Source: Hester Peirce and Benjamin Klutsey, eds., *Reframing Financial Regulation: Enhancing Stability and Protecting Consumers*. Arlington, VA: Mercatus Center at George Mason University, 2016.

CHAPTER 14
Regulating Bitcoin—On What Grounds?

WILLIAM J. LUTHER
Kenyon College

Bitcoin is a relatively new technology with much promise. As the world's first successful cryptocurrency, it functions as an alternative means of making electronic payments. Its cryptography keeps transactions secure and protects merchants from chargeback fraud. Its use of a blockchain, or public ledger, and distributed peer-to-peer network to process these transactions seems likely to lower the costs of transacting. The Bitcoin protocol, which simultaneously rewards those on the network known as miners for processing blocks of transactions and ensures that the bitcoin supply grows at a steady, known rate, prevents users from spending balances they do not have while removing the prospect of unexpected and undesirable monetary expansions. Seeing these benefits, some customers and businesses, large and small, have already turned to bitcoin. And bitcoin proponents believe many others will make use of it as the benefits become more apparent.

Despite these benefits, many regulators seem concerned. In the New Jersey legislature, the Financial Institutions and Insurance Assembly Committee held a hearing on February 5, 2015, to consider how best to regulate bitcoin.[1] In the same week, the New York Department of Financial Services released a revised draft version of its BitLicense proposal that would require some entities in the bitcoin community to be licensed by the state.[2] At the federal level, the Financial Crimes Enforcement Network (FinCEN) has offered guidance on how bitcoin will be treated within its existing regulatory framework.[3] The US Commodity Futures Trading Commission (CFTC) took action against an unregistered bitcoin options trading platform in September 2015.[4] In December 2015, the US Securities and Exchange Commission (SEC) charged two bitcoin mining companies and their founder with fraud.[5] In all of the efforts to regulate or apply existing regulations to bitcoin to date, there is a strong presumption that something must be done.

There are three principal justifications for regulating bitcoin: to protect consumers, to prevent illegal transactions and transfers, and to promote broader macroeconomic policy goals. Such justifications imply that there are potential benefits to regulating bitcoin. Of course, regulations also impose costs. In addition to compliance costs, excessive regulation could dissuade some or all users from transacting in bitcoin and, hence, from realizing the benefits thereof. Efficient regulation requires that the rules adopted, and the extent to which those rules are enforced, are limited to cases in which the benefits exceed the costs.

In this chapter, I consider the three principal justifications for regulating bitcoin. Since efficient regulation is the goal, I consider the merits of each justification by assessing the extent of the problem regulation might address, the likely effectiveness of regulation in addressing that problem, and the likely costs of regulation on the regulated actors and the system as a whole. I conclude by offering some simple guidelines for regulators. Ideally, such guidelines would bring about a superior regulatory framework. If nothing else, though, one can hope that some regulatory clarity will emerge soon.

CONSUMER PROTECTION

Justifications for consumer protection regulation generally come in naïve and more sophisticated forms. Both views suggest that some consumers will be exploited, defrauded, misled, or otherwise taken advantage of in the absence of regulation.[6] The naïve view assumes, at least implicitly, that (1) consumers are never willing to acquire the requisite information to prevent being mistreated, (2) that competition or the threat of competition is never sufficient to prevent mistreatment, and/or (3) that the optimal amount of mistreatment is equal to zero. A more sophisticated view recognizes that consumers are generally interested in protecting themselves and will incur costs to do so; that firms are generally interested in maintaining relationships with consumers over a long period of time and regularly incur costs to keep consumers satisfied; and that, at some point, the cost of providing additional protection to consumers exceeds the benefits. Regulation is desirable, in this more sophisticated view, when it lowers the information costs to consumers or more properly aligns the incentives of firms. Even then, regulation is unlikely to prevent all instances of abuse.

When considering regulation on the basis of consumer protection, it is important to understand who is being protected and from whom they are being protected. In the case of bitcoin, the relevant agents include individual users, small business users, large business users, e-wallet services, exchanges, miners, and mining pool administrators. The term "user" refers to one making, accepting, or receiving payments in bitcoin. E-wallet services refer to counterparties that enable users to send, accept, receive, or store bitcoin more conveniently. Exchanges refer to services that allow one to exchange bitcoin for traditional or other virtual currencies. Miners are those processing bitcoin transactions via the Bitcoin protocol in exchange for new bitcoin or transaction fees. Mining pool administrators refer to those organizing a collection of miners and/or distributing payments to miners in the pool.

The National Association of Attorneys General (NAAG) lists three risks to consumers using bitcoin: exchange rate volatility, lack of security, and the inability to execute chargebacks.[7] Let me consider each in turn.

Exchange Rate Volatility

One concern with bitcoin is that, to date, it has been characterized by a highly volatile exchange rate. Over a twelve-month period, the dollar per bitcoin closing price on the BitStamp exchange has ranged from a low of $209.72 in August 2015 to a high of $467.42 in April 2016.[8] The average closing price was $340.32. The Bitcoin Volatility Index shows that the exchange rate is less volatile today than it has been in the past.[9] Still, with a thirty-day estimated volatility around 1.52 percent, it is more volatile than gold (1.2 percent) and other major currencies (0.5 to 1.0 percent).

The supply of bitcoin is exogenously determined and known in advance. The observed fluctuations in the exchange rate, then, reflect changes in demand. Demand is volatile for many reasons. Since the network of bitcoin users is relatively small at present, a user's decision to buy or sell relatively small amounts of bitcoin can have a significant effect on the price.[10] Of course, such fluctuation becomes less prevalent as the network grows. Uncertainty surrounding the future network size of bitcoin also contributes to this volatility. If everyone knew that everyone else would use bitcoin in the future, it would be very valuable today. On the other hand, if no one will use bitcoin in the future, it would not be very valuable today. Unfortunately, the future is, to some extent, unknown and unknowable. As our best guess of the future network size of bitcoin changes, so too does the current trading price. Finally, the future network size depends, in part, on the regulatory environment. The regulatory environment is unclear at the moment and expectations about the future regulatory environment might change as new evidence becomes available.[11] Hence, if nothing else, clarifying the regulatory approach to bitcoin could reduce exchange rate volatility.

A volatile exchange rate makes bitcoin risky to hold. One might suffer huge losses or realize huge gains over short periods of time. Fortunately, most agents are already aware of the volatility and have taken steps to mitigate the downsides. Others are being compensated for (knowingly) bearing this risk. As such, regulations intended to mitigate the risks of exchange rate fluctuations are limited to (1) reducing uncertainty by clarifying the regulatory environment and (2) providing general information to users about the volatility of bitcoin.

