Maintaining Trust in Peer-to-Peer Barter Relationships

Kenji Saito
Graduate School of Media and Governance
Keio University
ks91@sfc.wide.ad.jp

Abstract

This paper proposes a barter currency system called i-WAT[12] to promote sustainable economy in peer-to-peer internetworking. i-WAT itself is a peer-to-peer system, without necessitating a central point of authority. It uses a digitally signed, electronic form of promissory note as the medium of exchange.

This paper illustrates how it should assist internetworking of peer-to-peer systems, and discusses, in particular, how trust can be maintained in such a currency system.

Among other means, the current design of i-WAT allows the notes to be transported over Jabber[8, 9] instant messaging protocol. A prototype of an i-WAT checkbook has been developed as a plug-in for a Jabber client. We are beginning to experiment on the actual usage of the currency system using the checkbook as well as provisional web applications.

1. Introduction

1.1. Peer-to-peer is a form of economy

My Japanese dictionary says that economy is "the act and process of production, distribution and consumption of goods and services which forms the bases of human communities, and the whole body of social relationships built upon such activities." It is not just about saving but about how finite resources are distributed in or among communities, which influences on how people interact with each other.

In this sense, economy and peer-to-peer are closely related; in fact, peer-to-peer is a form of economy, in which distribution of resources is performed without the necessity for central coordination.

1.2. Economy in autonomous distributed systems

Recent interests in *distributed algorithmic mechanism design*[5], unified efforts between economics (*mechanism design* part) and computer science (*distributed algorithmic* part), shows that researchers of distributed systems are beginning to pay more attention to incentives for cooperation and fairness of sharing resources.

Autonomous distributed systems require coordination among nodes to achieve their goals or to satisfy their requirement specifications. Since each node may behave selfishly to maximize its benefit, *incentive-compatibility*, roughly restated as the goal of the system being accomplished by collection of selfish behaviors, becomes important. Relationships among nodes in such a system necessitate fair exchange of the computing resources. Media for barter relationships seem essential for such designs, which may take forms of points or barter currencies [12].

2. Peer-to-peer currency

2.1. Reason for peer-to-peer currency

Money plays an important role in economy. As a medium of exchange, it eliminates the need for *double coincidence of wants*, in which each of the two parties is willing to consume what the other is producing. Resources are more effectively distributed without such a need for coincidence.

Today, however, money looks more like a problem than a solution. Its another role, a medium for accumulating wealth, has resulted in scarcity of the media, dividing the world into haves and have-nots, the former having control over the latter.

To be independent from such control, and to achieve sustainable local economy even in presence of attacks or global/national depressions, alternative forms of money have been proposed and tested. Successes of such experiments include Wörgl[13] in 1932, in Comox Valley[14] in

Proceedings of the 2004 International Symposium on Applications and the Internet Workshops (SAINTW'04)
0-7695-2050-2/04 $20.00 © 2004 **IEEE**

1983 and in Ithaca[6] since 1991. The one in Comox Valley promoted barter relationships.

Many of the successes are short-lived, however, because most designs of alternative money are dependent on the qualities of their administrations. Many experiments owe their successes to their first administrations which were more adequately motivated than later ones.

It would thus benefit the sustainability of economy if we could design a currency system without the necessity for central administration. As far as sustainable economy is concerned, currencies, too, need to be peer-to-peer.

2.2. Example of peer-to-peer currency

WAT System[16] is one of a few examples of existing peer-to-peer currency, in which a form of promissory note called *WAT note*, a physical sheet of paper, is used as the medium of exchange. Figure 1 shows the three types of trade in WAT System:

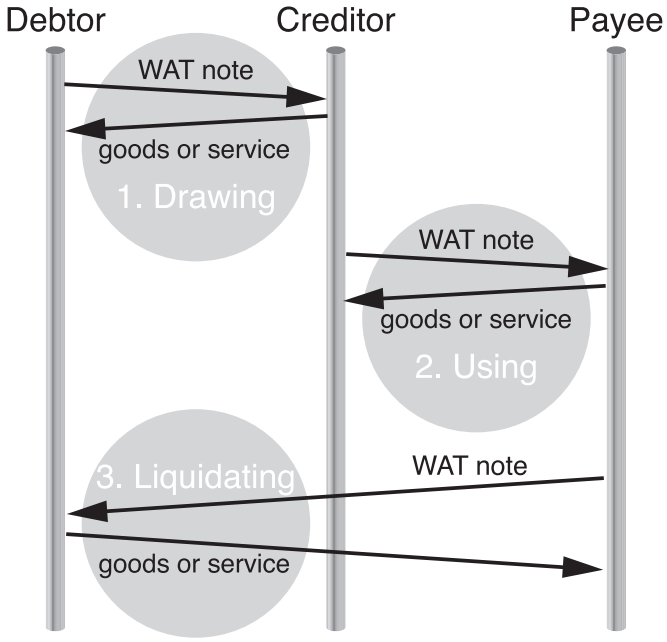

Figure 1. Trading with a WAT note

1. Drawing trade

   A person in want of some goods or service becomes a debtor, and issues a WAT note. The debtor writes on the note the name of the provider of the goods or service, the amount of debt[1] and the debtor's signature. The debtor hands the note to the one who becomes the creditor, and in return obtains the goods or service.

2. Using trade

   The creditor can use it for another trading. To do so, he or she writes the name of the payee on the back of the note. The payee becomes the new creditor, repeating which the WAT note circulates among people. The length of the chain of creditors shows how much trust the note has gained.

3. Liquidating trade

   The WAT note is invalidated when it returns, as a result of a trade, to the debtor.

[1]Typically in a unit called *WAT*, which represents cost of producing electricity from natural energy sources, but anyone can create their own units.

WAT System is a *free* currency in the following ways:

1. Administration-*free*

   Anyone can spontaneously start WAT System with a sheet of paper if they follow a few rules.

2. Interference-*free*

   It is independent of national or global economy.

3. *Free* location

   Any WAT note is compatible with any other WAT notes in the world, and the currency system is globally operable (although within the limit where one's credit can be trusted).

3. *i*-WAT: the Internet WAT

3.1. Overview

We developed *i*-WAT[12] as an extension of WAT System so that it can be used on the Internet. It is intended to be used by people or by autonomous programs in distributed systems.

The medium of exchange in *i*-WAT is a message signed in OpenPGP[4], by which transferring the ownerships of electronically represented WAT notes is implemented. The exchanged messages are called *i-WAT messages*, and the note represented by the messages is called an *i-WAT note*.

Table 1 shows the types of *i*-WAT message. All *i*-WAT messages are signed by its sender, and are formatted in the canonical form of XML[3] which handles nested signatures well.

3.2. Protocol

The three types of trade are implemented as follows:

Table 1. *i*-WAT messages

No.	Message name	Function
1	*i*-WAT <draw>	Draws an *i*-WAT note.
2	*i*-WAT <use>	Uses an *i*-WAT note.
3	*i*-WAT <accept>	Confirms the readiness to accept the provided *i*-WAT note once its validity is verified.
4	*i*-WAT <reject>	Rejects an *i*-WAT note.
5	*i*-WAT <approve>	Guarantees the validity of an *i*-WAT note, and approves the transaction.
6	*i*-WAT <disapprove>	Denies an *i*-WAT transaction.

Drawing trade

1. The debtor sends *i*-WAT <draw> message which contains the e-mail addresses of the debtor and the creditor, an identification number and the amount of debt. This message becomes the original *i*-WAT note after the protocol is completed.
2. The creditor sends back the *i*-WAT <draw> message to the debtor. This is called *i*-WAT <accept> message.
3. The debtor sends an *i*-WAT <approve> message to the creditor.

Using trade

1. The creditor adds to the *i*-WAT note the e-mail address of the payee, and sends it to the payee as *i*-WAT <use> message. This becomes the valid *i*-WAT note after the protocol is completed.
2. The payee forwards the *i*-WAT <use> message to the debtor as an *i*-WAT <accept> message. If the creditor wants to use multiple *i*-WAT notes at once, the payee must forward all the *i*-WAT <use> messages to all the debtors.
3. The debtor verifies the validity of the note, and sends an *i*-WAT <approve> message to the creditor and payee, as well as all other debtors in case multiple *i*-WAT notes are used at once, in order to assure atomicity of the transaction; the notes will not be transferred to the payee unless all <approve> messages are collected.

Liquidating trade

1. Like using trade, the creditor sends an *i*-WAT <use> message to the payee.
2. If the payee equals the debtor, the debtor invalidates the *i*-WAT note as the debt is now liquidated. The debtor sends *i*-WAT <approve> message to the creditor.

Figure 2 shows the most complicated case where a creditor uses multiple *i*-WAT notes issued by different debtors.

