

Fair Trading of Information: A Proposal for the Economics of Peer-to-Peer Systems

Kenji Saito*
Keio University

Eiichi Morino
Gesell Research Society Japan

Jun Murai
Keio University

Abstract

A P2P currency can be a powerful tool for promoting exchanges in a trusted way that make use of under-utilized resources both in computer networks and in real life.

There are three classes of resource that can be exchanged in a P2P system: atoms (ex. physical goods by way of auctions), bits (ex. data files) and presences (ex. time slots for computing resources such as CPU, storage or bandwidth). If these are equally treated as commodities, however, the economy of the system is likely to collapse, because data files can be reproduced at a negligibly small cost whereas time slots for computing resources cannot even be stockpiled for future use.

This paper clarifies this point by simulating a small world of traders, and proposes a novel way for applying the "reduction over time" feature[14] of i-WAT[11], a P2P currency. In the proposed new economic order (NEO), bits are freely shared among participants, whereas their producers are supported by peers, being given freedom to issue exchange tickets whose values are reduced over time.

1 Introduction

1.1 Exchanges in P2P Systems

Exchanging is a necessary building block of peer-to-peer (P2P) systems, which can potentially harness the under-utilized power of the network of computers connected to one another via the Internet. Such power is often used for sharing values in real life, such as music, video, or even physical goods such as furnitures by way of auctions. There seem to be three classes of values or resources that can be made subjects of exchanges in P2P systems: 1) *atoms*, or physical goods, that can be stockpiled for future use, 2) *bits*, or information, that can be digitally copied, and 3) *presences*, or labors, that cannot be digitally copied or

stockpiled. Time slots for computing resources are typical presence-type values in P2P systems.

Since these values and resources are distributed over autonomous entities, exchanges of them need to be performed in an *incentive-compatible*[7] way: the coordination accomplished as an outcome of collective selfish behaviors. A medium of exchange which represents a guaranteed value should take an important role in the designs of P2P systems.

1.2 Complementary currencies

Money is a well-known medium of exchange, but its scarcity has caused a lot of problems. *Complementary currencies* (CC), or alternative forms of monetary media, have been proposed and tested in real life to achieve autonomy in the local economy even in short of money. There have been successful cases, such as experiments in Wörgl in 1932 (stamp scrip[16]), in Comox Valley in 1983 (LETS[17]) and in Ithaca since 1991 (Ithaca HOURS[10]).

These currencies are used to support values which are not readily circulated in today's economy, such as volunteer works, daily helps and enjoyments, or skills that are not regularly utilized. Studies of such currencies would benefit the designs of P2P systems, which are also intended to make use of under-utilized resources.

1.3 Classification of currencies

Currencies can be classified into categories shown in Table 1. In *debt-oriented currencies*, creation of an exchange medium implies that someone in the system is in debt, whereas in *labor-oriented currencies*, the systems themselves are in debt. Many of the existing currencies fall into the category of MCS[15] (Mutual Credit System), a form of debt-oriented currency in which participants freely credit one another, and the tradings are recorded in a single accounting system.

Many P2P currencies, or systems of exchange usable among peers on the Internet, can be thought analogous to the existing CC's as shown in Table 2. MojoNation[1] and Karma[18] are examples of MCS-counterparts in the P2P

*E-mail: ks91@sfc.wide.ad.jp

Table 1. Classification of CC's

	Centralized	Not centralized
Debt-oriented	MCS (LETS, Ithaca HOURS)	The WAT System
Labor-oriented	Stamp scrip	–

Table 2. Classification of P2P currencies

	Centralized	Not centralized
Debt-oriented	MCS (Karma, MojoNation)	<i>i</i> -WAT, PPay, Samsara
Labor-oriented	–	BitTorrent

context. PPay[20] resembles the WAT System[19], a poly-centric CC using *WAT tickets* as its media of exchange. A *WAT ticket* is like a bill of exchange, but without a specified redemption date or place.

