Criminal use of cryptocurrencies – a great new threat or is cash still king?

Simon Butler[1]

Information Security Group, Royal Holloway, University of London, UK

Simon.Butler.2015@live.rhul.ac.uk

Simon Butler has an extensive background working in security-related roles. These include service as both a military and law enforcement intelligence officer, as well as more recently as a security consultant for a large technology company. He completed an MSc in Information Security at Royal Holloway, University of London before joining the EPSRC Centre for Doctoral Training in Cyber Security at Royal Holloway. His research interest is in blockchain technology and cryptocurrencies. His work aims to provide some clarity in the polarising debate about cryptocurrencies and the future of money.

Criminal use of cryptocurrencies – a great new threat or is cash still king?

In July 2018, the Federal Reserve Chairman told the US Congress that cryptocurrencies are 'great' for money laundering. Many media headlines follow comments such as this, suggesting that cryptocurrencies are a significant criminal tool that should be feared.

This article examines academic research, particularly those that analysed the Bitcoin blockchain, to see if the results matched the headlines. This was then compared to wider government and think-tank reporting. Contrary to popular opinion, this article shows that cryptocurrencies are currently used in a very small percentage of crime and they are not the great future threat that many assert.

Cash is the real enemy for crime fighting and remains 'king'. It is anonymous[2] and far more useful to criminals than cryptocurrencies. However, the future of money is uncertain and policy makers need to understand that there is more to the debate about cryptocurrencies than the headlines suggest.

Keywords: word; cybercrime, cyber security, criminal financing, cryptocurrencies, bitcoin

Word count: 8559 (not including abstract, endnotes and references)

Introduction

The history of money is an intriguing subject, and we are very much in the middle of the story. Money is central to the workings of our planet and core to issues of politics and security. It is against this backdrop that we have witnessed the emergence of cryptocurrencies.[3] They enjoy fervent support amongst those that embrace their cypherpunk roots, who believe in them as a new financial system, free from control by traditional actors. But there have been others who have denounced them 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[4] as stupid and he has labelled it a fraud (Son, Levitt, and Louis 2017). 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). 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 has received even more attention after Facebook announced plans to launch their own cryptocurrency, the 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 and Popper 2019)

This article will examine the use of cryptocurrencies in cybercrime. Are the headlines accurate and should policy makers and politicians prioritise this technology in their fight against crime? It is important to note, however, that usage should not be conflated with the future potential threat of cryptocurrencies. These pillars of the debate need to be considered in separation, but alongside each other – failure to do so leads to a confused view of the issue and the potential to focus on the wrong priorities in fighting crime. The future is difficult to predict, but this article will consider the threat that cryptocurrencies could one day pose and show that there is less to fear than the headlines currently suggest.

Money

To thoroughly explore the use of cryptocurrencies in crime, they should be considered as part of the bigger picture of man's use of money, as we enter an ever more digital world. It is important to understand why they have emerged and where they fit into the wider world of money. Cash, as the physical equivalent of a cryptocurrency, will also be given some consideration as it will serve as a comparator throughout much of this article.

A brief history

The value of metal to man can be traced all the way back to our emergence from the Stone Age (Davies 2002). Coinage developed several hundred years BC (63) and was established long before our popular images of its use in Ancient Greece or in the Roman Empire. 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 is only in the twentieth century that we saw significant change in how we spend; credit cards, debit cards and automated electronic payments all arrived. So, too, did the internet and the subsequent boom in e-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).

To understand our modern-day use of money we should first look back to the end of the Second World War. At that time, there was a growing recognition that the international monetary system needed attention and that failures in this area in the inter-war period were at least in part to blame for political tensions in the world. 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. 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 is an ongoing economic debate. Fiat money is backed by the government that issues it, often via a central bank. 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).

International settlement

Modern times have also been shaped by the dominance of the 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) (Martin, Mukhopadhyay, and van Hombeeck 2017).

This is relevant to the discussion of currencies due to 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 to 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. 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 (International Monetary Fund 2019), 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 - recent trade escalations and the threat of a currency war between the US and China exemplify this tension (Brown 2019).

