BitCoin: The Case Against Strict Regulation

Michael Sherlock[*]

Abstract

BitCoin is an innovative technology that offers several benefits, such as fast transaction speeds, low costs, and the elimination of the need for a third-party intermediary to process transactions. Unfortunately, BitCoin has faced resistance from regulators because the technology has been used for nefarious purposes, including online drug purchases and Ponzi schemes. This note provides a basic explanation of how BitCoin works and is currently regulated on federal and state levels. This note argues that BitCoin should not be forced into old regulatory frameworks that do not adequately balance security concerns with the benefits of BitCoin. BitCoin should not be regulated at the federal level. Instead, state regulations should focus on BitCoin providers that can unilaterally transfer or block transfers of BitCoin on behalf of users. State regulators should require such providers to register with their given states, maintain adequate books and records, implement advanced cyber security standards, conduct audits of their operations, and submit reports to state regulators. In crafting these regulations, regulators should keep in mind that vague or poorly drafted regulations will chill innovation.

Table of Contents

I.   Introduction

Satoshi Nakamoto created the virtual currency called BitCoin in early 2009.[1] BitCoin is digital money that is not backed by the government,[2] and is treated as currency and used to purchase goods and services.[3] It is a collection of computer code that is stored either digitally or, in rare cases, in printed form.[4] Many benefits of BitCoin explain its growing popularity. First, BitCoin allows individuals to anonymously purchase goods and services online.[5] Further, BitCoin technology results in faster, transactions that are less costly than traditional monetary transactions that require third-party intermediaries.[6] Moreover, BitCoin's centralized public ledger that records all BitCoin transactions reduces redundancies and inefficiencies.[7]

---

[1] Benjamin Wallace, *The Rise and Fall of Bitcoin*, Wired (Nov. 23, 2011, 2:52 PM), https://www.wired.com/2011/11/mf_bitcoin/ [https://perma.cc/N8EU-362P] ("Nakamoto himself mined the first 50 bitcoins—which came to be called the genesis block—on January 3, 2009.").

[2] Edward V. Murphy et al., Cong. Research Serv., R43339, Bitcoin: Questions, Answers, and Analysis of Legal Issues 1 (2015).

[3] *See, e.g.*, Jonas Chokun, *Who Accepts Bitcoins As Payment? List of Companies, Stores, Shops*, 99Bitcoins (June 19, 2016), https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/ [https://perma.cc/5339-MTWW] (listing online vendors who accept BitCoin as payment, including Overstock, Microsoft, and Dell).

[4] *See* Wallace, *supra* note 1 ("Some users protected their bitcoins by creating multiple backups, encrypting and storing them on thumb drives, on forensically scrubbed virgin computers without Internet connections, in the cloud, and on printouts stored in safe-deposit boxes.").

[5] *See What Can You Buy with Bitcoin?*, CoinDesk (Oct. 19, 2015), http://www.coindesk.com/information/what-can-you-buy-with-bitcoins/ [https://perma.cc/HA9G-ZAXT].

[6] *See* Kimberly Johnson & Blythe Masters, *What Blockchain Is and What It Can Do*, Wall St. J. (June 19, 2016), http://www.wsj.com/articles/what-blockchain-is-and-what-it-can-do-1466388185 [https://perma.cc/DYM5-4B89] (stating that the technology underpinning BitCoin can "cut a significant amount of cost out of the process of post-trade financial manufacturing and actually reduce risk because it reduces the time it takes to complete a financial transaction once it has been agreed in the marketplace").

[7] Since BitCoin requires only one ledger that is controlled by a decentralized network of computers, errors are reduced and costs are saved compared to the current "infrastructures that were designed and built 20 to 30 years ago."

However, as BitCoin has grown in popularity, so too has its use in nefarious activities.[8] The private nature of BitCoin provides an avenue for criminals to perpetrate white-collar crimes like tax evasion and money laundering.[9]

In addressing BitCoins' benefits and concerns, the U.S. government currently lags behind the evolving technology in its development of appropriate and concise regulations.[10] This note examines the various approaches regulators are employing, which include treating BitCoin as a security and as money under existing anti-money laundering statutes and state regulatory schemes.[11] This note also describes a proposed regime that balances the benefits of BitCoin with its security concerns.[12] This note argues that BitCoin should be regulated sparingly, with standard purchases in BitCoin not subject to regulation, and regulations imposed only on certain providers that can unilaterally transfer or block transfers of BitCoin on behalf of users.

Following this Introduction, Part II of this note explains the logistics of BitCoin technology and summarizes how BitCoins function as a virtual currency. Part III explores the benefits of BitCoin technology compared to traditional forms of online exchange. Part IV examines the risks associated with the use of BitCoin technology. Part V states the objectives of BitCoin and how such objectives are

---

Id. ("We're talking about billions of dollars in annual savings for the banking industry, and percentage points on capital ratios to be freed up.").

[8] *E.g.*, S.E.C. v. Shavers, No. 4:13–CV–416, 2014 WL 4652121, at *1 (E.D. Tex. Sept. 18, 2014) ("From February 2011 through August 2012, contrary to representations Shavers made to BTCST investors, BTCST was a sham and a Ponzi scheme, whereby Shavers used new bitcoins received from BTCST investors to make payments on outstanding BTCST investments and diverted BTCST investors' bitcoins for his personal use.").

[9] Primavera De Filippi, *We Must Regulate Bitcoin. Problem Is, We Don't Understand It*, WIRED (Mar. 1, 2016, 1:09 PM), http://wired.com/2016/03/must-understand-bitcoin-regulate [https://perma.cc/78W8-7M9T] ("Given this current lack of a central regulatory authority . . . [BitCoin] provides opportunities for criminal activities, including tax-evasion and money laundering.").

[10] *Cf. id.* ("The challenge is that most regulations today are defined by the product they are meant to regulate.").

[11] *See* discussion *infra* Parts VI & VII (summarizing each form of government's strategy for regulating BitCoin).

[12] *See* discussion *infra* Part VIII (recommending a new regulatory approach that is tailored to BitCoin).

paramount to BitCoin regulation. Part VI describes how BitCoin is classified and regulated at the federal level, and Part VII summarizes the current attempts to regulate BitCoin on a state level. Finally, this note concludes by arguing for a minimalist approach to BitCoin regulation.

II.   *Background: What is BitCoin?*

Internet transactions typically require financial intermediaries, such as banks, to ensure that buyers complete transactions.[13] These systems usually suffer from high transaction costs.[14] Satoshi Nakamoto created the theoretical framework for BitCoin and its underlying technologies[15] with the intention of fostering peer-to-peer transactions that did not require a "trusted third party" to facilitate payment.[16] BitCoin exists solely on the internet and is not backed by any tangible commodity or monetary system, although it can be exchanged for currencies, including the U.S. dollar.[17]

BitCoin technology functions in the following manner. BitCoin itself is "a chain of digital signatures"[18] that defines who holds (i.e., owns) the coin.[19] Each individual in the network has a unique wallet, similar to an account, which holds coins.[20] Wallets may

---

[13] *Cf.* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN 1 (Mar. 23, 2017), http://bitcoin.org/bitcoin.pdf [https://perma. cc/8DGC-THBR] ("A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.").

[14] Transaction costs are incredibly important to consider because these hidden costs, representing "the cost of reaching and enforcing bargains," impact whether transactions occur and whether markets for goods and services exist. *See* Wendy J. Gordon, *Fair Use as Market Failure: Markets, Market Failure and Rights of Use*, 82 COLUM. L. REV. 1600, 1628 (1982).

[15] *See* Wallace, *supra* note 1.

[16] *See* Nakamoto, *supra* note 13, at 1 (claiming BitCoin was created to be a system "based on cryptographic proof instead of trust . . . without the need of a trusted third party").

[17] *Meissner v. BF Labs Inc.*, No. 13–2617–RDR, 2014 WL 2558203, at *2 (D. Kan. June 6, 2014).

[18] Nakamoto, *supra* note 13, at 2.

[19] *Id.* In other words, a BitCoin is really just a long string of computer code that defines who currently holds the coin and all those who previously held the coin. *See id.* at 2.

[20] *See* Evan L. Greebel & Kathleen H. Moriarty, KATTEN MUCHIN ROSENMAN

be stored locally on an individual's own computer or on third-party servers.[21] Server storage makes the user's wallet accessible anywhere via the Internet.[22] Users download software onto their computers or smartphones to send BitCoins.[23] Each individual in the network has both a public and a private key.[24] The public key acts as a public address for assigning and holding coins, while the private key functions like a password, allowing users access and control only to coins that he or she holds.[25] In order to pass the BitCoin to a new holder, the current holder adds code to the coin, which memorializes the transaction and assigns the coin to the next holder's public key.[26]

       There are three ways in which individuals can acquire BitCoins.[27] First, users can exchange physical currency for BitCoins on BitCoin exchanges.[28] These exchanges function similarly to traditional currency exchanges, and allow individuals to exchange traditional currency for the equivalent value in BitCoin.[29] The exchange rate is determined solely by the market's value scale of BitCoin on any given day because there is no commodity backing BitCoin.[30] To acquire BitCoins through an exchange, users must visit an exchange, create an account, connect a bank account or credit card to the account,

---

LLP, *The Evolution of a New Asset Class*, LAW360 (Jan. 2, 2014, 6:04 PM), http://www.law360.com/articles/495823/the-evolution-of-a-new-asset-class [https://perma.cc/2WYW-PES2].

[21] Wallace, *supra* note 1.

[22] *See id.*

[23] *Frequently Asked Questions*, BITCOIN, https://bitcoin.org/en/faq#how-dif-ficult-is-it-to-make-a-bitcoin-payment [https://perma.cc/A92Z-8VNP]. In order to send a BitCoin, the transaction needs to be signed. *See How Does Bitcoin Work*, BITCOIN, https://bitcoin.org/en/how-it-works [https://perma.cc/HG4V-FP7E]. BitCoin wallets generate signatures that are unique to the coin, based on the private key. *Id.* The Blockchain will only accept a transfer of a particular coin if the signature is correct. *Id.*

[24] Greebel & Moriarty, *supra* note 20.

[25] *See* Nakamoto, *supra* note 13, at 2.

[26] *Id*. The mechanics are similar to that of a standard transaction where a user takes money from his or her wallet and exchanges it for goods or services. Greebel & Moriarty, *supra* note 20.

[27] *See* MURPHY ET AL., *supra* note 2, at 2.

[28] *See id.* (listing exchanges including "Okcoin, Coinbase, and Kraken").

[29] *See id.*

[30] *How Can I Buy Bitcoins?*, COINDESK (Oct. 28, 2015), http://www.coindesk.com/information/how-can-i-buy-bitcoins/ [https://perma.cc/2JE3-XXQD].

exchange currency for a corresponding amount of BitCoins, and then store the BitCoins in their wallets.[31]

Second, individuals can acquire BitCoins by trading a good or service for compensation in BitCoin.[32] In this scenario, buyers merely append the seller's public key to a BitCoin the buyer holds.[33] Once the seller has the coin in his or her wallet, payment is complete.

Third, users can acquire new BitCoins by using their computer to verify BitCoin transactions.[34] This method of acquiring BitCoins is known as mining.[35] Through this process, a BitCoin user is compensated with twenty-five BitCoins when he or she uses a computer, either with or without optimized computer hardware designed for mining, to solve a complex mathematical problem that verifies a BitCoin transaction.[36] After a transaction has been verified, it is recorded on the BitCoin network.[37] These computations ensure that the entire chain of transactions is accurate and absent of any fraudulent activity.[38] Mining for new BitCoins becomes progressively more resource and time intensive, because the computations become increasingly difficult.[39]

---

[31] *Id.*

[32] *Id.*

[33] *See* Greebel & Moriarty, *supra* note 20.

[34] *Id.* Individuals interested in serious BitCoin mining are more likely to purchase optimized computer hardware designed specifically for mining. *See, e.g.*, *Getting started with Bitcoin mining*, Bɪᴛᴄᴏɪɴᴍɪɴɪɴɢ.ᴄᴏᴍ, https://www.bitcoinmining.com/getting-started/ [https://perma.cc/AXP5-X9JC].

[35] *Id.*

[36] *How Bitcoin Mining Works*, CᴏɪɴDᴇsᴋ (Dec. 22, 2014), http://www.coindesk.com/information/how-bitcoin-mining-works/ [https://perma.cc/TW3H-T5LQ].

