Discussion Paper Series A No.617

Can We Stabilize the Price of a Cryptocurrency?: Understanding the Design of Bitcoin and Its Potential to Compete with Central Bank Money

Mitsuru Iwamura
(Graduate School of Commerce, Waseda University)
Yukinobu Kitamura
(Institute of Economic Research, Hitotsubashi University)
Tsutomu Matsumoto
(Faculty of Environment and Information Science,
Yokohama National University)
and
Kenji Saito
(Keio Research Institute at SFC, Keio University)

November, 2014

Institute of Economic Research
Hitotsubashi University
Kunitachi, Tokyo, 186-8603 Japan

Can we stabilize the price of a Cryptocurrency?: Understanding the design of Bitcoin and its potential to compete with Central Bank money

Mitsuru Iwamura, Yukinobu Kitamura,
Tsutomu Matsumoto and Kenji Saito*

October 25, 2014

Abstract

This paper discusses the potential and limitations of Bitcoin as a digital currency. Bitcoin as a digital asset has been extensively discussed from the viewpoints of engineering and security design. But there are few economic analyses of Bitcoin as a currency. Bitcoin was designed as a payments vehicle and as a store of value (or speculation). It has no use bar as money or currency. Despite recent enthusiasm for Bitcoin, it seems very unlikely that currencies provided by central banks are at risk of being replaced, primarily because of the market price instability of Bitcoin (i.e. the exchange rate against the major currencies). We diagnose the instability of market price of Bitcoin as being a symptom of the lack of flexibility in the Bitcoin supply schedule - a predetermined algorithm in which the proof of work is the major driving force. This paper explores the problem of instability from the viewpoint of economics and suggests a new monetary policy rule (i.e. monetary policy without a central bank) for stabilizing the values of Bitcoin and other cryptocurrencies.

Key words: Bitcoin, Cryptocurrency, Currency competition, Friedrich A. Hayek, Proof of work.

JEL classification: B31, E42, E51

*Mitsuru Iwamura is a professor at the Graduate School of Commerce, Waseda University (Address: 1-6-1 Nishi Waseda, Shinjuku-ku, Tokyo 169-8050, Japan) Yukinobu Kitamura is a professor at the Institute of Economic Research, Hitotsubashi University (Address: 2-1 Naka, Kunitachi-shi, Tokyo 186-8603, Japan), Tsutomu Matsumoto is a professor at the Faculty of Environment and Information Sciences, Yokohama National University (Address: 79-7 Tokiwadai, Hodogaya-ku, Yokohama, Kanagawa, 240-8501, Japan) and Kenji Saito is a visiting senior researcher at Keio Research Institute at SFC, Keio University (Address: 5322 Endo, Fujisawa-shi, Kanagawa, 252-0882, Japan). Address correspondence to kitamura@ier.hit-u.ac.jp

1. Bitcoin as a virtual registry system

Circulation of Bitcoin [1] as digital asset is guaranteed by authentication process between traders. This process consists of both an asymmetric key cryptosystem and by competition between coin-releasing 'miners' who validate transactions to prevent double spends by traders. It is important to recognize that it is operationally feasible for traders to authorize transactions by means of a digital signature, based on a asymmetric key cryptosystem. It is by far more difficult to validate transactions of Bitcoin, or other digital assets, whilst preventing double spending of assets. For paper money and checks anti-counterfeit technology, such as holograms and signatures, prevents forgery. But the state of digital assets never deteriorates and it is not a simple task to identify a genuine transaction from a forged one.

Many electronic securities and electronic money systems employ either a centralized (a node with hub function) trading system or an IC card system with secret key that prevents such doubled spending. The former system requires a centralized administration with a reasonable governance structure. The latter system requires an IC card operation. These systems may transfer incidents of regulation and other institutional risks to the owners of digital assets.

In Bitcoin the validation of transactions (preventing double spending) is made possible by sharing the virtual registry book that contains all information on transactions and ownership of Bitcoin. The virtual registry book is always open to every participant, so any double spend is easily identified. Bitcoin gives the impression that it is a set of independent gold-like coinage assets with its co-option of 'mining' and 'coin' phrases. But Bitcoin more closely resembles a real estate register or record in which the new owner of each lot of real estate is recorded whenever a new transaction is taken place. This virtual real estate register record contains 21 million lots (i.e. 21 million

[1] In this paper, we refer to Bitcoin as either a software package that can buy and sell Bitcoin or an operational system under which miners are voluntarily involved. It does not necessarily reflect the original idea of Satoshi Nakamoto (2008).

BTCs) before sub-dividing[2]. To issue Bitcoin is to attach an ID number to each BTC lot, a settlement BTC is to replace an ID number by new number[3].

As of July 20, 2014, 13.04 million BTCs have been issued in the market with ID numbers (about 62% of 21 million BTCs). Roughly every ten minutes, 25 BTCs are being issued with new IDs. This procedure of new issue is implemented as a reward for the first person/group to validate transactions without double spends that have been collected in a block. This is a competition of validation via computation, with the aim of solving a specific mathematical problem[4]. This computation is described as mining, and those who conduct mining are miners. The speed of new issue of Bitcoin on the register record is set to be halved in every four years. At the beginning of the Bitcoin system in January 2009, the reward was 50 BTCs per ten minutes, it was halved to 25 BTCs per ten minutes on November 25, 2012. It remains the same reward per ten minutes till now[5]. It will be halved to 12.5 BTCs per ten minutes in around November 2016, and this halving process will continue until 2140 when new issue of BTC will be terminated. Total circulation of BTC will be fixed at 21 million BTCs.

There are differences between a real estate registry system and the Bitcoin system. In Japan, for instance, the real estate registry system is maintained and administered solely by the Legal Affairs Bureau. The real estate register record is kept exclusively by the Legal Affairs Bureau and the public is only allowed to read the record. In contrast, the virtual registry book that contains all information on Bitcoin transactions and ownership is maintained individually among participants. This decentralized nature of virtual registry

[2] The minimum unit of BTC is not 1 BTC, but it can be divided into $1/10^8$ units of BTC.

[3] In fact, settlement is made over (multiple) part of lots that can only be identified as quantities. But we believe that this metaphor by a real estate register record captures an essence of BTC trading.

[4] We will discuss this problem in detail in Section 2.

[5] Four years after January 2009 must be January 2013. The actual event seems to happen quicker than the original statement. This is due to the program that sets a reward to be halved in every 210 thousand BTC block extensions, i.e. a mining reward is halved not by calendar, but by the block extension numbers. In section 2, the meaning of block extension is fully explained.

book-keeping activity may create some inconsistencies among participants. In the Bitcoin protocol, when an identical Bitcoin segment is used twice for different payments –leading to a Bitcoin segment having two branches (double spends) - the majority decision rule is used to determine which payment is genuine. The advantage of majority decision rule is to solve a deadlock situation in which two parties disagree with each other. However, as Eyal and Sirer (2013) argue, the majority decision is not enough to protect against selfish mining pools that command less than 1/4 of the resources, given the delayed finality confirmation structure[6].

To be more precise, the Bitcoin protocol authenticates a genuine Bitcoin registry book in which a block-chain, after branching, extends the longest[7]. This decision rule works due to the delayed finality confirmation structure. We will discuss this in the next section.

The book-keeping method of ownership transaction is not restricted to a type of real estate registry system in which the ownership of each segment is recorded. Deposit account data in a banking system keeps transaction and balance records for individuals; in Bitcoin phrasing, this is equivalent to the number of segments the deposit account holder has previously used and can currently use. The advantage of this method is that it allows the management of a large number of segments with a relatively small number of accounts[8]. The reason why the Bitcoin protocol employs the real estate-like registry system, rather than the bank deposit-like account system is probably because Mr. Nakamoto and his collaborators think that it is suitable for decentralized processing.

The Bitcoin protocol uses a hash value of a beneficiary's public key as its ID number. A hash value is a sort of digest of original data, which is

---

[6] Eyal and Sirer (2013) illustrates that Bitcoin's mining algorithm is not incentive compatible, and that the Bitcoin ecosystem is open to manipulation, and potential takeover, by miners seeking to maximize their rewards (p.15).

[7] According to Nakamoto (2009), the system is supposed to authenticate the longest block-chain, in practice, however, the chain whose "total difficulty" is the greatest prevails.

[8] For example, in case of ten trillion yen deposits by 1000 million people, it can be possible to keep the ownership records of each yen, it may require a very large computational and maintenance costs. Design of such a system is far more complex than a bank account type of record keeping.

obtained after a designated calculation process by some specific algorithm (we will come back to this later). By using a hash value as an ID number, together with a public key itself, the Bitcoin protocol is able to maintain anonymity with as well as trustworthiness of trade. The Bitcoin protocol recommends owners utilize asymmetric key cryptography[9].

2. Miners' important, exhausting role

The essence of the Bitcoin protocol is its structure that guarantees the uniqueness of the segment information 'registry book'. This confirmation process broadly corresponds to one provided by the centralized payment system in the case of traditional banking. The Bitcoin protocol validates all transactions by means of open competition among profit seeking miners as described above. This whole process is referred to as confirmation in the Bitcoin protocol.

