Journal of Economic Perspectives—Volume 29, Number 2—Spring 2015—Pages 213–238

Bitcoin: Economics, Technology, and Governance[†]

Rainer Böhme, Nicolas Christin, Benjamin Edelman, and Tyler Moore

Bitcoin is an online communication protocol that facilitates the use of a virtual currency, including electronic payments. Since its inception in 2009 by an anonymous group of developers (Nakamoto 2008), Bitcoin has served approximately 62.5 million transactions between 109 million accounts. As of March 2015, the daily transaction volume was approximately 200,000 bitcoins—roughly $50 million at market exchange rates—and the total market value of all bitcoins in circulation was $3.5 billion (Blockchain.info 2015). Table 1 summarizes Bitcoin activity to date. (We will follow the convention in the computer science literature of using capital-B Bitcoin to refer to the system, and lower-b bitcoin to refer to the unit of account.)

Bitcoin's rules were designed by engineers with no apparent influence from lawyers or regulators. Rather than store transactions on any single server or set of servers, Bitcoin is built on a transaction log that is distributed across a network of participating computers. It includes mechanisms to reward honest participation, to bootstrap acceptance by early adopters, and to guard against concentrations of power. Bitcoin's design allows for irreversible transactions, a prescribed path of money creation over time, and a public transaction history. Anyone can create a

■ *Rainer Böhme is Professor of Security and Privacy, University of Innsbruck, Innsbruck, Austria. Nicolas Christin is Assistant Research Professor, Department of Electrical and Computer Engineering and CyLab, Carnegie Mellon University, Pittsburgh, Pennsylvania. Benjamin Edelman is Associate Professor of Business Administration, Harvard Business School, Boston, Massachusetts. Tyler Moore is Assistant Professor of Computer Science and Engineering, Southern Methodist University, Dallas, Texas. Their email addresses are rainer.boehme@uibk.ac.at, nicolasc@cmu.edu, bedelman@hbs.edu, and tylerm@smu.edu.*

[†] To access the disclosure statements, visit
http://dx.doi.org/10.1257/jep.29.2.213 doi=10.1257/jep.29.2.213

Table 1
Bitcoin Activity to Date
(as of March 2015)

Total bitcoins minted	≈ 14 million
US dollar equivalent at market price	≈ 3.5 billion
Total number of reachable Bitcoin nodes	≈ 6,500[a]
Total (cumulative) number of transactions	≈ 62.5 million
Total number of accounts ever used	≈ 109 million
Block chain size	≈ 30.3 GB
Number of blocks to date	≈ 350,000
Estimated daily transaction volume	≈ 200,000 BTC (≈ $50 million)
Average transaction value	≈ 2 BTC (≈ $500)[b]
Computation invested in puzzle solutions	≈ 4,254 exaflops[c]
Power consumption	> 173 MW (continuously)[d]

Source: Authors' compilation and own computations derived from (Yeow 2015; Blockchain.info, 2015; Bitcoincharts.com, 2015; Bitcoin Wiki 2015b).
[a] Reports only publicly reachable notes and excludes "private" nodes, for example, nodes hosted on private networks behind a firewall, which are likely to represent the majority of the network but cannot be reliably measured.
[b] Excludes change. The distribution is skewed toward small transactions. We estimate the median transaction amount to be around 0.02 bitcoins ($5).
[c] This corresponds to roughly 11,500 times the combined power of the top 500 supercomputers in the world. That said, supercomputers can perform all sorts of mathematical operations, while Bitcoin miners are generally highly specialized in a single type of cryptographic operation.
[d] Reflects a computation similar to Bonneau's (2014) lower bound. According to Bitcoin Wiki (2015b), the most energy-efficient mining hardware can perform 1,957 millions of cryptographic operations ("hashes") per Joule (W/s). The current aggregate power of the Bitcoin network is 340,000 terahashes (10^{12}) per second (Bitcoincharts.com 2015). This capacity would require continuous consumption of 173 MW, if every miner used the most energy-efficient hardware.

Bitcoin account, without charge and without any centralized vetting procedure—or even a requirement to provide a real name. Collectively, these rules yield a system that is understood to be more flexible, more private, and less amenable to regulatory oversight than other forms of payment—though as we discuss in subsequent sections, all these benefits face important limits.

Bitcoin is of interest to economists as a virtual currency with potential to disrupt existing payment systems and perhaps even monetary systems. Even at their current early stage, such virtual currencies provide a variety of insights about market design and the behavior of buyers and sellers. This article presents the platform's design principles and properties for a nontechnical audience; reviews its past, present, and future uses; and points out risks and regulatory issues as Bitcoin interacts with the conventional financial system and the real economy.

Bitcoin Design Principles

Scarcity is a prerequisite for ascribing value to any form of money. At a micro level, scarcity protects against counterfeiting. More broadly, scarcity bounds the growth path of the monetary base and facilitates price stability. In modern economies, where money is held in electronic forms, scarcity is preserved by legal rules ensuring the correctness of bookkeeping records: that is, electronic money involves a financial system in which transactions trigger a credit for one account and a corresponding debit to another. Central banks hold the power to adjust the absolute quantity of money in circulation.

Against this backdrop, Bitcoin can be understood as the first widely adopted mechanism to provide absolute scarcity of a money supply. By design, Bitcoin lacks a centralized authority to distribute coins or to track who holds which coins. Consequently, the process of issuing currency and verifying transactions is considerably more difficult than in classic bookkeeping systems. Meanwhile, Bitcoin issues new currency to private parties at a controlled pace in order to provide an incentive for those parties to maintain its bookkeeping system, including verifying the validity of transactions.

Enabling Technologies and Processes

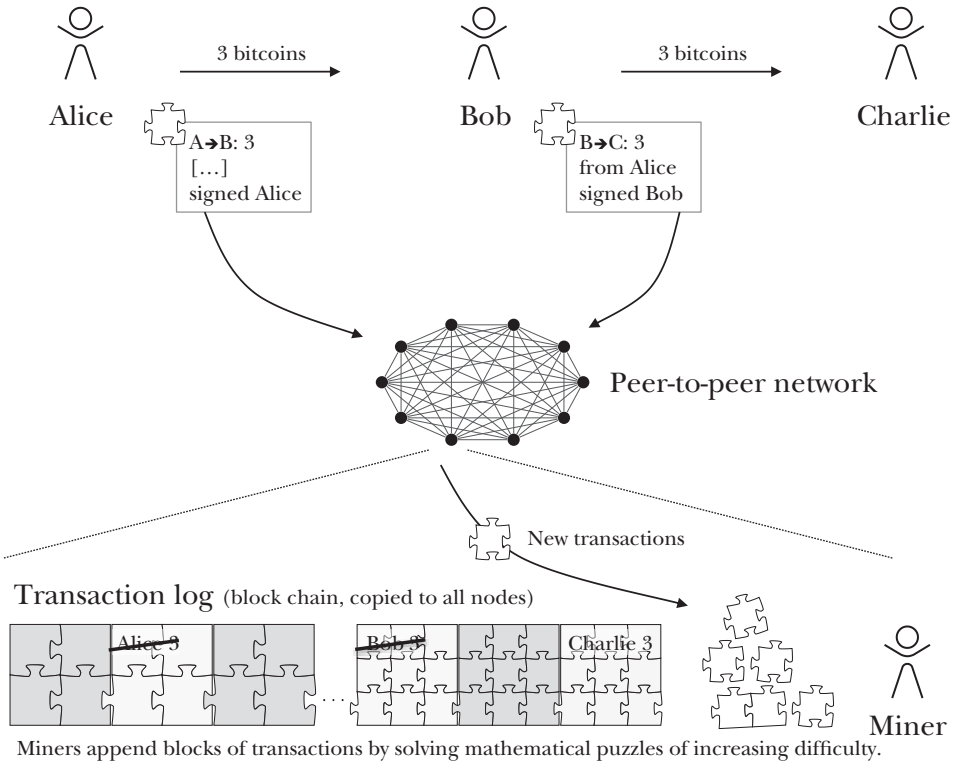
The "Bitcoin core" software can be freely downloaded at https://bitcoin.org/en/choose-your-wallet. The standard Bitcoin implementation includes a number of features. Typically, it creates a "wallet" file for the user that can store bitcoins (without giving a name or proof of identity); it creates an individual node for the user in the peer-to-peer Bitcoin network that can be used with a standard Internet connection; and it provides access to the "block chain" data structure that verifies all past Bitcoin activity.

Transactions and the Block Chain

Bitcoins are recorded as transactions. For instance, some user Charlie does not simply "hold" three bitcoins. Rather, Charlie participates in a publicly verifiable transaction showing that he received three bitcoins from Bob. Charlie was able to verify that Bob could make that payment because there was a prior transaction in which Bob received three bitcoins from Alice and there was no prior transaction in which Bob spent these three bitcoins. Figure 1 illustrates these interactions.

