Hitotsubashi Journal of Economics 60 (2019), pp.41-60.

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
Shinjuku, Tokyo 169-8050, Japan
iwamuram@waseda.jp

Yukinobu Kitamura**

Institute of Economic Research, Hitotsubashi University
Kunitachi, Tokyo 186-8603, Japan
kitamura@ier.hit-u.ac.jp

Tsutomu Matsumoto

Faculty of Environment and Information Sciences, Yokohama National University
Yokohama, Kanagawa 240-8501, Japan
tsutomu@ynu.ac.jp

Kenji Saito

Keio Research Institute at SFC, Keio University
Fujisawa, Kanagawa 252-0882, Japan
ks91@sfc.wide.ad.jp

Received October 2018; Accepted January 2019

Abstract

Although Bitcoin was designed as a payment vehicle and as a store of value, it seems unlikely that currencies provided by central banks are at risk of being replaced, primarily because of the market price instability of Bitcoin. We diagnose the instability as being a symptom of the lack of flexibility in the Bitcoin supply schedule - a predetermined algorithm

* An earlier version of this paper was presented at MIT Media Lab Conference on "the Ecology of Digital Assets: Identity, Trust and Data" on July 30-31, 2014. We are grateful to Joi Ito (Director of MIT Media Lab) and Alex Pentland (MIT Media Lab, Faculty Director MIT Connection Science). We are also very grateful to Luke Meehan (Australia National University) for his excellent editorial supports. We express our sincere thanks to Prof. Makoto Saito, the editor-in-chief of Hitotsubashi Journal of Economics, for being the referee of this paper.
** Corresponding author.

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 for stabilizing the values of Bitcoin and other cryptocurrencies.

Key words: Bitcoin, cryptocurrency, currency competition, Friedrich A. Hayek, proof of work
JEL Classification Codes: B31, E42, E51

I. *Bitcoin as a Virtual Registry System*

Bitcoin (Nakamoto (2008)) is an electronic cash system designed to work without central management. Despite recent enthusiasm, Bitcoin and other so-called cryptocurrencies are not ideal as means for payment, because of instability of their market prices against major currencies. This paper explores the problem of such instability from the viewpoint of economics, and proposes a new monetary policy for stabilizing the values of these cryptocurrencies. First, we begin by describing the institutional details of Bitcoin.

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 an 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 takes place. This virtual real estate register record contains 21 million lots (i.e. 21 million BTCs) before sub-dividing[2]. To issue Bitcoin is to attach an ID number to each BTC lot, and a settlement of BTC is to replace the ID number by a new number[3].

[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).

[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

As of October, 2018, 17.31 million BTCs have been issued in the market with ID numbers (about 82% of 21 million BTCs). As of 2018, roughly every ten minutes on average, 12.5 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 28, 2012. It remained the same reward per ten minutes until it was halved to 12.5 BTCs per ten minutes on July 9, 2016[5], and this halving process will continue until 2140 when new issue of BTC will be terminated. Total circulation of BTC will be fixed at little less than 21 million BTCs.

There are differences between a real estate registry system and the Bitcoin system. In Japan, for instance, 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 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. To be more precise, the Bitcoin protocol authenticates a genuine Bitcoin registry book in which a chain of blocks or *blockchain*, after branching, extends the longest[6]. 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 collective selfish mining that command more than 1/3 of the whole resources[7], given the delayed finality confirmation structure we describe 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 the large number of segments with a relatively small number of accounts[8]. The reason why the Bitcoin

---

this metaphor by a real estate register record captures an essence of BTC trading.

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

[5] Four years after January 2009 and November 2012 must be January 2013 and November 2016, respectively. The actual events seem 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 II, the meaning of block extension is fully explained.

[6] According to Nakamoto (2008), the system is supposed to authenticate the longest blockchain, in practice, however, the chain whose "total difficulty", which is the sum of difficulties to win the mathematical lottery associated with each block in the chain, is the greatest (therefore usually the longest chain) prevails.

