Working Paper Series

No. 13-01

May 2013

Bitcoin:
A Search-Theoretic Approach

Tetsuya Saito

Research Institute of Economic Science

College of Economics, Nihon University

Bitcoin: A Search-Theoretic Approach

Tetsuya Saito[1]

[1]Ph.D. (Economics), Associate Professor of Economics, Nihon University College of Economics; Address: 1-3-2 Misakicho, Chiyoda-Ku, Tokyo, Japan 101-8360; Phone/Fax: (+81) 03-3219-3803; Email: saito.tetsuya@nihon-u.ac.jp

Abstract

This paper considers whether or not the Bitcoin stably stay in the market as a method of payment using a dual-currency money-search model. In the model, there are traditional money and Bitcoin. The two currencies are classified by the storage cost and the probability that sellers accept particular money for payments. Agents are randomly matched for transactions. To consider substitution effect between monies, we allow new entries every period. In the beginning of each period, new entrants come into the matching process with a unit of money of their choice. A certain number of sellers also come into the same process to maintain the population share of sellers at a constant level. With appropriately chosen parameters, we find that there can be stable and instable equilibria of the share of bitcoiners. In this case, a stable equilibrium is a success (bitcoiners take a large share) while the other is a failure (bitcoiners take a marginal share or vanish). However, if the inflation rate of traditional money gets smaller, the successful equilibrium disappears to start approaching the failure even if it is currently widely accepted. Furthermore, welfare comparisons suggest an increase in the share of bitcoiners has a negative effect; hence, the benefit from reductions in the transaction costs must compensate for the welfare erosion if Bitcoin is accepted as a new kind of payment system. If we are heading to the success, the Bitcoin community or the public authorities need to prepare for protecting the system from several illicit activities.

JEL Classifications: C78; E41; E42

Keywords: *Bitcoin; dual-currency; private money; peer-to-peer payment system*

1 Introduction

Bitcoin, which has been launched in 2009, is a math-based digital currency project operated by nongovernmental entities.[1] Anyone can obtain bitcoins if the one could solve a math problem (mining). The math problem gets harder as more coins are mined. The math problem is so hard that miners use computers for mining; hence, the money supply is constrained by the progress of computing technologies. Once a coin is mined, it can circulate as an ordinary coin within the Internet. Bitcoins can also be exchanged with other currencies, such as Euro and US dollar (USD). For example, Figure 1 shows the exchange rate with USD at the Mt. Gox that shows a steady increase in its value: from almost zero to $100 in May 2013.[2] According to this chart, it seems Bitcoin is heading to a success to establish a new payment method out of any authority's control.

There are several digital currencies other than Bitcoin such as eBay Anything Point, Facebook Credits, and the likes. Several new projects are also launching, such as Amazon Coin and Ripple. In addition, mileage points of commercial airlines and shopping points of credit card venders, for example, are look-alike of these digital currencies. Why Bitcoin is so focused beyond them? Recently, some major financial companies, such as Western Union and MoneyGram, are approaching Bitcoin venders.[3] In addition, public authorities, such as the Fed and the FBI, are also interested in the activities using Bitcoin, as it may help criminal activities such as money laundering and tax evasions, and may be targeted by various cyber crimes.[4]

There are three major versions of money-search model: the first generation that uses indivisible money and goods (Kiyotaki and Wright [22]); the second generation model that uses indivisible money and completely divisible goods (Trejos and Wright [34]); and the third generation model that uses completely divisible money and goods (Lagos and Wright [25]).[5] The discussion is based on a second-generation money-search model. We extend the basic model by Trejos and Wright [34] to a dual-currency model as Craig and Waller [10]. The reason to use the second generation model is due to its simplicity for extension and its capability of dealing with price differences in methods of payments.

In the dual-currency system, there are two currencies coexisting in a unified market as methods of payments. In place of keeping the seller to buyer ratio constant, this paper allows new entries of sellers and buyers. Accepting new entrants, who observe the previous period's market performance of each currency, allows correlations among parameters within each currency, and eventually an interdependence of shares of traditional money and Bitcoin users. With such a framework, we examine if Bitcoin can stay in the market as a method of payment. In addition, we consider dynamic stabilities of bargaining outcomes and population

shares of respective agent types. It is then clarified that Bitcoin may fail to exist if the inflation rate is sufficiently low relative to the storage cost (or gain) of Bitcoin. Actually, the financial crisis in Europe has brought Bitcoin on the stage. To overcome such a time on the cross, bitcoiners may have to accept major financial institutions to involve in the community.

The analysis proceeds as follows. Section 2 defines the dual-currency framework and provides some basic results. The dual-currency framework is extended to examine the dynamics of population share of bitcoiners in Section 3. In Sections 2 and 3, the key results are also examined by numerical examples. Section 4 argues social welfare with and without Bitcoin. We then conclude the discussion in Section 5. In the conclusion, we summarize the key results and provide scopes for further studies. For reference, Appendix A considers an explicit inclusion of the Bitcoin exchange market to apply the analysis of this paper without modifications.

2 Basic Framework

2.1 The Dual-Currency Model

We consider an extension of the second-generation money-search model (Trejos and Wright [34]) similar to Craig and Waller [10]. In this model, there are a traditional money and a math-based virtual money (*Bitcoin* hereafter). Each money is used as a medium of exchange. The two monies are indivisible and agents in this model are not allowed to hold more than one unit of them at one time. If an agent holds money, one is called a *buyer*. If an agent does not hold money, one is called a *seller*. By storing money beyond a period, in the beginning of the new period, the money holder accepts transferable utility γ_m, where m is an index to identify monies: $m = 1$ indicates the variable is for traditional money and $m = 2$ for Bitcoin. For convenience, we may write m-money to refer traditional money and Bitcoin for $m = 1$ and $m = 2$, respectively. If $\gamma_m < 0$, m-money is costly to store, as ordinary fiat money. If $\gamma_m \geq 0$, the m-money is not costly to store, as commodity money. Agents live infinitely long and discount the future by a common moment discount rate r. The length of each period is $\tau > 0$; for example, the periodical discount rate is then approximately τr.

Within each period, agents are randomly matched one-to-one. The frequency of matching is represented by Poisson arrival rate λ for each moment; hence, $\tau\lambda$ is the periodical arrival rate. Without loss of generality, we can set τ as small as possible to keep $\lambda < 1$ in order for λ to be the probability of meeting another person. Agents are capable of producing a differentiated good and enjoying products of others.

If an agent consumes q units of merchandise that the one likes, there is a utility repre-

sented by $u(q)$, such that $u(0)=0$, $u'(q)>0$, and $u''(q)<0$. If an agent produces q units of merchandise, as ordered by one's paired partner, there is a cost represented by $c(q)$, such that $c(0)=c_0\geq 0$, $c'(q)>0$, and $c''(q)\geq 0$. It is popular to introduce an increasing-return technology in a digital economy. Technically in the second-generation money-search framework, furthermore, an increasing-return technology $c_0>0$ allows a possibility of a deflation economy to have a stable monetary-trade equilibrium.

