Making Bitcoin Legal

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

When you come to a fork in the road, take it – *Yogi Berra*

Abstract

What would happen if the existing laws were actually enforced on the rich and powerful? Social reformers often clamour for new rules but ignore the huge changes that might happen if our existing rules were applied equally to all. And in the brave new world of ICOs and thousand percent cryptocurrency inflation, the rich and powerful are the bitcoin exchanges. What would happen if FinCEN regulations and the laws against money laundering were applied to them, and extended by sensible case law? We argue that this could mitigate most of the worst excesses of cryptocurrency world, and turn a dangerous system into a much safer one. The curious thing about this change is that it would not involve changing the protocol. It would not even necessarily involve changing the law. It might be enough to take some information that's already public, publishing it again in a more easily understood format.

1 Introduction

Bitcoin set out to provide a working online currency outside the control of governments, and has developed from a cypherpunk toy through a way to buy drugs online to a means of getting flight capital out of countries with exchange controls – to an investment product quoted on major exchanges. It has been criticised for wasting a lot of electricity, for being a classic investment bubble, for providing no consumer protection to its users, and for facilitating crimes – from old crimes such as drug dealing, to new ones such as ransomware.

The purpose of this paper is twofold. First, we discuss how the law might actually regulate bitcoin and other cryptocurrencies so as to provide the benefits, ranging from low-cost international money transfers and decentralised resilient operation to competitive innovation, while mitigating the harms – specifically the use of cryptocurrencies in extortion, money laundering and other crimes, and the difficulty that crime victims experience in getting redress. We show that where the relevant case law is used as a basis, it becomes much easier to track stolen bitcoins than previously thought.

Second, we use this discussion to illustrate that the characteristics of a payment protocol can depend much more sensitively than one might expect on the surrounding context. This may be of scientific interest to the protocols community, and also of practical interest to regulators. Payment systems suffer from strong network effects and it may be harder than it seems to sustain a government-backed 'GoodCoin' in competition with established systems such as Bitcoin and Ethereum. It is therefore important to explore the practical options for taming the systems that already exist.

On the policy front, we have repeatedly seen a pattern whereby the promoter of an online platform claims that old laws will not apply. The Internet was supposed to interpret censorship and route around it; yet child sex abuse images are banned almost everywhere. Napster set out to free all music from the surly bonds of copyright; it was closed down. Uber was going to create a single taxi firm that worked worldwide from a convenient app, regardless of local legacy monopolies; yet when legacy taxi drivers complained about their new competitors working sixteen hours a day, and passenger safety issues piled up, Uber was banned in one city after another. Yet such innovations often make a real difference once a new legal equilibrium is achieved. The music-company mafias have yielded to Spotify and YouTube, which make most music available to anyone who'll listen to occasional ads; competition from Uber has cut Cambridge taxi fares by over 20%; and the Internet has made many more good things available to all.

The key is making online challengers obey the law – and the laws may not need to change much, or even at all. Fixing new problems using existing laws is usually preferable, given the difficulty of getting primary legislation passed.

So where does this leave Bitcoin?

In this paper we assume the reader is familiar with the mechanics of Bitcoin and of blockchains in general. A later paper will present more detail for readers interested in law or policy.

2 Ideal Regulation

The obvious first step towards regulation was to bring bitcoin exchanges within the financial system by applying anti-money-laundering (AML) regulations to them. Thus anyone wishing to exchange bitcoin for cash, or for ether or any other means of payment, has to satisfy know-your-customer (KYC) rules just as if they were opening a bank account, typically by showing government-issue photo ID plus two utility bills as proof of address. This started in 2013, when the Financial Crimes Enforcmeent Network (FinCEN) directed bitcoin exchanges to register as money service businesses [3]. Most countries have now followed suit, partitioning the world of exchanges into compliant and rogue components.

The second step would be for both enforcement agencies and exchanges to have effective means of tracking tainted coins. If my bitcoin wallet is stolen I can now go to the police and report it. The stolen assets are completely traceable through the blockchain and whenever anybody tries to bank them at an exchange, they can be seized. How might the courts actually do that?

