Current Policy Perspectives

FEDERAL RESERVE BANK OF BOSTON™

No. 14-4

Bitcoin as Money?

Stephanie Lo and J. Christina Wang

Abstract:

The spectacular rise late last year in the price of bitcoin, the dominant virtual currency, has attracted much public attention as well as scholarly interest. This policy brief discusses how some features of bitcoin, as designed and executed to date, have hampered its ability to perform the functions required of a fiat money—as a medium of exchange, unit of account, and store of value. Furthermore, we document how various forms of intermediaries have emerged and evolved within the Bitcoin network, particularly noting the convergence toward concentrated processing, both on and off the blockchain. We argue that much of this process would have been predicted by established theories of financial intermediation, and we consider the theories' implication for the future evolution of intermediaries serving users of bitcoin or alternative virtual currencies. We then compare Bitcoin with other innovations to facilitate payment services, from competing alternative digital currencies to electronic payment protocols. We conclude with a broad consideration of the major factors that will likely shape the future development of Bitcoin versus other alternative payment systems. We predict that Bitcoin's lasting legacy will be the innovations it has spurred to payment technology, although the payment system will remain dominated by large processors because of economies of scale.

Keywords: money, medium of exchange, liquidity, speculative bubble
JEL Classifications: E41, E42, E51, G12, G21.

Stephanie Lo is a Ph.D. student at the economics department of Harvard University. J. Christina Wang is a senior economist and policy advisor in the research department of the Federal Reserve Bank of Boston. Their e-mail addresses are shlo@post.harvard.edu and christina.wang@bos.frb.org, respectively.

We would like to thank Oz Shy and Joe Peek for helpful discussions and comments. We also thank Alison Pearson and especially Daniel Tartakovsky for excellent research assistance.

This version: September 4, 2014

Motivation

Bitcoin is a peer-to-peer network that enables the proof and transfer of ownership without the need for a designated third party. The unit of the network is referred to as bitcoin, which is generally regarded as the best-known virtual (or electronic, digital) currency to date.[1] Some consider Bitcoin to be a major financial innovation in recent years. What attracted unprecedented interest in Bitcoin around the turn of the year, however, was the meteoric rise of bitcoin's price. During November 2013, the price of a bitcoin skyrocketed from less than $200 to nearly $1200, as shown in Figure 1.

The ultimate goal of Bitcoin, according to its advocates, is to serve as an alternative to the existing payments system and to enable transactions across national borders and currency denominations without the interference of sovereign entities or central banks, and without the alleged exploitation by traditional financial intermediaries such as banks. From the viewpoint of supporters of virtual currencies, national governments often impose undesirable controls, such as restrictions on convertibility, while central banks may facilitate an oversupply of currency, leading to hyperinflation. At the same time, many groups bemoan the exorbitant fees, among other alleged abuses imposed by banks. In contrast, Bitcoin appears to offer the following advantages, according to its supporters: 1) it is supposed to be an entirely decentralized system—not associated with any sovereign entities, central banks, or established payment systems, which are dominated by banks—and hence it is supposed to be less prone to exploitation or corruption; 2) it features pseudonymous accounts; 3) it imposes no direct fees on transactions and promises the potential for lower transaction fees in general.

To use a bitcoin, a user submits her account number ("public key") and password ("private key") for verification on the public transaction ledger, known as the '"block chain." Individuals ("miners") use their computing power to verify that the transaction is real by solving a computationally intensive problem (finding the "hash" of a "nonce").[2] In return for verifying the transaction, the first individual to post the solution to the problem is rewarded with a given number of bitcoin, adding to the stock of

[1] Following user convention, we use "Bitcoin" with a capital "B" to refer to the entire network along with all its functionality, inclusive of the specific contingent claim that is transmitted on the network, which is typically referred to as "bitcoin" with a little "b." We use Bitcoin in cases where the distinction is not so clear cut.

[2] For an accessible explanation of the rationale behind the technical features of Bitcoin, see "How the Bitcoin protocol actually works" by Michael Nielson at http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/. While we refer to miners as "individuals," nowadays hardly anyone is able to operate independently because of the massive computing power required to successfully mine bitcoin. Miners thus form pools in order to combine their computing power, and they split mining profits accordingly. Therefore, it is more accurate to think of the miners as coalitions of individuals, or "mining pools."

bitcoin and hence constituting money creation. The pre-programmed algorithm automatically adjusts the computational difficulty ("hash rate") of verifying transactions in order to ensure that each transaction takes on average 10 minutes to verify. This same algorithm also fixes the eventual supply of bitcoin, which is 21 million units to be mined by 2140, although it does not preset the exact growth path of bitcoin. Some randomness in the amount of time actually taken to verify each transaction is inevitable.

In this brief, we examine how well the overall Bitcoin network has enabled bitcoin to fulfill the functions of a fiat money. An important issue in this context is what types of intermediaries have emerged to facilitate the functioning of the Bitcoin network, and what are the rationales underlying their emergence and growth. We note that this is not intended to be a comprehensive overview of all the issues surrounding Bitcoin, such as whether Bitcoin is truly an anonymous system, what is the optimal design to ensure secure transactions, and what are the legal ramifications of a non-state fiat money.

Bitcoin as Money

Since the express purpose of Bitcoin's invention is to serve as an alternative form of money that agents can use to transact with one another without the involvement of sovereign entities, central banks, or banks, one naturally asks: how well has bitcoin served the function of "money"?[3] Economists generally consider money to be an instrument that serves as a medium of exchange, a unit of account, and a store of value. We therefore discuss, in turn, how bitcoin has fulfilled these three functions.

Bitcoin as A Medium of Exchange

To serve as a "medium of exchange," bitcoin must be accepted as payment for a sufficiently large set of goods or services, or other assets. A user is willing to accept a fiat money as payment for other objects of value only if she is confident that enough others will be willing to accept it in turn from her. Unlike regular fiat money, however, bitcoin is not backed by any sovereign entity that can compel the acceptance of its affiliated fiat money within a certain realm. Therefore, in order to serve as a medium of exchange, bitcoin has to rely solely on the self-fulfilling expectation on the part of private agents that it will be accepted.

[3] We refer to the subject as bitcoin—the unit of the network—in the ensuring discussion, instead of as Bitcoin, because it is more natural to compare a financial claim with "money," although we note that much of the medium-of-exchange function cannot be accomplished without the overall Bitcoin network.

Since its inception and until a few months ago, the use of bitcoin was confined to online e-commerce sites, most rather small and some illicit (such as the now-defunct Silk Road, an online market for illegal goods such as drugs and weapons). In recent months, the acceptance of bitcoin has spread to more mainstream vendors. Online merchant Overstock.com, which sells anything from bedding to jewelry and had annual sales of over $1.3 billion in 2013 (compared with $74.5 billion for Amazon), started accepting bitcoin as payment on January 9, 2014; in the first 22 hours of this new regime, Overstock accepted 800 orders in bitcoin totaling approximately $126,000.[4] Overstock CEO Patrick Byrne has since announced his prediction that approximately 1 percent of the site's 2014 sales, or $13 million, will be paid for in bitcoin.[5] A few weeks after the New Year, Tiger Direct, an online electronics retailer, followed suit. Several other companies—particularly online-only gaming and services companies such as Zynga and OKCupid—including the Sacramento Kings of the National Basketball Association and space-tourism provider Virgin Galactic, have also embraced bitcoin as a means of payment. More recently, Dish Network and Expedia announced on May 30 and June 12, respectively, that they will start to accept bitcoin payments soon. Adoption by these much larger and better-known companies signals that the new technology represented by bitcoin is perceived by the mainstream to offer sufficiently positive net benefits to be worth experimentation.

The primary, if not the only, benefit is, of course, saving on payment processing costs incurred by merchants. Offsetting this benefit is the extreme volatility of bitcoin's price. All of these vendors have therefore adopted policies to minimize their exposure to the bitcoin "exchange rate" risk, which results in inconvenience for their operations. At least two important difficulties arise for merchants because of bitcoin's extreme price volatility. First, since merchants invariably prefer their merchandise to have a (much) less volatile price than bitcoin, they all post prices in dollars to minimize visible price volatility, and they update the check-out price in bitcoin frequently in order to collect the required amount of dollars.

