Cryptographic Currencies from a Tech-Policy Perspective: Policy Issues and Technical Directions

Emily McReynolds, Adam Lerner, Will Scott,
Franziska Roesner, and Tadayoshi Kohno

Tech Policy Lab and Computer Science & Engineering
University of Washington

Abstract. We study legal and policy issues surrounding crypto currencies, such as Bitcoin, and how those issues interact with technical design options. With an interdisciplinary team, we consider in depth a variety of issues surrounding law, policy, and crypto currencies — such as the physical location where a crypto currency's value exists for jurisdictional and other purposes, the regulation of anonymous or pseudonymous currencies, and challenges as virtual currency protocols and laws evolve. We reflect on how different technical directions may interact with the relevant laws and policies, raising key issues for both policy experts and technologists.

1 Introduction

Bitcoin [32] and other crypto currencies have recently become a key topic of research interest for the financial cryptography community and have seen significant adoption. The research community has considered numerous aspects of crypto currencies, including: the development of new crypto currencies with different properties (e.g., [8, 31]), the measurement of existing currency deployments [30], and the uncovering of vulnerabilities in currency protocols followed by the creation of defenses (e.g., [19]). In the applied world, we have seen numerous commercial efforts to mine bitcoins, serve as bitcoin exchanges, and provide financial tools based on bitcoins. Bitcoin has been featured regularly in the news, from the acceptance by well-known institutional investors to the scandals surrounding Mt. Gox and the Silk Road. Bitcoin has also gained a level of acceptance from traditional merchants, with leading organizations like Dell [16], Overstock.com [34], and Wikipedia [24] supporting the technology.

These incidents have given observers some insights into the legal standing of crypto currencies today, as well as the challenges to making them secure, robust, and widely-used. However, to the best of our knowledge, the public academic community has not stepped back and asked from a holistic perspective: what are the most important legal and policy issues surrounding Bitcoin and other crypto currencies, and how do those issues interact with technical design options? We seek to fill that gap here. Our team combines expertise in computer security, cryptography, and law to evaluate key issues surrounding crypto currencies. In doing so, we hope to inform present and future crypto currency designers about

key issues linking technology and policy. Given our legal background, we also write this paper with law and policy experts as an intended audience and hope that this paper can be used to inform future national and international policies.

In the following sections, we consider in depth a variety of issues surrounding law, policy, and crypto currencies — also commonly referred to by regulators as *virtual currencies* — including Bitcoin. We consider the legal requirements that exist around Bitcoin (§4), the location of where Bitcoin's value exists physically (§5.1), the regulation of anonymous or pseudonymous currencies (§5.2), and challenges as virtual currency protocols and laws evolve (§5.3).

This paper does not intend to deep dive into *all* of the technical and legal nuances related to virtual currencies, about which entire volumes could be written. Rather, we aim to expose key issues that have yet to be addressed and technical directions. In determining what were the key issues we looked to both existing policy work on Bitcoin (e.g., [9, 20, 10]), and the central questions arising in our own discussions (see §2). For tractability, our focus is also on the legal system of a single country (the United States), though we do refer to laws and policies in other countries when appropriate.

2 Our Process

We survey our research process here, to provide a context for interpreting our results. Our team is interdisciplinary, including members trained in computer security, cryptography, and the law. In parallel with significant literature reviews (including technical academic publications, as well as governmental legal and policy determinations), we initiated our research with numerous co-located meetings in which we brainstormed important areas of technology, policy, and law that relate directly or indirectly to crypto currencies.

We observed that most of our conversations centered around questions — questions from those with legal expertise about the properties of technology, and questions from those with technical expertise about aspects of the law and policy. Since these questions can represent knowledge gaps, we considered it valuable to capture these questions — and their answers — for the greater computer security and policy communities. We therefore chose to structure this paper around those questions. We then proceeded to iterate on the questions and answers, the final form appearing in §5. We realize that the resulting discussions are not exhaustive — there are countless other questions one might ask. However, we aim to cover questions of interest to both policy experts and technologists.

3 Background: Bitcoin and Crypto Currencies

Chaum's electronic cash. There is a long history of work in the cryptographic community on electronic currencies. In 1982, Chaum described an untraceable form of electronic cash [13], and in 1988 enhanced that design to prevent double-spending [12]. The premise of this system of cash was to prevent giving the same piece of electronic cash to two people ("double-spending") by holders of cash while also preserving the anonymity of those spenders. In Chaum's system, a central issuer (a "bank") participated in the protocol to issue cash and to confirm to participants that transactions were valid.

Bitcoin and relatives. More recently, Nakamoto proposed Bitcoin [32], an electronic cash system which does away with the need for a central bank. Unlike Chaum's electronic cash, Bitcoin is fully decentralized, with no bank acting as issuer. Instead, all transactions are completely public and can be verified by any participant. The Bitcoin protocol consists of peer-to-peer interactions between participants, which maintain a public ledger of every transaction, including both the issuing of new cash and all transfers of cash. This ledger is called the *block chain*, composed of *blocks* that include one or more transactions in a time period, where the mining reward (described below) is counted as a transaction. Not all participants in the Bitcoin network need to store the entire block chain in order to verify transactions. An individual using Bitcoin generates a public-private keypair which becomes their pseudonym in the network. A *wallet* may house one or more key pairs. Transactions in the network are identified only by these pseudonyms. Bitcoin does not directly link pseudonym to real-world identities, allowing its design to claim the possibility of some level of anonymity for its users. Yet while Bitcoin tries for anonymity, there is significant evidence that de-anonymization of its users via transactions is possible [30].

