Bitcoin

Rainer Böhme, Nicolas Christin, Benjamin Edelman, Tyler Moore

forthcoming in *Journal of Economic Perspectives*
(subject to revisions not reflected in this draft)

draft as of July 15, 2014

Bitcoin is an online communication protocol that facilitates virtual currency including electronic payments. Since its inception in 2009 by an anonymous group of developers (Nakamoto, 2008), Bitcoin has served approximately 41.8 million transactions between 62.8 million accounts. As of July 2014, the daily transaction volume was approximately 100,000 bitcoin (roughly $50 million at market exchange rates) and the total market value of all bitcoins in circulation was $8 billion. (Blockchain.info 2014).

Many Bitcoin design principles are familiar from the Internet's architecture. For one, Bitcoin's rules were designed by engineers, not lawyers or regulators. Furthermore, Bitcoin emphasizes decentralization. Rather than store transactions on any single server or set of servers, Bitcoin uses a distributed transaction log with mechanisms to reward honest participation, bootstrap acceptance by early adopters, and guard against concentrations of power. Anyone can create an account, without charge and without any centralized vetting procedure or requirement to provide a real name.

Other key features of Bitcoin's design are irreversible transactions, a prescribed path of money creation, and a public transaction history. Collectively, these 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 in part for its potential to disrupt existing payment systems and perhaps monetary systems, and also for the wealth of data it provides about agents' behavior and about the Bitcoin system itself. This article presents the platform's design principles and properties for a non-technical 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

The History of Scarce Tokens

Most economics research defines money not by its form but by its functions (Hicks 1967, p.1). Money serves as a means of exchange, as a store of value, and as a unit of account. In principle, virtual currencies can provide all these functions.

Scarcity is a prerequisite for ascribing value to any form of money. In the small, scarcity protects against counterfeits--preventing an attacker from creating money at will. More broadly, scarcity bounds the growth path of the monetary base and facilitates price stability.

History reveals three broad sources of scarcity. First, precious metals and shell tokens were *observed* to be scarce in nature, which made them good choices for money (especially when combined with their transferability, durability and to some extent fungibility). Later, scarcity of paper money and other man-made tokens relied on asymmetric access to technology. In particular, with superior access to capital, a government printing press was intended to provide superior printing technology which poorly-funded forgers would be unable to mimic. Finally, book money is scarce thanks to legal rules ensuring the correctness of bookkeeping records.

These sources of scarcity are not absolute. Nobody knows how much gold there exists in the universe or how cheaply it may be synthesized in the future. From alchemy to the exploitation of colonial wealth, history shows numerous attempts to overcome scarcity, and technological advances and cost reductions have reduced the technological gap between governments and forgers (Murdoch, 2006; Christin, 2012).

Meanwhile, scarcity writ large depends on trust in the institutions that govern the mint or oversee bookkeeping in the banking system. In modern monetary systems, the lack of absolute scarcity has been reimagined as a feature that lets central banks adjust the amount of money in circulation (typically in some form of monetary transmission process linked to lending) in order to serve policy goals.

Against this backdrop, Bitcoin can be understood as the first widely adopted mechanism to provide absolute scarcity enforced by mechanized logic, specifically the closure of a family of mathematical expressions. Bitcoin specifies the expressions indirectly through a software algorithm that checks whether a given unit of value is genuine and announces each transaction publicly. Bitcoin then implements this algorithm in a massively distributed system: many networked computers, ideally owned and controlled by many equal and independent parties, continuously run a protocol that compares computation results and establishes consensus by majority vote with very high probability. The underlying mathematics and associated verification systems assure that bitcoins are scarce, which facilitates their use as a virtual currency.

Enabling Technologies

The Bitcoin core consists of the protocol (including an open-source reference implementation), many globally distributed computers connected in a peer-to-peer network on top of standard Internet protocols, and the state of the system, which is encoded in a distributed data structure that holds the system's transaction ledger. The Bitcoin core is surrounded by an ecosystem of agents who use Bitcoin and offer related services, as discussed in subsequent sections.

By design, Bitcoin lacks a centralized authority to distribute coins or track who holds which coins. Consequently, the process of issuing currency, verifying validity, and confirming balances is considerably more difficult than in classic bookkeeping systems. The primary innovation in Bitcoin's design is its ability to perform these functions without a centralized authority.

Bitcoins are actually 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. Indeed, each bitcoin can readily be traced back through all transactions in which it was used, and thus to its start of its circulation.

A consequence of decentralized verification and consensus is that all 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 (e.g., Bob pays Charlie using bitcoin he received from Alice).

The Role of Cryptography

Whereas most encryption conceals information from public scrutiny, Bitcoin uses cryptography for the fundamentally different purpose of enforcing system fairness. First, Bitcoin uses private keys to authorize spending money: Only with an account-holder's private key may funds from that account be spent. Digital signatures then allow others to verify that a given message, purportedly spending funds from a given account, in fact occurred with permission from the authorized user of that account. Notice that no centralized bookkeeper is needed; no single party need know all account holders. Rather, the system is open, and standard public-private cryptography (Diffie and Hellman 1976) lets anyone verify that a message comes from its putative sender.

Second, Bitcoin uses cryptographic principles to facilitate an accurate and non-gameable record of transactions, known as the "block chain." In principle the Bitcoin system could use 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, known as a Sybil attack (Douceur, 2002). 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 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."

Incentives for Participation

Keeping the transaction record operational is a public good, serving the Bitcoin system as a whole. To encourage users to assist, the Bitcoin system periodically awards newly-minted bitcoins to the user who solves a puzzle in the proof-of-work system. Upon solving the puzzle, the user broadcasts a "block" containing the solution, all observed transactions that have taken place since the last puzzle solution was announced, and a reference to the previous block. Because the puzzle depends on the contents of the block, the solution to the puzzle prevents tampering with the block (and hence prevents modifying prior transactions). After verifying the solution, users start working on a new block containing new outstanding transactions. This recursively ensures that the total historical ordering on all blocks ("chain") is agreed by the entire network.

Through this design, the proof-of-work mechanism simultaneously discourages Sybil attacks and also provides incentives to participate in verifying the block chain. Because this task yields a periodic reward, it is typically called *mining*, apropos of the search for precious metals.

Despite the benefits of miners updating the block chain, their computational efforts carry significant costs. In particular, the proof-of-work calculations are quite power-intensive, consuming more than 100 megawatts of electricity continuously (Bonneau, 2014). That is approximately 15% of an average nuclear power plant, approximately $108 million per year at average US residential electricity prices. This cost has grown sharply and is likely to rise further because the Bitcoin protocol automatically adjusts puzzle difficulty in a feedback loop so that the interval between two blocks stays at roughly ten minutes. As more computing power is added, puzzles automatically become commensurately more difficult, increasing computing and electricity requirements for those who wish to seek favorable chances to win. In fact, an arms race has ensued as the price of bitcoin has risen. Taylor (2013) compares the difficulty of solving the puzzle to the bitcoin-dollar exchange rate, finding that spikes in the exchange rate have been followed by increases in computational difficulty.

The final purpose of the mining process is to inject new currency into circulation. At first, miners solving the puzzle received a reward of 50 bitcoins. This reward is periodically cut in half, and it now stands at 25. When 21 million bitcoins have been created, the reward falls to zero and no further bitcoins will be created. Hence, Bitcoin's "monetary policy" is set in advance by the protocol design.