Cash – notes and coins

It is necessary to 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, there is discord about the mechanisms of international finance and, at lower levels, our usage has been trending towards digital transactions. Despite this

trend, though, demand for cash has grown. This phenomenon deserves some further examination, as, according to one former IMF economist and now 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)

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). 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 use of cash continues to decline, especially given its use in criminal activity? A 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' (223-224). The size of these markets cannot be accurately given, due to the 'untraceable nature of cash' (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 nature of cash (which will be explored in the next section) that makes 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.

Cash – and crime

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). 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 we have seen. Using these as starting figures, there have been attempts to produce rough estimates about 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).

Having established that cash remains key to criminal activities, analysis of the issuance of large denomination notes needs consideration. Cash, in large 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 (Europol 2015,6; Casciani 2010). 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 a number of other large notes, including the £50 note, but many still 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 is to 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.

One possible motivation for the continued circulation of cash is that governments make significant incomes from controlling the supply. 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 report 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). It is ironic that it is governments that take clean money and dirty it by supplying cash to criminals – a process referred to as 'reverse money laundering' (Rogoff 2016, 4).

The world is moving towards increasing digital transactions and this presents us with interesting times in terms of how criminals finance and conduct their operations. If 'cash really is king' for criminals, then why 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?

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. Bitcoin, as the primary cryptocurrency, will be the focus of this article. It was the first cryptocurrency and is the overwhelmingly dominant network with a market capitalisation of $188 billion, accounting for 66 per cent of the entire marketplace of over 2000 cryptocurrencies[5] (Coinmarketcap 2019). The threat that privacy-focussed cryptocurrencies pose will be considered separately later in the article.

The properties of cash and cryptocurrencies

Money, of all forms, has three widely accepted functions: 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). Cash, though, has some further properties. Firstly, it is anonymous (except for serial numbers). Secondly, 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. Thirdly, 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. Hence we have mature anti-money laundering regimes and requirements such as Suspicious Activity Reports (SARs). It is worth noting, here, that cash use is 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. For example, 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).

It is useful to draw out the properties of cash because cryptocurrencies are often described as 'digital cash'. It 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 do 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, but no identity is 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 to 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.

Bitcoin

It was against the backdrop of the 2007-2008 financial crisis that Bitcoin emerged. In November 2008, Satoshi Nakamoto[6] (2008) released a paper describing 'a peer-to-peer electronic cash system'. Email evidence and text in the genesis block[7] suggest that the motivation for the system was related to the financial crisis or it at least provided good timing for a system that did not rely on a trusted third party and was not controllable by governments (Carney 2018, 6-7). Yet this was not the first attempt at a digital cash system. Bitcoin's roots go back to the 1980s and academic papers produced by cryptographers at the time and since (see, for example, Chaum 1983; Nick Szabo 2008). There were several attempts to develop a digital monetary system in the subsequent decades but they never quite succeeded for one reason or another. Perhaps it was just a natural evolution, as each iteration provided an improvement over the previous and incorporated further developments in the field. But it is Bitcoin that has

managed to bring together all the right elements and features to produce a system that has not only survived, but has gained considerable traction to become a multi-billion dollar market that is known all over the world.

There are several reasons for its success. Timing is one – as we have seen it came at a time of increased fiat money supply. The global financial crisis also provided a good argument for a system that could not be controlled by governments and central banks. Cryptocurrency owners can hold their coins independently in a 'wallet', such as on a mobile phone. And transactions are processed by a distributed computation system of 'miners', using a 'proof of work' algorithm to achieve consensus (Antonopoulos 2017, 4). Bitcoin also has a fixed supply, a feature that marks it in stark contrast to fiat currencies. Whilst the US paper dollar supply has grown at pace to stand at $1.72 trillion in circulation as of 26 December 2018 (The Federal Reserve n.d.), Bitcoin has a mathematically fixed supply of 21 million coins. This makes it a rare deflationary system.[8]