Indeed, each individual bitcoin can readily be traced back through all transactions in which it was used, and thus to the start of its circulation. All Bitcoin transactions are readable by everyone in records stored in a widely replicated data structure. In general, transactions are ordered recursively by having the input of a transaction (roughly, the source of funds) refer to the output of a previous transaction. (For example, the transaction might reveal that Bob pays Charlie using bitcoin he received from Alice.)

Figure 1
Bitcoin's Approach to Transaction Flow and Validation



Miners append blocks of transactions by solving mathematical puzzles of increasing difficulty.

Source: Authors.

Bitcoin relies on two fundamental technologies from cryptography: public-private key cryptography to store and spend money; and cryptographic validation of transactions. Standard public-private key cryptography lets anyone create a public key and an associated private key (Diffie and Hellman 1976). Public keys are designed to be widely shared—hence the name. Messages encrypted with a public key can only be descrambled by someone who possesses the corresponding private key, allowing anyone to encrypt a message that only the specified recipient can read. Similarly, messages encrypted with a private key can only be descrambled with the corresponding public key, allowing a specified sender to create a message that can be confirmed to be authentic. Public-private key cryptography is widely used: in the best-known example, web browsers on a HTTPS "secure website" encrypt communications with that site's advertised public key in order to begin a secure connection. In Bitcoin, similar encryption fundamentals authenticate instructions to transfer money to other participants. Such an instruction is encrypted using the sender's private key, confirming for everyone that the instruction in fact came from the sender.

Suppose that Alice has three bitcoins that she wants to give to Bob. She publishes a message in the Bitcoin network indicating that she is transferring three of her existing bitcoins, along with a reference to the transaction where she had received those bitcoins. Part of this message is encrypted by Alice's private key to prove that the instruction came from her, in a method akin to a signature on a paper check. Later, if Bob wants to send bitcoins to Charlie, he publishes a message, again encrypted with his private key, indicating that he got his bitcoins from Alice and what he wants to send to whom. The Bitcoin network identifies Alice, Bob, and Charlie only by their public keys, which serve as account numbers.

Every new transaction that is published to the Bitcoin network is periodically grouped together in a "block" of recent transactions. To make sure no unauthorized transactions have been inserted, the block itself is compared to the most recently published block—yielding a linked sequence of blocks, or "block chain." A new block is added to the chain roughly every ten minutes. With this data structure in place, any Bitcoin user can verify that a prior transaction did in fact occur.

Keeping the transaction record operational and updated is a public good, as it is the foundation of the entire Bitcoin system. To encourage users to assist, the Bitcoin system periodically awards newly minted bitcoins to the user who solves a mathematical puzzle that is based on the pre-existing contents of the block (which prevents tampering with the block and hence modifying prior transactions) and which can only be solved by computationally intensive methods that include a random component. Thus, faster computing is more likely to solve a given problem and will solve a greater number of these problems, but speed alone will not guarantee success.

Upon solving the puzzle, the user publishes a "block" which contains a proof-of-work that a solution was carried out along with all observed transactions that have taken place since the last puzzle solution was announced and a reference to the previous complete block. After other users verify the solution, they start working on a new block containing new outstanding transactions. This process is called "mining" and recursively ensures that the total historical ordering on all blocks ("chain") is agreed by the entire network.

A Bitcoin transaction does not clear (and hence is not final) until it has been added to the consensus block chain. Transaction batches are added every ten minutes on average. However, miners are continuously working on adding blocks of transactions, and building on previous transactions. By continually presenting their solutions to the puzzles, with the associated new tail of the block chain, miners are in effect "voting" on the correct record of Bitcoin transactions, and in that way verifying the transactions. In some cases, a transaction batch will be added to the block chain, but then a few minutes later it will be altered because a majority of miners reached a different solution. Sources typically recommend considering a Bitcoin transaction final only after six confirmations, to assure that the transaction is truly recorded in a permanent part of the block chain. While this provides greater assurance, it creates a delay of approximately one hour before a Bitcoin transaction is finally validated.

As miners update the block chain, their computational efforts carry significant costs. In particular, the computerized proof-of-work calculations are quite power-intensive, consuming more than 173 megawatts of electricity continuously. For perspective, that amount is approximately 20 percent of an average nuclear power plant (World Nuclear Association 2015), or approximately $178 million per year at average US residential electricity prices. These computational costs have grown sharply and may rise further because Bitcoin automatically adjusts puzzle difficulty so that the time interval between two blocks remains roughly ten minutes. As more computing power joins the Bitcoin system, the puzzles automatically become more difficult, increasing computing and electricity requirements. In fact, an arms race ensued as the price of bitcoin rose. Taylor (2013) compares the difficulty of solving the puzzle to the bitcoin-dollar exchange rate, finding that spikes in the exchange rate—bitcoins becoming more valuable in terms of US dollars—have been followed by increases in computational difficulty.

Built-in Incentives

Bitcoin includes several built-in incentives to encourage useful behavior. The miners who verify the block chain are rewarded with—what else?—bitcoins. At first, miners solving the puzzle received a reward of 50 bitcoins. This reward is periodically cut in half, and it stands at 25 as of March 2015. After 21 million bitcoins have been minted, the reward falls to zero and no further bitcoins will be created. Hence, the protocol design for Bitcoin sets a controlled pace for the expansion of the currency and an ultimate limit to the number of bitcoins issued.

Miners have a second potential source of revenue (which will become the only source of revenue once all bitcoins have been created). When listing a transaction, the buyer and seller can also offer to pay a "transaction fee," which is a bonus payment to whatever miner solves the puzzle that verifies the transaction. These fees are optional, but 97 percent of the transactions in 2014 include a fee, most often set at the default rate of the standard client software, 0.0001 bitcoin. In relative terms, the transaction fees are below 0.1 percent of total transaction value (Möser and Böhme 2014). However, as the mathematical puzzles become harder, there will presumably be a point where the automatic reward for solving the puzzle drops below the cost of doing so. At that point, one possibility is that those who wanted a Bitcoin transaction could bid up the optional fees. Houy (2014a) models equilibria for the level of transaction when the minting reward drops below the cost of mining.

Early in Bitcoin's operation, updating the block chain yielded bitcoins more often and hence more readily per unit of computing power provided. This design benefited those who ran the Bitcoin platform at the outset—helping to create the critical mass needed to bootstrap the platform (Böhme 2013). Today, some users still find mining profitable, but effective mining now requires specialized hardware (particularly well-suited to solving the mathematical puzzles at issue) as well as access to low-cost electricity.

Requiring miners to solve a puzzle helps avoid certain types of fraud. In principle, a system like Bitcoin could validate transactions using a simple consensus by

majority vote, with a majority of connected users able to affirm that a given transaction in fact occurred. But then an attacker could game the system by creating numerous fake identities. In response, the Bitcoin protocol makes it costly to submit fake votes. Consistent with the Internet's open architecture, anyone can connect multiple computers to the Bitcoin system. But voting on the authenticity of a transaction requires first working to solve a mathematical puzzle that is computationally hard to solve (although easy to verify). Solving the puzzle provides "proof of work"; in lieu of "one person, one vote," Bitcoin thus implements the principle of "one computational cycle, one vote." Through this design, the proof-of-work mechanism simultaneously discourages creating numerous fake identities and also provides incentives to participate in verifying the block chain.

What Bitcoin Doesn't Have

Compared with conventional payment systems, Bitcoin lacks a governance structure other than its underlying software. This has several implications for the functioning of the system. First, Bitcoin imposes no obligation for a financial institution, payment processor, or other intermediary to verify a user's identity or cross-check with watch-lists or embargoed countries. Second, Bitcoin imposes no prohibition on sales of particular items; in contrast, for example, credit card networks typically disallow all manner of transactions unlawful in the place of sale (MacCarthy 2010). Finally, Bitcoin payments are irreversible in that the protocol provides no way for a payer to reverse an accidental or unwanted purchase, whereas other payment platforms, such as credit cards, do include such procedures. As discussed in subsequent sections, these design decisions are intentional—simplifying the Bitcoin platform and reducing the need for central arbiters, albeit raising concerns for some users.

Centralization and Decentralization in the Bitcoin Ecosystem

The key innovation in Bitcoin, compared to other forms of cryptographic cash (Chaum 1983) or virtual currencies (European Central Bank 2012), is its decentralized core technologies. Early adopters praised decentralization and by all indications chose Bitcoin because they wanted to use a decentralized system (Raskin 2013). Decentralization offers certain advantages. It avoids concentrations of power that could let a single person or organization take control. It often promotes availability and resiliency of a computer system, avoiding a central point of failure. It offers at least the appearance of greater privacy for users (and perhaps greater genuine privacy) because in theory an eavesdropping adversary cannot observe transactions across the system by targeting any single point or any single server. (However, as we discuss below, significant privacy concerns remain.)

