Bitcoin Redux

Ross Anderson, Ilia Shumailov, Mansoor Ahmed and Alessandro Rietmann
Cambridge University Computer Laboratory

May 28, 2018

Abstract

We study how attempts to regulate cryptocurrencies, or at least to mitigate the harm they do, are misdirected. We started by looking at how one might blacklist stolen bitcoin, and find that two established legal principles – the nemo dat rule and the Clayton's case precedent – make tracing crime proceeds much simpler than researchers previously thought; they support a first-in first-out rule for taint tracking, which turns out to be much more efficient. However once we published initial results and were approached by theft victims, we discovered a more serious problem. Many bitcoin exchanges do not now give their customers actual bitcoin, but rather do off-chain transactions with other exchange customers or transact on customers' behalf with outsiders. Except where customers withdraw cryptocurrency into self-hosted wallets, the ownership of these assets is unclear. The number of off-blockchain transactions has increased enormously in the last eighteen months; we can't find good figures but the volume is sufficient to raise serious concerns and the practice falls under e-money regulations that are not being enforced. In short, the security, economics and regulatory problems of cryptocurrencies in 2018 turn out to be rather different from those described in the academic literature. The real problem is that we are seeing the emergence of a shadow banking system. Cryptocurrencies do not solve the underlying problems that made bank regulation necessary, and we sadly predict that many of the familiar second-order problems will also reappear. We discuss the implications for regulating cryptocurrencies and smart contracts more generally, and suggest eight things that regulators and central banks might usefully do.

1 Introduction

Bitcoin has become "a combination of a bubble, a Ponzi scheme and an environmental disaster," according to the Bank for International Settlements [Car18]. An idealistic experiment – in which cypherpunks tried to create a currency independent of central banks – went viral after the 2008-9 financial crisis. With its peak valuation of over $840bn exceeding Apple's market cap, the cryptocurrency bubble has attracted ever more speculators, ever more implausible startups and ever more attempts at regulation. The energy consumed by miners now exceeds that of Ireland, and is six times that of Europe's biggest wind farm [Her17]. Europol estimates that 3–4% of Europe's crime proceeds are laundered through cryptocurrencies, with the figure rising rapidly [Eur17]. New criminal applications have emerged, from online

drug markets to ransomware, and helped drive demand for bitcoin. Some of them may become permanent even if bitcoin disappears completely (now that its value fluctuates wildly, ransomware authors demand Amazon gift vouchers instead). The latest crime wave is bitcoin robberies – where investors in cryptocurrencies are held up at gunpoint and forced to transfer large sums on the spot to the robbers [Pop18]. The question of how to track and recover stolen bitcoin is urgent.

When asked by policymakers what might be done, technologists tend to be pessimistic: the cryptography appears sound, and as there's no-one in charge for the courts to go after, there's no obvious pressure point.

We beg to differ. Time and again, tech firms have challenged incumbent firms by circumventing an established industry's rules and regulations. Sometimes the outcome has been beneficial: online travel bookings make life easier than it was under old-fashioned travel agents, and online rating services make it more predictable. Sometimes we just replace one set of oligopolists by another: iTunes, YouTube and Spotify have displaced and impoverished the music majors. And sometimes the results are unpleasant. The cosy taxi monopolies in many cities may have been ripe for a shake-up; but when Uber started letting drivers work sixteen hours a day, failed to perform background checks on drivers and didn't report crimes against passengers, mayors acted. It was not enough for the company to say "We're not a taxi company, we're a platform.' They were found to be a taxi company soon enough, and in some cities – such as London – their license was withdrawn.

In many application areas, from taxis and hotels through insurance broking and air travel to health services, the solution turns out to be simple: just find ways to enforce the rules we already have. They have evolved over decades or even centuries and tend to fit their industries fairly well.

Our question in this paper is therefore whether the harm that cryptocurrencies do could be mitigated using existing laws and existing regulatory structures with at most very minor tweaks. We will answer this question cautiously in the affirmative. To do so we need to consider not just blockchain technology in the abstract, but actual industry practice and the relevant law and economics.

The contributions of this paper are to analyse how the law of stolen goods and existing financial regulations can create a natural framework in which the proceeds of crime can be traced in an efficient and incentive-compatible way. Section 2 deals with the issues of private and public law; section 3 with the shortcomings of existing approaches to blockchain tainting and bitcoin due diligence, and what a better approach would look like in both technical and business terms; section 4 presents empirical results, and section 5 describes the actual operation of the cryptocurrency markets; section 6 discusses policy options, and section 7 summarises our conclusions.

We turn to the law first.

2 Nemo Dat Quod Non Habet

'No-one can give what they don't own' is a rough translation of this section's title, an established principle of nearly all systems of law. If Alice steals Bob's horse and sells it to Charlie, Charlie doesn't end up owning it; when Bob sees him riding it, he can simply demand it back. This is natural justice; the horse wasn't Alice's to sell. However, it does leave a shadow of doubt over ownership in general. How can

you buy something without constantly living in fear that a rightful owner will turn up and ask for it back?

In medieval times there arose a specific exception for a 'market overt': if Alice steals Bob's horse and then takes it to the local public market, where she sells it openly between dawn and dusk to Charlie, then Charlie does indeed now own the horse. Bob can still seek damages from Alice, or seek to have her transported to the colonies or even hanged; but the horse is now Charlie's. This incentivises people to buy and sell at markets (which the king can regulate and tax), and also encourages crime victims to go to the local market to check whether their property's on sale there, which in turn may deter crime.

Britain abolished the 'market overt' exception to the 'nemo dat rule', as lawyers call it, in 1995 following abuse by thieves selling stolen antiques. But two exception remain that are of possible relevance to some cryptocurrencies: for money and for bills of exchange.

The nemo dat rule and its exceptions are discussed in the case of bitcoin by Fox [Fox16], whose analysis we draw on and extend here. See also his book on the law of money, especially chapter 8 [Fox08]. Now the USA has designated bitcoin a commodity, but there is a lot of lobbying pressure to treat some of it, or at least some cryptocurrencies, as money; Japan has gone as far as designating it 'virtual money' while other countries treat it as money for some purposes [Gla18]. In the UK, the tax authorities treat it as foreign currency for the purposes of value-added tax but as a commodity for income tax. There is a survey of cryptocurrency status by Freshfields according to which there appears to be nowhere that treats bitcoin simply as money [Fre18]. In the most important jurisdiction of all, the USA, it is treated as a commodity.

In what immediately follows, we will assume that bitcoin is a commodity We will explore what the consequences might be if it comes to be treated as money, or as a bill of exchange, in section 6. For present purposes, all we need to know is that someone who receives money or a bill of exchange in good faith and for value can get good title to it. Unless cryptocurrencies acquire this privileged status, there is no general exception to the nemo dat rule – so a theft victim can pursue and retrieve his stolen property.

First we need to look at what governments are already doing to help crime victims and to olice the sector generally.

2.1 The push for bitcoin regulation

Following the 9/11 terrorist attacks and the US Patriot Act, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) led a worldwide push to standardise anti-money laundering (AML) measures in order to make life harder for those who finance terrorism, and for others involved in serious crime. These measures include regulation of money service businesses (MSBs), which include not just banks but also remittance services, foreign exchange dealers, and businesses such as law firms that handle clients' money. MSBs are generally required to have know-your-customer (KYC) measures that typically involve knowing the ultimate beneficial owner of a corporate body, and in the case of a personal customer, getting a copy of their passport or ID card, plus a proof of address such as a utility bill.

By 2013, Bitcoin had been forced on the attention of the US authorities by Silk

Road, a website operated as a Tor hidden service that enabled people to buy and sell drugs by post. The key innovation was that payments could be made anonymously using bitcoin. (This service may have significantly increased the demand for bitcoin, raising its price from the tens of dollars to the low hundreds.) In March 2013, FinCEN issued regulatory guidelines directing miners and exchanges to register as money service businesses, and in May seized US accounts belonging to Mt. Gox, a Japanese bitcoin exchange that had failed to register. In September, the FBI arrested Ross Ulbricht, the Silk Road operator, and seized BTC 26,000 from his computer. The price of bitcoin crashed from $145.70 to $109.76 – but other online drug marketplaces were set up and the price quickly recovered. (Such illegal enterprises continue to turn over about half a million dollars a day [SC15]; for a detailed study of post-Silk-Road drug markets, see Bhaskar et al. [BLM17].)

In February 2014, Mt. Gox (then the second-largest bitcoin exchange) ceased trading and filed for bankruptcy, reporting that BTC 744,000 had been stolen. This is the largest cryptocurrency theft to date in terms of number of bitcoin; there have been bigger thefts in terms of dollar value, with perhaps 10% of all the money raised recently through Initial Coin Offerings having been stolen [She18]. It is commonly estimated that somewhere between 6–9% of issued bitcoins have now been stolen at least once [Lov14, Gra18].

Cryptolocker was the pioneer ransomware, spread from September 2013 to May 2014 by the Zeus botnet. It was a malware program that would encrypt your hard disk and demand a ransom in bitcoin for the decryption key. It also appears to have moved the price of bitcoin, and it has had many followers and imitators since – notably the Wannacry malware (later ascribed to the government of North Korea) which impacted a number of businesses, including the Spanish phone company Telefónica and half a dozen UK hospitals.

It is harder to tell what proportion of bitcoin are crime proceeds, not least because crimes vary by jurisdiction. Quite apart from Europol claims that $7-8bn a year of European crime proceeds are now laundered through cryptocurrencies [Sch18], they have reportedly been used by residents of countries with exchange controls, such as Russia, China and South Africa, to get their money out of the country[1]. India now outlaws the purchase of cryptocurrency using rupees. As the USA and Europe don't have exchange controls, exchange control offences are not recognised there. Other grey areas include Uber's decision to use bitcoin in Argentina in 2016 after the government there blocked its credit card payments.

Overall, therefore, one might suppose that somewhere between 10–20% of issued bitcoin by value might count as the proceeds of crime, depending on one's definitions of crime. But it's more complex than that, as coins are repeatedly split and consolidated as they are spent. (We will discuss how to deal with this later.)

Against this backdrop, FinCEN's efforts to compel bitcoin exchanges to register as money service providers have made steady progress, with many governments now following the US line. Their regulations vary quite a lot, though: while the Philippines simply requires exchanges to register as foreign exchange dealers, Italy has a decree on 'virtual money' which fairly comprehensive reporting requirements – but which is vague about whether cryptocurrencies are legally money [BC18].