We have proposed, implemented and been deploying *i*-WAT[11] based on the WAT System, implementing the tickets electronically by exchanging messages signed in OpenPGP[3].

It is debatable whether Samsara[5] and BitTorrent[4] are currencies or not, but they are systems of exchange. Their exchange media are computing resources such as storage space or bandwidth, respectively.

It is also debatable whether or not a decentralized labor-oriented currency is a possible concept, because if some peer works for another, that another peer is in debt, and the system is indistinguishable from being debt-oriented.

1.4 Contributions of this paper

This paper clarifies by simulations of existing currency systems the asymmetry in the possible outcomes of P2P tradings when atoms, bits and presences, or three classes of resources with different reproduction characteristics, are equally treated as commodities. This paper then proposes a solution called NEO (New Economic Order), in which bits are shared for free, while their producers are supported by peers, being given freedom to issue *reduction* tickets, or exchange media whose values are reduced over time.

NEO is compatible with the GNU manifesto[8] which states that software must be freely shared while programmers need support from communities. NEO is potentially useful for building economy around open source software.

2 MCS: Mutual Credit System

2.1 Concept

An MCS is an accounting system of exchange. When a member joins, the initial balance of their account is set to

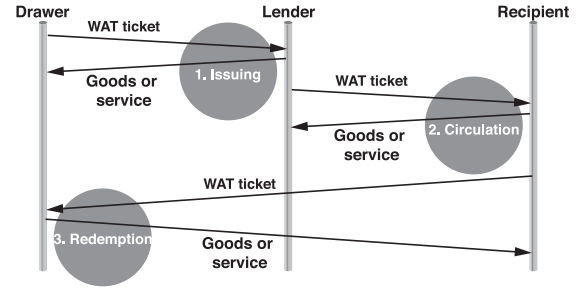


Figure 1. The WAT Core

zero. The system allows negative balance to some extent, and values are transferred between accounts by subtracting an amount at one end and adding the same amount at the other, as two members participate in a trade.

2.2 Implementations

LETS (Local Exchange Trading System) is the most common implementation of MCS which does exactly the above, but many other currency systems can be viewed as different forms of MCS by appropriate transformations without changing their semantics.

Many P2P currencies, including MojoNation, fall into the category of MCS.

2.3 Safety and risks

Theoretically, all accounts sum to zero in an MCS, which is a safety property of the system. However, maintaining this in practice is problematic.

If one has a deficit on one's account in an MCS, the debt is owed to the rest of the members[9]. This distribution of cost may lead to their indifference to the risks that the debt remains unpaid. This problem is discussed in depth in [13].

Sometimes, the expectation of the loss is compensated in the forms of maintenance fees, deposits or demurrages.

3 WAT/*i*-WAT currency system

3.1 The WAT System

3.1.1 Overview

The WAT System[19] uses a *WAT ticket*, a physical sheet of paper resembling a bill of exchange, as the medium of exchange. A lifecycle of a *WAT ticket* involves three stages of trading (or the *WAT Core*) as illustrated in Figure 1:

Issuing A *drawer* issues a WAT ticket by writing on an empty form the name of the provider (*lender*) of the goods or service, the amount of debt, the present date, and the drawer's signature. The drawer gives the ticket to the lender, and in return obtains some goods or service.

Circulation The person to whom the WAT ticket was given can become a *user*, and use it for another trading. To do so, the user writes the name of the recipient, as well as their own, on the reverse side of the ticket. The recipient will become a new user, repeating which the WAT ticket circulates among people.

Redemption The WAT ticket is invalidated when it returns to the drawer.

3.1.2 Security

In case the drawer fails to meet their promise on the ticket, the lender assumes the responsibility for the debt. If the lender fails, the next user takes over. The responsibility follows the chain of endorsements (*security rule*). The longer the chain is, the more firmly backed up the ticket is.