[37] *See id.*

[38] *See id*. For a more technical explanation of this mathematical process, see Morgen Peck, *The Future of the Web Looks a Lot Like Bitcoin*, IEEE: Sᴘᴇᴄ-ᴛʀᴜᴍ (July 1, 2015, 7:00 PM), http://spectrum.ieee.org/computing/networks/the-future-of-the-web-looks-a-lot-like-bitcoin   [https://perma.cc/VA9X-JR3S].

[39] *How Bitcoin Mining Works*, *supra* note 36 ("The bitcoin network has to make it more difficult, otherwise everyone would be hashing hundreds of transaction blocks each second, and all of the bitcoins would be mined in minutes."). Note that the number of BitCoins in circulation is artificially capped at 21 million coins in order to stabilize the supply and combat inflation. *See* Mᴜʀᴘʜʏ ᴇᴛ ᴀʟ., *supra* note 2, at 2–6.

One incentive to mine is an optional transaction fee that applies to 97 percent of BitCoin transactions, and is often priced at .0001 BitCoin.[40]

       The Blockchain is a public ledger that records all BitCoin transactions.[41] Miners power the Blockchain,[42] and after they solve and verify the computations, the Blockchain reflects the transaction.[43] This process helps ensure that only legitimate transactions are recorded.[44] The Blockchain also mitigates the risk of users double spending their BitCoins.[45] A double-spend fraud could only theoretically be perpetrated on the Blockchain if a fraudulent user possessed an incredible amount of computer processing power.[46] More precisely, the fraudulent user would need enough computing power not only to resolve the math problems used in processing a particular coin, but also enough power to solve all subsequent math problems in the sequence at a faster rate than all the other non-fraudulent users.[47] This is most likely impossible, but at a minimum extremely unlikely.[48] Accordingly, one of the many benefits of BitCoin is that BitCoin transactions are inherently safe.

III.   Benefits of BitCoin Technology

A.   Decreased Transaction Time and Costs

       BitCoin transactions, unlike other transfers, can close quickly in about ten minutes, whether they are domestic or international.[49] This is drastically shorter than international wire transfers that can

---

[40] Rainer Böhme et al., *Bitcoin: Economics, Technology, and Governance*, 29 J. ECON. PERSPECTIVES 213, 218 (2015).

[41] Greebel & Moriarty, *supra* note 20.

[42] *See* Nakamoto, *supra* note 13, at 2–3.

[43] *See id.* at 3 ("Nodes accept the block only if all transactions in it are valid and not already spent.").

[44] *See* Peck, *supra* note 37.

[45] *See id*. at 2.

[46] *See* Nakamoto, *supra* note 13, at 3 (explaining the technical background of the Blockchain that minimizes the risk of double spending).

[47] *Id.* ("If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes.").

[48] *Id.*

[49] *Id.*

take several days.[50] BitCoin also reduces transaction costs[51] (i.e., the costs of doing business).[52] Blockchain technologies "cut a significant amount of cost out of the process of post-trade financial manufacturing and actually reduce risk because it reduces the time it takes to complete a financial transaction once it has been agreed in the marketplace."[53] Blockchain technologies are particularly cost saving where "coordination of activity and the exchange of value" occur.[54]

There are two primary transaction costs that merchants normally pay when making internet purchases.[55] The first is the fee paid to a trusted third party, such as a bank or credit card company, which serves as an intermediary in order to validate the transaction.[56] These fees occur each time a purchase is made and become expensive in the aggregate.[57] By contrast, BitCoins allow individuals to transact amongst themselves without a third-party intermediary and avoid this expense.[58]

The second significant transaction cost comes from the uncertainty associated with transaction reversibility or, in other words, the ability to return or cancel a transaction.[59] Chargebacks make reversibility more expensive in traditional transactions than in

---

[50] Jerry Brito et al., *Bitcoin Financial Regulation: Securities, Derivatives, Prediction Markets, and Gambling*, 16 Colum. Sci. & Tech. L. Rev. 144, 151 (2014).

[51] *Cf.* Johnson & Masters, *supra* note 6 (explaining how Blockchain technology can "cut a significant amount of cost out of the process of post-trade financial manufacturing").

[52] These include costs associated with time, risk, and procedural concerns. Paul M. Johnson, *Transaction Costs*, *in* A Glossary of Political Economy Terms, http://www.auburn.edu/~johnspm/gloss/transaction_costs [https://perma.cc/JG6J-HUDR].

[53] Johnson & Masters, *supra* note 6.

[54] *Id.*

[55] Murphy et al., *supra* note 2, at 5.

[56] *See id.*

[57] *See, e.g.*, Ben Dwyer, *Credit Card Processing Fees & Rates*, CardFellow, https://www.cardfellow.com/credit-card-processing-fees/ ("Visa, MasterCard and Discover make money by charging assessments on every transaction involving one of their credit cards . . . . In January 2015, Visa raised its assessment on credit volume from 0.11% to 0.13%.").

[58] *See supra* notes 16–17 and accompanying text (explaining the peer-to-peer design of Bitcoin).

[59] Murphy et al., *supra* note 2, at 5 (stating that reversibility concerns are costly for merchants).

BitCoin transactions.[60] A chargeback occurs when a bank removes a charge from its customer's account.[61] When a chargeback occurs, the merchant is not paid for the good or service it provided.[62] Additionally, credit card networks charge merchants 3 to 4 percent of the amount of a transaction, while BitCoin transactions may cost less than 1 percent.[63] Merchants account for the risk of not being paid and for the fees charged by credit card companies by embedding transaction costs in the price of the good.[64] This shifts the expense of transaction costs, here a third-party intermediary and the risk of a chargeback, onto the consumer.[65] These transaction costs exist even if a merchant does not explicitly and separately bill for them.[66] However, BitCoin transactions are not reversible, and therefore bear no risk of merchants not receiving payment.[67] Because BitCoin transactions neither require a third-party intermediary nor run the risk of a chargeback, merchants' transaction costs are reduced.[68] By extension, at least theoretically, the costs passed onto consumers should also be reduced.[69]

B.   Security

In 2014, 8.6 million individuals were estimated to have experienced credit card fraud.[70] The Blockchain mitigates the risk of identity theft because in BitCoin transactions all parties' identities are anonymous.[71] Each party in a BitCoin transaction only knows the other

---

[60] *See id.*

[61] *See* Robin Edwards, *Exclusion of Cardholder Chargeback Rights*, 17 BOND L. REV. 47 (2005).

[62] *See id.* at 47–48.

[63] Brito et al., *supra* note 52, at 151.

[64] Merchants that have the power to set prices can include whatever factors they wish in the price of a good, such as labor, raw materials, and, pertinent here, transaction costs. *See* LUDWIG VON MISES, HUMAN ACTION: A TREATISE ON ECONOMICS 332 (Scholars ed., 1998).

[65] *Cf. id.*

[66] *Cf.* R.H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 15 (1960).

[67] MURPHY ET AL., *supra* note 2, at 5.

[68] Böhme et al., *supra* note 41, at 224. For example, in 2015 Overstock.com offered a one percent discount to consumers that paid in BitCoin. *Id.*

[69] *See* MURPHY ET AL., *supra* note 2, at 5.

[70] Press Release, Bureau of Justice Statistics, 17.6 Million U.S. Residents Experienced Identity Theft In 2014 (Sep. 27, 2015), http://www.bjs.gov/content/pub/press/vit14pr.cfm [https://perma.cc/QPF4-TY2J].

[71] *See* Nakamoto, *supra* note 13, at 6 ("The public can see that someone

party's digital identity and public key. Similarly, the Blockchain itself only shows a coin passing between two public keys; private identifying information about the parties is not disclosed.[72] For additional privacy, groups of BitCoin users can pool their transactions together to obfuscate the connection between specific buyers and sellers.[73] Also, from a data breach standpoint, there is no central currency storage location, akin to a financial institution, that can be robbed or hacked.[74] Rather, BitCoin is a string of computer data stored in a wallet either on a user's computer, webserver, or in printed form.[75]

   The Blockchain is also reliable.[76] It is "guaranteed to be safe and secure [and] everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer."[77] The only way to access and transfer a coin is with the private key.[78] The Blockchain checks the legitimacy of each coin before allowing it to be transferred

---

is sending an amount to someone else, but without information linking the transaction to anyone."). *But see* Murphy et al., *supra* note 2, at 3 ("Because of the public ledger, researchers have found that, using sophisticated computer analysis, transactions involving large quantities of Bitcoin can be tracked . . . .").

[72] *See, e.g.*, Nakamoto, *supra* note 13, at 6.

[73] This process is called mixing and involves pooling transactions together to disguise who sends BitCoins to whom. For example, "[t]o mislead an observer who tracks these payments, Alice and Charles could both pay a mixer 'Minnie' and provide additional confidential instructions for Minnie to pay Bob and Daisy one bitcoin each. An observer would see flows from Alice and Charles to Minnie, and from Minnie to Bob and Daisy, but would not be able to tell whether it was Alice or Charlie who sent money to Bob." Böhme et al., *supra* note 41, at 221.

[74] *See* Nakamoto, *supra* note 13, at 2 ("The problem with [the traditional] solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.").

[75] *See supra* notes 19–26 and accompanying text (discussing how Bitcoin is comprised of a string of computer code, and exists solely on the internet).

[76] *See* Michael Jackson, *Bitcoin's Big Challenge in 2016: Reaching 100 Million Users*, CoinDesk (Jan. 1, 2016, 4:34 PM), http://www.coindesk.com/2016-bitcoin-challenge-100-million-users/   [https://perma.cc/87FE-9BHJ].

[77] *Id.*

[78] *See supra* note 25 and accompanying text (analyzing the key system in maintaining privacy).

to another individual.[79] Again, the amount of computer power required to fraudulently alter the Blockchain is too high to pragmatically occur.[80] BitCoin transactions are protected by the underlying computing power of the Blockchain, rather than the security of a single financial institution.[81]

C.   Limited Inflation Concerns

Because BitCoin is not backed by a central government, monetary policy and its effects on inflation will not cause a decrease in BitCoins' purchasing power.[82] An artificial cap placed on the number of BitCoins in circulation helps curb inflation concerns.[83] This cap ensures a stable money supply, unlike a traditional government-backed currency that can be inflated by government intervention.[84] BitCoin is valued by market forces rather than government intervention.[85] The stability of the BitCoin supply, combined with the safety and reduced transaction speeds and costs of BitCoin transactions, make BitCoin a technology that should be supported, not stifled, by excessive regulation and government intervention.

---

[79] Each node checks the authenticity of a BitCoin before recording the transaction. *See supra* notes 43–46 and accompanying text (mentioning how Blockchain serves as a record of all BitCoin transactions).

[80] *See supra* notes 46–50 and accompanying text (discussing the ways that Blockchain promotes security).

[81] The only way to fraudulently modify the Blockchain would be with more computing than the summation of all honest computers in the Blockchain. *See supra* note 48–50 and accompanying text (discussing the near impossibility of fraudulently modifying the Blockchain).

[82] *See* MURPHY ET AL., *supra* note 2, at 6 ("Most often governments (or their central bank) regulate the supply of money and credit and most often some degree of mismanagement of this government function is at the root of a persistent high inflation problem.").

[83] *See id.*

[84] *Id.* ("[D]espite being a currency with no intrinsic value, the Bitcoin system's operation is similar to the growth of money under a gold standard . . . .").

[85] *Id.*

IV.   Risks Associated with BitCoin

A.   BitCoin Exchange Mismanagement

Although Blockchain technology is itself relatively secure, BitCoin exchanges may pose security risks to users.[86] BitCoin exchanges are critical to the BitCoin marketplace because they allow users to convert traditional currencies to BitCoin.[87] However, poorly managed BitCoin exchanges have a checkered history.[88] In 2014, Mt. Gox was the world's largest BitCoin exchange.[89] Although the exchange appeared to be functioning effectively, internally it was in disarray.[90] Mt. Gox suffered a minor technology flaw that impacted its ability to pay out BitCoins.[91] Mt. Gox did not employ "version control software—a standard tool in any professional software development environment."[92] After Mt. Gox filed for bankruptcy[93] it became clear that over $400 million worth of BitCoins were lost and stolen.[94] As of May 2016, 650 thousand BitCoins, worth $292 million, were still unaccounted for.[95] However, the Mt. Gox failure was a result of

---

[86] *See, e.g.*, Robert McMillan, *The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster*, WIRED (Mar. 3, 2014), http://www.wired.com/2014/03/bitcoin-exchange/ [https://perma.cc/SHF3-BYPZ].