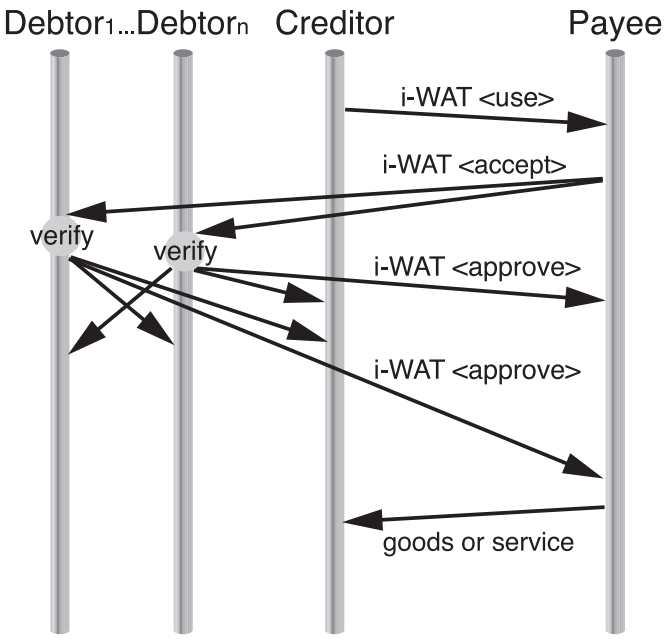

Figure 2. Trading with *i*-WAT messages

3.3. Usage

i-WAT can be used as the basis of various interpersonal/corporative interactions. Some specific applications are discussed in [12].

i-WAT can assist designs of cooperative peer-to-peer systems by providing a way of exchanging promises to cooperate. For example, a self-sufficient distributed computing system is conceivable, which provides services in return of *i*-WAT notes promising contributions of processor time, memory and/or disk storage.

4. Internetworking with i-WAT

4.1. Incentives for internetworking

There needs to be reasons for nodes to participate in and cooperate across multiple peer-to-peer systems or even within a single peer-to-peer system. Although i-WAT may work as a medium of exchange, that alone does not mean that it will assist the designs of actual autonomous distributed systems. We need to provide a mechanism for incentives and fairness.

In a monetary economy, accumulation of bank notes forms an incentive. As we described earlier, this results in scarcity of the media, and does not promote a fair exchange. Therefore, instead of using accumulation of notes, we use accumulation of trust of the nodes to build an incentive-compatible mechanism. Our hypothesis is that trust can be represented by how much transactions the node has successfully processed.

For example, the trust value of a node can be expressed in the following formula, which works as an incentive for the node to make transactions, and prompts the node for both using notes in possession and providing services for liquidating its debt, so that its income and outlay are balanced.

$$trust = \log \frac{income \times outlay}{|income - outlay| + 1}$$

This is the basic formula we use for now, a variation of which is discussed in section 6.2.

4.2. Example of exchange mechanism

The semantics of *i*-WAT inherited from WAT System allows the notes to be freely associated with values. Such values include *i*-WAT notes in different units in different currencies.

Figure 3 shows how *i*-WAT notes in different currencies can be exchanged with one another.

The figure shows three communities, A, B and C, depicted as rings. These communities can be circles of people, rings of Chord[15] (or some other forms of distributed hash tables), or just any groups of nodes in autonomous overlay networks. We assume that methods for message-routing exists among these communities. The communities use currencies A', B' and C' respectively.

An entity belonging to both communities A and B can become an exchange point between currencies A' and B'. Such an exchange point can take a note in A', and draw a new note in B', or vice versa. The value of the new note is backed up by the exchange point's possession of the original note.

A node in community A can ask the exchange point to draw a note in B' in return of a note in A'. The obtained note can be used to ask for some service in community B. *i*-WAT requires that the each end of a transaction must have the other's trusted public key. Those public keys can be signed by the exchange point.