To investigate empirically whether on net merchants offer a better or worse price for purchases paid with bitcoin than for those paid with dollars, we hand-collected product prices daily from May 19 to June 3, 2014. Specifically, we recorded the bitcoin (BTC) and U.S. dollar (USD) prices of two goods, a Kingston flash drive and an iPhone 5C case, from Overstock and TigerDirect.[6] We selected these two

[4] http://www.wired.com/business/2014/01/overstock-bitcoin-sales/

[5] http://www.businessweek.com/news/2014-01-22/bitcoin-targets-giants-visa-to-jpmorgan-with-lower-cost-payments#p3

[6] Our requests for more systematic information on the pricing algorithm have not been answered.

online merchants because they had been accepting bitcoin payments for a few months by the time of this study. We chose these two goods because it is easily ascertained that the product offerings of the two vendors are identical according to the technical specifications.

While the USD price of these goods remained constant over our sample period, the BTC price was given only at checkout, and every updated price quote remained valid for only a short time. This interval is set at 10 minutes for Overstock and 15 minutes for TigerDirect. To compare the USD and BTC price, we compute the bitcoin-price markup as follows: we first convert the BTC price to a USD price using the BTC/USD exchange rate, which we collect from the bitcoin exchange Bitstamp, then subtract each vendor's quoted USD price, and finally calculate the "markup" to be this difference as a percentage of the vendor's quoted USD price. Clearly, the exact magnitude of the markup depends on the BTC/USD exchange rate used in the calculation, since the BTC/USD exchange rate fluctuates at a high frequency. Given that the merchants allow 10 to 15 minutes over which a customer can "lock in" the bitcoin price, we experiment with two reasonable timing choices of the BTC/USD exchange rate used to compute the markup: the average exchange rate within the minute when the product prices are collected (which will be referred to as the spot rate) and the average exchange rate over the previous 15 minutes.

Figure 2 compares the histogram of the markups (in percentage terms) calculated using these two exchange rates. The markups are close to zero: as a percentage of the USD list price, the spot bitcoin exchange rate implies a discount of 0.86 percentage points, while the 15-minute lagged bitcoin exchange rate implies a discount of 0.16 percentage points. Both of these values are fairly small and translate into a higher dollar-denominated (that is, a lower bitcoin-denominated) price of only a few cents. These numbers should, of course, be interpreted with caution: our sample size is small, and bitcoin prices generally rose over our sample period, suggesting that using a lagged average exchange rate can bias our results toward finding a discount.

At the same time, simple regressions reveal a counterintuitive result: a more volatile price period in fact deepens the discount on bitcoin purchases. Specifically, we regress our two estimates of the bitcoin-price markup (corresponding to using the average exchange rate over the last 15 minutes or the spot rate) on the volatility of the BTC/USD exchange rate over the last 15 minutes and the price change over that period. The price change is included to control for possible bias in case our estimates of the markup embed measurement errors that happen to be highly correlated with the exchange rate volatility over our small sample. As shown in Table 1, for both measures of the markup, the coefficient on the lagged volatility is negative and significant at the 1 percent level. Given our rather small sample size (four

goods, 15 observations each, over the course of two weeks), we caution against placing too much weight on these coefficient estimates. There may be features of the retailers' pricing algorithm that we are unaware of and that require controls beyond just the average price change over the last 15 minutes. We interpret these estimates as suggesting that retailers do not significantly adjust upward the markup on their prices in bitcoin.

These caveats notwithstanding, our finding that these retailers do not charge a premium and may in fact offer a discount, albeit slight, on purchases made with bitcoin suggests that retailers consider that payments made with bitcoin are on net at least as profitable as payments made with standard means.[7] The most likely reason is that accepting bitcoin lowers merchants' costs by reducing payment processing costs, chief among which are the credit card interchange fees, typically on the order of 2 to 4 percent. These savings, on average, more than offset the potential risk, and hence the discount retailers would presumably demand because of bitcoin's extreme price volatility. The most plausible explanation for the low discount on exchange rate risk is that the retailers have little exposure to the bitcoin exchange rate volatility since they are adequately hedged through intermediaries such as Coinbase, which immediately convert bitcoins paid into dollars and credit the retailers' accounts. Even allowing for lower net processing costs for retailers from bitcoin payments, it is still interesting to note that these retailers have chosen to share the cost savings with bitcoin customers. One possibility is that likely bitcoin users are the type of customers these retailers want to attract, and that the lack of a bitcoin markup we observe is part of the retailers' strategy to target such potential customers with a lower price markup in general.

The second difficulty merchants face concerning purchases made with bitcoin is how to deal with returns. Because bitcoin transactions cannot be cancelled but can only be offset with a new transaction in the opposite direction, all of these merchants have chosen to offer only in-store credit should a customer want to return an item. For example, TigerDirect states that "Returns on orders paid by Bitcoin will be accepted for a refund as a TigerDirect.com Gift Card." Since the in-store credit is typically denominated in dollars, the merchants also save the hassle of having to calculate the up-to-the-minute amount of bitcoin owed to the customer at the moment of the return. These coping mechanisms on the part of merchants highlight the impediment to bitcoin's ability to perform the medium-of-exchange function posed by the

[7] This sample is probably too small to support a general conclusion about whether merchants offer a discount on the bitcoin prices and, if they do, what the average level of the discount is and whether it is adjusted in response to the perceived degree of froth or volatility in bitcoin's price.

currency's extreme price volatility. This price volatility likely also inhibits its ability to serve as a unit of account, as we discuss in the next section.

Bitcoin supporters—businesses and individuals alike—have primarily promoted the currency's potential to lower transaction costs, at least in terms of direct out-of-pocket fees. This offsets some of the risks specifically associated with bitcoin as discussed above. Peer-to-peer micropayments are possible with bitcoin, which charges variable transaction fees,[8] versus the $0.30 flat per transaction fee charged by PayPal, a popular intermediary for mostly e-commerce-related payments. Large-scale money transfers may also be cheaper if done through the Bitcoin network: wire transfers in the United States can run as much as $30 per transfer domestically and $50 internationally.[9] These fees are much higher than necessary to cover the costs of such transfers, as evidenced by comparable services in Europe that are offered at much lower or no cost.[10]

It seems reasonable to consider the "fundamental" value of bitcoin in its role as a form of fiat money, as derived from its function as a medium of exchange.[11] Retail sales are an obvious application. We conjecture that online (including mobile) transactions, collectively known as e-commerce, are the segment of retail where it is conceivable for bitcoin to capture a nonnegligible market share. We base this educated guess on the observed sample of retailers that already accept bitcoin for payments or have announced an intent to do so. We are also informed by the fact that the entire Bitcoin infrastructure is optimized for online communications. It is thus not surprising that, anecdotally, the typical user tends to be well versed in internet applications and even programming. It should be noted, however, that even a trivial share of the brick-and-mortar retail market is substantial in terms of absolute scale because it is an order of magnitude larger than e-commerce, as Figure 3 shows: the latter constitutes 6.0 percent of total retail sales in 2013: Q4, the latest quarter for which data are available.

---

[8] See, for instance, https://bitcoin.org/en/faq#how-much-will-the-transaction-fee-be. "Most transactions can be processed without fees, but users are encouraged to pay a small voluntary fee for faster confirmation of their transactions and to remunerate miners. …The precise manner in which fees work is still being developed and will change over time. Because the fee is not related to the amount of bitcoin being sent, it may seem extremely low (0.0005 BTC for a 1,000 BTC transfer) or unfairly high (0.004 BTC for a 0.02 BTC payment). The fee is defined by attributes such as data in the transaction and transaction recurrence. For example, if you are sending a large number of tiny amounts, then fees for sending will be higher. Such payments are comparable to paying a restaurant bill using only pennies. Spending small fractions of your bitcoin stock rapidly may also require a fee. If your activity follows the pattern of conventional transactions, the fees should remain very low."