The winner of the open competition provides the hash value as a stamp on the registry book, marking a validation of the trades in the specific block. At the same time this winner receives newly created Bitcoin, and is recorded as the owner of such in the registry book. This process is called mining. In this paper we distinguish the *confirmation* process in which all mining activities are involved from the *validation* process in which the winner of competition provides the hash value as a stamp on the registry book.

Miners play an important role in the validation of Bitcoin transactions that guarantees the uniqueness of the registry book. We call them miners because they are not a trusted third party that is assigned to prevent double spend events, but are voluntary participants seeking for a reward from the open competition of validation. Only the winner receives Bitcoin in reward, all other miners receive nothing

[9] See https://bitcoin.org/en/protect-your-privacy.

and must pay their mining costs. This is perhaps a cruel system from the viewpoint of miners.

This competition of validation is open every (about) ten minutes. Trades collected by a miner before such ten minute intervals form a block. After the validation, a new block is added to the existing blocks – a process called extending a block chain. Newly created Bitcoin received as a reward for validation can be used for payment after reasonably long block chains are extended (i.e. long enough to prevent disputes over double spends)[10]. The Bitcoin protocol employs a delayed finality confirmation structure in which Bitcoin cannot be used immediately after a transaction from the other party, even after validation of transaction is made. This structure is quite different from the centralized payment system employed by the banking sector.

The Bitcoin protocol sets a variable difficulty of computation factor, to be solved by the miners in approximately ten minutes. When the miners' computation speed becomes faster (i.e. less than ten minutes), a parameter that determines a difficulty of computation is reset to make a block chain interval approximately ten minutes[11].

This delayed finality confirmation structure is regarded as a weakness of the Bitcoin system from alternative cryptocurrency creators' point of view. However, there certainly exists a trade-off between approaching real-time finality and increasing risk in alterations of validated transactions.

Let us clarify the validation process in the Bitcoin protocol. This is a block chain extension process after confirming finality in all past transactions:

(1) The hash value[12] h_0 in the immediately previous block,

---

[10] Bitcoins transferred between users can conventionally be used after 6 block-chain extensions (about one hour later) Generated bitcoins and transaction fees as a reward for a block-chain extension (we will discuss this later) can only be used after 100 block-chain extensions (about 17 hours later).

[11] This parameter adjustment is based on the algorithm for the Bitcoin protocol. The algorithm examines the speed of new block is created in every 2016 block extensions (if one block is created in ten minutes, 2016 blocks are equivalent to two weeks) and makes parameter adjustment.

[12] According to Wikipedia, a hash function is any function that can be used to map data of arbitrary size to data of fixed size, with slight differences in input data producing very big

(2) The hash value q included in all transactions in the current block,

(3) Search for a value r that satisfies certain conditions, and

(4) New hash value h_1 is generated from three inputs (h_0,q,r). This new hash value h_1 is used as a validation stamp on the virtual registry book (see Figure 1 for illustration).

In the Bitcoin protocol, h_0 and q are exogenously given (these figures depend on the past history of trades), and miners have to search r to satisfy the condition $h_1 \leqq t$ (target). This exercise is called the proof of work. This concept of proof of work comes from Dwork and Naor (1992). They provide a computational technique for combatting junk mail and controlling access to a shared resource. Their main contribution is requiring a user to compute a moderately hard, but not intractable, function in order to gain access to the resource, thus preventing frivolous use. In the Bitcoin system, this concept is used to give confirmation of the transactions via the mining competition. In exchange the winner of the competition receives a reward. This incentive mechanism is the most innovative part of the Bitcoin system and it works well.

3. Proof of Work or Proof of Waste?

Let us clarify the meaning of the problem the Bitcoin protocol imposes on the miners. The problem is "to search x to satisfy the condition $h_1 \leqq t$ (target in 256 bit) where the hash value h_1 is generated from (h_0, q, x). Put solution x as r." If we do not impose any restriction on r (that is, t=2^{256}-1), any number would satisfy the problem. If we set t to be small, a probability of finding r in the hash

differences in output data. The values returned by a hash function are called hash values. A cryptographic hash function is a hash function which is considered practically impossible to invert, that is, to recreate the input data from its hash value alone. A hash algorithm turns an arbitrarily-large amount of data into a fixed-length hash. The same hash will always result from the same data, but modifying the data by even one bit will completely change the hash. Bitcoin uses the SHA-256 hash algorithm to generate verifiably "random" numbers in a way that requires a predictable amount of CPU effort.

function would drop sharply[13]. If the difficulty (as measured by parameter n) of this problem goes beyond a certain point, any standard personal computer cannot find a solution within a certain period of time (ten minutes in this case).

This implementation differs from the original design by Nakamoto (2008). The original design states that “to search a hash value h_1 obtained form (h_0, q, x) whose first n bit is zero. Put solution x as r.” In this design, a difficulty parameter n for the proof of work can be adjusted, but allows only for a discrete change. The current design is superior and encompasses the original design[14].

The original design of Nakamoto is intuitive, a description of which follows. Note, in this paper, we use t and n interchangeably since $t=2^{256-n}-1$.

The difficulty parameter n becomes a very useful operational instrument.

(1) If n is reasonably smaller than 256, search value r, given h_0 and q, can exist almost infinitely.

(2) If n grows gradually larger from zero, a probability to find a serch value r becomes very small and ultimately closer to zero.

By adjusting the difficulty parameter n, together with exogenous technological change and miner entry and exit, the speed of a block formation can be controlled. Parameters t or n enable the speed of block formation to stay more or less constant at ten minutes.

As is clear from the above discussion, a choice of parameter t or n in the proof of work depends on computational power technological change and the numbers of miners[15]. The impact of technological

[13] If r is any arbitrary number in 256bit and the hash function used in this protocol can generate an ideally uniform random diffusion, the probability would be about $1/2^{256-\log_2 t}$. Actual protocol is a bit more complex, r is called nonce in 32 bit value, q would change when a miner obtains bitcoins as a reward, the hash function (SHA-256) could generate an identical output from different inputs with a very small probability, actual probability would be a little bit smaller than $1/2^{256-\log_2 t}$.

[14] The original design of Nakamoto allows select a real number t such that $\log_2 t$ generates an integer. In the current Bitcoin protocol allows to select any real number for a difficulty parameter.

[15] Due to the characteristics of hash function in the proof of work problem, a number of trades

change is intuitive: if the computational power doubles, difficulty of the problem must double: *n* must shift to *n+1*. The impact of number of miners is basically similar, but more important in practice as it is more likely the number of miners will double than would computational power.

Let us further elaborate upon the issues related to the proof of work. The essence of this issue is that to we may assume a miner's probability of finding a solution to some arbitrarily large number of calculations is independent even if there are reasonable numbers of miners. Let us assume a miner's rare event of finding some *r* that satisfies the required conditions within a ten minute interval is set to probability λ (provided all miners have the same computational power), and M miners participate in the mining competition, the probability of no miner finding *r* within an interval is given as $(1-\lambda)^M$, the probability of a miner finding *r* within an interval is $1-(1-\lambda)^M$. We also assume that a probability of such a rare independent event follows the Poisson distribution. Then an average waiting time for such a rare event is an inverse of the probability of event,

$$\theta = \frac{1}{1-(1-\lambda)^M} \tag{1}$$

Transforming eq.(1),

$$\theta = \frac{1}{\sum_{i=0}^{M}(-1)^i {}_M C_i \lambda^i} = \frac{1}{M\lambda + \sum_{i=1}^{M}(-1)^i {}_M C_i \lambda^i} \tag{2}$$

i is the number of miners who experience events (i=0,1,2,…), λ is a very small number compared with M, the second term in the denominator can be ignored, then we can simplify eq.(2) as such,

$$\theta \fallingdotseq \frac{1}{M\lambda} \tag{3}$$

in a block does not matter with *n* or *t*. If trades use some divisions or mergers of bitcoin segments within a block, the validation process could be a bit more complex although calculation burden does not increase much. It is true that transaction fees are paid to the miners with such additional calculations are involved. A share of transaction fees in the miners' rewards is very small (see https://en.bitcoin.it/wiki/Transaction_fees).

Furthermore, let us assume the average computational power of miner within an interval is set constant K. By construction of the hash function, K must be reasonably small compared with 2^{256-n},

$$\lambda \fallingdotseq \frac{K}{2^{256-n}} \tag{4}$$

Put $K/2^{256}=k$, eq.(4) becomes

$$\theta \fallingdotseq 2^n/kM \tag{5}$$

That is to say, the average time of a block validation (the average waiting time for the miner to find r)

(1) increases as difficulty n for the proof of work at the speed of 2^n.

(2) decreases in inverse proportion to the number of miners M and

(3) decreases in inverse proportion to the computational power.

These are the basic determinants of Bitcoin productivity.

