The Economics of Bitcoin and Similar Private Digital Currencies

Gerald P Dwyer

Clemson University and the University of Carlos III, Madrid

8. May 2014

The Economics of Bitcoin and Similar Private Digital Currencies*

Gerald P. Dwyer
Clemson University
University of Carlos III, Madrid

Abstract

Recent innovations have made it feasible to transfer private digital currency without the intervention of an institution. A digital currency must prevent users from spending their balances more than once, which is easier said than done with purely digital currencies. Current digital currencies such as Bitcoin use peer-to-peer networks and open-source software to stop double spending and create finality of transactions. This paper explains how the use of these technologies and limitation of the quantity produced can create an equilibrium in which a digital currency has a positive value. This paper also summarizes the rise of 24/7 trading on computerized markets in Bitcoin in which there are no brokers or other agents, a remarkable innovation in financial markets. I conclude that exchanges of foreign currency may be the obvious way in which use of digital currencies can become widespread and that Bitcoin is likely to limit governments' revenue from inflation.

July 2014

* Michael Dwyer assisted my exploration of the technical aspects of Bitcoin. I received useful comments on an earlier draft at the Mercatus Conference "Instead of the Fed", at the University of Carlos III and at the Infiniti conference in Prato, Italy. Glenn Blomquist, Warren Coats and John Devereux provided helpful comments. Research support was provided by the Spanish Ministry of Education and Culture for support of project ECO-2010-17158.

Electronic money has been the next best thing for fifteen years or more but until recently has not attracted attention outside narrow computer-science and economics circles. Currency which has only a digital representation has received a great deal of attention in mainstream media and some attention from economists and lawyers (e.g. Selgin 2013 and Grinberg 2012). A particular currency – Bitcoin – has received most of this attention, although there are alternatives in existence such as Litecoin and proposed currencies such as Ripple. Furthermore, there are liabilities being issued by entities such as Amazon and Facebook that might be characterized as digital currencies (Gans and Halaburda 2013).

There are two types of electronic money – currency and deposits. Currency can be defined in various ways. A definition that seems consistent with usage and the economic differences between currency and deposits is that electronic currency is an asset which can change hands from one person to another and is evidenced by a balance that the owner of the currency keeps.[1] Deposits can be defined as money which are evidenced by an account at a bank which is a liability of that institution.[2] Electronic money generally is viewed as storage of value in an electronic medium such as on a card or on a hard disk. In this respect, digital currency is not dramatically different from electronic storage of the value of deposit accounts other than concerns about theft. It is very different from electronic deposits though if an asset called electronic or digital currency can be transferred without intermediation of a financial institution.

Digital currency has a serious problem unless steps are taken to solve it. Bits – digital representations of anything – are trivial to create and reproduce on a computer, but bits cannot be used as currency unless they are hard or virtually impossible to reproduce. In the literature on digital currency, this is known as the double-spending problem: a digital representation of currency requires that it not be possible to create multiple copies and spend the same digital currency two or more times (Wayner 1997). The double-spending problem is similar to counterfeiting using an image of valid currency. If the double-spending problem is not solved, the value of the bits is the same as the marginal cost of reproducing any particular set of bits: zero.

For currency to have value, it must not be possible to spend digital currency more than once yet, if digital currency is similar to paper currency in this respect, there is no institution checking to make sure the transfer of purchasing power reflects available funds. Deposits in banks are represented on banks' computers by bits and the bank certifies that funds are available for the transfer. No person or institution necessarily certifies that a transfer of digital currency is possible unless one is introduced by design. For physical currency, the issuer creates value in part by making it difficult to reproduce the currency. For digital currency, reproduction could not be easier.

[1] It is tempting to add "and the transfer is final without the intervention of a bank" because this is true for fiat money, but some proposals for digital currency do in fact require certification by a keeper of central records.
[2] A "bank" is defined as an institution which has such accounts.

One solution to this problem is external certification that a particular piece of currency has not already been spent. An obvious way to do this would be to have a central authority which keeps a record of all transfers and certifies that a transfer of digital currency is a transfer of currency owned by the person making the transfer. Effectively, this central authority performs a role similar to that played by a bank holding a deposit. The primary difference is that the currency is not a liability of the authority certifying the transaction. Trust in the central authority's competence and honesty is a prerequisite.

A central authority is not how double spending has been solved for digital currencies such as Bitcoin. Instead, it has been solved by creating distributed databases with no central authority responsible – contractually or otherwise – for certifying transfers. Instead, resolution of transactions occurs in peer-to-peer networks of people in which no person or institution is in charge of certifying exchanges.

There is a growing literature on Bitcoin, although it still is thin in some respects. From two papers available in early 2013, there now are several papers available as of this writing. Most of them are papers on legal aspects of Bitcoin, its regulation and its role in the payments system, a topic not discussed in this paper. Selgin (2013) argues that Bitcoin and similar currencies are a new phenomenon, which he labels synthetic commodity money because of similarities to commodity money. Luther and Olson make the important point that Bitcoin involves a physical manifestation of memory as in Kocherlakota's theory of money (1998). Yermack (2013) argues that Bitcoin is not a "real currency" now and will not be one in the future.

The purpose of this paper is to provide an overview of Bitcoin and similar private digital currencies. Bitcoin is the most prominent as of this writing and I focus on it. Bitcoin is similar in many respects to other private digital currencies which use the same underlying technology. As with any other good, the supply and demand for such private digital currency is a solid basis for beginning to think about how Bitcoin might work. I also discuss the behavior of Bitcoin's price since Bitcoin began trading on electronic exchanges and provide a comparison of the volatility of Bitcoin's price compared to gold and foreign exchange.

Supply of Digital Currencies

The complex issues concerning digital currencies are on the supply side. Besides the double-spending problem, there are other issues. How is the digital currency created? If there is revenue from creating the currency, who receives it? What determines changes in the nominal quantity of money?

Overview

Bitcoin and at least some other digital currencies resolve these issues in the context of a peer-to-peer network using open-source software.

A peer-to-peer network operates very differently than a government's fiat money. A government's fiat money is created by a single issuer, certified by the issuer and used by many.[3] In terms of networks, this is similar to a client-server model in which one server receives requests from clients and responds to them. The server ensures the correctness of data, information or whatever is provided. In the case of fiat money, the issuer designs the currency to make counterfeiting difficult and enforces laws making counterfeiting a crime.

A peer-to-peer network is organized as a set of nodes into a self-organizing connected network.[4] Some or even all of the nodes can act as both clients and servers and the nodes are connected with each other, although not necessarily with all other nodes. While the peer-to-peer architecture cam be more costly because it is duplicative to some degree, this need not be particularly important. The cost of maintaining the peer-to-peer network may not be that much higher than a client-server network and it may be faster. Probably most pertinent for digital currencies, a peer-to-peer network can be more resilient to attack or problems at one specific location. All nodes need not be equally reliable. If some nodes are more reliable and online more than others, the nodes do not have to have the same standing.

Besides relying on a peer-to-peer network, Bitcoin relies on open-source software. Most generally, open-source software is software with source code distributed with little or no copyright restriction on use and modification of the program.[5] Open-source software is similar to a peer-to-peer network in the sense that software development is organized by the participants – programmers in this case – and no one is formally in charge of development due to ownership of the software. In practice, a subset of programmers is recognized as having a comparative advantage at organizing changes to the source code and makes decisions for the development of the software.

Bitcoin, the most prominent digital currency as of now, is organized in particular ways, some of which are not intrinsic to digital currency. It is simpler to examine the overall organization in the context of Bitcoin rather than speculate on developments.

Bitcoin was conceived by a person or persons using the pseudonym Satoshi Nakamoto.[6] In a paper made available to a user group on the Internet in 2008, Nakamoto outlined a digital currency based on peer-to-peer authentication with rules to determine the amount produced and the conditions for producing that quantity.[7] In conjunction with others, this proposal was

---

[3] This is purposefully written to cover currency unions such as the European Union.

[4] Minar and Hedlund (2001) provide a brief history of peer-to-peer models in the Internet's history.

[5] Copyright for software was not effective in the United States for source code until the late 1970s and early 1980s. Raymond (1999) summarizes the development of open-source software after the development of copyrights for software.

Many but not all licenses have restrictions on using the source code in software sold for a monetary price. Many but not all licenses require that any distribution of an executable program based on the source code include all the source code.

[6] A documented history of Bitcoin has yet to be written. This discussion is based on sources such as the Bitcoin wiki (http://en.bitcoin.it/wiki/ visited at various times in 2013. Essentially the same stories appear elsewhere.

