Discussion Paper Series A No.602

Is Bitcoin the Only Cryptocurrency in the Town? Economics of Cryptocurrency and Friedrich A.Hayek

Mitsuru Iwamura
(Graduate School of Commerce, Waseda University)
Yukinobu Kitamura
(Institute of Economic Research, Hitotsubashi University)
and
Tsutomu Matsumoto
(Faculty of Environment and Information Sciences,
Yokohama National University)

February, 2014

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

Is Bitcoin the Only Cryptocurrency in the Town? Economics of Cryptocurrency and Friedrich A.Hayek

Mitsuru Iwamura, Yukinobu Kitamura and Tsutomu Matsumoto*

February 28, 2014

Abstract

This paper overviews the entire landscape of Bitcoin-like cryptocurrencies. Bitcoin has not emerged out of cryptocurrency competition, but rather became a dominant currency as the first broad market based cryptocurrency. But there are more than a hundred of cryptocurrencies in the market, and some are catching up to Bitcoin. This is a healthy sign of currency competition á la Hayek. Through this competition new technological and security innovations may emerge. In this paper, we point out potential problems with Bitcoin and propose some ideas for an alternative cryptocurrency.

Key words: Bitcoin, Cryptocurrency, Friedrich A. Hayek.

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), and 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). Address correspondence to kitamura@ier.hit-u.ac.jp

1. Introduction

The major characteristics of the Bitcoin system can be summarized as follows[1]:

(1) No authority is responsible for issuing and managing the Bitcoin system. It has operational rules open to everyone (i.e. transparent). No discretionary intervention is expected to happen. According to Nakamoto (2008), "a purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution".

(2) In order to verify that an owner does not double-spend a coin, the Bitcoin system uses a timestamp procedure on a peer-to-peer basis. All Bitcoin transactions are organized in the log into blocks, which contain a sequence number, a timestamp, the cryptographic hash of the previous block, some metadata, a nonce, and a set of valid Bitcoin transactions. The block forms a hash chain; each new block contains the cryptographic hash of its predecessor, allowing anyone to verify that no preceding block has been modified.

(3) Any player may choose to become a miner and mine new blocks that add new transactions to the log. A new block is a valid addition to the log if its nonce is chosen so that the new block's hash is less than a target value. This procedure is called the proof-of-work[2].

(4) Nakamoto (2008) also argues that the proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU

[1] Here we basically follow Nakamoto (2008).

[2] The logic of this procedure has been used earlier, for example, in Hashcash by Back (2002).

power is controlled by honest nodes, the honest chain will grow the fastest and outplace any competing chains[3].

(5) To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour[4].

(6) Incentive is paid for the proof-of-work. Every few years the creation rate of Bitcoin is halved, namely, it was 50 Bitcoins in 2009-2012, 25 Bitcoins in 2013-2016, 12.50 in 2017-2020, 6.25 in 2012-2024, and so on to zero in 2140[5]. Incentive is also paid by transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. After reaching the total supply limit at 21 million Bitcoins, the incentive falls entirely on transaction fees.

Many researchers and policy makers, including the chairman of Federal Reserve Board, Ben Bernanke, have commented on the Bitcoin system in recent years[6]. Many security experts and programmers focus on security issues, whilst policy administrators and central bankers care about policy effectiveness and controllability implications. From an academic researcher's point of view, it is

[3] This point is challenged by Eyal and Sirer (2013). They propose a practical modification to the Bitcoin protocol that protects against selfish mining pools that command less than 1/4 of the resources.

[4] The Bitcoin system controls new Bitcoin issues about every 10 minutes by its program. Because of increasing computing speed and enthusiastic mining activities among professional programmers and hardware makers, the difficulty of calculation expressed in its mathematical digits increased from n=32 on January 3, 2009, to n=40 on December 30, 2009 and to n=62 now. According to Vance and Stone. (2014), "mining was supposed to be a democratized thing, but it's now only accessible to the elite of the elites".

[5] By program, new Bitcoin releases continue for more than a hundred years.

[6] Ben Bernanke actually wrote "while these types of innovations may pose risks related to law enforcement and supervisory matters, there are also areas in which they may hold long-term promise, particularly if the innovations promote a faster, more secure and more efficient payment system". (A letter to the Bitcoin Senate hearing on November 18, 2013).

important to consider Bitcoin in the entire space of the financial system. Currently Bitcoin's share of the global financial system is minute; no financial authority need worry about Bitcoin's impact on financial markets in the near future. But, as Bernanke remarked, it could have a profound impact on the payment system in the long-run.

