Multiplication Over Time to Facilitate Peer-to-Peer Barter Relationships

Kenji Saito*
Graduate School of Media and Governance
Keio University

Eiichi Morino
Gesell Research Society Japan

Jun Murai
Faculty of Environmental Information
Keio University

Abstract

A peer-to-peer complementary currency can be a powerful tool for promoting exchanges that make use of under-utilized computing resources in a trusted way. i-WAT[11] is a proposed such currency based on the WAT System[16], a polycentric complementary currency using WAT tickets *as its media of exchange: participants spontaneously issue and circulate the tickets as needed, whose values are backed up by chains of trust. i-WAT implements the tickets electronically by exchanging messages signed in OpenPGP[3].*

This paper proposes an extension to the design of i-WAT to facilitate trades. In particular, we propose additional "multiplication" tickets whose values increase over time. By deferring redemption of such tickets, the participants can receive the premium realized by increased debts of the issuers. A game-theoretical analysis shows that this feature is incentive-compatible: the issuers have no reason to strategically default despite the increased debts.

A reference implementation of i-WAT has been developed in the form of a plug-in for an XMPP[5][6] instant messaging client. We have been putting the currency system with the proposed feature into practical use.

1 Introduction

1.1 Peer-to-Peer Complementary Currency

To make use of under-utilized computing resources in a network of computers, proper exchanging is a necessity. Since the resources are distributed over autonomous entities, such exchanging needs to be performed in an incentive-compatible[7] way: the coordination must be accomplished by collection of selfish behaviors. A medium of exchange which represents a guaranteed value should take an important role.

Money is a well-known medium of exchange, but its scarcity has caused a lot of problems. *Complementary currencies*, or alternative forms of monetary media, have been proposed and tested in real life to achieve an autonomous and sustainable local economy even in short of money. There have been successful cases, such as experiments in Wörgl in 1932 (stamp money[14]), in Comox Valley in 1983 (Local Exchange Trading System[15]) and in Ithaca since 1991 (Ithaca HOURs[9]).

Those complementary currencies, being generated closer to the places in need, 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. Translating them onto the Internet would benefit design of peer-to-peer systems, which are also intended to make use of under-utilized resources. But then, those currencies also need to be peer-to-peer.

We proposed *i*-WAT[11] in year 2003 as such a currency usable on the Internet, based on the WAT System[16]. The WAT System is a real-life, polycentric complementary currency 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. *i*-WAT implements the tickets electronically by exchanging messages signed in OpenPGP[3]. It has been put into practical use since June 2004.

1.2 Varying Over Time for Facilitation

It is known among the practitioners of complementary currencies that reducing the value of the exchange medium over time accelerates spending. The stamp money experiment in Wörgl in 1932 is a well-known example. It was based on the idea of *stamp scrip*[8] introduced by Sylvio Gesell, who believed exchange media must also deteriorate as the exchanged goods do.

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

Proceedings of the 16th International Workshop on Database and Expert Systems Applications (DEXA'05)
1529-4188/05 $20.00 © 2005 **IEEE**

In [13], we applied the notion of *calendar money*[4] by Arthur 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.

But varying over time needs not to be limited in one direction. There is another example of a real-life complementary currency, called MAAS[10], whose exchange medium increases its value over time. A MAAS ticket is intended to be issued by an artist, who promises to provide (artistic) goods in the future which will worth more than the value being exchanged in an ongoing trade. MAAS helps those who want to create something but lack resources to do so at the moment.

1.3 Contributions of This Paper

This paper proposes an extension to the design of *i*-WAT to realize *multiplication* tickets, similar to those of MAAS[1], whose values increase over time. It shows that the extension is incentive-compatible by a game-theoretical analysis.

Multiplication tickets can be used in peer-to-peer systems to facilitate exchanges of data or services which are strongly needed by some parties to create new data or services (new values), without sacrificing their current ownerships of resources. They can even control the timing of redemption to some extent by an incentive mechanism.

Applications may include collection of sensory data from many locations to provide value-added services, such as weather or traffic forecasting.