For simplicity, we assume that the preference of each agent is *ad hoc* and whether or not one likes paired partner's product is random at all, by probability $s\in(0,1]$; hence, s^2 provides the probability of double coincidence of wants. If there is a single-coincidence as such the buyer likes the product of the seller, there is a monetary trade. We define σ_m to be the trade-success rate when there is a single-coincidence that is decomposed as

$$\sigma_m \equiv s\alpha_m, \tag{1}$$

where α_m is the probability that the m-money is accepted by the seller. In this sense, as buyer's preference about seller's product, seller's preference about the payment method is also considered as *ad hoc*. For now, we assume that here is no correlation between the share of bitcoiners in the population μ_m and the trade-success rate σ_m.[6]

If a buyer and a seller are paired and the buyer likes seller's product, they bargain over the quantity of trade for a unit of money. In the model, for simplicity, we suppose the quantity is determined by a take-it-or-leave-it offer by the buyer.[7]

If there is a double-coincidence, the pair can choose either barter or monetary trade. In this analysis, we suppose that pairs with double-coincidence always choose barter transactions, as it is known that they obtain an instantaneous net utility that maximizes the social welfare in the barter trade: $\nu^*\equiv\max_q\{u(q)-c(q)\}$.[8]

We let $V_0(t)$ be the value function of a seller from period t on. Similarly, we let $V_m(t)$ be the value function of an m-money holder. The Bellman equation of a seller is then given by

$$\begin{aligned}(1+\tau r)V_0(t) &= \tau\lambda\sigma_1\mu_1\{V_1(t+\tau)-c(y_1)\}+\tau\lambda\sigma_2\mu_2\{V_2(t+\tau)-c(y_2)\}\\ &\quad+\tau\lambda s^2\{v^*+V_0(t+\tau)\}+(1-\tau\lambda\chi)V_0(t+\tau)+o(\tau),\end{aligned} \tag{2}$$

where $o(\tau)$ is the counting loss function, such that $\lim_{\tau\to 0}o(\tau)/\tau=0$ and χ the probability of trade of any kinds:

$$\chi=\sigma_1\mu_1+\sigma_2\mu_2+s^2. \tag{3}$$

The Bellman equation (2) is arranged to get

$$\begin{aligned} rV_0(t) &= \lambda\sigma_1\mu_1\{V_1(t+\tau)-c(y_1)\}+\lambda\sigma_2\mu_2\{V_2(t+\tau)-c(y_2)\} \\ &\quad +\lambda s^2 v^* - \lambda(\sigma_1\mu_1+\sigma_2\mu_2)V_0(t+\tau)+\frac{V_0(t+\tau)-V_0(t)}{\tau}+\frac{o(\tau)}{\tau}. \end{aligned} \tag{4}$$

For $\tau \mapsto 0$, the Bellman equation (4) reaches

$$rV_0 = \lambda\sigma_1\mu_1\{V_1 - c(y_1) - V_0\} + \lambda\sigma_2\mu_2\{V_2 - c(y_2) - V_0\} + \lambda s^2 v^* + \dot{V}_0. \tag{5}$$

The Bellman equation of a buyer that holds m-money is given by

$$\begin{aligned} (1+\tau r)V_m(t) &= \tau\lambda\theta\sigma_m\{u(x_m)+V_m(t+\tau)\}+\tau\lambda s^2\{v^*+V_m(t+\tau)\} \\ &\quad +\left\{1-\tau\lambda\left(\theta\sigma_m+s^2\right)\right\}V_m(t+\tau)+\tau\gamma_m+o(\tau), \end{aligned} \tag{6}$$

where θ is the share of sellers in the population:

$$\theta \equiv 1-(\mu_1+\mu_2). \tag{7}$$

Similarly to the Bellman equation of the seller (4), for $\tau \mapsto 0$, the Bellman of the buyer that holds m-money reaches

$$rV_m = \lambda\theta\sigma_m\{u(x_m)+V_0-V_m\}+\lambda s^2 v^*+\gamma_m+\dot{V}_m. \tag{8}$$

Since the buyer makes a take-it-or-leave-it offer, the bargaining solution $q_m = x_m = y_m$ is given by equating the IC condition of the seller $V_m - c(q_m) \geq V_0$ as

$$V_m - c(q_m) = V_0. \tag{9}$$

In this case, the value function of the seller is computed as

$$rV_0 = \dot{V}_0 + \lambda s^2 v^*. \tag{10}$$

In addition, differentiating the both sides of the bargaining rule (9) with respect to time provides the motion function of q_m as

$$\dot{q}_m = \frac{\dot{V}_m - \dot{V}_0}{c'(q_m)}, \tag{11}$$

where $\dot{q}_m \equiv dq_m/dt$. We substitute value functions (8) and (10) into (11) to get

$$\dot{q}_m = \frac{(r + \lambda\theta\sigma_m)\, c(q_m) - \lambda\theta\sigma_m u(q_m) - \gamma_m}{c'(q_m)}. \tag{12}$$

We search equilibrium that satisfies $\dot{q}_m = 0$.

Since $c'(q_m) > 0$, we now find the equation that provides law of motions of q_m as

$$\dot{q}_m \gtreqless 0 \quad \Longleftrightarrow \quad rc(q_m) - \gamma_m \gtreqless \lambda\theta\sigma_m \{u(q_m) - c(q_m)\}, \tag{13}$$

and the equilibrium is determined as depicted in Figure 2, where LHS and RHS denote the left-hand-side and the right-hand-side of the inequality (13). In this figure, the black bullet ($q_m = q_m^*$ hereafter) represents the stable equilibrium and the hollow circle the instable one. To guarantee the existence of a stable monetary trade equilibrium $q_m^* \in (0, \bar{q}_m)$, where $\bar{q}_m$ solves $u(\bar{q}_m) = c(\bar{q}_m)$,[9] parameters have to be appropriately chosen (*i.e.*, choosing modest storage cost).

If the parameter set is not appropriately chosen, the stable equilibrium disappears. If the intercept of $LHS(1)$ is less than the intercept of $RHS(1)$, $rc_0 - \gamma_m < -\lambda\theta\sigma_m c_0$, only the instable equilibrium *can* exist, but a small perturbation drives out the instable equilibrium to $q_m = 0$ or $q_m = \bar{q}_m$. If $LHS(1)$ locates above $RHS(1)$ for each q_m, the stable and the instable equilibria disappear and the market approaches $q_m = \bar{q}_m$. In case of $q_m = 0$ or $q_m = \bar{q}_m$, the value of monetary transaction using m-money vanishes and then m-money cannot stay in the market as a method of payment.

It is noteworthy that the equilibrium of our dual-currency model behaves *as if* a standard single-currency model *à la* Trejos and Wright [34] so long as the share of sellers in the entire population $\theta \equiv 1 - (\mu_1 + \mu_2)$ is fixed and there is no correlation between μ's and σ's, as the equilibrium of m-money is dependent only on *own* parameters, such as σ_m and γ_m, and *common* parameters, such as θ, λ, and r.

Remark 1 *For each m, if there is no correlation between μ's and σ's, $dq_m^*/d\sigma_m < 0$ and $dq_m^*/d\gamma_m < 0$, and $dq_m^*/d\sigma_k = dq_m^*/d\gamma_k = 0$ for $k \neq m$.*

Proof. Since there is no correlation between μ's and σ's, From (13) shows that an increase in σ_m makes a downward shift of RHS in Figure 2 to reduce q_m^*. Similarly, an increase in γ_m makes a downward shift of LHS to reduce q_m^*; hence, $dq_m^*/d\sigma_m < 0$ and $dq_m^*/d\gamma_m < 0$. Changes in σ_k and γ_k ($k \neq m$) do not affect (13); hence, $dq_m^*/d\sigma_k = dq_m^*/d\gamma_k = 0$. ■

2.2 New Entries

The basic framework is defined to be similar to Craig and Waller [10]. We now introduce new agents that observe the market of previous period to come into the matching process in the beginning of current period. To enter the process, there are three options: (1) entering as a traditional-money holder, (2) entering as a bitcoiner, and (3) entering as a seller (non money holder). In order to keep θ constant, the population of new sellers is given exogenously depending on the population of new buyers.

We suppose that the hours to work to obtain a unit of money m for agent i to join the matching process is given by $L_m^i > 0$. For example, an agent that wants to bring traditional money needs L_1^i hours as a waged worker. If an agent wants to bring bitcoins, one needs L_2^i hours for mining. If one can obtain Bitcoin in a market, such as Mt. Gox, eBay, and the likes, at rate π_i, we define L_2^i to be hours to work to purchase a unit of Bitcoin, as $L_2^i = \pi_i L_1^i$ (Appendix A briefly verifies the inclusion of an exchange market).[10] The disutility from working L_m^i hours is given by a linear form as ξL_m^i, where $\xi > 0$ is a preference parameter. Agent i then brings traditional money into the matching process if

$$V_1 - \xi L_1^i > V_2 - \xi L_2^i \quad \Longrightarrow \quad V_1 - V_2 > \xi \left(L_1^i - L_2^i \right), \tag{14}$$

where $\delta_i \equiv \xi \left(L_1^i - L_2^i \right)$ is distributed as cumulative distribution $F(\delta_i)$ with probability distribution $F'(\delta_i) \equiv f(\delta_i)$. Similarly, agent i brings Bitcoin if

$$V_1 - \xi L_1^i \leq V_2 - \xi L_2^i \quad \Longrightarrow \quad V_1 - V_2 \leq \xi \left(L_1^i - L_2^i \right). \tag{15}$$