[7] 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. It points out that collective miners having over as little as 33% of the total computational power (instead of widely believed 50%) can cheat the system with selfish mining and earn more than their fair share.

protocol employs the real estate-like registry system, rather than the bank deposit-like account system is probably because Nakamoto and his collaborators think that it is suitable for decentralized processing.

The Bitcoin protocol uses a hash value[9] of a beneficiary's public key as its ID number. A hash value is a sort of digest of original data, which is 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.

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

This competition of validation is open every ten minutes on average. 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 blockchain. Newly created Bitcoin received as a reward for validation can be used for payment after a reasonably long blockchain is extended (i.e. long enough to prevent disputes over double spends)[10]. The Bitcoin protocol

[8] For example, in case of ten-trillion-yen deposits by 1000 million people, although it is 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.

[9] A hash value is the value returned by a hash function that maps data of arbitrary size to data of fixed size. A cryptographic hash function is a one-way hash function, so that it is practically impossible to recreate the input data from its hash value. The same hash value will always result from the same data, but modifying the data by even one bit will completely change the hash value. In this paper, the term *hash value* is used to denote the value returned by a cryptographic hash function. Bitcoin uses SHA-256 and RIPEMD-160 hash algorithms to generate identifiers from public keys, and applies SHA-256 twice to generate verifiably "random" numbers from a block in a way that requires a predictable amount of computational effort as described in section II.

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

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 on average), a parameter that determines a difficulty of computation is reset to make the block 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 extension process after confirming all past transactions:

(1) The hash value h_0 of the immediately previous block,
(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) and Back (2002). 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.

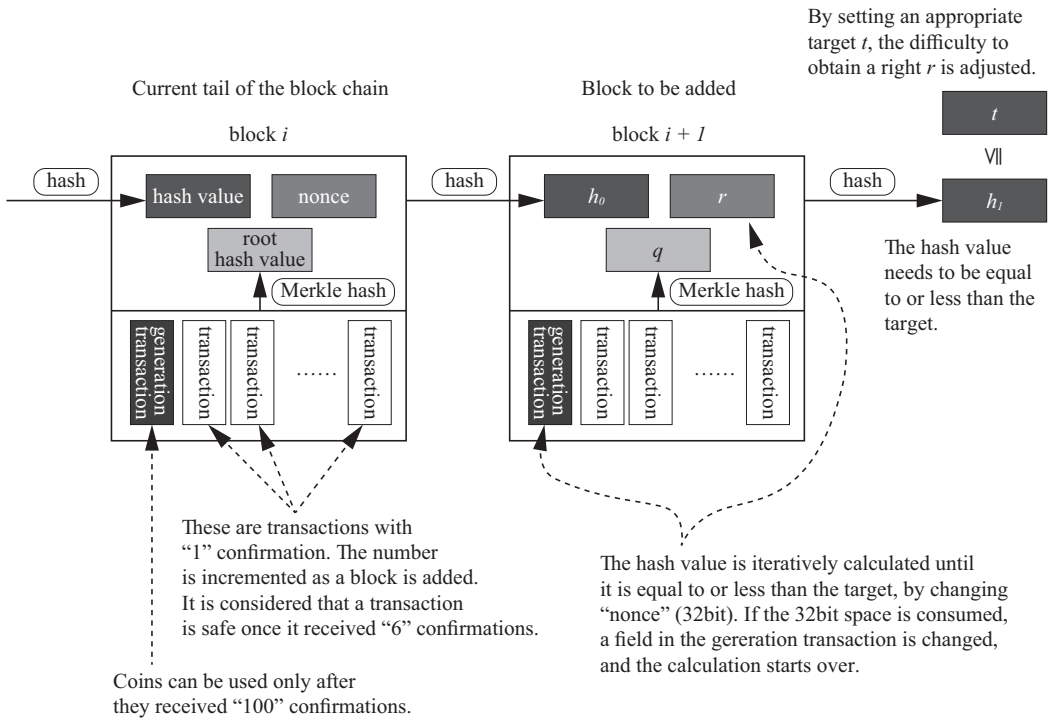
III. *Proof of Work or Proof of Waste?*

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 function would drop sharply[12]. If the difficulty (as measured by parameter

used after 100-block 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 creation in every 2016-block extensions (if one block is created in ten minutes, 2016 blocks are equivalent to two weeks), and makes parameter adjustment.