2 WAT/*i*-WAT Currency System

2.1 The WAT System

2.1.1 Overview

The WAT System[16] is a complementary currency designed by Eiichi Morino, a coauthor of this paper.

A *WAT ticket*, a physical sheet of paper resembling a bill of exchange, is used as the medium of exchange in the system. A lifecycle of a WAT ticket involves three stages of trading (or the *WAT Core*) as illustrated in Figure 1:

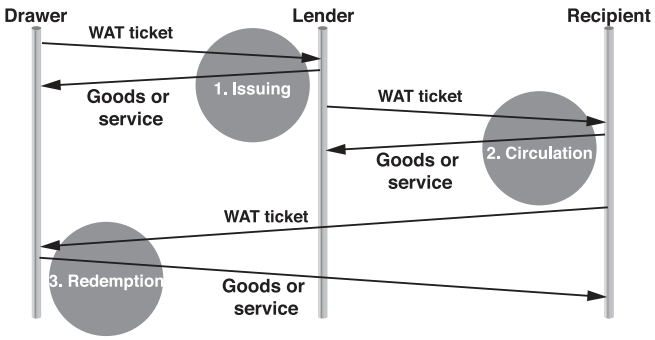


Figure 1. The WAT Core: three stages of trading with a WAT ticket

1. Issuing – the birth of a WAT ticket

   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[2], the present date, and the drawer's signature. The drawer gives the ticket to the lender, and in return obtains some goods or service.

2. Circulation – ordinary exchange

   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.

3. Redemption – the return of the WAT ticket

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

2.1.2 Security of the WAT System

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. The longer the chain is, the more firmly backed up the ticket is.

2.2 *i*-WAT: the Internet WAT System

2.2.1 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 electronically represented WAT ticket (*i-WAT ticket*).

An *i*-WAT ticket contains the identification number, amount of debt and public key user IDs of the drawer, users and recipients. Endorsements are realized by nesting PGP signatures over the stanzas in the canonical form[1] of XML[2].

[1] MAAS is indeed a variation of the WAT System.

[2] Typically in the unit kWh, which represents cost of producing electricity from natural energy sources.

2.2.2 Changes from the WAT System

Upon translating the WAT Core onto the digital communication domain, 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.

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 MOT: Multiplication Over Time

3.1 Concept

We make 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 a function of time $F(t)$. If minimum/maximum values are not applicable, V_m/V_x are set to be $\perp/\top$ respectively.

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 the value of a ticket to vary 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 [13], 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.

3.2 Multiplication Over Time

This paper focuses on clarifying the semantics of a *multiplication* ticket. Multiplication of the value means that the drawer's debt is increased. The increased value is first potentially received as a premium by the lender who credits the drawer, and then shared among the endorsers as illustrated in Figure 3. The amount of the total increase is manifested to the drawer upon redemption. By deferring redemption, the participants can maximize their gains. Intuitively, this would motivate the participants to receive the ticket (and to provide something in return).

