered for potential bias – this was more relevant for media sources. As a general strategy, documents were chosen from more established media outlets, good-quality research publications and from reputable companies and organisations. This process included assessing the author of the document to ensure that the document was suitable for use. Through all these steps the documents were screened for credibility.

My approach to analysing the documents was 'interviewing' them based on my research questions (498). By asking the research questions of the documents, I was able to highlight passages of text within Mendeley. Using Mendeley, I could use different colours to highlight relevant text and add notes to sections of interest. This worked as a research journal in effect, although I also used a paper-based journal as well for observations and notes. As a large part of this strand was concerned with the quantitative scale of illicit use of cryptocurrencies, I found that Mendeley was sufficient for this research, and I did not need to use a qualitative data management program. I also found it sufficient for gathering and managing qualitative data regarding narratives. Mendeley was a useful tool which I continued to use throughout my PhD, although I did use other qualitative programs in later chapters.

There were two key aims of this chapter as they relate to data analysis. The first was to search for and identify securitising speech acts. During my literature review, I came across many headlines and papers about security issues in cryptocurrencies and added them to my library. I also actively searched for them online using academic and regular search engines. This revealed both media articles of interest as well as academic papers about the security threat of cryptocurrencies. In terms of securitisation theory, ‘who’ said or made a security-led claim about cryptocurrencies was of particular note, especially if they were from the state or a representative of the state. For example, a speech by a government employee talking about cryptocurrencies may be reported in the media. The content and reasoning of the speech are of interest, but so too is ‘who’ they are, their position and what organisation or department they represent. Importantly though, as well as the ‘who’, I was analysing any security-led speech acts to understand the reasons given as to why cryptocurrencies were being presented as a security threat. I expected to see concerns about illicit use but also wanted to learn about what other threats were identified. It was also important to assess which of the threats was most common or positioned as the most pressing. This was done by reader assessment of the documents, as opposed to a quantitative approach. This was sufficient to achieve a good appreciation of which threats were most dominant in the documents.

The second key aim of the chapter in terms of data analysis and securitisation theory was to examine the justification of the threat. The securitising actor claims that something is a threat, and the analyst must assess whether the actor is justified in that claim. To do this, the sources were examined to understand how great the threat is. In this part of the analysis, the focus moved from the media documents to academic and organisational reporting. Studies that explored the threat of cryptocurrencies were of the most interest to gain a better understanding of the extent to which cryptocurrencies were being used for security-related threats. Crucially, a common flaw identified in the literature was that cryptocurrencies are often described as a threat but without any quantifiable data or any comparison to existing alternatives. The analysis, therefore, aimed to address both of these failings to reveal the extent to which the potentially securitising speech acts were justified. This work becomes an important foundation for the rest of the thesis and the later analysis that follows.

3.2.1.4 Ethics

As this strand is an exploratory piece of research on secondary data, the ethical considerations were minimal, certainly in comparison to some of the later work. No confidential or personal documents were assessed as part of this chapter. All of the documents were open-source and so there were no access requirements. Furthermore, as secondary data analysis, there was no participant interaction. Any individuals quoted in the chapter are public figures, with the source most often the media. Consequently, there are no privacy issues regarding the materials used. Other research strands had more central ethical considerations and those issues are discussed in the relevant sections later in this chapter.

3.2.2 Chapter 5: Cryptocurrency Usage on the Dark Net

The dark net has been a popular research topic for academics, particularly in regard to the sale of illicit narcotics. Despite this, there is often confusion over exactly what is meant by the term. The dark net refers to areas of the internet that require special software or mechanisms to access (Owen and Savage, 2015: 1). Tor is the most famous of these and is often used synonymously with the dark net - even though there are others such as Freenet and I2P (Gehl, 2018: 1). Tor requires open-source software to access it, enabling enhanced privacy on the internet by routing 'traffic through multiple servers and encrypt[ing] it each step of the way' (Tor Project, 2019). As well as providing anonymous access to the internet, Tor also enables people to host websites anonymously – the Tor hidden services (Owen and Savage 2015: 2). Whilst Tor can be used for many social activities (for example forums, activism, or censorship avoidance), it can also be used for illicit purposes, such as the provision of marketplaces for the sale of illegal goods and services. Dark nets, therefore, are a logical focus for the use of cryptocurrencies in crime.

The Tor dark net hosts most of the marketplaces where illicit trade takes place, but not all (Owen and Savage, 2015: 2). In 2019, the Libertas marketplace moved to I2P from Tor, citing its propensity for denial of service attacks (Cimpanu, 2019). Tor, though, was chosen as the focus of this part of the study as it hosts the bulk of illicit activity. This limits the scope of inquiry if minority markets like Libertas are not focussed upon. A natural question to ask is whether this limitation would affect research findings. That is, would the insight gained from research of other dark nets, such as I2P, reveal a materially different outcome to that which could be gained from the Tor dark net alone? Given the size of the Tor dark net in comparison to others, and that most marketplaces are on Tor, the assumption here is that research on Tor was sufficient and most suitable for the exploration of attitudes and motivations concerning the usage of cryptocurrencies, especially for illicit purposes.

3.2.2.1 Data Collection Method

Other than the site of research choice on the dark net, two other key decisions guide the methodology here. First, where can this information be obtained from within the dark net. And second, how to gather the information desired. As described, there is a significant body of research on the dark net and much that can be learned from the experience and guidance of other researchers. Of particular use is Gehl's field guide for studying the dark net (2018). Gehl implores for more 'humanistic inquiry' (2) and provides advice based on many years of studying the dark net. The author notes that ethnographic work on the dark net has mainly been focussed on marketplaces and not on other sites, such as 'forums and social networking sites' (3). This study aims to explore the attitudes and motivations toward the usage of cryptocurrencies and so forums and social networking sites on the internet and dark net are of great interest. They are where discussion about the dark net takes place, including how to use the system (6). This includes discussion of cryptocurrencies, as the payment method of the dark net, and as such forums were, therefore, the most suitable target for research.

There are two broad strategies used by researchers to explore online activity. The first is active engagement. This approach comes with significant implications, particularly on the dark net. Barratt and Maddox (2016) conducted such a study and provide many insights into the practicalities and realities of this method. Their work required substantial preparatory work: developing suitable and secure communications, ensuring the privacy of traffic, and trying to achieve credibility with the community being researched. On this latter point, the researchers were open about their role as researchers; providing a study statement, their university email addresses and even their real names (706). Most significantly, the researchers were met with some negativity from their engagement – including ‘graphic death threats’ (711). This presents a serious ethical and personal safety dilemma. In a study of a dark net social network, Gehl chose to abide by the network’s own rules – ‘No personal information. No real names’ (2016). Active engagement, therefore, is a difficult strategy. If you declare your identity this is a serious personal safety issue and if you are active, yet anonymous, this raises further ethical questions.

With this in mind, the second main approach that can be employed to explore underground and dark net forums is to do so without active engagement. Typically, researchers use ‘web scraping’ technologies to download information from the dark net and the internet. Web scraping simply means visiting websites and downloading content, often in an automated fashion. This can include copies of web pages on a marketplace or conversation threads from a forum. Moore and Rid used scraping in their study, for example (2016). Whilst scraping sites oneself is an option, there are a number of repositories that have stored the results of scraping and made them publicly available to save the repetition of effort (Gehl, 2018: 6).

Considering the experiences of previous researchers, which method is most suitable and would yield the best information for this part of the study on the use of cryptocurrencies on the dark net? Given my background in law enforcement, an identified, active engagement strategy would unlikely be met with a positive response and would very likely draw significant personal risk. Furthermore, an anonymous active engagement brings substantial ethical concern and requires extra preparations and time to try and find participants. This part of the study is exploratory and datasets of forum posts that have already been captured are suitable for this purpose. They offer a magnitude, breadth, and temporal scale far greater, and better suited to exploratory work than an active engagement could offer. For these reasons, research of a dataset without active engagement was selected as the best option. Active engagement would have perhaps been more suitable for a follow-up study if more in-depth probing of specific issues was required.

Analysing a dataset also offers the added advantage that the information is obtained with less influence from the researcher. That is, from a positionality perspective, participants would not be influenced by my law enforcement background, nor would they be responding to questions that could be leading or biased. Any pre-collected material needs, of course, to be analysed and the methods, such as choosing search terms, must be thorough and examined for bias. Active engagement, in contrast, has the potential to alter the reaction of participants, especially if identity and purpose are revealed. Furthermore, an archive of pre-scraped data is particularly suitable here as the data covers a wide period, from the early use of cryptocurrencies up to more recent times.

Relating this to the literature on social research design, analysis of internet and dark net datasets falls, to some varying degree, into direct observation and the use of documents. Participant observation has been described as the central technique of qualitative research (Corbetta, 2003: 235; Wolcott, 2012: 14). For Corbetta, there is a distinction to be made between observation and participant observation; namely, that the latter involves interaction with the participants (Corbetta, 2003: 235). In this regard, the method that was used is observational, as there was no ‘participation’ by the researcher with dark net users. This could also be described as documentary research. The argument here is that analysis of conversations on forums bears similarity to both methods, albeit not fitting neatly into traditional definitions of either.

3.2.2.2 Sample Selection

The selection of the Tor dark net as the site for study was sufficient to achieve a representative sample of opinions on cryptocurrency usage on Tor. That is, it was not felt necessary to specifically research dark nets other than Tor to find the information that this research required.

Similarly, there are many open forums on Tor and the main internet providing ample material for research, without needing to take additional attempts to delve deeper into Tor, such as by trying to access restricted areas. This work was exploratory and had not been done before with regard to cryptocurrencies. As such, it is hoped that the research provides a base layer that other researchers may wish to take further in due course. But for this research strand, existing scraped datasets were sufficient.

There are a number of scraped datasets that could have been used for research. For example, Gehl describes one 50GB source covering dates between 2011-2015 (2018: 6). Another extensive dataset has been assembled by Cambridge University's Cybercrime Centre. They describe their dataset as follows:

> We "scrape" a number of publicly available underground forums where there is discussion of cybercrime and advertising of the results of cybercrime. Some of these forums have been operating for many years and we have now amassed a complete collection of posts... Currently we have over 40 million posts, some dating back more than 10 years. (University of Cambridge, 2019)

The Cambridge data has been professionally collected and covers a more extensive period than the other dataset mentioned. For these reasons, it was chosen as the sample for research. The dataset from the Cambridge Cybercrime Centre is called CrimeBB and it was created in recognition of the fact that prior research had relied on insufficient and out-of-date datasets (Pastrana et al., 2018). Underground forums provide a place for people to discuss and exchange information, products and services, which are sometimes of an illicit nature – as such, they help researchers better understand 'behaviours of offenders and pathways into crime' (2018: 1845). CrimeBB was created using a crawler called CrimeBot, which was specifically designed for the task:

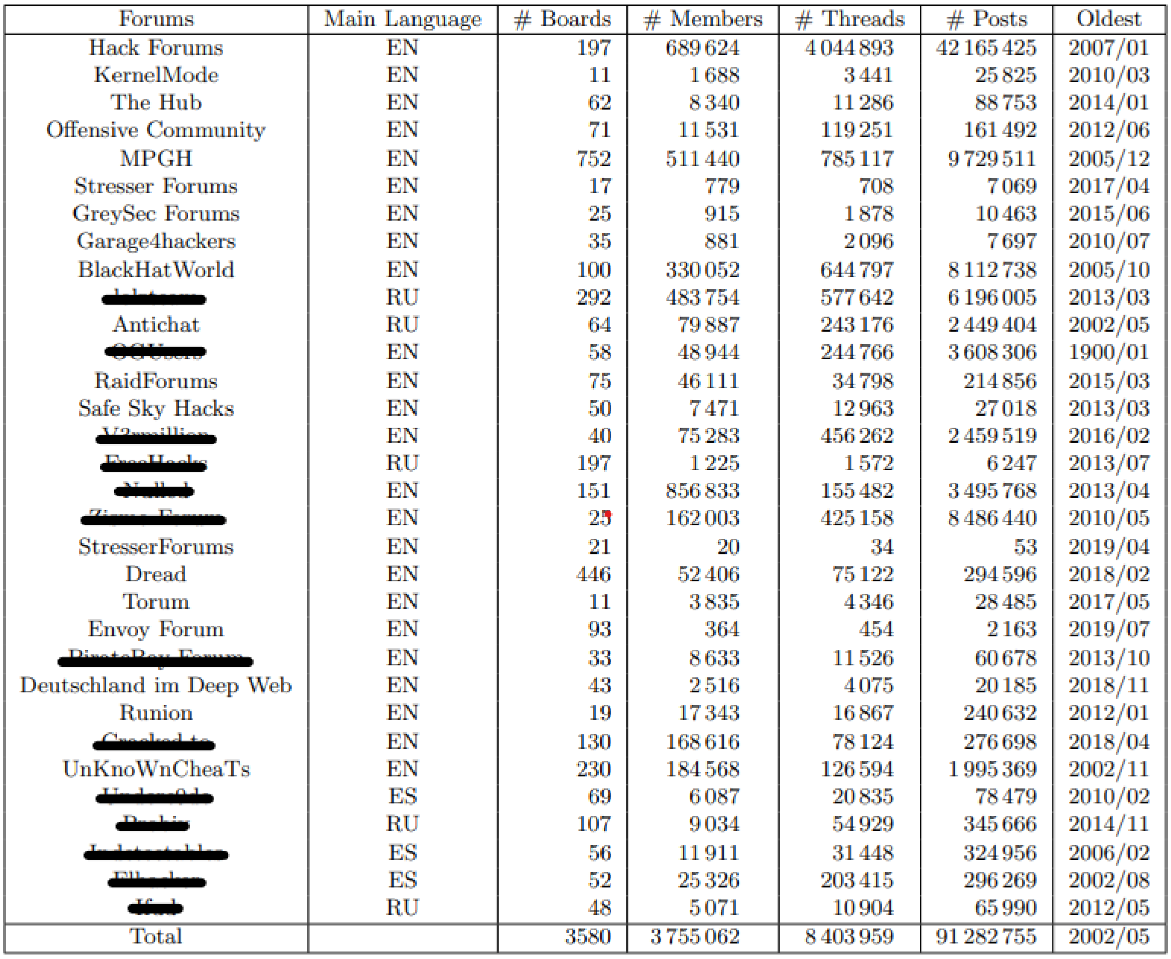
> CrimeBot is implemented in Python and Bash scripts, using Selenium to automatically fetch and store HTML pages, and XPath to scrape the content. A PostgreSQL database with an encrypted filesystem running on FreeBSD is used for storage. (Pastrana et al., 2018: 1848)

CrimeBot regularly updates CrimeBB with content from the sites visited. Initially, the database had over 48 million posts, 4.5 million threads and 1 million accounts drawn from four forums, covering a timespan of a decade (2018: 1846). CrimeBot is given a main URL to visit and then it identifies the URLs of any sub-forums. It then fetches the web pages and updates the database with the contents. The contents include details about the forum, the threads captured, the posts and the members. Cambridge Cybercrime Centre now make this data available to other researchers ‘under a legal agreement, designed to prevent misuse and provide safeguards for ethical research’ (2018: 1845).

The dataset continues to grow as more forums are included and more recent scrapes add to the 100 million posts collected. In 2019, CrimeBB had data from fifteen underground forums, such as Hackforums which is the largest of its kind in the English language (Pastrana et al., 2019: 465). The Cambridge Cybercrime Centre has detailed instructions available about CrimeBB and CrimeBot (Pastrana & Vu, 2021; Pastrana et al., 2018), which include full descriptions of the structure of the datasets and the technical workings of CrimeBot. There is also a detailed table of all the data fields that are scraped from the forums. For this strand of research, I was primarily interested in the ‘content’ field, i.e., the text content of forum posts. Additionally, other metadata was also useful such as a ‘timestamp’ of when the post was written, and ‘thread’ and ‘post’ identification numbers (threads being linked collections of individual posts). There is information scraped about the members of the forums, but this was not data I analysed, nor is it referred to in any of the work due to ethical considerations which are discussed fully in Section 3.2.2.4.

At the time that I was given access to CrimeBB, there were datasets for eighteen underground and dark net forums. These are shown in Table 2 (Pastrana & Vu, 2021), with subsequently added forums blacked out. CrimeBB is one of the largest datasets available to researchers, covering a wide timespan and a variety of different internet and dark net forums:

Table 2: Summary of CrimeBB



Forums	Main Language	# Boards	# Members	# Threads	# Posts	Oldest
Hack Forums	EN	197	689 624	4 044 893	42 165 425	2007/01
KernelMode	EN	11	1 688	3 441	25 825	2010/03
The Hub	EN	62	8 340	11 286	88 753	2014/01
Offensive Community	EN	71	11 531	119 251	161 492	2012/06
MPGH	EN	752	511 440	785 117	9 729 511	2005/12
Stresser Forums	EN	17	779	708	7 069	2017/04
GreySec Forums	EN	25	915	1 878	10 463	2015/06
Garage4hackers	EN	35	881	2 096	7 697	2010/07
BlackHatWorld	EN	100	330 052	644 797	8 112 738	2005/10
[redacted]	RU	292	483 754	577 642	6 196 005	2013/03
Antichat	RU	64	79 887	243 176	2 449 404	2002/05
[redacted]	EN	58	48 944	244 766	3 608 306	1900/01
RaidForums	EN	75	46 111	34 798	214 856	2015/03
Safe Sky Hacks	EN	50	7 471	12 963	27 018	2013/03
[redacted]	EN	40	75 283	456 262	2 459 519	2016/02
[redacted]	RU	197	1 225	1 572	6 247	2013/07
[redacted]	EN	151	856 833	155 482	3 495 768	2013/04
[redacted]	EN	25	162 003	425 158	8 486 440	2010/05
StresserForums	EN	21	20	34	53	2019/04
Dread	EN	446	52 406	75 122	294 596	2018/02
Torum	EN	11	3 835	4 346	28 485	2017/05
Envoy Forum	EN	93	364	454	2 163	2019/07
[redacted]	EN	33	8 633	11 526	60 678	2013/10
Deutschland im Deep Web	EN	43	2 516	4 075	20 185	2018/11
Runion	EN	19	17 343	16 867	240 632	2012/01
[redacted]	EN	130	168 616	78 124	276 698	2018/04
UnKnoWnCheaTs	EN	230	184 568	126 594	1 995 369	2002/11
[redacted]	ES	69	6 087	20 835	78 479	2010/02
[redacted]	RU	107	9 034	54 929	345 666	2014/11
[redacted]	ES	56	11 911	31 448	324 956	2006/02
[redacted]	ES	52	25 326	203 415	296 269	2002/08
[redacted]	RU	48	5 071	10 904	65 990	2012/05
Total		3580	3 755 062	8 403 959	91 282 755	2002/05

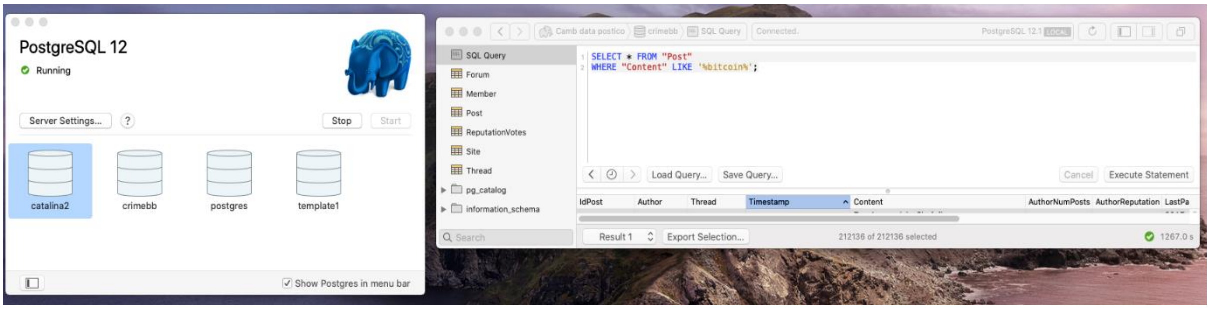
3.2.2.3 Data Analysis

Many other academic researchers have approached and studied the digital world. As the internet has grown, social networks have become commonplace and a popular area for sociological research. This led to the use of Social Network Analysis (SNA) and network theory in research on the internet (Pink et al., 2015: 134). These approaches are not suitable for this study as the relationships between individuals and the structure of forums are not under investigation. More widely, Pink et al. imagine research on the internet as a study of experiences, practices, things, relationships, social worlds, localities and events (2015). Analysis of cryptocurrency usage on underground and dark net forums could be studied from a variety of these perspectives. I did not explore the forums as social worlds or investigate events but was instead interested in cryptocurrencies as technological ‘things’ and primarily analysed the data from a user perspective to learn more about their experiences and relationship to cryptocurrencies. I wanted to explore what users thought about cryptocurrencies, their usefulness and why and how they used them.

Qualitative content analysis was used to make sense of the selected CrimeBB data. This inevitably relied on my experience of the subject to analyse and determine what is relevant or useful in terms of the research questions. This technique has been used by other researchers of the internet, as explored further in Chapter 2 (see Baur et al., 2015; Bancroft, 2017; Van Hout and Bingham, 2014; Maddox et al., 2015; Bancroft and Scott Reid, 2016; and Hutchings and Pastrana, 2019 where coding is used for the analysis of CrimeBB).

> Coders must draw upon their everyday knowledge as participants in a common culture in order to be able to code the material with which they are confronted. (Bryman, 2012: 306)

A central pillar for most types of qualitative data analysis is coding or indexing (Bryman, 2012: 575). This can be done manually but due to the amount of data to review, I chose to use software to assist with the coding process. The Cambridge dataset consists of more than 100 million posts so it would not be possible to read all the material in detail to code it. For this reason, this strand of research used a three-step approach to textual data analysis. The first challenge was how to analyse the 100 million plus posts. As it was not possible to read them all, the posts had to be searched for relevant material which could then be analysed in further detail. To achieve this, all the posts were added to a PostgreSQL database. This is an open-source relational database, capable of handling the amount of data involved. Microsoft Excel, for example, is not suitable as it can only hold a little over a million rows of data. With all the posts in Postgres, the database was then interrogated using structured query language (SQL), a programming language for relational databases. To do this, queries were written in SQL to return content that matched the requirements. The question that follows is what terms were used and how were they selected in a way that did not result in bias or an unfair representation?



```
SELECT * FROM "Post"
WHERE "Content" LIKE '%bitcoin%';
```

Figure 2: CrimeBB Database in Postgres and a SQL Query

The first step of the methodology adopted here was to test the database with common search terms related to the topic. Obvious terms included ‘Bitcoin’ and ‘cryptocurrencies’. From experience of trying this, ‘Bitcoin’ was selected as a primary search term that reduced the 100 million posts down to over 200,000 - a much more manageable number that could then be analysed in more detail. This may seem simplistic at first glance but makes a lot of sense if scrutinised further. First, Bitcoin was the earliest cryptocurrency. As the posts go back several years, there was a time when Bitcoin was the only currency and so this must be the search term for this period. Ethereum for example, the second cryptocurrency by market capitalisation, was only created in 2015 some six years after Bitcoin was launched. Second, by market capitalisation, Bitcoin to this day accounts for over two-thirds of the entire cryptocurrency market (Coinmarketcap, 2020). And third, with regard to the dark net, Bitcoin is the only currency that is accepted by all vendors. For all these reasons, ‘Bitcoin’ was an appropriate search term to narrow down the 100 million posts to those related to this study. To test this further, other currencies (Monero and ZCash – two privacy coins) were also checked against the data. Two points that emerged are worth noting: first, searching with other currencies did not produce many results and second, the posts discovered also contained ‘Bitcoin’ within them. That is, these smaller currencies were covered by the more general term ‘Bitcoin’.

A fair challenge to this method is how do you know that you are not missing important material that is not covered by the search term selected. The second and third steps of the methodology address this concern. For the second step, the data was analysed using IBM’s SPSS Modeler. This software tool uses text analytic capabilities to extract and organise key concepts, and to group the concepts into categories (IBM, 2019). IBM SPSS Statistics is a well-known quantitative data analysis tool that has been used by researchers for years (Bryman, 2012: 330). IBM SPSS Modeler adds to this range of tools with other capabilities that can be used for qualitative research. In 2014, researchers (Baur, Breitsprecher and Bick: 6) analysed the growing text analytics market and identified IBM SPSS Modeler as one of the four main offerings. The research highlights the wide range of topics (including health care, law enforcement and politics) where text analytics has been used in published research (Baur, Breitsprecher and Bick, 2014: 2). In one paper, researchers used IBM SPSS Modeler to analyse text collected from ‘Yahoo! Answers’ (Oh & Park, 2013). They used the tool as ‘an automatic way to analyse data, using the predictive models contained in the software…by extracting words and concepts from texts and identifying the relationships between them’ (2013: 2). The researchers felt that SPSS Modeler was a useful tool for extracting the main concepts using the provided vocabularies, but it required some manual analysis too, to ensure important content was not missed (2013: 4). Other researches have used SPSS Modeler to analyse data about electric vehicle customers (Qiu et al., 2014).

SPSS Modeler can be used on large unstructured datasets using built-in vocabularies. For example, the dictionaries include synonyms, so the tool can group terms so that their combined relevance becomes apparent. But the tool is more advanced than using simple synonyms or statistics of the most common terms. SPSS Modeler uses linguistics-based text mining to provide better categorisation. For example, a simple tool may take the word ‘reproduction’ and include a synonym such as ‘birth’. But Modeler can understand the language context i.e., that in this case reproduction is about making copies and so birth is not a synonym. The text mining algorithms are proprietary, so it is not possible to analyse the code to reveal exactly how the tool works and this is an accepted limitation (IBM, 2021a). When the tool processes data, it produces ‘concepts’ which are the building blocks for ‘categories’. For example, a ‘concept’ of ‘seat’ would include material about ‘seat belts’ or ‘seat belt buckles’. Or a concept of ‘price’ might include documents that have multiple common terms, such as ‘price and ‘availability’. Concepts are grouped into higher-level ‘categories’ (IBM, 2021b). In this way, SPSS Modeler can identify common and connected terms to reveal the main concepts within categories of information.

I used SPSS Modeler to process the ‘Bitcoin’ posts to identify the key concepts in the material. In essence, if the first step takes a pre-chosen search term (i.e., ‘Bitcoin’), this tool analyses all the material to identify the search terms using the built-in vocabularies and data mining techniques described in the previous paragraph. By using SPSS Modeler, a key concept may be revealed that had not been previously thought of. These terms can then be put into new SQL queries to check that important material has not been missed. Figure 3 shows a concept map generated in SPSS Modeler – you can see some of the concepts most closely connected to ‘Bitcoin’. I was then able to review the concepts manually. Here, some were not of particular interest such as ‘png’ or ‘post’. But where the tool was useful was in identifying other terms such as ‘btc’ (a trading abbreviation for Bitcoin), ‘paypal’ and ‘money’. Interestingly, ‘paypal’ becomes significant in the analysis of Chapter 5, even though it was not originally chosen as a search term.

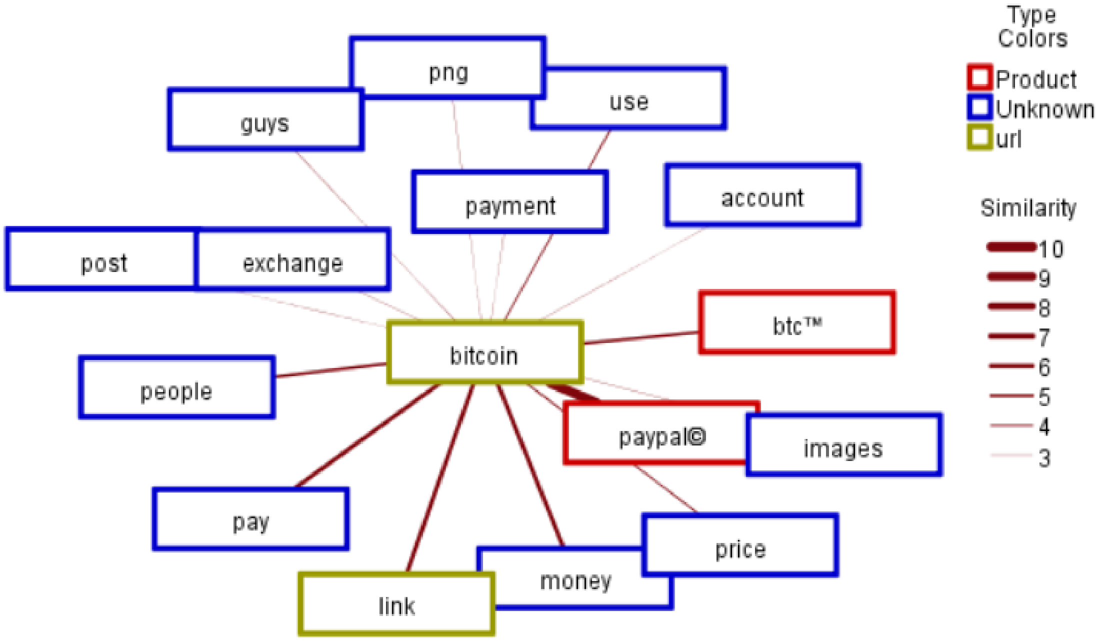
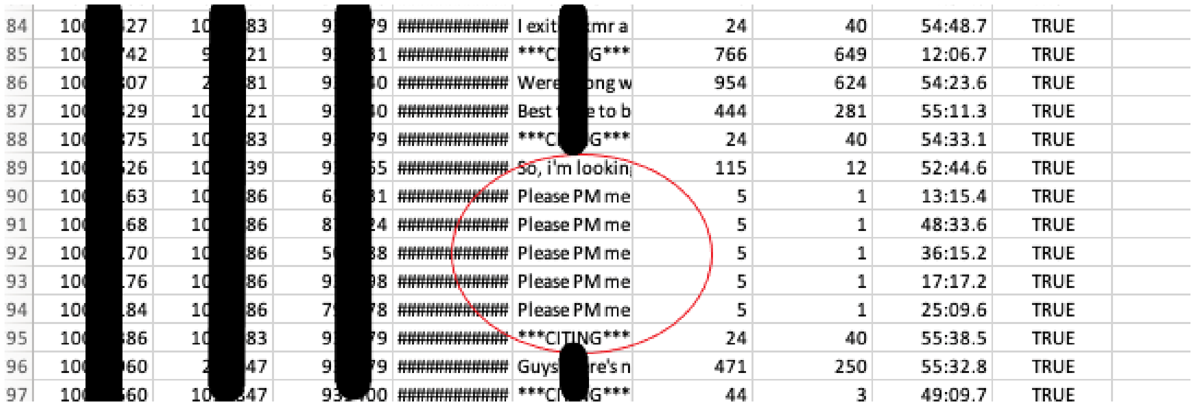


Figure 3: Concept Map From 'Bitcoin' Search Term

Using the categories from SPSS Modeler and my own experience, a final selection of search terms was chosen (the terms are described in Chapter 5 and shown in Table 4). These terms were then used in SQL queries to return data of interest. For small forums with less than 1,000 ‘Bitcoin’ results, all of the search terms were searched for individually in the forum database. For the larger forums, the search terms were combined with the master term ‘Bitcoin’ in order to return a smaller set of results. For example, Hackforums had 177,000 ‘Bitcoin’ results (of note, this is not a dark net site). This is too much to code, so SQL statements were written to search for ‘Bitcoin’ AND each of the other search terms. For Hackforums, this resulted in a more manageable selection of 14,000 posts. This method effectively expanded the search for the smallest forums and reduced it for the largest forums. This was necessary as the smallest forum only returned 58 ‘Bitcoin’ results, in comparison to Hackforums’ 177,000. Using this method for each of the forums reduced the 200,000 ‘Bitcoin’ posts to 23,000 posts.

The data was then manually analysed in the third step. Here, the reduced posts from Postgres were extracted to Excel spreadsheets. A different worksheet was used for each underground or dark net forum analysed. The data was then manually cleaned to reduce the number of posts to those with interesting content. Some posts mention cryptocurrencies and Bitcoin but have no content. An example could be an advert for a malicious service. Similarly, one advert or post may be repeated many times and the duplicates can be deleted. Manually looking through the remaining posts then revealed content of interest relating to the use of cryptocurrencies on these underground and dark net forums. In most cases, this content was discussion from topic threads. The threads themselves were then also examined in Postgres, to go deeper from the search term that identified them. Similarly, the discovery of interesting material also revealed new search terms that were then sent back to Postgres for a new query.



84	10[redacted]27	10[redacted]83	9[redacted]79	############	I exit[redacted]mr a	24	40	54:48.7	TRUE
85	10[redacted]42	9[redacted]21	9[redacted]31	############	***C[redacted]G***	766	649	12:06.7	TRUE
86	10[redacted]07	2[redacted]81	9[redacted]0	############	Were[redacted]ong w	954	624	54:23.6	TRUE
87	10[redacted]29	10[redacted]21	9[redacted]0	############	Best [redacted]e to b	444	281	55:11.3	TRUE
88	10[redacted]75	10[redacted]83	9[redacted]79	############	***C[redacted]G***	24	40	54:33.1	TRUE
89	10[redacted]26	10[redacted]39	9[redacted]65	############	So, i'm lookin	115	12	52:44.6	TRUE
90	10[redacted]63	10[redacted]86	6[redacted]31	############	Please PM me	5	1	13:15.4	TRUE
91	10[redacted]68	10[redacted]86	8[redacted]24	############	Please PM me	5	1	48:33.6	TRUE
92	10[redacted]70	10[redacted]86	5[redacted]38	############	Please PM me	5	1	36:15.2	TRUE
93	10[redacted]76	10[redacted]86	9[redacted]98	############	Please PM me	5	1	17:17.2	TRUE
94	10[redacted]84	10[redacted]86	7[redacted]78	############	Please PM me	5	1	25:09.6	TRUE
95	10[redacted]86	10[redacted]83	9[redacted]79	############	***CITING***	24	40	55:38.5	TRUE
96	10[redacted]60	2[redacted]47	9[redacted]79	############	Guys[redacted]re's n	471	250	55:32.8	TRUE
97	10[redacted]60	10[redacted]47	93[redacted]00	############	***C[redacted]G***	44	3	49:09.7	TRUE

Figure 4: Example of Repeated Posts in Excel for Cleaning

The three steps provided a combination of self-selected search terms based on the topic, automated categorisation, and search term feedback from the material itself. This resulted in a robust method of analysis that captured a fair representation of discussions. The result of the three-step process was a final selection of 16,405 posts for coding. To complement this process, a diary was also kept to record decisions made regarding the data. Initially, the posts were exported into Nvivo, a popular qualitative program, but the software struggled to handle the large amount of data. Each coding selection took more than 30 seconds to process. This was unworkable so an alternative was needed. Other tools such as Taguette and CATMA were considered but there were concerns about where the data would be stored. Due to the ethical considerations and potential sensitivity of this strand, a local program that did not connect to any external service was preferred. QDA Miner was such a tool and, on trial, was found to be capable of handling the data. It was therefore used as the qualitative tool for coding.

The coding process for the CrimeBB chapter was similar to that described in the previous strand, albeit using different software. QDA Miner is similar to Nvivo, and it enables the researcher to manually code selected items of text. A structural coding technique was used based on the research questions, rather than attributes such as location, for example. Topic coding was also used as the material was read. This enabled an overall view of the use of cryptocurrencies, which was the aim. A second coding cycle using pattern coding grouped codes together where there was commonality.

An important part of the process was to do the coding alongside taking written analytical notes in a journal. As well as coding posts, I wrote down comments about issues that struck me as of particular interest. For example, I have a starred note in my journal noting that there were lots of PayPal disputes discussed and that this was pushing people towards Bitcoin. Or if a post was particularly interesting, I noted down post and thread identifiers so that the topic that the post appeared in could be explored more fully. The journal, therefore, captured some of the most interesting findings, which could be reviewed easily. Post-coding, I printed out the coded material and reviewed it many times. Physically moving around the printed papers and making notes on them helped draw out the connections. Starring some of the top quotations was also a useful focussing strategy. Through all of the above processes, I was able to identify the main themes and concepts that struck me from the material.

To close this section, it is worth considering positionality as it relates to this strand of empirical work. The methods chosen for this analysis of the dark net purposefully did not require interaction with the participants, mainly due to ethical and safety reasons. This also reduced any influence I had on the research and the selection of material was based on a robust process as described.

3.2.2.4 Ethics

Ethical considerations were central to the design of this part of research on the dark net. Without careful design, there is the risk of personal harm to the researcher and the researched. There is also the potential to stray into illegal activity; Barratt and Maddox warn of one researcher who was arrested and had his materials seized (Barratt and Maddox, 2016: 713). The choice here of using the CrimeBB dataset minimised such risks, to the point that they were negligible. There was no participation in illegal activities in this work. Furthermore, this research is not interested in real-life user identities or the actions they have taken. The aim was to explore attitudes and motivations towards using cryptocurrencies, which is not a crime, even if their usage of them is in several countries. The research is therefore distinct from the activities that cryptocurrencies may be used for.

The ethical principles of the Association of Internet Researchers (AoIR) were also used to assess the ethical implications of the research proposed in this study (Markham & Buchanan, 2012). A key point raised by AoIR is about expectations of privacy. Given that there has been extensive research on the dark net, including forums, it does not appear that this has been problematic for researchers. Put another way, it is unlikely that individuals posting on internet or dark net forums would expect that comments are private. Other significant considerations highlighted by AoIR are minimised here. There was no interaction with any individuals from the dataset - this alone eliminated a great deal of risk. Data management was also simplified. The Cambridge dataset was accessed from an authenticated login and any downloaded data was stored on an encrypted laptop. There was no need for a communications strategy with participants. Similarly, a data breach would only reveal information that has already previously been made public.

The guidance of the British Society of Criminology (BSC, 2015) also informs this methodology. They advise researchers to consider the particular issues that arise when conducting internet-based research. Even though forums are public, information gained from the internet ‘should always be critically examined and the identity of individuals protected unless it is a salient aspect of the research’ (8). This research aims to explore group behaviour and usage of cryptocurrencies, it is not necessary, therefore, to identify users by their usernames. Furthermore, the British Sociological Association (Sugiura, 2017) advise that data from online forums should not be copied verbatim. This research strand complies with the guidance of both organisations and does not present usernames or verbatim quotations.

The British Society of Criminology provides further ethical guidance concerning the law and obligations for researchers. In the UK, individuals (including researchers) are not legally obliged to report crimes they witness to the police unless an act relates to terrorism, child abuse or money laundering (BSC, 2015: 11). The nature of the data analysed here was unlikely to relate to the first two categories. One advantage of using a pre-collected dataset is that images are often removed as part of the scraping process. This reduces the chance of viewing certain types of data. The obligation with regard to money laundering relates to the Proceeds of Crime Act 2002 and relates primarily to the regulatory sector (11). An ethics note by the University of Sheffield (2018: 2) also comments that most information collected by researchers is likely to amount to intelligence or hearsay – it is not ‘hard proof of criminality’ (2018: 2). There is, therefore, a negligible chance that this research will reveal anything that would cause concern with respect to the obligations mentioned. However, should any material have arisen during the research that had the potential to meet a duty to report then this would have been discussed with the supervisory team before taking any further action. This eventuality, however, did not arise.

With respect to the spectrum of research activities and designs that can be employed on the dark net, this strand of the study was, therefore, at the low end of potential risk. The research design mitigated much risk by choice. As such, it was highly unlikely that there would be any ethical or legal outcomes as a result of this work. To date, no issues have arisen. A full ethics review of this study was submitted, and the research was approved by the University's Research Ethics Committee.

3.2.3 Chapter 6: From the Perspective of Law Enforcement

The object of research in this section is the view of law enforcement. I did try to arrange interviews with participants from other governmental departments (including regulators and the Bank of England) but was not successful. The author's background enabled access to law enforcement through prior connections and this was likely the difference in response. The main rationale for researching this group is that they have close experience of the illicit use of cryptocurrencies in terms of investigating and prosecuting cases involving them. As a key pillar of the state in terms of the threat that cryptocurrencies potentially pose, it would be incredibly interesting to learn about the opinions and experiences of law enforcement, and ultimately to determine if they are the securitising 'who' (that is, the state's representative) or behind the justification for any securitising speech acts. Where there are claims of the usefulness of cryptocurrencies for illicit activity, law enforcement is on the opposing side of this dynamic. With a constructivist view, it is for illicit users of cryptocurrencies to describe why they use them (as will be examined in Chapter 5), and it is for law enforcement officials to describe their views on whether cryptocurrencies hinder their investigations and to comment on the extent to which they see them as a security threat. That is, we should not too readily accept the views of third parties on someone else's experiences.

It is shown in many areas of this study that much is made of the use of cryptocurrencies for criminal purposes. And this area serves as one of the main arguments against the existence of these systems. One interesting observation that emerges from Chapter 2 is that a lot of the headlines relating to this topic come from the words of public, often political figures. Yet, an agent of the US Drug Enforcement Administration claimed that they want criminals to continue using cryptocurrencies due to the tools that are available to identify people (Russo, 2018). This speaks to the original paradox that has been discussed - are cryptocurrencies a great tool for criminals or not? In terms of securitisation, who is it that says they are and on what grounds? Due to this conflict and the central position of criminality in the debate about cryptocurrencies, this strand explored the view of UK law enforcement officers to examine this DEA claim further.

With regard to law enforcement, two main organisations cover policing in the UK. From a national perspective, the UK police forces have a responsibility domestically. The National Crime Agency (NCA) has a wider remit that transcends national boundaries. Furthermore, the NCA is home to the National Cyber Crime Unit which leads the response to cybercrime. The NCA was, therefore, the primary organisation that this study aimed to research. The NCA also works closely with the police on cyber matters, including with Regional Organised Crime Units (ROCUs) which are part of the national policing structure and have the capability for cybercrime investigation (HMIC, 2015). These two organisations house the UK’s specialist officers relating to cybercrime and investigations relating to cryptocurrencies. Researching both organisations gave a complete perspective of the view of law enforcement on these monetary systems.

The research was designed to explore the view of officers from these organisations toward cryptocurrencies. How useful are they to criminals or do they, like the DEA, wish for these systems to be used due to the public nature of the ledger? What are the properties of cryptocurrencies that they potentially object to? Are some worse than others, if so, why? An understanding of their views in relation to cryptocurrency use on the dark net was also examined. Finally, the research explored issues of regulation and deterrence, particularly around the dark net. Relating this to the theoretical discussion of securitisation, this part of the study is very much concerned with the ‘who’ and on ‘what grounds’. Is it the view of law enforcement that cryptocurrencies are a great tool for criminals and is this behind the claims of political figures concerning the security risk of these technologies? Or if law enforcement does not view cryptocurrencies as a great security issue, could there be an argument for de-securitisation? These are crucial questions that this part of the thesis explored.

3.2.3.1 Data Collection Method

Of Corbetta's three categories, in-depth interview was selected as the most suitable method for examining this research group. The aim was to select and identify participants who were close to cryptocurrencies in their work. This enabled conversation with informed individuals who have experience working in this area and a familiarity with the properties of cryptocurrencies. Document collection or observation were no longer practical options following the outbreak of COVID-19. Documents relating to law enforcement and cryptocurrencies would also likely be subject to data classification – access to much of this material would not be practicable. Likewise, observation from extended or embedded time within law enforcement was not a feasible option due to lockdowns. Cryptocurrencies are still small from a financial perspective and so in-depth interview with some of the few members of law enforcement working in this area was the best method to obtain information. Interviews were semi-structured, online, and one-to-one.

3.2.3.2 Sample Selection

Initial contact was made with officers from the police and the National Crime Agency (NCA). Permission to interview NCA officers required Deputy Director approval, which was given. The initial plan was to try and speak to as many relevant officers as was necessary to satisfy answering the questions. At each interview, I asked if there were other officers to speak to. I did contact as many as I could but invariably only succeeded in securing interviews with a smaller group. Access and participant willingness to talk were issues. I contacted two senior officers for example – one did not respond, and the other did not think he was a suitable person to talk to. It is likely the reluctance was either down to the position of the participant or that as a senior officer there may not have been the subject matter expertise required. I do not have a figure for the number of law enforcement officers that have cryptocurrency experience but some of the participants I interviewed were key members of law enforcement expertise in cryptocurrencies. I, therefore, felt that I had spoken to the most suitable participants with the greatest knowledge.

The research took place after the first COVID-19 lockdown in 2020. This affected the availability of the officers and made interview arrangements difficult. Cyber officers faced a surge in demand due to lockdown and I had to rearrange a number of interviews. The lockdown also meant that all interviews had to be switched to being conducted remotely. Whilst this was not an issue, I did feel that this made some of the arrangements more difficult. It was certainly easier for a participant to cancel an interview last minute, perhaps more so than if a physical meeting had been arranged. But otherwise, I did not have any problems with remote interviewing and felt that the participants were also relaxed about this method. In total, the interviews in this thesis took many months to arrange and complete. I started arrangements in late 2019 to early 2020, and the final interview (for the HullCoin chapter) was in late October 2020. Interviews were conducted using Zoom or Skype, at a time convenient for the participants.

3.2.3.3 Data Analysis

Interviews were recorded and transcribed. Verbatim transcription was conducted in order to fully use the material. Transcription then enabled the use of qualitative software for data analysis. With a smaller volume of data than the CrimeBB posts, Nvivo was sufficient for coding and was selected as the qualitative data analysis tool. In the previous two strands, the data was already collected, and I was subsequently 'interviewing' the data. In this and the HullCoin strands, there was now direct participant interaction through interviewing. The interviews were prepared for and semi-structured. But once the interviews were transcribed, the coding process was very similar to the previous strand. Analytical notes were taken as coding was conducted. First-cycle coding was structural, as discussed, with topic coding used additionally. Second-cycle pattern coding grouped codes based on commonality. Post coding, all the material was printed and used physically to take notes, move pages around and highlight top quotations. My favourite technique was then to ask myself what the key findings and major themes were, or what struck me most from the material. I found that this helps focus on the most significant parts of the research.

3.2.3.4 Ethics

As per the University ethics approval, consent and information forms were provided to and discussed with all participants. Due to COVID-19, no site visits were possible, so the gathering was solely done through online interviews. I did not, therefore, gather any documents from sites or have any other similar concerns. There was no need to identify participants by name, so they have been omitted from the thesis. The NCA officers had Deputy-Director level approval to take part in the research. I took care, as did the officers, to not discuss any active or past cases specifically. As this was an exploratory piece of research about more general experiences and views, there was not a great deal of risk in terms of revealing sensitive material. No names of any subjects or operations were discussed. Overall, the ethical risks were minimised and minimal.

Reflexivity is important in this part of the research. Care was taken to ensure that results were interpreted impartially. Positionality also deserves specific consideration to reiterate previous discussion. Participants were aware of the author's background. To some extent, this was advantageous and probably put the participants at ease knowing they were talking to someone who understood their position as law enforcement officers. However, it must be considered whether this affected the information that was gathered. This is discussed openly here, and the reader can make their own judgement. Research questions and the interviews were planned carefully to ensure that they did not lead the participants. Many of the questions asked were open. My background views were also reflected upon so that they did not affect any questions. I was conscious to try and gather their thoughts and experiences without giving away much of what I thought. In most cases, this proved to be quite simple as all of the officers seemed happy to talk freely and fully. Whilst not related to my positionality, there was also some thought given to the extent that participants felt that they were freely able to discuss matters given their employment. For the NCA officers, I got the impression that they were particularly comfortable talking as they had been given Deputy-Director level permission. In any case, for all of the officers, both police and NCA, I did not feel that they were trying to 'watch what they said'. That is, all interviews felt like honest discussions about their personal views and opinions about cryptocurrencies and their experiences in dealing with them.

3.2.4 Chapter 7: HullCoin - Cryptocurrencies in Civil Society

The chosen strategy of inquiry for this strand of the research was a case study of community usage of cryptocurrencies. This is an important aspect of the thesis as it broadens the perspective on cryptocurrencies beyond illicit use, the dark net and law enforcement. There are uses for cryptocurrencies other than on the dark net and this strand captures some of this experience. Illicit use of cryptocurrencies often dominates the debate, so this work provides a different view. It also contrasts the work on the dark net by focussing on a specific community group. This zooms the perspective out from the individual level to see how cryptocurrencies could serve or be used at higher levels, with more of a civil society focus. In this way, this chapter questions whether cryptocurrencies could play a legitimate part in money or society. That is, can they be a force for good and have a positive role, rather than being just a tool for illicit activity?

The subject of local currencies was discussed in more detail in Chapter 2, but a few words are necessary here to explain the rationale for this part of the study. Local currencies have been in operation around the world for some time. In the UK, there are a number including the Brixton Pound. These currencies are often a way of helping local businesses and communities, principally by keeping the currency within a local area (Gilson, 2014). That is, the currency cannot be taken out of the town and spent elsewhere. In 2014, Hull City Council launched the HullCoin, the first digital local currency; the HullCoin website (2020) describes the initiative as the 'world's first Community Loyalty Point', where individuals can earn HullCoin through community activity and then spend them through discounts at local retailers. Dave Shepherdson, one of the founders of HullCoin, was the Financial Inclusion Support Officer for Hull City Council at the time of the launch. He described the project as follows:

> It’s about people on low incomes, in financial distress, being able to subsidize to an extent and compliment their incomes through undertaking activities that will be linked to the things in field of finance. [Furthermore] it can be used to instigate voluntary activity, or it can be issued close to the point of demand for a service which would help them, which they would not normally have the ability to pay for. (Gilson, 2014)

The case study aimed to speak to people involved in the project to learn about this community use of a cryptocurrency.

3.2.4.1 Data Collection Method

Interview was the primary data-gathering technique for this group, supplemented by some documentary sources. These were the most suitable methods to conduct a case study on community use of a cryptocurrency, especially given that the HullCoin project had ended and the research period was during COVID-19 lockdown. Observation of activity that is based on a digital transaction would be difficult and document analysis alone would have had limited utility. Interview enabled more depth through discussion. Again, the interviews were semi-structured. The case study was originally planned to take place in the community selected and the vision was to spend time in Hull to conduct interviews. This was not possible due to the COVID-19 outbreak, and, as with the previous strand, the interviews were forced online. Initially, this was a disappointment. But as became clear once the interviews began, this was not an issue in the end as HullCoin was no longer an active project at that time. So, there would have been less value in physically being present in Hull. There would have been no shops or residents actively using HullCoin that could have taken part in the study. As a result of this, the information gathering was bolstered by some further sources. First, one of the founders provided me with some documents related to the project prior to interview. HullCoin had received a lot of media attention at the time of its launch and shortly thereafter so there were some materials available from that time. In addition to this, there were also some media reports and even a BBC News piece that were also drawn on as sources. As a case study, the data gathering techniques were therefore widened from interview and included some document analysis as well.

3.2.4.2 Sample Selection

This work intended to get a community perspective on the use of cryptocurrencies. According to an infographic on the HullCoin website (2020b), there were three main groups involved in the functioning of the currency: users, retail and community groups. In addition to this, the team that conceived and executed the project could be considered a further group. The original plan was to identify individual attitudes and motivations from researching all these groups, with the breadth enabling analysis of the benefits or otherwise to the community as well. However, due to COVID-19 and the fact that the HullCoin project was dormant at the time of my inquiry, it was not possible to get as wide a view as at first hoped. The project simply did not get to the point of a full launch in the community so there was not an opportunity to do widespread interviews of business owners or residents – the project did not get that far. In some ways, this made this case study more interesting, in terms of exploring the reasons why the project faltered. As such, the focus became more about the founders of the project, their rationale for it and their experience of setting up the world's first local cryptocurrency.