Nonetheless, the decentralization touted by Bitcoin has not fully come to fruition. While the Bitcoin protocol supports complete decentralization (including the possibility of all participants acting as miners), significant economic forces push

towards de facto centralization and concentration among a small number of intermediaries at various levels of the Bitcoin ecosystem. We review four key categories of intermediaries that have shaped Bitcoin's evolution: currency exchanges, digital wallet services, mixers, and mining pools. A fifth type of intermediary, payment processors, is discussed further below.

Currency Exchanges

Currency exchanges allow users to trade bitcoins for traditional currencies or other virtual currencies. Most operate double auctions with bids and asks much like traditional financial markets, and charge a commission ranging from 0.2 to 2 percent. Some exchanges offer more advanced trading tools, such as limit or stop orders. To date, derivatives markets and short-selling remain rare.

At present, many trades in bitcoin are accompanied by one or even two conversions from and/or to conventional currencies. Furthermore, price quotes in bitcoin are almost always computed in real time by reference to a fixed amount of conventional currency. Thus, Bitcoin today resembles more a payment platform than what economists consider a currency.

While few technical barriers impede setting up intermediaries in the Bitcoin ecosystem, there are significant regulatory requirements. In the United States, currency exchanges generally operate as "money transmitters" and thus must register with the Financial Crimes Enforcement Network (FinCEN) as money services businesses. Registration includes a state-by-state licensing requiring both legal fees and posting bonds. Certification in a single state often costs at least $10,000, so nationwide participation can easily reach six figures on fees alone. Other countries have broadly similar rules. In Germany, currency exchanges that manage deposits on behalf of clients are viewed as "deposit banks" with a minimum capital requirement of €5 million.

In addition, currency exchanges need online infrastructure capable of withstanding attacks including hacking and denial-of-service attacks. For these reasons, the number of Bitcoin exchanges has remained modest, and the number of Bitcoin exchanges with significant volume has been even smaller. In spring 2012, the Japan-based Mt. Gox exchange served over 80 percent of all Bitcoin transactions. However, Mt. Gox collapsed in early 2014 and reported in its bankruptcy filing "losing" 754,000 of its customers' bitcoins worth approximately $450 million at the time of closure (Abrams, Matthew, and Tabuchi 2014). In March 2015, the seven largest exchanges were BTC China, OKCoin, Huobi, Bitfinex, LakeBTC, Bitstamp, and BTC-e, which jointly served more than 95 percent of all bitcoin trade from October 2014 to March 2015 (Bitcoinity.org 2015).

Digital Wallet Services

Bitcoin wallets are data files that include Bitcoin accounts, recorded transactions, and private keys necessary to spend or transfer the stored value. Some users install specialized wallet software (such as Armory, Electrum, or Hive) on their personal devices to maintain control over their bitcoins. However, many users find

this task unappealing. Bitcoin wallet software can be difficult to install, and can impose onerous technical requirements—such as storing a copy of the entire block chain, which was 30 gigabytes as of March 2015. (Not all participants need to download the entire chain, but the system does rely on some users electing to do so.) Other users worry about security: a crash or attack on the computer holding the digital wallet could cause the loss of a user's bitcoins.

As a result, many users rely on a digital wallet service that keeps the required files on a shared server with access via the web or via phone-based apps. A key distinction among digital wallet services is whether the service knows the account's private key. Some services (including Blockchain.info, StrongCoin, and CoinPunk) let the user maintain control over private keys, meaning that the service is incapable of spending the user's bitcoin (nor could hackers do so even if they fully infiltrated the wallet service). For such firms, the user must keep and present the private key when needed, and a user who loses the key or allows it to be compromised is at high risk. In contrast, other services (such as Coinbase and Xapo) require users to let the service store their private keys, which increases risk if the digital wallet service is compromised. In practice, digital wallet services tend to increase centralization—either expanding the role and importance of exchanges, or adding an additional service that is likely to be centralized due to high fixed costs, low marginal costs, and limited diversity in users' needs.

Mixers

As initially envisioned, the Bitcoin transaction log shows each transaction made from each payer to each payee, along with the public keys serving as pseudonyms of each. As a result, anyone who knows the identity of any user from any transaction—perhaps the mailing address used for delivery of purchased goods, or the bank account used to purchase bitcoins—can track that user's other transactions made with the same pseudonym, both before and since.

To preserve privacy against this tactic, *mixers* let users pool sets of transactions in unpredictable combinations, thus preventing tracking across transactions. Suppose Alice wants to pay Bob one bitcoin, and Charles wants to pay Daisy one bitcoin. To 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. In practice, mixers must ensure that timing does not yield clues about money flows, which is particularly difficult since it is rare for different users to seek to transmit the exact same amount. Mixers have been used to promote anonymity in online communications, most famously by the Tor network, so their limitations are now widely known (Danezis and Diaz 2008). In addition to standalone services, some mixers are incorporated as a feature provided by digital wallets.

While mixers seem to improve privacy, they create additional challenges. For one, the finality of Bitcoin payments leaves payers with little recourse if a mixer

absconds with their funds. Furthermore, mixing protocols are usually not public, so their effectiveness cannot be proven. Indeed, correlations in timing might still reveal transaction counterparts, particularly at little-used mixers (Möser, Böhme, and Breuker 2013). Finally, mixers charge 1 to 3 percent of the amount sent, increasing costs for those who choose to use them.

Mining Pools

As discussed above, bitcoins are created when a miner successfully solves a mathematical puzzle. The puzzles have become significantly more difficult over time, and lumpy rewards mean a lone miner is now at risk of contributing resources in an attempt to solve a puzzle but then receiving no reward. In response, mining pools now combine resources from numerous miners. Miners work independently, but upon winning a miner shares earnings with others in the pool (much like consumers sharing resources to buy lottery tickets). As of March 2015, the two largest pools are AntPool and F2Pool, which together account for around one-third of Bitcoin mining activities.

Oversized mining pools threaten the decentralization that underpins Bitcoin's trustworthiness. In several instances including a twelve-hour interval in June 2014, GHash briefly held more than 50 percent of total mining power, which could have allowed GHash pool operators to attempt manipulations. An attacker who holds a majority of Bitcoin's computational resources can alter some of the system's records, including inserting false transactions and rejecting actual transactions (albeit with a strong chance that others will notice), or deviate from the protocol rules.

Uses of Bitcoin

Early: Silk Road and Other Illicit Activities

After early proof-of-concept transactions, the first notable adopters of Bitcoin were businesses that sought features not easily available through alternatives: greater anonymity and the absence of rules concerning what could be bought or sold.

One prominent example involved the online sale of narcotics including marijuana, prescription drugs, and benzodiazepines (a class of psychoactive drugs). Drugs had been sold online for years, typically on informal bulletin boards and on websites such as "The Farmer's Market," a website that listed various narcotics available for purchase with payment using other services including PayPal (Kim 2014). When Bitcoin is used with tools to anonymize network traffic such as Tor (Dingledine, Mathewson, and Syverson 2004), marketplaces could provide stronger assurances of anonymity. Transaction volume grew sharply: Christin (2013) estimates that the turnover on the Silk Road anonymous online marketplace, the first to support Bitcoin transactions exclusively, reached $15 million per year just one year after it began operation. Silk Road's own category classifications confirm the prevalence of narcotics items, which dominated Silk Road's top categories as shown in Table 2. Examining 30 months of Silk Road data from February 2011 to July 2013,

Table 2
The Ten Most Popular Product Categories on the Silk Road Website in January–July 2012

Category	*Number of items*	*Percentage*
Weed	3,338	13.7%
Drugs	2,193	9.0%
Prescription	1,784	7.3%
Benzodiazepines	1,193	4.9%
Books	955	3.9%
Cannabis	877	3.6%
Hash	820	3.4%
Cocaine	630	2.6%
Pills	473	1.9%

Source: Christin (2013).
Note: Categories are self-reported by sellers.

the government evidence in the case against Ross Ulbricht lists 9.9 million bitcoins of transactions, which, accounting for the varying exchange rates, corresponds to $214 million (US v. Ulbricht, 2014, Government Exhibit 940). After the demise of Silk Road at the hands of law enforcement (discussed further below), alternative markets opened in its stead—a "new" Silk Road, as well as more than 30 competitors—and it is unclear whether the Silk Road takedown actually reduced contraband activity using Bitcoin.

While litigation documents largely focus on Silk Road as a marketplace for drugs and other contraband, the site's general-purpose platform stood ready to sell *anything*. Reputation systems ensured trustworthiness of the transaction parties; escrow services mitigated counterparty risk; and, in some cases, hedges protected customers against currency volatility. Criminal charges criticized Silk Road's fees: for escrow service, these averaged 8 percent in comparison to credit card system fees of approximately 3 percent—allegedly an indicator of Silk Road's distinctive profit from misbehavior. But eBay's fees typically somewhat exceed Silk Road's fees, calling into question whether high fees in and of themselves indicate a platform's purpose or responsibility.