3.2 *i*-WAT: the Internet WAT System

3.2.1 Overview

i-WAT is a translation of the WAT Core onto the Internet. In *i*-WAT, messages signed in OpenPGP (*i*-WAT messages) are used to implement transfers of an electronic WAT ticket (*i*-WAT ticket). An *i*-WAT ticket contains a unique number, amount of debt and public key user IDs of the drawer, users and recipients. Endorsements are realized by nesting PGP signatures over canonical XML expressions.

3.2.2 Changes from the WAT System

Upon translating the WAT Core onto the digital networks, we have made the following changes from the state machine of a WAT ticket: 1) Trades need to be asynchronously performed. Intermediate states, such as waiting for acceptance or approval, are introduced, and 2) Double-spending needs to be prohibited. The drawer is made responsible for guaranteeing that the circulating ticket is not a fraud. This means that every trade has to be approved by the drawer of the involved ticket.

The semantics of this design and the trust model of *i*-WAT are discussed in detail in [12].

3.3 ROT: Reduction Over Time

It is known among the practitioners of complementary currencies that reducing the value of the exchange medium

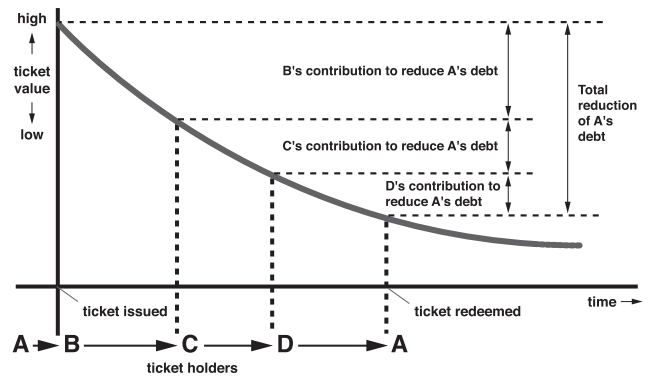


Figure 2. Reduction over time

over time accelerates spending, because users want to use the medium before its value decreases.

In [14], we applied the notion of *calendar money*[6] by A. Dahlberg to achieve it in our currency system. We have realized that this has potential effects of not only promoting exchanges, but also providing participants with means to mutually support peers, by sharing debts among one another in a form of currency.

We made a generalization to the value of an *i*-WAT ticket such that it is expressed as a tuple $\langle V_0, V_m, V_x, f \rangle$ presented by the drawer, where V_0 is the face value (initial value) of the ticket, V_m is the minimum value, V_x is the maximum value, and $f(t)$ is the differentiation (derivative) of some function of time $F(t)$.

The effective value V_t of a ticket at time t is given by the following equation:

$$V_t = \min(\max(\int_0^t f(t)dt + V_0, V_m), V_x)$$

This is a generalization to allow drawers to specify that the value of their ticket varies over time, limited by some minimum/maximum values. Typically, it holds that either $f(t) = 0$ for all t (*regular* ticket), $f(t) < 0$ for all t (*reduction* ticket) or $f(t) > 0$ for all t (*multiplication* ticket).

In [14], we clarified the semantics of a *reduction* ticket: reduction of the value means that the drawer's debt is reduced. The cost of reduction is first admitted by the lender who credits the drawer, and then shared among the endorsers as illustrated in Figure 2.

4 NEO: New Economic Order

We describe the concept of NEO (New Economic Order), which is a new way to treat information and their providers in the economy of digital networks.

Information has a near-infinite productivity once it is formed, because it can be copied at a minimum cost. Treating information as commodities together with physical resources and labors, including computing power, storage space and communication channels, is potentially problematic, because information providers can sell their information virtually unlimited times, accumulating purchasing power not comparable to those of others, whereas laborers or computers cannot even stockpile their time slots for future use, and may have limited occasions for selling.

In NEO, participants agree that information is shared for free, but the providers of information are supported by their allowance to issue *reduction* tickets.

5 Simulation model

5.1 Principles

This simulation is to help understanding the inherent properties of currency systems by using the simplest model possible. Thus, in the model, there is no money bill, there is only one bank (MCS) and no financial market. This is a model of a pure trust economy.