[7] Nakamoto (no date) is a version which may have been edited after discussion of the original proposal.

modified somewhat and eventually Bitcoin came into existence. Nakamoto passed the oversight of Bitcoin to Gavin Andresen, who is the Chief Scientist at the Bitcoin Foundation. While not its reason for being, Bitcoin may well have reached its current prominence partly because it became the currency usable on the Silk Road – a website on which drugs and some legal goods could be bought anonymously (Wallace 2011).

It might seem that Gavin Andresen and the Bitcoin Foundation become the owner of Bitcoin in some sense, but any ownership rights are attenuated by the use of open-source software and an open protocol. With open-source software and an open protocol, anyone has the right to take the software's source code and start their own digital currency if they or holders of bitcoins are dissatisfied with aspects of Bitcoin.

Bitcoins are created by solution of a computational problem by "miners." Finding the answer to the problem provides "proof of work" which verifies that the miner did the work. Others are able to verify at low cost that the solution has been found although reproducing the work is not low cost. The difficulty of the algorithm is subject to increasing cost over time, with an eventual limit on the number of bitcoins that can be created.

The announced limit on the number of bitcoins is 21 million. The increase is determined by a simple rule which halves the increase every four years (Nakamoto 2009) and generates a decreasing increase over time. This inelasticity of supply is viewed as an advantage by some economists and a disadvantage by others. An inelastic supply is roughly in line with Friedman's solution for the optimal quantity of money (Friedman 1969) if the income elasticity of the demand for the money is one and loss of bitcoins is unimportant. From the viewpoint of a private currency such as Bitcoin, an advantage is predictability of the quantity produced even if a different rule for the evolution of the stock of bitcoins would have advantages.

Transactions and the Block Chain

Bitcoin and similar digital currencies are called crypto-currencies by some because the underlying algorithms and security are intimately related to digital cryptographic algorithms.

Unlike fiat currency issued by governments, a publicly available database records every trade of currency. Every bitcoin is associated with an address and a transaction is a trade of bitcoins from one address to another. This database is called the "block chain". A transaction in bitcoin is not final until it is included in the block chains available from many sources. No bitcoins exist or are held independently of the block chain.

What keeps the block chains scattered around the peer-to-peer network the same? There is a rule that the correct block chain is the longest one. Additions to the block chain are made as part of the process of mining bitcoins, and the answer to the question cannot be understood without a bit of detail about the block chain and how miners add to it.

The block chain is a chain of records of transactions and bitcoins produced. Miners add to the block chain by solving a computational problem and adding new transactions.

Miners compete to add the next chain to the block chain, which includes the record of the miner's acquisition of the new bitcoins and recent transactions. Transactions fees provide an incentive for miners to include recent transactions. While bitcoins are being produced, miners also receive new bitcoins and this currently is the major payoff from adding to the block chain.

In order to add to the block chain, a miner starts from a hash of certain information in specific fields. The information in each increment of the block chain includes information about new transactions including bitcoins received by the miner, a hash referencing the previous increment to the block chain, the hash of the transactions in this increment and identifying information for the block.

A hash is a transformation of the original information. Bitcoin relies extensively on hash functions. A hash function take a message *M* with arbitrary length and produces the hash value *h*, that is $h = \mathrm{H}(M)$. For the block chain, obviously the hash is much shorter than the message length. Bitcoin uses one-way hash functions, which are a subset of hash functions. One-way hash functions are not invertible except at high, preferably prohibitive, marginal cost. A one-way hash function has the following characteristics (Schneier 1996, p. 429): 1. Given *M*, it is easy to compute *h*; 2. Given *h*, it is hard to compute *M* such that $\mathrm{H}(M) = h$; 3. Given *M*, it is hard to find another message *M*' such that $\mathrm{H}(M) = \mathrm{H}(M')$. Miners' difficulty in solving the computational problem is not computing the hash, which is easy.

The difficulty in solving the computational problem posed for miners arises because the hash value *h* is restricted to be less than or equal to some value.[8] The problem is solved by searching for a hash value that is less than or equal to *h**, and miners change open fields in the message space to alter the hash and achieve *h**. There is a target for Bitcoin of having an increment to the block chain roughly every ten minutes and, as the amount of mining increases, the difficulty is increased by reducing *h**.

Miners can increase the probability of finding a small enough hash value by using faster computers and more computers. Specialized devices are sold to mine bitcoins. In addition, miners form pools to work on finding a small enough hash value, effectively pooling their computers. Miners participate in some of these pools on a piece-rate basis. Miners also participate in some of these pools as employees, who receive a fixed payoff whether or not the pool finds a small enough hash first.

Mining is a contest. Multiple miners and mining pools are working simultaneously on finding a small enough hash. Because there is no guarantee of being the first to find a small enough hash, the actual outlay of resources by a miner or pool of miners is unlikely to be as high as the value

[8] This is described as requiring leading zeroes in the hash because the overall hash has a maximum value.

of the bitcoins received from being successful. If miners are maximizing expected earnings, resource use by any pool will be as high as the expected value of bitcoins received on finding a hash less than or equal to h^*.

In order to maintain its reliance on competition in mining, it is important that mining be distributed across mining pools. In fact though, one mining pool has approach 50 percent of computing power twice (References). There is an underlying reason for such combinations of miners. A miner participating in the mining contest faces the idiosyncratic risk of losing the contest. By pooling resources with others, the miner can reduce their idiosyncratic risk. In the limit, if all miners participate in one pool, there is no idiosyncratic risk of losing the contest. This pooling of risk creates an incentive for miners to combine together in the largest pool. While not suggestive that mining eventually will be dominated by one mining pool, it is a tendency contrary to mining being competitive.[9]

The website block chain.info presents information which suggests that mining has generated negative net revenue since July 2013. This of course is possible if mining has positive nonpecuniary returns, for example if a mined bitcoin is worth more to a miner than a purchased bitcoin, or if miners can use others' resources to mine.

Wallets

The evidence of ownership of bitcoins is entirely in the block chain. Holders of bitcoins use "wallets" to keep track of their balances as well as to send and receive bitcoins. Despite the use of the word "wallet", this wallet does not contain bitcoins. The wallet is more akin to a spreadsheet program which keeps track of a balance than a wallet full of currency. Every bitcoin is associated with an "address", which is the name for a public key in Bitcoin transactions.

Public-key cryptography is essential for recording transactions and keeping track of the balance held by any individual. Public-key cryptography relies on private and public keys to encrypt and decrypt messages and this is crucial for verifying whether a transaction is valid.[10] The address to which bitcoins are sent is the recipient's public key. The sender's digital signature is an encryption using the private key, which can be unencrypted using the sender's public key. In this way, the sender is verified and the address of the recipient is known.

The digital wallet keeps track of the public key, called the address, and the private key. If someone loses their private key, the bitcoins are lost because it is not possible to produce the digital signature to transfer the bitcoins to anyone else without that private key.

---

[9] Details are provided in Dwyer (2014). There is a contrary tendency. There is no known way to prove that a particular set of transactions will produce a small enough hash. If one pool were mining, it would have to have a rule for when to change the set of transactions to search for a small enough hash. Two or more mining pools effectively solve this problem by searching with different transactions at the same time.

[10] The recipient of a message has a private key known only to them and a public key which is widely known. The sender encrypts the message with the public key. The recipient then decrypts the message with the private key known only by the recipient.

If an intruder into a computer obtains access to someone else's private key, the intruder can send the bitcoins to an address using the private key, effectively stealing the bitcoins. There is no way for the victim to recover the bitcoins even though the victim knows the thief's address (which is a public key). The victim does not know the thief's private key and cannot reverse the transaction. By the name "address", it might seem that an address would identify the thief but any user can create an arbitrary number of sets of private and public keys with no reason to identify a particular person or computer with any public key. Furthermore, the trail of transactions can be obscured by trades of bitcoins designed to obscure the trail.[11]

Every transaction in the block chain includes information about the sender and recipient to identify them in the block chain. The identification is based on public-key cryptography. The previous transaction record is hashed together with the recipient's public key, and the sender's digital signature is appended.

Authentication of Transactions in the Block Chain

Bitcoin uses authentication by a peer-to-peer network to solve the double-spending problem, which is quite different from central authentication proposed by Chaum, Fiat and Naor (1990) for example.[12] Multiple websites maintain copies of the block chain and update their copies by making copies from other nodes on the network.

Which chain of transactions is the correct one? The longest valid chain available on the Internet is the correct version and nodes obtain copies of the database from other nodes when the other nodes have longer chains. Transactions can occur in a matter of seconds, although the risk of double spending is not reduced to a low level for ten or more minutes when it is included in a block in the chain. The risk of double spending in fast transactions cannot be eliminated (Karame, Androulaki and Capkun, 2012).