Another possible reason for success is that Bitcoin did not rely on the uptake of merchants to be useable – it had good utility from inception for peer-to-peer transactions. Even in this age of internet commerce, it can be slow and expensive to send money abroad (via a third-party bank). Bitcoin offered a fast and cheap way to send funds globally - 24 hours a day, seven days a week. Transactions are confirmed approximately every ten minutes and are considered secure to consensus attacks after six confirmations i.e. after one hour (Antonopoulos 2017, 255). At the time of writing the fee is $0.35 for a transaction in the next confirmation – however, looking at historic daily averages, at a time of network congestion that can rise to over $35 (bitcoinfees.info 2019). Crucially, fees are related to the amount of data the transaction takes and market activity, rather than Bitcoin value (Antonopoulos 2017, 127). A recent Bitcoin transaction worth $468 million was sent for less than $400 in fees (Canellis 2019). In comparison, traditional remittance fees are related to the currency value and have a global average of 6.84 per cent – banks are the most expensive with an average price of 10.49 per cent (The World Bank 2019). In terms of speed, Barclays bank, for example, guarantee next day settlement for Single Euro Payments Area (SEPA) credit transfers, 3-4 working days for Europe and North America and within eight days for the rest of the world using their international payments services (Barclays 2019).

This is not to say that Bitcoin is flawless. It struggles with demand at times due to only being able to process seven transactions per second, compared to 56,000 per second for Visa (Croman et al. 2016). There are technical proposals for scaling cryptocurrencies, such as the Lightning Network for Bitcoin, where transactions are carried out 'off-chain', with the 'base-layer' being the main blockchain (Gudgeon et al. 2019). This method would also reduce fees. Several cryptocurrencies offer different design choices resulting in faster transaction confirmation and, in some cases, even zero fees (Williams 2018).

Bitcoin has been operating for over a decade but its usefulness as money is still debatable. Most major companies do not accept it as a form of payment and it is not legal tender. This may, of course, change in time. As a form of digital money, though, it has been the most successful to date - regardless of where it goes from here.

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 illegal 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 payment 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 (such as Zetter 2012). It was here that the early narrative around Bitcoin as a criminal tool began.

Criminal use

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. However, a recent report for the European Parliament (Keatinge, Carlisle, and Keen 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 currently do not present any great advantage over existing methods. Where then is the criminal activity that has been reported?

To answer questions about the extent of criminal use, we must look toward the dark net and to Tor hidden services. The dark net refers to areas of the internet that require special software or mechanisms to access them (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 legitimate activities (for example forums, activism or censorship avoidance), it can also be used for illicit purposes, such as the provision of dark net marketplaces for the sale of illegal goods and services. Dark nets, therefore, are a logical focus for the use of cryptocurrencies in crime. For the remainder of this article, the dark net will refer to Tor unless specified, as it hosts most marketplaces.

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[9] marketplace 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 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) gives a global cocaine value in the region of $38 billion. This is a valuation just for cocaine production, not the entire drugs 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[10] 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. It is logical that 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, as reported by the DEA. These early figures are also from a time before Bitcoin became more widely acknowledged. In fact, the DEA analysis of 2018 now shows that this figure has flipped following the surge in awareness of Bitcoin in 2017 – 10 per cent of Bitcoin transactions are 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 comparing these figures. Firstly, they are far apart in time. Secondly, 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 policymakers 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.

Anonymity and money laundering

A key criticism of cryptocurrencies, certainly in regard to their use on the dark net, is the anonymity that they afford. Cash is anonymous, cryptocurrencies less so. Bitcoin is the dominant player and, as discussed earlier, is pseudonymous. 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 anonymization in Bitcoin is not as strong as believed. Techniques such as re-identification[11] 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 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 pled guilty to laundering over $250 million. 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 opportunity and cases are seen in established finance too. In fact, 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 for 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[12] sites received an approximate share of 25 per cent each. 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 for 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.

In conclusion, as long as there are criminals, there will be money laundering. Whether mankind is 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)

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 methods. Increased regulation and lax use of cryptocurrency privacy features offer plenty of opportunity 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.

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. Research is needed to understand whether an improved payment method results in an increase in volume of this crime type. Similarly, do cryptocurrencies 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)? 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.

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[13] 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 usefulness as a medium of exchange, an attacker may gain further if the assets are held and they appreciate. However, these amounts are modest in relation 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 so is not a major financer of crime groups. This does not trivialise all the other significant impacts that ransomware causes.