To compute the left-hand-side of conditions (14) and (15), $V_1 - V_2$, we consider

$$\dot{V}_m - \dot{V}_0 = (r + \lambda\theta\sigma_m)(V_m - V_0) - \lambda\theta\sigma_m u(q_m^*) - \gamma_m = 0, \tag{16}$$

which provides

$$V_m - V_0 = \frac{\lambda\theta\sigma_m u(q_m^*) + \gamma_m}{r + \lambda\theta\sigma_m}. \tag{17}$$

Thus, $V_1 - V_2$ is computed as

$$V_1 - V_2 \equiv D(\bullet) = \frac{\lambda\theta\sigma_1 u(q_1^*) + \gamma_1}{r + \lambda\theta\sigma_1} - \frac{\lambda\theta\sigma_2 u(q_2^*) + \gamma_2}{r + \lambda\theta\sigma_2}. \tag{18}$$

Axiom 1 *If Bitcoin is normal, an increase in σ_2 increases the share of bitcoiners; hence, $dD/d\sigma_2 > 0$. Similarly, in this case, an increase in γ_2 increases the share of bitcoiners; hence, $dD/d\gamma_2 > 0$.*

Based on conditions (14) and (15) and Axiom 1, we find the distribution of shares of respective money types, as depicted in Figure 3. This figure plots $D(\sigma_2; \dots) = V_1 - V_2$ in the right-half space to take δ_i for the vertical axis. In the left-half space, the density function $f(\delta)$ is placed in order to obtain the shares of respective money types in the population of new entrants: the darker area corresponds to the share of bitcoiners, $F(\delta)$, and the brighter area the share of traditional-money holders, $1 - F(\delta)$.

Proposition 1 *If Bitcoin is normal as in Axiom 1, for a given σ_2, the share of bitcoiners in the population of entrants increases if γ_1 decreases (e.g., further inflation of traditional money) or γ_2 increases (e.g., further deflation of Bitcoin).*

Proof. By symmetry of the problem described in (18), the sign of derivative of D-function with respect to γ_1 is opposite to the sign of $dD/d\gamma_2$; hence, Axiom 1 implies $dD/d\gamma_1 < 0$ by $dD/d\gamma_2 > 0$. Therefore, a decrease in γ_1 and an increase in γ_2 make upward shifts of D-function in Figure 3. This implies an increase in the share of bitcoiners for a given σ_2, as stated in this proposition. ■

2.3 A Numerical Example

For numerical analysis, we provide utility and cost functions as

$$u(x) = \log(x+1) \quad \text{and} \quad c(y) = 0.1y + 0.5. \tag{19}$$

We assume that the probability that a traditional-money holder always likes seller's product and the seller always accept traditional money for payment; hence, $\sigma_1 \equiv 1$. Bitcoin holders also always like respective seller's product. However, some sellers do not accept bitcoins for payment. In this case, we have $\sigma_2 < 0$. The share of sellers in the population and the arrival rate are a half ($\theta = 0.5$ and $\lambda = 0.5$). The traditional money is costly to store and its inflation rate is given by either 3% or 5% ($\gamma_1 = -0.03$ or -0.05). The discount rate is supposed to be 5% ($r = 0.05$).

Using above parameters, Figure 4 shows the result for $\sigma_2 \in [0, 1]$ and $\gamma_2 = \{-1\%, 1\%, 2\%\}$ that are consistent with Axiom 1 and Proposition 1.

3 Dynamics of the Share of Bitcoiners

3.1 An Extension

We allow a correlation between μ_m and σ_m that implicitly allow a correlation between traditional money and Bitcoin. In this case, Remark 1 does not hold as it is due to feedback

effects, but the independence between the two currency is still held. The revision of the remark is formally provided as follows.

Remark 2 *If there is a correlation between μ_m and σ_m, Remark 1 holds as partial effects instead of total effect; hence, $\partial q_m^*/\partial \sigma_m < 0$ and $\partial q_m^*/\partial \gamma_m < 0$, but the independence between the currencies is still held: $dq_m^*/d\sigma_k = dq_m^*/d\gamma_k = 0$ for $k \neq m$.*

For more detailed arguments, we extend our model by setting up the rule of correlation of the two parameters. We suppose s is constant overtime. In this case, the dynamic version of σ_m is given by

$$\sigma_m(t) \equiv s\alpha_m(t). \tag{20}$$

We assume that sellers always accept traditional money while they may not accept bitcoins:

$$\alpha_1(t) \equiv 1 \quad \text{and} \quad \alpha_2(t) \in (0,1). \tag{21}$$

The correlation between μ_m and σ_m is actually a correlation between μ_m and α_m, as s is stationary and of buyer's preference; hence, the relationship between μ_m and σ_m is obtained as

$$\alpha_2(t+\tau) = \phi[\mu_2(t)] \quad \Longrightarrow \quad \mu_2(t) = \phi^{-1}\left(\frac{\sigma_2(t+\tau)}{s}\right) \equiv g[\sigma_2(t+\tau)], \tag{22}$$

where ϕ^{-1} represents the inverse function of ϕ-function. In order to make bitcoins attractive, we assume that there is a positive acceptance rate even if nobody is a bitcoiner (or to say before launching Bitcoin). In addition, all sellers need to accept bitcoins if all buyers are bitcoiners. In equation, the two conditions are written as

$$\phi(0) > 0 \quad \text{and} \quad \phi(1) = 1. \tag{23}$$

Letting $N_2(t)$ be the population of bitcoiners in period t, the share of bitcoiners in period t is arranged to get

$$\mu_2(t) = \frac{N_2(t-\tau) + \Delta N_2(t)}{N(t-\tau) + \Delta N(t)} = \frac{\mu_2(t-\tau) + \Delta N_2(t)/N(t-\tau)}{1+n(t)}, \tag{24}$$

where $N(t)$ represents the total population and $n(t)$ the population growth rate given by

$$n(t) \equiv \frac{\Delta N(t)}{N(t-\tau)}. \tag{25}$$

By definition, the population of bitcoiners increases in period t by

$$\Delta N_2(t) = F[\delta^*(t)]\,\Delta M(t), \tag{26}$$

where $\delta^*(t)$ is a cut-off level of $\xi(L_1^i - L_2^i)$ determined by $\sigma_2(t)$ as shown in Figure 3; $M(t)$ represents the population of buyers (sum of traditional-money holders and bitcoiners); and $\Delta M(t)$ the increase in the population of buyers. By assumption, the share of sellers in the population is fixed at θ; hence, the population of buyers satisfies

$$M(t) \equiv (1-\theta) N(t) \quad \Longrightarrow \quad \Delta M(t) \equiv (1-\theta)\,\Delta N(t). \tag{27}$$

In order to compute (24), using (26) and (27), we arrange $\Delta N_2(t)/N(t-\tau)$ as

$$\frac{\Delta N_2(t)}{N(t-\tau)} = \frac{F[\delta^*(t)]\,\Delta M(t)}{\Delta N(t)} \cdot \frac{\Delta N(t)}{N(t-\tau)} = (1-\theta)\,n(t)\,F[\delta^*(t)]. \tag{28}$$

We then substitute (28) into (24) to get

$$\mu_2(t) = \frac{\mu_2(t-1) + (1-\theta)\,n(t)\,F[\delta^*(t)]}{1+n(t)}. \tag{29}$$

Let $\dot{\mu}_2 \equiv \mu_2(t) - \mu_2(t-\tau)$ be a periodical change in the share of bitcoiners to arrange (29) to get

$$\dot{\mu}_2 = (1-\theta)\,n(t)\,F[\delta^*(t)] - n(t)\,\mu_2(t). \tag{30}$$

We search equilibrium that satisfies $\dot{\mu}_2 = 0$ by taking $\tau \mapsto 0$ in (30) and substituting $\mu_2 = g(\sigma_2)$ into it. The condition to verify dynamic stability of equilibria is then provided as

$$\dot{\mu}_2 \gtreqless 0 \quad \Longleftrightarrow \quad (1-\theta)\,F(\delta^*) \gtreqless g(\sigma_2) \quad (\tau \longmapsto 0). \tag{31}$$

Since δ^* is determined by σ_2 via $D(\sigma_2; ...)$, (32) is eventually written only with σ_2 as

$$\dot{\mu}_2 \gtreqless 0 \quad \Longleftrightarrow \quad (1-\theta)\,F[D(\sigma_2; ...)] \gtreqless g(\sigma_2). \tag{32}$$

The phase diagram based on the stability condition (32) is depicted in Figure 6, where $LHS(2)$ and $RHS(2)$ denote the left-hand-side and right-hand-side of condition (32), respectively. In this diagram, ϕ-function (or g-function equivalently) is depicted as a linear function.[11] In addition, the left-hand-side of inequality (32) is derived from the cumulative distribution function and a monotonically increasing D-function. Thus, the left-hand-side of inequality (32) keeps basic characteristics of cumulative distribution function and the locus

in the figure must be as depicted. Prior to make further discussions, we confirm the existence of at least one equilibrium by the next remark.