Copies of the database are maintained because miners maintain copies as part of mining. Miners must have a copy and be linked to other sites in order to post their solution to the computational problem in the database. In addition, if someone else solves the cryptographic problem first and this information is likely to be reasonably widely known, miners' optimal strategy is to move onto the next block. Hence, miners have an incentive to update frequently and stay informed about the state of the block chain. Furthermore, they have an incentive to make this information available to others.[13]

---

[11] There are real limits to the ability to obscure the trail of bitcoins without giving up ownership of the bitcoins to an anonymous party for a while and possibly forever if the anonymous party does not return bitcoins. Meiklejohn at al. (2013) provide a very informative tracking of bitcoins.

[12] The most obvious way to authenticate transactions is to have a trusted central authority inform a recipient of the currency that the currency is indeed owned by the other party to the transaction. The central authority then updates the database on the ownership of the currency and the transaction occurs. The novelty in the solution proposed by Chaum et al. (1990) was anonymity of the exchange partners.

[13] Each block includes the previous hash value in the newly encrypted block, which makes the blocks a chain.

By design, the determination of valid transactions is one CPU, one vote. Otherwise, someone could become a controlling force for determining blocks by using multiple email or network addresses, which are much cheaper to acquire than acquiring more than 50 percent of the CPU power on the Bitcoin network.

On occasion, more than one new block is added to a set of previous blocks. Which block is correct? The rule is to use the longest block. While there can be more than one longest block at any one time, accretions soon result in one block becoming the longest block and being used.

What is to prevent a node from substituting a solution for a prior block, adding solutions for later blocks and creating the largest block? This is an example of a "Sybil attack": an attack by creating clones of valid nodes. The authentication by the longest chain could be subject to such an attack. In this context, such an attack would involve creating earlier apparently valid transactions and the longest chain, thereby appropriating coins earned by other miners. This attack requires that the attacker have more than 50 percent of the computing power among miners, which is regarded as unlikely.

Demand for Digital Currency

Why would anyone use digital currency? As with physical currency, the most obvious reason is a low cost of transfer from person to person. Digital deposits can be used in many transactions and no doubt will be used in more transactions in the future given plausible technological developments. Still, digital deposits are not transferable without the intervention, in general, of two banks and possibly a clearing institution. The payer's bank and the payee's bank both must effect the transfer of funds. Among other things, such a transfer with finality is not possible offline for digital deposits any more than it is possible for bitcoins.

Another aspect of currency transfers is their anonymity. Transfers of physical currency are anonymous in the sense that no agent has a central database with all transfers of currency stored.[14] While no institution has a central database of all transfers of bank deposits, aggregation of information across banks would make this possible. Nonetheless, transfers of physical currency self-verify that an agent has receipts from one or more sources sufficient to transfer purchasing power in exchange for something else.

Bitcoin is not anonymous and anonymity was not included as a design goal (Nakamoto no date). While a user of bitcoins can take steps to make his identity and a sequence of counter-parties less obvious, the evidence available so far does not support the proposition that it is particularly simple to hide one's sequence of transactions (Meiklejohn 2013; Reid and Harrigan

[14] The U.S. government does require selected institutions including banks to report cash transactions of $10,000 or more.

2013). It may well be impossible. If someone desires anonymous transactions, physical currency has the advantage if it is possible to use transfer the currency directly.

Even so, loss of the associated private key associated with an address and its balance of bitcoins has the same consequence as the loss of paper currency: it is gone. In addition, theft of a private key results in loss of the associated bitcoins just as does theft of paper currency.

Current physical currencies are associated with particular countries or sets of countries, but digital currency need not be associated with a particular country. Hence, the common strategy of defining the real quantity of money as the nominal quantity divided by a price level for an economy identified as a country does not work for a private digital currency. Because people can only be in one place at one time and there are nontrivial time and other costs of travel, households generally are concerned with the level of prices in a particular locale. In general, there seems no reason to think the demand for money is different in this respect with or without digital currency.[15]

Prices of digital currencies including Bitcoin in various fiat monies are readily available. Starting from price levels in terms of the prices of goods and services in a fiat money in a particular locale, conventionally identified as a nation, the real quantity of money demanded could be determined using the exchange rate of digital currency for the currency in which local goods and services are priced. While local goods and services could be priced in terms of the digital currency, it is not necessary. If there are multiple digital currencies, at this level of generality, there is even less reason to expect prices to be denominated in any particular digital currency. Nonetheless, there are virtually no data to decide how many bitcoins to allocate to what country and therefore there is no obvious way to compute a real quantity of bitcoins.

Because bitcoins are not redeemable in anything else from some particular agent or set of agents, bitcoins are not an immediate store of value. A full-bodied metallic coin requires resources to produce it but much of the value of the resources can be recovered by melting the currency down.[16] Historically, successful private notes for which the value of the paper represents a small fraction of the face value of notes generally are redeemable in some fixed quantity of an asset with value. The valuable resources used to produce bitcoins are the electricity and computer wear and tear plus a small amount of related labor. All of these resources are services consumed in production and are not available to anyone after a bitcoin is produced. They are sunk costs. It would make no difference if existing bitcoins were produced at zero marginal cost other than the relationships between mining, maintaining the block chain and distributing new bitcoins.[17]

---

[15] As with physical currency, there is an issue of whether currency and deposits should be aggregated. As with physical currency, it depends on the question being asked.

[16] Full-bodied coins are ones for which the metal in the coin has a face value equal to the face value or close to it. A token coin Is one for which the metal is a small fraction of the face value.

[17] It would of course make a difference in terms of efficiency. If there is a less costly mechanism for distributing new digital currency, this is a quite inefficient mechanism for creating bitcoins. One obvious alternative would be to distribute new currency to existing holders, which has its own advantages and disadvantages.

Equilibria with Positive Values for Bitcoin

Is Bitcoin designed in such a way that there is an equilibrium in which it is held? Irredeemable currency raises issues not raised by redeemable currency. Redeemable currency includes a promise that the currency can be turned into something else. The value of bitcoins is determined by the demand for bitcoins in conjunction with the rules governing supply.

While possibly undesirable in some respects, the rule limiting the number of bitcoins combined with the use of a peer-to-peer network for bitcoins created makes it relatively easy to determine whether additional bitcoins are being added to the stock other than those promised.

Even if bitcoins were costless to produce, there would be equilibria in which bitcoins are valued. It might seem that available theoretical results are not applicable because the theoretical literature has focused on private currency created with zero marginal cost. The production cost is irrelevant, though, once bitcoins have been produced because those costs are sunk. Hence, theoretical results are applicable. Results in Marimon, Nicolini and Teles (2012) for currency created with zero marginal cost indicate that an equilibrium with private currency held by consumers exists with commitment.[18] And knowledge of the quantity produced is a commitment device in their setup.

The possibility of entry is not addressed by Marimon et al. (2012). It is possible to create a digital currency with a positive marginal cost of production as for Bitcoin, but it is possible to create other digital currencies with zero marginal cost of production. If the marginal cost of production is zero and holders of digital currency are largely indifferent between various currencies, the value of digital currency will go to zero in equilibrium.

Marimon et al. do consider the possibility of multiple currencies but as in the early paper by Klein (1974), the existence of an equilibrium with positive values for private currencies requires there be a reputational equilibrium in which the currencies are distinguishable. There has to be something which distinguishes between the currencies and prevents them from being perfect substitutes. The digital representation of these currencies means that physical differences are uninteresting, although characteristics associated with finality of transactions and other characteristics may come into play. For example, Litecoin updates its block chain more frequently than Bitcoin. Some other currencies have rules for continued creation of new coins forever.

The liquidity of exchanges of a digital currency for goods and services, physical currencies and other digital currencies is a plausible differentiating factor. As for stocks in which exchanges become dominant due to liquidity on the exchange (Demsetz 1968), the liquidity of the currencies is likely to be a very important factor in determining their relative use. This

[18] See also Berentsen (2006) and Martin and Schreft (2008).

characteristic suggests that a solution with the value of digital currency positive is possible although not certain.

While mining new bitcoins is ongoing, miners update the record of valid transactions because mining is impossible without making the record of valid transactions available to the network. Mining will end at some point. The final number of bitcoins will be determined by the marginal cost of mining and the marginal return in terms of bitcoins, with an upper limit of 21 million.[19] If mining produces a number of bitcoins falling by half every four years (Nakamoto no date), 20.7 million bitcoins will be produced by 2041 given the algorithm.

Who will maintain the block chain of valid transactions when there is no mining? Nakamoto (no date) makes the supposition that transactions fees will support those who make the record available and update it. Such fees currently are collected but they are small relative to the new bitcoins received for completing a block. While a block would be created without transactions fees, competition among transactions to be included quickly in the block chain results in positive fees even today because there is no incentive to include a particular transaction in a new block without a transaction fee.[20] Babaioff, Dobzinski, Oren and Zohar (2012) point out that the structure of those fees will be more important for creating an equilibrium in which bitcoins are useful when there is no payoff in terms of new bitcoins.