Hull City Council was the instigator of the project and Dave Shepherdson was a central individual involved so he was identified as a key participant. Mr Shepherdson agreed to take part in the study, and he was able to cover some of the background to the project, including the motivation for it as well as some crucial questions about design choices. It was interesting to learn more about why a cryptocurrency model was chosen over the type of currency used in other areas, such as the Brixton Pound which is a physical currency. Lisa Bovill was another central figure in the launch of HullCoin and was identified as the second key participant and she too was happy to be interviewed. As the Welfare Rights Manager for Hull City Council at the time (Gilson, 2014), Lisa was able to provide more information about the goals of the project and the benefits they hoped for at a community level. Both individuals were central to HullCoin. One other prominent HullCoin member initially agreed to take part, but then withdrew as the project had ended in some acrimony. However, having done the interviews, I felt that David and Lisa had provided sufficient data to answer the research questions. The team only ever consisted of a few people, and Dave and Lisa were longer-term members. The interviews with them turned out to be very in-depth, which was a more appropriate technique considering there had been issues and the project had ultimately come to a close.

The sample selection was therefore small for the interviews. As the main interviews were with the founders of the project, the extent to which they were objective must be considered. They were obviously supporters of the project having conceived and founded it, however, as neither worked for the project at the time of interview I did not feel that there was anything more to the conversations than a frank and honest discussion of how the project went. The founders were heavily invested in the project and there may well be others who have a different view of HullCoin and this is accepted as a limitation of the research.

As mentioned, the project did not reach full launch. There were, however, some trials that had taken place in the early days of HullCoin. I was keen to try and speak to someone else with a different perspective. I was not able to identify any users to speak to, and the project did not get far enough for users or community projects to be significant research subjects. I did manage to identify two businesses that had some involvement in HullCoin trials. One did not respond to attempts to make contact, but a second business owner did and agreed to interview. This turned out to be limited, as again the project did not go as far as going live in their shop. The key to this case study then was the in-depth interviews that the two central founders gave. They were incredibly rich and also made for a fascinating story about this intriguing project. Furthermore, some of the insights from the project proved to be very important for the overall discussion and conclusions of this thesis.

3.2.4.3 Data Analysis

The data analysis method was the same as for the law enforcement interviews. Interviews were again recorded online and transcribed. Nvivo was used for qualitative content analysis. First-cycle coding methods were structural and topic. Second-cycle used pattern coding. Post coding techniques included using printouts and analytic notes from a coding journal. Focussing techniques looked at top quotations and major findings to highlight the key concepts and themes.

3.2.4.4 Ethics

This strand of research is the least sensitive to ethical issues. Consent and information sheets were provided to all participants. The other team member who mentioned the acrimony did not take part and nothing more was heard of these issues. The topics discussed in the interviews were not sensitive and no personal data was gathered. In terms of positionality, the author’s background did not have any particular impact. As with the interviewing of law enforcement, care was taken with question design to ensure that participants were not influenced. As this part of the study is not controversial in any obvious way, it was the least likely to be affected by any ethical issues. The participants appeared happy and free to discuss the HullCoin project.

4 The Security Narratives

Cryptocurrencies first gained mainstream attention throughout 2017 as a speculative phase in the price of Bitcoin brought increasing interest, and more of the general public became aware of them. Bitcoin was a frequent topic of media reporting and discussion. It was no longer just some obscure internet technology, but an emerging asset with a price that rose to the region of $20,000 by the end of the year. During this period, a security-led narrative formed and I was interested in this on a professional level as described in Chapter 3.

This chapter relates to the first research sub-question, which has two parts: 'How are security-led narratives about the use of cryptocurrencies constructed and to what extent are they justified?' This question is much more interesting in the context of the theoretical debates about money and in light of securitisation theory. The research design for this chapter is detailed in Section 3.2.1, but in essence, this part of the research is based upon a document search of work that claimed that cryptocurrencies are a security threat. The first section of this chapter aims to analyse these documents in terms of potential securitisation by the state or its representatives, and the focus is more on the media reporting that has built up the security narrative about cryptocurrencies. The aim is not to capture every security-led concern ever made, nor to quantify or formally classify such concerns. Rather, the aim here is to examine some of the narrative concerning the state's view of cryptocurrencies, in order to build an argument as to whether there has been an attempted securitisation of cryptocurrencies by the state and on what grounds. Has the state or its representatives claimed that cryptocurrencies pose an existential threat? 'Who' has made the securitising speech acts? 'What' is being protected? And in what ways are cryptocurrencies described as a threat?

Having considered these questions, the analyst in securitisation theory must then ask whether these claims are justified. To do this, the chapter moves on to examine the empirical academic and organisational reporting of the threat of cryptocurrencies, rather than the more media-based focus of the first section, to see if existing research supports any securitising speech acts. In Section 4.2, the similarities between cash and cryptocurrencies are first established. If cryptocurrencies are potentially a threat, then any justification must be made in comparison to existing, alternative monies that can, and are, already used for illicit purposes. This highlights the ways in which cryptocurrencies could be a preferred tool to existing illicit methodologies. Cash is identified as a leading monetary tool for illicit activity, so this medium is then examined in more detail to establish what we know about the use of cash and the extent of its use for illicit activity. This is vital and provides the comparator for Section 4.3, where the use of cryptocurrencies in illicit activity is examined in detail. Whether any securitising speech acts about cryptocurrencies are justified depends on comparison with alternative methods. If existing tools are better and used in more illicit activity than cryptocurrencies, then any securitising speech acts must be questioned. It will be harder to legitimately claim and justify that cryptocurrencies are an existential threat which requires exceptional handling if even greater threats are not viewed or treated in the same way.

Much of this chapter was published as an article in the Chatham House *Journal of Cyber Policy* titled, ‘Criminal use of cryptocurrencies: a great new threat or is cash still king?’ (Butler, 2019). However, this thesis chapter brings a far greater and more interesting understanding of the findings, that goes beyond the extent to which cryptocurrencies are used for illicit activity.

4.1 First Users and the Early Narrative

Bitcoin started to regularly record over 1,000 transactions per day in 2011. Some of the earliest adopters of Bitcoin did so for illicit purposes; analysis from the US Drug Enforcement Administration (DEA) showed that about 90 per cent of Bitcoin transactions in 2013 were related to criminal activity (Russo, 2018). A payment mechanism that did not rely on a trusted third party and that could be self-enrolled onto (by creating your own key pair – analogous to your account) was appealing to criminals. So too were further properties of cheap international payments that could not be reversed. It is, perhaps, no coincidence that the increase in Bitcoin transactions took place as illicit marketplaces gained traction on the dark net. Adding the properties of Bitcoin to the anonymity provided by the dark net created a working ecosystem for criminal behaviour on the internet. This combination proved attractive material to journalists and many stories about the illegal underworld and Bitcoin ensued. It was here that the early narrative around Bitcoin as a criminal tool began. One such headline emerged after an internal FBI report was leaked:

> FBI fears Bitcoin’s popularity with criminals. (Zetter, 2012)

It is likely that early media headlines such as this, and the connection between Bitcoin and the dark net, led to the early narrative about Bitcoin as a criminal tool. The FBI report raised some observations about the potential challenge that Bitcoin represents. As there is no central authority, there is no one for law enforcement to ‘go to’ in order to request more customer details, as with traditional finance. The article notes that Bitcoin is only pseudonymous and that the degree of anonymity depends to a large extent on the user. This is a specific point that is explored in great detail in the following chapter. This article is useful then as it establishes that there was a concern expressed by law enforcement in the earlier days of Bitcoin and it establishes the connection of this threat to dark net markets.

4.1.1 ‘Who’ is Concerned and ‘Why’?

In this section, some of the headlines and reporting about the security threat of cryptocurrencies are highlighted and discussed. This is not exhaustive. The aim is to consider ‘who’ had been delivering some of the securitising messages that appeared from 2017 onwards and to analyse the grounds for concern. This enables, in the latter parts of the chapter, an examination to take place of these claims. The examples given are taken from some of the most prominent articles and headlines that emerged from the searches that were conducted as per Section 3.2.1, and they are often ones that had significant media exposure at the time because they were somewhat controversial or had been made by high-profile individuals.

One such media report that caused a stir was based upon comments by Jamie Dimon who, in 2022, was still the long-serving CEO of one of America’s largest banks, JP Morgan Chase. He said that Bitcoin was a ‘fraud’, worse than the tulip bubble and that ‘someone is going to get killed’. Furthermore, he would fire any employees who traded Bitcoin as it is ‘stupid’ (Imbert, 2017b). These are strong sentiments, which led to this headline on *Bloomberg*:

> Jamie Dimon Slams Bitcoin as a Fraud. (Son et al., 2017)

As the CEO of a large US bank, Dimon’s comments on financial matters are taken seriously. The concern here appears to be that he thinks Bitcoin has no basis as money. It is unlikely that this concern is based on a commodity theory perspective, so perhaps it is just scepticism of a token-based, non-state money. But the language he uses is strong, suggesting that Bitcoin will get people killed or that it is a fraud. In this respect, it seems that his concern is for individuals who will suffer as a result of its failure.

A slightly later piece from 2018 quoted Jerome Powell, the Chairman of the US Federal Reserve (the US central bank), as saying in evidence to US Congress that ‘cryptocurrencies are great if you are trying to hide or launder money’ (Shi, 2018). These comments made headlines such as this from an online cryptocurrency news outlet:

> Fed Chair: Cryptocurrencies Are 'Great' For Money Laundering. (Shi, 2018)

The reporting here was again of a significant figure. The Chairman of the US Federal Reserve is arguably the most important commentator on monetary matters in the world. His opinions and comments are watched very carefully. The grounds for this threat that appear in the headlines is again illicit usage, like the FBI headline. But the article does also report that Chairman Powell had concerns that cryptocurrencies have no ‘intrinsic value’ and thus there were investor protection issues. What exactly needs protecting by labelling cryptocurrencies is harder to identify, as it could be financial investors or even victims of crime. Interestingly though, the article further notes that at that time the Federal Reserve was not concerned that cryptocurrencies were a threat to financial stability, as the market was too small. This identifies financial stability as another potential referent object, but this comment also links to the issue of the scale of the potential threat posed. If cryptocurrencies are too small a market to affect financial stability, are they a significantly big enough threat in other areas to warrant moving the issue out of ordinary politics?

In 2019, Steven Mnuchin, the US Treasury Secretary at that time, discussed cryptocurrencies during a White House briefing, following news that Facebook was planning to launch its own cryptocurrency called Libra. Mnuchin was reported to say that cryptocurrencies posed a threat to national security as they can be used to fund illicit activity. This again became a prominent headline, for example in *The New York Times:*

> Cryptocurrencies Pose National Security Threat, Mnuchin Says. (Rappeport & Popper, 2019)

Perhaps, then, it is illicit activity that is the significant threat posed by cryptocurrencies. And perhaps it is the scale of this threat that is the justification for the securitising speech acts. This will be examined in Sections 4.2 and 4.3. But notably, these comments came about in response to a different type of cryptocurrency, that is, one proposed by a US company. Facebook said they would not launch Libra without regulatory approval. Libra would therefore be very much more under US jurisdiction and would not be as decentralised a currency as Bitcoin, for example, and yet, it was still objected to by US officials. Even a regulatory-compliant and US-based proposal was still considered to be a concern and a threat.

In securitisation theory, it is important to consider ‘who’ the people are making the claims, especially in the context of monetary history. The first quotation is from the head of a private bank, the second from the head of the US central bank and the third from the United States Treasury representative – in short, the memorable alliance. As discussed elsewhere, there are a wide variety of doubters of cryptocurrencies for a range of reasons. An academic criticising cryptocurrencies may not get as much attention as leading US government officials. And the media no doubt amplifies or sensationalises some of the material that they report on. But some of the most prominent criticism has come from the memorable alliance. Perhaps this is due to the positions that they hold but this is still an important observation in terms of the ‘who’.

In this chapter, there has been a focus on the United States, and this is intentional. As has been explained previously, the US dollar became the de facto world global currency following Bretton Woods in 1944. As the world's superpower, the dominance of the dollar is central to consideration of the threat of cryptocurrencies as it is the most important state money. The views then of US bankers, politicians, and Federal Reserve officials (central bankers) are arguably the most significant and powerful in terms of the memorable alliance as it relates to the US dollar. It is the dollar that affords the US an 'exorbitant privilege' (Canzoneri et al., 2013: 372) and it is the dollar that exemplifies the Triffin Dilemma, and the conflict that comes from using a national currency simultaneously as a global one. The remarks of key US officials about cryptocurrencies are therefore a focus for analysis of the security threat that they pose and the potentially securitising language of the narrative examined.

As a further note to this, there are other significant state currencies such as the Pound Sterling. But anything that applies to the US dollar will apply to the Pound only on a lesser scale. UK figures of the memorable alliance have also commented on cryptocurrencies, but the issues raised are largely the same as those raised by US officials. For example, the Governor of the Bank of England gave a speech in 2018 on the future of money. In relation to cryptocurrencies, he questioned their ability to be money, stated that they currently do not 'pose material risks to financial stability' and that 'authorities are rightly concerned given their inefficiency and anonymity, one of the main reasons for their use is to shield illicit activities' (Carney, 2018: 9-10). The speech acts are very similar across the major countries, but the commentaries of the US officials are of the greatest importance due to the position of the US dollar.

The concerns about cryptocurrencies are certainly not one-dimensional and restricted solely to the issues of investor protection, financial stability, and illicit usage. In 2019, a headline showed another angle:

> Bitcoin Threatens To 'Take Power' From The U.S. Federal Reserve.
> (Bambrough, 2019)

The article was in relation to an attempt by a US Congressman to ban Bitcoin and cryptocurrencies. In a meeting at the House Financial Services Committee, the Congressman was quoted as saying:

> An awful lot of our international power comes from the fact that the U.S. dollar is the standard unit of international finance and transactions… It is the announced purpose of the supporters of cryptocurrency to take that power away from us, to put us in a position where the most significant sanctions we have against Iran, for example, would become irrelevant. So whether it is to disempower our foreign policy, our tax collection enforcement or traditional law enforcement, the advantage of crypto over sovereign currency is solely to aid in the disempowerment of the United States and the rule of law. (Bambrough, 2019)

Here, the main concern is regarding the power that the US enjoys as a result of its domestic currency being the main currency of international finance. As a reminder, in Chapter 1, the Triffin Dilemma described the conflict that arises from this position and the geopolitical tension that exists regarding it. The Congressman does mention the implications for law enforcement, but we can see from the sources already analysed that the reasons for concern about cryptocurrencies vary, although the criminal threat appears to be a consistent theme throughout. Is the threat the criminal usage of cryptocurrencies, that it is not ‘valid’ money, or are the concerns wider, in terms of the power that states enjoy from controlling money, and in particular, the US as a world superpower controlling the money of international trade and sanction? The securitising speech acts often list several threats, making it hard to be precise about what is the main concern, or indeed what it is that they are trying to protect. The link between money and power was explored in Chapter 2 and we will come back to this question in the conclusion of the thesis.

4.1.2 A Shift in Narrative?

For now, though, we return to some further examples of the narrative and note how there is evidence of a shift during the course of this study. In 2017, Larry Fink, the US CEO of Blackrock, the largest asset management firm in the world, described Bitcoin as an ‘index of money laundering’ (Imbert, 2017a). But then in late 2020, Fink was quoted as saying that Bitcoin could ‘possibly’ evolve into a global market asset (DeCambre, 2020). The cryptocurrency market is an incredibly fast-moving market, and it would be hard to explain this example of a potential shift in position. Perhaps the perception of Bitcoin as just a criminal tool has evolved from the early FBI report days, or maybe the market, and the fact that Bitcoin endures has forced some to rethink their positions. Only the individuals concerned can explain their thinking.

It is worth noting here, that I made several attempts to engage with the ‘memorable alliance’ for my research but was unsuccessful. Perhaps this was because I was an ‘outsider’, and they were not comfortable talking to me. I also applied for a placement at the Bank of England, but this too was unsuccessful. In the same way that I have managed to research the law enforcement view in this thesis, there is an excellent opportunity to research the memorable alliance should any researchers wish to take this further.

In 2019, the concern over the illicit use of cryptocurrencies continued. President Trump said that he was not a fan of Bitcoin as it was ‘not money’ and it enabled criminal activity (Cuthbertson, 2019). But it was not only Bitcoin that faced resistance. The G7 warned that cryptocurrencies pose a risk to the global financial system and this warning came days after Mastercard and Visa withdrew from the Facebook Libra project due to regulatory uncertainty (Chan, 2019). The G7 task force was made up of central bank officials – the memorable alliance. We should ask why Facebook’s Libra is opposed. If Bitcoin is beyond direct control as a decentralised system, would a regulated, identifiable public corporation like Facebook fare any better? It seems not. Why are these currencies opposed, whether decentralised or not? The HullCoin case study proves to be an important chapter in this context. What has been the fate of other cryptocurrencies, how have they been viewed, and can any alternative or complementary currency find acceptance from the state? Or do they all pose too great a risk, too much of an opportunity for illicit activity that they should all be resisted? And is it only state money that can be trusted and relied upon in all these regards?

It has been interesting to observe some of the shifts in narrative over these past few years. The opposition is still there, but it seems that there has been an increase in support from more official areas. COVID-19 has also changed perceptions and provides an example of developing support for cryptocurrencies or their technologies from public officials. In 2020, 11 Members of Congress wrote to the US Treasury Secretary urging the Treasury to:

> …utilize private sector innovations such as blockchain and DLT to support the necessary functions of government to distribute and track relief programs and direct that all guidance support the use of technology to facilitate delivery of CARES Act benefits. (Brett, 2020a)

There are several significant points to consider here. First, COVID-19 has raised the question of whether the state should have direct banking links to its citizens (disrupting the memorable alliance and cutting banks out of the profitable position they have enjoyed). As suggested by the Members of Congress, the state could (using blockchain for example) directly send money to every citizen, rather than using cheques or the traditional organisation of the memorable alliance (Brett, 2020a, 2020b). This, again, is something that links to the HullCoin research in Chapter 7 and is also reflective of the wider tension and questions that exist over our forms of money. Different use cases are being imagined but resistance to them persists. But where the lines of resistance lie between Bitcoin, Libra or a private blockchain remain unclear.

Resistance however is not universal, and we must consider whether any attempted securitisation of cryptocurrencies has been successful. On this last point, we will finish this look at the narrative surrounding cryptocurrencies with some more examples that highlight significant recent developments. China has long had an uneasy relationship with cryptocurrencies and various bans have been announced over several years relating to cryptocurrencies. In late 2021, The People’s Bank of China declared all cryptocurrency activity illegal:

> Recently, cryptocurrency speculation has increased, disturbing economic and financial order, breeding illegal and criminal activity such as gambling, illegal fundraising, fraud, pyramid schemes and money laundering. This all seriously endangers the people’s safety. (The People’s Bank of China as quoted in Olcott & Szalay, 2021)

So, it is not just the West that objects to cryptocurrencies, but the threats described by The People’s Bank of China and the potential referent objects are familiar once more, with the welfare of the citizen being presented as of concern. Again, though, is a concern for the welfare of individuals the real motivation for the memorable alliance? Gambling harms citizens, for example, but it is widely legal. And state money is used in crime, but that too is not securitised. Of course, China is outside of the Western alliance with regard to the control of money, so Chinese state motivations may be somewhat different. However, it is worth noting that China is one of the more advanced nations in terms of digital transactions, and The People’s Bank of China has been working on a Central Bank Digital Currency for some time, with further trials due in 2022. It is likely that China, and other governments, want to control their currency and a CBDC offers the potential for greater control and surveillance than existing monies.

2021 was also the year that the first nation-state declared Bitcoin as a legal tender. This was a watershed moment for Bitcoin enthusiasts, but was met with mixed reaction more widely, such as in this headline from a piece written by an economics academic:

> El Salvador’s adoption of Bitcoin as legal tender is pure folly. (Frankel, 2021)

The move by El Salvador prompted a warning from the IMF that widespread use of cryptocurrencies would threaten stability due to the volatility of cryptocurrency prices, and also potentially integrity as well through illicit use:

> *Financial integrity*: Crypto assets could open the door to illicit money, terrorism financing, and tax evasion, because of the anonymity they provide. (International Monetary Fund, 2022)

The narrative of the threat posed by illicit use persists. What is noticeable, though, in all these articles and commentaries by various officials, is that there is very little justification or quantification of any of the risks. To what *extent* cryptocurrencies are a risk is never explained. The threats are merely stated without any comparison to existing systems or, in this case, existing illicit methodologies. Therefore, whilst it is clearer what the grounds are for potentially securitising speech acts, the commentary does not help us understand if these threats are justified. This is why this aspect will be examined in the later sections of this chapter.

Interestingly though, since El Salvador made Bitcoin legal tender, various US officials have made comments indicating that there are no plans for cryptocurrency bans in America:

> SEC Chief Says the U.S. Won't Ban Cryptocurrencies. (Bain, 2021)

The SEC Chief said that their approach is ‘really quite different’ to China’s ban and looks to bring cryptocurrencies within existing regulations (Bain, 2021). This may be because bans would require the state to issue sufficient punishment, which may be difficult (Hendrickson & Luther, 2017). Geopolitically, though, we can see that there is a mixed position towards cryptocurrencies that varies by state. Larger countries, with control over some of the world’s major currencies, seem to be in greater opposition than some of the smaller ones. Do El Salvadorian politicians fear illicit use of cryptocurrencies as much as some other countries? Or, again, is the threat beyond illicit use, risks to stability or even as a challenge to existing sources of power and control?

For now, though, despite the improved US regulatory stance, the same fears about cryptocurrencies continue to be seen in the media. In early 2021, the new US Treasury Secretary made familiar headlines. Janet Yellen is quoted as saying, ‘I see the promise of these new technologies, but I also see the reality: cryptocurrencies have been used to launder the profits of online drug traffickers; they've been a tool to finance terrorism’ (Robertson, 2021). Once more, the illicit use of cryptocurrencies is the justification for concern that makes the headlines:

> Janet Yellen says 'misuse' of cryptocurrencies like Bitcoin is a growing problem, as regulators increase scrutiny after surge in interest. (Robertson, 2021)

We have seen that several threats have been stated by a variety of officials. But it is the use of cryptocurrencies in illicit activity that is arguably the most prominent. Perhaps this angle generates more media interest, or it may be that ‘security’ is thought of by politicians and officials as a stronger justification for any action, rather than say investor protection. Regardless, though, it is illicit use that often dominates the headlines and therefore the narrative that cryptocurrencies are a security threat, so this area requires greater analysis.

The key question to return to, therefore, is to what extent have cryptocurrencies been used for illicit activity? Do we take the position of Moore and Rid in Chapter 2 and ask whether the legitimate activity is greater than the illicit, and if so, does that make the cost an acceptable one? To consider this, we turn to the remaining parts of this chapter to analyse these questions, which are important to this thesis. The illicit use of cryptocurrencies is often given as grounds for opposition to cryptocurrencies by the state, as has been shown by the headlines we have seen. But is this claim justified in terms of securitisation theory? How valid is this position, and how do cryptocurrencies compare to existing state monies? This last question has begun to get wider attention in recent years and there is now something of a counter-narrative that can be seen in the media, such as in this headline from *Forbes*, and it is one that we now move on to explore:

> The False Narrative Of Bitcoin’s Role In Illicit Activity. (Lennon, 2021)

4.2 Cash and Cryptocurrencies

We must understand our current financial system, its limitations, and attitudes towards it if we are to critically analyse where cryptocurrencies fit in and why. At higher levels, we have seen that there is discord about the mechanisms of international finance, and, at lower levels, our usage of money has been trending evermore towards digital transactions. Before exploring the security narrative about cryptocurrencies further, it is also important to first consider the properties of cryptocurrencies. If cryptocurrencies are to be thought of as a threat, in what ways do they differ from our current monies and methods offered by the traditional financial system? What is it about them that makes them more of a threat than another? Cryptocurrencies are sometimes described as digital cash and so in this section, we will briefly consider the properties of cryptocurrencies and physical cash in order to draw out the differences. Documentary analysis is then used to examine the extent to which state monies are used in crime. This is contrasted with an exploration of the illicit use of cryptocurrencies in Section 4.3 to analyse whether they are used more or less in illicit activity than in the traditional financial system. This analysis is important to the consideration of whether the securitising speech acts are justified in claiming that cryptocurrencies are a threat due to their illicit use.

4.2.1 The Properties of Cash and Cryptocurrencies

Cryptocurrencies are classified as ‘virtual assets’ by the Financial Action Task Force (FATF). They describe virtual assets as ‘a digital representation of value… [that] do not include digital representations of fiat currencies’ (Financial Action Task Force, 2018: 124). This clearly separates cryptocurrencies from national currencies, including cash. For the time being, we will focus on Bitcoin as the primary cryptocurrency. The threat that privacy-focussed cryptocurrencies pose will be considered separately later in the chapter.

Money, of all forms, has three widely described functions in economics: as a medium of exchange (for goods, rather than bartering), a store of value (so you can buy goods later) and as a unit of account (to price goods so they can be compared). But different monies have other distinct properties that affect their usefulness and appeal for certain activities. Physical cash, for example, has several of these properties. First, cash is anonymous (except for serial numbers). Second, it is a bearer instrument which means that whoever holds the money is the owner and there is no information recorded about whose it is. Third, there is no mechanism implicit in cash itself that records transactions – that is, any recording that occurs is the result of other protocols, rules and laws that are introduced. For example, we have mature anti-money laundering regimes and requirements such as Suspicious Activity Reports (SARs). It is worth noting here, though, that cash use has been the main reason for reporting suspicious activity in the EU (Europol, 2015: 16). And finally, settlement is instant when using cash – when you give someone cash for a good the deal is done; there is no middleman when two people transact in the street and there is no mechanism to undo the transaction. It is this 'anonymous and untraceable nature of cash' (HM Treasury, 2018: 14) that makes it such a convenient criminal tool. It is good for money laundering as, compared to electronic transactions, 'it is difficult to ascertain the source of cash and impossible to know the intended beneficiary' (Europol, 2015: 9).

The comparison of cryptocurrencies as digital cash is apt, as they do mimic the above properties, albeit with some subtle, but important distinctions. Like cash, once a cryptocurrency transaction has taken place, the exchange is final and there is no recourse to undo the transaction, and there is no third party like a bank to go to. But cryptocurrencies vary in two important ways. For a currency like Bitcoin, the system is *pseudonymous*, not anonymous. It is possible to see addresses where transactions have come from and gone to (and amounts), but no identity is directly linked to these addresses. (Privacy coins, however, employ other cryptographic techniques to overcome this pseudonymity to provide anonymity – a threat we will explore later). The other big difference from physical cash is that all Bitcoin transactions are recorded on a public blockchain. Every single movement of funds from one party to another is captured and recorded in a manner that prevents any of the data from being tampered with (save for theoretical consensus attacks, such as the '51 per cent attack', which would require huge resources - note this attack is not the result of a flaw in the system but a symptom of its design) (Antonopoulos, 2017:

253). These are significant differences and ones that are not to the advantage of a malicious party.

4.2.2 Cash and Crime

If cryptocurrencies are arguably less anonymous than cash, and they leave a permanent record of transactions on the internet, then why are they considered more of a threat than cash as an existing alternative tool that is useful for criminals? This question is the exact one that drew me into researching cryptocurrencies in the first place. Interestingly, even though our use of money has become increasingly electronic, the demand for cash has grown. This is an interesting phenomenon that deserves some further examination, especially as, according to one former IMF economist and Harvard Professor:

> Cash plays a starring role in a broad range of criminal activities, including drug trafficking, racketeering, extortion, corruption of public officials, human trafficking and, of course, money laundering. (Rogoff, 2016: 2)

If cash plays such a starring role in criminal activities, yet we are increasingly transacting digitally, why has demand for cash grown, and why are cryptocurrencies viewed as a security threat in relation to their illicit use? Before exploring this question in more detail, it is worth noting that the COVID-19 pandemic has only served to increase these trends. The Bank of England reports that cash use declined in 2020 by 35 per cent compared to 2019, with only 17 per cent of payments in the UK made in cash. But again, there was also a large increase in notes in circulation – 10 per cent in 2020, and another 19 per cent increase in 2021 (Bank of England, 2021). We will first explore cash usage before then discussing cryptocurrencies, as the comparator, in more detail.

In the UK, as an example, the demand for banknotes has outstripped GDP for several decades, with the total value of Notes In Circulation (NIC) doubling to approximately £70 billion between 2005 and 2017 alone (Cleland, 2018). The total is now over £80 billion (Bank of England, 2022). Paradoxically though, whilst NIC has grown, late 2017 marked the year that debit card transactions overtook cash in the UK (which continued its decline by another 15%) (UK Finance, 2018). So why has demand for notes doubled whilst the use of cash continues to decline, especially given its use in criminal activity? The Bank of England speculates that cash is being used as a store of value, despite inflation surging since early 2021 (Bank of England, 2021). And a further Bank of England bulletin suggests that no more than half of the NIC are used domestically for transactions or hoarding – with the rest overseas or used in the shadow economy (Fish and Whymark, 2015: 32). The shadow economy consists of legal and illegal activities that attempt to 'avoid government regulation, taxation or observation' (2015: 223-224). The size of these markets cannot be accurately given, due to the 'untraceable nature of cash' (2015: 216). This is a concern, as we do not know how much cash is used for crime. A Europol strategic report on the use of cash by criminals reaches the same conclusion:

> …perhaps the most significant finding around cash is that there is insufficient information around its use, both for legitimate and illicit purposes. (Europol, 2015)

It may be surprising that a leading law enforcement agency does not know the extent to which cash is used for criminal activity, but it is the properties of cash as described that make it hard to know what it is used for. Central banks have a detailed grasp on how much cash is in circulation, but they 'simply do not know' who is holding it (Rogoff, 2016: 32). In all, we are left with an intriguing situation: cash usage is falling and has been overtaken by debit card transactions, but demand for cash has doubled even as we move towards more digital payments. If a minority percentage of cash use is for actual transactions, then the Europol conclusion is alarming. The extent to which cash is an enabler of crime appears to be an under-researched and under-appreciated situation.

Given that both the Bank of England and Europol acknowledge that the extent of criminal use of cash is not known, what can be said of its use for that purpose? Reporting indicates that 'cash is still king' when it comes to criminal financing (Europol, 2015; Rogoff, 2016: 67; Kruisbergen et al., 2019). Furthermore, according to a UK national risk assessment on money laundering and terrorist financing, cash remains one of the main methods employed and the report also notes that ‘a significant amount of criminal activity in the UK generates its proceeds in cash’ (HM Treasury and Home Office, 2017: 5-6, 19). Whilst we do not have reliable statistics on the use of cash by criminals, central banks do know how much cash they introduce into the system, as described. Using cash production as a starting point, there have been attempts to produce rough estimates of the extent of the use of cash by criminals. In an article published by the American Institute for Economic Research, one estimate is that ‘more than a third of all US currency in circulation is used by criminals and tax cheats’ (Luther, 2017). And even when it comes to the use of cryptocurrencies, which will be examined more fully later, the end goal for most illicit actors is to transfer gains into cash:

> One of the most striking similarities between cybercrime and traditional crime is the offenders’ preference for cash. In the analysed cases, malware and phishing offenders as well as online drug traffickers change their digital currencies for cash, at least in part. (Kruisbergen et al., 2019: 569)

Having established that cash remains key to criminal activities, it is worth briefly discussing the issuance of large denomination notes. Cash, in high volumes, is heavy and this presents a transportation challenge to criminals. For example, £1 million in 500 euro banknotes weighs 2kg, whilst in twenty-pound notes, this would weigh 50kg (Casciani, 2010). For many years, law enforcement has observed that large denomination notes are not used in ordinary transactions and are instead a useful tool for criminals (Casciani, 2010; Europol, 2015: 6). The European Central Bank recognised this and halted production of the 500 euro note after ‘taking into account concerns that this banknote could facilitate illicit activities’ (European Central Bank, 2016). There have been calls to remove several other large notes, including the £50 note, but many remain (Sands et al., 2016). In the UK, a recent Treasury report (HM Treasury, 2019) acknowledges that the £50 note is not used routinely for transactions, but it will be kept for a number of reasons. These include that it is used as a store of value and that, given inflation, it may be needed in the future. (This latter point may well be of concern to those that are troubled by excessive government spending and debt).

One possible motivation for the continued circulation of cash is that governments make significant incomes from controlling the supply. This links in with our previous discussions about the history of money. It is very cheap to make large denomination bills and thus a profitable monopoly. For the US and the Eurozone, paper money earns in the region of 0.5 per cent of GDP, approximately $70 billion for the US in 2015 and a similar figure for the EU (Rogoff, 2016: 81). HM Treasury acknowledges that reducing cash and moving to digital transactions may reduce tax avoidance and money laundering, although this could be limited 'if the dishonest minority continue to use cash to hide or suppress their income' (HM Treasury, 2018: 15). There are likely, then, to be substantial savings by reducing or eliminating criminal use of cash; HMRC reports that just two behaviours, evasion and the hidden economy, account for £8.3 billion in lost tax revenue or a little short of a quarter of the total tax gap (the difference between expected and received tax) (HM Revenue & Customs, 2019: 10). Ironically, it is governments that create clean money and dirty it by supplying cash to criminals – a process referred to as 'reverse money laundering' (Rogoff, 2016: 4).

As the world moves increasingly towards digital transactions, this presents us with interesting times in terms of how criminals finance and conduct their operations. If 'cash is king' for criminals, then why was there, or has there been, a prevailingly negative narrative around cryptocurrencies? Are they currently used as extensively in crime as some say? And are cryptocurrencies likely to become a significant threat in the future should they ever achieve widespread adoption? These are important questions to consider regarding the potential securitisation of cryptocurrencies, particularly on the grounds of illicit use. If cash is more anonymous than cryptocurrencies and a preferred criminal tool, then in what ways are cryptocurrencies any worse than this?

4.3 Illicit Use of Cryptocurrencies

Having established the differences between cash and cryptocurrencies, and having examined the extent of the use of cash in crime, this section now explores the illicit use of cryptocurrencies. Again, document analysis is used in order to get an overall perspective of the issue. There are many academic, think tank and government reports that have researched this area, and these are drawn upon in this section. The existing research enables a specific consideration of the use of cryptocurrencies on the dark net, as well as of individual crime types such as ransomware. This section aims to assess the extent to which cryptocurrencies are an illicit threat in comparison to traditional financial systems.

There are many ways that criminals could use cryptocurrencies for crime. They can take them as a form of payment in place of cash in the real world, or they can use the digital form of money to transact online. But how prevalent is this activity? It is not sufficient to claim that cryptocurrencies are used in illicit activity. The analysis must go much deeper and consider the scale in terms of monetary value, as well as the proportion of cryptocurrency activity that is illicit. Without this level of understanding, the literature, research and headlines about the illicit use of cryptocurrencies often have little wider meaning. For example, a research paper titled, ‘The Rise in Popularity of Cryptocurrency and Associated Criminal Activity’ had this to say:

> Cryptocurrency such as bitcoin, Ethereum, and, more recently, Monero has become the currency of choice for many drug dealers and extortionists. (Kethineni & Cao, 2019)

This study looked at over 100 crimes involving cryptocurrencies. But there is no context given to any wider use of other tools in crime. The picture given, therefore, is potentially misleading, as there is no quantification of what ‘many’ even means. This is important as in securitisation theory, the securitising actor must argue their case, and this can only be done with proper consideration of alternatives.

The benefits of doing so are clear. For example, a report for the European Parliament (Keatinge et al., 2018) concluded that there have only been a small number of cases where virtual currencies have been used in connection with terrorist financing, for example, and that cryptocurrencies did not present any great advantage over existing methods. Where, then, is the criminal activity that causes cryptocurrencies to be viewed as such a security threat? And what evidence is there of this threat? To answer questions about the extent of criminal use, we first look toward the dark net and Tor hidden services, before exploring other specific crime types. For the remainder of this chapter, the dark net will refer to Tor unless specified, as it hosts most marketplaces.

4.3.1 The Tor Dark Net

In 2015 researchers from the University of Portsmouth analysed traffic on Tor over a six-month period (Owen and Savage, 2015). Surprisingly, the Silk Road dark net marketplace which was prominent between 2011 and 2013, was only receiving a little over 8,000 requests per day. In terms of usage at least, they showed that the vast majority of Tor is concerned with child abuse imagery, not with illegal trade where the use of cryptocurrencies is most associated.

The demise of the Silk Road provided further information about the extent of illegal markets on Tor. Evidence is available from the founder's trial (including from his laptop) that helps build the picture of the size of his operations. A research report on Tor marketplaces between 2013 and 2015 provides further interesting insight (Soska and Christin, 2015). In 2013, their results showed the Silk Road had sales of $300,000 per day, projecting to over $100 million per year or sales commissions in the region of $1.1-1.2 million. This is consistent with the trial evidence figure for the lifetime of Silk Road income as $214 million. The report also states sales figures of $6-8 million for the Silk Road 2. Lastly, the authors report daily sales volumes of $300,000-500,000 for the entire Tor marketplace ecosystem, based on an analysis of 35 marketplaces operating in the four years since the Silk Road began.

On first take, there appears to be some contradiction between these findings; if the traffic requests for the Silk Road were a very small part of Tor, can this be reconciled with a supposed 'massive' demand for drugs online (Soska and Christin, 2015: 46)? The figures give us a rough estimate of the size of Tor marketplaces at that time. More recent reporting also enables us to understand the scale of the issue on the dark net. According to the UN (United Nations Office on Drugs and Crime, 2018: 15), the AlphaBay marketplace had 200,000 users over its lifetime. Other researchers show that there are on average seventeen marketplaces available to users at any time (Foley, Karlsen, and Putniņš, 2018: 22). This is close to the figure observed of fourteen operational marketplaces in a joint report by the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) and Europol (2017). Using the upper figure of seventeen marketplaces and the AlphaBay users estimate of 200,000, gives a total serviceable dark net market of 3.4 million users.

To determine the extent to which dark net marketplaces represent a threat, we must consider the wider, global drugs market. The United Nations Office on Drugs and Crime's World Drug Report (2018) stated that 2016 saw the highest-ever production of cocaine at 1,410 tons. Some quick calculations based on a street value of £30 per gram (Shapiro and Daly, 2016) give a global cocaine value in the region of $38 billion. This is a valuation just for cocaine production, not the entire drug market. An EMCDDA report (2016) estimates the total retail value of the drugs market in the EU at a little over €24 billion. Furthermore, a White House report (Office of National Drug Control Policy, 2014) looking at American drug use put consumer spending on illegal drugs in the US at $100 billion per year, with some 23 million Americans classed as chronic users (defined as using drugs four or more times in a month) of just four main drugs. Whilst the dark net market figures are not directly comparable to these numbers, they are offered to enable the reader to consider the size of the threat that each represents. Although there is more to consider than scale alone, the likes of the Silk Road, with yearly sales of around $100 million, represent a small but significant fraction of the problem.

This conclusion begs the earlier question of why cryptocurrencies have such a widely associated connection with criminality. In part, it is because the strong properties of cryptocurrencies are as useful to criminals as they are to law-abiding citizens. Logically, criminals were early adopters of a new technology that offered enhanced privacy, as they have a lot to hide. This resulted in the high percentage of criminal activity in Bitcoin usage in 2013, as reported by the DEA. These early figures are also from a time before Bitcoin became more widely acknowledged. In fact, later DEA analysis from 2018 showed that this figure has flipped following the surge in awareness of Bitcoin in 2017 – 10 per cent of Bitcoin transactions were related to criminal activity, with the majority of transactions related to financial speculation (Russo, 2018). Whilst this ratio has fallen, the market has grown and so too, therefore, has the dollar amount of this criminal usage.

More recent research by a blockchain intelligence company that monitors cryptocurrency transactions reports that this ratio has fallen even further - with illicit activity in Bitcoin at only 0.5 per cent, based on $829 million spent on the dark net. They compare this figure to an estimated $300 billion of proceeds of crime in the US in 2010, which was about 2 per cent of the overall US economy (Robinson, 2019). There are several reasons to be careful in comparing these figures. First, they are far apart in time. Second, as discussed earlier, it is very hard to gather accurate information where the use of cash is involved. However, in terms of the threat that cryptocurrencies pose now, this is interesting. The ratio of criminal activity is very low – remember one earlier estimate that over a third of US cash is involved in tax avoidance and crime. Also, the scale of criminal activity in dollar terms is a much smaller problem than for cash. This supports the assertion here that whilst cryptocurrencies need to be considered for their criminal usage, this should not remove the focus of policy makers from the greater threat that cash poses in the present time. Finally, we must also repeat that usage now is a different concern to threat in the future, which we will come to shortly.

4.3.2 Anonymity and Money Laundering

A key criticism of cryptocurrencies, certainly concerning their use on the dark net, is the anonymity that they afford. Yet, cash is anonymous whilst some cryptocurrencies like Bitcoin are only pseudonymous. Bitcoin users have an address, but the identity of the person using the address is not made public. That is the theory, but how anonymous is the system in practice? There has been significant academic research in this area in particular. Ron and Shamir (2013), Androulaki et al. (2013) and Meiklejohn et al. (2013) have shown that anonymisation in Bitcoin is not as strong as believed. Techniques such as re-identification (creating an account with a vendor, for example, and transacting with them to identify addresses used) and crawling of websites to identify users who have displayed an address (for example, to receive a donation) are some that can be used. Their research shows that criminals trying to withdraw large amounts of funds need to use central exchange services, which is an obvious opportunity for law enforcement to de-anonymise thieves. They conclude that Bitcoin is not an attractive system for large amounts of illicit activity such as money laundering. This is in part because there are now several cryptocurrency intelligence companies that monitor all transactions on several blockchains, including Bitcoin (Cointelegraph, 2017). They use the techniques above and analyse the transactions in order to offer services to law enforcement and other interested entities (Wolfson, 2018). Their work also gives us an insight into cryptocurrency transactions in a way that cannot be done with cash.

Of course, this does not mean that criminals will not use Bitcoin for money laundering. In 2016, the founder of the Liberty Reserve digital currency service, a centralised pre-cursor to cryptocurrencies, pled guilty to laundering over $250 million. And more recently, the head of Europol is reported as saying that around 4 per cent of the £100 billion laundered in Europe is done using cryptocurrencies (The Economist, 2018). Once more, we should note that this means that 96 per cent of this money laundering is still being conducted using traditional methods, including cash. The point, though, is that criminals will launder wherever there is an opportunity and cases are seen in established finance too. Penalties on traditional banks since the financial crisis rose to $321 billion by the end of 2016 (Grasshoff et al., 2017). An internet search reveals countless cases of money laundering in traditional banks related to staggering sums of money. Again then, cryptocurrencies need to be kept in perspective with other methods of committing crime.

A report by Elliptic (Fanusie and Robinson, 2018), one such cryptocurrency intelligence company, looked at the flow of half a million Bitcoins from 102 illicit entities over a four-year period from 2013 to 2016. The study did not aim to cover all illicit activity, but it aimed to show what was done with these Bitcoins in a significant sample. They showed that over the four years, the source of over 97 per cent of the illicit Bitcoins was dark net marketplaces. Of note though, was that in 2016 this figure was around 80 per cent with ransomware taking almost a 16 per cent share. This rise of ransomware as a source of illicit Bitcoins from zero per cent in 2013 deserves some further examination that we will return to later. From a money laundering perspective, the report revealed some other interesting results. Looking at the destination of illicit Bitcoins, 45 per cent went to Bitcoin exchanges but there were two other significant recipients – both gambling and mixer sites received an approximate share of 25 per cent each. Mixer sites provide a service to hide the source of a cryptocurrency (Higgins, 2019). This is important to note for regulation; other services receive as large a share of illicit Bitcoins as exchanges, where fiat typically enters and exits cryptocurrency. We must also consider what percentage of total transactions are illicit; for exchanges less than 1 per cent, gambling sites 2 per cent and mixers 16 per cent. Whilst not all illicit Bitcoin is covered by the study, the figures do show that certain services require extra focus for anti-money laundering effort.

It is also interesting that, in 2016, criminals were becoming dissatisfied with the cost and speed of Bitcoin due to increased demand on the network, rather than with issues of anonymity (Barysevich and Solad, 2018: 1). As a result, Litecoin emerged as the second most accepted currency on the dark net (by 30 per cent of vendors), although Bitcoin retained its number one position and was accepted by all dark net vendors (5). It is important to note that cryptocurrencies focussed on privacy were not enjoying wide acceptance despite growing awareness - Monero, for example, was only supported by 6 per cent of vendors. The conclusion is that speed and cost appear to matter more to criminals than anonymity. The question of the importance of anonymity to cryptocurrencies as an illicit tool will be covered in more detail in the next chapter, as will the limited adoption of privacy coins. Researching users of cryptocurrencies for illicit purposes will reveal more about the properties that are most important to them.

In conclusion to this section, as long as there are criminals, there will be money laundering. Whether societies are using physical cash, traditional banking, or cryptocurrencies this is an enduring problem. The head of Europol's £4 billion estimate puts cryptocurrency money laundering as an arguably greater threat than commerce on the dark net. However, Europol's Internet Organised Crime Threat Assessment (2017) states that cryptocurrencies are not the biggest problem:

> Cash continues to play an important role when it comes to criminals realising their criminal gains; it has well-established methodologies for laundering, and

> is as readily exchangeable, relatively untraceable, and pseudo-anonymous – similar to the cryptocurrencies favoured in the digital underground. As a result, virtual currencies have yet to be adopted to any large degree by established money launderers who are likely to favour long established methodologies. (Europol EC3, 2017)

If the European Parliament and law enforcement agencies such as Europol and the US DEA have reported that illicit cryptocurrency usage is limited and that state money is a better tool, why do the headlines show a security narrative against cryptocurrencies that continues to this day? Are some of the memorable alliance, whom we have seen commentating about the threat of cryptocurrencies, misinformed, or is a security argument intentionally used when other issues are potentially of greater concern?

Criminal attitudes do not yet show a strong move towards more privacy focussed alternatives, so there remain opportunities for de-anonymisation certainly whilst Bitcoin remains ubiquitous on the dark net. The threat then of cryptocurrencies in relation to money laundering remains relatively low when compared to cash and other traditional methods. Increased regulation and lax use of cryptocurrency privacy features offer plenty of opportunities to trace funds for the foreseeable future, especially as tighter regulation arrives at the key nexus points of exchanges and other service providers. Specific services, such as gambling sites and in particular mixers, should be given extra attention by regulators and law enforcement due to the higher percentage of illicit funds they receive.

4.3.3 Ransomware

The Elliptic research in the previous section presented an interesting anomaly. Whilst dark net marketplaces are the source of the majority of illicit Bitcoin, in 2016 there was a leap in ransomware as the source. This deserves some further attention to better understand the part that cryptocurrencies play in these attacks.

In a study of most of the ransomware seen between 2006 and 2014, only 2.86 per cent used Bitcoin as a ransom method, with 10 per cent using premium numbers and the majority, at a little over 88 per cent, using prepaid online services such as Paysafecard (Kharraz et al., 2015). Using a system such as Paysafecard, the attacker receives vouchers from the victim which can then be sold elsewhere. More recent research (Paquet-Clouston, Haslhofer, and Dupont, 2018), however, comments that nearly all the ransomware families observed used Bitcoin for payment, suggesting that this is now a preferred method. Interestingly, cryptocurrencies also potentially offer an improvement to other traditional crimes, such as in a case of real-world kidnap where a cryptocurrency ransom was claimed instead of cash (Libell and Martyn-Hemphill, 2019). This is likely to be a small crime type in comparison to ransomware. Policy makers should consider, though, that ransomware can operate without cryptocurrencies. Other forms of digital value exist, which criminals will use should cryptocurrencies no longer be available. This is also discussed in the next chapter looking at users of cryptocurrencies for illicit purposes.

Another point to consider is the amount of money that ransomware raises for the perpetrators. Using the example of CryptoLocker, a notable ransomware that had a large impact, we can see that it raised 1,226 Bitcoin as of 15 December 2013 (Spagnuolo, Maggi, and Zanero, 2014). Using the price of Bitcoin on that date (price as shown on Coinmarketcap, accessed 07 August 2018) gives an approximate value of Bitcoin raised of $1 million. Further research provides an estimate of the total value raised from ransomware, between 2013 to mid-2017, at nearly $13 million (Paquet-Clouston, Haslhofer, and Dupont, 2018). Whilst cryptocurrency value is extremely volatile, which impacts its usefulness as a medium of exchange, an attacker may gain further if the assets are held, and they appreciate. However, these amounts are modest compared to the global sums of criminal activity seen so far. It must be stressed that whilst the ransom secured may be unexceptional, the wider impact that these attacks have is huge - WannaCry, for example, is estimated to have incurred a wider cost of $4 billion (Berr, 2017), perhaps explaining why Europol has commented that ‘ransomware attacks have eclipsed most other global cybercrime threats’ (Europol EC3, 2017: 10). The point to be made is that ransomware does not raise huge amounts of money, and it is not a major financer of crime groups. This does not trivialise all the other significant impacts that ransomware causes.

Indeed, the scourge of ransomware continues. Ransom payments increased by 300 per cent from 2019 to 2020, totalling over $400 million (Europol, 2021). In 2021, the Colonial Pipeline attack was one of several high-profile ransomware attacks. Perpetrated by Darkside, a Russia-linked group, the attack disrupted gas supplies in the US and demanded 75 Bitcoin in ransom - approximately $4.4m at the time (Winder, 2021). An interesting side point was that the US authorities managed to recover $2.3m of the ransom through subsequent activities. The head of the UK's National Cyber Security Centre (NCSC) has described state-sponsored attacks as a 'strategic threat' but commented that the main threat for most businesses and individuals was criminals (K. Hayes, 2021). But the line between the two is often blurred, resulting in ransomware becoming an increasingly geopolitical issue. At a summit in Cornwall in 2021, the G7 called on Russia to 'hold to account those within its borders who conduct ransomware attacks' (as quoted in Hayes, 2021: 11). Cryptocurrencies clearly have a part to play in ransomware, but it is too simplistic to simply see them as the sole cause.

We can see the political dimension that these attacks can have in two of the most high-profile ransomware attacks of all time, WannaCry and NotPetya, which occurred in 2017 and impacted the United Kingdom as well as many other countries. WannaCry is memorable in the UK for the disruption that it caused to the NHS. WannaCry, though, was associated with only six Bitcoin addresses and approximately $100,000 of Bitcoin; NotPetya had only one address and four Bitcoin or a value of about $11,000 at the time (Paquet-Clouston, Haslhofer, and Dupont, 2018: 7). These numbers are particularly low and of even more interest when we consider that the US Computer Emergency Response Team (US-CERT) released a malware analysis report of NotPetya and summarised that the design did not appear to make it possible for the attackers to decrypt a victim's files even if they had paid a ransom (US-CERT, 2017). In both cases, the UK publicly attributed the attacks to state actors; in the case of WannaCry to the North Korean Lazarus Group, citing sanctions avoidance (Foreign & Commonwealth Office and Lord Ahmad of Wimbledon, 2017) and for NotPetya the blame was placed on the Russian

Government, where the attack ‘masqueraded as a criminal enterprise but its…primary targets were Ukrainian’ (Foreign & Commonwealth Office, National Cyber Security Centre, and Lord Ahmad of Wimbledon, 2018).

These last two attacks show the political dimension that ransomware can have. As such, policy makers should recognise that the role cryptocurrencies played in them was marginal, with the motivation potentially more political than financial. In the case of NotPetya, the use of cryptocurrencies was incidental and the motive for the attack was more directly political. As discussed, if cryptocurrencies did not exist then attacks like NotPetya or WannaCry could continue, either with an alternative payment method or without one at all. We consider the potential efficacy of a cryptocurrency ban in the next chapter, as well as revisit the other payment mechanisms that exist that an illicit group may turn to should cryptocurrencies not be available.

4.3.4 The Future Threat and Privacy Coins

This chapter has focussed so far on the criminal use of cryptocurrencies from two perspectives: the absolute scale of crime and criminal activity as a percentage of total activity. There will be no attempt to predict these figures in terms of future threats, as the world of cryptocurrencies is volatile and unpredictable. However, there are several key areas to consider in terms of the future threat that cryptocurrencies pose.