[1]Indeed the latest Bitcoin bull run started in October 2016 when the Renminbi dropped in value against the dollar, driving the bitcoin price from the $600 at which it had been stable through the summer to the high 700s

Initially, some bitcoin exchanges only insisted on passports and utility bills from customers who wanted to change cryptocurrency to or from dollars or other fiat money, not on those who wished to change bitcoin for other cryptocurrencies such as ether. During 2017, FinCEN raided several such businesses in the USA and established their guilt in court [Har17]. Without such a rule, it would be trivial for criminals to launder money by changing it from bitcoin to ether and back again. FinCEN has also taken action against exchanges overseas, including BTC-e – which apparently handled many of the bitcoin stolen from Mt. Gox[2]. Other countries have taken even stronger measures; Germany, for example, has banned LocalBitcoins (which let individuals trade cryptocurrency and normal money face-to-face) and bitcoin ATMs [Han18], which are associated in the UK with laundering drug money [CG17].

Japan, with many bitcoin users, has registered 11 exchanges, including market leader BitFlyer, and in late 2017 had a further 17 applicants in the pipeline, all of whom will have to not just know their customers and manage client money separately, but also meet minimum capital requirements [Rev17]. Twelve exchanges that could not meet these criteria were shut down. South Korea has taken an even more aggressive approach: bitcoin exchanges must pay tax and will soon have to share customer transaction data with banks, to enable the detection of tax avoidance [Mey18]. The announcement of this rulemaking broke the January bubble's bull run, causing a drop in bitcoin's value of over 50% from the peak.

The latest turn of the screw comes from the European Commission, which announced in November 2017 'empowerments to set-up and maintain a central database registering users' identities and wallet addresses accessible to financial intelligence units' [Jou17]. The original proposal was self-declaration forms for bitcoin owners; however in December the Council decided that providers of wallet hosting services will have to register as money service businesses. This change was announced in May just as we were preparing the final version of this paper; we describe its provisions in section 5.2 below. As most cryptocurrency owners now appear to use online wallet services to hold their coins[3], this will bring the great majority of bitcoin transactions and holders within the regulatory net, at least to the extent that they use regulated exchanges rather than rogue ones.

2.2 Bitcoin laundries

Given that the cryptocurrency market is now partially regulated, it is curious to see money laundering services being promoted openly. Here the perspectives of lawyers and bitcoin enthusiasts may be somewhat different.

Cryptographers have long worked on remailers or mixes, invented in 1982 by Chaum, which enable email and other message traffic to be sent and received anonymously. If Alice wants to send an anonymous email to Bob, she can send it first to Charlie and ask him to forward it to Bob. Chaum proposed that, to frustrate naïve traffic analysis, Charlie would accumulate a number of encrypted messages and mix them up before relaying them. If Alice doesn't want Charlie to read her

[2] the available bitcoin mixes have nothing like the capacity needed to launder the proceeds of such large crimes

[3] or at the very least, an app tied to online back-end and backup services, which amounts to the same thing for present purposes

message, she can first encrypt it with Bob's public key. If she doesn't want to let her ISP (or a police wiretap) know she's communicating with Bob, she can take the message that's already encrypted with Bob's public key, and now encrypt it also with Charlie's public key, so that all the police see is a message to Charlie. If she wants Bob to be able to reply to her, she can include a cryptographic reply coupon. As we think of more and more possible threats, such systems become ever more complex. The most common anonymity system, Tor, sends worldwide web traffic through three nodes between your Tor browser and the server you wish to visit, so that your anonymity is protected against one or two of them being compromised. There is now a very substantial literature on anonymity systems, with all sorts of clever attacks on them and complex trade-offs between performance and security.

Cryptographic 'mixmaster' remailers were a significant part of the cypherpunk culture from which bitcoin emerged, and so it is unsurprising that various people started offering mixing services for bitcoin, with evocative names such as bitcoinfog, coinjoin and tumblebit. (A newer cryptocurrency, Zcash, has a kind of Aladdin's laundry: it lets users put their coins back in the mine and get out new coins that are indistinguishable from other freshly mined coins.) Some of these 'schemes', as cryptographers tend to call them, use clever tricks such as ring signatures and smart contracts. Others are simpler; Möser et al reported that one bitcoin laundry turned out to be just a single fat wallet, and if a customer paid in some bitcoin on a Monday, the operator would return a slightly smaller sum on Tuesday [MBB13]. But whatever the quality of the mixing – in some technical sense – the underlying idea is that if you put one black coin into a sack with nine white ones and shake them hard enough, the output will be ten white coins.

However, we noted above that even if cryptocurrency become money, you have to get coins in good faith in order to acquire good title; this is discussed extensively by Fox [Fox16]. As all bitcoin transactions ever made are in plain sight on the blockchain, the act of passing a bitcoin through a laundry should put all its subsequent owners on notice that something may very well be wrong. Coin checking has been discussed since at least 2013, coin checking services exist, and bitcoin exchanges claim to do it. If coin checking is now a reasonable expectation, the likely outcome of feeding one black coin and nine white coins into a bitcoin laundry isn't ten white coins, but ten black ones. When matters come to court, any laundries that are clearly identifiable as such are likely to have exactly the opposite effect from that asserted by their designers and operators. In short, people designing money laundering mechanisms have been using quite the wrong metrics of quality. We will return to this later.

Let us first consider how one might trace stolen bitcoins, from a purely technical point of view.

3 Tracing the proceeds of crime

Every bitcoin consists of its entire history since it was mined. What a wallet stores as a bitcoin is just a pointer to the relevant unspent transaction output (UTXO) and the signing key needed to assign the value therein to someone else. However the value derives from a series of pointers to previous transactions in the blockchain, each of which has inputs and outputs, going all the way back to where the bitcoin's constitutive components were originally mined. So it is fairly straightforward to

trace a transaction's history, at least in principle. How might it work in practice?

There has been significant work already on tracing transactions and analysing their patterns in the blockchain; a good starting point is Meiklejohn et al [MPJ+13]. For convenience, bitcoin operators use multiple wallets and pass money between them using automated scripts; change wallets are used to break up large amounts and give change, while peeling chains are used to pay multiple recipients out of a single wallet and multisource transactions are used to consolidate small sums into larger ones. (If this is unfamiliar, the book by Narayanan et al. [NBF+16] describes bitcoin mechanics in detail.) Clustering analysis can link up the different wallet addresses used by a single principal; we noted that Meiklejohn identified over half a million addresses used by Mt. Gox, then the second-largest bitcoin exchange. Commercial blockchain analysis firms do this at scale. Their customers are typically law enforcement, and those exchanges who wish to do due diligence on payments to and from third parties.

There is also research by academics trying to understand and map out the ecosystem. Seminal papers were by Ron and Shamir who traced a significant number of Silk Road bitcoin that the FBI had missed [RS13], and two papers by Möser, Böhme and Breuker. In 2013, they used test transactions to analyse the operation of Bitcoin Fog, BitLaundry and other anonymisation services [MBB13]; in the second, they present a detailed analysis of how taint tracking might work through multiple transactions [MBB14]. Their focus was on two algorithms for dealing with multisource transactions of which one input was tainted: these were 'poison' (whereby the whole output is tainted) and 'haircut' (where the output is tainted by the percentage of input value tainted). It appears that 'haircut' tainting is a default.

The commercial blockchain analysis firms are cagey about their methods – their terms of service typically require customers not to reverse engineer their algorithms. They employ staff to make multiple small payments into and out of both exchanges and the underground merchants using bitcoin, use clustering analysis to link together the wallets each actor uses, and then track the flows between them; the focus is at the application layer of payer and payee intent rather than at the level of the blockchain. Whatever the details, coin checking appears to be accepted good practice; even some rogue bitcoin exchanges claim to do it.

Curiously, there is no publicly-available blacklist for the blockchain, tracking coins that are reported stolen, extorted or otherwise proceeds of crime. Blockchain.info used to make one available [MBB13], but this has been discontinued.

3.1 Practical tracing on the blockchain

So we set out to construct our own taint of the blockchain, and then to make test purchases of due diligence reports to see how they compared.

Our work had started in the context of a project to measure the cost of cybercrime, where we sought to estimate the proceeds of ransomware by developing analytics to spot ransom payments on the blockchain. Starting with cryptolocker, we rapidly found 3,500 infections in 2013–4, generating millions of dollars in ransom payments. However, ransomware patterns have become more complex over time and the parameters have to be tuned carefully to avoid false positives. It also appears that quite substantial sums obtained by ransomware may have mixed in with crime proceeds from underground drug markets. We therefore wanted better tools to trace

the flows of bitcoins of mixed origin.

To get ground truth on tainting, we started with some addresses of reported bitcoin thefts [4], collected from online reports, and tracked the stolen coins forwards through hundreds of thousands of blocks. At this point we encountered the difficulty already described by Möser et al. Bitcoins are not only split into smaller amounts in change transactions, but also joined together by multisource transactions. Over thousands of blocks of transactions, 'haircut' tainting smears the taint over the actively traded bitcoin stock. Bitcoin laundries are designed to make this even worse.

We therefore studied tainting more closely, and discovered that legal scholars already have an interesting answer.

3.2 Clayton's case

In English law, there is a long-standing legal precedent on tracing stolen funds. It was established in 1816, when a court had to tackle the problem of mixing after a bank went bust and its obligations relating to one customer account depended on what sums had been deposited and withdrawn in what order before the insolvency. Clayton's case (as it's known) sets a simple rule of first-in-first-out (FIFO): withdrawals from an account are deemed to be drawn against the deposits first made to it [vN16]. Although a judgment of the High Court in London, the legacy of the British Empire and Commonwealth ensured that this principle has become embedded in the law of many other countries too [vHMtQ03].

The FIFO rule makes tracing bitcoins deterministic and, at least in principle, straightforward. The 744,000 bitcoins stolen from Mt. Gox can be traced to the same amount[5] available as UTXOs for spending at addresses on the blockchain today. In what follows, we will assume FIFO tainting as a default, except where the circumstances of a set of transactions mandate a different approach – as with bitcoin laundries or mixes, where the manifest bad faith directs us to use poison tainting instead. There are also different rules where one of the principals in a transaction is a trustee, which might be the case if a bank or investment fund were buying and selling bitcoin on behalf of clients.

3.3 Empirics of FIFO tainting

We constructed a first attempt at a FIFO taint starting from a few well-publicised coin thefts[6], and ran it from the genesis block to 2016, we found that it concentrated the taint more than a haircut tainting strategy does.

