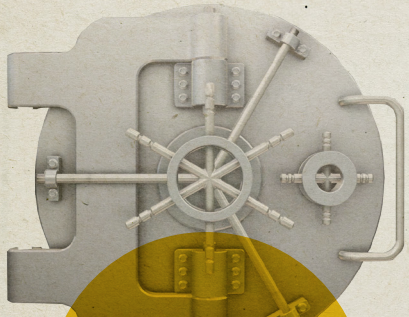

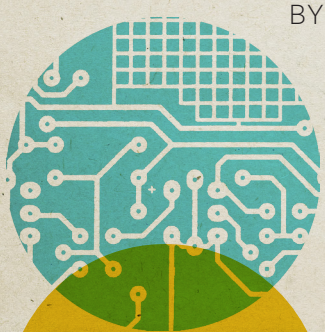

BITCOIN

A Primer for Policymakers

BY JERRY BRITO AND ANDREA CASTILLO

MERCATUS CENTER
George Mason University

Mercatus Center
George Mason University
3351 Fairfax Drive, 4th Floor
Arlington, VA 22201-4433
(703) 993-4930
mercatus.org

Bitcoin is the world's first completely decentralized digital currency. Four short years ago, knowledge of it was confined to a handful of hobbyists on Internet forums. Today, the bitcoin economy is larger than the economies of some of the world's smaller nations. The value of a bitcoin (or BTC) has grown and fluctuated greatly, from pennies in its early days to more than $260 at its peak in April 2013. The current market capitalization of the bitcoin economy is estimated to be more than $1 billion.[1] Businesses big and small have shown interest in integrating the Bitcoin platform into their operations and providing new services within the bitcoin economy. Venture capitalists, too, are eager to put their money behind this growing industry.[2] The development of Bitcoin and its early successes are an exciting testament to the ingenuity of the modern entrepreneur.

Because Bitcoin is decentralized, it can be used pseudonymously, and this has attracted the attention of regulators. The same qualities that make Bitcoin attractive as a payment system could also allow users to evade taxes, launder money, and trade illicit goods. Both the Financial Crimes Enforcement

1. Financial information provided at bitcoincharts.com estimates total market capitalization to be $1,457,815,292 as of May 29, 2013.

2. Sarah E. Needleman and Spencer E. Ante, "Bitcoin Startups Begin to Attract Real Cash," *Wall Street Journal*, May 8, 2013, http://online.wsj.com/article/SB10001424127887323687604578469012375269952.html.

Network (FinCEN) of the US Department of the Treasury[3] and the Department of Justice[4] have released official statements regarding the regulation of virtual currencies, including Bitcoin. A Government Accountability Office report on virtual currencies urged the IRS to reduce tax-compliance risks by issuing a guidance.[5] The appendix of that report contains a letter from IRS Deputy Commissioner Steven T. Miller, who assured the office that the IRS is "working to address these risks." Additionally, a commissioner of the Commodities Futures Trading Commission recently expressed interest in exploring whether Bitcoin falls within the commission's jurisdiction.[6] In considering how to best oversee this still-nascent technology, government regulators should take care that their overlapping directives do not hinder the promising growth potential of this innovative financial platform.

This paper will provide a short introduction to the Bitcoin network, including its properties, operations, and pseudonymous character. It will describe the benefits of allowing the Bitcoin network to develop and innovate, while highlighting issues of concern for consumers, policymakers, and regulators. It will describe the current regulatory landscape and explore other

---

3. US Department of the Treasury, Financial Crimes and Enforcement Network, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies" (Regulatory Guidance, FIN-2013-G001, US Department of the Treasury, Washington, DC, March 18, 2013), http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

4. Jennifer Shasky Calvery, "Combating Transnational Organized Crime: International Money Laundering as a Threat to Our Financial Systems" (Statement for the Record Before the Subcommittee on Crime, Terrorism, and Homeland Security of the House Committee on the Judiciary, February 8, 2012), http://www.justice.gov/ola/testimony/112-2/02-08-12-crm-shasky-calvery-testimony.pdf.

5. US Government Accountability Office, "Virtual Economies and Currencies: Additional IRS Guidance Could Reduce Compliance Risks" (report to the Senate Committee on Finance, GAO-13-516, May, 2013), http://www.gao.gov/assets/660/654620.pdf.

6. Tracy Alloway, Gregory Meyer, and Stephen Foley, "US Regulators Eye Bitcoin Supervision," *Financial Times*, May 6, 2013, http://www.ft.com/intl/cms/s/0/b810157c-b651-11e2-93ba-00144feabdc0.html.

potential regulations that could be promulgated. The paper will conclude by providing policy recommendations that will assuage policymakers' common concerns while allowing for innovation within the Bitcoin network.

WHAT IS BITCOIN?

Bitcoin is an open-source, peer-to-peer digital currency. Among many other things, what makes Bitcoin unique is that it is the world's first completely decentralized digital-payments system. This may sound complicated, but the underlying concepts are not difficult to understand.

Overview

Until Bitcoin's invention in 2008 by the unidentified programmer known as Satoshi Nakamoto, online transactions always required a trusted third-party intermediary. For example, if Alice wanted to send $100 to Bob over the Internet, she would have had to rely on a third-party service like PayPal or MasterCard. Intermediaries like PayPal keep a ledger of account holders' balances. When Alice sends Bob $100, PayPal deducts the amount from her account and adds it to Bob's account.

Without such intermediaries, digital money could be spent twice. Imagine there are no intermediaries with ledgers, and digital cash is simply a computer file, just as digital documents are computer files. Alice could send $100 to Bob by attaching a money file to a message. But just as with email, sending an attachment does not remove it from one's computer. Alice would retain a copy of the money file after she had sent it. She could then easily send the *same* $100 to Charlie. In computer science, this is known as the "double-spending" problem,[7] and

7. David Chaum, "Achieving Electronic Privacy," *Scientific American*, August 1992, 96–101.

until Bitcoin it could only be solved by employing a ledger-keeping trusted third party.

Bitcoin's invention is revolutionary because for the first time the double-spending problem can be solved without the need for a third party. Bitcoin does this by distributing the necessary ledger among all the users of the system via a peer-to-peer network. Every transaction that occurs in the bitcoin economy is registered in a public, distributed ledger, which is called the block chain. New transactions are checked against the block chain to ensure that the same bitcoins haven't been previously spent, thus eliminating the double-spending problem. The global peer-to-peer network, composed of thousands of users, takes the place of an intermediary; Alice and Bob can transact without PayPal.

One thing to note right away is that transactions on the Bitcoin network are not denominated in dollars or euros or yen as they are on PayPal, but are instead denominated in bitcoins. This makes it a virtual currency in addition to a decentralized payments network. The value of the currency is not derived from gold or government fiat, but from the value that people assign to it. The dollar value of a bitcoin is determined on an open market, just as is the exchange rate between different world currencies.[8]

Operation

So far we have discussed what Bitcoin is: a decentralized peer-to-peer payments network and a virtual currency that essentially operates as online cash. Now we will take a closer look at how Bitcoin works.

8. "Markets," Bitcoincharts, accessed July 30, 2013, http://bitcoincharts.com/markets/.

Transactions are verified, and double-spending is prevented, through the clever use of public-key cryptography.[9] Public-key cryptography requires that each user be assigned two "keys," one private key that is kept secret like a password, and one public key that can be shared with the world. When Alice decides to transfer bitcoins to Bob, she creates a message, called a "transaction," which contains Bob's public key, and she "signs" it with her private key. By looking at Alice's public key, anyone can verify that the transaction was indeed signed with her private key, that it is an authentic exchange, and that Bob is the new owner of the funds. The transaction—and thus the transfer of ownership of the bitcoins—is recorded, time-stamped, and displayed in one "block" of the block chain. Public-key cryptography ensures that all computers in the network have a constantly updated and *verified* record of all transactions within the Bitcoin network, which prevents double-spending and fraud.

What does it mean when we say that "the network" verifies transactions and reconciles the ledger? And how exactly are new bitcoins created and introduced into the money supply? As we have already seen, because Bitcoin is a peer-to-peer network, there is no central authority charged with either creating currency units or verifying transactions. This network depends on users who provide their computing power to do the logging and reconciling of transactions. These users are called "miners"[10] because they are rewarded for their work with newly created bitcoins. Bitcoins are created, or "mined," as thousands of dispersed

---

9. Christof Paar, Jan Pelzl, and Bart Preneel, "Introduction to Public-Key Cryptography," chapter 6 in *Understanding Cryptography: A Textbook for Students and Practitioners*, ed. Christof Paar and Jan Pelzl (New York: Springer, 2010). Sample available at http://wiki.crypto.rub.de/Buch/download/Understanding-Cryptography-Chapter6.pdf.