2.1 Clayton's case

Until now, there were two algorithms used for taint tracking in the blockchain – poison and haircut [12]. These taint multisource transactions, of which one input is tainted, either completely, or in proportion. Thus a transaction whose inputs are three stolen bitcoin and then seven good bitcoin has an output on 'poison' of ten stolen bitcoin, and on 'haircut' of ten bitcoin each of which is marked as 30% stolen.

However, this ignores the precedent of Clayton's case, where a court in 1816 had to tackle the problem of mixing good and bad funds through an account after a bank went bust and the outcome depended on which deposits to an account were to be matched with which later withdrawals. The Master of the Rolls set 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 [16].

In order to test this rule, we coded FIFO and haircut taint tracking, and ran them from the genesis block to 2016, starting from 132 well-publicised bitcoin crimes. FIFO turns out to be very much more precise. The 2012 theft of 46,653 bitcoin from Linode tainted 2,694,051 addresses, or almost 5% of the total, using the haircut algorithm, while with FIFO, it's 371,544 or just over 0.67%. The effect is even more pronounced with a shorter propagation

period; for example, the 2014 Flexcoin hack (where 'the world's first bitcoin bank' closed after all their coins were stolen) tainted only 18,208 accounts by 2016 using FIFO, but 1,429,794 using haircut. Overall, most bitcoin accounts[1] have zero taint using FIFO, while less than 24% escape taint if we use a haircut approach.

This is a very striking result. Many people assumed that bitcoin tracking was usually impractical, because the taint spreads widely as coins circulate. However once we apply the law and use FIFO, tracking turns out to be much more practical. And FIFO tracking is reversible; you can track forwards from a coin that's been reported stolen, or backwards from a coin you've just been offered. This isn't possible with haircut tainting, as it loses information.

We also looked at bitcoin laundries or mixes. These are based on the idea that if you put one black coin in a bag with nine white ones and shake hard enough, you'll get ten white ones out. But depending on the algorithm in use, FIFO tainting will decide that one of the outputs is black (and no owner of a white coin will want to risk that outcome), or that all coins are a sandwich of black and white components (which is also an undesirable outcome). In any case, mixes have never had the scale, throughput or latency to cope with the proceeds of serious crime; the bitcoin stolen from Mt Gox were traced to BTC-e which was raided and its operator arrested [8].

There is an interesting piece of research to be done here on protocols, documenting the precise effects of FIFO tainting on the various mixing and money-laundering strategies proposed to date, or documented in the wild [11, 13, 14]. People who have been doing research on financial anonymity without paying attention to Clayton's case have simply been using the wrong metric.

Efficient coin tracing may damage the fungibility of bitcoin. A commodity is called fungible if one unit can replace another; examples are gold coins, and ears of corn. Technology has in the past reduced fungibility. If ten sheep wandered in Roman times from Marcus's field into Pliny's, then the court would let Marcus take any ten of Pliny's sheep; but today, all sheep have electronic tags, so Marcus can get the right sheep back. So too with bitcoin.

2.2 Nemo Dat Quod Non Habet

'Nobody can give what isn't theirs' is a fundamental principle of law in England, with variants in many other jurisdictions. You cannot get effective

[1] slightly over 72% of all bitcoin accounts with a nonzero balance

title to stolen goods simply by buying them; indeed, you can be prosecuted for receiving them. If Alice steals Bob's horse and sells it to Charlie, Charlie doesn't own it; whenever Bob seems him riding it, he can demand it back.

There are a few exceptions. For centuries, if stolen goods were sold at a 'market overt' – a designated public market – between sunrise and sunset, then the buyer would get good title. (So if Charlie had bought Bob's horse in Cambridge market, all Bob could now do would be to sue her for the value, or perhaps have her transported to the colonies.) This rule was abolished in the UK in 1995, following abuse by antique thieves, but it survives in specific forms in some markets to which the idea had spread in the meantime. The relevant case for our purposes is money.