Bitcoin assumes that at least half of participants are honest, and thus that half of the computational power in the system is controlled by honest participants. Nakamoto describes this as *one-CPU-one-vote*. Adding a new transaction to the block chain ledger takes a large amount of computational work, which is performed by participants in the system known as *miners*, who must solve a computational puzzle based on a cryptographic hash before including a new transaction in the block chain. Participants only accept blocks in the chain for which the answer to the puzzle has been computed and included. As such, the length of the block chain is determined by the total amount of computational power possessed by miners in the system.

Block chain forks might exist, but the protocol is designed to recover from such forks. An attacker might spend coins and then attempt to create a new block chain which does not include those spending transactions. This is effectively a double-spending attack: the attacker spends the coin once, receives goods or services for it, and then performs an attack to form a new block chain in which the spending transaction is removed, effectively recovering the coin. To defend against fake block chain forks, participants consider the longest block chain in existence to be the correct one, and a transaction is considered recorded if a sufficient number of blocks follow it in the longest block chain. Since the protocol assumes that more than half of the computational power in the network is honest, and more computational power means a block chain will be longer, it follows that the block chain worked on by honest participants will be the longest. Attackers need to control more computational power than all other participants combined in order to create a malicious block chain that is trusted as the real ledger.

Physical electronic currency. Recall that bitcoins are stored in "wallets" consisting of public-private key pairs. The power to spend the coins in a wallet is held by anyone who possesses the enclosed private key. Thus, it is possible to create physical versions of Bitcoin by writing, printing, or engraving the private

key for a wallet onto a physical artifact like a banknote or a coin. The private key is often hidden in a tamper-resistant or tamper-evident manner (e.g., under a sticker), to allow the coin to transfer multiple times while providing assurance to the final recipient that the private key has not been stolen en route.

Note that a user might also make their own physical copies of their private key. For example, a person might store a key, printed on paper, in a safe. Additionally, a person might keep multiple digital copies of a private key on different storage media or devices for backup or easier usage.

Exchanges and real-world use. Bitcoin and several of its relatives, such as Dogecoin and Litecoin, have entered real-world use recently. Businesses with the role of converting electronic coins into accepted national currencies have sprung up and are known as *exchanges*, by analogy to ordinary currency exchanges. Exchanges (such as Coinbase) facilitate the buying and selling of real currencies for electronic currencies and vice-versa. These exchanges represent a significant level of centralization in the system, as many users wish to be able to convert between *real-world* currencies and different types of electronic cash.

Internally, exchanges typically operate by matching requests to transfer value between a pair of currencies. A percentage of matched volume is typically taken from one of two parties as revenue for the exchange. Most Bitcoin exchanges require that users transfer coins they wish to sell into a wallet controlled by the exchange. This lowers risk for prospective buyers, who now only need to trust the exchange and not also the user who previously owned the bitcoins they are buying. The risk is instead held by sellers who must trust the exchange to honor its obligations, and to protect their personal information needed for payments.

4 Analysis of Relevant Legal Contexts

The first step in any legal analysis of an emerging technology is to look to existing legal frameworks. Before examining the key tech-policy issues, in the this section we begin with an overview of existing legal frameworks and current legal status of virtual currencies. While our effort in this paper is focused on virtual currencies in general, because of Bitcoin's widespread examination and adoption, many of our examples rely on determinations specific to Bitcoin.

It is often said that technology moves faster than law, and while that can be true, laws and regulations should be designed when possible to be broad enough to cover future developments. There is currently some proposed Bitcoin-specific regulation, including in the U.S. (New York State) [33] and in France [29], but the danger is that the legislation will be out of date before it can even be fully implemented. Examining virtual currencies as a general category, as the U.S. and European Union (EU) have done, allows laws to be more adaptable.

In the U.S., the starting point for laws and regulations is the U.S. Constitution, which includes the authority for the U.S. Congress to "coin money" and "regulate the value thereof" [1]. The Constitution provides the U.S. Congress with the ability to pass laws, which may include the creation of federal agencies with the ability to create rules. Thus, while the U.S. currently has no specific

Bitcoin regulation, many federal agencies have interpreted existing regulations for their application to virtual currencies and thus Bitcoin (e.g., [22, 14, 27, 42]).

Legal status of Bitcoin and other virtual currencies. The legal status of Bitcoin and virtual currencies varies from country to country. Often Bitcoin's legality is related to a country's currency controls. In China, where there are strong currency controls, Bitcoin was specifically banned for financial and payment institutions; however, participating in the network and mining appears to be allowed [39]. Sometimes Bitcoin's use is limited due to a lack of understanding. In Thailand, for example, the Central Bank halted its use after an attempt by a Bitcoin exchange to present their business to banking authorities [7]. The Thai determination was made based on the lack of applicable laws.

Meanwhile, Bitcoin is (at time of writing) legal in other countries, including the U.S. and the EU, who are working to regulate virtual currencies (e.g., [22, 18, 27]. We mention specific U.S. regulations where they apply in later sections.

Thailand's ban may be lifted when the legislature clarifies Bitcoin's legal standing, but some Bitcoin enthusiasts believe that the myriad of rules the U.S. government is applying may actually be more detrimental to Bitcoin's future since, while an outright ban may be lifted, the layered regulations in the U.S. are complicated and make Bitcoin less easy to use [25]. With this legal background we turn to tech-policy issues for cryptographic currencies.