[9] http://www.mybanktracker.com/news/2013/04/18/wire-transfer-fees-2013/

[10] http://www.money.co.uk/money-transfers/money-transfer-to-europe.htm

[11] Whether to call any portion of the nonzero price of an asset that does not pay explicit return a fundamental value is a matter of definition, at least to some extent, as discussed more fully later.

Another plausible area of application, because of Bitcoin's clear cost advantage (at least in terms of the explicit cost), is remittances, especially across borders.[12] A likely serious impediment to Bitcoin's adoption in this case is that the bulk of remittances are to developing countries. One could imagine that the potential users in these markets have neither the specific knowledge nor the digital devices necessary to utilize Bitcoin. This would explain why, to date, Bitcoin has no presence in this market. On the other hand, there is the mitigating factor that most such users have cell phones and many are comfortable with mobile applications. To the extent that a mobile application for international remittances using the Bitcoin network can be developed and accepted by a broad range of providers around the world, it can be possible for Bitcoin to capture a nontrivial share of this market. The crucial, yet difficult to assess, element is whether enough providers in different countries will be willing to adopt the Bitcoin technology, or some variant.

One could attempt to estimate the "fundamental" value of bitcoin—defined as its value derived from being a medium of exchange—using, for example, the quantity equation for money. The difficulty is that every input variable in such a relationship is subject to a tremendous degree of uncertainty. We experimented with estimating the quantity equation with a reasonable range of assumptions of the share of e-commerce and remittances that might possibly be intermediated by bitcoin along with the velocity of bitcoin, and yet even our most generous estimates of bitcoin's value still fall noticeably below the peak price reached in November 2013. Moreover, analysis by Ron and Shamir (2013) of blockchain data up to May 13, 2012, suggests that about half of bitcoin stock was not spent within at least three months after having been received, suggesting that these bitcoin are held more as a store of value than as a medium of exchange. We therefore suspect that the current high value of bitcoin is supported to a fair extent by optimistic expectations of Bitcoin enthusiasts. As previous research (see, for example, Ofek and Richardson 2003) has demonstrated, assets can be seriously overvalued when agents with widely heterogenous beliefs face short-sale restrictions, because the market price then reflects predominantly the optimists' valuation. By all accounts, it is practically impossible to short bitcoin: there is no bitcoin lending market, nor bitcoin derivatives.[13]

---

[12] According to a March 2014 report by Goldman Sachs, "All About Bitcoin," the average cost of remittances is 8.9 percent, compared with the typical cost of 1.0 percent charged by bitcoin wallet application providers such as Coinbase.

[13] In recent months, a few bitcoin derivatives have emerged on the fringe. These include bitcoin futures, the largest market for which is "ICTBIT.se," which supposedly facilitated more than 15 million dollars of futures trading during the last month. Predictious (https://www.predictious.com/) offers bitcoin option spread derivatives. TeraExchange

A chief advantage of bitcoin touted by its supporters is that transactions are free. This claim, however, considers only the explicit out-of-pocket expense faced by users as required by the protocol. It ignores the fact that the protocol, as designed, imposes an implicit cost on every existing holder of bitcoin whenever a transaction request is sent out to the network, in that a given number of new bitcoin will be created to reward the first miner who solves the hash function, and thus validates the transaction. This is equivalent to money creation that results in inflation, and hence the devaluation of all existing money holdings, all else being equal. This is clearly a form of negative externality—call it seignorage externality––in that the person initiating the transaction imposes on everyone a cost for which the initiator is not charged.

A related interesting development is that some users have voluntarily started to pay explicitly for having their transactions validated even though they are not required to do so. Figure 4 depicts the average explicit fee measured in dollars paid by Bitcoin network users since early 2009.[14] Clearly, even ignoring the implicit cost of the seignorage externality, the transaction fees paid for using Bitcoin have been nontrivial when measured in dollars, especially in recent months. This is because the fees are more or less fixed in bitcoin units. Their dollar value thus moves proportionally with the bitcoin price, which has risen substantially since late last year. The emergence of explicit fees seems to be a precursor of what will become inevitable in the long-run steady state when the supply of bitcoin will have stopped growing according to the built-in algorithm. At that time, for bitcoin to continue serving its medium-of-exchange role, miners will have to be paid directly by individuals requesting to have their transactions verified.

In addition to the implicit as well as the explicit cost for carrying out transactions in bitcoin, adopters of Bitcoin also face nonnegligible transaction fees when they convert standard currencies into bitcoin through the major bitcoin exchanges, as displayed in Table 2.

Moreover, some users may also consider the amount of time necessary to have a transaction eventually confirmed and entered into the blockchain, a nonpecuniary but nonetheless real cost: in order for a transaction to be considered completely final, Bitcoin users must wait up to an hour.[15] To the extent

---

recently created a bitcoin swap, according to Reuters (http://www.reuters.com/article/2014/03/24/us-bitcoin-derivatives-idUSBREA2N1CX20140324).

[14] https://blockchain.info/charts/transaction-fees

[15] There is some randomness to how long it takes for a particular transaction to be validated, due to the stochastic nature of "mining" and the total size of the transaction block. Smaller transactions get lower priority, and those users who offer a large (optional) transaction fee to the miners are likely to have faster verifications due to increased miner interest. Bitcoin transactions are not considered final until there are five subsequent blocks added to the blockchain.

that users also prefer to know with certainty how long it will take for their transaction requests to be confirmed, the volatility in the confirmation time, as depicted in Figure 5, results in disutilities as well.[16] Although it may seem a rather brief delay by the standard of settlement in the mainstream financial system, it can be regarded as lengthy by those users who adopted Bitcoin for its promise of instantaneous settlement. Perhaps more importantly, one hour is a long time in the realm of electronic transactions, potentially creating opportunities for hackers to attack the system with false data.

A variety of intermediaries have emerged to support the Bitcoin network and facilitate bitcoin's use as a medium for transactions, as discussed in greater detail below. Their ability to address various practical issues, and thus facilitate the use of bitcoin, has enabled them to grow rapidly along with the Bitcoin network.

Bitcoin as A Unit of Account

Bitcoin's use as a unit of account is so far entirely derived from, and hence secondary to, its medium-of-exchange function. In fact, even merchants who accept bitcoin as payment tend to post prices in standard currencies, such as dollars or euros, instead of bitcoins. Furthermore, as discussed already, many of them have chosen to minimize the exchange rate risk by converting bitcoin into standard currency right away or frequently. This is because bitcoin prices have been highly volatile, especially over the last year or so. For example, in dollar terms, bitcoin's realized monthly volatility was 265 percent between May 2012 and May 2014, while daily volatility was above 200 percent over the same period.[17] By comparison, the fluctuation of gold prices (annualized rate of monthly changes) is 88 percent over the past 10 years, and 118 percent according to an index (by S&P and Goldman Sachs) of all commodities. Even typical emerging-market currencies have exhibited volatilities on average of only about 9 percent, and no higher than 20 percent, over the past three years. Bitcoin's price volatility is orders of magnitude greater than the range of typical fluctuations in the prices of most goods and services.[18] To the extent that

---

Since the difficulty of mining is adjusted so that miners succeed in validating a block every 10 minutes on average, it takes an hour for the transaction to be considered final.

[16] Note that this is the amount of time for the initial verification. A transaction will be permanently included into the blockchain after five subsequent transactions have been successfully verified.

[17] Authors' calculations with data from bitcoinity.com. Volatility is defined as the standard deviation of percentage changes in price. Monthly and daily volatility over the two-year period is calculated using data from Bitstamp, which is the most active exchange for bitcoin trading in U.S. dollars since Mt. Gox filed for bankruptcy in early 2014.

[18] For example, according to Bils and Klenow (2004), who used the micro data underlying the consumer price index and found more frequent price changes than previous studies, half of prices last more than 4.3 months.

customers incur a psychological cost when they see the posted price (in dollars) of a typical good fluctuate rapidly, bitcoin's extreme volatility renders it less, or not at all, suitable as a unit of account. It is also conceivable that bitcoin's volatility diminishes its ability to serve as a medium of exchange if users dislike not knowing ex ante how many bitcoin they will need to pay for a good when they are eventually ready to buy.