Bitcoins and other alternative currencies raise red flags for government agencies such as the Financial Crimes Enforcement Network (FinCEN) of the U.S. Department of the Treasury. While Bitcoin itself is not completely anonymous, international exchanges for bitcoins can make it possible to move money around the globe. In addition, the trail of ownership of bitcoins can be muddied by mixing different users' coins at firms that perform that service. Any firm in the world dealing with U.S. citizens is subject to a variety of regulations and money-transfer firms are subject to more regulations (Sparshott 2013). While other governments' regulations for their citizens may be less daunting, governments have laws they seek to enforce to prevent money laundering and to collect taxes.

Bitcoins' Use in Exchanges for Goods and Services and Competing Currencies

Not surprisingly, it is difficult to obtain data on Bitcoin's use in exchanges for goods and services. Obtaining such an estimate is similar to trying to estimate the use of physical currency in exchange for goods and services. Such estimates may be possible but it is even less obvious how to make estimates that would be comparable to estimates made for physical currency.[21] Bits of information about Bitcoin's use in exchanges are generated by trials such as a Forbes'

[19] As of October 2013, there are about 11.8 million Bitcoins.

[20] For practical purposes, a miner is indifferent between including or ignoring a transaction when creating the next block.

[21] A website (http:www.wheresgeorge.com) tracks the locations at which U.S. dollars appear, which is quite limited relative to the information provided by the block chain.

columnist who lived on bitcoins for a week in San Francisco (Hill 2013) and some detailed information is available in Meiklejohn et al. (2013)[22]

The block chain makes information on transfers of bitcoins readily available, although it does require substantial programming and analysis to summarize trades. Some addresses in the block chain represent addresses of exchanges. In addition, any person can transfer from one address to another one owned by himself. Furthermore, some users act as "mixers", taking delivery at their address of bitcoins, mixing up any one person's bitcoins with other persons' bitcoins and then transferring an assortment of bitcoins which can make it difficult for someone else to track the bitcoins. As a result, any detailed analysis of the block chain must be taken as only an indication of the relevant statistics for underlying holdings of bitcoins and transactions.

The block chain does contain information on transfers and some possibilities can be ruled out. Following the early analysis by Reid and Harrigan (2012), Ron and Shamir (2013) analyze the block chain through May 13, 2012 to estimate the turnover of bitcoins and the fraction of balances that have not been transferred from one "entity" to another since creation. They attempt to identify "entities" from bitcoin transfers although the estimates probably overestimate the number of separate entities.[23]

The bitcoin value of the total number of transfers as of May 13, 2012 was about 423 million bitcoins. They estimate that the 3.7 million different addresses in the system were associated with 1.9 million different entities which had transactions and 3.1 million different addresses. Six hundred and nine thousand additional addresses had never sent a bitcoin to another address. The average entity held 3.7 bitcoins, although the distribution was very skewed. At the then current price of $30 per bitcoin, the average balance was about $100. Eighty-five percent of the entities held less than 0.01 bitcoins, and one entity held between 200,000 and 400,000 bitcoins worth about $6 to $12 million at the time. A rough estimate from their Table 3 indicates that about half the total holdings of bitcoins were in entities holding 1,000 to 10,000 bitcoins.

As of the date of their study, most bitcoins had never been transferred from the address receiving them at creation. Their estimate indicates that 78 percent of all bitcoins were at addresses which had never sent a bitcoin to another address.[24] Access to some of these bitcoins may be lost forever because the private key was erased when bitcoins were worth little, and some private keys likely have been lost in hard disk failures and similar events.

[22] The limits of such analyses are indicated by Ron and Shamir themselves (no date), who claimed a possible link between an account, Satoshi Nakamura and the Dread Pirate Roberts who ran Silk Road. Dustin Trammell (2013) came forward and indicated the account was his, also stating that he was not Satoshi Nakamura and that the never had transacted with Silk Road.

[23] Important technical issues related to how bitcoins are transferred affect the computations (Ron and Shamir 2013).

[24] As they note, there is an embedded duration problem since bitcoins were created at different dates before the cutoff date.

The distribution of transactions by entity also was highly skewed, with 97 percent of all entities having fewer than 10 transactions and 75 entities having at least 5,000 transactions.

Meiklejohn et al. (2013) attempt to characterize transactions and aggregate entities through April 13, 2013. They opened accounts and made purchases to obtain addresses and supplemented that information by self-identified addresses available on Bitcoin forums. They analyze bitcoin transfers, in large part to determine whether bitcoins are useful for illicit activity. They conclude that bitcoin is not useful for high-value illicit use such as money laundering or drugs. They also find a trend toward smaller transactions and faster spending which is largely due to one service: Satoshi Dice, an online gambling site. Sales through legal vendors also achieve increasing importance in late 2012 and early 2013, although Satoshi Dice is quite a bit larger.

It is clear that Bitcoin and other digital currencies can co-exist, at least with flexible exchange rates between them. Alternatives have arisen and others are likely to arise. One interesting alternative is Ripple, which is similar to Bitcoin but uses transactions fee from the start to provide an incentive to authenticate transactions.[25] It also avoids the lost resources due to imposing an artificial marginal cost of producing the currency but it does require a rule to distribute the initial distribution of digital currency.

Price Data

Bitcoin is a currency which is traded for other currencies. While it is not clear how much Bitcoin is used in trading for goods and services, it is used in relatively frequent transactions against national currencies.

This trading is rather remarkable from the viewpoint of financial market microstructure.

Until late 2013 when it closed, the Mt. Gox exchange in Tokyo was the most important exchange on which bitcoins were traded. Mt. Gox opened as an exchange for Bitcoin in 2010 and the last trade recorded by bitcoincharts.com was on February 25, 2014 at 1:59 AM GMT. Citizens of many countries traded bitcoins on Mt. Gox in a computerized trading environment. Mt. Gox was an order-driven exchange on which individual posted bids and offers or market orders. As a result, Mt. Gox had the potential to have trades 24 hours a day, seven days a week and it did have such trades. These trades were not intermediated through brokers, agents or any similar financial intermediary. Data on trades on Mt. Gox including prices and other characteristics were available from Mt. Gox.

Bitstamp and btce are two other exchanges which have substantial trading of bitcoins for U.S. dollars. Data on prices for the Mt. Gox, Bitstamp and btce exchanges are available from bitcoincharts.com. The price data for Mt. Gox from bitcoincharts.com and from Mt. Gox directly

[25] See https://ripple.com.

appear to be similar. All prices used in this paper are prices in trades for U.S. dollars, which is the largest single currency traded for bitcoins as of this writing.

Prices on Exchanges

One set of data for this paper starts from a set of data provided on the Internet by Mt. Gox starting on July 17, 2010 at 11:09 PM Greenwich Mean Time (GMT), shortly after the beginning of trading, and running through May 23, 2013 at 2:32 PM GMT. I also downloaded data for U.S. dollar trades from a data feed provided by Mt. Gox from May 23, 2013 to February 14, 2014 23:15 GMT. In addition to the price and time of trading, these data include the number of bitcoins traded and details about the initiating order. After merging the two datasets, there are 8,364,956 trades included in the data, all of which are unique in terms of the variables included.

The second set of data is from a secondary source: bitcoincharts.com. These data include only prices and time stamps. In this paper, I use data on U.S. dollar trades on Mt. Gox from July 17, 2010 at 11:09 PM GMT to February 25, 2014 at 1:59 AM GMT. There are 8,295,809 observations. The data for Bitstamp include 3,118,971 trades from September 13, 2011 at 1:53 PM GMT to March 3, 2014 at 11 AM GMT. The data for btce include 10,834,761 trades from August 8, 2011 at 2:15 PM GMT to March 3, 2014 at 11:01 AM GMT. Some of these large numbers of trades reflect more than one transaction at the same second and the same price on the same exchange. After deleting such apparently duplicate transactions, there are 22,249,361 unique trades across the three markets.

Mt. Gox was a computerized 24/7 exchange, as are other bitcoin exchanges. Figure 1 shows the number of U.S. dollar trades and the number of bitcoins traded for U.S. dollars by month from the start of trading until the end of 2013. The years 2012 and 2013 stand out as having substantially more trades than the two earlier years.