For example, the 2012 theft of 46,653 bitcoin from Linode now taints 16,855,619 addresses, or just over 93% of the total, if we use the haircut algorithm; with FIFO, it's 245,120 or just over 1.35%. More recent hacks spread the taint even less; for example, the 2014 Flexcoin hack (where 'the world's first bitcoin bank' closed after all their coins were stolen) now taints only 15,265 accounts if we use FIFO, but 10,421,112 (or over 57% of all addresses) if we use haircut.

[4] 132 in our first paper [ASA18] and 56 in this one

[5] less burned coins

[6] data from https://bitcointalk.org/index.php?topic=576337.msg6289796#msg6289796

The reasons should be clear from the graphics here. Imagine that the red bitcoin input to a transaction are stolen, the green ones are blacklisted as they're from Iran, the blue ones have been marked by an anti-money-laundering screening program as the output of a bitcoin laundery, and the yellow ones are the proceeds of drug sales on an underground forum. The question is: which of the outputs of each transaction is tainted, and to what extent?

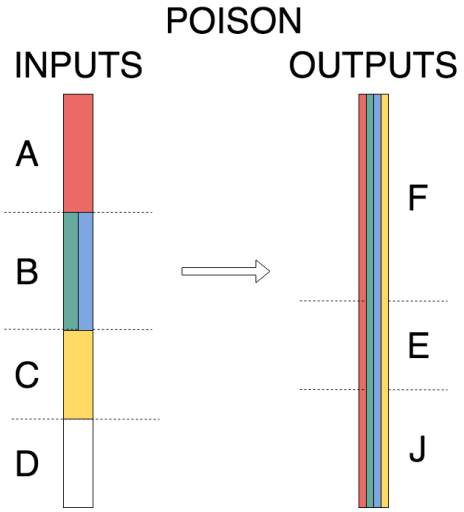

Figure 1: poison tainting

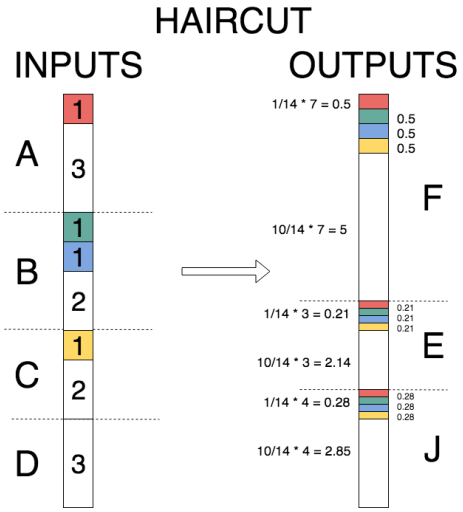

Figure 2: haircut tainting

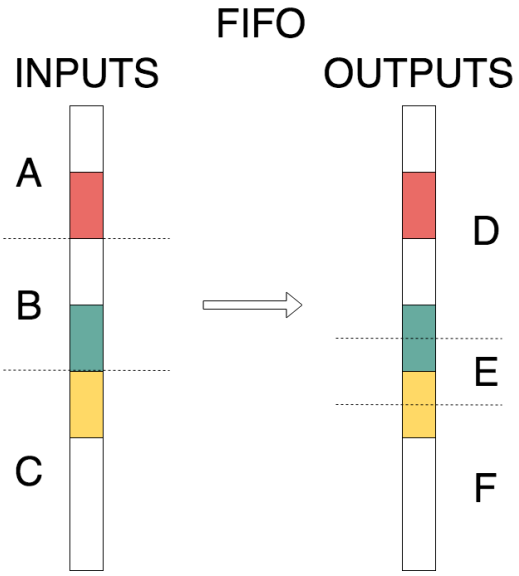

Figure 3: FIFO tainting

The poison diagram shows how all outputs are fully tainted by all inputs. In the haircut diagram, the percentages of taint on each output are shown by the extent of the coloured bars. The taint diffuses so widely that the effect of aggressive asset recovery via regulated exchanges might be more akin to a tax on all users.

With the FIFO algorithm, the taint does not go across in percentages, but to individual components (indeed, individual Satoshis) of each output. Thus the first output has an untainted component, then the stolen component – both from the

first input – and then part of the Iranian component from the second input. As the taint does not spread or diffuse, the transaction processes it in a lossless way. This means that we can trace a bitcoin's heritage backwards as well as tracing taint forwards, and we can do tracing extremely efficiently once the appropriate index tables have been built.

3.4 Empirics and incentives of taint tracking

The existing taint-tracking services have two customers: law enforcement and intelligence agencies, who typically focus on serious crimes such as underground drug markets and multimillion-dollar hacks of exchanges, and the provision of coin-checking services to exchanges and financial institutions who want to be able to demonstrate that they exercised due diligence when acquiring cryptocurrency assets.

Now due diligence is well known to suffer from perverse incentives. No banker really wants to know that one of his clients is a mafiosi, and certainly no banker would be comfortable with a law that made him strictly liable if a customer turned out to be one. Lobbying pressure from financial institutions leads to risk management morphing into standardised due diligence procedures that can be applied mechanically – of which the standard requirement that new bank customers show a passport and two utility bills is a good example.

We therefore made a number of test purchases of AML reports on specific UTXOs which we identified as suspect. In one case, a 'Standard AML/KYC Risk Report' assesses a tainted coin as 'medium risk', noting 'illicit activity risk' (but giving two risk levels of 64% and 11% with no explanation), and unquantified 'Danger detected' for 'transactions impeding track of funds' and 'transactions with distinctive patterns'. Other reported categories for which danger was detected included cybercrime risk, industry risk and connected parties. Yet this coin contained a significant component that had been publicly reported stolen. In a second case, a checking firm returned 'scam alert: none' to one of the main Cryptolocker addresses and also to the main Sheep Marketplace theft laundry address. In a third case, a checking service gave the all-clear to an address being used by cryptomining malware distributors on an underground forum scraped by colleagues at the Cambridge Cybercrime Centre.

When we asked one firm why they stopped publishing negative recommendations and removed old ones from their websites, they said they 'wouldn't match risk appetite of every user thus we can only provide risk assessment and leave the decision to the user.' In short, the due-diligence market is not just a market for lemons, but one in which many customers show at least symptoms of information avoidance [GHL17].

The incentives facing firms who supply blockchain intelligence to law enforcement are better. If hundreds of online test purchases of drugs provide evidence of drug dealers laundering their proceeds through an unregulated exchange such as BTC-e, this may provide probable cause for a warrant. And indeed the sales pitches of such firms target major crime. Bitfury, for example, claims in its sales presentation that by the end of August 2017, the Wannacry attackers had collected 53.46 BTC, approximately 52 BTC of which were transferred further; they name the HitBTC exchange as the destination of some of the extorted funds. Their pitch is that 'investigators could catch the perpetrators of such crimes much more efficiently, potentially preventing significant damage' [Bit18]. (We will consider what's actually

involved in recovering money from HitBTC later.)

But there are still shortcomings: the leading police and intelligence agencies tend to focus more on big busts, rather than on protecting ordinary consumers. This is already a problem in frauds using normal banking and payment systems; despite the fact that most property crimes in developed countries are now frauds rather than burglary or car theft, the resources devoted by most police forces to 'cybercrime' are tiny and they push crime victims to complain to their bank when they can, or even blame the victim for the crime [And16]. Given the common police view that bitcoin users tend to acquire cryptocurrency with a view to buying drugs online, it is even less likely that they will bestir themselves to help ordinary bitcoin crime victims, and we have come across no sign of such enforcement action. If ordinary people are going to use cryptocurrencies at all, how can they protect themselves?

We therefore decided to make our blockchain taint public. It will display deterministic tracking of reported crime proceeds and will also support analytics to spot tumblers and some non-reported crimes such as ransomware. We hope to facilitate the emergence of an open crime-tracking community, first, as a resource for innocent bitcoin users to check out coins they're offered in payment; second, as a resource for small law-enforcement agencies who don't have the budget to buy in specialist services; third, as a platform for academics studying cybercrime; and fourth, as a means of mitigating the lemons market in due diligence.

We call our public database of blockchain taint 'the taintchain'. We are making it available at `http://www.taintchain.org` and the software via the Princeton BlockSci project.

3.5 What else our new tools can tell us

Although the focus of this research project was looking at the proceeds of ransomware and then at the proceeds of crime more generally, FIFO taint tracking can be used for other research purposes. In particular it can be used to analyse local money flows, local clustering and other economic factors that lie somewhere between micro and macro. We observe for example that some bitcoin have been repeatedly circulated by bad actors, having been stolen more than once. We observe that taint from theft becomes entangled with taint from drug trafficking and from the trade in cybercrime tools. These are topics for further papers and for research by others now that our tools are available to all.

4 Dealing with crime proceeds

We are not the first to propose a public blacklist. The Bitcrime project produced recommendations in January 2017 to the effect that Europol should maintain a public blacklist for Europe [BGP+17]. However that was developed in the context of German privacy law and recommended that the public blacklist contain only the taints resulting from coin crimes on which a court had made a final decision.

4.1 Theft reporting in theory

The Bitcrime authors were concerned about the rights of bitcoin holders who might be falsely accused, and about the property rights not just of the immediate recipients

of disputed coins but about the rights of subsequent holders. The Bitcrime authors therefore proposed that when bitcoin crimes are reported, the affected coins would go on a blacklist maintained privately by the local prosecutor's office. With tens of thousands of prosecutors worldwide, this does not really scale. And attackers might launch a service-denial attack on the taintchain by making large numbers of malicious theft reports. Prudent practice is to require victims to report crimes in person to the police. There are also issues around forensics, but these are already familiar from the investigation of conventional bank frauds.

In English law, there is no statute of limitations for theft and, so long as bitcoins are commodities rather than money or bills of exchange, the original owner can demand them back. This should apply with particular force if stolen coins end up in the wallets of bitcoin exchanges that are regulated financial service firms; and once hosted wallet service providers fall under the EU's 4th anti-money laundering directive from November 2018, it will apply through them to the great majority of everyday users. There should be effects on other actors too. FIFO tainting will taint not just regular transaction outputs but also mining fees. Mining pools will therefore have an incentive to avoid mining tainted transactions, and there are various ways to do this without the overhead of making thousands of taintchain lookups per block, such as by mining only blocks from regulated actors.