Silk Road sellers appear to have exploited some arbitrage opportunities. For instance, marijuana is generally cheaper in the Netherlands than in Australia, providing Netherlands-based Silk Road sellers an opportunity to compete advantageously with street sellers in Australia. Numerous online discussions flagged this opportunity and the sellers who invoked it, and analysis of Silk Road's transactions confirms disproportionate items sold from the Netherlands.

Gambling sites also turned to Bitcoin, both to protect customer privacy and to receive funds from customers unable to use other payment methods. The most popular single Bitcoin gambling game is Satoshi Dice, a simple betting game in which a player wins if a dice roll is less than the player's chosen number. This service reported 2012 earnings of approximately 33,000 bitcoins (or roughly $403,000 at

then-applicable rates) with an average monthly growth of 78 percent at the time (Matonis 2013). For several months, the service's (low value) payments accounted for up to 80 percent of total Bitcoin transactions (Möser and Böhme 2014). The Bitcoin Wiki (2015a) now reports around 100 casinos, poker sites, dice games, lotteries, and betting services.

Bitcoin can also be used to evade international capital controls. In December 2013, the People's Bank of China, the central bank of China, banned Chinese banks from relationships with Bitcoin exchanges, a decision which the *Economist* magazine attributed to a desire to prevent yuan from being moved overseas via Bitcoin (D.K. 2013). Similarly, interest in Bitcoin appears to be particularly high in Argentina, where government policy strictly limits transfers to other currencies (McLeod 2013).

Current: Consumer Payments, Buy-and-Hold

In light of widespread criticism of the fees charged by credit and debit card networks (Anderson 2012), Bitcoin could offer an alternative that might pressure card networks to lower their prices to merchants. Some early evidence seems to confirm that Bitcoin may have this effect. Overstock.com, an online retailer, began to receive payments by Bitcoin in January 2014. Overstock reported a favorable response, including significant revenue gains, large average order sizes, and desirable customer demographics (Sidel 2014). Other merchants subsequently added Bitcoin support, including Expedia (travel), Newegg (electronics), Foodler (restaurant delivery and takeout), Gyft (gift cards for dozens of merchants), and TigerDirect (electronics). Payment processors help online merchants adjust their websites to accept Bitcoin. Early user reviews are mixed: users seem largely satisfied, though technical glitches sometimes occur. Merchants appear particularly pleased because Bitcoin payment processing is strikingly low-cost for them. For example, Coinbase (a payment processing firm) currently charges zero percent on incoming payments up to $1 million per merchant per annum, and 1 percent thereafter, which is considerably lower than the fees that merchants bear when a credit card is used to pay for a purchase.

It is less clear that consumers benefit from paying by Bitcoin. Many credit cards provide consumers with rebates of 1 percent, 2 percent or even more, as well as benefits of similar value such as frequent flyer points and merchandise credits. A consumer who pays by Bitcoin loses such rebates or bonuses. Edelman (2014) points out that even if a consumer already has bitcoins, the consumer would be better off making a purchase with a 1.5 percent cashback credit card, paying a 1 percent fee to convert bitcoins to dollars, then using those dollars to pay the credit card bill. Some merchants have responded by providing additional benefits to consumers who pay by Bitcoin: for example, Overstock provides a 1 percent rebate. However, if competing Bitcoin exchanges bid the 1 percent fee for converting from currency to bitcoin downwards, there could be room to make both consumers and merchants better off than through payments by credit card.

The block chain poses a further barrier to using Bitcoin for general-purpose payments. Every Bitcoin transaction, large or small, must be copied into all future

versions of the block chain. If Bitcoin expanded to include a huge volume of transactions—as from millions of users' small day-to-day payments—the storage burden would need to be addressed. Furthermore, updating the block chain entails an undesirable delay, making Bitcoin too slow for many in-person retail payments.

Meanwhile, other users appear to be buying bitcoins not to use them but to hold them in appreciation. Meiklejohn, Pomarole, Jordan, Levchenko, McCoy, Voelker, and Savage (2013) finds that of the bitcoins mined in 2009–2010, more than 60 percent remain unspent or took more than one year to be spent.

Overall, some question whether the growth of Bitcoin payments is actually as rapid as one might expect for a successful payments service. Evans (2014) compares Bitcoin's growth to that of mPesa, a widely used person-to-person payment system using mobile phones in Kenya. Aligning the services based on months since launch, Evans finds Bitcoin's adoption less than one-twentieth as rapid.

Possible and Future: General-Purpose Payments, Mainstream Store of Value, and Enabling Technology

Some proponents envision Bitcoin evolving into an all-purpose payment mechanism. If a payer already held bitcoins and if a payee was content to retain bitcoins rather than convert to a traditional currency, fees would be relatively low: the only costs are transaction fees paid to the successful miner who solved that block's puzzle (and perhaps also a small minting reward). However, to date most payments entail at least one party needing to convert to or from bitcoin, which adds to transaction costs. Overstock.com, the first prominent retailer to accept bitcoins, reports keeping 10 percent of its bitcoin gross receipts in that form (Sidel 2014), but given Overstock's net margin of 0.6 percent (per its 2014 SEC 10-K), this effectively requires transferring profits from the company's other operations.

It might seem natural for consumers to use Bitcoin for international remittances, which may sometimes cost $50 or more, rather than as a substitute for credit card payments where consumers often receive a rebate. But so far, there is little sign of Bitcoin use in this area. The fees from services such as Western Union may appear high at first glance. But Western Union also offers a suite of services including accepting and dispensing cash, which is distinctively useful in low-income countries where transfer from bitcoin to local currency is likely to be difficult and where merchants are unlikely to accept payment by Bitcoin.

Some computer scientists and entrepreneurs report excitement at Bitcoin not for its role in facilitating payments, but for its ability to create a decentralized record of almost anything. Marc Andreessen (2014), best known as coauthor of Mosaic (the first widely-used web browser), presented the rationale:

> Bitcoin gives us, for the first time, a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer. . . . All these are exchanged through a distributed network of trust that does not

> require or rely upon a central intermediary like a bank or broker. What kinds of digital property might be transferred in this way? Think about digital signatures, digital contracts, digital keys (to physical locks, or to online lockers), digital ownership of physical assets such as cars and houses, digital stocks and bonds . . . and digital money.

To date, there has been only limited use of the Bitcoin platform to provide services other than payment. Entrants building on the Bitcoin platform include Namecoin, an alternative domain name system; Colored Coins, a means to manage virtual property rights (Rosenfeld 2012); CommitCoin, a secure commitment scheme (Clark and Essex 2012), a timed version of which can be repurposed to ensure fairness in multi-party computation (Andrychowicz, Dziembowski, Malinowski, and Mazurek 2014) in order to run auctions without an auctioneer; and FutureCoin (Clark, Bonneau, Felton, Kroll, Miller, and Narayanan 2014), which enables decentralized prediction markets. However, none of these startups has attracted large-scale use to date, and each faces significant competition from firms and processes using more traditional system design.

Risks in Bitcoin

Bitcoin's design presents distinctive risks that differ from other payment methods and stores of value. Here, we review market risk, the shallow market problem, counterparty risk, transaction risk, operational risk, privacy-related risk, and legal and regulatory risks.

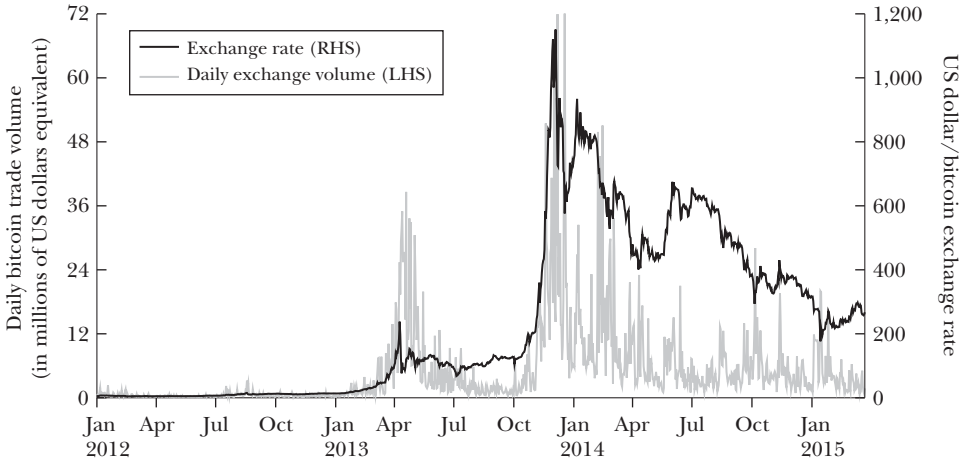
Any user holding bitcoins faces *market risk* via fluctuation in the exchange rate between bitcoin and other currencies. Figure 2 plots the average US dollar–bitcoin exchange rate at the largest exchanges, along with the weekly trade volumes. A user might dismiss the short-term price spikes before mid-2013 as part of the price of using a new currency. But the sharp movements from late 2013 through 2015 would be a source of concern, both for users considering Bitcoin for transactions and for those using it as a store of value.