5 Tech-Policy Issues for Crypto Currencies

We now consider questions that span technology, policy, and the law. Through literature review and our discussions, we identified three areas under-addressed in previous work: understanding where the money resides; distinguishing anonymity versus pseudonymity; and issues that arise as the world evolves. These questions span multiple areas of law; our aim is not an exhaustive examination but to look at the current situation, both legal and technical, with a view towards technical mechanisms that will improve policy outcomes. We anchor much of our discussions in Bitcoin in particular due to its current popularity, but many of our analyses extend to other cryptographic or virtual currencies.

5.1 Where is the Money?

We found the following question arise in numerous forms: Where is the money located in Bitcoin or any similar crypto currency system? This question is relevant to understanding the laws applicable to interactions between virtual currencies and international border crossings, taxation, theft, and insurance.

From a technical perspective, it may be tempting to say that there is no physical manifestation of the money, and hence it does not exist in any one physical place at a given time. However, from a legal perspective, determining the location of the money is seen by governments and their regulators as the first step to concluding who has jurisdiction — who has the official power to make regulatory and policing decisions. Thus, though a technologist may argue that the money has no physical location, the law will likely decide that it does, and hence we explore a set of options below. Although we consider these different

possibilities for the location of virtual currencies and particularly Bitcoin, we stress that not all options are equal in terms of technical or legal viability.

Location of private keys. Because the private key gives access to the bitcoins for transactions, one might argue that the private key location could provide the basis for legal location. However, a private key is not a singular item: unlike a safe deposit box that exists in only one location, a private key can be stored on a hard drive, in the cloud, on a piece of paper, or even memorized so as not to be written anywhere. Further, a private key could be split into multiple components that are each stored at different locations or using different storage mechanisms.

Money is with the individual. In practice, an individual could access their bitcoins from anywhere, since all they need is their private key and Internet connectivity. In this situation, a determination that the bitcoins are where the individual is or is using their bitcoins could provide a workable foundation for application of laws. In U.S. criminal cases thus far — Silk Road/Ulbricht [5], Bitcoin Savings and Trust Ponzi Scheme [3], Faiella and Schrem [6] — the prosecution has evaluated jurisdiction based on the location of the individual and the exchange. From a technical perspective, we observe that a person might use a remote server to perform transactions, which means that their private keys may not be near them.

Location of the exchange. While some transactions go directly between individuals, others use exchanges. If an exchange is used for Bitcoin transactions, determining the location of the bitcoins may be an easier task for jurisdictional purposes. Exchanges might hold Bitcoins for you (like having an account at a bank), might facilitate buying and selling of Bitcoin (like a stock market), and even provide insurance. While exchanges began with very little regulation attached to them, currently government authorities in many countries are beginning to regulate them. In the U.S., exchanges must register as a money services business with the Department of the Treasury, requiring them to follow money transmitter laws in all of the U.S. states [22]. In 2013, Mt. Gox (prior to all of its other problems) and its U.S. subsidiary were pursued for failing to register as a money services business [4]. If bitcoins are stored in an exchange, like Coinbase or Bitinstant, because that business should be registered with a government somewhere, jurisdiction could be based on the location of the exchange.

The generation of bitcoins through the mining process is also centralized in practice in the form of *mining pools*. If the mining pool is registered as a business it would provide jurisdictional location similar to an exchange. In mining pools, users submit hashes to a centralized coordinator, who divvies earnings from the pool across all members based on work. Mining pools are typically distinct entities from exchanges, and so far have received less regulatory scrutiny, but we can expect that they could be subject to similar policies in how they pay out earnings to participants.

Money is stored in block chain. One might argue that the money is also stored in all locations in which the block chain is stored, even if not all parties storing the block chain can access the bitcoins. This brings up many of the same issues governments have had with regulating conduct on the Internet. The

U.S. authorities have used the Internet's ubiquitous nature to prosecute crimes federally, establishing jurisdiction with the location of the prosecutor [37]. While establishing that the money as stored in all locations the block chain is stored might seem outlandish technically, legally it could be an option.

The legal process. From a legal perspective, determining what constitutes the location of the money will likely be an iterative process, involving different courts that may make different decisions. In the U.S. if the courts decide in one case that the money is with the private key, another court can decide in a different case that the money is with the individual. For example, Ross Ulbricht is currently in federal court but at a district court level, which means any decisions made there do not have to be followed by other courts [5]. In the case of an appeal, decisions made by a Federal Appeals Court apply only to that court's region; cases may go to the Supreme Court when one circuit disagrees with another [40].

Case studies. We now present several case studies in which we consider what the law is trying to accomplish by locating the money. We explore what the law currently is, what future laws might be, the technical mechanisms that should be considered for future policymaking, as well as possible directions for the technical community. We conclude the section with a discussion of what technologists might consider to impact these laws.

5.1.1 Border Crossings

Current situation. Most countries have a requirement that monetary instruments above a certain value be declared as people cross the border. When transferring bitcoins through an exchange, most likely the exchange has established the necessary legal procedures registering either as a money services business, as is currently required in the U.S. and Canada, or meeting other government requirements. If the law determines that a bitcoin does have a location (contrary to a technical argument that no such location exists), then carrying it across a national border will have legal implications. Currently, in the United States any amount over $10,000 must be declared on a FinCEN form 105, and the penalty for not doing so can be up to a $500,000 fine and up to ten years in prison [41]. These rules are in place as part of anti-money laundering measures; the implications of money laundering will be discussed further in §5.2.

Future possibilities. There is discussion that virtual currencies are not monetary instruments. Using the IRS's determination that virtual currency is property and not currency [27], the Silk Road's accused founder argued through his attorney that Bitcoin could thus not be a monetary instrument [17]. Presently, the argument had been unsuccessful [23] but could be revisited on appeal. This may mean that future laws will clarify virtual currency's status. Already a bill has been proposed in the U.S. Congress to declare Bitcoin currency [36].