It would be bizarre if regulators did not eventually require licensed exchanges to confiscate crime proceeds; Europol is already complaining of their lack of cooperation [Sch18]. Governments already seize drug-traffickers' money and vehicles under local asset-forfeiture laws [Eco17], and it will be natural to extend this effort to cryptocurrencies, which facilitate many other crimes too [VM15b, VM15a]. Rapid automatic taint tracking has the potential not just to return stolen bitcoin automatically to crime victims but to cut the incentive for a number of other crimes too.

So we wrote a technical paper with some early results [ASA18], publicised it with a Computerphile video [And18a], and waited for some theft reports to roll in.

4.2 Theft reporting in practice

Talking to real victims and looking at real theft cases has led us to radically revise our view of the cryptocurrency world. With one exception, the victims we talked to were using hosted wallets[7]. So rather than downloading wallet software and running it on their own machine, they had simply gone to an online service – typically a firm that was also an exchange – and exchanged their dollars, euros or pounds for bitcoin. When they logged on, a balance was displayed to them, and they could spend it by entering a payee and an amount, just like at a conventional bank website.

In one case (one of the thefts from Mt. Gox) the theft was clearly by an insider; our complainant reported a bitcoin balance that amounted to thousands of dollars at the time had simply gone to zero, with an insider presumably having intercepted the password or bypassed the password-checking mechanism. The outgoing transactions for that day include a set of four equal transactions, closely spaced in time, equal to the missing amount. That is the extent of the traceability. The liquidators of Mt. Gox have shown little interest in such small cases.

[7] At least at the time of the theft; one had BTC 42 in a desktop wallet, and after he transferred it to a hosted wallet, it was stolen by an exchange insider

Other cases are similar although it is generally less clear whether the compromise resulted from a customer's credentials being guessed, or stolen by malware, or whether there was inside collusion. In no case could we find any clear documentation of the actual ownership of the missing cryptocurrency.

On inspection, this opens up a number of cans of worms.

5 How the market really works now

Although the hosted 'wallet' of the exchange customer is represented as being essentially similar to a self-hosted wallet, which contains a signing key that can be used to authenticate a transfer of a UTXO to another blockchain address, the reality is different. Exchanges appear to keep most of the bitcoins that their customers think they own in offline machines known as 'cold wallets' for security reasons, and transfer bitcoin to and from them several times a day so that 'hot wallets', or online machines used for actual trading, have enough bitcoin to transact but not so much as to pose a catastrophic theft risk.

If that were the only optimisation introduced by the exchanges then it would matter little for coin tracing. If the bitcoin I bought from, or deposited at, an exchange were kept faithfully for me and made available for me to spend when I wished, then a stolen coin I received would still be traceable through my hands when I spent it later. This may have been the case at the time of Mt. Gox, but it does not appear to be generally the case now. A big change has taken place over the past eighteen months.

5.1 Who owns the bitcoin stock anyway?

There are two basic models for an institution to hold value on behalf of a customer. The first is the gold merchant. If I pay (say) £30,000 for a 1Kg bar of gold, the merchant would in the old days place a sticker on that bar in his vault with my name on it[8]. If the merchant went bust, I could turn up at the vault with my paperwork and collect the gold from the receivers; it was my gold after all, and the company was merely keeping it for me.

The second model is the bank. If I had placed my £30,000 at HSBC, then the bank does not stick my name on 1,500 £20 notes; it merely owes me the sum of £30,000. If it goes bust, I have to stand in line with all the other creditors to get my share.

Similarly, there are basically three ways you can buy and hold cryptocurrency.

1. You buy it from an exchange and get them to transfer it to your own wallet which is resident on your computing device and that contains your private key(s). This is the equivalent of collecting your gold from the bullion dealer or withdrawing your cash from the bank.

2. You buy it from an exchange and keep it there in a hosted wallet where the exchange holds the private key(s) on your behalf and the cryptocurrency actually resides in that wallet, in the sense that the keys are available to no other customer. Here the exchange actually has control over your keys and executes

[8] nowadays the bars have QR codes

transactions on your behalf, but only in respect of your cryptocurrency. This is the equivalent of the gold merchant who keeps identifiable and marked gold bars on behalf of customers. You can buy, hold and sell gold without actually taking possession of it, and you can even order it to be transferred to the account of a different customer of that merchant, but it is identifiably yours. We will call this '**the gold merchant model**'.

3. You buy it from the exchange and keep it in an account where you have a claim against a certain amount of cryptocurrency that the exchange is holding in its own wallet on your behalf. In other words, your balance is off-blockchain and intermediated by the exchange. This is typically how investors work as the exchange simply runs an account for them which is backed by the exchange's assets. The exchange might not actually possess assets that correspond exactly to its liabilities to its customers; it might lend cryptocurrency to other exchanges, trade in futures and options, and so on. The exchange may also offer transaction services whereby they will remit various cryptocurrency amounts, at your mandate, to the internal or external accounts of other parties. In other words, the exchange is operating as a bank. This appears to be the dominant business model but exchanges seem to be reluctant to spell this out in their contract terms. Anyway, we call this '**the bank model**'.

We have read the terms and conditions of a number of bitcoin exchanges and not one of them makes clear whether the exchange is like a gold merchant, selling you specific units of cryptocurrency and keeping them safe for you, or like a bank in that you merely have a claim against a certain quantum of its aggregated cryptocurrency assets.

Users appear to believe that the former is the case while industry insiders seem to assume it's the latter, and the blockchain appears to bear this out – as does the experience of theft victims.

We therefore looked at the accounts filed by the leading UK exchange, Coinbase. It consists of two companies, CB Payments Ltd., which holds customers' fiat money balances and is now regulated under the E-money Regulations, and Coinbase UK Ltd. which handles digital currency and is not regulated. According to accounts filed at Companies House, the first of these companies shows an operating loss of £162,760 in the year to December 2016 (the only year for which accounts have been filed) and a balance sheet of £958,874 – the amount left after its shareholders' funds of £1,121,635 were reduced by that amount. The second company is more substantial with a balance sheet showing £23,386,921 of creditors, balanced by £22,326,568 of cash, customer deposits and trade debtors. Such accounts have been filed for several years, the amounts roughly doubling each year. They appear to contain no record of digital currency assets.

Of course, the UK Coinbase companies are part of a larger group, so perhaps all the digital currency assets are kept by the US parent; and the boom in off-balance sheet transactions has taken place since the accounting date in question. A recent press profile of Coinbase emphasises its commitment to compliance and notes that it has $20bn in assets under management [Par18]. Nonetheless such a small balance sheet would be considered odd in a UK bank with an overseas parent. If the total market cap of cryptocurrencies is £300bn, and the UK's share of that is in line with its 5% share of world GDP, and Coinbase has a third of the UK market, then we'd

expect to see a balance sheet of £5bn, not £20m. Alternatively if the UK is 20% of the size of the US market and Coinbase has the same share in both, we'd expect to see $4bn. In short, we're out by two orders of magnitude. Looking for a hint, we note that Coinbase claims that all customer funds are kept in its cold wallet, with only 1% of the total being in its hot wallets for trading at any one time, and that this 1% consists of its own reserves [Par18].

It is curious that we see no trace of customers' pooled assets on the Coinbase balance sheet, which does not look anything like that of a bank. Perhaps the assets appear on the balance sheet of a different group company, or perhaps Coinbase has transitioned from being like a gold merchant to being like a bank in the seventeen months since the last accounts were filed. Certainly Coinbase goes out of its way to present itself as the good guy in the Wild West of cryptocurrency and we are not imputing any impropriety whatsoever. But if even the best actors fall short of the standard of transparency normal in legacy banking, this raises further questions, to which we will return in section 6.

5.2 Off-chain transactions

In practice, Alice goes to a bitcoin exchange and pays it (say) £1000. The exchange gives her (say) BTC 0.17 and displays this balance as being available to her to spend. If Alice now orders a payment of BTC 0.05 to Bob, then the exchange looks to see whether Bob is also a customer. If so, then the transfer is just a ledger entry; the balance seen by Alice reduces to BTC 0.12 while Bob's increases by BTC 0.05. This is known in the trade as an 'off-blockchain transaction.' These appear to have become the default over the period 2016–18.

The idea that off-chain transactions might become the norm was in fact first mooted by bitcoin pioneer Hal Finney: '*Bitcoin itself cannot scale to have every single financial transaction in the world be broadcast to everyone and included in the block chain... Most Bitcoin transactions will occur between banks, to settle net transfers. Bitcoin transactions by private individuals will be as rare as... well, as Bitcoin based purchases are today.*' [Dem18]

Getting hard data on the scale of off-chain transactions is harder. Demeester reports that Western exchanges do $80m in off-chain transactions per day [Dem18]; while charts by Cryptovoices show trading volumes per on-chain transaction taking off from early 2017 and showing peaks in the range of 6 to 14 times with a recent average of about 8 [Cry18]. There have been various attempts to create off-chain payment mechanisms between exchanges but it appears, talking to industry insiders, that the great bulk of off-chain payments (at least for bitcoin) are between customers at the same exchange. One of the drivers appears to have been the massive congestion in the blockchain in late 2016, when transactions could wait in the mempool for a day before being mined into the blockchain and transaction fees hit $50; now many blocks are partly empty and mining fees are near zero. All such figures need to be treated with caution: Ribes investigated various bitcoin exchanges via test transactions and concluded that the largest exchange at the time was faking 93% of its trading volume; the Chinese and Russian exchanges were generally suspicious when assessed using his methodology [Rib18].

In effect, crypto-currencies are morphing rapidly into an unregulated shadow banking system. While this may have been driven by congestion, it has a secondary

effect of consolidation: network effects appear to be pushing particular communities to consolidate round specific exchanges. Many bitcoin users in the USA and the UK use Coinbase, while Chinese speakers are more likely to use Binance, Japanese use bitFlyer and South Africans use Luno. It's convenient to use the same exchange as your counterparties: transactions are instant and fees are much lower – as bitFlyer explicitly notes in their marketing material. Gandal et al. noted that cryptocurrencies showed network effects up till about 2014 as transaction demand dominated, favouring bitcoin; then for a period the network effects vanished as investment demand took over [GH14]. Now it seems that network effects are kicking back in thanks to off-chain transcations. We really need better data on all this.