The relatively low weekly trade volumes suggest that Bitcoin users also experience a *shallow markets problem*: for example, a person seeking to trade a large amount of bitcoin typically cannot do so quickly without affecting the market price.

Given centralization in the Bitcoin ecosystem, *counterparty risk* has become substantial. Exchanges often act as de facto banks, as users convert currency to bitcoin but then leave the bitcoin in the exchange. However, 45 percent of the Bitcoin currency exchanges studied by Moore and Christin (2013) ultimately ceased operation. High-volume exchanges were more likely to close because of a security breach, while operators of low-volume exchanges were more likely to abscond without explanation. Of the exchanges that closed, 46 percent did not reimburse their customers after shutting down. If users avoid holding their bitcoins in an exchange and instead use a digital wallet service, other risks arise, as these firms

Figure 2

US Dollar–Bitcoin Exchange Rate, January 2012–March 2015, along with Daily Bitcoin Trade Volume (in US Dollar Equivalent) at Four Top Currency Exchanges



Source: Authors using data from Blockchain.info and Quandl.com.

have become a lucrative target for cybercriminals. Examples include 4,100 bitcoins (valued at $1.2 million at then-applicable rates) taken from Bitcoin wallet inputs.io in November 2013, leading to that company's default (McMillan 2013) as well as 1,295 bitcoins ($1 million) taken from Bitcoin payment processor BIPS the next month following denial-of-service attacks (Southurst 2013).

The irreversibility of Bitcoin payments creates heightened *transaction risk*. If bitcoins are sent due to error or fraud, the Bitcoin system offers no built-in mechanism to undo the error. Of course, a buyer and seller can voluntarily agree to correct errors, but the Bitcoin protocol has no mechanism to retake the funds by force. In a world of competing payment methods, irreversibility puts Bitcoin at a disadvantage: all else equal, consumers should favor a payment system that allows reversal of unwanted or mistaken charges.

Transaction risk also arises when receiving payments. As discussed above, Bitcoin transactions do not clear (and hence are not final) until they have been added to the authoritative block chain. Transaction batches are only added every ten minutes on average. This creates at least two potential avenues for abuse. First, there is a low but persistent risk that what was once viewed as the authoritative block chain will later be cast aside, as voted on by a majority of participants, canceling any transactions recorded in that version of the block chain. Second, malevolent participants could double-spend bitcoins, particularly through rapid transactions before the block chain is updated. The protocol has taken steps to mitigate this possibility, but researchers have demonstrated viable attacks if Bitcoin is used for faster payments than intended by design (Karame, Androulaki, and Čapkun 2012).

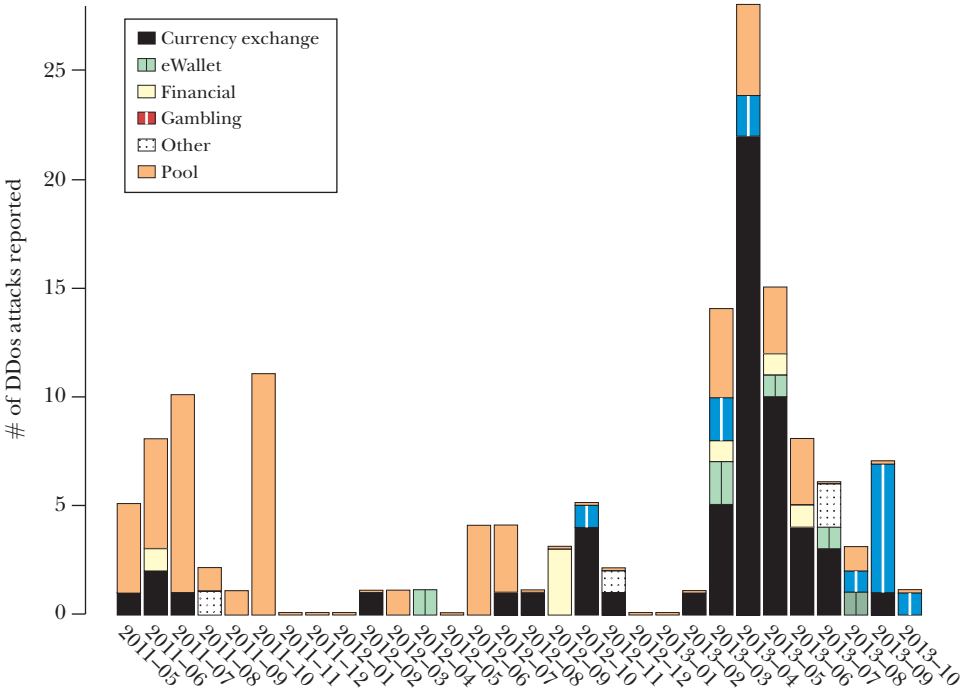
A separate transaction risk arises from proposals to blacklist tainted Bitcoins, specifically those that have been obtained through theft. Some set of arbiters would publicly announce the ill-gotten bitcoins (much like a list of serial numbers on stolen paper currency), and the proposals call on the community to refuse incoming payments appearing on the blacklist. However, blacklists are controversial within the Bitcoin community (Bradbury 2013). After all, blacklists create the prospect of rejecting transactions that have already occurred—transferring losses to those who had unknowingly accepted bitcoin that later turned out to be ill-gotten. Blacklists add significant complexity and create a risk of abuse by those who manage the blacklists. Finally, widespread use of blacklists could undermine the fungibility of bitcoins. With the block chain available for public inspection, each bitcoin can be traced to its unique transaction history, and in principle market participants could place varying values on bitcoins according to their apparent risk of future blacklisting.

Operational risk encompasses any action that undermines Bitcoin's technical infrastructure and security assumptions. For example, despite a user's efforts to keep a private key secure, vulnerabilities are to be expected—including operator error, security flaws, and malware that scours hard drives in search of wallet credentials and private keys. At least as worrisome, the Bitcoin platform faces operational risks through potential vulnerabilities in the protocol design or breakthroughs in cryptanalysis. Community attention has focused on the so-called "51 percent attack," in which if some group can reliably control more than half the computational power, they can seize control of the system (Barber, Boyen, Shi, and Uzen 2012). If such attacks arose, the Bitcoin community might devise defenses, but the conflict and transition would be chaotic and would probably undermine trust in Bitcoin.

Denial-of-service attacks form a particularly prominent operational risk, particularly large for those who use Bitcoin through various intermediaries. Denial-of-service attacks entail swamping a target firm with messages and requests in such volume that it becomes unusable or very slow. Such attacks have diverse motivations. For example, an attack on a mining pool can prevent a pool's participants from solving the current puzzle and thus give an advantage to all other miners (Johnson, Laszka, Grossklags, Vasek, and Moore 2014). News of an attack can undermine trust in an exchange or even in Bitcoin itself—allowing an attacker to buy bitcoin at lower prices. Finally, attackers can demand ransom from service providers (such as exchanges), threatening attacks that would undermine the service's operation and customers' confidence. Figure 3 plots the number of denial-of-service attacks reported by users on the popular bitcointalk.org forum in 2011 to 2013, showing progression from attacks on mining pools to attacks on exchanges. While denial-of-service attacks occur throughout the web, they seem to be particularly effective in the Bitcoin ecosystem due to the relative ease of monetizing the attacks.

Bitcoin raises certain *privacy risks*, most notably the risk that transactions can be linked back to the people who made them. Bitcoin transactions are not truly anonymous: instead, they are *pseudonymous*, in that each transaction specifies account information (the user's public key) albeit without personal names, and the block

Figure 3
Reported (Distributed Denial of Service) DDoS Attacks on Bitcoin Services over Time



Source: Vasek, Thornton, and Moore (2014).

chain publishes transactions by that user identifier. Moreover, transactions made using Bitcoin often reveal real names—for example, as funds are converted to or from currencies in traditional banks, or when purchases from retailers reveal a customer name and mailing address. In principle, a Bitcoin user's identity could be obtained from one such source and then associated with the user's other transactions—flouting the widespread expectation of privacy.

Finally, Bitcoin systems face numerous *legal and regulatory risks* across countries. For example, a law-abiding user could lose funds in an exchange that is frozen or seized due to criminal activity—even if only a portion of the exchange's customers were in fact engaged in such activity. Furthermore, uncertain tax treatment of Bitcoin gains and losses hinders tax planning. We explore these questions in the next section.

