Peer-to-Peer Money: Free Currency over the Internet

Kenji Saito

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

Abstract. *This paper proposes a resilient, alternative monetary system on the Internet called i-WAT, based on WAT System[1] which uses a form of promissory note as the medium of exchanging goods and services. i-WAT uses an electronic version of the note, ownership of which is transferred by exchanging messages signed in OpenPGP[2].*
i-WAT can be used as the basis of various interpersonal/corporative transactions in the globally distributed computing environment. Specific applications being investigated include distributed consumer reports, an alternative copyright system and spam-free e-mail exchange.
A prototype of an i-WAT checkbook has been developed as a plug-in for a Jabber[3] client. Experiments are ongoing.

1 Introduction

1.1 Need for a Resilient, Alternative Monetary System

As the Internet has become more seriously taken, efforts are now undertaken in order to make it a more resilient infrastructure[4]. Such efforts include construction of archival storage mechanisms which let information to survive in the face of global disaster. It should be obvious that what we really want to make survive here is our activities which require that information. The Internet has become such an important infrastructure for our lives that it is not permitted to fail. However, that alone cannot assure survival of our ways of lives.

Economy is also an important infrastructure, based on which we can continue our activities and relationships. Yet it does not require a destructive event to destroy the regional economy. The monetary systems today are susceptible not only to physical damages but also to economic attacks or even just depressions.

Researches and experiments have been conducted in the area of local currency to achieve sustainable local economies even in presence of global or national depressions. There have been successes, some are glorious, such as experiments in Wörgl[5] in 1932, in Comox Valley[6] in 1983 and in Ithaca[7] since 1991.

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

It would thus benefit the sustainability of economy if we could design an administration-free monetary system. Since such a system gives anyone freedom of creating one's own autonomous economy, it would in fact benefit human activities in general, without presence of a crisis; anyone will be able to create and apply alternative economy suitable for specific activities, which are not made possible with national currencies. This would especially benefit the activities on the Internet where people are less restricted.

1.2 Proposed Goal

We propose to design an alternative monetary system satisfying the following:

1. Administration-freedom
   The system should not require presence of a government or any central point of control. In particular, it should not introduce any single point of failure.
2. Interference-freedom
   The system should not be affected by global or surrounding economy.
3. Location-independence
   Circulation of the currency should not be limited within a local community. In fact, it should circulate globally over the Internet.

Since the third property makes it inappropriate to call it a local currency, we would like to call it *free currency*, after the original idea of alternative monetary system by Sylvio Gesell[8].

As it turns out that local currency system which satisfies most of the above properties (except global circulation over the net) exists, our approach is to translate it onto a system on the Internet.

2 WAT System

2.1 Overview

WAT System[1] is a local currency designed by Dr. Eiichi Morino, the founder of Gesell Research Society Japan[9]. A form of promissory note called *WAT note*, a physical sheet of paper, is used as the medium of exchange in the system.

Figure 1 shows the three types of trade involving 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.

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

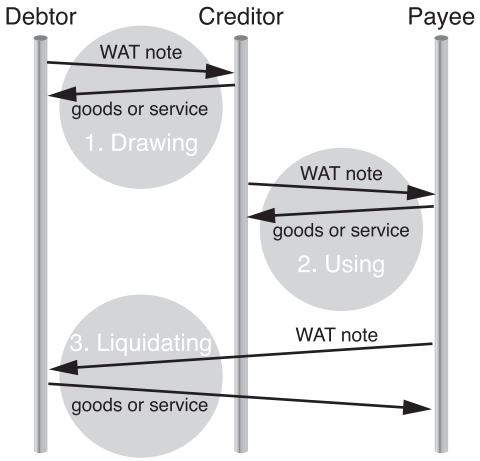

Fig. 1. Trading with a WAT note

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

2.2 WAT System's Architecture

WAT System is characterized by its polycentric nature. While almost all other local currency systems require a central office, WAT System can be operated without any centralized authority.

Anyone can begin using WAT System with a sheet of paper if 1) it contains the names of debtor and the first creditor with a place for the sequence of the payees' names, 2) there is a proof of drawing, and 3) they follow the rule that the debt is liquidated when the note comes back to the debtor.

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

These properties are useful for constructing a resilient, autonomous monetary system on the Internet.

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.

3 *i*-WAT: the Internet WAT

3.1 Overview

This paper proposes *i*-WAT as an extension of WAT System on the Internet.