The final point to consider in relation to cryptocurrencies and ransomware is the political dimension that these attacks can have. Two of the most recent and high-profile ransomware attacks of all-time, WannaCry and NotPetya, 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 was associated with only six bitcoin addresses and approximately $100,000 of bitcoin; NotPetya 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 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 other issues at play. In the case of NotPetya, the use of cryptocurrencies was incidental – the motive for the attack was political. Observers should not conflate the severe impact that ransomware can have with the part that cryptocurrencies play in them. As discussed, if cryptocurrencies did not exist then attacks like NotPetya or WannaCry could still continue, either with an alternative payment method or without one at all.

Future threat

This article has focussed so far on criminal use of cryptocurrencies from two perspectives: 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 threat, 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 there are several parts of the world that 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 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 article?

Firstly, 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 the US Treasury Secretary recently 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 them 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 described in this article. 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. 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). We have also now seen Facebook announce their intention to launch a cryptocurrency called the

Libra, in early 2020 (Libra Association Members 2019). These plans have been met with 'serious concerns' (Rappeport and Popper 2019) and Facebook's head of blockchain projects faced further scepticism in recent evidence to the US Senate Banking Committee (Brandom 2019). The fate, then, for cryptocurrencies is at best uncertain and as much a societal issue as anything else, which threatens to become ever more 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 does not aim to do either, Bitcoin does both (Dodd 2017, 37). Whilst Facebook has stated they will not launch the Libra without regulatory approval (Lee 2019), Bitcoin has already been operational for over ten years. Regulation is, therefore, another key area to consider for the future of cryptocurrencies.

The FATF Recommendations require that countries should regulate virtual asset service providers (VASP) (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) will also need to be amended into national law by 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 certain 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.

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 (Business Insider 2018). In Sweden for example, over a recent ten-year period, reported fraud crime has tripled (The Swedish National Council for Crime Prevention (Bra) 2019). 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.

The final area to consider in terms of the future threat of cryptocurrencies is privacy focussed coins. We saw earlier that criminals 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 it 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 its 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 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.

Conclusion

There is no doubt that Bitcoin and other cryptocurrencies are used for crime. But this is true for all forms of money, none more so than physical cash. Cash remains king for criminals and if the world wants to scrutinise money in criminal activities then this is where the focus should be. The overall scale of criminal use of cryptocurrencies is small when compared to cash, and the percentage of criminal transactions is low and reducing. Most use is speculative rather than criminal. There are future threats to consider regarding cryptocurrencies; in particular the issue of privacy coins. But these coins arguably bring more risk to the user than cash and their use is as much a societal question of privacy as it is of crime. As we move towards cashless societies, usage of cash for transactions is falling - yet its role in criminal activities continues to be pivotal. For law enforcement, there may well be benefits in moving anonymous, untraceable cash transactions to a digital form. Cash is the greatest facilitator of crime, not cryptocurrencies, and is likely to remain so as long as it exists.

If we arrive at a future without physical cash, what do we want this to look like? Will private monetary systems, like cryptocurrencies or Facebook's Libra, be allowed or be a part of the mix? Or will a sovereign digital currency eventually emerge? These are global questions, which sit behind increasing geopolitical tensions; from sanctions avoidance as we saw with WannaCry and North Korea, to the possibility of a US-China currency war. The world is in a period of monetary history and transition. It is digital. It is global. And it brings in to question how the world currently operates, on a system of fiat money. The financial crisis served as the fire from which Bitcoin emerged, and raised with it wider questions of government-controlled finances. Bitcoin and cryptocurrencies, if nothing else, add to the multitude of payment options that now exist in the world. Whilst it is highly doubtful that they will replace any of the dominant sovereign currencies anytime soon, they could yet play a role in money, even if only a small one. The risks that they pose, both now and in the future, are not as great as some proclaim.

References

Alderman, Liz. 2018. “Sweden’s Push to Get Rid of Cash Has Some Saying, ‘Not So Fast.’” The New York Times. 2018. https://www.nytimes.com/2018/11/21/business/sweden-cashless-society.html.

Androulaki, Elli, Ghassan O Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. 2013. “Evaluating User Privacy in Bitcoin.” In *Paper Presented to Financial Cryptography and Data Security, 17th International Conference, Okinawa, Japan, 1-5 April*.

Antonopoulos, Andreas. 2017. *Mastering Bitcoin: Programming the Open Blockchain*. Second. Farnham: O’Reilly Media.