[87] *See supra* notes 28–31 and accompanying text (discussing the role of Bit-Coin exchanges).

[88] *See* McMillan, *supra* note 88 ("From a distance, the world's largest bitcoin exchange looked like a towering example of renegade entrepreneurism. But on the inside, according to some who were there, Mt. Gox was a messy combination of poor management, neglect, and raw inexperience.").

[89] *Id.*

[90] *Id.*

[91] *Id.*

[92] *Id.* When developing code on a team, different programmers sometimes end up simultaneously working on the same code; version control software prevents overwriting "a colleague's code if they happened to be working on the same file." *Id.*

[93] *Id.*

[94] *Id.* However, it is important to remember that a BitCoin cannot be transferred unless someone has both the public key *and* private key. *See supra* notes 24–25 and accompanying text.

[95] Jake Adelstein & Nathalie-Kyoko Stucky, *Behind the Biggest Bitcoin Heist in History: Inside the Implosion of Mt. Gox*, DAILY BEAST (May 19, 2016, 1:00 AM), http://www.thedailybeast.com/articles/2016/05/19/behind-the-biggest-bitcoin-heist-in-history-inside-the-implosion-of-mt-gox.html [https://perma.

flawed programing and leadership, not an inherent flaw with BitCoin or Blockchain technology.[96]

B.   Nefarious Uses of Technology

BitCoin has been used to facilitate illegal transactions. For example, Silk Road was an online web store where users could use BitCoins to purchase guns, drugs, and other illegal items anonymously online.[97] Silk Road was a website where sellers sold goods and services, and buyers could read reviews of these goods and services before purchase.[98] The operators of Silk Road did not sell anything themselves, but rather provided a platform to connect suppliers and purchasers.[99]

Silk Road required the use of Tor, a service that hides buyers' and sellers' IP addresses.[100] The anonymous nature of BitCoin, coupled with the Tor requirement, fostered Silk Road's market for "contraband and narcotics."[101] Although the original Silk Road was

---

cc/Q334-QATW]. Recently, more details of the Mt. Gox fiasco have come to light. Apparently, eighty thousand coins, worth about $62,400 in April 2011, were stolen from Mt. Gox before Karpeles, the owner of Mt. Gox at the time of the bankruptcy, even purchased the exchange. *Id.* As BitCoin prices went up and the losses grew more expensive, Karpeles began taking coins offline by printing the BitCoins, which made Mt. Gox's accounting even more difficult to follow. *Id.*

[96] *See* McMillan, *supra* note 88 ("Mt. Gox was a messy combination of poor management, neglect, and raw inexperience.").

[97] *See* Benjamin Weiser & Matt Apuzzo, *Inquiry of Silk Road Website Spurred Agents' Own Illegal Acts, Officials Say*, N.Y. Times (Mar. 30, 2015), http://www.nytimes.com/2015/03/31/nyregion/silk-road-case-federal-agents-charges.html?_r=0 [https://perma.cc/RMC7-5LK5].

[98] Kyle Soska & Nicolas Christin, *Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem*, 24 USENIC Sec. Symp. 33 (2015), https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska-updated.pdf [https://perma.cc/GKX4-UX9A].

[99] *Id.*

[100] Soska & Christin, *supra* note 100, at 33 ("The anonymity properties were achieved by combining the network anonymity properties of Tor hidden services—which make the IP addresses of both the client and the server unknown to each other and to outside observers—with the use of the pseudonymous, decentralized Bitcoin electronic payment system.").

[101] *Id.* ("Embolden by the anonymity properties Silk Road provided, sellers and buyers on Silk Road mostly traded in contraband and narcotics.").

shut down, a continuous cycle of new anonymous marketplaces have emerged.[102] However, nefarious uses of BitCoin do not result from an inherent flaw with BitCoin technology, and should not dictate the technology's regulation as a whole since the Blockchain itself enables law enforcement to deal with such cases.[103]

C.   Inherent Problems

BitCoin suffers from a few inherent problems, which currently limit its broad acceptance and use, thereby making crafting appropriate regulations especially difficult. However, if BitCoin transactions are encouraged, rather than stifled with burdensome regulations, each of these concerns will automatically diminish as a result of market forces.

First, BitCoin technology is new and confusing. Even some BitCoin aficionados have trouble explaining how Blockchain works,[104] because the underlying technology is hard to comprehend.[105] If the technology were easier to use, it is hypothesized that a larger percentage of the population would transact in BitCoin.[106] The former Chief Operating Officer of Skype agrees with this sentiment and has stated the "next goal" is removing technological complication from BitCoin transactions.[107] As new software tools make BitCoin easier to use, more individuals will begin transact with it.

Second, BitCoin technology currently suffers from liquidity concerns because such a small subset of the population uses the technology.[108] Without a robust BitCoin market, it can be cumbersome

---

[102] See id. at 47 ("More remarkably, anonymous marketplaces are extremely resilient to takedowns and scams – highlighting the simple fact that economics (demand) plays a dominant role.").

[103] See infra notes 354–61 and accompanying text (discussing how the Blockchain enables law enforcement to track fraudulent BitCoin users).

[104] See Sydney Ember, Data Security Is Becoming the Sparkle in Bitcoin, N. Y. Times (Mar. 1, 2015), http://www.nytimes.com/2015/03/02/business/dealbook/data-security-is-becoming-the-sparkle-in-bitcoin.html [https://perma. cc/HZ33-6LCA] ("Explaining how the block chain [sic] works can tangle the tongues of even those who are most enthusiastic about Bitcoin.").

[105] Cf. Jackson, supra note 78 ("Yet, the challenge in 2016 will be captured by the companies that can successfully obfuscate the complexity of bitcoin and bring frictionless value transfer to the next 100 million daily users.").

[106] Id.

[107] Id.

[108] Cf. Tom Zanki, SEC Approval of Digital Shares Could Spur Experimentation, Law360 (Dec. 18, 2015, 9:27 PM), http://www.law360.com/

to exchange traditional currency, goods, or services for BitCoin, causing price volatility.[109] Although several online retailers have started accepting BitCoins,[110] most online retailers have not. If trading in BitCoin is too unwieldy, there will not be enough buyers and sellers to create a vibrant market and BitCoin will lose popularity. Nevertheless, the number of daily transactions has risen steadily since 2012; there were over 200 thousand daily transactions in early 2016.[111] The more people use BitCoin, the more vibrant the BitCoin market will become, and the current BitCoin liquidity concerns will diminish.

    Finally, the price of BitCoins varies drastically, which can make it difficult to use as currency.[112] In a two-month period in early 2013, "Bitcoin's dollar exchange rate rose from about $50 to $350 and then fell back to near $70."[113] By the end of 2013, the exchange rate rose to over $1,000.[114] This price pattern suggests that "speculative investors," rather than active users increasing the number of BitCoin transactions, are driving the BitCoin market.[115] Logically, this variance could discourage potential users from using BitCoin out of fear of a vast devaluation. Moreover, such extreme price variations encourage users who hold BitCoins "to hoard Bitcoins rather than spend them," a major problem when trying to encourage widespread adoption of BitCoin.[116] Venture capitalist Fred Wilson posited that BitCoin prices would become more stable if the velocity of the BitCoin supply increased.[117] Accordingly, to address acceptance, liquidity,

---

articles/739837/sec-approval-of-digital-shares-could-spur-experimenta-tion [https://perma.cc/TFS9-CBYC].

[109] *Id.*

[110] *See* Chokun, *supra* note 3.

[111] Jackson, *supra* note 78.

[112] Murphy et al., *supra* note 2, at 7.

[113] *Id.*

[114] *Id.*

[115] *Id.*

[116] *Id.* (stating that hoarding BitCoins is "the opposite of what would need to happen to make a currency a successful medium of exchange such as the dollar"); *see* Böhme et al., *supra* note 41, at 225 ("[O]f the bitcoins mined in 2009–2010, more than 60 percent remain unspent or took more than one year to be spent."). In fact, BitCoin adoption is about "one-twentieth as rapid" as the adoption of mPesa, a mobile phone application in Kenya that also allows for user-to-user transactions. *Id.*

[117] *See* Nermin Hajdarbegovic, *Investor Fred Wilson: Security and Hoarding Are Holding Back Bitcoin*, CoinDesk (July 21, 2014, 9:24 AM), http://www.

and stability concerns currently associated with BitCoin, regulations should foster a supportive environment in which the technology can become more widely adopted. A regulatory environment that stifles widespread adoption of the technology will only exacerbate BitCoin's current problems, and minimize the many actual and potential benefits of BitCoin.

V.   *Guideposts for Regulation*

Strict BitCoin regulation will defeat the speed and efficiency gains created by BitCoin and chill innovation technologies based on the Blockchain.[118] Current regulations, such as money transmitter and securities laws, should not be used to enforce BitCoin activities.[119] Instead, only tailored regulations should be adopted to address specific BitCoin concerns.[120] Moreover, the free market is a better determinant than the government of whether BitCoin continues to grow or becomes less popular.[121]

---

coindesk.com/investor-fred-wilson-security-hoarding-holding-back-bitcoin/ [https://perma.cc/7Q63-JQWR] ("Right now, most people who get bitcoin hold it, they don't transact with it. That's part of what causes all of the volatility—if there was a very vibrant system where bitcoin was just getting swapped around like crazy, the velocity of the money would cause bitcoin's price to stabilize and there would be a much more liquid market.").

[118] *Cf.* Kevin V. Tu & Michael W. Meredith, *Rethinking Virtual Currency Regulation in the Bitcoin Age*, 90 Wash. L. Rev. 271 (2015) ("The foregoing notwithstanding, today Bitcoin app development continues to grow, which lends further support to the view that Bitcoin is gaining more widespread acceptance.").

[119] *Id.*

[120] *Id.*; Jonathan W. Lim, *A Facilitative Model for Cryptocurrency Regulation in Singapore*, *in* Handbook of Digital Currency 360, 368 (David Lee Kuo Chuen ed., 2015) ("Targeted laws addressing specifically identified cryptocurrency risks or regulatory interests are appropriate and consistent with the facilitative framework: targeted cryptocurrency regulation would ensure that products or practices that are harmful are appropriately contained while at the same time preserve the benefits of innovation and allow new business models to experiment, compete fairly, and flourish.").

[121] Nikolei M. Kaplanov, Comment, *Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation*, 25 Loy. Consumer L. Rev. 111, 171–72 (2012) ("By letting the market determine whether or not bitcoin should survive is preferable to federal policy seeking to shut it down.").

A.   BitCoin Objectives

It is critical to ensure that using BitCoin remains inexpensive and efficient.[122] BitCoin regulation that dramatically increases costs or slows down transactions is critically flawed because such regulations would attack the greatest benefits of BitCoin.[123] The free market, not the government, should dictate whether BitCoin has a competitive advantage over other forms of currency. Additionally, BitCoin has the potential to serve as a social science sandbox.[124] In sandboxes, scholars have the opportunity to observe BitCoin and learn everything from the "design of financial markets to user behavior [to] myriad questions of law and regulation."[125] Moreover, BitCoin sandboxes provide the opportunity to study monetary policy.[126] BitCoin is fertile ground for research because its "contained environment [has] a clear set of rules," transactions are publically recorded, and much data, including prices and trade volume, is available to researchers.[127] Supporting the growth of BitCoin will allow this research to continue, perhaps illuminating "some of the longstanding issues on the conduct

---

[122] *Cf.* Brito, *supra* note 52, at 151.

[123] *See id.* (explaining that BitCoin transactions are also resistant to censor-ship, as there is no financial intermediary that controls who a user may trans-act with or donate to).

[124] Böhme et al., *supra* note 41, at 232 ("Bitcoin has the potential to be a fer-tile area for social science research. Scholars should appreciate Bitcoin's con-tained environment with a clear set of rules (albeit not free from frictions), the publicly available record of transactions (unusual for most means of ex-change), and the general availability of data even beyond the block chain (including market prices and trading volumes)."); *see* Peter Van Valkenburgh, *Framework for Sec. Reg. of Cryptocurrencies*, COIN CTR. REP., Jan. 2016, at 53–54 (2016) ("Anyone with a computer and an Internet connection can de-velop and share her own currency, her own vision of the future.").