At present, most bitcoin users—be they individuals, small businesses, or large businesses—do not hold much wealth in bitcoin. They merely use bitcoin as a convenient means of payment. Intermediaries, like Coinbase, function as an exchange and e-wallet service. They permit users to convert traditional currencies into bitcoin at the time of making a payment and permit the conversion of bitcoin into traditional currencies.[12] Hence, a typical transaction involves a dollar to bitcoin exchange, a bitcoin transfer from payer to payee, and a bitcoin to dollar exchange. The payer can spend bitcoin without having held wealth in bitcoin. The payee can accept bitcoin without having to hold bitcoin. Both incur a small fee to convert into and out of bitcoin on the spot to make a transaction.[13] If neither payer nor payee holds bitcoin for an extended period of time, they need not be concerned with—and will not suffer losses from—the fluctuating exchange rate.[14] As such, there is not much scope for protecting these users with regulation.

Of course, someone must be holding bitcoin and, hence, bearing the risk of a fluctuating exchange rate. Intermediaries accept this risk by (1) agreeing to convert dollars to bitcoin and bitcoin to dollars at the current market rate when a transaction is made and (2) holding bitcoin between transactions. Given that they knowingly accept this risk and are compensated with a fee paid by the payer and/or payee for intermediating the transaction, there is little reason to think they are in need of regulatory protection. Moreover, the risk is arguably quite low for these entities to the extent that they deal in a large number of transactions. Sometimes they will incur losses. Other times they will experience gains. While the losses and gains from a fluctuating exchange rate will generally cancel out, the gains from fees and a general tendency for the value of bitcoin to increase over time with the size of the network makes intermediating transactions a profitable venture.

Although not specifically addressed by the NAAG, one might also consider protecting miners and mining pools from a volatile exchange rate. Miners incur costs to process transactions. Since only the first miner to successfully process a batch of transactions is rewarded with new bitcoin, miners frequently join pools to share the rewards in proportion to the computing power each miner employs.[15] Some miners might incur costs on the expectation that bitcoin will have a given value at the time a reward is issued, only to be disappointed when bitcoin has a lower value than expected. Still, there are at least three reasons to believe miners would not benefit greatly from regulation. First, miners (like the intermediaries discussed) tend to be sophisticated participants. They already know about the volatility of bitcoin and have chosen to participate anyway. Second, rewards are paid out roughly every ten minutes and miners have the option to exchange rewards for traditional currencies on the spot. As with users, they need not hold their wealth—even that obtained through mining—in bitcoin for an extended period of time. Third, miners have the option to join mining pools and, if they do, receive a steady stream of payments from mining. As with intermediaries, the gains and losses from a volatile exchange rate will largely cancel out for miners receiving rewards (or a fraction thereof) regularly.

There is no denying that the exchange value of bitcoin is much more volatile than that of many other assets. However, there is not much scope for improving matters in this regard with regulation. The fluctuation stems from changes in demand. It is widely known. And those in the bitcoin system have already taken steps to allocate risk efficiently and compensate those individuals bearing the risk. As such, regulatory improvements in this regard are limited to (1) reducing uncertainty concerning the future network size by clarifying the regulatory environment and (2) providing general information to users about the volatility of bitcoin. The latter is desirable insofar as the regulatory authority can provide this information at a lower cost than each individual user would incur collecting it.

Security Concerns

Another concern with bitcoin is the degree to which one's electronic balance is secure. Regulators naturally worry that the bitcoin system might be hacked;[16] that a large mining pool might compromise the system;[17] and that digital balances might be lost or stolen.[18] Some of these concerns are unfounded or might be alleviated with some simple precautionary actions, as I will discuss. Others are genuine, providing some scope for regulatory action on the grounds of consumer protection.

Concerns about the core Bitcoin protocol are largely unfounded. Dan Kaminsky, renowned security expert and Chief Scientist of White Ops, famously tried—and failed—to hack the Bitcoin protocol in 2011.[19] Based on this experience, Kaminsky concluded that "the core technology actually works, and has continued to work, to a degree not everyone predicted." By relying on algorithmic and open source governance, the bitcoin system is able to process transactions securely and ensure that only those users with the appropriate credentials can transfer and receive a given balance of bitcoin.[20]

Recognizing that concerns regarding the core Bitcoin protocol are largely unfounded is not to accept that the system is immune from attack. It is widely recognized, for example, that the system could be compromised if a miner or mining pool controlled more than 50 percent of the computing power on the network.[21] Since the Bitcoin protocol recognizes the longest blockchain on the peer-to-peer network as legitimate, and since computing power is the limiting factor for adding new blocks to a blockchain, a miner or group of miners with more than 50 percent of the computing power could outcompete other miners to produce the longest blockchain. And, with such power, a miner or mining pool could prevent other users from making transactions or undo past transactions, enabling users to double-spend balances.

While possible, such an attack seems less likely in practice. For one, it would require gaining and *maintaining* more than 50 percent of the computing power. When legitimate miners recognize a threat, they have an incentive to increase the computing power they contribute to the system. If legitimate miners can regain control, they can undo what has been done. Moreover, it is not clear that such an attack is in the interest of the attacker.[22] In weakening the system, an attack would discourage users from participating. The value of bitcoin would fall as existing users exit the system and potential new users refuse to join. Recall that miners are rewarded with bitcoin after successfully processing a block of transactions. It is therefore in their interest to promote the integrity of the system, since that would bolster the value of the newly created coins they earn.

Recent experience confirms the idea that those in a position to make a 51 percent attack are unlikely to do so. On June 12, 2014, the mining pool GHash.io maintained majority power for twelve hours.[23] It did not attempt to undermine the system by double-spending or preventing transactions.[24] A statement issued by the mining pool noted that "the threat of a 51% attack . . . is damaging not only to us, but to the growth and acceptance of Bitcoin long term, which is something we are all striving for."[25] Still, the price of bitcoin fell as some users feared such an attack, thereby discouraging even benevolent mining pools from gaining majority computing power.[26]

A law limiting the processing power of individual miners or mining pools to something less than 50 percent might mitigate the threat of attack. However, for reasons discussed previously, that threat is probably overstated in popular accounts. Moreover, to the extent that miners can coordinate activities in private, it would be difficult to enforce such a law. Finally, if such a law were applied broadly to other cryptocurrencies, it might rule out permissioned blockchain protocols where a smaller fraction of known users verify transactions.

Another security concern exists in the relationship between miners and mining pool administrators. Recall that miners contribute computing power to a mining pool in exchange for a share of the reward earned by any member of the pool. Hence, miners must trust that the mining pool administrator will deliver on the promise to distribute the reward. In practice, this is not much of a concern. Most pools pay their miners several times a day.[27] As such, exploits along these lines are significantly limited. Still, the relationship between miners and pool administrators could be governed by standard contract law. It would not require additional regulation.

For reasons discussed, the benefits from regulations aimed at protecting the system from malicious miners and mining pools or miners from malicious mining pool administrators are probably quite small. Moreover, the costs of such regulations—to the extent that they discourage mining or the development and implementation of alternative protocols—could be large. Recall that the bitcoin system depends crucially on a large, diverse base of miners to ensure that only legitimate transactions are executed. Discouraging mining would therefore undermine the system's ability to fend off attacks. Likewise, alternative protocols—like permissioned blockchains—might provide many of the benefits of bitcoin at an even lower cost. The regulatory framework should not discourage such innovations except in cases where there is a clear and significant risk of abuse.