5.3 The e-money directive

The fact that substantial transaction volumes are now handled off-blockchain raises the issue of whether financial regulators in Europe should require exchanges to comply with the E-money Directive of 2009 [EMD99]. According to this, "electronic money" means *'electronically stored monetary value as represented by a claim on the electronic money issuer which is issued on receipt of funds for the purpose of making payment transactions; is accepted by a person other than the electronic money issuer; and is not excluded by regulation'.*

This regulation seeks to ensure, inter alia, that an issuer of prepaid debit cards has and maintains enough assets to back the credit balances on the cards that it currently has on issue. Exactly the same problem arises with bitcoin exchanges: what is to stop a exchange taking my money and displaying to me a credit of bitcoin (or other cryptocurrency assets) than it does not actually have? What is to stop an exchange selling $200m worth of bitcoin but buying only $100m in actual bitcoin, taking out the other $100m as dividends for its shareholders, and hoping to get away with it for a while? The rate at which exchanges have gone bust should warn regulators against complacency.

The text of the E-Money Directive appears to describe an exchange's transaction processing business well. So do financial regulators make exchanges comply with this Directive, via the regulations that implement it in each Member State? The answer appears to be no. In the UK it is down to the Financial Conduct Authority to instruct the Payment Services Regulator to apply the E-Money Regulations (2011) to particular payment systems; the Regulator tells us that as the FCA has not instructed her to regulate cryptocurrencies, she only applies the Regulations to the conventional currency balances kept at UK bitcoin exchanges. We will return to the FCA's position in 5.5 below. Meanwhile, their reluctance to regulate anything other than the fiat money component of a transaction is exploited by the exchanges. Coinbase's terms and conditions [Coi18], for example, make a clear distinction between 'E-money services' which relate to customer sterling balances, are regulated, and are provided by CB Payments Ltd., while 'digital money services' are provided by a separate company Coinbase UK, Ltd. We are warned '*You should be aware that the risk of loss in trading or holding Digital Currencies can be substantial. Digital Currency Services are not currently regulated by the Financial Conduct Authority or any other regulator. You should therefore carefully consider whether trading or holding Digital Currencies is suitable for you in light of your financial condition.'*

The situation in Germany is similar, but with different details. The regulator,

Bafin, has held back from imposing e-money regulation on cryptocurrencies with the argument that they do not represent any claims on an issuer, as there is no issuer, so they are not e-money within the meaning of the German Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetz); bitcoin are however financial instruments, units of account like foreign exchange with the difference that they do not refer to a legal tender[9] [Aut18a]. Bafin does note that '*Those buying and selling VCs commercially in their own name for the account of others carry out principal broking services which are subject to authorisation* and remarks in passing that '*In practice, VC undertakings often did not offer detailed explanations as to how they work at all, or did so in a vague manner. In many cases, no general terms and conditions were provided.*' And there has been enforcement action: Bafin has issued cease and desist notices to ban the promotion of the 'OneCoin' trading system in Germany [Aut17b] and an unlicensed broker, Crypto.exchange GmbH [Aut18b].

The OneCoin case is particularly interesting because the cease-and-desist order related to the company's not having an e-money license in respect of Euro remittances made within Germany to acquire Onecoins [Aut17a]. In that case, players in the system were 'merely adjusting balances' to transfer funds. In any case, an institution providing off-blockchain transactions at scale would appear to fall under 1.1(1)5 of the the German Payment Services Supervision Act as they are *'enterprises that provide payment services either commercially or on a scale that requires a commercially equipped business operation'*.

In short, in both the UK and Germany, the law empowers the regulator to require that digital currency operators who settle payments by means of off-blockchain transactions to register under the E-Money Directive, yet they have so far neglected to do so. Perhaps the cryptocurrency scene is simply moving too fast for them; the explosion in off-chain payment volumes seems to have happened since the start of 2017. Once they catch up – perhaps being forced to act by some scandal – the tools already exist. The UK E-money Regulations, for example, provide two years in prison for operating an e-money service without a license[10].

Once we realised that regulators were failing to apply applicable law to tackle the risks around off-blockchain transactions, we made a submission to the UK Parliament's Treasury Committee describing these risks and recommending that the E-money Regulations be applied to exchanges' digital currency services as well as to their customer balances in fiat currency [And18b]. We amplify that recommendation below, along with others on which our thinking has developed since our submission to parliament.

5.4 Directive PE CONS 72/17

On May 12th, the European Union published Directive PE CONS 72/17 [Uni18], with the snappy title of *'Directive of the European Parliament and the Council amending Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU'*. This was agreed quietly between the European Parliament and the Council (the Member States) in April, somewhat changes the regulatory landscape. Although it is justified as an antiterrorism measure, it will

[9] This could of course be fixed if some microstate could be persuaded to declare it to be such

[10] There is a survey of the regulatory status of cryptocurrencies in various countries at [Fre18]

have implications for consumer protection.

In December the Commission had signaled that regulation would be extended from exchanges to wallet hosting services. The new Directive does this but in a way that leaves a significant loophole.

The new Directive has at page 40 a definition of a 'custodian wallet provider' which is just about services that hold cryptographic keys. Recall that in section 4 we described two models of exchange wallet operation: the gold merchant case where the wallet provided by the exchange to its customer contains merely the cryptographic keys needed to sign transactions with the customer's own cryptocurrency assets, and the bank case where the customer merely has a claim on the exchange's asset pool. This definition covers the gold merchant case but fails on the bank case – which is what actually happens in practice.

The Directive says at recital 10 that virtual currencies (as it calls cryptocurrencies) should not be confused with electronic money, since although they can be used for payment, they can be used for other things too. This text does not exclude the application of the E-money Directive to off-blockchain transactions but may be used to confuse matters and argue that exchanges should continue to have a regulated business for fiat e-money balances and an unregulated one for digital currencies.

The Directive's intent is clarified (if that is the right word) on p39 that the definition of electronic money is that given in Directive 2009/110/EC: *'electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer'*. That seems to cover off-blockchain payments fair and square, and to our mind on-chain payments too. There is also a definition of 'virtual currency' at p40 as '*a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.*'

However most of the substance of the new Directive consists of detailed amendments to the Fourth Anti-Money Laundering Directive which can only be understood by painstaking cross-reference to the original. Some of the intentions are clear enough, such that there should be centralised systems recording the relationship between addresses and identified holders, which can be queried automatically by investigators on the trail of money laundering or terrorist financing (recital 21). Of real importance may be section 6: '*Member States shall prohibit their credit institutions and financial institutions from keeping anonymous accounts, anonymous passbooks or anonymous safe-deposit boxes*' (page 44). The directive also requires better public disclosure of the ultimate owners or beneficiaries of companies and trusts.

The lawgiver has in this case been contemplating only the money-laundering aspects of bitcoin exchanges, and not the fact that anyone can open an exchange and sell more bitcoin then they have. In addition to this consumer-protection risk there may also be a prudential risk, namely that the apparent $350bn market cap of the cryptocurrencies currently in issue may not be all that's at stake.

We are not lawyers, but feel that financial regulator should do more. As some Member States (notably Malta but also Estonia and the UK) try to market them-

selves an natural homes for cryptocurrency innovation, there will be a temptation to race to the bottom.

5.5 Positions of UK stakeholders, April 2018

The UK parliament's Treasury Select Committee called an inquiry into digital currencies to which many interested parties (including the first author) made submissions in April 2018. Following oral hearings, the written evidence was published on May 22nd, just before the final deadline for this paper. The submissions make for interesting reading.

We already noted that although off-chain transactions appear to fall squarely under the EU E-Money Directive and the UK E-Money Regulations, the Payment Services Regulator can't apply them as the Financial Conduct Authority (FCA) has not asked her to. The FCA explains its position in its Treasury submission [FCA18]. It follows the definition in EU Directive PE CONS 72/17 in that it sees wallets as storing keys (p1); there is no recognition or mention of off-chain transactions in its table of which operations around cryptocurrencies may or may not be regulated (p2), and like the European Commission sees wallets as simply storing the customer's cryptographic key (p1). It does not use the word 'currency', preferring its own term 'crypto-assets' which further helps ignore off-chain transactions, and claims 'Where crypto assets form part of regulated services, regulated firms can take steps to mitigate the money laundering risks' (p6). This may be somewhat optimistic given that Coinbase has separate firms for fiat money and crypto and carefully states in its terms and conditions that only the former is regulated, but the FCA is not too worried: unlike the EU, it sees the money-laundering risk as mostly in 'non-crypto asset typologies'. This position brings to mind the literature on information avoidance [GHL17]. The FCA appears to be shying away from a problem it should fix but which would complicate its mission. If it wants "crypto-assets" to be treated exactly the same way as shares in Tesco, then it should forbid regulated exchanges from providing any service that allows one customer to transfer them to another directly as a means of payment. But it does not.

The FCA is not the only institution that just doesn't want to know. The UK Financial Reporting Council, in its submission, discusses the difficulty of valuing crypto-assets. They should be valued at market if they are financial assets, but they don't meet the definition; so they have to be valued at cost as commodities, unless we change the rules to treat them like gold. However, this just isn't on the agenda of the International Accounting Standards Board.

6 Broader policy implications

So regulators are just not managing to keep up, and policy perspectives have changed hugely in three years. The 2015 survey of bitcoin economics, technology and governance by Böhme et al. now seems to come from a different century [BCEM15]. The number and scale of the scams together with the environmental harm caused by mining have created a consensus among governments and central bankers in favour of regulation, but so long as this is based on an outdated view of the problem it's not likely to be optimal.

In this section, we put forward some recommendations for discussion based on the state of play as we see it in May 2018.

Our **main recommendation** is that governments should regulate exchanges in the EU, or that do business with EU citizens, and which offer off-blockchain payments or consolidate cryptocurrency assets rather than merely holding crypto keys on behalf of customers, in respect of all these cryptocurrency assets under the E-Money Directive. Off-chain transactions, at the very least, fall within the definition of e-money and are vulnerable to exactly the kinds of scams and payment service failures that the E-Money Directive was established to prevent.

If regulators continue to believe that cryptocurrency exchanges fall outside the definition of e-money, then we will need a similar directive (let's call it the c-money directive) to tackle the same problems. But that would just waste everybody's time. We have a workable law, and just need to enforce it.

What more might be needed?

6.1 Consumer protection

A crime victim who asks an exchange for a refund of stolen bitcoin that were stolen from an account there can expect to be told that as digital currency is unregulated, they are out of luck.