Where goods started to function as money – as with gold – regulation developed to accommodate it. Banks started in some countries as goldsmiths who would give receipts for gold, and on demand would give an appropriate amount of gold back, though not necessarily the same bars. So a gold thief might lodge his loot at a goldsmith, and take the receipt back a week later to get clean bars instead[2].

Fast forward through a lot of history, and you can now get good title to stolen money in two main cases.

1. You got the money in good faith for value. For example, you bought a microwave oven at a high street store and got a £10 note in your change. That note is now yours even if it was stolen in a bank robbery last year.

2. You got the money from a regulated institution, such as from an ATM. Then even if it was stolen in a robbery last year, that's now the bank's problem, not yours.

It is not surprising that the cryptocurrency industry would very much like to have bitcoins declared to be money, as this would enable everyday users to stop worrying about the possibility that some of their bitcoin were stolen. And this is a real fear; the major reported robberies alone account for about 6–9% of all bitcoin in circulation [10]. If we add the proceeds

[2]Monetary law over the centuries has had the same ambivalent attitude about whether money consists of the physical goods that used to embody it, such as coins or notes, or the value they embody – just as bitcoin promoters claim that cryptocurrencies are money or goods depending on which will best help them escape regulation

of crime more generally we will get a much larger figure but will encounter many complexities of definition, jurisdiction and so on. The proceeds of drug crimes, in particular, are exposed to quite draconian seizure laws in a number of countries.

However nothing in life is free, and being a regulated financial institution has significant costs of its own: capital adequacy requirements, criminal-records background checks for staff, and (most important for our purposes) 'know your customer' (KYC) rules feeding into anti-money-laundering (AML) surveillance systems. Large transactions are reported, as are patterns of smaller ones, and banks demand your passport and a couple of utility bills when you open an account.

Since 2013, the US Treasury Department's Financial Crimes Enforcement Network (FinCEN) has directed bitcoin exchanges to register and follow these rules; other countries have been following suit. Since 2017, several non-compliant exchanges have been prosecuted [6]. The latest development is that the EU proposes to amend the 4th Anti-Money Laundering Directive so as to extend regulation, including a KYC duty, to firms that operate hosted wallet services. That may eventually bring most bitcoin users under the umbrella. The question then will be how the regulators will discharge the responsibility they have now assumed. Might they do something to reassure ordinary investors that they won't lose money as a result of buying stolen bitcoin? Of course they could demand that registered exchanges make good any customers to whom they sell bitcoin that later turn out to be stolen, but is there anything else?

2.3 Registering or even insuring title

One way of insuring title would be for the state to register ownership, as it does in many countries with real estate, motor vehicles and patents. But there are subtleties here about whether or not the register is constitutive of ownership, as with patents, or not, as with cars; and whether it provides a guarantee, as with property.

But given the scale of bitcoin thefts and robberies, and the anonymity preferences of bitcoin users, state guarantees are unlikely to be an attractive option for many stakeholders. A government-controlled blockchain would give neither the platform for innovation that cryptocurrencies do, nor the price, performance and market responsiveness of ordinary bank accounts.

2.4 Might the courts do the job?

So far, no government has declared bitcoin to be money, although Japan and Italy have tiptoed around the edges of this. However, courts may find that bitcoin can be treated as money for some purposes. A relevant precedent established that carbon credits are property, and they possess many of the same characteristics as bitcoins [5].

Monetary status might be thought ideal for investors who hold cryptocurrencies in the hope of capital gains. At present, the investor can only check that her asset has not yet been reported as crime proceeds – but most crime reports don't come with public lists of affected addresses. If bitcoin were money, and she got her bitcoin directly from a regulated exchange, she would have good title.

If someone hacks your Bitcoin wallet, or uses ransomware to extort bitcoin from you, or holds you up at gunpoint and forces you to transfer your savings to them – a crime that's become extremely fashionable of late [15] – then the stolen bitcoin can be traced. Now that coin tracing is practical, the victim can trace the stolen bitcoin through the blockchain, and sue the current holder – or any regulated exchange through which it passed.