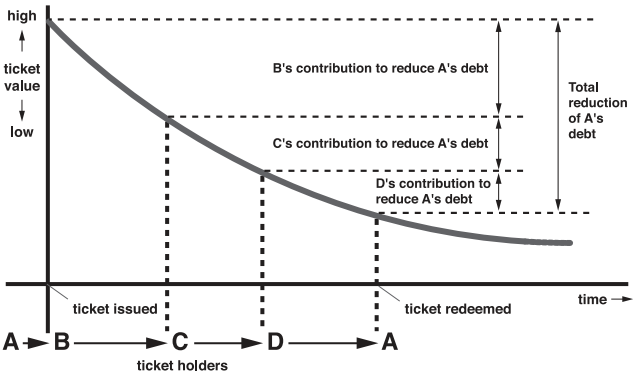


Figure 2. Giving relief by deferring redemption of a reduction ticket

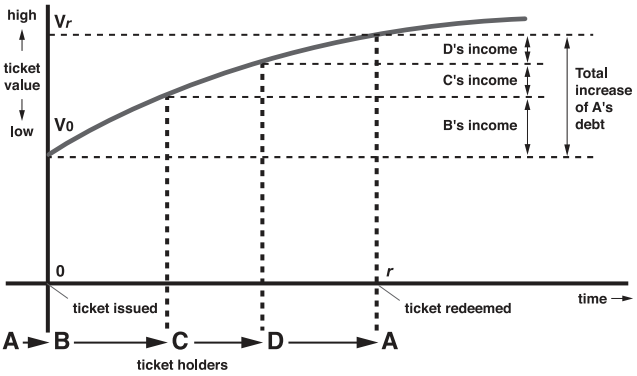
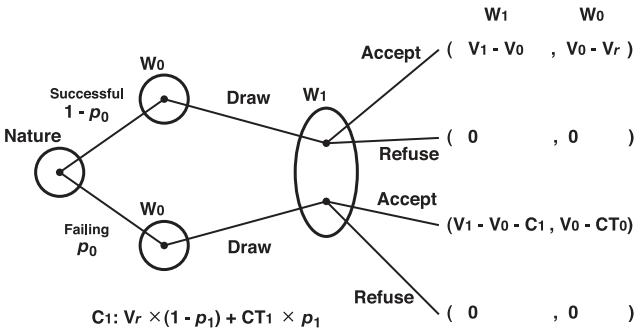


Figure 3. Offering a premium by allowing deferred redemption of a multiplication ticket

In the analysis to follow,

- Participants are denoted as W (for WAT friends) indexed by the order of their appearance: drawer = W_0, lender = W_1, ..., current recipient = W_n.
- Probability of W_i's failing to redeem is p_i.
- To simplify arguments, time is not evenly distributed in this model; W_i uses the ticket at time i. Redemption takes place at time r.
- Cost to rebuild trust relationships (including *whitewashing* the identity) for W_i is CT_i. It is assumed that this cost does not vary in a large extent among participants, and is generally worth more than a value of a



* $V_r = V_1$ and $p_1 = 0$ if W_1 is the last user

Figure 4. Game tree for issuing a multiplication ticket

ticket. This assumption should be justified by the fact that the *i*-WAT trust model requires construction of a *web of trust*[12].

- No transactional cost or benefit is modeled. For example, it should be beneficial for the drawer W_0 if the lender W_1 accepts the ticket at time 0, even though W_0 has to redeem it at time r by the increased price V_r. But this benefit is not expressed in the model.

3.3 Analysis

Our analysis resulted in the following predictions.

Prediction 1 (Deferred Redemption) *If the lender W_1 accepts the ticket, they are likely to use it against the drawer W_0 themselves, and to defer it until the effective value reaches V_x.*

Prediction 2 (No Strategic Default) *The drawer W_0 is incentivized to successfully redeem the multiplication tickets they issue. The upper bound of V_x is CT_0.*

Prediction 3 (Acceptance Criterion) *The lender W_1 is likely to accept the ticket if $1 - \frac{V_0}{V_x} > p_0$. The drawer W_0 will try to increase the chance by keeping p_0 low.*

Prediction 4 (Ease of Flow) *If the lender W_1 is willing to take the risk, later participants W_n are likely to accept the ticket where n is sufficiently large.*

Figure 4 shows a game tree for issuing a *multiplication* ticket. The tree is read from left to right. There are two types of the drawer W_0: *successful* and *failing* to redeem. Inside parentheses are the gains of W_1 and W_0 in each combination of W_0's type and W_1's action.

3.3.1 Deferred Redemption

If W_0's type is *successful*, W_1 can maximize the gain by choosing the largest possible value for V_1, which is V_x. If W_0's type is *failing*, W_1 can minimize the loss to be V_0 by not forwarding the ticket to the third person. Therefore, to maximize the gain and to minimize the loss, W_1 chooses to wait until the effective value reaches V_x and tries to use it against W_0. In the discussions to follow, it is assumed that $V_1 = V_r = V_x$.

3.3.2 No Strategic Default

If $V_r \leq CT_0$, then there is no reason for W_0 to default. If $V_r > CT_0$ (thus $V_x > CT_0$), then W_1 knows that W_0 is likely to default. To prevent the loss of V_0, W_1 would not accept the ticket if $V_x > CT_0$. Therefore the upper bound for V_x of an acceptable ticket is CT_0.