It is worthwhile to consider the Bitcoin system from a wider perspective. In this paper, we will interpret and investigate the Bitcoin system mainly from the viewpoint of economics as such is missing from the literature. We will discuss two issues in particular: first the pricing mechanism of Bitcoin, and second the money supply rule and its implications for interest rates and inflation/deflation.

The paper is organized as follows: Section 2 discusses the intrinsic price instability of Bitcoins; Section 3 considers interest rate and inflation/deflation under the Bitcoin system; Section 4 provides our proposals for alternative cryptocurrencies; Section 5 concludes.

2. Price Instability

One of the problems with Bitcoin is the instability of its market value in the exchange market. This phenomenon partly reflects the weakness of regulations over Bitcoin. It may also reflect the total issue limit (i.e. 21 million Bitcoin) and issue patterns (at every 10 minutes with decreasing amounts over time). As of February 2014, the total number of Bitcoin in circulation so far was just above 12 million Bitcoin that are traded at a value of approximately 624.20USD/ Bitcoin[7]. Once market participants in Bitcoin start considering the terminal value (i.e. the value of the last Bitcoin issue), they would think about the exact date of the last issue, mining cost of the last

[7] In February 2012, it was 6 USD/Bitcoin. Thus the price of Bitcoin went up 100 times in exactly two years.

Bitcoin, and the discount rate to calculate the present value of the last Bitcoin, in comparison with the current Bitcoin value.

The pricing mechanism of Bitcoin may have some resemblance to pricing to the oil field exploration rights[8]. Bitcoin values can be expressed in the general form;

$$\mathrm{V(Bitcoin)} = \mathrm{MPC(Bitcoin)} + \mathrm{V(Credibility)} + \mathrm{V(Bubble)} \qquad (1)$$

Where MPC=marginal production cost, V stands for value function.

Note that V(Bubble) is not observable *ex ante*. It can be calculated *ex post* such that

$$\mathrm{V(Bubble)} = \mathrm{V(Bitcoin)} - \mathrm{MPC(Bitcoin)} - \mathrm{V(Credibility)} \qquad (2)$$

By the construction of the Bitcoin protocol, we do not know anything about the credibility and liability of a specific issuer of Bitcoin, so that V(Credibility)=0[9]. Marginal production costs can be a very small for Bitcoin issuer while marginal production costs for miners cannot be negligible. In this case, we use the marginal production cost of miners[10]. Given the total final supply limit, the Bitcoin system may or may not create a bubble[11].

[8] Of course, it is fundamentally an asset pricing model. Asset price corresponds to the present value of a cost of producing assets plus an expected normal return of holding assets plus an expected capital gain due to the real demand increase and the speculative demand that leads to the bubble. See Duffie (1996), Back (2010) and Pennacchi (2008) for more formal discussions of the asset pricing model.

[9] Alternatively we can argue that credibility is a matter of comparison. Common people in Cyprus may prefer to shift their cash into Bitcoin because it may be more reliable and safer than to keep their cash in the banks in Cyprus.

[10] Marginal production cost is an increasing function of the amount of Bitcoin in circulation, i.e., production technology of Bitcoin is an increasing return to scale.

[11] We wonder whether Bitcoin is an oil-like useful natural resource, or rather an ammonite-like (precious but useless) natural resource. If everyone thinks Bitcoin resembles ammonite because it is simply a set of figures, with no other use, then a bubble would not be created. On the other hand, if many people believe Bitcoin resembles oil, then a bubble could be created. The time-series data of Bitcoin-USD exchange rate indicates that until January 2013, 32USD/Bitcoin was the highest rate. Then, it shot up to 266USD/Bitcoin in April 2013 and it reached

From Eq.(2), however, we can expect that the bubble will burst as MPC(Bitcoin) will increase in the near future. As is always the case, the size of the bubble can be measured only *ex post* and we cannot forecast exactly when the bubble will burst.