FIGURE 1. FLOW CHART OF THE PROOF OF WORK



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[13].

However, the original design by Nakamoto is intuitive. Note, in this paper, we use t and n interchangeably since $t=2^{256-n}-1$. Then,

(1) If n is zero, search value r, given h_0 and q, can be any value.
(2) If n grows gradually from zero, the probability to find a search value r becomes rapidly smaller (if n increases by 1, the probability gets halved).

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

[12] 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 $1/2^{256-\log_2 t}$.

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

the speed of block formation to stay more or less constant at ten minutes on average.

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[14]. The impact of technological 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 we 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 θ for such a rare event is an inverse of the probability of event, thus $\frac{1}{\theta}$ is defined as $1-(1-\lambda)^M$. Approximating $\frac{1}{\theta}$ by the first-order Taylor expansion at $\lambda=0$ leads to $\frac{1}{\theta}\approx M\lambda$, or

$$\theta\approx\frac{1}{M\lambda} \tag{1}$$

Miners try to find some number less than or equal to 2^{256-n} among 2^{256} possibilities. Consequently, the winning probability λ is proportional to $\frac{2^{256-n}}{2^{256}}$ at the coefficient of computational power K.

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

Substituting eq.(2) into eq.(1), we obtain

$$\theta\approx\frac{2^n}{KM} \tag{3}$$

The average time of a block validation (the average waiting time for the miner to find r) is determined as follows:

(1) It increases as difficulty n for the proof of work at the speed of 2^n.
(2) It decreases in inverse proportion to the number of miners M and
(3) It decreases in inverse proportion to the computational power.

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

The difficulty parameter n for the proof of work was 32 in January 2009, raised to 40 by December 2009, raised to 62 by December 2013, and is 74 as of October 2018. These changes cannot be explained by increases in computational technological change, but must reflect the fact that many new miners entered in mining competition.

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 12.5 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 their 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[15].

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.

[15] Of course, we need to consider how fair mining competition is. But if the loser 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.

FIGURE 2. MARKET PRICE OF BITCOIN IN USD AS OF OCTOBER 7, 2018

Source: blockchain.com

FIGURE 3. SUPPLY AND DEMAND OF BITCOIN: CASE OF A VERTICAL SUPPLY CURVE

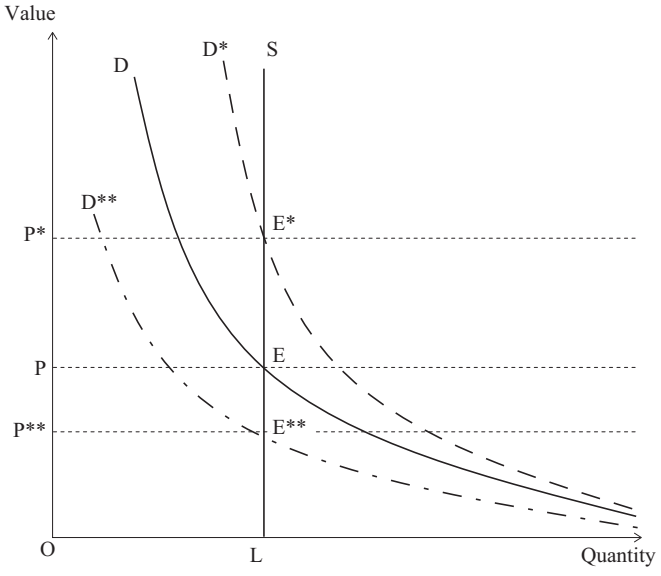
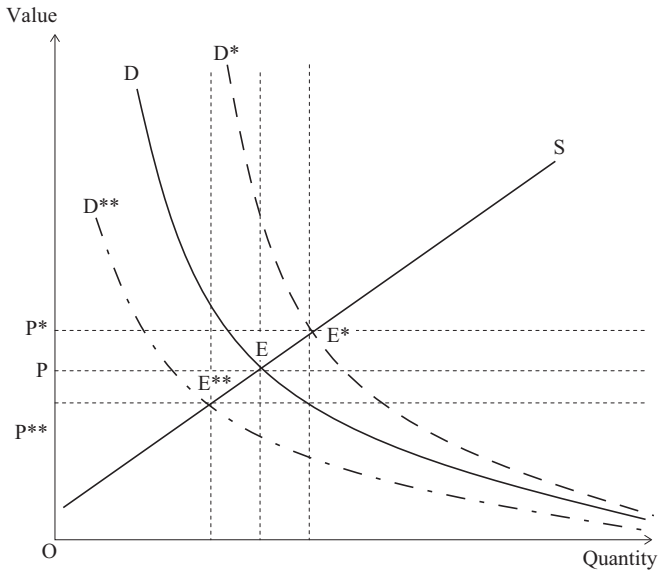