The difficulty parameter n for the proof of work was 32 in January 2009, raised to 40 in December 2009, raised to 62 in December 2013, and is 64 as of June 2014. These changes cannot be explained by increases in computational technological change, but must reflect the fact that many new miners entered in mining competition by the end of 2013 and they almost stopped after 2014.

These observations hint at the nature of proof of work as the core concept of the Bitcoin system. As shown above, difficulty parameter n is nothing to do with the quality of validation of a block. That's why n can be raised and reduced flexibly without affecting a validation process. That is, the proof of work is not an issue in maintaining the quality of Bitcoin, but is the cost to maintain a steady speed of new issues of Bitcoin (at the moment, it is 25 BTCs per about ten minutes). In order to evaluate the nature of proof of work, this role must be examined. The role is properly carried out, it would be considered reasonable. Otherwise it would not be the proof of work, but it would be the proof of *waste* because it would be a mechanism to provide rewards for the mining competition with excessively large computational cost.

It is essential the Bitcoin system provides an incentive for those who contribute to the maintenance of the system. In case of standard electronic money, an issuer of electronic money receives participation fees directly from the retail shops; they are paid not by the electronic money they issue, but by central bank notes. Central banks themselves pay maintenance costs and receive service rewards in the money they issue.

In case of Bitcoin, the miner who contributes to the maintenance of the system receives Bitcoin as his reward, and so it resembles to the central bank system. A difference between the Bitcoin system and the central bank system lies in the fact that the former gives a reward to a miner who happens to win the mining competition while the latter receives a reward constantly. If there is a single miner in the Bitcoin system, r can be any arbitrary 256 bit value (n can be zero). In such a case, the competition mechanism that guarantees a validity of proof of work does not work and we require some alternative. If an alternative works, it could be sufficient to prevent double spends. This situation can be described as the mint model of cryptocurrency.

The mint model differs from the Bitcoin model in a sense that the former model uses a finality confirmation structure with legal enforcement, while the latter model uses a finality confirmation structure via mining competition. Note again that the winner of the competition is the only competitor to be rewarded with Bitcoin. The probability of winning a reward must be based on the proportional computational power of an individual miner to the total computational power of all mining participants: all miners may expect to receive rewards proportional to their computational power after a reasonable number of mining competitions[16].

Then we must ask ourselves, can the proof of work contribute to the stability of Bitcoin value? Nakamoto(2008) states “once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free”(p.4).

Answer is no. As Figure 2 amply illustrates, the values of Bitcoin as measured in U.S. dollar fluctuate wildly compared with those of other foreign currencies. The reason for this high volatility is apparent. Demand for Bitcoin, regardless of the motivation for holding (i.e. payment or speculation), increases as its price decreases and vice-versa. As Figure 3 shows, the demand curve of Bitcoin, therefore, would be downward sloping[17] while supply curve of Bitcoin at any point of time would be vertical. All demand shocks (such as E^* or E^{**}) must be absorbed in price adjustments (such as P^* or P^{**}).

We note Bitcoin pricing differs from the pricing mechanism under the gold standard in two aspects. First, the supply of gold as natural resource must be adjusted to the marginal cost (i.e. the miner would set its production so as to make the market value of gold equal to the marginal cost of gold mining). Secondly, gold can be used for industrial and jewelry purposes as well as a money. If the price of gold coin goes up, the gold used for industrial and jewelry uses would be converted to the gold coins and vice versa.

Gold coins should consequently be expected to manifest an upward sloping supply curve (see Figure 4). In this case, as shown in Figure 4, demand shocks can be absorbed in both prices and quantities. Compared with Bitcoin, the price of gold coins would be consequently

[16] Of course, we need to consider how fair mining competition is. But if the looser with lower computational power would have no chance to win the competition, he/she would exit from the competition after several trials. In the long run, all competition participants must have more or less the similar computational powers.

[17] If people take into account of Bitcoin prices and all news up to the previous periods and expect the current price properly, then they form their demand curve fairly close to horizontal (i.e. flat). We do not discuss such a case here.

less volatile due to this supply elasticity[18]. The price volatility of Bitcoin may reflect a rather naïve understanding by the designers of the Bitcoin system that the monetary value of Bitcoin would be stabilized with a fixed money supply rule.

4. Dual Instability

Let us consider the miner's behavior from a broad cost/benefit analytic perspective. Miners voluntarily participate in the mining competition, and invest in their computational power, and would exit if mining costs exceed its benefits. In principle, this situation of entry and exit is common to all industries. The only difference from standard industries is that supply of Bitcoin is independent from miners' entry and exit.

To elaborate upon this point, we divide the miners' computational powers into M units. M varies according to miners' entry and exit. But the reward for the winner of mining competition is fixed as about Z per hour (at the moment, 25 BTCs per ten minutes, Z would be about 150) regardless of entry and exit of miners[19]. Assuming the Bitcoin protocol sets *n* properly, Z would be fixed for a certain period of time. This fact is reflected in the vertical supply curve of Figure 3.

Expected reward/benefit per unit per hour is Z/M. If the market value of Bitcoin is given as P, the market value of expected reward is PZ/M. If the mining cost is lower than PZ/M, then the miners obtain

---

[18] Of course, the price stability of gold coin under the gold standard may not be attributable solely to the supply curve adjustment mechanism. As to the gold price stability in the late 19th century to the early 20th century, Keynes (1924) argues "for when gold was relatively abundant and flowed towards them, it was absorbed by their allowing their ratio of gold reserves to rise slightly; and when it was relatively scarce, the fact that they had no intention of ever utilising their gold reserves for any practical purpose, permitted most of them to view with equanimity a moderate weakening of their proportion. A great part of the flow of South African gold between the end of the Boer War and 1914 was able to find its way into the central gold reserves of European and other countries with the minimum effect on prices" (pp.166-167). The supply shocks of gold and silver discovery sometime cause volatility of the gold and silver coins. From 1550 to 1620, the prices in Western Europe as measured in the silver coins increased 2.5 times (annual inflation rate is about 1.5%) as a result of new flow of silver from the American continent. This is called the price revolution period.

[19] We put "about" because the Bitcoin protocol set a time interval of a block 10 minutes on average by adjusting difficulty parameter *n*.

net benefit/return, and vice versa. Let us reflect these aspects in the past one year or so.

(1) If the market value of expected reward PZ/M exceeds the average cost of adding one unit (it is given exogenously by a technological change), new entry would increase. But as M increases accordingly, the expected reward/return per unit (average productivity) would drop. Eventually new entry would cease. This situation is a kind of equilibrium and remains until news on the Bitcoin price arrives. Good news, or Bitcoin price increases, induces new entry which continues up to the point where M equilibrates between the marginal cost and the market price. The problem happens when bad news arrives.

(2) Assume bad news arrives when the Bitcoin system equilibrates. If bad news reduces the Bitcoin market price, the miners' net return would be negative. If the miners' computational power can be reallocated to the other purposes, migration from Bitcoin mining would happen gradually. Accordingly, depending on the size of the M decrease, the expected return per unit would recover. This situation could happen when the mining is conducted in a spare time of mainframe computer. This can described as the pastoral reality of early Bitcoin mining.

(3) But the current reality is not pastoral at all. As Figure 2 illustrates, the Bitcoin price shot up after November 2013[20]. This fact rendered the mining business very profitable. As a result, many entrepreneurs entered into the Bitcoin mining competition equipped with super powerful computers with designated IC chips[21]. The current situation

[20] The Bitcoin market price was about ten dollars in the early 2013. It shot up above 1000 dollars in the end of November 2013. It is hard to tell the exact reason for this. We cannot exclude a possibility of the bubble because the Bitcoin system tends to create babble as the supply curve stands vertically. If Bitcoin was used to transfer capital from Cyprus in case of financial crisis 2012-13, the price hike of Bitcoin can be explained reasonably by this event. Suppose, if one Bitcoin is ten dollars, 100 million dollar transfers from Cyprus require 10 million BTCs. That would exhaust almost all Bitcoins in the market.

[21] This movement is consistent with change in difficulty parameter n. As eq.(5) indicates, an increase in n (from n to n+1) is equivalent to double the number of miners units M.

resembles a heavy equipment industry in which it is easy to enter, but it difficult to exit because of large sunk costs.

(4) Suppose that the Bitcoin price drops a by substantial, but not a deadly, margin. To be more precise, it falls to some price lower than the average cost per unit but above the average variable cost. The miners would continue mining because it is rational to keep operations as long as return/revenue exceeds variable cost (i.e. total cost minus fixed cost); the eventual operational loss would be smaller than that incurred by immediate stoppage. According to some reports on Bitcoin mining, many large-scale miners who entered after the Bitcoin boom in late 2013 continue running their operations even with negative returns. They may not actively anticipate the return of above-1000 dollar/Bitcoin days, but they might simply assume that eventual operational loss would be minimized by continued operation.

