The Economics of Private Digital Currency

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

Abstract

Recent developments have made private digital currency possible. Any digital money must prevent users from spending their balances more than once, easier said than done with purely digital currencies. Current and recent digital currencies use peer-to-peer networks and open-source software to stop double spending. This paper explains how the use of these technologies can be equilibrium strategies. This paper also discusses the rise of 24/7 trading on a computerized market in Bitcoin, a remarkable innovation in financial markets.

October 2013

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 economic circles. Variously known as digital currency, virtual currency and crypto-currency, currency which has only a digital representation has received a great deal of attention in mainstream media and some attention from economists and lawyers (Selgin 2013, Grinberg 2012). A particular currency – Bitcoin – has received most of this attention, although there are alternatives in existence and proposed currencies such as Ripple.

There are two types of electronic money – currency and deposits. Currency can be defined in various ways. A definition that seems consistent with usage is that digital currency consists of funds that can change hands from one person to another and are evidenced by a balance that the owner of the currency keeps.[1] Deposits can be defined as money that is 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, electronic currency is not different than electronic storage of the value of deposit accounts. It is very different than electronic deposits though if something called electronic currency can be transferred without the intervention of a financial institution.

Digital currency seems to have a serious problem. Bits – digital representations of anything – are trivial to create on a computer, but bits cannot be used as currency unless they are hard or virtually impossible to reproduce. In the literature on digital money, this is known as the double-spending problem: a digital representation of money requires that it not be possible to create multiple copies and spend the same digital currency two or more times. 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.

The double-spending problem is in fact a serious problem for digital currency. 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 but the bank certifies that funds are available for the transfer. No person or institution necessarily stands behind the transfer of digital currency 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.

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

[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 the keeper of central records.
[2] A "bank" is defined as an institution which has such accounts.

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 would be 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 nominally in charge.

As with any other good, the supply and demand for digital currency is a solid basis for beginning to think about how it might work. While money has differences from other goods, the similarities are important when thinking about what might make a money successful.

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.

One other 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.[3] 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.

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. Nonetheless, prices of digital currency in various fiat monies are readily available and in fact are available for Bitcoin.

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 prices in a particular locale. In general,

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

there seems no reason to think the demand for money is different in this respect with or without digital currency.[4]

Digital currency is denominated in its own units. Starting from price levels in terms of the prices of goods and services in a particular locale, conventionally identified as a nation, the real quantity of money demanded cannot be determined independent of an 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 either. 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.

Supply of Digital Currencies

The most pressing issues concerning digital currencies are on the supply side. Besides solving the double-spending problem, there are more basic problems. 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? These questions are related to the double-spending problem. Solving the double-spending problem is necessary to create a currency with anything other than zero marginal value.

The resolution of these issues is tied up with other aspects of the digital currencies which have evolved recently. Bitcoin and at least some other digital currencies are based on peer-to-peer networks and open-source software.

A peer-to-peer network is very different from a government's fiat money. A government's fiat money is created by a single issuer, certified by the issuer and used by many.[5] 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.

A peer-to-peer network is organized as a set of nodes into a self-organizing connected network.[6] 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 it might seem that the peer-to-peer architecture is inherently more costly because it is duplicative, this need not be particularly important. Besides, a peer-to-peer network can be more resilient to attack or problems at one specific location. The nodes do not have to have the same standing. Some may be more prominent or reliable or may be online more than others.

---

[4] 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. I assume that so-called simple-sum aggregation is fine for the this discussion.

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

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

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.[7] Open-source software is similar to a peer-to-peer network in 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.[8]

Bitcoin, the most prominent digital currency as of now, is organized in particular ways, some of which are not intrinsic to digital money. It is easiest to see the organizational problems addressed in Bitcoin and then briefly examine the issues more generally.

Bitcoin was conceived by a person or persons using the pseudonym Satoshi Nakamoto.[9] 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 it.[10] In conjunction with others, this proposal was modified somewhat and eventually Bitcoins came into existence. While not its reason for being, Bitcoin may well have reached its current prominence 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).

Bitcoins are created by solution of a cryptographic algorithm by "miners." Finding the answer to the algorithm 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. This makes the supply perfectly inelastic at 21 million Bitcoins. This inelasticity of supply is viewed as an advantage by some economists and a disadvantage by others. It is worth noting that an inelastic supply is roughly in line with Friedman's solution for the optimal quantity of money (Friedman 1969). From the viewpoint of a private currency such as Bitcoin, an advantage for the currency is predictability even if a different rule for the evolution of the stock of Bitcoins would have advantages.