But this is nothing new. In fiat banking, a customer who complains of phantom withdrawals from her account used to get into an argument with his bank who stonewalled her with something like 'Our systems are secure so you must have been negligent or collusive.' Yet the law eventually caught up in most countries. In the USA, early court cases paved the way for Regulation E and Regulation Z which provide much of the consumer protection on which bank customers rely in card transactions [vC80]. In the EU, the Payment Services Directive requires that the contract terms governing the use of the payment instrument must be 'objective, non-discriminatory and proportionate' (article 69), and where a transaction is disputed, 'it is for the payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency' (Article 71) [PSD00]. Crucially, 'the use of a payment instrument recorded by the payment service provider, including the payment initiation service provider as appropriate, shall in itself not necessarily be sufficient to prove either that the payment transaction was authorised by the payer or that the payer acted fraudulently or failed with intent or gross negligence to fulfil one or more of the obligations' (Article 72). European law not only agrees that payment records are not constitutive of title to money; they also impose reasonable constraints on what may be expected of users. Simply saying 'you should have chosen a better password' won't do; neither will 'the blockchain now says that your money belongs to Fred.'

At this point a conflict may arise if the provider's terms of service say 'you can't sue us' while consumer-protection law holds such contract to be unfair. Again, the Payment Services Directive comes into play, and there are other laws too around unfair contract and product liability. These can give some clarity if policy degenerates into a tussle over the burden of proof.

So our **second recommendation** is that the relationship between an exchange and its customer should be covered by the second Payment Services Directive.

6.2 Unregistered exchanges

Unregistered and downright criminal exchanges are an issue. Suppose that you were hit by the Wannacry ransomware, had paid a ransom, and wanted to get your money back. According to the US government, Wannacry was the work of North Korean government agents, but this isn't much help. So you note from the BitFury report that almost all of the bitcoin collected by Wannacry was laundered through the HitBTC exchange, so you want to serve a court order on them (whether for compensation, or merely to see the passport presented by whoever cashed those coins). You then find that their website does not contain a physical address for service, contrary to the E-commerce Directive, Article 5.1(b) of which requires '*the geographic address at which the service provider is established*' to be provided. A quick Google search reveals that others, including disappointed customers, have sought this information repeatedly; in 2014 someone purporting to represent HitBTC said that their business headquarters was in Copenhagen while their R&D was in Tallinn, and the address of the former would be provided 'soon'. (We're still waiting.) Others looked for the company name that appears on the website, and found a similarly-named UK company that had been deregistered in 2009. HitBTC does claim to abide by FATF rules, so where is it registered as a money service business? The Directive requires at 5.1(e) that it publishes '*where the activity is subject to an authorisation scheme, the particulars of the relevant supervisory authority*' yet there is no sign. It should perhaps surprise no-one that HitBTC is on Ribes' list of exchanges that appear to significantly overstate their trading volume; he uses the word 'fraud' [Rib18].

HitBTC is believed in the industry to be run by criminals in Russia, and promotes ICOs heavily – which is likely to involve offences under securities law in other countries. If it turns out that HitBTC is in a noncompliant jurisdiction, so it can't be raided and shut down, then conversations need to turn to sanctions, and whether regulated exchanges should be permitted to transact with such operators at all. Unregulated exchanges also pose a direct risk to users; Moore and Christin reported in 2013 that of 40 bitcoin exchanges, 18 had already closed, with customer account balances often wiped out [MC13]; their later study in 2017 showed that things had not improved [MCS17].

The means to do this exist in the new anti-money-laundering directive discussed earlier, which imposes a duty in respect of transactions involving high-risk third countries, which must be presumed to apply to HitBTC and BTC-e. Article 11 requires EU institutions to implement a number of enhanced due-diligence measures on such transactions including getting more information on the customer, the beneficial owner, the nature of the business relationship, the source of funds and the reasons for the intended transactions (p 50). What's more, the EU institution doing such a transaction must have it approved by senior management. It is hard to see how a UK exchange could discharge these duties in respect of a transaction to or from HitBTC.

Again, this is nothing new. Cryptocurrencies do not solve the underlying problems that made bank regulation necessary, and we can expect that many of the familiar second-order problems will also reappear in due course.

Our **third recommendation** is that regulators should prohibit the cryptocurrency exchanges they regulate from clearing and settling transactions with unregulated exchanges.

6.3 Innovation and the role of central bank cryptocurrency

Debate continues on whether bitcoin and blockchains have actually achieved anything other than emitting carbon dioxide and facilitating crime. Stinchcombe argues that ten years into its development, nobody has found a legal killer app for bitcoin yet [Sti17]. 'Each purported use case – from payments to legal documents, from escrow to voting systems – amounts to a set of contortions to add a distributed, encrypted, anonymous ledger where none was needed. What if there isn't actually a use case for the blockchain at all?'

But the markets still believe otherwise, and the recent surge in ICO valuations suggests that the future direction may be the use of smart contracts as a platform for innovation. Such applications generally use Ethereum, a system similar to Bitcoin but with a more expressive scripting language; from the legal viewpoint, they are simply contracts whose enforcement is automated.

As Raskin notes, 'innovative technology does not necessitate innovative jurisprudence' [Ras17]. In fact, a decent starting point is the existing law on vending machines and on the starter interruptors used to enforce some motor vehicle credit agreements. But although smart contracts are nothing especially new, regulatory intervention may be needed in egregious cases. Attempts to hide contracts behind machines have failed in the past: an early vending machine was invented by a 17th-century book publisher, Richard Carlile, who did not want to be jailed for selling books considered blasphemous. He argued that the purchaser's contract was with the machine, not with him; the court didn't buy this argument, and sent him to jail. The fact that he flaunted his attempts to evade prosecution made the case an easy one for the court [Ras17]. We can expect courts to be similarly unimpressed by contracts that are unfair, unconscionable or illegal; that are made using the visible proceeds of crime; or that are clearly contrary to public policy.

Regulators will have to think carefully about what regulation might mean if ether payment mechanisms are embedded in millions of low-cost devices. This will be made more complex by gas, the ether that is used up to pay for running smart contracts.

In this context, both regulators and entrepreneurs should consider common-mode failure risks. People have noted for some time that bitcoin is not as decentralised as some of its promoters claim. Gervais et al. raised this issue in 2014 [GKCC14], and Narayanan et al. expanded on it in their book [NBF+16], noting that a number of players – from the Bitcoin Core developers through the mining cartels to the exchanges – have some power in the system. Recently, Vorick has told the story of an attempt to set up a mining equipment vendor, which revealed that Bitmain now has a near-monopoly in the mining equipment market [Vor18]; it now apparently earns $4bn a year [Eco18, dV18].

Indeed, as Narayanan and his coauthors noted, the amazing and noteworthy thing about bitcoin is that it continues to operate as a (sort-of) global trusted computer despite having various parts of its kill chain controlled by vendors, miners, developers and exchanges. However many people expect a denouement sooner or later, and this is one of the reasons that central banks might consider a properly-engineered cryptocurrency to be worthwhile.

A quite different approach is that being pursued by the Enterprise Ethereum Alliance, who have adapted blockchain technology to work in closed groups. Nawaz, for example, describes a project at JP Morgan to use enterprise ethereum to auto-

mate the clearing and settlement of financial assets – which would not only enable the financial institutions who are members of an exchange to manage the asset register collectively. This enables the common-mode failure risks, the risks of transacting with criminal counterparties, and the more traditional solvency and liquidity risks, to be managed transparently. (The proposal would also make the assets programmable, so that participants could offer futures, options and other derivatives of arbitrary complexity – which may raise other regulatory issues, but they are not our concern here.)

So how might central bankers help?

Bitcoin promoters have hoped for some years that bitcoin would become fungible, in the way that coins are – one coin is as good as any other. One way of promoting fungibility was by providing mixes and other money-laundering facilities, but, as we have discussed, such facilities do not work very well and are counterproductive as they simply taint the laundered coins as being crime proceeds.

Another approach has been to argue that bitcoin should be money. If it is, then there are two exceptions to the 'nemo dat quod non habet' rule: money, and bills of exchange. In the case of money, you can get good title to stolen money if you received it in good faith and for value. Thus if you get a $20 note in change from a high street store, and it was actually stolen in a robbery last year, your acting in good faith cures the defect in title; and the same happens if you get it from an ATM. However if you trade something for cash with a shady character in the car park of a transport cafe, then the circumstances of the sale are sufficient to put you on notice that all may not be what it seems. If the money then turns out to be the proceeds of a robbery, you're out of luck.

The simplest way for a cryptocurrency to become money would be for a central bank to issue it. If the Bank of England were to provide cryptocoins saying, as banknotes do, *'I promise to pay the bearer on demand the sum of £20'*, then anyone who holds such a coin would be able to rely on it[11].

A 'LegitCoin', for want of a working name, would thus have powerful advantages over competitors: certainty of title, trust in it as a platform, and predictable value. So it is of great interest to hear that a consortium of Japanese banks is preparing to launch 'J coin', a digital currency convertible into Yen at par, with the backing of the Bank of Japan, and in time for the 2020 Tokyo Olympics [AL17]. The E-Money Directive would apply immediately and directly, at least in Germany, as such a coin would have a defined value.

So why should a central bank issue cryptocurrency? The best reason, as we see it, is to support innovation by providing a platform for smart contracts whose tokens can be converted into real money at par. If smart contracts are to provide a new infrastructure for entities in the Internet of Things to act as autonomous economic agents, simplicity and certainty will be of real value. Firms promoting businesses based on smart contracts should not have to contend with a wildly fluctuating exchange rate between ether and sterling, nor with the uncertainty that comes from dealing with coins that may previously have been crime proceeds. (A third source of uncertainty is technical: the programming language used to create the smart

[11] The general exemption from the nemo dat rule is bills of exchange, which include cheques, bills of lading, and indeed banknotes. We've kept the discussion to banknotes for simplicity. However if we end up with central banks issuing cryptocurrencies that support smart contracts for supply chain management, other bills of exchange will surely be constructed using them

contracts, which in the case of ether is far from ideal.)

One of the pieces of existing infrastructure that central banks might consider for smart contract functionality can be found in the Hyperledger project, a Linux Foundation hosted project that aims to provide a multitude of permissioned blockchain systems depending on the application. One of its subprojects, Hyperledger Fabric[12], looks promising given its use of a mature programming language, extensive architecture modularity and wide industry support. Being in active development, however, only time will tell if it lives up to its promise.

Our **fourth recommendation** is that central banks consider issuing a cryptocurrency that supports smart contracts, has the legal status of a bill of exchange and is redeemable at par for fiat money.

Meanwhile, the Japanese experiment will be worth watching.