(5) Miners may also migrate to another mine in which they can continue mining, should computational powers be convertible to the new mine[22]. As we mentioned before, if the miners migrate to the other mines, the size of M decreases, and the expected return per unit would recover. By this mechanism Bitcoin mining can survive even under a very volatile Bitcoin price. On the other hand, miners' computing equipment may reach the end of its useful life, and miners might have to stop mining before they recover all their sunk costs.

(6) Bitcoin mining might end another way. If the Bitcoin price drops sharply below the average variable cost, all miners would exit from mining. Many miners entered the Bitcoin mining competition after the Bitcoin boom in the late 2013. Their computational power would be expected to be broadly similar[23]. If that is the case, the miners' exit

[22] Many alternative cryptocurrencies to Bitcoin emerge recently. If the operational protocol is closer to that of Bitcoin, it would be much easier to convert their mining operation into the new cryptocurrency. There already exists a service to inform relative mining profitability among alternative cryptocurrencies so that the miners can move around the profitable mines.

[23] Most of calculation in the Bitcoin mining is allocated to search for the value r to solve the

strategy would not be a gradual one, but could be sudden. If the Bitcoin price drops below a threshold, the Bitcoin system as a whole may collapse or the Bitcoin users are limited to a very small number of inner members with which Bitcoin is exchanged at a very small scale. Once all miners leave the Bitcoin mining, no one would be engaged in the proof of work. A validation of a block would be delayed or stopped, and in consequence Bitcoin ceases to be a useable currency. This type of risk doesn't' exist in gold mining[24].

From the above observations, it is clear that the Bitcoin system intrinsically manifests dual instability. The first instability stems from an inflexible supply curve of Bitcoin, which amplifies Bitcoin price volatility; the miners' revenue/reward fully absorbs any price changes. There is no price stabilization mechanism. The second instability comes from risks to the sustainability of mining. During a Bitcoin price boom miners engage in mining activity which guarantees the supply of Bitcoin. But during a Bitcoin price depression, no smooth way to induce exits from mining exists[25]. The current situation of the Bitcoin system can be interpreted as a freezing equilibrium with dual instability.

5. Scene after the Gold Rush

The dual instability could be accelerated by miners' strategic behavior. Remember that the Bitcoin system shares the virtual registry book among all participants, and that everyone can monitor what all others do. It is not a big problem when new miners enter mining activity as a result of the Bitcoin boom. Strategic behavior becomes a problem when no additional profit can be found after the miners' rush.

---

problem. This calculation is made by the Bitcoin mining dedicated IC chips (ASIC). Computational power is proportional to the numbers of ASIC. We suppose the productivity of miners in terms of computational power per unit is more or less equal.

[24] This fact indicates that Bitcoin is not necessarily a cheap payment tool. We have to realize that Bitcoin has an externality. We will come back to this in Section 7.

[25] Once the price falls into the level that is lower than the average cost per unit but above the average variable cost, one solution for the miners is to sell their computers to the other miners. But this action might induce a sharp drop in the price of Bitcoin mining dedicated IC chip. That, in turn, makes exit more difficult. This could be the worst scenario for the miners.

An example is voluntary and collective mining pool formation. Figure 5 illustrates how the mining pool occupies the Bitcoin mining business. Two large pooling groups (i.e. GHash.IO and Discus Fish) occupy almost 50% of its shares[26].

How can a mining pool be created easily in the Bitcoin system? The virtual registry book is shared commonly, so every ID number can be traced by all participants, enabling miners to form a collective mining pool. Once the pool is created, it is easy for the pool administrator to monitor the behavior of all members in the pool[27]. It becomes very difficult to observe from the outside what mining strategy the pool uses. Asymmetric information between the insider and the outsider of the pool is generated via a virtual registry book and some special ID replacement system.

In the long run, any reward/return from mining competition is probabilistic and realized returns would converge to expected returns. But in the short run, from the individual miner's viewpoint the risk of low return is non-negligible. It is quite rational to form a mining pool to reduce the risk of return volatility without changing the expected return. Pool member miners typically agree to allocate returns in proportion to their contributed computational power.

Let us clarify the rationale for the mining pool. If the search item is rare, the miners can divide their search area by space so that the miners can avoid inefficiently searching the same space. But Bitcoin can be considered as 2^{256-n} coins being randomly distributed over a large space of 2^{256} lots. From the view point of reducing the waiting time between rare events to happen, the mining pool does not help. But pools can reduce the risk of an individual miner's return.

The Bitcoin mining competition is repeated every ten minutes (equivalent to 144 races with equal odds repeated daily). If the

[26] Eyal and Sirer (2014) points out that pools over 25% can cheat the system with selfish mining and earn more than their fair share, over 33% presents risk of unilaterally successful selfish mining, large pools risk double spends with low confirmations, and over 50% is an unmitigated disaster and that such majority miners are toxic.

[27] As Ron and Shamir (2013) shows, from certain characteristics of transactions, ID numbers in the Bitcoin system can be traced backwardly and identified the owners of Bitcoin.

miners' risk in measured not in each competition but in a day, it would be reduced to 1/12 (i.e. the square root of 144). On the other hand, if 100 miners form a mining pool, their risk can be reduced to 1/10 of the applicable standard deviation. Taking into account pool administration cost, actual pool formation may go beyond the rationale for the mining pool of risk diversification.

Why do we care about the mining pool? It can be a source of strategic and opportunistic behavior, which may in turn damage the credibility of the Bitcoin system. Firstly, the miners in the pool can force losses upon the miners outside the pool and encourage them to exit mining[28]. Second, if multiple numbers of sizable pools exist, each pool can rotate their mining in proportion to the computational power. In so doing, each pool can raise their mining efficiency[29]. As Figure 5 illustrates, small numbers of mining pools accumulate computational power. That said, we cannot find any evidence of strategic behavior of the miners in the pool, as indicated by Eyal and Sirer (2013)[30].

The current situation of Bitcoin mining remains us of the scene after the gold rush in California. The miners entered after the Bitcoin boom look exactly like the 49ers[31]: most of them made little or lost money.

It is true that mass migrations during the gold rush period to California laid down the foundations of economic prosperity in later years. The same can be said of Bitcoin, which attracts substantial public attention. If we take advantage of this opportunity we can foster an improved Bitcoin that can compete with central bank money.

6. Monetary Policy without a Central Bank

[28] See Eyal and Sirer (2013).

[29] Suppose two mining pools are oligopoly, economic efficiency can be raised by one pool mining while the other resting. This type of collusion can keep difficulty parameter *n* to remain low or raise high as they wish.

[30] We do not know exactly that such strategic behavior has not been taken place or that the actions are taken but they are not known to the public.

[31] This name is given to the gold prospectors who arrived in northern California around 1849 during the California gold rush.

Cryptocurrencies like Bitcoin do not depend on a central bank. With some amendments to its design, we can use this cryptocurrency (we call this currency, an extension to Bitcoin, Improved Bitcoin or IBC) to implement some equivalent policy effects as a central bank conducting monetary policy. It is indeed *monetary policy without the central bank*. To do so, we need to conquer the dual instability issues discussed in Section 4.

6-1. Currency Boards as inspiration

A simple and straightforward currency supply rule is that - given the market value/price of IBC vis-à-vis U.S. dollar or Euro as a benchmark - if the market value of IBC increases, the system would issue IBCs until the market value returns to the benchmark level. This rule can be described as the pegging rule of exchange rates, or the currency board system.

To be more concrete, suppose the market value/price of IBC is P dollar at the moment. A reward for the proof of work, V is set to rise when the market value P is above the benchmark value and a reward V is set to be zero when P is below the benchmark. Alternatively some difficulty parameter *n*, adjusting the speed of proof of work is to be changed. In this case, without changing V, the quantity of new issue of `IBC per hour Z is adjusted[32]. Which rule is better? In theory, both rules affect the market value of IBC equally. The above discussion can be considered a starting point to consider the market value stability of a cryptocurrency. In the Bitcoin type of cryptocurrency, without a central authority, the policy framework for market value stabilization must be rule- rather than discretion-based.

This method has a serious defect: to reduce the new issue of IBC to zero is not equivalent to absorbing excess IBC in circulation. Figure 6 illustrates the kinked supply curve of IBC, with current point E as a refraction point (for simplicity, let us assume supply and demand equilibrates at E). A positive demand shock to IBC (increase in IBC

[32] Here Z=V/θ where θ is the average waiting time.

demand) can be absorbed by shifting the supply curve from L to L^*. A negative demand shock to IBC (decrease in IBC demand) cannot be absorbed because the supply curve is vertical in this case. Consequently the market value of IBC drops to P^{**}.

The supply of central bank notes can easily expand and contract. For a positive demand shock to bank notes (shifting from consumption/investment to money: i.e. it is a deflationary shock), the central bank increases money supply by buying securities and foreign currencies. For a negative demand shock to bank notes, the central bank absorbs money in circulation by selling securities and other assets. In case of IBC, the latter operation is not included in its protocol. That is to say, the cryptocurrency protocol usually includes the currency supply rule, but does not have a currency absorption or write-off protocol. Can we reduce this irreversibility?