10. Miners tend to be ordinary computer enthusiasts, but as mining becomes more difficult and expensive, the activity will likely become somewhat professionalized. For more information, see Alec Liu, "A Guide to Bitcoin Mining," *Motherboard*, March 22, 2013, http://motherboard.vice.com/blog/a-guide-to-bitcoin-mining-why-someone-bought-a-1500-bitcoin-miner-on-ebay-for-20600.

computers solve complex math problems that verify the transactions in the block chain. As one commentator has put it,

> The actual mining of Bitcoins is by a purely mathematical process. A useful analogy is with the search for prime numbers: it used to be fairly easy to find the small ones (Eratosthenes in Ancient Greece produced the first algorithm for finding them). But as they were found it got harder to find the larger ones. Nowadays researchers use advanced high-performance computers to find them and their achievements are noted by the mathematical community (for example, the University of Tennessee maintains a list of the highest 5,000).
>
> For Bitcoins the search is not actually for prime numbers but to find a sequence of data (called a "block") that produces a particular pattern when the Bitcoin "hash" algorithm is applied to the data. When a match occurs the miner obtains a bounty of Bitcoins (and also a fee if that block was used to certify a transaction). The size of the bounty reduces as Bitcoins around the world are mined.
>
> The difficulty of the search is also increased so that it becomes computationally more difficult to find a match. These two effects combine to reduce over time the rate at which Bitcoins are produced and mimic the production rate of a commodity like gold. At some point new Bitcoins will not be produced and the only incentive for miners will be transaction fees.[11]

So, the protocol was designed so that each miner contributes a computer's processing power toward maintaining the infrastructure needed to support and authenticate the currency network.

---

11. Ken Tindell, "Geeks Love the Bitcoin Phenomenon Like They Loved the Internet in 1995," *Business Insider*, April 5, 2013, http://www.businessinsider.com/how-bitcoins-are-mined-and-used-2013-4.

Miners are awarded newly created bitcoins for contributing their processing power toward maintaining the network and verifying transactions in the block chain. And as more processing power is dedicated to mining, the protocol will increase the difficulty of the math problem, ensuring that bitcoins are always mined at a predictable and limited rate.

This process of mining bitcoins will not continue forever. Bitcoin was designed to mimick the extraction of gold or other precious metals from the earth—only a limited, known number of bitcoins can ever be mined. The arbitrary number chosen to be the cap is 21 million bitcoins. Miners are projected to painstakingly harvest the last "satoshi," or 0.00000001 of a bitcoin, in the year 2140. If the total mining power scales to a high enough level, the difficulty in mining bitcoins will have increased so much that procuring this last satoshi will be quite a challenging digital undertaking. Once the last satoshi has been mined, miners that contribute their processing power toward verifying transactions will be rewarded through transaction fees rather than mined bitcoins. This ensures that miners still have an incentive to keep the network running after the last bitcoin is mined.

Pseudonymity

A great deal of attention given to Bitcoin in the media centers on the anonymity that the digital currency is supposed to lend its users. This idea stems from a mistaken understanding of the currency, however.

Because online transactions to date have required a third-party intermediary, they have not been anonymous. PayPal, for example, will have a record of every time Alice has sent Bob money. And because Alice's and Bob's PayPal accounts are tied to their respective bank accounts, their identities are likely known. In contrast, if Alice gives Bob a $100 bill in cash, there is no intermediary and no record of the transaction. And if Alice and Bob don't know each other's identities, we can say the transaction is completely anonymous.

Bitcoin falls somewhere between these two extremes. On the one hand, bitcoins are like cash in that once Alice gives bitcoins to Bob, she no longer has them and Bob does, and there is no third-party intermediary between them that knows their respective identities. On the other hand, unlike cash, the fact that a transaction took place between two public keys, the time, the amount, and other information is recorded in the block chain. Indeed, every transaction that has ever occurred in the history of the bitcoin economy is publicly viewable in the block chain.[12]

While the public keys for all transactions—also known as "Bitcoin addresses"[13]—are recorded in the block chain, those public keys are not tied to anyone's identity. Yet if a person's identity were linked to a public key, one could look through the recorded transactions in the block chain and easily see all transactions associated with that key. So, while Bitcoin is very similar to cash in that parties can transact without disclosing their identities to a third party or to each other, it is unlike cash in that all the transactions to and from a particular Bitcoin address can be traced. In this way Bitcoin is not anonymous, but pseudonymous.

Tying a real-world identity to a pseudonymous Bitcoin address is not as difficult as some might imagine. For one thing, a person's identity (or at least identifying information, such as an IP address) is often recorded when the person makes a Bitcoin transaction at a website, or exchanges dollars for bitcoins at a bitcoin exchange. To increase the chances of remaining pseudonymous, one would have to employ anonymizing software like Tor, and take care never to transact with Bitcoin addresses that could be tied back to one's identity.

Finally, it is also possible to glean identities simply by looking at the block chain. One study found that behavior-based clustering techniques could reveal the identities of 40 percent of Bitcoin

12. Note that this might be a boon to economic researchers.

13. *Bitcoin wiki*, s.v. "Address," accessed July 30, 2013, https://en.bitcoin.it/wiki/Address.

users in their simulated Bitcoin experiment.[14] An early analysis of the statistical properties of the Bitcoin transaction graph showed how a passive network analysis with the appropriate tools can divulge the financial activity and identities of Bitcoin users.[15] A later analysis of the statistical properties of the Bitcoin transaction graph garnered similar results with a larger dataset.[16] Another analysis of the Bitcoin transaction graph reiterated that observers using "entity merging"[17] can observe structural patterns in user behavior and emphasized that this is "one of the most important challenges to Bitcoin anonymity."[18] In spite of this, Bitcoin users do enjoy a much higher level of privacy than do users of traditional digital-transfer services, who must provide detailed personal information to the third-party financial intermediaries that facilitate the exchange.

Although Bitcoin is frequently referred to as an "anonymous" currency, in reality, it is very difficult to stay anonymous in the Bitcoin network. Pseudonyms tied to transactions recorded in the public ledger can be identified years after an exchange is made. Once Bitcoin intermediaries are fully compliant with the bank-secrecy regulations required of traditional financial intermediaries, anonymity will be even less guaranteed, because Bitcoin intermediaries will be required to collect personal data on their customers.

---

14. Elli Androulaki et al., "Evaluating User Privacy in Bitcoin," *IACR Cryptology ePrint Archive* 596 (2012), http://fc13.ifca.ai/proc/1-3.pdf.

15. Fergal Reid and Martin Harrigan, "An Analysis of Anonymity in the Bitcoin System," in *Security and Privacy in Social Networks*, ed. Yaniv Altshuler et al. (New York: Springer, 2013), http://arxiv.org/pdf/1107.4524v2.pdf.

16. Dorit Ron and Adi Shamir, "Quantitative Analysis of the Full Bitcoin Transaction Graph," *IACR Cryptology ePrint Archive* 584 (2012), http://eprint.iacr.org/2012/584.pdf.

17. Entity merging is the process of observing two or more public keys used as an input to one transaction at the same time. In this way, even if a user has several different public keys, an observer can gradually link them together and remove the ostensible anonymity that multiple public keys is thought to provide.

18. Micha Ober, Stefan Katzenbeisser, and Kay Hamacher, "Structure and Anonymity of the Bitcoin Transaction Graph," *Future Internet* 5, no. 2 (2013), http://www.mdpi.com/1999-5903/5/2/237.

BENEFITS

THE FIRST QUESTION that many people have when they learn about Bitcoin is, Why would I want to use bitcoins when I can use dollars? Bitcoin is still a new and fluctuating currency that is not accepted by many merchants, so the uses for Bitcoin may seem mostly experimental. To better understand why people might want to use Bitcoin, it helps to think of it, not necessarily as a replacement for traditional currencies, but rather as a new payments system.

Lower Transaction Costs

Because there is no third-party intermediary, Bitcoin transactions are substantially cheaper and quicker than traditional payment networks. And because transactions are cheaper, Bitcoin makes micropayments and other innovations possible. Additionally, Bitcoin holds much promise as a way to lower transaction costs for small businesses and global remittances, alleviate global poverty by improving access to capital, protect individuals against capital controls and censorship, ensure financial privacy for oppressed groups, and spur innovation (within and on top of the Bitcoin protocol). On the other hand, Bitcoin's decentralized nature also presents opportunities for crime. The challenge, then, is to develop processes that diminish the opportunities for criminality while maintaining the benefits that Bitcoin can provide.