Other, more plausible security problems exist. Consider the prospect that an inexperienced user loses bitcoin. Bitcoin can be lost when one loses a private key, the hardware where one secures a private key fails, or the private key is not transferred in the event of one's death. In an oft-cited case, one UK man lost 7,500 bitcoin—worth approximately $1.90 million today—when he threw out an old hard drive in 2013.[28] Although most instances of lost bitcoin have involved early adopters who left the network before bitcoin was very valuable, the potential for losing bitcoin remains a problem for users.

The problem of lost bitcoin has some rather straightforward solutions. Users could keep a backup of their private key; they could keep a paper wallet—that is, a physical copy of their private key—and they could make arrangements for private keys to be passed on in the event of death. Other solutions involve trusting a third party (usually an e-wallet provider) with your primary key or employing a multisignature wallet, which requires two of three digital signatures to make a transaction, with the e-wallet provider maintaining one of the three signatures. In the first case, access is recoverable by providing sufficient identifying information to the third party. In the second case, access is recoverable in the event that one but not both keys held by the user is lost or irretrievable.

There are two problems with these solutions to lost bitcoin. First, the users most likely to lose their bitcoin are probably least likely to obtain information on how to prevent such a loss in advance. Their relative inexperience drives both results. The bitcoin community has certainly taken steps to make this information widely available. And, as noted, some e-wallet providers go beyond the mere provision of information by requiring multiple signatures and/or maintaining a copy of the private key. Nonetheless, regulators could potentially improve the flow of information and, in doing so, might help those in the community discover and establish appropriate security and insurance standards. Second, while reducing the likelihood of losing bitcoin, the solutions outlined increase the risk that one's bitcoin will be stolen. Storing multiple copies of your private key increases the number of places where your private key might be discovered. Trusting a third party with a private key provides the opportunity for that trust to be broken. Moreover, inexperienced users—those most likely to lose bitcoin—are probably also less likely to secure private keys appropriately and less able to assess the trustworthiness of a given third party. As such, the possible remedies to the lost bitcoin problem might be worse than the disease.

What is the likelihood that a bitcoin is stolen? Perhaps it is greater than one might think. According to one 2014 estimate, some 918,142.965 bitcoin worth roughly $415.99 million had been stolen.[29] Considering that, at the time of this writing, there are roughly 15,558,175 bitcoin in circulation, a little more than 5.9 percent, or 1 in 17, have been stolen.[30] Bitcoin can be stolen when one does not take the necessary precautions to protect a private key.[31] The biggest heists, however, involve third parties holding access to the accounts of multiple users. For example, the Japan-based bitcoin exchange Mt. Gox tops the list, losing an estimated 850,000 of its users' bitcoin in what the company described as a "transaction malleability" attack that had taken place—unbeknownst to users—over several years.[32] A Tokyo Metropolitan Police investigation concluded that cyberattacks were responsible for only 1 percent of the missing balances at Mt. Gox.[33] Whether such losses result from outside attacks, embezzlement, or the mere mismanagement of funds, they illuminate the difficulties of keeping bitcoin secure.

The blockchain technology presents an interesting problem for thieves. Although users are pseudonymous—that is, their physical identities can be kept private—all transactions taking place on the blockchain are publicly observable. Any user can follow a stolen balance of bitcoin as it is transferred from one address to the next.[34] Indeed, a small team of computer scientists, using only publicly available data, was able to trace bitcoin stolen in well-known thefts to popular exchanges. As they note, "following stolen bitcoins to the point at which they are deposited into an exchange does not in itself identify the thief; however, it does enable further de-anonymization in the case in which certain agencies can determine (through, for example, subpoena power) the real-world owner of the account into which the stolen bitcoins were deposited."[35] Others point out that "a well-equipped law enforcement agency could de-anonymise the network even further."[36]

The prospect of theft presents, perhaps, the strongest case for regulating bitcoin on consumer protection grounds. On one hand, bitcoin is vulnerable like other electronic payment mechanisms and should be regulated as such. On the other hand, bitcoin has unique features that might be leveraged by regulators to create an even more robust system. If thieves can be prevented from cashing out large sums at exchanges, for example, they are reduced to cumbersome alternatives to convert digital balances into usable wealth. Knowing they will be unable to liquidate large balances easily, some thieves will be deterred from stealing balances altogether. However, the costs of preventing or delaying large-scale liquidations—the legitimacy of which might be difficult to assess over short periods of time—might be overly burdensome, discouraging some users from participating in the network altogether. And, to the extent that exchanges or e-wallet service providers are participating in the theft or mismanagement of funds, such regulations would have little effect. A better option, then, would be to require e-wallet and exchange services to (1) register with the proper authorities and (2) collect identifying information on users before exchanging large amounts of bitcoin. In the event of a theft, the victim would then have recourse to go after the appropriate exchange for assisting—knowingly or otherwise—in the transfer of stolen funds and the authorities could subpoena the information held by the exchange or e-wallet service provider. Such regulations would be imperfectly designed and imperfectly enforced. Still, they could have a significant effect on reducing the extent of bitcoin theft.

Chargebacks

Some regulators might be concerned by the inability to execute chargebacks under the Bitcoin protocol without the current owner of a balance agreeing to return the funds in question. This stands in sharp contrast to traditional, centralized payment processing mechanisms that can reverse a transaction when a dispute is made. Indeed, the inability to reverse transactions contributes to the problem of theft: it is impossible to return funds to their rightful owner without consent of the thief. But more mundane instances—like receiving a product of inferior quality or not receiving a product at all—come to mind.

In being unable to execute chargebacks, the Bitcoin protocol is no different than cash.[37] And there are good reasons to permit such a payment mechanism. For one, it prevents the sort of chargeback fraud that plagues small businesses.[38] Indeed, some shopkeepers save so much from the elimination of chargeback fraud that they give their customers steep discounts for paying with bitcoin.[39] It promotes international business as well.[40] High rates of fraud have led traditional payment processors to forgo business in over fifty countries, preventing individuals in those countries from making convenient payments to American businesses. In eliminating a large class of fraud, bitcoin makes transacting with individuals in those countries possible—and profitable.[41] Hence, bitcoin has the potential to increase commerce for small and large businesses alike.

For better or worse, the inability to execute chargebacks under the Bitcoin protocol is part of what it means to transact with bitcoin. Some users will no doubt prefer a payment mechanism that gives them recourse when dealing with potentially unscrupulous sellers. Provided that they are willing to pay the higher fees that come with the ability to execute chargebacks, such users should eschew bitcoin for traditional payment mechanisms. Others can enjoy the lower fees and unique transaction networks made possible with bitcoin. Provided that consumers are aware of the inability to execute chargebacks when making payments with bitcoin, there is no compelling reason to reduce consumer choice in payment mechanisms.