In *i*-WAT, the medium of exchange is a message signed in OpenPGP[2], 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 messages. All *i*-WAT messages are signed by its sender, and are formatted in the canonical form of XML[10] which handles nested signatures well.

i-WAT is designed so that it maintains the polycentric nature of WAT System, while avoiding to follow the predecessor where straightforward translation of WAT System into the digital domain makes it easy to practice fraud.

i-WAT is carefully designed not to introduce any single point of failure.

3.2 Conditions

Trusted Public Keys The following conditions have to be met:

1. The debtor has the trusted public keys of all creditors appearing in the lifecycle of the *i*-WAT note they issued.
2. A creditor has the trusted public keys of the debtor and the immediate payee.
3. A payee has the trusted public keys of the immediate creditor and the debtor.

These conditions can be satisfied, albeit marginally, according to the transitive nature of trust in PGP[11], if the both parties of a transaction have each other's trusted public keys. The first condition defines *community-locality* of the system; *i*-WAT works best if it is used in a small group of people closely working together, regardless of their locations.

Reliable Multicast Communication channels need to satisfy reliable multicast[12]:

1. Validity – If a correct process multicasts a message m, then it will eventually deliver m.
2. Agreement – If a correct process delivers a message m, then all other correct processes in the group will eventually deliver m.

Today's e-mail tranfer or instant messaging protocol virtually supports validity and agreement, and it can be used for verifying the protocol design of *i*-WAT in the early deployment stage.

3.3 Protocol

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 will become a 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 would like to use multiple *i*-WAT notes at once, the payee must forward all the *i*-WAT <use> messages to all the debtors, the initiators of the notes.
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 in one transaction, 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. 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.

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

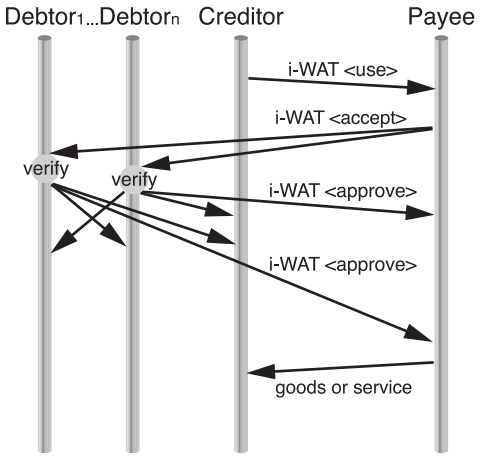

Fig. 2. Trading with *i*-WAT messages

4 Applications

4.1 DCR: Distributed Consumer Reports

DCR is an attempt to create a structure for administration-free exchange of information among consumers about the goods and services they use. Its challenges are to maintain liveness of and credibilities to the circulated information, to which we approach by letting subscribers of reports make payments in *i*-WAT.

DCR is also a subsystem of *i*-WAT. Many applications of *i*-WAT require that the balance of a user's *i*-WAT account is made available to others. Since *i*-WAT is decentralized, this needs to be achieved by collecting information from each transaction, and constructing an image of a user's account based on that information. DCR is used for building and circulating such an image associated with the user's public key, as well as the trustworthiness of the key itself.

The current design of DCR utilizes Distributed Hash Table (DHT)[2] , but the specific algorithm to be used is still undecided. DCR makes multiple nodes responsible for a given item, by applying a technique introduced by Tapestry[14], in order to avoid having a single point of failure.

Figure 3 shows how DHT and *i*-WAT can be applied to making and circulating distributed consumer reports. Nodes A and E are the *informatin roots* for a given item, based on the DHT algorithm in use. For a different item, a different

[2] DHT provides a lookup service of <key, value> pairs, which maps the key to the responsible node in the distributed system. Typically, keys and node IDs share the same n-bit name space, and are evenly distributed in the space using a one-way hash function. Several DHT-based overlay network prototypes have been proposed, including Chord[13] and Tapestry[14].