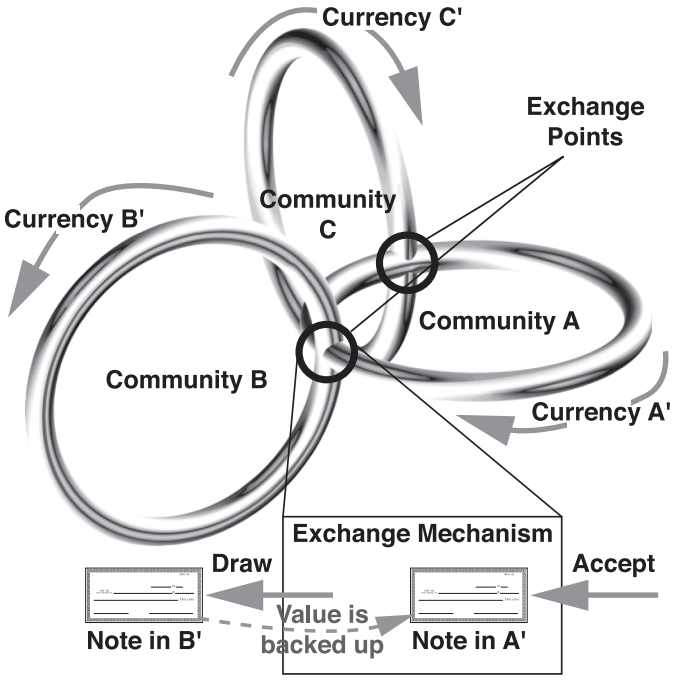

Figure 3. Exchanging *i*-WAT notes among different currencies

The exchange points are motivated to collect the drawn notes and give up the original notes, as it will insure the increase of their trust values. They are also motivated to advertise their services.

If someone in community B wants to issue a note in currency C', then they use the two exchange points in Figure 3 to exchange a note in B' to A' and A' to C'.

5. Discussions on trust

5.1. Embedded locality

In i-WAT, the debtors need to have the trusted public keys of all creditors appearing in the lifecycle of the notes they issued, because they are responsibile for verifying all the transactions using the notes.

Some argues that it is unlikely to happen in real-life. But we believe that this defines the system's locality; the above condition can easily be satisfied in a small group of people closely working together, where every one can verify and sign each other's public key. The condition can also be sat-

isfied, albeit marginally, according to the transitive nature of trust in PGP[1], because the both parties of a transaction must have each other's trusted public keys. While it is possible for an *i*-WAT note to travel across communities, the note would be more trusted if it stayed within one community. This is the reason for the need for exchange points described in section 4.2.

5.2. ID's accountability

The most frequent criticism against *i*-WAT is that it uses e-mail addresses (or whatever IDs coupled with PGP public keys) for identifying parties, which can be changed, reused or forged easily.

Suppose a PGP key-pair is generated for an imaginary person. Since the immediate parties of transactions must contain each other's trusted public key in *i*-WAT, the public key of the imaginary person must be signed by someone directly in acquaintance with the person: the creator of the person and thus, the forger. In order for the public key to be transitively trusted, the forger must be included in the chain of the creditors. If the imaginary person fails to liquidate the debt, as the forger intends, the forger him or herself must take over the debt being its immediate creditor. Therefore the cost of lying is considered high.

5.3. Distributed auditing

Since *i*-WAT is decentralized, calculation of the trust values of participating nodes needs to be achieved by collecting information from each transaction, and constructing an image of the node's account based on that information. There is no guarantee that the collected information is truthful if there are incentives for lying or colluding.

In order to tackle this problem, we first take a look at how a user's account information can be used for calculating their trust values. Table 2 shows how records of notes in a user's checkbook can be used in measuring their trusts.

We argue that the following statements are true:

1. There is no incentive to conceal the records of liquidated or used notes.

   The users would not claim less income and outlay in balance than there actually is because that would decrease their trust values.

2. One cannot lie to have more debit by claiming to have drawn more notes than they actually have, or more credit by claiming to possess more notes than they have, because they may be asked for proofs in auditing processes.

   If there are proofs for transactions which never happened, we believe that it should be considered a set of different problems: transactions without actual practice of bartering, and inflation in the value system which might result from such transactions. We believe there can be operational solutions for this sort of problems, and experimenting on solutions in the actual barter economies described later.

3. The only reasonable way to tell a lie is not to reveal the existence of debits or credits.

   As a countermeasure for this, we can apply the protocol for *fair sharing* described in [11].

Protocol to detect concealed debits (CD):

CD-1. At a random interval, to a randomly chosen user, one asks for a list of their possession of notes.

CD-2. For each note in the list, the one asks its debtor for the list of drawn notes.

CD-3. If the note in question is not included in the list, the debtor is lying about their debit.

Protocol to detect concealed credits (CC):

CC-1. At a random interval, to a randomly chosen debtor, one asks for a list of their drawn notes.

CC-2. For each note in the list, the one asks its current owner for the list of all notes they possess.

CC-3. If the note in question is not included in the list, the creditor is lying about their credit.