The world is becoming increasingly cashless; in the UK online transactions have overtaken cash and several parts of the world are moving towards cashless societies – Sweden and China being two that are widely reported (Alderman, 2018; Yang, 2018). Whilst there are concerns about the decline of cash, including for use by the elderly and vulnerable, the trend is clear (HM Treasury, 2019: 2). Should we reach the point that cash usage becomes minimal, or even obsolete, how does that change the analysis of this chapter?

First, if cryptocurrencies are a scam, do not function as money and cannot compete with fiat currency, then there is little chance that they will ever become a significant part of global finance. As a US Treasury Secretary once said, ‘I won’t be talking about Bitcoin in ten years, I can assure you of that’ (Isige, 2019). If this is the case, then we need not spend much time debating cryptocurrencies as they will fade away in time. However, the world is in a very unsettled period in terms of the forms of money available and our usage of them, as discussed. We are in a period of ‘increasing monetary pluralism’ – there is more choice now in how we transact than ever before (Dodd, 2017: 36). It is presumptuous to rule out any one form.

The mix of options is still evolving. As discussed, the emergence of cryptocurrencies has led central banks, including the Bank of England and others, to investigate whether they should develop a CBDC (Carney, 2018: 11; Huang, 2019). We also saw Facebook’s attempt to launch a cryptocurrency called Libra and that those plans were met with opposition. As a result of the increasing scrutiny, Libra subsequently rebranded to ‘Diem’ and scaled back its ambitions, moving from its base in Switzerland back to the US (Wilson & Schroeder, 2021). This still was not enough, though, and the project closed down in 2022. The challenge to create an alternative or complementary money that is accepted by the memorable alliance continues.

The future for cryptocurrencies remains uncertain and the issues are societal, rather than anything else. And also geopolitical as the future of money unfolds. At the heart of the debate, though, is the issue of the disintermediation of banks and the state from money - Facebook did not aim to do either, but Bitcoin continues to do both (Dodd, 2017: 37). Whilst Facebook stated they would not launch Libra without regulatory approval (Lee, 2019), Bitcoin has already been operational for over ten years, yet Libra/Diem never even made it to market. Regulation, and acceptance by the memorable alliance, are, therefore, key areas to consider for the future of cryptocurrencies.

The FATF Recommendations require that countries should regulate virtual asset service providers (VASPs) (Financial Action Task Force, 2018: 15). This means that all VASPs, including key nexus points for cryptocurrency activities like exchanges, are subject to the same rules and standards of other financial institutions. The EU’s

5th Anti-Money Laundering Directive (5AMLD) was also amended into national law in January 2020 and amongst its aims is preventing risk from cryptocurrencies by extending to them Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) rules (European Commission, 2018). Furthermore, below these levels of intergovernmental and supranational regulation are the array of approaches at a national level (Blandin et al., 2019). Some countries, such as China, have banned cryptocurrency activities whilst in the UK a 'Cryptoassets Taskforce' was established to develop a response to this new technology (HM Treasury, Financial Conduct Authority, and Bank of England, 2018). As the regulatory environment tightens, the ease of criminal activity reduces; for example, through identity being required to use services.

But if a share of untraceable cash transactions moves to a digital form this may be an improvement from a law enforcement perspective, as commented on by the DEA:

> The blockchain actually gives us a lot of tools to be able to identify people…I actually want [criminals] to keep using them. (Russo, 2018)

Ironically though, this could see an increase in crime and a change in crime figures, as cash is reduced and more digital crime is discoverable (Business Insider, 2018). In Sweden for example, over a ten-year period, reported fraud crime has tripled (The Swedish National Council for Crime Prevention (Bra), 2019). And more recently as a further example, the MET police seized £180m of cryptocurrency related to international money laundering (BBC News, 2021a). This also shows that opportunities still exist for law enforcement in cryptocurrency-related crime. Of further note from this case, the Deputy Assistant Commissioner was quoted as saying:

> While cash still remains king in the criminal world, as digital platforms develop we're increasingly seeing organised criminals using cryptocurrency to launder their dirty money. (As quoted in BBC News, 2021)

Policy makers should note that a reduction in cash usage would see criminal behaviour change and adapt, resulting in increases in different types of crime.

Nonetheless, these quotations are key, as they speak to the original paradox in my first thoughts about cryptocurrencies. Again, if a law enforcement agency sees a policing advantage in the continued use of cryptocurrencies by criminals, does this not once more clash with the illicit usage narrative that is often used in objection to them? This is an even starker observation in face of the fact that several agencies have also commented that traditional finance, and state-provided currency, primarily physical cash, remain better and more effective tools for illicit activity. This is, of course, the justification for the research chapter to examine this view of law enforcement further. But it is of note, that the securitising language appears to be coming from the memorable alliance, rather than from the law enforcement agencies closest to the issue of the illicit use of cryptocurrencies. The law enforcement chapter will explore these issues and examine whether the claims we have seen in the narrative are shared by those in policing.

The final area to consider in terms of the future threat of cryptocurrencies is privacy focussed coins. We saw earlier that dark net users had become frustrated by the fees and speed of Bitcoin during heavy demand, but this did not lead to a significant shift to privacy coins, which aim to be more anonymous than Bitcoin. What if this shift does occur? Are privacy coins as ‘anonymous and untraceable’ as cash? There is a growing body of academic literature examining these coins, which shows that they too are vulnerable to de-anonymisation. Kappos et al. showed that most users of Zcash did not even use its main anonymity features, whilst those that do use them do so in a way that is identifiable and reduces anonymity for other users (2018: 475). Research into Monero showed that the origin of funds can be shown in 88 per cent of cases (Kumar et al., 2017); further weaknesses are also shown in a separate study (Moser et al., 2018). As with all technologies, if they are not implemented or used correctly then there is a risk it does not achieve their aims. A criminal must also bear in mind that should a flaw emerge in a privacy coin at a later date, this may suddenly enable the identity of historic transactions to be revealed. These flaws are fixed over time, improving these coins but future risks remain. Considering these issues, even privacy coins are unlikely to be preferred to cash, which remains more useful as an anonymous and untraceable tool. If you also factor in the impact that improved regulations are having, then there will continue to be significant risk and difficulty in the use of privacy coins. Whether these coins should be an accepted currency is also a societal question regarding privacy, as an extension of the same unresolved debates that exist over the use of cryptography for confidentiality purposes (see, for example, Moore and Rid, 2016). Perhaps Bitcoin, as a pseudonymous system, provides a more acceptable balance between privacy and traceability that is better suited to society than a truly anonymous privacy coin – this is a tough issue for policy makers to ponder. We explore some of these issues in the following chapter, where we also move on to research the actual users of cryptocurrencies for illicit purposes.

4.4 Conclusion

In this chapter, we set out to examine the first research sub-question. First, there was an exploration of how the security-led narrative about cryptocurrencies has been constructed. To do this, the focus was on the US dollar and the officials of the memorable alliance in the US monetary system. Through document analysis, securitising headlines were examined of some key US officials, including the Treasury Secretary, the Federal Reserve Chairman and CEOs of the largest US banks. Security concerns about the illicit use of cryptocurrencies ran as a persistent thread through the narrative. There are other concerns, such as whether cryptocurrencies can even be considered as money, but even in 2021, cryptocurrencies were still being labelled by US officials as a tool for money laundering, drug trafficking and terrorism.

The chapter then moved on to examine the second part of the research question; exploring the extent to which cryptocurrencies are more or less of a threat than traditional financial systems. Using a variety of sources, we saw that cash remains king for criminal activity and that traditional finance remains a favoured methodology. Research also showed that criminal usage of cryptocurrencies is smaller in comparison. This trend continues. In 2020, the illicit activity in cryptocurrency transactions fell from 2.1 per cent in 2019 to 0.34 per cent. In terms of transaction volume, this represented a fall from $21.4 billion to $10 billion (Chainalysis, 2021). As the cryptocurrency economy grows, illicit use has become smaller, and it remains small in comparison to traditional finance.

If cash is the premier illicit tool, and it is provided by the state, why is there a prevailing security concern about cryptocurrencies? We also saw that US law enforcement officials had reported the low use of cryptocurrencies in crime and that they had even remarked that they want criminals to use cryptocurrencies as they offer great opportunities for enforcement. This apparent contradiction leads us to our next chapters. First, we return to a gap identified in the research by exploring how useful cryptocurrencies are for crime by examining the views of users of them for illicit purposes. In this way, we will see if the users find them as useful as the narrative suggests. The following chapter will then address a further gap in the research by interviewing law enforcement officers about their experiences with cryptocurrency investigation. Through these two chapters, the aim is to gain a deeper understanding of the criminal threat cryptocurrencies pose. And by doing so, are the contradictions resolved or does the research suggest a different perspective on the security threat that cryptocurrencies pose, other than merely as a criminal tool?

5 Cryptocurrency Usage on the Dark Net

The previous chapter showed how some of the memorable alliance have attempted to securitise cryptocurrencies on the grounds of their illicit use. This included claims that cryptocurrencies are an excellent tool for illicit activity. But, as per the methodology described in Chapter 3, what do the actual users of cryptocurrencies for illicit purposes say about them and which properties are most useful? In the next two chapters, the security narrative of cryptocurrencies is researched more deeply from two different perspectives. Chapter 5 addresses this user perspective and relates to research sub-question two, 'What evidence is there that cryptocurrencies are actually useful for illicit activity?' The following chapter then looks at these issues from the point of view of law enforcement officers. Through these two chapters, therefore, we learn more about the security threat of cryptocurrencies from those who are more familiar with them, have used them and, arguably, know more about them and their advantages and disadvantages.

Chapter 2 also highlighted that there was a gap in knowledge about the views of illicit users specifically, as the many user studies reviewed focussed on more 'regular' groups such as students. Given that illicit use is such a prominent issue in the securitising narrative, this is a crucial gap in the research that this chapter will address. Furthermore, for all the research that takes place about the dark net, little if any has explored the payment mechanisms that facilitate illicit internet activity. This chapter, therefore, also deepens our understanding of payments on the dark net from a security perspective. An article based upon the research of this chapter was published at STAST2020 (Butler, 2020).

5.1 Background

This section provides some additional background context for the research conducted. It is first worth noting that for all the headlines that we saw in the previous chapter, there was little detail in them or the accompanying pieces about the specific threat that cryptocurrencies purportedly pose. The FBI was reported as being concerned about the lack of a central authority in relation to cryptocurrencies, but they also noted that Bitcoin is only pseudonymous and that the degree of anonymity depended in large part on the user. This gap between the memorable alliance and law enforcement has been commented on extensively and the next chapter will examine this more closely. But this leaves us with a question raised before – what exactly is it about cryptocurrencies that is the threat? And more precisely, which properties, in particular in comparison to cash, are to the advantage of an illicit user? Furthermore, if the analysis of the previous chapter showed that cryptocurrencies are not as useful for crime as traditional methods, then why does the narrative persist?

On 25 February 2015, the Superintendent of New York State's Department of Financial Services (DFS) delivered a speech at Columbia Law School about the role of regulators after the Great Financial Crisis. In a section on cyber security in the financial sector, the Superintendent made clear the extent of his department's fears:

> We are concerned that within the next decade (or perhaps sooner) we will experience an Armageddon-type cyber event that causes a significant disruption in the financial system for a period of time – what some have termed a "cyber 9/11". (Mondovisione.com, 2015)

On the very same day, DFS released its revised proposed rules for businesses with cryptocurrency services; the so-called 'Bitlicense' regulation, which came into force a few months later. This quotation highlights the rhetoric of extreme fear that often surrounds matters of cybercrime. Indeed, for several decades there were predictions that 'Cyberwar is Coming!', to which Thomas Rid responded that 'Cyber War Will Not Take Place' (Rid, 2012). The point is not that there are no risks, nor that cyber-attacks are trivial, but the comparison is drawn to show the need for 'a more nuanced terminology' in relation to these threats (5). Has this 'fear' of cybercrime spread to cryptocurrencies? Or could a lack of understanding of them, or even just a fear of new technologies, explain the reaction to them? The analysis in the previous chapter, especially in terms of total amounts and the percentages of illicit usage of cryptocurrencies, certainly suggests there is potentially some irrationality in the opposition to cryptocurrencies on the grounds of illicit use.

If the Chairman of the Federal Reserve commented that cryptocurrencies are ‘great if you are trying to launder money’, in what way are they great? The reporting of law enforcement agencies and others seems to contradict this opinion, with cash and traditional methods still favoured by illicit actors. And more than a decade after Bitcoin went live, cryptocurrencies have not yet played a critical role in a Cyber War, a Cyber 9/11, or been responsible for an explosion in dark net crime that threatens society. The DFS Superintendent said of virtual currencies in a 2013 interview that ‘it feels as if the major advantage they’re providing is anonymity’ (Farrell & Larson, 2013). And in evidence given in 2014, DFS was told that illicit activity using virtual currencies ‘reduces or even eliminates practical barriers to entry’ thereby enabling the purchase of drugs globally with ‘essentially the push of a button’ (US Department of Justice, 2014). There is little dispute that cryptocurrencies are used for criminal activity, but we return to the core questions of this chapter: How useful are they really? Is anonymity their major advantage? And is purchasing on the dark net as simple as clicking a button? A social constructivist approach to these questions is taken. In the previous chapter, we saw what some of the memorable alliance had to say about cryptocurrencies, now we ask what the users *themselves* say of their attitudes and motivations towards the usage of cryptocurrencies for illicit purposes. To this end, this chapter presents the first user study of cryptocurrencies for illicit activity.

Chapter 3 contains detailed descriptions of the data collection, sample selection, data analysis and ethics as they relate to this research chapter. This will not be repeated here, but a summary is provided as a reminder. The results are then presented in relation to three main findings. First, we examine whether anonymity is the major advantage of cryptocurrencies. Second, we explore the extent to which illicit internet activity relies on cryptocurrencies as a payment mechanism. And third, we address the concern that the dark net and cryptocurrencies enable the global purchase of illicit goods and services ‘with the click of a button’. The chapter concludes with a greater insight into the extent to which cryptocurrencies can be useful for illicit activity and provides a clearer understanding of another dimension to the illicit threat that cryptocurrencies pose. This is of course useful to the overall discussion and conclusions of this thesis.

5.2 Methodology

This section briefly summarises the relevant parts of Chapter 3 and adds some detail regarding the final search term selection. As a reminder, a dark net research expert had called for more ‘humanistic inquiry’ of the dark net and had noted that forums and social networking sites were under-researched (Gehl, 2018). Given positionality and ethical considerations, a passive data collection strategy was selected and the CrimeBB dataset from the Cambridge Cybercrime Centre (CCC) was chosen as the data sample for analysis. The dataset contained more than 100 million posts taken from 18 underground and dark net forums. The forum files were downloaded from CCC and then collated into a SQL database. A three-step process was then applied to data analysis to reduce the posts to a manageable number for coding. ‘Bitcoin’ was selected as a master search term, and this reduced the sample to more than 200,000 posts.

A coding test showed that 200,000 posts would take one year of full-time work. As per Chapter 3, IBM’s SPSS Modeler was then used to identify the top 500 concepts in the posts. These concepts were analysed, and some additional search terms were selected based on relevance to the topic and frequency of the posts. These terms are shown in Table 3. ‘BTC’ is the three-letter trading ticker for Bitcoin. Monero was chosen as it is a prominent privacy coin and anonymity is a key property of cryptocurrencies for research.

Table 3: Search Terms Selected from Top 500 SPSS Concepts

Search Term	**Concept Ranking**	**Percentage of Documents**
Money	3	10
BTC	5	9
Cryptocurrency	89	2
Monero	321	1

In addition to the four terms from the Top 500 SPSS concepts, a further four related terms were selected from other smaller identified concepts. These were ‘Zcash’ which is another privacy coin, ‘police’ in relation to illicit use, ‘privacy coin’ and ‘criminal’. To complete the final search term selection, I also added three more search terms based on experience: ‘Dash’ (another privacy coin), ‘Feds’ as a common term for law enforcement and ‘Jail’ as a final term that might reveal interesting content related to illicit activity. Using the search term process as described in Chapter 3, a final selection of 16,405 posts was captured and then uploaded to QDA Miner Lite for coding and analysis.

Table 4: Final Search Term Selection

Master Term	**Top 500 SPSS Concepts**	**Other SPSS Concepts**	**Related Terms**
Bitcoin	Money	Zcash	Dash
	BTC	Police	Feds
	Cryptocurrency	Criminal	Jail
	Monero	Privacy Coin	

We now move on to the results of this strand of research. As per the ethics discussion in Chapter 3, neither usernames nor verbatim quotations are used. This makes it harder to clearly present the words and opinions of users. Where a specific post from CrimeBB is discussed, the term ‘author’ is used generically in lieu of any username connected to a post.

5.3 Results

Cryptocurrencies present a user with an alternative financial system with differentiated properties from traditional state money. Among the key properties are anonymity (or pseudonymity), speed, low cost (usually), decentralisation (no third parties), self-sovereignty, the immutability of the blockchain and finality. Finality here is defined as a payment transaction that, once made, cannot practically be undone (in this sense, like a bearer asset such as cash). For the university students surveyed by Bashir, Strickland and Bohr (Bashir et al., 2016), there was a political motivation towards usage and novelty was a greater draw than anonymity. But how does this view change amongst different user groups with different needs and wants? Specifically, which properties were most important for the adoption of cryptocurrencies by underground and dark net forum users? By researching and analysing the properties that the users themselves find useful, we gain a better understanding of the usefulness of cryptocurrencies as a tool for illicit activity. And this enables us to more critically assess the claims seen in the previous chapter.

5.3.1 Anonymity – The Major Advantage?

In the background section, the DFS Superintendent remarked that anonymity is perhaps the major advantage of cryptocurrencies. And this makes sense at a surface level – if there was a digital currency that could be used anonymously that enabled the purchase of illegal drugs at the click of a button, then surely this would be a threat? But the academic research in Section 4.3.2 on anonymity showed that cryptocurrencies like Bitcoin are only pseudonymous. If Bitcoin is not anonymous, then logically anonymity cannot be its major advantage as it does not have that property. This is a paradox that deserves some investigation. Anonymity is important to those that conduct illicit activities but does Bitcoin or any other cryptocurrency solve this problem?

The research of this chapter is predominantly qualitative, based on the content of the posts, but in order to support some discussion, I also submitted some key search terms related to the properties of cryptocurrencies into QDA using the text retrieval function to give a sense of the frequency that certain terms appeared in the 16,405 posts. The results of this exercise are shown in Table 5:

Table 5: Total Number of Posts Containing the Selected Search Terms

Search Term	**Number of Posts with Hits**
Anonymity	396
Anonymous	776
Pseudonymous	23
PayPal	3325
Chargeback/Charge back	333 (123/210)
Privacy coin	109
Monero/XMR	1337 (993/344)
Dash	238
Zcash	130
Verge	53
Decentralised/Decentralized	360 (54/306)
Speed	1233
Cost	855
Immutable	11
Libertarian	27
Cypherpunk	3

The meaning derived from this table is crude, but it is useful in a discussion of the properties that were important to the users of this study, especially in relation to Chapter 2. Of note, there was very little discussion observed in the posts of the libertarian or Cypherpunk ideals that are often mentioned in connection to cryptocurrencies, as we saw in the results of other user studies. As can be seen in the table, ‘Cypherpunk’ is seen only three times and ‘Libertarian’ 27 times. This again suggests that different groups find different properties important for different reasons. The other figures from the table need to be handled cautiously. Some terms, like ‘speed’ and ‘cost’, appear relatively frequently but may have been used in many different contexts among the posts. Others, such as ‘decentralis(z)ed’, were present in many ‘generic’ posts that served as introductions to cryptocurrencies. In contrast, the difficulty that many users had with traditional finance stood large as a theme in its own right. The term ‘chargeback’ is singular in its meaning compared to ‘cost’ for example, which caused it to emerge, along with ‘PayPal’, as significant codes of interest. Notably, neither of these terms was used in the initial filtering of posts from CrimeBB. The issue of chargebacks will be considered in more depth later in the chapter.

Table 5 shows that anonymity is a relatively frequent term in posts. The dark net forums, in particular, are dense with discussions about operational security, or how not to get caught. However, a crucial point authors note is that complete anonymity is impossible to achieve – the best that can be hoped for is sufficient security to be practically safe. Second, anonymity is achieved through a raft of measures, not solely through one method such as the payment mechanism. A layering of protection is needed to create obscurity. (There will be more on this in the following sections.) These are important distinctions, as anonymity is not, therefore, the ‘main advantage’ offered by cryptocurrencies. They can aid in the endeavour but do not solve the issue in its entirety.

Analysis of CrimeBB is also interesting from a longitudinal perspective, as we can observe the changes in attitude and behaviour towards cryptocurrencies. It also reveals the spectrum of user knowledge about the properties of cryptocurrencies and how to use them for illicit activity. There is strong evidence from 2011/12 that many users believed that Bitcoin was fully anonymous. They were likely using the Silk Road thinking that tracking or any form of identification was not possible. Despite this, there were other users, as early as 2012, who were aware of the pseudonymous nature of Bitcoin. In one such post, an author expresses his exasperation that others keep claiming that Bitcoin is completely anonymous. There is a clear difference in understanding between those that are technically savvy and well-read, and those who are not. To those that are not, there was a belief that Bitcoin was as anonymous as cash and served that purpose as ‘cash on the internet’. Posts show that users felt it was anonymous as they did not have to provide a genuine name when creating a wallet. But there is much more to consider when conducting an illicit transaction than just the payment method alone. Even if Bitcoin was fully anonymous, this does little for privacy if, for example, the Bitcoin was bought using an account connected to a real-world name. Many such examples have led to arrest, perhaps none more prominent though than that of Russ Ulbricht, the founder of the Silk Road dark net marketplace, whose downfall was linked to a Gmail address with his real name (Hume, 2013).

By 2014, the underground forums evidence a widespread recommendation to use third-party ‘tumbler or mixer’ services with Bitcoin as the prevailing method to increase the obscurity of any trail. Ultimately though, as one author explains, Bitcoin is only as anonymous as the individual behind it – a point made in the leaked FBI report that led to the 2012 headline shown in Chapter 4. Despite this, claims of Bitcoin’s complete anonymity continue through all years, as well as posts of disbelief at this lack of knowledge. Remarkably, in 2019 there is even evidence that users were buying cryptocurrencies on regulated exchanges with real-world details and then sending funds directly to illicit sites. There is a noticeable difference between the underground and dark net forums in these matters. In general, the dark net forums are heavily dominated by operational security discussion and so are much more aware of the issues and take them more seriously. This makes sense and Tor appears to filter some of the banality that the easier access to underground forums enables. And perhaps this mixed understanding of the anonymity provided by Bitcoin is paralleled by a lack of understanding by those who claimed that this was the major advantage of cryptocurrencies. A new ‘cyber’ tool, connected with dark net marketplaces, may well have caused fear in officials, especially since the research and knowledge we have now were not present in those early years.

The use of tumblers continued to be a widespread practice from 2014 to 2016. After this time, however, users moved away from this method, citing trust (some services have control of your funds and can disappear with them) and also efficacy – you may mix your ‘dirty’ coin only to receive another ‘dirty’ coin in return. In 2017, one of the main tumblers closed its services as it changed its philosophy, realising that Bitcoin was intended as a transparent system. This change also aligns with the other significant development of this time, which was the emergence of privacy coins, designed with enhanced anonymity in mind in comparison to Bitcoin.

Table 5 is again a useful reference at this point. Dash, or Darkcoin as it was previously known, had some prominence in the 2014-15 period but posts show that users moved from it, questioning if its technology enabled any more security than

Bitcoin. Instead, it was Monero that emerged as the most talked-about privacy coin of choice. By 2018, there was a marked clamour about the use of Monero, with some proclaiming it the rescuer and future of dark net markets. This is supported by Monero's daily transaction chart, which has been on an upward trend since early 2019 and now regularly records more daily transactions than the peak of the 2017 bubble (Bitinfocharts.com, 2020). Despite the increased security on offer from Monero, Bitcoin retains its prominence even on dark net markets (Europol, 2021: 36). Why is this the case? That is exactly the question that many post authors raise. In 2018, one author commented that Monero was not an option on many markets. A 2019 post notes that Bitcoin is awful for anonymity or privacy. It also becomes noticeable at this time that there is anger towards Bitcoin as users cannot understand why anyone would use it for illicit activity when it has a traceable, public ledger. There are even outright calls and advice to stop using it on the dark net. Others thought it obsolete in terms of the privacy it offers and even described it as terrible for illicit activity. This is interesting in the context of the securitising speech acts we have seen. Again then, if anonymity really is the main advantage of cryptocurrencies, why would anyone still use Bitcoin for illicit transactions when it is now widely known that it is only pseudonymous?

Several explanations arise. First, there are the network effects that Bitcoin has achieved. It is *the* cryptocurrency that is universally available and accepted. People have also learnt how to use it over more than 12 years of operation. One seller questions the ability of buyers to use a new currency (Monero), suggesting it would be easier to accept Bitcoin and take responsibility for anonymity as part of their own operational security. Another user explains that there is no cyber law enforcement in their country, meaning there is nothing to worry about if using Bitcoin. This question of deterrence also emerges in many other posts. The widespread opinion is that law enforcement only cares about large dark net participants – if you are a buyer of small quantities then again Bitcoin will probably do. Similarly, another author states that major criminals do not need Bitcoin and that it is a poor tool for money laundering. Once more, the exact opposite of the claim we saw by the Chairman of the US Federal Reserve in Chapter 4. Some other users fall into the categories of careless, misinformed, stupid, entrenched and even lazy, as the author explanations for the continued use of Bitcoin. Additionally, Monero is viewed as harder to get and use than Bitcoin. Users also worry that a connection to Monero looks suspicious. In a 2019 post, another author asks why anyone would use Monero, as none of the markets had multi-signature transactions – leaving participants to run the risk of market exit scams. One final post gets to the crux of the issue – the main advantage of Bitcoin is not anonymity.

That Bitcoin is still widely used even though it is common knowledge that it does not offer strong anonymity is prima facie evidence that this is not the main advantage on offer. To return to a point made earlier, anonymity is not and should not be sought from one element of activity. It takes many aspects of operational security to achieve sufficient anonymity – that is, a transparent currency can be used for an illicit payment as long as other countermeasures are used. For example, a user could acquire a currency with fraudulent details; in this case, it does not matter that the transaction is not anonymous. And so it is with Bitcoin and cryptocurrencies. The payment mechanism is only one part of a whole set of other considerations that work to achieve the desired anonymity. It is not singularly important for Bitcoin to be anonymous – if it was, it would not be used. In this way, we can say that dark net markets are not dependent on cryptocurrencies or a perceived advantage of anonymity. They can survive without this necessity. This conclusion supports Bancroft and Reid who argued the same based on the existence of drug trading on the internet with no attempt to hide identity (2016: 508).

How, though, is it possible to trade illicit goods on the internet if Bitcoin does not provide anonymity? Later sections will explore this in more detail. For now, we can summarise that illicit activity requires an overall level of anonymity, but this is not achieved through Bitcoin or a privacy coin. In this way, Bitcoin can be pseudonymous and still be used, as long as other methods are employed. Privacy coins enhance anonymity, but even so, do not provide a singular solution. If anonymity is not, therefore, the major advantage of cryptocurrencies, then what is?

5.3.2 If It’s Not Anonymity, What Is It?

Whilst anonymity *generally* is important to those conducting illicit activities, it was the property of finality that emerged strongly from the coding. Returning to Table 5, ‘PayPal’ was by far the most common search term, whilst ‘Chargeback’ was seen significantly more often than either ‘Libertarian’ or ‘Cypherpunk’. Many authors spoke of difficulties with using traditional finance and discussion about PayPal, in particular, was of note. In 2014, PayPal extended the time to raise a dispute from 45 to 180 days. The feeling among many authors on CrimeBB was that this was great for scammers and terrible for sellers - the issue being that a trade could be made, only for a buyer to complain later causing accounts and funds to be frozen. Authors reported losing large sums of money due to chargebacks, which sometimes were even related to payments made with stolen funds. One comment summed up the situation: no one would exchange Bitcoin for PayPal, as Bitcoin is not reversible whilst PayPal is.

Furthermore, the view was that third parties tended to side with the buyer rather than the seller. The result was that many people looked for alternatives without chargebacks. In one discussion of different payment processors, the answer given was simply to accept Bitcoin, as there is no chargeback risk. Another author commented similarly that Bitcoin’s volatility was acceptable as the main advantage was that once a payment was made it cannot be recalled. Sellers remarked that there is nothing that you can do to avoid chargebacks, other than use a payment method that does not have them. And there are several mechanisms other than Bitcoin that can also be used, such as cash or cheques. More is said on this later. But if a seller uses a mechanism such as PayPal, then there is nothing that can be done to avoid chargeback – if a stolen card has been used, or a buyer opens a dispute then a seller is locked into a disagreement that could take months, and even court action, to resolve. The desire for finality in payments is therefore clear to see.

In 2014 when Bitcoin was relatively unknown, there were sellers considering accepting only Bitcoin despite the fear of losing most of their customers by rejecting more accepted payment methods. It is also important to note that this issue was not limited to illicit activity - a lot of this discussion took place on the underground forums, even as far back as 2012 when authors had problems using Liberty Reserve. The discussion also highlighted some of the other reasons why people were frustrated with traditional finance and sought alternatives: PayPal, for example, is not supported in every country, under 18s are restricted from many financial services and others talked of their problems using existing services after having had previous financial difficulty. All these experiences led to the adoption of Bitcoin (primarily) as a tool open to all. Bitcoin is free for anyone to use, regardless of geography, age, financial history, or any other reason that can exclude someone from traditional finance. Bitcoin does of course, though, require computing equipment, connectivity and a certain level of education to use it, but these points also generally apply to traditional finance as well.

Another point illustrated in the posts that relates to finality is decentralisation. Whilst this was not a point that the authors spoke specifically about to any large degree, it is one of the properties that enables the finality of payment. Using PayPal, one author described how the company restricted their account, affecting them financially. Whilst this may well have been for legitimate reasons on the part of PayPal, this example illustrates the difficulties that can emerge when there is a third party involved in transactions as a payment processor. Bitcoin, though, removes the intermediary through its decentralisation thereby removing that third-party risk. In this way, it enables the peer-to-peer nature envisaged by the Bitcoin whitepaper. As the author remarked, the availability of Bitcoin lessened the impact of PayPal intervening as there was an alternative payment mechanism that could still be used. In this way, we can think of an asymmetry of power when using a mediated service; and this is not always beneficial to all the parties concerned. This point is reflected in several posts. Whilst in theory chargebacks are useful for consumer protection, there are invariably those who will try and abuse this asymmetry for their advantage. As a result, many sellers commented on the proliferation of scammers on PayPal who would buy goods and then open up disputes. With an irreversible payment mechanism, these risks are avoided.

One limitation of CrimeBB is the periods covered. The underground forum posts are from as early as 2010, whilst the dark net forums date from 2014 onwards (one of the foreign language forums, however, goes back to 2012). It is not possible, therefore, to see dark net posts from the very early days of Bitcoin or indeed of the Silk Road era. However, there is a crossover from the underground forums where these matters are discussed. Much is also known of the dark net and the Silk Road from these times from existing research, where Bitcoin was long established as a payment mechanism for trade. And it was and is the finality of transactions that has been at the heart of Bitcoin’s acceptance for illicit activity as it overcomes one of the difficulties of the internet – that of trust. As one author puts it, there is little trust on the internet. Another urges others to trust in cryptography over anything a human might say. Finality, with an immutable public ledger, enabled trust to increase, above that of the alternatives that existed at the time. Authors note that they could verify funds had been sent and be secure knowing they would not suffer chargebacks or other problems - a situation enhanced further with escrow and eventually multi-signature transactions.

The volume of posts, and their strength and tone, caused finality to emerge as the most useful property of cryptocurrencies. This finding aligns with Anderson’s paper pre-dating Bitcoin that ‘reveals that revocability is more important’ than traceability for online fraudsters using ‘nonbank payment services’ (Anderson, 2007). Speed was not a top concern in our sample when, in the case of purchasing drugs on the dark net, for example, packages were to arrive by post. Reduced cost of transactions was an attractive feature, but lower down the order than the benefits of finality. The other structural characteristics of Bitcoin contribute to achieving this benefit but were not the overt reason why it was adopted – finality solved real problems of existing alternatives. Of course, this problem was an issue whether the activity was legitimate or illicit. We now return to illicit activity and the unresolved questions from earlier in the chapter. If Bitcoin or indeed privacy coins do not solve anonymity, then how can they be used for illicit activity, particularly on the dark net? Countless posts (amongst those that care) take place on the underground and dark net forums discussing how to best transact. This will now be examined.

5.3.3 The Payment Mechanism

The payment mechanism used to conduct illicit activity is just one of a suite of considerations that conscientious users must scrutinise if they hope to achieve a sufficient level of operational security. To aid the discussion of this, an Operational Security Taxonomy for Illicit Internet Activity is proposed, as shown in Figure 5. This diagram is not based on any other models and was created as a way of visualising the range of issues that an illicit user is faced with. As the reader can see, there is a great deal to consider if you seek to conduct illicit activity as securely as possible. The seven areas of security are not exhaustive but capture the main elements that contribute to relative anonymity. The dashed boxes are also not exhaustive but illustrate some of the considerations in each area. At the top, there is a cross-cutting theme of ‘procedures’, which applies to all seven security areas. For example, a procedure may be implemented to erase all hard disks weekly, or in relation to shipping to ensure that a home address is free of illicit material prior to an expected delivery. CC is short for cryptocurrency.

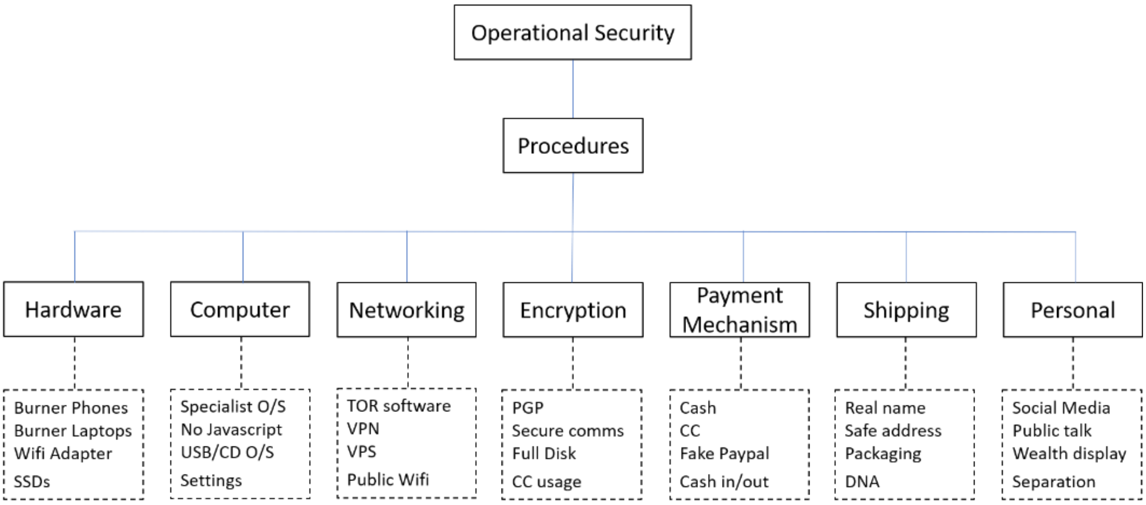


Figure 5: Operational Security Taxonomy for Illicit Internet Activity

Our focus here is on the payment mechanism and to initiate discussion the following claim is made – banning cryptocurrencies would not materially reduce illicit internet activity. In many areas of the taxonomy, one can think of there being ‘tools for the job’. The history seen through CrimeBB shows that when one payment mechanism falls, another is quickly found. When Liberty Reserve ceased, other options were soon adopted. As difficulties with traditional finance grew, demand for Bitcoin increased. And now, as Bitcoin is scrutinised, many want to move to Monero. There are always alternative payment mechanisms. Table 6 highlights just some of those used and discussed in CrimeBB:

Table 6: Selection of Payment Mechanisms in CrimeBB

Payment Type	**Example Mechanisms**
Cryptocurrencies	Bitcoin/Litecoin/Monero/Dash/Zcash
Payment Processors	PayPal, Western Union, MoneyGram, Skrill (Moneybookers), Payza, Webmoney, Moneypak,
Bearer Assets	Cash, Gift Cards
Fintech	Perfectmoney, Cashapp, Venmo, Greendot, Dwolla, Perfectmoney, UKash, Virwox, Paysafecard
Gaming Currency	Runescape Gold, Second Life Linden Dollars
Traditional Finance	Bank Account, Credit/Debit Cards, Prepaid Debit Cards, Polish Bank Cards

The table shows that a ban on cryptocurrencies would only restrict one potential mechanism, leaving several other options available. If we consider just the bearer type, we see that it is an ultimate recourse should every other type become unavailable. Bearer assets are owned by the holder and so offer a finality of transaction, like cryptocurrencies. Cash is the most common example and finality explains why ‘cash is still king’ for criminal transactions, as explored in the previous chapter. Indeed, as several authors point out, cash is the main mechanism for purchasing drugs more widely. Another author describes successfully sending cash through the mail system – established techniques such as this would be extremely difficult to counter and exist as proven payment mechanisms should other methods disappear. Gift cards are another readily available bearer mechanism discussed and used in a multitude of posts. As a look forward to the interviews of law enforcement officers, it should be briefly noted that there remain differences between the use of cash and cryptocurrencies – namely, that in-person illicit cash transactions offer recourse to violence in a way that Bitcoin and others do not. And this is not to the advantage of, particularly, larger-scale illicit trades.

Several authors question the logic of a ban on cryptocurrencies. They view cash as being a greater enabler of criminal activity than cryptocurrencies and believe there is hypocrisy in targeting cryptocurrencies over cash or the traditional financial system. The irony then is that users of payment mechanisms for illicit activity say that government-provided cash is best, and government officials say that cryptocurrencies are best. Authors acknowledge that cryptocurrencies are used in crime but ask if that is different from any other payment mechanism. It is worth noting at this point the central role that cash also plays in illicit internet activity. Not only is it used as a payment mechanism, but it also acts as a fundamental tool for achieving anonymity. One of the most discussed topics, particularly on the dark net forums, is the subject of 'cashing in or out' of cryptocurrencies. As cryptocurrencies are still a relatively small market and not accepted widely in the world, the authors describe the need to transfer any cryptocurrencies into and out of cash for use in the real world. In this way, cash can often be thought of as the anonymity wrapper applied around a pseudonymous Bitcoin transaction. This again explains why anonymity is not the main property needed from cryptocurrencies as an illicit payment mechanism - as long as anonymity can be achieved elsewhere as part of the process. And it is cash, once more, that is the key tool.

If physical cash is a great enabler of real-world crime, why should there be opposition to a cash-like tool on the internet? There is hypocrisy here that the authors speak of. If both forms enable crime, why do cryptocurrencies receive greater criticism for this? One possible explanation is that physical cash is state-provided, and the other is not. Considering that physical cash is an enabler of more crime than cryptocurrencies, from a logical perspective it would make sense to think of cash as the greater threat. At the very least, policy should find them both a threat, rather than just one. This argument will be returned to in the final chapters of the thesis.

The increasing difficulties of cashing in/out, arguably brought on by improving regulation of legitimate cryptocurrency services, have deterred some illicit activity. One author describes being put off from selling on the dark net due to this difficulty of cashing out. There is a further interesting paradox to consider about the efficacy of bans. Currently, most illicit transactions have a connection to legitimate services. This brings opportunities for enforcement. However, a ban would likely push users to illicit mechanisms and reduce some of these opportunities. Cash can be sent in the mail or deposited into a bank account. Or legitimate mechanisms would be used fraudulently, such as registering for services using fake identification. These methods are harder to stop and arguably leave less opportunity for enforcement. In this way, a ban would reduce opportunity for legitimate users and merely push illicit activity towards other established mechanisms that are harder to control. Dark net market activity would be temporarily affected but users would likely soon find alternatives, as they have done after Liberty Reserve ceased or the repeated closure of markets themselves. Legitimate services drain liquidity away from illicit methods, making them rarer and harder to use.

As a final point in this section, policy makers must consider whether they could even achieve a ban. The nature of cryptocurrencies means that they cannot be shut down as easily as a centralised service like Liberty Reserve. And as long as a decentralised cryptocurrency system persists, there is little that can be done about individuals meeting in the real world to trade cryptocurrencies for cash, for example. As one author puts it, Bitcoin could still be used for illicit activity if it was banned, and only ordinary users would be affected. Another writes that Bitcoin is simple for legitimate activity but hard for illicit. Regulated exchanges combined with a transparent record of transactions make illicit payments harder. On this point, an author writes that analysis of the Bitcoin blockchain has been central to all dark net market prosecution and that, if you use Bitcoin, you must ensure that every aspect of your operational security is infallible. In another post, the author decries the hype around cryptocurrencies or that they are revolutionary to simply say that they are just a useful tool to transact with, like other monies. Cryptocurrencies are, then, useful for illicit activity as they are a useful payment mechanism. But it is too simple to say they are ‘great’ for illicit activity - there is far more to consider in terms of their usage.

They are a tool among many, as the taxonomy shows, but as an individual mechanism, they come with significant disadvantages to the illicit actor.

5.3.4 Dark Nets are Hard

In another study that analysed CrimeBB, the researchers concluded that ‘cybercrime is (often) boring’ (Collier et al., 2020). Analysis of the CrimeBB posts here adds to this by showing that cybercrime, particularly on the dark net, is also hard. The dark net is fraught with risk – scammers abound, and law enforcement action has been successful to an extent. The taxonomy shows that there is a significant educational and technical barrier to illicitly transact relatively securely on the internet. Even for a careless user, the minimum required to use the dark net is a computer with Tor set up, a delivery address and a working knowledge and possession of cryptocurrencies. The argument here, therefore, is that dark net markets are a niche, and they are unlikely to grow significantly in comparison to traditional counterparts. The dark net may reduce the risk of acquiring narcotics, for example, but it is arguably much easier, as some of the authors claim, to get cash and buy drugs in the real world. Dark net markets only cater for a small volume of overall crime – the threat should not be overexaggerated.

There are countless guides and posts on the underground and dark net forums discussing how to conduct illicit transactions. Even just the payment mechanism part of the taxonomy requires substantial knowledge. Users must also keep up with changing methodologies as services come and go, regulation tightens, and behaviours evolve. One author describes studying for many months before being able to start selling on a market. Another author tells of mental exhaustion from researching how to buy. The author thought it would be simple, perhaps as easy as ‘pushing a button’ - the reality was the opposite. There is no better example of this than the Dark Net Market’s Buyer Bible (Anon, 2018). This is a guide written for users wanting to purchase on dark net markets – it is 133 pages long. It is not necessary to discuss all the advice of the Bible but here follows a few items that highlight some of the complexity involved: use a non-windows, Linux-based machine for a specialist operating system such as Tails or Whonix on a portable media

(USB/CD), acquire a VPN service anonymously, learn to use PGP for encryption, use pre-installed IP tables as needed, disable JavaScript in the browser, get onion addresses from a reputable website, use a self-destructing messaging service, acquire BTC using cash from an ATM using a disguise and burner phone, convert Bitcoin to Monero using a non-exchange wallet… Advice for sellers is even more exhausting. The extent of the advice shows that cryptocurrencies do not enable the purchase of illicit materials globally with a simple click of a button – the taxonomy illustrates that it is far more complicated than that.

The complexity across the taxonomy also explains why privacy coins are not a panacea for anonymity. The user must acquire Monero, for example, most probably with Bitcoin. Websites exist to highlight services such as VPN providers and decentralised exchanges that aid in anonymity (Kycnot.me, 2020). For example, a popular service on CrimeBB is xmr.to, which will send Bitcoin to a recipient in exchange for Monero. Or morphtoken.com which exchanges cryptocurrencies e.g., Monero for Bitcoin. However, even with these tools a user still needs to cash in/out, plus do every other part of the taxonomy securely. It is a difficult task.

The environment of the dark net must also be considered. One user from the first days of the dark net commented on how much more difficult it had become. Whilst there had been early disdain for law enforcement capability, authors now acknowledge much improvement since the Silk Road market. There is evidence of some fear of law enforcement activity. However, an author notes in 2014 that arrest is more likely in the real world; a point confirmed in Chapter 2 (Aldridge et al., 2018). As such, the view remains that buyers of small amounts have little to worry about. The extent of deterrence on the dark net is therefore limited. Operation has become more difficult, but buyers do not think there is much chance of law enforcement interest in their activities. The role that Bitcoin analysis has played in prosecution is known but sellers continue, believing that they can operate if they take sufficient precautions. Recent views from 2019, though, show that dark net marketplaces are hard to trust and often disappear after short periods. This all leads to a sense of containment if nothing else, as authors hope for improved days based on innovation using new technologies. The desire for a truly decentralised marketplace using Monero is there to see. There is a paradox here, that every law enforcement success leads to a Darwinian hardening of the system, which one day could leave little enforcement opportunity.

To finish this section, consider the words from three final posts. One author reminds readers that even if you do everything right (according to the taxonomy), using the dark net still requires trust and ‘hope’. Hope that someone else has not done something to compromise your security, such as a seller who is caught and has not deleted customer addresses. Another reminds us that people make errors and security cannot be applied retrospectively. You must get everything right from the beginning, which is difficult and can lead to silly mistakes getting you caught (as in the case of Ross Ulbricht). This leads us to the final user comment, that the dark net appears to be easy and safe to use – but it isn’t. It is a risky domain, and it requires a lot of research and capability to use it relatively securely. And for these reasons, it is not for everyone.

5.4 Conclusion

This chapter addresses a gap in the literature by conducting the first user study of cryptocurrencies for illicit activity. It also adds to the research on the dark net by focussing on payment mechanisms, rather than well-researched aspects such as harm or drug availability. In this chapter conclusion, some limitations of the research are discussed, and four key policy implications are outlined, which are based on the main findings of this study. These findings are important to the thesis, and so they will be returned to in more detail in Chapter 8.

CrimeBB is an excellent resource. The CCC deserves thanks, as the dataset is a richer and deeper source than anything any one individual would likely be able to produce. Its professional curation also helps avoid some of the ethical pitfalls that this site of enquiry can engender. Having said this, the dataset does cover limited periods for each forum, meaning there is a wide range in the amount of material available, and this limitation is accepted.

Particular care was taken in this study in choosing search terms, and using a content analysis method enabled themes to emerge naturally. As a qualitative study, any claims here are not ‘proven’ but the findings from the material justify them based on the analysis that emerged. Verbatim use of quotations from posts would have been preferred to clearly show the discussions that led to the results, but the ethical guidance discussed in Chapter 3 advised against this. CrimeBB is available to other researchers should they wish to know more or to corroborate the results. However, I think that this approach to presenting research material from online sources is overly cautious, and it is not followed consistently by the research community. I would, therefore, implore researchers in this area to review this issue, as research of this type would be greatly improved if verbatim quotations could be used. This point is discussed in more detail in Chapter 8 in terms of any future research of this type that others may wish to do.

The four main results sections of this chapter reveal several significant findings about the use of cryptocurrencies for illicit purposes. The anonymity of cryptocurrencies is not their major advantage, the finality of transactions is. This contrasts the view as expressed in the securitising narrative. The results also show that the payment mechanism is only one of a whole suite of necessary considerations should a user wish to conduct illicit internet activity relatively securely. And finally, cryptocurrencies do not make the purchase of drugs as simple as the ‘push of a button’. These findings translate to four main implications for policy:

1. Anonymity: Users adopted cryptocurrencies because they were a useful tool that solved real-world problems. Finality was the property most sought. Policy makers should recognise the issues people had that led to this adoption. Traditional systems must be inclusive and fair to all; they should not drive users to alternatives.

2. Banning Cryptocurrencies: This is unlikely to do more than disrupt illicit internet activity. If anything, this reduces the opportunity for legitimate use, pushes liquidity to illicit methods and reduces law enforcement opportunities by reducing contact with regulated systems. Many other payment mechanisms could be used for illicit activity; some, such as cash, are even harder to monitor than

cryptocurrencies. A ban would also likely be ineffective due to the decentralised nature of cryptocurrency systems.

3. Deterrence: Law enforcement action has contained dark net activity and created a degree of deterrence, but little at the small buyer level. For these buyers, research shows that the dark net may reduce harm. Policy makers must also consider the evolutionary nature of markets and the impact that future technology could have on law enforcement impact.

4. Niche Markets: Illicit internet activity is hard to achieve relatively securely, as the taxonomy shows. Dark net markets are therefore a niche and are unlikely to explode in size. The creators of Silk Road and AlphaBay markets were not from traditional crime groups. Policy makers should take into account the threat that the dark net measurably poses and react accordingly. There is a danger that headlines make it seem more of a threat than it is. It is unlikely that dark net markets will capture significant shares of real-world counterparts.

If the previous chapter showed that cryptocurrencies are not used in an overwhelming amount of crime, then this chapter helps explain why this is the case. Analysis of CrimeBB has shown that cryptocurrencies are not as useful for crime as the headlines from the memorable alliance suggest. They do not solve problems of anonymity, and so illicit transactions do not become trivial. Now that we have seen what users of cryptocurrencies think about them, there is a better understanding of their most useful properties, both for legitimate and illicit activity. In the next chapter, examination of the security threat that cryptocurrencies pose is taken further through the interview of law enforcement officers. As a key entity in the evaluation of the threat of cryptocurrencies, their view is an important one to explore. Especially considering the disconnect that was identified in Chapter 4 between the memorable alliance and the DEA, one of the US law enforcement agencies.

6 From the Perspective of Law Enforcement

In Chapter 4, evidence was presented of the securitising narrative of the memorable alliance with regard to the illicit use of cryptocurrencies. Yet, the research analysed on this topic showed that cryptocurrencies are not used in an overwhelming volume of crime and that the financial tools provided by the memorable alliance (cash and the traditional financial system) remain preferable for illicit activity. Importantly, it was also shown that law enforcement reporting reflected this contradiction; even to the extent that a US DEA agent was quoted as saying that they would like criminals to continue using cryptocurrencies as the publicly accessible blockchain offers the opportunity for enforcement. As, perhaps, another more recent example of this apparent contradiction, Binance, one of the leading cryptocurrency exchanges, was commended by a Regional Organised Crime Unit (ROCU – see Section 3.2.3 for more description) for its contribution to law enforcement. This does not speak to what law enforcement officers think about cryptocurrencies directly, but again raises questions about the threat that cryptocurrencies represent:

> @Binance received a letter of commendation from UK South East Regional Organised Crime Unit for our efforts in helping them to fight bad players in the cyber space. (Tweet by the Binance CEO, Zhao, 2021)

Chapter 5 added to this backdrop by showing that cryptocurrencies are not a panacea for illicit activity and the core problem of remaining anonymous. Additionally, cryptocurrencies do not enable criminal activity at the click of a button – illicit internet activity is fraught with difficulty and takes great care to conduct relatively securely.

In this chapter, the aim is to explore the view of law enforcement officers toward cryptocurrencies more deeply in order to add to what has already been learnt by studying users on underground and dark net forums. It is worth noting that in the last 200 years of theoretical discussion and debate about money, as discussed in Chapter 2, criminal use has never featured as a prominent issue. It may be a practical concern, but the debates and controversies revolve around the form of money (commodity versus credit theories), the means of production and the philosophy or politics behind money. Yet, in the securitising speech acts shown, illicit use is a central claim and grounds for labelling cryptocurrencies as a security threat. This is an interesting dislocation that deserves further enquiry.

It is important, therefore, to examine the extent to which law enforcement officers view cryptocurrencies as a security threat. Will this support the claims of the memorable alliance, or will the contradiction strengthen? The answer to this will help shape the discussion and conclusions of the thesis. If law enforcement officers do not view cryptocurrencies as a security threat, then one must ask why the memorable alliance do? Is there a misunderstanding or is the security threat used as a means of creating a securitising narrative when the referent object is something unrelated?