So honest customers would like the exchanges' addresses to be public, so that anyone tracing stolen funds could see that a coin went through a regulated exchange before they bought it. The exchanges will resist, not wanting to make it easier for theft victims to sue them. Bitcoin enthusiasts might well side with the exchanges, on the principle that bitcoin public keys are pseudonyms. But it's increasingly the investors who're floating the boat.

3 Changing the Rules of the Game

This pressure point may give an opportunity to change the rules of the game. Fox notes "Information about the tainted provenance of individual cybercoins may be discoverable by specialised forensic techniques. But there is as yet no standard practice of applying them to routine payments" [4, 5]. We have shown that coin provenance can be tracked very much more easily than people assumed. The economic pressure point sits on a technical fissure, between the technical community's insistence that the only concept of ownership of bitcoin is control of the private key for the wallet in which it's stored [1] versus the lawyers' insistence that the registration of a bitcoin on

the blockchain is not 'constitutive of ownership' as is the case with registered property rights such as patents.

Cryptocurrency promoters and investors will continue to lobby for a law making bitcoin fungible, arguing that governments make money from selling bitcoin confiscated as the proceeds of crime [7] – even if in the past they have ineptly sold bitcoin at way below market value [2]. They will also point out that when the government of Korea tried to crack down on cryptocurrencies, it suffered a public backlash [9].

But even if bitcoin becomes money, the law and the blockchain will still diverge when you buy a bitcoin knowing it to be stolen – or being on notice that it might be, or being negligent that it might be.

For bitcoin to work as some of its promoters wish, governments would have to go further than declaring it to be money. They would have to declare the blockchain to be constitutive of ownership. This would be an extreme measure, and seems unlikely, given that even registers of motor vehicles don't have such a status. The register simply records where speeding fines and unpaid tolls should be sent; it does not establish ownership. If we want to make ownership of bitcoin more certain, we need a different approach.

4 Taintchain: a Public Trail of Breadcrumbs

As Fox noted, tainted provenance can be discovered using forensics, yet applying these to routine payments is not standard practice.

Our critical new assumption is this. Suppose there exists free and open-source software that makes an up-to-date taint analysis publicly available. This will follow the blockchain forward from all reported crimes, and also from crimes whose existence can be reliably deduced from the internal evidence of the blockchain, and will mark every bitcoin in existence with a taint. Either the coin is clean, or some part of it was stolen. In that case, the taint will document the chain of evidence back to the crime and quantify it under certain assumptions (which we discuss later). We call this public trace the *Taintchain*, and propose to make our FIFO tracing software public so that anyone can build one.

There may well be multiple versions. For example, if a Chinese national uses bitcoin to extract money from China in contravention of its exchange control laws, that will not be a crime in the UK which has no exchange controls. Similarly, if a software company in Estonia pays a developer in

Ukraine in bitcoin so she can evade both exchange controls and tax, the authorities in Tallinn may well not be interested. Different legislatures take different views of right and wrong; different taintchains are the inevitable result. The machinery of international law – MLATs, dual-criminality checks for extradition warrants, evidence rules – may eventually find its expression in protocols and in chain analysis code.

Let us ignore issues of jurisdiction for the time being, and consider two possible ways forward. First, what might happen under optimal but light-touch regulation? And second, might private law get us there instead – in other words, if the victims of bitcoin crime were to sue to get their assets back, then might decisions in the courts get us to roughly the same place?

4.1 Protocol research problems

Suppose the government simply declares that people who purchase bitcoin in good faith from regulated exchanges following established AML and KYC rules will get good title, and that the exchanges must refund theft victims.

Thus when someone pays in a bitcoin amount, of which (say) 8.4% has been reported stolen, the exchange will seize that portion of the deposited amount and apply due process to return either the actual coins or their value to the rightful owners.