5.2 The world

The world consists of a set of participants U such that $|U| = 500$, set of materials of equal values M such that $|M| = 100$, and a manufacturer function f such that $f : U \mapsto M$. The manufacturers are evenly distributed, and approximately equal number of participants $u \in U$ manufacture a material $m \in M$, which they can trade with others.

The participants form a network $\langle U, K \rangle$ where K is an acquaintance relation (also called *links*) such that $K \subset U \times U$. It is assumed that the relation is symmetric: xKy always implies yKx . Initially, the population forms a scale-free network[2], and all participants can be reached from any other participants in a small number of hops.

Time is abstracted as a series of rounds. There is a special variable t of type integer to denote a round.

5.3 Production and consumption

The amount of material m owned by participant u at time t is denoted as R_t^{mu} . It is defined that u is satisfied with m at time t if $R_t^{mu} \geq 1.0$. Each material can have its own production and consumption rates, denoted as pr_m and cr_m , respectively.

The amount R_t^{mu} may vary during a round because of trades, and is finalized at the end of the round. The initial amount R_{t+1}^{mu} for time $t + 1$ is calculated as follows:

$$R_{t+1}^{mu} = R_t^{mu} \times (1.0 - cr_m) + Z$$

Table 3. Common parameters

Maximum debt	10.0
Maximum active trades per round	3
Probability to search the 2nd hop for a partner	0.2

where $Z = pr_m$ if $f(u) = m$, and $Z = 0$ otherwise.

This models production and consumption of material goods such as foods, but by adjusting pr_m and cr_m , it can also model labors ($cr_m = 1.0$) or information such as a data file (very large pr_m) as commodities, which are more notable subjects of exchanges in P2P systems.

5.4 Currencies

Currencies are valued by the amount of materials.

Each participant u has an account in an MCS, whose balance at time t is denoted as B_t^u .

Every participant u can use WAT/*i*-WAT currencies. A_t^u is the set of tickets u has acquired by time t , and D_t^u is the set of tickets u has drawn by time t . Every ticket $k \in A_t^u$ or $k \in D_t^u$ is considered to be a sequence of endorsers, where the drawer and lender are denoted as k_0 and k_1 , respectively. Thus for every $k \in D_t^u$, it holds that $k_0 = u$.

5.5 Welfare

Welfare W_t^u is a value representing how well the participant u has spent their lives in the world up to time t , based on the defined satisfaction condition $R_t^{mu} \geq 1.0$.

$$W_t^u = \sum_{i=1}^t \sum_{m \in M} \min(R_i^{mu}, 1.0)$$

The goals of the currency systems are twofold: 1) to maximize the welfare of participants, and 2) to minimize the variability in the distribution of welfare in the world.

5.6 Balance

Balance B_t^u is a value representing the purchasing power of the participant u at time t . Each participant can purchase materials as long as their debt (negative component of the balance) does not exceed the predefined maximum value.

$$B_t^u = \sum_{a \in A_t^u} \text{value}(a, t) - \sum_{d \in D_t^u} \text{value}(d, t) + B_t^u$$

For the purpose of this paper, uses of MCS accounts and WAT/*i*-WAT tickets are mutually exclusive.

Table 4. Production/consumption rates

	Products		
	Atoms	Presences	Bits
Production rate	3.0	3.0	250.0
Consumption rate	0.1	1.0	1.0

5.7 Trades

An *active trade* is to purchase 1.0 of a partner’s manufactured material. The condition for a successful trade for a participant u and their partner u' is $R_t^{mu'} \geq 1.0 \wedge R_t^{mu} < 1.0$ where $f(u') = m$. The maximum number of active trades allowed to a participant in one round is predefined.

A *passive trade* is to vend a material by the request of a partner. There is no limit in the number of passive trades.