Despite the prominence that criminality plays in the debates about cryptocurrencies, this area has seen little academic focus and research on the views of law enforcement was identified as a gap in the literature in Chapter 2. Along with Chapter 5, this chapter aims to achieve a better understanding of the use of cryptocurrencies in crime and the extent to which they are a threat. In Chapter 3, a constructivist approach to research was chosen based on the rationale that it is for those that use cryptocurrencies for illicit activity to articulate why they do so and, similarly here, it is for those charged with countering the threat of illicit activity to articulate the extent to which cryptocurrencies are a security threat in relation to criminality and the investigations that they are involved in on behalf of the state. This chapter, therefore, relates to research sub-question three:

> To what extent do law enforcement opinions and experiences of cryptocurrencies support or contrast claims for their securitisation?

6.1 Methodology

To research this gap, a series of in-depth, semi-structured interviews were conducted with UK law enforcement officers with many years of experience in criminal investigation. Chapter 3 described the approach to this strand of research and also described the organisations they work for, so this is not repeated here. One point that does need discussion, though, is the shift in focus here to UK officers, rather than the US. As per the methodology in Chapter 3, my position as an ex-officer was probably key in getting access to UK law enforcement. This also required Deputy Director approval for the NCA officers. It is very unlikely that I would have had the same level of access to US agencies. More importantly, though, I do not think the findings from US officials would have been materially different. Whilst the focus of the narrative was on the US due to the role of the US dollar, the effect that cryptocurrencies have on investigations is likely to be similar to all officers, regardless of country. This is an assumption, but the questioning in this chapter explores the impact of cryptocurrencies at a technical level, so the country-specific context is less significant. The investigations, legal systems, roles and responsibilities of UK and US law enforcement officers are mainly similar.

In total, eight semi-structured interviews were conducted with four participants between May and September 2020. The collection period was therefore after the outbreak of the COVID-19 pandemic. This had two impacts. First, the interviews were conducted remotely over Zoom and Skype, as in-person interviews were no longer possible. Functionally this worked well, although I did find that several interviews were cancelled last minute and then had to be re-scheduled for a later date. Second, the virus placed a greater load on law enforcement officers, who found that there was an increase in cybercrime reporting. This again made the scheduling of interviews difficult and explains some of the cancellations.

The same semi-structured interview plan was used for all the officers. Interviews varied in length with most of the officers requiring multiple interviews to cover the questioning. More than eight hours of video was captured, with the longest single interview being almost one and a half hours long. Cryptocurrency investigation is a niche area in law enforcement, so these interviews were in-depth with a small number of expert participants. There are no publicly available breakdowns of department numbers but to indicate the size of the NCA's National Cyber Crime Unit (NCCU) we can compare the NCA headcount to the MET police, the UK's largest police force. The MET has more than 40,000 staff, of which 33,000 are police officers (Metropolitan Police, 2021). The NCA headcount is just over 6,000 (National Crime Agency, 2021) but of that, only about 1,250 are warranted investigators i.e. with powers of arrest like police officers (Wikipedia, 2021). From my experience in the NCA cyber department in 2011, there were only a handful of cyber investigators. This has likely grown since then, but the numbers are still relatively small.

Participants are not identified by name or specifically by role in order to afford some anonymity. This is only taken as a general precaution in terms of their roles, rather than as a measure to counter a particular threat. It is also worth noting, that some of the officers obtained senior-level approval to take part in the research. Their views, however, are personal and do not reflect any official positions of the organisations that they work for. In this regard, I found that all the officers were very open in their responses and did not feel that they were under any pressure to present anything other than their genuinely held beliefs.

Verbatim quotations are used in this chapter, and they are attributed to the four participants, officer numbers 1-4. Hesitations and disfluencies have been removed in order to aid comprehension. This does not affect the content of the quotations and was done merely to assist the reader. Some of the quotations have more meaning given the role of the participant so a summary of each officer’s role and background follows. Officer 1 worked in a police economic crime unit and became involved in cryptocurrency investigation as early as 2013 and has worked in that area ever since. The officer worked at the time of the interviews in a ROCU as a cybercrime expert who specialises in cryptocurrencies. Officer 2 is familiar with cryptocurrencies but has focussed more on traditional drugs, corruption and money laundering investigations, providing a useful perspective on traditional financing. Officer 3 is also a deep expert in cryptocurrency investigation having been involved in some of the earliest police work in this area. The officer has had responsibility for training other investigators about the use of cryptocurrencies and has experience at local, national, and international levels. Finally, Officer 4 is a manager in the NCA’s NCCU and has experience in a range of cybercrime investigations.

All the officers have significant experience in criminal investigation, with three of them directly involved in cryptocurrencies. These officers were the most suitable participants for this research as they have many years of experience in hands-on cryptocurrency investigation. For this reason, these interviews were in-depth. I did have contact with a senior officer in the NCCU, but they declined to be interviewed without giving a reason. It is, however, unlikely that a senior officer would have had the depth of knowledge and practical experience that these participants have. As we have seen, unsubstantiated narratives are often presented about cryptocurrencies. Here, we hear from some of the most intimately involved officers in cryptocurrency investigation in UK law enforcement.

The interviews were semi-structured, fully transcribed, and then coded in NVIVO 12. Structural and topic coding were used. The interviews were structured around three main categories for questioning, which were based on the thesis research questions:

1. The first main category of interview questions explored the officers' thoughts and attitudes towards cryptocurrencies generally. Questions covered their opinions and experiences of them, the properties of cryptocurrencies and their advantages and disadvantages for criminal activity.

2. The second structural area was the dark net, as it is a prominent area of concern for the use of cryptocurrencies. The officers were questioned about the use of cryptocurrencies on the dark net, the overall threat that the dark net poses, and their views on policy and deterrence in this area.

3. The third main category of questions related specifically to securitisation theory. The theory was explained to each of the officers and we discussed the security threat narrative about cryptocurrencies; '**who** securitizes, on **what** issues (threats), for **whom** (referent objects), **why**, with **what results**, and, not least, under **what conditions** (i.e., what explains when securitization is successful)' (Buzan et al., 1998: 32).

These three structural areas were then reflected in three main categories for coding. Descriptive codes were then added to the main categories during the first cycle of coding. Following completion and analysis of the material, however, several themes emerged, and these are used in part to structure the three main sections of this chapter that follow.

Section 6.2 explores what the officers thought about the usefulness of cryptocurrencies and the extent to which they are used for illicit activity. This section is intended as a parallel to similar discussions in Chapter 5, and both serve to provide a greater understanding of the security threat posed by cryptocurrencies as expressed in the security-led narratives.

With the officers’ general views of cryptocurrencies explored, Section 6.3 is based upon a theme that emerged of trust on the dark net. It is noted that trust itself is developing as a wider theme in the thesis. Here, though, trust relates to payment mechanisms, as we saw in the last chapter, but the responses from the officers also revealed an interesting insight into the nature of trust in illicit internet activity that is important in terms of the extent to which cryptocurrencies are a security threat. This is considered in the specific context of the dark net, as a key site of concern regarding the use of cryptocurrencies for illicit activity.

And finally, the third main section, 6.4, discusses another theme that emerged, regarding an ambivalence toward the technology used in crime. Findings related to this theme are then used as support in consideration of the specific responses that the officers had to securitisation theory as it relates to cryptocurrencies. This enables an assessment of whether law enforcement officers are labelling cryptocurrencies as a security threat and, therefore, whether their views and experience provide the justification for securitising claims.

6.2 Cryptocurrencies as an Illicit Tool

A great deal of the discussion about the criminal use of cryptocurrencies concerns how useful they are as a criminal tool. Where Chapter 5 explored this angle from the perspective of users on underground and dark net forums, this chapter examines the counterparty view of law enforcement officers. This section begins by examining the usefulness of cryptocurrencies for illicit activity as seen by the officers. They were also questioned about the extent that cryptocurrencies are being used. The section finishes with a consideration of privacy coins as a special case that has been discussed throughout the thesis.

This section, therefore, gives us an understanding of the attitudes and opinions of the officers towards cryptocurrencies. It is also complementary to the research of Chapter 5 and contributes to our overall understanding of the usefulness of cryptocurrencies as an illicit tool, whether they are preferred to existing methods and, again, whether they enable the purchase of illicit goods with the click of a button. This section reflects the first category of questions from the interview, which were designed to be open in order to allow the officers to freely talk about cryptocurrencies and their experiences with them.

6.2.1 Usefulness

One question put to all participants was ‘What is a more useful tool for criminality, cash or cryptocurrency?’ Interestingly, the three officers who work most closely with cryptocurrencies said cryptocurrencies, whereas Officer 2, who does not work in a cyber department, chose cash. This may be explained by another general theme that emerged from the coding about how cyber policing is organised. An interesting element of this theme is the extent to which cyber officers work in silos and, combined with limited research data about threats, can become blinkered to wider issues. If you work in a niche area every day, there is perhaps a natural tendency to think that the area is larger than it necessarily is:

> I've just been in a group of a few guys who see criminals using (cryptocurrencies)… so it's hard to ever stop and think how much of a threat is this in wider circles and how is it perceived wider. So yes, it's not something I've ever really stopped to consider much. (*Officer 1)*

This quotation raises an important point that will be explored later in the chapter about how things are constructed as a threat and more specifically, about what a threat means to different actors and how something qualifies as a threat. Officer 1 works in a small group and acknowledges not knowing how big a threat cryptocurrencies may be in comparison to other methods. And if teams work in isolation, how can this translate to a measured assessment of threats?

Regarding the question of how useful cryptocurrencies are for illicit activity, the officers have many interesting things to say. First, how useful they are depends on the user:

> It depends how knowledgeable the criminal is... your should we say non-technical so a low-level drug dealer for example, who is using cryptocurrency to store and transfer value he or she is arrested and devices seized then it would be a lot easier to... attribute and follow lines of inquiry from someone who really doesn't understand the principles of the blockchain and transactions and the pseudonymous nature of it. Contrast that with your more sophisticated actors who are involved in cyber, for example, who understand the principles of cryptocurrencies and the sort of limitations of privacy in the Bitcoin blockchain and associated infrastructure... as a result of that you see more sophisticated methods to obfuscate transactional flows. (*Officer 3)*

This quotation supports the findings in Chapter 5, where there was a mistaken perception about the anonymising properties of Bitcoin in particular. Whilst some users on the dark net are incredibly savvy, many others are ignorant of the technicalities of cryptocurrencies. This also echoes another point made in Chapter 5 that using cryptocurrencies and transacting on the dark net, for example, is not as simple as is often reported. Officer 1 also notes that the landscape has changed with the push for more stringent regulation. In the early years of cryptocurrencies, the industry was not well overseen. Now, exchanges are largely covered by existing anti-money laundering and counter-terrorist financing regulations. As a result, know-your-customer (KYC) due diligence has improved. Like when opening a bank account, a user has to provide identity documents to open an exchange account. This has made it harder for criminals to stay anonymous and to cash out of cryptocurrencies and has afforded more opportunities to law enforcement through the development of blockchain analytic companies, which assist the regulated sector and law enforcement in their endeavours. At the same time though, cryptocurrencies have become ever easier to use. But Officers 1 and 4 support Officer 3 in the statement that cryptocurrencies offer them lots of opportunities, but their efforts are hampered if technical criminals use cryptocurrencies with a high level of operational security.

Regarding anonymity, the situation is again a reflection of the capabilities of the user. But, as Officer 1 points out, ‘in the world of cybercrime it’s difficult to ever have anything that’s not hackable and it’s difficult to ever have anything that’s truly private’. Similarly, Officer 2 states that ‘people are getting increasingly paranoid about how traceable Bitcoin is because I don’t think that sense of anonymity is the same as it was maybe seven, eight years ago’. Furthermore, Officer 2 believes that many criminals do not trust cryptocurrencies and prefer to use traditional items that do not have a permanent record associated with them such as cash, high-value items and bonds:

> What is better for criminals? I think it depends on the education of the criminal themselves as to what they're going to choose to use and I think most criminals use cash because it's easy to move, transfer and the ways of doing so are well trodden and well understood and actually fairly risk-free when you compare that to the risk of trying to deal in large amounts of money or something that you're not 100% sure about which is very volatile. Whereas cash, such as sterling and euro and dollar isn't as volatile on the markets as Bitcoin has proven to be in the last couple of years and it's accepted in more places to buy more things. (*Officer 2)*

This quotation supports the conclusion in Chapter 4 that cash is still king for criminal activity. And part of the reason for this is that no matter how good user operational security is, there is always the fundamental problem of how to cash out of cryptocurrencies and buy things.

> If you ever want to cash out of the cryptocurrency… then that's going to leave you with the trail but it's the same as doing a sophisticated fraud… it's always going to be the cash out, moving out of that dirty association that is the difficult bit and it's the attempt to break that chain which is difficult… Even when you do cash out, you're cashing out anything other than cash, it is

> regulated or if you're cashing out through anything other than like a hawala network or something like that or a deliberately illegal network if you're cashing out into the regulated sector… a level of KYC will apply so I think that makes… it less attractive but you have to remember that criminals have manipulated and have successfully operated within the regulated sector bypassing all of our KYC for a considerable amount of time, so you know that doesn't necessarily mean it's less attractive to them for that reason. (*Officer 2)*

And this is why cash remains a crucial element of illicit activity because it does not have the transactional record that cryptocurrencies have. It is also more widely accepted and usable for spending. And if the goal of most illicit activity is to end up with cash or other forms of money in the traditional system then why use cryptocurrencies? Again, this supports the finding in Chapter 5 about the advantages that come from keeping cryptocurrencies as a legal, regulated payment mechanism. That enables law enforcement investigation and makes cryptocurrencies harder to use for illicit purposes.

Given the usefulness of cash for illicit activity, it is hard to find ways in which cryptocurrencies are overwhelmingly superior to cash to the extent that they warrant pressing treatment and securitisation. In what ways, then, are cryptocurrencies useful for criminal activity? For Officer 2, they offer a quick and cheap way of making small purchases, such as on a dark net market, with a level of anonymity that would otherwise take a lot of skill to achieve in the traditional financial system. Chapter 5 showed that the deterrent effect is very limited on the dark net, and so even Bitcoin offers a workable level of security for a small user if they are confident that they will not be a target of law enforcement investigation:

> You could literally just use your credit card to buy cryptocurrency and then have a level of anonymity and that you wouldn't have otherwise and because of this I think it makes it very useful for… small scale drug purchases on the dark net or various other purchases of other illicit materials at that kind of a level. But once you start consolidating that money as a serious criminal… it doesn't actually particularly help you because you need to move that 200,000 sterling or 300,000 euros worth of cryptocurrency into something that you can

> use with that and then you have to bring it into the regulated sector and people are going to start asking questions and then you fall into the same trap that you have always. (*Officer 2)*

Officers 1, 3 and 4, who are more intimately involved with cryptocurrencies, identify transporting value as a key benefit of cryptocurrencies. Bulk transportation of cash has traditionally been a problem for criminals and offers the opportunity for interdiction, where concealment is an issue. Cryptocurrencies present an opportunity to move near-limitless amounts of money through the physical movement of a wallet containing funds. A wallet can be transported on a piece of paper, or a USB stick or it can even be memorised.

For these officers, the key threat area where cryptocurrencies are useful is ransomware. As a cyber-dependent crime, the role of cryptocurrencies is arguably more important than in other cyber-enabled crime types such as the drug trade. In cyber-enabled crimes, there is a real-world analogue to any cyber activity. One can buy drugs for cash, as opposed to on a dark net market for example. This duality, therefore, lessens the impact that any new advent in cyberspace affords as there is always a non-cyber way of doing the crime. With cyber-dependent crimes though, such as ransomware, the role of cryptocurrencies becomes more prevalent as there are limited alternative payment methods. Could a ransomware operator demand payment through other payment media? It is arguably more difficult, and this issue was considered in Chapter 5.

Ransomware was also discussed as a specific threat in Section 4.3.3, and it was noted that two of the most prominent attacks of recent times were both, in fact, nation-state attacks and that in one case, the malware analysis showed that payments could not even be made. That is, the ransomware attacks were more political than financial. We also saw that the amounts raised from ransomware are very small in the scheme of crime. As noted previously, there is a much wider impact from ransomware than just the ransom, but these details remain important in assessing the extent to which cryptocurrencies are part of the crime or the extent to which this crime type is a threat. Furthermore, ransomware is a preventable and recoverable crime type; if companies employ good cyber security practices and backup data then the impact and the sustainability of ransomware as a crime type are greatly reduced.

Officer 4 also notes that cryptocurrencies are often used for the payment of server infrastructure used for illicit activity. As a payment mechanism, there is nothing here that requires the exclusive use of cryptocurrencies. That is, if cryptocurrencies were not available then other payment means could be employed, be it other bearer assets, such as cash, or the use of compromised accounts in traditional finance. And if the existence of other payment mechanisms means that many crimes could continue without cryptocurrencies, then again, how can cryptocurrencies be considered an urgent threat requiring special measures to deal with them? That is, ordinary measures and ordinary politics should be sufficient.

6.2.2 Extent of Use

In Chapter 4, we saw that blockchain analysis showed that the percentage of illicit activity in cryptocurrencies is small. Officer 1 notes this and argues that the amount of crime is still increasing but it is being eclipsed by a greater increase in legitimate usage. The officer acknowledges, though, that our perception of the extent that cryptocurrencies are used in crime may be distorted by the narrative and coverage that the topic receives:

> You'll get one significant cryptocurrency seizure and you've got the whole cybercrime and economic crime network in the UK talking about it in addition to CPD events suddenly springing up and policing conferences discussing it as best practice and that'll just be one case. You'll get a fifty grand cash seizure from a traffic officer tonight… and no one will know about it so I wonder if maybe because of its rarity and the fact it's new we maybe talk up the number or the amount of opportunities for seizing crypto and I imagine the reality will probably be that criminals stashing bags of cash still continues pretty much in the same vein but maybe you know one in twenty of them also dabbled in sticking it on a hardware wallet as Bitcoin as well for example. (*Officer 1)*

Interestingly, and despite three of the officers viewing cryptocurrencies as a better tool for criminality, the situation is reversed when asked, ‘What is more of a security threat, cash or crypto?’ Here, three of the four officers thought that cash was more of a security threat, as cryptocurrencies are only used in a niche of crime and traditional methods remain the modus operandi:

> It's cash definitely. You look at anything like terrorism financing or I've talked about drugs loads during the interview, I still think cash is king. You've got a niche of criminals mostly aligned to cyber criminality that prefer to use crypto because by its nature its online… its borderless. Outside of that nearly all of the crimes… I'd say now cash is still king. (*Officer 1)*

This is interesting from a securitisation perspective. These quotations provide a stark contrast to the securitising speech acts seen in Chapter 4. There is no sense from these quotations that cryptocurrencies are being used in an overwhelming amount of crime or that they are a significant threat which requires special measures. That is, the language of the officers is not securitising cryptocurrencies. Ironically, it is the government-supplied cash that is perceived as the greater threat, which undermines the justification of the speech acts against cryptocurrencies on the grounds of illicit use.

Whilst Officer 1 believes that cybercrime, such as ransomware, has increased alongside cryptocurrencies, there have only been small increases in other crime types such as drugs on dark net markets. These latter crimes have likely taken some of the real-world crime online, rather than generating new levels of absolute crime. However, Officer 1 does note that anecdotally some of the online vendors they’ve investigated were not involved in the drugs trade in the real world. Officer 1 also supports the earlier observation that the majority of drug transactions are low-level personal supply.

Officer 2, who works primarily in traditional investigations, has not seen cryptocurrencies being ‘used as much as cash or other traditional forms of money laundering and asset layering processes’. Again, cryptocurrencies are used for small-scale suppliers/consumers of drugs but, when it comes to larger volumes, any large amount of cryptocurrency would have to be cashed out. As a result, the ‘vast majority of investigations’ still revolve around traditional assets such as cash and property. As Officer 3 puts it:

> There is a possibility we're overstating the threat, in comparison to the illicit movement of traditional cash. It's very difficult to say… It's only a minority that actually use [cryptocurrencies] for criminal purposes and I think that's been evidenced in a few reports from the track-and-trace companies, Chainalysis and Elliptic and the like, who argue that yeah there is substantial cryptocurrency criminal abuse, but it is a very small percentage. (*Officer 3)*

Officer 4 discusses the prevalence of cryptocurrencies in the cyber-dependent crimes we have already discussed but noted that in a current money-laundering investigation the laundering is via traditional finance through challenger banks where KYC may not be as robust as in established banks. Cash is also described as being involved in more crime than cryptocurrencies and identified as a continuing pillar of criminal methodology:

> I would say that cash-based money laundering is still as active as it was five, ten years ago. There's still projects being run in the NCA that's still focused on cash-based money laundering…Drug dealing is a cash-based industry and the volumes of drugs being shifted doesn't seem to be going down. (*Officer 4)*

As in Chapter 4, cash continues to play a starring role in criminal financing, and this is acknowledged by all the officers. Considering that Bitcoin has been operational for more than a decade, it does not appear to have revolutionised criminal methodologies. The speech of the officers does not portray cryptocurrencies as a significant and urgent problem:

> Compared to cash I've not seen any sudden evolution of criminals changing their behaviours when it comes to remittance services like Western Union for example. It's the same old tricks, the same use of money mules, the same

> organisational process by which you'll recruit mule herders... I just don't see a big change over the last ten years. (*Officer 1)*

6.2.3 Privacy Coins

Whilst privacy coins have not emerged as a theme to discuss, they are a topic that deserves specific mention. In the early stages of research for this thesis, privacy coins were a prominent concern or area that needed particular attention. If Bitcoin is only pseudonymous, what of privacy coins where even more of the transactional data is obscured? Chapter 5 has gone some way to reducing concern over these cryptocurrencies, as has Chapter 2. First, the technical research discussed about privacy coins has shown that opportunities for identification can arise even when using a privacy coin (such as Ron & Shamir, 2013; Kappos et al., 2018; Meiklejohn et al., 2013; Androulaki et al., 2013; Kumar et al., 2017; Moser et al., 2018). They can be complicated to use, and a user does not know if any fault or vulnerability might compromise security at a later date. But the operational security taxonomy in Chapter 5 shows that a transaction is not an abstract event on a blockchain. Someone has to send and receive the cryptocurrency. A user had to acquire the cryptocurrency and a user invariably will want to cash out of the cryptocurrency. It was for this reason, that anonymity was not the main advantage of cryptocurrencies. And if it is not the main advantage, then it is of no more concern if a user chooses to use a privacy coin over any other:

> If your [operational security] is up to scratch, then you don't necessarily need to be concerned about that permanent record on the blockchain. If you're following practices such as only using an address once and using tumblers and things like that then you can be pretty sure that you're going to preserve your anonymity in terms of using cryptocurrencies. (*Officer 4)*

This quotation links well with the analysis from Chapter 5. Regardless of which cryptocurrency someone may use, they can only hope for anonymity within the payment mechanism part of the taxonomy. Even if they have used cryptocurrencies flawlessly, their activities will still be part of a wider series of events and considerations that also require good operational security. The taxonomy, therefore, also highlights the potential ineffectiveness of a securitising move against one aspect. In this way, privacy coins and cryptocurrencies do not serve as a solution to anonymity in illicit activity. This is also in part why privacy coins are not taking over from Bitcoin (as well as the fact Bitcoin is widespread and easy to use).

> What has quite amazed me from all my years dealing with cybercrime and dealing with Bitcoin I think, anyone working in this area is waiting for the next privacy-centric coin to kind of take off and the criminals grab hold of it and run with it. So obviously cryptocurrency as a whole are just like 95% of the means for cyber criminals to move money but Bitcoin in that space, I think has certainly without question remained the cryptocurrency of choice for criminals. And sometimes I'm surprised because I think there are other means by which you can maintain privacy.
>
> For example, when Alphabay was still going as well as accepting Bitcoin they accepted Monero and so the question I sometimes get asked is well why didn't everyone just use Monero if it's next to impossible to trace the transaction back to an individual? And the answer is it's just it's harder to use than Bitcoin so people have just used Bitcoin, and I wonder if the reason criminals haven't moved towards other privacy-centric coins… and remained with Bitcoin is, I mean take ransomware, for example, you need your victim to be able to pay you and it's hard enough buying Bitcoin for most people let alone some other obscure currency where it's not supported with exchanges or wallets software and it's made very difficult. So, I think they're kind of forced to stay with Bitcoin just because of how easy it's been made to allow them to receive payment of extortion demands and the like so yeah, I found that quite interesting. (*Officer 1)*

Officer 3 echoes these sentiments. A sophisticated actor can just use Bitcoin if careful enough in the other aspects of the taxonomy. And in this sense, they, therefore, do not *need* to use a privacy coin, as anonymity is not what they are using cryptocurrencies primarily for. Having said this, if privacy coins became ubiquitous then some of the opportunities around the careless use of Bitcoin would disappear:

> I guess our capability really is primarily focused on Bitcoin so if they start moving away to other types of cryptocurrency, again thinking of Monero specifically, but there are numerous other ones as well, then that presents in some instances a pretty insurmountable obstacle to us. (*Officer 4)*

Perhaps in response to this fear, the regulatory landscape has tightened around the use of privacy coins. Exchanges have even delisted privacy coins such as Monero, Zcash and Dash (the three privacy coin search terms used in Chapter 5) (Reynolds, 2021). Whilst this may allay some fear, it is unlikely to deter much illicit activity and users can continue to use Bitcoin as discussed previously. If Bitcoin is acquired using cash (and you are not identified by a seller) then there is no way identity can be attributed to that Bitcoin address (unless you reveal it). This is one of the reasons why Bitcoin continues to be used for illicit activity, even though it is not anonymous. Here, crucially though, it is the cash that provides the anonymity. In this way then, various methods can be used to transact with Bitcoin relatively securely. Bitcoin has network effects and an overwhelmingly legitimate usage of the system, so it would be hard to overcome that for a privacy coin, especially now that liquidity has been removed from regulated exchanges. And even with a privacy coin, many of the same problems still exist, and with them the same issues. How do you cash out of a privacy coin, how do you acquire them – all without making a mistake or revealing an identity?

6.3 The Dark Net Security Threat

The narrative that cryptocurrencies are a tool for criminality has already been discussed in several of the chapters. This section now returns to the use of cryptocurrencies specifically on dark net markets. This usage is often the focal point of the securitising narrative, and a recurring theme of concern, so it is important to consider this site of use from the perspective of the law enforcement officers. The dark net generates a lot of securitising headlines, but it was shown in Chapter 4 that the scale of activity for many crime types is a very small proportion of real-world activity. Scale is important in securitisation theory and ‘the problem with scale is endemic to all kinds of security logic' (Buzan et al., 1998: 106). Especially since 9/11, this debate can be seen in airport security, as an example, where the cost versus benefit is often scrutinised (Stewart & Mueller, 2013). If the scale of the dark net threat is relatively small, then how can it be sufficient enough to qualify as a legitimate security issue?

Illegal trade, especially in drugs, has appeared as a specific issue in terms of economic security (Buzan et al., 1998: 98). So, it is important to consider this further and look at the views of the law enforcement officers about the dark net as a key site of illicit cryptocurrency usage. There is a great deal of academic research about the dark net in terms of quantities and types of goods for sale or harm reduction, but less in terms of the views of law enforcement and very little to no research on the use of payment mechanisms. It is important to understand the officers' views about this area before more substantial claims about their position on the security threat of cryptocurrencies can be made.

This section begins with the analysis of a theme that emerged from the coding, and it relates to trust in illicit transactions on the dark net. Bans of cryptocurrencies are then discussed as a way of considering whether cryptocurrencies are central to illicit internet activity. Before moving on, we should acknowledge a point made by Officer 3 that there are several crime types within the dark net and dark net markets themselves. These are often grouped together, and blanket assessments are given about the dark net. This is problematic and not something that is done by law enforcement elsewhere. Some granularity is needed, and specific crime types are identified where possible to enable these distinctions.

6.3.1 Trust and Recourse

> I think potentially it is [the dark net punished harder], because of the media reporting around the dark net and I find myself when I mention anything dark web related to the judiciary or a magistrate when applying for a warrant, there's this sense of fear almost this big underground horrible part of the internet that's just full of horrendous violent crime and that's kind of the

> perception so, sadly for some individuals I'm sure that goes against them when it comes to… the subsequent sentencing outcomes. (*Officer 1)*

Perhaps it is that the dark net feeds into wider fears about the threat of cybercrime more generally. But this quotation is interesting in relation to the disconnect that appears to exist between the perceived threat of particular cybercrimes and the scale of the threat in terms of security logic. How great a threat then is the dark net as viewed by the officers? It was established in Section 6.2.1 of this chapter that cryptocurrencies are used for low-level drug activity, on the dark net in particular. And an interesting theme that emerged from the coding was *trust and recourse*, where reasons arose to explain why this activity was only low-level:

> Some traditional criminals don't understand [cryptocurrencies] much like a lot of traditional policemen don't understand it. I think also it's a rife area for scammers, and criminals are well aware of the problems that you can get if you are scammed online and there's no recourse. Whereas in the criminal fraternity, if you know who you're doing business with there's always recourse because obviously, criminals have no recourse within law you need to have some sort of recourse if you're trusting people with large quantities of money… If you're buying large quantities of drugs or doing anything else... the anonymity works against it if you see what I mean. (*Officer 2)*

The issue of 'trust' has been widely studied in the social sciences but scholars have often struggled to find clarity about what it means, although one common view is that 'trust has to do with how people cope with risk and uncertainty' (Von Lampe & Johansen, 2006: 166). And in regard to organised crime, trust is related to the connections that underpin criminal networks (Von Lampe & Johansen, 2006: 167). As discussed in Chapter 2, though, the dynamics of trust are twisted on the internet and familiar bases of trust such as familial or cultural ties are weakened (Yip et al., 2013: 520). Similarly, in the context of online activity, whether there is a lack of trust is also important. This is particularly so on the dark net, where there is little initial trust and significant mistrust. In those situations, the illicit actors may seek a functional alternative to trust – typically resorting to violence as a way of increasing the cost of betrayal (Von Lampe & Johansen, 2006: 179). But this is again very difficult in an online setting and is evidenced by the fact that harm and violence are lower on dark net markets compared to the real world (Barratt, Ferris and Winstock, 2016: 24).

This links back to Section 6.2.1 where Officer 2 said that many criminals do not trust cryptocurrencies and prefer to handle physical instruments, such as cash, gold, or other high-value items. But in the previous quotation, there is an interesting concept of *recourse*. Recourse in our discussion, then, relates to what happens when there is a ‘violation of trust’ – where there may be recourse to retribution, which can be violent (Von Lampe & Johansen, 2006: 177). Officer 2 observed that, at higher levels of criminality, they require a degree of *trust* and that using cryptocurrencies on the dark net removes this trust. And in the absence of recourse through the law, criminals often turn to recourse through violence. That is, for legitimate trade on the internet there are statutory consumer protections. Companies have to abide by laws to ensure that they operate within guidelines, that products are safe and that they treat customers appropriately. Should any of this fail, consumers can seek recourse through the courts or trade bodies. However, these protections and mechanisms are not available for illicit trade, in real-life or online. In this way, trust arguably becomes even more important. For a consumer of illicit drugs, for example, you may find a dealer with a good reputation on the recommendation of a friend you trust. But this matter of trust becomes inherently more difficult online. For a dealer, trust may again be easier to establish in the real world, through dealing with known associates and customers. But part of the reason the dark net is attractive for buyers is that the threat of violence is lowered – a customer fears no physical violence from an untrustworthy dealer. So, whilst the dark net is a beneficial place for low-level supply, it is not as useful for large-scale trade:

> I do not think [the dark net] would become the preferred method of selling large quantities of drugs because… wholesaling anything is based on trust and you need to have recourse to someone or something, the state if you cannot get your, the thing that you're purchasing wholesale with a lot of money. You don't have that in the criminal world, so the only thing you have recourse to is violence and you need to know who to hold accountable in order to use that, just the same as you need to know who to hold accountable

> if you're wholesaling anything else, whereas for smaller transactions that's less important. (*Officer 2)*

Officer 1 also has some thoughts on this topic:

> I think the big bulk and supply of drugs across borders etc that… doesn't tend to touch the dark net. What you will see are sort of middle-level amounts… you might see a kilo of coke or whatever it might be, but I think you hit a kind of upper limit in terms of the risk an individual's prepared to take even on a dark net market because by its nature you're having to trust the dark net market itself with the escrow and the exchange not being taken down or being monitored by police. You've got the risk of the person you're dealing with, who is that, and then from a recipient point of view arranging delivery. And a drop location for a large significant amount of drugs I think becomes tricky when you're trying to arrange that via a dark net market using their communications facilities and platforms and stuff. So, I think there's kinda like an upper limit there. (*Officer 1)*

This helps explain why the trade of drugs on dark net markets is niche and why dark net vendors appear to be non-traditional sellers who make small profits. We saw from the Silk Road takedown in Chapter 4, that dark net market sales are relatively modest. This again does not support any justification for securitising cryptocurrencies if the scale of the threat is small. It would be hard, if this is the case, to identify what cryptocurrencies threaten existentially. Officer 3 also notes that previous takedowns have shown that 'a very small percentage of the vendors on the dark net who've made a million pounds… but the majority of people selling drugs… they've never made more than ten thousand pounds'. Officer 3 also states that the majority of illegal firearms trade is 'outside the dark net, again probably contrary to what most people believe'. These findings support the assertion in Chapter 5 that the dark net is a niche and is unlikely to grow to more than that and will most likely continue to represent a very small fraction of crime in the real world. This is particularly true for the drugs trade, which is the main product traded on markets. In short, traditional methods continue to be preferable:

> People fundamentally don't really like change, do they? Even if it is becoming easier to use dark net markets and use cryptocurrencies, it would still be sort of insurmountable for some people to still use that technology and they would much prefer to make a phone call and have a hand-to-hand supply of drugs and actually use cash because people have used cash their whole lives and this is a new technology… Setting up with a cryptocurrency exchange, for example, you may need a UK bank account, you may need ID and it may deter certain people from ever stepping into this particular world in this particular sort of market really and more reliant on some sort of traditional means. (*Officer 3)*

Interestingly, Officer 4 also comments that the dark net is ‘not really’ within the remit of the NCA’s NCCU. This is primarily because dark net markets represent cyber-enabled crime, whereas their work focuses more on cyber-dependent crime such as ransomware. But Officer 4 concurs that the dark net is for personal consumption levels of drug activity. ‘Violence is at the heart of traditional organised crime groups’ regulation and control of various markets, but in the context of the internet, there appears to be no directly analogous tool’ (Lusthaus, 2013: 58). Without this ability to regulate and control illicit markets on the internet, it is hard to see how large-scale activity can flourish. And if this is the case, then the securitising speech acts once again struggle with scale in terms of security logic.

6.3.2 Banning

If some of the concern about cryptocurrencies is their use for illicit activity, and if much of that concern is linked to their use on the dark net, then what policies might be effective in relation to this threat? Across the world, there have been bans on cryptocurrencies, and in this section, the effectiveness of such a policy and the view of the participants on this issue are explored. This is useful as it allows us to imagine the threat that cryptocurrencies supposedly enable should cryptocurrencies be banned. That is if cryptocurrencies disappeared, would the threat they are connected to also then disappear?

Officer 1 notes that banning would be very problematic. The decentralised nature of cryptocurrencies prevents bans from being effective, and the result would be to push trade underground as the cryptocurrency systems themselves are hard to stop. Officer 1 also discusses peer-to-peer exchanges which enable people to meet up in person to make a cryptocurrency trade using cash. This kind of exchange would see transactions move away from regulated exchanges where there is the opportunity for law enforcement action:

> If you just stopped cryptocurrency, it could almost have a risk that… you've given it a sense of it's underground, it's illicit, it's not regulated anymore, it's the Wild West and if you want some, I'll meet you near that pub and give you 500 quids' worth of Bitcoin if you come with the cash. I can't see [a ban] having too much of an effect on trade volumes on dark net markets and it could actually run the risk of increasing it… You would probably almost give people a sense of right it's now more anonymous because no one touches it from a regulated point of view, so… no one can trace you, so I wouldn't be surprised if it actually pushed volumes up. (*Officer 1)*

This aligns with the conclusion on banning from Chapter 5. Regulated exchanges are important for several reasons and banning cryptocurrencies would end their services and push trade underground where far less can do done. In fact, all the officers agree that banning cryptocurrencies would be an unsuccessful policy. Officer 2 states that a ban would see users turn to other bearer assets, as per the taxonomy in Section 5.3.3, and that 'you might as well just ban cash as well'. This again speaks to the issue of policy consistency. Officer 3 also notes the likely prohibition effect:

> Owing to its decentralized nature I think it would be very difficult to ban a cryptocurrency out of existence. There's been evidence of certain nation states trying to ban crypto in the past where it's had that sort of prohibition effect where it just pushed it further underground and makes it more difficult then for the regulatory... and legislation to ever have any real impact because you just force it underground and there's obviously no KYC or due diligence then… I think by striking an effective balance by having a regulatory regime that is effectively fit for purpose is probably a better way to proceed. There's

> obviously challenges with more privacy-centric coins going forward and the question of regulation in relation to them, but I don't think the solution is to try and ban them out of existence because I don't think it would work. (*Officer 3)*

Officer 4 also dispels any notion that there would be less drug taking if cryptocurrencies did not exist. And whilst takedowns of dark net markets might create some sense of paranoia ‘it’s a bit whack-a-mole, isn’t it?’ There remain then, questions over what to do about the dark net. Banning cryptocurrencies would appear to achieve little, and takedowns of dark net marketplaces do not deter buyers. And research in Chapter 2 showed that illicit drugs are also even sold on the main internet without any attempt to achieve anonymity. Given these considerations, and the issue of scale extensively discussed, it is hard to see how cryptocurrencies qualify as a security threat.

6.4 ‘Who’ Fears Cryptocurrencies Really?

In the first section of this chapter, we saw the officers’ views of cryptocurrencies as an illicit tool - considering their usefulness, the extent of their use and also the specific issue of privacy coins. To this, a deeper examination of the dark net was added as a specific site of threat where cryptocurrencies are used and feared. And now, all of these elements are used as justification and explanation for a theme that emerged from the coding – *ambivalence toward technology*. This theme pulls together the findings from the chapter so far in terms of whether the officers view cryptocurrencies as a security threat. Based upon this, we can then revisit the contradiction of Chapter 4 where the law enforcement view appeared at odds with the US officials. Are law enforcement officers securitising actors who support and provide the ‘case’ for the securitising speech acts seen in that chapter? An answer to this question helps provide a clearer view of the ‘who’ and thereby narrows the potential options for what the referent object might be for those who do view cryptocurrencies as a security threat and have labelled them as such.

6.4.1 Ambivalence to Technology

> [Cryptocurrencies have] caused us difficulties in terms of investigations, securing prosecutions, understanding the threat picture, it's also provided us with opportunities for sure. There's been plenty of criminals also want to make the leap into using Bitcoin as money, not quite understand it and then almost make things easy for us to be fair compared to if they just remained using the traditional fiat banking system. So, it's not all for me doom and gloom from a policing perspective. I think very much like the internet it can be seen as a force for good, it has created opportunities for criminals to exploit and made things hard in some ways, just like the internet has with policing, but potentially helped us in some ways and I think we'd have to accept it's a technology that certainly for the short, medium-term it's here to stay. We need to do our best as law enforcement to upskill and be prepared for whatever technology is around the corner and be prepared to upskill our judiciary to understand this stuff as well, which is a big challenge. (*Officer 1)*

This summative quotation from Officer 1 provides a good overview of the collective stance of the officers towards cryptocurrencies. There are, of course, criminals using cryptocurrencies but none of the participants expressed any hostility or even dislike for cryptocurrencies. In fact, some of them were very positive about them as a potential force for good in the world. And even though there are some challenges posed by cryptocurrencies, the collective does not appear to be overly concerned with their creation or existence. A theme that emerges as a possible explanation for this position is that of *ambivalence to technology*. This relates closely to common discussions about the nature of technology. Indeed, the view of Heidegger is that technology of itself is neither good nor evil, rather it is the abuse of technology that causes harm (Alawa, 2013). Officer 1 likens cryptocurrencies to the internet and calls on law enforcement to react to whatever technologies emerge. In this sense, cryptocurrencies are just another technology, another tool that criminals will adopt if it offers any opportunity to further their ends. This is interesting philosophically because if you have an ambivalent view of technology, then in what ways would it be possible to securitise something that is seen merely as a tool? This contrasts with the view of the memorable alliance presented, who perhaps have a different philosophical take, viewing the tool itself as the problem, rather than those using the tool.

In a discussion in a later interview, Officer 2 adds that the problem of crime on the dark net is not due to cryptocurrencies but rather ‘human nature is the fundamental problem’. As the officer puts it, ‘I wouldn’t say [crime on the dark net is] the fault with a cryptocurrency any more than I’d say that…crime is the fault of cash.’ Officer 3 also displays a similar sentiment when likening the arrival of cryptocurrencies to the emergence of mobile phone technology - ‘the police have to adapt…and this is no different. It is a threat, but the police need to adapt and find a way to effectively investigate the emergence of new technology, and this is no different in my mind’.

This last paragraph raises a central issue for this thesis more generally. How do different actors define what a security threat is and, importantly, what are the criteria that therefore qualify something as a threat? It seems that it is easy to label something as a threat, but on what grounds is this done? To say that something is a threat as it is involved in illicit activity is not sufficient – Chapter 4 shows that there is more to consider, whether that is at a quantitative or qualitative level. And this has also been discussed in Section 1.3.1 in relation to securitisation theory and the economic sector. Perhaps then there should be a grading of threats based on criteria such as a threat to life, harm caused, market size in monetary terms or volumes of illicit products. We see this kind of grading more widely in threat intelligence, such as with terror levels. But, of course, as we see here, there is also possibly a decision to be made about whether you can even consider a piece of technology a threat; should, instead, the threat assessment be made only of the entity wielding the technology? Officer 3 has also been responsible for training others about cryptocurrencies, and this ambivalent view of cryptocurrencies as just another technology is apparent. Does it make sense to label something a threat, when it is used by many different groups for many different reasons?

> In my opinion, it is a force for good, it is just another form of technology and as was the internet in the early sort of 2000s and different applications that have been developed on top of the internet as its progressed, I think Bitcoin is just another example of a new technology. And as with anything new,

> technologies are adopted by organized criminals to advance their... either means of communication or their means of storing or transferring value and Bitcoin and cryptocurrencies are no different really to the criminal uptake. But one of the things I do try and get across is that it isn't just for criminals and there are a lot of real-world use cases, from remittance through being a value store... I'm not a libertarian but I can see the libertarian appeal as an alternative to traditional fiat currency… Getting that across to the audience when I'm delivering training is a little bit challenging. (*Officer 3)*

Overall, the view presented by the participants is that the 'tool' is not the focus for law enforcement. Their interest lies in policing the behaviour associated with the tool. That is, it is not the technology itself that is the problem but rather it is criminal users and illicit services that are the focus of their attention. In this way, they see their role as helping legitimate cryptocurrency usage by trying to reduce the illegitimate.

But this issue of what a threat is or what qualifies as one remains uncomfortably unresolved. Moore and Rid engaged with the same issue in 'Cryptopolitik and the Darknet' (2016). One approach is to 'require a reaffirmation of established moral choices in a new technical reality', and ask the primarily empirical question: do specific technologies 'encourage more illegitimate than legitimate behaviour' (9)? Chapter 4 showed that cryptocurrency usage is overwhelmingly legitimate and on this basis, cryptocurrencies do not 'cross the line'; cryptocurrency usage is 'better most of the time, but not all of the time' (9). In this regard, perhaps they should not qualify as a threat and one could argue, therefore, that there is a case for de-securitisation – that is, if they have even been accepted as a security threat in the first place.

Quoting Timothy May, a Cypherpunks founder, Moore and Rid also discuss cryptography in comparison to free speech. If free speech is abused, it does not mean you should end free speech. Or as May puts it, 'Just because some people mis-use camcorders to film naked children is no reason to ban… camcorders' (26). The same debates can be had with cryptocurrencies, as was highlighted in Chapter 2. The law enforcement officers take this more ambivalent approach to technology as has been shown. In this way then, it seems that they are not the ones securitising cryptocurrencies – that is, they are not the ‘who’. ‘Who’ is labelling something as a security threat is a fundamental question in securitisation theory and thus a fundamental part of the research of this thesis. Was it the experience and reporting of law enforcement that provided the grounds for the claims seen in Chapter 4? The analysis here so far suggests not. But understanding whether law enforcement officers label cryptocurrencies as a security threat provides further evidence as to whether they are part of the ‘who’.

6.4.2 The Who

One of the fundamental questions of securitisation theory is ‘who’ has labelled something as a security threat. Chapter 4 highlighted several examples of this securitising language from the memorable alliance. Yet, the key gap in our knowledge, though, is where that view came from and why. Chapter 4 also examined the extent to which cryptocurrencies are used in crime, to provide more of a quantitative view in terms of the scale of illicit use. Was it that law enforcement identified cryptocurrencies as a national security threat, a position which was then recognised by others such as the memorable alliance? One of the aims of this strand of research is to get a deeper understanding of those who know the criminal threat best, that is those involved with cryptocurrencies in law enforcement. To do this, securitisation theory was explained to the participants in the interviews and a category of questions was aimed at exploring this area.

All of the participants were asked if they thought that cryptocurrencies are a security threat. As this is an important question, quotations from each of their replies are given as follows. This question enables us to see if the officers label cryptocurrencies as a security threat, and therefore whether law enforcement should be considered as part of the ‘who’. Additionally, the question helps us further understand what constitutes a threat from their perspective:

> Interesting question because as money there's certainly a threat, there's a threat across the criminal landscape in terms of it just simply being used as money to facilitate laundering of proceeds of crime or to facilitate some other

> sort of criminality whether it's cyber fraud, drugs, whatever, but cryptocurrencies as a whole to be a threat against security? I'm not so sure about… It's just a technology we are reacting to from the criminal side. (*Officer 1)*
>
> I think they enable the buying and selling of small quantities of drugs quite rapidly… but no more in terms of large-scale dealings, no more so than hawala banking or smurfing and the other traditional forms have enabled criminality over within the regulated sector and for the last 20 years or however long that's been going on for. (*Officer 2)*
>
> No, I wouldn't... well I don't see them... as a security threat, no. It's digital cash, in the physical world should we say cash exists and is... and provides privacy and anonymity to the user of that cash to then transact. Cryptocurrencies are no different. (*Officer 3)*
>
> I wouldn't view them per se as a security threat, it's more the manner in which they're used is the security threat… (*Officer 4)*

Whilst none of the participants expressly view cryptocurrencies as a security threat, these quotations reflect some of our earlier analysis; that there is an ambivalence to technology as a tool, that there is a policy inconsistency compared to existing methods and that law enforcement focusses on the use of the tool rather than the tool itself. This last point is worthy of distinction in terms of the narrative. Are cryptocurrencies themselves a threat or is the small percentage of their use for criminal activity a threat? This is a philosophical point, as has been discussed, but it seems in this regard the officers do not view cryptocurrencies as a security threat in terms of it as a tool. Like Heidegger, for the officers, the issue is a question of abuse of the tool by criminal actors, not the tool itself. However, there is also evidence in these quotations that scale is relevant to the officers, as it is in securitisation theory. Officer 2 notes that cryptocurrencies are used in buying small quantities of drugs, but this is no worse than existing methodologies. In this way, the scale of the threat is not there and therefore no securitising language. The conclusion drawn from this is that in the UK at least, law enforcement officers do not appear to be labelling cryptocurrencies as a security threat. And in Chapter 4, it was politicians and those from traditional finance that have done the labelling. Officer 3, when asked if cryptocurrencies are as big as a problem as is portrayed, said this:

> No, I think a lot of news reporting, a lot of the release of statements by certain individuals in government or heads and executives of large financial companies and I think they may have a lack of understanding in relation to cryptocurrency technology and a vested interest in briefing against it really… Is it the police's responsibility to investigate a technology that presents a threat to the current fiat financial system or is it our responsibility to investigate individual crime? And I think a lot of the briefing that you see is from only people or institutions who may have concerns about the rise of cryptocurrencies and the opportunities that affords the nation-state in terms of control of finance. (*Officer 3)*

Securitisation theory helps us understand why this quotation is interesting, as it speaks to the other key concept of the referent object – the thing that needs protecting. Is the referent object victims of crime, law and order or, as mentioned here, the traditional financial system? Or if it is the memorable alliance that is doing the labelling, is the referent object power, control or even fiat currency itself? Understanding what the referent object is provides a much clearer view of why something is being labelled a threat. But as noted in Chapter 1, it is hard to precisely identify it, especially in the economic sector. As a result, this will be discussed more deeply in Chapter 8.

Finally, Officer 4 also had this to say when asked if law enforcement had labelled cryptocurrencies as a threat:

> I think we've heard just more pragmatically that it's a tool that criminals are using and so it's an area that we need to develop our knowledge, skills and capabilities to keep up with them. There's plenty of tools that criminals do use. A lot of them have completely legitimate uses as well, you can't label them all a security threat and they're just tools of the trade. (*Officer 4)*

6.5 Conclusion

Chapter 4 showed that the scale of crime using cryptocurrencies is very small - evidence that does not support the securitising narratives seen. In this chapter, the views and experiences of UK law enforcement officers were explored through interviews. The aim of this was to learn more about cryptocurrencies from the other key entity that has the closest experience with them. This complemented the research in Chapter 5, which explored the view of users of cryptocurrencies for illicit purposes.

In Section 6.2, the general view of the officers was explored towards cryptocurrencies. The officers noted that it was hard for them to know the true scale of the illicit use without more research with a wider perspective of all crime types. This is important to this thesis, and more widely, in that how can a case be made for something as a security threat if accurate research about the threats is absent? This likely leads to more subjective claims that could prioritise the wrong threats, as is warned by securitisation theory. The officers did remark that cryptocurrencies can be a useful illicit tool, but the success that a user has in terms of maintaining their anonymity and evading law enforcement depends to a certain extent on their education and care. And whilst this is the case, cryptocurrencies do present opportunities for law enforcement.

Despite any advantage that cryptocurrencies may bring, a user with illicit intent is still faced with the same problem of cashing out. In this regard, cash plays a prominent role in attempts at anonymity, illicit trade itself and the proceeds of crime. As a result, most of the officers saw cash as a greater security threat than cryptocurrencies as it is still ‘king’. Indeed, the officers saw no great change in criminal methodologies in the more than a decade since Bitcoin was launched. This presents difficulty from a securitisation perspective. From an illicit usage standpoint at least, it is hard to see how cryptocurrencies could be seen as a pressing existential threat. And similarly, if cryptocurrencies could be replaced by other payment mechanisms as per the taxonomy, then it is likely that securitising one part of it would only have a limited effect.

In Section 6.3, the theme of trust and recourse was discussed. It was noted that these terms have wider roots and meaning in social science. The observations of the officers about the nature of illicit activity on the dark net were relevant to debates about the extent to which organised crime can exist on the internet. Violence in the real world is a key way that illicit actors increase the cost of betrayal as an alternative to trust. And without recourse, it seems that it is not possible to have large-scale, organised crime on the internet (Lusthaus, 2013). The officers noted that illicit crime on the dark net was lower-level and not likely to scale. This is again important to the analysis here in terms of securitisation theory. If the use of cryptocurrencies for illicit activity, particularly on the dark net, is a concern, then how justified is this if the very nature of that location means that it is unlikely to ever be a large threat? This is a logical problem for securitising acts as the scale is an important factor. A referent object needs to be existentially threatened, and that is unlikely to be the case if the threat is small.

In the third main section, 6.4, the theme of ambivalence to technology was explored. The officers viewed cryptocurrencies in the sense of Heidegger as a tool, that was abused by people. Based on this, and the fact that the officers did not see a significant scale of threat in cryptocurrencies, the conclusion drawn is that they are not a securitising actor. Their language does not evidence a securitising move and so they are not a part of the ‘who’. The sample is small, but it does not appear that law enforcement opinions or experiences are behind the justification for the securitising moves of the memorable alliance. This chapter provides more evidence to that effect, in resolution of the contradiction in previous chapters between the view of law enforcement, who wanted illicit users to continue using cryptocurrencies, and the memorable alliance who claim that they are a security threat.