Regulating Virtual Currencies

The original vision of Bitcoin is broadly in tension with regulation and government control. In this respect Bitcoin extends a line of cyber-libertarianism, traced

back at least to John Perry Barlow's 1996 "Declaration of the Independence of Cyberspace," denying the role of governments in overseeing online communications. But contrary to the initial view that Bitcoin's decentralization made it impossible to regulate, there now appears to be ample possibility of regulatory oversight, as well as circumstances in which such intervention could be useful.

Fighting Crime

Bitcoin receives regulatory scrutiny for three classes of criminal concerns: Bitcoin-specific crime, money laundering, and Bitcoin-facilitated crime.

Bitcoin-specific crimes are attacks on the currency and its infrastructure like bitcoin theft, attacks on mining pools, and denial-of-service attacks on exchanges to manipulate exchange rates. Law enforcement often struggles to prevent or solve these crimes due to their novelty, lack of clarity on which agency and jurisdiction are responsible, technical complexity, procedural uncertainty, and limited resources.

Second, Bitcoin can be used for *money laundering*. Bitcoin money laundering could evolve to become more difficult to trace, particularly when funds are routed through mixers, with mixing records concealed from the public and perhaps unavailable to law enforcement. These characteristics might assist perpetrators in concealing or mischaracterizing the proceeds of crime. That said, Bitcoin also includes design elements that could facilitate the tracing of funds, including publication of the block chain (providing permanent publicly available records of what funds moved where).

Finally, *Bitcoin-facilitated crime* entails payment for unlawful services delivered (or purportedly delivered) offline, like the illegal goods and services sold on Silk Road and payment of funds in extortion. Criminals may be drawn to virtual currencies because they perceive a lack of regulatory oversight, because they distinctively value irreversible transactions, or because they have been banned or ejected from other payment mechanisms.

Consumer Protection

A related justification for regulatory action is the need for consumer protection. Such discussions were particularly frequent after the February 2014 failure of Bitcoin exchange Mt. Gox, which lost bitcoins valued at more than $300 million. In light of this failure and others (Moore and Christin 2013), it is desirable to have orderly processes that distribute any remaining assets equitably. The risk of collapse also calls for disclosures to help consumers understand the products they are buying.

Broader consumer protection concerns result from irreversibility of Bitcoin transfers. Most electronic payment systems provide mechanisms to protect consumers against unauthorized transfers, and indeed such protections are often codified into law. (For example, credit card dispute rights are guaranteed by the US Fair Credit and Billing Act, 15 USC § 1666.) The absence of such protections in Bitcoin therefore appears to be contrary to longstanding public policy.

Regulatory Options

A key challenge for prospective regulators is where to impose constraints. It is infeasible to regulate all peers in the Bitcoin network due to their quantity, their geographic distribution, and the privacy protections in the network. Instead, regulators are naturally drawn to key intermediaries. But intermediaries raise predictable defenses. Why, they ask, should they face liability for the conduct of third-party users, customers, or suppliers? Furthermore, some users will anticipate regulators targeting intermediaries and will act to avoid such scrutiny, just as criminals can pay each other in cash to hide illegal activities from financial institutions.

The FBI takedown of Silk Road in 2013 illustrates both the challenges of regulation and regulators' ultimate power. Silk Road was hosted as a "hidden service" on Tor, a system which is purpose-built for anonymity of both visitors and operators. Payments were only accepted in bitcoin. However, the Silk Road domain site was seized by the FBI when the site's alleged operator, Ross Ulbricht, was arrested on charges of conspiracy to distribute controlled substances, computer hacking, money laundering, and murder-for-hire charges. The private keys associated with Ulbricht's 144,000 bitcoins were also seized by the FBI (Greenberg 2013). Investigators targeted large merchants and administrators on Silk Road, exploiting poor operational security tactics to find their real identities. Ulbricht himself was identified by finding an early Silk Road advertisement posted on an online forum using his personal Gmail address (Zetter 2013). Silk Road's online presence and electronic records in some respects made it an easier target than, say, a small-time dealer of drugs or weapons.

Transfers through currency exchanges are also within regulators' grasp. In March 2013, the US Financial Crimes Enforcement Network issued guidance on when virtual currency operators should be classified as money-services businesses, requiring certain registration, reporting, and recordkeeping obligations. As exchanges complied, account details became available to regulators, and two months later, a US judge signed a seizure warrant for an account at the Mt. Gox exchange. In China, a December 2013 policy was broadly similar, requiring that Bitcoin intermediaries implement know-your-customer registrations for account-holders (People's Bank of China and Five Associated Ministries 2013). These regulatory requirements will not impede peer-to-peer bitcoin transactions that are not facilitated by currency exchanges. But it seems longstanding reporting requirements can provide a level of compliance for virtual currencies similar to what has been achieved for traditional currencies.

In principle, Bitcoin's electronic implementation in some ways makes it easier to regulate than offline equivalents. Consider the problem of theft. Once stolen cash enters circulation, little can be done to reclaim it. In contrast, Bitcoin blacklists could let law enforcement claw back all ill-gotten or stolen bitcoins—albeit with the problems discussed earlier.

Tax treatment of Bitcoin remains unsettled. In March 2014, the Internal Revenue Service (2014) issued guidance that transactions to and from virtual currencies may create taxable events for federal tax purposes. Thus, if a user converts

dollars to bitcoin at one exchange rate, then later converts back at a higher rate, the user may owe tax on the appreciation; conversely, losses could offset gains elsewhere. Depending on the user's purpose and primary activity, the gains and losses could be ordinary income or capital (Notice 2014-21). While this guidance seems well-grounded in longstanding principles of US tax law, it was criticized for creating additional record-keeping and complexity, particularly for those whose conversions are frequent.

While Bitcoin now appears to be subject to regulatory oversight, the authority of regulators faces certain limits. For example, if one country places too large a burden on Bitcoin services based there, services are likely to develop elsewhere. If many countries impede use of Bitcoin, some users will resort to services like Zerocash with even stronger security precautions—likely letting criminals continue to use the service yet, perhaps, adding too much complexity for mainstream consumers. The overall regulatory goal should not take aim at Bitcoin or any other specific system or company, but instead should consider regulations in the broader context of a global market for virtual currency services.

Bitcoin as a Social Science Laboratory

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 record 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). To date, researchers have considered diverse questions ranging from design of financial markets to user behavior along with myriad questions of law and regulation. This research is of course quite recent, and much of it is still in working paper form. Many questions remain open, particularly to researchers who combine a deep understanding of Bitcoin with technical skills to collect data and a solid background in social science. Here are some of the issues this research has tackled and could approach in the future.

Bitcoin as a Financial Asset

After comparing exchange-traded volume of bitcoins to total transaction volume within the Bitcoin network, Glaser, Zimmerman, Haferkorn, Weber, and Sterling (2014) conclude that most users (by volume) treat their bitcoin investments as speculative assets rather than as means of payment. Bitcoin investments seem to offer diversification benefits according to Brière, Oosterlinck, and Szafarz (2013), who study correlations between bitcoin and other asset classes. Gandal and Halaburda (2014) examine exchange rates of different virtual currencies to observe comovement and identify opportunities for triangular arbitrage. Preliminary results on daily "closing" prices indicate little opportunity, although this may reflect that the arbitrageurs operate faster than the frequency of data points. Of course, given

ongoing fluctuations in bitcoin prices and innovations in other virtual currencies, new data is already available for these kinds of studies.

Incentive-compatibility in Bitcoin Protocols

When confronted by a set of protocols, economic agents naturally look for ways to participate that increase their own gains. For example, early mining pools faced selfish behavior in the form of "pool hopping": Miners opted out of the pool in long rounds, in which the potential block reward has to be shared with a larger group. This drew attention to the mechanism design problem of keeping the expected payoff constant over time (Rosenfeld 2011).

Overall, the standard Bitcoin client software does not always act in the best interest of its principal. Both on the peer-to-peer network layer (Babaioff, Dobzinski, Oren, and Zohar 2012) and for the block mining protocol (Eyal and Sirer 2014), the prescribed rules are not equilibrium strategies if one considers the option to withhold information on a selective and temporary basis. Furthermore, Houy (2014b) observes that larger blocks are less likely to win a block race than smaller ones, meaning that a miner reduces the chance of collecting a reward when including new transactions into blocks—raising the question of why miners include transactions into blocks at all. So far, these concerns are theoretical. We are not aware of empirical evidence demonstrating substantial deviations from the suboptimal rules.

Privacy and Anonymity

The protection of online privacy and personal information arises in many contexts, and Bitcoin offers a specific set of rules and firms like the "mixers" that seek to offer privacy—although as we have seen, the privacy protections can be breached in various ways. Several papers analyze the public Bitcoin transaction history (Reid and Harrigan 2012; Ober, Katzenbeisser, and Hamacher 2013; Ron and Shamir 2013), finding a set of heuristics that can help to link Bitcoin accounts with real-world identities as long as some additional information is available for a related transaction. Androulaki, Karame, Roeschlin, Scherer, and Čapkun (2013) quantify the anonymity in a simulated environment similar to Bitcoin, finding that almost half of the users can be identified by their transaction patterns.