ILLICIT TRANSACTIONS AND TRANSFERS

Bitcoin has attracted a lot of attention from regulators on the grounds that it might facilitate illegal transactions and transfers.[42] Senator Charles Schumer (D-NY) was among the first to take note, describing bitcoin as "an online form of money laundering used to disguise the source of money, and to disguise who's both selling and buying the drug."[43] Senator Joe Manchin (D-WV) also recommended regulation, given the "clear ends of Bitcoin for either transacting in illegal goods and services or speculative gambling."[44] Indeed, many seem to believe "bitcoin is basically for criminals."[45] Others have warned that bitcoin might be used to fund terrorism.[46] So, I will discuss the merits of regulating bitcoin on these grounds.

To date, the sort of black market transactions of concern to Schumer, Manchin, and others seems to comprise a small fraction of the total bitcoin economy. The US Treasury Department found no evidence of bitcoin's widespread use in funding terrorism.[47] Similarly, while media reports have directed much attention at mail-order drug sites conducting business in bitcoin, the volume of transactions actually made through these sites is quite small. Consider the Silk Road, which operated from February 2011 to October 2013 and was described by one media outlet as the Amazon of drugs.[48] The best available evidence, collected over eight months from late 2011 to early 2012, suggests that roughly $1.2 million worth of transactions were made on the Silk Road each month.[49] More recent estimates put the figure at roughly $4.7 million per month for the life of the site.[50] By either estimate, the volume of trading is quite small for a global marketplace.[51] Moreover, the monthly transaction volume for the entire bitcoin system averaged roughly $206.34 million from February 2011 to October 2013.[52] In other words, Silk Road transactions comprised less than 2.28 percent of all transactions. Hence, even if regulations could eliminate all illegal sales conducted in bitcoin, the benefits would be small. And the costs would be borne, at least in part, by the much larger class of users employing bitcoin for legitimate ends.

As I have argued elsewhere, the "US government should find it awkward to regulate bitcoin on the grounds that it facilitates illegal transactions. Its own currency—and the $100 bill in particular—has done so for years."[53] A recent study maintains that 48 percent of the US currency stock is employed in the domestic underground economy.[54] When this analysis is extended to the world, one finds that roughly 76 percent of the US currency stock, or $960 billion, is used to facilitate exchange beyond the reach of tax and law enforcement authorities.[55] To the extent that bitcoin is like cash, the regulatory authority should treat it as such.

Of course, bitcoin is not exactly like cash. It enables electronic transfers. As such, it creates a trail for law enforcement authorities not possible with cash. Although transactions are pseudonymous—that is, virtual addresses are not necessarily tied to physical identities—all transactions are recorded in the public ledger, or blockchain. So, once a criminal is identified in the physical world and linked to a digital address, law enforcement agencies could potentially uncover a string of past criminal transactions. Had they been conducted in cash, these past transactions would be nearly impossible to trace. Moreover, to the extent that exchanges and e-wallet services cooperate—or can be compelled to cooperate—the authorities could uncover and investigate a criminal's past trading partners, who might also be involved in criminal activity.[56] Hence, law enforcement agencies would perhaps be better served by working with the bitcoin network rather than against it.

Furthermore, legal uses of bitcoin are likely to be more sensitive to regulation than illegal uses.[57] Legal users often conduct business with a physical presence; even those conducting business exclusively online often make their physical identities known. Illegal users, in contrast, typically employ anonymizing technology like Tor, preferring to conduct business on the so-called dark web. Hence, the illicit transactions justifying regulatory action are exceptionally difficult to stamp out. To the extent that regulatory efforts make transacting with bitcoin more costly or cumbersome, one should expect legitimate users to exit the network while illegitimate users merely avoid the channels through which such laws are enforced.

There is no denying that bitcoin can be used to make illegal transactions and transfers. The relevant question is whether the benefits of regulating bitcoin on these grounds exceed the costs. Given that the fraction of bitcoin users engaged in illicit transactions or transferring funds to terrorist groups is probably quite small and regulatory efforts to stamp out such transactions are unlikely to succeed, it seems unlikely that regulating on these grounds would produce many benefits. On the other hand, the costs imposed on a system comprised primarily of legitimate users in search of a few bad apples could be substantial. As such, the prudent course of action would seem to require investing in the requisite technology to de-anonymize users in the event that they are suspected of criminal activity.

MACROECONOMIC POLICY

Regulators might also worry that bitcoin could impede the government in promoting broader macroeconomic policy goals. As one commentator put it, bitcoin "looks like it was designed as a weapon intended to damage central banking and money issuing banks, with a Libertarian political agenda in mind—to damage [states'] ability to collect tax and monitor their [citizens'] financial transactions."[58] Having addressed issues of financial monitoring and oversight previously, I now turn to the extent to which the government would lose revenues or be unable to conduct monetary policy effectively if individuals used bitcoin instead of dollars.

Budgetary Policy

When discussing illicit transactions and transfers, I have limited the analysis to black market transactions. However, governments might also be concerned with gray market transactions—that is, buying and selling legal goods or services illegally in order to avoid sales or income tax. Whereas governments want to prevent black market transactions altogether, they do not want to discourage the underlying transactions taking place on the gray market. Rather, they want to force these transactions out of the gray market so that they can collect taxes on the sales and incomes supported by these transactions.

Tax evasion is already a significant problem in the United States. It has been estimated that between 18 to 19 percent of total reportable income goes unreported, reducing tax revenues by $400 billion to $500 billion per year.[59] To the extent that bitcoin obscures one's identity, it could replace cash in such transactions. It is unclear, however, whether bitcoin would promote *additional* tax evasion. On the one hand, it is easier to hold and transact with large balances of bitcoin than cash, which occupies physical space. As such, bitcoin might increase the scope of tax evasion. But, as noted already, bitcoin offers law enforcement authorities a trail of transactions to follow that they would not have if those transactions were made with cash. Hence, bitcoin might fail to replace cash entirely in this domain. In any event, it seems unlikely that the effect of bitcoin on tax evasion would be large, if only because tax evasion is so pervasive already.[60]

In addition to revenues raised through taxing income and sales, governments earn seigniorage revenue from issuing base money. Seigniorage revenue results from holding interest-bearing assets purchased with base money. In the United States, the Treasury's Bureau of Engraving and Printing produces currency and sells it to the Federal Reserve System at cost. The Federal Reserve uses this currency and the balances it creates on its books as reserves held at the

Federal Reserve to purchase interest-bearing assets. Then, after covering its operating costs, the Federal Reserve remits the net income to the Treasury. If demand for base money—that is, currency and reserves held at the Federal Reserve—were to fall as individuals switch to bitcoin, the Federal Reserve would earn less income and therefore remit less to the Treasury. As such, some have warned that the federal government would lose seigniorage revenues if bitcoin were adopted.[61]

In practice, the loss of revenues would be small. In 2013, Fed remittances to the Treasury totaled $79.6 billion—just 0.53 percent of current expenditures by the federal government.[62] Moreover, the extent of revenues lost would be proportional to the number of users switching from dollars to bitcoin. If bitcoin were to function as a niche currency, adopted by a subset of potential users or used in conjunction with dollars, the decline in revenues would be far less than the total amount of remittances.[63] Hence, the benefits of regulating bitcoin on these grounds are quite small. Moreover, sustaining seigniorage revenues in the face of competition from bitcoin would require dissuading some or all users from transacting with bitcoin when, by their own assessments, bitcoin is the preferred alternative. Hence, the costs of regulating bitcoin on these grounds—roughly equal to the losses that users experience from employing an inferior base money—could be quite large. As such, regulating bitcoin on the grounds that it would reduce revenues would almost certainly be inconsistent with the principle of efficient regulation.