6-2. Built-in Revaluation Rule for Exchange Rate

It is the irreversibility of cryptocurrency supply that concerns us most, perhaps because of our obsession of understanding currency supply in terms of numbers. If we try to control currency quantities in terms of real purchasing power, it may not be so difficult to absorb surplus currencies in circulation. It is possible to include an inflation rate in the supply rule to amend irreversibility of currency. If our basic idea is closer to a currency board, this amendment is an amended currency board with the build in revaluation rule for exchange rates.

Our proposed amendment uses the market value of IBC, P, vis-à-vis the benchmark price as policy indicator to control our policy instruments, V, Z and n. The amendment uses the market value P with inflation rate α, i.e. $P^*\exp(\alpha\tau)$ as policy indicator to control policy instruments, V and n (τ is time periods since the starting point). With this rule, we can virtually absorb excessive currency or purchasing power in circulation due to currency demand shocks or policy mistakes. That is, we may not be able to eliminate currency in circulation but we can reduce its real value by allowing inflation.

How can we determine inflation rate α? It is clear that a higher α is more effective at absorbing demand shocks. Figure 7 illustrates this situation. Horizontal axis is converted quantity, rather than (currency) quantity. Converted quantity measures the real purchasing power of IBC in terms of benchmark currency. With higher α, real purchasing power at the moment shifts from L to L^{**} and equilibrium point also shifts from E to E^{**}. As a result, if a demand shock shifts D curve to D^{**}curve, the supply side absorb this shock and stabilizes the market value/price accordingly.

However, it is not necessarily true that higher α is better. Higher α implies that monetary value depreciates quickly. With higher α, people would avoid holding IBC per se. If the IBC system maintains a delayed finality confirmation structure like the Bitcoin system, participants must hold IBC in their wallet for a while after receiving IBC as their reward for mining or in exchange for the transaction of goods and services. It would be painful for IBC holders to see such depreciation during their hoarding period.

In order to make our built-in revaluation rule practically workable, it may be better to separate the IBC operation rule from the benchmark price vis-à-vis the U.S. dollar. To do so, we need to investigate an intrinsic value for IBC.

6-3. Monetary Policy without a Central Bank

The first task is to construct an IBC supply rule that can absorb a positive demand shock. From our discussion in Sections 6-1 and 6-2, if the IBC system can adjust supply proportional to computational power, the market value/price of IBC would rise and new miners would participate in IBC mining. For the long run[33] we can construct an IBC supply schedule similar to Figure 6.

Recall in Section 3 we obtain the following result, $\theta \fallingdotseq 2^n/kM$. The current Bitcoin system adjusts difficulty parameter n to stabilize an average waiting time θ as the number of miners M increase. What will

[33] Here the demand and supply adjustment presumes new entry of the IBC miners.

happen if n is not adjusted to an increase in M? From eq. (5), θ will shrink inversely proportional to M. If a reward for the proof of work V is fixed for a certain period, new IBC issue per hour ($Z=V/\theta$) would go up or down depending on M. If θ becomes too small, n could be raised (i.e. n+1 would double θ) or alternatively V could be doubled. In allowing for the duration of a block formation θ to shorten as M increases, a duration of finality confirmation would also be shorten. That has merit, but, at the same time, the risk of admitting double spends increases. Recall that the new issue policy $Z=V/\theta$ depends solely on M[34].

Now the IBC system has acquired a built-in revaluation mechanism[35]. It is the first step towards monetary policy without a central bank. The monetary value of IBC with such a rule will be far more stable over time: an upward change in price induces new entry of miners up to the point where the marginal cost becomes equal to the reward measured in the price of IBC.

As discussed in Section 6-1, the IBC system can accommodate a positive demand shock (i.e. an upward change of price or a deflationary shock). This system cannot react properly to a negative demand shock (i.e. a downward change of price or an inflationary shock). Is there any remedy for this?

6-4. Implicit Inflation Target in Cryptocurrency

The answer is to set a structure that makes the IBC mining cost (determines the market value/price of IBC) gradually decreasing over time. To be more precise, a reward V for a block formation increases at a designated growth rate of β. Together with a technological change

[34] This is somewhat related to the labor theory of value, initially suggested by Adam Smith, David Ricardo, and Karl Marx. The value of IBC is directly linked with the mining work. That is to say, the real economic activity is linked with monetary economy. This is also related to the idea of the gold standard in which the gold is convertible with the paper money at the fixed rate. The gold is the real anchor.

[35] Allowing for these amendments, the IBC protocol has to be completely changed. For example, due to the alteration of supply rule, total amount of IBC supply should be infinite. Duration of a block formation can be variable.

rate γ[36], the IBC mining cost per hour decreases at the rate of $\beta\gamma$; market participants expect inflation at $\exp(\beta\gamma)$ per hour and the real value of IBC would drop. As long as a negative demand shock reduces IBC demand within the range of IBC value depreciation, we can avoid unexpected IBC inflation shocks.

From Figure 7, the point L^{**} is the real IBC purchasing power discounted by expected inflation. $L-L^{**}$ is depreciation of purchasing power. If a negative demand shock falls in the range between D and D^{**}, such a shock can be absorbed perfectly. Taking into account of inflation expectation in the IBC valuation, an inflationary shock via monetary policy can be offset.

We note this rule is closely related to the inflation targeting policy implemented by many central banks. Inflation targeting is effective in softening an unexpected inflectionally shock[37]. The current rule has the same effect. We may call this rule an implicit inflation target for cryptocurrency. This rule, however, is different from inflation targeting by the central banks, in that their inflation target depends heavily on expectations formation by the public, and credibility of the central bank in general and the governor in particular. Both do not necessarily have strong linkages with the real economy, as a result, their effects are sometimes vague and usually controversial. Our rule, on the contrary, depends on an economic principle, i.e. the cost structure of the mining that is real economic activity.

7. Friedrich A. Hayek's Currency Competition

We have analyzed the Bitcoin system in general and the role of mining as the proof of work. We've proposed an alternative to Bitcoin, Improved Bitcoin (IBC) that is supposed to overcome the inherent instability of Bitcoin. But can IBC compete with major currencies issued

---

[36] As technological change increases in k ($k=K/2^{256}$; K=computational power), IBC supply per hour will increase through shortening θ. We assume the technological change rate γ is exogenously given.

[37] For detailed discussions, see Iwamura and Watanabe (2006).

by major central banks? We note at least four problems with such cryptocurrencies.

First, cryptocurrencies are more expensive to produce, and the production costs are hard to retrieve. Bank notes issued by the central banks require some printing and material costs. These costs are negligible compared with the face (nominal) value.

Second, bank notes are reversible between new issues and absorption because the central bank basically buys and sells securities with bank notes. A cryptocurrency cannot be absorbed, but if equipped with a built-in value stabilization mechanism, this shortfall of irreversibility can be softened (but not eliminated) in practice.

Third, Bitcoin-type cryptocurrencies use a delayed finality confirmation structure to avoid double spending. Consequently it typically takes hours to use obtained money. Bank notes can be used immediately as obtained.

Fourth, Bitcoin type cryptocurrencies face security risks, such as Denial of Service attacks, more widely than bank notes.

The third and fourth points are relative problems, and also intrinsic to Bitcoin-type currencies. They are not general problems with cryptocurrency. The third point considers a problem directly compared with bank notes for direct transactions. Considering transactions with Bitcoin-type currency may occur over a remote distance, finality confirmation may be quicker and much cheaper with a Bitcoin-type currency than that through a bank. The fourth point is closely related to the protocol design of a Bitcoin-type currency, and is not a general cryptocurrency issue. The instability associated with mining pools due to strategic behaviors between and within pools can be reduced substantially if the valuation system is improved in line with our suggestions.

The first and second points are fundamental shortfalls of cryptocurrency. As currently described, cryptocurrency values are based on associated production costs. This mechanism is similar to commodity money, notably gold and silver coins. Historically gold and silver coins have been replaced by credit (or fiat) money basically because of the above-mentioned first and second points.

As Vance and Stone (2014) reports, the production cost of Bitcoin are the mainly variable costs of equipment and electricity. In general Bitcoin mining appears to be a loss-making but stable industry (i.e. no net entry). Under these circumstances, the Bitcoin reward per hour reflects the marginal cost of mining. For example, if the market value of Bitcoin is USD$600, then the Bitcoin system is maintained by issuing 25 *600 =$15000 dollars per ten minutes (i.e. 90 thousand dollar per hour, 2.16 million dollar per day). This is not a small amount. The Bitcoin system is often described as inexpensive because maintenance costs are not charged to the Bitcoin users, but are generated as reward to mining. In short, Bitcoin is based on a system that takes advantage of an externality. It is not a cheap system at all.

This capitalization-by-externality will be liquidated sometime in the future. A collapse in Bitcoin value might happen in the near future. Who pays this bill?