First, Bitcoin is attractive to cost-conscious small businesses looking for ways to lower the transaction costs of doing business. Credit cards have greatly expanded the ease of transacting, but their use comes with considerable costs to merchants. Businesses that wish to offer the option of credit card payments to their customers must first pay for a merchant account with each credit card company. Depending on the terms of agreement with each credit card company, businesses must then pay a variety of authorization fees, transaction fees, statement fees, interchange fees, and customer-service fees, among other charges. These fees

quickly add up and significantly increase the cost of doing business. However, if a merchant neglects to accept credit card payments to save on fees, he or she could lose a considerable amount of business from customers who enjoy the ease of credit cards.

Since Bitcoin facilitates direct transactions without a third party, it removes costly charges that accompany credit card transactions. The Founders Fund, the venture capital fund headed by Peter Thiel of PayPal and Facebook fame, recently invested $3 million in the payment-processing company BitPay because of the service's ability to lower the costs of doing online commerce across borders.[19] In fact, small businesses have already started to accept bitcoins as a way to avoid the costs of doing business with credit card companies.[20] Others have adopted the currency for its speed and efficiency in facilitating transactions.[21] Bitcoin will likely continue to lower transaction costs for businesses that accept it as more people adopt the currency.

Accepting credit card payments also puts businesses on the hook for charge-back fraud. Merchants have long been plagued by fraudulent "charge-backs," or consumer-initiated payment reversals based on a false claim that a product has not been delivered.[22]

---

19. Tom Simonite, "Bitcoin Hits the Big Time, to the Regret of Some Early Boosters," *MIT Technology Review*, May 22, 2013, http://www.technologyreview.com/news/515061/bitcoin-hits-the-big-time-to-the-regret-of-some-early-boosters/.

20. Gabrielle Karol, "Small Business Owners Say Bitcoins Better Than Credit Cards," *FOX Business, Small Business Center*, April 12, 2013, http://smallbusiness.foxbusiness.com/entrepreneurs/2013/04/12/small-business-owners-say-bitcoins-better-than-credit-cards/.

21. Bailey Reutzel, "Why Some Merchants Accept Bitcoin Despite the Risks," *Payments Source*, May 21, 2013, http://www.paymentssource.com/news/why-some-merchants-accept-bitcoin-despite-the-risks-3014183-1.html.

22. Emily Maltby, "Chargebacks Create Business Headaches," *Wall Street Journal*, February 10, 2011, http://online.wsj.com/article/SB10001424052748704698004576104554234202010.html. One such scam involves Alice sending Bob a PayPal payment for a laptop that Bob has listed on Craigslist. Alice comes by Bob's house, picks up the laptop, and soon thereafter initiates a "charge-back" (i.e., reverses the payment). PayPal generally requires proof of shipment before reversing a charge-back, so Bob is out of luck.

Merchants therefore can lose the payment for the item and the item itself, and also have to pay a fee for the charge-back. As a nonreversible payment system, Bitcoin eliminates the "friendly fraud" wrought by the misuse of consumer charge-backs. This can be very important for small businesses.

Consumers like charge-backs, however, because that system protects them from unscrupulous merchants or merchant errors. Consumers may also enjoy other benefits that merchant-account fees help fund. Indeed, many consumers and merchants will probably stick to traditional credit card services even if Bitcoin payments become available. Still, the expanded choices in payment options would benefit people of all preferences.

Those who want the protection and perks of using a credit card can continue to do so, even if they pay a little more. Those who are more price- or privacy-conscious can use bitcoins instead. Not having to pay merchant fees means that merchants who accept Bitcoin have the option to pass the savings on to consumers. That is the business model of the Bitcoin Store,[23] which sells thousands of consumer electronics at discounted prices and only accepts bitcoins. The same Samsung Galaxy Note tablet that sells on Amazon for $779 plus shipping[24] sells at the Bitcoin Store for a mere $480.[25] In this way, Bitcoin provides more low-cost options to bargain hunters and small businesses without detracting from the traditional credit card services that some consumers prefer.

---

23. Vitalik Buterin, "Bitcoin Store Opens: All Your Electronics Cheaper with Bitcoins," *Bitcoin Magazine,* November 5, 2012, http://bitcoinmagazine.com/bitcoin-store-opens-all-your-electronics-cheaper-with-bitcoins/.

24. Amazon listing for a Samsung Galaxy Note tablet, accessed May 29, 2013, http://amzn.com/B00BJXNGIK.

25. Bitcoin Store listing for a Samsung Galaxy Note tablet, accessed May 29, 2013, https://www.bitcoinstore.com/samsung-galaxy-note-gt-n8013-10-1-32-gb-tablet-wi-fi-1-40-ghz-deep-gray.html. Products on the Bitcoin store are priced in both bitcoins and US dollars. At the point of purchase, Bitpay, a Bitcoin payment processing company, determines the currency conversion rate and holds that price for 15 minutes. See the Bitcoin Store FAQ: https://www.bitcoinstore.com/faq.

As an inexpensive funds-transfer system, Bitcoin also holds promise for the future of low-cost remittances. In 2012, immigrants to developed countries sent at least $401 billion in remittances back to relatives living in developing countries.[26] The amount of remittances is projected to increase to $515 billion by 2015.[27] Most of these remittances are sent using traditional brick-and-mortar wire services such as Western Union and MoneyGram, which charge steep fees for the service and can take several business days to transfer the funds.[28] In the first quarter of 2013, the global average fee for sending remittances was 9.05 percent.[29] In contrast, transaction fees on the Bitcoin network tend to be less than 0.0005 BTC,[30] or 1 percent of the transaction.[31]This entrepreneurial opportunity to improve money transfers has attracted investments from big-name venture capitalists.[32] Even MoneyGram and Western Union are contemplating whether to integrate Bitcoin into their business models.[33] Bitcoin allows for instantaneous, inexpensive remittances, and the reduction in the cost of global remittances for consumers could be considerable.

---

26. World Bank Payment Systems Development Group, *Remittance Prices Worldwide: An Analysis of Trends in the Average Total Cost of Migrant Remittance Services* (Washington, DC: World Bank, 2013), http://remittanceprices.worldbank.org/~/media/FPDKM/Remittances/Documents/RemittancePriceWorldwide-Analysis-Mar2013.pdf.

27. Ibid.

28. Jessica Silver-Greenberg, "New Rules for Money Transfers, but Few Limits," *New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/02/business/new-rules-for-money-transfers-but-few-limits.html?pagewanted=all&_r=0.

29. World Bank, *Remittance Prices*.

30. *Bitcoin wiki,* s.v. "Transaction fees," accessed July 30, 2013, https://en.bitcoin.it/wiki/Transaction_fees.

31. Andrew Paul, "Is Bitcoin the Next Generation of Online Payments?," *Yahoo! Small Business Advisor*, May 24, 2013, http://smallbusiness.yahoo.com/advisor/bitcoin-next-generation-online-payments-213922448--finance.html.

32. Simonite, "Bitcoin Hits the Big Time."

33. Andrew R. Johnson, "Money Transfers in Bitcoins? Western Union, MoneyGram Weigh the Option," *Wall Street Journal*, April 18, 2013, http://online.wsj.com/article/SB10001424127887324493704578431000719258048.html.

Potential to Combat Poverty and Oppression

Bitcoin also has the potential to improve the quality of life for the world's poorest. Improving access to basic financial services is a promising antipoverty technique.[34] According to one estimate, 64 percent of people living in developing countries lack access to these services, perhaps because it is too costly for traditional financial institutions to serve poor, rural areas.[35] Because of the impediments to developing traditional branch banking in poor areas, people in developing countries have turned to mobile banking services for their financial needs. The closed-system mobile payment service M-Pesa has been particularly successful in countries such as Kenya, Tanzania, and Afghanistan.[36] Entrepreneurs are already moving to this model; the Bitcoin wallet service Kipochi recently developed a product that allows M-Pesa users to exchange bitcoins.[37] Mobile banking services in developing countries can be further augmented by the adoption of Bitcoin. As an open-system payment service, Bitcoin can provide people in developing countries with inexpensive access to financial services on a global scale.

Bitcoin might also provide relief to people living in countries with strict capital controls. The total number of bitcoins that can be mined is capped and cannot be manipulated. There is no central authority that can reverse transactions or prevent the exchange of bitcoins between countries. Bitcoin therefore provides an escape hatch for people who desire an alternative

---

34. Muhammad Yunus, *Banker to the Poor: Micro-lending and the Battle against World Poverty* (New York: Public Affairs, 2003).

35. Oya Pinar Ardic, Maximilien Heimann, and Nataliya Mylenko, "Access to Financial Services and the Financial Inclusion Agenda around the World" (Policy Research Working Paper, World Bank Financial and Private Sector Development Consultative Group to Assist the Poor, 2011), https://openknowledge.worldbank.org/bitstream/handle/10986/3310/WPS5537.pdf.