Monetary Policy

Others are concerned that bitcoin will prevent the Federal Reserve from conducting monetary policy effectively.[64] Indeed, this is in part why Nobel Prize–winning economist Paul Krugman advanced the claim that “bitcoin is evil.”[65] The view is relatively straightforward: if individuals use bitcoin instead of dollars as money, the Federal Reserve will not be able to control the supply of money in circulation. There is some truth to this view. The supply of bitcoin is built into the Bitcoin protocol. A central monetary authority cannot control it. Moreover, the protocol cannot be modified without the consent of a majority of users on the system. And, at least for bitcoin, changes to the money supply rule are widely considered to be off the table.[66]

Many users like the money supply constraint embedded in the Bitcoin protocol. The protocol ensures that a predetermined amount of bitcoin enters the system every ten minutes. The precise amount of bitcoin created, which serves as a reward for those processing transaction blocks, is cut in half roughly every four years. Prior to November 2012, the reward totaled 50 bitcoin. Later it was halved to 25 and again to 12.5. Roughly every two weeks, the system confirms that a block of transactions was processed every ten minutes on average. It then adjusts the difficulty of the cryptographic problem required to process transactions to ensure that the ten-minute processing time is achieved. Since new bitcoin are only created when a block is processed, the supply grows steadily at a declining rate over time.

There are at least two problems with the view that bitcoin undermines the Federal Reserve's ability to conduct monetary policy, thereby generating macroeconomic instability. First, bitcoin will have little effect on macroeconomic fluctuation if the dollar continues to function as the actual or effective unit of account.[67] Textbook models of macroeconomic fluctuation depend on so-called sticky prices that do not adjust instantaneously. If prices are denominated in dollars, the Federal Reserve will not lose control of monetary policy.

It seems likely that the dollar will continue to serve as the unit of account. Most bitcoin transactions at present involve goods or services actually priced in dollars, with the transaction being made at the current market rate. One entrepreneur has even developed digital price tags that update the bitcoin-price of products at current market rates, given the dollar prices chosen by merchants.[68] Hence, even when bitcoin prices are employed, the dollar often continues to function as the effective unit of account. If such a state persists, one need not be concerned that bitcoin will generate undesirable macroeconomic fluctuation.

Second, the Fed only loses control of monetary policy to the extent that individuals choose to switch from dollars to bitcoin. Considering that network effects favor the incumbent money, such a switch would indicate that the net gains from switching to bitcoin are perceived to be large.[69] Such gains would be large, for example, if the Federal Reserve were not very good at managing the money supply. But, in this case, the Federal Reserve could discourage the switch by committing to offer better monetary policy. In this view, bitcoin would function as a desirable check on monetary mischief.

The potential effect of bitcoin on monetary policy ranges from inconsequential to serving as a desirable check on the monetary authority. In the former case, there are no gains from regulating bitcoin on these grounds. In the latter case, regulation would almost certainly reduce the attractiveness of monetary policy. Hence, bitcoin should be welcomed on the grounds of promoting monetary stability.

CONCLUSION

Bitcoin—and the blockchain technology at its core—offers users many benefits over existing alternatives. When considering regulation, then, one should think carefully about the likely costs and benefits. I have reviewed the three principal justifications for regulating bitcoin. The scope for efficient regulation is limited in two ways. First, private governance structures and fee-based services have already begun addressing many of the known problems, such as protecting consumers from volatile exchange rates and preventing them from losing access to their accounts. As such, the benefits from regulation are typically low. Second, since most regulations would have the (intended or unintended) consequence of discouraging use, the costs—in terms of technological gains forgone—are potentially high. Nonetheless, there seems to be some scope for regulation in the provision of information and requirement of registration, thereby ensuring one has recourse in the event of theft.

Regulators interested in efficient regulation would do well to follow certain guidelines.

1. **Clarify the regulatory framework.** Provided that the gains from bitcoin are as large as many proponents believe, entrepreneurs can find ways to work within a wide range of regulatory frameworks. However, they cannot move forward confidently until the regulatory framework is settled.[70] Much clarity is needed, at the moment, over (1) who the appropriate regulators are, (2) what existing rules apply to bitcoin, and (3) what future rules are likely to be adopted. Clarity along these lines will enable entrepreneurs to take the requisite actions today. It will also allow users to make a more informed decision regarding whether the currency will be useful for their desired ends.
2. **Regulate transactions—not the transactions medium.** To the extent that some transactions and transfers are deemed undesirable, the

government should attempt to prevent them, at least insofar as the benefits of preventing them exceed the costs. However, the government should attempt to prevent these transactions without criminalizing the transactions medium. In the case of drug transactions, for example, that means buy-busts and monitoring similar to that currently employed for such transactions traditionally made in cash. Attempting to prevent such transactions by regulating the transactions medium imposes costs on legitimate users while having little effect on criminal users.

3. **Regulate exchanges—not users, miners, mining pool administrators, or software developers.** Many of the benefits of regulation can be realized by merely requiring large exchanges to register and collect identifying information on users exchanging bitcoin. Moreover, since such enterprises are large nodes in the bitcoin system, the costs of regulating them are probably low. Regulations that discourage users from adopting bitcoin, miners from processing blocks of transactions, or software developers from offering new programs to track, store, or transfer bitcoin, by contrast, are likely to impose large costs. As such, the latter should be avoided.
4. **Err on the side of technological progress.** Technological change is the primary driver of economic growth. New technologies are often disruptive, but entrepreneurs often react to these growing pains by making improvements to the underlying technology or developing ancillary products and services to ease the transition. Regulators should encourage technological progress by committing to an environment of *permissionless innovation*.[71] Reaffirm that those who venture out in search of better ways of doing things will be rewarded when they succeed. And, to the extent possible, reduce the barriers to such ventures.

Bitcoin is still in its infancy. Over the last seven years, users have joined the network; exchanges have made it easier to enter and exit; e-wallet services have made it more convenient to store and transact with bitcoin; miners have found ways to lower costs of processing transactions; and entrepreneurs more generally have developed a host of products in the bitcoin system. There are still problems with the bitcoin system—it is far from perfect. Some of these problems can and will be addressed with additional innovation. Others will, no doubt, require regulation. However, in pursuing the latter, one would do well to keep an eye to the future. Regulators should not let the minor problems of today justify preventing major gains in the future. Instead, regulators should aim to adopt only those regulations that deliver large benefits at a low cost.