Our proposed amended supply schedule, i.e. the built-in revaluation mechanism and the implicit inflation target has an implication beside the value stabilization of IBC. These rules would prevent excessive currency demand due to the externality. The same is true of gold and silver coins: it is truly waste of limited resources if such are kept in a safe or in computers after expending a large production or mining cost. Then can we say bank notes are superior to cryptocurrencies? Not with any certainty.

Direct production costs of bank notes are not high. But we cannot ignore the implicit costs generated dependence of monetary value on policy decisions by governments or central banks. The central bank always has an option to engage in an unexpected policy change. Many economists agree that perfectly expected inflation is welfare neutral.

But under the name of a bold policy initiative, monetary policy may generate welfare losses due to unexpected inflationary and/or deflationary pressures.

Reversibility of bank notes - between new issues and absorption - is based on the exchange between bank notes and government bonds at some point in time. This is nothing to be proud of. If the credibility of government bonds is shaken, that of bank notes would be also shaken. On the contrary, if government bonds dominate the capital market, the central bank, simply monetizing it, has to worry about ever-expanding its balance sheet[38]. Reversibility of bank notes has merit, and inescapable costs.

Shall we prefer bank notes or a cryptocurrency? There is no unconditional answer. Bitcoin-type cryptocurrencies, with some amendments, can be reasonably competitive with central bank notes in terms of value/price stability. Currency competition in a sense of Fridrich A. Hayek is desirable. Such competition must be encouraged, not only between central bank notes and a cryptocurrency, but also between central bank notes and among different cryptocurrencies.

Indeed, currency competitions among cryptocurrencies are already taking place. Some hundreds of cryptocurrencies already exist, following the sensational success of Bitcoin. If this was the 'big bang' of currency competition among cryptocurrencies, a better designed cryptocurrency (such as an IBC) may emerge and become strong contender to the central bank notes.

How about central bank notes? Central bankers are keen on international cooperation, but not so keen currency competition. The current generation of central bankers in U.S., Europe and Japan indicate to markets that they care more for business than for price stability. It is increasingly accepted that price stability may not be the only goal of central bankers. Excessive international cooperation may obstruct

[38] Fiscal theory of the price level (FTPL) discusses these issues. See Iwamura and Watanabe (2002) for a full discussion.

capital's exit; if investors worry about the future of the yen, then the prospects of the Euro or dollar are not so different under the current set of circumstances. Some investors have consequently shifted their capital to Bitcoin, in which the price is very volatile and no credible authority guarantees its value.

Central bankers should not indulge in pondering how to give minor shocks to markets, given limited usages of money, but they should investigate why people are so attracted to Bitcoin and what features can be used in monetary policy.

The key differentiation of Bitcoin from central bank notes and existing digital cash type electronic money is a framework in which all vintage information of each segment of Bitcoin are recorded[39]. Not many people are aware of this useful feature of Bitcoin. If this feature is introduced in to bank note-like electronic money, each atom of bank note-like electronic money with its vintage information can reflect time value, i.e. each note is priced differently according to the time passed since its issuance. In other words, we can provide interest with each note. This system implies that owners of bank note-like electronic money can receive interest or pay some penalty, depending on economic conditions. In the current central banking system, these benefits are transferred to the government as *seigniorage*. Note that the monetary interest rate, as measured a unit of money today, is how much the same amount is anticipated to be worth one year from now. It is different from nominal interest rate that is a return from investment of zero interest bearing money[40].

If the legal system permits, these bank note-like electronic moneys can provide a substantial business opportunity. Strangely, the current generation of central bankers do not pay a lot of attention to the

[39] In practice, when Bitcoin is issued, all vintage information is recorded. After some transactions, divisions and merges are repeated so that original vintage information can no longer carry over. A design of electronic money that can keep all vintage information cannot be used in the Bitcoin system as it is now. We suppose there is a way to maintain all vintage information even after repeated transactions. It is an important research question.

[40] Silvio Gesell (1918) advocated the idea of stamped money. His idea is used in some regional moneys now. Alas, most of these moneys employ only in the region of negative interest rate (i.e. penalty charge). It is also worthwhile pointing out that Keynes (1936) spares his Chapter 23, Section 6 to discuss and evaluate Gesell's idea of stamped money positively.

associated opportunities: to expand the flexibility of monetary policy by converting from paper money to bank note-like electronic money with vintage information. With this framework, central banks are no longer vulnerable to Keynes' (1936) liquidity trap, by avoidance of the zero lower bound interest rate[41].

8. Conclusion

Why Bitcoin did not exist until recently? Decentralized money provision, and similar economic systems with P2P technology, were proposed well before Bitcoin. But these trials failed to grow like Bitcoin. Perhaps early challengers may take the nature of money and autonomy of economic activity too seriously.

The major drivers behind Bitcoin's success are (1) a naïve understanding of currency, (2) the employment of an easy-to-understand asymmetric key cryptosystem for validation of transactions and a virtual register system, and (3) the creation of a participatory system with a P2P network maintained by the elliptic curve digital signature algorithm and a hash function. This framework has attracted many programmers and collaborators to improve user software and that, in turn, attract many users of Bitcoin.

In addition, the originator of Bitcoin - Satoshi Nakamoto - and his collaborators demonstrated they can create a currency without a central bank via proof of work, and that there exists demand for such a currency.

A unexpected feature of Bitcoin is that, contrary to the original belief of Satoshi Nakamoto that he can create currency without inflation by means of controlling and preannouncing total supply of Bitcoin, the market value/price of Bitcoin fluctuates up (deflation or the value of Bitcoin goes up) and down (inflation or the value of Bitcoin goes down).

[41] It is possible to add vintage information to the current paper money by printing the issue date. It would be far troublesome to handle each note differently. If in case of digital currency, that problem can be solved easily.

We hope that Satoshi Nakamoto's important contributions can nullify his misunderstandings. We are grateful to Satoshi for his imperfect Bitcoin innovation. There remains much room for improvement, and for discussion of our future monetary system.

References

Back, Adam.(2002) "Hashcash - A Denial of Service Counter-Measure", http://www.hashcash.org/papers/hashcash.pdf.

Barber, S., X,Boyenm E.Shi, and E.Uzun. (2013) "Bitter to Better: How to make Bitcoin a Better Currency", in Proceedings of Financial Cryptography, 2013.

Bergstra, Jan A. and Karl de Leeuw.(2013a) "Bitcoin and Beyond: Exclusively Informational Money", Informatics Institute, University of Amsterdam, arXiv:1304.4758v3.

Bergstra, Jan A. and Karl de Leeuw.(2013b) "Questions related to Bitcoin and other Informational Money", Informatics Institute, University of Amsterdam, arXiv:1305.5956v2.

Böhme, Rainer. (2013) "Internet Protocol Adoption: Learning from Bitcoin: Position Paper", IAB Workshop on Internet Technology Adoption and Transition (ITAT), University of Cambridge, December 2013.

Bruce, J.D.(2013) "Purely P2P Crypto-Currency with Finite Mini-Blochchin", www.bitfreak.info.

Chapman, Bruce and Scott, Freeman. (2001) *Modeling Monetary Economies*, 2nd ed., Cambridge University Press.

Courois, Nicolas T, Marek Grajek and Rahul Naik.(2014) "The Unreasonable Fundamental Incertitudes Behind Bitcoin Mining", arXiv:1310.7935v3.

Decker, Christian and Wattenhofer, Roger. (2013) "Information Propagation in the Bitcoin Network", 13th IEEE International Conference on Peer-to-Peer Computing.

Dwork, Cynthia and Moni Naor.(1992) "Pricing via Processing or Combatting Junk Mail", In *Crypto92*, Springer, 1992, pp.138-147.

Eyal, Ittay and Emin Gün Sirer. (2013) "Majority is not Enough: Bitcoin Mining is vulnerable", mimeo, Cornell University.

Eyal, Ittay and Emin Gün Sirer. (2014) "How to Disincentivize Large Bitcoin Mining Pools", http://hackingdistributed.com/2014/06/18/how-to-disincentivize-large-bitcoin-mining-pools/

Friedman, Milton.(1960) *A Program for Monetary Stability*, New York: Fordham University Press.

Gesell, Silvio.(1918) *The Natural Economic Order*, 3rd ed. (translated by Phillip Pye), available in http://www.archive.org/details/TheNaturalEconomicOrder

Goldwasser, Shafi and Mihir Bellare. (2008) *Lecture Notes on Cryptography*, MIT.

Hayek, Fridrich, A. (1976) *Denationalization of Money: An Analysis of the Theory and Practice of Concurrent Currencies*, London: Institute of Economic Affairs. Reprinted in Kresge, Stephen (ed). (1999) *The Collected Works of F.A.Hayek: Good Money, Part II: The Standard*, Liberty Fund.

Iwamura, Mitsuru and Tsutomu Watanabe (2002) "Price Level Dynamics in a Liquidity Trap", RIETI Discussoin Paper Series, 03-E-002.