Because Mt. Gox was a 24/7 exchange, it is interesting to examine the intra-daily pattern of trading to see whether there are predictable increases and decreases in trading. The results of this analysis also will be useful for examining the daily volatility of Bitcoin's prices compared to related assets. Figure 2 shows regression coefficients of dummy variables by hour for the logarithm of the number of trades. There is an increase in activity from about 3 PM GMT to about 10 or 11 PM GMT. The time 3 PM GMT is 10 AM Eastern Standard Time (EST) and 7 AM Pacific Standard Time (PST), which is consistent with the clock in the United States being related to the volume of trades of bitcoins for U.S. dollars. Overall, the change in the number of trades suggests that trading activity of bitcoins for dollars reflects the clock in the United States in 2011 and 2012. This daily seasonal is much less prominent in 2013. While these estimates might suggest shifting the clock to Eastern Time, they also indicate that leaving the time stamps on Greenwich Mean Time does not split up trading in a "day" even when there is a daily seasonal. I leave the data on Greenwich Mean Time.

Figure 3 shows the prices of bitcoins for U.S. dollars for the three exchanges.[26] It is clear that the prices have increased substantially. The first trade on Mt. Gox on July 7, 2010 was a trade of 20 bitcoins for $0.04951.[27]

There has been substantial discussion of the volatility of the price of bitcoins, for example by Coats (2014). In one sense, it is not surprising that the price has increased given that it did not go to zero. Valued at $0.05 per bitcoin, the total stock of about 12.5 million bitcoins in March 2014 would have been worth about $625 thousand.

On the other hand, the price has increased and decreased quite a lot. The maximum price for a trade on Bitstamp was $1163 in seven trades on November 30, 2013.[28] The last price in these data for Bitstamp was $586 on March 3, 2014. This represents a decrease in price of 50 percent in about three months.

Is a price of $586 high or low? This question is even harder to answer than for governments' fiat monies. There is no reason to use Purchasing Power Parity for bitcoins to assess the price even if it were feasible.

A simple and somewhat informative way to look at the question is to examine the aggregate purchasing power in dollars represented by the quantity of bitcoins. There were about 12.5 million bitcoins on March 9, 2014, as computed at the website https://bitcoincharts.com. At a price of $586 per bitcoin, this indicates an approximate value of bitcoins of $7.32 billion. While not trivial, this is small compared to the value of U.S. M2 of $11.0 trillion for January 2014. Does a ratio of worldwide holdings of bitcoins to U.S. dollars of 0.07% seem out of line? It is obvious that the U.S. dollar is in no danger of being replaced by bitcoins in terms of value. It also is obvious that the value of bitcoins in dollars outstanding today is not particularly large. While it is hard to guess what the value of bitcoins outstanding might be in the future, it does seem clear that a total quantity of bitcoins less than twice as high as today's quantity could be associated with a significantly higher price.[29] Such appreciation may never materialize because Bitcoin will disappear. In addition, any appreciation is likely to be limited to an unpredictable extent by competition from other digital currencies.

Another way of looking at the aggregate value of bitcoins is to compare their value to the value of reserves in the banking system. This comparison is suggested by the possibility that bitcoins

[26] While not literally identical, the data directly from Mt. Gox do not extend as close to their demise and add nothing to these data.

[27] This is an odd price taken by itself but it is not so odd if the transaction fee was $0.00049, which would make the total payment one dollar.

[28] The maximum price on Mt. Gox was $1242 but bitcoins traded higher on Mt. Gox in late 2013 due to difficulties transferring dollar but not bitcoins out of Mt. Gox.

[29] Bitcoins are divisible by construction to the eighth digit after the decimal place, which allows for quite a bit of subdivision of units.

will be useful in finalizing transactions between other monies. In some ways, this is similar to the use of banking reserves to clear transactions between deposits in various banks. Before the Financial Crisis of 2007-2008, reserves in the U.S. banking system alone were $8.75 billion. These primarily were clearing balances maintained by banks. The value of all bitcoins in March 2014 of $7.32 billion is about 84 percent of this value of reserves in the Federal Reserve. Given the early stage of development of bitcoin, this seems quite large if the only role of bitcoins is for finalizing transactions in U.S. dollars. On the other hand, bitcoins are not useful only in the United States and $7.32 billion of bitcoins may be small relative to reserves weighted by holdings of bitcoins and possible future use.

The Volatility of Bitcoin's Value

Besides changing dramatically at times, is the value of a bitcoin highly volatile on a regular basis? Figure 4 shows the monthly standard deviation of daily log returns of bitcoins on the three exchanges. There clearly have been months when prices and returns have been volatile. Compared to the well-known one-percent per day typical standard deviation of broad stock return indices in the United States, the standard deviation is quite high. The mean standard deviations across months are 7.2 percent per day for Mt. Gox, 5.1 percent per day for btce and 5.5 percent for Bitstamp.[30] The standard deviations are very skewed, with lower medians of 5.2 4.7 and 4.4 percent per day, respectively. While this is lower, it is not low relative to holding a broad portfolio of stocks. The minimum values of the standard deviations are quite a bit lower, being 1.1, 0.9 and 1.0 percent for the three exchanges respectively. To some extent, the volatility can be attributed to extraordinary developments, with maximum standard deviations of 17.0 percent in June 2011 for Mt. Gox, 16.2 percent in April 2013 for btce and 16.2 percent in October 2011 for Bitstamp. There are high correlations of the standard deviations, even though the differing dates of maximum volatility might suggest otherwise.[31]

Is this volatility large or small? It seems useful to compare this volatility to the volatility of gold prices and foreign exchange in U.S. dollars.

Figure 5 shows monthly standard deviations of daily log returns on gold from January 2010 to February 2014. These estimates of monthly volatility are not an order of magnitude lower than the volatility of returns for Bitcoin, but they are quite a bit lower. The mean standard deviation is 1.1 percent and the median is little different at 1.0 percent. The maximum standard deviation of 2.2 percent is an order of magnitude lower than the maximum standard deviation of returns for Bitcoin of 16 or 17 percent. At least in this period, holding gold has much less idiosyncratic risk than holding bitcoins. Absent a sudden drop in Bitcoin's volatility, gold is likely to be a less volatile investment for at least some time.

[30] These mean standard deviations exclude the incomplete months at inception and Mt. Gox's final incomplete month.

[31] All correlations of standard deviations across exchanges are above 0.9. Mt. Gox was the only exchange operating in June 2011. All three exchanges had high volatility in April 2013. This just was overshadowed for Bitstamp by idiosyncratic extraordinary volatility on Bitstamp in its first full month of trading.

As for bitcoins and gold, I computed monthly standard deviations from daily log returns on the values of foreign currencies for U.S. dollars with daily data at the Federal Reserve Bank of St. Louis.[32] The data cover January 2010 to February 2014. There is substantial variance across countries, with some countries having some difficulties in this period and others pegging to the dollar. That said, the average monthly standard deviation of daily log returns is 0.5 percent per day. This is an order of magnitude lower than Bitcoin's volatility and lower than any monthly standard deviation of daily returns for Bitcoin seen through February 2014. There is overlap of the volatility of the return in dollars for Bitcoin and for these currencies. The maximum standard deviation is 2.2 percent per month across these countries, which is twice the minimum volatility for Bitcoin on the three exchanges. These data do not include countries in substantial monetary difficulties such as Zimbabwe during its hyperinflation or Argentina more recently, which would be likely to make the comparison less one-sided because some developments for such currencies are likely to be less predictable.

A Comparative Advantage for Bitcoin

The exchanges for bitcoin illustrate one possible comparative advantage of digital currency. Digital currency and exchanges such as Bitcoin are much cheaper venues for trading currency than alternatives available to final consumers today. If a person holds accounts in various currencies, it is lower cost to transfer funds from one account to another through a digital exchange and a digital currency relative to the current cost of obtaining foreign exchange.

In addition, Bitcoin can be used to avoid currency controls instituted by national governments. While currency controls can prevent using exchanges such as Mt. Gox, they cannot effectively prevent people from bringing digital currency into a country and trading them for local currency. The purchaser of the digital currency then trades them for a preferred currency outside the country. While hardly zero marginal cost, the marginal benefit to the purchaser can be substantially greater than the marginal cost.[33]

Conclusion

Bitcoin embodies a major innovation in trading. A peer-to-peer network validates transactions and finalizes them, with no trust in a central authority required.

The design of Bitcoin and similar currencies does not have any debilitating flaw. Bitcoin's design is such that off-the-shelf theoretical results (Marimon et al. 2012) indicate that an equilibrium with positive value for such a currency is possible. I know of no game-theory results which characterize a dynamic equilibrium for the central mechanism of Bitcoin's functioning: the block chain with its use of competition and proof of work to finalize transactions. Developing

[32] The countries and Eurozone currency area are quite varied, with exchange rates for Australia, Brazil, Canada, China, Denmark, the Eurozone, Hong Kong, India, Japan, South Korea, Malaysia, Mexico, New Zealand, Norway, Sweden, Singapore, South Africa, Sri Lanka, Switzerland, Taiwan, Thailand and the United Kingdom.