Linking money creation with incentives to provide a public good also helped to reward early users of Bitcoin. In particular, 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 rewarded 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 low-cost electricity.

A notable similarity between Bitcoin mining and the historic search for (say) gold is that both entail important elements of waste. Searching for gold is manifestly wasteful--diverting productive resources into finding a resource of no intrinsic value, creating no genuine social benefit. In Bitcoin, miners' energy is used in part to support the system and update the block chain, valuable in making the Bitcoin system reliable and trustworthy. Yet the ever-increasing puzzle difficulty yields large increases in energy requirements. While the search for gold primarily creates jobs (miners, those who build the machines they use, and the surrounding ecosystem), the most notable effect of Bitcoin mining is to consume electricity, increasing energy prices for others.

What Bitcoin Doesn't Have

Compared with other payments systems, Bitcoin notably lacks a governance structure to shape or constrain its operations. For example, Bitcoin imposes no obligation for a financial institution, payment processor, or other intermediary to verify a user's identity or cross-check with

watchlists 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. Finally, Bitcoin payments are irreversible in the sense that the protocol provides no way for a payor 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. In particular, Bitcoin relies on network consensus rather than central authorities both for verifying transactions and for minting new currency. Decentralization offers several benefits. First, it avoids concentrations of power that could let a single person or organization take control. Second, decentralization often promotes availability and resiliency of a computer system, avoiding a central point of failure. Third, decentralization offers at least the appearance of greater privacy for users (and perhaps greater genuine privacy), since in theory, an eavesdropping adversary cannot observe transactions by targeting any single point or any single server. (That said, as we discuss below, privacy concerns remain.) Early adopters praised decentralization and by all indications chose Bitcoin because they wanted to use a decentralized system. (Raskin, 2013)

While the Bitcoin protocol supports complete decentralization (including all participants acting as miners), there is *de facto* centralization 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 in “Uses of Bitcoin” (below).

Currency Exchanges

Currency exchanges let users 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 of 0.2 to 2%. Some exchanges offer more advanced trading tools, such as limit or stop orders. Derivatives markets and short-selling remain rare as of July 2014.

While there are few technical barriers to setting up intermediaries in the Bitcoin ecosystem, in practice there are significant regulatory requirements as well as technical challenges. 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 expenses are often not negligible, particularly since registration includes a state-by-state licensing requiring both legal fees and posting bonds. With certification in a single state often costing at least $10,000, nationwide participation could easily cost well into the six figures. 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 €5M. In addition, currency exchanges are attractive targets and need online infrastructure capable of withstanding denial-of-service, hacking, and other 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% of all Bitcoin transactions. As of July 2014, the five largest exchanges were OKCoin, Huobi, Bitfinex, Bitstamp, and BTC-e which jointly served more than 90% of all Bitcoin trade over January-June 2014 (Bitcoinity.org 2014).

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 computers to maintain control over their bitcoins. However, many users find this task unappealing: Bitcoin wallets can be difficult to install, and some impose onerous technical requirements (such as storing a copy of the entire block chain, 19 gigabytes as of July 2014). Other users worry about security: a crash or attack could cause the loss of a user’s bitcoins.

As a result, many users rely on a digital wallet service that keeps 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 (including Blockchain.info, StrongCoin and CoinPunk) let the user keep 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). But then 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 them store their private keys, increasing risk if the service is attacked. In practice, digital wallets tend to increase centralization--either expanding the role and importance of exchanges, or adding an additional service 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 payor to each payee, along with the pseudonyms of each. Then anyone who knows the identity of any user from any transaction (perhaps due to the mailing address used for delivery of purchased goods, or the bank account used to purchase Bitcoins) can track that user’s other transactions, both before and since.

To defend against this tactic, *mixers* let users pool sets of transactions in unpredictable combinations--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. 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 payors with little recourse if a mixer absconds with their funds. Furthermore, mixing protocols are usually not public, so their effectiveness cannot be formally proven. Indeed, there is reason to suspect that correlations in timing could reveal transaction counterparts, particularly at little-used mixers. (Möser et al., 2013) Finally, mixers charge 1% to 3% 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 cryptographic puzzle. Puzzles have become significantly more difficult, and lumpy rewards mean a lone miner is now at risk of contributing resources but receiving no reward. In response, 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 July 2014, the two largest pools are GHash and Discus Fish which together account for more than half 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% of total mining power, which could have allowed GHash pool operators to attempt manipulations. Indeed, an attacker who holds a majority of Bitcoin's computational resources can alter the system's records, including inserting false transactions and rejecting actual transactions (albeit with a strong chance that others will notice at least their position of control, if not their actual alterations). More generally, the concentration of control over computational power in the hands of a few mining pools could allow these pool operators to collude and arbitrarily rewrite protocol rules or transaction history.

On the whole, then, the decentralization initially touted by Bitcoin has not fully come to fruition. Indeed there seem to be significant forces pushing towards concentration despite Bitcoin's design.

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 the unusual features of the Bitcoin payment system not available through alternatives. Two features were particularly distinctive: First, Bitcoin provided (or appeared to provide) greater anonymity than other online payment systems. Second, the Bitcoin platform imposed no rules on what could be bought or sold. These features fueled Bitcoin's adoption in

markets serving customers who sought anonymity and in markets that other payment platforms rejected.

A notable early example came in the online sale of narcotics (e.g., marijuana, prescription drugs, benzodiazepines). 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 then using other services including PayPal). (USA v. Willems et al. 2011) When used with tools to anonymize network traffic such as Tor (Dingledine et al. 2004) Bitcoin allowed the creation of marketplaces with stronger assurances of anonymity. Transaction volume grew sharply: Christin (2013) estimates through measurements that the turnover on the Silk Road anonymous online marketplace, the first to exclusively support Bitcoin transactions, reached $15 million per annum just a year after it began operation. Silk Road's own category classifications confirm the prevalence of narcotics items, which dominate Silk Road's top categories as shown in Table 1. Examining 30 months of Silk Road data from February 2011 to July 2013, a FBI complaint reports 9.5 million bitcoins of transactions; even allowing for varying exchange rates during this period, the amount at issue was at least $100 million and plausibly twice that. After the demise of Silk Road (discussed further in Regulation, below), alternative markets opened in its stead—a "new" Silk Road, as well as more than thirty competitors—and it is unclear whether the Silk Road takedown actually reduced contraband activity using Bitcoin.

While litigation documents largely present 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, hedging protected customers against currency volatility. Criminal charges criticized Silk Road's fees, which averaged 8% for escrow service—allegedly an indicator of Silk Road's distinctive profit from misbehavior, in comparison to credit card system fees of approximately 3%. But note that eBay's fees typically somewhat exceed Silk Road's fees, calling into question whether high fees in and of themselves define a platform's purpose or responsibility.

For better or worse, Silk Road seems to have facilitated international, cross-border trade that is ordinarily viewed favorably. Indeed, 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 advantageously compete with street sellers in Australia. Numerous online discussions flagged this opportunity and the sellers who invoked it, and Table 2's tabulation of shipping origins and destinations confirms disproportionate items sold from the Netherlands.

Gambling sites also turned to Bitcoin to protect customer privacy and to receive funds from customers unable to use other payment methods. For example, Satoshi Dice offers 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% at the time (Matonis, 2013). While

Satoshi Dice is plausibly the most popular Bitcoin gambling game, but the Bitcoin Wiki (2014) reports around 100 casinos, poker sites, dice games, lotteries and betting services.