NOTES

1. Higgins, "Bitcoin Panel Seeks New Take."
2. Rizzo, "Breaking Down New York's Latest BitLicense Revision."
3. FinCEN, "Application of FinCEN's Regulations."
4. CFTC, "CFTC Orders Bitcoin Options Trading Platform Operator."
5. SEC, "SEC Charges Bitcoin Mining Companies."
6. This need not imply that all consumers will be treated poorly; nor that all firms will engage in unscrupulous practices. It merely states that, in the absence of regulation, some firms will take advantage of some consumers. Of course, some firms might continue to take advantage of some consumers in the presence of regulation—though those employing the naïve justification often overlook this prospect.
7. The NAAG separates security issues into "hacking of virtual wallets or Bitcoin platforms" and "fraudulent transactions." Both are considered in this chapter under the general heading Security Concerns. NAAG, "An Explanation of Bitcoin."
8. All exchange rate data used herein comes from BitcoinCharts.com.
9. The Bitcoin Volatility Index measures volatility as the standard deviation of daily returns for the preceding thirty- and sixty-day windows. Dourado, "Bitcoin Volatility Index."
10. On the network effects problem as it pertains to bitcoin, see Luther, "Cryptocurrencies."
11. See Brito and Dourado, "Comments to the New York Department of Financial Services." Under New York's proposal, for example, it was "unclear whether individual cryptocurrency miners would be required to obtain a BitLicense" (4); whether software wallets and multisignature wallets are engaged in Virtual Currency Business Activity (VCBA) and, hence, are subject to regulation as such (5–6); whether introducing an AltCoin constitutes VCBA (10); what criteria will be employed by the superintendent to offer exemptions to chartered banks (13); whether exempted banks are subject to custodial limitations (14); and so on.
12. Luther and White, "Can Bitcoin Become a Major Currency?"
13. At the moment, fees are in the neighborhood of 1 percent of the transaction value—much less than traditional merchant accounts. Some, like BitPay, have forgone fees based on transaction value in favor of a flat annual or monthly fee.
14. Brito, "Benefits and Risk of Bitcoin," 3.
15. This distribution scheme prevails because computing power determines the likelihood of success.
16. "Virtual currencies are targets for highly sophisticated hackers, who have been able to breach advanced security systems." CFPB, "Risks to Consumers."
17. The CFPB warns that the blockchain "is maintained by vast unidentified private computer networks spread all over the world. It is possible that elements of these networks could abuse

the power that comes with maintaining the ledger, for example by undoing transactions that you thought were finalized." See ibid.

18. In its 2014 consumer advisory, the CFPB states, "If you store your virtual currency yourself" and "you lose your private keys, you have lost all access to your funds." Moreover, "virtual currency wallet companies may disclaim responsibility for replacing your virtual currency if it is stolen on their watch." See ibid.

19. Kaminsky, "I Tried Hacking Bitcoin."

20. Algorithmic governance refers to the actual code, which limits what users in the bitcoin network can do. Open source governance refers to the formal rules and informal norms that have emerged between Bitcoin Core developers, other developers, miners, and users. For a full discussion of these issues, see Dourado and Brito, "Cryptocurrency."

21. Berkman, "What Is a 51 Percent Attack?"

22. Indeed, Dourado and Brito ("Cryptocurrency," 5–6) "observe some self-regulation by the mining pools, which are heavily invested in the success of Bitcoin. Whenever the top pool starts to approach 40% or so of computing power of the network, some participants exit the pool and join another one."

23. Goodin, "Bitcoin Security Guarantee."

24. Farivar, "After Reaching 51% Network Power."

25. Smith, "GHashi.io Is Open for Discussion."

26. Hornyak, "One Group Controls 51 Percent."

27. Dourado and Brito, "Cryptocurrency," 4.

28. Sparkes, "The £625m Lost Forever."

29. "List of Major Bitcoin Heists."

30. While considering the role governments might play in *preventing* bitcoin thefts, it is also worth noting that government officials have *perpetrated* bitcoin thefts. In August 2015, former Secret Service agent Shaun Bridges plead guilty to money laundering and obstruction charges in connection with the theft of more than $800,000 in bitcoin. He is suspected of additional thefts as well. Higgins, "US Prosecutors Believe Ex–Secret Service Agent."

31. Victims of theft are not limited to relatively inexperienced or unsophisticated users. See, for example, Brandom, "Anatomy of a Hack."

32. Rizzo and Southurst, "Mt. Gox Allegedly Loses $350 Million."

33. Stucky and Adelstein, "Japanese Bitcoin Heist."

34. Edwards, "Thief Is Attempting to Hide $100 Million."

35. Meiklejohn et al., "Fistful of Bitcoins."

36. Dourado and Brito, "Cryptocurrency," 7.

37. As with cash, transactions with bitcoin can be charged back when an escrow service is employed; see Dourado, "Stop Saying Bitcoin Transactions Aren't Reversible." Indeed, the company Bitrated offers such a service; see Perez, "How Bitrated Wants to Put the Trust."

38. Maltby, "Chargebacks Create Business Headaches."

39. Wile, "Brooklyn Bodega Owner."

40. Brito, "Benefits and Risk of Bitcoin," 2.

41. Love, "Guy Who Owns a Bitcoin-Only Electronics Store."

42. Brito, "Beyond Silk Road."

43. Wolf, "Bitcoin Exchanges."

44. Greenberg, "Senator Calls for Bitcoin Ban."

45. Edwards, "CLAIM."

46. Brantly, "Financing Terror Bit by Bit."

47. Dougherty and Farrell, "Treasury's Cohen Sees."

48. Chen, "Underground Website."

49. Christin, "Traveling the Silk Road," 213–24.

50. These estimates, reported by Brito, "Beyond Silk Road," 2n2, are based on a forthcoming study by Nicolas Christin that is not publicly available at present. Brito also explains why estimates put forward by the FBI in the criminal complaint against Ross William Ulbricht overstate the volume of transactions.

51. For comparison, annual revenues at Amazon totaled $74.45 billion in 2013. At roughly $6.2 billion per month, that is more than 370 times the highest monthly transaction volume estimated for the Silk Road.

52. Figures calculated by author using data from "Estimated USD Transaction Value," Blockchain.info, last modified October 26, 2016, https://blockchain.info/charts/estimated-transaction-volume-usd?timespan=all.

53. Luther, "Dark Dollar Dealings."

54. Feige, "New Estimates of U.S. Currency Abroad."

55. Luther, "Dark Dollar Dealings."

56. Indeed, some exchanges already seem to be cooperating. See Sparshott, "Bitcoin Exchange Makes Apparent Move."

57. Brito and Castillo, *Bitcoin*, 26–27.

58. Stross, "Why I Want Bitcoin to Die."

59. Feige and Cebula, "America's Underground Economy."

60. Bitcoin might make it easier to hide more of one's wealth in financial assets. But that wealth is only valuable insofar as it can be exchanged for other goods and services. Suggesting that bitcoin will have a significant effect on tax evasion amounts to claiming individuals are able to hide a significantly larger portion of their purchases. Given that just a little less than one-fifth of income is going unreported already, that seems unlikely.