Remark 3 *There exists at least one stable equilibrium.*

Proof. By definition, $(1-\theta) F[D(\sigma_2;...)] \geq 0$ at $\sigma_2 = 0$ and $(1-\theta) F[D(\sigma_2;...)] \leq 1$ at $\sigma_2 = 1$. In addition, $g(\sigma_2)$ passes $(s,1)$ and $(\tilde{\sigma}_2, 0)$, where $\tilde{\sigma}_2 \equiv s\phi(0) > 0$; hence, $g(0) < 0$, and functions F and g are continuous. Thus, the left-hand-side and the right-hand-side of condition (32) must have intersect at least once. If there is an intersection, $g(\sigma_2)$ cuts $(1-\theta) F[D(\sigma_2;...)]$ from below, as $g(0) < (1-\theta) F[D(0;...)]$ and $g(1) \geq (1-\theta) F[D(1;...)]$. This implies that such an equilibrium is stable. ■

As Figure 6 shows, if key values are appropriately chosen, we find two stable and an instable equilibria. However, any of these equilibria are shown to be degenerate. For further discussions, we propose another axiom regarding matching equilibrium.

Axiom 2 *If monies are in stable matching equilibria, primary effects dominate respective feedback effects.*

If a large number of sellers declares to accept bitcoins before launching Bitcoin, or $s\phi(0)$ exceeds a certain level, in contrast, the instable equilibrium and the failure one disappear, as $RHS(2)$ shifts rightward. Only the success equilibrium may realize then (*á la* big-push theory). A similar result with the big-push in a reverse causality is proposed by Martin [27]. In his analysis, "single-currency equilibrium" realizes when the money supply rapidly increases to substitute the other money. If the preference is represented by a so small s, $RHS(2)$ locates further left in Figure 5, the instable equilibrium and the successful one seize to exist. Only the failure equilibrium may realize then. If $RHS(2)$ shifts from left to right, the two stable equilibria, if they exist, move from left to right; hence, μ_2 and σ_2 maintain a positive correlation in stable equilibria.[12]

There are potential risks of counterfeiting, or double-spending, and such risks affect σ_2. The math problem for counterfeiters are designed to be much more difficult than obtaining genuine bitcoins, as each coin has blocks that are added after each transaction. In order to protect Bitcoin from counterfeiting, official venders add blocks faster than a computing speed of counterfeiters. This strategy looks like an arms race between groups of offenders and potential victims, as studied in Ehrlich and Saito [17]. The difference is the weapon to use. In the arms race, weapons are strike capabilities. In Bitcoin, the weapon is math.

Is the cost of counterfeiting bitcoins really high? Crackers use computers, so that counterfeiting definitely consumes computing resources while it may not impose too much cost

on crackers themselves. They can enjoy other activities while their computers are running to win the race. A lower counterfeiting cost increases the risk of counterfeiting. In a random-matching literature, Green and Weber [18] find out the basic relationship between counterfeiting risks and counterfeiting costs, [37] discusses a problem in private money and its counterfeiting risk, and Cavalcanti and Nosal [6] consider a mechanism design to depress counterfeiters in a monetary economy with private money.[13] Among them, Nosal and Wallace [29] propose the most naïve insight about a monetary equilibrium with a counterfeit. In their analysis, if they apply the intuitive criterion Cho and Kreps [8], illegal tenders cannot stay in circulation in the monetary-trade equilibrium. In such a case, the cost of counterfeiting must be sufficiently high, otherwise, illegal tenders may stay in circulation. If illegal tenders stay in circulation, in contrast, the monetary-trade equilibrium fails to exist. Li and Rocheteau [26] extend this argument to show impacts of threats of counterfeiting that affect the value of the legal tender.[14] Threats of counterfeiting, which reduce the value of money, will make a leftward shift of $RHS\,(2)$ in Figure 5, as sellers increase suspicions about bitcoins when threats of counterfeiting and double-spending increase. As a result, threats of counterfeiting and double-spending reduce the share of bitcoiners in the stable equilibrium. In some cases, the successful equilibrium disappears to reach the failure one, similarly as Nosal and Wallace [29] propose.

Bitcoin is a network-based peer-to-peer currency and that enables venders to cancel coins immediately once it is found particular coins involve in illicit activities. This implies that potentially the Bitcoin venders are capable of providing sufficient threats of punishment to enforce public rules. However, even in the digital economy, punishments and enforcements are costly, as monitoring activities consumes computing resources and investigations use human resources in the real world. The question is the feasibility for us to ask the Bitcoin community to prepare to be such an authority. If it is infeasible, we may have to accept governmental entities to involve in monitoring and investigating activities. In accordance with Camera [3], in a random-matching environment, for example, an over-supplied money increases transactions associated with money laundering. In this case, an advantage of Bitcoin seems the limited money supply. However, Bitcoin is an addition to the existing monetary system and it increases supply of medium of exchange. An increase in money laundering is not only caused by Bitcoin, but also externality effect of other currencies. Without interventions of public entities, the Bitcoin society may have to provide excessive resources against money laundering inclusive of such side effects. A rational choice is to compare the cost and benefit of accepting governmental entities and the demand and supply of illicit activities as discussed in literatures in economics of crime: for example, Becker [1] and Ehrlich [13, 14, 15, 16].[15]

Bitcoin is also a kind of private money. Usually, private monies are backed up by reserve funds and credibility of private-money providers. The credibility is, for example, measured by the capability of the issuer bank to choose a good investment project (Williamson [36]). Issued private notes are liabilities and receivers (sellers) are anxious about the credibility of each private money. In case of Bitcoin, the Bitcoin vender does not make investment as ordinary banks. This indicates that the credibility, or sustainability, of Bitcoin depends only on the market value at the exchange and the purchasing power. A decrease in the credibility makes a leftward shift of $RHS\,(2)$ in Figure 5, similarly as an increase in the threat of counterfeiting or double-spending.

Next, we consider changes in γ's under Axioms 1 and 2 to apply Remark 2. Let γ_2 be fixed. A decrease in the inflation rate of traditional money reduces the value of D-function (*cf.* Proposition 1 and Figure 4). The locus of $LHS\,(2)$ then shifts downward and it may drive out the instable equilibrium and the successful one. In turn, let γ_1 be fixed instead of γ_2. A decrease in the benefit of holding bitcoins again reduces the value of D-function (*cf.* Proposition 1 and Figure 4). Similarly, the locus of $LHS\,(2)$ then shifts downward and it may only leave the failure equilibrium. If $LHS\,(2)$ shifts from up to down, the two stable equilibria, if they exist, move from right to left; hence, there is a positive correlation between γ_2 and σ_2 and a negative correlation between γ_1 and σ_2.[16]

Usually, interest and inflation rates are determined by productivity of an issuer bank and money supply. However, as stated, Bitcoin does not have reserve funds and investment plans, as ordinary private money issuers. Thus, the real interest rate of Bitcoin γ_2 is determined by the inflation rate of traditional currency and the expected capital gain from Bitcoin. In these three years, the exchange rate at Mt. Gox, Bitcoin continues rising steadily as shown in Figure 1 from almost zero to above $100. An expectation of a larger capital gain will make a leftward shift of $RHS\,(2)$ in Figure 5 to approach the success. A strong market trend may raise the acceptance rate α_2 to make another shift of $LHS\,(2)$ to reinforce the success of Bitcoin.

