LUISS Guido Carli
LIBERA UNIVERSITA' INTERNAZIONALE DEGLI STUDI SOCIALI

DEPARTMENT OF ECONOMICS AND BUSINESS

CASMEF Working Paper Series

THE ECONOMICS OF PRIVATE DIGITAL CURRENCY

Gerald P. Dwyer

Working Paper No. 2
January 2014

Arcelli Centre for Monetary and Financial Studies
Department of Economics and Business
LUISS Guido Carli
Viale Romania 32, 00197, Rome -- Italy
http://casmef.luiss.edu

© Gerald P. Dwyer. The aim of the series is to diffuse the research conducted by CASMEF Fellows. The series accepts external contributions whose topics are related to the research fields of the Center. The views expressed in the articles are those of the authors and cannot be attributed to CASMEF.

The Economics of Private Digital Currency*

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 be equilibrium strategies in which a digital currency has a positive value. This paper also summarizes the rise of 24/7 trading on a computerized market in Bitcoin, 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.

January 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” in November 2013. Research support was provided by the Spanish Ministry of Education and Culture for support of project ECO-2010-17158.

©Gerald P. Dwyer, 2013 and 2014

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. 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 (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.

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 digital 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, electronic currency is not dramatically different than electronic storage of the value of deposit accounts other than concerns about theft. It is very different than electronic deposits though if an asset called electronic currency can be transferred without the intervention 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 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.

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 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.

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

[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.

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.

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 over time. While money has differences from other goods, the similarities are important when thinking about what might make a money successful.

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 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

[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.

or problems at one specific location. The nodes do not have to have the same standing: Some may be more prominent or reliable and some may be online more than others.

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 money. 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 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 are the owners 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 source code to the software 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

---

[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 open-source 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. Lerner and Tirole (2002) and Dwyer (1999) analyze some aspects of the economics of open-source software. There is a tendency to think of programming open-source software as a hobby. Tapscott and Williams (2008, pp. 77-88) detail IBM's participation in the development of Linux.

[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.

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 attempts to halve 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. 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" and I will follow that usage. 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 taking 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] There is a target for Bitcoin of having an increment to the block chain roughly every ten minutes and, as the number of miners increases, the difficulty is increased. Miners can change open fields in the message space to alter the hash and achieve the desired solution. The problem is solved by searching for a hash value that is small enough.

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 can participate in some of these pools as employees, who receive a fixed payoff whether or not the pool finds a small enough hash first.

Multiple nodes 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 of a bitcoin. Instead, it will be as high as the expected value of bitcoins received on finding a small enough hash, if miners are maximizing expected earnings.

The website blockchain.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, if miners can use others' resources to mine, or if a mined bitcoin is worth more to a miner than a purchased bitcoin. That said, Blockchain.info's method for computing net revenue is important for understanding what their estimate implies.

Wallets

Public-key cryptography is essential for recording transactions and keeping track of the balance held by any individual.

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

The evidence of ownership of bitcoins is entirely in the block chain. Holders of bitcoins use "wallets" to keep track of their balances and 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 relies on private and public keys to encrypt and decrypt messages and this is crucial for verifying whether a transaction is valid.[9] 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.

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 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 to obscure the trail.[10]

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 than using central authentication proposed by Chaum, Fiat and Naor (1990) for example.[11] Multiple websites maintain copies of the block chain and update their copies by making copies from other nodes on the network.

---

[9] 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.

[10] 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.

[11] 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

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 fast 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 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 current unsolved problem. Furthermore, they have an incentive to make this information available to others.[12]

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, different new blocks are added to 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

---

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.

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

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.[13] 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 (Reid and Harrigan 2013). It may well be impossible. If one desires anonymous transactions, physical currency has the advantage.

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.

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, there seems no reason to think the demand for money is different in this respect with or without digital currency.[14]

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. 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.

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

[14] 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 this discussion.

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.[15] 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 relationship between mining and maintaining the block chain.

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 and 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. In one sense, there are no directly applicable theoretical results because the theoretical literature has focused on private currency created with zero marginal cost. The production cost is irrelevant once bitcoins have been produced because those costs are sunk. Hence, theoretical results are applicable, leaving aside the important issue of maintenance of the block chain after mining ceases. 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.[16] Knowledge of the quantity produced is a commitment device in their setup.

The possibility of entry is not addressed in the paper by Marimon et al. and other papers. 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 and the proposed currency Ripple has 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.

---

[15] 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.

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

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.