If we remove law enforcement from those that have labelled cryptocurrencies, then there must be a re-evaluation of the ‘who’ and certainly the ‘why’. At the beginning of this chapter, we noted that criminal use has never been a contested area in the long history of debate about money. If we were to also then remove criminal use from the debate about cryptocurrencies, then we must ask what the debate and labelling are really about.

7 HullCoin - Cryptocurrencies in Civil Society

In Chapter 2, we saw that there have been several studies of cryptocurrency users which examined individual perspectives. A gap was identified in the literature concerning users of cryptocurrencies for illicit activity, and this was addressed in Chapter 5. In this chapter, the aim is to provide a different perspective by exploring HullCoin, reportedly the world's first local government cryptocurrency (Gilson, 2014; Watson, 2014). Rather than focussing on what individuals think and feel about cryptocurrencies, this chapter zooms out to examine how and why a cryptocurrency was used at a local, community level. The research sub-question, therefore, for this chapter is:

> What prognosis is there for cryptocurrencies to play a valid role in money and society?

Much of this thesis has explored the use of cryptocurrencies for illicit activity and considered the threat that they pose. The case study of HullCoin in this chapter does the inverse by exploring how cryptocurrencies can be used for positive, legitimate outcomes rather than merely as a vehicle for speculation or crime - can they be a force for good? This is an important consideration in relation to Moore and Rid's arguments about the use of cryptography as discussed in Section 2.2.1, where the central empirical question was whether 'cryptographic architectures encourage more illegitimate than legitimate behaviour.' (2016: 9). This thesis has examined the extent that cryptocurrencies are used in illicit activity and the ways in which they may be useful for this, but the 'illegitimate' also needs to be deliberated in the context of 'legitimate' use as well. Not just in terms of the percentage of illicit activity versus legitimate, but also in terms of the ways cryptocurrencies may have something useful to offer.

The threats that cryptocurrencies pose are vital to the analysis of any case made for securitisation but if cryptocurrency usage is more legitimate than illegitimate, and if there are positive ways that they may contribute, then there may be a case for the desecuritisation of cryptocurrencies and 'the shifting of issues out of emergency mode and into the normal bargaining processes of the political sphere' (Buzan et al., 1998: 4). Furthermore, this chapter returns us to the core topic of money. The HullCoin project provides additional insight into the state's reaction to alternative monies, which enhances our understanding of any attempted securitisation of Bitcoin and cryptocurrencies.

HullCoin was chosen for this case study not only as it was the first local government cryptocurrency which is of great interest in its own right, but also because it is a particular example of a complementary currency, being based on Lietaer's Civics. There are other complementary currencies, such as the Bristol Pound, which was discussed in Chapter 2, and there have been other complementary currencies that have moved to a cryptocurrency model such as Colu (which is discussed later in this chapter) but HullCoin was the first to use blockchain technology and Civics as the underlying theory. Furthermore, as the first of this type of project, HullCoin enjoyed a considerable amount of media attention and interest from government departments which again made it a compelling object of study. Finally, as HullCoin was UK based that made it a practical option for research compared to Colu, for example, which is an Israeli-based organisation.

The chapter is organised into two main sections. In Section 7.1, the methods used in the research and the background of the HullCoin project are first laid out. The concept of complementary currencies, which exist alongside national currencies, is then introduced and described. This is followed by some more detailed discussion of Lietaer's Civics, as this was the specific conception of a complementary currency that HullCoin was modelled on.

Section 7.2 then presents the findings and analysis of the chapter. The case study examined why a cryptocurrency was used as a model for this local currency, as opposed to other existing forms. This concerns the technical but also the philosophical aims that the creators of the HullCoin hoped to achieve. Whilst this is interesting and useful to understand, the reactions to HullCoin as a money, the ways in which the founders hoped it would deliver social benefit, and the problems they encountered are arguably of greater meaning and interest. Finally, HullCoin is also analysed through the lens of securitisation theory. Was HullCoin labelled a threat in the same way that Bitcoin has been? If not, how does this contribute more widely to this thesis and the understanding of Bitcoin and cryptocurrencies as a security threat?

7.1 Method and Background

7.1.1 Method

The methods used in this study were affected by the outbreak of COVID-19 and this is described in more detail in Chapter 3. Several in-depth semi-structured interviews were conducted, primarily with the two main founders of HullCoin, Dave Shepherdson and Lisa Bovill. Both were officers in Hull City Council and worked in financial inclusion. Dave Shepherdson left the HullCoin project around 2017, whilst Lisa Bovill remained a board member of the controlling organisation that ran HullCoin until a few months before the interviews took place in the middle of 2020. As such, these two participants provide good coverage of the project from its inception to its effective end. As the project did not quite make it to full launch, I feel that these were the two key people to interview to learn about the conception of HullCoin, its social, philosophical, and technical basis and, ultimately, to understand what worked, as well as what did not.

There was only a small team who worked on HullCoin and I did try to secure further participants. One person initially agreed to be interviewed but later withdrew due to personal issues related to the project. I also tried to contact the technical team member who developed the blockchain system and other components but did not receive a response. Whilst this would have been an interesting perspective, I did manage to get answers to some of the more technical questions from the founders and so feel that there is a sufficient understanding of these aspects.

I also set out to interview wider groups of businesses and individuals who may have taken part in HullCoin. However, the project did not reach the stage where it was fully deployed. I did however manage to interview a business owner who participated in early trials. Some useful observations came from this, but the owner explained that things did not move beyond the trial stage, so it did not get as far as being active in their business.

In addition to the interviews, I was also subsequently provided with some documents regarding HullCoin by Dave Shepherdson. This included some briefing papers and also a transcript of a media interview that the founders conducted at the time in 2017. These documents were added to Nvivo and coded along with the interview transcripts that I produced. Finally, this case study also makes use of several media reports that were found through internet searches. The HullCoin project gathered a significant amount of media interest and so these web pages were also used as a valuable resource. This included, for example, a video piece on BBC Sounds from a reporter who visited Hull at the time. Altogether, the sources combine to provide a fascinating case study of the world's first local cryptocurrency. Throughout the rest of the chapter, the founders are referred to by their first names, Dave and Lisa, and any quotations used from the interviews are verbatim. Hesitations and disfluencies have been removed in quotations to aid comprehension. I do not think this affects the meaning or how the quotations are presented, and this is merely done to make the quotations easier to read.

7.1.2 HullCoin

The HullCoin project emerged from the founders' work within Hull City Council. Dave was employed in a role that concerned anti-poverty work in the city, whilst Lisa's involved advising about civil legal issues such as housing, debt, and employment. The founders were, therefore, looking for ways to help the local population and address the issue of poverty in the city when the idea of HullCoin was conceived (Gilson, 2014). Hull, or Kingston upon Hull, is a port city in East Yorkshire. The city has high levels of poverty and deprivation, with correspondingly higher levels of unemployment and crime. Hull is the third most deprived local authority in England out of 326 (Hull City Council, 2017). According to ONS data from September 2020, Hull had the highest jobless rate in the country along with Blackpool. Furthermore, nearly 10 per cent of the city's working-age population was on unemployment benefits and more than one in three of working age had their income supported by the state (Gerrard, 2020). The aim of HullCoin, therefore, was to introduce a local currency that would encourage social activity and help tackle poverty.

A not-for-profit social technology company called Kaini Industries was created in 2014 as the vehicle to run the HullCoin project, operating aside from the local council where Dave and Lisa worked. The company was formally dissolved on 21 September 2021, with HullCoin having reached its peak between 2014 and 2017. One of the documents that Dave provided was a briefing paper from Kaini Industries and it is useful for some of the project background (Kaini Industries, 2014). The company was funded by grants from the charity sector and included support from Comic Relief as well as the Big Lottery Fund’s Accelerating Ideas programme. The idea was for HullCoin to work in a similar way to a corporate loyalty scheme but instead, as a community loyalty scheme that rewards positive social action. HullCoin would work with local services that would distribute HullCoin to the public when they carried out a piece of community work (10 million tokens were ‘pre-mined’ or created upfront). The public would then be able to exchange HullCoin for discounts on goods and services provided by local businesses. The model for HullCoin would utilise local economic capacity, without cost to the local authority. The design of the system was based on blockchain technology for the creation and management of the HullCoin tokens.

The briefing document provides several examples of the activities that could be undertaken to earn HullCoin. Schools could reward attendance with coins that could be used for uniform discounts. People seeking work could be rewarded for job-seeking activities, and then access reduced costs for training such as driving tuition. Those in prison could earn HullCoin to support family or access reduced rent on release. And within health, HullCoin could reward all kinds of activities such as quitting smoking or losing weight.

The briefing document also provides some information on the specification of the HullCoin platform. An online marketplace was created where organisations could post activities and businesses could advertise discounts. The platform connected to Android and IOS apps which then enabled the exchange of HullCoin through a digital wallet. The HullCoin cryptocurrency was built upon Bitcoin 0.11, a version of the

Bitcoin software. This is extremely interesting. Bitcoin is run as an open-source project called ‘Bitcoin Core’ and a volunteer community of developers support the project and maintains the ‘Bitcoin Core’ software releases which can be downloaded for free on the internet (Bitcoin Core, 2021). In effect then, HullCoin is a ‘software project fork’; that is, it is a separate project built using the Bitcoin software (Coinut.com, 2019). Several other cryptocurrencies have been created this way, including Litecoin as perhaps the biggest example. To an extent then, HullCoin *is* Bitcoin – just a different version, run by different people. Philosophically this is an important point for this chapter. If, at a technical level at least, Bitcoin and HullCoin are very similar then what differences or similarities can be seen in how they were received? Is HullCoin also then a security threat and concern regarding its use for illicit activity? And what reasons might explain any differences in how the two projects were treated? These questions will be returned to throughout the chapter.

7.1.3 Complementary Currencies

Before moving on to the results and analysis, it is necessary to first discuss some important concepts that emerged from the case study of HullCoin. When I first began this strand of research, I thought it would provide a useful counter to the illicitly focussed earlier chapters. But some impactful theories of money emerged from this work that have become central to how I now frame money and the security debates about cryptocurrencies. As a result, this chapter has become far more significant to the overall thesis than I originally envisaged. And it also becomes more significant in shaping my overall thoughts for the discussion and conclusions in Chapter 8.

For most people, a dominant national currency is the most common way to experience money. In the modern world, we are most familiar with money issued by the state and other large financial institutions such as banks. This was certainly my experience of money as I began this project. But throughout history, there have often been alternatives. There have even been periods of successful ‘free banking’ in several countries of the world when ‘unrestricted competition in the business of note issue’ was allowed, but ‘the theory and implications of unregulated and decentralized currency supply have been largely ignored' (Selgin, 1988: 7, 3). As a result, the dominance of the state monopoly of money continues.

However, Ingham (2020: 104) notes that there are other alternative payment mechanisms at the top and bottom ends of the economy that do exist today. At the top end, companies issue IOUs. And at the lower end of the economy, local communities and small businesses create their own means of payment. (Examples of these in the UK, such as the Bristol and Brixton pounds, were introduced in Chapter 2). The digital age has also ushered in Dodd's era of 'monetary plurality' and many fintech organisations have added to the ways and means that we can transact. And of course, we can now add cryptocurrencies as yet further examples of alternative financial networks.

Interestingly, Ingham also observes that a 'proliferation of non-state monies is inversely related to state power' (2020: 104). This suggests that state power is currently under threat and makes sense in terms of securitisation theory, especially in the context of the conflict that comes from a national currency being used as the international reserve. If there is a threat to the state's monopoly of money, then it follows that we should be in a time where there has been an explosion in alternative finance. The question to consider then, is why do some alternatives become labelled as a security threat whilst others do not. Or do all monies pose the same level of threat to the state? To enable the discussion of these questions, some terminology must first be introduced. Ingham uses the term 'complementary' to describe currencies that exist alongside dominant state money and 'alternative' for currencies that aim to replace national money (2020: 107). This distinction is important moving forward, as Bitcoin and HullCoin are considered further.

It can be difficult, however, to identify a currency as an alternative one as the lines can become blurred. Even for Bitcoin, it is hard to claim conclusively that it was created to replace national currencies. Satoshi expected any adoption of Bitcoin to be slow and, in all likelihood, niche (Champagne, 2014). In this respect, perhaps it too was intended more like a complementary electronic currency that could have many applications – Satoshi was certainly conscious of the swarm from the 'hornet's nest' in connection to Bitcoin being used by Wikileaks (325). It seems that Satoshi viewed Bitcoin more simply as a technological solution to the 1990s problems in creating electronic money. No doubt Bitcoin could potentially replace fiat if it proved to be better money and was chosen by enough people, but this is not to say that there was a strongly expressed political drive to do so. Indeed, Satoshi wrote:

> I would be surprised if 10 years from now we’re not using electronic currency in some way, now that we know a way to do it that won’t inevitably get dumbed down when the trusted third party gets cold feet… It could get started in a narrow niche like reward points, donation tokens, currency for a game or micropayments for adult sites. (Satoshi as quoted in Champagne, 2014)

Complementary currencies, though, are easier to identify. A political agenda to replace the national currency is absent, and they often emerge in small, geographic areas. They are also not a new phenomenon - there are more than 4,000 of them across the globe, following a surge in their number since the 1980s (Lietaer and Dunne, 2013: 5). Complementary currencies offer their communities the opportunity to drive economic activity outside of a dominant national currency. For example, in a local economy, there may not be many jobs available but that simply means that there is unused economic productivity in that region. There may be many people who want to work but cannot, as there are no jobs. Local currencies enable the utilisation of that unused capacity by creating, in effect, a secondary market that is paid for with the complementary currency. In HullCoin as one such example, a social act can be rewarded with the token which can then be used in the local economy for a discount on a good or service. These currencies also keep the value within a locality, so that the money cannot be spent elsewhere – a HullCoin token has no value or use in any other city.

It is also worth noting, that there have long existed further flavours of these concepts. Timebanks allow a person to fulfil an activity and ‘bank’ that time to be repaid by someone else doing another activity. For example, an individual may spend an hour helping an elderly person with their shopping and then exchange that credited hour for the services of someone else who may cut their lawn. In the UK, Timebanking UK (TBUK) is a national charity that was set up in 2002 and by March 2021 six million hours had been exchanged in this fashion by its members (2021). And there are other similar systems with a variety of names such as LETS (local exchange trading systems) and mutual credit trading systems.

7.1.4 Lietaer's Civics

These monetary concepts are important as further evidence of the multitude of payment mechanisms that exist, and that state money is not the only conception of how we can transact. And these concepts are also central to this chapter and HullCoin as in one of the interviews it was revealed that HullCoin was inspired by Bernard Lietaer and his concept of the 'Civics' complementary currency. Lietaer was a leading monetary reformer and he held many roles in the field over a 40-year career, including as a professor but also in the Central Bank in Belgium (Positive Money Europe, 2019).

Conventionally, funding for social projects comes from taxes or debt, or in the charitable sector from donations, which indirectly affects government income (Lietaer et al., 2012: 293). Lietaer proposed Civics as an alternative way to fund labour in social projects, which is typically the most expensive part. In short, the system works as follows (using UK terminology). A local authority would request that all citizens contribute a portion of their council tax in Civics, which is 'an electronic unit issued by the city which are earned by residents through activities contributing to the city's publicly agreed upon aim' (293). An hour of time could be the unit of account in this system. So, if the aim is to have a cleaner city, residents could earn one Civic by spending one-hour picking litter. If a resident was required to pay 10 Civics as part of their council tax, equivalent to £1000, then anyone who earns less than £100 per hour should be interested in taking part in the system (Lietaer and Dunne, 2013: 147). Some people then will be incentivised to earn more than 10 Civics, and this will enable those with a surplus to exchange any spare Civics, whilst others who earn more than £100 per hour may simply pay the full amount of council tax. The result is to drive social activity without requiring taxes or debt to do so – 'a decentralised Keynesian stimulus at the city scale' (147).

Two further points must be mentioned in terms of the concept of Civics. First, the government should ensure that only genuine Civics are in circulation and that exchanges are transparent and fair. This is not a trivial task and one that would normally come at a non-trivial cost. Ordinarily, this would require a centralised entity to manage these processes. And second, the value of the Civic should not be tied to the national currency as the idea is to have a complementary but independent system. If the government wants the value of the Civic to strengthen or weaken, then this can be achieved by requiring more or less Civics to be paid in contribution.

Lietaer wrote extensively about monetary reform, and his work has influenced this thesis not only in terms of Civics as the basis for HullCoin but also in terms of his wider views on monetary systems, their problems, the causes of those problems and possible solutions to them as well. This was discussed in Section 2.1.5 on Modern Money (Theory), where Lietaer argued that our current systems drive inequality by systematically transferring wealth to the top of society, resulting in a highly unstable monetary system that is far from resilient. Furthermore, societies with multiple currencies have enjoyed greater stability and equality. Lietaer also wrote that there has been a widespread belief that ‘community breakdown has become a universal pattern all over the modern world’ (Lietaer, 2001: 179). The structure of the family has eroded, as evidenced by divorce rates and smaller households to name a few measures. And whilst monetary systems are the cause of these problems, for Lietaer they are also the solution:

> We just learned the apparently general rule that whenever money gets involved, community breaks down. However, this turns out to be true only when scarce, competition-inducing currencies, such as our official national currencies are involved. In fact, the use of some other types of currencies can have exactly the opposite effect of building community. (Lietaer, 2001: 187)

These notions tie in with our earlier consideration of monetary theories, where money was seen in economics as a passive means of exchange but by others as having a life and effect of its own. Similarly, this also aligns with the theoretical clash of those who argue for the power of the state and a dominant currency against those, such as Hayek, who called for the de-nationalisation of money and the opportunity for currencies to compete freely. And in this regard, perhaps there are ways cryptocurrencies can be imagined as part of the solution to volatility in the current financial system. The HullCoin project is an excellent case study to explore these thoughts further.

7.2 The Interviews (and other sources)

The following sections of this chapter are mainly based on the interviews, but there are also some quotations and references to the other documents that were also collected and analysed. Any quotations from the interviews with the founders are referenced by their first names, *Dave,* and *Lisa,* in italics. The interviews were semi-structured around four main areas of questioning which were based on the thesis research questions.

The first of these areas concerned the technical aspects of the choice of a cryptocurrency model for HullCoin. I was interested in why this model was chosen rather than the existing form of other similar currencies. Beyond the purely technical motivations, I was also interested in which properties of cryptocurrencies were important to the founders. In other user studies in Chapter 2 we saw that some are motivated to use cryptocurrencies by their libertarian appeal, others by a desire to use an alternative to an untrusted traditional financial system and some purely by speculation. The second area of questioning concerned some of the more philosophical questions about HullCoin as a form of money. We have seen that Bitcoin is criticised as money for its non-physical form, and some believe it has no value as it is not 'backed' by anything. Was HullCoin considered money and was it backed by anything? The third area of questioning was about the lessons learnt from the HullCoin project. As the project did not launch fully, there was less to say about the benefits of the coin to the community and no community impact to assess. However, there is still much to learn from HullCoin as the first of its kind. And finally, the questions explored HullCoin from the perspective of securitisation theory. Given that HullCoin was built using Bitcoin's open-source code, was it also labelled as a security threat? As a clone of Bitcoin, did it represent a threat in the same way that some believe Bitcoin does?

Whilst there were four categories for the interview questions, the results that follow are presented more thematically. The first section explores why a cryptocurrency model was chosen but the remaining sections are based on themes that emerged from the coding. Philosophical objections to HullCoin as a ‘magic token’ money are explored in the context of Simmel’s work. Then, we move on to see how HullCoin was received in this context and look at the design choices that the founders had to make about HullCoin as money. The final two sections explore the potential benefits of social currencies but also the problems that they face, especially in terms of the reaction of the state to them.

7.2.1 Why a Cryptocurrency Model?

The HullCoin team examined the different ways that they could build their project, including looking at a paper-based system as some other local currency projects have done. One of the key problems that they identified with a paper system is the increase in costs as the project scales. More paper means more administration and greater costs. A decentralised blockchain model offered an automated system that would scale more efficiently. Wallet software can be made available in app stores and all the transactions are recorded on an immutable ledger. And this approach also ties in with the wider trend of falling cash usage:

> We did an assessment of all of our options including paper but again if you want to scale and you’re running something on paper and you’ve got loads of administrative costs which are a burden, then the more successful that you are the bigger your running costs, whilst having a decentralised model which is automated through blockchain technology means that you can scale much more efficiently. (*Dave*)

Additionally, a cryptocurrency model also solves a key requirement of Civics – that only genuine Civics are in supply and that transactions are transparent and fair. A blockchain records all token transactions in a transparent and immutable fashion and is therefore suitable for this task. It is worth noting that a physical, cash-based Civics would present a far greater challenge in monitoring the trade of the complementary currency and ensuring that counterfeits are not made. This echoes some of the previous discussion about the differences between the properties of cryptocurrencies and cash. It is effectively impossible to counterfeit a cryptocurrency as, in the case of Bitcoin, the ledger records the unspent transaction outputs (UTXOs) which are secured using the underlying cryptographic technology. Paper, on the other hand, can be copied more easily. Similarly, cash is more anonymous than cryptocurrencies, which is why they are a preferred method for illicit activity. This makes it harder to monitor a physical cash-based local currency in comparison to a cryptocurrency one. For HullCoin, the blockchain offered a scalable way to monitor and issue tokens, all for a limited cost. Furthermore, the project felt that there was an ethical benefit in this design choice, due to transparency and the ability for users to custody their own coins:

> A feature of the system, I think it was self-sovereignty… that was something that was important, that they owned their own wallet and their own data, and their transaction history and they have control over it…That was included in the design, it was more of an ethical consideration. (*Dave*)

HullCoin was implemented as a private blockchain, unlike Bitcoin which is a public blockchain. With a public blockchain, anyone is free to take part in the consensus mechanisms which regulate and secure the system, approve transactions, and commit them to the blockchain. But in a private blockchain, all of those functions are only available to selected parties or they take place within one organisation. Kaini Industries was an example of the latter. It was a standalone company that controlled the running of the HullCoin blockchain; the company ran three nodes (computers that ran the adapted Bitcoin code) and, as a centralised entity in the system, retained some power and capability that would not be seen in Bitcoin. For example, they could freeze a wallet if some suspicious activity took place. Similarly, another early concern was over the speed of Bitcoin, which confirms blocks of transactions approximately every ten minutes. The team wanted HullCoin transactions to appear instant and they were able to achieve this through a private blockchain instantiation. Interestingly, they did not have difficulty using cryptocurrency technology and they had more problems with the platform that listed the community activities, as it required a bespoke build rather than using the open-source code of Bitcoin.

What is particularly worth noting, is that many of the properties that were significant in other user studies are not of importance here. Decentralisation was not a goal (as Kaini retained control) nor was libertarianism or anonymity. Speed was a problem though and a big issue, that they overcame by running a private blockchain. Dave stated that self-sovereignty was a good thing, but it did not appear to be a crucial design goal. In fact, this sums up the overall approach of HullCoin in terms of the properties of cryptocurrencies that are commonly discussed; that is, there was nothing philosophically important about HullCoin being a cryptocurrency, it was just that the technology offered them a cheap and scalable way to offer a local currency:

> If you look at what was developed, there's no mention of blockchain technology. That does not sell to the public. We benefit from the infrastructure internally. (*Dave* as quoted in Fernando, 2017)

There was no attempt by the project to capitalise on any hype around blockchain and this is supported in the interview with the business owner who said he did not even know that HullCoin was a cryptocurrency until I mentioned it. The team thought that even mentioning that HullCoin was a cryptocurrency might confuse people. In this way, it was simply the case that the technology was useful – not merely a tool for criminality. A cryptocurrency model was cheaper, scalable, and enabled monitoring through an accountable and transparent system. They saw cryptocurrencies as something secure that could be adapted quickly and easily for a social purpose. And HullCoin used a blockchain as a novel way of deploying such a system:

> When we did the testing out in the communities, we didn't mention Bitcoin, we didn't mention blockchain technology. It was a smartphone app, 88% of people in Hull own a smartphone, you've got a big smartphone culture in Hull… So, whilst certainly, in the early days a lot of the focus [from the press] was around cryptocurrency and what it was, to the end-user no-one’s really going to care, know we were using cryptocurrency… In terms of the user experience of Hull Coin… then no, we didn't see any reason to mention

> blockchain technology because it just confuses people. You just create a barrier where you don't need to create one. (*Dave*)

7.2.2 Magic Token Money

A recurring theme in discussions about Bitcoin is whether it can even be considered as money. In Chapter 2, this was explored in relation to commodity versus claim theory, and the long-debated nature of money. Does money need to be physical, have ‘intrinsic value’ or can it function in a digital, token form? In this section, we will first see the initial reaction to HullCoin and note that this relates to this question about the nature of money, which was discussed in detail in Section 2.1.2 in the context of Simmel’s *The Philosophy of Money*. It is important to do this as the fundamental theoretical divides of commodity versus claim theory and state theories of money shape many responses to the concept of cryptocurrencies. Those that believe in the ‘commodityness’ of money often object to token forms of money, even more so when money is not produced by the state. But Section 2.1.2 showed that discussion needs to move past this old theoretical stance so that we can see where the issues with cryptocurrencies really lie. And in the context of this chapter too, these issues are relevant in many of the same ways:

> I don't like [paper-based local currency], it's like some weird cash thing… it's weird. I think… an app-based [HullCoin] would be the only way to make it work. A bit… like I would use Apple Pay… you build up your points accordingly and then you'd… add them onto your haircut and you take the money off. It's much easier than having actual money, weird fake money, you know that'd be weird. (*Business Owner)*

As Dave remarked, most of Hull’s population uses smartphones and this is becoming an increasingly common way of conducting financial transactions, to the point that, as the business owner describes, physical cash is becoming the ‘weirder’ form of money. Despite this flipped view of commodity versus claim theory of money, there is still reticence when it comes to digital forms of money. And HullCoin too was met with concern by Hull City Council not long after it was conceived.

In 2014, Dave discussed the HullCoin concept at a local forum in the city that had an interest in financial inclusion and poverty. Unbeknownst to him at the time, a freelance journalist was at the forum and this led to one of the articles that has been used as a source in this chapter titled, ‘HullCoin: The World’s First Local Government Cryptocurrency’ (Gilson, 2014). The article was published at 10:47 a.m. on 30 March 2014. That same evening, at 11:45 p.m., *The Telegraph* published another article, with the following subtitle (the main title was similar but shorter):

> Hull City Council is “printing its own money” by creating a Bitcoin-like digital currency called HullCoin which it will use to pay people for carrying out voluntary work, tax-free and without loss of benefits. (Sparkes, 2014)

Up until this time, Dave explained that the Council had been aware of the project, but HullCoin was only a concept at that stage. The Council had been broadly supportive but only to the level of, ‘we don’t really understand this thing, but it sounds really interesting’. Around this time, the story of the project went ‘viral’, with even international media organisations requesting quotations from the Council. And *The Telegraph* headline ‘lit the touchpaper of it all’:

> So, the council freaked out, to be honest with you. Just 'What is this?' I mean, 'Who are these people? What’re they doing in Hull?’ And ‘Are we going to have to accept this for council tax? Can people pay their rent with this money that has been created?'… What I found actually with HullCoin it's always been quite polarising. Some people liked it; some people hated it. And that was very much the same with [the] City Council… I avoided getting sacked. (*Dave*)

As discussed in Chapter 2, Dodd wrote that Bitcoin is fascinating as it has the same contradictions and debates that money more widely has (2017: 36). Society, and the academic debate about money that lies beneath it, have not reached agreement on the form of money. And, as we have argued, this is no more important than now as we move deeper into a digital world. This lack of certainty showed in the reaction to HullCoin.

After HullCoin attracted media attention, the Council distanced itself from the project. The team had received a small research grant to learn about mining equipment and cryptocurrencies, and at this point, the Council said that they could not own any of it and they advised them to set up a not-for-profit company, which became Kaini Industries. The project was only just developing conceptually at this point, even as it garnered international media interest. And the polarising and confusing theoretical nature of money soon became evident in relation to HullCoin:

> It was polarizing within Hull City Council… They was frightened to death that at a time where they're facing cuts from the central government grant that a message would go out to communities that you don't have to pay your council tax… So, the two financial officers of Hull City Council disliked it immensely on that… Instead of the council getting cash it was all these magic tokens that people would be trying to pay the council tax with, and he didn't like that. (*Dave*)

There are two significant points to make here. First, the idea of Civics is to give people a second way to pay for their council tax, other than with the national currency. In this way, it offers more ways to pay rather than just fiat. But this is perhaps quite a revolutionary concept, especially for a finance officer in local government. There was little prospect then for HullCoin to be a true implementation of Civics, and the team, therefore, decided that HullCoin would not have any connection to council tax. The quotation is also revealing through the term ‘magic tokens’. This speaks to commodity and state theories of money, and beliefs that money needs to be either state money and/or connected to some physical commodity. And that without either of these properties, money cannot function or even be considered as money.

But this is axiomatic, and a dated conception of money as has been discussed. For thousands of years, money was physical and for hundreds of years, it was backed by something physical. And even though electronic forms have been commonplace for many decades, fear and mistrust of non-physical forms of money remain entrenched, particularly if it is not a national currency. For HullCoin, the fear and polarisation were about a loss of national currency revenues but also, as the founders discuss, councils are not known to be places for progressive, experimental initiatives based on emerging technologies. Theoretically, though, Section 2.1.2 showed that money can take a token form. But the benefits of alternative systems be they unregulated, decentralised or of complementary form are largely disregarded. This is despite the fact that there have been many successful examples of such systems. And this dismissal is even more striking given the volatility and inequality presented by the monopolistic nation-state monetary system.

7.2.3 Money and Value – ‘Bitcoin for Good’

The previous section established some of the concerns about HullCoin as money, but there were also important issues for HullCoin that went beyond the philosophical to the practical and regulatory level. With outdated, entrenched views of money, it will likely always be difficult to innovate and implement a scheme that encroaches on the territory of state money, even when the project is based on Civics and the ideas of a prominent monetary reformer.

Some of the early planning of HullCoin concerned these exact issues of whether it was money and how the value of a HullCoin would be ascertained. These are now familiar questions to this thesis. In the eyes of UK law cryptocurrencies are not money, however, and, ironically, that gave the founders the regulatory freedom to use Bitcoin as the basis of the HullCoin. There were concerns that if HullCoin was viewed as a currency officially, then that would cause difficulties with tax authorities and other government departments. But, as the Civics model suggests, HullCoin was not linked to a fiat currency and so one HullCoin did not equal one pound. In this way, the design of HullCoin was as a non-monetary reward system that was based on social outcomes, rather than time as in a timebank:

> It was never really designed to be money and it certainly wasn't designed to be perceived as a payment for something and so we wanted to occupy a bit of a grey area. But again, it was a bit of a fudge, and it was a bit of a cop-out really in terms of nobody would be forced to accept HullCoin if they didn't want

> to accept it, and nobody would be forced to issue HullCoin if they didn't want to issue it. (*Dave*)

After the HullCoin story went viral early in its development and the subsequent media interest, there were questions from government departments. In response, Lisa wrote to the Department of Work and Pensions (DWP) and to HMRC to explain the legal position of cryptocurrencies and that they were not taxable.

> Initially, [DWP and HMRC] were very hostile to it. The lack of understanding particularly in 2014… from government and from even legislators around what this was and how this should be classified gave us a lot of freedom to develop things which I think if I just started giving out raffle tickets and said it's a currency, the DWP would've jumped on my back. (*Dave*)

There are some interesting observations to unpack here. First, the Chartalist view of money as the preserve of the state is very strong in our society. There seems to be a general acceptance that money is the purview of the state and that it is protected and enshrined in law. But this is not the only theoretical conception of money as has been highlighted several times. Instinctively, though, the founders knew that a challenge to state money would be frowned upon, to say the least. Likewise, the initial reaction of the government departments was very hostile, but this receded after HullCoin was established as a non-monetary form. The council, HMRC and DWP lowered (or dropped, as we will see) their opposition once HullCoin was understood to not challenge or replace the national currency. This is interesting from a securitisation perspective and suggests that their objection was related to the protection of the position of the national currency. And once that threat was removed, HullCoin was no longer a threat, even though it was a Bitcoin-based cryptocurrency system.

Bitcoin, in contrast, is thought of popularly as a payment system that many hope will replace national currencies. And certainly, as a global multi-billion-dollar market, Bitcoin is much more prominent and, therefore, more of a ‘threat’ than HullCoin. Consequently, it could be said that HullCoin meets our definition of a complementary currency whereas many think of Bitcoin as an alternative one. There was nothing in the design or conceptualisation of HullCoin that presented it as a threat or challenge to the national currency, and so it met with less resistance once this was accepted. And yet, of course, HullCoin *is* Bitcoin in that it is built on Bitcoin's code. Despite this, with a different narrative and positioning as exemplified by Lisa writing to DWP and HMRC, HullCoin became less of a challenge to state money even though its DNA was the same as Bitcoin's. In this way, could it be argued that cryptocurrencies are not themselves a threat and whether they are or not depends on the interpretation of the entity doing the labelling? Indeed, HullCoin was almost given the tag of 'Bitcoin for good' according to Dave.

> The concern wasn't so much about being shut down; the concern was more I think about… the authorities not accepting it... People get really upset when you challenge the concept of money, that's one of the big lessons that I learnt… They think that money has value in itself when it doesn't, it's just a mechanism of exchange and if you start questioning that then people think it's somehow wrong or dodgy. (*Lisa)*

This is a fascinating quotation that speaks to many of the issues in this thesis. It seems to have become an almost unquestionable position that the state is the master of all matters money. The state must accept or tolerate any other form, and if anyone challenges conceptions of money, value, or how we exchange then this is invariably met with opposition. The founders purposefully had to design HullCoin as a system without *financial* value, in order to avoid a collision course with governmental authorities. The system only ever enabled a user to earn a discount on a good or service and so the coin had no financial value. From a regulatory perspective then, HullCoin was not money, and that enabled them to proceed. But the founders knew that they could still replicate the 'transactional relationship to money' (*Dave*) and that this would be a powerful tool in trying to gain traction and achieve a mass adoption that time banking and other local currencies had failed to achieve:

> Once people have done something and they go back to their accounts on the system and see that they have been credited with a balance, they feel that they have been paid. It feels like money. That's the psychology of money. So,

> we replicate the psychology of money within the system; the technology in terms of blockchain and Bitcoin, from the user side of things, is completely irrelevant. (*Dave* as quoted in Fernando, 2017)

To conclude this section, one enduring difficulty that the project faced should be mentioned, and that was how to value a single HullCoin if it was not pegged to a national currency, like a Bristol or Brixton pound. This will not be discussed in detail as it is moving off-topic, but it was an interesting wider finding in terms of this type of social project. The team did not want a HullCoin to be time-based, as in Civics, as they felt that doing a good deed would then be too much like work. Instead, they left the valuation to the organisations that distributed the currency and issued some guidelines, with the hope that the 'economy' would work out a value by itself. This was a topic of some note in the interviews and the business owner also showed some concern here. One hour of activity could be rewarded by one HullCoin or ten, depending on the distributor, and a business owner would have trouble working out how much discount to give for one HullCoin.

Without HullCoin having proceeded further it is hard to know if self-regulation would have solved these issues. But Bitcoin also has no pegged value, and this likewise leaves some struggling and questioning its 'inherent value' as discussed. What is one Bitcoin worth? In relation to the work of Simmel, this is not important for token money, and its use is as a facilitator of transactions – it has no value of its own. In this regard, the team perhaps did not need to give HullCoin a value and may have been able to let market forces decide. This was a difficult topic for the HullCoin team, but the fundamental idea was that the coin was backed by the community, rather than by something physical or a fiat currency, and it was up to them to work out what a HullCoin was worth:

> It's not backed by any commodity. It's backed by the community itself. (*Dave* as quoted in Fernando, 2017)

This is another deeply philosophical aspect to consider about the nature of money, particularly in relation to non-state monies. I have expressed my view that, due to the historical abuse of money by the state, we should try to conceive of possibilities beyond state money. But the question then is what ‘backs’ a money, can it only be the state, or could it be a community? This is one of the most important fundamental questions that has emerged from this thesis, and it will be deliberated further in Chapter 8.

7.2.4 Social Currency

> When you've got suppressed communities economically and you've got high levels of unemployment and you're also going through a programme of austerity, what you end up with is underused assets and unmet need. So, you've got a lot of people got time, they've got assets that they can use but they're lying dormant within those communities because the economy isn't able to accommodate those assets. But you've also got that unmet need within those communities because those people need services and need more support because of those organizations which would normally deliver those services are being cut. (*Dave*)

A paper-based complementary currency is simply a medium of exchange in the traditional economic sense. It is money but in a local area. The value is pegged to the national currency, and you spend it as you do fiat. HullCoin aimed to be completely different. The coins were ‘generated into existence through social outcomes’ (*Dave*) rather than swapped for fiat. In this way, they were targeted at the secondary economy where the unmet need could be met with unused resources. As Lisa explained, many councils do not receive all their expected council taxes, as some people do not have the fiat currency to pay the taxes due. But our societies do not then offer an individual any other way to pay back what is owed. And this is the idea of Civics. That person who may not have fiat might have the capacity to do a good deed in the community instead. But we do not utilise the secondary economy in society. We focus on measures of value that are economic and do not allow for other ways of social value creation.

In large part, this is likely due to orthodox economic thinking about money as an inert object of exchange, rather than the counter view of it as a force of its own. A perennial source of evil or a force for good (see Chapter 2)? Conceptions of money have never been allowed to stray far from the state form of money. The concept of Civics and HullCoin goes against the orthodox view and shows how money can be conceived of as a force for good. It was in this vein that the founders describe HullCoin as a social currency, rather than an economic one. Another interesting element of the HullCoin design enabled by cryptocurrencies was the concept of ‘social CVs’. The idea was that distributors of the coin could insert text about a good deed into a transaction for HullCoin. In this way, there would be a record on the blockchain of the history of good deeds that had been done. And, by way of a crucial difference, tokens would be generated as the result of a positive community deed, in contrast to the creation of money through increasing debt:

> Money is mainly generated by debt and [HullCoin] would be… something of value that was completely different, and it would be generated by positive social action which is much more valuable than debt. (*Lisa)*

Whilst the project faced some initial hostility from government departments as shown earlier, DWP later became a supporter of HullCoin and could see its benefits. Dave thought ‘we’d have hell with them’ but instead they had several meetings with the DWP. Their interest was two-fold. First, the government spends millions on making benefit payments to citizens. A blockchain-based payment system has the potential to reduce that cost significantly and create a direct monetary link between the state and the citizen. (Notably, this would cut the banks out of this part of the memorable alliance.) It is here that HullCoin aligns closely with the concept of UBI, where the state makes a regular universal payment to its people. Currently, citizens do not have bank accounts with the state, something which has gained increasing relevance since the outbreak of COVID-19. Many countries embarked on extensive support packages for their economies and, in the US for example, stimulus payments were made direct to citizens. But this was difficult and slow as there is no direct payment mechanism between the state and the citizen. Some recipients even received paper cheques sent in the post. A blockchain system or a CBDC could change this situation. The HullCoin team were aware of this potential, and this was another benefit of a cryptocurrency system. Many further opportunities could also be exploited if something like HullCoin was in place, such as UBI payments or in smart cities. In a smart city, for example, data and technology are used to enhance the running of the city and the quality of life (McKinsey Global Institute, 2018). With a fast, efficient payment mechanism established between government and citizens, this could be even further imagined. For example, micro-payments could be made to citizens who recycle well.

> [HullCoin] could be plugged into the Smart Cities agenda, I think, like Universal Basic Income. It pulls directly into it in terms of tech monetary reform and diversifying your economy, utilising technology to be able to do that. (*Dave)*

The second area of interest for DWP was the positive enforcement model that HullCoin offered. Currently, ‘we have quite the punitive, regressive sort of benefits system, welfare system’ (*Dave*) where the ultimate sanction from the state is to stop payments. The system does not have any mechanism to reward good behaviour. In this sense, the system is all stick and no carrot. A HullCoin model offers the ability to reward an individual for doing more than is required. For example, if a job seeker is required to apply for three jobs but applies for five, the individual could be rewarded with two HullCoin for the extra applications.

These concepts are important to this thesis as they help establish the benefits that can come from a complementary currency. The mindset that we saw in the narrative about cryptocurrencies, and as we have seen in the reaction to HullCoin, is that there is only one currency and that is the national, state currency. This chapter gives another example of how a complementary currency could be a benefit, rather than a threat. Not only this but there is a pattern that can be observed of the state reacting strongly to anything that moves in on its monopoly of money. Complementary currencies can be a helpful tool in building resilience in a financial system, as you do not need to rely on the strength of one currency alone. In this way, HullCoin aimed to help citizens in the secondary economy, especially in times when the primary economy is difficult. Complementary currencies may well also play a part in a future world based on UBI. If technology replaces enough jobs, then there will be a greater pool of unused resources – we may well soon live in a world where there are not enough jobs for everyone. A complementary currency enables those with capacity the opportunity to do something with their time and to earn more. These concepts may well have been purely theoretical but are becoming increasingly likely. UBI trials have been taking place across the world (Fairclough, 2021). And new imaginings of currencies will play a part in how these issues are solved.

7.2.5 Problems for Social Technology

Funding was a persistent problem for the HullCoin project and one of the main reasons why it did not launch fully. A theme emerged from the coding about how social technology can be funded but that is somewhat off-topic here. However, it is worth exploring some of this theme in terms of the reaction to HullCoin and social initiatives like it by the state. HullCoin found themselves in an endless cycle of applying for grants for the next tranche of money that would keep them going. Ultimately, this ran its course. As has been explained, the council were not going to have the resources to fund an initiative like this and neither would venture capitalists as there was no profit incentive. HullCoin, therefore, applied to various bodies such as the Lottery. One of the other issues that they faced in regard to funding, was that some of the funding bodies had more of a national vision for the project. That is, they wanted the scheme to be more than just a local system for Hull. This too presented difficulty, as the HullCoin project was being pushed to be more than it aimed to be. And visions for the project were often ahead of what they could deliver.

On the topic of funding, I asked whether they had considered running an Initial Coin Offering (ICO). ICOs are a controversial way for cryptocurrency projects to raise funds in exchange for tokens, due to scams and questions over their legitimacy. HullCoin did consider this method, but interestingly Dave mentioned that another Israeli group had subsequently run an ICO along similar lines as HullCoin. Called Colu, the organisation ran a blockchain project ICO that concluded in 2018. Colu and HullCoin did have conversations but there was a difference of opinion about how they should work. Colu was more like local money with a peg to the national currency. This was something that Dave was clear in his opposition to. With a peg in place, the HullCoin argument was that earning the coin was tantamount to work, and with that would come complications with the monetary authorities. You could not combine HullCoin and a pegged local currency into one system. This proved to be a wise point of view (and the position of Civics).

In 2019, following the launch of the Colu project in cities including London, Liverpool, and Tel Aviv, Colu announced that they were moving away from blockchain and would buy back the tokens they had issued. The reasons given were due to regulatory uncertainty, technical challenges and other non-blockchain opportunities (Kuhn, 2019). Then in 2020, Colu made another announcement that they were closing down their digital wallet app and returning funds to customers. Colu's CEO is quoted as saying that the Israeli Payments Services Law allows 'only the banks operating their payments companies, such as Bit, and Apple Pay and Google Pay [to] remain' (Berkovitz, 2020).

There is not enough evidence to suggest that Colu was forced out of the Israeli market intentionally, nor can it be said that it was done to protect the memorable alliance. But the outcome of events was to protect the traditional financial system. Again then, there is evidence of smaller, non-state money, social-good initiatives being excluded from innovation in the monetary arena. Lisa commented in interview that cryptocurrencies do not pose a threat, and had this response to a question about what the threat is that governments are concerned about:

> I think it's control. If people choose to exchange without big banks and government then that is a potential threat [to the system]. But actually, then you know they're not really doing it, I think it's just a fear. (*Lisa)*

In securitisation theory, it is hard to pin down exactly what is threatened in the economic sector. It is easier to identify 'who' securitises things, but it is less clear as to what the referent object is that is existentially threatened. For now, though, it is fair to claim that non-state social initiatives are often met with some kind of state resistance. As another example, in 2013 a complementary currency called the Bangla-Pesa was introduced in Africa by a former Stanford physicist, who was also inspired by Lietaer. Following a familiar securitising media article suggesting a connection between this new currency and terrorism, the founders found themselves in jail and they subsequently ended up spending more on legal fees than they did on the project. Eventually, the project was deemed legal, and it has now also moved to a blockchain model for transparency (Herbst, 2019). It is interesting to note another project recognising the benefit that a cryptocurrency model brings, but also the clash with the state that the project endured. New monetary initiatives invariably seem to encounter these types of problems and securitisations:

> I think that there will be, has been… a lot of resistance [to cryptocurrencies]. I think people should be able to trade in whatever mechanism they want to trade as long as that's fair and they're aware. But that's why I think… money in itself is at its heart corrupt and the way that money is generated is generally through debt, people don't understand that. People don't understand the origins of money, how it works and how it works for the few. So, I think it's a corrupt system. I think that… anything that would disrupt that corrupt system is going to meet resistance. (*Lisa)*

Whilst there was no overt 'rebellious' intent seen on the part of the HullCoin founders, this quotation does indicate Lisa's view of the existing financial system. And that view, like Lietaer's, is that a state-centric system benefits the few and society could well benefit from complementary forms of money. In a similar finding to the law enforcement chapter, neither of the HullCoin founders thought of cryptocurrencies as a particular threat and saw them more as a technology that could be used for illicit purposes, like any other tool. They did not think that they were a device simply for criminal activity:

> That's been levelled [at cryptocurrencies] loads but it's an exchange mechanism or a store of wealth and just like any exchange mechanism or store of wealth it can be used for whatever purpose. I don't think there's many arms dealers or people abusing sex workers that are using Bitcoin. I mean there might be arms dealers, I'm not sure about that one, but I don't think on the street people buying drugs and you know kerb-crawling are using Bitcoin. The exchange mechanism itself is not the issue, it is humans and the way that they use things is the issue and that happens with any exchange mechanism. (*Lisa)*

The view of cryptocurrencies displayed by both of HullCoin's founders is very much like the ambivalence to technology that the law enforcement officers displayed. And similarly, Chapter 4 shows that an overwhelmingly greater amount of crime is facilitated by the existing financial system and cash than is conducted using cryptocurrencies. Dave also expressed the view that money laundering takes place using established methods and that cash remains the tool of choice on the streets as it 'is pretty untraceable'. Both founders were aware of the narrative that follows cryptocurrencies and were clear in not accepting the link between cryptocurrencies and crime. Similarly, neither thought that cryptocurrencies should be securitised.

Significantly, DWP was supportive of HullCoin. The interview questions asked the founders if DWP had security concerns about HullCoin or whether the talk of cryptocurrency bans had an impact on the project. DWP only wanted to know that the system itself was secure (i.e., concerning funds/coins), there was no specific concern about the use of HullCoin for crime. Similarly, there were no issues for the project in relation to any potential bans of cryptocurrencies. HullCoin then, as a copy of the Bitcoin code, was not labelled as a security threat.

Dave commented that 'the psychology of the human race is wedded to money as an exchange mechanism, and it would take quite a lot for that to be moved in a new direction'. This relates once more to the economic view of money, where others have tried to move the view of money as a force of its own. It will likely take a huge shift in our perceptions of money for councils, politicians, and others to accept that a monopoly of money is not the only way for the financial system to exist. Lietaer's Civics, the Bangla-Pesa, Colu, HullCoin and the thousands of other complementary currencies all aim to create a fairer, more robust system that gives more opportunity to individuals in deprived areas. It will be hard to ever achieve these aims without breaking some of the age-old conceptions of money.

7.3 Conclusion

This chapter provides a case study of the world's first local cryptocurrency, HullCoin. In doing so, two new perspectives on cryptocurrencies are provided. First, cryptocurrencies are shown from a community viewpoint, rather than the individual user perspective which is mainly seen in Chapter 2. And second, this research strand explores how cryptocurrencies can be employed for legitimate purposes beyond their prominent use as a speculative vehicle.

The background section on the history of money shows that there have been centuries of debate about the form of money and the functioning of our financial systems. Scholars, economists, and politicians continue this discussion to this day. It is beyond doubt that the system is flawed but it will be very hard, if not impossible, to reach a consensus on what to do about it. Throughout the thesis so far, a pattern has emerged of resistance to any new system that challenges the position of the memorable alliance. How much this is conscious I do not know. And there are only a handful of people amongst the memorable alliance that could answer that question. The motivation for the HullCoin team was to help reduce poverty in their town and it was only through the careful design of HullCoin to not be money that they managed to avoid significant resistance themselves. If the existing financial system works for the few, what incentive is there for accepting new ways of doing things? And this applies to Bitcoin, perhaps even more so than HullCoin.

The results show that HullCoin was met, predictably, with two initial reactions. There was concern shown by some that HullCoin was not ‘real’ money. This speaks to the old debate about the physicality of money versus Simmel’s conception of token money. Some people find it hard to conceive of money if it is not either state money or backed by something physical. HullCoin was also met with initial hostility from some government departments as it encroached on the status quo of state money. Interestingly though, the team managed to navigate these difficulties by designing HullCoin specifically as ‘not money’. This enabled them to exist in a grey area and avoid any collision with the state. It was also interesting that the project hid any reference to blockchains from the public and that this model was chosen solely because it offered them the best way of achieving their goals. The motivation for using a cryptocurrency had nothing to do with libertarianism, anonymity, decentralisation, or any of the other main properties that often describe cryptocurrencies. And this contrasts with some of the findings of other user studies discussed in Chapter 2. A cryptocurrency model had technical advantages over a traditional paper-based alternative. It enabled a quick and cheap way to monitor transactions and offered a suitable level of transparency for a Civics-inspired project. In this way, blockchain technology was providing a real-world solution to a problem and a cryptocurrency was being used for a legitimate, beneficial purpose.

At no point was HullCoin labelled as a security threat nor were there ever any concerns raised that it would be a tool for criminality. And yet, HullCoin is based on Bitcoin’s code. If they are effectively the same thing at their core, why do they receive different levels of treatment? Scale is an obvious first answer, that one is small and local whereas the other is known across the world. But the difference is possibly also about the narrative of users that reflects back on the cryptocurrency. HullCoin was presented as a local token, there was no stated aim of a challenge to the national currency. And for this reason, it constituted no threat to the established financial system, and it was tolerated. There were no securitising actors.

As we have seen in this chapter, though, and throughout this thesis, money is an evocative subject. The debate about money is fierce and discussion is often heated and unresolved. It will be hard, as the founders of HullCoin note, to change people’s perceptions of money. There is still a fear of ‘magic tokens’ and it is hard to establish a complementary currency, even though the theory and benefits of such a system are well known. Across the world, projects continue to try, but whether it is HullCoin, the Bangla-Pesa or Colu, the result has been to run into difficulties. And yet, all these projects set out with honest aims of trying to help the poorest in society. Chapter 2 described the flaws of the current financial system and noted that it often benefits the few. Perhaps social technologies can help with these issues, but they need to be allowed to do so.

8 Conclusion

In 2017 as I began my PhD programme, I became aware of many headlines discussing the criminal use of cryptocurrencies and the great threat that they pose. As a former law enforcement investigator, I was intrigued by the central paradox that inspired this study – why would a payment system with a permanent and openly-accessible record of all transactions be advantageous for illicit activity? Many of the debates about cryptocurrencies that I encountered in 2017 are still as popular today. And cryptocurrencies continue to be divisive, with many critics and supporters alike. Money is 'the pivotal institution of modern capitalism' as Ingham explained (2020: 18). With that being so, this research topic is of great importance as money underpins and shapes society and how our world functions. It plays a critical role geopolitically (wars are funded with money), money is key to power but also integral to personal aspects of freedom, equality, and future security. New forms of money may well play a part in the future of money, so it is vital that they are not dismissed but instead, are researched thoroughly to inform the debate as society moves forward.