Iwamura, Mitsuru and Tsutomu Watanabe (2006) "Monetary and Fiscal Policy in a Liquidity Trap: The Japanese Experience 1999-2004", in Takatoshi Ito and Andrew K. Rose, (eds) *Monetary Policy under Very Low Inflation in the Pacific Rim*, NBER and University of Chicago Press.

Kaynes, John Maynard. (1924) *A Tract on Monetary Reform*, Macmillan

Kaynes, John Maynard. (1936)*The General Theory of Employment, Interest and Money*, Macmillan.

Kroll, Joshua, A., Davey, Ian. C. and Felten, Edward W. (2013) "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries", paper presented at the twelfth workshop on the economics and information security (WEIS 2013), June 11-12, 2013.

Martin, Antoine and Stancey L. Schreft. (2006) "Currency Competition: A Partial Vindication of Hayek", *Journal of Monetary Economics*, 53, 2085-2111.

Miers, Ian, Christina Garman, Matthew Green and Aviel D. Rubin.(2013) "Zerocoin: Anonymous Distributed E-Cash from Bitcoin", mimeo, Department of Computer Science, The Johns Hopkins University.

Nakamoto, Satoshi. (2008) "Bitcoin: A Peer-to-Peer Electronic Cash System", http://bitcoin.org/bitcoin.pdf.

Ron, Dorit and Adi Shamir. (2013) "How Did Dread Pirate Roberts Acquire and Protect His Bitcoin Wealth?", The Weizmann Institute of Science, Israel, mimeo.

Samuelson, Paul. A.(1958) "An Exact Consumption-Loan model of Interest With or Without The Social Contrivance of Money", *Journal of Political Economy*, 66, 467-82.

Starr, Ross M. (2012) *Why is there Money?* Edward Elgar.

Stinson, Douglas R.(1995) *Cryptography: Theory and Practice*, CRC Press.

Vance, Ashlee and Brad Stone. (2014) "Bitcoin Rush", *Bloomberg Businessweek*, January 9, 2014.

Woodford, Michael. (2003) *Interest and Prices*, Princeton University Press.

Figure 1 Flow Chart of the Proof of Work

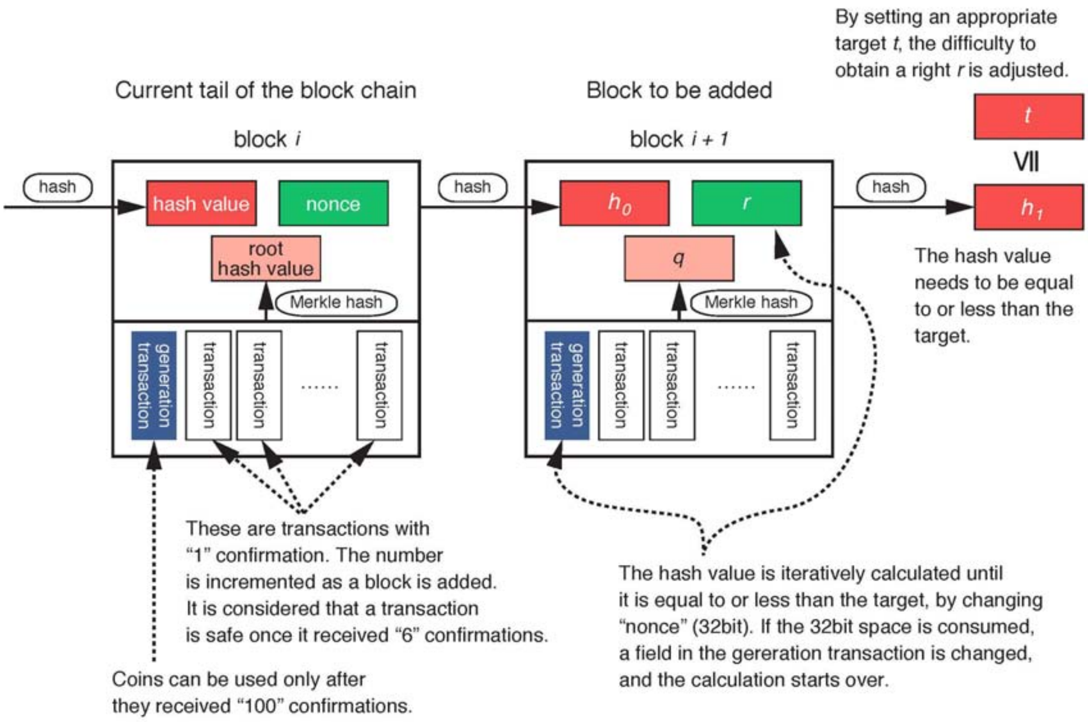


Figure 2 Market Price of Bitcoin in USD as of October 25, 2014

Source: blockchain.info.