61. Davies, "Bitcoin."

62. Hendrickson, Hogan, and Luther, "Political Economy of Bitcoin."

63. Luther, "Cryptocurrencies," 30–34, discusses bitcoin's prospects as a niche currency.

64. Note that such a view implicitly accepts that the Fed is able to conduct monetary policy effectively in the absence of bitcoin. The historical record raises doubts on this point. See Selgin, Lastrapes, and White, "Has the Fed Been a Failure?"

65. Krugman, "Bitcoin Is Evil." A vice president of the Federal Reserve Bank of St. Louis has acknowledged that "the threat of Bitcoin (and of currency substitutes in general) places constraints on monetary policy"; see Andolfatto, "Bitcoin and Central Banking." Similarly, a

representative of the Bank of Canada has warned that, if bitcoin were widely adopted, "central banks would struggle to implement monetary policy"; see Higgins, "Bank of Canada."

66. Dourado and Brito, "Cryptocurrency," 5.

67. Ibid., 6.

68. Luther and White, "Can Bitcoin Become a Major Currency?"

69. Luther, "Cryptocurrencies."

70. Some banks have refused to work with bitcoin companies, citing regulatory uncertainty; see Rizzo, "Bank Stops Working with Bitcoin Exchange." Bitcoin ATMs have also been halted; Rizzo, "Bitcoin ATM Shutdown."

71. Thierer, *Permissionless Innovation*.

REFERENCES

Andolfatto, David. "Bitcoin and Central Banking." *MacroMania*, November 12, 2015. http://andolfatto.blogspot.com/2015/11/bitcoin-and-central-banking.html.

Berkman, Fran. "What Is a 51 Percent Attack, and Why are Bitcoin Users Freaking Out about It Now?" *The Daily Dot*, June 13, 2014. http://www.dailydot.com/business/bitcoin-51-percent-attack/.

Brandom, Russell. "Anatomy of a Hack: A Step-by-Step Account of an Overnight Digital Heist." *The Verge*, March 4, 2015. http://www.theverge.com/a/anatomy-of-a-hack.

Brantly, Aaron. "Financing Terror Bit by Bit." *CTC Sentinel*, October 31, 2014. https://www.ctc.usma.edu/posts/financing-terror-bit-by-bit.

Brito, Jerry. "Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies." Testimony before the Senate Committee on Homeland Security and Governmental Affairs, Mercatus Center at George Mason University, Arlington, VA, November 18, 2013.

———. "Benefits and Risk of Bitcoin for Small Businesses." Testimony before the House Committee on Small Business, Mercatus Center at George Mason University, Arlington, VA, April 2, 2014.

Brito, Jerry, and Andrea Castillo. *Bitcoin: A Primer for Policymakers*. Arlington, VA: Mercatus Center at George Mason University, 2013.

Brito, Jerry, and Eli Dourado. "Comments to the New York Department of Financial Services on the Proposed Virtual Currency Regulatory Framework." Public Interest Comment, Mercatus Center at George Mason University, Arlington, VA, August 14, 2014.

Bureau of Consumer Financial Protection (CFPB). "Risks to Consumers Posed by Virtual Currencies." *Consumer Advisory*, August 11, 2014. http://files.consumerfinance.gov/f/201408_cfpb_consumer-advisory_virtual-currencies.pdf.

Chen, Adrien. "The Underground Website Where You Can Buy Any Drug Imaginable." *Gawker*, June 1, 2011. http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160.

Christin, Nicolas. "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace." Proceedings of the 22nd International World Wide Web Conference, May 2013.

Davies, Gavyn. "Bitcoin: Miracle or Madness?" *Financial Times*, January 19, 2014. http://blogs.ft.com/gavyndavies/2014/01/19/bitcoin-miracle-or-madness/.

Dougherty, Carter, and Greg Farrell. "Treasury's Cohen Sees No Widespread Criminal Bitcoin Use." *Bloomberg*, March 18, 2014. http://www.bloomberg.com/news/articles/2014-03-18/treasury-s-cohen-says-regulation-helps-virtual-currencies.

Dourado, Eli. "Stop Saying Bitcoin Transactions Aren't Reversible." *Eli Dourado*, December 4, 2013. https://elidourado.com/blog/bitcoin-arbitration/.

———. "The Bitcoin Volatility Index." Retrieved March 26, 2015. https://btcvol.info/.

Dourado, Eli, and Jerry Brito. "Cryptocurrency." In *The New Palgrave Dictionary of Economics Online Edition*, edited by Steven N. Durlauf and Lawrence E. Blume. New York: Palgrave Macmillan, 2014.

Edwards, Jim. "CLAIM: Bitcoin Is Basically for Criminals." *Business Insider*, November 27, 2013. http://www.businessinsider.com/claim-bitcoin-is-basically-for-criminals-2013-11.

———. "A Thief Is Attempting to Hide $100 Million in Stolen Bitcoins—and You Can Watch It Live Right Now." *Business Insider*, December 3, 2013. http://www.businessinsider.com/a-thief-is-attempting-to-hide-100-million-in-stolen-bitcoins-and-you-can-watch-it-live-right-now-2013-12.

Farivar, Cyrus. "After Reaching 51% Network Power, Bitcoin Mining Pool Says 'Trust Us.'" *Ars Technica*, June 16, 2014.

Feige, Edgar L. "New Estimates of U.S. Currency Abroad, the Domestic Money Supply and the Unreported Economy." MPRA Paper No. 34778, Munich Personal RePEc Archive, September 2011.

Feige, Edgar L., and Richard Cebula. "America's Underground Economy: Measuring the Size, Growth and Determinants of Income Tax Evasion in the US." MPRA Paper No. 29672, Munich Personal RePEc Archive, January 2011.

Financial Crimes Enforcement Network (FinCEN). "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies." Guidance FIN-2013-G001, March 18, 2013. http://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

Goodin, Dan. "Bitcoin Security Guarantee Shattered by Anonymous Miner with 51% Network Power." *Ars Technica*, June 15, 2014. http://arstechnica.com/security/2014/06/bitcoin-security-guarantee-shattered-by-anonymous-miner-with-51-network-power/.

Greenberg, Andy. "Senator Calls for Bitcoin Ban in Letter to Financial Regulators." *Forbes*, February 26, 2014. http://www.forbes.com/sites/andygreenberg/2014/02/26/senator-calls-for-bitcoin-ban-in-letter-to-financial-regulators/.

Hendrickson, Joshua R., Thomas L. Hogan, and William J. Luther. "The Political Economy of Bitcoin." *Economic Inquiry* 54, no. 2 (2016): 925–39.