Technical mechanisms. We now explore technical nuances that should be considered for future policymaking. Using the location of the private key for jurisdiction makes sense when the private key is stored on paper or on a hard drive in a location such as a safe. It could then be considered to be in that location rather than on the person crossing the border. However, if the private

key is stored in a safe in the U.S. and another copy is stored in another country, then the authority seeking to determine its location may argue that the coins are in both locations. If the courts make such a determination, then by replicating a key in different locations, an individual may subject themselves to each of those jurisdictions. This possibility suggests that replicating keys in multiple locations (something individuals may wish to do for recovery purposes if one location's keys are destroyed) may create new legal challenges for the individual.

Another possibility is if the private key is in a password-protected format. In the U.S., it would be difficult for an authority to force individuals to reveal their password because of rights against self-incrimination; however, there are many countries where this would not be true. If threshold cryptography were used to split the private key into two parts, with each part stored on a different smartcard where both smartcards are needed to perform transactions with this private key, a government authority might simplify the situation by attributing location to the individual. Governments would likely make the same attribution — that the money is with the individual — if individuals use other sophisticated techniques to obscure (their belief of the interpretation of) the "location" of the money, e.g., by encrypting the private key with another key for which the corresponding decryption key is stored in another jurisdiction. Thus, as with some of the earlier examples, we see that technical mechanisms designed to achieve one valuable property (e.g., security) have the potential to negatively impact an individual when trying to determine the location of the user's coins.

Turning to exchanges, we observe that an exchange can be treated similar to a bank and therefore when an individual crosses a border it is as if the money is in a bank account. However, this also leads to the following scenario: A user transfers bitcoins from his private wallet managed by an exchange in Japan to purchase goods from a U.S. merchant using an exchange in Canada. If the locations of the exchanges are used as the location of the money, this process could be interpreted as him or her transferring funds from Japan to Canada — even if he or she, and the destination merchant, were in the U.S. the entire time.

5.1.2 Taxes

Current situation. Countries have taken different stances on the status of virtual currencies for tax purposes. In the U.S., the IRS has determined that virtual currency and Bitcoin will be taxed as property [27]. This means that capital gains tax applies and even that Bitcoin mining must be reported under self-employment tax requirements. Both Brazil and Finland have also required citizens to report Bitcoin investment income as capital gains [38]. While some countries have established how virtual currencies like Bitcoin are to be taxed, the real-world application of taxation is quite complicated. In the U.S. there are rules covering different kinds of income, taxes based on where and how the income was earned, and when securities are bought and sold. There are also requirements about reporting income earned in foreign countries [26]. We do not go into detail here about forms of taxation for that reason.

Future possibilities. While virtual currency has been considered taxable income in countries including the U.S. for years [28], the determination that it and Bitcoin is to be taxed as property is a recent development [27]. Since there is little Bitcoin-specific regulation thus far, it is possible that a legislature or central bank could still determine that Bitcoin is currency. In the U.S., legislators have begun proposing laws to classify Bitcoin as currency [33, 36] Whether this classification would have a positive impact is unclear. If it were currency, the legal implications could be problematic because of laws in many countries establishing that only the government has the right to issue currency [38].

Technical mechanisms. If the private key provides the legal location of the money, and the key is stored in a single location such as a safe, then determining which government's taxation rules apply might be simpler than in alternate scenarios. If, however, the location of the money is with the individual, the complex rules for an individual's income, whether earned in their country of residence or foreign location, would likely apply. Attributing the location of the money to an exchange may provide more clarity if the exchange is registered with a government, though rules about individual income taxation would likely still apply. Even if one were to argue that the money in Bitcoin is in the block chain and therefore on every node, tax authorities would likely still rely on the individual's location and self-reporting of income. In other words, technical options (like claiming that the money does not exist in any single location) cannot enable people to avoid laws like taxation, and legal determinations may not always match what (some) technologists believe to be true.

Stepping back, we find that the question of taxation is related to the previous question of "where is the money?" because the location of the money can determine the applicable jurisdiction. As with the earlier discussions, technical decisions can help simplify the determination of where the money is (e.g., only store a single copy of the private key in a single location) or complicate matters (e.g., replicate a key across multiple jurisdictions, or use secret-sharing to split a key across multiple jurisdictions so that pieces from different jurisdictions are required in order to reconstruct the key). However, policymakers may choose specific answers for questions like "where is the money?" that are not directly correlated to the system's technical properties. Nevertheless, we believe that it will empower technologists to understand the issues that we analyze here.

5.1.3 Theft and Fraud

Current situation. If an unauthorized charge is made on a bank account or credit card as a result of card or identity theft, there is recourse to be had. The financial institution will typically reimburse the false charges. If consumers object to a charge on their account, banks may even reverse the charge. Today's widely-deployed virtual peer-to-peer currencies do not provide this option. Once a Bitcoin transaction is confirmed into the block chain it is not reversible (under normal functioning of the system, with an honest miner majority). Proving bitcoins were stolen may eventually lead to the government seizing them from the guilty party, when technically possible, e.g., when the government obtains the

corresponding private keys. If the thieves have "lost" their private keys, however, then the money may be lost from the system entirely.