Note that in the above protocols, CD-1 and CC-2, as well as CD-2 and CC-1, are indistinguishable to the receiving end of the queries. Therefore there are disincentives to lie to the queries.

A debtor and the immediate creditor may have a reason to collude. They might lie that the transaction never took place. However, the relationship between a debtor and the immediate creditor is not symmetrical. It is riskier for the creditor because lying means denial of their crediting debt.

We are investigating further to make distribute auditing an inexpensive process.

5.4. Sustainability

Trust is also dependent on sustainability of *i*-WAT itself. *i*-WAT inherits the polycentric nature of WAT System, and should be difficult to break.

In *i*-WAT, the debtor is responsible for guaranteeing that the circulated note is not a fraud. In this sence the debtor is privileged, but it is not a single point of failure because once

Table 2. Meanings of *i*-WAT notes in the checkbook

Debtor of the note	Description	Role in trust value
This user	Liquidated	Balanced income and outlay
This user	Not liquidated	Negative balance or debit
Not this user	Possessed	Positive balance or credit
Not this user	Used	Balanced income and outlay

the debtor fails the immediate creditor takes the debtor's role; the function of the debtor follows the chain of creditors.

Which means that the rational behavior is never to take an *i*-WAT note directly from a debtor. While it is very true, people do not always act rationally, especially in a small group of people where everyone knows each other well. There is some risk if a note travels across communities, but as described in section 4.2, a community member is never obliged to take notes issued by members of other communities.

6. Deployment and experiments

6.1. Jabber-based *i*-WAT

i-WAT needs a decentralized message transport to assure its sustainability. While a DHT-based overlay network is being investigated to provide such functionality, we need to verify the design of *i*-WAT by quickly deploying it even in absence of a desired infrastructure.

i-WAT allows the underlying carrier of messages to be existing e-mail or presence/instant messaging system. A prototype of an *i*-WAT checkbook has been developed as a plug-in for a Jabber[8, 9] client, which will be made available to public soon.

A pre-release version has been used by a small group, and there are some findings. In particular, we discovered that even people with sufficient knowledge of PGP found the key exchange cumbersome. Perhaps there needs to be a support for secure public key exchange as a subsystem of *i*-WAT.

6.2. OMELETS and WIDE Hour

With distributed auditing described in section 5.3, we can treat the peer-to-peer currency system as if the account information comes from central sources.

There is an example of a barter currency with central authority called LETS (Local Exchange Trading System), which was first introduced in Comox Valley[14] in 1983.

We have developed OMELETS (Open, Modular and Extensible LETS), a collection of Java classes to implement LETS as a web application, in the hope that it becomes useful in verifying the designs of mechanisms using barter currencies.

An application of OMELETS have been developed for WIDE Project[18], a research project of distributed systems which has more than 700 active members. The barter currency for the project is called WIDE Hour[17] (the web site is for WIDE members only), based on the number of hours of labor for the project. The trust value is called *WIDE Power*, given by the following formula:

$$WIDE\ Power = \log \frac{income \times outlay}{|income - outlay| + 1} - penalty$$

where *penalty* is decided by the administration.

The maximum WIDE Hours each member can spend is limited to 24 WIDE Hours a day.

WIDE Hour was introduced in a four-day meeting in September 2003, and more than 500 transactions have been processed after one month.

6.3. Internetworking between web and peer-to-peer barter currencies

i-WAT can also implement WIDE Hour, and we are planning to connect the two implementations together in December 2003. Figure 4 illustrates how it should work.

WIDE Project has a strict notion of membership, but its activities often involve non-members. While it does not always make sense to provide non-members with accounts in OMELETS version of WIDE Hour, *i*-WAT notes in WIDE Hour can always be issued outside the project. By the internetworking mechanism, such notes can be made comptabile with the OMELETS version of WIDE Hour.

In the figure, there are two types of overlays. One is the overlays of activity groups, and the other is the overlay of OMELETS version of WIDE Hour. The former is peer-to-peer and the latter is a star network. The former overlays can interact with each other using *i*-WAT notes in WIDE Hour. A WIDE member can obtain such a note by asking WIDE Hour Office for an exchange.

It works just like the exchange point in Figure 3, only that the office accepts payments in LETS, which backs up the value of the new *i*-WAT note.