36. Jeff Fong, "How Bitcoin Could Help the World's Poorest People," *PolicyMic,* May 2013, http://www.policymic.com/articles/41561/bitcoin-price-2013-how-bitcoin-could-help-the-world-s-poorest-people.

37. Emily Spaven, "Kipochi launches M-Pesa Integrated Bitcoin Wallet in Africa," *CoinDesk*, July 19, 2013, http://www.coindesk.com/kipochi-launches-m-pesa-integrated-bitcoin-wallet-in-africa/.

to their country's devalued currencies or frozen capital markets. We have already seen examples of people turning to Bitcoin to evade the harmful effects of capital controls and central-bank mismanagement. Some Argentines, for instance, have adopted Bitcoin in response to the country's dual burdens of a 25 percent inflation rate and strict capital controls.[38] Demand for bitcoins is so strong in Argentina that one popular bitcoin exchange is planning to open an Argentine office.[39] Argentine Bitcoin use continues to surge in the face of Argentina's capital mismanagement.[40]

Individuals in oppressive or emergency situations might also benefit from the financial privacy that Bitcoin can provide. There are many legitimate reasons why people seek privacy in their financial transactions. Spouses fleeing abusive partners need some way to discreetly spend money without being tracked. People seeking controversial health services desire financial privacy from family members, employers, and others who might judge their decisions. Recent experiences with despotic governments suggest that oppressed citizens would benefit greatly from the ability to make private transactions free from the grabbing hands of tyrants. Bitcoin provides some of the privacy that has traditionally been afforded through cash—with the added convenience of digital transfer.

Stimulus for Financial Innovation

One of the most promising applications of Bitcoin is as a platform for financial innovation. The Bitcoin protocol contains the

38. Jon Matonis, "Bitcoin's Promise in Argentina," *Forbes*, April 27, 2013, http://www.forbes.com/sites/jonmatonis/2013/04/27/bitcoins-promise-in-argentina/.

39. Camila Russo, "Bitcoin Dreams Endure to Savers Crushed by CPI: Argentina Credit," *Bloomberg*, April 16, 2013, http://www.bloomberg.com/news/2013-04-16/bitcoin-dreams-endure-to-savers-crushed-by-cpi-argentina-credit.html.

40. Georgia Wells, "Bitcoin Downloads Surge in Argentina," *Wall Street Journal Money Beat*, July 17, 2013, http://blogs.wsj.com/moneybeat/2013/07/17/bitcoin-downloads-surge-in-argentina/.

digital blueprints for a number of useful financial and legal services that programmers can easily develop. Since bitcoins are, at their core, simply packets of data, they can be used to transfer, not only currencies, but also stocks, bets, and sensitive information.[41] Some of the features that are built into the Bitcoin protocol include micropayments, dispute mediations, assurance contracts, and smart property.[42] These features would allow for the easy development of Internet translation services, instantaneous processing for small transactions (like automatically metering Wi-Fi access), and Kickstarter-like crowdfunding services.

Additionally, programmers can develop alternative protocols on top of the Bitcoin protocol in the same way that the Web and email are run on top of the Internet's TCP/IP protocol. One programmer has already proposed a new protocol layer to add on top of the Bitcoin protocol that can improve the network's stability and security.[43] Another programmer created a digital notary service to anonymously and securely store a "proof of existence" for private documents on top of the Bitcoin protocol.[44] Other programmers have adopted the Bitcoin model as a

---

41. Jerry Brito, "The Top 3 Things I Learned at the Bitcoin Conference," *Reason*, May 20, 2013, http://reason.com/archives/2013/05/20/the-top-3-things-i-learned-at-the-bitcoi.

42. Mike Hearn, "Bitcoin 2012 London: Mike Hearn," YouTube video, 28:19, posted by "QueuePolitely," September 27, 2012, http://www.youtube.com/watch?v=mD4L7xDNCmA. Smart property is a concept to control ownership of an item through agreements made in the Bitcoin block chain. Smart property allows people to exchange ownership of a good or service once a condition is met using cryptography. Although smart property is still theoretical, the basic mechanisms are built into the Bitcoin protocol. See *Bitcoin wiki*, s.v., "Smart Property," accessed July 30, 2013, https://en.bitcoin.it/wiki/Smart_Property.

43. J. R. Willett, "The Second Bitcoin Whitepaper" (white paper, 2013), https://sites.google.com/site/2ndbtcwpaper/2ndBitcoinWhitepaper.pdf.

44. Jeremy Kirk, "Could the Bitcoin Network Be Used as an Ultrasecure Notary Service?," *ComputerWorld*, May 23, 2013, http://www.computerworld.com/s/article/9239513/Could_the_Bitcoin_network_be_used_as_an_ultrasecure_notary_service_.

way to encrypt email communications.[45] Another group of developers has outlined an add-on protocol that will improve the privacy of the network.[46] Bitcoin is thus the foundation upon which other layers of functionality can be built. The Bitcoin project can be best thought of as a process of financial and communicative experimentation. Policymakers should take care that their directives do not quash the promising innovations developing within and on top of this fledgling protocol.

CHALLENGES

Despite the benefits that it presents, Bitcoin has some downsides for potential users to consider. It has exhibited considerable price volatility throughout its existence. New users are at risk of improperly securing or even accidentally deleting their bitcoins if they are not cautious. Additionally, there are concerns about whether hacking could compromise the bitcoin economy.

Volatility

Bitcoin has weathered at least five significant price adjustments since 2011.[47] These adjustments resemble traditional speculative bubbles: overoptimistic media coverage of Bitcoin prompts waves of novice investors to pump up Bitcoin prices.[48] The exuberance reaches a tipping point, and the value eventually plummets.

---

45. Jonathan Warren, "Bitmessage: A Peer-to-Peer Message Authentication and Delivery System" (white paper, November 27, 2012), https://bitmessage.org/bitmessage.pdf.

46. Ian Miers et al., "Zerocoin: Anonymous Distributed E-Cash from Bitcoin" (working paper, the Johns Hopkins University Department of Computer Science, Baltimore, MD, 2013), http://spar.isi.jhu.edu/~mgreen/ZerocoinOakland.pdf.

47. Timothy B. Lee, "An Illustrated History of Bitcoin Crashes," *Forbes*, April 11, 2013, http://www.forbes.com/sites/timothylee/2013/04/11/an-illustrated-history-of-bitcoin-crashes/.

48. Felix Salmon, "The Bitcoin Bubble and the Future of Currency," *Medium*, April 3, 2013, https://medium.com/money-banking/2b5ef79482cb.

Newcomer investors eager to participate run the risk of overvaluing the currency and losing their money in a crash. Bitcoin's fluctuating value makes many observers skeptical of the currency's future.

Does this volatility foretell the end of Bitcoin? Some commentators believe so.[49] Others suggest that these fluctuations are stress-testing the currency and might eventually decrease in frequency as mechanisms develop to counteract volatility.[50] If bitcoins were only used as stores of value or units of account, the currency's volatility could indeed endanger its future. It does not make sense to manage business finances or keep savings in bitcoins if the market price swings wildly and unpredictably. When Bitcoin is used as a medium of exchange, however, volatility is less of a problem.[51] Merchants can price their wares in terms of a traditional currency and accept the equivalent number of bitcoins. Customers who purchase bitcoins to make a one-time purchase don't care about what the exchange rate will look like tomorrow; they simply care that Bitcoin can lower transaction costs in the present. Bitcoin's usefulness as a medium of exchange might explain why the currency has grown more popular among merchants in spite of its price volatility.[52] It is also possible that the value of bitcoins will become less volatile as more people become familiar with the Bitcoin technology and develop realistic expectations about its future.

---

49. Maureen Farrell, "Strategist Predicts End of Bitcoin," *CNNMoney*, May 14, 2013, http://money.cnn.com/2013/05/14/investing/bremmer-bitcoin/index.html.

50. Adam Gurri, "Bitcoins, Free Banking, and the Optional Clause," *Ümlaut*, May 6, 2013, http://theumlaut.com/2013/05/06/bitcoins-free-banking-and-the-optional-clause/.

51. Jerry Brito, "Why Bitcoin's Valuation Really Doesn't Matter," *Technology Liberation Front*, April 5, 2013, http://techliberation.com/2013/04/05/why-bitcoins-valuation-doesnt-really-matter/.

52. Today, merchant service providers accept the risk presented by the volatility and nevertheless maintain low fees. It remains to be seen whether this model will be sustainable in the long run.