Future possibilities. Exchanges may prove to be a policy-based answer to providing recourse for theft and fraud victims. Depending on their terms of service and the country they are registered in, an exchange could provide similar services to those financial institutions currently perform. For example, exchanges could build into their model the cost of lost bitcoins, just as banks do not often recover the money they refund customers but view it as a cost of doing business. In other words, exchanges could absorb the cost of lost bitcoins rather than reversing transactions. There is also a developing market for insurance. Most insurance protections against crime do not protect against bitcoin theft, though certain exchanges (e.g., Circle, Coinbase, Elliptic, and Xapo) do provide some form of insurance. Insurance may be an easier solution for bitcoin theft, compared to pursuing criminal charges and possible later seizure from the guilty party.

Technical mechanisms. There are several technical options for responding to theft that could be implemented through protocol changes. As one technical direction, though not one that we necessarily advocate for, would be to modify the Bitcoin protocol such that coins can be tagged with a set of allowable target addresses (or domains) for transactions. Thus, the system could ensure that bitcoins never leave a set of authorized exchanges, and these exchanges could have an agreement to (effectively) revoke transactions. Alternately, it might be possible to modify the Bitcoin protocol and allow coins to be "tainted." For example, trusted authorities could somehow flag bitcoins to indicate that they are "dirty." Miners or individuals could choose to ignore dirty money and any money that derives from that money. Such a protocol modification would allow a trusted party to revoke transactions — a change that may be met with resistance by some members of the cryptographic currency community, but may help prevent criminals from spending stolen money.

5.1.4 Technical Directions and the Law

Above we reflected on the legal context surrounding Bitcoin and other cryptographic currencies and have discussed the interplay between technology and policy. In doing so, we raised potential directions for additional exploration within the technical community. However, we stress that while technical innovations may affect legal decisions — that is, technical architectures *can* affect policies — technical innovations cannot prevent prosecution. For example, suppose someone uses threshold secret sharing with a private keys in an attempt to avoid laws in a particular jurisdiction. If the person did something illegal, the courts would still try to find a way to prosecute, even if the details of the case (e.g., where the money is) may not directly relate to technical properties of the system.

5.2 What About Anonymity and Pseudonymity?

There are a number of public misconceptions surrounding anonymity in virtual currency. Part of legislators' concerns over money laundering is their belief that cryptographic currencies provide anonymity. However, as some Bitcoin experts

would point out, the blockchain's public nature makes Bitcoin pseudonymous rather than anonymous. Providing a better understanding of Bitcoin's status as pseudonymous is key to successful policymaking.

Bitcoin and other crypto currencies explore a new space in financial privacy compared to other technologies like cash, checks, and credit cards. One key difference is that the block chain is public, though identities can be pseudonyms. Another key difference is that virtual currencies enable the quick transfer of large sums of money outside of conventional systems (e.g., without banks).

While in Bitcoin it may not always be possible to use the public block chain to link transactions with the involved parties, it can sometimes be possible [30]. While Bitcoin entities can use techniques to make linking more difficult, like using mixers (aka, tumblers or laundries) or throw-away public-private key pairs, the mere potential for anyone with access to the public block chain to link transactions with individuals raises challenges for the finance sector. Similarly, the potential for individuals to mask their identities and transfer large sums of money also creates challenges for the financial sector. We explore these issues, as well as the implications of strongly anonymous crypto currencies, here.

On the potential for anyone to link some transactions to parties. Bitcoin's public block chain has proven to allow transactions to be traceable both by academics and authorities. Meiklejohn et al. [30] studied methods that could be used to re-identify the groups behind Bitcoin transactions.

In traditional banking, there are privacy requirements regarding what information banks can share with other groups and how they must preserve an individual's privacy [11]. These provisions have yet to be applied to virtual currencies and Bitcoin specifically. The nature of the protocol likely means that they could not apply to the protocol itself but since exchanges have to register in the same way that financial institutions do [22], they may eventually be subject to the same compliance requirements.

There exist numerous other examples for which the ability to link transactions with individuals might lead individuals to not use (accept or send) bitcoins. For example, consider political party donations. The U.S. Federal Election Commission has decided that campaigns may accept bitcoins, but that such a contributor must provide his or her name, physical address, and employer, and affirms that the contributed bitcoins are owned by him or her and that the contributor is not a foreign national [21]. These requirements could link them to that wallet and/or transaction, as well as enable the tracing of others.

On the potential for parties to mask their identities. One of the central concerns about virtual currencies for governments is the potential for money laundering through the potential for anonymity that Bitcoin and other virtual currencies provide [10, 38]. Money laundering is generally defined as activities and financial transactions that are undertaken to hide the source of the money. Part of the money laundering concern is based in a misunderstanding of Bitcoin's status as an anonymous exchange. Since Bitcoin transactions have proven to be traceable, it is not strongly anonymous but rather pseudonymous.

On strongly anonymous crypto currencies. Zerocoin [8, 31] poses a more realistic anonymous money laundering threat. Zerocoin uses the same distributed ledger as Bitcoin, but encodes transactions such that they do not reveal how much currency was transferred or publicly reveal the public keys of the sender and receiver, while still allowing for distributed verification of the ledger. While transfer in and out of the Zerocoin system in practice continues to use centralized exchanges which could be subject to regulation, transactions within the system cannot be monitored in the same way as with Bitcoin, and it is not possible for an external observer to determine how much currency an individual wallet possesses without access to the private key.

As currently designed, Zerocoin would validate regulator concerns over the money laundering threat of virtual currencies. The development of Zerocoin, if its use becomes widespread, could have a large impact on the developing regulation around Bitcoin and virtual currencies. We stress, however, that there are are both advantages and disadvantages with strongly anonymous cryptographic currencies. As noted above, increased anonymity could facilitate adoption by financial institutions given current laws about bank transaction privacy, and anonymity could also facilitate adoption in contexts where privacy is highly valued (e.g., paying for certain types of medical care).