Furthermore, there are a number of basic conceptual shortcomings in Bitcoin's initial design for it to function as a currency along the dimension of facilitating and stabilizing economic activity. Research in monetary economics has shown quite convincingly that it is generally preferable to rely on a central bank to adjust the money supply according to economic conditions instead of relying on a money supply that fluctuates exogenously. Moreover, the conditions for an optimal single currency area are stringent and therefore should not be attempted lightly, as highlighted by the euro crisis in 2010 and 2011. Hence, it is not advisable to adopt a single currency across many countries.

Bitcoin as a Store of Value and Speculative Investment

Like any valued financial claim, bitcoin also serves as a store of value and can become a vehicle for speculative investment. For any object whose market price is below its intrinsic value to be able to serve as a medium of exchange, it has to rely to varying degrees on an expectation of others' willingness to accept it for future transactions. Compared with commodity money, which has an intrinsic value, such as gold, or official fiat money backed by a sovereign entity, the current market value of bitcoin to any given user hinges entirely on her expectation of others' willingness to accept it later at a sufficiently greater value.[19] Viewed from this perspective, bitcoin becomes conducive to speculation, and hence subject to bubbles, because its value in any equilibrium rests wholly on self-fulfilling expectations. The extreme price volatility, numerous headlines about large speculative holdings in bitcoin,[20] and large

[19] However, some would argue that the intrinsic value of gold as an industrial input is negligible compared with its price. The value of gold as a commodity money stems from its property of being stable, durable, and easy to divide and verify purity. Unlike bitcoin, it requires real resources to mine gold, and the volume of gold production tends to rise with the price of gold as marginal mines become profitable. The resource cost of bitcoin "mining," in contrast, is purely by design and not technically necessary.

[20] See, for instance, "Winklevosses: Bitcoin worth at least 100 times more" http://www.cnbc.com/id/101190181

swings in transaction volume that are correlated with price movements all suggest that bitcoin displays some characteristics associated with purely speculative bubbles.[21]

A further rough metric for understanding the speculative versus fundamental value of bitcoin is the ratio of transaction volume to trading volume. The transaction volume is measured using the estimated number of bitcoin sent over the Bitcoin network (Figure 6), while the trading volume is measured by the number of bitcoin trades on exchanges (against fiat currencies). The ratio between the transaction and the trading volume is plotted in Figure 7. In principle, the transactions in which bitcoin is used to pay for merchandise (such as on Overstock.com) must be verified through the network by miners. Likewise, transfers across accounts due to purchases of bitcoin using traditional currencies via wallets are also processed by the network. There is, however, some "leakage" because of the internal transaction processing by bitcoin intermediaries such as Coinbase. It is likely that they accept bitcoin payments on behalf of the retailers, convert the bitcoin paid into dollars on an exchange such as Bitstamp, and then pay the retailers in dollars. Even though we have not been able to ascertain the extent of this kind of off-blockchain transaction processing, the blockchain data likely understate the volume of transactions for purposes of transfers and commerce. In comparison, most of the transactions affiliated with accounts held with an exchange, such as purchases of bitcoin with regular currencies or the reverse trades, are processed internally by the exchange. Hence, an increase in this ratio of transaction-to-trading-volume suggests an increase in the amount of bitcoin used for transaction purposes relative to that used for speculative trading purposes on exchanges, and vice versa. An increase in this ratio can thus indicate increased popularity of bitcoin as a medium of exchange, whereas a decrease in this ratio can indicate greater interest in bitcoin as a speculative asset.

Intermediaries Facilitating the Bitcoin Network

One primary motivation for the invention of Bitcoin, according to its alleged inventor, is supposedly to design a decentralized system that avoids the perceived tyranny of giant financial intermediaries at the core of today's financial system. Chief among these traditional financial intermediaries, reviled in public opinion for their role in the global financial crisis, are the major

[21] These bubbles are rational in that they are an equilibrium outcome given heterogeneous beliefs and the short-sale restriction. By comparison, some new-monetarist models can generate sunspot, cyclical, or chaotic equilibria, owing to the strong strategic complementarity of money adoption, which would be indistinguishable from bubbles; see, for example, Lagos and Wright (2003).

commercial banks and the former investment banks. It is therefore somewhat ironic that various forms of organized intermediaries have either existed from the very early days of Bitcoin or emerged over time to perform indispensable functions for the operation of the Bitcoin network. Since, by design, there would be no intermediaries, no entity is tasked with overseeing the lawful conduct and soundness of any of the intermediaries that, do, in fact, exist. It is thus almost inevitable that some of them have behaved less than prudently, resulting in customer losses. In this section, we describe the variety of these Bitcoin intermediaries and discuss how their existence, essentially inevitable, would have been predicted by the established theory of financial intermediation. Furthermore, theory also offers lessons for the kind of regulation that is likely necessary.

The first type of intermediary is the exchanges where buyers and sellers of bitcoin trade. The primary function of these exchanges is to facilitate trading with publicly posted prices and order books. Customer orders are directly and anonymously matched via automated algorithms. Judged by these attributes, the bitcoin exchanges are more akin to electronic communications networks (ECNs), such as Island, than to more traditional exchanges, such as the NASDAQ or the New York Stock Exchange (NYSE) and their counterparts in other countries. These traditional exchanges are almost invariably intermediated by market makers, such as dealers on the NASDAQ and specialists on the NYSE. In contrast, customers trade directly with one another on the bitcoin exchanges. There are five primary exchanges that account for the bulk—over 95 percent on average—of the bitcoin trading volume: Mt. Gox (prior to its bankruptcy filing on February 28, 2014), Btcchina, Huobi, Bitstamp, and Btce (see Table 3).

The dominance of just a few exchanges in the world of this virtual financial claim resembles the structure of the U.S. equity market prior to the introduction of the SEC's Regulation National Market System (Reg NMS) in 2005. Before Reg NMS was put in place, equity trading also was dominated by a few exchanges, especially the NYSE and the NASDAQ, although each of them is populated by many market makers. Concentration is a feature that we would expect according to theories of financial intermediation: the first and foremost function served by an exchange is to provide liquidity—matching buyers and sellers with as little delay as possible. Since liquidity generally increases monotonically in the number of trades, all else being equal, it is more efficient to have a small number of exchanges serving a large number of traders.

One reason why the number of exchanges serving a class of assets often exceeds one is that traders may place different weights on different attributes of trade execution. For instance, some may care more about receiving the best price offer, whereas others may care more about the speed of the

execution. This is, in fact, how the overall market for equity trading has evolved since Reg NMS was introduced: new venues such as ECNs and alternate (automated) trading systems have emerged to offer an array of differentiated services (such as proprietary data feed, rebates, or fees), as the scope for competing merely on price has been diminished by the "national best bid and offer price" requirement imposed, in effect, by Reg NMS. As a result, the market shares of both the NYSE and NASDAQ have plummeted to below 17 percent as of January 2014.[22] If a similar rule were to be introduced for bitcoin exchanges, we would expect to see a convergence of prices across exchanges. The cross-exchange dispersion of bitcoin prices has been substantial and persistent at times. On the other hand, more exchanges may emerge to offer services with more diverse features. The experience of equity trading's evolution in response to Reg NMS suggests some degree of caution in introducing similar rules into markets for new financial claims such as bitcoin: the regulation needs to be designed carefully to balance the benefit of investors' fair access to the best price against the potential loss of liquidity.

In the bitcoin context, these exchanges tend to combine the function of an ECN with services that are typically associated with brokers and dealers. Depending on one's perspective, however, certain services are regarded as restrictive requirements. They are analogous to tying arrangements in certain product markets, such as a two-year cell-phone contract required for a subsidized new phone. In particular, to trade on an exchange, customers are generally required to maintain accounts with the exchange where they hold their balance of bitcoin and regular currencies for trading purposes. Arguably, the primary advantage of these exchange-based accounts is faster confirmation of trades, because the exchanges act as the intermediary, offering instantaneous verification of the trades between affiliated accounts so that the transactions do not have to go out to the network at large and await verification by miners, which can take up to an hour.[23]

With this benefit, however, comes a serious risk: should an exchange fall short in safeguarding customers' accounts, the holders can experience severe losses. This risk did, in fact, materialize for customers of Mt. Gox: when the exchange proved unable to fix the security flaw that enabled hackers to steal bitcoins from its customers' accounts and eventually had to declare bankruptcy after suspending account access for several weeks, its customers lost essentially all their bitcoins held with the exchange. This episode demonstrates that, somewhat ironically, intermediaries are, in fact, as important in the

[22] According to BATS Global Markets. The degree of market fragmentation is even greater than reflected in exchange trading data because almost 40 percent of total volume is, in fact, accounted for by off-exchange trading accounts.
[23] See, for example, the rules listed on https://en.bitcoin.it/wiki/Trade.