Security Breaches

As a digital currency, Bitcoin presents some specific security challenges.[53] If people are not careful, they can inadvertently delete or misplace their bitcoins. Once the digital file is lost, the money is lost, just as with paper cash. If people do not protect their private Bitcoin addresses, they can leave themselves open to theft. Bitcoin wallets can now be protected by encryption, but users must choose to activate the encryption. If a user does not encrypt his or her wallet, bitcoins could be stolen through malware.[54] Bitcoin exchanges, too, have at times struggled with security; hackers successfully stole 24,000 BTC ($250,000) from a bitcoin exchange called Bitfloor in 2012[55] and mounted a massive series of distributed denial-of-service (DDoS) attacks against the most popular bitcoin exchange, Mt.Gox, in 2013.[56] (Bitfloor eventually repaid the stolen funds to its customers, and Mt.Gox ultimately recovered from the DDoS attacks.) Of course, many of the security risks facing Bitcoin are similar to those facing traditional currencies. Dollar bills can be destroyed or lost, personal financial information can be stolen and used by criminals, and banks can be robbed or targeted by DDoS attacks. Bitcoin users should take care to learn about and prepare for security concerns just as they currently do for other financial activities.

---

53. Most of the security challenges concern wallet services and bitcoin exchanges. The protocol itself has proven to be considerably resilient to hacking and security risks. Renowned security researcher Dan Kaminsky tried, but failed, to hack the Bitcoin protocol in 2011. See Dan Kaminsky, "I Tried Hacking Bitcoin and I Failed," *Business Insider*, April 12, 2013, http://www.businessinsider.com/dan-kaminsky-highlights-flaws-bitcoin-2013-4.

54. Stephen Doherty, "All Your Bitcoins Are Ours . . . ," *Symantec Blog*, June 16, 2011, http://www.symantec.com/connect/blogs/all-your-bitcoins-are-ours.

55. Devin Coldewey, "$250,000 Worth of Bitcoins Stolen in Net Heist," *NBC News*, September 5, 2012, http://www.nbcnews.com/technology/250-000-worth-bitcoins-stolen-net-heist-980871.

56. Meghan Kelly, "Fool Me Once: Bitcoin Exchange Mt.Gox Falls after Third DDoS Attack This Month," *VentureBeat*, April 21, 2013, http://venturebeat.com/2013/04/21/mt-gox-ddos/.

Criminal Uses

There are also reasons for policymakers to be apprehensive about some of Bitcoin's exaptations. Because Bitcoin is pseudonymous, policymakers and journalists have questioned whether criminals can use it to launder money and accept payment for illicit goods and services. Indeed, like cash, it can be used for ill as well as for good.

For one example, we can look at the infamous Deep Web[57] black-market site known as "Silk Road." Silk Road takes advantage of the anonymizing network Tor and the pseudonymous nature of Bitcoin to make available a vast digital marketplace where one can mail-order drugs and other licit and illicit wares. Although Silk Road administrators do not allow the exchange of any goods that resulted from fraud or harm, like stolen credit card information or photographs of child exploitation, it does allow merchants to sell illegal products like forged identity documents and illicit drugs. The pseudonymous nature of Bitcoin allows buyers to purchase illegal goods online in the same way that cash has been traditionally used to facilitate illicit purchases in person. One study estimated the total monthly Silk Road transactions amount to be approximately $1.2 million.[58] But the Bitcoin market amassed $770 million in transactions during June 2013; Silk Road sales constitute a small drop in the total bitcoin economy bucket.[59]

Bitcoin's association with Silk Road has tarnished its reputation. Following the publication of an article on Silk Road in

---

57. *Wikipedia*, s.v. "Deep Web," accessed July 30, 2013, http://en.wikipedia.org/wiki/Deep_Web.

58. Nicolas Christin, "Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace," *Carnegie Mellon CyLab Technical Reports: CMU-CyLab-12-018*, July 30, 2012 (updated November 28, 2012), http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12018.pdf.

59. Jerry Brito, "National Review Gets Bitcoin Very Wrong," *Technology Liberation Front*, June 20, 2013, http://techliberation.com/2013/06/20/national-review-gets-bitcoin-very-wrong/.

2011,[60] senators Charles Schumer and Joe Manchin sent a letter to Attorney General Eric Holder and the Drug Enforcement Administration's administrator Michele Leonhart calling for a crackdown on Silk Road, the anonymizing software Tor, and Bitcoin.[61]

Another concern is that Bitcoin can be used to launder money for financing terrorism and trafficking in illegal goods. Although these worries are currently more theoretical than evidential, Bitcoin could indeed be an option for those who wish to discreetly move ill-gotten money. Concerns about Bitcoin's potential to facilitate money laundering were stoked after Liberty Reserve, a private, centralized digital-currency service based in Costa Rica, was shut down by authorities on charges of money laundering.[62]

While Liberty Reserve and Bitcoin appear similar because they both provide digital currencies, there are important differences between the two. Liberty Reserve was a centralized currency service created and owned by a private company, allegedly for the express purpose of facilitating money laundering. Bitcoin is not. The transactions within the Liberty Reserve economy were not transparent. Indeed, Liberty Reserve promised its customers anonymity. Bitcoin, on the other hand, is a decentralized open currency that provides a public record of all transactions. Money launderers may attempt to protect their Bitcoin addresses and identities, but their transaction records will always be public and accessible at any time by law enforcement. Laundering money through Bitcoin, then, can be seen as a much riskier undertaking than using a centralized system like Liberty Reserve. Additionally,

---

60. Adrian Chen, "The Underground Website Where You Can Buy Any Drug Imaginable," *Gizmodo,* June 1, 2011, http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable.

61. Brett Wolf, "Senators Seek Crackdown on 'Bitcoin' Currency," *Reuters,* June 8, 2011, http://www.reuters.com/article/2011/06/08/us-financial-bitcoins-idUSTRE7573T320110608.

62. "Liberty Reserve Digital Money Service Forced Offline," *BBC News—Technology*, May 27, 2013, http://www.bbc.co.uk/news/technology-22680297.

several bitcoin exchanges have taken steps to comply with anti–money laundering record-keeping and reporting requirements.[63] The combination of a public ledger system and the cooperation of bitcoin exchanges in collecting information on their customers will likely make Bitcoin less attractive to launderers relative to private anonymous virtual currencies.

It is also important to note that many of the potential downsides of Bitcoin are the same as those facing traditional cash. Cash has historically been the vehicle of choice for drug traffickers and money launderers, but policymakers would never seriously consider banning cash. As regulators begin to contemplate Bitcoin, they should be wary of the perils of overregulation. In the worst-case scenario, regulators could prevent legitimate businesses from benefitting from the Bitcoin network without preventing money launderers and drug traffickers from using bitcoins. If bitcoin exchanges are overburdened by regulation and shut down, for instance, money launderers and drug traffickers could still put money into the network by paying a person in cash to transfer his or her bitcoins into their virtual wallets. In this scenario, beneficial transactions are prevented by overregulation while the targeted activities are still able to occur. The challenge for policymakers and regulators is how to develop a system of oversight that assuages their twin concerns about money laundering and illicit purchases without smothering the benefits that Bitcoin is poised to provide to legitimate users in their everyday lives.

REGULATION

Current law and regulation does not envision a technology like Bitcoin, so it exists in something of a legal gray area. This is largely

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

the case because Bitcoin does not exactly fit existing statutory definitions of currency or other financial instruments or institutions, making it difficult to know which laws apply and how.

This situation is reminiscent of regulatory uncertainty surrounding other new technologies, such as Voice over Internet Protocol (VoIP).[64] When VoIP first emerged, the Communications Act and Federal Communications Commission (FCC) regulations only contemplated voice communications over the traditional public switched telephone network. Like Bitcoin, VoIP competed with a highly regulated legacy network, was less expensive, and was often peer-to-peer. To this day Congress and the FCC continue to grapple with VoIP policy questions, including which public-interest obligations should be required of VoIP providers and whether VoIP providers must comply with law-enforcement wiretap requests.

Luckily, however, Congress and the FCC have charted a path for VoIP that has clarified much of the regulatory ambiguity without saddling the new technology with the legacy regulatory burden intended for monopoly telephone service. As a result, VoIP has flourished as a technology, has introduced competition to a previously stagnant market, and has lowered costs and improved access for consumers. Policymakers should seek to achieve the same with Bitcoin.

Bitcoin has the properties of an electronic payments system, a currency, and a commodity, among other things. As a result, it will likely receive scrutiny from several regulators. Below is an outline of some of the questions confronting these agencies as they prepare to regulate Bitcoin.

---

64. Sam Rozenfeld, "FCC'S VoIP Regulation Dilemma," *Telephony Your Way*, April 30, 2011, http://www.telephonyyourway.com/2011/04/30/fccs-voip-regulation-dilemma/.