I began researching cryptocurrencies in 2018 after they became much more prominent following the 2017 boom. Although my interest was initially in the illicit use of cryptocurrencies, the topic drew me ever deeper into the underlying debates and issues about money that have existed for centuries. Using the lens of securitisation theory, I conducted four main strands of research, which align with the four research sub-questions, in order to inform the central research question:

> To what extent and for what reasons has the state or its representatives attempted to securitise Bitcoin and other cryptocurrencies?

This chapter begins in Section 8.1 with a review and discussion of the empirical chapters and the research sub-questions. This highlights the main contributions of each strand of research at a chapter level. In Section 8.2, we zoom out to consider the central research question in the context of securitisation theory and the economic sector. Here, several deductions about the overall thesis are made and discussed.

We then return for a final time to consider Bitcoin and cryptocurrencies in terms of the core issue of money and its place in society. The final sections of the chapter from 8.3 onwards conclude the thesis with a review of its contributions, limitations, a number of policy recommendations, and some suggestions for future work.

8.1 Research Summary

8.1.1 Chapter 4: The Security Narratives

1. How are security-led narratives about the use of cryptocurrencies constructed and to what extent are they justified?

Chapter 4 serves as a foundational part of this thesis and is structured around the two halves of the research sub-question. First, the chapter captures and explores some of the security-led narratives that exist about cryptocurrencies. Section 1.3.1 described why securitisation theory was chosen as a theoretical lens for this research. As a prominent theory that has been applied widely in security studies, it provides precise language and a coherent, central structure for the analysis of the threats that cryptocurrencies potentially pose. Core to the original Copenhagen school theory is a focus on ‘who’ the securitising actors are and an examination of their speech acts. The US dollar is the pre-eminent global fiat currency and so the focus was on US officials as the most important actors. Document analysis was used to highlight media reporting of the views of these officials.

Whilst several threats were commented on, including threats to power and concern over investor protection, criminal usage emerged as a constant and prominent justification for opposition to cryptocurrencies. This part of the chapter was not an exhaustive review of every speech act but served the purpose of establishing that the speech acts exist, and that criminal usage was persistent grounds for objection. It is also important to mention that this part of the chapter was influenced by Ingham’s conception of the memorable alliance (of the central bank, the treasury, and the private banks) as the axis of modern-day capitalism. It was, therefore, of particular interest to see what the Chairman of the US Federal Reserve, the US

Treasury Secretary and the leaders of the largest US banks had to say on the subject. Whilst these individuals raised concerns about the illicit use of cryptocurrencies, it was interesting to note that some US law enforcement officers did not feel the same way – that is, they were happy for criminals to use cryptocurrencies as they offered opportunities for investigation. If law enforcement did not view cryptocurrencies as a threat, then why would the memorable alliance claim they were a threat on the grounds of illicit usage?

This question, in relation to securitisation theory, speaks to the need for the securitising actor to 'make their case' or justify their claims for labelling something a threat. The second part of the chapter, therefore, examined the extent to which cryptocurrencies are used for illicit activity. If the evidence showed that cryptocurrencies were responsible for or used in an overwhelming shift in illicit activity, then this would support the speech acts and justify their claims. A wide range of sources was examined from academic research and organisations such as the UN and Europol to assess the extent that cryptocurrencies are used in illicit activity. The dark net was focussed on, as it is often a feature of the reporting about the use of cryptocurrencies. As this part of the chapter also served to establish some knowledge for the rest of the thesis, it was again suitable to make use of documentary analysis of reporting and research that already existed. The results were significant.

Cryptocurrencies were used in a small amount of overall crime and the percentage of illicit transactions was also small and declining. Indeed, the majority of cryptocurrency usage is legitimate. This trend has continued, as shown in the 2022 Chainalysis Crypto Crime Report. Cryptocurrency crime reached a high of $14 billion in 2021, nearly double the $7.8 billion in 2020. However, during this time transaction volume grew over 500 per cent to $15.8 trillion. That is, legitimate usage is far out-pacing illicit. In 2021, just 0.15 per cent of cryptocurrency transactions involved illicit addresses, although the true figure is likely somewhat higher (Chainalysis, 2022). But again, it must be stressed that $14 billion is a small figure in global crime. The UNODC estimates that just one crime type, money laundering, amounts to '2 - 5% of global GDP, or $800 billion - $2 trillion' (United Nations Office on Drugs and Crime, 2022). Likewise, dark net markets also only represent a small part of the drug trade in particular.

Strikingly, the research highlighted that cash (state-provided money) remains king for criminal activity. Traditional finance is also used for significant amounts of crime. NatWest, for example, was recently fined £265 million after failing to prevent £400 million of money laundering by one firm, with £700,000 in cash even being deposited at a branch in black bin bags (BBC News, 2021b). If physical cash is provided to criminals by governments in a process known as ‘reverse money laundering’ and is king for criminal activity, why do governments express concern over cryptocurrencies for this same reason? The evidence suggests that they are not justified in doing so or, at the very least, that there is a contradiction in the memorable alliance attempting to securitise cryptocurrencies due to criminal threat, yet at the same time providing cash as the premier criminal tool. If cash is accepted in the physical world despite its criminal usage, then why should there be such an objection to cryptocurrencies as a cash-like money in the digital world, especially if it represents less of a threat as shown by the analysis? This does not make sense unless of course there are deeper explanations.

8.1.2 Chapter 5: Cryptocurrency Usage on the Dark Net

2. What evidence is there that cryptocurrencies are actually useful for illicit activity?

Despite the prominence of illicit usage in debates about cryptocurrencies, Chapter 2 revealed little to no research about this area. There have been several sociological studies looking at individual perceptions and experiences of cryptocurrencies from a legitimate perspective, and they were typically researched using surveys and interviews. This chapter contributes to this illicit usage gap and adds further understanding to the findings of the previous chapter. Given that cash was revealed as the prominent tool for illicit activity, how useful are cryptocurrencies for that purpose given the properties that they have, especially in contrast to cash? To answer this, a qualitative and constructivist approach to the methodology was chosen. There has been a lot of technological research about cryptocurrencies but less from a qualitative standpoint. As the narrative about cryptocurrencies has often been speculative and third person, Chapter 5 sought to explore what users said for themselves about using cryptocurrencies for illicit purposes and their properties, rather than the likes of the Chairman of the US Federal Reserve.

With ethical considerations in mind, the best and most appropriate method was to research an existing dataset of underground and dark net forum posts scraped from the internet over a long period. An agreement was reached with the Cambridge University Cybercrime Centre to use their CrimeBB dataset of over 100 million posts. Using a three-part methodology, 16,405 posts of interest were selected and analysed in QDA Miner Lite, a qualitative analysis tool. The ethical considerations significantly affected the presentation of results, as verbatim quotations were not used.

Four main findings emerged from the analysis of the posts. First, anonymity is not the major advantage of cryptocurrencies for illicit use as is often portrayed. Instead, the finality of transactions came to the fore as the second main finding. These first two findings challenge established assumptions and show the value of qualitative research on this subject. Particularly in illicit activity, where trust is most difficult to achieve, users wanted and needed a payment system that could not be reversed and that was free for anyone to use. Bitcoin met that brief and traditional finance did not, where the likes of PayPal excluded people due to geography and age or froze funds in disputes. These results also explain why Bitcoin remains ubiquitous on dark net markets, as anonymity is not necessarily what it provides.

Third, there are seven main areas of security that an illicit user must consider in order to transact relatively securely on the internet, as illustrated by the taxonomy in Figure 5. The payment mechanism is but one, hence why it does not ‘solve’ anonymity. An anonymous payment protocol is not of much use if you have to reveal your identity to use the system or to receive goods for example. Thinking about the illicit use of cryptocurrencies has often, therefore, been too abstract and removed from the real-world considerations and issues that an illicit user must face. And this likely overstates the usefulness, and ease of use, of cryptocurrencies for illicit activity.

And finally, the research showed that using dark nets is hard. It does not enable the purchase of drugs, for example, at the click of a button. Dark net markets are small relative to global trade, and fear of them is overexaggerated and has likely transferred onto cryptocurrencies as a result. Banning cryptocurrencies is unlikely to be effective; determined users will switch to another payment mechanism, some of which are already established and proven. Or they will find a way to continue using cryptocurrencies. The dark net is, therefore, a niche; it is not an existential threat. Furthermore, any ban would push cryptocurrencies underground and, in a type of security dilemma, would remove the opportunity for law enforcement that exists in trade that is legal but tightly regulated. The security dilemma traditionally refers to a situation where a state tries to increase its security but this comes at the expense of lessening another state's security, which can exacerbate problems (Jervis, 1978: 169). Interestingly, fear is the 'ultimate source' of a security dilemma (Tang, 2009: 590). If fear is a key source in relation to the use of cryptocurrencies on the dark net, then there may well be a dilemma that arises by pursuing policies trying to strengthen security in an area that is ultimately a relatively small threat.

Overall, these results help explain the contradiction between the memorable alliance and law enforcement, and the difference in the narrative about cash and cryptocurrencies. Bitcoin is not as anonymous as cash but, in many respects, has proven to be the next best thing on the internet for illicit transactions. Is it 'great' for illicit activity? The answer is a predictable yes and no. Yes, in that it proved to be a useful payment mechanism, offering finality and open access to those cut off from traditional finance; in the lexicon of the Technology Acceptance Model, it had a utility that led to adoption. No, in that using cryptocurrencies for illicit activity is difficult, they are traceable and the dark net itself can be an inhospitable place. Even privacy coins do not solve the anonymity problem; users must still cash in and out and must also overcome significant barriers to use cryptocurrencies relatively safely, as shown by the taxonomy. So, cryptocurrencies are useful for illicit activity but only to a point, as they come with significant difficulties that are not to the advantage of the illicit user. They leave a permanent trail and present opportunities for law enforcement. As a recent example, two people were recently arrested for the 2016 hack of the Bitfinex exchange and the theft of over 100,000 Bitcoin. The funds have been monitored ever since the hack and, despite obfuscation efforts, the perpetrators eventually faced justice (Elliptic, 2022).

In several ways, then, cryptocurrencies are less of a useful tool than physical cash, which supports the position of cash as king for criminal activity. Yet the narrative appears to support the reverse of this view. Part of the explanation for this disparity is a general fear that surrounds cyber security and, in relation to cryptocurrencies, their use on the dark net. Chapter 4 also showed that the fear and perception of the dark net as a key and significant location of illicit activity goes far beyond the reality of its scale and the volume of trade conducted on it. If dark net markets are small, then again, the fears about the use of cryptocurrencies on them may be similarly out of proportion.

Together, Chapters 4 and 5 analyse the criminal threat that cryptocurrencies pose, supporting each other in concluding that the threat is not as significant as the headlines suggest. It is government-produced cash and the traditional financial system that continues to afford and host the majority of illicit activity. In this regard then, Chapters 4 and 5 do not support the securitising claims of the state or its representatives. The scale and usefulness of cryptocurrencies for illicit activity force us, therefore, to question whether they can be thought of as an existential threat, or whether they are truly deserving of special measures. Section 8.2 answers these questions, drawing on the perspectives of the remaining empirical chapters in support of the wider thesis conclusions.

8.1.3 Chapter 6: From the Perspective of Law Enforcement

3. To what extent do law enforcement opinions and experiences of cryptocurrencies support or contrast claims for their securitisation?

If the properties of cash are more useful for crime than cryptocurrencies, primarily through greater anonymity, and if the volume of cryptocurrency crime is small then is the view of the DEA agent in Chapter 4 representative of the law enforcement view more generally? If the CrimeBB analysis showed the view of the actual users of cryptocurrencies for illicit purposes, then the law enforcement chapter aimed to do the same from the other main party primarily involved in illicit activity. Whilst the focus was on the US in Chapter 4 as explained, for Chapter 6 I had the privilege of being an ‘outside-insider’ to UK law enforcement. An assumption made was that UK law enforcement officers’ thoughts and experiences of cryptocurrency investigations would likely be similar to other nationalities. Given the difficulty that there is accessing these participants, I thought that UK law enforcement officers would be the most appropriate subjects to research.

Interviews were selected as the method for this part of the study as the aim was to conduct in-depth research on participants with good working knowledge of the illicit use of cryptocurrencies. There are only relatively small numbers of officers that have deep experience in this area. The purpose of these interviews was to add to the knowledge gained from previous chapters but, crucially, to also investigate the DEA finding further to see if UK law enforcement officers were concerned about the use of cryptocurrencies in illicit activity. And if they were, did this explain why this area was used as a justification for an attempted securitisation? In this way, the findings speak to the research sub-questions of the previous two chapters as well.

There were again several main findings. The officers displayed ambivalence to technologies used in crime. They viewed cryptocurrencies merely as a tool, in the same way, that they might view the internet as a tool. Cryptocurrencies were not seen as a security threat in their own right – the threat was the individuals or groups that use the tool. The results of the interview analysis also showed that the officers predominantly thought that cash was a greater security threat than cryptocurrencies, although there are advantages of cryptocurrencies over cash such as moving large amounts of value. This again ties in with the findings of the previous empirical chapters. And finally, the interviews revealed significant findings about the dark net. Online transactions remove the ability for physical recourse and in this regard can be disadvantageous for illicit activity, supporting why cash may often be preferred in the real world. Furthermore, this explains why the dark net is mainly suitable for low-level activity, such as retail drug trading rather than anything more substantial.

Overall, it does not appear that law enforcement is part of the ‘who’ that is attempting to securitise cryptocurrencies. None of the law enforcement participants thought that cryptocurrencies were as big a threat as portrayed, and none saw them as a security threat overall. This, of course, then begs the question why have politicians and figures in finance used crime as grounds for securitising? Perhaps it is just a case of misplaced fear, or a lack of understanding of the scale or usefulness of cryptocurrencies, particularly in comparison to the provision of cash. This question would benefit from further research. Efforts were made to contact individuals in the financial sector, but I was unsuccessful in finding any participants for interview. It will be difficult to access these communities, so this is beyond the scope of this work. But as I argued for the need to research law enforcement officers themselves, so too does this logic apply to politicians and those in traditional finance. Whilst they cannot be spoken for here, the building analysis of this thesis is suggestive of certain conclusions regarding the threat that cryptocurrencies pose, and this will be explored further in the remainder of this chapter.

In Section 2.1.3, Ingham’s concept of the ‘memorable alliance’ was introduced; of the government, the central bank and traditional finance (primarily banks) (2020: 68). This is the ‘who’. The memorable alliance has been labelling cryptocurrencies as a security threat and they have done so to protect their referent object. Since I was not successful in interviewing anyone from the memorable alliance, it is not possible to provide their perspective on what the referent object is, but deductions can be made. The referent object is likely the existing financial system – or certain elements or benefits that come from the alliance such as control, wealth, and power. Cryptocurrencies threaten that, and this better explains the attempted securitisation of cryptocurrencies than any desire to fight crime or protect investors from scams. And this is the very same referent object that has been fought over for hundreds of years.

There is no doubt that there are law enforcement officers and those in the memorable alliance who have legitimate concerns about cryptocurrencies, whether they be to do with harm to the public or notions of power. And so, the analysis here is theoretical, rather than a sweeping conclusion regarding every individual. One of the officers, for example, notes a general desire to protect the public.

Cryptocurrencies are used in crime and, since 2017 in particular, there has been a great deal of scam activity around cryptocurrencies. There is no doubt genuine and welcomed motivation to stop this kind of activity.

However, one of the officers noted that cryptocurrencies have driven large amounts of finance, such as remittance, away from other established sectors. And in another comment, the current financial system was identified as the thing that is threatened by cryptocurrencies. That is, the current financial system is the referent object that politicians and figures in traditional finance are protecting:

> The threat is above and beyond the volume of… the commodities, be they child sexual abuse images or drugs that are traded on it, because it is an existential threat to the state and to the state's backing of its own currency and its ability to control what is and isn't sold within its borders. (*Officer 2)*

Another officer also names the control of traditional financial structures as the referent object, where the goal is ‘to protect the status quo’. Perhaps it is this that is at the heart of any attempted securitisation of cryptocurrencies, not the threat of crime to a referent object of law and order, or even the protection of citizens from financial crime.

8.1.4 Chapter 7: HullCoin - Cryptocurrencies in Civil Society

4. What prognosis is there for cryptocurrencies to play a valid role in money and society?

The HullCoin chapter was initially conceived as a means of providing some balance to the previous chapters by exploring the ways that cryptocurrencies could be used by people and communities for lawful and beneficial purposes. If the overwhelming amount of cryptocurrency activity is legitimate, in what ways are they useful and can they add value to society? As Moore and Rid intimate, if the legitimate is greater than the illegitimate then perhaps the benefits outweigh the costs (2016: 9). A lot of the sociological studies examined in Chapter 2 focussed on individual experiences of using cryptocurrencies for legitimate purposes. Chapter 7 took more of a community-level perspective as there was far less research of this type.

HullCoin was described as the world's first local government cryptocurrency, and a case study was chosen as the most appropriate way of exploring this innovative community project. Travel to Hull was originally planned but was not possible due to the pandemic. However, as the project had reached its peak in 2017, it did not get as far as becoming established in the community and so the inability to travel to Hull was not overly problematic. As a result, in-depth interview of the two main founders was chosen as the primary research method for investigating the project further. Several interviews were conducted with the two founders, and a business owner who had been involved in some early trials was also interviewed. This material was then augmented with some further documents from the time of HullCoin's advent and the subsequent peak of exposure. Together, these resources were analysed in Nvivo.

The findings and learning from this case study proved to be influential in terms of the overall meaning of this thesis, and more so than originally envisaged. One of the main findings from the case study was that HullCoin was based on Lietaer's Civics and that cryptocurrencies were a useful tool for implementing this kind of social technology project which would normally see little in the way of investment. Cryptocurrencies offered a cheaper way of delivering Lietaer's concept of a complementary currency, and this model has been adopted by several other similar projects across the world. Importantly, complementary currencies have existed globally in many forms. There have also been successful periods of free banking, and even other types of money such as IOUs. The idea, therefore, that state fiat is and has been the only option is a false one. In the eyes of the founders, HullCoin was a social currency, backed by the community rather than the state. And the evidence suggests that there is much good that can come from complementary financial systems. In this way, there is hope, or at least promise, that cryptocurrencies could have a positive role to play, like these other forms of money, if allowed to do so.

Significantly though, another key finding was that HullCoin, and similar projects elsewhere, faced resistance from the state. There was an initial fear of HullCoin and opposition to it appeared to be related to worries that HullCoins were ‘magic tokens’. This relates to the prior discussions in this thesis about the nature of money, including consideration of Simmel’s work. The interesting observation is that token money is an ideal form and that Bitcoin or HullCoin are no more ‘fake’ than the fiat currencies of nation-states. The only difference being that fiat is decreed by law, returning us once more to the fundamental issue of whether money must be the preserve of the state. Crucially, criminal usage was never discussed as part of any concern regarding HullCoin. The issues related to whether HullCoin was money and the impacts that might have. It was only by designing and presenting HullCoin as ‘not money’ that they were able to proceed, and in due course, they even received some interest from government departments. This last point has particular significance given that HullCoin was a project fork of Bitcoin. The code may have had the same origin, but the experiences and reactions to these two projects were ultimately very different.

With this in mind, the contentious part of Bitcoin and cryptocurrencies in terms of the state is its relationship to money, not crime. This supports the evidence of Chapter 6 and the view that law enforcement is not part of the ‘who’. Furthermore, it strengthens the notion that the referent object in terms of the state is related to money. The chapter showed other examples of complementary currencies that have been securitised or at least ceased to exist, as a result of state intervention. But despite the flaws and inequalities in the existing financial system, and the benefits that come from having multiple currencies, alternative or complementary monies often struggle in their relationship with the state. Yet people, like Lisa, have challenged the idea that money can only be generated through debt and shown that there are other conceptions for the future of money beyond ever-increasing debt based on state fiat. And Lisa, too, like some of the officers in the previous chapter, points to the existing system as the thing that the state will resist any challenge to. The prognosis, therefore, for cryptocurrencies to play a valid role in money and society is mixed. It is good in terms of the potential for these systems to be useful for people at an individual and community level. But whilst dated conceptions of the nature of money and the state’s role in money exist, complementary, and certainly alternative monetary systems, are likely to continue to be met with opposition.

8.2 Discussion

> The future design of crypto systems should be informed by hard-nosed political and technical considerations. A principled, yet realistic, assessment of encryption and technology more broadly is needed, informed by empirical facts, by actual user behaviour and by shrewd statecraft – not by cypherpunk cults, an ideology of technical purity and dreams of artificial utopias. Pragmatism in political decision-making has long been known as realpolitik. Too often, technology policy has been the exception. It is high time for cryptopolitik. (Moore & Rid, 2016: 30)

The purpose of this study was to examine and explore an apparent securitisation of Bitcoin and cryptocurrencies. The research chapters applied Moore and Rid's cryptopolitik to the question about the security threat of cryptocurrencies to ensure that it is informed by empirical facts, by actual user behaviour, and not by uninformed narratives or by focusing on cults or utopian dreams. In doing so, this thesis has explored the extent to which cryptocurrencies are a security threat from many perspectives. The previous section presented several new results which give a deeper understanding of what is invariably a nuanced subject.

Cryptocurrencies need cryptopolitik; they need to be assessed rationally and empirically, as securitisation theory highlights the price that is paid for excessive treatment above normal politics. It is de-democratising, stifles innovation and draws resources from more pressing threats. It is for these reasons that the results of this thesis are important. And the results should help us determine whether cryptocurrencies ought to be the focus of extraordinary measures or whether they should be moved from the arena of security to that of normal politics. It is not possible to answer whether cryptocurrencies are a threat with a simple yes or no, as the answer depends on the perspective of the subject answering the question and on the many intricacies of the arguments involved. For this reason, however, securitisation theory is particularly useful, as it gives us a framework around which some answers can be built. There are several significant findings from this study that inform the overarching research problem, and, in this section, we zoom out from the results of the empirical chapters to consider the central research question more deeply through the lens of securitisation theory and the economic sector.

> To what extent and for what reasons has the state or its representatives attempted to securitise Bitcoin and other cryptocurrencies?

In securitisation theory, a ‘case’ has to be made by the securitising actors and the previous chapters have served to gather the evidence from the relevant parties. We have seen what the memorable alliance has said of cryptocurrencies, what users and law enforcement officers think of their use in illicit activity, and we have also seen how a cryptocurrency model was used positively in a community project. With these differing perspectives established, it is now possible to analyse the security threat of cryptocurrencies more deeply, especially through the lens of securitisation theory. To continue the analogy, we can now move on to consider the findings.

The empirical chapters suggest that the issues with cryptocurrencies are more about money than crime. In this section, therefore, we first return to securitisation theory to consider what this means in the economic sector. Securitisation theory helps us define what constitutes a security threat and also identify what the likely referent object is. In Section 8.2.2, we consider if cryptocurrencies could legitimately be considered as an existential threat but also widen the discussion beyond the original theory to highlight further potential evidence of attempted securitisation. Having done this, the remaining sections return to the topic of money more directly. Section 8.2.3 considers why there has been an (attempted) securitisation and whether there is an opportunity for cryptocurrencies to be reframed as a useful part of a more stable monetary system. We then move back to the issue of trust to see if Bitcoin could perform a role in money. Finally, in Section 8.2.5, the discussion concludes with a refinement of Ingham’s money question to clarify what the real issues in money are and with a consideration of what this means for society and the future of money.

Society continues to wrestle with questions of liberty and security. ‘There is a consensus among critical scholars that the amount of social life that is governed by ‘security’ claims has increased since 9/11 — but not all securitizing moves have been successful' (M. B. Salter, 2008: 330). Revelations about the increasing intrusion of the state, such as in the Snowden leaks, have raised more questions about the balance between claims for 'security' and liberty. As such, we need to take care in our response to perceived threats (Amoore & De Goede, 2005). Or, at the very least, continue to look for ways 'out of the impasse of security'.

8.2.1 The Economic Sector and The Referent Object

Buzan et al. reason that positions on economic security 'reflect different views about whether states and societies or markets should have priority and whether private economic actors have security claims of their own' (1998: 95). The two broad positions of opposition are between the mercantilists, where economies are used to empower the state, and the liberals, who argue that the market should operate freely and unimpeded by the state (95). These positions are familiar to us and reflect the conflicts in monetary theory, as examined in Chapter 2. There too, the tension lies between the statists, such as Knapp and his state theory of money, and the Austrian theorists, such as Hayek, who argued for less state interference in money and the freedom of competing currencies. Again then, the literature draws us towards state centred debates about money and the economy, rather than to existential threats related to criminal use of a new money.

Interestingly, Buzan et al. note that 'it can also be argued that liberalism is about protecting the position of the capitalist elite'; and it is liberalism that has shaped economic security discourse since the end of the Cold War, marginalising the economic nationalism of the mercantilists and socialists (1998: 96). The suggestion that liberalism is also about protecting the position of the capitalist elite is fascinating given our discussion of the memorable alliance and 'who' is labelling cryptocurrencies as a threat. It also speaks further to our as yet unresolved question of the referent object that needs protecting from cryptocurrencies:

> The liberal ideal is ultimately to dissolve national economies, with their exclusive currencies and restrictions on factor movement, into a global economy with relatively few restraints on the movement of goods, capital,

> services, and (more hesitantly) people. The problems are how to maintain economic and political stability and how to handle the widening gap between the very rich and the very poor that unrestricted markets tend to generate while simultaneously removing many powers and functions from states. (Buzan et al., 1998: 96-7)

This quotation gets to the crux of the issues around cryptocurrencies; there is a conflict between the liberalisation of economies in a globalised world and the loss of power and control that this brings. How can a state control its domestic economy, yet be part of a wider global economy? How can a free market be encouraged that is unimpeded by the state, yet simultaneously allow retention of the power and functions of the state? These are inherent contradictions. And in the same way, if the liberalist ideal is for a free global market, then surely this would benefit from a global currency free from the interference of the state, free from the Triffin Dilemma – an idea proposed as far back as Bretton Woods in 1944. It seems that it is hard for states to let go of the state conception of the world, even in the face of a conflicting ideal. National economies and exclusive currencies cannot be dissolved without a re-conception of society and the state-centric view of the world. Buzan et al. note that ‘It is often difficult to separate attempts to securitize economic issues from the more general political contest between liberal and nationalist approaches to economic policy’ (99). And consequently, they ask, ‘how much of what is talked about as economic security actually qualifies for that label’ (99)? This is a central question in the economic sector of securitisation theory, and it relates closely to the central research question of this thesis.

To answer this, we must first consider the security actors and referent objects in the economic sector. Although the state is rooted ‘in the political and military sectors, it is one of the major units in the economic one’ and ‘states far outshine firms and classes as the principal referent objects of economic security’ (100-01). This is interesting, as the theory also supports the analysis in this thesis that the referent object is more likely the state (or a part of it) rather than individuals who need protecting, for example, as a result of scams related to cryptocurrencies. Individuals, classes, and firms can be referent objects but often to a lesser extent. Firms, for example, struggle to be classed as a referent object, as a feature of the capitalist system is that they should be subject to market forces. Banks, though, have been considered as an exception to this, and we are familiar with the term ‘too big to fail’ in reference to the perceived threat to the international financial system should they collapse. (It should be noted that Lehman Brothers was allowed to go bankrupt during the Great Financial Crisis). Subsystem and system-level objects are also identified as potential referent objects. Inter-governmental organisations (IGOs) such as the World Bank or the EU are ‘relatively concrete’ but the objects can also be abstract such as the liberal international economic order (LIEO) (102). These abstract and higher-level conceptions of referent objects are of great interest given the role of the memorable alliance as the axis of the capitalist system as discussed in Chapter 2:

> These higher-level referent objects are typically securitized by officials of the IGOs or by representatives of states, industry, or capital with interests in their maintenance. (Buzan et al., 1998: 102)

Cryptocurrencies have been labelled as a security threat by representatives of the state, industry and capital, and it makes more sense that this is in protection of their interests, rather than a concern about crime (especially given the ‘reverse money laundering’ of state cash). Abstract entities like the LIEO or the memorable alliance can only be viewed as referent objects as they do not have a ‘voice’. But it is the representatives of states, IGOs and to an extent firms who are the most effective securitising actors (103). A parallel can be drawn from this observation to Chapter 4 where the memorable alliance did not ‘speak’ for itself, but we heard the views of the US Treasury Secretary and the Chairman of the Federal Reserve as representatives of the state, and from the CEOs of large banks as representatives of industry and capital. With this framing, it seems that officials of the state, industry and capital have been attempting to securitise cryptocurrencies with the maintenance of a higher-level referent object in mind.

In the original Copenhagen School vision of securitisation theory, the referent object needs to be threatened existentially. It is not enough that there is a threat to individual employment or that welfare levels may suffer – these are ordinary issues of politics and economics. The state, banks, the LIEO and the memorable alliance are, though, referent objects that could see their existence threatened. But if Bitcoin were to make banks obsolete, would this not be an act of Hayekian capitalistic liberalism that should be supported? And if Bitcoin did replace banks, then its financial system would be in operation as an alternative to the current system. That is, economic stability would not be threatened existentially. It does not seem likely then that banks are the referent object, although representatives of them may well be securitising actors with an interest in maintaining the status quo. It is certainly hard to think of any plausible ways that the illicit use of cryptocurrencies could existentially threaten banks.

The state then and the abstract concept of the LIEO or the memorable alliance, remain as more likely referent objects. But here, the fundamental conflict between liberalism and retention of power and control resurfaces as an inherent contradiction present in our modern capitalist system. Liberalism promotes competition and globalisation, and firms are free to fall victim to economic Darwinism, but the same is not applied to the nation-state or national currencies, which are still ‘viewed as an indispensable part of national monetary policy’ (Selgin, 1988: 3). Likewise, there is a tendency to think of states as ‘permanently rooted structures’ (Buzan et al., 1998: 104). This leads to an axiomatic view of the state and of state money – that they are insoluble, and the way things must be. But this does not have to be so. We can conceive of a future global society that is ordered beyond old assumptions. And a new world order could be better served by new imaginings of money. Old axioms deserve challenge. In Chapter 7, we saw how cryptocurrencies can be used for legitimate purposes through a case study of HullCoin. This demonstrated that Bitcoin and cryptocurrencies could play a part in future monetary systems and that there are potential advantages to them doing so.

For now, though, if states are effectively permanent structures, we must consider if cryptocurrencies could in any way constitute an existential threat to them and thus whether securitisation could be valid. As we saw in relation to the Triffin Dilemma, the United States has the famous exorbitant privilege of the dollar and can expand its monetary supply at will, leading to the exponential rise in its debt as already discussed. At a basic level then, it is inconceivable that Bitcoin could threaten the outside supplies of resources to the US – this being the only threat to the national economy that could be ‘legitimately securitized’ by liberals (Buzan et al., 1998: 105). Whilst it may be difficult for liberals to talk coherently about economic security, system-level structures frequently become securitised objects (106):

> The LIEO is existentially challenged by anything that threatens to unravel commitments to remove border constraints on the international movement of goods, services, and finance… The LIEO thus lives in permanent tension with impulses toward both protectionism and monopoly. (Buzan et al., 1998: 106)

Yet Bitcoin does aim to remove border constraints and improve international finance, so in this regard, it supports the LIEO, rather than exists as a threat to it. Again, the answers lie in the final sentence of the quotation and the tension between promoting the liberal ideal and the impulse towards protectionism and monopoly. The monopoly of money is a profitable business, the memorable alliance is profitable for the alliance – a global currency beyond the control of a state threatens existing hegemonies. The memorable alliance, therefore, emerges as the most likely referent object, rather than the state itself or the LIEO. And this is a plausible explanation for the securitising moves we have seen.

8.2.2 Existential Threat or Action-Focussed

The illicit use of cryptocurrencies (on the dark net) is relatively small, so there is certainly no conceivable way that cryptocurrencies can be thought of as an existential threat to the state itself or the existing financial system. Furthermore, scale is an important factor in securitisation theory when evaluating what counts ‘as a legitimate security issue’ (106):

> Like humans, firms, and states, systems can lose an arm or a leg without being existentially threatened. Security threats to such systems occur when leading actors or large numbers of members begin either to question the constitutive principles of the system or to break or fail to support the rules and practices that uphold the system. Securitization is sometimes attempted on less significant threats. Such attempts usually fail, but sometimes they

> function to legitimize action against dissenters from the global liberal economic order. (Buzan et al., 1998: 107)

It has already been noted that further research of states or the memorable alliance would be interesting to see if their principles are beginning to break or fail, but this is beyond the scope of this thesis. However, it was noted in Chapter 4 that there has been something of a shift toward cryptocurrencies as seen through the words and actions of some US officials. Perhaps this is evidence of a questioning of constitutive principles and a threat to the memorable alliance. And perhaps the securitising speech acts against cryptocurrencies are attempts to deter dissenters from the memorable alliance; this is after all what Bitcoin represents – the disintermediation of the state and banks from money.

Chapter 2 explored the problems of the existing monetary system and raised the idea that some people are using Bitcoin in a counter-securitising way to protect themselves from the state and its flawed monetary system. The irony then is that the state is protecting a system that is a threat to itself and others. The explosion of debt, the growth of derivates and even forex markets are arguably greater economic security threats than cryptocurrencies (see Section 1.1.6). As Bjerg noted, many of the criticisms of Bitcoin apply equally to the existing monetary system, and perhaps even more so (2016: 69). The inherent contradictions in the liberal approach to economic security are clear to see:

> How does liberal security logic deal with systems whose organizing principles are themselves defective in the sense that they create a significant probability of systemic crises (Polanyi 1957 [1944])? What does it mean to protect the stability of a system if the system is a threat to itself?... It can be argued, for example, that the LIEO contains such faults. The relentless pursuit of free trade may eventually create such pressures of adjustment and loss on states, as well as the polarization of societies, that it triggers reactions against the basic principles of the system. (Buzan et al., 1998: 108)

The speed and scale of fundamental change are important factors in securitisation theory in terms of what qualifies as an economic security threat and how that affects actors in the system. ‘Sudden and massive structural change might count as an economic security issue’ (Buzan et al., 1998: 108). But in more than a decade of Bitcoin’s existence, neither it nor any illicit usage connected with it has led to any fundamental change as a result of a sudden, sizeable shock. In this respect, it cannot be considered an economic security threat. The financial system, states, and the world economy have all had many years to adjust to the presence of cryptocurrencies. It is therefore hard to conceive of them as an existential threat to some referent object, such as the memorable alliance. In the economic sector, genuine security issues are rare and although frequent attempts are made to securitise issues, few receive substantial support (Buzan et al., 1998: 109).

If ‘there has long been a debate about the coming destabilization of the liberal international economic order consequent upon the decline (or, in some versions, corruption) of the United States as a hegemonic leader’ (Buzan et al., 1998: 110), then a securitising move against cryptocurrencies is possibly a materialisation of this reality. And Bitcoin may well play a role in this decline. If the US loses its privilege and status as the sole superpower, then this could lead to the collapse of the LIEO, and the risk of conflict may grow – but how much Bitcoin could be blamed for this would certainly be debatable. The flaw in the current capitalist system that sees support for competition amongst firms yet resists competition in money, long pre-dates the invention of Bitcoin. It is contradictory and protectionist. And anything that challenges this status quo, and the status quo of the memorable alliance, is usually met with resistance.

The evidence in this thesis shows that the overwhelming majority of cryptocurrency usage is legitimate (see Section 8.1.1). If we use Moore and Rid’s yardstick, then cryptocurrencies should not be viewed as a security threat, they should not warrant extraordinary treatment and they should, instead, be handled in the normal course of politics – like cash. In this section, the memorable alliance has been identified as the likely referent object and the authorities of the government, central banks and private banks as the securitising actors who have been delivering the speech acts. Crucially, though, using the Copenhagen School vision of securitisation theory, it is hard to argue that Bitcoin or cryptocurrencies existentially threaten the memorable alliance. Time and scale are important factors but, after more than thirteen years of existence, Bitcoin has not brought about an end to anything readily identifiable as a referent object, certainly not the memorable alliance.

In Section 1.3.1, it was noted that the original Copenhagen School securitisation theory has been criticised and reworked by subsequent scholars in several ways. Securitising actors may use media other than just speech, the 'audience' has been expanded upon and, significantly, the ways in which something qualifies as being successfully securitised have also been advanced. In this thesis, the extent of the securitising speech acts has been shown and the main focus of the empirical research was to examine the reasons why cryptocurrencies have been labelled as a security threat and whether the actors are justified in their claims. If cryptocurrencies are not a valid threat in the economic sector due to time and scale, then whether an 'audience' has accepted the case for securitisation is less of a pressing issue. Indeed, this thesis did not aim to scrutinise the audience to see if securitisation has been successful. This is an interesting question for further research, but it does not seem that law enforcement has accepted that cryptocurrencies are a security threat and, judging by the continued growth of cryptocurrencies, it does not seem that the wider public has either.

However, whilst cryptocurrencies do not qualify as a security threat in terms of the economic sector in the Copenhagen School conception of securitisation theory, other scholars have proposed other ways of determining if something has been successfully securitised. A broader conception of what constitutes success is useful, therefore, for a fuller discussion of the extent and reasons for an attempted securitisation of cryptocurrencies. If the Copenhagen School's criteria for success is 'too demanding' then we may learn more by lowering it, as suggested by Salter and Leonard for example (Floyd, 2019: 175). In this way, 'audience acceptance alone does not make for successful securitization' (Floyd, 2019: 181).

Even though the economic sector has been largely ignored by securitisation theorists, Floyd argues that there is utility in this sector and proposes an 'action-focused approach that ties securitisation's success to relevant behavioural change/action in response to a securitising speech act' (2019: 187). With this approach, there is less of a focus on whether a claim is legitimate and by looking below the level of exceptional measures we can more easily identify securitisation. Again, it is not an aim of this thesis to exhaustively analyse all the actions taken against cryptocurrencies by states as evidence of securitisation (although this could be another area of future work). But some discussion of this is useful. We have seen that several countries including China and India have banned cryptocurrencies at various times. This likely counts as extraordinary measures, but in any case, is evidence of action-focussed securitisation. In particular, though, the actions of US officials are of great interest as always.

In the US, like elsewhere, the issue of regulation and policy about cryptocurrencies is still under development and is a complicated area in its own right. In 2021, US Congress introduced 35 bills on cryptocurrency policy and regulation (Brett, 2021). Of note, is that a US law on cash was changed to include cryptocurrencies, even though cryptocurrencies are not viewed as legal tender. This subsequently resulted in Coin Center, a US cryptocurrency policy group, filing a court suit against the US Treasury Department (the memorable alliance) (Sarkar, 2022). And in another example, the New York Senate passed a bill banning new proof-of-work mining operations due to potential environmental concerns (De & Ligon, 2022). These appear to be action-focussed evidence of securitisation. However, we also need to consider the impact of inaction or blocking by the state. Several countries have allowed the creation of Exchange Traded Funds (ETFs) for Bitcoin investment, but the US has repeatedly blocked applications for such a fund, to the extent that applicants are considering suing the US Securities and Exchange Commission (Benson, 2022). In another example, Bitcoin bank Custodia has sued the Federal Reserve for delaying its application for a master account at the bank for nearly two years (del Castillo, 2022). Similarly, any demands for cryptocurrencies to be accepted as legal tender can and have been dismissed by the state, preventing their increased acceptance. In this regard, the action-focussed approach would benefit from expansion to include inaction or blocking as well. These ‘moves’ are perhaps even more significant and arguably more important to identify as potential evidence of securitisation.

8.2.3 Complementary or Alternative Money

Having considered the threat of cryptocurrencies through both the lens of the Copenhagen School and through Floyd's action-focussed approach to the economic sector, we now move back to the topic of money and the reasons why there has been an attempted securitisation. If the securitising speech acts are not about the threat of illicit activity, if the memorable alliance is the referent object, if there is evidence of securitisation, and if the threat is neither timely nor sufficiently large, then in what way are cryptocurrencies really a threat?

It is through the HullCoin case study that the wider meaning of this thesis becomes apparent. The opposition to cryptocurrencies is not about crime – it is about power. Here, we return to Chapter 2 and the background on money that has developed throughout the thesis. Ingham's definition of the two sources of power also becomes integral - having more money than anyone else and controlling the supply.

Money has long been contested, and control of its production and supply has long been closely linked to the state. Dodd wrote that Bitcoin is disintermediating the banks and the state from money, and it is here that the tension really lies. For hundreds of years, the memorable alliance has controlled, benefitted, and profited from the monopolistic control of money. In the modern age, this continues and has become easier than ever as supply can be increased with the tap of a computer. But the issue, as always, is that the new money is not spread evenly. In the UK, following the Great Financial Crisis and COVID-19 spending, commercial banks were given some £900 billion through QE. The government also pays interest to the banks on this amount which, depending on the interest rate, is another £9-40 billion per year (Murphy, 2022). In contrast, the 2022-23 support package for the inflationary cost of living crisis was worth about £22 billion (Gov.uk, 2022).

The position of the memorable alliance has likewise been defended throughout history. There was immediate opposition to HullCoin from the government, and any conflict was avoided by the team carefully constructing and narrating HullCoin as 'not money', even though it was a fork of Bitcoin. In this way, and due to its locality and size, it avoided being a challenge to state money and was then even supported by some government departments by virtue of the benefits it could potentially bring. A hypothesis here is that government believes that an alternative, and even possibly a complementary, currency would critically affect the state's power. But a state would remain the largest holder of any currency through taxation and the rule of law. It seems that currently the two aspects of Ingham's power are conflated into one. And therefore, the threat that cryptocurrencies pose to power is potentially overstated. This would certainly be worthy of further research.

Likewise, it is not possible in this thesis to determine if the memorable alliance has an insufficient understanding of cryptocurrencies and the threat they pose, or whether 'security' and the fear that it can induce is better grounds in their minds for opposition to cryptocurrencies which, for the alliance, is really about their own self-interest. Salter observes that 'a popular appeal to national security is often effective in popular and elite politics, but may be less convincing in a scientific realm' (2008: 331). An audience study would reveal whether people have accepted the securitising claims, but the evidence here suggests it has not, certainly amongst users of cryptocurrencies and the law enforcement officers interviewed. Perhaps this is because of a higher level of education and experience with cryptocurrencies, or because the power relations are different in that some people are using cryptocurrencies to protect themselves from the state. As later theorists have noted, 'the power relationship between the securitizing actor and the audience is not as one-sided as suggested by the initial formulation of securitization' (Balzacq et al., 2016: 501). It may be that the decentralised nature of cryptocurrencies bolsters 'the power of the audience to accept or reject a securitizing move' (2016: 502).

HullCoin was inspired by Lietaer's Civics, and Lietaer argued that there are real benefits to a financial system that has more than one currency. And in Chapter 2, many scholars were shown to have argued against the state monopoly of money and the abuse and misuse that comes from such a system. If there is ever to be a de-securitisation of cryptocurrencies (putting aside whether they have been accepted as such), then the state will have to move past a state-centric view of money. And unless it does, the likes of Bitcoin, HullCoin and the thousands of complementary currencies that attempt to improve local economies will likely continue to face resistance.

Lietaer and others, such as Hayek, saw non-state monies as part of the solution to the volatility and the boom-bust cycles that regularly trouble our existing financial system. More widely, state centralised governance and state ownership have also been criticised. In this regard, Bitcoin could be viewed as a potential solution to some of the faults of money, rather than merely as a problem. The key issue for Bitcoin and cryptocurrencies, then, is whether they are framed exclusively as a strict alternative to the national monopoly or whether they could, instead, be seen as a complementary currency with something positive to offer.

Nobody owns the Bitcoin network, and nobody runs it as if it were a traditional organisation with which we are familiar. As such, what it appears to be now is often driven by the narratives that surround it. It was argued in Section 2.2.1 that it is a mistake to label cryptocurrencies as libertarian, for example, because some people who support them are libertarian. Simmel demonstrated that this is an error of philosophical logic in that an object has its own properties, and those properties define it, not any outside thinking or narrative. Whether Bitcoin is labelled as a threat, complementary or alternative money, does not change anything about how the system functions – it stays the same regardless. But it does affect how Bitcoin is viewed and treated.

Satoshi Nakamoto was certainly aware of conflict with the state. In emails, Satoshi warned of ‘the hornet’s nest’ swarming towards Bitcoin, following the suggestion that WikiLeaks could benefit from using it (Champagne, 2014: 5). The idea of Bitcoin was to create a money free of middlemen and third parties that could abuse it. So, in this regard, Bitcoin was certainly intended as a competitor to state money. Satoshi saw a future for trustless electronic money but realised it might take many years for it to develop. In this time, it would clearly exist alongside state currencies and potentially be used in niche applications like ‘reward points, donation tokens, the currency for a game or micropayments for adult sites’ (Champagne, 2014: 335). This is not the language of an existential threat to state money.

For Bitcoin and cryptocurrencies then, there is an opportunity for de-securitisation by reframing the narrative to one of complementary currencies rather than alternative.

Some supporters will of course object to this, and others would not. But the reality is that states are run through force and the rule of law, and this power ensures that state monies are used. It is, therefore, unlikely that an independent currency like Bitcoin will replace state money, and certainly not sooner than many decades. What could be far more possible, is that Bitcoin could be framed as a complementary currency. Not one to replace the national currency, but as a system that lives alongside the present one to provide resilience to it, and to act as a regulator to the excesses of the existing system. I side with Lietaer, that a single currency system does not have the resilience that society needs. ‘Resilience as an operational strategy of risk management’ has also been adopted in financial security discourses and this also aligns with the free market thinking of Hayek’s Austrian philosophies, where markets are viewed as complex financial ecosystems (Walker & Cooper, 2011). This argument, of course, applies to Bitcoin as well. Even if it achieved global dominance, that would again leave us too dependent on one source of failure. The better answer is likely to be multiple, competing currencies, and this viewpoint may see less resistance to Bitcoin if it were more widely adopted. And of course, there may well be other benefits to society beyond resilience in terms of equality and opportunity, as previously discussed.

Bitcoin, though, does have a narrative associated with it that establishes it as a threat to the existing system, and the memorable alliance. It needs stressing, however, that this is only the view of some of Bitcoin’s users. Many now see it as gold 2.0 (Shawdagor, 2022), whilst others prefer Bitcoin alternatives with other properties. The point is repeated that just because a group cheers it as a threat to state money does not mean that it necessarily is. There is an opportunity to change the narrative surrounding Bitcoin. If this could be done, then Bitcoin and cryptocurrencies could be de-securitised, leaving them free to be used as useful legitimate tools and even be beneficial to the financial system by providing resiliency through greater redundancy and an end to the monopoly of state money. Securitisation theory teaches us that there is a cost to focussing on the wrong issues. More effort should be spent on fixing the existing system rather than scrutinising alternative efforts to do something about it.

Any change in approach or response would likely require a re-examination of the power that the state gets from money. And this relationship is most relevant for the largest state powers that benefit from the existing system, such as the US. But even if Bitcoin did replace a state currency, it would not mean the end of state power. The state would invariably have more money than anyone else and would retain a significant position of power. Fear is a constant theme in the discussion about money and in the economic sector of securitisation theory (Floyd, 2019: 174), and there appears to be a fear of Bitcoin shown by the memorable alliance. In Section 4.1.1, this is reflected in the headlines and particularly in the quotation from the US Congressman, as well as in Chapter 5 and the fear of a cyber 9/11. Perhaps this fear could be allayed with a more thorough understanding of the risks.

Interestingly, the disruption of the old arrangement of the memorable alliance may well affect the trilogy in different ways. The private banks are arguably more at risk of being cut out of their profitable position than the state is from being cut off from power. But whilst the state can maintain its position of power by having more money than anyone else, the likes of Bitcoin do have the potential to impact the state’s ability to arbitrarily produce more money. Inflation is a repeating theme of state currencies and, indeed, the world is once again facing a cost of living crisis as inflation reaches 40-year highs (Rockeman, 2022). The presence of a fixed supply money such as Bitcoin could hamper the extreme debt and money creation that we have seen. But there are many, including myself, that do not see this as a fault of Bitcoin and more a fault of the existing system, and one that needs to be controlled as it leads to rising inequality and limits growth. Here again, the state may have to rethink its established ways. It may no longer be able to inflate away debt or create money at a whim – and in this regard, it would have to fundamentally change its behaviour. If ever the state did have a reduced ability to create money, then it would no longer be able to stealthily tax its population through inflation, and it would have to raise funds through direct taxation instead. This would likely have a significant impact on government financing and policy. War, for example, may well become harder to fund if it is not supported by the population and taxation for it is opposed.

8.2.4 Money and Trust

This thesis shows that crime is not a valid threat argument against Bitcoin and argues that the current financial system is flawed and that there should be a place for competing, complementary currencies. Yet, in Chapter 2, it was also shown that Bitcoin is criticised more than other new forms of payment. We have seen that there have been previous proposals to separate the banks from money and that in the 1970s Hayek also had ideas about separating the state from money. But it is Bitcoin that is doing both, in response to a loss of trust in banks and the state in their involvement in money:

> The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. Their massive overhead costs make micropayments impossible. (Satoshi Nakamoto as quoted in Champagne, 2014: 100)

A Bank of England bulletin notes that 'money is a social institution that provides a solution to the problem of a lack of trust…money in the modern economy is an IOU that everyone in the economy trusts' (Mcleay et al., 2014). But this trust has been broken and many no longer trust state money. Simmel is again useful here. Moving from private, commodity-based exchange between two individuals to abstract exchange between larger groups requires the creation of 'higher supra-individual formations' (Simmel, 2004: 173). That is if you are using an abstract money and you do not know who you are dealing with, then the money itself becomes an important part of making transactions possible. Broader exchange 'depends upon the economic community or upon the government as its representative' (176). Some entity or the community using a money is needed as a third party to the exchange. Interestingly, Simmel's words show that the community does not necessarily depend on a government, although it may do and, in the past, often has. Simmel goes on to say that 'money transactions would collapse without trust' and so an economic community needs ‘an element of social-psychological quasireligious faith’ (178). That Bitcoiners are fervent in their beliefs is a strength for their community, not a weakness, and testament to their corresponding lack of faith in fiat. For all monies, there needs to be a belief within an economic circle that the money will be accepted and for no form is there a one hundred per cent guarantee that a money can always be used (179). ‘The guarantee of the general usefulness of money’ and its issuance is undertaken by a ‘representative of the community’ (179-80), ‘an objective institution’ (182). And at scale, money becomes a ‘public institution’ (184).

In the political dimension, the critical question is not only ‘who’ can this institution be but now also ‘what’? Must it be the state, or can other higher supra-individual formations fulfil this role? Simmel is clear that these ‘formations exist in great variety’ (173). In ancient Greek culture, the relationship between money and the central institution was religious, not political. The institution, therefore, does not *have to* be the state. Indeed, a Hegelian conception of the nation-state is only two hundred years old (Chernilo, 2007: 40). Hayes argues that blockchains ‘*are* the very institutions they succeed’ and that each blockchain has its own rules and social commitments like banks do. In this way, blockchains are a new free market of competing institutions (A. Hayes, 2019: 17-18), or even ‘self-contained money-worlds’ (A. Hayes, 2021: 136). To this, I add that Bitcoin *is* a public institution in the Simmelian sense. Furthermore, Bitcoin is prima facie evidence that other types of higher supra-individual formation can fulfil this role in society, and money. It is for those in the economic community of Bitcoin to believe in it as money, to have faith in it, and Bitcoin *is* the third party that provides the degree of guarantee. It is not only the state that can give confidence in money. Money tends to be over-complicated by theory and it is easy to become lost in its philosophy. Money is simply whatever a group of people agree and trust to use as a means of payment (Lietaer, 2001: 41; Bjerg, 2016: 61).