[125] Böhme et al., *supra* note 41, at 232.

[126] *Id.* at 233–34 ("Just as overly rapid growth of a money supply is clas-sically linked to inflation, the fixed slow growth rate of Bitcoin creates the possibility of deflation if Bitcoin was to be used widely. . . .").

[127] *Id.* at 232 ("Bitcoin has the potential to be a fertile area for social science research. Scholars should appreciate Bitcoin's contained environment with a clear set of rules (albeit not free from frictions), the publicly available re-cord of transactions (unusual for most means of exchange), and the general availability of data even beyond the block chain (including market prices and trading volumes).").

and effects of monetary policy."[128] In fact, some believe Blockchain technology "could revolutionize regulators' approach to monitoring systemic risk in areas such as collateral reuse."[129]

B.   Impossibility of Effective Strict BitCoin Regulation

Although strict government regulation or an outright ban of BitCoin is a proposed solution to avoiding the risks of BitCoin, it is not pragmatic.[130] As a pseudo-anonymous, peer-to-peer system, BitCoin will continue to operate regardless of congressional decree.[131] When it comes to BitCoin, there is no building to raid or subpoena to issue.[132] Even if the government banned BitCoin, a "new bitcoin-like system could be [created and] solely maintained by foreign users and in a manner that does not disclose all transactions publicly."[133] Without all transactions being publically recorded, the Blockchain loses one of its strongest checks against fraud. A BitCoin-like system without public disclosure of transactions would therefore cause far more concern than the current public Blockchain.[134] Similarly, over-regulation of BitCoin could push users to use services like Zerocash, which allows for peer-to-peer transactions "that reveal neither the origin, destination, or amount of the payment."[135] This system would cause increased difficulty in tracking criminals and heighten the technological barrier to entry for normal consumers.[136]

---

[128] *Id.* at 234.

[129] Tom Zanki, *SEC Commissioner Says Bitcoin Tech Demands Closer Look*, Law360 (Nov. 10, 2015, 4:40 PM), https://www.law360.com/articles/725512/sec-commissioner-says-bitcoin-tech-demands-closer-look   [https://perma.cc/8RHB-NZKU].

[130] Kaplanov, *supra* note 123, at 167–69 (listing potential issues with trying to ban BitCoins including failure to stop the underlying criminal activity, hurting prosecutors' ability to build cases using BitCoin related information, the practical impossibility of a successful ban).

[131] *Id*. at 168.

[132] *Id.*

[133] *Id.* at 169.

[134] *Id.* at 170 (relating the benefits to law enforcement of having a globally public log of transactions).

[135] *Overview of Zerocash*, Zerocash, http://zerocash-project.org [https://perma.cc/E2ET-LDF].

[136] Böhme et al., *supra* note 41, at 232.

Overall, BitCoin regulation must satisfy two critical components. First, BitCoin regulation must ensure that the unique benefits of BitCoin remain.[137] Second, BitCoin regulation must be tailored to the specific risks faced by consumers. Strict regulation or an outright ban of BitCoin will eliminate the efficiency benefits of the technology, worsen liquidity and acceptance problems, and increase the risks of illegal activity associated with BitCoin or BitCoin-like technologies.

VI.   Federal Classification and Regulation

The federal government so far has been unable to keep up with BitCoin technology, leading courts and agencies to regulate BitCoin by treating it like various other regulated items and services, including investment contracts, money, property, and commodities.[138] However, treating BitCoin like other regulated entities will stifle its potential benefits, and many small businesses will struggle to gain regulatory approval.[139] In turn, the competitive market forces that would drive faster, more efficient transactions will be restrained.[140]

A.   BitCoin Classified as a Security

In 2014, a Texas court ruled that a BitCoin investment opportunity was a security.[141] *S.E.C. v. Shavers* arose out of Bitcoin Savings and Trust, an "online investment scheme in which [its founder and operator] Shavers solicited and accepted all investments, and paid all purported returns," in BitCoin.[142] Shavers solicited individuals online to invest in his business, falsely promising "investors up to 1% interest daily to be paid every three days at first, or 7% interest weekly, purportedly based on Shavers' trading of bitcoin against the U.S. dollar."[143] However, Shavers was not actually trading BitCoins against

---

[137] *See* Lim, *supra* note 122 ("[T]argeted cryptocurrency regulation would ensure that products or practices that are harmful are appropriately contained while at the same time preserve the benefits of innovation and allow new business models to experiment, compete fairly, and flourish.").

[138] *See* Filippi, *supra* note 9.

[139] *Id.*

[140] *Id.*

[141] S.E.C. v. Shavers, No. 4:13–CV–416, 2014 WL 4028182, at *2 (E.D. Tex. 2014).

[142] *Id.* at *1.

[143] *Id.* at *1.

the U.S. dollar; rather, he was paying off withdrawals and interest with new deposits while appropriating funds for personal use.[144] Final judgment was entered against Shavers for operating a Ponzi scheme and defrauding investors out of over 700 thousand BitCoins."[145]

In 2013, the court ruled on the preliminary issue of whether it had subject matter jurisdiction over the case pursuant to the Securities Act of 1933 and the Exchange Act of 1934 (Securities Act).[146] In order for the court to have subject matter jurisdiction, it had to find that the BitCoin scheme was a security.[147] But, it first needed to find whether there was an investment contract in the BitCoin investments.[148] If so, the investment would be a security.[149]

The Supreme Court in *S.E.C. v. W.J. Howey Co*. provided the test to determine whether an investment contract exists.[150] In order to constitute an investment contract, there must exist a "scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party . . . ."[151] In determining whether the investments made to Shavers were an investment of money,[152] the court found that BitCoin was similar to money because it could be used to purchase goods and services.[153]

---

[144] *Id.* at *5.

[145] Litigation Release No. 23090, U.S. Securities & Exch. Comm'n, Final Judgment Entered Against Trendon T. Shavers, A/K/A/ "Pirateat40" - Operator of Bitcoin Ponzi Scheme Ordered to Pay More Than $40 Million in Disgorgement and Penalties (Sept. 22, 2014), https://www.sec.gov/litigation/litreleases/2014/lr23090.htm [https://perma.cc/85X2-VGN9].

[146] S.E.C. v. Shavers, 2013 WL 4028182, No. 4:13–CV–416, at *1 (E.D. Tex. Aug. 6, 2013).

[147] *Id.*

[148] *See id.* at *2.

[149] *See id.*

[150] S.E.C. v. W.J. Howey Co., 328 U.S. 293, 298–99 (1946) ("[A]n investment contract for purposes of the Securities Act means a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party, it being immaterial whether the shares in the enterprise are evidenced by formal certificates or by nominal interests in the physical assets employed in the enterprise.").

[151] *Id.*

[152] *Shavers*, 2013 WL 4028182, at *2.

[153] *Id.*

Despite the fact that BitCoin has limited acceptance,[154] the court found that BitCoins can "be exchanged for conventional currencies," and therefore are a form of money.[155] This finding is important in establishing BitCoin as a type of currency.[156]

In determining whether the profits were "derived from the efforts of the promotor, [sic]"[157] the Court found that Shaver's promise of 1 percent daily interest to investors clearly satisfied this prong.[158]

Finally, the common enterprise component of the *Howey* test[159] required an "interdependence between the investors and the promotor [sic] . . . ."[160] Evidence demonstrated that Shavers promised returns to investors based on his expertise in "trading and exchanging Bitcoin."[161] Moreover, investors relied solely "on Shavers' expertise in BitCoin markets and his local connections."[162] This evidence was sufficient for the court to find the common enterprise prong of the investment contract test satisfied.[163]

However, others have made the argument that BitCoin itself fails to satisfy the common enterprise requirement,[164] which they assert requires horizontal commonality linking the outcome of a single investor to the outcomes of all investors.[165] BitCoin lacks this horizontal commonality because of each BitCoin promoter is independent and no BitCoin business involving making money off of investments.[166] Moreover, one can argue that BitCoin exchanges are so impactful on BitCoin pricing that the BitCoin developers alone cannot possibly constitute a common enterprise.[167]

---

[154] *Id.* ("The only limitation of Bitcoin is that it is limited to those places that accept it as currency.").

[155] *Id.*

[156] *Id.* at *1–2.

[157] *Id.*

[158] *Id.*

[159] *Id.*

[160] *Id.*

[161] *Id.*

[162] *Id.*

[163] *Id.*

[164] Reuben Grinberg, *Bitcoin: An Innovative Alternative Digital Currency*, 4 HASTINGS SCI. & TECH. L. J. 159, 197 (2011), http://ssrn.com/abstract=1817857 [https://perma.cc/M3LV-WSDY].

[165] *Id.* at 194–99.

[166] *Id.*

[167] *See id.* at 197–98.

Nevertheless, the *Shavers* court found that all of the prongs of the *Howey* test were satisfied, and held that BitCoins were investment contracts and therefore securities.[168] Because securities are subject to strict consumer protection rules, such as the requirement to register the security before selling or delivering it,[169] this ruling allowed the Securities and Exchange Commission (SEC) to prosecute Shavers for securities violations. However, the *Shavers* court held that this scheme amounted to a security, not the BitCoins themselves.[170] The victims of the Ponzi scheme invested in Shavers' scheme in BitCoin and Shavers' scheme claimed returns were generated based on betting on BitCoin pricing.[171] This distinction highlights the need for regulation that is tailored to the specific circumstances in which BitCoin can be used to harm consumers.

This note argues that the Securities Act should not apply to BitCoin because BitCoin is not a security. Courts should focus on economic reality rather than form when classifying investments as securities.[172] The economic reality is that BitCoins are used to make purchases online without the need for an intermediary.[173] They are used as a means of exchange rather than as an investment by which a consumer gains profits.[174] As more businesses begin to accept BitCoin as a medium of exchange, the argument grows stronger that BitCoins are used to facilitate exchange.[175]

Alternatively, if BitCoins are securities, they should be exempt from the securities laws. Jerry Brito, the executive director of Coin Center,[176] argues that the underlying policy rationale "of

---

[168] *Id.*

[169] *See, e.g.*, 15 U.S.C. § 77e(a) (2012) (prohibiting certain activities for un-registered securities).

[170] *Shavers*, 2013 WL 4028182, at *2.

[171] *Id.* at *1.

[172] Tcherepnin v. Knight, 389 U.S. 332, 336 (1967) (citing S.E.C. v. W.J. Howey Co., 328 U.S. 293, 298 (1946)).

[173] As of early 2015, an average of 200 thousand BitCoins were transacted every day. Böhme et al., *supra* note 41, at 213–14.

[174] Individuals trade in foreign currency for profit, but that does not mean foreign currency is a security. Similarly, some trade in BitCoin to profit on pricing fluctuations. This does not mean BitCoin is a security.

[175] *Cf.* Grinberg, *supra* note 166, at 198 (stating that the limited number of merchants that accepted BitCoins in 2011 was a limiting factor in BitCoins' use as a currency).

[176] Coin Center is "the leading non-profit research and advocacy center fo-

financial regulation is to protect the users of financial instruments from fraud, manipulation, and other types of misconduct that results in real economic losses."[177] He asserts that these policy goals do not align with BitCoin because of the public nature of the Blockchain.[178] Therefore, he argues that BitCoin should be exempt from securities laws, like private company securities.[179] Even though the definition of security is meant to be broad and flexible,[180] BitCoin does not resemble a security[181] and should not be regulated as such.[182] Rather, it is used to make purchases and functions like currency.

B.   BitCoin Classified as Currency

In 2014, in the case of *U.S. v. Ulbricht*, which dealt with Silk Road, the Southern District of New York classified BitCoin as currency.[183] The court found that BitCoins could be considered money that could be laundered.[184] The most pertinent issue examined in *Ulbricht* is how digital currency should be classified.[185] Reading the language of the money laundering statute broadly, the court found that BitCoins could be used to launder money if they fit within the definition of financial transactions.[186] The opinion stated that financial transactions capture movement of all "funds,"[187] which should be read

---

cused on the public policy issues facing cryptocurrency and decentralized computing technologies like Bitcoin and Ethereum." *About Us*, COIN CENTER, https://coincenter.org/about [https://perma.cc/67XU-5P4Y].