Bank of England. 2019. “What Is Money?” 2019. https://www.bankofengland.co.uk/knowledgebank/what-is-money.

Barclays. 2019. “International Business Payments.” 2019. https://www.barclays.co.uk/business-banking/business-abroad/international-payments/.

Barysevich, Andrei, and Alexandr Solad. 2018. “Litecoin Emerges as the Next Dominant Dark Web Currency.”

Berr, Jonathan. 2017. “"WannaCry" Ransomware Attack Losses Could Reach $4 Billion.” CBS News. 2017. https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/.

bitcoinfees.info. 2019. “Bitcoin Transaction Fees.” 2019. https://bitcoinfees.info/.

Blandin, Apolline, Ann Sofie Cloots, Hatim Hussain, Michel Rauchs, Rasheed Saleuddin, Jason Grant Allen, Bryan Zhang, and Katherine Cloud. 2019. “Global Cryptoasset Regulatory Landscape Study.” https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2019-ccaf-global-cryptoasset-regulatory-landscape-study.pdf.

Boughton, James M. 2001. *Silent Revolution : The International Monetary Fund, 1979-89*. Washington DC: International Monetary Fund.

Brandom, Russel. 2019. “Senators Aren’t Sold on Facebook’s Libra Project.” The Verge. 2019. https://www.theverge.com/2019/7/16/20696350/facebook-libra-senate-banking-committee-hearing-david-marcus-cryptocurrency.

Brown, Randy. 2019. “In A U.S.-China Currency War, Who Wins?” Forbes. 2019. https://www.forbes.com/sites/randybrown/2019/08/15/in-a-us-china-currency-war-who-wins/#202f79ee751c.

Business Insider. 2018. “Sweden’s Reduced Cash Circulation Means Black Market Crimes Increase.” 2018. https://www.businessinsider.com/swedens-reduced-cash-circulation-means-black-market-crimes-increase-2018-6?r=US&IR=T.

Canellis, David. 2019. “Bitcoin Whale Moves $468 Million Crypto-Fortune for Less than $400.” Thenextweb.Com. 2019. https://thenextweb.com/hardfork/2019/07/29/bitcoin-whale-moves-468-million-crypto-fortune-for-less-than-400/.

Carney, Mark. 2018. “The Future of Money.” 2018. https://www.bankofengland.co.uk/-/media/boe/files/speech/2018/the-future-of-money-speech-by-mark-carney.pdf?la=en&hash=A51E1C8E90BDD3D071A8D6B4F8C1566E7AC91418.

Casciani, Dominic. 2010. “500 Euro Note - Why Criminals Love It So.” BBC News. 2010. http://news.bbc.co.uk/1/hi/8678979.stm.

Chaum, David. 1983. “Blind Signatures for Untraceable Payments.” In *Advances in Cryptology*, 199–203. https://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF.
Cleland, Victoria. 2018. “Cash and Digital Payments in the New Economy: Response from the Bank of England to HM Treasury’s Call for Evidence.” www.bankofengland.co.uk.
Coinmarketcap. 2019. “Cryptocurrency Market Capitalizations.” Coinmarketcap. 2019. https://coinmarketcap.com/.
Cointelegraph. 2017. “IRS Uses Chainalysis to Track Down Bitcoin Tax Cheats.” 2017. https://cointelegraph.com/news/irs-uses-chainalysis-to-track-down-bitcoin-tax-cheats.
Croman, Kyle, Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, et al. 2016. “On Scaling Decentralized Blockchains.” In *International Conference on Financial Cryptography and Data Security*. https://doi.org/10.1007/978-3-662-53357-4_8.
Davies, Glyn. 2002. *A History of Money: From Ancient Times to the Present Day*. Cardiff: University of Wales Press.
Dodd, Nigel. 2017. “The Social Life of Bitcoin.” *Theory, Culture & Society* 35 (3): 35–56. https://doi.org/10.1177/0263276417746464.
European Central Bank. 2016. “ECB Ends Production and Issuance of €500 Banknote.” 2016. 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.” http://www.emcdda.europa.eu.
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.” https://www.europol.europa.eu.
Europol EC3. 2017. “Internet Organised Crime Threat Assessment (IOCTA) 2017.” https://doi.org/10.2813/55735.
Fanusie, and Tom Robinson. 2018. “Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services.” http://www.defenddemocracy.org/media-hit/yaya-j-fanusie-bitcoin-laundering/.
Ferguson, Niall. 2008. *The Ascent of Money: A Financial History of the World*. London: Allen Lane.
Financial Action Task Force. 2018. “International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations.” www.fatf-gafi.org.
Fish, Tom, and Roy Whymark. 2015. “How Has Cash Usage Evolved in Recent Decades? What Might Drive Demand in the Future?” *Bank of England Quarterly Bulletin* 55 (3). http://www.bankofengland.co.uk.
Foley, Sean, Jonathan R. Karlsen, and Tālis J. Putniņš. 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.” 2017. https://www.gov.uk.