Technical mechanisms. While privacy advocates may disagree, from an intellectual perspective, the law and policy community may be interested in the existence of escrowed anonymity systems. For example, would it be possible to create a cryptographic currency that is strongly anonymous unless a quorum of trusted third parties agree to de-anonymize a set of transactions? Or would it be possible to create a cryptographic currency that is strongly anonymous for n-years, after which the strong anonymity of each transaction melts away? For example, each transaction could be encrypted in a provably verifiable way to a time-specific public key of a trusted authority (or set of authorities). Those authorities could commit to releasing the corresponding private keys after the appropriate time has lapsed. The resulting protocol would not require trusting the authorities to assist in the preservation of the integrity of the network, but would trust the authorities not to de-anonymize transactions early. We encourage the technical community to explore these and similar dimensions as well.

5.3 What Happens as the World Evolves?

The world is not static. New crypto currencies will be developed, the Bitcoin protocol will evolve, and the uses of Bitcoin and the Bitcoin infrastructure may evolve as well. We now shift our attention to policy and technical issues to consider as this evolution takes place. We begin with a short detour: a discussion of the Computer Fraud and Abuse Act.

Computer Fraud and Abuse Act. In the U.S., the Computer Fraud and Abuse Act (CFAA), passed in 1986, assesses whether someone knowingly accessed a computer without authorization or exceeded their authorized access [2]. Prosecutors in the U.S. have used a broad interpretation of these clauses in criminal cases. Many countries, including Brazil, the UK, and others, have equivalent

laws [15], but the U.S. is one of the prominent prosecutors. Though the CFAA may seem broad and unlikely to apply to virtual currencies, recent history has shown that it is often applied to most criminal cases involving computers.

While U.S. courts have not yet specifically ruled on the CFAA's application to virtual currencies or Bitcoin, the alleged creator of the Silk Road has been charged with violations of CFAA [5]. Because CFAA covers unauthorized access, there are a number of possible applications to protocol attacks.

The 51% attack, and other attacks. It is well known that an adversary with more than 50% of the resources in the Bitcoin mining network could cause attacks against the integrity of the block chain. Other attacks also exist, such as selfish mining [19]. Suppose that a party — such as a mining pool — can put itself in a position to mount one of these attacks, e.g., by controlling 51% or more of the resources in the mining network. Depending on the method of attack and its impact, it is possible that the operators could be charged with CFAA violations or their local equivalent. While technically we desire a cryptographic currency that is strong enough to resist reasonable technical attacks, we find the conclusion in this paragraph valuable because it means that even if an organization develops the capability of compromising the integrity of the block chain, there may be legal impediments for them making use of those attack capabilities.

Vulnerabilities. When a vulnerability is discovered in a popular product produced by a major manufacturer — such as a browser or an operating system — it is generally clear who the responsible party is for fixing the vulnerability. If a vulnerability is found in a particular Bitcoin mining or client software package, then it is also clear who should be responsible for fixing the vulnerability. But suppose that the vulnerability is uncovered in the protocol itself. There would need to be a process to ensure that the protocol — as well as all relevant implementations — can be updated quickly after a vulnerability is discovered. This means having a process in place in advance of any vulnerability discovery. As Bitcoin (or any other cryptographic currency) becomes more popular and accepted by societies and governments, we argue that there becomes an increasing need for a clear process for protocol updates. Whereas there may already be a set of core developers trusted with the process today, the acceptable trust model may change if a government determines that the protocol constitutes a currency. As a point to consider: would laws speak to specific protocol versions, or protocol update processes?

Because of the challenges with protocol updates, we propose a technical stopgap mitigation technique which could potentially be incorporated into the protocol: If people own bitcoins under version M of the protocol, and version M is found to be insecure, those people could have the capability to freeze their bitcoins (so that they cannot be spent) until version N of the protocol, $N > M$.

Illegal content in the block chain. Bitcoin miners store copies of the block chain, and they may have some expectations for what will be stored in the block chain. For example, they may have the expectation that only transactions are stored in the block chain. There are already, however, many non-transaction related images and text embedded in the block chain [35]. Suppose that some

malicious party, Mallory, inserts illegal content in the block chain (such as classified government documents, certain types of pornography, and so on). Mallory's actions could cause Alice's and Bob's computers to store copies of that illegal data, without Alice's and Bob's knowledge or consent. Alice and Bob might face liability in criminal charges though they did not put the content there.

While one might evaluate whether the license agreements for some (although perhaps not all) Bitcoin clients and miners clarify that arbitrary content may be stored in the block chain, raising the awareness of such potential does not mean that illegal or inappropriate content might not be inserted into the block chain. A separate question therefore arises: could Mallory's actions ultimately lead to Bitcoin becoming illegal in some jurisdictions? For example, what would the legal implications be if any node wishing to store the entire block chain must, by definition, also store certain types of illegal pornography? (The definition of legal content may vary between legal jurisdictions.) Similarly, suppose that someone inserts classified U.S. documents or corporate intellectual property into the block chain. Could these possibilities lead to Bitcoin becoming too risky for citizens to use or could these possibilities result in it becoming illegal to run a full Bitcoin node? It may be possible to hold those storing the node legally responsible for the block chain content because it is on their server or computer.