[177] Brito et al., *supra* note 52, at 194.

[178] *See id.*

[179] *Id.*

[180] Tcherepnin v. Knight, 389 U.S. 332, 338 (1967).

[181] *Cf.* Van Valkenburgh, *supra* note 126, at 53 (stating that the *Howey* test is better fitted for low transparency virtual currencies that do not provide "visibility into the operation of the technology [because] there is no reason to believe that profits come from anything other than a promoter's hype").

[182] *Id.* (indicating that BitCoin is ill-fitted to the *Howey* test "because of a lack of vertical commonality or a discernible third party or promoter upon whose efforts investors rely").

[183] United States v. Ulbricht, 31 F. Supp. 3d 540 (S.D.N.Y. 2014).

[184] *Id.* at 570.

[185] *See id.*

[186] *See id.* ("Congress intended to prevent criminals from finding ways to wash the proceeds of criminal activity by transferring proceeds to other similar or different items that store significant value.").

[187] 18 U.S.C. § 1956(c)(4) (2010) ("The term 'financial transaction' means

in a "colloquial sense" to mean something that "can be used to pay for things."[188] "Sellers using Silk Road [were] not alleged to have given their narcotics and malicious software away for free—they [were] alleged to have sold them."[189] As such, the court held that BitCoins are "funds," and therefore a part of financial transactions.[190] By extension BitCoins are included within financial transactions and can be used to launder money.[191]

Although BitCoin shares many of money's attributes, state statutes that deal with BitCoin should be specifically tailored to virtual currency.[192] A Florida state court found that its state anti-money laundering statute did not cover BitCoin transactions because the statute was drafted too vaguely to include virtual currency.[193] The defendant was not convicted for laundering BitCoins.[194] Accordingly, in order to prevent nefarious uses of BitCoins and bring them within existing currency regulations, state regulations should explicitly include digital currency.

C.   BitCoin Classified as Property

Because BitCoins can be traded for goods and services and exchanged for cash, the act of acquiring BitCoins has tax implications. In 2014, the Internal Revenue Service (IRS) issued guidelines in treating

---

a transaction which in any way or degree affects interstate or foreign commerce involving the movement of funds by wire or other mean.").

[188] *Ulbricht*, 31 F. Supp. 3d at 570.

[189] *Id.*

[190] *Id.*

[191] *Id.*

[192] Florida v. Espinoza, CR–F14–2923 (11th Cir. Jul. 22, 2016). In *Espinoza*, the defendant was involved in an undercover operation wherein an undercover detective traded cash to the defendant in exchange for BitCoins. After a few transactions, the undercover detective told the defendant that he was involved in the buying and selling of stolen credit cards for profit. One issue for the court to consider was whether the defendant's sale of BitCoins to the detective in exchange for "dirty" money constituted money laundering under the state money laundering statute. In order to launder money, an individual must have "the intent to promote carrying on of the illegal activity." The court ultimately found that the defendant could not have laundered because the statute was too vaguely drafted to include virtual currency. *Id.* at 5–6.

[193] *Id.* at 7.

[194] *Id.*

BitCoin for federal tax purposes.[195] The guidelines treat BitCoin as convertible property.[196] Specifically, the IRS stated that "[g]eneral tax principles applicable to property transactions apply to transactions using virtual currency."[197] For instance, if a taxpayer "successfully 'mines' virtual currency, the fair market value of the virtual currency as of the date of receipt is includible in gross income."[198] In sum, if an individual uses his computer to support the Blockchain and mine for BitCoins, and the individual is awarded coins successfully verifying a transaction, he or she must pay income tax on those coins. [199]

Recently, the IRS has grown more aggressive in seeking out individuals who use BitCoins to evade taxes.[200] In November 2016, the IRS sent a John Doe summons to "Coinbase, the largest Bitcoin exchange in the United States, asking for the records of all customers who bought virtual currency from the company from 2013 to 2015."[201] Coinbase had approximately three million customers.[202] A federal court ultimately authorized the service of the John Doe summons on Coinbase in the belief "that virtual currency users may have failed to comply with federal tax laws."[203] The summons requires Coinbase

---

[195] I.R.S. Notice 2014-21 (Apr. 14, 2014), https://www.irs.gov/pub/irs-drop/n-14-21.pdf [https://perma.cc/Y4K9-B8DH].

[196] *Id.* at 2. Interestingly, the *Ulbricht* court seems to simply disregard this position. *Ulbricht*, 31 F. Supp. 3d at 569 ("In any event, neither the IRS nor FinCEN has addressed the question of whether a 'financial transaction' can occur with Bitcoins.").

[197] I.R.S. Notice 2014-21 (Apr. 14, 2014), https://www.irs.gov/pub/irs-drop/n-14-21.pdf [https://perma.cc/Y4K9-B8DH].

[198] *Id.* at 4 (However, if the gain is less than $200, it is not taxable.).

[199] *Id.*

[200] *See, e.g.*, Nathaniel Popper, *Bitcoin Users Who Evade Taxes Are Sought by the I.R.S.*, N.Y. TIMES (Nov. 18, 2016), https://www.nytimes.com/2016/11/19/business/dealbook/irs-is-seeking-tax-evaders-who-use-bitcoin.html?r-ref=collection%2Ftimestopic%2FBitcoin [https://perma.cc/8TQ5-4S7Z] (describing the I.R.S. investigation into Coinbase).

[201] *Id.* According to the IRS, "a John Doe summons is a summons that does not identify the person with respect to whose liability the summons is issued. The Internal Revenue Code authorizes the Service to issue a John Doe summons pursuant to an investigation of a specific, unidentified person or ascertainable group or class of persons." IRM 25.5.7.2(1) (Feb. 18, 2016).

[202] Popper, *supra* note 203.

[203] *Court Authorizes Service of John Doe Summons Seeking the Identities of U.S. Taxpayers Who Have Used Virtual Currency*, U.S. DEP'T OF JUST. (Nov. 30, 2016), https://www.justice.gov/opa/pr/court-authorizes-service-

to supply information to the IRS regarding the identity and trading records of its users.[204] Coinbase is currently fighting the order.[205] Nevertheless, the IRS's posture indicates that it is taking enforcement action against BitCoin users seriously.[206]

D.   BitCoin Classified as a Commodity

In September 2015, the Commodity Futures Trading Commission (CFTC) provided guidance on the regulation of BitCoin.[207] *In re Coinflip, Inc.* dealt with a risk management system called Derivabit that allowed users to enter put and call options against fluctuations in BitCoin prices.[208] Users could create accounts, load their account with BitCoins for payment, and receive premium payments in BitCoins.[209] The "strike and delivery prices" were set in U.S. dollars.[210]

In its analysis, the CFTC began by defining a commodity as "all services, rights, and interests . . . in which contracts for future delivery are presently or in the future dealt in."[211] The CFTC stated that this definition should be construed broadly.[212] With no further

---

john-doe-summons-seeking-identities-us-taxpayers-who-have-used [https://perma.cc/PNU6-DVCF].

[204] *Id.*

[205] Mark C. Milton, *Bitcoin Users Should Expect More IRS And DOJ Scrutiny*, LAW360 (Jan. 30, 2017, 6:23 PM), https://www.law360.com/privacy/articles/886479/bitcoin-users-should-expect-more-irs-and-doj-scrutiny [https://perma.cc/U9GS-MJJ8]. The impact on taxpayers could be significant, as penalties for tax evasion include penalty fees, interest, additional taxes, and possible prison time. *Id.* Moreover, "information could potentially aid the federal government in pursuing other types of criminal charges against digital currency users, such as violations of money laundering, drug trafficking and money transmitting laws." *Id.*

[206] *Id.*

[207] *In re* Coinflip, Inc., CFTC No. 15-29, 2015 WL 5535736 (Sept. 17, 2015).

[208] *Id.* at 2.

[209] *Id.*

[210] *Id.* Strike and delivery price are financial terms of art and have to do with when a put or call is executed. *See Strike Price*, INVESTOPEDIA, http://www.investopedia.com/terms/s/strikeprice.asp [https://perma.cc/PBD6-TU8R]; *Delivery Price*, INVESTOPEDIA, http://www.investopedia.com/terms/d/deliveryprice.asp [https://perma.cc/P8KN-LZHT].

[211] 7 U.S.C. § 1a(9) (2012).

[212] *In re Coinflip*, 2015 WL 5535736, at *3 (citing Board of Trade v. S.E.C.,

explanation, the CFTC stated that virtual currency is properly classified as a commodity.[213] Because the BitCoin was found to be a commodity, and Derivabit did not register with the CFTC to offer commodity options, Coinflip was required to cease and desist.[214]

The CFTC's guidance has a few implications.[215] First, it demonstrates that virtual currencies are not securities because, if they were, the SEC would have brought the action.[216] Second, it is evident that the CFTC's oversight of BitCoin is limited in scope to BitCoin-related financial instruments.[217] However, it is not clear whether BitCoins are an excluded commodity like currency or an exempt commodity like gold.[218] This difference could create regulatory implications for certain financial products like BitCoin swaps.[219]

The distinction between currency and commodity is also relevant in bankruptcy proceedings. For example, the U.S. Bankruptcy Court for the Northern District of California dealt with whether BitCoins are commodities or U.S. currency.[220] In *In re Hashfast Technologies,* Dr. Lowe entered into an agreement with HashFast Technologies to help promote and sell HashFast's BabyJet BitCoin mining hardware.[221] Under the agreement, Dr. Lowe earned the

---

677 F.2d 1137, 1142 (7th Cir. 1982)).

[213] *Id.* at *3.

[214] *Id.* at *3–6 ("Respondents shall cease and desist from violating Sections 4c(b) and 5h(a)(1) of the Act, 7 U.S.C. §§ 6c(b) and 7b-3(a)(l) (2012), and Commission Regulations 32.2 and 37.3(a)(1), 17 C.P.R. §§ 32.2 and 37.3(a)(1) (2014).").

[215] Pete Rizzo, *CFTC Ruling Defines Bitcoin and Digital Currencies as Commodities*, COINDESK (Sep. 17, 2015, 10:06 PM), http://www.coindesk.com/cftc-ruling-defines-bitcoin-and-digital-currencies-as-commodities/ [https://perma.cc/DG8K-QMQN].

[216] *Id.*

[217] *Id.*

[218] *E.g.*, Houman B. Shadab, *Regulating Bitcoin and Block Chain Derivatives* 4–5 (N.Y.L.S. Legal Studies Research Paper, 2014), Oct. 9, 2014, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2508707 [https://perma.cc/83DY-CN9D].

[219] *Id.* at 5.

[220] Issac M. Marcushamer & Andrew M. Hinkes, *Bitcoin in Bankruptcy: Is It Commodity Or Currency?*, LAW360 (Feb. 18, 2016, 10:26 AM), http://www.law360.com/articles/760393/bitcoin-in-bankruptcy-is-it-commodity-or-currency [https://perma.cc/8HQJ-VJUV].

[221] Defendant Opposition to Motion For Partial Summary Judgment at 3, *In re* Hashfast Tech., No. 14-30725 (Bankr. N.D. Cal. 2016).

BitCoin equivalent of $5,600 per BabyJet that he helped sell.[222] Dr. Lowe was entitled to $308,000 for his services when the first round of BabyJets were sold.[223] After this transfer occurred, HashFast filed for bankruptcy.[224] In bankruptcy proceedings, the Trustee asserted the transaction was fraudulent and was "subject to a 'clawback' action'."[225] At the time of the transfer, the three thousand BitCoins were valued at $363,861.43, which appreciated to $1.3 million by the time of the bankruptcy proceedings.[226] The distinction between currency and commodity came into play in this case, because if BitCoins were a commodity the trustee was entitled to the BitCoins or their current value of $1.3 million, while if the BitCoins were U.S. currency, it was entitled only to $363,861.43."[227]

The trustee argued that BitCoins were a commodity based on both the CFTC's guidance and IRS classifications.[228] Furthermore, the trustee asserted that BitCoin "serves as a medium of exchange" more closely resembling a commodity like gold because its value changes over time.[229] Moreover, the trustee argued that it is incorrect to read criminal law cases that classify BitCoin as currency under the anti-money laundering statute because that statute construes money broadly in order to further the policy goal of decreasing criminal activity.[230]

Dr. Lowe's used SEC and district court rulings to support his argument that BitCoins are currency.[231] Specifically, Dr. Lowe pointed to the Treasury Department's ruling that virtual currency should be regulated in the same manner as currency.[232] Dr. Lowe further argued that *Ulbricht* "found that Bitcoin was a monetary instrument" and that,

---

[222] *Id.*

[223] *Id.*

[224] Marcushamer & Hinkes, *supra* note 223.