The liquidity of exchanges of a digital currency for other digital currencies or physical currencies is the most plausible differentiating factor. As for stocks in which exchanges become dominant due to liquidity on the exchange (Demsetz 1968), the liquidity of the currencies may become a very important factor in determining their relative use. This characteristic suggests that a solution with the value of digital currency positive is possible but far from 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.[17] If mining produces a number of Bitcoins falling by half every four years (Nakamoto 2009), 20.7 million Bitcoins will be produced by 2033.[18] Whether the actual number of Bitcoins will reach this level or continue afterwards to 21 million remains to be seen. In any case, mining will continue for some time.

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. It currently is possible to collect such fees but they are unimportant in practice. 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.

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. 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.

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

[18] The geometric decrease in the number of bitcoins produced means that the number produced would approach zero only asymptotically if the marginal cost of producing bitcoins were zero.

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).[19]

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.[20] 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.

---

[19] There are a few papers analyzing transactions (Meiklejohn *et al.*, 2013; Ron and Shamir 2013a, 2013b.) Unfortunately they cannot provide light on the other side of Bitcoin trades.

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

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 around the world 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.

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 12.3 million bitcoins on January 29, 2014, as estimated at the website https://blockchain.info. At a price of $909 per Bitcoin, this indicates an approximate value of Bitcoins of $11.2 billion. While not trivial, this is small compared to the value of M2 of $11.0 trillion for December 2013. Does a ratio of worldwide holdings of Bitcoins to U.S. dollars of 0.10% 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.[21] 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.

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

[21] 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 in January 2007. These primarily were clearing balances maintained by banks. The value of all bitcoins was $11.2 billion on January 29, 2014 which is large – about 1.28 times this value of reserves in the Federal Reserve. Given the early stage of development of Bitcoin, this seems large if bitcoins ultimately are useful only for trading between other currencies. On the other hand, bitcoins are not useful only in the United States and $11.2 billion of bitcoins may be small relative to reserves weighted by holdings of bitcoins and possible future use.

Mt Gox illustrates 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, the cost to transfer funds from one account to another through a digital exchange and a digital currency is less than the current cost of obtaining foreign exchange.[22]

In addition, Bitcoin can be used to avoid currency controls instituted by national governments. While currency controls can prevent citizens from using exchanges such as Mt. Gox, they cannot effectively prevent people from trading local currency in the country for bitcoins and trading the bitcoins for foreign exchange in another country. The end result is a decrease in the demand for the local currency and an increase in its price level, eroding the government's revenue from inflation. While hardly zero marginal cost, the marginal benefit to the purchaser can be substantially greater than the marginal cost.[23]

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 inherent flaw. The fixed, final quantity is an interesting alternative to the alternatives. One alternative rule is to set the quantity of money as governments do, following procedures but with substantial discretion and associated uncertainty about long-term values of their monies. Another alternative rule would be to have the money redeemable, but this redemption requires a reputational equilibrium even so for the money to have a positive value. The fixed, final quantity does mean that the price is allowed to vary, instead of being fixed relative to a redemption value.

Is bitcoin too arcane for the typical holder of money? 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.

[22] Some source claimed that U.S. banks don't offer foreign-denominated accounts due to regulatory pressure.
[23] Physical currency not only has the problem of bulk but Argentina reportedly was able to train dollar-sniffing dogs to foil imports of dollars from Ecuador.

There is a major difference between Bitcoin and deposits in banks 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.

More importantly, most people seem to prefer to have their assets and liabilities denominated in the same currency. This hedges some risk, which is not trivial given the volatility of exchange rates. While some countries' 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.

Bitcoins and similar digital currencies may 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 though the users probably are sophisticated in terms of computer usage, programming and some in 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.

Bitcoins and similar digital currencies also are likely to undermine government's ability to generate revenue from inflation taxes. I am dubious that such an effect will be important with inflation of one or two percent but 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.

It might seem that Bitcoin and similar currencies are too technically sophisticated for many low-income countries, such as Zimbabwe. The rise in Africa of money transfers using mobile phones suggests such a difference for low-income countries easily could be over-stated.

A major issue concerning Bitcoin and other private digital currencies is the volatility of their values. If Bitcoin were redeemable in something else of value, fluctuations in the value of bitcoin would be limited by an estimate of the probability of redemption. Bitcoin substitutes inelastic supply for the perfectly elastic supply with redemption (if the probability of non-redemption is ignored). Some of the implications for the volatility of the value of bitcoins are obvious and some are not. I currently am working on this issue.