Bitcoin network as they are in the standard banking system, and users are exposed to greater, not less, risk concerning an individual intermediary's soundness and solvency. This idiosyncratic risk is exacerbated by the lack of regulatory oversight and a safety net for the average user. In contrast, users of credit cards and debit cards are entitled to a high degree of protection that limits their potential loss should they fall victim to fraudulent activities. This evidently calls for some form of regulation to provide additional incentives for exchanges to bolster their security and to protect individual exchange users.

The second type of intermediary is miners, operating individually or as part of a coalition. The Bitcoin network was designed to rely on these miners to verify the validity of every transaction, although as noted above, trading on exchanges is processed by the exchanges internally, and even some transfers and commercial transactions are being processed off-blockchain by so-called bitcoin wallets such as Coinbase (discussed in greater detail later). This basic, yet crucial, function of any modern financial system is primarily performed by traditional commercial banks, which in turn rely on private clearing houses, as well as on transfer systems run by the monetary authority, to facilitate inter-bank fund flows, including clearing checks and physically transporting and disposing of currencies. Since a digital currency dispenses with the need to handle physical objects, all that remains for verifying transactions is a purely bookkeeping task, which is a form of information processing. Studies of information economics as well as established theories of financial intermediation, such as Diamond (1984), have demonstrated that there are substantial economies of scale, and hence, it is efficient to delegate such tasks to a small number of intermediaries. This is exactly how the mining operation in the aggregate has evolved: a few large coalitions of miners have emerged in the miner community. This contrasts with the initial state of the "mining industry," consisting primarily, if not exclusively, of miners operating alone, according to the Bitcoin protocol's original design.

As designed, the computations needed to verify transactions are well understood but intensive, and they become increasingly so, according to the built-in algorithm. As a result, allocating verification as a contest across a large number of miners is clearly sub-optimal from the viewpoint of social efficiency. The only potential justification is to argue that the participants have a sufficiently strong aversion to centralized processing that their disutility more than offsets the efficiency gain. The empirical evidence to date seems to suggest that the inventors of the Bitcoin protocol might have a strong preference for decentralizing every aspect of the network, as revealed by the original architecture of the mining operation. However, enough participants have since recognized the efficiency gain from having

informally delegated agents specializing in verifying transactions and, by revealed preference, have considered the gain to outweigh whatever dislike they may have for organized mining.

The consolidation of the mining operation may still be at an early stage, since anecdotal evidence suggests that some standalone miners remain, although there are no systematic data on the evolution and current composition of the mining community. Nevertheless, we foresee that mining will become more concentrated in the future as individual miners gradually exit or join a coalition because, sooner or later, they will have to recognize that their operation is no longer viable due to the efficiency advantage of mining coalitions. On the other hand, it is hard to predict how many coalitions will emerge to dominate the bitcoin market in the steady state, assuming there will be a viable steady state. Regardless of the exact future structure of the mining operation, the inevitable increase in concentration suggests the need for enhanced oversight, either by the players themselves or by an independent third party, to guard against the likelihood of collusion or other noncompetitive behavior.

The third kind of intermediaries are those that connect the final user-owner of bitcoin with the network. This includes the so-called bitcoin wallets, such as Coinbase Incorporated, which in general provide a platform for users to exchange regular currencies into and out of bitcoin, manage their bitcoin balances, and transact with others in bitcoin (including to pay for goods and services). These services—bookkeeping to ensure the accuracy of balances through time and when making payments—are comparable to those offered by a traditional transaction account, such as a checking account at a bank or a money market mutual fund account. The similarity in functionality naturally raises the question of consumer protection: bitcoin wallets are almost entirely free of the range of regulations with which mainstream financial institutions that provide similar services, such as traditional banks and money market mutual funds, must comply.[24] These regulations are intended to protect the safety, security, and accuracy of customers' balances. In light of the severe losses inflicted on customers by the security breach at Mt. Gox, it seems imperative to devise some similar forms of consumer protection in order to reduce the chance of similar losses in the future. The special nature of digital currency makes its safety almost synonymous with data security. Hence, it is also possible that new technology will be developed to

[24] One exception is that the financial crimes enforcement network (FinCEN), the U.S. Treasury department agency responsible for implementing the Bank Secrecy Act, ruled on March 18, 2013, that bitcoin should be treated like currency or "monetary value" for the purposes of U.S. anti-money-laundering laws, which means that certain types of bitcoin businesses involved with the transmission or buying and selling of bitcoin, such as wallets and exchanges, are subject to federal regulation as money transmitters. They must register with FinCEN and must comply with federal anti-money-laundering laws, such as "know your customer" rules and the reporting of suspicious transactions.

provide the safety that users demand. In fact, regulation that mandates a higher level of data security can provide additional impetus for startups in this space to supply the technological solution. For example, Circle.com, a startup offering custodial services for digital currency holders, seeks regulation, such as insurance of account balances (similar to FDIC deposit insurance) and reimbursement of consumer payments.

One important service these digital wallets offer to make it easier for a retail bitcoin user to transact with others is to manage the verification process on behalf of the account holders so that their transaction requests can be verified in a more timely and secure manner without the need for continual monitoring of each individual user. On the flip side, they also make the transaction process easier and more secure for merchants who sign up with them. Different wallet providers charge for their services in somewhat different ways. Coinbase, for example, charges a 1 percent fee for converting bitcoin into and out of a regular currency. Bitcoin ATMs have also emerged, and an increasing number are being installed in major cities. These are specially produced ATMs that allow users to deposit regular currency for the purpose of being converted into bitcoin. One example of bitcoin ATM makers and installers is Liberty Teller, which has brought ATMs for bitcoin to Boston, with reported use of over 500 customers in the first three weeks in February 2014.[25] "Bitcoin shops," physical stores to facilitate the exchange of bitcoin for fiat currency, have also begun to operate in Hong Kong, the United Kingdom, and other countries.[26]

Looking Ahead

It is almost a cliché to say that the only certainty about the future of bitcoin and the Bitcoin network is uncertainty. For that matter, the development of digital currencies in general, or more broadly any new technology for making payments, is also subject to considerable uncertainty. One reason is the rapid evolution of technology. For instance, agents maintaining the Bitcoin network are trying to improve its transaction processing capacity, which is a necessary condition for Bitcoin to handle any nontrivial fraction of the realistic volume of transactions routinely processed by networks such as Visa and MasterCard. In addition, how the legal and regulatory system will react to the changes is equally hard to

[25] http://www.redorbit.com/news/technology/1113097242/liberty-teller-launches-second-bitcoin-kiosk-in-boston/

[26] See, for instance http://www.dailymail.co.uk/news/article-2562854/Bitcoin-Its-not-just-online-Britains-physical-shop-virtual-currency-bought-opens-London.html and http://www.ibtimes.co.uk/asia-nexgen-opens-hong-kongs-first-bitcoin-shop-1438278

predict. Nevertheless, in this section, we venture to make some qualitative predictions, not only about Bitcoin, but also about some likely developments of digital means to facilitate transactions.

Regarding specific aspects of the Bitcoin network, we suspect there will be further consolidations in the mining community, ending in a few coalitions that dominate the network. There may also be consolidations among digital wallets: those able to offer desirable services at a competitive price and demonstrate superior security should win market share. There may even be mergers across exchanges, if some can execute trades faster or at a lower cost or with greater security. This scenario is more likely to occur without a rule, similar to the SEC's Reg NMS, that mandates the availability of best bid/ask prices. Such a rule would diminish the scope for plain vanilla price competition and could, in fact, give exchanges incentives to compete along other dimensions and encourage entry of new exchanges, as the emergence of changes in the equity trading arena after the introduction of Reg NMS would suggest.