5.8 Bankruptcy

At the end of a round, a participant may go bankrupt if their debt is equal to or greater than a specified limit, by a predefined probability p . This probability is called *bankruptcy rate* henceforth in this paper, but the actual probability p' for any participant to go bankrupt during a simulation is dependent on the probability p'' for their debt to reach the limit.

$$p' = 1 - \prod_{i=1}^t (1 - p \times p'')$$

The procedure for a bankruptcy of a participant u at time t is as follows: 1) Remove all (u, x) and (x, u) from the acquaintance relation K , 2) Add (u, x) and (x, u) to K for a random partner x , 3) Set $B_t^u = 0$ (the debt becomes inaccessible), 4) Empty D_u after for all $k \in D_u$ and $x = k_1$, adding k to D_x and removing u from k (the security rule), and 5) Empty A_u after for all $k \in A_u$ and $x = k_0$, removing k from D_x (treated as redemption).

In other words, u resets their relationships with others, and starts again.

6 Results

6.1 Settings

The population is evenly divided into three kinds of professions: providers of physical matters such as foods (atom providers), providers of labors (presence providers) and providers of information (bit providers). Each class of commodity comes with a different set of production and consumption rates, as shown in Table 4.

Presence providers have equal productivity as atom providers, but their products cannot be stored for future use.

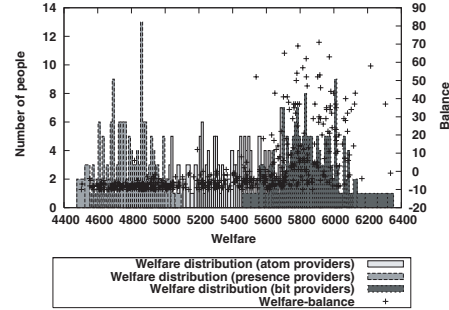


Figure 3. MCS (1)

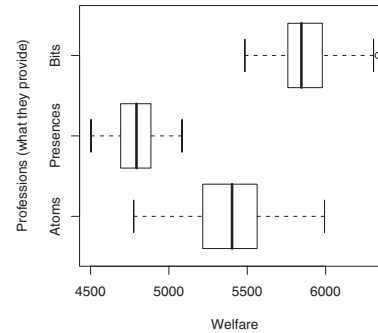


Figure 4. MCS (2)

Bit providers show extremely high productivity, but likewise, the information has to be regenerated in each round.

6.2 Results on MCS

Figures 3 (histogram/scatter plot) and 4 (box-and-whisker plot) show how the welfare distributions differ among different professions of participants in case of an MCS. A box-and-whisker plot shows the median as a thick line, and a box is drawn around them to cover first and third quartiles. Small circles represent values that are extreme. The box-and-whisker plots in this paper are made horizontal so that it is easier to compare them with the histograms.

The plots show that providers of information experience significantly high welfare than others. On the other hand, providers of labors seem to experience significantly low welfare. The scatter plot of welfare-balance in Figure 3 indicates that there is a strong asymmetry in the purchasing powers of participants, which resulted from the extremely reproductive nature of information; the bit providers never run out of their commodities, and the currency tends to be accumulated in their accounts.

Figure 5 shows how the differences grow as the time proceeds. The three professions are more separated in terms of their welfare as the time proceeds.

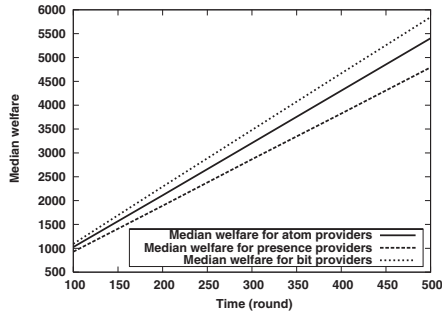


Figure 5. Growth of median welfare (MCS)

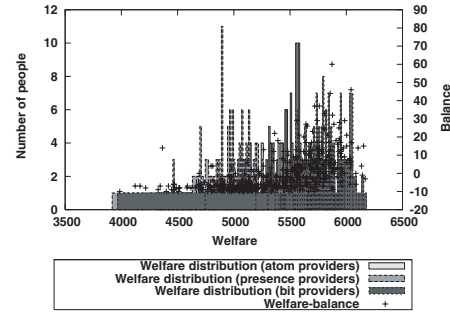


Figure 6. *i*-WAT (1)

6.3 Results on *i*-WAT

Figures 6 and 7 show how the welfare distributions differ among different professions of participants in case of an *i*-WAT currency. Although differences are smaller, providers of information still tend to experience significantly high welfare than others. There is a small correlation between having a high purchasing power and being a bit provider.