Is Private Currency Legal?

One of the most common initial questions about Bitcoin is whether the online currency is legal, given the federal government's monopoly on issuing legal tender. The answer seems to be yes. The Constitution only prohibits the states from coining money.[65] Privately issued currencies are not forbidden, and in fact many local currencies are in circulation.[66] To promote local economies, businesspeople and lawmakers have developed several alternative currencies in recent years, such as the Cascadia Hour Exchange in Portland and Life Dollars in Bellingham, Washington.[67]

What private parties may not do is issue currency that resembles US money.[68] One notorious case is that of Bernard von NotHaus, who was convicted in 2011 after printing and distributing a gold-backed currency called the "Liberty Dollar." His crime was not that he issued an alternative currency, but that it was similar in appearance to the US dollar and that von NotHaus attempted to spend his currency into circulation as dollars and encouraged others to do so as well.[69] In contrast, Bitcoin is in no danger of being confused with US currency.

Money-Transmission Laws

A business that transmits funds from one person to another is a money transmitter and in 48 states and the District of Columbia

65. U.S. Const. art I § 10.

66. Reuben Grinberg, "Bitcoin: An Innovative Alternative Digital Currency," *Hastings Science & Technology Law Journal* 4 (2011): 159–208.

67. Blake Ellis, "Local Currencies: 'In the U.S. We Don't Trust,'" *CNN Money*, January 27, 2012, http://money.cnn.com/2012/01/17/pf/local_currency/index.htm.

68. 18 U.S.C. §§ 485 and 486.

69. Grinberg, "Bitcoin," 193n158.

must obtain a license to operate.[70] Money transmitters are also subject to the Bank Secrecy Act (BSA), as implemented by regulations from FinCEN. Additionally, the USA PATRIOT Act made it a criminal offense to operate an unlicensed money-transmission business.[71]

The purpose of state licensing of money transmission has traditionally been consumer protection.[72] Because money transmitters (such as money-order issuers) are typically not FDIC-insured banks, consumers can be left holding the bag if a money transmitter does not forward the funds to the intended recipient. Licensing attempts to minimize this risk. Money-transmitter licensing in the States became widespread after the widely publicized defaults of several money-order companies in the 1980s.[73]

The BSA, on the other hand, is intended to prevent or detect money laundering and terrorist financing.[74] It requires money transmitters and other financial institutions to register with FinCEN, implement anti-money-laundering programs, keep records of their customers, and report suspicious transactions and other data.

Because it's not a company or legal entity, but instead a global peer-to-peer network, Bitcoin itself can't be said to be a money transmitter. The question then is, Do any of the actors in the Bitcoin ecosystem fit the statutory definitions of "money transmitter" that would subject them to state and federal regulation?

---

70. *Hearing on the Regulation of Non-bank Money Transmitter—Money Services Businesses, 112th Congress* (2012) (statement of Ezra C. Levine), testimony before the Subcommittee on Financial Institutions and Consumer Credit of the House Committee on Financial Services, http://financialservices.house.gov/uploadedfiles/hhrg-112-ba15-wstate-elevine-20120621.pdf.

71. 18 U.S.C. § 1960.

72. Aaron Greenspan, *Held Hostage: How the Banking Sector Has Distorted Financial Regulation and Destroyed Technological Progress* (Palo Alto, CA: Think Computer Corporation, 2011), http://www.thinkcomputer.com/corporate/white-papers/heldhostage.pdf.

73. Ibid., 3.

74. 31 U.S.C. § 5311.

In March 2013, FinCEN issued guidance on the application of the BSA to virtual currencies, which include Bitcoin. The guidance defines three categories of persons potentially subject to its regulations as money transmitters:

> A *user* is a person that obtains virtual currency to purchase goods or services. An *exchanger* is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. An *administrator* is a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency.[75]

We can apply each of these definitions to persons in the Bitcoin ecosystem. The clearest definition is that of an *exchanger*. If one is in the business of exchanging dollars for bitcoins or vice versa, then we can conclude that one is a money transmitter under this guidance and must register with FinCEN and comply with the relevant record-keeping and reporting requirements. Also, because states often look to FinCEN's determinations about which types of entities are or are not money transmitters, an exchanger likely must obtain state money-transmitter licenses as well.

Less straightforward are the obligations of mere "users" of Bitcoin. The guidance states that if one obtains bitcoins "to purchase real or virtual goods or services," then one is not a money transmitter and not subject to FinCEN's regulations. It does not explain, however, how the law applies if one obtains bitcoins *not* to purchase goods or services. Some other reasons why one might obtain bitcoins include (1) speculation that the price of bitcoins will go up, (2) simply because one trusts a virtual currency's

75. FinCEN, *Application of FinCEN's Regulations.*

stability more than that of a particular "real currency" (think of Argentina or Zimbabwe), or (3) because one wants to make a remittance to a family member overseas. In none of these cases would Bitcoin users be assured that they are exempted from FinCEN's registration, record-keeping, and reporting requirements. This creates an uncertain regulatory environment that might unduly dampen use of Bitcoin.

Most confusing is how the guidance applies to Bitcoin miners, who create new bitcoins by lending their computing power to the Bitcoin network. The third class of persons that it defines is "administrators," but the definition only applies to centralized virtual currencies in which a central authority creates the currency. For example, Amazon.com is clearly the administrator of its new "Amazon Coins" virtual currency.[76] The guidance, therefore, has a section addressing decentralized virtual currencies such as Bitcoin. According to that section, a miner who mines bitcoins and then uses them "to purchase real or virtual goods and services" is considered a user not subject to the regulations.[77] But if the miner sells the mined bitcoins "to another person for real currency or its equivalent" then the miner qualifies as a money transmitter subject to regulation.[78]

It is not clear how such regulation of miners as money transmitters would further either consumer protection or anti-money-laundering interests. Miners are not transmitting bitcoins from one party to another; they are creating new bitcoins from thin air. If miners sell the bitcoins they mine, there are only two parties to the transaction. As a result, there is neither a consumer to protect nor a potential criminal seeking to convert "dirty money" into clean money.

---

76. Ingrid Lunden, "Amazon Now Offers Amazon Coins Virtual Currency on Kindle Fire, Gives $5 in Free Coins to All Users," *TechCrunch*, May 13, 2013, http://techcrunch.com/2013/05/13/amazon-launches-amazon-coins-virtual-currency-on-kindle-fire-gives-5-in-free-coins-to-all-users/.

77. Ibid.

78. Ibid.

Finally, the guidance notes that FinCEN regulations define currency as the currency of a state, and so the guidance also refers to this definition as "real currency."[79] It then develops a new concept that it calls "virtual currency" on which all the guidance is predicated.[80] The guidance defines virtual currency as "a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency."[81] It goes on to introduce another concept by stating that there are different kinds of "virtual currency" and that the present guidance only extends to "convertible virtual currency," which it defines as one that "either has an equivalent value in real currency, or acts as a substitute for real currency."[82] While the definition of currency (aka "real currency") was adopted through rulemaking, the other new and substantive concepts of "virtual currency" and "convertible virtual currency" exist only in the guidance. As a result, the guidance may be seen as encompassing new law and not merely interpretations of existing law or regulations, thus necessitating a rulemaking under the Administrative Procedure Act.

CFTC Regulation

By their nature, bitcoins can be conceived of either as a commodity or as a currency. Indeed, economist George Selgin has called Bitcoin "synthetic-commodity money."[83] This has attracted the attention of the Commodity Futures Trading Commission (CFTC), which has authority to regulate commodity futures

79. FinCEN, *Application of FinCEN's Regulations*.

80. Ibid.

81. Ibid.

82. Ibid.

83. George Selgin, "Synthetic Commodity Money" (working paper, Department of Economics, University of Georgia, Athens, 2013), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000118.

and the markets in which they trade, as well as to regulate some foreign-exchange instruments.[84]

Bart Chilton, one of five CFTC commissioners, recently told the *Financial Times* that Bitcoin "is for sure something we need to explore."[85] Other sources confirmed that the CFTC is "seriously" looking at the virtual currency.[86] To the extent it chooses to regulate bitcoin transactions, one obvious question is whether CFTC will do so under its commodity futures or foreign-exchange authority.

While the Commodity Exchange Act defines "foreign-exchange forwards" and "foreign-exchange swaps," it does not define "foreign exchange" or "foreign currency," presumably because Congress considered the meaning of those terms obvious. Therefore, if the CFTC moves to apply its foreign-exchange regulations to Bitcoin transactions, it will have to make the determination that bitcoins are considered "foreign currency." While conceivable, such a determination would be at odds with the common understanding of foreign currency, as the money coined by foreign governments.