Another source of comparative advantage that may emerge is regulation. We will likely observe more market segmentation along this dimension: exchanges domiciled in countries with lighter digital currency regulation should attract more agents who are suspicious of "the Establishment," or are keener to chase the technology frontier, or less risk averse.[27] In contrast, exchanges that are more regulated, and therefore presumably more secure, should attract more agents, to the extent that digital currency becomes a class of contingent claims absorbed into the mainstream financial system.

If the current price of bitcoin is sustained over the next year or two, more competing alternative digital currencies (altcoins) may emerge, especially since the barriers to entry in virtual currency are low. The growth of altcoins depends inversely on Bitcoin's first-mover advantage, such as the network effect of the breadth of acceptance for conducting transactions, the strength of which is uncertain. To differentiate themselves from bitcoin, these altcoins will likely offer different features along various dimensions, such as in transaction validation schemes, fees, supply growth, etc.

By comparison, more regulation is almost inevitable. For example, bitcoin wallets must already comply with anti-money-laundering rules, and the Internal Revenue Service has just issued a ruling regarding how bitcoin earnings should be taxed. Agencies such as the Financial Industry Regulatory Authority and even the Securities Exchange Commission may issue rulings about the safety and soundness of exchanges.

[27] In this consideration, we exclude what we would call "captive digital currencies," such as Facebook Credits and Amazon Coins. Analyzing the factors affecting the emergence and growth of such instruments is beyond the scope of this brief. See Gans and Halaburda (2013) for such an analysis.

The Bitcoin network as originally designed, and especially its associated digital currency, will probably not survive in the long run. Some serious design flaws of the current Bitcoin system have been identified, and some of them may eventually prove fatal. First, realistic growth projections of the scale of the blockchain indicate that it will likely become infeasible for individual users to store the data on their personal computers, and this may happen as soon as within a year or two. Currently, it already requires nearly 10 gigabytes of hard drive space to store the entire blockchain. Second, the resource cost of mining is becoming increasingly unaffordable, not to mention the inefficiency associated with this aspect of the system design. Again, it is possible that within a few years it will become infeasible to rely on this distributed model, however consolidated, to verify transactions.

Nevertheless, there is growing recognition that the lasting legacy of Bitcoin most likely lies in the technological advances made possible by its protocol for computation and communication that facilitates payments and transfers. The revolution in payments technology pioneered by Bitcoin helps to accelerate the development of better technologies for making payments and transfers cheaper, faster, and more secure. For instance, a new technology called Ripple, essentially a protocol that allows disparate systems to communicate in order to transfer funds and make payments, has recently been developed. One notable point, made clear by Ripple, is that the development of new technologies for making payments does not need to be accompanied by a new financial claim.

In fact, our confidence in predicting the emergence of one or a few protocols for making payments and transferring funds in general across many disparate systems is greater than our confidence in predicting the survival of any specific virtual currency. The current system that performs the essential functions of enabling transactions is fragmented, sometimes even within the same bank, and inefficient. So it is imperative that new methods be invented to improve efficiency. In some cases, it may be cheaper to replace the existing system wholesale than to try to reconfigure it piecemeal. In principle, any of the functionality or services related to payment and transfer offered in the existing financial system should be, and likely will be, a candidate for reform if such reform can result in greater efficiency by using technology developed in the open-source distributed network framework that is at the foundation of Bitcoin.

In short, the growing attention among the general public and researchers on the topic of digital currency and alternative payment technologies, along with the potentially revolutionary impact of such technologies on commerce, justify spending some resources on developing a framework for understanding the related issues. For example, what are the fundamental needs satisfied by digital

currencies such as bitcoin? How, if at all, should Bitcoin intermediaries be regulated? What are the main drivers of bitcoin price movements? Many interesting questions remain to be explored.

References

Bils, Mark and Peter J. Klenow. 2004. "Some Evidence on the Importance of Sticky Prices." *Journal of Political Economy* 112(5): 947–985.

Diamond, Douglas W. 1984. "Financial Intermediation and Delegated Monitoring," Review *of Economic Studies* 51(3): 393–414.

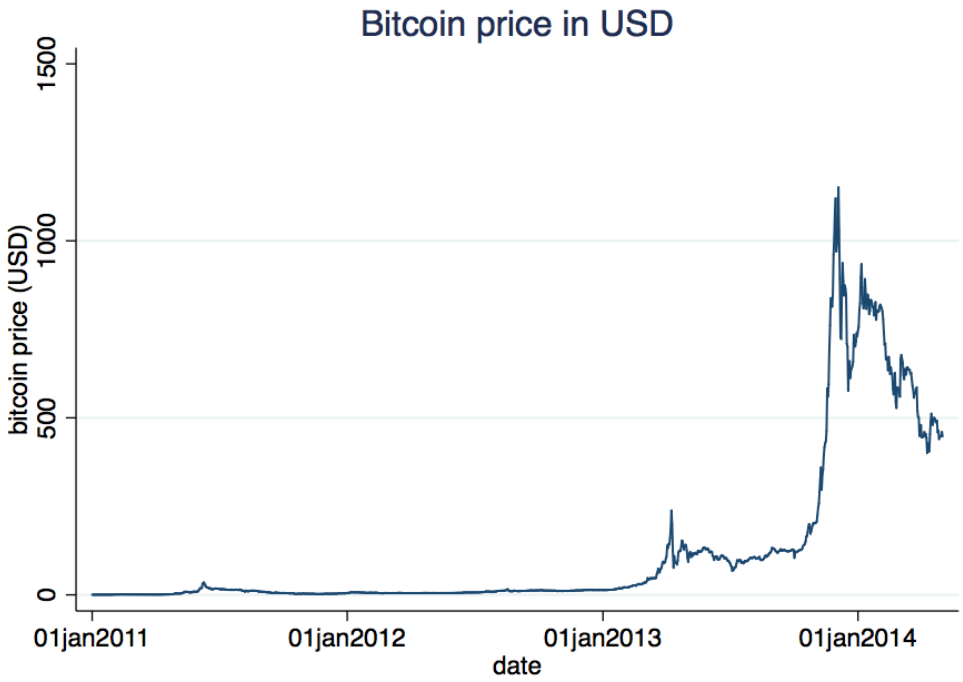
Gans, Joshua S., and Hanna Halaburda. 2013. "Some Economics of Private Digital Currency." *Economics of Digitization*. University of Chicago Press.

Lagos, Ricardo and Wright, Randall. 2003. "Dynamics, Cycles and Sunspot Equilibria in 'Genuinely Dynamic, Fundamentally Disaggregative' Models of Money." *Journal of Economic Theory* 109: 156–171.

Ofek Eli and Matthew Richardson. 2003. "DotCom Mania: The Rise and Fall of Internet Stock Prices," *Journal of Finance*, 58(3): 1113–1137.