Equalizing this situation would require more drastic changes in how the economy works in this world.

6.4 Results on NEO

Figures 8 and 9 shows how the welfare distributions differ among different professions of participants in case of NEO, where bits are not sold but shared for free, and their providers are appreciated by the society's allowance to them to issue *reduction* tickets.

In this simulation, a bit provider is allowed to issue "vanishing" *reduction* tickets, whose values are scheduled to be reduced down to zero, with the over-time rate of -0.1 per round, and a presence provider is allowed to issue *reduction* tickets whose values are reduced down to half with the same over-time rate. The production and consumption rates for the commodity of a bit provider, which is no longer information but perhaps a labor to design new information, are set to 1.5 and 1.0, respectively.

The plots show that the distributions of welfare overlap one another for different professions. No correlation is found between the welfare and the purchasing power.

Readers may have noticed that shown welfare is significantly smaller in NEO than in other cases. This is because information is not treated as a commodity, which does not contribute in calculation of welfare, unlike other cases.

Figure 10 shows how the differences stay negligible in NEO as the time proceeds.

These results may look significant, but they have been achieved by manual adjustments of parameters for this particular simulation, and it is not at all clear how good

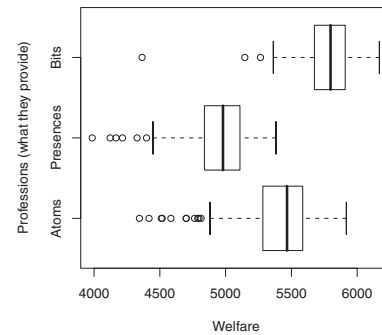


Figure 7. *i*-WAT (2)

these parameters will be in practice. We need a more autonomous, self-adapting way of allowing *reduction* tickets.

Figures 11 and 12 show results of NEO', in which all peers are non-discriminatively given freedom to issue *reduction* tickets whose values are reduced down to zero.

Although this seem to produce an equally fair outcome, we think this would be difficult to achieve in practice. Taking a *reduction* ticket necessarily means a loss of some amount, and there needs to be an incentive for the receivers of these tickets to help the issuers.

We need to come up with an incentive-based, self-adapting scheme somewhere between NEO and NEO' presented in this paper.

6.5 Results on MCS⁻

Readers may wonder that, since NEO is derived as a special usage of *i*-WAT, whether it is possible or not to derive a special usage of MCS which has a similar effect.

One answer may be an MCS with a demurrage (denoted MCS⁻), which is practiced in some CC's in real life, in order to bring an equity to the participants.

Figures 13 and 14 shows how the welfare distributions differ among different professions of participants in case of an MCS with a demurrage of -1% per round for the positive

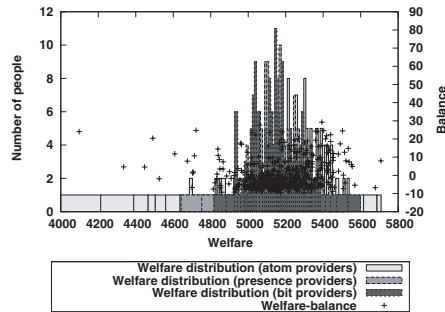


Figure 8. NEO (1)

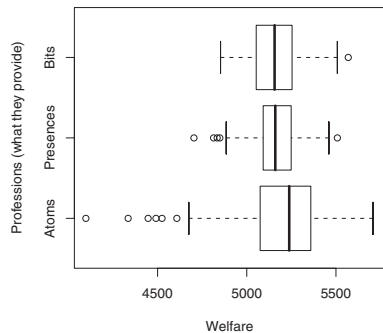


Figure 9. NEO (2)

balance. In this simulation, a bit provider can sell their bits, but their positive balance will be reduced after a round.