Figure 3.Supply and Demand of Bitcoin: Case of a Vertical Supply Curve

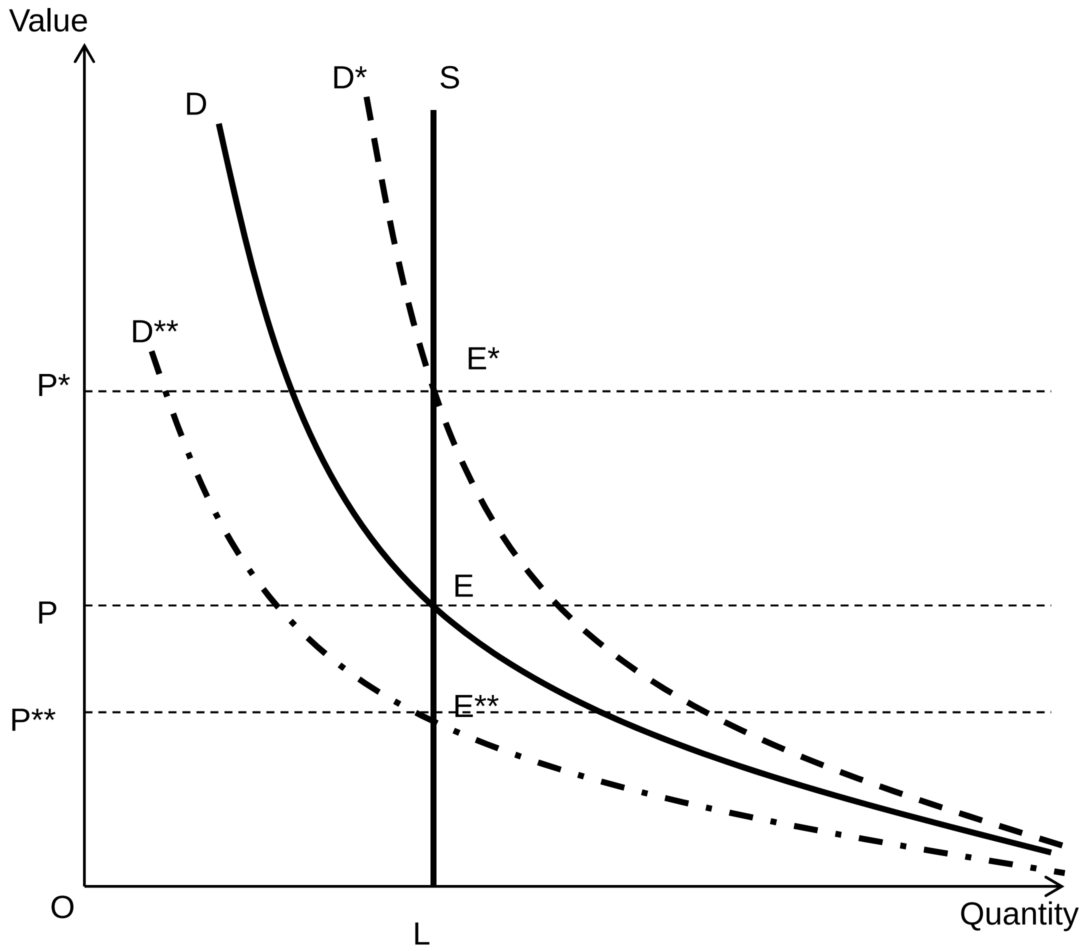


Figure 4.Supply and Demand of the Gold Coin: Case of Upward Sloping Supply Curve

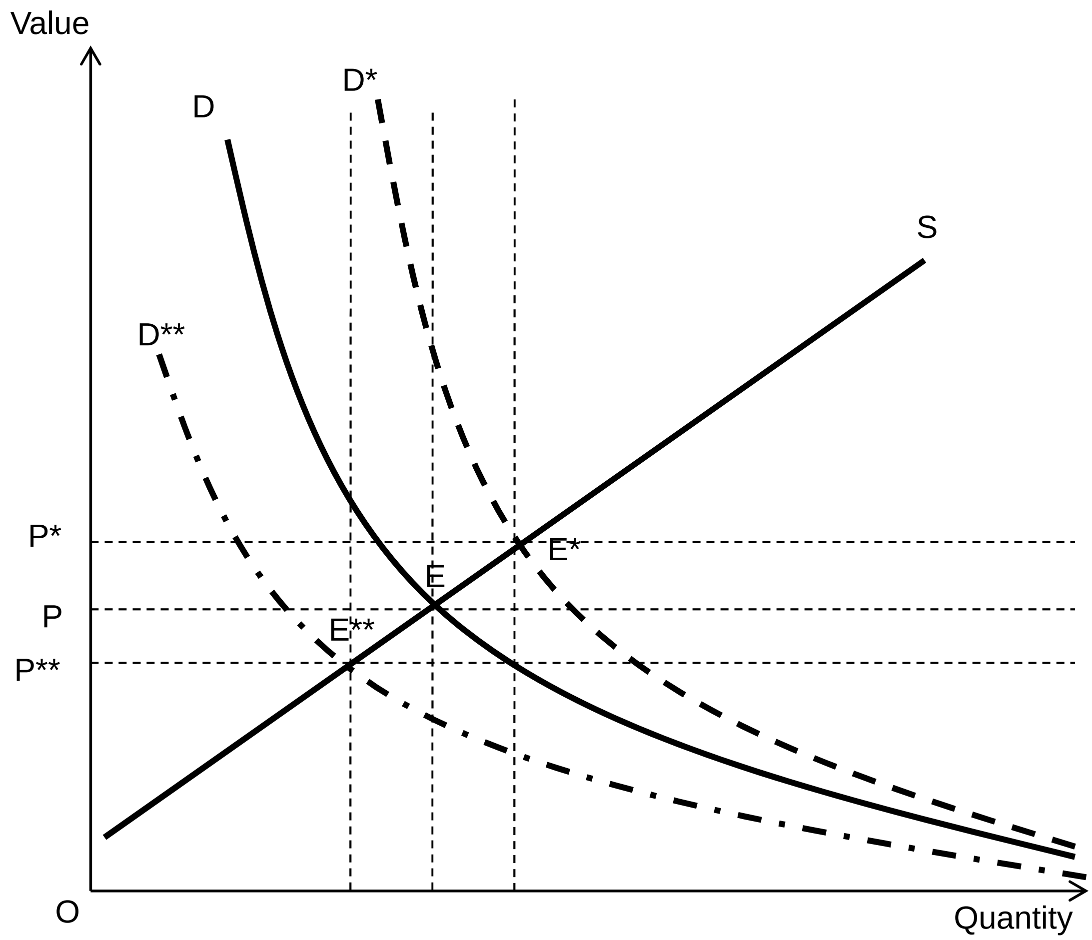
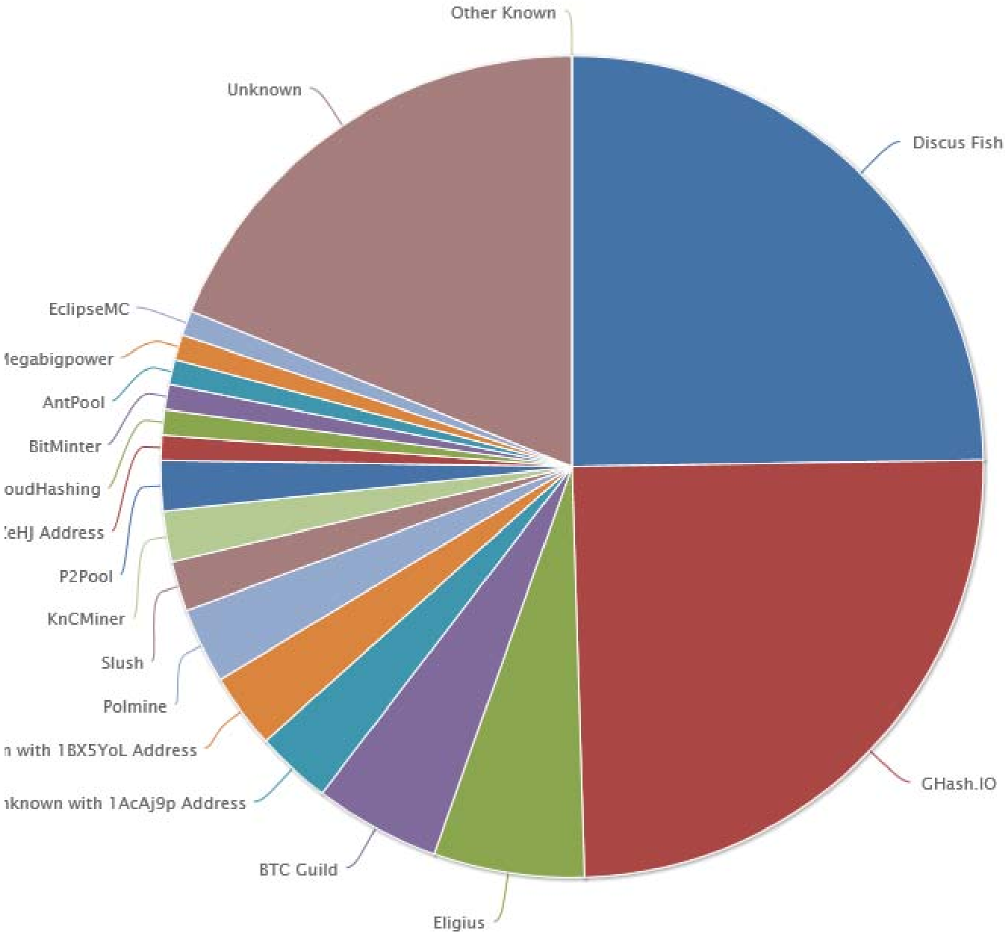


Figure 5. Share of Mining Pool as of October 25, 2014.



Source: blockchain.info

Figure 6. Supply and Demand of Improved Bitcoin: Case of Kinked Supply Curve

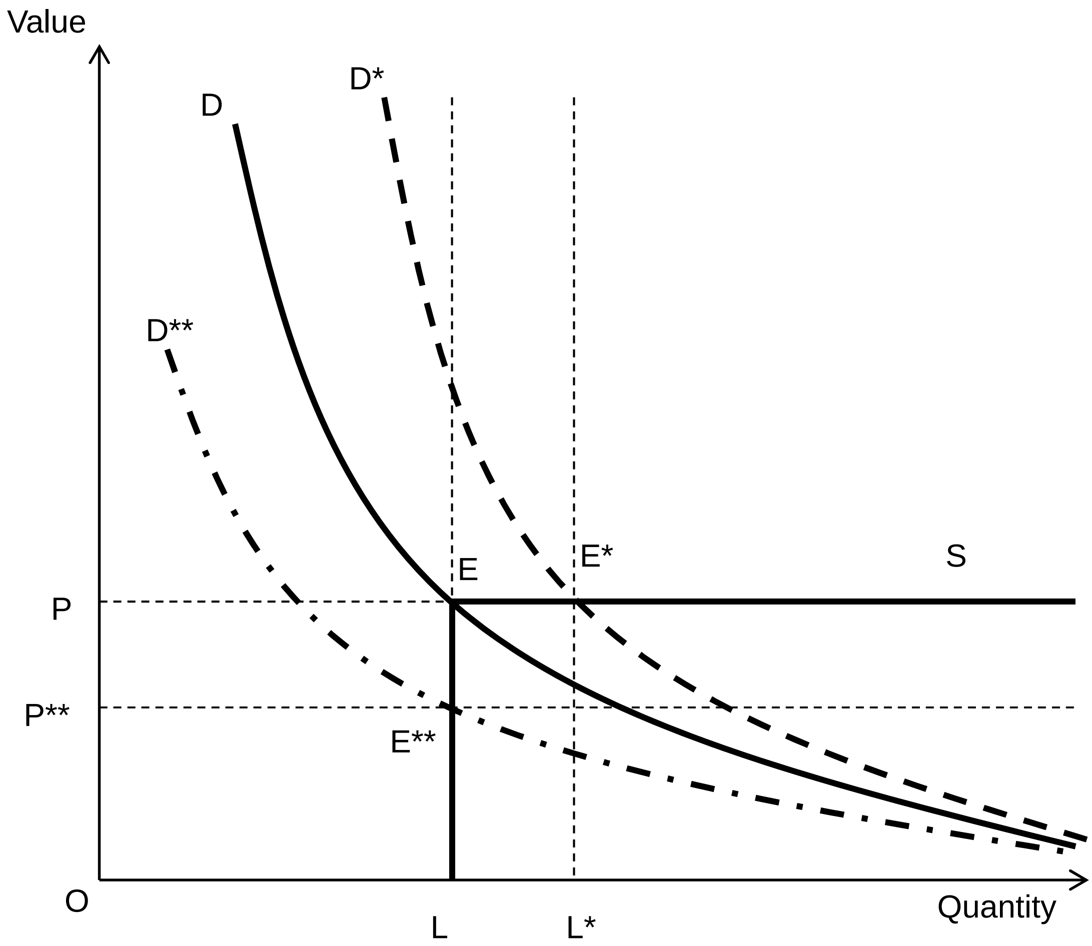


Figure 7. Supply and Demand of Improved Bitcoin: Case of Amended Supply Curve