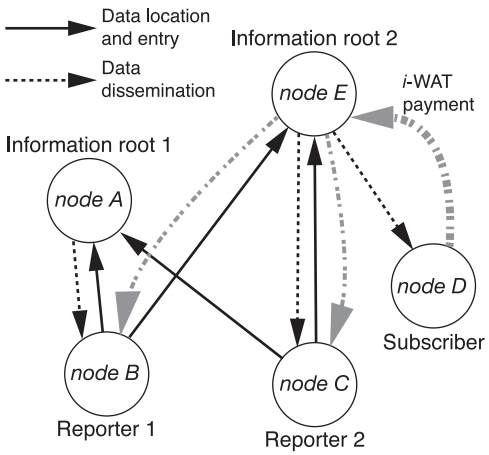

Fig. 3. Application of DHT and *i*-WAT to consumer reports

set of nodes would be selected as its roots. The selection is made autonomously and deterministically without imposing an expensive agreement protocol. Reports are compiled at the information roots based on the information gathered from the *reporters* (nodes B and C). A *subscriber* (node D) can obtain the reports from either of the information roots (decided by proximity), and pays an agreed amount in *i*-WAT to the one they choose to use. The payed amount are shared among the root and the reporters. In case the reports are about the trust or account information of *i*-WAT users, they should be obtained free of charge, because the cost of maintaining the monetary system should be equally shared among the users (also, we need to avoid infinite recursion). The reports can be either obtained by queries, or disseminated among registered users.

4.2 Share-ik: an Alternative Copyright System

Share-ik[15] (Share intelligence and knowledge) encourages derivation of new work from copyrighted materials.

Share-ik is essentially a set of rules close to the GNU General Public License[16], which defines a logical shared space from which public domain materials and their descenders may not leave. In order to apply this idea of "copyleft" to artistic creations such as music, Share-ik adds a rule for mutual evaluation: when new work is produced by reusing some existing work in the shared space, the reuser is asked to make a payment in *i*-WAT (in a unit called *share*) to the authors of the original work whom they appreciate. *i*-WAT protocol lets the original authors choose not to receive the payment for typically two reasons: 1) they do not agree with the new creation, or 2) a DCR query shows that the credibility of the reuser is doubtful. The latter can be a result of their work not being appreciated by others in the community, leading to much less income in *share* than its outlay.

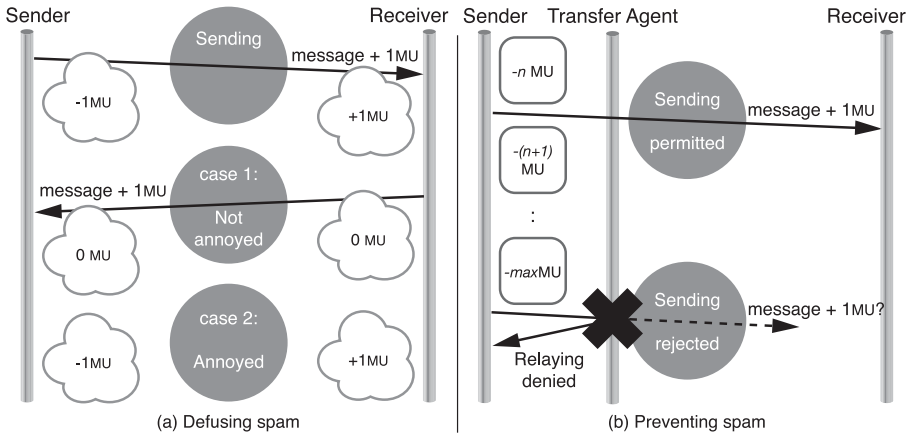

Fig. 4. Defusing/preventing spam in spam-free e-mail exchange

In this way, the original authors can know how much appreciation their work are receiving, and the reuser can know whether their creation was agreeable to the original authors, or if they are welcome in the community.

4.3 SAFEE: SpAm-Free E-mail Exchange

SAFEE takes a psycho-economical approach to solve the problem of spam. Let us define spam as an e-mail message receiving which the receiver feels a loss rather than a benefit. Our solution is to counterbalance the loss with an *i*-WAT payment. The unit of payment in SAFEE is called *MU* (Mail Unit).

In SAFEE, there is one simple rule:

> The sender of a message must pay $1MU$ to each receiver of the message.

The assumption here is that if any two parties have a healthy relationship, on average the amount of messages exchanged between them is evenly balanced, and they should not feel loss.[3] On the other hand, few people would reply to unsolicited e-mail, which means that the sender loses $1MU$ for each receiver of their message. The receivers gain $1MU$ each, which they can use for sending an e-mail message or exchange with other *i*-WAT currencies; the loss is compensated by the payment. Figure 4(a) illustrates this idea of defusing spam.

This message transfer system can be augmented by the following rule:

> A transfer agent must reject relaying a message if the negative balance of the sender's *MU* account is more than *max MU*.

[3] A small difference is not a problem as *i*-WAT has a weak budgetary constraint.

where *max* is sufficiently large so that it does not prevent ordinary people from sending messages. A DCR query is used for checking the sender's account. Figure 4(b) illustrates this idea of preventing spam.