Bitcoin's lack of national boundaries makes it useful for evading international capital controls. In December 2013, the People's Bank of China (China's central bank) banned Chinese banks from relationships with Bitcoin exchanges, a decision which the Economist attributed to preventing 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-Holding

Some have envisioned Bitcoin competing with, and perhaps ultimately replacing, the credit and debit card networks that facilitate many consumer payments. In light of widespread criticism of the fees charged by those card networks (Anderson 2012), Bitcoin could offer a lower-price alternative that might pressure those card networks to lower their prices to merchants.

Some early evidence seems to confirm that Bitcoin can be used in this way. Best known among merchants accepting Bitcoin, Overstock.com began to receive payments by Bitcoin in January 2014. Overstock reported favorable response, including revenue they viewed as significant as well as 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 web sites to accept Bitcoin, using standard interfaces that match the way sites process credit cards. Early user reviews are mixed, sometimes reporting technical glitches but largely seemingly satisfied. Merchants appear to be particularly pleased with the offering, as Bitcoin payment processing is strikingly low-cost for them. For example, Coinbase currently charges 0% on incoming payments up to $1M per merchant per annum, and 1% thereafter. The elimination of credit card chargebacks and other card network fees further increased a merchant's savings when using Bitcoin.

It is less clear that consumers benefit from paying by bitcoin. Many credit cards provide consumers with rebates, widely 1% but sometimes 2% or even more, and well as similar benefits such as frequent flyer points and merchandise credits. If a consumer pays by Bitcoin rather than credit card, the consumer foregoes these benefits—paying the same gross price (the retailer's standard price for the chosen items) but losing the rebate or bonus. Edelman 2014 points out that the lack of benefits makes Bitcoin a poor value for many consumers: Even if a consumer already has Bitcoin, the consumer would be better off making a purchase with a 1.5% cashback credit card, paying a 1% fee to convert Bitcoins to dollars, then using those dollars to pay the credit card bill—a procedure that yields a 0.5% cost savings compared to paying the merchant directly. If the consumer was going to incur a 1% fee to convert dollars to Bitcoin in the first place, the benefits of Bitcoin grow even more distant.

Some merchants have responded by providing additional benefits to consumers who pay with Bitcoin. For example, Overstock provides a 1% rebate to consumers who pay by Bitcoin. Even

then, it is not clear that benefits can be set to make all parties better off. Consider a merchant that pays a 2.9% fee to accept credit card payments (a standard fee for card-not-present online purchases.) Such a merchant might be willing to pay up to a 2.9% rebate or other benefit if a consumer pays by Bitcoin. However, even at a 2.9% discount, a savvy consumer should prefer to pay by credit card: The consumer would incur a 1% charge to convert dollars to Bitcoin, plus the consumer can get a 2% credit card. So the consumer would need at least a 3% discount to prefer Bitcoin over credit card. But at a 3% discount for Bitcoin, the merchant would receive higher net revenue by sticking with credit cards. That said, if competing Bitcoin exchanges bid the 1% conversion fee downwards, there could be room to make both consumers and merchants better off than through payments by credit card.

Notwithstanding merchants' apparent excitement for Bitcoin, some question whether Bitcoin payments growth is actually as rapid as should be expected for a successful payments service. Noting that success implies rapid "hockey-stick" growth, 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.

The Bitcoin block chain poses a further barrier to using Bitcoin for general-purpose payments. First, space in the block chain carries a high social cost: Every transaction, large or small, must be copied into all future block chains. Although this social cost is not yet passed to consumers through a transaction cost, a huge volume of transactions--as from millions of users' small day-to-day payments--would pose a burden that would need to be addressed. Second, Bitcoin transactions are slow; many authorities recommend considering a transaction final only after six confirmations to assure that the transaction is truly recorded in a permanent version of the block chain. This delay, approximately one hour, is unsuitable for most in-person retail payments.

Meanwhile, other users appear to be buying bitcoins not to use them but to hold them in appreciation. Meiklejohn (2013) finds that of the bitcoins mined in 2009-2010, more than 60% remain unspent or took more than one year to be spent.

Possible & Future: General-Purpose Payments and Mainstream Store of Value

Some proponents envision Bitcoin evolving into a general-purpose payment mechanism widely used for payments large and small, near and distant, routine and occasional. In principle Bitcoin can help consumers and merchants avoid fees charged by longstanding payment methods. (For example, US debit cards largely charge merchants $0.21 per transaction as a result of 2012 regulatory changes. Merchants' credit card expenses often total 3% or more. Consumers making international remittances sometimes pay $50 or even more.) Bitcoin's costs are likely to be lowest if a payor already held bitcoins, and if a payee was content to retain bitcoin rather than immediately convert to a traditional currency. In that circumstance, fees are relatively low: The only costs are transaction fees paid to the successful miner who solved that block's puzzle (on top of the minting reward). These fees are optional, but 96% of the transactions in January-June 2014 include a fee, most often the default rate of the standard client software, 0.0001

bitcoin. In January to July 2014, these transaction fees were below 0.02% of total transaction value.

Despite the promise of pure Bitcoin payments, to date most payments entail at least one party needing to convert to or from Bitcoin, yielding adding costs. For one, many consumers do not have bitcoin in the first place, so must use an exchange (and pay exchange fees) to get bitcoin. Furthermore, when merchants accept payment by Bitcoin, they need traditional currency to pay their suppliers. For example, Overstock reports keeping 10% of its Bitcoin gross receipts in that currency (Sidel 2014), but given Overstock's net margin of 1.2% (per its 2014 Q1 SEC 10-Q filing), this effectively requires transferring profits from the company's other operations.

Meanwhile, there is little sign of Bitcoin used for international remittance. Many Bitcoin enthusiasts point to high fees from services such as Western Union. But Western Union offers a suite of services including accepting and dispensing cash, distinctively serving payees in low-income countries where transfer from Bitcoin to local currency is likely to be particularly difficult and where merchants are exceptionally unlikely to accept payment by Bitcoin. Bitcoin is not a realistic substitute for these payees. A closer competitor is Paypal which, like Bitcoin exchanges, effectively requires that both payor and payee have computer access and bank accounts to transfer funds in and out of Bitcoin. Paypal performs within-country transactions at no fee to consumers who fund the transactions with bank account transfers, leaving no room for Bitcoin to offer a lower price. For international transfers, Paypal charges 0.5% to 2% plus currency conversion at Paypal's rates (often 2% above prevailing rates), leaving some room for a low-fee entrant but much less than comparisons to Western Union.

In principle Bitcoin could play the role of a reserve currency in clearing transaction between future payment schemes, including decentralized systems (such as refinements of Bitcoin) as well as centralized systems (including the myriad proprietary virtual currencies from private firms). Consensus around Bitcoin would seem to facilitate pegging other schemes to a common unit of account, and capital held in Bitcoin can build trust in a new scheme by securing customer deposits.

Risks in Bitcoin

Bitcoin's design presents distinctive risks rather different from other payment methods and stores of value.

For any user holding bitcoins (rather than immediately converting to another currency), a key concern is *market risk* via fluctuation in the exchange rate between bitcoin and other currencies. Exchange rates have fluctuated sharply over time. Figure 1 plots the average USD-bitcoin exchange rate at the largest exchanges. The exchange rate has been significantly correlated with public interest. The additional plots within Figure 1 show the relative popularity of the search term "bitcoin" among US Google users (0.806 correlation with USD-bitcoin exchange rate) and weekly total transaction volume at the four largest exchanges (correlation 0.891).