FIGURE 4. SUPPLY AND DEMAND OF THE GOLD COIN: CASE OF UPWARD SLOPING SUPPLY CURVE



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[16] 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. 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 less volatile due to this supply elasticity[17]. The price volatility of Bitcoin may reflect a rather naïve

[16] 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.

[17] 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

understanding by the designers of the Bitcoin system that the monetary value of Bitcoin would be stabilized with a fixed money supply rule.

IV. *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 power 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, 12.5BTC per ten minutes, Z would be about 75) regardless of entry and exit of miners[18]. Assuming that the Bitcoin protocol sets n properly, Z would be fixed for a length of an hour. This fact is reflected in the vertical supply curve of Figure 3.

As we make two assumptions: 1) the winning probability is proportional to the computational power, and 2) the power is evenly distributed among M miners, 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. We argue that this equals to the marginal cost of mining (mc) at equilibrium.

$$mc = \frac{PZ}{M} \tag{4}$$

If the mining cost is lower than PZ/M, then the miners obtain net benefit/return, and vice versa. Let us reflect these aspects in the past one year or so.

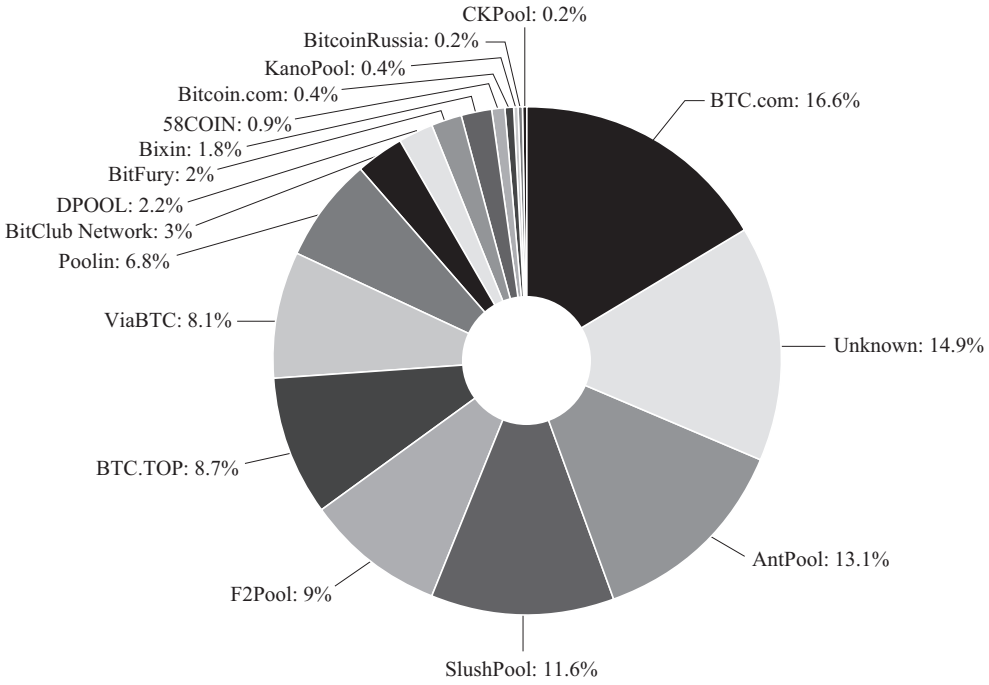
(1) If the market value of expected reward PZ/M exceeds the average cost of adding one unit (it is given exogenously by a technological change), new entry would increase. But as M increases accordingly, the expected reward/return per unit (average productivity) would drop. Eventually new entry would 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 M decreasing, the

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.