---

[7] 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 based on the source code include all the source code with the executable file or files.

[8] If some programmers are opposed to a decision, they have the right to take the software and develop it in their preferred direction. This "forking" of development is limited by the substantial advantages of having a common set of code for future development.

[9] 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.

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

The supply of Bitcoins increases over time until the limit of 21 million Bitcoins is reached. The increase is determined by a simple rule which attempts to halve the increase every four years (Nakamoto 2009) and generates a decreasing increase over time.

The rule for the supply of Bitcoins targets creating one block every ten minutes with a block worth a decreasing number of Bitcoins. As indicated above, Bitcoins are not created at zero marginal cost. The cost of creating Bitcoins includes the fixed cost of computing hardware and the marginal cost of computing time on that hardware including electricity plus network access. This cost might sound trivial but competition for creating Bitcoins suggests that the marginal cost will rise to equal the marginal return.

Miners solve a cryptographic problem and simultaneously maintain a record of transactions. Knowing about aspects of the cryptographic algorithm is useful for understanding why Bitcoin works. The cryptographic algorithm is used in public-key cryptography and digital signatures.[11]

Bitcoin relies on public-key algorithms and hash functions. A public-key algorithm is one in which one key encrypts a message, another key decrypts it, and neither key can be derived from the other. Two one-way hash functions are the basis for the encryption and decryption.

A one-way hash function is not invertible at high, preferably prohibitive, marginal cost. A one-way hash function H(*M*) of a message *M* with arbitrary length *m* produces the hash value *h*. 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 H(M)=h; and 3. Given M, it is hard to find another message M' such that H(M)=H(M').

Public-key cryptography is based on pairs of one-way hash functions. A private key is a key that only one person knows. A public key is a key which is not secret and can be made widely available. The system can be used for digital signatures with h computed by the private key and M computed from h by the public key, thereby verifying the sender. There is no security of the message but the sender is verified. Alternatively, a private key and a public key can be used for encrypting messages. A message can be encrypted by the public key, generating h. Then the private key known only to the recipient is used to reverse the hash, computing M from h. A common well researched hash function is used in mining Bitcoins.

Such a hash function by itself would make mining trivial. Instead, the target hash value is less than a pre-determined value, effectively requiring zeroes in initial digits' places. This target is attained by changing a one-time value in the block until the target is attained. The number of zeroes is increased to increase the number of computations necessary to solve the problem and keep the desired frequency of solution at about once every ten minutes.

[11] This reliance on results from cryptography, including that Bitcoin is the public key and private key is actual thing traded, explains why Bitcoin and similar currencies sometimes are called "crypto-currencies."

Transactions in Bitcoins are verified by databases available on the Internet. As with any electronic currency, Bitcoin would have "double spending" if no one kept track of transactions.

Bitcoin uses authentication by a peer-to-peer network to solve the double-spending problem, which is quite different than using central authentication proposed by Chaum, Fiat and Naor (1990) for example.[12] Multiple websites maintain copies of the database 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 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 cryptographic problem in the database. In addition, if someone else solves the cryptographic problem first and there no reason to think this information is little known, miners' optimal strategy is to move onto the next block. Hence, they have an incentive to update frequently and stay informed about the current unsolved problem. Furthermore, they have an incentive to make this information available to others. Each block includes the previous hash value in the newly encrypted block, which makes the blocks a chain. (Nakamoto no date)

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 CPUs on the Bitcoin network.

The website blockchain.info presents information on difficulty, estimated profitability and other statistics. The information is informative although it is difficult to determine its accuracy. The estimate of net revenue on this site indicates that mining generated negative net revenue from July 2013 to October 2013.

Issues concerning Bitcoin

What is to prevent a node from substituting a solution for a prior block, adding solutions for later blocks and having 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

[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. was anonymity of the exchange partners.

attack requires that the attacker have more than 50 percent of the computing power among miners, which is regarded as unlikely.

While mining new Bitcoins is ongoing, miners maintain 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.[13] If mining produces a number of Bitcoins falling by half every four years (Nakamoto 2009), 20.7 million Bitcoins will be produced by 2033. Whether the actual number of Bitcoins will reach this level or continue afterwards to 21 million remains to be seen. In any case, it seems that mining will continue for some time.