Foreign & Commonwealth Office, National Cyber Security Centre, and Lord Ahmad of Wimbledon. 2018. “Foreign Office Minister Condemns Russia for NotPetya Attacks.” 2018. https://www.gov.uk.

Gehl, Robert W. 2018. “Archives for the Dark Web: A Field Guide for Study.” In *Research Methods for the Digital Humanities*, 31–51. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-96713-4_3.

Global System for Mobile communications Association. 2018. “The Mobile Economy.” *GSMA Intelligence*, no. 35: 11–11. https://doi.org/10.5121/ijcsit.2015.7409.

Grasshoff, Gerold, Zubin Mogul, Thomas Pfuhler, Norbert Gittfried, Carsten Wiegand, Andreas Bohn, and Volker Vonhoff. 2017. “Global Risk 2017: Staying the Course in Banking.” Boston Consulting Group. 2017. https://www.bcg.com.

Gudgeon, Lewis, Patrick Mccorry, Pedro Moreno-Sanchez, Arthur Gervais, and Stefanie Roos. 2019. “SoK: Off The Chain Transactions.” https://eprint.iacr.org/2019/360.pdf.

Higgins, Stan. 2019. “EU Authorities Shut Down Bitcoin Transaction Mixer.” Coindesk.Com. 2019. https://www.coindesk.com/eu-authorities-crack-down-on-bitcoin-transaction-mixer.

HM Revenue & Customs. 2019. “Measuring Tax Gaps 2019 Edition.” https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/820979/Measuring_tax_gaps_2019_edition.pdf.

HM Treasury. 2018. “Cash and Digital Payments in the New Economy: Call for Evidence.” https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/689234/Cash_and_digital_payments_in_the_new_economy.pdf.

———. 2019. “Cash and Digital Payments in the New Economy: Summary of Responses.” https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/799548/CfE_-_Cash___Digital_Payments_Response_020519_vf_digicomms.pdf.

HM Treasury, Financial Conduct Authority, and Bank of England. 2018. “Cryptoassets Taskforce: Final Report.” https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf.

HM Treasury, and Home Office. 2017. “National Risk Assessment of Money Laundering and Terrorist Financing 2017.” www.gov.uk/government/publications.

International Monetary Fund. 2019. “Special Drawing Right (SDR).” Imf.Org. 2019. https://www.imf.org/en/About/Factsheets/Sheets/2016/08/01/14/51/Special-Drawing-Right-SDR.

Isige, John. 2019. “‘I Won’t Be Talking about Bitcoin in 10 Years’ US Treasury Secretary Mnuchin.” FXStreet. 2019. https://www.fxstreet.com/cryptocurrencies/news/i-wont-be-talking-about-bitcoin-in-10-years-us-treasury-secretary-mnuchin-201907241546.

Kappos, George, Haaroon Yousaf, Mary Maller, and Sarah Meiklejohn. 2018. “An Empirical Analysis of Anonymity in Zcash.” In *Proceedings of the 27th USENIX Security Symposium*. www.usenix.org/conference/usenixsecurity18/presentation/kappos.

Keatinge, Tom, David Carlisle, and Florence Keen. 2018. “Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses.”

Kharraz, Amin, William Robertson, Davide Balzarotti, Leyla Bilge, Engin Kirda, and

William Robertson. 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.