6.4 Nature of ownership

As we've seen, a serious issue with existing exchanges is that it's unclear whether the bitcoins in the exchange's cold wallet are owned by the customer (as with a gold merchant) or by the exchange (as with a bank). The regulator should force exchanges to make that clear in their terms and conditions. As we noted, exchanges used to act sort-of like gold merchants (in the days of Mt. Gox) and appear to act sort-of like banks now. The lack of clarity goes back at least to Mt. Gox. According to their 2012 terms and conditions, *'it (MtGox) will hold all monetary sums and all Bitcoins deposited by each Member in its Account, in that Member's name as registered in their Account details, and on such Member's behalf.'* [Gox12] The comment of one of the victims to us was: 'It does not state that customers were signing up to a fractionally reserved exchange, and so customers had the understanding that MtGox (albeit in separate cold storage) actually possessed the bitcoins which customers saw in their balances when they logged in.'

Indeed, at present the fungibility of bitcoin seems to flow from the lack of clarity around ownership; although theft victims can trace stolen assets, they cannot establish whether they actually owned these assets, and so cannot sue to get them back. Clarity will enable the victims to sue either the exchange of which they were a customer when the theft occurred, or the exchange in whose custody the bitcoin now rest.

A separate policy issue is the nature of ownership of a digital asset. Some assets exist by virtue of registration, patents being an example. With most assets, the nemo dat rule makes the situation more complicated. Cryptographers assumed that owning the private key associated with a bitcoin's address was constitutive of ownership, but the law does not accept this at all. If registration is to constitute ownership (as with patents) there had better be a law to say so; but, as we noted above, the EU Payment Services Directive says the opposite.

A legislature that made cryptography constitutive of ownership would violate a number of established rights and principles, as we discussed. It would exclude, or at least make more complex, legal reasoning about intent, agency, liability and other issues that have already been discussed in the context of the law on digital signatures. Probably the most that might reasonably be done is to treat the signature as a rebuttable presumption of ownership, following the electronic signature

[12] https://www.hyperledger.org/projects/fabric

directive [ESD99]. However that had such adverse effects on liability that qualified electronic signatures found only very limited use. Here, we merely flag up such issues as needing clarification, perhaps in the central bank study project we recommend in the section above.

In any case, our **fifth recommendation** is that regulators compel exchanges to make clear in their contracts with their customers whether they are custodians of cryptocurrency assets that the customers own, or whether the assets are owned by the exchange with the customers simply having a claim on the asset pool.

It is natural for exchanges to try to avoid stating publicly whether they are trustees, banks or both, as either choice brings responsibilities. It is time for regulators to force them to choose.

6.5 Dark market currencies

A further policy issue is how to deal with cryptocurrencies that are explicitly designed to provide more substantial transaction anonymity or even unlinkability, such as Zcash and Monero, and also to identifiable persons promoting anonymity services on bitcoin and other public and address-identifiable blockchains. In the case of Zcash, the system works like bitcoin except that coin holders can have their coins re-mined, so that they become indistinguishable from other recently mined coins. The analysis in this paper would suggest that when a tainted coin is treated in this way, all the coins then mined become tainted, and the victim would have a cause for action against any of their holders.

Perhaps the victim could also sue the operators or promoters of such a system for negligence – in that they knew that some wallets would be stolen and yet designed a system that would make it impossible to get the money back. It's not obvious that this right would be extinguished by a legal precedent that declared ordinary, traceable, bitcoin to be money. A related policy issue is what the law should consider to constitute behaviour 'in good faith'. We have argued here that bitcoin mixes are certainly bad faith, and the use of systems like Monero might be held to count as such.

However the new anti-money laundering regulations may settle the matter. As noted above, article 6 requires that 'Member States shall prohibit their credit institutions and financial institutions from keeping anonymous accounts, anonymous passbooks or anonymous safe-deposit boxes'. A sensible transposition of the directive would discountenance anonymous instruments.

Our **sixth recommendation** is therefore that regulators should prohibit exchanges from buying and selling cryptocurrencies that are explicitly designed to evade money-laundering and terrorist financing controls. Perhaps anonymity should be restricted to cryptocoins issued by central banks, so that controls can be ramped up later if the need arises. We note that Coinbase won't touch Zcash or Monero, and that Coincheck has just joined them [Fun18]. But although the market might separate the sheep from the goats eventually, it might take its time.

6.6 Capital requirements

If the only thing that could go wrong with a bitcoin was that it had been stolen, and all thefts were promptly and dependably reported, then a technically competent

exchange can write scripts to fragment all incoming coins into clean layers and stolen layers. The payer could get value for the clean money, while the victims of theft get their money back and the drug money can go into the local asset-forfeiture pot. We call this *satoshi sorting*.

Satoshi sorting is not always a practical solution, though, for at least three reasons. First, there are issues other than theft, such as whether drug money or flight capital is to considered tainted – and some of these questions vary by jurisdiction. Second, crimes are not always discovered and reported immediately; a big drug bust may result in the tainting of coins in transactions from months or even years ago. Third is the complexity of evidence. A victim of bitcoin theft may take time to establish that fact and a theft report might only get to the taint chain after years of litigation.

Thus valid claims against an exchange's cryptocurrency assets can arise for months to years after these assets are received. This risk cannot be managed by a clearing period and it follows that, if exchanges are responsible under the E-money Directive, or equivalently under securities law, for ensuring that the bitcoin balances they sell to their customers are backed by cryptocurrency assets that are sufficient in quantity and quality, then they will have to keep a significant level of reserves.

In order to set appropriate standards for reserves, proper accounting standards are also needed. We noted that Coinbase – a leading exchange, which tries to be one of the good guys – has published accounts that do not reflect the assets under its control. In an ideal world, if Coinbase operates like a bank, we'd like to see its balance sheet look like a bank's balance sheet, and we'd like to have international standards for capitalisation and reserves compatible with Basel III.

Yet according to the UK Financial Reporting Council, the accounting standards needed for exchanges are just not there. Cryptocurrencies should be probably valued at market as financial assets, but they don't meet the definition; so they have to be valued at cost, unless we change the rules to treat them like gold; but this isn't even on the agenda of the International Accounting Standards Board [Geo18].

Our **seventh recommendation** is therefore that regulators should require regulated exchanges to be adequately capitalised – and develop proper accounting standards to support this.

6.7 Mitigating environmental harm

Our final policy issue is serious and controversial: the 'environmental disaster', as the Bank for International Settlements describes bitcoin mining. A recent detailed analysis by De Vries puts cryptocurrency mining energy use at between 3 and 8 GW, that is, between Ireland and Austria; he notes that the current economics will drive usage towards the latter figure [dV18]. Given the role of CO_2 in anthropogenic climate change and the relevant international agreements including the Paris treaty, regulators should seek to mitigate the environmental damage done by miners, for example by moving from proof-of-work systems to Byzantine fault tolerance or to proof-of-X for various values of X. Asking bank regulators to make technology choices might not be ideal, so perhaps the appropriate policy instrument here would be a carbon tax on mined coins.

Various policy mechanisms might be used to get from here to there including issuing central-bank cryptocurrencies or monetising existing crytocurrencies, but

only where regulated entities such as exchanges, miners and wallet hosting firms support adequate consumer protection mechanisms and pay their carbon taxes. The market could then decide whether to moving to proof-of-stake coins, or even (if they're properly capitalised) of letting the exchanges run a ledger directly.

Our **eighth recommendation** is therefore that regulators decide how to levy a carbon tax on cryptocurrency mined using proof-of-work methods, and that the very minimum acceptable should be the Eur 33 per tonne floor of the Emissions Trading Scheme.

7 Conclusions

In this paper we analysed the treatment of stolen bitcoins from legal, economic and engineering perspectives. Technologists claimed that taint tracking was hard, as they assumed that taint would mix and dilute when coins are joined; yet the relevant case law specifies first-in-first-out tracking, which turns out to be technically easy. Technologists also assumed that bitcoin mixing made coins derived from innocent and stolen inputs innocuous, whereas the legal effect of attempts to conceal the source of funds is to taint the entire output.

We discussed in section 2 the measures taken by many governments to tackle the most urgent serious-crime threats including large-scale money laundering and underground drug markets, notably by forcing exchanges to register and perform basic due diligence on their customers. These have culminated in the EU's amending the fourth anti-money-laundering directive to bring wallet hosting service providers as well, with effect from November 2018. However, this still only tackles the problems of two years ago.

We discussed in section 3 how to make it practical to trace stolen coins on the blockchain, at least in the theoretical world described in academic research. The same applies to coins acquired via other crimes from ransomware to drug trafficking. A public blacklist, run by Interpol, had already been proposed by Böhme and others; as such institutions may take years to establish, we have constructed a public taintchain for bitcoin, as a platform on which others may build. Our taint-tracking software is being made available via the Princeton toolkit Blocksci.

In section 4 we explored the limitations on the use of taint-tracking in practice, at least by individual crime victims, and went on to describe how many bitcoin exchanges have started working since early 2017, with many off-blockchain transactions and the ownership of the underlying bitcoins often obscure, at least in the case of the hosted wallets now used for most transactions. In section 5 we described how regulation has failed to keep up. While regulators have tackled the access and egress points where real money is transferred into digital currency and vice versa, they have failed to notice that the growing volume of off-blockchain transactions has created an unlicensed shadow banking system. This will have to be regulated, just as the real banking system is, and for precisely the same reasons.

In the absence of effective regulation, the cryptocurrency bubble is somewhat like a teenage party that's got a bit rowdy, and it's time for the grown-ups to take the punch bowl away. As a guide for future regulatory efforts, we make eight recommendations in section 6, which we gather together here for convenience.

1. The E-Money Directive must apply to exchanges doing business with EU citizens which offer off-blockchain payments or consolidate cryptocurrency assets rather than merely holding crypto keys on behalf of customers, in respect of all these payments and assets.

2. The relationship between an exchange and its customer should be covered by the second Payment Services Directive.

3. Governments should prohibit the cryptocurrency exchanges they regulate from clearing and settling transactions with unregulated exchanges.

4. Central banks should consider issuing a cryptocurrency that supports smart contracts, has the legal status of a bill of exchange and is redeemable at par for fiat money.

5. Regulators should compel exchanges to make clear in their terms and conditions whether they are custodians of cryptocurrency assets that the customers own, or whether the assets are owned by the exchange with the customers simply having a claim on the asset pool.

6. Regulators should prohibit exchanges from buying and selling cryptocurrencies that are explicitly designed to evade money-laundering and terrorist financing controls.

7. Regulators should require regulated exchanges to be adequately capitalised, and develop proper accounting standards to support this.