Higgins, Stan. "Bitcoin Panel Seeks New Take on Regulation at New Jersey Hearing." *CoinDesk*, February 6, 2015. http://www.coindesk.com/bitcoin-panel-regulation-redo-new-jersey/.

———. "Bank of Canada: Bitcoin Could Create 'New Monetary Order.'" *CoinDesk*, November 16, 2015. http://www.coindesk.com/bank-of-canada-chief-bitcoin-monetary-policy/.

———. "US Prosecutors Believe Ex–Secret Service Agent Stole More Bitcoin from Silk Road." *CoinDesk*, February 24, 2016. http://www.coindesk.com/us-government-secret-service-agent-stole-silk-road-bitcoins/.

Hornyak, Tim. "One Group Controls 51 Percent of Bitcoin Mining, Threatening Security Sanctity." *PCWorld*, June 16, 2014. http://www.pcworld.com/article/2364000/bitcoin-price-dips-as-backers-fear-mining-monopoly.html.

Kaminsky, Dan. "I Tried Hacking Bitcoin and I Failed." *Business Insider*, April 12, 2013. http://www.businessinsider.com/dan-kaminsky-highlights-flaws-bitcoin-2013-4.

Krugman, Paul. "Bitcoin Is Evil." *New York Times*, December 28, 2013. http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/?_r=0.

"List of Major Bitcoin Heists, Thefts, Hacks, Scams, and Losses." *Bitcoin Forum*, April 19, 2014, posted by "dree12." https://bitcointalk.org/index.php?topic=576337#post_toc_71.

Love, Dylan. "A Guy Who Owns a Bitcoin-Only Electronics Store Is Revealing Everything on Reddit." *Business Insider*, March 18, 2014. http://www.businessinsider.com/e-commerce-with-bitcoin-2014-3.

Luther, William J. "Dark Dollar Dealings." *U.S. News & World Report*, February 23, 2015. http://www.usnews.com/opinion/economic-intelligence/2015/02/23/us-has-no-business-regulating-bitcoin-because-of-illegal-dealings.

———. "Cryptocurrencies, Network Effects, and Switching Costs." *Contemporary Economic Policy* 34, no. 3 (2016): 553–71.

Luther, William J., and Lawrence H. White. "Can Bitcoin Become a Major Currency?" *Cayman Financial Review*, August 8, 2014. http://www.compasscayman.com/cfr/2014/08/08/Can-bitcoin-become-a-major-currency-/.

Maltby, Emily. "Chargebacks Create Business Headaches." *Wall Street Journal*, February 10, 2011. http://www.wsj.com/articles/SB10001424052748704698004576104554234202010.

Meiklejohn, Sarah, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage. "A Fistful of Bitcoins: Characterizing Payments among Men with No Names." *;login:* 38, no. 6 (December 2013): 10–14.

National Association of Attorneys General (NAAG). "An Explanation of Bitcoin and Its Implications for Consumer Protection." *NAAGazette* 8, no. 6–7 (July 24, 2014). http://www.naag.org/publications/naagazette/volume-8-number-6/an-explanation-of-bitcoin-and-its-implications-for-consumer-protection.php.

Perez, Yessi Bello. "How Bitrated Wants to Put the Trust Back in Bitcoin." *CoinDesk*, April 12, 2015. http://www.coindesk.com/how-bitrated-is-aiming-to-put-trust-back-in-bitcoin/.

Rizzo, Pete. "Bank Stops Working with Bitcoin Exchange CampBX Due to 'Regulatory Uncertainty.' " *CoinDesk*, February 1, 2015. http://www.coindesk.com/bank-stops-working-bitcoin-exchange-campbx-regulatory-uncertainty/.

———. "Breaking down New York's Latest BitLicense Revision." *CoinDesk*, February 5, 2015. http://www.coindesk.com/breaking-down-new-york-bitlicense-revision/.

———. "Bitcoin ATM Shutdown Spotlights Regulatory Uncertainty in Vermont." *CoinDesk*, February 17, 2015. http://www.coindesk.com/bitcoin-atm-shutdown-regulation-vermont/.

Rizzo, Pete, and Jon Southurst. "Mt. Gox Allegedly Loses $350 Million in Bitcoin (744,400 BTC), Rumoured to Be Insolvent." *CoinDesk*, February 25, 2014. http://www.coindesk.com/mt-gox-loses-340-million-bitcoin-rumoured-insolvent/.

Selgin, George, William D. Lastrapes, and Lawrence H. White. "Has the Fed Been a Failure?" *Journal of Macroeconomics* 34, no. 3 (2012): 569–96.

Smith, Jeffrey. "GHashi.io Is Open for Discussion." GHashi.io Press Release, June 16, 2014. http://www.scribd.com/doc/229951141/GHash-Press-Release-June-16-2014.

Sparkes, Matthew. "The £625m Lost Forever—The Phenomenon of Disappearing Bitcoins." *Telegraph*, January 23, 2015. http://www.telegraph.co.uk/technology/news/11362827/The-625m-lost-forever-the-phenomenon-of-disappearing-Bitcoins.

Sparshott, Jeffrey. "Bitcoin Exchange Makes Apparent Move to Play by U.S. Money-Laundering Rules." *Wall Street Journal*, June 28, 2013. http://online.wsj.com/article/SB10001424127887323873904578574000957464468.html.

Stross, Charlie. "Why I Want Bitcoin to Die in a Fire." *Charlie's Diary*, December 18, 2013. http://www.antipope.org/charlie/blog-static/2013/12/why-i-want-bitcoin-to-die-in-a.html.

Stucky, Nathalie-Kyoko, and Jake Adelstein. "Japanese Bitcoin Heist 'an Inside Job,' Not Hackers Alone." *The Daily Beast*, December 31, 2014. http://www.thedailybeast.com/articles/2014/12/31/japanese-bitcoin-heist-an-inside-job-not-hackers-alone.html.

Thierer, Adam. *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom, Revised and Expanded Edition*. Arlington, VA: Mercatus Center at George Mason University, 2016.

US Commodity Futures Trading Commission. "CFTC Orders Bitcoin Options Trading Platform Operator and Its CEO to Cease Illegally Offering Bitcoin Options and to Cease Operating a Facility for Trading or Processing of Swaps without Registering." Press Release, September 17, 2015. http://www.cftc.gov/PressRoom/PressReleases/pr7231-15.

US Securities and Exchange Commission. "SEC Charges Bitcoin Mining Companies." Press Release 2015-271, December 1, 2015.

Wile, Rob. "A Brooklyn Bodega Owner Told Us Why All Merchants Should Start Accepting Bitcoin." *Business Insider*, November 11, 2013. http://www.businessinsider.com/brooklyn-bitcoin-bodega-2013-11.

Wolf, Brett. "Bitcoin Exchanges Offer Anti-Money-Laundering Aid." *Reuters*, June 15, 2011. http://www.reuters.com/article/2011/06/15/financial-bitcoin-idUSN1510930920110615.