Intuitively, this should work because the purchasing power is averaged by the enforcement of a demurrage. The plots, however, show that the purchasing power is in fact averaged, but the demurrage does not seem to have such an effect of averaging welfare. This should be attributed to the fact that the purchasing power of a bit provider is not decreased until the end of a round, and they can purchase as many commodities as they find possible during a round.

7 Future Work

The work presented in this paper is just a start of devising a new system of exchange, and much more work is needed to make it both usable and useful in practice.

An important question is whether or not making information free deprives their producers of motivations to produce the information. We argue that NEO can motivate people to produce information because then they will be allowed to issue *reduction* tickets. These tickets can be issued only when the lenders agree to take it, and rational lenders would take them only when those tickets are likely to be taken by others, because they do not want to hold on to

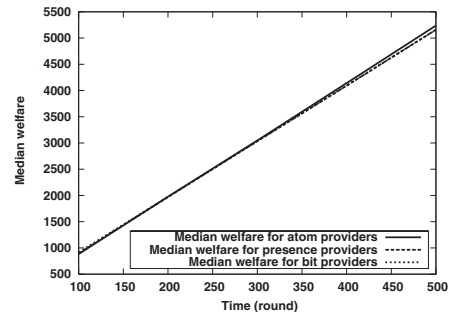


Figure 10. Growth of median welfare (NEO)

tickets whose values keep decreasing. Which suggests that producers will be rewarded by different levels of freedom to issue tickets based on the popularities of their work.

We will investigate how such different levels of freedom will affect the exchange systems.

8 Conclusions

Fair trading of information is potentially a problem in P2P systems because of the differences in reproduction of three classes of resources: atoms, bits and presences.

This paper clarified this point by simulating a small world of traders using existing trading systems. We proposed NEO (New Economic Order), in which bits are freely shared among participants, whereas their producers are supported by peers, being given freedom to issue exchange tickets whose values are reduced over time. We showed that this reduces the asymmetry in the outcomes of trades drastically, but more work is needed to make this mechanism more autonomous and usable in practice.

References

- [1] AZI. Mojo Nation technology overview. Online archive. Available electronically at http://web.archive.org/web/20020127125928/http://www.mojonation.net/docs/technical_overview.shtml.
- [2] A.-L. Barabási and R. Albert. Emergence of scaling in random networks. *Science*, 286, October 1999.
- [3] J. Callas, L. Donnerhacker, H. Finney, and R. Thayer. *OpenPGP Message Format*, November 1998. RFC 2440.
- [4] B. Cohen. Incentives build robustness in bittorrent. In *Proceedings of the First Workshop on Economics of Peer-to-Peer Systems*, May 2003.
- [5] L. Cox and B. Noble. Samsara: Honor among thieves in peer-to-peer storage. In *Proceedings of the ACM Symposium on Operating Systems Principles*, October 2003.
- [6] A. Dahlberg. *When Capital Goes On Strike*. Harper & Brothers Publishers, 1938.

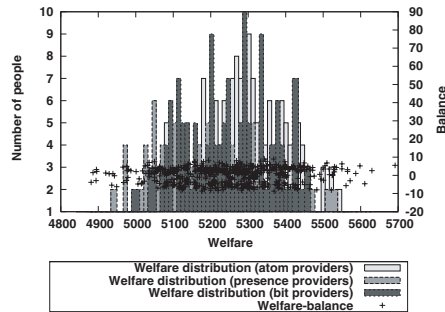


Figure 11. NEO' (1)

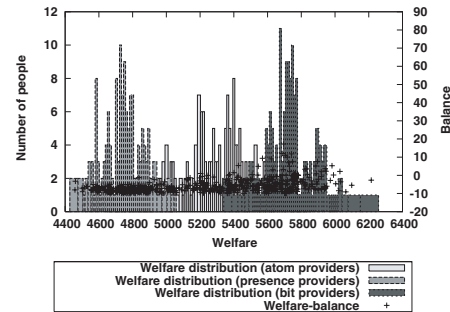


Figure 13. MCS- (1)