A money flow from traditional currencies to Bitcoin is caused by an increase in the inflation rate of traditional currency (especially in Europe) as well as a strong Bitcoin exchange market trend. It implies that Bitcoin may not success if the inflation rate of major traditional currency goes back to a lower level and the market trend is weakened. The success of Bitcoin seems vulnerable to a decrease in the relative benefit $\gamma_2 - \gamma_1$ and *vice versa* for traditional currencies. Rocheteau [31] studies a choice between fiat money and assets based on informational transparency and capital gains. This argument can also be applied to discuss the choice between Bitcoin and traditional money to reach an analogous argument as ours in conjunction with σ_2 and $\gamma_1 - \gamma_2$. A similar vulnerability result in a multiple currency

system is, for example, also discussed in other contexts such as Chang *et al.* [7], Martin [27], Nosal and Wallace [29], Williamson [36], and many others.

Money has a role to reduce informational asymmetry in transactions, for example, as discussed by Ostroy [30] and Berentsen and Rocheteau [2]. A disadvantage of private money in the informational asymmetry, as discussed in Williamson [36] and Cavalcanti *et al.* [5], does not exist, or ignorable, since Bitcoin is entirely market-based and everything is disclosed. This is an advantage of Bitcoin as a private money. However, as Cavalcanti *et al.* [5] suggests, in a random matching environment, where claiming is stochastic, the Central Bank or an alternative authority needs to stabilize the financial system including private monies by controlling reserve funds. A sufficient reserve fund protects the financial system and it protects the financial system from the crash. However, Bitcoin has no reserve system. In other words, the credibility of Bitcoin entirely depends on the exchange market and a minor turmoil in a Bitcoin exchange may be magnified to suffer the basis of Bitcoin to crash (*á la* Kiyotaki and Moore [21]). For example, a turmoil may result in a leftward shift of $RHS\,(2)$ and a rightward shift of $LHS\,(2)$ in Figure 5 (Appendix A shows another approach by explicitly including the exchange market). Thus, we cannot allow a server down by a DDoS attack as the Mt. Gox has experienced in April 2013.[17]

This result is also consistent with Camera *et al.* [4] that allow agents to keep two units of currencies (without new entries, however) in a study of dollarization. In their study, dollarization is avoided so long as the national currency is sufficiently safe. The currency substitution effect in our model is implemented by allowing new entries instead of allowing holding more than one unit of money. In the context of this paper, "Bitcoinization" is avoided so long as traditional currencies are sufficiently safe. For general assessments, theoretical results are summarized in the next proposition.

Proposition 2 *Let us consider a stable equilibrium under Axioms 1 and 2 whose existence is backed up by Remark 3. The share of bitcoiners increases as bitcoins get more accepted for payments. The share of bitcoiners decreases as traditional money gets less costly to store compared with bitcoins. If there are two stable equilibria, one is successful and the other is failure. The successful equilibrium is likely to realize when there is a big-push or a higher inflation in traditional money.*

3.2 A Numerical Example (Continued)

We continue on the functions and parameters provided in Section 2.3. The additional functions and parameters are given as follows.

We suppose that α_2 is 5% if nobody is a bitcoiner and 100% if everyone is. For simplicity, we assume that ϕ is a linear function and $s = 1$. In this case, we find the relationship between σ_2 and μ_2, as ϕ-function, to be

$$\sigma_2 = 0.95\mu_2 + 0.05, \tag{33}$$

We suppose $\xi\left(L_1^i - L_2^i\right)$ is distributed as normal: $\xi\left(L_1^i - L_2^i\right) \sim \mathrm{N}(0.03, 0.025)$. Figure 6 (Left) then depicts the result when the inflation rate of traditional money is 5% ($\gamma_1 = -0.05$). In this figure, points A and C are stable and B is instable. Between the two stable equilibria, A is a failure equilibrium, as the share of bitcoiners vanishes, while C is a successful one, as bitcoiners take a large share. This example also shows that Bitcoin cannot stably stay in the market as a payment method unless sellers accept bitcoins exceeding the level given by point B.

As shown in Figure 4, a decrease in the inflation rate of traditional money makes a downward shift in $D\left(\sigma_2; ...\right)$. This implies that it also makes a downward shift in $F\left[D\left(\sigma_2; ...\right)\right]$, as depicted in Figure 6 (Right). In this figure, the inflation rate of traditional money is 3% (the same ϕ-function is applied). This decline in the inflation rate wipes out equilibrium points B and C, and then the economy start approaching the vanishing point, A in Figure 6 (Right), even if the economy stably stayed around the stable equilibrium, C in Figure 6 (Left), before the change. The obtained results confirm a consistency with the axiom-based theoretical discussion in Section 3.1.

4 Welfare Comparisons: A Discussion

We have to know how much beneficial to keep Bitcoin. However, in our framework, it is ambiguous whether the successful equilibrium generates a higher welfare level than the failure one, as the social welfare is computed as

$$\mathcal{W} = \theta V_0 + (1-\theta)\left[\left\{1 - F\left(\delta^*\right)\right\} V_1 + F\left(\delta^*\right) V_2\right]. \tag{34}$$

This social welfare function is rearranged as

$$\tilde{W} = (1-\theta)\left\{\left(V_1 - V_0\right) - \delta^* F\left(\delta^*\right)\right\}, \tag{35}$$

where $\tilde{W} \equiv W - V_0$ for $V_0 = \lambda s^2 \nu^*$ when $\dot{V}_0 = 0$.

Proposition 3 *The social welfare is decreasing in the share of bitcoiners if generating bitcoins is easier than obtaining traditional money.*

Proof. Differentiating (35) with respect to σ_2 provides

$$\frac{d\tilde{W}}{d\sigma_2} = \frac{dV_1}{d\sigma_2} - \left\{F\left(\delta^*\right) + \delta^* f\left(\delta^*\right)\right\}. \tag{36}$$

By definition, $V_1 \geq V_2$ holds for $\delta^* \geq 0$. In this case, as $dq_1/d\sigma_2 = 0$ (Remark 2), an increase in σ_2 reduces V_1 since the expectation to obtain a higher value, V_1, declines as ϕ-function; hence, $dV_1/d\sigma_2 \leq 0$ and then $d\tilde{W}/d\sigma_2 < 0$. If $\delta^* < 0$, $d\tilde{W}/d\sigma_2 \geq 0$ may hold, so long as $F\left(\delta^*\right) < dV_1/d\sigma_2 - \delta^* f\left(\delta^*\right)$, where $dV_1/d\sigma_2 > 0$ and $\delta^* f\left(\delta^*\right) < 0$. Therefore, $\tilde{W}$ is an increasing or a hump-shaped function for δ^* while it is a decreasing function for $\delta^* \geq 0$.

Next, ϕ-function provides a positive correlation between σ_2 and μ_2. As $\delta^* \equiv \xi\left(L_1^i - L_2^i\right)$ determines the cutoff level for conditions (14) and (15) for each σ_2, $\delta^* \geq 0$ indicates that generating bitcoins is easier than obtaining traditional money. Therefore, an increase in the share of bitcoiners reduces the social welfare for $\delta^* \leq 0$. ■

Numerical examples to confirm Proposition 3 are shown in Figure 7. In this figure, σ_2 to assign $\delta^* = 0$ for $\gamma_2 = 1\%$ and $\gamma_1 = -3\%$ for Figure 7 (Left) and $\gamma_2 = -5\%$ Figure 7 (Right) are $\sigma_2 \simeq 0.36$ ($\mu_2 \simeq 0.33$) and $\sigma_2 \simeq 0.29$ ($\mu_2 \simeq 0.25$), as indicated by solid grid lines. In the figures the flat segment indicates that Bitcoin vanishes and $\tilde{W} \equiv (1-\theta) V_1$ holds. The examples also confirm that $\tilde{W}$ is decreasing in σ_2 for $\delta^* \geq 0$ and it is hump-shaped for $\delta^* < 0$, as stated in the proof of the proposition.