Monetary Policy

In a broad sense, the Bitcoin economy implements a variant of Milton Friedman's (1960, p. 90) "k-percent rule"—that is, a proposal to fix the annual growth rate of the money supply to a fixed rate of growth. Indeed, Bitcoin's protocol calls for an end of the minting phase at which point $k = 0$. In fact, k may even be negative in the future, because bitcoins can be irreversibly destroyed when users forget their private keys. This raises one of the classic questions in monetary policy: What happens when the size of an economy grows at a different rate than the quantity of money in that economy? Or if viewing Bitcoin as a social science laboratory, what happens if the Bitcoin economy grows faster than the supply of bitcoins?

Just as overly rapid growth of a money supply is classically linked to inflation, the fixed slow growth rate of Bitcoin creates the possibility of deflation if Bitcoin was to be used widely, as Krugman (2011) noted while comparing the Bitcoin economy to the gold standard. In response to this risk, developers proposed alternative system rules. For example, Primecoin and Peercoin modify Bitcoin to provide an unlimited money supply, with k fixed to approximately 1 percent for Peercoin.

It remains unclear whether decentralized cryptographic currencies can be designed with monetary policies that include feedback or even discretion. Bitcoin's design embodies a basic version of monetary policy that does not consider the state of the real economy. We note that Bitcoin's block chain presents a crude measure of monetary indicators—specifically the number of transactions and their nominal amount—but offers no information about what value was actually provided in exchange for payment. The block chain thus lays the groundwork for automatic monetary policy based solely in nominal data, but does not facilitate any policy based on real economic activity. Human arbiters could presumably add information about economic conditions or could introduce discretion by judgment, but they would also introduce the governance questions Bitcoin set out to overcome. Further experience with Bitcoin and other virtual currencies may illuminate some of the longstanding issues on the conduct and effects of monetary policy.

Looking Ahead

What is the future of Bitcoin and other virtual currencies? To replace credit cards for everyday consumer payments? To displace Western Union and other firms for international cash payments? To supplant banks for short-term deposits? Will Bitcoin and other virtual currencies favor low costs (to undercut competitors), privacy (to serve users who distinctively seek that benefit), or decentralization (to avoid a single point of control)? When disputes arise, do Bitcoin service providers protect sellers (who seek finality) or buyers (who often want refunds)? The original vision of Bitcoin offered one set of answers, but as new constituents approach the service, it becomes less clear that early design decisions meet prevailing requirements. It is also uncertain whether a single service can serve all needs. For example, those who seek greater privacy may be prepared to accept greater technical complexity and perhaps higher fees. However, recruiting mainstream consumers and merchants seems to call for a focus on simplicity and lower prices.

Bitcoin may be able to accommodate a community of experimentation built on its foundations. Mixers already close the most obvious privacy shortcomings in Bitcoin's early design, while pools help reduce risk for miners, and wallets address some of consumers' usability and security concerns.

Other aspects of Bitcoin architecture are largely locked in place through its protocol design. For example, the block chain is the essence of Bitcoin. There is no clear way for Bitcoin to substitute a different approach to record-keeping while retaining installed Bitcoin software, remaining compatible with intermediary

systems, and, most importantly, retaining the overall consensus that has coordinated around Bitcoin. Instantaneous transaction confirmations seem to require equally fundamental changes. In these and other respects, Bitcoin will struggle to make adjustments.

Numerous competing virtual currencies are waiting in the wings. For example, Litecoin confirms transactions four times faster than Bitcoin, potentially facilitating retail use and other time-sensitive transactions. NXT reduces the electrical and computational burden of Bitcoin mining by replacing proof-of-work mining with proof-of-stake, assigning block chain duties in proportion to coin holdings. Zerocash (Ben-Sasson et al. 2014), which is not yet operational, will seek to improve privacy protections by concealing identifiers in the public transaction history. Peercoin allows a perpetual 1 percent annual increase in the money supply.

To offer their competing design decisions, alternative virtual currencies would first need to achieve confidence in their value and adoption. Bitcoin benefited from early excitement for its service, buyers and sellers at Silk Road, and favorable press coverage. A replacement virtual currency would struggle to obtain this combination of advantages, but without favorable expectations for growth, few would be willing to convert traditional currency into a competing coin. Whether or not Bitcoin expands as its proponents envision, it offers a remarkable experiment, a lab for researchers, and an attractive means of exchange for a subset of merchants and consumers.

References

Abrams, Rachel, Goldstein, Matthew, and Tabuchi, Hiroko. 2014. "Erosion of Faith Was Death Knell for Mt. Gox." *New York Times*, February 28.

Anderson, Ross. 2012. "Risk and Privacy Implications of Consumer Payment Innovation in the Connected Age." Proceedings of the Conference on Consumer Payment Innovation in the Connected Age, Federal Reserve Bank of Kansas City, March 29–30. pp. 99–116. http://www.kc.frb.org/publicat/pscp/2012/Session-3.pdf.

Andreessen, Marc. 2014. "Why Bitcoin Matters." *New York Times*, DealBook, January 21.

Androulaki, Elli, Ghassan O. Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Čapkun. 2013. "Evaluating User Privacy in Bitcoin." In *Financial Cryptography and Data Security*, vol. 7859 of *Lecture Notes in Computer Science*, pp. 34–51. Springer.

Andrychowicz, Marcin, Stefan Dziembowski, Daniel Malinowski, and Łukasz Mazurek. 2014. "Secure Multiparty Computations on Bitcoin." *Proceedings of the 35th IEEE Symposium on Security and Privacy*, May 18–21. IEEE Press.

Babaioff, Moshe, Shahar Dobzinski, Sigal Oren, and Aviv Zohar. 2012. "On Bitcoin and Red Balloons." In *Proceedings of 13th ACM Conference on Electronic Commerce*, pp. 56–73. ACM.

Barber, Simon, Xavier Boyen, Elaine Shi, and Ersin Uzun. 2012. "Bitter to Better—How to Make Bitcoin a Better Currency." In *Financial Cryptography and Data Security*, vol. 7397 of *Lecture Notes in Computer Science*, pp. 399–414. Springer.

Barlow, John Perry. 1996. "A Declaration of the Independence of Cyberspace." https://projects.eff.org/~barlow/Declaration-Final.html (last accessed March 15, 2015).

Ben-Sasson, Eli, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. 2014. "Zerocash: Decentralized Anonymous Payments from Bitcoin." *Proceedings of the 2014 IEEE Symposium on Security and Privacy,* May 18–21, 2014.

Bitcoincharts.com. 2015. "Bitcoin Network." http://bitcoincharts.com/bitcoin/ (last accessed March 20, 2015).

Bitcoin Wiki. 2015a. "Category:Gambling." https://en.bitcoin.it/wiki/Category:Gambling (last accessed March 20, 2015).

Bitcoin Wiki. 2015b. "Mining Hardware Comparison." https://en.bitcoin.it/wiki/Mining_hardware_comparison (last accessed March 20, 2015).

Bitcoinity.org. 2015. "Exchanges." https://bitcoinity.org/markets/list (last accessed March 20, 2015).

Blockchain.info. 2015. "Bitcoin Charts." https://blockchain.info/charts/ (last accessed March 20, 2015).

Böhme, Rainer. 2013. "Internet Protocol Adoption: Learning from Bitcoin." *Proceedings of the IAB Workshop on Internet Technology Adoption and Transition (ITAT)*, Cambridge, UK.

Bonneau, Joseph. 2014. "Estimating the Power Consumption of Bitcoin." Presented at Financial Cryptography and Data Security, 18th International Conference (rump session), Bridgetown, Barbados, March 4, 2014.

Bradbury, Danny. 2013. "Anti-Theft Bitcoin Tracking Proposals Divide Bitcoin Community." *Coindesk*, November 15.

Brière, Marie, Kim Oosterlinck, and Ariane Szafarz. 2013. "Virtual Currency, Tangible Return: Portfolio Diversification with Bitcoins." Available at SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2324780.

Chaum, David. 1983. "Blind Signatures for Untraceable Payments." In *Advances in Cryptology*, edited by D. Chaum, R. L. Rivest, and A. T. Sherman, 199–203. Springer.

Christin, Nicolas. 2013. "Traveling the Silk Road: A Measurement Analysis of a Large Online Anonymous Marketplace." *Proceedings of the 22nd International World Wide Web Conference (WWW'13)*, pp. 213–24. Rio de Janeiro, Brazil, May 2013.

Clark, Jeremy, Joseph Bonneau, Edward W. Felten, Joshua A. Kroll, Andrew Miller, and Arvind Narayanan. 2014. "On Decentralizing Prediction Markets and Order Books." Workshop on the Economics of Information Security, State College, Pennsylvania, June 2014.