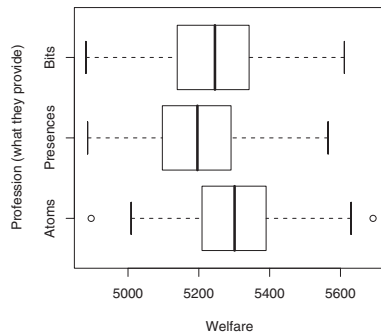


Figure 12. NEO' (2)

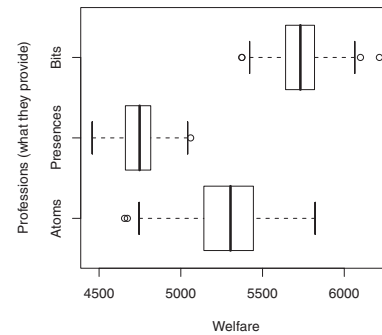


Figure 14. MCS- (2)

[7] J. Feigenbaum and S. Shenker. Distributed algorithmic mechanism design: Recent results and future directions. In *Proceedings of the 6th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communication (DIALM '02)*, September 2002.

[8] Free Software Foundation, Inc. The GNU operating system, since 1996. Hypertext document. Available electronically at <http://www.gnu.org/>.

[9] Global Public Media. Richard Douthwaite speaks with Julian Darley (Jan 2003). Hypertext document. Available electronically at <http://www.globalpublicmedia.com/interviews/123>.

[10] P. Glover. Ithaca HOURS Online. Hypertext document. Available electronically at <http://www.ithacahours.com/>.

[11] K. Saito. Peer-to-peer money: Free currency over the Internet. In *Proceedings of the Second International Conference on Human.Society@Internet (HSI 2003)*, Lecture Notes in Computer Science 2713. Springer-Verlag, June 2003.

[12] K. Saito. WOT for WAT: Spinning the web of trust for peer-to-peer barter relationships. *IEICE TRANSACTIONS on Communication*, Vol.E88-B(No.4), April 2005.

[13] K. Saito, E. Morino, and J. Murai. No risk is unsafe: Simulated results on dependability of complementary currencies. In *Proceedings of the First International Conference on Availability, Reliability and Security*, April 2006.

[14] K. Saito, E. Morino, and J. Murai. Reduction over time to facilitate peer-to-peer barter relationships. *IEICE TRANS-*

ACTIONS on Information and Systems, Vol.E89-D(No.1), January 2006.

[15] J. Schraven. Mutual credit systems and the commons problem: Why community currency systems such as LETS need not collapse under opportunistic behavior. *International Journal of Community Currency Research*, vol.5, 2001. Available electronically at <http://www.geog.le.ac.uk/ijccr/>.

[16] F. Schwarz. Das experiment von Wörgl, 1951. Hypertext document. Available electronically at <http://userpage.fu-berlin.de/~roehrigw/woergl/>, (*Shortened English translation by Hans Eisenkolb is available at http://www.sunshinecable.com/~eisehan/woergl.htm*).

[17] S. Seron. Local Exchange Trading Systems 1 - CREATION AND GROWTH OF LETS. Hypertext document. Available electronically at <http://www.gmlets.u-net.com/resources/sidonie/home.html>.

[18] V. Vishnumurthy, S. Chandrakumar, and E. G. Sirer. KARMA: A secure economic framework for p2p resource sharing. In *Proceedings of the Workshop on the Economics of Peer-to-Peer Systems*, June 2003.

[19] watsystems.net. WATSystems home page. Hypertext document. Available electronically at <http://www.watsystems.net/>.

[20] B. Yang and H. Garcia-Molina. PPay: micropayments for peer-to-peer systems. In *Proceedings of the 10th ACM conference on Computer and communications security (CCS '03)*, October 2003.