With its valuation seemingly linked to the vagaries of public attention, Bitcoin's exchange rate is correspondingly volatile. Table 3 reports the coefficient of variance for the daily USD-bitcoin exchange rate between January 2, 2011 and July 5, 2014, along with the same calculation for

other exchange rates and stock market indices. By this measure, USD-bitcoin volatility is more than 41 times as variable as the exchange rate from USD to EUR.

Second, Bitcoin suffers problems typical of markets with limited depth. For example, a person seeking to trade large amount of bitcoin typically cannot do so quickly without moving the market price.

Legal and regulatory risks remain weighty. Payments are highly regulated in most countries, exposing Bitcoin systems to numerous legal requirements. Powerful incumbents have every incentive to object to a competitor escaping oversight and compliance obligations. Even law-abiding users face significant risk from regulation. For example, if a 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 users were in fact engaged in such activity. Furthermore, uncertain tax treatment of Bitcoin gains and losses hinders tax planning. We discuss these questions in the next section, Regulating virtual currencies.

Given de facto 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. 45% of the Bitcoin currency exchanges studied by Moore and Christin (2013) ultimately ceased operation. Sometimes the closure was precipitated by a large security breach, while in a few cases the operators simply absconded without explanation. Low-volume exchanges were more likely to close whereas high-volume exchanges were more likely to experience a security breach. 46% of the exchanges that closed did not reimburse their customers after shutting down. When Mt. Gox, formerly the largest currency exchange, collapsed in early 2014, it reported in its bankruptcy filing losing 744,000 of its customer' bitcoins (worth approximately US$300 million at the time of closure) (Abrams 2014).

Seeing these vulnerabilities, some users elect to place Bitcoin in digital wallets. While simplifying the process of holding Bitcoins for less technical users and escaping the risk of holding funds in exchanges, these intermediaries introduce other risks. By remotely storing the private keys which "unlock" customers' bitcoins, wallet servers become a lucrative target for cybercriminals. Indeed, attackers have routinely exploited weaknesses. Examples include 4,100 bitcoins ($1.2M USD) taken rom inputs.io, which subsequently defaulted (McMillan 2013), and 1,295 bitcoins ($1M) taken from BIPS following distributed denial-of-service (DDoS) attacks (Southurst 2013). Finally, an wallet operator may itself abscond with deposited funds, as some have alleged for the operators of inputs.io. To date there has been no authoritative investigation, leaving those allegations unsubstantiated.

The threat of DDoS attacks looms particularly large for Bitcoin. Such attacks have diverse motivations. First, attacks can target mining pools, preventing a pool's participants from solving the current puzzle and giving an advantage to all other miners. (Johnson et al. 2014) Second, they 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 2 plots the number of DDoS 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 DDoS attacks occur throughout the web, attacks seem to be particularly effective in the Bitcoin ecosystem due to the relative ease of monetizing the attacks.

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, if Alice sends Bob 50 bitcoins, but intended to send only 5, she can ask him to return the excess in a second transaction. But Alice is at Bob's mercy; the Bitcoin protocol has no mechanism to forcefully retake the funds. The irreversibility of transactions is the result of an explicit design choice within the Bitcoin protocol, and it is sometimes touted to merchants as an advantage over payment cards (which allow customers to "chargeback" a transaction, with high fees to merchants--fees merchants widely perceive as unjust, particularly if users are opportunistic). In a world of competing payment methods, irreversibility puts Bitcoin at a disadvantage: All else equal, consumers should favor a system that allows reversal of unwanted or mistaken charges.

Despite irreversibility, 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, if a transaction is not added to the block chain, then others will not recognize the transfer. There is also a low but persistent risk that what was once viewed as the authoritative fork in the chain will later be cast aside for a different fork, as voted on by a majority of participants. Second, malevolent participants could double-spend bitcoins. 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 et. al 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 highly controversial within the Bitcoin community (Bradbury 2013). For one, 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. Furthermore, 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 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. Idiosyncratic operational risks affect individual users, such as the loss, theft or accidental disclosure of a private key. Anyone who knows a private key can immediately transfer the corresponding bitcoins to their own control. Despite a user's efforts to keep a 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 systemic operational risks through potential vulnerabilities in the protocol design or breakthroughs in cryptanalysis. Community attention has focused on the so-called "51% attack". As explained in Technologies above, transactions are added to the block chain when a miner solves a computational puzzle. Miners with more computational power can try more solutions. If a single miner or group of miners can reliably control more than half the computational power, they can seize control of the system including preventing legitimate transactions from being added to the block chain, double-spending coins held by the attacker, and collecting newly minted Bitcoins without having to actually incorporate everyone's transactions onto the chain (Barber et al. 2012). If such attacks arose, the Bitcoin community might devise defenses such as rejecting untrusted versions of the block chain, but the transition would be chaotic and would probably undermine trust in Bitcoin.

Finally, Bitcoin raises certain *privacy risks*, most notably the risk that transactions can be linked back to the people who made them. For traditional currencies, there is little privacy risk because there is little expectation of privacy built into the system. (For example, credit cards certainly receive, process, and even sell information about customers' spending.) While banks take steps to protect the confidentiality of account details and transactions, "know-your-customer" regulations compel financial institutions to maintain records about account-holders. There is no such requirement in the Bitcoin protocol, which contributes to the misunderstanding that Bitcoin transactions are anonymous. In fact, they are *pseudonymous*, in that transactions specify account information (user's public key) albeit without personal names, and the block chain publishes all transactions by that user ID. Moreover, transactions with exchanges often reveal customer names to the counterparties (e.g. as funds are moved to traditional banks), as do purchases from retailers (revealing customer name and mailing address). In principle a Bitcoin user's identity could be obtained from one such source, then associated with the user's other transactions--flouting the widespread expectation of privacy.

Regulating Virtual Currencies

Contrary to the initial view that Bitcoin's decentralization made it unregulable, there now appears to be ample possibility of regulatory oversight, as well as circumstances in which such intervention could be useful.

Monetary Policy

If Bitcoin were to serve as a currency, it would be natural for regulators to set monetary policy. The design of Bitcoin seems to leave little role for monetary policy, as the growth rate of the money supply time is specified in the protocol. Changing these rules would require agreement from miners representing a majority of mining power, and they have little incentive to give up their power under the current rules. In this sense, the Bitcoin economy implements a variant of Milton Friedman's "k-percent rule" (Friedman 1960, p. 90), a proposal to fix the annual growth rate of the money supply to k irrespective of economic development, apropos of longstanding debate on rules versus discretion in monetary policy.

Bitcoin's fixed money supply creates the possibility of deflation if Bitcoin were to be used widely. Considering the classic quantity theory of money, the price level P is proportional to the ratio of money supply, M, and the output of the Bitcoin economy in real terms, Y:

$$P = \frac{M \cdot V}{Y}$$

where V is the velocity of money which is often assumed constant in the short run. If innovations yield increasing productivity, Y grows at a positive rate. Whenever the money supply grows at a rate k greater than the real growth rate, P increases and the economy is subject to inflation. Conversely, if k is lower than real output growth, then P decreases. This situation would be likely in a Bitcoin-based economy, as 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 as bitcoins can be irreversibly destroyed when users forget their private keys. Meanwhile, during adoption booms, the Bitcoin economy grows faster than k, leading to a soaring exchange rate and typical signs of deflation such as money hoarding. In deflationary circumstances, Bitcoin has no obvious mechanism to manoeuvre the system back to positive inflation, nor any central arbiter focused on this task. For these reasons, many trades in bitcoin are accompanied by one or even two conversions from and/or to conventional currencies. Furthermore, prices quotes in bitcoin are almost always computed in real time by reference to a fixed amount of conventional currency. Bitcoin thus today resembles more a payment platform than what economists consider a currency.