[33] Physical currency not only has the problem of bulk but Argentina has trained dollar-sniffing dogs to foil imports of dollars from abroad (Martinez-Carter 2012).

such a result is the major hole in current knowledge about the block chain and, by extension, Bitcoin and similar currencies.

Innovations to allow people to use their smartphones to transfer funds to others are coming. On a smartphone, there is no technical difference between using dollars and bitcoins.

There is a major difference between digital currency and digital deposits in one respect. The finality of transactions in bitcoins is not guaranteed by an institution such as a bank. Some view this as an advantage but it may not be particularly important to many end users. In other words, there may be little demand for this distinction. To the extent that use of the system requires blind faith in anonymous people's expertise, the complexity is a disadvantage.

Furthermore, most people seem to prefer to have their assets and liabilities denominated in the same currency. This reduces their risk in terms of their own currency, which is not trivial given the volatility of exchange rates. This preference is one explanation for why banks promise to redeem deposits at fixed values in local currency (Dwyer and Samartín 2009). It is hard to see the U.S. dollar being replaced by Bitcoin or other private digital currencies for everyday transactions. While some monies are in fact displaced, such as the Zimbabwean dollar in recent years, this usually only occurs after dramatic inflation. In fact, Luther's interesting evidence for Somalia (2013) indicates that currency issued by a non-existent government can continue in circulation for some time.

It is possible that bitcoins and similar digital currencies will be most successful in exchanges for other currencies. Mt. Gox has shown that an order-driven exchange among peers around the world is feasible. There is no reason to think Mt. Gox's clientele was financially sophisticated or particularly wealthy, even though the users probably were sophisticated in terms of computer usage, programming and some were knowledgeable about cryptography. Currently most withdrawals of local funds in a foreign country drawn on a U.S. bank account cost three percent of the amount. On Mt. Gox and similar exchanges, the cost can be dramatically less and is likely to be even smaller if more consumers participate. Remittances are very expensive. Bitcoin definitely has the capability of disintermediating banks and payments processors in such uses. Regulation raises major unresolved hurdles.

Bitcoin and similar digital currencies also are likely to undermine government's ability to generate revenue from substantial inflation. It is hard to imagine such an effect being important with inflation of one or two percent. It is quite possible the effect will be substantial in countries such as Argentina which use exchange and capital controls to keep foreign monies out and limit citizens' exchanges of local currency for other currencies. The ability to evade capital controls may well be a very important effect of Bitcoin and similar private digital currencies.

Are some countries or much of the world on the brink of the denationalization of money (Hayek 1977)? It is hard to get beyond "Maybe so, maybe not" but that is farther than a plausible conclusion could go until very recently.

References

Babaioff, Moshe, Shear Dobzinski, Sigel Oren and Aviv Zohar. 2012. On Bitcoins and Red Balloons. *Proceedings of the 13th ACM Conference on Electronic Commerce*. 56-73.

Berentsen, Aleksander. 2006. On the Private Provision of Fiat Currency. *European Economic Review,* 1683-98.

Chaum, David, Amos Fiat and Mona Naor. 1990. Untraceable Electronic Cash. In *Advances in Cryptology – CRYPTO '88* Lecture Notes in Computer Science, 403, 319-27.

Demsetz, Harold. 1968. The Cost of Transacting. *Quarterly Journal of Economics*. 82 (1), 33-53.f

Dwyer, Gerald P. 2014. Are Bitcoin Mining Pools a Natural Monopoly? At http://www.jerrydwyer.com/blog. July.

Dwyer, Gerald P., and Margarita Samartín. 2009. Why Do Banks Promise to Pay Par on Demand? *Journal of Financial Stability* 5, 147-169.

Dwyer, Gerald P. 1999. The Economics of Open Source and Free Software. Unpublished paper available at http://www.jerrydwyer.com/pdf/opensource.pdf.

Friedman, Milton. 1969. The Optimum Quantity of Money. In *The Optimum Quantity of Money and Other Essays*, pages 1-50. Chicago: Aldine Publishing Company.

Gans, Joshua S. and Hanna Halaburda. 2013. Some Economics of Private Digital Currency. Unpublished paper, University of Toronto.

Grinberg, Reuben. 2011. Bitcoin: An Innovative Alternative Digital Currency. *Hastings Science & Technology Law Journal*. 160-206.

Hayek, F. A. 1976. *Denationalisation of Money*. Second (extended) edition. London: Institute of Economic Affairs.

Hill, Kashmir. 2013. Living on Bitcoin for a Week: Bitcoin Is the Internet Applied to Money (And I Survived It). *Forbes*. May 7.

Karame, Ghassan O., Elli Androulaki and Srdjan Capkun. 2012. Double-spending Fast Payments in Bitcoin. *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, 906-917.

Klein, Benjamin. 1974. The Competitive Supply of Money. *Journal of Money, Credit and Banking* 6 (4), 423-53.

Kocherlakota, Narayana R. 1998. Money is Memory. *Journal of Economic Theory* 81, 232-51.

Lerner, Josh, and Jean Tirole. 2002. Some Simple Economics of Open Source Software. *Journal of Industrial Economics* 50 (2, June), 197-234.

Luther, William J. 2013. Friedman versus Hayek on Private Outside Monies: New Evidence for the Debate. *Economics Affairs*. 127-35.

Luther, William J. and Josiah Olson. Bitcoin is Memory. Unpublished paper, Kenyon College.

Marimon, Ramon, Juan Pablo Nicolini and Pedro Teles. 2012. Money Is An Experience Good: Competition and Trust in the Private Provision of Money. *Journal of Monetary Economics* 59, 815-25.

Martin, Antoine and Stacey L. Schreft. 2008. Currency Competition: A Partial Vindication of Hayek. *Journal of Monetary Economics* 53, 2085-2111.

Martinez-Carter, Karina. 2012. Argentina's Dollar-Sniffing Dogs. Business Week. January 12.

Meiklejohn, Sarah, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker and Stefan Savage. 2013. "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names." IMC' 13 Proceedings of the 2013 Conference on Internet Measurement, 127-40.

Minar, Nelson and March Hedlund. 2001. A Network of Peers. In *Peer-to-Peer: Harnessing the Power of Disruptive Technologies*, pp. 3-20. Edited by Andy Oram. Sebastopol, California: O'Reilly.

Nakamoto, Satoshi. (No date). "Bitcoin: A Peer-to-Peer Electronic Cash System." Available at http://bitcoing.org/bitcoin.pdf.

O'Mahoney, Donal, Michael Pierce and Hitesh Tewari. 1997. *Electronic Payment Systems*. Boston: Artech House.

Raymond, Eric. 1999. A Brief History of Hackerdom. In *Open Sources: Voices from the Open Source Revolution*. Edited by Chris DiBona, Sam Ockham and Mark Stone. Sebastopol, California: O'Reilly.

Reid, Fergal and Martin Harrigan. 2013. An Analysis of Anonymity in the Bitcoin System. In *Security and Privacy in Social Networks*, pp. 197-223.

Ron, Dorit and Adi Shamir. 2013. Quantitative Analysis of the Full Bitcoin Transaction Graph. In *Proceedings of the 17th International Conference on Financial Cryptography and Data Security.*

Ron, Dorit and Adi Shamir. 2013. How Did Dread Pirate Roberts Acquire and Protect His Bitcoin Wealth? Unpublished paper, Weizmann Institute of Science, Israel.

Selgin, George. 2013. Synthetic Commodity Money. Unpublished paper, University of Georgia.

Schneier, Bruce. *Applied Cryptography*. 1996. Second Edition. New York: John Wiley & Sons, Inc.

Sparshott, Jeffrey. 2013. Web Money Gets Laundering Rule. *Wall Street Journal*, March 22.

Wallace, Benjamin. 2011. The Rise and Fall of Bitcoin." *Wired*, November 23. Available at http://www.wired.com/magazine/2011/11/mf_bitcoin/all/1.