To illustrate this, we can look at the 2009 Dodd-Frank Wall Street Reform and Consumer Protection Act, which expands the CFTC's authority to regulate foreign exchange. Title 10 of the act also establishes the Consumer Financial Protection Bureau (CFPB), and for purposes of that title defines "foreign exchange" as "the exchange, for compensation, of currency of the United States or of a foreign government for currency of another government."[87] This definition gives a hint of what Congress's conception of "foreign exchange" is, and bitcoin exchange would clearly fall outside it, because bitcoins are not the currency of any government.

---

84. 7 U.S.C. §§ 2(C) and 2(E).

85. Alloway, Meyer, and Foley, "US Regulators Eye Bitcoin."

86. Ibid.

87. Dodd-Frank Wall Street Reform and Consumer Protection Act § 1002 (16); 12 U.S.C. § 5481 (16) (2012).

The connection between foreign currency and government issuance is commonplace. For example, the Treasury Department's definition of currency (adopted through rulemaking, as noted earlier) is

> the coin and paper money of the United States or of any other country that is designated as legal tender and that circulates and is customarily used and accepted as a medium of exchange in the country of issuance. Currency includes US silver certificates, US notes and Federal Reserve notes. Currency also includes official foreign bank notes that are customarily used and accepted as a medium of exchange in a foreign country.[88]

This comports with the Uniform Commercial Code's definition of "money," which is "a medium of exchange authorized or adopted by a domestic or foreign government [including] a monetary unit of account established by an intergovernmental organization or by agreement between two or more nations."[89]

In contrast, the CFTC would have no problem treating bitcoins as commodities. The Commodity Exchange Act defines commodities as all "goods and articles . . . and all services, rights, and interests . . . in which contracts for future delivery are presently or in the future dealt in," except onions and motion-picture box-office receipts.[90] Therefore, bitcoins could certainly qualify as a commodity because they are articles that can be traded and made subject to futures contracts. That said, it is interesting to note that bitcoins are unlike traditional commodities such as gold, corn, or oil, which are tangible and have intrinsically valuable uses. It is also important to note that the CFTC's authority is over, not commodities themselves, but commodity futures. An exchange

88. 31 C.F.R. § 1010.100(m).

89. Unif. Commercial Code §§ 1–201.

90. 7 U.S.C. § 1a (9).

of bitcoins for dollars or other national currency, however, typically occurs instantaneously, and not as part of a futures contract. Therefore, CFTC regulation of bitcoins *as commodities* may be limited. To the extent bitcoin futures markets develop, however, they will certainly be subject to CFTC supervision.[91]

Electronic Fund Transfer Regulation

The final possible vector for regulation of Bitcoin under existing law that we will consider is regulation under the Electronic Fund Transfer Act (EFTA)[92] and its application through the Federal Reserve's Regulation E.[93] The purpose of the EFTA is to establish the respective rights and responsibilities of consumers and financial institutions in electronic fund transfers.[94] Like the other laws and regulations we have seen, the EFTA does not seem to contemplate a decentralized virtual currency like Bitcoin.

The act defines electronic fund transfers as "any transfer of funds, other than a transaction originated by check, draft, or similar paper instrument, which is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account."[95] It further defines "financial institution" as "a State or National bank, a State or Federal savings and loan association, a mutual savings bank, a State or Federal credit union, or any other person who, directly or indirectly, holds an account belonging to a consumer."[96]

---

91. There are, however, emerging Bitcoin futures markets. See Cyrus Farivar, "'Taming the Bubble': Investors Bet on Bitcoin via Derivatives Markets," *Ars Technica*, April 11, 2013, http://arstechnica.com/business/2013/04/taming-the-bubble-investors-bet-on-bitcoin-via-derivatives-markets/.

92. 15 U.S.C. §§ 1601–1692 (2013).

93. 12 C.F.R. §§ 205.1–205.20.

94. 15 U.S.C. § 1693(b).

95. 15 U.S.C. § 1693a (7).

96. 15 U.S.C. § 1693a (9).

These definitions, and the regulations they undergird, assume that electronic fund transfers will necessarily involve "financial institutions" and "accounts." Bitcoin, however, runs counter to that notion.

The Bitcoin system itself does not qualify as a "financial institution" because, as noted earlier, it is not a company or legal entity but instead a global peer-to-peer network. As a result, a Bitcoin address with which bitcoins are associated on the network cannot be said to be an account of a financial institution. Furthermore, as noted above in the technical discussion of how bitcoins are transferred between addresses, in the Bitcoin system there is no "financial institution" or other third party of any kind that "debit[s] or credit[s] an account." Electronic fund transfers between addresses are carried out by users alone, who sign a transaction with the private key associated with a Bitcoin address under their control. The Bitcoin network merely confirms that the transaction is legitimate.

While many users keep the "wallet files"[97] containing their private keys on their own computers or other devices,[98] some delegate securing their keys to online wallet services.[99] Such third-party wallet services often also provide greater ease-of-use than desktop Bitcoin software. Users typically create an "account" on such a wallet service, and their Bitcoin addresses are associated with those accounts. It is conceivable that such online services could fit the definition of "financial institution" under the EFTA, and thus be subject to the regulation. An argument could be made, however, that these services are not engaged in electronic

97. *Bitcoin wiki*, s.v. "Wallet," accessed July 30, 2013, https://en.bitcoin.it/wiki/Wallet.

98. Matthew Sparks, "Winklevoss Twins Back Bitcoin as Bubble Bursts," *Telegraph*, April 12, 2013, http://www.telegraph.co.uk/technology/news/9989610/Winklevoss-twins-back-bitcoin-as-bubble-bursts.html.

99. *Bitcoin wiki*, "EWallet," accessed July 30, 2013, https://en.bitcoin.it/wiki/EWallet.

fund transfers because they do not initiate transfers.[100] Transfers are made by the users directly and are verified by the Bitcoin network; online wallet services merely provide the software and storage that allows users to interact with the Bitcoin network.

Finally, new rules from the Consumer Financial Protection Bureau (CFPB) amending Regulation E target remittance-transfer providers. The regulations require remittance providers to disclose exchange rates and fees associated with international transfers, and to investigate and remediate processing errors.[101] They also require that consumers be afforded 30 minutes or more to cancel a transfer.[102] This requirement can be seen as incompatible with the Bitcoin protocol, because all bitcoin transactions are irreversible. One way to comply with this regulation might be to delay the execution of transactions. The real problem, though, is that this requirement is fundamentally at odds with the purpose of the technology.

POLICY RECOMMENDATIONS

As we have seen, Bitcoin does not easily fit into existing regulatory boxes. That is often the hallmark of a disruptive technology. Indeed Bitcoin is a revolutionary technical achievement that heralds amazing potential benefits to human welfare. However, like any technology that can be used for good, it can also be used for ill. The challenge for policymakers will be to foster Bitcoin's beneficial uses while minimizing its negative consequences. We conclude with some recommendations to help policymakers meet this challenge.

---

100. Nikolei M. Kaplanov, "Nerdy Money: Bitcoin, the Private Digital Currency, and the Case against Its Regulation," *Loyola Consumer Law Review* 25, no. 1 (2012).

101. Consumer Financial Protection Bureau, "Summary of the Final Remittance Transfer Rule (Amendment to Regulation E)" (Washington, DC: Consumer Financial Protection Bureau, 2013), http://files.consumerfinance.gov/f/201305_cfpb_remittance-transfer-rule_summary.pdf.

102. Ibid.

Don't Restrict Bitcoin

Because Bitcoin is essentially online cash, some who trade in drugs and other illicit goods online have found it to be an ideal medium of exchange.[103] Confronted with this fact, the initial impulse of some policymakers will be to call for restrictions on the technology.[104] There are many good reasons, however, to resist such an impulse.

First, as a technology, Bitcoin is neither good nor bad; it is neutral. Paper dollar bills, like bitcoins, can be used in illicit transactions, yet we do not consider outlawing paper bills. We only prohibit their *illicit use*. Furthermore, there is only anecdotal evidence about the extent to which bitcoins are utilized in criminal transactions. It would be wise to put the criminal use of the technology in perspective alongside its legitimate uses. As the bitcoin economy grows, legitimate uses of bitcoins will likely dwarf criminal transactions,[105] just as we see with paper dollar bills.