Paul Krugman was the first to note the deflation risk in the Bitcoin economy, comparing it to the gold standard (2011). In response, developers proposed alternative system rules. For example, Primecoin and Peercoin modify Bitcoin to provide an unlimited money supply, with k fixed to approximately 1% for Peercoin.

It remains unclear whether decentralized cryptographic currencies can be designed with monetary policies that include feedback or even discretion. Bitcoin's design of periodic minting for a time, followed by cessation, embodies a basic version of monetary policy without considering the state of the real economy. Human arbiters could add information about economic conditions or could introduce discretion by judgment, but they would introduce the governance questions Bitcoin set out to overcome. We note that Bitcoin's block chain presents a crude measure of monetary indicators, 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 little to facilitate any policy based on real economic activity.

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. These crimes are mainly operational risks discussed previously, such as bitcoin theft, attacks on mining pools, and denial-of-service attacks on exchanges to manipulate exchange rates. Many of these attacks update longstanding attacks on classic currencies, including counterfeiting and bank robbery, albeit through importantly different channels (e.g. computer security rather than lithography). By raising doubts about the future value of Bitcoin and the feasibility of using or converting Bitcoin when desired, these attacks reduce the value of Bitcoin and thus harm everyone who holds Bitcoin as of the time of an attack. 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, and limited resources.

Second, Bitcoin can be used for *money laundering*. Despite broad similarities with schemes using classic currency, 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. Examples include illegal goods and services sold on Silk Road and payment of funds in extortion. It seems criminals are 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 greater consumer protection. Such discussion were particularly frequent after the February 2014 failure of Bitcoin exchange Mt. Gox, which inexplicably lost 744,000 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 (e.g. credit card dispute rights 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

The original vision of Bitcoin is broadly in tension with regulation and government control. Early Bitcoin users often described themselves as libertarians, distrusting governments generally and monetary policy specifically. (Raskin 2013) 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.

A key challenge for prospective regulators is where to impose constraints. The Bitcoin protocol is decentralized by design, and it is infeasible to regulate all peers due to their quantity and their geographic distribution. Instead, regulators are more naturally drawn to key intermediaries. But intermediaries raise predictable defenses, including denying liability for conduct originated by third-party users, customers, or suppliers. Furthermore, some users will anticipate regulators targeting intermediaries and will seek 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. At the start, some perceived Silk Road to be invulnerable. The site was hosted as a Tor hidden service, which is purpose-built for anonymity of both visitors and operators. Payments were only accepted in bitcoin, which meant that traditional financial intermediaries could not be pushed to reveal customer identities. Yet the Silk Road site itself was vulnerable: the domain 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 (US vs. Ross Ulbricht). The private keys associated with Ulbrict's 144,000 bitcoins were seized by the FBI (Greenberg 2013). Investigators targeted large merchants and administrators on Silk Road, exploiting poor operational security tactics to connect to 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). Far from invulnerable to regulatory oversight, 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 2013 the US Financial Crimes Enforcement Network (FinCEN) issued guidance on when virtual currency operators should be classified as money-services businesses, requiring registration with FinCEN as well as reporting and recordkeeping obligations. As exchanges complied, account details became available to regulators, and a US judge soon signed a seizure warrant for an account at Mt. Gox. In China, a December 2013 policy was broadly similar, requiring that Bitcoin intermediaries implement know-your-customer registrations for account-holders. (Bank of China, 2013) These regulatory requirements will not impede peer-to-peer transactions that are not facilitated by currency exchanges. But it seems longstanding reporting requirements can provided a level of compliance for virtual currencies similar to what has been achieved for traditional currencies.

In principle, Bitcoin's electronic implementation can make it considerably more regulable 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 in Risks (above).

Tax treatment of Bitcoin remains unsettled. In March 2014, the IRS 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 well-grounded in longstanding principles of US tax law, this guidance 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, we note the limits of regulators' authority. 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 with even stronger security precautions such as Zerocash--likely letting criminals continue to use the service, yet perhaps adding too much complexity for mainstream consumers. Tempting as it is to clean up Bitcoin to the utmost, these factors provide some grounds for hesitance.

Looking Ahead

Bitcoin and other virtual currencies ultimately struggle with competing visions of their future. Do they seek to replace credit cards for everyday consumer payments? To displace Western Union for international payments of cash? To supplant banks for short-term deposits? Do they 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 they 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. Yet recruiting mainstream consumers and merchants seems to call for a focus on simplicity and lower prices.

In some respects, Bitcoin may be able to accommodate a community of experimentation built on top of its Bitcoin foundations. Mixers already close the most obvious privacy shortcomings in Bitcoin's early design. Pools help reduce risk for miners, and wallets address some of consumers' usability and security concerns. Yet other changes raise more fundamental challenges. Consider an effort to add third-party dispute resolution services to investigate any buyer complaints and, if they see fit, issuing refunds (broadly similar to the current credit card chargeback system). To some extent such services would add consumer protections to refine Bitcoin's current finality. Yet a dispute resolution service would most naturally be paid by the seller, raising an obvious conflict of interest by inviting a seller to choose services predisposed to rule in its favor.

Meanwhile, other aspects of Bitcoin architecture are largely locked in place through the initial protocol design. For example, the block chain is the essence of Bitcoin, despite its potentially-undesirable distribution of records of users purchase. 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 retaining the 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 lie 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, not yet operational) improves privacy

protections by avoiding a block chain listing transaction history. Peercoin allows perpetual 1% annual increase in the money supply.

To offer their competing design decisions, they would first need to achieve confidence in their value and adoption. Bitcoin took off thanks to early excitement for its service, buyers and sellers at Silk Road who had little alternative to Bitcoin, and favorable press coverage. A replacement would struggle to obtain this combination of benefits, but without favorable expectations for growth, few would be willing to convert traditional currency into a competing coin.

On balance we are neutral as to Bitcoin's prospects. Whether or not Bitcoin expands as its proponents envision, it offers a remarkable lab for researchers and, to merchants and some consumers, a convenient means of exchange.

References

Abrams, Rachel, Goldstein, Matthew and Tabuchi, Hiroko. “Erosion of Faith Was Death Knell for Mt. Gox”. New York Times, February 28, 2014. http://dealbook.nytimes.com/2014/02/28/mt-gox-files-for-bankruptcy/

Anderson, Ross. 2012. “Risk and Privacy Implications of Consumer Payment Innovation.” Mimeo.

Andreessen, Marc. Why Bitcoin Matters. New York Times - DealB%k. January 21, 2014. http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/

Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. March 18, 2013. http://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html

Barlow, John Perry. 1996. “A Declaration of the Independence of Cyberspace.” https://projects.eff.org/~barlow/Declaration-Final.html (14 July 2014)

Ben-Sasson, Eli, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, Madars Virza. 2014. “Zerocash: Decentralized anonymous payments from Bitcoin.” *Proceedings of the 2014 IEEE Symposium on Security and Privacy (SP).* San Jose, CA. May 2014.