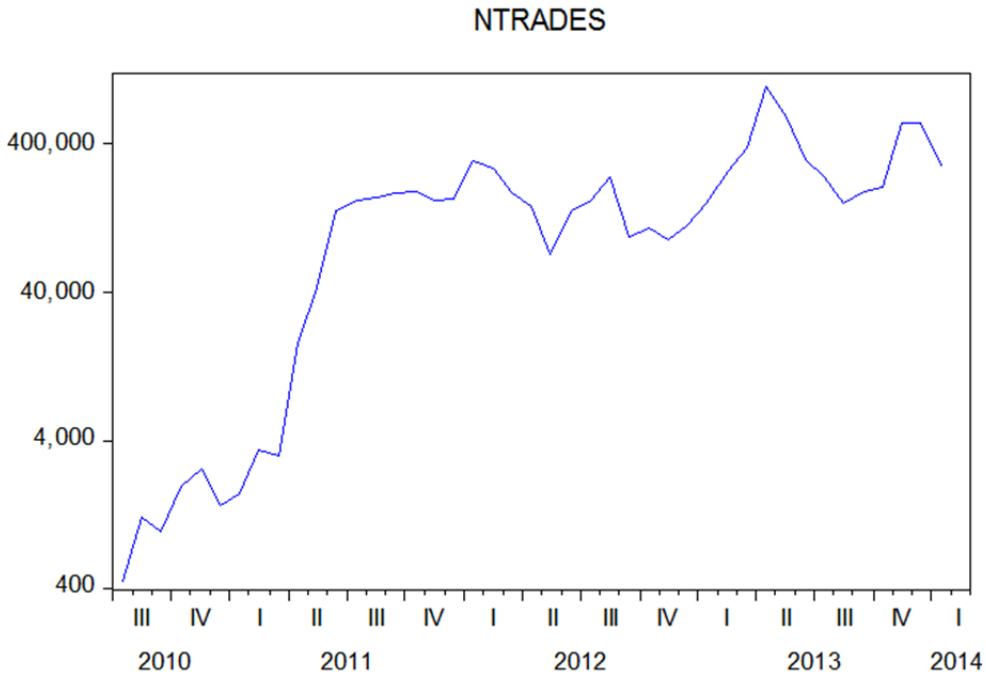
Wayner, Peter. 1997. Digital Cash. 2nd edition. London: AP Professional.

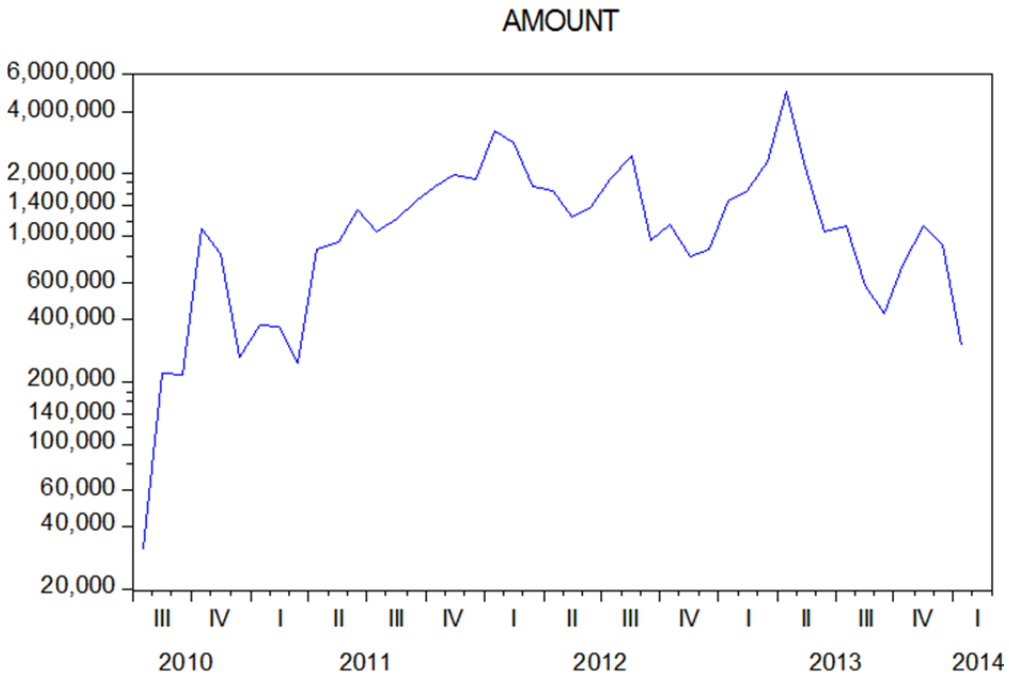
Yermack, David. 2013. Is Bitcoin a Real Currency? An Economic Appraisal. Unpublished paper, National Bureau of Economic Research.

Figure 1

Number of Trades and Number of Bitcoins Trades

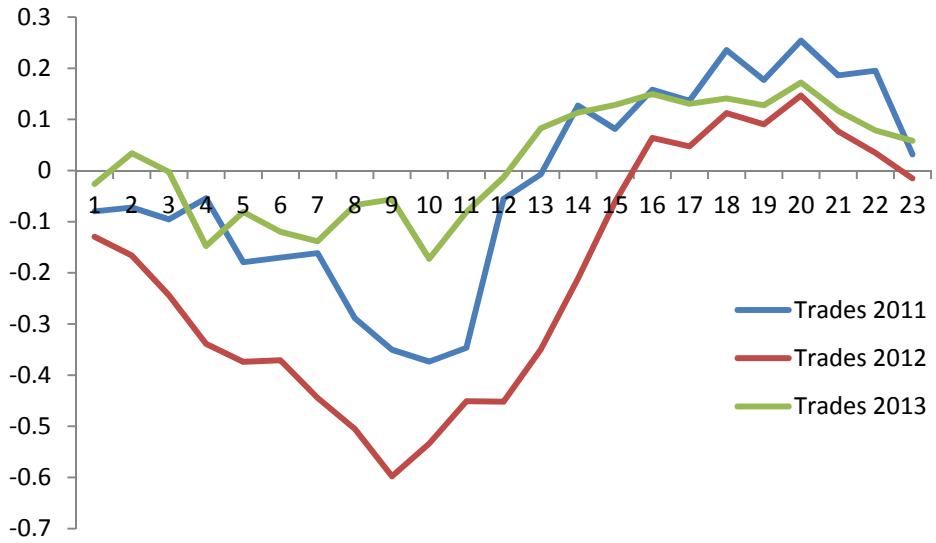
July 2010 to December 2013





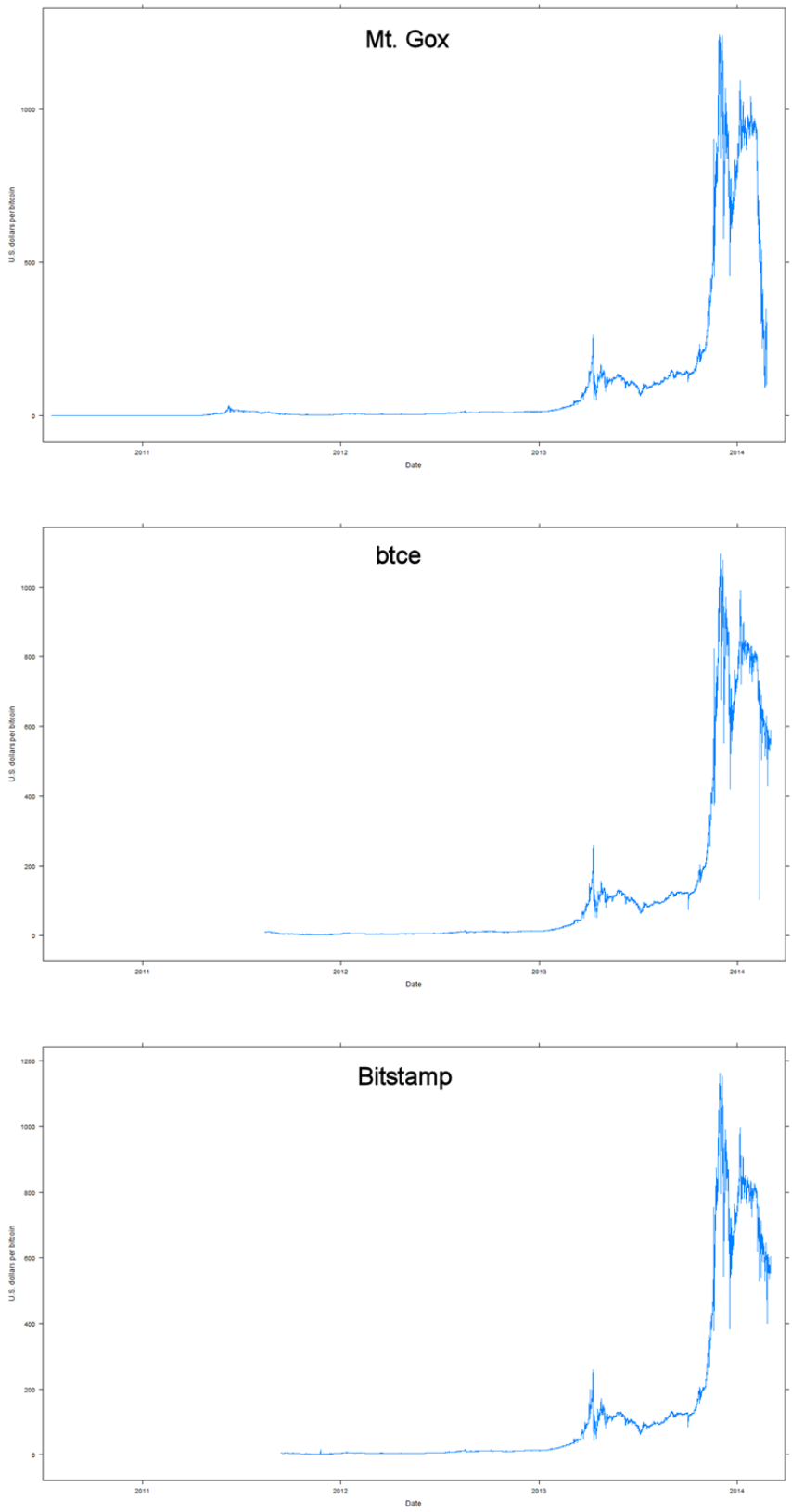
The figure shows the monthly number of trades and the number of bitcoins traded for U.S. dollars on Mt. Gox from July 2010 to December 2013. The number of trades and number of bitcoins traded increased rapidly in 2010 with the number of trades but not the number of bitcoins traded increasing in the first half of 2011 as well. The possible trend down in the number of bitcoins traded in 2012 and 2013 is concomitant dramatic increase in price over this period.