Let us elaborate on this as a paradoxical situation emerges here. As the Bitcoin fever grows, it attracts increased public attention and consequent monetary transactions (i.e. exchanged with US Dollar, Euro, Yen, and Renminbi). As a result, the market value of Bitcoin shoots up. This also attracts mining activity. Many professional engineers and programmers participate in Bitcoin mining on a full-time basis, as is fully illustrated in Vance and Stone (2014). This makes Bitcoin mining very competitive and there is no possibility to mine Bitcoin on layman's computers[12]. By construction, rewards from mining have been declining as the total supply of Bitcoin is binding, while the costs of mining can be increasing because of high technology competition for scarce resources. Eventually miners of Bitcoin will find mining activity to no longer be profitable.

Consider that, in the five years since its launch, more than half of total potential Bitcoin have already entered circulation. It is likely that the creation rate of Bitcoin will drop sharply from now on. This Bitcoin incentive distribution mechanism might reflect a simplicity of programming (halving the incentive every few years). But it gives too-generous incentives for the initial miners/participants and too little for the later comers[13]. With this incentive mechanism it will be very difficult to sustain the current number of miners for the next 100 years; they will have to go somewhere else. In addition, if miners

900USD/Bitcoin in November 2013. Therefore there seems to be a bubble in 2013-2014. This bubble element makes Bitcoin pricing indeterminate.

[12] The Bitcoin mining activity will be monopolized by a small number of computer experts due to the fact that Bitcoin production technology is an increasing return to scale.

[13] Mathematically it is a simple series such that $S=1+1/2+(1/2)^2+\ldots+(1/2)^n$. Suppose, for simplicity' sake, if n becomes infinite, then S=2. Approximately the initial miners take a half of incentives and the rest is divided by the numerous later comers.

begin leaving Bitcoin mining, the market value of Bitcoin would drop, the profitability of mining would drop further, and the immigration of miners would accelerate[14].

Where will these professional miners go? There exist more than a hundred of Bitcoin-like cryptocurrencies in the market. Although technical details may differ, the fundamental framework may remain identical to the Bitcoin system. It is likely miners can easily migrate to other promising mines[15].

Indeed, other cryptocurrencies have already achieved substantial market capitalizations: Ripple is now 20% of Bitcoin and Litecoin is 5% of Bitcoin as of February 21, 2014. We know followers can start from where the Bitcoin system reaches and improve upon it[16]. Although we have not recognized any revolutionary improvements in cryptocurrencies other than Bitcoin, we anticipate substantial improvements would eventually be made. It is important for us to distinguish both technical and security variations between cryptocurrencies[17]. Then we can assign to different cryptocurrencies different fair prices and exchange these currencies in the market. This is the currency competition Friedrich A. Hayek insisted upon.

Hayek (1999) states "once the system had fully established itself and competition had eliminated a number of unsuccessful ventures, there would remain in the free world several extensively used and

[14] Vance and Stone (2014) indicate that mining revenue per operation has fallen to near zero level already in January 2014.

[15] This is exactly what happened in the gold mining and oil field exploration in the past. Note that as is usual the cases with the gold mining, the miners do not make a big money. Those who sell tools and donkeys to the gold miners earn most. Those who design the cryptocurrency mining computers and its specialized chip may earn most, apart from the initiators of Bitcoin.

[16] Historically copycat currencies always follow genuine money. In a sense, Bank of Japan notes and Bank of England notes are also copycats of the previous bank notes. Miers, Garman, Green and Rubin (2013) proposes Zerocoin as an extension of Bitcoin such that the protocol allows for fully anonymous currency transactions.

[17] If we cannot distinguish a good currency from a bad currency, then Gresham's law would prevail, i.e. a bad currency would drive out a good currency. On this issue, see for example, Camera, Craig and Waller (2002) and Martin and Schreft (2006).

very similar currencies. In various large regions one or two of them would be dominant, but these regions would have no sharp or constant boundaries, and the use of the currencies dominant in them would overlap in broad and fluctuating border districts. Most of these currencies, based on similar collections of commodities, would in the short run fluctuate very little in terms of one another, probably much less than currencies of the most stable countries today, yet somewhat more than the currencies based on a true gold standard. If the composition of the commodity basket on which they are based were adapted to the conditions of the region in which they are mainly used, they might slowly drift apart. But most of them would thus concur, not only in the sense of running side by side, but also in the sense of agreeing with one another in the movements of their values." (p.223)

The currency competition we see now in cryptocurrencies has a merit of its own. As alternative cryptocurrencies attract more miners and participants, the bubble elements of Bitcoin would be removed[18]. The pricing of each cryptocurrency will be based on the fundamentals, i.e. the marginal production costs and expected normal returns from holding.