Clark, Jeremy, and Aleksander Essex. 2012. "CommitCoin: Carbon Dating Commitments with Bitcoin." In *Financial Cryptography and Data Security*, vol. 3797 of *Lecture Notes in Computer Science*, pp. 390–98. Springer.

Danezis, George, and Claudia Diaz. 2008. "A Survey of Anonymous Communication Channels." Microsoft Research Technical Report MSR-TR-2008-35.

Diffie, Whitfield, and Martin E. Hellman. 1976. "New Directions in Cryptography." *IEEE Transactions on Information Theory* 22(11): 644–54.

Dingledine, Roger, Nick Mathewson, and Paul Syverson. 2004. "Tor: The Second-Generation Onion Router." In *Proceedings of the 2004 USENIX Security Symposium*. USENIX.

D.K. 2013. "Bitcoin's Collapse: China Blues." *The Economist,* December 18.

Edelman, Benjamin. 2014. "Consumers Pay More When They Pay with Bitcoin." PYMNTS.com, May 20.

European Central Bank. 2012. *Virtual Currency Schemes*. Technical Report, October. https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf (last accessed April 1, 2015).

Evans, David S. 2014. "Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms." Coase-Sandor Institute for Law and Economics Working Paper 685, April.

Eyal, Ittay, and Emin Gün Sirer. 2014. "Majority is Not Enough: Bitcoin Mining is Vulnerable." In *Financial Cryptography and Data Security*, vol. 8437 of *Lecture Notes in Computer Science*, pp. 436–54. Springer.

Financial Crimes Enforcement Network (FinCEN), US Department of the Treasury. 2015. "Enforcement Actions for Failure to Register as a Money Services Business." http://www.fincen.gov/news_room/ea/ea.msb.html (last accessed March 20, 2015).

Friedman, Milton. 1960. *A Program for Monetary Stability*. New York: Fordham University Press.

Gandal, Neil, and Hanna Halaburda. 2014. "Competition in the Crypto-Currency Market." Presentation at the Workshop on the Economics of Information Security, State College, PA, June 2014.

Glaser, Florian, Kai Zimmermann, Martin Haferkorn, Moritz Christian Weber, and Michael Siering. 2014. "Bitcoin—Asset or Currency? Revealing Users' Hidden Intentions." *Proceedings of the 22nd European Conference on Information Systems*, Tel Aviv, June 2014.

Greenberg, Andy. 2013. "FBI Says It's Seized $28.5 Million in Bitcoins from Ross Ulbricht, Alleged Owner of Silk Road." *Forbes,* October 25.

Hicks, John R. 1967. *Critical Essays in Monetary Theory*. Clarendon Press.

Houy, Nicolas. 2014a. "The Economics of Bitcoin Transaction Fees." GATE WP 1407

Université de Lyon, Groupe d'Analyse et de Théorie Economique (GATE), February. Available at SSRN: http://ssrn.com/abstract=2400519.

Houy, Nicolas. 2014b. "The Bitcoin Mining Game." March. Available at SSRN: http://ssrn.com/abstract=2407834.

Internal Revenue Service (IRS). 2014. "IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply." March 25.

Johnson, Benjamin, Aron Laszka, Jens Grossklags, Marie Vasek, and Tyler Moore. 2014. "Game-Theoretic Analysis of DDoS Attacks against Bitcoin Mining Pools." In *Financial Cryptography and Data Security*, vol. 8438 of *Lecture Notes in Computer Science*, Part I: First Workshop on Bitcoin Research, pp. 72–86. Springer.

Karame, Ghassan O., Elli Androulaki, and Srdjan Čapkun. 2012. "Double-spending Fast Payments in Bitcoin." In *Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS '12)*, pp. 906–917. ACM.

Kim, Victoria. 2014. "Dutch National Pleads Guilty to Running Online Marketplace for Drugs." *Los Angeles Times*, September 3.

Krugman, Paul. 2011. "Golden Cybervetters." *New York Times,* September 7.

MacCarthy, Mark. 2010. "What Payment Intermediaries Are Doing about Online Liability and Why It Matters." *Berkeley Technology Law Journal* 25(2): 1037–1120.

Matonis, Jon. 2013. "Bitcoin Casinos Release 2012 Earnings." *Forbes,* January 22.

McLeod, Andrew Saks. 2013. "Bitcoins Soar in Value in Argentina due to Capital Control Laws." *Forex Magnates*, July 9.

McMillan, Robert. 2013. "$1.2M Hack Shows Why You Should Never Store Bitcoins on the Internet." *Wired*. November 7.

Meiklejohn, Sarah, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage. 2013. "A Fistful of Bitcoins: Characterizing Payments among Men with No Names." In *Proceedings of the 2013 ACM Internet Measurement Conference (IMC),* pp. 127–40. ACM.

Moore, Tyler, and Nicolas Christin. 2013. "Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk." In *Financial Cryptography and Data Security*, vol. 7859 of *Lecture Notes in Computer Science*, pp. 25–33. Springer.

Möser, Malte, and Rainer Böhme. 2014. "Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees." Available at SSRN: http://ssrn.com/abstract=2530843. Forthcoming in *Proceedings of the 2nd Workshop on Bitcoin Research*, January 2015.

Möser, Malte, Rainer Böhme, and Dominic Breuker. 2013. "An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem." *Proceedings of APWG eCrime Researchers Summit*, San Francisco.

Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." https://bitcoin.org/bitcoin.pdf (last accessed March 31, 2015).

Ober, Micha, Stefan Katzenbeisser, and Kay Hamacher. 2013. "Structure and Anonymity of the Bitcoin Transaction Graph." *Future Internet* 5(2): 237–50.

People's Bank of China and Five Associated Ministries. 2013. "Prevention of Risks Associated with Bitcoin." Notice. Translation available at https://vip.btcchina.com/page/bocnotice2013 (last accessed March 20, 2015).

Raskin, Max. 2013. "Meet the Bitcoin Millionaires." *Bloomberg Businessweek,* April 10.

Reid, Fergal, and Martin Harrigan. 2012. "An Analysis of Anonymity in the Bitcoin System." In *Security and Privacy in Social Networks,* edited by Yaniv Altshuler et al., pp. 197–223. Springer.

Ron, Dorit, and Adi Shamir. 2013."Quantitative Analysis of the Full Bitcoin Transaction Graph." In *Financial Cryptography and Data Security*, vol. 7859 of *Lecture Notes in Computer Science*, pp. 6–24. Springer.

Rosenfeld, Meni. 2011. "Analysis of Bitcoin Pooled Mining Reward Systems." November 17. https://bitcoil.co.il/pool_analysis.pdf (last accessed March 20, 2015).

Rosenfeld, Meni. 2012. "Overview of Colored Coins." https://bitcoil.co.il/BitcoinX.pdf (last accessed March 20, 2015).

Sidel, Robin. 2014. "Overstock CEO Sees Bitcoin Sales Rising More than Expected." *Wall Street Journal,* March 4.

Song, Sophie. 2014. "The Rise and Fall of Bitcoin in China: Central Bank Shuts Down All Chinese Bitcoin Exchanges." *International Business Times*, March 27.

Southurst, Jon. 2013. "Bitcoin Payment Processor BIPS Attacked, Over $1m Stolen." *CoinDesk,* November 25.

Taylor, Michael Bedford. 2013. "Bitcoin and the Age of Bespoke Silicon." Presented at the "International Conference on Compilers, Architecture and Synthesis for Embedded Systems (CASES)," September–October, 2013. http://cseweb.ucsd.edu/~mbtaylor/papers/bitcoin_taylor_cases_2013.pdf (last accessed March 20, 2015).

United States of America v. Mark Peter Williams et al. 2011. C.D.CA Case No. CR-11-01137.

United States of America v. Ross William Ulbricht. Indictment. S.D.NY Case No. 14-CRIM-068.

United States of America v. Ross William

Ulbricht. Government Exhibit 940. S.D.NY Case No. 14-CRIM-068.

Vasek, Marie, Micah Thornton, and Tyler Moore. 2014. "Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem." In *Financial Cryptography and Data Security*, vol. 8438 of *Lecture Notes in Computer Science*, Part 1: First Workshop on Bitcoin Research, pp. 57–71. Springer.

World Nuclear Association. 2015. "Nuclear Power in the World Today." http://www.world-nuclear.org/info/Current-and-Future-Generation/Nuclear-Power-in-the-World-Today/ (last accessed March 20, 2015).

Yeow, Andy. 2015. "Global Bitcoin Nodes Distribution." https://getaddr.bitnodes.io/ (last accessed March 20, 2015).

Zetter, Kim. 2013. "How the Feds Took Down the Silk Road Drug Wonderland." *Wired*, November 18.