Figure 2
Trades of Bitcoins on Mt. Gox by Hour



The figure shows the regression coefficients of the logarithm of the number of trades by hour of the day. These three regressions are for the years in which Mt. Gox operated for the entire calendar year. The regressions also include dummy variables for the day of the week and for the month of the year. The hour zero is the excluded hour. The hour zero runs from midnight GMT to 12:59:59 GMT. Hence, hour 23 runs from 23:00:00 GMT to 23:59:59 GMT. Each regression includes statistically significant coefficients and some statistically insignificant coefficients at the 5 percent significance level, with coefficients closer to zero not being different than zero.

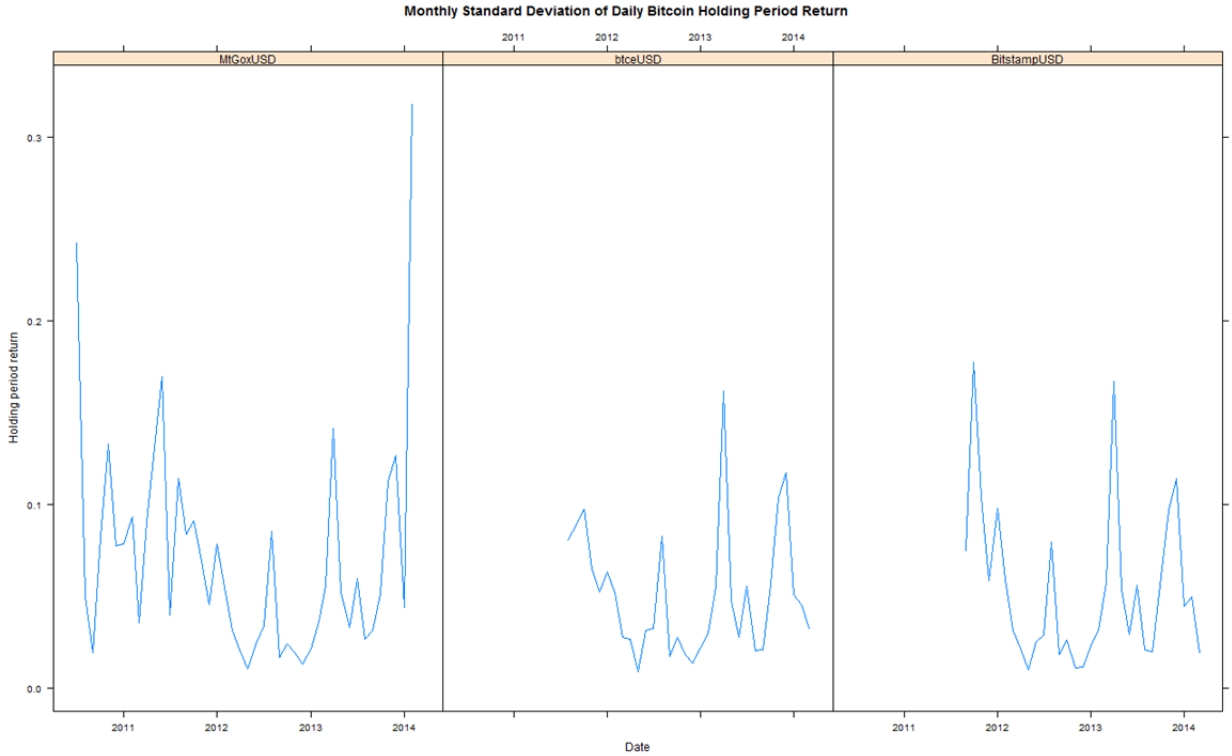
Figure 3
Prices of Bitcoins per U.S. Dollar on Major Exchanges



This figure shows prices of bitcoins for U.S. dollars for all trades on the three exchanges. The data start at the inception of trading on each exchange. They end on February 25, 2014 at 01:59:06 GMT for Mt. Gox, the last trade available. They end on 2014-03-03 close to 11:00 GMT for Bitstamp and btce.

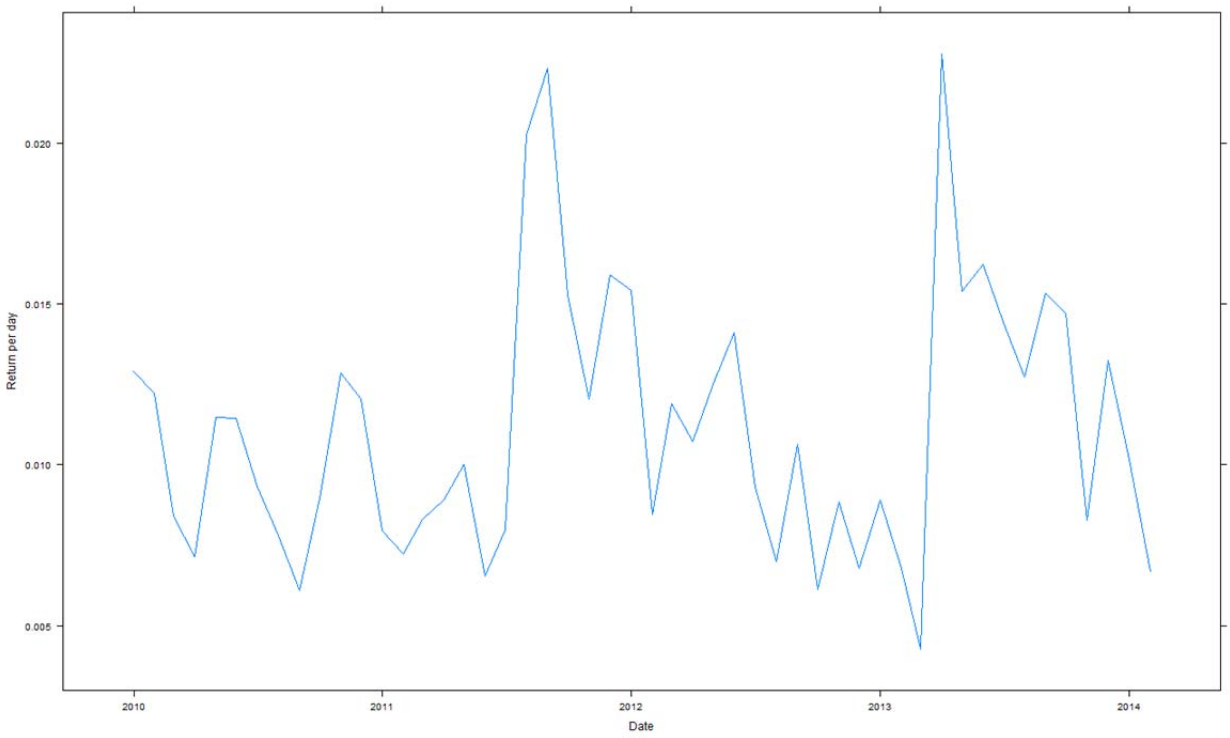
Figure 4

Monthly Standard Deviations of Daily Holding Period Returns on the Exchanges



The U.S. dollar prices in trades for bitcoins are converted to daily data using GMT with the final price in the day retained. These final prices in each day are used to compute log holding period returns for each day. The figure shows the standard deviations of these daily holding period returns for each month with a full month of trading.

Figure 5
Monthly Standard Deviation of Holding Period Returns for the Price of Gold
January 2010 to February 2014



The log holding period return on gold is computed using gold fixing prices in U.S. dollars on the London Bullion Market at 3 P.M. across days. The data are from the Federal Reserve Bank of St. Louis. Not all days are trading days; as is usual, I compute returns across weekends and holidays as a single trading day.