Bitcoin Wiki. “Category:Gambling”. Last accessed July 14, 2014. https://en.bitcoin.it/wiki/Category:Gambling

Bitcoinity.org. “Exchanges”. Last accessed July 14, 2014. https://bitcoinity.org/markets/list

Blockchain.info. “Bitcoin Charts”. Last accessed July 15, 2014. https://blockchain.info/charts/

Böhme, Rainer. 2013. “Internet Protocol Adoption: Learning from Bitcoin.” *Proceedings of the IAB Workshop on Internet Technology Adoption and Transition (ITAT)*, Cambridge, UK. http://www.iab.org/wp-content/IAB-uploads/2013/06/itat-2013_submission_17.pdf (July 7, 2014)

Bonneau, Joseph. 2014. “Estimating the Power Consumption of Bitcoin.” Financial Cryptography rump session. Bridgetown, Barbados, March 4.

Bradbury, Danny. “Anti-Theft Bitcoin Tracking Proposals Divide Bitcoin Community”. Coindesk, November 15, 2013. http://www.coindesk.com/bitcoin-tracking-proposal-divides-bitcoin-community/

The People’s Bank of China and Five Associated Ministries Notice, 2013. “Prevention of Risks Associated with Bitcoin.” Translation available at https://vip.btcchina.com/page/bocnotice2013

Buterin, Vitalik. “Bitcoin Network Shaken by Blockchain Fork.” Bitcoin Magazine. March 12, 2013. http://bitcoinmagazine.com/3668/bitcoin-network-shaken-by-blockchain-fork/

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)*, pages 213-224. Rio de Janeiro, Brazil. May 2013.

Christin, Nicolas, Alessandro Acquisti, Adrian Perrig, and Bryan Parno. Monetary Forgery in the Digital Age: Will Physical-Digital Cash Be a Solution? In *I/S: A Journal of Law and Policy for the Information Society*, Volume 7, Number 2, pages 171-206. Winter 2012.

Diffie, Whitfield and Martin E. Hellman. 1976. "New Directions in Cryptography." *IEEE Transactions on Information Theory*, 22 (11): 644-654.

D.K. "China Blues." The Economist. December 18, 2013.

Douceur, John R. 2002. "The Sybil Attack." *Lecture Notes in Computer Science*, vol. 2429, pp. 251-260.

Enforcement Actions for Failure to Register as a Money Services Business. http://www.fincen.gov/news_room/ea/ea.msb.html

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

Edelman, Benjamin. "Consumers Pay More When They Pay with Bitcoin." PYMNTS.COM. 2014. http://www.pymnts.com/in-depth/2014/consumers-pay-more-when-they-pay-with-bitcoin/ .

Friedman, Milton. 1960. "A Program for Monetary Stability." New York.

Greenberg, A. "FBI Says It's Seized $28.5 Million In Bitcoins From Ross Ulbricht, Alleged Owner Of Silk Road", Forbes, October 25, 2013. http://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/

Hicks, John R. 1967. "Critical Essays in Monetary Theory." Oxford.

IRS Notice 2014-21. www.irs.gov/pub/irs-drop/n-14-21.pdf

Johnson, Benjamin, Aron Laszka, Jens Grossklags, Marie Vasek, and Tyler Moore. 2014. Game-theoretic analysis of DDoS attacks against Bitcoin mining pools. In *1st Workshop on Bitcoin Research*, volume 8438 of *Lecture Notes in Computer Science*. Springer, March 2014.

Karame, Ghassan, Elli Androulaki, and Srdjan Capkun. 2012. "Double-spending Fast Payments in Bitcoin." In *Proceedings of the 2012 ACM Conference on Computer and Communications Security* (CCS '12). ACM, New York, NY, USA, 906-917.

Krugman, Paul. 2011. "Golden Cybervetters." New York Times Blogs. September 7, 2011. http://krugman.blogs.nytimes.com/2011/09/07/golden-cyberfetters/ .

Matonis, Jon. 2013. "Bitcoin Casinos Release 2012 Earnings." Forbes. January 22, 2013. http://www.forbes.com/sites/jonmatonis/2013/01/22/bitcoin-casinos-release-2012-earnings/

McMillan, Robert. "$1.2M Hack Shows Why You Should Never Store Bitcoins on the Internet." Wired. November 7, 2013. http://www.wired.com/2013/11/inputs/

Moore, Tyler and Nicolas Christin. Beware the middleman: Empirical analysis of Bitcoin-exchange risk. In *Financial Cryptography and Data Security*, volume 7859 of *Lecture Notes in Computer Science*, pages 25-33. Springer, April 2013.

Murdoch, Steven J. 2006. Software Detection of Banknote Images, http://www.cl.cam.ac.uk/research/security/posters/sjm217-currency.pdf (July 7, 2014).

Meiklejohn, Sarah, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage. “A Fistful of Bitcoins: Characterizing Payments Among Men with No Names”. *ACM Internet Measurement Conference (IMC)*, 2013. http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf .

McLeod. “Bitcoins Soar In Value In Argentina Due To Capital Control Laws.” Forex Magnates. July 9, 2013. http://forexmagnates.com/bitcoins-soar-in-value-in-argentina-due-to-capital-control-laws-bitcoin-meetup-held-in-nations-capital/ .

Möser, Malte, Rainer Böhme, Dominic Breuker. 2013. “An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem.” *Proceedings of APWG eCrime Researchers Summit*, San Francisco, pp. 1-16. DOI 10.1109/eCRS.2013.6805780

Raskin, Max. Meet the Bitcoin Millionaires. BloombergBusinessweek. April 10, 2013.

Ron, Dorit and Adi Shamir. “Quantitative Analysis of the Full Bitcoin Transaction Graph.” In *Financial Cryptography and Data Security*, volume 7859 of *Lecture Notes in Computer Science*, pages 6-24. Springer, April 2013.

Ron, Dorit and Adi Shamir. “How Did Dread Pirate Roberts Acquire and Protect His Bitcoin Wealth?” In *1st Workshop on Bitcoin Research*, volume 8438 of *Lecture Notes in Computer Science*. Springer, March 2014.

Sidel, Robin. “Overstock CEO Sees Bitcoin Sales Rising More Than Expected.” Wall Street Journal. March 4, 2014. http://online.wsj.com/news/articles/SB10001424052702304815004579418962232488216

Song, Sophie. 2014. “The Rise And Fall Of Bitcoin In China: Central Bank Shuts Down All Chinese Bitcoin Exchanges.” International Business Times. http://www.ibtimes.com/rise-fall-bitcoin-china-central-bank-shuts-down-all-chinese-bitcoin-exchanges-1563826 .

Southurst, Jon. “Bitcoin Payment Processor BIPS Attacked, Over $1m Stolen.” CoinDesk. November 25, 2013. http://www.coindesk.com/bitcoin-payment-processor-bips-attacked-1m-stolen/ .

Taylor, Michael Bedford. “Bitcoin and The Age of Bespoke Silicon.**”** International Conference on Compilers, Architecture and Synthesis for Embedded Systems (CASES), 2013. http://cseweb.ucsd.edu/~mbtaylor/papers/bitcoin_taylor_cases_2013.pdf .