An obvious problem with SAFEE is that since *i*-WAT is based on OpenPGP, it is easy to forge one's identity by creating key pairs for arbitrary e-mail accounts. To handle such situations, the transfer agents can also check with a DCR query if the public key of the sender is backed up by trusted signatures.

5 Deployment and Future Work

i-WAT needs a decentralized message transport to make its full use. 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[3] client, which will be made available to public soon. The client and plug-in will also be used for simulating a peer group network to verify the design of distributed consumer reports, which is an important subsystem of *i*-WAT.

Spam-free e-mail exchange is especially difficult to test and deploy on the current e-mail system, since it would require a redesign of its core protocols. Instead, we will start with implementing the rules on Jabber messaging, which has not gained much popularity yet.

6 Related Work

Magic Money[17] is an example of message-based currencies on the Internet using PGP signatures in the early 1990s. Although there was a few enthusiasts, the use of Magic Money did not spread widely for several reasons:

1. It utilized Chaum's blind signature protocol[18] which was patented at the time (still is). Since Magic Money was distributed as a free, open source software, its existence itself was unlawful.
2. It required presence of a server, which had to be maintained by someone.
3. It pursued untraceability while there was nothing to back up the values of the digital coins. The system was regarded as untrustworthy.

We regard Magic Money as an important lesson, and will make further analysis on the reasons why it did not become so successful.

7 Conclusions

In order for humanity to survive in presence of global disasters, depressions or attacks, economy needs to be just as resilient as the underlying information

structures. It would also help anyone who has presence on the Internet to create and apply alternative economy that would benefit their activities.

This paper proposed *i*-WAT, a free currency on the Internet, to achieve these. Its polycentric nature helps realizing a system without a single point of failure. Whether or not appropriate economy can be derived from this monetary system is being verified by the designs of proposed applications.

References

1. watsystems.net: WATSystems home page. Hypertext document. Available electronically at http://www.watsystems.net/.
2. Callas, J., Donnerhacke, L., Finney, H., Thayer, R.: OpenPGP Message Format. (1998) RFC 2440.
3. Miller, J.: XMPP Instant Messaging. (2003) Internet-Draft.
4. IRIS project: IRIS: Infrastructure for Resilient Internet Systems. Hypertext document. Available electronically at http://iris.lcs.mit.edu/.
5. Schwarz, F.: Das experiment von Wörgl (1951) Hypertext document. Available electronically at http://userpage.fu-berlin.de/∼roehrigw/woergl/.
6. Seron, S.: 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.
7. Glover, P.: Ithaca HOURs Online. Hypertext document. Available electronically at http://www.ithacahours.com/.
8. Gesell, S.: The Natural Economic Order. The Free Economy Publishing Co. (1934) Translated from the sixth German edition (originally published in 1913).
9. Gesell Research Society Japan: Gesell Research Society Japan. Hypertext document. Available electronically at http://www.grsj.org/.
10. Boyer, J.: Canonical XML Version 1.0. (2001) W3C Recommendation. Available electronically at http://www.w3.org/TR/xml-c14n.
11. Abdul-Rahman, A.: The PGP trust model. EDI-Forum: the Journal of Electronic Commerce (1997)
12. Hadzilacos, V., Toueg, S.: A modular approach to fault-tolerant broadcasts and related problems. Technical Report TR94-1425, Department of Computer Sciecne, Cornell University (1994)
13. Stoica, I., Morris, R., David Karger, M.F.K., Balakrishnan, H.: Chord: A scalable peer-to-peer lookup service for internet applications. In: Proceedings of ACM SIGCOMM. (2001)
14. Zhao, B.Y., Kubiatowicz, J.D., Joseph, A.D.: Tapestry: An infrastructure for fault-tolerant wide-area location and routing. Technical Report UCB//CSD-01-1141, U.C.Berkeley (2000)
15. Kitamura, I.: Construction of a model to share and evaluate music on the Internet (2003) Graduate thesis, Faculty of Policy Management, Keio University *(in Japanese)*.
16. Free Software Foundation, Inc.: GNU general public license (1991) Hypertext document. Available electronically at http://www.gnu.org/licenses/gpl.html.
17. Woodcock, M.: Magic Money. Hypertext document. Available electronically at http://www.csee.umbc.edu/ ∼woodcock/cmsc482/proj1/magmoney.html.
18. Chaum, D.: Blind signatures for untraceable payments. In: Advances in Cryptology – Crypto '82, Springer-Verlag (1983)