Kumar, Amrit, Clément Fischer, Shruti Tople, and Prateek Saxena. 2017. “A Traceability Analysis of Monero’s Blockchain.” In *Proceedings of the 22nd European Symposium on Research in Computer Security*. https://doi.org/10.1007/978-3-319-66399-9.

Lee, David. 2019. “Facebook Won’t Rule out Digital Currency Launch without US Approval.” BBC News. 2019. https://www.bbc.co.uk/news/technology-49092713.

Libell, Pryser, and Richard Martyn-Hemphill. 2019. “Cryptocurrency Ransom Demanded for Wife of Norwegian Tycoon.” The New York Times. 2019. https://www.nytimes.com/2019/01/10/world/europe/norway-kidnapping-monero.html.

Libra Association Members. 2019. “An Introduction to Libra: White Paper.” https://libra.org/en-US/white-paper/.

Luther, William. 2017. “How Much Cash Is Used by Criminals and Tax Cheats?” American Institute for Economic Research. 2017. https://www.aier.org/article/sound-money-project/how-much-cash-used-criminals-and-tax-cheats.

Martin, Fernando Eguren, Mayukh Mukhopadhyay, and Carlos van Hombeeck. 2017. “The Global Role of the of US Dollar and Its Consequences.” *Quarterly Bulletin, Bank of England* Q4.

Meiklejohn, Sarah, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. 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.

Moore, Daniel, and Thomas Rid. 2016. “Cryptopolitik and the Darknet.” https://doi.org/10.1080/00396338.2016.1142085.

Moser, Malte, Kyle Soska, Ethan Heilman, Kevin Lee, Henry Heffan, Jason Hennessey, Andrew Miller, Arvind Narayanan, and Nicolas Christin. 2018. “An Empirical Analysis of Traceability in the Monero Blockchain.” In *Proceedings on Privacy Enhancing Technologies*, 143–63. https://doi.org/https://doi.org/10.1515/popets-2018-0025.

Nakamoto, Satoshi. 2008. “Bitcoin: A Peer-to-Peer Electronic Cash System.”

Nick Szabo. 2008. “Bit Gold.” Unenumerated.Blogspot.Com. 2008. https://unenumerated.blogspot.com/search?q=bit+gold.

Office of National Drug Control Policy. 2014. “What America’s Users Spend on Illegal Drugs : 2000-2010.” *RAND Corporation*.

Owen, Gareth, and Nick Savage. 2015. “The Tor Dark Net.” *Global Commission on Internet Governance Paper Series*, no. 20.

Paquet-Clouston, Masarah, Bernhard Haslhofer, and Benoit Dupont. 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.

Polleit, Thorsten. 2012. “The Fiasco of Fiat Money.” Mises Institute. 2012. https://mises.org/library/fiasco-fiat-money.

Rappeport, Alan, and Nathaniel Popper. 2019. “Cryptocurrencies Pose National Security Threat, Mnuchin Says.” The New York Times. 2019.