In accordance with our result, the single-currency system is more preferable. If Bitcoin is not so beneficial in the end, we should abandon bitcoins. Bitcoin is a kind of international currency. As proposed by Matsuyama *et al.* [28], a unified currency may reduce the welfare level, as merchants specialize in productions of general goods instead of locally tailor-made ones, which could be traded only between locals, as sellers choose to larger opportunities to trade with general goods. In this study, in contrast, a less acceptability as a payment method generated a welfare-decreasing result, as buyer's preference is completely *ad hoc*.

Our Proposition 3 and Matsuyama *et al.* [28] propose negative results for Bitcoin to improve social welfare. When we consider welfare gains from Bitcoin, however, we also need to take into account for the vehicle currency issue. If Bitcoin takes a role as a vehicle currency, it provides further benefits by eliminating fees for one-to-one exchanges.[18] In this case, the welfare erosion by an increase in the share of bitcoiners as must be compensated by the reduction of foreign exchange cost, which is what Bitcoin actually aims at. In addition, Devereux and Shi [11], for example, claim that the welfare of countries within the vehicle currency system is eroded by a higher inflation rate of the center country. In this sense, such an erosion of welfare is reduced by making Bitcoin a vehicle, as its inflation rate is

subject to the math problem that eventually becomes unsolvable within a reasonable time (no money-supply growth then). According to Devereux and Shi's study, there is also a possibility of coexistence of multiple vehicle currencies depending on respective storage cost (inflation rate). Therefore, there is a possibility that USD, Euro, and Bitcoin can coexist and it can still have a room for improving social welfare. Once we decide to accept Bitcoin as a new method of payment, we need to go back to the argument how to maintain the Bitcoin system healthy, inclusive of discussions whether or not accepting involvements of public authorities, as discussed in the previous section.

5 Concluding Remarks

In order to examine the potential sustainability of Bitcoin, this paper has analyzed a dual-currency money-search with new entries keeping the buyer-seller ration constant. We then have found that sustainability of Bitcoin may be vulnerable to a decrease in the inflation rate of a major currency and a decrease in the credibility of Bitcoin. Such criteria for the sustainability is analogous to ordinary money except for the fact that Bitcoin is not based on traditional banking system. Bitcoin is based only on the market.

The theory predicts that Bitcoin can coexist with traditional money so long as the inflation rate and credibility issues are cleared. In such a case, however, an increase in the share of bitcoiners reduces social welfare, as sellers may reject Bitcoin for payments. We then need to consider if we accept Bitcoin as a new method of payment. If Bitcoin cannot reduce transaction costs sufficiently, it is better to abandon Bitcoin. If we accept Bitcoin, we still need to control the system appropriately against several criminal activities, such as money laundering, tax evasions, counterfeiting (double-spending), cracking, and the likes. Tracking transactions seems much easier than traditional currencies, but there are a huge monitoring cost due to the size of the data. Even if Bitcoin is hard to copy and based on a secure system, even the existence of threats of counterfeiting affects the value of Bitcoin. In addition, without public entities, the Bitcoin community may have to provide resources against illicit activities inclusive of the ones caused by external effects. The decision to accept/reject involvements of public entities should be done with rational thoughts, such as comparisons of cost and benefit in conjunction with demand and supply of offenses.

Let us suppose Bitcoin is accepted as a part of current payment system and approaching the success equilibrium. Its public responsibility then becomes further significant. This implies that the Bitcoin community prepare for protecting the system from several illicit activities and market turmoils. For the protection, large financial and human resources are needed. For the community, it is the time on the cross, as they need to decide whether

or not admit public authorities to involve in Bitcoin. If they reject public controls, they need sufficient resources (funds) or public authorities may need to compulsorily intervene the Bitcoin system. To what extent the authorities involve in Bitcoin is then determined, for example, by comparisons between costs and benefits in the market for offenses. If public authorities involve in the Bitcoin community, as a positive side effect, the acceptance rate may improve to improve the social welfare level in the equilibrium. If Bitcoin likely fails to exist in the near future, for example, by a decrease in inflation rates of major traditional currencies or a so weak Bitcoin-market trend, public authorities do not need to involve in Bitcoin so much.

Appendix

A Inclusion of Exchange Market

When we include an exchange market, we need to consider the demand and supply of bitcoins. The demand for bitcoins is derived from the population of new entrants that purchase bitcoins. We then assume a portion of bitcoiners goes out of the market in the end of every period. To keep θ, the corresponding traditional-money holders and sellers also go out of the market then. This is an analogous thought as used in marriage-market random-matching model. If we accept such a framework, the analysis is processed without any modification. Another modeling strategy is to include outside options of agents, as Dutu [12] in a study of dollarization. However, it does not change the course of discussions so long as outside options are given exogenously.

A possible change in the result is the shift of cumulative distribution function F. An increase in the relative population of coming bitcoiners relative to out-going bitcoiners β increases the average market value of Bitcoin and that affects $\delta_i = (1 - \pi_i) L_1^i$ for $L_2^i = \pi_i L_1^i$. Thus, a stronger Bitcoin market increases the transformation rate π_i to reduce δ_i. As a result, it makes a rightward shift of F, which results in a decrease in the inflation rate of traditional money in Figure 3. As a result, a stronger market reduces the share of bitcoiners in the stable equilibrium in Figure 5. A too strong Bitcoin trend has the successful equilibrium disappear to reach the failure one. However, it improves social welfare as indicated by Figure 7. A weaker Bitcoin trend makes an analogous result as an increase in the inflation rate of traditional money. If it has little effect in sellers' preference about payment methods, the weaker trend increases the share of bitcoiners. However, a too weak trend may result in a crash of Bitcoin as sellers may hesitate to accept bitcoins then (a further leftward shift of g-function in Figure 5).

Notes

[1]Bitcoin is proposed by Satoshi Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, 2009. This article is freely available online at http://bitcoin.org/bitcoin.pdf. Yet, Satoshi Nakamoto is not identified who is he.

[2]Mt. Gox is a Tokyo-based Bitcoin exchange that deals most of Bitcoin exchange trades.

[3]Robin Sidel (2013, April 13). Bitcoin Investors Hang On for the Ride. *The Wall Street Journal*. Retrieved April 13, 2013, from http://online.wsj.com.

[4]Jeffrey Sparshott (2013, March 21). Web Money Gets Laundering Rule. *The Wall Street Journal*. Retrieved March 21, 2013, from http://online.wsj.com.

[5]Rupert *et al.* [33] provides a detailed survey for the first and the second generation models, and Williamson and Wright [38] summarize the recent developments in this field including the third generation model.

[6]The independence between μ_m and σ_m is eased in Section 3.

[7]This simplification is popular in money-search literature. It is known that the social welfare reaches efficient level when buyers make take-it-or-leave-it offers. In addition, the basic behavior of the model is maintained so long as the bargaining power of compaired models are on the buyer's side — for example, please see Saito [19] that also shows models that assign relatively larger bargaing power to sellers violate participation constraint. However, in a dual-currency framework, this simplification delete impacts of the other currency in seller's value function.

[8]In particular, when an agent process a barter transaction, one's continuation value is $u(x) - c(y) + V_m - V_m = u(x) - c(y)$. In barter trade, we assume agents have even bargaining powers. In this case, by symmetry of agents' problem, we have $x = y = q$, and then the bargaining solution coincides with the social optimum.

[9]Incentive compatibility conditions of sellers and buyers are $V_m - c(q_m) \geq V_0$ and $u(q_m) + V_0 \geq V_m$, respectively. If the two conditions are simultabeously satisfied, $u(q_m) - c(q_m) \geq 0$ must be satisfied; hence, $\bar{q}_m$ is the upper bound of monetary trade.

[10]The transformation rate π_i differs one-by-one, as one may obtain Bitcoin at eBay and the other at Mt. Gox. Auction prices are not uniform even if several transactions are made simultaneously. In addition, individuals have different network environment and skills to affect π_i.

[11]Linear ϕ-function is sufficient to present important results so long as it is a monotonically increasing function.

[12]In the instable equilibrium, there is an opposite correlation between μ_m and σ_m.

[13]In Wallace [37] and Cavalcanti and Nosal [6] consider this problem under an assumption that private money has is intrinsically much easier to counterfeit than legal tenders. In case of Bitcoin, it is still ambiguous.

[14]Kultti [23] and Soller-Curtis and Waller [32] also study impacts of illegal tenders in monetary economy in random matching environment when not only threats but illegal tenders do circulate to reduce the value of legal tenders and to invite a welfare loss when there is a sufficent supply of legal medium of exchange.