An important theme of *The Philosophy of Money* is the development of money in parallel to the development of society. As our intellectual ability advanced, money moved from commodity to abstraction. And society evolved from private transactions to ever-widening economic circles. This progress was also marked by a trend towards *centralisation*, which Simmel saw as mankind’s concentration of energies, forces and unity in order to achieve more with less effort – some examples being machinery, gunpowder, and family (Simmel, 2004: 196-98). The modern state represents an ‘unrivalled concentration of forces’ and money, as it develops, increasingly expresses values in the ‘most concise and condensed way’ (197). Yet, our current financial systems and monies were shaped by an industrial-age world where ‘nationalism, competition, endless growth and colonization were encouraged’ (Lietaer, 2001: x). A national currency was a powerful tool for national consciousness (45), but the creation of hundreds of currencies along nationalistic lines, with its inconveniences, instability and speculation, cannot be a final realisation of the centralisation of money. For Simmel, in an ideal social order money would have no intrinsic value and would be purely symbolic (2004: 191). It would also be centralised in the sense of maximising its force and unity. But our current systems are based on crumbling ‘hierarchies of power based on control’ and ‘hierarchies of politics based on geography’ (Lietaer, 2001: 61). In a global, digital age, our world is deserving of a more fitting money, one that reflects a society that evolves beyond borders, and perhaps one that does not depend upon nation-state law and even violence for its protectionism. And more widely, too, these forces of nationalism, protectionism and geopolitical conflict are competing with the liberal ideals of a borderless world with strong international institutions.

With this in mind, this thesis argues for a reimagination of the commonly held view that ‘Bitcoin does not rely on trust in a central authority’ and that it ‘is radically different from fiat money issued by a state’ (Bjerg, 2016: 61). Bitcoin *is* a central authority, a public institution, in the same way, that the state performs that role in money. And it is centralising ‘great forces at a single point’ (albeit through a decentralised computing system), combining the energies of hundreds of currencies limited by borders (Simmel, 2004: 196). Bitcoin represents an evolution of higher supra-individual formations and an evolution in money paralleled by a developing global society.

8.2.5 The Question of Money

Bitcoin is used by a variety of groups, be it criminals, speculators, libertarians, hard-money Bitcoin vigilantes or even just those that find it useful. However, it ‘is arguably a social movement as much as it is a currency’ (Dodd, 2017: 40), based upon the properties of Bitcoin and primarily concerning the disintermediation of the state and the banks. In this way, Bitcoin challenges the memorable alliance of the state, the central banks and the private financial institutions that form the basis of our modern capitalist system (Ingham, 2020: 65). This is where the tension lies.

Bitcoin directly challenges the soft money of the state, which puts it in conflict with those that benefit from the power that control of money brings. In this way, this is further evidence that money is more than merely a means of exchange. It is a ‘source of power – infrastructural and despotic’; ‘infrastructural’ in the sense of a public institution that allows us to transact, but ‘despotic’ as a weapon and ‘essential element of state sovereignty’ (Ingham, 2020: 13). For Ingham, the power comes from having more money than others but, more importantly, from the ability to create it. Bitcoin does not stop the state from accumulating money and power through taxation (leaving aside any collection problems related to the self-sovereignty of assets). Specifically, Bitcoin threatens *only* the state’s ability to wield power by *creating* money. The implications of this require further study, but the prospect is feared nonetheless, as we saw in Chapter 4:

> An awful lot of our international power comes from the fact that the U.S. dollar is the standard unit of international finance… It is the announced purpose of the supporters of cryptocurrency to take that power away from us. (US Congressman Brad Sherman, as quoted in Bambrough, 2019)

It is in the political dimension, therefore, that the issues with Bitcoin and money lie. We should no more be concerned with what money is, where it came from or its form. These issues are largely settled, in practice if not in theory – modern money no longer has intrinsic value. But *supply* is very much contested, and it *is* the issue of the political dimension. I, therefore, propose a refinement of Ingham’s money question to my ‘question of money’, which is solely about supply, broken into the same three elements – first, who or what can be a public institution for the management of money; second, how is money produced and, crucially, how much (the rate of new supply or destruction); and third, is money (new and old) distributed fairly in society?

These are the questions we must concern ourselves with. The state has failed at the second and third elements of the question of money. I do not argue here that Bitcoin can or will replace state money but analyse it to reveal the truth - that the issue of supply is central and remains powerful enough after many centuries to evoke continued resistance. Supply is the fundamental theoretical issue of our time. Can the state retain power in creating money, as a 'force for good'? Or is the 'only way' to have something that is beyond its power to abuse and misuse?

Centuries of great minds have shown that there is a problem with the state in money; namely that power to create it invariably ends in ruin. There has been a fundamental misinterpretation of several key monetary thinkers in justification or support of government spending without specific plans for the repayment of that debt. The explosion of government-issued money devalues all money, making us all poorer. Schrodinger's debt is real, and the price is paid by all in society through rising prices and inequality. Bitcoin has emerged as a possible solution to these problems but has often been criticised and dismissed. Using Ingham's 'money question' and Simmel's *The Philosophy of Money* as a core text, I have shown that Bitcoin, as well as fiat, are good forms of money that are closer than gold to Simmel's 'final outcome' vision of token money. This settles the debate 'about the nature of money and the relation between money and commodities' (Bjerg, 2016: 58). And I agree with Ingham, that the fundamental clash over commodity versus claim theory should be 'laid to rest'. The debate must move past these old divisions, as money does not need to be a commodity.

Instead, we must focus on the political dimension of money. Here, the control of *supply*, and the power that comes from it, is the real source of tension. It is supply that led to metallism, as we turned to gold in an attempt to address the 'alchemy' of the state problem in money and temper the irresistible desire of those in power to debase it. Commodity versus claim theory is not, therefore, about a physical ‘commodityness’. It is about the issue of supply, which transcends from the political dimension.

The state has failed throughout history in the management of money, and we may be better off without it monopolising that position. Modern money is founded on outdated industrial-age thinking, nationalism, and crumbling hierarchies of power. Trust in it has been broken. Bitcoin has emerged as social resistance and as a new type of higher supra-individual formation, where it is a community institution alongside the state – money as a public institution. And Bitcoin has expanded economic circles beyond the physical, geographic borders of state currency and proven that money does not depend on the state for guarantee. It is for an economic community to believe in a money, and the wider a money is used the better it needs to be. Bitcoin may be very different to state money technically and politically, but it is very similar philosophically. Bitcoin is a centralised institution for money, a machine for the concentration of the forces of value.

For Simmel, the future of money trends toward institutional centralisation and abstract money, with widening economic circles, and is paralleled by an intellectual advancement of society. Society, at its fullest potential, with increased social and economic differentiation, may find that Bitcoin, or others like it, could be desecuritised as part of the solution to money and its volatility, rather than framing it as only a problem. And a society tending towards individuation and individualisation might lead to such social conditions that the future of money will not be Orwellian, based on the industrial age thinking of hundreds of state monies, enforced by law, threat, coercion and violence. In the information age of the future, economic relations will be Simmelian, based on freedom, choice, and voluntary adoption. ‘Good money does not have so many side-effects as does base money, and… its use need not be so strictly regulated or supervised’ (Simmel, 2004: 194). An ideal society is worthy of ideal money. And the future does matter.

> The wealth of the world’s 10 richest men has doubled since the pandemic began. The incomes of 99% of humanity are worse off because of COVID-19. Widening economic, gender, and racial inequalities—as well as the inequality that exists between countries—are tearing our world apart. This is not by

> chance, but choice: “economic violence” is perpetrated when structural policy choices are made for the richest and most powerful people. This causes direct harm to us all, and to the poorest people, women and girls, and racialized groups most. Inequality contributes to the death of at least one person every four seconds. But we can radically redesign our economies to be centered on equality. We can claw back extreme wealth through progressive taxation; invest in powerful, proven inequality-busting public measures; and boldly shift power in the economy and society. If we are courageous, and listen to the movements demanding change, we can create an economy in which nobody lives in poverty, nor with unimaginable billionaire wealth—in which inequality no longer kills. (Oxfam Briefing Paper, Ahmed et al., 2022)

8.3 Contributions

8.3.1 Knowledge

Chapter 2 revealed a number of gaps in the literature and this thesis contributes to knowledge of this subject in several ways. Chapter 4 makes a key contribution in analysing the securitising speech acts of the memorable alliance and the usage of cryptocurrencies for illicit purposes. The chapter provides a different perspective that cryptocurrencies are used in a relatively small amount of crime and that they are not necessarily as useful for crime as is often suggested. This is important to stress, as securitisation theory shows that any disproportionate treatment of cryptocurrencies comes at a price, and this includes diverting resources from more serious threats. Part of this work was published in the Chatham House *Journal of Cyber Policy* (Butler, 2019).

The sociological research reviewed in Chapter 2 also highlighted many user studies from a legitimate usage perspective. The CrimeBB analysis in Chapter 5 added to this knowledge by researching users from the perspective of illicit activity. This revealed several important differences in why cryptocurrencies were used by this group and what the advantages were. The chapter shows that the adoption of Bitcoin was not about libertarianism or anonymity but the trust-eliminating property of the finality of transactions. Furthermore, this research showed that cryptocurrencies and dark nets do not make the purchase of illegal goods as simple as clicking a button. These are significant contributions if effective and proportionate policy is to be developed in this area. This work was presented at STAST2020, as part of ESORICS 2020, and later published (Butler, 2020).

The research chapters also contribute to further gaps in knowledge. For all the discussion about illicit usage, there has been no research exploring the views and experiences of law enforcement in relation to criminal investigations involving cryptocurrencies. This has also been an important gap to address, especially as this issue is central to the opposing narrative towards cryptocurrencies. And whilst there has been a great deal of research on the individual use of cryptocurrencies, there has been far less at the community level. The HullCoin chapter, therefore, aimed to reduce this gap by examining a community-level usage of cryptocurrencies. This revealed the reaction that HullCoin initially faced, but also that the technology proved to be useful for the implementation of a Civics-like project. That is, cryptocurrency technology was useful and not just a criminal tool.

Simmel’s *The Philosophy of Money* was applied to Bitcoin in new ways, showing that token money is the best form and that old scholarly debates about commodity versus claim theory should now be laid to rest. Bitcoin is money, and it can be thought of as a machine for money and a public institution for money in a Simmelian sense. A revised version of Ingham’s money question, the Question of Money, is also presented which I argue should be the basis for consideration of money moving forward. This work was published in *Theory, Culture and Society* titled, ‘The Philosophy of Bitcoin and The Question of Money’ (Butler, 2021).

Finally, the overall conclusion of this study is that illicit use is not a valid argument upon which to attempt a securitisation of Bitcoin and cryptocurrencies. The scale of cryptocurrencies is too small and too much time has passed that they cannot feasibly be considered as an existential threat to the memorable alliance, or likely any other referent object. Having said this, using a lower standard of what constitutes securitisation, we can see that there is evidence of securitisation in respect of action being taken against them, as well as blocking moves by the state that are limiting their use. Ultimately, the securitising speech acts are more likely to be about money, and more specifically the power that comes from being able to create money. The threat of cryptocurrencies, then, is to the control of the supply of money, which has long been a critical part of state sovereignty.

8.3.2 Theory

As a reflective observation, I would like to mention that there were some difficulties I faced initially with this project due to its interdisciplinary nature. The most significant of these was where to locate this project academically. Cybercrime as a subject does not appear to be considered an integral part of cyber security more widely. Should a piece of work such as this fit within criminology, security studies, international relations, or economic sociology? Some of this invariably is due to logistical matters within university departments, but I would like to see interdisciplinary works such as this sit more comfortably within cyber security as a field in its own right. Cyber security is a large field, and it is now widely accepted that the scope is broader than just the technical aspects. I think that cybercrime is integral to it and interdisciplinary projects like this should equally be a part of cyber security as much as more technical ones are.

Part of the above observation is explained by the location of different theories. In this study, I drew on economic sociology and the insights of security studies, specifically securitisation theory. In due course, it may be that more theories about cybercrime develop from within cyber security departments and that this type of project will become more ‘normal’ in this field. This is also reflective of the call for more sociological work on cryptocurrencies seen in Chapter 2.

This thesis also contributes to the first use (that I am aware of) of securitisation theory in the analysis of Bitcoin. In the earlier stages of this PhD process, I was conscious of blind empiricism and the potential advantages that a theoretical lens could bring. I considered several theories, from criminology and elsewhere, but did not find one that I felt added to the consideration of my research problem. It was only after a considerable amount of reading that I revisited securitisation theory and then saw how it may prove to be useful. Initially, as I first examined the headlines about the criminal use of cryptocurrencies, I did not consider more deeply ‘who’ was describing them as a threat. And similarly, securitisation theory raised the question more prominently about defining what exactly was under threat.

In addition, securitisation theory can be applied to the economic sector, and this was also useful in reaching the conclusions of this thesis. Significantly, despite the fact that securitisation theory is popular and has been applied to several areas, it has largely been ignored in the economic sector as Floyd points out (2019: 174). The Copenhagen School securitisation theory recognises that it is hard to identify the referent object in the economic sector but notes that the object might be abstract. This was an essential insight for this thesis as I conclude that the referent object is the memorable alliance. Securitisation theory was useful, then, in structuring my thinking about the question of the security threat of cryptocurrencies, but it also specifically helped define what could be considered a threat in the economic sector and what might be the referent object. In these ways, securitisation theory proved suitable and beneficial when applied to Bitcoin and money.

As there has been almost no research in the economic sector with regard to securitisation theory, this project contributes to this area of knowledge. In Section 8.2.2, this thesis also contributes to the action-focussed approach in the economic sector by suggesting that the theory be expanded to include notions of inaction and blocking by the state. Extreme measures have been taken by states against cryptocurrencies, namely banning them, but in more liberal societies the inactivity of states or the blocking attempts are arguably as important as the actions that they take. An expansion of the action-focussed theory would see these instances of inaction and blocking also be interpreted as evidence of securitisation.

This thesis has also contributed to the ways in which we think about security. The state is often viewed as an institution that stops us from descending into lawless chaos. But there are often times when citizens need to be protected from the state. These can be clear abuses, but what happens when abuse and misuse are more subtle, for example, at a financial system level? How can citizens have financial agency when it is the state that is enforcing a monopoly? These questions are implicitly social. By applying Simmel to Bitcoin, I contributed a new way of thinking about Bitcoin. The mantra in Bitcoin circles is ‘don’t trust, verify’ – that the blockchain enables you to be free of trust in some ways. But I showed that Bitcoin is not so different from fiat monies philosophically. They are both token monies, but Bitcoin can be thought of as an advancement of Simmel’s higher supra-individual formations. Bitcoin still requires trust - trust in Bitcoin itself as a public institution for the management of money, and faith that the community of users continues to trust in Bitcoin. The world needs a better financial system, and a more developed society is likely to have one.

8.3.3 Methodology

This thesis took a constructivist approach to the research and this choice adds a great deal to the study of cryptocurrencies, especially given that narrative about cryptocurrencies is so important. Focussing more on the views of participants brings about a much greater understanding of the actual use of cryptocurrencies. Chapter 5 is a good example of this in particular. While officials and others believed that the main benefit of cryptocurrencies for illicit activity was anonymity, the users themselves revealed a different reality. Importantly, the research design of this thesis took a range of perspectives: state narratives, illicit use, law enforcement and also civic. In this way, the wider analysis is much stronger as a whole due to the overlapping nature of the findings.

Several design choices had a fundamental impact on the research conducted. For the law enforcement interviews, my position as an ‘outside-insider’ needed careful thought in terms of any potential impact on the research. But also, this position was likely crucial in gaining access to the participants, and I expect that I may not have had the same access to officers from other countries. This is supported by the fact that without this status I was not able to interview participants from the memorable alliance.

Ethics also had a large impact on the analysis of CrimeBB. As discussed in Section 5.4, I believe that advice to not use verbatim quotations is overly conservative and the chapter would have been stronger with a clearer display of what the users had actually said. This would also have made my observations and analysis less opaque. I do feel that the choice of analysing a pre-scraped dataset was right for this project in terms of ethical approval and the minimising of risks. For an early career researcher, illicit internet activity has several potential pitfalls that must be navigated with care.

This thesis also used multiple techniques of engagement. Document analysis was used in Chapter 4 to explore the state narratives and the extent of the use of cryptocurrencies in illicit activity. Chapter 5 utilised a dataset scraped from less visible areas of the internet, which provided a deeper insight rather than a study of more accessible participants, such as students. A qualitative analysis of law enforcement interviews and a case study of a civic use of cryptocurrencies also combined to provide a novel and thorough examination of this topic. I would also like to argue that this design provides a deeper and richer understanding of issues than a technical examination of blockchain transactions for example.

Finally, whilst the analysis of forums is not a new methodology, I believe that this study includes the first forum analysis of illicit cryptocurrency users. Most of the other user studies I reviewed used surveys or interviews as their methods. A key issue in the CrimeBB analysis was how to reduce 100 million posts to a qualitatively manageable amount. The three-step process I used achieved this, which included the use of IBM’s SPSS Modeler. SPSS Statistics is commonly used in research, but other researchers may also consider using SPSS Modeler in the way that this study has. It helped ensure a more robust method was used in selecting forum posts.

8.4 Limitations

There are several limitations to this study that are worthy of mention. In Chapter 4, I focussed on the views of US actors due to the position of the US dollar. There is of course a large difference that is seen across the world by different states to Bitcoin, and the reasons for these positions vary. Elsewhere in the thesis, we discussed China and also smaller countries like El Salvador which has made Bitcoin legal tender. Where I have discussed the state in this work it has primarily been in relation to the western states who benefit from the liberal international economic order. There may well be further research that could provide more detail about the variety of positions that many different countries have taken.

When I began this research, I was initially interested in the criminal usage of cryptocurrencies as it relates to the securitising speech acts (due to my background). Whilst this study contributes several findings to that end, the results have led to more questions about the memorable alliance and their views. This was not an initial focus of this research and explains why some of the wider meaning of this thesis is found in a discussion section. For this study, the limited research in Chapter 4 was sufficient to enable the later empirical chapters. But there is certainly more that could be done here, and this is discussed in the later section on further work. In particular, there was no direct research of the memorable alliance in this research, and this would be of great interest moving forward. In the same way that I wanted to explore the direct opinions of cryptocurrency users in terms of illicit activity in Chapter 5, and also of law enforcement officers in Chapter 6, it would be interesting to directly explore what members of the memorable alliance say about cryptocurrencies.

The limitations in the CrimeBB chapter were firstly methodological in relation to ethical considerations. Other studies on the dark net have conducted direct interaction with participants, but this was not necessary for this study and would have brought unnecessary risk. However, in-depth interaction with participants may well reveal interesting insight compared to the techniques that were used here. Similarly, some limitations come from using a dataset. First, is the period that the data was collected over. CrimeBB was selected as it is a live dataset and so it offered more up-to-date data than other studies reviewed in the literature. Having said that, the cryptocurrency field is fast-moving, and so more current information will always be of interest as views and reasons change over time. There were also limitations in the number of posts that I could qualitatively assess. I reduced the dataset to a small sample compared to the full amount, but this was still a huge amount of work to analyse. There may be much in the wider material that is of interest. I did use IBM SPSS Modeler as an automated solution to this issue but accept that more advanced techniques in topic modelling may be of use, but this was beyond my expertise. The focus of the research on CrimeBB was qualitative and interested in the depths of the content rather than automated classifications of it. And finally, the dataset is limited to the sample of underground and dark net forums reviewed. These also come and go frequently. I do argue that the sample chosen is likely to be representative of opinions, but that is certainly open for scrutiny by other researchers should they choose.

The pandemic arrived shortly before my research period began and affected the methodologies employed. Interaction with participants was reduced to online interviewing. I do not believe that in-person interviews would have revealed anything substantially different from that which was gathered online, but the academic community may have more to say on that subject in the coming years. The pandemic did prevent me from travelling to Hull but, as discussed, the impact of that was reduced by the fact that the project had ceased. I am not convinced that more would have been achieved if I had been able to travel to Hull. I also felt that online interview worked well for the purposes I had. I did not need to see or interact further with the participants in any physical sense and so felt that I was able to achieve what I wanted in an online capacity.

A key limitation that I had with the law enforcement strand was participation. The organisations and subject matter are somewhat sensitive and so finding willing participants is more of a challenge. Chapter 4 had a US focus due to the US dollar, and the initial observation of a conflict with law enforcement related to a US agent. As an ex-UK law enforcement officer, I was an ‘outside-insider’ to UK law enforcement. Due to access issues of these specialist officers, I decided to try and find UK law enforcement participants, rather than US. Having completed the research, I am not sure that I could have secured any participants without this status, and it would also have likely been very difficult to secure participants from another country where I am unknown. My assumption, though, is that the findings in Chapter 6 are likely to be representative of wider law enforcement, as the research was more about the officers’ technical experience of cryptocurrencies in investigations and their opinions about them. That is, there is less of a geographical importance to this research in comparison to the importance of the US members of the memorable alliance in terms of narrative and securitising speech acts.

Cryptocurrency investigation is also a niche area, within a niche area that is cybercrime. This meant that my sample for interviews of law enforcement officers was small. As the interviews were in-depth and with some key, knowledgeable individuals from the Police and the NCA, which are the two key UK law enforcement organisations, I felt that the material gathered was excellent and sufficient. However, I certainly note that other researchers may wish to take this further if they think more could be gained from additional interviews or research. I did attempt to find wider participation than law enforcement, contacting regulators as well as members of the memorable alliance but I was not successful in securing participants. One individual from a regulator declined due to sensitivity around some ongoing work, and individuals at the Bank of England stopped replying to my emails without reason after being initially receptive. I have no indication why this was the case. I also had a negative response from a higher-ranking officer within law enforcement. This may well also have been due to sensitivity about being able to comment. My research was on practitioners of cryptocurrencies in law enforcement, and they appeared to be free to talk. There is certainly scope for wider research of other entities or seniorities, and this would be welcomed.

And finally, there were some other limitations to the HullCoin case study. The HullCoin project involved a small team and Kaini Industries was dissolved in 2021. Again, I was able to interview the two key founders and so I felt that I gathered the information that was needed. But I was limited to online work, and it may well be that research in the geographical area could have been beneficial even though the project had ended. I did try to contact other team members. One declined as there had been some acrimony and the technical team member did not respond. I would of course have liked to have spoken to these individuals as well.

The sample sizes for the interviews of law enforcement officers and the HullCoin case study were, therefore, small and this is an accepted limitation of this study. Whilst access is necessarily a challenge, especially for law enforcement officers, the small size of the samples does potentially raise questions for other researchers. However, I believe the rich depth of the interviews provides fascinating insights nonetheless.

8.5 Key Implications

There will likely be no solution to the ‘security impasse’ about cryptocurrencies in the foreseeable future. Whilst cryptocurrencies are not an existential threat, the prospect of viable, competing non-state monies does have the potential to change how states conduct their affairs, especially those that have enjoyed the ‘exorbitant privilege’ that monopoly of state money can bring. Several key implications emerge from the research questions of this study. This section presents them by groups of the most relevant stakeholders:

1. Monetary theorists

- This thesis contends that there is a problem with a state monopoly of money, as other researchers and famous thinkers have claimed. In the immediate term, there is a need for a more consistent and clearer definition of money. The terminology used in the literature can be conflicting and leads to confused definitions, including in law. Clearer definitions would go some way towards achieving a base to move discussions about money forward.

- In the longer term, there is a need to reform money in ways that allow for innovation. Clarity about monetary definitions, particularly in law, would allow for experimentation. Interestingly, inflation used to be about the money supply but this has transformed into a modern focus on price inflation. The elements proposed here in the ‘question of money’ would provide a longer-term focus for theoretical work on money.

2. Securitisation theorists

- The economic sector of securitisation theory has much to offer and is a valid area for further research. More studies are encouraged in this under-researched area of the theory.

- The Copenhagen version of securitisation theory is particularly useful for the ‘early’ stages of security threat analysis e.g., who, why, and what threats. The theory then struggles when it comes to what is evidence of securitisation and whether something has been accepted as securitised. This is reflected in the literature on the theory. For an analyst using the theory, this makes the ‘later’ stages of analysis less clear. Perhaps the theory could be improved to consolidate other scholarly views into a working modern theory. This could include, as suggested here, the inclusion of inaction and blocking as evidence of potential securitisation.

3. Security researchers

- Bitcoin and cryptocurrencies are not used in an overwhelming amount of crime – by volume or percentage of use. In the short term, this needs to be monitored and attention paid to any area where this changes.

- A great deal of academic research has focussed on the extent to which cryptocurrencies provide anonymity. If this is not the main advantage of cryptocurrencies, as suggested here, then there may be value in researching the finality of transactions as the more important driver of use.

- The dark net threat is a niche, retail market. The threat is overexaggerated. The implication is that effort is potentially focussed on the wrong threats. Law enforcement as well as security researchers should consider this point and aim to do more research on major threats that do not get as much attention. For example, there is little research on the use of cash in crime.

4. Complementary currency researchers

- A cryptocurrency model appears to be a useful one for complementary currencies, offering a low-cost, scalable solution. This may be worth noting for future complementary currency initiatives.

- Longer-term, there are several issues that need addressing if complementary currencies are to have a sustained impact. Firstly, HullCoin had issues about being money. Projects will continue to face resistance without a legal basis for these endeavours. This ties in with the points above for monetary theorists, and legal scholars as creators of laws on money. Funding for social initiatives was also a key factor in the end of the HullCoin project. How non-profit projects are funded is also a longer-term concern.

- Following on from the previous point, there is a challenge in changing the perceptions of complementary currencies. Normalising their concept and establishing them as legitimate and needed currencies alongside state monies would alleviate many of the difficulties that projects repeatedly encounter.

5. Policy makers

- Banning cryptocurrencies is unlikely to work – The network effects that Bitcoin in particular has achieved across borders means that bans may be futile. In a security dilemma, bans would likely push illicit activity underground and reduce the opportunity for law enforcement success. It is better to continue with the regulation of legitimate services, as several countries are doing.

- The dark net should be kept in perspective – Empirical facts and user behaviour should determine which threats to focus on. Fear of the dark net has overexaggerated the threat that it poses, and this has come at the cost of significant effort being deflected from more pressing concerns.

- Reconsider the monopoly of state money – History conclusively shows the abuse and misuse that has taken place of state money. In particular, complementary currencies like Lietaer’s Civics should be allowed to attempt to improve economic conditions in disadvantaged communities. Theoretical proposals about how to better manage the supply of money should be developed.

- Consider that future societies will move beyond state money – There needs to be a conceptual shift if any tension about money is to dissipate. To do this, policy makers will need to challenge the axiomatic belief that only the state can manage money. This thesis has shown that this is not the case and that there will be advantages to having competing currencies beyond the state level.

8.6 Future Work

I began this work with few expectations, beliefs, or positions, but I leave with many of the latter two. I am now convinced that the existing financial system is flawed, systemically drives inequality and is likely to continue its boom-bust nature. And for these reasons, I believe that this is an important topic and one which is deserving of further research. In particular, there are three main areas that I would like to see studied in greater depth.

My initial interest in this topic was the criminal use of cryptocurrencies, but it was only after I discovered that this is not a valid basis for a securitising claim against cryptocurrencies that I delved further into the history of money. There, I found the long struggle that there has been over state money. The research took me deeper into this aspect, but it was not the original focus of this study. There is, therefore, much that could be done to research the memorable alliance further. I did attempt to do this in the course of this work. I applied for an internship at the Bank of England, I also tried to recruit participants from UK regulators and also the Bank of England, but none of these attempts were successful. Research of the views of the memorable alliance would be fascinating if anyone could get access. In particular, does the alliance conflate Ingham's two sources of power? That is if the alliance could not freely increase the supply of money, would they still retain power by having more money than anyone else? Whilst I have shown that criminal use of cryptocurrencies does not amount to an existential threat in the economic sector, further research could be done into the threats that the memorable alliance perceive. If cash is a more useful criminal tool, why do they think that cryptocurrencies are a threat? Is crime really the concern or is it to do with power as I suggest in this chapter? I used a constructivist approach to examine illicit use from the perspective of the users, a similar approach to the memorable alliance may also be revealing. And finally, can they conceive of a future beyond state money or, at least, of other ways to better manage the supply of money?

The second broad area I would like to see more research in is the application of securitisation theory to Bitcoin and cryptocurrencies, and in the economic sector more generally. This thesis focussed on the extent and reasons for an attempted securitisation, but some aspects could be researched in more depth. Whilst I have argued that the public and law enforcement officers appear not to have accepted that cryptocurrencies are a security threat, further work could be done to research audiences specifically. Perhaps other audiences have accepted securitisation. In terms of the economic sector and a lower threshold for securitisation, more research could also be done examining the measures that states have taken against cryptocurrencies. There are likely many other examples that are evidence of securitisation in terms of an action-focussed approach.

Lastly, the final area where I think there is scope for further research is the use of cryptography in society. This is also of great importance to discussions about cryptocurrencies. Whether financial transactions could or should be private is another fundamental issue that underpins much uncertainty in this subject. As an extension of the debates about the confidentiality of messages, should the state retain an ability to monitor citizens' financial transactions? This is particularly of interest to me as this question is more of a modern phenomenon. Before the internet and electronic transactions, the state did not have the abilities that it has now, and society appeared to function well enough. Especially since 9/11 though, there has been an increased motivation for prevention rather than reaction. And this has led to more invasion of privacy. There will likely be continued tension and confusion in policy about cryptocurrencies, and especially more privacy focussed variants, as long as larger questions about the use of cryptography and the privacy of financial transactions go unanswered and unresolved.

9 Bibliography

Abramova, S., & Böhme, R. (2016). Perceived Benefit and Risk as Multidimensional Determinants of Bitcoin Use: A Quantitative Exploratory Study. *Proceedings of the Thirty-Seventh International Conference on Information Systems (ICIS 2016)*, 1–20.

Ahmed, T., Becker, C., Berkhout, E., Boe, K., Bunting, H., Carty, T., Collins, C., Cortes, H., Craeynest, L., Daar, N., Duvisac, S., Espinoza Revollo, P., Gielfeldt, J., Grainger, M., Guijt, I., Hallum, C., Harnett, V., Hersi, A., Jacobs, D., … Hardoon, D. (2022). *Inequality Kills*. https://doi.org/10.21201/2022.8465

Alawa, P. (2013). Martin Heidegger on Science and Technology: It’s Implication to the Society. *IOSR Journal Of Humanities And Social Science (IOSR-JHSS)*, *12*(6), 1.

Albanesi, S. (2007). Inflation and inequality. *Journal of Monetary Economics*, *54*(4), 1088–1114. https://doi.org/10.1016/j.jmoneco.2006.02.009

Alderman, L. (2018). *Sweden’s Push to Get Rid of Cash Has Some Saying, ‘Not So Fast.’* The New York Times. https://www.nytimes.com/2018/11/21/business/sweden-cashless-society.html

Aldridge, J., Stevens, A., & Barratt, M. J. (2018). Will growth in cryptomarket drug buying increase the harms of illicit drugs? *Addiction*, *113*(5). https://doi.org/10.1111/add.13899

Ali, M., B, A., Emms, M., & Moorsel, van A. (2017). Does The Online Card Payment Landscape Unwittingly Facilitate Fraud? *IEEE Security & Privacy*.

Alshamsi, A., & Andras, P. P. (2019). User perception of Bitcoin usability and security across novice users. *International Journal of Human-Computer Studies*, *126*, 94–110. https://doi.org/10.1016/J.IJHCS.2019.02.004

Ammous, S. (2018). Can cryptocurrencies fulfil the functions of money? *The Quarterly Review of Economics and Finance*, *70*, 38–51. https://doi.org/10.1016/J.QREF.2018.05.010

Amoore, L., & De Goede, M. (2005). Governance, risk and dataveillance in the war on terror. *Law & Social Change*, *43*, 149–173. https://doi.org/10.1007/s10611-005-1717-8

Ampleforth. (2021). *The Basics*. https://www.ampleforth.org/basics/

Anderson, R. (2007). *Closing the Phishing Hole-Fraud, Risk and Nonbanks*.

Androulaki, E., Karame, G. O., Roeschlin, M., Scherer, T., & Capkun, S. (2013). Evaluating user privacy in Bitcoin. *Paper Presented to Financial Cryptography and Data Security, 17th International Conference, Okinawa, Japan, 1-5 April*.

Anon. (2018). *Dark Net Market's Buyer Bible*.

Antonopoulos, A. (2017). *Mastering Bitcoin: Programming the Open Blockchain* (Second). O'Reilly Media.

Aste, T., Tasca, P., & Di Matteo, T. (2017). Blockchain Technologies: foreseeable impact on industry and society. *Computer*, *50*(9), 18–28. https://doi.org/10.1109/MC.2017.3571064

Bailey, A. M., Rettler, B., & Warmke, | Craig. (2021a). Philosophy, politics, and economics of cryptocurrency I: Money without state. *Philosophy Compass*. https://doi.org/10.1111/phc3.12785

Bailey, A. M., Rettler, B., & Warmke, | Craig. (2021b). Philosophy, politics, and economics of cryptocurrency II: The moral landscape of monetary design. *Philosophy Compass*. https://doi.org/10.1111/phc3.12784

Bain, B. (2021). *U.S. Won't Ban Crypto Like China, Says SEC Chair Gensler*. Bloomberg.Com.

Balzacq, T., Léonard, S., & Ruzicka, J. (2016). 'Securitization' revisited: theory and cases. *International Relations*, *30*(4), 494–531. https://doi.org/10.1177/0047117815596590

Bambrough, B. (2019). *Bitcoin Threatens To "Take Power" From The U.S. Federal Reserve*. Forbes.

Bancroft, A. (2017). Responsible use to responsible harm: illicit drug use and peer harm reduction in a darknet cryptomarket. *Health, Risk and Society*, *19*(7–8), 336–350. https://doi.org/10.1080/13698575.2017.1415304

Bancroft, A., & Scott Reid, P. (2016). Challenging the techno-politics of anonymity: the case of cryptomarket users. *Information, Communication & Society*. https://doi.org/10.1080/1369118X.2016.1187643

Bank of England. (2019). *What is money?* https://www.bankofengland.co.uk/knowledgebank/what-is-money

Bank of England. (2021). *Update on the future of Wholesale Cash Distribution in the UK*. https://www.bankofengland.co.uk/paper/2021/update-on-the-future-of-wholesale-cash-distribution-in-the-uk

Bank of England. (2022). *Banknote statistics*. https://www.bankofengland.co.uk/statistics/banknote

Barratt, M. J., & Aldridge, J. (2016). Everything you always wanted to know about drug cryptomarkets* (*but were afraid to ask). *International Journal of Drug Policy*, *35*. https://doi.org/10.1016/j.drugpo.2016.07.005

Barratt, M. J., Ferris, J. A., & Winstock, A. R. (2016). Safer scoring? Cryptomarkets, social supply and drug market violence. *International Journal of Drug Policy*, *35*. https://doi.org/10.1016/j.drugpo.2016.04.019

Barratt, M. J., & Maddox, A. (2016). Active engagement with stigmatised communities through digital ethnography. *Qualitative Research*, *16*(6), 701–719. https://doi.org/10.1177/1468794116648766

Bartlett, J. (2014). *The Dark Net*. Random House.

Barysevich, A., & Solad, A. (2018). *Litecoin Emerges as the Next Dominant Dark Web Currency*.

Bashir, M., Strickland, B., & Bohr, J. (2016). What motivates people to use Bitcoin? *LNCS*, *10047*, 347–367. https://doi.org/10.1007/978-3-319-47874-6_25

Batini, N., Eyraud, L., Forni, L., & Weber, A. (2014). *Fiscal Multipliers: Size, Determinants, and Use in Macroeconomic Projections*.

Baur, A., Breitsprecher, M., & Bick, M. (2014). Catching Fire: Start-Ups in the Text Analytics Software Industry. *AMCIS 2014 Proceedings*.

Baur, A., Bühler, J., Bick, M., & Bonorden, C. S. (2015). Cryptocurrencies as a disruption? empirical findings on user adoption and future potential of Bitcoin and Co. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9373*, 63–80. https://doi.org/10.1007/978-3-319-25013-7_6

BBC News. (2015). *All Greek to you? Greece’s debt jargon explained*. https://www.bbc.co.uk/news/world-europe-33311405

BBC News. (2018). *Bill Gates says crypto-currencies cause deaths*. https://www.bbc.co.uk/news/technology-43239781

BBC News. (2021a). *Met Police seize record £180m of cryptocurrency in London*.

BBC News. (2021b). *NatWest fined £265m after bin bags of cash laundered*.

Belur, J. (2014). Status, gender and geography: power negotiations in police research. *Qualitative Research*, *14*(2), 184–200. https://doi.org/10.1177/1468794112468474

Benson, J. (2022). *Grayscale Considers Flipping the Script and Suing SEC Over Bitcoin ETF*. Decrypt. https://decrypt.co/96239/grayscale-considers-flipping-script-suing-sec-bitcoin-etf

Berkovitz, U. (2020). *Colu shuts digital wallet, leaves Israeli market*. Globes. https://en.globes.co.il/en/article-colu-shuts-digital-wallet-leaves-israeli-market-1001349550

Berr, J. (2017). *"WannaCry" ransomware attack losses could reach $4 billion*. CBS News. https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/

Binder, C. (2019). Inequality and the inflation tax. *Journal of Macroeconomics*, *61*, 103122. https://doi.org/10.1016/j.jmacro.2019.103122

Bitcoin Core. (2021). *About*. https://bitcoincore.org/en/about/

Bitinfocharts.com. (2020). *Monero Transactions Chart*. https://bitinfocharts.com/comparison/monero-transactions.html

Bitinfocharts.com. (2021). *Bitcoin Sent in USD Chart*. https://bitinfocharts.com/comparison/sentinusd-btc.html#6m

BitMEX Research. (2021). *The Blocksize War – Chapter 1 – First Strike*. BitMEX Blog. https://blog.bitmex.com/the-blocksize-war-chapter-1-first-strike/

Bjerg, O. (2016). How is Bitcoin Money? *Culture & Society*, *33*(1), 53–72. https://doi.org/10.1177/0263276415619015

Blandin, A., Cloots, A. S., Hussain, H., Rauchs, M., Saleuddin, R., Allen, J. G., Zhang, B., & Cloud, K. (2019). *Global Cryptoasset Regulatory Landscape Study*.

Bohr, J., & Bashir, M. (2014). Who Uses Bitcoin? An exploration of the Bitcoin community. *2014 Twelfth Annual International Conference on Privacy, Security and Trust*, 94–101. https://doi.org/10.1109/PST.2014.6890928

Bold, C. (2012). *Using Narrative in Research*. SAGE Publications Ltd. https://doi.org/10.4135/9781446288160

Boughton, J. M. (2001). *Silent revolution : The International Monetary Fund, 1979-89*. International Monetary Fund.

Brady, M. E. (2020). The Myth of Richard Kahn and the Multiplier: Keynes, Not Kahn, Created the Multiplier Concept in 1921 in His a Treatise on Probability and Taught Kahn How to Write His June, 1931 Economic Journal Paper. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3659745

Brandom, R. (2019). *Senators aren't sold on Facebook's Libra project*. The Verge.

https://www.theverge.com/2019/7/16/20696350/facebook-libra-senate-banking-committee-hearing-david-marcus-cryptocurrency

Brett, J. (2020a). *11 Members Of Congress Urge Treasury Secretary Mnuchin To Use Blockchain For COVID-19 Stimulus Payments*. Forbes.

Brett, J. (2020b). *Digital Dollar And Digital Wallet Bill Surfaces In The U.S. Senate*. Forbes. https://www.forbes.com/sites/jasonbrett/2020/03/24/digital-dollar-and-digital-wallet-legislation-surfaces-in-the-us-senate/#4b8df12c3866

Brett, J. (2021). *In 2021, Congress Has Introduced 35 Bills Focused On U.S. Crypto Policy*. Forbes. https://www.forbes.com/sites/jasonbrett/2021/12/27/in-2021-congress-has-introduced-35-bills-focused-on-us-crypto-policy/

Bryman, A. (2012). *Social Research Methods* (Fourth). Oxford University Press.

BSC. (2015). *British Society Of Criminology Statement Of Ethics 2015*.

Business Insider. (2018). *Sweden's reduced cash circulation means black market crimes increase*. https://www.businessinsider.com/swedens-reduced-cash-circulation-means-black-market-crimes-increase-2018-6?r=US&IR=T

Butler, S. (2019). Criminal use of cryptocurrencies: a great new threat or is cash still king? *Journal of Cyber Policy*, *4*(3), 326–345. https://doi.org/10.1080/23738871.2019.1680720

Butler, S. (2020). *Cyber 9/11 Will Not Take Place: A User Perspective of Bitcoin and Cryptocurrencies from Underground and Dark Net Forums*. 135–153. https://doi.org/10.1007/978-3-030-79318-0_8

Butler, S. (2021). The Philosophy of Bitcoin and the Question of Money. *Theory, Culture & Society*. https://doi.org/10.1177/02632764211049826

Buzan, B., Waever, O., & de Wilde, J. (1998). *Security: A new Framework for Analysis*. Lynne Rienner Publishers.

Cagan, P. (1989). Hyperinflation. In J. Eatwell, M. Milgate, & P. Newman (Eds.), *Money* (pp. 179–184). Palgrave Macmillan UK. https://doi.org/10.1007/978-1-349-19804-7_20

Canzoneri, M., Cumby, R., Diba, B., & López-Salido, D. (2013). Key currency status: An exorbitant privilege and an extraordinary risk. *Journal of International Money and Finance*, *37*, 371–393. https://doi.org/10.1016/J.JIMONFIN.2013.06.006

Carney, M. (2018). *Speech - The Future of Money*. Bank of England.

Casciani, D. (2010). *500 euro note - why criminals love it so*. BBC News. http://news.bbc.co.uk/1/hi/8678979.stm

Chainalysis. (2021). *The 2021 Crypto Crime Report*.

Chainalysis. (2022). *Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity*.

Champagne, P. (2014). *The Book of Satoshi*. E53 Publishing LLC.

Chan, S. P. (2019). *Facebook's digital currency dealt another blow*. BBC News.

Chaum, D. (1983). Blind Signatures for Untraceable Payments. *Advances in Cryptology*, 199–203.

Chernilo, D. (2007). *A social theory of the nation-state: The political forms of modernity beyond methodological nationalism*. Routledge. https://doi.org/10.4324/9780203932650

Chertoff, M. (2017). A public policy perspective of the Dark Web. *Journal of Cyber Policy*, *2*(1), 26–38. https://doi.org/10.1080/23738871.2017.1298643

Cimpanu, C. (2019). *I2P network proposed as the next hiding spot for criminal operations*. ZDNet. https://www.zdnet.com/article/i2p-network-proposed-as-the-next-hiding-spot-for-criminal-operations/

Cleland, V. (2018). *Cash and digital payments in the new economy: Response from the Bank of England to HM Treasury's call for evidence*.

CNBC Television. (2019). *Former FDIC Chair Sheila Bair: Americans are right to cut back on spending*.

Cobbett, W. (1828). *Paper against Gold*.

Coinbase. (2021). *About - Coinbase*. https://www.coinbase.com/about

Coinbase. (2022). *About*. https://www.coinbase.com/about

Coinmarketcap. (2020). *Bitcoin price, charts, market cap, and other metrics | CoinMarketCap*. https://coinmarketcap.com/currencies/bitcoin/

Cointelegraph. (2017). *IRS Uses Chainalysis to Track Down Bitcoin Tax Cheats*. https://cointelegraph.com/news/irs-uses-chainalysis-to-track-down-bitcoin-tax-cheats

Coinut.com. (2019). *Is Litecoin a fork of Bitcoin?* https://coinut.com/blog/is-litecoin-a-fork-of-bitcoin/

Collier, B., Clayton, R., Hutchings, A., & Thomas, D. R. (2020). Cybercrime is (often) boring: maintaining the infrastructure of cybercrime economies. *Workshop on the Economics of Information Security*. https://doi.org/https://doi.org/10.17863/CAM.53769

Corbetta, P. (2003). *Social research: theory, methods and techniques*. SAGE Publications.

Council of Economic Advisors. (2020, February 20). *Gross Federal Debt*. Retrieved from FRED, Federal Reserve Bank of St. Louis. https://fred.stlouisfed.org/series/FYGFD

Creswell, J. W. (2009). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (Third). SAGE Publications.

Cuthbertson, A. (2019). *Trump tweets he is 'not a fan' of bitcoin, inadvertently boosting cryptocurrency price*. The Independent.

Damsa, D., & Ugelvik, T. (2017). A Difference That Makes a Difference? Reflexivity and Researcher Effects in an All-Foreign Prison. *International Journal of Qualitative Methods*, *16*(1), 160940691771313. https://doi.org/10.1177/1609406917713132

Davies, G. (2002). *A History of Money: From Ancient Times to the Present Day*. University of Wales Press.

De Goede, M. (2012). The SWIFT Affair and the Global Politics of European Security*. *Journal of Common Market Studies*, *50*(2), 214–230. https://doi.org/10.1111/j.1468-5965.2011.02219.x

De, N., & Ligon, C. (2022). *New York State Senate Passes Bitcoin Mining Moratorium*. Coindesk. https://www.coindesk.com/policy/2022/06/03/new-york-senate-passes-bitcoin-mining-moratorium/

DeCambre, M. (2020). *Head of world's largest asset manager says bitcoin can possibly 'evolve into a global market' asset*. MarketWatch. https://www.marketwatch.com/story/head-of-worlds-largest-asset-manager-says-bitcoin-can-possibly-evolve-into-a-global-market-asset-11606854857

del Castillo, M. (2022). *Bitcoin Bank Custodia Sues Federal Reserve, Demanding Decision On Master Account*. Forbes. https://www.forbes.com/sites/michaeldelcastillo/2022/06/07/bitcoin-bank-custodia-sues-federal-reserve-demanding-decision-on-master-account/

Diffie, W., & Hellman, M. E. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644–654. https://doi.org/10.1109/TIT.1976.1055638

Dodd, N. (2012). Simmel's Perfect Money: Fiction, Socialism and Utopia in The Philosophy of Money. *Theory, Culture and Society*, *29*(7–8), 146–176.

https://doi.org/10.1177/0263276411435570

Dodd, N. (2017). The Social Life of Bitcoin. *Theory, Culture & Society*, *35*(3), 35–56. https://doi.org/10.1177/0263276417746464

Dolliver, D. S., & Kenney, J. L. (2016). Characteristics of Drug Vendors on the Tor Network: A Cryptomarket Comparison. *Victims & Offenders*, *11*(4), 600–620. https://doi.org/10.1080/15564886.2016.1173158

Dolmas, J., Huffman, G. W., & Wynne, M. A. (2000). Inequality, Inflation, and Central Bank Independence. *The Canadian Journal of Economics*, *33*(1), 271–287.

Drezner, D. W. (2010). Will currency follow the flag? *International Relations of the Asia-Pacific*, *10*(3), 389–414. https://doi.org/10.1093/irap/lcq008

Elliptic. (2022). *New York Husband and Wife Arrested for Laundering Bitcoin*. https://www.elliptic.co/blog/elliptic-analysis-new-york-husband-and-wife-arrested-for-laundering-5-billion-in-bitcoin-stolen-from-bitfinex-in-2016

European Central Bank. (2016). *ECB ends production and issuance of €500 banknote*. https://www.ecb.europa.eu/press/pr/date/2016/html/pr160504.en.html

European Commission. (2018). *Strengthened EU rules to prevent money laundering and terrorist financing*.

European Monitoring Centre for Drugs and Drug Addiction. (2016). *EU Drug Markets Report*.

European Monitoring Centre for Drugs and Drug Addiction and Europol. (2017). *Drugs and the darknet*.

Europol. (2015). *Why Cash is Still King? A strategic report on the use of cash by criminal groups as a facilitator for money laundering*.

Europol. (2021). Internet Organised Crime Threat Assessment (IOCTA) 2021. In *Publications Office of the European Union*.

Europol EC3. (2017). *Internet Organised Crime Threat Assessment (IOCTA) 2017*. https://doi.org/10.2813/55735

Fairclough, S. (2021). *Universal basic income: Wales' trial "should include everyone."* BBC News.

Fan, L.-S., & Fan, C.-M. (2002). The Mundell-Fleming Model Revisited. In *The American Economist* (Vol. 46, Issue 1).

Fanusie, & Robinson, T. (2018). *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services*.

Farrell, G., & Larson, E. (2013). *Lawsky Says 'So Be It' If Transparency Harms*

Bitcoin. Bloomberg.Com.

Ferguson, N. (2008). *The Ascent of Money: A Financial History of the World*. Allen Lane.

Fernando, A. (2017). *The English city with its own cryptocurrency: Q&A with the founders of HullCoin*. Shareable. shareable.net

Ferreira, J., Perry, M., & Subramanian, S. (2015). Spending Time with Money: From Shared Values to Social Connectivity. *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing - CSCW '15*, 1222–1234. https://doi.org/10.1145/2675133.2675230

Financial Action Task Force. (2018). *International Standards on Combating Money Laundering and the Financing of Terrorism &amp; Proliferation: The FATF Recommendations*.

Financial Conduct Authority. (2018). *Cyber and technology resilience in UK financial services*. Speech by Megan Butler. https://www.fca.org.uk/news/speeches/cyber-and-technology-resilience-uk-financial-services

Fish, T., & Whymark, R. (2015). How has cash usage evolved in recent decades? What might drive demand in the future? *Bank of England Quarterly Bulletin*, *55*(3).

Fisher, I. (1922). *The Purchasing Power of Money*. Macmillan.

Floyd, R. (2019). Evidence of securitisation in the economic sector of security in Europe? Russia's economic blackmail of Ukraine and the EU's conditional bailout of Cyprus. *European Security*. https://doi.org/10.1080/09662839.2019.1604509

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2018). Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? *Ssrn*. https://doi.org/10.2139/ssrn.3102645

Foreign & Commonwealth Office and Lord Ahmad of Wimbledon. (2017). *Foreign Office Minister condemns North Korean actor for WannaCry attacks*. https://www.gov.uk

Foreign & Commonwealth Office, National Cyber Security Centre, & Lord Ahmad of Wimbledon. (2018). *Foreign Office Minister condemns Russia for NotPetya attacks*. https://www.gov.uk

Frankel, J. (2021). *El Salvador's adoption of bitcoin as legal tender is pure folly*. The

Guardian.

Friedman, M. (1968). The Role of Monetary Policy. *The American Economic Review*, *58*(1), 1–17.

Furnham, A., Wilson, E., & Telford, K. (2012). The meaning of money: The validation of a short money-types measure. *Personality and Individual Differences*, *52*, 707–711. https://doi.org/10.1016/j.paid.2011.12.020

Gao, X., Clark, G. D., & Lindqvist, J. (2016). Of Two Minds, Multiple Addresses, and One Ledger: Characterizing Opinions, Knowledge, and Perceptions of Bitcoin Across Users and Non-Users. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/2858036.2858049

Gehl, R. W. (2016). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media and Society*, *18*(7). https://doi.org/10.1177/1461444814554900

Gehl, R. W. (2018). Archives for the Dark Web: A Field Guide for Study. In *Research Methods for the Digital Humanities* (pp. 31–51). Springer International Publishing. https://doi.org/10.1007/978-3-319-96713-4_3

Gerrard, J. (2020). *Hull has highest jobless rate in the UK as unemployment soars*. Hull Daily Mail. https://www.hulldailymail.co.uk/news/hull-east-yorkshire-news/hull-unemployment-highest-jobless-rates-4526465

Gharibshah, J., Atlantic, F., Raton, B., Evangelos, F., & Papalexakis, E. (2019). An Empirical Study of Malicious Threads in Security Forums. *The Web Conference*, 176–182. https://doi.org/10.1145/3308560.3316501

Gilson, D. (2014). *Hullcoin: The World's First Local Government Cryptocurrency?* Coindesk. https://www.coindesk.com/hullcoin-worlds-first-local-government-cryptocurrency

Glaser, F., Zimmerman, K., Haferkorn, M., Weber, M., & Siering, M. (2014). Bitcoin - Asset or Currency? Revealing Users' Hidden Intentions. *22nd European Conference on Information Systems*.