Are we on the brink of the denationalization of money (Hayek 1977)? It is hard to get beyond "Quite possibly" 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*. 84 (1, February), 33-53.

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.

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

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.

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.

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. *Proceedings of the 2013 Conference on Internet Measurement*. New York: Association for Computing Machinery.

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.

Ron, Dorit, and Adi Shamir. 2013a. Quantitative Analysis of the Full Bitcoin Transaction Graph. In In *Financial Cryptography and Data Security*, edited by Ahmad-Reza Sadeghi, pp. 6-24. Proceedings of the 2013 Financial Cryptography Conference. Lecture Notes in Computer Science, volume 7859. Berlin: Springer-Verlag.

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

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.

Tapscott, Don, and Anthony D. Williams. 2008. *Wikinomics: How Mass Collaboration Changes Everything*. Expanded edition. New York: Portfolio.

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

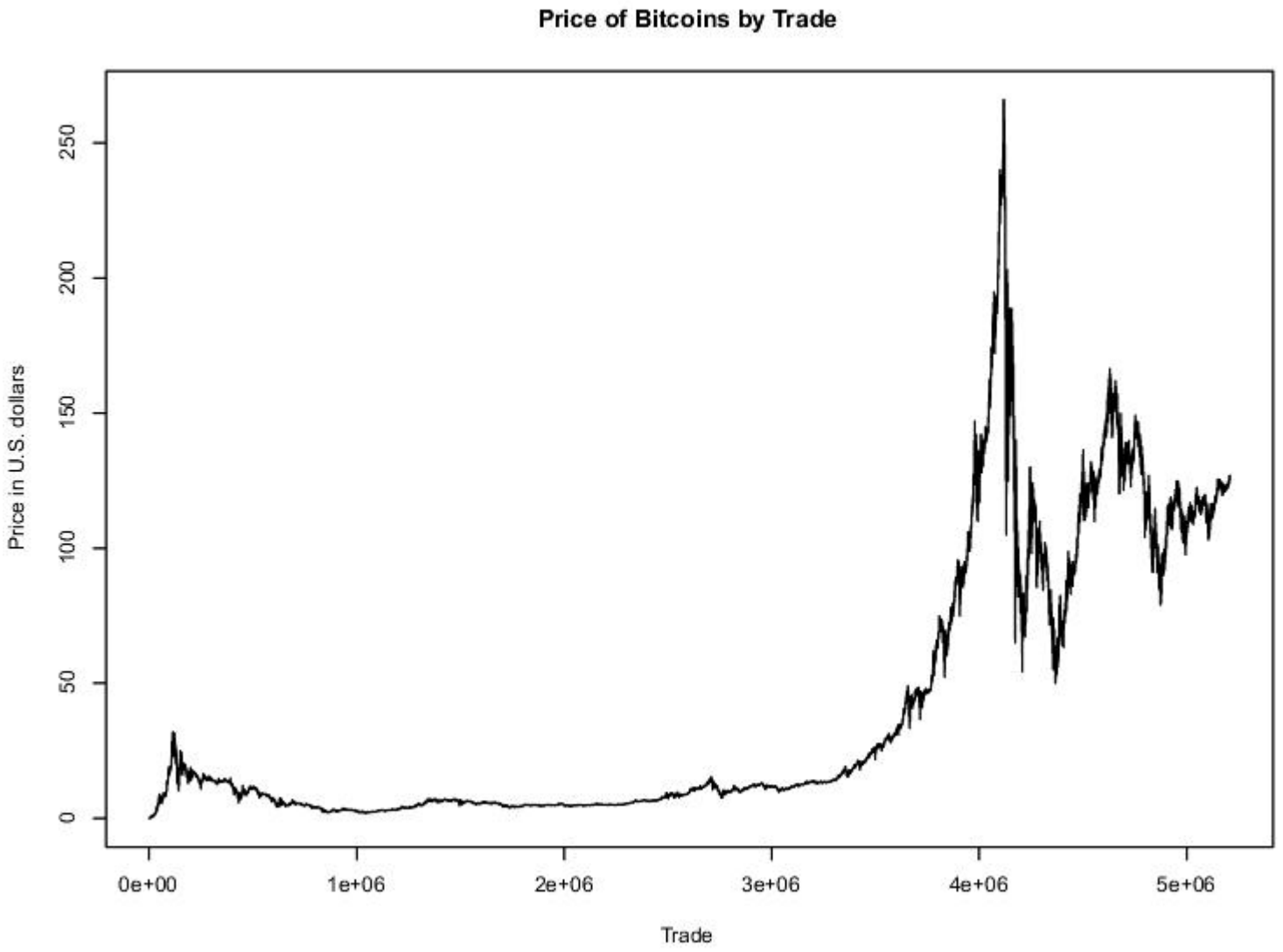
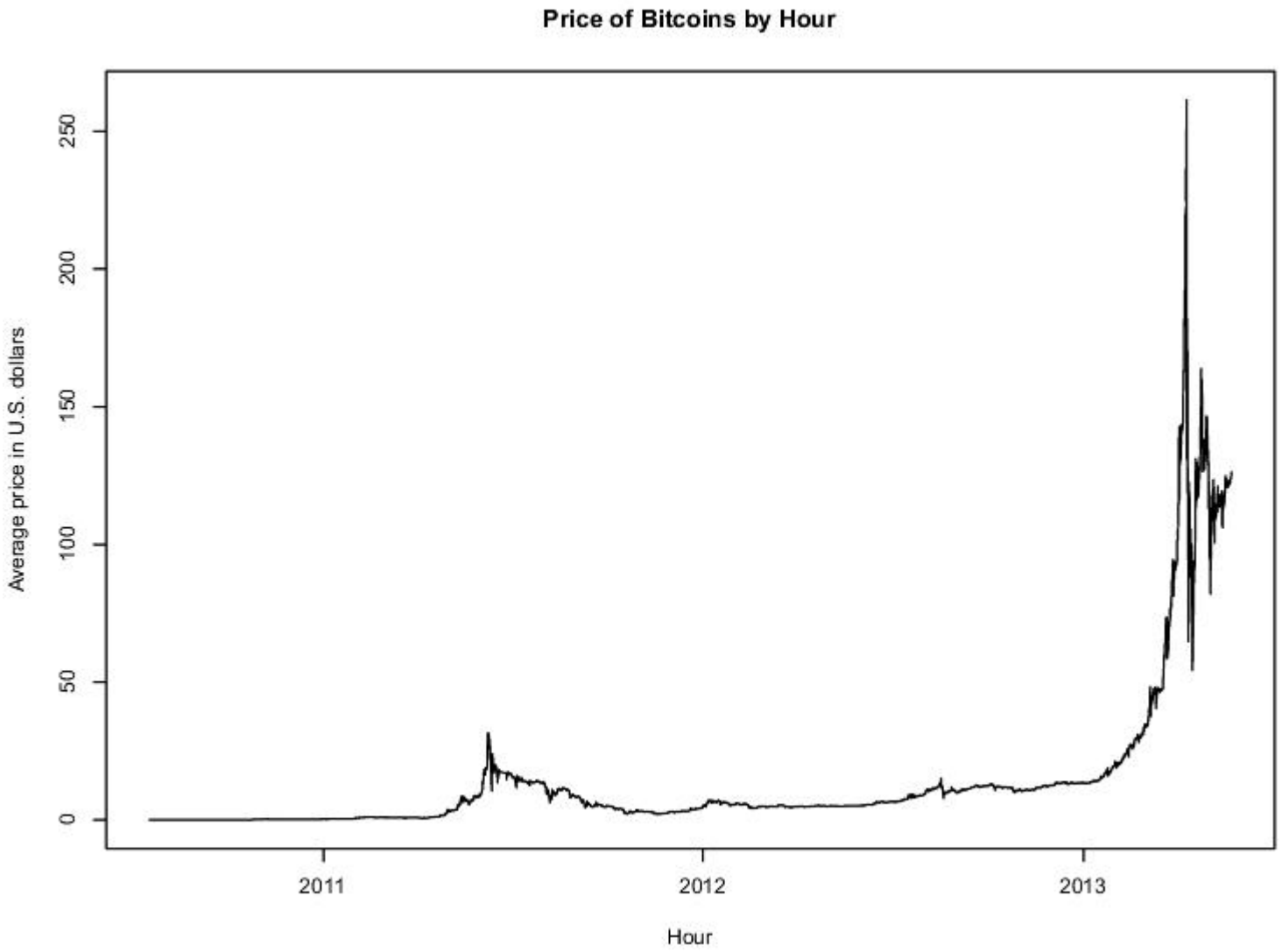

Price of Bitcoins by Trade
Price in U.S. dollars
0
50
100
150
200
250
0e+00
1e+06
2e+06
3e+06
4e+06
5e+06
Trade

Figure 2


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