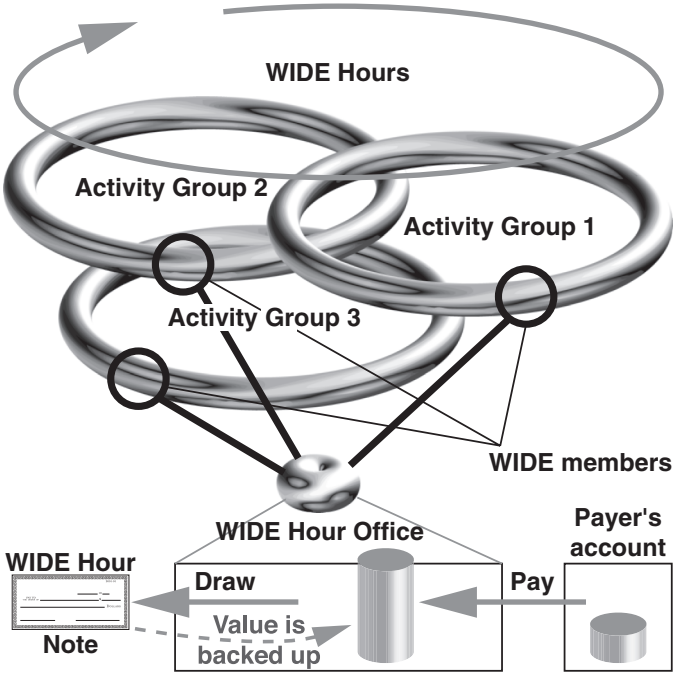

Figure 4. Exchanging WIDE Hours outside the WIDE members

6.4. MANA

MANA is another application of OMELETS, involving a book[10] equipped with an Auto-ID[2]-compilant 2.45GHz RFID (Radio Frequency IDentification) tag.

The barter economy of MANA allows the users to obtain points by visiting certain locations where RFID readers are placed, and having their books identified by the readers. Obtained points can be used in a community residing on the web[7].

This is a large-scale experiment; about 10,000 copies of the book is expected to be circulated by March 2004, and we expect that about 2,000 people will participate in the experiment.

We plan to experiment on internetworking between web and peer-to-peer currencies using this barter economy also.

7. Conclusions

This paper proposed usage of a barter currency system called *i*-WAT to promote sustainable economy in peer-to-peer internetworking.

i-WAT inherited its polycentric nature from WAT System, its predecessor in the physical world. It is carefully designed not to introduce any single point of failure. Trust is also maintained without necessitating a central authority.

A prototype of an *i*-WAT checkbook as well as provisional web applications have been developed. Experiments are ongoing.

References

[1] A. Abdul-Rahman. The PGP trust model. *EDI-Forum: the Journal of Electronic Commerce*, April 1997.

[2] Auto-ID Center. Auto-ID Center - About The Center. Hypertext document. Available electronically at http://www.autoidcenter.org/.

[3] J. Boyer. *Canonical XML Version 1.0*, March 2001. W3C Recommendation. Available electronically at http://www.w3.org/TR/xml-c14n.

[4] J. Callas, L. Donnerhacke, H. Finney, and R. Thayer. *OpenPGP Message Format*, November 1998. RFC 2440.

[5] J. Feigenbaum and S. Shenker. Distributed algorithmic mechanism design: Recent results and future directions, September 2002.

[6] P. Glover. Ithaca HOURs Online. Hypertext document. Available electronically at http://www.ithacahours.com/.

[7] Media Art Online (ed.). ACCIANCO.JP. Hypertext document. Available electronically at http://www.accianco.jp/.

[8] J. Miller. *XMPP Core*, January 2003. Internet-Draft.

[9] J. Miller. *XMPP Instant Messaging*, January 2003. Internet-Draft.

[10] J. Murai. *Explorers! of the Wonderful Internet*. TaroJiro-Sha Editus, 2003. *(in Japanese)*.

[11] T.-W. J. Ngan, D. S. Wallach, and P. Druschel. Enforcing fair sharing of peer-to-peer resources. In *2nd International Workshop on Peer-to-Peer Systems (IPTPS)*, Berkeley, California, February 2003.

[12] 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.

[13] 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)*.

[14] 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.

[15] I. Stoica, R. Morris, M. F. K. David Karger, and H. Balakrishnan. Chord: A scalable peer-to-peer lookup service for internet applications. In *Proceedings of ACM SIGCOMM*, August 2001.

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

[17] WIDE Hour Office. WIDE Hour Web. Hypertext document. Available electronically at https://fran.sfc.wide.ad.jp/hour/.

[18] WIDE Project. WIDE Home Page. Hypertext document. Available electronically at http://www.wide.ad.jp/.