In the next section, we will discuss whether we can expect a normal return from holding a cryptocurrency.

3. Where is the Interest Rate in a Cryptocurrency system?

Legal tender and central bank notes and coins do not generate any interest: zero interest rates. But if you deposit them in the banks or other financial institutions, you usually earn interest income.

[18] It should be noted there would not be a problem even if the price of Bitcoin should fall sharply after the removal of bubble elements. Every participant should understand all price movements are due to changes in market valuation. The government and the central bank do not need to do anything because it is purely private activity in the free market. If, on the other hand, the government and the central bank start regulating the issuers of cryptocurrencies, they would create responsibilities and accountabilities. That would, in turn, distort the pricing mechanism.

Bitcoin and other cryptocurrencies, as a matter of principle[19], refuse to have any relationship with the banks and other financial intermediaries[20]. Furthermore, as the price of the last Bitcoin is indeterminate as we discussed before, the interest rate is also indeterminate. It does not mean that we cannot calculate an implicit interest rate for Bitcoin, but it means the value of an implicit interest rate would be quite volatile and practically useless[21].

However, in theory, any money and currency, including cryptocurrencies, can earn interest income in exchange of lending or deposit. In fact, McCandless and Wallace (1991) demonstrate that (1) fiat money and other assets must offer the same rate of return as private borrowing and lending do and (2) if there are two fiat monies, in an equilibrium in which they both have value, they must each give the same rate of return through arbitrage. As long as Bitcoin and its followers are considered as money, it must yield the same rate of return as those from the legal tenders such as Yen, U.S. Dollar, and Euro[22].

Sooner or later, someone will create a system or derivative to generate the rate of return for lending cryptocurrencies to a third party[23].

[19] The main innovation of this type of cryptocurrency is to introduce a peer-to-peer electronic payment system. No third party involvement is the vital issue.

[20] Of course, there are Bitcoin and other cryptocurrency exchange service platform such as Mt.Gox, BitPay, and WalletBit and assorted services and goods are provided by many companies within the Bitcoin ecosysytem.

[21] Šurda (2013) empirically calculates price volatility and velocity of circulation of Bitcoin, probably for the first time. Both seem to be quite high compared with the other legal tenders.

[22] Here is an interesting research question. Since the interest rate differs among countries, the same exchange rate between the two countries differs from country to country. Bitcoin as a global currency may also face different rates of return in different countries. Is there any mechanism to adjust the rate of return for Bitcoin globally?

[23] It is a very challenging issue to design a financial intermediary under a peer-to-peer electronic payment system. The Bitcoin exchange service platform would do it.

Why did Nakamoto (2008) set a limit of total Bitcoin issues? Because he seemed to believe that a decreasing supply of money will not lead to inflation[24]. A geometrical reduction of the money supply rate does not necessarily create deflation[25]. But it will create a sharp drop in the profitability of mining activity, even if we take into account of technological growth based on the Moore's Law. We think it is this real factor that determines inflation and deflation in the Bitcoin ecosystem.

4. Proposals for Ideal Qualified Cryptocurrency

Following what we have discussed so far, we can provide some characteristics of an ideal qualified cryptocurrency (IQC).

(1) No supply limit of IQC is imposed. Or if a limit exists, it is so large that we do not need to consider the mining problem of the last issue of IQC[26].

(2) The current price of IQC must reflect the marginal cost of IQC production that, in turn, includes electricity, security and the other hardware costs.

[24] Although his paper does not refer to it, he may be influenced by the writing of Milton Friedman on his money supply rule. See Friedman (1960).

[25] Many researchers predict deflation in Bitcoin denominated goods and services due to a deflationary spiral (i.e. hoarding Bitcoin waiting for a higher purchasing power in the future).