[225] *Id.*

[226] *Id.*

[227] *Id.*

[228] *Id.* (explaining the argument and position the trustee took in this matter).

[229] Memorandum of Points and Authorities in Support of Motion for Partial Summary Judgment at 5, *In re Hashfast Tech.*, No. 14-30725.

[230] *Id.* at 7–8 ("These cases are inapposite, as the money laundering statute is concerned with shutting down criminal enterprises, and so defines the terms 'funds' and 'money' as broadly as possible.").

[231] Marcushamer & Hinkes, *supra* note 223.

[232] Defendant Opposition to Motion for Partial Summary Judgment at 9, *In re Hashfast Tech.*, No. 14-30725.

therefore, BitCoins should be considered currency.[233] Similarly, Dr. Lowe stated that in two cases the Southern District of New York found that "virtual currency exchangers" were money transmitters[234] and that there was no difference "between real currencies and convertible virtual currencies."[235]

The difference in classification in this case had a $1 million impact.[236] In response to this summary judgment motion, the bankruptcy court found that BitCoins were not U.S. dollars, [237] but did not rule on whether BitCoins are "currency or commodities for purposes of the fraudulent transfer provisions of the bankruptcy code."[238]

In sum, the current federal regulation of BitCoin is unsettled in many respects. First, while some courts have held otherwise, BitCoin should not be treated as a security because it is used as a means of exchange, not as an investment by which a consumer gains profits. Second, in order to prevent nefarious uses of BitCoin, digital currencies should be expressly and consistently included in laws regulating currency, including money laundering statutes. Third, while it is clear that BitCoin is treated as property and accordingly subject to taxes, tax law should be made more clear and explicit to increase consumer compliance. Finally, the federal government should make clear whether BitCoin is treated as a currency or commodity. Because federal attempts at BitCoin regulation are unsettled at best, one must consider the state attempts at regulating BitCoin to evaluate how BitCoin should be classified.

VII.   State Level Regulation

A.   CSBS Model Framework

In September 2015, the Conference of State Bank Supervisors (CSBS), a non-profit organization that seeks to develop consistent

---

[233] *Id.* at 11–12.

[234] *Id.* at 12 (citing United States v. Faiella, 39 F. Supp. 3d 544, 546 (S.D.N.Y. 2014)).

[235] *Id.* (United States v. Budovsky, No. 13cr368 (DLC), 2015 WL 5602853, at * 10 (S.D.N.Y. 2015)).

[236] *Id.*

[237] Order on Motion For Partial Summary Judgment at 1, *In re Hashfast Tech.*, No. 14-30725.

[238] *Id*.

banking regulatory policy amongst the states,[239] published a model regulatory framework for BitCoin and other virtual currency.[240] The objective of the model framework is to assist states' regulation of virtual currency and, more importantly, to promote consistent regulation amongst the states.[241] However, the framework is not binding on any jurisdiction.[242] The model framework applies to activities that involve a third party, such as an exchange or wallet, maintaining control over an individual's virtual currency.[243] The framework does not apply to individuals or businesses that use virtual currency simply to transact for goods or services.[244]

The model framework suggests that states should use a "licensing system that enables states to share licensing and enforcement data in real time."[245] There should be a "uniform application" amongst the states in order to enhance efficiency and communication between regulators.[246] Moreover, licensees would be required to maintain

---

[239] *See About the Conference of State Bank Supervisors*, CONF. ST. BANK SU-PERVISORS, https://www.csbs.org/about/what/Pages/default.aspx [https://per-ma.cc/QR7K-BJ3R] ("The Conference of State Bank Supervisors (CSBS) is the nationwide organization of banking regulators from all 50 states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands. . . . For more than a century, CSBS has given state supervisors a national forum to coordinate supervision of their regulated entities and to develop regulatory policy.").

[240] CONF. ST. BANK SUPERVISORS, STATE REGULATORY REQUIREMENTS FOR VIRTUAL CURRENCY ACTIVITIES CSBS MODEL REGULATORY FRAMEWORK, (2015), https://www.csbs.org/regulatory/ep/Documents/CSBS-Model-Regulatory-Frame-work(September%2015%202015).pdf [https://perma.cc/Y326-UJE8] [here-inafter CSBS Model].

[241] Press Release, Conference of State Bank Supervisors, State Regula-tors Issue Model Regulatory Framework for Virtual Currency Activities (Sept. 15, 2015), https://www.csbs.org/news/press-releases/pr2015/Pages/PR091515.aspx [https://perma.cc/NAA3-KBD7].

[242] Charles M. Horn et al., *The Conference of State Bank Supervisors Adopts Model Regulatory Framework for Virtual-Currency Businesses*, MORGAN LEWIS (Oct. 14, 2015), https://www.morganlewis.com/pubs/csbs-adopts-mod-el-regulatory-framework-for-virtual-currency-businesses [https://perma.cc/4532-G99X].

[243] CSBS Model, *supra* note 243, at 11.

[244] *Id.*

[245] *Id.* at 12.

[246] *Id.* at 4 n.12.

strict capital requirements and investment reserves.[247] Licensees would also be required to maintain strong consumer protection standards, possess a robust cyber security program, and implement a compliance program.[248] Further, they would be required comply with the Bank Secrecy Act[249] and Anti-Money Laundering statutes,[250] maintain adequate books and records, and comply with state and federal regulations.[251] Particularly beneficial for small companies, the framework does not require companies acquire costly cyber risk insurance.[252]

Unfortunately, the model framework is lacking in certain respects. First, the definition of covered activities is prefaced with the phrase "at a minimum,"[253] which means that internet service providers and companies that provide developers with server space could be pulled into the definition of a covered activity and required to register.[254] This is most likely an unintended consequence of the language, but nevertheless it is a flaw in this model regulation.[255] Moreover, the model framework does not include an "on ramp" provision to exempt startups and small companies from regulation.[256] This lack of on

---

[247] *Id.* at 12.

[248] *Id.* at 13.

[249] Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114-4 (1970) (codified as amended in scattered sections of 12 U.S.C., 18 U.S.C., and 31 U.S.C.) ("Amend[ing] the Federal Deposit Insurance Act to require insured banks to maintain certain records, to require that certain transactions in United States currency be reported to the Department of the Treasury, and for other purposes.").

[250] *E.g.*, 31 U.S.C. § 5318(h) (2014) (requiring financial institutions to "establish anti-money laundering programs").

[251] CSBS Model, *supra* note 243, at 13–14.

[252] *Id.* at 7.

[253] CSBS Model, *supra* note 243, at 11.

[254] *See* Peter Van Valkenburgh, *Freshly Unveiled CSBS Model Regs: Good Goals, Poor Execution*, Coin Center (Sep. 15, 2015), https://coincenter.org/entry/freshly-unveiled-csbs-model-regs-good-goals-poor-execution [https://perma.cc/HXC4-A3QL] (criticizing the possibility of companies such as Amazon and Google from being considered virtual currency business).

[255] *Id.*

[256] CSBS Model, *supra* note 243, at 3–4 (declining to exempt startups and small companies because "consumers can be harmed by entities regardless of size"). Some argue that an exemption for startups is essential for innovation because the liability and compliance costs would prohibit innovation in the virtual currency space. *See* Letter from Elec. Frontier Found. to

ramp is a critical omission because it places the same regulatory and financial burden on startups as it does on mature businesses. This burden will stifle the growth and proliferation of BitCoin companies that is essential to reducing the liquidity and stability concerns currently associated with BitCoin, and is appropriately addressed with New York's conditional BitLicense option, discussed in the following section.[257]

B.   New York

In mid-2015, New York regulators published the final version of their BitLicense regulations, which regulate the use of BitCoin.[258] New York's BitLicense allows New York "persons"[259] to engage in certain virtual currency business activities,[260] such as operating an exchange or wallet, or issuing virtual currency.[261] Merchants who simply want to accept virtual currency in exchange for goods or services, however, do not need a BitLicense.[262] Among other rules and requirements, companies holding a BitLicense are required to: (1) have a BitLicense compliance officer and policy,[263] (2) maintain

---

Chairman Steven M. Glazer and Vice-Chairman Andy Vidak, Cal. Senate Banking & Fin. Insts. Comm., at 5–6 (Aug. 11, 2016),   https://www.eff. org/files/2016/08/18/eff_letter__oppose_ab_1326_aug._2016_-_final_. pdf [https://perma.cc/6GVQ-XQUJ]).

[257] See *infra* notes 270–73 and accompanying text (explaining New York's conditional license).

[258] *See* Michael Bobelian, *NY's BitLicense Reveals The Difficult Trade-offs Of Regulating Bitcoin*, Forbes (June 8, 2015), http://www.forbes. com/sites/michaelbobelian/2015/06/08/nys-bitlicense-reveals-the-diffi-cult-trade-offs-of-regulating-bitcoin/2/#1ca0c4c9b0e8   [https://perma.cc/ A4AS-DLHN].

[259] 23 N.Y. Law § 200.2(i) (defining person as "an individual, partnership, corporation, association, joint stock association, trust, or other entity, how-ever organized").

[260] § 200.3(a) ("No Person shall, without a license obtained from the super-intendent as provided in this Part, engage in any Virtual Currency Business Activity."). For the full definition of virtual currency business activities, see § 200.2(q).

[261] § 200.2(q).

[262] § 200.3(c)(2).

[263] § 200.7. The regulations require that a "[e]ach licensee shall maintain and enforce written compliance policies, including policies with respect to an-ti-fraud, anti-money laundering, cyber security, privacy and information se-

strict capital levels,[264] (3) keep financial books and records for seven years,[265] and (4) face compliance examinations no less than every two years.[266]

Applicants who do not satisfy all of the aforementioned regulatory requirements may be granted a conditional BitLicense.[267] Although a conditional license lasts two years, the superintendent may renew it.[268] The conditional license allows startups and smaller companies to innovate without having to meet the high regulatory burden of a BitLicense.[269] A licensee with a conditional license may be examined more thoroughly than a licensee holding a full license.[270] This conditional license addresses the problems presented to startups

---

curity, and any other policy required under this Part, which must be reviewed and approved by the Licensee's board of directors or an equivalent governing body." § 200.7(c).

[264] § 200.8 ("Each licensee shall maintain at all times such capital in an amount and form as the superintendent determines is sufficient to ensure the financial integrity of the Licensee and its ongoing operations based on an assessment of the specific risks applicable to each Licensee."). The superintendent will consider many factors including composition of assets and liabilities, the leverage and liquidity of the licensee, and the financial protection the licensee implements to protect its customers. § 200.8(a).

[265] § 200.12 ("Each Licensee shall, in connection with its Virtual Currency Business Activity, make, keep, and preserve all of its books and records in their original form or native file format for a period of at least seven years . . . in a condition that will allow the superintendent to determine whether the Licensee is complying with all applicable laws, rules, and regulations").

[266] § 200.13 ("Each Licensee shall permit and assist the superintendent to examine the Licensee whenever in the superintendent's judgment such examination is necessary or advisable, but not less than once every two calendar years . . . .").

[267] § 200.4(c)(1).

[268] § 200.4(c)(3).

[269] *See* Tanaya Micheel, *Lawsky Outlines Revisions to New York's BitLicense in DC Speech*, COINDESK (Dec. 18, 2014, 04:31 PM), http://www.coindesk.com/lawsky-outlines-revisions-new-yorks-bitlicense-dc-speech/ [https://perma.cc/G66U-LRLN] ("'Those firms will still be required to meet robust standards for consumer protection and anti-money laundering requirements,' he said. 'But we wanted to provide some flexibility as the firms work to get off the ground.'").