Who will maintain the database 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. Babaioff, Dobzinski, Oren and Zohar (2012) point out that the structure of those fees will be important for creating incentives for an equilibrium in which Bitcoins are useful.

Bitcoin is not anonymous and anonymity was not included as a design goal (Nakamoto no date). It is possible to have a digital currency with authentication which is anonymous (e.g. Chaum, Fiat and Naor 1990). While a user of Bitcoins can take steps to make his identity and 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 (Reid and Harrigan 2013). It may well be impossible. If one desires anonymous transactions, physical currency has the advantage.

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, an international exchange such Mt. Gox for Bitcoins can make it possible to move money around the globe. Any firm in the world dealing with U.S. citizens is subject to a variety of 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. 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. Bits of information about Bitcoins' use in exchanges are generated by trials such as a Forbes' columnist who lived on Bitcoins for a week in San Francisco (Hill 2013).

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

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 one is Ripple, which is similar to Bitcoin but uses transactions fee from the start to provide an incentive to authenticate transactions.[14] This avoids the loss due to imposing an artificial marginal cost of producing the currency. It does however require a solution to dividing up the initial distribution of digital currency.

Mt. Gox Exchange

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 other moneys.

This trading is rather remarkable.

The most important exchange on which Bitcoins are traded is Mt. Gox Exchange in Tokyo. Mt. Gox opened as an exchange for Bitcoin in 2010. Citizens of many countries trade Bitcoins on Mt Gox and trading is computerized. Mt Gox is an order-driven exchange on which individual post bids and offers or market orders. As a result, Mt. Gox has the potential to have trades 24 hours a day, seven days a week and it does have such trades.

Data on trades are available on the Internet. The data for the analysis in this paper starts from a trade on Mt. Gox on July 17, 2010 at 11:09 PM Tokyo Time, shortly after the beginning of trading, to May 23, 2013 at 1:12 PM Tokyo Time. These data are publicly available and provided directly by Mt. Gox.

As a first cut, I use only data on trades of Bitcoins for U.S. dollars. There are 5,205,373 trades of dollars for Bitcoins in this period. Such trades are 85 percent of all trades. This might suggest that aggregating to days based on the clock in the United States would not obscure much and might make some things clearer.

Analysis of the data provides no evidence of lulls commonly found on national exchanges in the middle of the day and at night. There is no obvious decrease in volume associated with weekends at any one place on Earth. No breakdown of the data into 24-hour days at any particular location is suggested by the data.

Because all time zones with major populations hit round hours at the same point in time, there is no reason to think that aggregation to hours is problematic. This aggregation makes it possible to produce more informative graphs despite the large number of observations.

---

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

Figure 1 shows the price of Bitcoins by trade. The early trades had quite low prices but the price clearly rose quickly. There was a brief period when the price per Bitcoin rose to $266.000 on April 20, 2013 at 12:35 PM but the price at the end of these data on May 23, 2013 at 1:12 PM was about $125.62. Clearly, there have been large swings. The lowest price in the data is one cent.

Figure 2 shows the price of Bitcoins by hour rather than by trade. After a brief initial startup, there have been trades every hour and the graph shows the price of a Bitcoin for every hour since July 17, 2010 at 11 PM. This provides a better picture of the evolution of the price in calendar time. Early on, not much happened. More recently, the price has been quite volatile.

Is this price 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 11.2 million Bitcoins on May 23, 2013, as estimated at the website https://blockchain.info. At a price of $125.62 per Bitcoin, this indicates an approximate value of Bitcoins of $1.41 billion. While not trivial, this is small compared to the value of M2 of $10.6 trillion for May 2013. Does a ratio of worldwide holdings of Bitcoins to U.S. dollars of 0.0132% 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.[15] Such appreciation may never materialize because Bitcoins will disappear. Any appreciation is likely to be limited to an unpredictable extent by competition from other digital currencies.

Conclusion

The design of Bitcoin and similar currencies does not have any inherent flaw. The finality of transactions need not depend on a central authority. Using a peer-to-peer network to finalize transactions is a major innovation. To date, details are not worked out to prove finality, at least finality of valid transactions almost surely.

Innovations to allow people to use their smartphones to transfer funds to others are coming. From the viewpoint of an end user, there is no technical difference between using dollars and Bitcoins.