[26] Ever since Samuelson (1958), it is well known that intrinsically useless fiat money can have value only in economies with no known terminal date. Imagine the final day of the earth, no one accepts money because no use after the final day, by backward induction, no one accepts money today. In the literature of economics, finance, game theory, and philosophy, it is crucially important to distinguish between infinite and finite horizon models. In case of the finite horizon model, we solve the problem by backward induction, i.e. from the terminal condition to the current condition. Needless to say that it is very difficult to calculate the marginal cost of the Bitcoin production in 2140, given all sorts of uncertainty around the Bitcoin. In case of the infinite horizon model, we assume time homogeneity and solve the problem for any arbitrary date. In this case, we do not need to worry about the last day's currency production. Note, however, that the issuer of Bitcoin assumes that it will be circulated even after reaching the total supply limit of Bitcoin. A fundamental reason for setting the total limit of Bitcoin is to make a maximum size of the log before implementing Bitcoin production.

(3) The marginal cost of IQC production can be evaluated properly by market competition. The marginal cost must be set fairly constant over time[27]. In so doing, the pricing of IQC becomes easier, more transparent and more democratic. Bubble elements would be removed.

(4) Give the stable marginal cost of IQC production, the pricing of IQC becomes feasible and competitive with other currencies. The implicit interest rate can be obtained by arbitrage between the price of IQC today and that of tomorrow or of the other currency tomorrow.

(5) The marginal cost (MC) of IQC pruduction must be discounted by the technological growth (TC) via the Moore's Law and operational specifications of IQC. Let us assume that the marginal cost pricing is used for IQC such that $P_t = MC_t/TC_t$. Inflation (π_t) can be defined as $P_{t+1} = (1+\pi_t)P_t$, Let us also assume that the marginal cost of production grows at the rate of β and the technology grows at the rate of α. In the two periods, inflation can be expressed as $1+\pi_t = (1+\beta)/(1+\alpha)$, rearranging yields $\pi_t = (\beta-\alpha)/(1+\alpha)$. If the technological change rate (α) is higher than the marginal cost growth rate (β), then deflation might happen and *vice versa*.

(6) If the marginal cost of IQC production increases above a certain threshold miners will immigrate to the other mines, i.e. other cryptocurrencies. The price of the current IQC would not drop so sharply because of this voluntary action. We can expect relatively moderate price fluctuations among competing cryptocurrencies and a stability of the cryptocurrency ecosystem in general.

[27] Here we assume that the IQC production technology is a constant return to scale. This is partly due to our preference of price stability by the constant marginal cost structure and partly due to our dislike of monopolization of the mining activity by a small number of experts as is happening with the Bitcoin mining.

In this proposal, we have not discussed anything about security issues and cryptographic methodology. We are fully aware of the limitations and weaknesses of proof-of-work in the Bitcoin system. We will discuss these in separate papers.

5. Conclusion

Bitcoin will be taken over by other cryptocurrencies with similar but somewhat improved technical as well as security structures in the future. It does not necessarily imply that one empire is taken over by the other. We would rather expect many cryptocurrencies to coexist around the world. It might be described as the cryptocurrency ecosystem.

In order for this to happen, any cryptocurrency must have common, reasonable properties such as we suggested in Section 4. What is needed is a proper design of cryptocurrency based on economic rationales; such are not exhibited by the current cryptocurrency ecosystem. In the long-run, any economic system is not sustainable without proper economic rationales.

References

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

Back, Kerry E.(2010) *Asset Pricing and Portfolio Choice Theory*, Oxford University Press.

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.

Bénassy, Jean-Pascal.(2007) *Money, Interest, and Policy: Dynamic*

General Equilibrium in a Non-Ricardian World, The MIT Press.

Camera, Gabriele, Craig, Ben and Waller, Christopher J. (2002) "Gresham's Law versus Currency Competition", Purdue CIBER Working Papers, 2001/2002-001.

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

Duffie, Darrell. (1996) *Dynamic Asset Pricing Theory*, Princeton University Press.

European Central Bank (2012) *Virtual Currency Schemes*, October 2012.

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

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

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.

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.

McCandless, Jr. George T. and Neil Wallace (1991) *Introduction to Dynamic Macroeconomic Theory*, Harvard University Press.

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.

Pennacchi, George. (2008) *Theory of Asset Pricing*, Pearson /Addison-Wesley.

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.

Schelling, Thomas, C. (1960) *The Strategy of Conflict*, Harvard University Press.

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

Šurda, Peter. (2013) *Economics of Bitcoin: Is Bitcoin an alternative to fiat currencies and gold?* , Diploma Thesis, WU Vienna University of Economics and Business.

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

Walsh, Carl E.(2003) *Monetary Theory and Policy*, 2nd ed., The MIT Press.

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