While the use of a central authority may be antithetical to some of the principles underlying Bitcoin, a future version of the protocol (or a similar protocol) might allow a central authority (or threshold set of trusted authorities) to remove specific blocks from the block chain. In the new cryptographic currency, it may be possible to use cryptographic techniques, under some trust model, to (1) allow the removal of the relevant block but create a new block that would (2) allow a verifier to verify that only certain transactions were removed or obfuscated and also (3) allow a third party to verify the details of the financial transactions associated with the illegal content (so that any money transferred with the illegal content is not lost). We leave as an open problem whether it might be possible to achieve these properties in a new cryptographic currency, or to otherwise develop a currency that would support the removal of illegal content under a reasonable threat model.

Excessive content in the block chain. Mallory might also attempt to excessively grow the size of the block chain, thereby depleting the resources of those nodes storing the entire block chain. In doing so, Mallory's actions will result in the consumption resources on those nodes without those nodes' consent. Depending on the agreements and contracts signed, Mallory could face liability in a tort lawsuit for damages and cost reimbursement.

Protocol updates. Society, corporations, and individuals may become more dependent on Bitcoin (or other crypto currencies) over time. Bitcoins are already accepted by major online organizations like Dell and Wikipedia, and the U.S. government has already determined that (for now) Bitcoin should be treated as a commodity. In the future, there is a possibility of Bitcoin (or a derivative) becoming a currency. A question arises: what happens if the Bitcoin protocol is subsequently updated? This question is important because a protocol update

could introduce a vulnerability or change the economics of participation in the Bitcoin ecosystem. In the latter case, we argue that for the United States, the U.S. National Institute of Standards and Technology (NIST) may be the appropriate body for specifying the details of the cryptographic protocol. Should NIST ever be put in a position of being asked to formalize the specification of a cryptographic currency, we suggest that NIST consider a competition-like process, similar to the process it used to select AES and SHA3. The resulting currency may be similar to Bitcoin but may not *be* Bitcoin if the current Bitcoin developers do not agree to transferring responsibility to NIST.

Digital divide. A virtual currency, almost by definition, suggests a technical requirement for participation in the ecosystem. While there are corner cases that might seem like exceptions (e.g., printed Bitcoin coins), individuals operating in those cases can still benefit from technology (e.g., to use a computer to verify the integrity of a printed coin). Virtual currencies thus have the potential to amplify the digital divide — to widen the gap between those who have technologies (and hence the ability to fully participate in the crypto currency ecosystem) and those who do not. A policy implication is that it may be unlikely for a virtual currency like Bitcoin to ever be the only currency accepted in a particular jurisdiction. A technical implication is the opportunity for a low cost, easily accessible Bitcoin hardware implementation which would assist in the narrowing of the gap — by making Bitcoin technology accessible to all (possibly with a government subsidizing the (low) cost of the hardware). Until such time, we believe that a crypto currency will likely not be the *only* currency in a jurisdiction.

6 Conclusion

The interactions between technology, policy, and law for crypto currencies such as Bitcoin are often complicated and nuanced. We have considered key issues, including the physical location of the value in a crypto currency, the interaction between regulation and anonymity or pseudonymity in a virtual currency, and challenges that arise as the world evolves. While technical architectures can affect laws and policies, and vice versa, we also observe that — contrary to what technologists might prefer — laws may not necessarily match a technologist's expectations. We explore the interplay between the law, policy, and technical mechanisms in our analysis.

We believe that the results of our analysis will be beneficial to law and policy makers. As a consequence of our interdisciplinary investigations into crypto currencies, we also proposed several directions for the technical community. Some of the directions we propose may be compatible with Bitcoin's underlying tenets such as distributed control, whereas others may require more centralization. In suggesting technical directions for future research and innovation, we do not mean to also suggest that any one directions is more valuable or appropriate than another; we leave that decision to the reader and the technical community based on their individual values and interests. The directions that we propose are possible approaches to address current legal and policy challenges, and may possibly also help shape future policies.

Appendix: Disclaimer

Since this effort involves the collaboration of individuals in both the law and technology fields, we must give this disclaimer: This analysis is for informational purposes only and does not constitute legal advice.

References

1. U.S. Constitution, Article I, Section 8
2. U.S. Title 18, Section 1030 (Computer Fraud and Abuse Act)
3. Securities and Exchange Commission vs. Trendon T. Shavers and Bitcoin Savings and Trust (Jul 2013), http://www.sec.gov/litigation/complaints/2013/comp-pr2013-132.pdf
4. Seizure Warrant for Mutum Sigillum, a subsidiary of Mt. Gox (May 2013), http://cdn.arstechnica.net/wp-content/uploads/2013/05/Mt-Gox-Dwolla-Warrant-5-14-13.pdf
5. United States vs. Ross William Ulbricht (Oct 2013), http://www.popehat.com/wp-content/uploads/2013/10/UlbrichtCriminalComplaint1.pdf
6. United States vs. Robert M. Faeilla and Charlie Shrem (Jan 2014), http://www.justice.gov/usao/nys/pressreleases/January14/SchremFaiellaChargesPR/Faiella,%20Robert%20M.%20and%20Charlie%20Shrem%20Complaint.pdf
7. Bangkok Pundit: Has Bitcoin really been banned in Thailand? (Jul 2013), http://asiancorrespondent.com/111332/has-bitcoin-been-banned-from-thailand/
8. Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M.: Zerocash: Decentralized anonymous payments from bitcoin. In: IEEE Symposium on Security and Privacy (2014)
9. Brito, J., Castillo, A.: Bitcoin: A Primer for Policymakers. Mercatus Center, George Mason University (Aug 2013), http://mercatus.org/publication/bitcoin-primer-policymakers
10. Bryans, D.: Bitcoin and Money Laundering: Mining for an Effective Solution. Indiana Law Journal 89(1) (2014)
11. Bureau of Consumer Protection: In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act (Jul 2002), http://www.business.ftc.gov/documents/bus53-brief-financial-privacy-requirements-gramm-leach-bliley-act
12. Chaum, D., Fiat, A., Naor, M.: Untraceable Electronic Cash. In: Advances in Cryptology. CRYPTO '88 (1988)
13. Chaum, D.: Blind Signatures for Untraceable Payments. In: Advances in Cryptology. CRYPTO '82 (1982)
14. Consumer Financial Protection Bureau: Risks to consumers posed by virtual currencies (Aug 2014), http://files.consumerfinance.gov/f/201408_cfpb_consumer-advisory_virtual-currencies.pdf
15. CyberCrime Law: Cybercrime laws from around the world, http://www.cybercrimelaw.net/Cybercrimelaws.html
16. Dell: Dell now accepts bitcoin (2014), http://www.dell.com/learn/us/en/uscorp1/campaigns/bitcoin-marketing
17. Dratel, J.L.: Memorandum of Law in Support of Defendant Ross Ulbricht's Pre-Trial Motions Challenging the Face of the Indictment (Apr 2014), http://www.wired.com/wp-content/uploads/2014/04/Ulbricht3.pdf
18. European Central Bank: Virtual Currency Schemes (Oct 2012), http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