https://www.nytimes.com/2019/07/15/us/politics/mnuchin-facebook-libra-risk.html.
Robinson, Tom. 2019. “Crypto Can Prevent Money Laundering Better than Traditional Finance.” Venturebeat. 2019. https://venturebeat.com/2019/07/20/crypto-can-prevent-money-laundering-better-than-traditional-finance/.
Rogoff, Kenneth S. 2016. *The Curse of Cash*. New Jersey: Princeton University Press.
Ron, Dorit, and Adi Shamir. 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.*
Russo, Camila. 2018. “Bitcoin Speculators, Not Drug Dealers, Dominate Crypto Use Now.” Bloomberg. 2018. https://www.bloomberg.com/news/articles/2018-08-07/bitcoin-speculators-not-drug-dealers-dominate-crypto-use-now.
Sands, Peter, Ben Weisman, Maja Sostaric, Alex Smith, Joel Smoot, Ofir Zigelman, and Joel Mathur. 2016. “Making It Harder for the Bad Guys: The Case for Eliminating High Denomination Notes.” www.hks.harvard.edu/mrcbg.
Shapiro, Harry, and Max Daly. 2016. “Highways and Buyways: A Snapshot of UK Drug Scenes 2016.” http://www.drugwise.org.uk.
Shi, Madeline Meng. 2018. “Fed Chair: Cryptocurrencies Are ‘Great’ For Money Laundering.” Coindesk. 2018. https://www.coindesk.com/fed-chair-cryptocurrencies-are-great-for-money-laundering.
Son, Hugh, Hannah Levitt, and Brian Louis. 2017. “Jamie Dimon Slams Bitcoin as a ‘Fraud.’” Bloomberg Technology. 2017. https://www.bloomberg.com/news/articles/2017-09-12/jpmorgan-s-ceo-says-he-d-fire-traders-who-bet-on-fraud-bitcoin.
Soska, Kyle, and Nicolas Christin. 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, Michele, Federico Maggi, and Stefano Zanero. 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.
The Economist. 2018. “Crypto Money-Laundering - Digital Detergent.” 2018. https://www.economist.com.
The Federal Reserve. n.d. “The Fed - How Much U.S. Currency Is in Circulation?” Accessed January 9, 2019. https://www.federalreserve.gov/faqs/currency_12773.htm.
The Swedish National Council for Crime Prevention (Bra). 2019. “Fraud and Economic Crime.” Brottsförebyggande rådet. 2019. https://www.bra.se/bra-in-english/home/crime-and-statistics/fraud-and-economic-crime.html.
The World Bank. 2019. “Remittance Prices Worldwide.” https://remittanceprices.worldbank.org/sites/default/files/rpw_report_june_2019.pdf.
Tor Project. 2019. “History.” 2019. https://www.torproject.org/about/history/.
UK Finance. 2018. “UK Payment Markets – Summary.” https://www.ukfinance.org.uk.
United Nations Office on Drugs and Crime. 2018. “World Drug Report 2018.”
US-CERT. 2017. “Malware Initial Findings Report (MIFR) - 10130295.”
Williams, Sean. 2018. “Which Cryptocurrencies Have the Lowest Transaction Fees?” The Motley Fool. 2018. https://www.fool.com/investing/2018/03/30/which-cryptocurrencies-have-the-lowest-transaction.aspx.
Wolfson, Rachel. 2018. “Tracing Illegal Activity Through The Bitcoin Blockchain To

Combat Cryptocurrency-Related Crimes." Forbes. 2018. https://www.forbes.com/sites/rachelwolfson/2018/11/26/tracing-illegal-activity-through-the-bitcoin-blockchain-to-combat-cryptocurrency-related-crimes/.

Xiaochuan, Zhou. 2009. "Reform the International Monetary System." Essay by the Governor of the People's Bank of China. 2009. www.bis.org.

———. 2017. "Statement of the Governor of the People's Bank of China at the 36th Minsiterial Meeting of the International Monetary and Financial Committee." Washington DC.

Yang, Yuan. 2018. "Why Millennials Are Driving Cashless Revolution in China." The Financial Times. 2018. https://www.ft.com/content/539e39b8-851b-11e8-a29d-73e3d454535d.

Zetter, Kim. 2012. "FBI Fears Bitcoin's Popularity with Criminals." Wired. 2012. https://www.wired.com/2012/05/fbi-fears-bitcoin/.

Endnotes

[1] Simon Butler was supported as part of the EPSRC Centre for Doctoral Training in Cyber Security at Royal Holloway, University of London (EP/K035584/1).
[2] Paper money has serial numbers, which has limited use for traceability.
[3] Terminology in this area varies but throughout this paper cryptocurrencies is used as an umbrella term for products and projects in this space but primarily refers to currencies such as bitcoin. Terms preferred by others include crypto-assets and virtual currencies.
[4] This paper adopts the accepted convention of using "Bitcoin" to refer to the system and "bitcoin" for the currency.
[5] Figures as at 02/08/2019.
[6] A pseudonym for an unknown individual or group.
[7] The first block of the blockchain.
[8] As open source projects they can be forked, implying a debatable form of inflation.
[9] The Silk Road was a prominent dark net marketplace between 2011 and 2013.
[10] Defined as using drugs four or more times in a month.
[11] Creating an account with a vendor, for example, and transacting with them to identify addresses used.
[12] Mixer sites provide a service to hide the source of a cryptocurrency (Higgins 2019).
[13] Price as shown on Coinmarketcap, <https://coinmarketcap.com>, accessed 07 August 2018.