Second, any attempt to restrict Bitcoin technology will only harm legitimate uses while leaving illicit uses largely unaffected. Because it is a decentralized global network, Bitcoin is virtually impossible to shut down. There is no Bitcoin company or other entity that can be targeted. Instead, Bitcoin and its ledger exist only in the distributed peer-to-peer network created by its users. As with the peer-to-peer file-sharing service BitTorrent, taking down any of the individual computers that

---

103. Andy Greenberg, "Founder of Drug Site Silk Road Says Bitcoin Booms and Busts Won't Kill His Black Market," *Forbes*, April 16, 2013, http://www.forbes.com/sites/andygreenberg/2013/04/16/founder-of-drug-site-silk-road-says-bitcoin-booms-and-busts-wont-kill-his-black-market/.

104. Charles Schumer and Joe Manchin, Letter to Attorney General Eric Holder and Drug Enforcement Administration Administrator Michele Leonhart, June 6, 2011. Available at http://www.manchin.senate.gov/public/index.cfm/press-releases?ID=284ae54a-acf1-4258-be1c-7acee1f7e8b3.

105. Jan Jahosky, "BitPay Eclipses Silk Road in Bitcoin Sales with Explosive $5.2M March," *BitPay Blog*, April 2, 2013, http://blog.bitpay.com/2013/04/bitpay-eclipses-silk-road-in-bitcoin.html.

make up the peer-to-peer system would have little effect on the rest of the network. Therefore, making the use of Bitcoin illegal would not undermine the network; it would only serve to ensure that law-abiding users are denied access to the technology. As a result, society would forgo enjoying the many potential benefits of Bitcoin without seeing any drop in criminal use.

Third, if Bitcoin were prohibited, the government would forego the opportunity to regulate intermediaries in the bitcoin economy, such as exchangers and money transmitters. The governmental interests in detecting and preventing money laundering and terrorist financing would be better advanced, not by prohibiting the technology, but by requiring intermediaries to keep records and report suspicious activities, just as traditional financial institutions do. Again, restricting the use of Bitcoin will only ensure that criminals alone will use the technology. Any illicit intermediaries that emerge, such as exchanges and payment processors, will be unregulated.

Finally, even if the United States prohibited the use of Bitcoin, it is likely that many other countries would not, recognizing the technology's many potential benefits. The Finnish central bank, for example, has stated that the digital currency is not illegal,[106] and as a result many Finnish businesses have begun to accept bitcoins.[107] By prohibiting Bitcoin use, the United States could put itself at an international competitive disadvantage in the development and use of what may be the next-generation payments system.

Normalize Regulation and Encourage Further Development

Rather than overreact to illicit uses of Bitcoin, policymakers would be wise to take a calm and careful approach to the challenges posed

106. Matt Clinch, "Bitcoin Utopia? Interest Is Sky High in This Euro Nation," *CNBC*, April 4, 2013, http://www.cnbc.com/id/100618694.

107. Jan Jahosky, "BitPay Exceeds 1,000 Merchants Accepting Bitcoin," *BitPay Blog*, September 11, 2012, http://blog.bitpay.com/2012/09/bitpay-exceeds-1000-merchants-accepting.html.

by the new technology. Doing so would allow law enforcement to pursue its interests in detecting and preventing money laundering and terrorist financing while ensuring that society does not forgo Bitcoin's many benefits. Luckily, regulators to date have taken such a cautious approach by slowly integrating Bitcoin into the existing financial regulatory framework. Policymakers can take a few basic steps to maintain the right balance.

In the short term, FinCEN should clarify its recent guidance, especially as it relates to miners and users who do not obtain bitcoins to purchase goods or services, but instead do so for other legal and legitimate purposes. It should do this by welcoming public participation of the Bitcoin community of developers, miners, businesses, and users in formal public notice and comment proceedings. While FinCEN's mission is to safeguard the financial system from illicit use, it also has an obligation not to unduly hinder its technological development. Working with Bitcoin's legitimate users, there is no doubt FinCEN can achieve its goals while minimizing regulatory uncertainty.

In the long term, policymakers should better define Bitcoin's broader regulatory status. As we have seen, the digital currency does not comfortably fit any existing classification or legal definition. It is not a foreign currency, nor a traditional commodity, nor is it simply a payments network. Consequently, applying existing rules to Bitcoin could unduly impede Bitcoin's legitimate development without any attendant gains to law enforcement or consumer welfare. As a result, policymakers may want to consider developing a new category that takes into account the technology's unique nature. They should also carefully consider what regulation, if any, bitcoin exchanges, payment processors, and users should face.

Finally, policymakers should not only allow Bitcoin's development to continue unimpeded, they should help foster its growth by revisiting existing regulatory barriers. One of the greatest obstacles to Bitcoin's legitimate adoption is the requirement that businesses engaging in money transmission acquire a license from

each state. This is a duplicative, laborious, and expensive process that presents a barrier to interstate commerce without much benefit to consumers. Federal lawmakers and regulators should consider whether preemption is necessary.

CONCLUSION

Bitcoin is an exciting innovation that has the potential to greatly improve human welfare and jump-start beneficial and potentially revolutionary developments in payments, communications, and business. Bitcoin's clever use of public-key encryption and peer-to-peer networking solves the double-spending problem that had previously made decentralized digital currencies impossible. These properties combine to create a payment system that could lower transactions costs in business and remittances, alleviate poverty, provide an escape from capital controls and monetary mismanagement, allow for legitimate financial privacy online, and spur new financial innovations. On the other hand, as "digital cash," Bitcoin can be used for money laundering and illicit trade. Banning Bitcoin is not the solution to ending money laundering and illicit trade, just as banning cash is not a solution to these same ills.

Bitcoin could ultimately fail as an experimental digital currency and payment system. An unanticipated problem could arise and undermine the bitcoin economy. A superior cryptocurrency could outcompete and replace Bitcoin. It could simply fizzle out as a fad. The possibilities for failure are endless, but one reason for failure should not be that policymakers did not understand its workings and potential. We are ultimately advocating not for Bitcoin, but for innovation. It is important that policymakers allow this experimentation to continue. Policymakers should work to clarify how Bitcoin is regulated and to normalize its regulation so that we have the opportunity to learn just how innovative Bitcoin can be.

FURTHER READING

Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System." White Paper, 2008. http://bitcoin.org/bitcoin.pdf.

Reuben Grinberg. "Bitcoin: An Innovative Alternative Digital Currency." *Hastings Science & Technology Law Journal* 4 (2011): 160–208. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1817857.

William J. Luther. "Cryptocurrencies, Network Effects, and Switching Costs." Mercatus Working Paper, Mercatus Center at George Mason University, Arlington, VA, forthcoming. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2295134.

George Selgin. "Synthetic Commodity Money." Working paper, University of Georgia Department of Economics, Athens, GA, April 10, 2013. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2000118.

Nikolei M. Kaplanov. "Nerdy Money: Bitcoin, the Private Digital Currency, and the Case against Its Regulation." *Loyola Consumer Law Review* 25 (2012): 111–174. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2115203.

European Central Bank. "Virtual Currency Schemes." October 2012. http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

ABOUT THE AUTHORS

Jerry Brito is a senior research fellow at the Mercatus Center at George Mason University and director of its Technology Policy Program. He also serves as an adjunct professor of law at George Mason University. His research focuses on technology and Internet policy, copyright, and the regulatory process. His op-eds have appeared in the *Wall Street Journal*, the *New York Times*, and elsewhere. Brito is a coauthor, with Susan Dudley, of *Regulation: A Primer*, and the editor of *Copyright Unbalanced: From Incentive to Excess*. He hosts *Surprisingly Free*, a weekly half-hour podcast featuring in-depth discussions with an eclectic mix of authors, academics, and entrepreneurs at the intersection of technology, policy, and economics. He also contributes to the *Technology Liberation Front*, a leading technology-policy blog. He has created several websites to foster transparency and accountability in government, including OpenRegs.com, which provides an alternative interface to the federal government's regulatory docketing system. Brito received his JD from George Mason University School of Law and his BA in political science from Florida International University.

Andrea Castillo is a program associate for the Spending and Budget Initiative at the Mercatus Center at George Mason University. She is a coauthor of *Liberalism and Cronyism: Two Rival Political and Economic Systems* with Randall G. Holcombe, and she blogs at *Neighborhood Effects* and is a columnist for *The Ümlaut*. She received her BS in economics and political science from Florida State University.

ABOUT THE MERCATUS CENTER

The Mercatus Center at George Mason University is the world's premier university source for market-oriented ideas—bridging the gap between academic ideas and real-world problems.

A university-based research center, Mercatus advances knowledge about how markets work to improve people's lives by training graduate students, conducting research, and applying economics to offer solutions to society's most pressing problems.

Our mission is to generate knowledge and understanding of the institutions that affect the freedom to prosper and to find sustainable solutions that overcome the barriers preventing individuals from living free, prosperous, and peaceful lives.

Founded in 1980, the Mercatus Center is located on George Mason University's Arlington campus.

www.mercatus.org