[15]Offenders supply offenses and potential victims "derive" demands for offenses. In particular, potential victims that are less prepared against criminal activities derive lager demands for offenses.

[16]In the instable equilibrium, there are opposite correlations between γ's and σ_2.

[17]The detail in given by the official press release at https://mtgox.com/press_release_20130404.html.

[18]Or to say a vehicle currency is introduced in order to minimize such costs from one-to-one exhcnages (for example, Jones [20], Chrystal [9], Krugman [24]).

References

[1] Becker, Gary S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy*, 76(2), 169–217.

[2] Berentsen, Aleksander and Guillaume Rocheteau (2004). Money and information. *Review of Economic Studies* 71(4), 915-44.

[3] Camera, Gabriele (2001). Dirty money. *Journal of Monetary Economics*, 47(2), 377-415.

[4] Camera, Gabriele; Craig, Ben; and Christopher Waller (2004). Dollarization and currency exchange. *Journal of Monetary Economics*, 51(4), 671-89.

[5] Cavalcanti, Ricardo; Erosa, Andres; and Ted Temzelides (1999). Private money and reserve management in a random-matching model. *Journal of Political Economy*, 107(5), 929-45.

[6] Cavalcanti, Ricardo and Ed Nosal (2011). Counterfeiting as private money in mechanism design. *Journal of Money, Credit and Banking*, 43(S2), 625-36.

[7] Chang, Winston W.; Kemp, Murray C.; and Ngo Van Long (1983). Money, inflation, and maximizing behavior: The case of many countries. *Journal of Macroeconomics*, 5(3), 251-63.

[8] Cho, In-Koo and David. Kreps, Signaling games and stable equilibria. *Quarterly Journal of Economics*, 102(2), 179-221.

[9] Chrystal, K. Alec (1977). Demand for international media of exchange. *American Economic Review*, 67(5), 840-50.

[10] Craig, Ben R. and Christopher J. Waller (2000). Dual-currency economies as multiple-payment systems. *Federal Reserve Bank of Cleveland Economic Review*, Q1, 2-13.

[11] Devereux, Michael B. and Shouyong Shi (2013). Vehicle currency. *International Economic Review*, 54(1), 97-133.

[12] Dutu, Ricardo (2008). Currency interdependence and dollarization. *Journal of Macroeconomics*, 30(4), 1673–87.

[13] Ehrlich, Isaac (1974). Participation in illegitimate activities: An economic analysis. In G.S. Becker & W.M. Landes (Eds.), *Essays in the economics of crime and punishment*, New York, NY: Columbia University Press, pp. 68-134.

[14] Ehrlich, Isaac (1981). On the usefulness of controlling individuals: An economic analysis of rehabilitation, incapacitation and deterrence. *American Economic Review*, 71(3), 307–322.

[15] Ehrlich, Isaac (1982). The optimum enforcement of laws and the concept of justice: A positive analysis. *International Review of Law and Economics*, 2(1), 3–27.

[16] Ehrlich, Isaac (1996). Crime, punishment, and the market for offenses. *Journal of Economic Perspectives*, 10(1), 43-67.

[17] Ehrlich, Isaac and Tetsuya Saito (2010). Taxing guns vs. taxing crime: An application of the market for offenses model, *Journal of Policy Modeling*, 32(5), 670-89. [Also available as *NBER Working Paper*, No. 16009.]

[18] Green, Edward J. and Warren E. Weber (1996). Will the new $100 bill decrease counterfeiting? *Federal Reserve Bank of Minneapolis Quarterly Review*, Summer, 3-10.

[19] Saito, Tetsuya (2012). Rationality and stability of equilibrium in a search-theoretic model of money. *Theoretical Economics Letters*, 3(2), 283-86.

[20] Jones, Robert A. (1976). The origin and development of media of exchange. *Journal of Political Economy*, 84(4), 757-75.

[21] Kiyotaki, Nobuhiro and John Moore (1997). Credit cycles. *Journal of Political Economy*, 105(2), 211-48.

[22] Kiyotaki, Nobuhiro and Randall Wright (1989). On money as a medium of exchange. *Journal of Political Economy*, 97(4), 927-54.

[23] Kultti, Klaus (1996). A monetary economy with counterfeiting. *Journal of Economics*, 63(2), 175-86.

[24] Krugman, Paul (1980). Vehicle currencies and the structure of international exchange. *Journal of Money, Credit and Banking*, 12(3), 513-26.

[25] Lagos, Ricardo and Randall Wright (2005). A unified framework for monetary theory and policy analysis. *Journal of Political Economy*, 113(3), 463-84.

[26] Li, Yiting and Guillaume Rocheteau (2011). On the threat of counterfeiting. *Macroeconomic Dynamics*, 15(S1), 10-41.

[27] Martin, Antoine (2006). Endogenous multiple currencies. *Journal of Money, Credit and Banking*, 38(1), 245-62.

[28] Matsuyama, Kiminori; Kiyotaki, Nobuhiro; and Akihiko Matsui (1993). Toward a theory of international currency. *Review of Economic Studies*, 60(2), 283-307.

[29] Nosal, Ed and Niel Wallace (2007). A model of (the threat of) counterfeiting. *Journal of Monetary Economics*, 54 (4), 994- 1001.

[30] Ostroy, Joseph M. (1973). The informational efficiency of monetary exchange. *American Economic Review*, 63(4), 597-610.

[31] Rocheteau, Guillaume (2008). Money and competing assets under private information. *Federal Reserve Bank of Cleveland Working Papers*, No. 0802.

[32] Soller-Curtis, Elisabeth and Christopher J. Waller (2000). A search-theoretic model of legal and illegal currency. *Journal of Monetary Economics*, 45(1), 155-84.

[33] Rupert, Peter; Schindler, Martin; Shevchenko, Andrei; and Randall Wright (2000). The search-theoretic approach to monetary economics: a primer. *Federal Reserve Bank of Cleveland Economic Review*, Q4, 10-28.

[34] Trejos, Alberto and Randall Wright (1995). Search, bargaining, money, and prices. *Journal of Political Economy*, 103(1), 118-41.

[35] Trejos, Alberto (1996). Search theoretic models of international currency. *Federal Reserve Bank of St. Louis Review*, 78(3), 117-32.

[36] Williamson, Stephen D. (1999). Private money. *Journal of Money, Credit and Banking*, 31(3), 469-91.

[37] Williamson, Stephen D. (2002). Private money and counterfeiting. *Federal Reserve Bank of Richmond Economic Quarterly*, 37-57.

[38] Williamson, Stephen and Randall Wright (2010). New monetarist economics: Methods. *Federal Reserve Bank of St. Louis Review*, 92(4), 265-302.

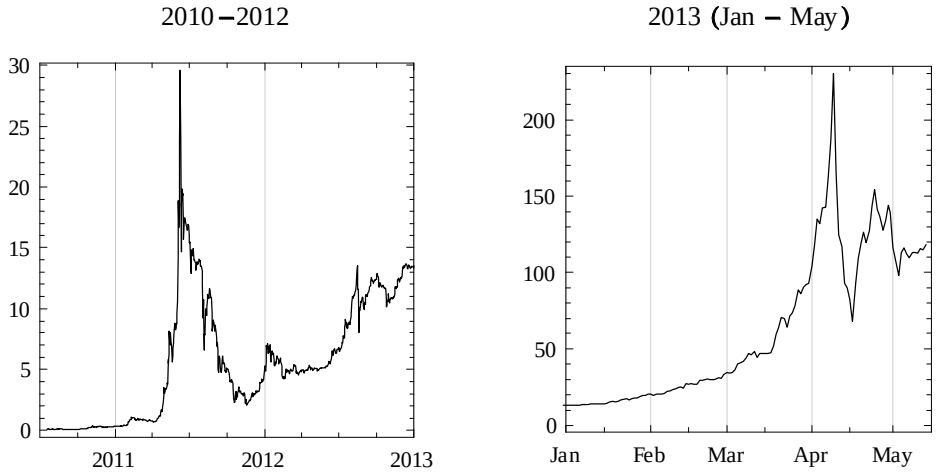

Figure 1: Bitcoin-USD Exchange Rate at Mt. Gox (Source: bitcoinchart.com)