19. Eyal, I., Sirer, E.G.: Majority is not Enough: Bitcoin Mining is Vulnerable. In: Financial Cryptography and Data Security (2013)
20. Fairfield, J.: Smart Contracts, Bitcoin Bots, and Consumer Protection. Washington & Lee University Law Review Online (Sep 2014), http://lawreview.journals.wlu.io/smart-contracts-bitcoin-bots-and-consumer-protection
21. Federal Election Commission: FEC Memorandum (May 2014), http://www.fec.gov/agenda/2014/documents/mtgdoc_14-24-b.pdf
22. Financial Crimes Enforcement Network: Guidance FIN-2013-G001: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (Mar 2013)
23. Greenberg, A.: Forrest Denial of Defense Motion in Silk Road Case (Jul 2014), http://www.scribd.com/doc/233234104/Forrest-Denial-of-Defense-Motion-in-Silk-Road-Case
24. Gruwell, L.: Wikimedia Foundation Now Accepts Bitcoin (Jul 2014), http://blog.wikimedia.org/2014/07/30/wikimedia-foundation-now-accepts-bitcoin/
25. Hill, K.: 21 Things I Learned About Bitcoin Living On It A Second Time (May 2014), http://www.forbes.com/sites/kashmirhill/2014/05/15/21-things-i-learned-about-bitcoin-living-on-it-a-second-time
26. Internal Revenue Service: http://www.irs.gov
27. Internal Revenue Service: Notice 2014-21 (Mar 2014), http://www.irs.gov/pub/irs-drop/n-14-21.pdf
28. Internal Revenue Service: Tax Consequences of Virtual World Transactions (Aug 2014), http://www.irs.gov/Businesses/Small-Businesses-&-Self-Employed/Tax-Consequences-of-Virtual-World-Transactions
29. Marini, P., Marc, F.: La Regulation a L'epreuve de L'innovation: Les Pouvoirs Publics Face au Developpement des Monnaies Virtuelles. French Senate (Jul 2014), http://www.bitcoin.fr/public/divers/docs/Rapport_de_la_commission_des_finance_du_Senat.pdf
30. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., Savage, S.: A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. In: Internet Measurement Conference (2013)
31. Miers, I., Garman, C., Green, M., Rubin, A.D.: Zerocoin: Anonymous Distributed E-Cash from Bitcoin. In: IEEE Symposium on Security and Privacy (2013)
32. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System (2008), https://bitcoin.org/bitcoin.pdf
33. New York State Department of Financial Services: BitLicense Framework: Title 23. Department of Financial Services Chapter I. Regulations of the Superintendent of Financial Services Part 200. Virtual Currencies (Jul 2014), http://www.dfs.ny.gov/about/press2014/pr1407171-vc.pdf
34. Overstock.com: Bitcoin on overstock.com (2014), http://www.overstock.com/bitcoin
35. Shirriff, K.: Hidden surprises in the Bitcoin blockchain and how they are stored: Nelson Mandela, Wikileaks, photos, and Python software (Feb 2014), http://www.righto.com/2014/02/ascii-bernanke-wikileaks-photographs.html
36. Stockman, S.: Stockman plans to introduce the "virtual currency tax reform act" (Apr 2014), http://stockman.house.gov/media-center/press-releases/stockman-plans-to-introduce-the-virtual-currency-tax-reform-act
37. Tavakoli, Y., Yohannan, D.: Personal Jurisdiction in Cyberspace: Where Does It Begin, and Where Does It End? Intellectual Property and Technology Law Journal (Jan 2011)

38. The Law Library of Congress, Global Legal Research Directorate Staff: Regulation of Bitcoin in Selected Jurisdictions (Jan 2014)
39. The People's Bank of China and Five Associated Ministries: Prevention of Risks Associated with Bitcoin (Dec 2013), https://vip.btcchina.com/page/bocnotice2013
40. United States Courts: Courts of Appeals, http://www.uscourts.gov/FederalCourts/UnderstandingtheFederalCourts/CourtofAppeals.aspx
41. U.S. Department of the Treasury: Report of International Transportation of Currency and Monetary Instruments
42. U.S. Securities and Exchange Commission: Investor Alert: Bitcoin and Other Virtual Currency-Related Investments (May 2014), http://investor.gov/news-alerts/investor-alerts/investor-alert-bitcoin-other-virtual-currency-related-investments