Global System for Mobile communications Association. (2018). The Mobile Economy. *GSMA Intelligence*, *35*, 11–11. https://doi.org/10.5121/ijcsit.2015.7409

Gloerich, I., Lovink, G., & De Vries, P. (Eds.). (2018). *MoneyLab Reader 2*. Institute of Network Cultures.

Gov.uk. (2022). *Council tax rebate: factsheet*. https://www.gov.uk/guidance/council-tax-rebate-factsheet

Grasshoff, G., Mogul, Z., Pfuhler, T., Gittfried, N., Wiegand, C., Bohn, A., & Vonhoff, V. (2017). *Global Risk 2017: Staying the Course in Banking*. Boston Consulting Group. https://www.bcg.com

Harvey, J., & Branco-Illodo, I. (2020). Why Cryptocurrencies Want Privacy: A Review of Political Motivations and Branding Expressed in “Privacy Coin” Whitepapers. *Journal of Political Marketing*, *19*(1–2), 107–136. https://doi.org/10.1080/15377857.2019.1652223

Hayek, F. A. (1990). *Denationalisation of Money: The Argument Refined* (Third). The Institute of Economic Affairs.

Hayek, F. A. (2005). *The Road to Serfdom: with The Intellectuals and Socialism* (Condensed). The Institute of Economic Affairs.

Hayes, A. (2017). Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin. *Telematics and Informatics*, *34*, 1308–1321. https://doi.org/10.1016/j.tele.2016.05.005

Hayes, A. (2018). Bitcoin price and its marginal cost of production: support for a fundamental value. *Applied Economics Letters*.

Hayes, A. (2019). The Socio-Technological Lives of Bitcoin. *Theory, Culture and Society*. https://doi.org/10.1177/0263276419826218

Hayes, A. (2021). World monies or money-worlds: A new perspective on cryptocurrencies and their moneyness. *Finance and Society*, *7*(2), 130–139.

Hayes, K. (2021). Ransomware: a growing geopolitical threat. *Network Security*, *2021*(8), 11–13. https://doi.org/10.1016/S1353-4858(21)00089-1

Hendrickson, J. R., & Luther, W. J. (2017). Banning bitcoin. *Journal of Economic Behavior & Organization*, *141*, 188–195. https://doi.org/10.1016/j.jebo.2017.07.001

Herbst, J. (2019). *Community Currency Program Aims to Boost Local Kenyan Economies*. Breakermag.Com. https://breakermag.com/community-currency-program-aims-to-boost-local-kenyan-economies/

Higgins, S. (2019). *EU Authorities Shut Down Bitcoin Transaction Mixer*. Coindesk.Com. https://www.coindesk.com/eu-authorities-crack-down-on-bitcoin-transaction-mixer

HM Revenue & Customs. (2019). *Measuring tax gaps 2019 edition*.

HM Treasury. (2018). *Cash and digital payments in the new economy: call for evidence*.

HM Treasury. (2019). *Cash and digital payments in the new economy: summary of responses*.

HM Treasury, Financial Conduct Authority, & Bank of England. (2018). *Cryptoassets Taskforce: final report*.

HM Treasury, & Home Office. (2017). *National risk assessment of money laundering and terrorist financing 2017*.

HMIC. (2015). *Regional Organised Crime Units: A review of capability and effectiveness*.

Holt, T. J. (2017). Identifying gaps in the research literature on illicit markets on-line. *Global Crime*, *18*(1), 1–10. https://doi.org/10.1080/17440572.2016.1235821

Huang, R. (2019). *China's Digital Currency Is Unlikely To Be A Cryptocurrency*. Forbes. https://www.forbes.com/sites/rogerhuang/2019/08/14/chinas-digital-currency-is-unlikely-to-be-a-cryptocurrency/#aa5654b6a521

Hughes, E. (1993). *A Cypherpunk's Manifesto*. https://www.activism.net/cypherpunk/manifesto.html

Hull City Council. (2017). *Hull Joint Strategic Needs Assessment*.

HullCoin. (2020a). *Giving your community the credit it deserves*. https://www.hull-coin.org/

HullCoin. (2020b). *HullCoin: How does it work?*

Hume, T. (2013). *How the FBI caught Ross Ulbricht, alleged creator of Silk Road*. CNN. https://edition.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht/index.html

Hutchings, A., & Pastrana, S. (2019). Understanding eWhoring. *Proceedings - 4th IEEE European Symposium on Security and Privacy, EURO S and P 2019*, 201–214. https://doi.org/10.1109/EuroSP.2019.00024

IBM. (2019). *About IBM SPSS Modeler Text Analytics*. https://www.ibm.com/support/knowledgecenter/en/SS3RA7_15.0.0/com.ibm.spss.ta.help/tmfc_intro.htm?pos=3

IBM. (2021a). *About text mining*. https://www.ibm.com/docs/en/spss-modeler/SaaS?topic=analytics-about-text-mining

IBM. (2021b). *How categorization works*. https://www.ibm.com/docs/en/spss-modeler/SaaS?topic=mining-how-categorization-works

Imbert, F. (2017a). *BlackRock CEO Larry Fink calls bitcoin an "index of money laundering."* CNBC. https://www.cnbc.com/2017/10/13/blackrock-ceo-larry-fink-calls-bitcoin-an-index-of-money-laundering.html

Imbert, F. (2017b). *JPMorgan CEO Jamie Dimon says Bitcoin is a "fraud" that will eventually blow up*. Cnbc.Com.

Ingham, G. (2004). The Nature of Money. *Economic Sociology: European Economic Newsletter*, *5*(2), 18–28.

Ingham, G. (2006). Further reflections on the ontology of money: Responses to Lapavitsas and Dodd. *Economy and Society*, *35*(2), 259–278. https://doi.org/10.1080/03085140600635730

Ingham, G. (2020). *Money*. Polity Press.

International Monetary Fund. (2022). *El Salvador's Comeback Constrained by Increased Risks*. https://www.imf.org/en/News/Articles/2022/02/15/cf-el-salvadors-comeback-constrained-by-increased-risks

Isige, J. (2019). *"I won't be talking about Bitcoin in 10 years" US Treasury Secretary Mnuchin*. FXStreet. https://www.fxstreet.com/cryptocurrencies/news/i-wont-be-talking-about-bitcoin-in-10-years-us-treasury-secretary-mnuchin-201907241546

Jaishankar, K. (2007). Cyber criminology and Space Transition Theory. In *International Journal of Cyber Criminology* (Vol. 1, Issue 2).

Jarvis, C. (2021). *Crypto Wars*. CRC Press. https://doi.org/10.1201/9781003123675

Jervis, R. (1978). Cooperation Under the Security Dilemma. *World Politics*, *30*(2), 167–214.

Kahney, L. (2019). *The FBI Wanted a Backdoor to the iPhone. Tim Cook Said No*. Wired. https://www.wired.com/story/the-time-tim-cook-stood-his-ground-against-fbi/

Kaini Industries. (2014). *HullCoin Briefing Paper*.

Kappos, G., Yousaf, H., Maller, M., & Meiklejohn, S. (2018). An Empirical Analysis of Anonymity in Zcash. *Proceedings of the 27th USENIX Security Symposium*.

Karlstrøm, H. (2014). Do libertarians dream of electric coins? The material embeddedness of Bitcoin. *Distinktion: Journal of Social Theory*, *15*(1), 23–36. https://doi.org/10.1080/1600910X.2013.870083

Keatinge, T., Carlisle, D., & Keen, F. (2018). *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*.

Kethineni, S., & Cao, Y. (2019). The Rise in Popularity of Cryptocurrency and

Associated Criminal Activity. *International Criminal Justice Review*, *30*(3), 325–344. https://doi.org/10.1177/1057567719827051

Kethineni, S., Cao, Y., & Dodge, C. (2018). Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes. *American Journal of Criminal Justice*, *43*(2). https://doi.org/10.1007/s12103-017-9394-6

Keynes, J. M. (1923). *A Tract on Monetary Reform*. Macmillan and Co Ltd.

Keynes, J. M. (1933). *An Open Letter to President Roosevelt*.

Keynes, J. M. (1936). *The General Theory of Employment, Interest, and Money*.

Kfir, I. (2020). Cryptocurrencies, national security, crime and terrorism. *Https://Doi.Org/10.1080/01495933.2020.1718983*, *39*(2), 113–127. https://doi.org/10.1080/01495933.2020.1718983

Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., Kirda, E., & Robertson, W. (2015). Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. *Paper Presented to the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Milan, Italy, 9-10 July*. https://doi.org/10.1007/978-3-319-20550-2_1

Knapp, G. F. (1924). *The State Theory of Money*. Macmillan and Co Ltd.

Kondor, D., Pósfai, M., Csabai, I., & Vattay, G. (2014). Do the rich get richer? An empirical analysis of the Bitcoin transaction network. *PLoS ONE*, *9*(2), 86197. https://doi.org/10.1371/journal.pone.0086197

Krombholz, K., Judmayer, A., Gusenbauer, M., & Weippl, E. (2016). The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy. *Financial Cryptography and Data Security: 20th International Conference, FC 2016, Christ Church, Barbados, February 22–26, 2016, Revised Selected Papers*, 555–580.

Kruisbergen, E. W., Leukfeldt, E. R., Kleemans, E. R., & Roks, R. A. (2019). Money talks money laundering choices of organized crime offenders in a digital age. *Journal of Crime and Justice*. https://doi.org/10.1080/0735648X.2019.1692420

Kuhn, D. (2019). *Colu May Buy Back ICO Tokens in Pivot Away From Blockchain*. Coindesk.Com. https://www.coindesk.com/colu-may-buy-back-ico-tokens-in-pivot-away-from-blockchain

Kumar, A., Fischer, C., Tople, S., & Saxena, P. (2017). A Traceability Analysis of Monero's Blockchain. *Proceedings of the 22nd European Symposium on Research in Computer Security*. https://doi.org/10.1007/978-3-319-66399-9

Kurylo, B. (2022). The discourse and aesthetics of populism as securitisation style.

International Relations, *36*(1), 127–147. https://doi.org/10.1177/0047117820973071

Kycnot.me. (2020). *Exchanges*. https://kycnot.me/

Ladegaard, I. (2018). We know where you are, what you are doing and we will catch you: Testing deterrence theory in digital drug markets. *British Journal of Criminology*, *58*(2). https://doi.org/10.1093/bjc/azx021

Lapavitsas, C. (2017). *Marxist Monetary Theory*. Brill.

Lee, D. (2019). *Facebook won't rule out digital currency launch without US approval*. BBC News. https://www.bbc.co.uk/news/technology-49092713

Lennon, H. (2021). *The False Narrative Of Bitcoin's Role In Illicit Activity*. Forbes.

Libell, P., & Martyn-Hemphill, R. (2019). *Cryptocurrency Ransom Demanded for Wife of Norwegian Tycoon*. The New York Times. https://www.nytimes.com/2019/01/10/world/europe/norway-kidnapping-monero.html

Libra Association Members. (2019). *An Introduction to Libra: White Paper*.

Lietaer, B. (2001). *The Future of Money*. Random House.

Lietaer, B. (2014). *Why money needs to change now!*

Lietaer, B., Arnsperger, C., Goerner, S., & Brunnhuber, S. (2012). *Money and Sustainability: The Missing Link*.

Lietaer, B., & Dunne, J. (2013). *Rethinking Money: How new currencies turn scarcity into prosperity* (First). Berrett-Koehler.

Lo, S., & Wang, J. C. (2014). Bitcoin as Money? In *Current Policy Perspectives, Federal Reserve Bank of Boston*.

Lusthaus, J. (2013). How organised is organised cybercrime? *Global Crime*, *14*(1), 52–60. https://doi.org/10.1080/17440572.2012.759508

Luther, W. J. (2017). *How Much Cash is Used by Criminals and Tax Cheats?* American Institute for Economic Research. https://www.aier.org/article/sound-money-project/how-much-cash-used-criminals-and-tax-cheats

Luther, W. J. (2018). Is Bitcoin Intrinsically Worthless? *Journal of Private Enterprise*, *33*(Spring 2018), 31–45.

Luther, W. J. (2020). Four Principles for a Base Money Regime. *Cato Journal*, *40*(2). https://doi.org/10.36009/CJ.40.2.16

Maddox, A., Barratt, M. J., Allen, M., & Lenton, S. (2015). Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital "demimonde."

Information, Communication & Society. https://doi.org/10.1080/1369118X.2015.1093531

Maddox, A., Singh, S., Horst, H., & Adamson, G. (2016). An ethnography of Bitcoin: Towards a future research agenda. *Australian Journal of Telecommunications and the Digital Economy*, *4*. https://doi.org/10.18080/ajtde.v4n1.49

Markham, A., & Buchanan, E. (2012). *Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee (Version 2.0) AUTHORS*.

Martin, F. E., Mukhopadhyay, M., & van Hombeeck, C. (2017). The global role of the of US dollar and its consequences. *Quarterly Bulletin, Bank of England*, *Q4*.

Martin, K. (2012). *Everyday Cryptography*. Oxford University Press.

Maurer, B., Nelms, T. C., & Swartz, L. (2013). "When perhaps the real problem is money itself!": the practical materiality of Bitcoin. *Social Semiotics*. https://doi.org/10.1080/10350330.2013.777594

Mays, N., & Pope, C. (1995). Rigour and Qualitative Research. *British Medical Journal*, *311*(6997), 109–112.

McKinsey Global Institute. (2018). *Smart city technology for a more liveable future*.

Mcleay, M., Radia, A., & Thomas, R. (2014). *Money in the modern economy: an introduction*.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2013). A fistful of bitcoins: characterizing payments among men with no names. *IMC '13: Proceedings of the 2013 Conference on Internet Measurement Conference, Barcelona, Spain*. https://doi.org/10.1145/2504730.2504747

Mendoza-Tello, J. C., Mora, H., Pujol-López, F. A., & Lytras, M. D. (2018). Social Commerce as a Driver to Enhance Trust and Intention to Use Cryptocurrencies for Electronic Payments. *IEEE Access*, *6*. https://doi.org/10.1109/ACCESS.2018.2869359

Menger, C. (1892). On the Origin of Money. *The Economic Journal*, *2*(6), 239–255.

Metropolitan Police. (2021). *Structure*. Met.Police.Uk.

Middelkoop, W. (2016). *The Big Reset*. Amsterdam University Press.

Mirea, M., Wang, V., & Jung, J. (2019). The not so dark side of the darknet: a qualitative study. *Security Journal*, *32*, 102–118. https://doi.org/10.1057/s41284-018-0150-5

Mitchell-Innes, A. (1914). The Credit Theory of Money. *The Banking Law Journal*, *31*, 151–168.

Mitchell, W., Randall Wray, L., & Watts, M. (2019). *Macroeconomics*. Red Globe Press.

Mondovisione.com. (2015). *New York State Department Of Financial Services Superintendent Remarks At Columbia Law School*. https://m.mondovisione.com/

Moore, D., & Rid, T. (2016). *Cryptopolitik and the Darknet*. https://doi.org/10.1080/00396338.2016.1142085

Moser, M., Soska, K., Heilman, E., Lee, K., Heffan, H., Hennessey, J., Miller, A., Narayanan, A., & Christin, N. (2018). An Empirical Analysis of Traceability in the Monero Blockchain. *Proceedings on Privacy Enhancing Technologies*, 143–163. https://doi.org/https://doi.org/10.1515/popets-2018-0025

Moser, S. (2008). Personality: A New Positionality? *Area*, *40*(3), 383–392.

Mundell, R. (1999). *A Reconsideration of the Twentieth Century*.

Munksgaard, R., & Demant, J. (2016). Mixing politics and crime-the prevalence and decline of political discourse on the cryptomarket. *International Journal of Drug Policy*. https://doi.org/10.1016/j.drugpo.2016.04.021

Murphy, R. (2022). *Sunak's choice: to support the banks and their ill-gotten gains or to save the people of this country from poverty?* Tax Research UK. https://www.taxresearch.org.uk/Blog/2022/06/10/sunaks-choice-to-support-the-banks-and-their-ill-gotten-gains-or-to-save-the-people-of-this-country-from-poverty/

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.

National Crime Agency. (2021). *Annual Report and Accounts 2020-21*.

Nelms, T. C., Maurer, B., Swartz, L., & Mainwaring, S. (2018). Social Payments: Innovation, Trust, Bitcoin, and the Sharing Economy. *Theory, Culture and Society*, *35*(3), 13–33. https://doi.org/10.1177/0263276417746466

Neocleous, M. (2008). *Critique of Security*. Edinburgh University Press.

O'Brien, P. K., & Palma, N. (2020). Danger to the Old Lady of Threadneedle Street? The Bank Restriction Act and the regime shift to paper money, 1797-1821. In *European Review of Economic History* (Vol. 24, Issue 2, pp. 390–426). Oxford University Press. https://doi.org/10.1093/ereh/hez008

O'Leary, Z. (2017). The Essential Guide to Doing Your Research Project. In *SAGE Publications Ltd* (Third). SAGE Publications Ltd.

Obstfeld, M., Shambaugh, J. C., & Taylor, A. M. (2004). Monetary Sovereignty, Exchange Rates, and Capital Controls: The Trilemma in the Interwar Period. In *IMF Staff Papers* (Vol. 51).

Office of National Drug Control Policy. (2014). What America's Users Spend on Illegal Drugs : 2000-2010. In *RAND Corporation*.

Oh, S., & Park, M. S. (2013). Text mining as a method of analyzing health questions in social Q&A. *Proceedings of the ASIST Annual Meeting*, *50*(1). https://doi.org/10.1002/meet.14505001130

Olcott, E., & Szalay, E. (2021). *China expands crackdown by declaring all crypto activities 'illegal.'* Financial Times.

Openpgp.org. (2020). *History*. https://www.openpgp.org/about/history/

Owen, G., & Savage, N. (2015). The Tor Dark Net. *Global Commission on Internet Governance Paper Series*, *20*.

Palframan, M. (2018). *Ten years after the financial crisis two-thirds of British people don't trust banks*. YouGov.

Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2018). Ransomware Payments in the Bitcoin Ecosystem. *Paper Presented to the 17th Annual Workshop on the Economics of Information Security, Innsbruck, Austria, 18-19 June*. https://doi.org/10.1016/j.specom.2007.01.008

Pastrana, S., Hutchings, A., Thomas, D., & Tapiador, J. (2019). Measuring eWhoring. *Proceedings of the Internet Measurement Conference (IMC '19). ACM, New York, NY, USA*, 463–477. https://doi.org/10.1145/3355369.3355597

Pastrana, S., Thomas, D. R., Hutchings, A., & Clayton, R. (2018). CrimeBB: Enabling Cybercrime Research on Underground Forums at Scale. *Proceedings of the 2018 World Wide Web Conference (WWW '18). Republic and Canton of Geneva, Switzerland*, 1845–1854. https://doi.org/10.1145/3178876.3186178

Pastrana, S., & Vu, A. V. (2021). *The CrimeBB and ExtremeBB Dataset*.

Pickering, G. (2019). The Relevance of Bitcoin to the Regression Theorem: A Reply to Luther. In *The Quarterly Journal of Austrian Economics* (Vol. 22).

Pink, S., Horst, H., Postill, J., Hjorth, L., Lewis, T., & Tacchi, J. (2015). *Digital Ethnography: Principles and Practice*. SAGE Publications Ltd. https://doi.org/10.1177/1461444817733962c

Polleit, T. (2012). *The Fiasco of Fiat Money*. Mises Institute. https://mises.org/library/fiasco-fiat-money

Positive Money Europe. (2019). *RIP Bernard Lietaer*. https://www.positivemoney.eu/2019/02/rip-bernard-lietaer/

Presthus, W., & O’Malley, N. O. (2017). Motivations and Barriers for End-User Adoption of Bitcoin as Digital Currency. *Procedia Computer Science*, *121*, 89–97. https://doi.org/10.1016/j.procs.2017.11.013

Qiu, R. G., Wang, K., Li, S., Dong, J., & Xie, M. (2014). Big data technologies in support of real time capturing and understanding of electric vehicle customers dynamics. *Proceedings of the IEEE International Conference on Software Engineering and Service Sciences, ICSESS*, 263–267. https://doi.org/10.1109/ICSESS.2014.6933559

Quinault, R. (1999). The French Invasion of Pembrokeshire in 1797: A Bicentennial Assessment. *Welsh History Review*, *19*(4), 618–643.

Rappeport, A., & Popper, N. (2019). *Cryptocurrencies Pose National Security Threat, Mnuchin Says*. The New York Times. https://www.nytimes.com/2019/07/15/us/politics/mnuchin-facebook-libra-risk.html

Reinhart, C. M., & Rogoff, K. S. (2010). Growth in a time of debt. *American Economic Review*, *100*(2), 573–578. https://doi.org/10.1257/aer.100.2.573

Reynolds, K. (2021). *Bittrex to Delist “Privacy Coins” Monero, Dash and Zcash*. Coindesk.

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Rid, T. (2016). *Rise of the machines : the lost history of cybernetics*. Scribe.

Roberts, M. (2017). Satan’s Bank Note. *History Today*.

Robertson, H. (2021). *Janet Yellen says “misuse” of cryptocurrencies like bitcoin is a growing problem, as regulators increase scrutiny after surge in interest*. Businessinsider.

Robinson, T. (2019). *Crypto can prevent money laundering better than traditional finance*. Venturebeat. https://venturebeat.com/2019/07/20/crypto-can-prevent-money-laundering-better-than-traditional-finance/

Rockeman, O. (2022). *US Inflation Hits 40-Year High of 8.6%: CPI Report*. Bloomberg.Com. https://www.bloomberg.com/news/articles/2022-06-10/us-inflation-unexpectedly-accelerates-to-40-year-high-of-8-6

Rogoff, K. S. (2016). *The Curse of Cash*. Princeton University Press.

Ron, D., & Shamir, A. (2013). Quantitative Analysis of the Full Bitcoin Transaction Graph. *Paper Presented to Financial Cryptography and Data Security, 17th International Conference, Okinawa, Japan, 1-5 April.*

Rothbard, M. N. (1981). The Myth of Neutral Taxation. *The Cato Journal*, 56–108.

Roussou, I., & Stiakakis, E. (2016). Adoption of Digital Currencies by Companies in the European Union: A Research Model combining DOI and TAM. *4th International Conference on Contemporary Marketing Issues*.

Russo, C. (2018). *Bitcoin Speculators, Not Drug Dealers, Dominate Crypto Use Now*. Bloomberg. https://www.bloomberg.com/news/articles/2018-08-07/bitcoin-speculators-not-drug-dealers-dominate-crypto-use-now

Salter, M. B. (2008). Securitization and desecuritization: a dramaturgical analysis of the Canadian Air Transport Security Authority. *Journal of International Relations and Development*, *11*, 321–349. https://doi.org/10.1057/jird.2008.20

Salter, M., & Mutlu, C. (2013). *Research Methods in Critical Security Studies*. Routledge.

Sands, P., Weisman, B., Sostaric, M., Smith, A., Smoot, J., Zigelman, O., & Mathur, J. (2016). *Making it Harder for the Bad Guys: The Case for Eliminating High Denomination Notes*.

Sarkar, A. (2022). *Coin Center takes US Treasury to court over alleged financial spying*. Cointelegraph. https://cointelegraph.com/news/coin-center-takes-us-treasury-to-court-over-alleged-financial-spying

Sas, C., & Khairuddin, I. E. (2015). Exploring Trust in Bitcoin Technology: A Framework for HCI Research. *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction*, 338–342. https://doi.org/10.1145/2838739.2838821

Schneier, B. (2019). *Blockchain and Trust*. Schneier on Security. https://www.schneier.com/blog/archives/2019/02/blockchain_and_.html

Schroeder, R. (2018). *Social Theory after the Internet: Media, Technology and Globalization*. UCL Press. https://doi.org/10.14324/111.9781787351226

Schultze-Kraft, R. (2021). *No, Bitcoin Ownership is not Highly Concentrated – But Whales are Accumulating*. Glassnode.Com. https://insights.glassnode.com/bitcoin-supply-distribution/

Schumpeter, J. A. (1954). *History of Economic Analysis*. Oxford University Press.

Selgin, G. (1988). *The Theory of Free Banking*. Rowman & Littlefield Publishers.

Shahzad, F., Xiu, G., Wang, J., & Shahbaz, M. (2018). An empirical investigation on the adoption of cryptocurrencies among the people of mainland China. *Technology in Society*, *55*, 33–40. https://doi.org/10.1016/J.TECHSOC.2018.05.006

Shapiro, H., & Daly, M. (2016). *Highways and buyways: A snapshot of UK drug scenes 2016*.

Sharpe, M. (2009). What Keynes Knew. *Challenge*, *52*(2), 124–131. https://doi.org/10.2753/0577-5132520206

Shawdagor, J. (2022). *Argo CEO Peter Wall claims Bitcoin is gold 2.0, will become hedge against inflation*. Cryptoslate. https://cryptoslate.com/argo-ceo-peter-wall-claims-bitcoin-is-gold-2-0-will-become-hedge-against-inflation/

Shi, M. M. (2018). *Fed Chair: Cryptocurrencies Are "Great" For Money Laundering*. Coindesk. https://www.coindesk.com/fed-chair-cryptocurrencies-are-great-for-money-laundering

Sieroń, A. (2019). Endogenous versus exogenous money: Does the debate really matter? *Research in Economics*, *73*(4), 329–338. https://doi.org/10.1016/J.RIE.2019.10.003

Simmel, G. (2004). *The Philosophy of Money* (D. Frisby (Ed.)). Routledge.

Simmons, B. A. (1996). Rulers of the game: central bank independence during the interwar years. *International Organisation*, *50*(3), 407–443.

Smith, A. (2007). *An Inquiry into the Nature and Causes of The Wealth of Nations* (S. Soares (Ed.)). MetaLibri.

Son, H., & Levitt, H. (2017). *Jamie Dimon would fire any employee trading bitcoin for being "stupid."* AFR. https://www.afr.com/companies/financial-services/jamie-dimon-would-fire-any-employee-trading-bitcoin-for-being-stupid-20170913-gyg7n0

Son, H., Levitt, H., & Louis, B. (2017). *Jamie Dimon Slams Bitcoin as a 'Fraud.'* Bloomberg. https://www.bloomberg.com/news/articles/2017-09-12/jpmorgan-s-ceo-says-he-d-fire-traders-who-bet-on-fraud-bitcoin

Soska, K., & Christin, N. (2015). Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. *Usenix Sec*, 33–48. https://doi.org/10.1007/s00253-017-8456-5

Spagnuolo, M., Maggi, F., & Zanero, S. (2014). BitIodine: Extracting Intelligence from the Bitcoin Network. *Paper Presented to Financial Cryptography and Data*

Security, 18th International Conference, Chrsit Church, Barbados, 3-7 March. https://doi.org/10.1007/978-3-662-45472-5_29

Sparkes, M. (2014). *Hull Council “printing its own money” by paying digital cash for voluntary work*. The Telegraph.

Steinberger, P. J. (2008). Hobbes, Rousseau and the Modern Conception of the State. *The Journal of Politics*, *70*(3), 595–611. https://doi.org/10.1017/s002238160808064x

Stewart, M. G., & Mueller, J. (2013). Terrorism Risks and Cost-Benefit Analysis of Aviation Security. *Risk Analysis*, *33*(5). https://doi.org/10.1111/j.1539-6924.2012.01905.x

Stritzel, H. (2014). Securitization Theory and the Copenhagen School. In *Security in Translation: Securitization Theory and the Localization of Threat* (pp. 11–37). Palgrave Macmillan UK. https://doi.org/10.1057/9781137307576_2

Sugiura, L. (2017). Researching Online Forums. In *British Sociological Association*.

Tang, S. (2009). The Security Dilemma: A Conceptual Analysis. *Security Studies*, *18*(3), 587–623. https://doi.org/10.1080/09636410903133050

The Economist. (2018). *Crypto money-laundering - Digital detergent*. https://www.economist.com

The Economist. (2021). *The geopolitics of money is shifting up a gear*. https://www.economist.com/leaders/2021/10/23/the-geopolitics-of-money-is-shifting-up-a-gear

The Swedish National Council for Crime Prevention (Bra). (2019). *Fraud and economic crime*. Brottsförebyggande rådet. https://www.bra.se/bra-in-english/home/crime-and-statistics/fraud-and-economic-crime.html

The University of Sheffield. (2018). *Research Involving Illegal Activities*.

Timebanking UK. (2021). *Overview*. https://timebanking.org/overview/

Tor Project. (2019). *History*. https://www.torproject.org/about/history/

Torpey, J. (1998). Coming and Going: On the State Monopolization of the Legitimate “Means of Movement.” *Source: Sociological Theory*, *16*(3), 239–259.

Torpey, K. (2017). *Here’s What Peter Schiff Got Wrong About Bitcoin on Joe Rogan’s Podcast*. Forbes.

Tsanidis, C., Dafni, ;, Nerantzaki, M., Karavasilis, G., Vrana, V., & Paschaloudis, D. (2015). Greek consumers and the use of Bitcoin. *The Business & Management Review*, *6*, 30–31.

UK Finance. (2018). *UK Payment Markets – Summary*.

UK Finance. (2019). *Fraud the Facts 2019: The definitive overview of payment industry fraud*.

United Nations Office on Drugs and Crime. (2018). *World drug report 2018*.

United Nations Office on Drugs and Crime. (2022). *Overview*. https://www.unodc.org/unodc/en/money-laundering/overview.html

United States District Court for the District of Columbia. (2008). *Transcript of Sentence Before the Honorable Rosemary M. Collyer*.

University of Cambridge, C. L. (2019). *Cambridge Cybercrime Centre: Description of available datasets*. https://www.cambridgecybercrime.uk/datasets.html

US-CERT. (2017). *Malware Initial Findings Report (MIFR) - 10130295*.

US Department of Justice. (2014). *Department Of Financial Services Hearing On Law Enforcement And Virtual Currencies*. https://www.justice.gov

van de Sande, M. (2015). Fighting with Tools: Prefiguration and Radical Politics in the Twenty-First Century. *Rethinking Marxism*, *27*(2), 177–194. https://doi.org/10.1080/08935696.2015.1007791

van Hout, M. C., & Bingham, T. (2014). Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. *International Journal of Drug Policy*, *25*(2), 183–189. https://doi.org/10.1016/j.drugpo.2013.10.009

von Lampe, K., & Johansen, O. (2006). Organized Crime and Trust:: On the conceptualization and empirical relevance of trust in the context of criminal networks. *Global Crime*. https://doi.org/10.1080/17440570500096734

von Mises, L. (1998). *HUMAN ACTION: A Treatise on Economics* (Scholar’s). Ludwig von Mises Institute.

von Mises, L. (2009). *The Theory of Money and Credit*. Ludwig von Mises Institute.

von Mises, L. (2012). *Economic Calculation in the Socialist Commonwealth*. Ludwig von Mises Institute.

Walker, J., & Cooper, M. (2011). Genealogies of resilience: From systems ecology to the political economy of crisis adaptation. *Security Dialogue*, *42*(2), 143–160. https://doi.org/10.1177/0967010611399616

Weber, M. (1919). *Politics as a Vocation* (H. Gerth & C. Wright Mills (Eds.); From Max W).

Weber, M. (1978). *Economy and Society*. University of California Press.

Wikipedia. (2021). *National Crime Agency*.

Wilson, T., & Schroeder, P. (2021). *Facebook-backed crypto project Diem to launch U.S. stablecoin in major shift*. Reuters.

Winder, D. (2021). *The five most important ransomware attacks of 2021*. Raconteur. https://www.raconteur.net/technology/the-five-most-important-ransomware-attacks-of-2021/

Wintour, P., & Gillan, A. (2008). *Lost in Iceland: £1 billion from councils, charities and police*. The Guardian. https://www.theguardian.com/business/2008/oct/10/banking-iceland

Wolcott, H. (2012). *Writing Up Qualitative Research* (Third). SAGE Publications.

Wolfson, R. (2018). *Tracing Illegal Activity Through The Bitcoin Blockchain To Combat Cryptocurrency-Related Crimes*. Forbes. https://www.forbes.com/sites/rachelwolfson/2018/11/26/tracing-illegal-activity-through-the-bitcoin-blockchain-to-combat-cryptocurrency-related-crimes/

Wray, L. R. (Ed.). (2004). *The Credit and State Theories of Money: The Contributions of A. Mitchell Innes*. Edward Elgar Publishing Ltd.

Xiaochuan, Z. (2009). *Reform the international monetary system*. Essay by the Governor of the People's Bank of China. www.bis.org

Xiaochuan, Z. (2017). *Statement of the Governor of the People's Bank of China at the 36th Minsiterial meeting of the International Monetary and Financial Committee*.

Yang, Y. (2018). *Why millennials are driving cashless revolution in China*. The Financial Times. https://www.ft.com/content/539e39b8-851b-11e8-a29d-73e3d454535d

Yelowitz, A., & Wilson, M. (2015). Characteristics of Bitcoin users: an analysis of Google search data. *Applied Economics*. https://doi.org/10.1080/13504851.2014.995359

Yermack, D. (2013). *Is Bitcoin a Real Currency? An Economic Appraisal*.

Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. *Policing and Society*. https://doi.org/10.1080/10439463.2013.780227

Zamani, E., He, Y., & Phillips, M. (2020). On the Security Risks of the Blockchain. *Journal of Computer Information Systems*, *60*(6), 495–506. https://doi.org/10.1080/08874417.2018.1538709

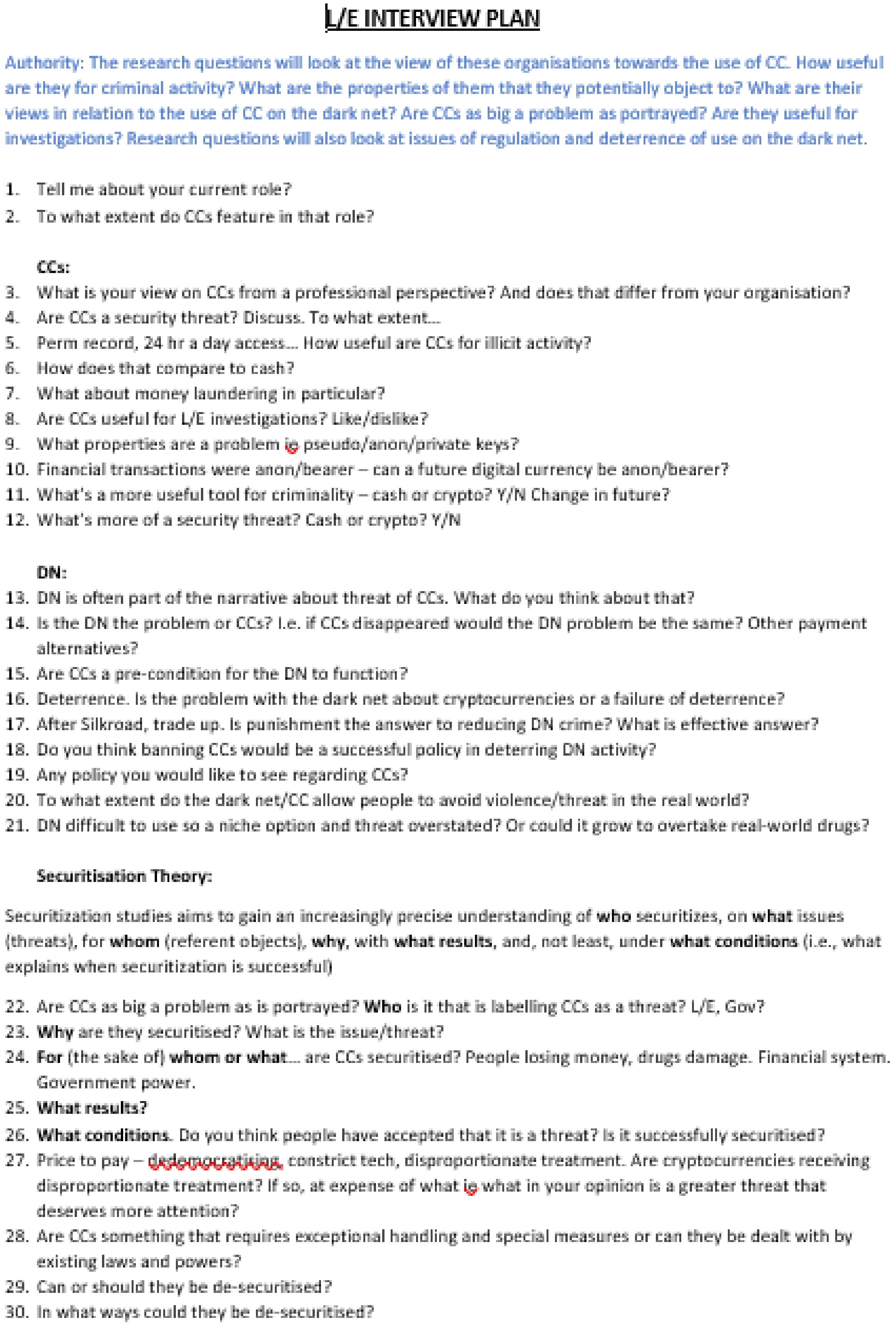
Zetter, K. (2012). *FBI Fears Bitcoin's Popularity with Criminals*. Wired.

https://www.wired.com/2012/05/fbi-fears-bitcoin/

Zhao, C. (2021). *@Binance received a letter of commendation from UK South East Regional Organised Crime Unit for our efforts in helping them to fight bad players in the cyber space.* https://twitter.com/cz_binance/status/1408010393214017545

10 Appendix A – Interview Plans

The following plans were used for the interview of the law enforcement officers in Chapter 6 and the HullCoin participants in Chapter 7. For openness, they are presented as used at the time. As such, they are somewhat dated in terms of the final thesis but they show the semi-structured basis of the interviews. They are also in note form as there was no intention to include them in full here when they were created. However, they may be useful to future researchers and so they are included in their original form. The abbreviations used are CC (cryptocurrencies), DN (dark net), LE (law enforcement) and HC (HullCoin).



L/E INTERVIEW PLAN

Authority: The research questions will look at the view of these organisations towards the use of CC. How useful are they for criminal activity? What are the properties of them that they potentially object to? What are their views in relation to the use of CC on the dark net? Are CCs as big a problem as portrayed? Are they useful for investigations? Research questions will also look at issues of regulation and deterrence of use on the dark net.

1. Tell me about your current role?
2. To what extent do CCs feature in that role?

CCs:

3. What is your view on CCs from a professional perspective? And does that differ from your organisation?
4. Are CCs a security threat? Discuss. To what extent…
5. Perm record, 24 hr a day access… How useful are CCs for illicit activity?
6. How does that compare to cash?
7. What about money laundering in particular?
8. Are CCs useful for L/E investigations? Like/dislike?
9. What properties are a problem ie pseudo/anon/private keys?
10. Financial transactions were anon/bearer – can a future digital currency be anon/bearer?
11. What's a more useful tool for criminality – cash or crypto? Y/N Change in future?
12. What's more of a security threat? Cash or crypto? Y/N

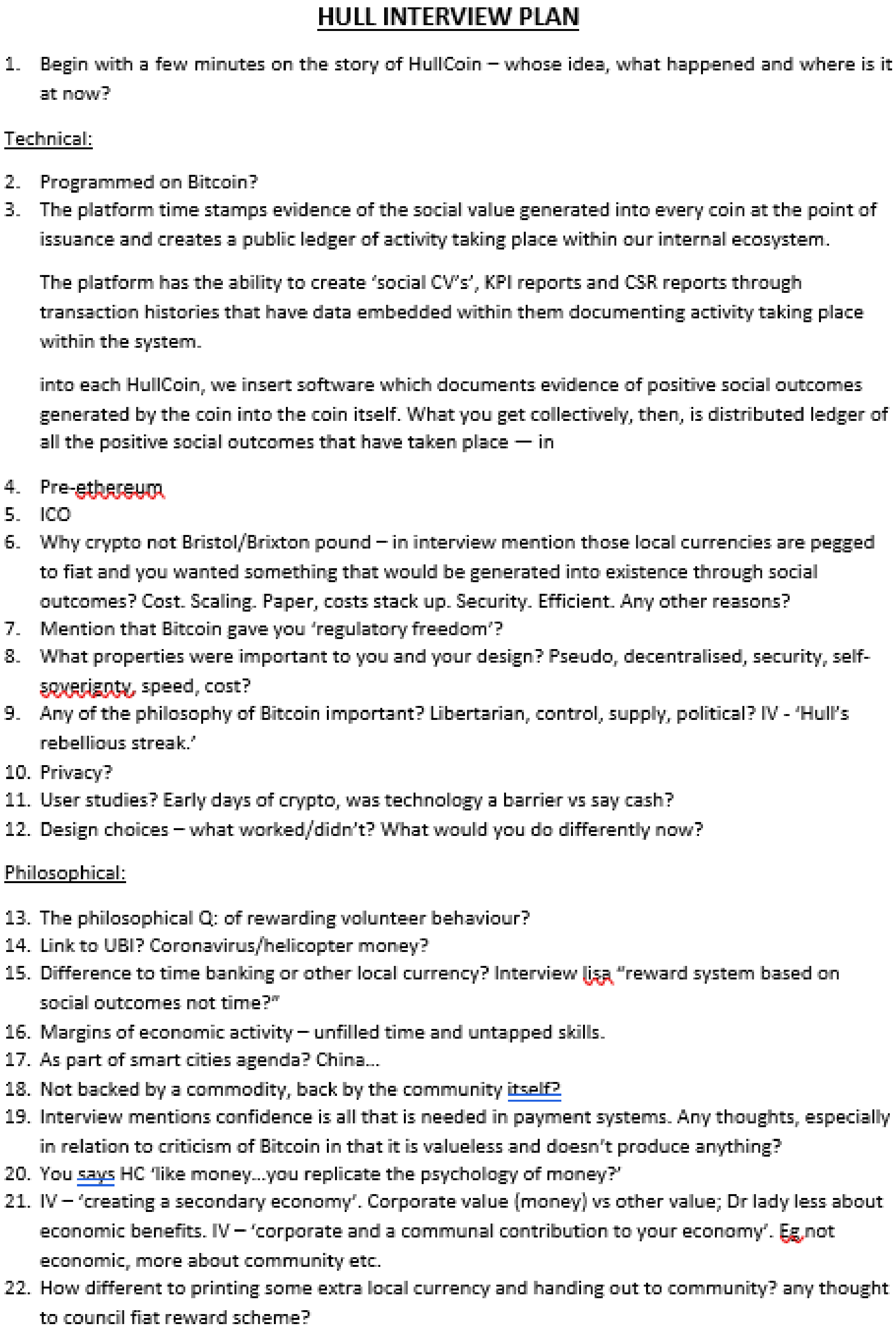
DN:

13. DN is often part of the narrative about threat of CCs. What do you think about that?
14. Is the DN the problem or CCs? I.e. if CCs disappeared would the DN problem be the same? Other payment alternatives?
15. Are CCs a pre-condition for the DN to function?
16. Deterrence. Is the problem with the dark net about cryptocurrencies or a failure of deterrence?
17. After Silkroad, trade up. Is punishment the answer to reducing DN crime? What is effective answer?
18. Do you think banning CCs would be a successful policy in deterring DN activity?
19. Any policy you would like to see regarding CCs?
20. To what extent do the dark net/CC allow people to avoid violence/threat in the real world?
21. DN difficult to use so a niche option and threat overstated? Or could it grow to overtake real-world drugs?

Securitisation Theory:

Securitization studies aims to gain an increasingly precise understanding of **who** securitizes, on **what** issues (threats), for **whom** (referent objects), **why**, with **what results**, and, not least, under **what conditions** (i.e., what explains when securitization is successful)

22. Are CCs as big a problem as is portrayed? **Who** is it that is labelling CCs as a threat? L/E, Gov?
23. **Why** are they securitised? What is the issue/threat?
24. **For** (the sake of) **whom or what**… are CCs securitised? People losing money, drugs damage. Financial system. Government power.
25. **What results?**
26. **What conditions**. Do you think people have accepted that it is a threat? Is it successfully securitised?
27. Price to pay – dedemocratising, constrict tech, disproportionate treatment. Are cryptocurrencies receiving disproportionate treatment? If so, at expense of what ie what in your opinion is a greater threat that deserves more attention?
28. Are CCs something that requires exceptional handling and special measures or can they be dealt with by existing laws and powers?
29. Can or should they be de-securitised?
30. In what ways could they be de-securitised?



HULL INTERVIEW PLAN

1. Begin with a few minutes on the story of HullCoin – whose idea, what happened and where is it at now?

Technical:

2. Programmed on Bitcoin?
3. The platform time stamps evidence of the social value generated into every coin at the point of issuance and creates a public ledger of activity taking place within our internal ecosystem.

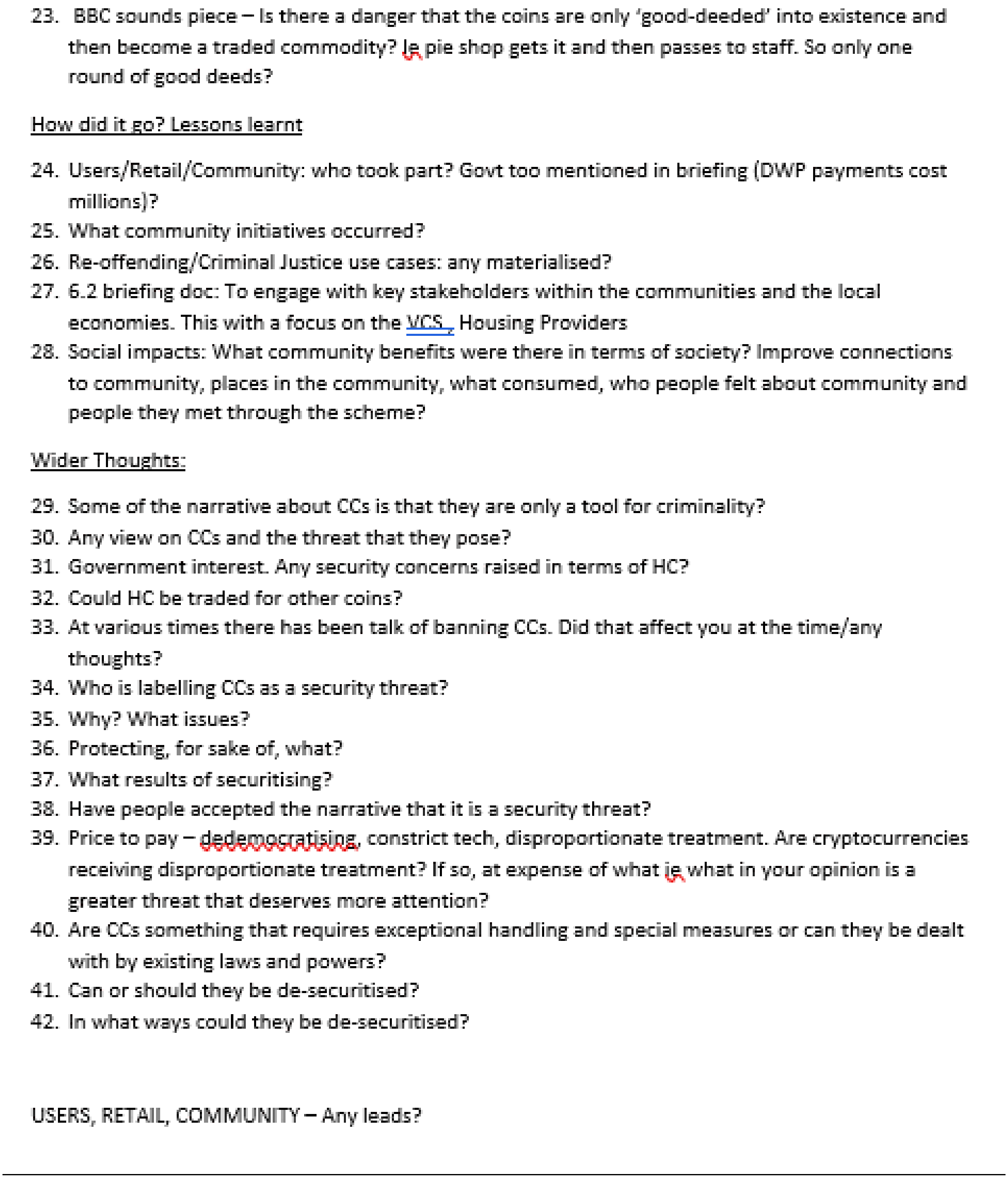
   The platform has the ability to create 'social CV's', KPI reports and CSR reports through transaction histories that have data embedded within them documenting activity taking place within the system.

   into each HullCoin, we insert software which documents evidence of positive social outcomes generated by the coin into the coin itself. What you get collectively, then, is distributed ledger of all the positive social outcomes that have taken place — in

4. Pre-ethereum
5. ICO
6. Why crypto not Bristol/Brixton pound – in interview mention those local currencies are pegged to fiat and you wanted something that would be generated into existence through social outcomes? Cost. Scaling. Paper, costs stack up. Security. Efficient. Any other reasons?
7. Mention that Bitcoin gave you 'regulatory freedom'?
8. What properties were important to you and your design? Pseudo, decentralised, security, self-soverignty, speed, cost?
9. Any of the philosophy of Bitcoin important? Libertarian, control, supply, political? IV - 'Hull's rebellious streak.'
10. Privacy?
11. User studies? Early days of crypto, was technology a barrier vs say cash?
12. Design choices – what worked/didn't? What would you do differently now?

Philosophical:

13. The philosophical Q: of rewarding volunteer behaviour?
14. Link to UBI? Coronavirus/helicopter money?
15. Difference to time banking or other local currency? Interview lisa "reward system based on social outcomes not time?"
16. Margins of economic activity – unfilled time and untapped skills.
17. As part of smart cities agenda? China…
18. Not backed by a commodity, back by the community itself?
19. Interview mentions confidence is all that is needed in payment systems. Any thoughts, especially in relation to criticism of Bitcoin in that it is valueless and doesn't produce anything?
20. You says HC 'like money…you replicate the psychology of money?'
21. IV – 'creating a secondary economy'. Corporate value (money) vs other value; Dr lady less about economic benefits. IV – 'corporate and a communal contribution to your economy'. Eg not economic, more about community etc.
22. How different to printing some extra local currency and handing out to community? any thought to council fiat reward scheme?



23. BBC sounds piece – Is there a danger that the coins are only 'good-deeded' into existence and then become a traded commodity? Ie pie shop gets it and then passes to staff. So only one round of good deeds?

How did it go? Lessons learnt

24. Users/Retail/Community: who took part? Govt too mentioned in briefing (DWP payments cost millions)?
25. What community initiatives occurred?
26. Re-offending/Criminal Justice use cases: any materialised?
27. 6.2 briefing doc: To engage with key stakeholders within the communities and the local economies. This with a focus on the VCS , Housing Providers
28. Social impacts: What community benefits were there in terms of society? Improve connections to community, places in the community, what consumed, who people felt about community and people they met through the scheme?

Wider Thoughts:

29. Some of the narrative about CCs is that they are only a tool for criminality?
30. Any view on CCs and the threat that they pose?
31. Government interest. Any security concerns raised in terms of HC?
32. Could HC be traded for other coins?
33. At various times there has been talk of banning CCs. Did that affect you at the time/any thoughts?
34. Who is labelling CCs as a security threat?
35. Why? What issues?
36. Protecting, for sake of, what?
37. What results of securitising?
38. Have people accepted the narrative that it is a security threat?
39. Price to pay – dedemocratising, constrict tech, disproportionate treatment. Are cryptocurrencies receiving disproportionate treatment? If so, at expense of what ie what in your opinion is a greater threat that deserves more attention?
40. Are CCs something that requires exceptional handling and special measures or can they be dealt with by existing laws and powers?
41. Can or should they be de-securitised?
42. In what ways could they be de-securitised?

USERS, RETAIL, COMMUNITY – Any leads?