[270] § 200.4(c)(2).

and small businesses by the CSBS Model Framework's lack of on ramp provision.[271]

The current BitLicense regulation took over two years for the New York Department of Financial Services to draft, review, and finalize.[272] Companies who receive a BitLicenses will not have to file suspicious activity reports with the Financial Crimes Enforcement Network of the Treasury Department and the New York Department of Financial Services.[273] Also, they do not need to apply for both a BitLicense and money transmitter license in order to operate in New York; instead, possessing a BitLicense will satisfy multiple regulatory requirements.[274] Thus far, regulators have issued BitLicenses to five companies, including Circle Internet Financial Ltd.[275] and Coinbase.[276] New York's regulations so far appear to be a successful attempt at regulating those entities that operate exchanges or wallets or issue BitCoins, without imposing overly burdensome regulations on startups and merchants that accept BitCoin, which will increase the popularity of BitCoin and thereby reduce the risks currently associated with BitCoin.

C.   North Carolina

North Carolina has also adopted a BitCoin regulatory regime. On July 6, 2016, former Governor Pat McCrory signed into law the North Carolina Money Transmitters Act.[277] The law redefines money

---

[271] *See supra* notes 256-57 and accompanying text.

[272] Evan Weinberger, *NY Regulator Issues 1ˢᵗ Ever License To Bitcoin Firm*, Law360 (Sep. 22, 2015, 12:13 PM), http://www.law360.com/articles/705711/ ny-regulator-issues-1st-ever-license-to-bitcoin-firm?article_related_content=1 [https://perma.cc/MR9M-ESCC].

[273] Evan Weinberger, *NY Drops Dual Transaction Reports From Final BitLicense*, Law360 (June 3, 2015, 12:23 PM), https://www.law360.com/articles/663233 [https://perma.cc/6XVH-YUW5].

[274] *Id.*; *see* § 200.3(a)(1).

[275] Weinberger, *supra* note 275. Circle's main product is a mobile payment application that is designed to allow users to quickly and securely move money. *About*, Circle, http://circle.com/en/about [https://perma.cc/9DFW-QYQR].

[276] Fola Akinnibi, *Coinbase Gets NY BitLicense, Clearance For Its Operations*, Law360 (Jan. 18, 2017, 3:29 PM), https://www.law360.com/articles/881814/coinbase-gets-ny-bitlicense-clearance-for-its-operations [https://perma.cc/88KQ-232T].

[277] Evan Weinberger, *Bitcoin Backers See Room For Improvement In NC Law*, Law360 (July 7, 2016 6:45 PM), http://www.law360.com/articles/814699/

transmission to include "maintaining control of virtual currency on behalf of others."[278] Under this law, operators of BitCoin wallets and exchanges will need to register as money transmitters.[279] As money transmitters, "the firms will be subject to consumer-protection, suspicious-activity-reporting and other requirements that more traditional money transfer businesses operate under."[280] This classification also requires annual reporting.[281]

Although the regulations are less burdensome than New York's, the North Carolina law fails to provide an on ramp for smaller firms.[282] Also, the language of the law is vague and is not future proof.[283] For example, the law only applies to firms that perform a "a custody function—essentially maintaining control of virtual currencies on others' behalf . . . ."[284] However, future iterations of Blockchain-like technologies could process transactions so quickly they do not technically provide a custodial function.[285] Accordingly, the law likely will require updates to accommodate new technology.[286] Finally, the law does not clearly define when a company is considered to maintain control of an individual's virtual currency,[287] which could lead to confusion for merchants who want to accept BitCoin as payment.[288] Although this law takes steps towards providing a regulatory framework for BitCoin, more needs to be done to better define the scope of covered activities.

---

bitcoin-backers-see-room-for-improvement-in-nc-law   [https://perma.cc/YP2V-LVZA].

[278] N.C. GEN. STAT. § 53-208.42(12)(b) (2016).

[279] § 53-208.43(a).

[280] Weinberger, *supra* note 280.

[281] § 53-208.53.

[282] Weinberger, *supra* note 280.

[283] *See id.* ("While the law is explicit about what firms operating now will be required to register, its language leaves questions about firms in the next iteration of bitcoin, like the Lightning Network.").

[284] *Id.*

[285] *Id.*

[286] *Id.*

[287] *See* Pete Rizzo, *North Carolina Governor Signs Bitcoin Bill Into Law*, COINDESK (July 6, 2016, 3:05 PM), http://www.coindesk.com/north-caroli-na-governor-signs-bitcoin-bill-law/ [https://perma.cc/4UUW-PB93].

[288] *See id.*

D.   California

Unlike New York and North Carolina, California has been unsuccessful in implementing BitCoin regulation.[289] The failures of the California bill help illuminate some pitfalls in drafting BitCoin regulation. California's BitCoin License bill, Assembly Bill 1326, was first introduced in 2015.[290] It immediately faced resistance, most notably from the Electronic Frontier Foundation (EFF).[291] The EFF believed that that virtual currency should not be regulated until the technology matures otherwise innovation would be chilled.[292] The EFF was also concerned that inconsistencies between state regulatory schemes would create confusion for users.[293] Similar to the North Carolina law, the California bill also did not clearly define what having control over virtual currency meant.[294]

The 2016 amended version of Assembly Bill 1326 tried to resolve some of these concerns.[295] It sought to regulate "Digital currency business," which encompassed exchanges and wallets.[296] The bill would have also regulated individuals who transmit virtual currency to one another, unless the transaction had no financial purpose.[297] This poorly worded carve-out essentially would have

---

[289] *See* Press Release, Assemb. Matthew Dababneh, Assembly Member Dababneh Issues Statement on the Regulation of Virtual Currency (Aug. 15, 2016), https://a45.asmdc.org/press-release/assemblymember-dababneh-issues-statement-regulation-virtual-currency [https://perma.cc/LFJ3-XQKF].

[290] *See* Rainey Reitman, *A License to Kill Innovation: Why A.B. 1326-California's Bitcoin License-is Bad for Business, Innovation, and Privacy*, Electronic Frontier Found. (Aug. 7, 2015), https://www.eff.org/deeplinks/2015/08/license-kill-innovation-why-ab-1326-californias-bitcoin-license-bad-business [https://perma.cc/UKU2-E2EE].

[291] *Id.*

[292] *Id.*

[293] *Id.*

[294] *Id.* ("The bill defines a virtual currency business as 'maintaining full custody or control of virtual currency in this state on behalf of others.' Not only is this vague and overbroad, but it also does not reflect how many virtual currencies actually function."). The imprecise drafting of the bill could result in overly broad regulation. *Id.*

[295] *See generally*, H.B.1326, 2015–2016 Reg. Sess. (Cal. 2015) (withdrawn).

[296] § 26002(d).

[297] § 26002(d)(1) (exempting only the "[t]ransmission of digital currency where the transaction is undertaken for nonfinancial purposes and does not involve the transfer of more than a nominal amount of digital currency nec-

required every BitCoin user to register for a license before they could buy or sell goods or services for BitCoins.[298] There was also no exemption for start-ups or small businesses.[299] Although these revisions were meant to strengthen the regulation, these additions would have "chilled a young and quickly evolving industry" in California[300] and made it extremely difficult for Californians to use virtual currency.[301] In August 2016, California State Assembly member Matt Dababneh withdrew the bill.[302] The rejection of Assembly Bill 1326 suggests that a bill will not pass unless its scope is clearly defined.

VIII. Suggested Regulation

Any state or federal regulation enacted should be specifically tailored for BitCoin and should supersede other regulatory regimes.[303] Such regulations should protect users while "preserv[ing] the benefits of innovation and allow[ing] new business models to experiment, compete fairly, and flourish."[304] Regulations specifically targeted as the risks associated with BitCoin properly balance the development of innovative technologies while ensuring "that products or practices that are harmful are appropriately contained."[305] BitCoins consist of essentially three main actors, each of which should be examined individually to determine what risks they cause consumers, and should be regulated in accordance with those risks.[306]

---

essary to complete the transaction").

[298] *See* Aaron Mackey, *California Lawmaker Pulls Digital Currency Bill After EFF Opposition*, Electronic Frontier Found. (Aug. 18, 2016), https://www.eff.org/deeplinks/2016/08/california-lawmaker-pulls-digital-currency-bill-after-eff-opposition [https://perma.cc/8ULC-NZKT].

[299] *Id.*

[300] *Id.*

[301] *Id.*

[302] *See* Dababneh, *supra* note 292.

[303] *See* Lim, *supra* note 122, at 368.

[304] *Id.*

[305] *Id.*

[306] *See generally* Jerry Brito & Peter Van Valkenburgh, State Digital Currency Principles and Framework (2015), https://coincenter.org/wpcontent/uploads/2015/04/StatePrinciplesandFrameworkV1-0.pdf [https://perma.cc/ZP9E-X3VE].

A.   Regulation of Trusted Providers

BitCoins "can *only* be transmitted by the holders of unique cryptographic keys."[307] BitCoin users trust certain intermediaries that have the power to unilaterally execute or prevent a transaction on behalf of the user.[308] There is risk to consumers when a business has the ability to lose, "misspend, permanently immobilize, or fail to protect a customer's funds entrusted to them."[309] Tailored regulations should be limited to these trusted providers,[310] which have the power to unilaterally execute or prevent transactions on behalf of users.[311]

These services should be required to implement consumer protection and cyber security safeguards, such as those discussed in the CSBS model framework.[312] Following the model framework, these businesses should be required to register with their given state regulatory authority, and registration should take place on a uniform application that streamlines the process and makes it easy for regulators in different states to interact.[313] Registered companies should ensure that deposits from users are kept separately and identifiably from other users.[314] Notice should be provided to alert users to the risks associated with using the service, including whether there is any virtual currency insurance protecting the user against loss.[315] The trusted provider should also keep accurate financial books and records.[316] Moreover, these services must implement advanced security procedures, which

---

[307] *Id.* at 2.

[308] *Id.*

[309] *Id.* at 5.

[310] *Id.* at 3 ("Trusted intermediaries, on the other hand, so long as they walk and quack like a money transmitting duck, offer the same case for regulation as traditional financial services.").

[311] *Id.* at 1 ("[O]nly a business that holds these [unique cryptographic] keys could ever have the ability to create a bitcoin transmission. A transmittal instrument for a digital currency is not, then, a promise to pay: it is the ability to pay—i.e. cash on hand—as measured by possession or knowledge of cryptographic keys sufficient to execute or prevent a transaction.").

[312] CSBS Model, *supra* note 243, at 13.

[313] *Id.* at 12.

[314] *Id.* at 13.

[315] *Id.*

[316] *Id.* at 13–14.

should be reported to the regulator, and the entity should be subject to audit to ensure the procedures are adequate.[317]

Consider the effect such regulations would have had on Mt. Gox.[318] The users impacted by the Mt. Gox breach not only used Mt. Gox to exchange traditional currency for BitCoins, but they also stored their private keys on Mt. Gox for convenience.[319] This means Mt. Gox had the power to unilaterally transfer those BitCoins because it held both the public and private keys.[320] If the CSBS regulations had been implemented, Mt. Gox would have been regulated due to its unilateral control.[321] The impact of these regulations would have greatly reduced the risk to the effected consumers.[322] Specifically, the advanced security features requirement would have ensured that Mt. Gox's internal database that contained the private keys was secure.[323] Alternatively, if Mt. Gox had been audited, the security shortcomings would have been exposed sooner.[324] Service that do not hold both keys, however, do not require such stringent regulations because they are unable to transfer BitCoins.[325]

B.   Regulation of Miners

Individuals or entities that hold BitCoins on behalf of users, but do not have the ability to unilaterally transfer or prevent transfers should not be regulated.[326] For example, BitCoin miners have the ability to validate BitCoin transactions,[327] but a specific miner

---

[317] *Id.* at 13.

[318] *See* McMillan, *supra* note 88 .

[319] Nicholas Galunic, *The (Private) Key To Unlocking Bitcoin Legal Issues*, Law360 (Feb. 19, 2015, 10:38 AM), https://www.law360.com/articles/622698/the-private-key-to-unlocking-bitcoin-legal-issues [https://perma.cc/3MN5-7879].

[320] *Id.*

[321] *See* CSBS Model, *supra* note 243, at 8 ("Entities that manage private keys for a public ledger risk losing customer funds if the private keys become unavailable upon failure. At a minimum, policies and procedures should cover how private keys are transferred or recovered in the event a licensee goes out of business.").

[322] *Id.* at 14.

[323] *See id.* at 12–14.

[324] *Id.* at 6.

[325] *Id.* at 3.

[326] Brito & Valkenburgh, *supra* note 309, at 4.