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

FIGURE 5. SHARE OF MINING POOL AS OF OCTOBER 7, 2018



Source: blockchain.com

expected return per unit would recover. This situation could happen when the mining is conducted in a spare time of mainframe computer. This can be 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[19]. 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[20]. The current situation resembles a heavy equipment industry in which it is easy to enter, but it is difficult to exit because of large sunk costs.

(4) Suppose that the Bitcoin price drops by a 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

[19] 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.

[20] This movement is consistent with change in difficulty parameter n. As eq.(3) indicates, an increase in n (from n to $n+1$) is equivalent to double the number of miners units M.

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[21]. 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[22]. If that is the case, the miners' exit 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[23].

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[24]. The current situation of the Bitcoin system can be interpreted

[21] 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.

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

[23] 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 V-5.

[24] 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

as a freezing equilibrium with dual instability.

V. *Monetary Policy without a Central Bank*

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 IV.

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, because the expected waiting time θ is affected by n, and Z is given as follows.

$$Z=\frac{V}{\theta} \tag{5}$$

In theory, both rules affect the market value of IBC equally. The above discussion can be 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.

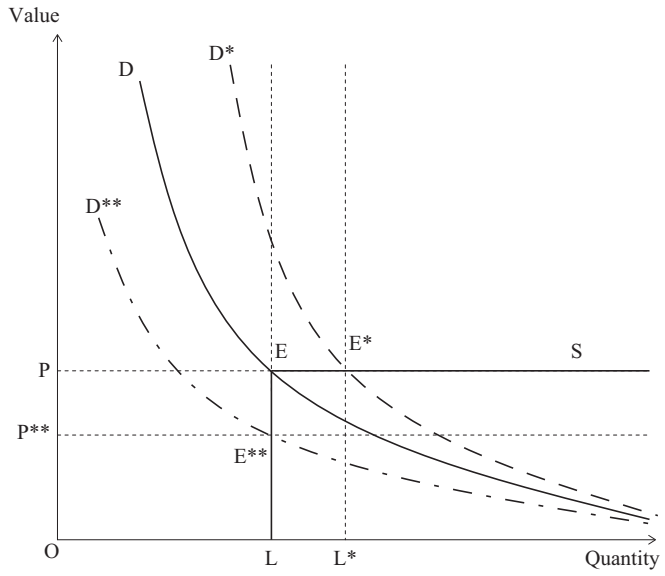
This method has a serious defect: to reduce the new issue of IBC to zero is not equivalent to absorbing excess IBC in circulation. Figure 6 illustrates the kinked supply curve of IBC, with current point E as a refraction point (for simplicity, let us assume supply and demand equilibrates at E). A positive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

---

the price of Bitcoin mining dedicated IC chip. That, in turn, makes exit more difficult. This could be the worst scenario for the miners.

FIGURE 6. SUPPLY AND DEMAND OF IMPROVED BITCOIN: CASE OF KINKED SUPPLY CURVE



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?

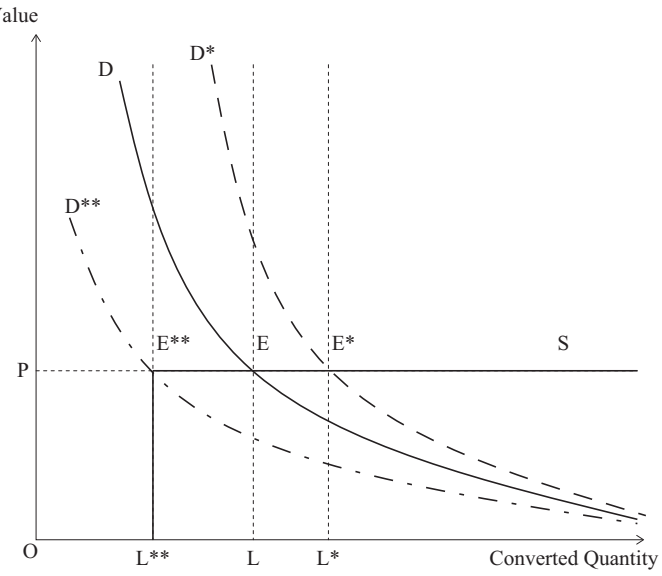
2. Built-in Revaluation Rule for Exchange Rate