There are many technical protocol aspects to explore. Can we support protocols that will let an exchange customer check whether a bitcoin payment will be accepted, or whether some of it will be confiscated as crime proceeds? If an identified customer says 'Hi, what will you give me for UTXO x?' and the exchange replies, 'Sorry, 22% of that was stolen in a robbery last Tuesday, so we'll only give you 78%' does the customer then have to turn over the crime proceeds? We'd presume so. (The exchange has her passport and utility bills on file, after all.)

If someone invented a protocol to check value in zero knowledge, they might be prosecuted for obstruction of justice. Even if not, the exchanges would be as leery of that as the credit card companies are at present of small transactions which might be used by thieves to check whether a card's been reported stolen yet. In fact, the difficulty of doing pre-purchase coin checking is a strong argument for a public taintchain.

Then there are issues familiar to the protocol community, of revocation and freshness. Suppose Alice checks a UTXO against the taintchain, sees that it's OK, and then transfers it to an exchange in good faith in order to

cash it for dollars. Meanwhile the victim of a bitcoin robbery reports some of it stolen, and by the time Alice's transaction is mined into the blockchain, it's tainted. Or perhaps the miners refuse to touch it as they don't want tainted mining fees. How do you sort out the mess? What combination of technical measures, social norms and legal rules might put us in a sweet spot? Presumably the exchanges will have to pick up some of the tab, as banks do at present, but what rules might work and what protocols might support them?

This is actually an old problem. Under the common-law statute of limitations, I can sue for negligence for up to seven years, and there is no limit in England for return of stolen goods. Under the old system for cheque clearing, I might be able to claw back funds for a few days to weeks. Under the EU Payment Services Directive, payments become irrevocable after 48 hours, and customer complaints must be made within 13 months. The disparity of rules indicates a role for the lawgiver in clarifying grace periods for cryptocurrencies. Clearly law enforcement will lobby for a long period while the exchanges will lobby for a short one.

Further rules need to be be explored. Where we can identify clearly conspiratorial behaviour, such as a mix, the whole of the output may be strongly considered tainted, at least in the case of bitcoin being money – where the requirement for good title is to transact 'in good faith'. Curiously, making cryptocurrencies into money would make anonymity harder, at least insofar as it's provided by detectable technical mechanisms. Cryptocurrencies such as Monero and Zcash might forever be incapable of being treated as money, because of their built-in laundromats. There, a default assumption of bad faith seems prudent.

4.2 So what might governments do?

Up till now, cryptocurrency promoters have campaigned for monetary status (often under the slogan of 'fungibility') while governments have largely dragged their heels, no doubt fearing that control would be completely lost, and that the tracing and recovery of crime proceeds would become even harder. We hope we've shown that it's not that simple.

One possible way forward would be the creation of a 'nemo dat exception' for regulated bitcoin exchanges, with a suitable notice period, and more detailed provisions for the extent to which crime victims might be made good beyond that. We propose that exchanges should also maintain a reserve

proportional to their trading activities, as banks do, so that they can continue to make victims good even when there are spikes of claims.

An alternative approach might be private-sector title insurance; once we have a good public taintchain, a bitcoin exchange or a bank might simply guarantee title to any bitcoin it sells, and publish its wallet addresses so that the tracking can stop and start there.

A useful starting point for negotiation between governments and exchange operators, or just for incremental policy development, might be the EU's second Payment Services Directive, which encapsulates Europe's experience to date in dealing with consumer-facing payment systems. Just as Uber was brought to heel by mayors saying 'We don't care if you claim to be a platform, whatever that is; you're a taxi company, and you'll get a license or we'll run you out of town', so a sound opening gambit would be to start enforcing the law as it stands.

For any of this to be feasible, a public taintchain may be the key. En route, there are many interesting protocol problems to tackle.

5 Conclusions

The bitcoin protocol is fascinating. It has created what appears to be a global trusted computer out of a mixture of cryptography and incentives, despite the facts that many of the actors are shady and many of the circulating cryptocoins have been stolen at least once.

Out of this swamp, the value of bitcoins has soared to peaks that few would have predicted two years ago. The demand is now largely for investment rather than transactions; so now may be the time to clean up bitcoin. How can we start?