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

There is a major difference in one respect. The finality of transactions in Bitcoin is not guaranteed by an institution such as a bank. While this is an advantage as viewed by some, this 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. While some monies are in fact displaced, such as the Zimbabwean dollar in recent years, this usually only occurs after dramatic inflation. It still is hard to see the U.S. dollar being replaced by Bitcoin, Ripple and other currencies for everyday transactions. Luther's interesting evidence for Somalia (2013) indicates that currency issued by a non-existent government can continue in circulation for some time.

Possibly 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 current clientele is financially sophisticated or particularly wealthy, even if it probably is sophisticated in terms of computer usage, programming, and for some, 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 smaller if more consumers participate. The major issues are regulatory.

Are we 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.

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.

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.

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.

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.

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

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.

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.

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

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

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.

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.

Figure 1

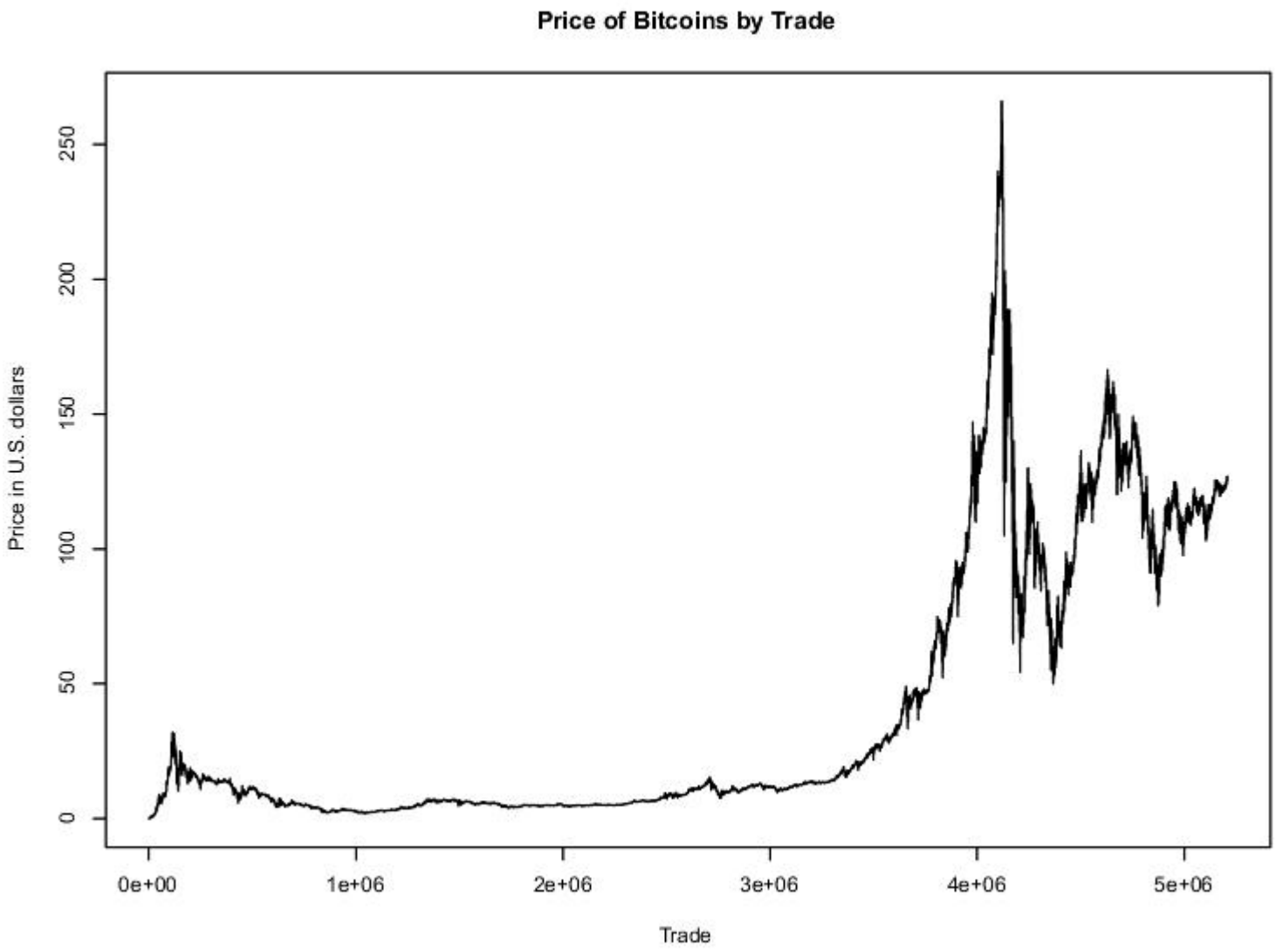
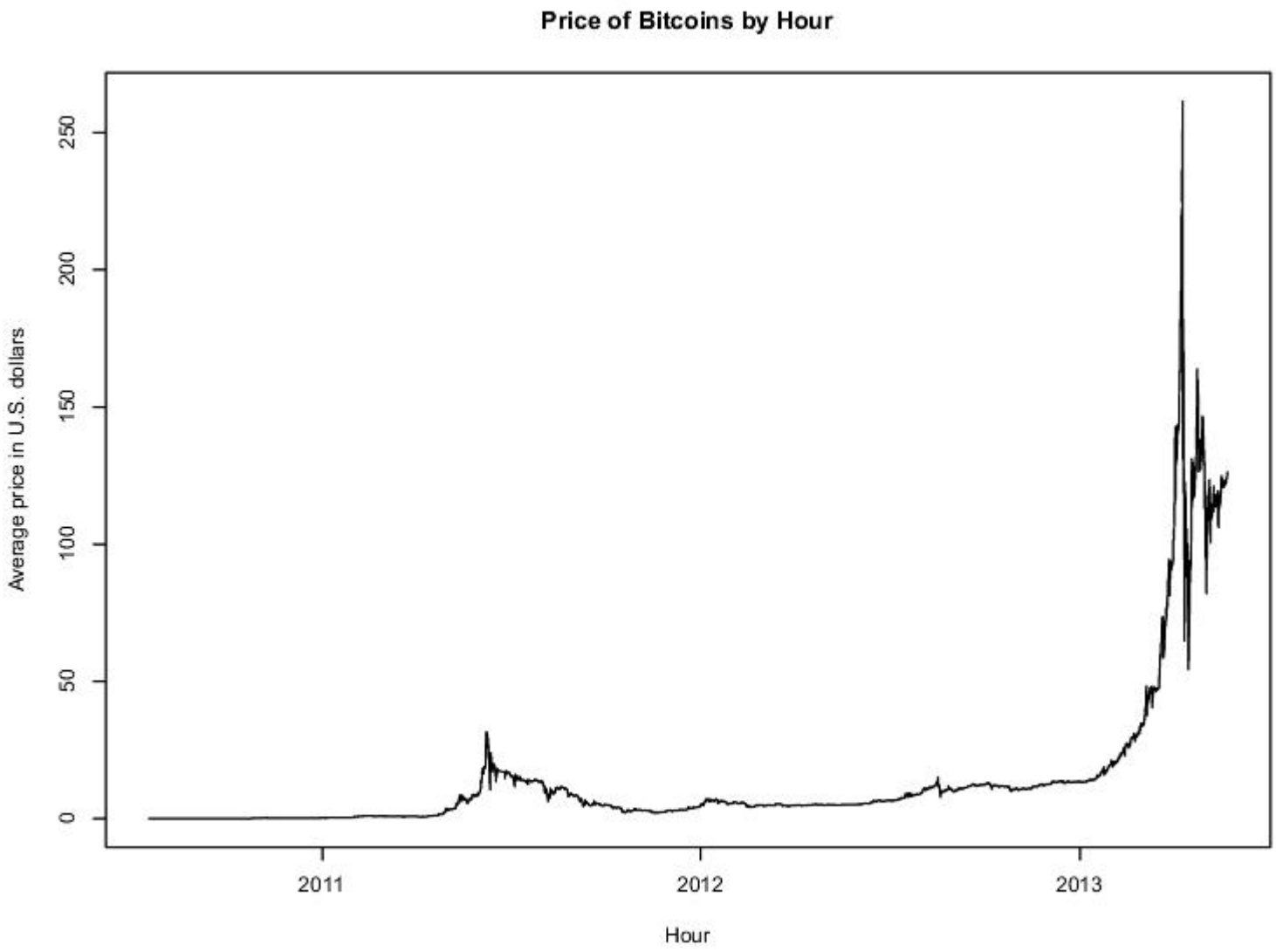

Price of Bitcoins by Trade
Price in U.S. dollars
0
50
100
150
200
250
0e+00
1e+06
2e+06
3e+06
4e+06
5e+06
Trade

Figure 2


Price of Bitcoins by Hour
Average price in U.S. dollars
0
50
100
150
200
250
2011
2012
2013
Hour