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

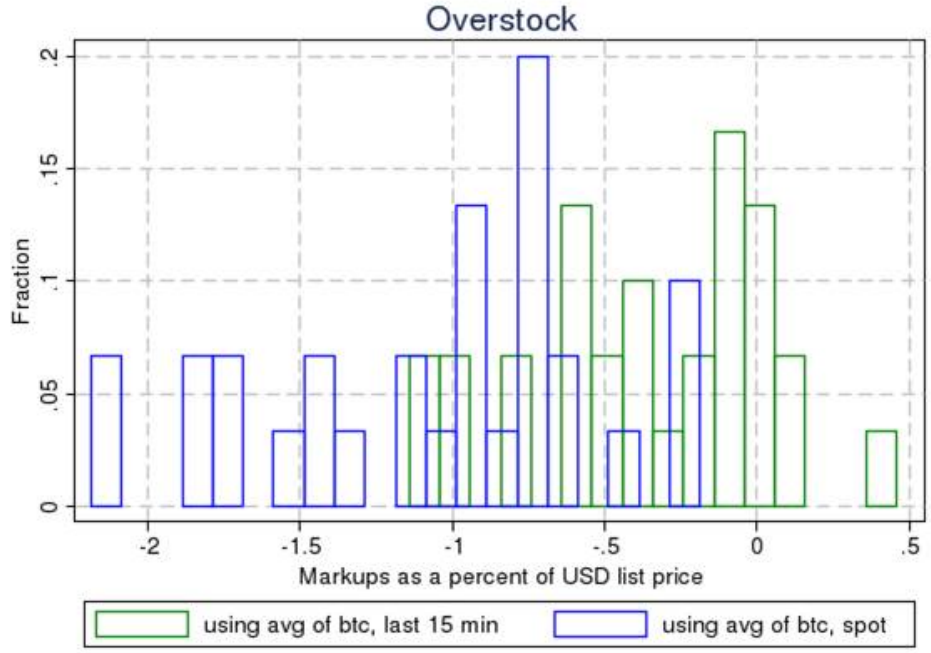
Figure 1. Time-series of bitcoin price since January 1, 2011



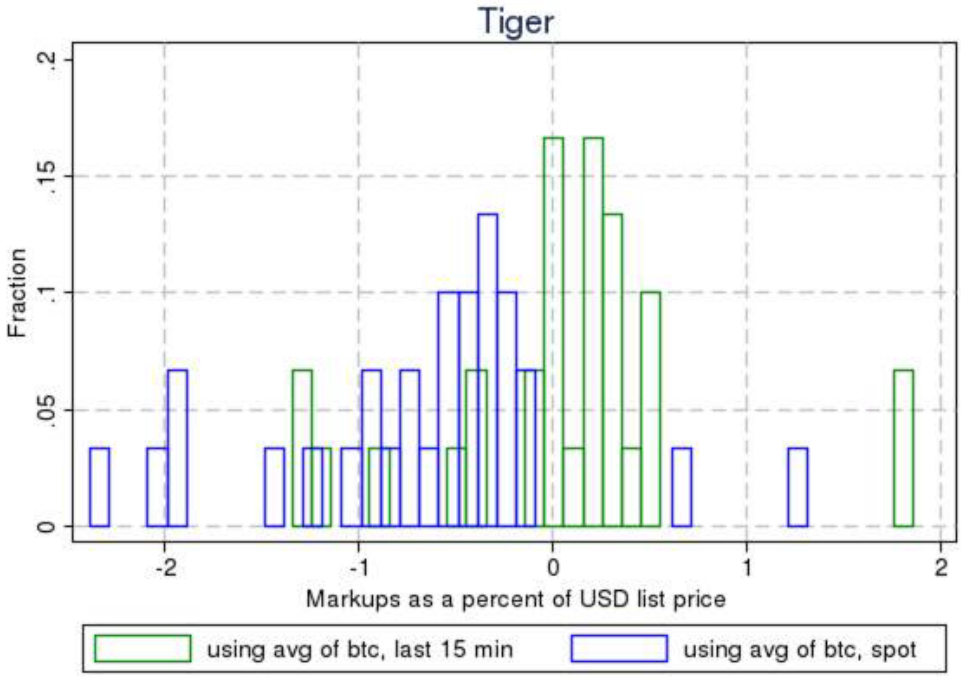
Source: https://blockchain.info/charts/market-price.

Figure 2. Bitcoin price markups of products by retailers

Panel A. Price markups on Overstock.com

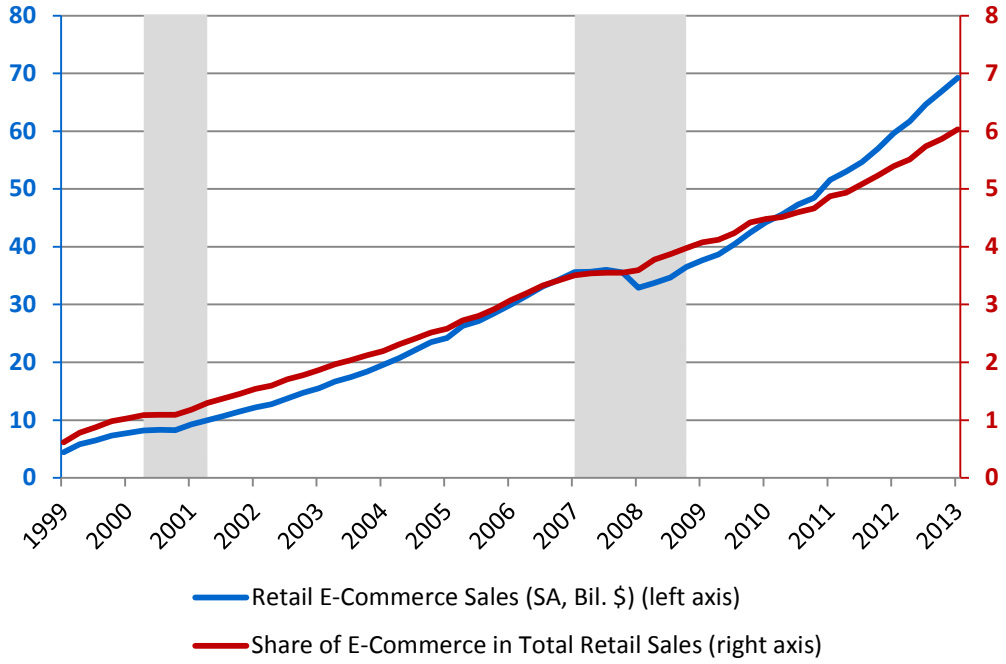


Panel B. Price markups on TigerDirect.com



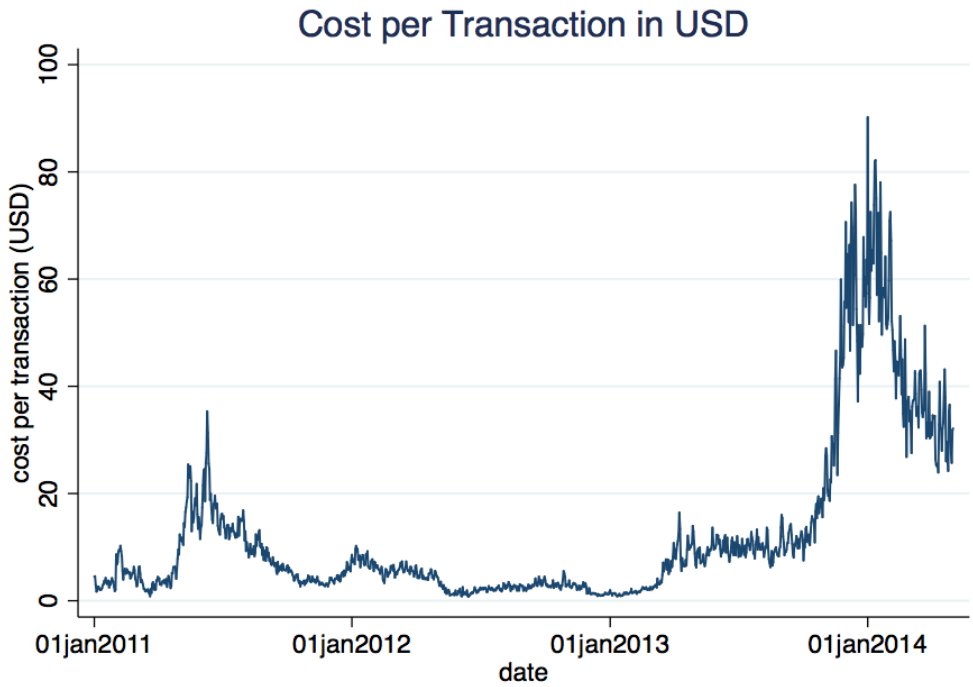
Source: Authors' calculations.