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

United States of America v. Ross William Ulbricht. http://www.wired.com/images_blogs/threatlevel/2014/02/US-v.-Ross-Ulbricht-Indictment.pdf

Marie Vasek, Micah Thornton, and Tyler Moore. “Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem”. In *1st Workshop on Bitcoin Research*, volume 8438 of *Lecture Notes in Computer Science*. Springer, March 2014.

Zetter, Kim. “How the Feds Took Down the Silk Road Drug Wonderland.” Wired. November 18, 2013. http://www.wired.com/2013/11/silk-road/ .

Sidebar: Bitcoin as a Platform and Distributed Transaction Log

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, best known as coauthor of Mosaic (the first widely-used web browser), presented the rationale in a column for New York Times:

> 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.

We credit the value of these benefits, but we are less sure that Bitcoin truly delivers. For example, hacks undermine Andreessen's suggestion that "nobody can challenge the legitimacy" of a Bitcoin payment. And block chain delays mean accepting Bitcoin payment isn't "safe" for any payee who needs immediate confirmation of payment.

In any event, to date the Bitcoin platform has not developed into the general-purpose platform Andreessen and others envisioned. To our knowledge, 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 2011), a timed version of which can be repurposed to ensure fairness in multi-party computation (Andrychowicz et al. 2014) in order to run auctions without an auctioneer; and FutureCoin (Clark et al. 2014), which enables decentralized prediction markets. In principle these entrants bear out Andreessen's excitement, but to date none has attracted large-scale use. Meanwhile each faces significant competition from established firms and processes using more traditional system design.

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*, IEEE Press, May 2014.

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

Clark, Jeremy and Aleksander Essex. 2012. “CommitCoin: Carbon Dating Commitments with Bitcoin - (Short Paper).” In Financial Cryptography and Data Security, volume 3797 of Lecture Notes in Computer Science, pages 390-398. Springer.

Rosenfeld, Meni. 2012. “Overview of Colored Coins.” https://bitcoil.co.il/BitcoinX.pdf (14 July 2014)

Sidebar: Bitcoin as a Lab

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 consider diverse questions ranging from design of financial markets to user behavior along with myriad questions of law and regulation. In this sidebar we highlight a few working papers that importantly rely on Bitcoin as a data source for empirical work or for applying theory. Research questions include:

- **Users' motivations for holding bitcoin.** Glaser et al. (2014) compare exchange-traded volume to transaction volume within the Bitcoin network and conclude that most users (by volume) treat their Bitcoin investment as speculative asset rather than as means to use Bitcoin for payments. Brière et al. (2013) study correlations between bitcoin and other asset classes, finding that bitcoin investments offer diversification benefits.
- **Arbitrage on Bitcoin exchanges.** Gandal and Halabruda (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.
- **Anonymity of Bitcoin users.** Several papers use graph theory to analyze the public Bitcoin transaction history using (Reid and Harrigan 2012, Ober et al. 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 et al. (2013) quantify the anonymity in a simulated campus environment, finding that almost half of the users can be identified by their transaction patterns.
- **Incentive-compatibility of the Bitcoin protocol.** 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 et al. 2012) and for the block mining protocol (Eyal and Sirer 2014), the prescribed rules are not equilibrium strategies if one considers the option to selectively and temporarily withhold information from other parties. Furthermore, Houy (2014b) observes that larger blocks are less likely to win a block race than smaller ones, meaning that a miner reduces his chance of collecting a reward when he includes new transactions into blocks--raising the question of why miners include transactions into blocks at all. That said, these concerns are theoretical. We are not aware of empirical evidence demonstrating substantial deviations from the sub-optimal rules.
- **Designing mining pool mechanisms.** Early mining pools observed selfish behavior in the form of "pool hopping": Miners opt out in long rounds where 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).

- **Transaction fees.** Houy (2014a) models equilibria for the level of transaction fees after the end of the minting era, when the mining reward drops below the cost of mining. (Recall that these fees are voluntary, akin to tips.) If space in the block chain is abundant and no minimum fees are imposed, a low-fee equilibrium could cause disinvestment in mining and erode the defense against 51% attacks. It is too early to test this result against data.

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.

Androulaki, Elli, Ghassan Karame, Marc Roeschlin, Tobias Scherer, Srdjan Capkun. 2013. "Evaluating User Privacy in Bitcoin." In *Financial Cryptography and Data Security*, volume 7859 of *Lecture Notes in Computer Science*, pages 34-51. Springer, April 2013.

Babaioff, Moshe, Shahar Dobzinski, Sigal Oren, and Aviv Zohar. 2011. "On Bitcoin and Red Balloons." In *Proceedings of ACM Conference on Electronic Commerce*, pages 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*, volume 3797 of *Lecture Notes in Computer Science*, pages 399-414. Springer.

Brière, Marie, Kim Oosterlinck, and Ariane Szafarz. 2013. "Virtual Currency, Tangible Return: Portfolio Diversification with Bitcoins." Working Paper. September 2013.

Eyal, Ittay and Emin Gün Sirer. 2014. "Majority is not Enough: Bitcoin Mining is Vulnerable." In *Financial Cryptography and Data Security*, volume 8437 of *Lecture Notes in Computer Science*, Springer.

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

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

Houy, Nicolas. 2014a. "The Economics of Bitcoin Transaction Fees." Working Paper, Université de Lyon, February 2014.

Houy, Nicolas. 2014b. "The Bitcoin Mining Game." Working Paper, Université de Lyon, March 2014.

Ober, Micha, Stefan Katzenbeisser, and Kay Hamacher. 2013. "Structure and Anonymity of the Bitcoin Transaction Graph." *Future Internet*, Volume 5, Number 2, pages 237-250.

Reid, Fregal and Martin Harrigan. 2011. "An Analysis of Anonymity in the Bitcoin System." http://arxiv.org/pdf/1107.4524v2 (14 July 2014)

Rosenfeld, Meni. 2011. “Analysis of Bitcoin Pooled Mining Reward Systems.” https://bitcoil.co.il/pool_analysis.pdf (14 July 2014)

Ron, Dorit and Adi Shamir. “Quantitative Analysis of the Full Bitcoin Transaction Graph.” In *Financial Cryptography and Data Security*, volume 7859 of *Lecture Notes in Computer Science*, pages 6-24. Springer, April 2013.

Tables and Figures

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%

Table 1: The ten most popular product categories on the Silk Road website in January-July 2012 (Christin, 2013)

Origin		Acceptable destinations	
Country	Percentage	Country/Region	Percentage
USA	43.83%	Worldwide	49.67%
Undeclared	16.29%	USA	35.15%
UK	10.15%	European Union	6.19%
Netherlands	6.52%	Canada	6.05%
Canada	5.89%	UK	3.66%
Germany	4.51%	Australia	2.87%
Australia	3.19%	World except USA	1.39%
India	1.23%	Germany	1.03%

Table 2: Shipping origins and acceptable destinations as stated by Silk Road sellers in 2012 (Christin, 2013)

Exchange	Coefficient of Variance (Jan 2011-July 2014)
USD-bitcoin Exchange Rate	1.704
USD-EUR Exchange Rate	0.040
USD-GBP Exchange Rate	0.029
USD-BRL Exchange Rate	0.127
USD-CNY Exchange Rate	0.023
USD-INR Exchange Rate	0.111
US Stock Market (S&P 500)	0.150
Argentina Stock Market (MERV)	0.393

Table 3: Coefficient of variance for USD-bitcoin exchange rate, compared to exchange rates for selected currencies and stock markets.