[327] *Id.* at 10.

cannot unilaterally control the flow of BitCoin.[328] The network itself, composed of many miners, controls the transaction,[329] and "[i]f a miner attempts to mark as valid a fraudulent transaction, the miner's work would be rejected by other network participants."[330] By spreading this power over many miners, potential nefarious miners lack the ability to approve or reject transactions.[331] Even if a specific miner wanted to fraudulently approve or reject a transaction, this would not pose a risk to individual transactions or to the marketplace of BitCoin transaction as a whole because of the other miners.[332] Therefore, miners should not be regulated.[333]

This argument parallels the Financial Crimes Enforcement Network (FinCEN) guidance, which states that BitCoin miners cannot be regulated as money transmitters.[334] Users who subsequently convert BitCoin "into real currency" are not to be regulated under this regime.[335] The architect of New York's BitLicense agrees, stating, "We are regulating financial intermediaries. We are not regulating software development."[336] In sum, mining does not pose a risk to consumers and therefore should not be regulated.[337]

C.   Regulation of Basic BitCoin Transactions

Users and merchants who simply want to transact BitCoins for goods and services also should not be regulated.[338] Such a regulation would "levy burdensome obligations on users," increase

---

[328] *Id.*

[329] *Id.*

[330] *Id.*

[331] *See id.* ("Therefore, in contrast to the unchecked power of a centralized digital currency administrator or issuer, individuals and businesses contributing to a decentralized digital currency are not trusted intermediaries.").

[332] *Id.*

[333] *Id.*

[334] *See* U.S. Dep't of the Treasury Fin. Crimes Enf't, FIN-2014-R001, Application of FinCEN's Regulations to Virtual Currency Mining Operations 3 (2014), https://www.fincen.gov/sites/default/files/shared/FIN-2014-R001.pdf [https://perma.cc/E6XC-B73A].

[335] *Id.*

[336] Brito & Valkenburgh, *supra* note 309, at 10–11.

[337] *Id.* at 11.

[338] *See* Letter, *supra* note 256, at 3.

transaction costs,[339] and chill innovation.[340] Moreover, regulating BitCoin transmission between users is not necessary because mere transmission does not pose risks to consumers, and the Blockchain itself provides adequate security.[341] First, the Blockchain ensures only valid transactions occur.[342] Second, because the true identity of a user and his or her personal information is anonymous in a BitCoin transfer, the possibility of identity theft is reduced.[343] Third, the Blockchain removes any potential for double-spending.[344] Fourth, private keys ensure only the holder of the BitCoin is able to spend it.[345] Fifth, BitCoin technology is incredibly transparent because every transaction is recorded on the Blockchain and publicly available online, the software that powers BitCoin is public, and any changes to the software are publically discussed and detailed.[346] In essence, there is no substantial risk associated with user-to-user BitCoin transfers because the Blockchain ensures only legitimate transactions are recorded.[347] Neither the CSBS model framework nor the New York BitLicense require registration for simple BitCoin denominated transactions,[348] which suggests that both the CSBS and New York regulators agree that the Blockchain is sufficient to allow for safe, online transactions. Accordingly, mere transfers need not be regulated.[349]

While Silk Road might suggest that BitCoin transactions should be regulated,[350] the Blockchain itself provides several features

---

[339] *Id.* at 2

[340] *Id.* at 2.

[341] *See Van* Valkenburgh, *supra* note 126, at 32 ("[B]itcoin's software has been scrutinized by a large though ultimately unknowable number of security analysts, critics, hackers, and academics. This means that it is unlikely that any backdoor or severe vulnerability exists in the protocol.").

[342] *See* Nakamoto, *supra* note 13, at 3–4; Van Valkenburgh, *supra* note 126, at 33.

[343] Nakamoto, *supra* note 13, at 6.

[344] *Cf.* Van Valkenburgh, *supra* note 126, at 33.

[345] *See id.* at 32–33; *How does Bitcoin Work?*, bitcoin, https://bitcoin.org/en/how-it-works [https://perma.cc/P6E2-CDTH].

[346] *E.g.*, Van Valkenburgh, *supra* note 126, at 30–36.

[347] Letter, *supra* note 256, at 3.

[348] *See* CSBS Model, *supra* note 243 (lacking any requirement for Bitcoin registration); *supra* note 270–73 and accompanying text (discussing New York's conditional license).

[349] Letter, *supra* note 256, at 3.

[350] *See* Weiser & Apuzzo, *supra* note 99 (outlining that the silk road was an

to help law enforcement in dealing with such cases.[351] The security issue present with BitCoin is determining the identity of the individual that corresponds to the BitCoin used in such a transaction.[352] This is not unique to BitCoin; rather, it is a problem that law enforcement faces in other cybercrimes as well.[353] However, using data from multiple sources, including the Blockchain, law enforcement is able to create a map to determine who owns a BitCoin used in an illegal transaction.[354] The Blockchain provides an instantly available and permanent record for BitCoins, including those used to purchases illicit goods and services.[355] Moreover, transactions that cross into other countries traditionally require "Mutual Legal Assistance Treaty (MLAT) process to seek foreign law enforcement assistance to obtain that evidence."[356] Since the Blockchain has no borders or international limitations because it exists on a distributed network of computers across the world, MLATs are unnecessary because law enforcement does not have to enter a foreign country to collect evidence.[357] Therefore, crime risk is reduced because of the Blockchain ledger.[358]

   In sum, the various actors in the BitCoin framework should be regulated differently since each poses unique risks to consumers.

---

online marketplace that allowed users to exchange BitCoins for drugs and weapons).

[351] Jerry Brito, *Silk Road Corruption Case Shows How Law Enforcement Uses Bitcoin*, Coin Center (Apr. 1, 2015), https://coincenter.org/entry/silk-road-corruption-case-shows-how-law-enforcement-uses-bitcoin [https://perma.cc/ZA5H-A7HF].

[352] Jason Weinstein, *How Can Law Enforcement Leverage The Blockchain in Investigations?*, Coin Center (May 12, 2015), https://coincenter.org/entry/how-can-law-enforcement-leverage-the-blockchain-in-investigations [https://perma.cc/S6FK-WRZK].

[353] *Id.*

[354] *Id.*; *see* Brito, *supra* note 354 (showing how IRS agents used the Blockchain to find a DEA agent who stole BitCoins during his investigation); Murphy et al., *supra* note 2, at 3 ("Because of the public ledger, researchers have found that, using sophisticated computer analysis, transactions involving large quantities of Bitcoin can be tracked . . . .").

[355] Weinstein, *supra* note 355 ("[T] the blockchain allows one to trace all transactions involving a given bitcoin address, all the way back to the first transaction. That gives law enforcement the records it needs to "follow the money" in a way that would never be possible with cash.").

[356] *See id.*

[357] *See id.*

[358] *Id.*

First, providers that have unilateral control over a user's BitCoins, including certain BitCoin exchanges and wallets, should be regulated when they hold both the public address and the private key required to transfer BitCoins.[359] Second, users that mine for BitCoins do not pose risks to consumers, because they do not possess unilateral control over users' BitCoins, and therefore should not be regulated.[360] Third, mere transactions in BitCoin do not pose risks to consumers and should not be regulated, so that use of BitCoins is encouraged.[361]

D.   Startup Exemption

Startups and small businesses should be exempt from the full scope of BitCoin regulations in order to encourage innovation.[362] As previously discussed, the New York BitLicense provides for a two-year conditional license that exempts, at the sole discretion of the superintendent, startups from the full scope of the regulations.[363] Exemptions that give regulators the option to provide a business relief from onerous regulation, like the New York conditional license, are helpful, but are not sufficient.[364] The uncertainty of whether an exemption will be granted (or even revoked) makes it difficult for a startup to plan ahead.[365] Instead, states should implement specific carve-outs for startups to reduce uncertainty.[366] These provisions should be clearly written to enable entrepreneurs to know whether their business is exempt.[367]

The startup carve-out could be a function of several factors. First, businesses that stay below a monetary threshold should be

---

[359] Brito & Van Valkenburgh, *supra* note 309, at 6.

[360] *See id.* at 10.

[361] *See id.* at 7.

[362] *See* Letter, *supra* note 256, at 5 ("[A]ny innovation friendly regulation of digital currency requires an exemption for start-ups, academics, and hobbyists."). *But see* CSBS Model, *supra* note 243, at 3–4 (stating that the model framework does not include an exception to the rules for startups because harm to consumers is still possible, however, it suggests that individual states may adopt these exceptions to test out the usefulness for the remaining states).

[363] *See supra* notes 270–73 and accompanying text.

[364] Brito & Van Valkenburgh, *supra* note 309, at 2.

[365] *Id.* at 20–21.

[366] *See id.* at 21 ("Small startups can be shielded from the costs of regulation by explicitly exempting them from regulation up until the point at which they pose serious consumer protective risks.").

[367] *Id.* at 22.

exempt.[368] The threshold could be raised if market conditions suggest a larger limit is appropriate, but those changes "should be explicit, apply generally across the industry, and be announced in advance so that firms can plan their compliance strategies efficiently."[369] Startups that exceed the threshold should be given a transition period wherein the startup could either return to below the threshold and continue its exemption, or adopt appropriate controls to meet the regulations.[370] Lastly, these companies must be required to provide notice to users detailing their unregulated status and how this status makes the use of their service risky.[371]

Overall, regulated services should mostly be concerned with keeping users' information and BitCoins safe from hackers, while providing consumers clear notice of the risks associated with using the services. The biggest risk to consumers comes from businesses that have unilateral control to transfer or block a transfer, so regulations should target that risk.[372] Startups should be provided a clearly defined exemption, rather than an exemption granted at the discretion of the regulator.[373] If startups are overly regulated, the cost of compliance will counterbalance the cost savings associated with BitCoin.[374] Minimal regulations will foster innovation and preserve BitCoin's low costs and quick processing, while the Blockchain will ensure that transactions are secure.

---

[368] *Id.* at 21–22 ("The $5 million per year transaction level is an appropriate threshold among companies that can pose serious, systemic risks to consumers (e.g. Mt. Gox), and those where risk-level is tolerable given the benefits that unfettered start-up innovation could bring.").

[369] *Id.* at 22.

[370] *Id.* at 21 ("This threshold could change from time to time or be based on some other ex ante specification (e.g. a time-delimited safe-harbor for companies younger than two years), affording the regulator some discretion to adjust regulatory policies in response to observed rates of fraud, consumer harm, or other extenuating circumstances.").

[371] *Id.*

[372] *Id.* at 6–13.

[373] *Id.* at 20.

[374] *Id.* ("As technological limits on diversity and scalability are lifted, it is important that those limits are not merely reinstated by a costly regulatory structure that is insensitive to the small size or rapid growth of new and innovative players,").

IX.   *Conclusion*

Thus far, BitCoin regulations are unsettled and often at odds with one another. Federal courts have forced BitCoin schemes into the securities laws,[375] while some federal agencies now treat BitCoin as property[376] or commodities.[377] Meanwhile, some states have tried to regulate simple purchases made in BitCoin[378] or have made it difficult for startups to innovate.[379] Optimal regulations balance the policy objectives of BitCoin, namely reduced transaction costs and quick processing, with security concerns. Specifically, only trusted intermediaries that have complete control to make or reject a transaction on a user's behalf should be regulated.[380] Simple user-to-user BitCoin transactions should not be regulated, and there should be a clearly defined exemption for small businesses. These regulations would preserve the benefits of BitCoin transactions, ensure the security of certain necessary exchanges, and allow small companies to innovate without being overwhelmed by regulation.

---

[375] S.E.C. v. Shavers, No. 4:13–CV–416, 2013 WL 4028182, at *2 (E.D. Tex. Aug. 6, 2013).

[376] *See* I.R.S. Notice 2014-21 (Apr. 14, 2014), https://www.irs.gov/pub/irs-drop/n-14-21.pdf [https://perma.cc/Y4K9-B8DH].

[377] *In re* Coinflip, Inc., CFTC No. 15-29, 2015 WL 5535736 (Sept. 17, 2015).

[378] *See* Mackey, *supra* note 301 (explaining that a proposed California bill would have subjected essentially anyone who used Bitcoin for any purpose to registration requirements and other regulations).

[379] *Cf.* Weinberger, *supra* note 280 ("[T]he North Carolina law does not provide small-scale innovators . . . the kinds of protection that would allow further virtual currency developments.").

[380] *See* Lim, *supra* note 122, at 370.