Figure 3. E-commerce and its share in total retail sales



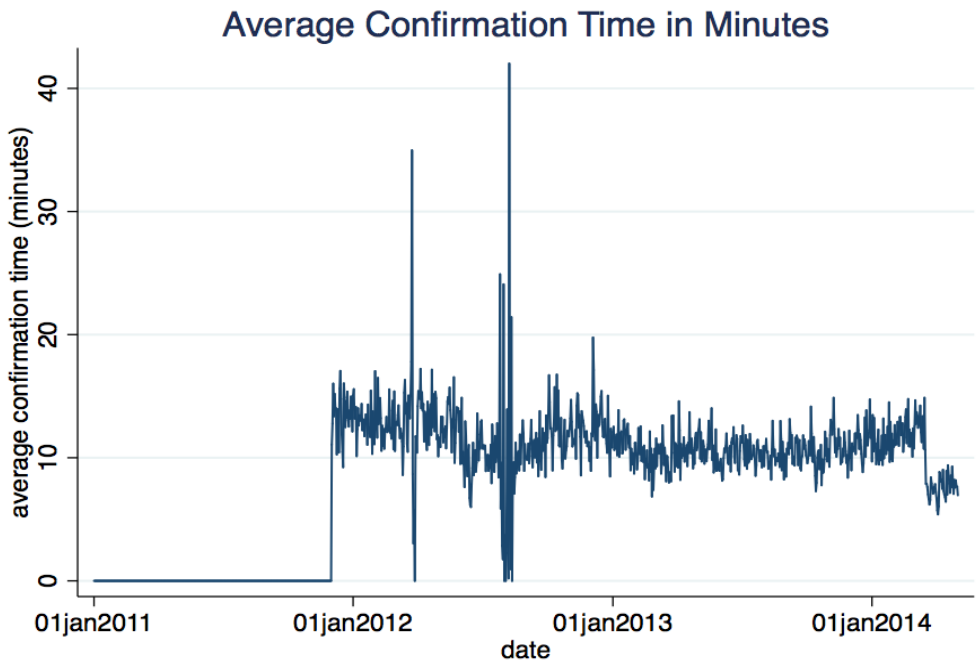
Source: Haver Analytics and authors' calculations.

Figure 4. Explicit fees per transaction on the Bitcoin network, in U.S. dollars



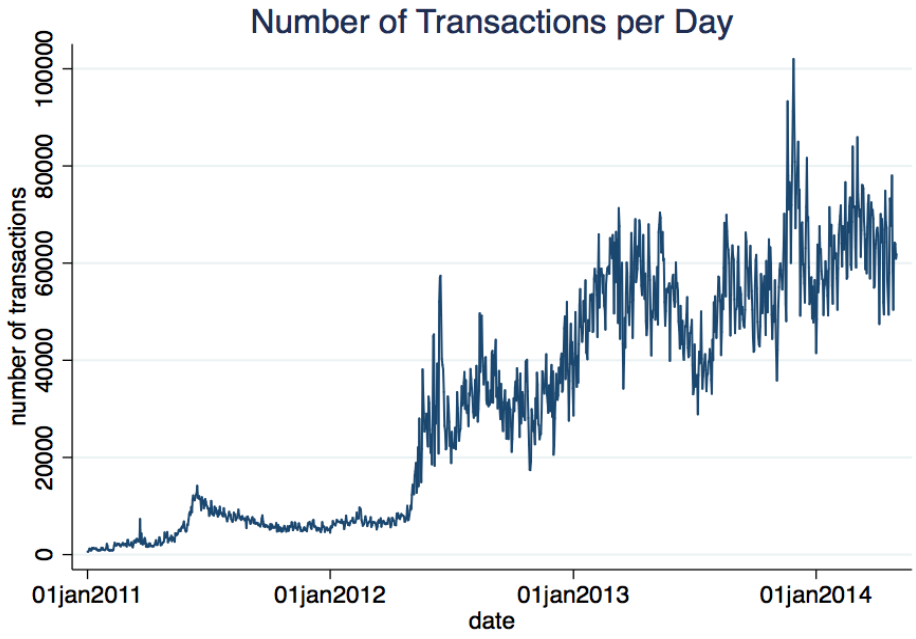
Source: https://blockchain.info/charts/transaction-fees.

Figure 5. Average confirmation time for each Bitcoin transaction



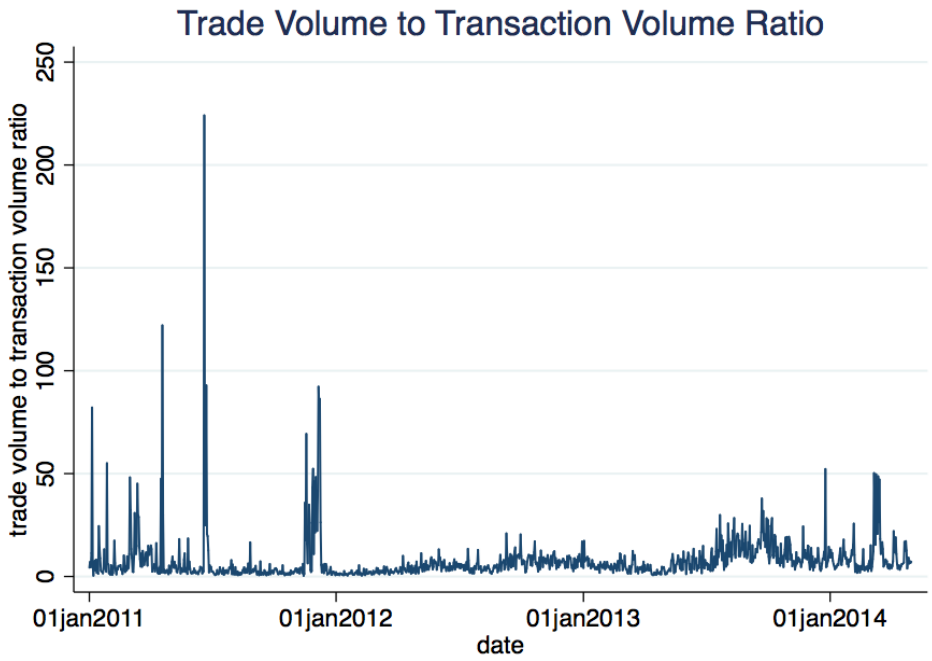
Source: https://blockchain.info/charts/avg-confirmation-time?timespan=2year.

Figure 6. Average daily number of transactions on the Bitcoin network



Source: https://blockchain.info/charts/n-transactions.

Figure 7. Ratio between trading volumes on bitcoin exchanges and transaction volume on Bitcoin network



Source: Authors' calculations, based on data from blockchain.info.

Table 1. Determinants of retailer bitcoin markups

VARIABLES	(1) 15-minute-markup	(2) spot-markup
15-min SD of price	-0.415***	-0.452***
	(0.0976)	(0.0960)
15-min change in price	-0.234	1.977
	(1.453)	(1.533)
Constant	0.156	-0.0929
	(0.237)	(0.249)
Observations	60	60
R-squared	0.184	0.279

Note: Robust standard errors in parentheses*** p<0.01, ** p<0.05, * p<0.1

Source: Authors' calculations.

Table 2. Fees Charged for Conversion and Withdrawal on Major Bitcoin Exchanges

Exchange	Conversion Fee	Withdrawal Fee (to bank)
Mt. Gox	0.6%	2% (EU banks)
Bitstamp	0.5%	0.09%, min $15
Btc-e	0.2%	1%
Localbitcoins.com	1%	0.0001-0.0004 BTC per outgoing transfer

Note: The numbers cited in this table may vary according to exact size and method of withdrawal. The numbers here are chosen to be representative of a standard transaction, but larger withdrawals may enjoy volume discounts.
Sources: https://en.bitcoin.it/wiki/Bitstamp#Withdrawing_funds, http://www.coindesk.com/btc-e-deposit-withdrawal-fees-customer-satisfaction-bid/.

Table 3. Market Share of Bitcoin Exchanges (March 2012 – March 2014)

Exchange	Volume [BTC]	Market share
mtgox	41.6M	51.70%
btcchina	9.88M	12.29%
huobi	9.16M	11.39%
bitstamp	8.59M	10.69%
btce	6.86M	8.54%
bitfinex	1.99M	2.48%
bitcoin24	811k	1.01%
campbx	639k	0.79%
localbitcoins	492k	0.61%
others	400k	0.50%

Source: bitcoinity.org