8. Regulators should decide how to levy a carbon tax on cryptocurrency mined using proof-of-work methods; the minimum acceptable should be the Eur 33 per tonne floor of the Emissions Trading Scheme.

We believe that existing laws can be used to tame the cryptocurrency jungle and make it safer both for private users and for innovation. The most important next step will be enforcing the EU's E-Money Directive in respect of digital currency assets held by EU exchanges on their customers' behalf, as well as for balances of Euros and other fiat money.

In the longer term, settling the legal status of digital currencies should be used as an opportunity to move operators from the proof-of-work systems that now emit more CO_2 than Ireland, to alternative systems that do not do as much environmental damage, by means of a carbon tax.

An interesting question is whether this would need new legislation, or even a trade treaty (as might be needed, for example, to impose a tax on the embedded carbon content of imported manufactures). If existing regulations can be used to used to implement our other seven recommendations, perhaps they can be used to enforce a carbon tax as well, by making it a condition of cryptocurrencies being traded on regulated exchanges.

Anyway, we set out these recommendations as a basis for discussion.

Acknowledgements

We are grateful to David Fox, Richard Clayton, Alexander Vetterl, Johann Bezuidenhoudt, Joe Bonneau, Shehar Bano, Nicolas Christin, Tyler Moore, Lawrence Esswood, Sergio Pastrana and Emma Rengers for helpful comments.

References

[AL17] Martin Arnold and Leo Lewis. Japan's big banks plan digital currency launch. *Financial Times*, September 26 2017.

[And16] Ross Anderson. GCHQ helps banks dump fraud losses on customers, 2016.

[And18a] Ross Anderson. Stolen Bitcoin Tracing https://www.youtube.com/watch?v=UlLNOQERWBs, 2018.

[And18b] Ross Anderson. Failures of trust and regulation in cryptocurrency, Apr 30 2018.

[ASA18] Ross Anderson, Ilia Shumailov, and Mansoor Ahmed. Making Bitcoin Legal. *Security Protocols Workshop*, 2018.

[Aut17a] BaFin Federal Financial Supervisory Authority. necoin ltd, dubai: Prohibition of involvement in unauthorised money remittance business, 18 Apr 2017.

[Aut17b] BaFin Federal Financial Supervisory Authority. Onecoin ltd (dubai), onelife network ltd (belize) und one network services ltd (sofia/bulgaria): Bafin issues cease and desist orders holding the companies to stop own funds trading in "onecoins" in germany, 20 Apr 2017.

[Aut18a] BaFin Federal Financial Supervisory Authority. Virtual Currencies (vc), 2018.

[Aut18b] BaFin Federal Financial Supervisory Authority. Crypto.exchange gmbh: Bafin orders cessation of unauthorized principal broking services, 5 Feb 2018.

[BC18] Marco Bellezza and Eleonora Curreli. Italy: Towards a register for cryptocurrencies operators. *Medici*, 13 Feb 2018.

[BCEM15] Rainer Boehme, Nicolas Christin, Benjamin Edelman, and Tyler Moore. Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives v 29 issue 2*, July 2015.

[BGP+17] Rainer Boehme, Johanna Grzywotz, Paulina Pesch, Christian Rueckert, and Christoph Safferling. Prevaention von Straftaten mit Bitcoins und Alt-Coins, 2017.

[Bit18] Bitfury. Use case – Crystal tracking ransomware payments. *at https://crystalblockchain.com/files/Crystal-Use-Cases-Ransomware.pdf*, 2018.

[BLM17] V. Bhaskar, Robin Linacre, and Stephen Machin. The economic functioning of online drugs markets. *CEP Discussion Paper 1490, LSE*, Aug 2017.

[Car18] Augustin Carstens. Money in the digital age: what role for central banks? *Bank for International Settlements*, 6 Feb 2018.

[CG17] Rebecca Camber and Chris Greenwood. Drug dealers using bitcoin cashpoints to launder money. *Daily Mail*, 4 December 2017.

[Coi18] Coinbase. Coinbase user agreement, 2018.

[Cry18] Cryptovoices. 24h trading volume Per On-Chain Payment, 2018.

[Dem18] Tuur Demeester. Bitcoin: digital gold or digital cash? Both., 10 Mar 2018.

[dV18] Alex de Vries. Bitcoin's growing energy problem. *Joule v 2 no 5 p801–805*, 16 May 2018.

[Eco17] The Economist. Why marijuana retailers can't use banks, 2017.

[Eco18] How a few companies are bitcoining it. *The Economist*, May 19 2018.

[EMD99] Directive 2009/110/ec of the european parliament and of the council of 16 september 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending directives 2005/60/ec and 2006/48/ec and repealing directive 2000/46/ec, 16 September 1999.

[ESD99] Directive 1999/13/ec of the European Parliament and the Council, 13 December 1999.

[Eur17] Europol. Drugs and the Darknet – Perspectives for Enforcement, 2017.

[FCA18] FCA. Financial conduct authority's written submission on digital currencies, April 2018.

[Fox08] David Fox. *Property Rights in Money*. Oxford, 2008.

[Fox16] David Fox. Cyber-currencies in private law. *University of Edinburgh*, 2016.

[Fre18] Freshfields. Virtual currencies: how regulators treat it (snapshot, january 2018), 2018.

[Fun18] Brian Fung. Move deliberately, fix things: How Coinbase is building a cryptocurrency empire. *Washingoton Post*, May 17 2018.

[Geo18] Paul George. Frc submission to the treasury select committee digital currencies inquiry, April 13 2018.

[GH14] Neil Gandal and Hanna Halaburda. Competition in the cryptocurrency market. *CEPR Discussion Paper No. DP10157*, 2014.

[GHL17] Russell Golman, David Hagmann, and George Loewenstein. Information avoidance. *Journal of Economic Literature, 55 (1): 96-135*, 2017.

[GKCC14] Arthur Gervais, Ghassan Karame, Srdjan Capkun, and Vedran Capkun. *Is Bitcoin a Decentralized Currency? IEEE Security and Privacy Magazine v 12 no 3*, 2014.

[Gla18] Phil Glazer. State of Global Cryptocurrency Regulation. *Hackernoon*, 21 Jan 2018.

[Gox12] Mt. Gox. Terms of use, https://web.archive.org/web/20130906174719/https://www.mtgox.com/terms_of_service?Locale=en_US, January 20, 2012.

[Gra18] Blockchain Graveyard, 2018.

[Han18] Andreas Hanl. Some Insights into the Development of Cryptocurrencies. *MAGKS Joint Discussion Series in Economics No. 04-2018, Marbueg*, 2018.

[Har17] Peter Hardy. Failure to register with FinCEN sustains guilty pleas by virtual currency exchangers. *Money Laundering Watch*, 2017.

[Her17] Alex Hern. Bitcoin mining consumes more electricity a year than ireland. *The Guardian*, 27 Nov 2017.

[Jou17] Věra Jourovà. Answer given by Ms Jourovà on behalf of the Commission. *European Parliament*, 3 Nov 2017.

[Lov14] Dylan Love. $500 million worth of bitcoin has been stolen since 2010. *Bitcoin Insider*, 11 March 2014.

[MBB13] Malte Möser, Rainer Böhme, and Dominic Breuker. An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem. *IEEE*, eCrime 2013.

[MBB14] Malte Möser, Rainer Böhme, and Dominic Breuker. Towards Risk Scoring of Bitcoin Transactions. *Financial Cryptography*, 2014.

[MC13] Tyler Moore and Nicolas Christin. Beware the middleman: Empirical analysis of bitcoin-exchange risk. *Financial Cryptography*, February 2013.

[MCS17] Tyler Moore, Nicolas Christin, and Janos Szurdi. Revisiting the the Risk of Bitcoin Currency Exchange Closure. *ACM Transactions on Information Technology*, 2017.

[Mey18] David Meyer. South Korea reportedly plans to hit bitcoin exchanges with massive tax bills. *Fortune*, 22 January 2018.

[MPJ+13] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey Voelcker, and Stefan Savage. A fistful of bitcoins: Characterising payments among men with no names. *IMC 2013*, 2013.

[NBF+16] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies*. Princeton, 2016.

[Par18] Helen Partz. Hacked Crypto Exchange coincheck Confirms Removal of Four Anonymity-Focused Altcoins. *Cointelegraph*, May 20 2018.

[Pop18] Nathaniel Popper. Bitcoin Thieves Threaten Real Violence for Virtual Currencies. *New York Times*, 18 February 2018.

[PSD00] Directive 2000/31/ec of the European Parliament and the Council, 8 June 2000.

[Ras17] Max Raskin. The Law and Legality of Smart Contracts. *I Geo L Tech Review*, 2017.

[Rev17] Nikkei Asian Review. Japan tries light touch in bringing cryptocurrencies out of regulatory limbo. 30 September 2017.

[Rib18] Sylvain Ribes. Chasing fake volume: a crypto-plague, 15 Jan 2018.

[RS13] Dorit Ron and Adi Shamir. How did Dread Pirate Roberts acquire and protect his bitcoin wealth? *IACR preprint 2013/782*, Financial Cryptography 2013.

[SC15] K. Soska and N. Christin. Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. In *Proceedings of the 23rd USENIX Security Symposium (USENIX Security'14)*, pages 33–48, 2015.

[Sch18] Mathew Schwartz. Criminals hide 'billions' in cryptocurrency, europol warns. *Bank Info Security*, 15 Feb 2018.

[She18] Lucinda Shen. Hackers have stolen $400 million from icos. *Fortune*, 22 Jan 2018.

[Sti17] Kai Stinchcombe. Ten years in, nobody has come up with a use for blockchain, 22 December 2017.

[Uni18] European Union. Pe cons 72/17: Directive of the european parliament and the council amending directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending directives 2009/138/ec and 2013/36/eu, May 12 2018.

[vC80] Judd v Citibank. 107 misc.2d 526, 1980.

[vHMtQ03] Wannan v Her Majesty the Queen. Ottawa, 2003 fca 423, 2003.

[VM15a] Marie Vasek and Tyler Moore. Analyzing the Bitcoin Ponzi Scheme Ecosystem. *Financial Cryptography*, 2015.

[VM15b] Marie Vasek and Tyler Moore. There's no free lunch, even using bitcoin: Tracking the popularity and profits of virtual currency scams. *Financial Cryptography*, 2015.

[vN16] Devaynes v Noble. 35 er 767, 781, 1816.

[Vor18] David Vorick. The State of Cryptocurrency Mining, May 13 2018.