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. Here, an inflation rate is defined in terms of not P, but 1/P. 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

FIGURE 7. SUPPLY AND DEMAND OF IMPROVED BITCOIN: CASE OF AMENDED SUPPLY CURVE



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.

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 V-1 and V-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 we can construct an IBC supply schedule similar to Figure 6. Here the demand and supply adjustment presumes new entry of the IBC miners.

Recall in Section III we obtain the following result, $\theta \approx 2^n/KM$. The current Bitcoin system

adjusts difficulty parameter n to stabilize an average waiting time θ as the number of miners M increase. What will happen if n is not adjusted to an increase in M? From eq. (3), θ will shrink inversely proportional to M. If a reward for the proof of work V is fixed for a block formation, 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 shorten. That has merit, but, at the same time, the risk of admitting double spends increases.

Now the IBC system has acquired a built-in revaluation mechanism[25]. 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.

4. Implicit Inflation Target in Cryptocurrency

As discussed in Section V-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?

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 rate γ[26], the IBC mining cost per hour decreases at the rate of γ; market participants expect inflation at $\beta+\gamma$ per hour and the real value of IBC would drop. Its mathematics is as follows. Substituting eq.(5) and eq.(3) into eq.(4) leads to

$$\frac{1}{P}=\frac{1}{mc\cdot M}\frac{V}{\frac{2^n}{KM}}=\frac{V}{mc}\frac{K}{2^n} \tag{6}$$

Suppose that the computational power K and the difficulty parameter n are fixed, that the marginal cost mc decreases at the gross rate of γ thanks to a technological progress where $mc_\tau=mc_0\exp(-\gamma\tau)$, and that the reward per block formation grows at the gross rate of β where $V_\tau=V_0\exp(\beta\tau)$. Then, the price level of Bitcoin $\frac{1}{P}$ inflates at the net rate of $\beta+\gamma$ where $\frac{1}{P}=\frac{V_0}{mc_0}\frac{K}{2^n}\exp((\beta+\gamma)\tau)$.

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

[25] 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.

[26] As technological change increases K, the computational power, IBC supply per hour will increase through shortening θ. We assume the technological change rate γ is exogenously given.

range between D and D^{**}, such a shock can be absorbed perfectly. Taking inflation expectation in the IBC valuation into account, 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[27]. 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.

5. Another Demerit and Another Merit of Bitcoin as Currency

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 by major central banks? In this section, we note one of many possible problems with such cryptocurrencies.

Cryptocurrencies are more expensive to produce while they cannot be absorbed once produced. 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. Also, bank notes are reversible between new issues and absorption because the central bank basically buys and sells securities with bank notes.

These 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 points.

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 (Hayek (1976)) 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 crypto-currencies.

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[28]. 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

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

[28] 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.

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[29].

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 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[30].

VI. *Conclusion*

Why Bitcoin did not exist until recently? Decentralized money provision, and similar economic systems with P2P (Peer-to-Peer) 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 their 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 they 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). We hope that Satoshi Nakamoto's important contributions can nullify their misunderstandings. We are grateful to Satoshi for the imperfect Bitcoin innovation. There remains much room for improvement, and for discussion of our future monetary system.

---

[29] 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.

[30] 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.

References

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

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

Eyal, I. and E.G. Sirer (2013), "Majority is not Enough: Bitcoin Mining is vulnerable", mimeo, Cornell University. Also (2018) in Communications of the ACM, Vol.61, Issue 7, pp.95-102

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

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

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

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

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

Keynes, J.M. (1924), *A Tract on Monetary Reform*, Macmillan.

Keynes, J.M. (1936), *The General Theory of Employment, Interest and Money*, Macmillan.

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

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