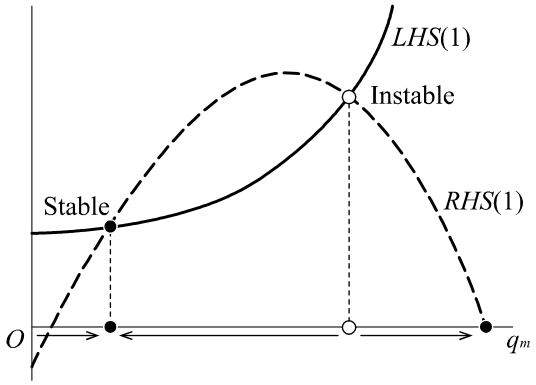

Figure 2: Existence of stable and instable equilibria

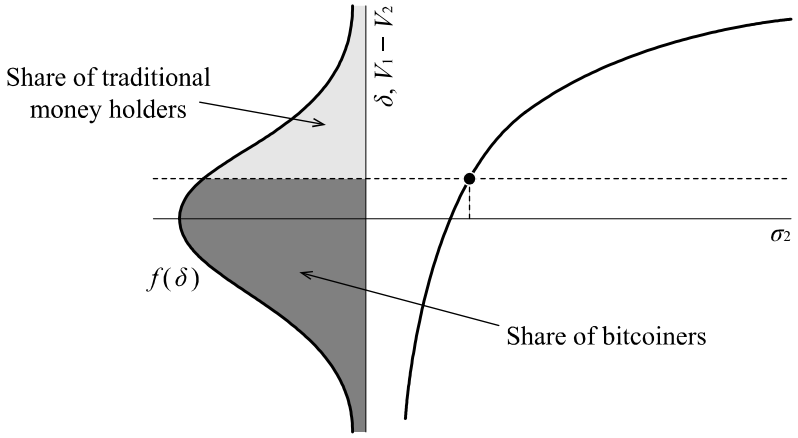

Figure 3: Determining shares of money holders

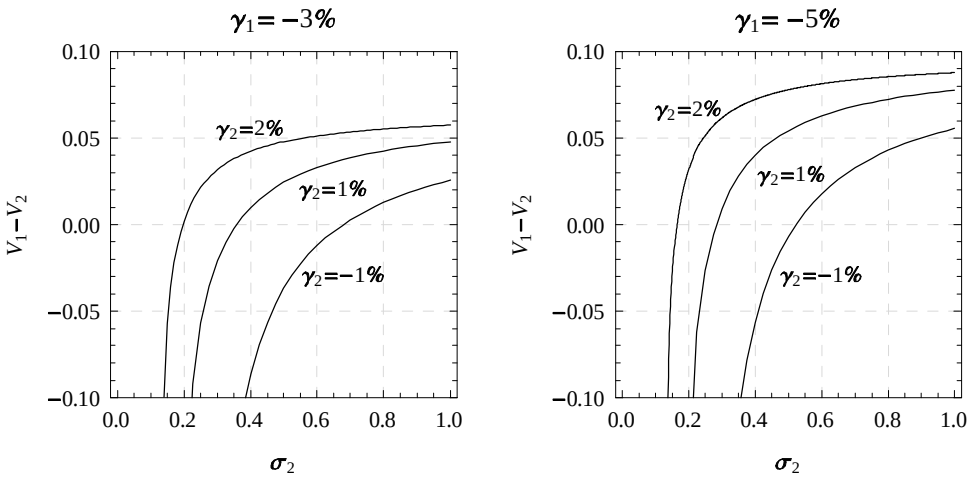

Figure 4: Determining shares of money holders (numerical examples)

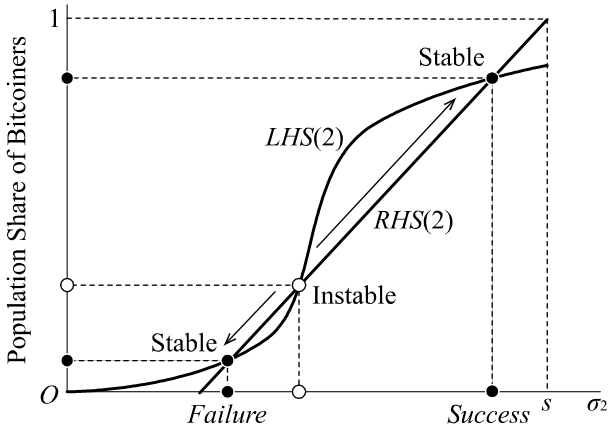

Figure 5: Dynamic stability of the share of bitcoiners

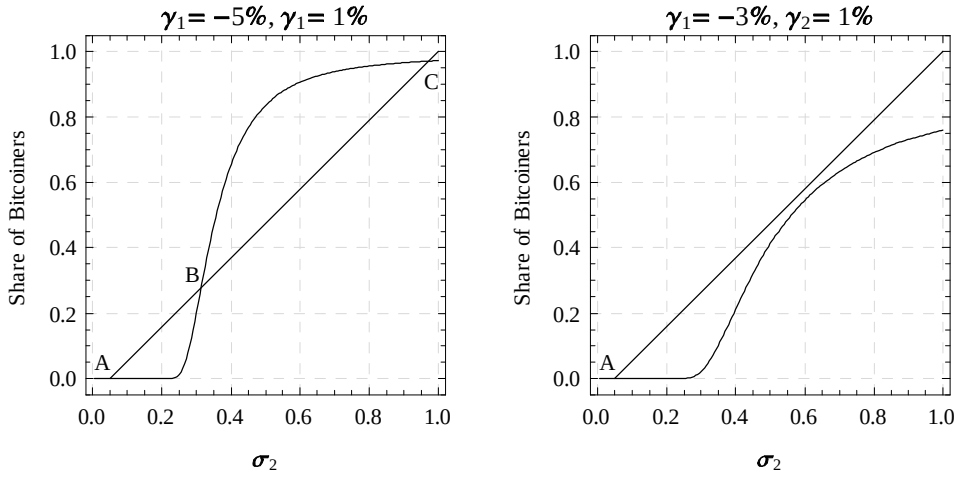

Figure 6: Dynamic stability of the share of bitcoiners (numerical example)

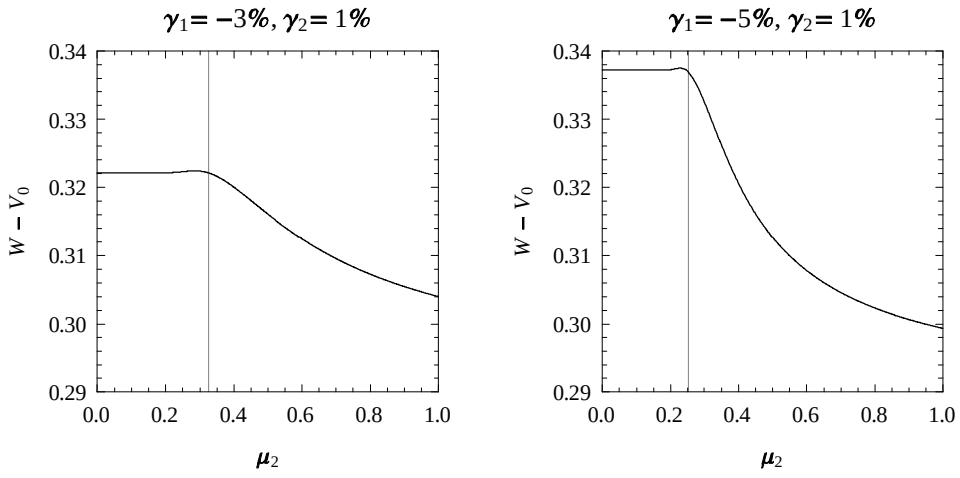

Figure 7: Social welfare and share of bitcoiners

Research Institute of Economic Science
College of Economics, Nihon University

1-3-2 Misaki-cho, Chiyoda-ku, Toyko 101-8360 JAPAN
Phone: 03-3219-3309　Fax: 03-3219-3329
E-mail: keikaken.eco@nihon-u.ac.jp
http://www.eco.nihon-u.ac.jp/center/economic/