Tracking stolen coins, so that crime victims can sue to get their property back, is the key. Up to now, people have been using haircut tainting to track stolen bitcoin. We've shown that's wrong, as a matter of both law and engineering. The law says you should use FIFO, and when you do so, the engineering works way better. It's much more precise, and is also reversible: in addition to tracing forward from a stolen bitcoin to see where it went, you can trace backwards from any UTXO and get its entire genealogy. In short, FIFO tracking is a powerful new analytic tool.

The way is now clear for financial regulators to apply the existing law on stolen property and on payment services to bitcoin exchanges.

The thought experiment in this paper illustrates a deeper fact. A protocol's security properties can depend in very subtle ways on context. There is some precedent for this; for example, the bug in shared-secret Needham-Schroeder became apparent once people started to consider insider threats.

The contextual change needed for bitcoin is really just a matter of clarity. The taint information is right there in the blockchain, and in the public theft reports; but combining the two so as to work out the taint on even one single UTXO has involved a key conceptual insight (FIFO) and some engineering effort. The output it a public taintchain that makes stolen coins visible to all. Then a test case, or regulation, might create a soft fork between good coins and bad. And as investment demand trumps transaction demand, good coins might drive out bad ones; and miners might also avoid bad ones as they won't want tainted transaction fees.

Honest users of bitcoin would then buy them from regulated exchanges, and pay them in again directly. Bitcoin would still support peer-to-peer payments, and would not in any engineering sense be 'centralised' or otherwise changed[3]. But most users would start to use bitcoin rather like they use other electronic money, which passes from the bank to the customer to the merchant and back to the bank.

In short, we might be able to turn a rather dangerous system into a much safer one – simply by taking some information that is already public (the blockchain) and publishing it in a more accessible format (the taintchain). Is that not remarkable?

Acknowledgements

We acknowledge helpful discussions with David Fox, Shehar Bano, Tyler Moore, Nicolas Christin, Rainer Böhme, Johann Bezuidenhoudt, Lawrence Esswood, Joe Bonneau and various attendees at Financial Cryptography 2018 where we presented some of the ideas here at a rump session talk.

References

[1] J. Bonneau, J. Clark, A. Narayanan, J. Kroll, and E. Felten. Sok: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. *IEEE S&P*

[3] the maintenance of the taintchain could and should be open, which in itself gives rise to interesting questions of governance, which will lead to protocol design questions too

2015, 2015.

[2] E. Cheng. US government misses out on $600 million payday by selling dirty bitcoins too early. *CNBC*, 3 Oct 2017.

[3] Financial Crimes Enforcement Network. *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies.* 2013.

[4] D. Fox. *Property Rights in Money.* Oxford, 2008.

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

[6] P. Hardy. Failure to register with fincen sustains guilty please by virtual currency exchangers. *Money Laundering Watch*, 24 April 2017.

[7] S. Higgins. US Marshals Service to Auction Off $54 Million in Bitcoin. *Coindesk*, 11 Jan 2018.

[8] S. Hudak. *FinCEN Fines BTC-e Virtual Currency Exchange $110 Million for Facilitating Ransomware, Dark Net Drug Sales.* 2017.

[9] C. Kim and H. Yang. Uproar over crackdown on cryptocurrencies divides South Korea. *Reuters*, 12 Jan 2018.

[10] T. Lee. A brief history of bitcoin hacks and frauds. *Ars Technica*, 12 May 2017.

[11] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. Voelcker, and S. Savage. A fistful of bitcoins: Characterising payments among men with no names. *IMC 2013*, 2013.

[12] M. Möser, R. Böhme, and D. Breuker. Towards Risk Scoring of Bitcoin Transactions. *Financial Cryptography*, 2014.

[13] M. Möser, R. Böhme, and D. Breuker. An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem. *IEEE*, eCrime 2013.

[14] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. *Bitcoin and Cryptocurrency Technologies.* Princeton, 2016.

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

[16] D. v Noble. 35 er 767, 781, 1816.