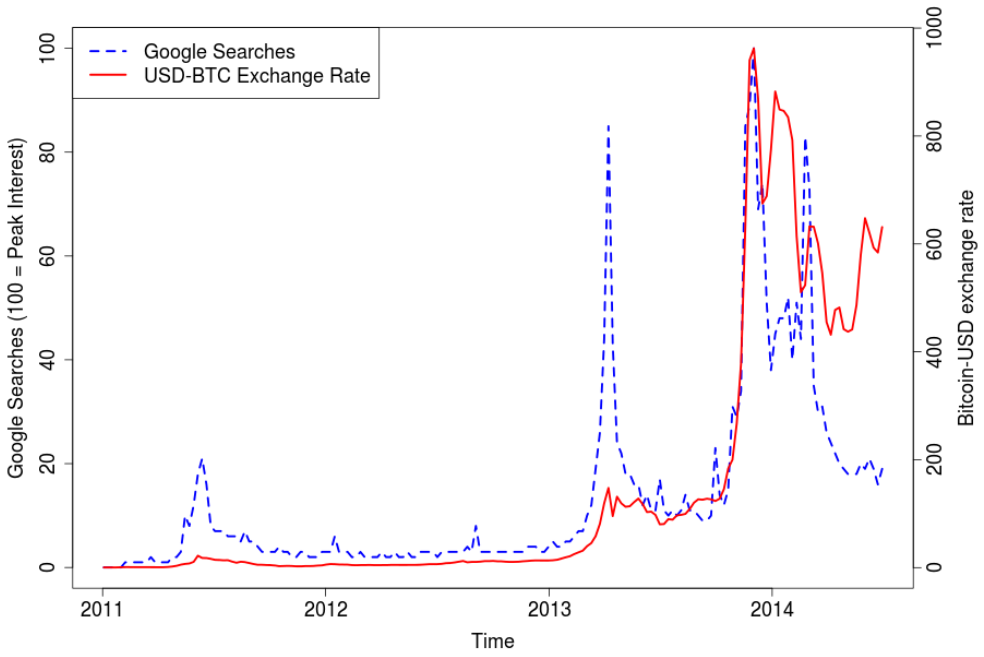

FIgure 1a: USD-bitcoin exchange rate January 2011-July 2014, overlaid with US Google web search popularity during the same period.

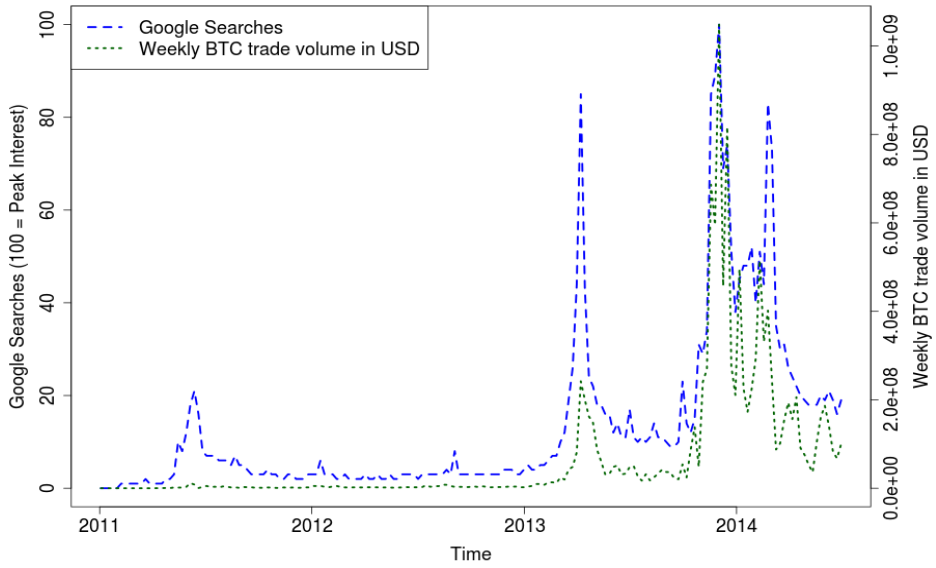

FIgure 1b: Weekly bitcoin trade volume (in USD equivalent) at four top currency exchanges for Jan. 2011-July 2014, overlaid with US Google web search popularity during the same period. (Data gathered from bitcoincharts.com as to exchanges Mt. Gox, Bitstamp, BitFinex and BTC-E.)

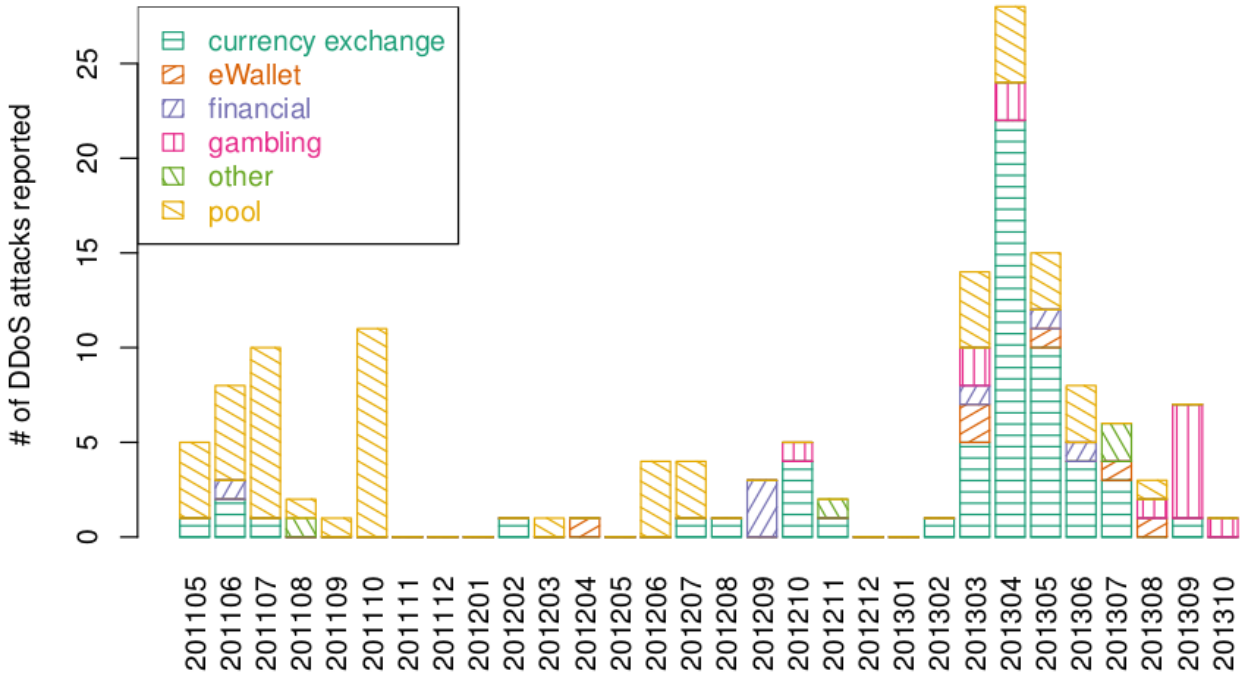

Figure 2: Reported DDoS attacks on Bitcoin services over time (courtesy Vasek et al. 2014)