A strategic default is still possible if there are more than one *multiplication* tickets W_0 have issued in circulation, and W_0 disappears and assumes a new identity (*accumulation attack*): CT_0 may be smaller than the sum of V_x's. Prevention of this is discussed briefly in section 5.

3.3.3 Acceptance Criterion

If W_1 chooses to accept a ticket, W_1's expectation is:

$$V_1 - V_0 - C_1 p_0$$

where V_1 and C_1 are both ultimately V_x given that $p_1 = 0$ (W_1 is the last user). W_1 chooses to accept the ticket if this value is greater than that of choosing to refuse it, which is zero. Therefore, the criterion is expressed in the following expression:

$$1 - \frac{V_0}{V_x} > p_0$$

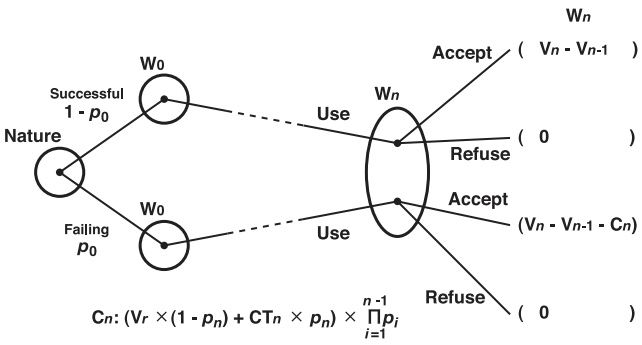
There are three variables: V_0, V_x and p_0, which W_0 can manipulate to increase the chance of acceptance. V_0 is decided by W_0's need, and V_x is bounded by CT_0. Therefore in actuality W_0 can only decrease p_0.

3.3.4 Ease of Flow

Figure 5 shows a game tree for circulating a *multiplication* ticket. Since $0 \leq p_i \leq 1$, $\prod_{i=1}^{n-1} p_i$ approaches zero as n increases, which makes the cost C_n negligible for W_n. Therefore W_n can choose to accept the ticket regardless of W_0's type if n is sufficiently large.

4 Implementation

We have been developing a reference implementation of *i*-WAT as a plug-in for *wija*, an XMPP (Extensible Messag-



* $V_r = V_n$ and $p_n = 0$ if W_n is the last one

Figure 5. Game tree for circulating a multiplication ticket

ing and Presence Protocol)[5][6] messaging client. The proposed MOT feature, as well as the formerly proposed ROT (Reduction Over Time) feature, have been implemented, and are included in the bundled plug-in for the latest version of *wija* which was released in April 2005.

wija is available at http://www.media-art-online.org/wija/.

5 Future Work

We have started experimenting on actual usage of MOT to verify our predictions, although we are still investigating how we can prepare a way for the drawers to signal their values of p_0 to the expected lenders.

Accumulation attacks can be prevented if the sum of the maximum values of all yet circulating *multiplication* tickets issued by the same drawer is known to all expected lenders. If the sum is greater than CT_0 then there is a possibility of the attack. Although there are privacy issues, we can operate the system in such a way that information on issued tickets is shared among community members.

Another consideration is, if a person is really in such a strong need, issuing necessary amount of *reduction* tickets may be a better solution as it requires no subjective cost of lying and deceiving people.

6 Conclusions

This paper proposed an extension to the design of *i*-WAT to implement MOT (Multiplication Over Time), which can help participants in peer-to-peer systems who are in strong need of some specific resources.

The extended design is shown to be incentive-compatible by a game-theoretical analysis. An implementation is available to the public, using which experiments are ongoing.

References

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

[2] T. Bray, J. Paoli, C.M.Sperberg-McQueen, and E. Maler. *Extensible Markup Language (XML) 1.0 (Second Edition)*, October 2000. W3C Recommendation. Available electronically at http://www.w3.org/TR/REC-xml.

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

[4] A. Dahlberg. *When Capital Goes On Strike*. Harper & Brothers Publishers, 1938.

[5] P. S.-A. (Ed). *Extensible Messaging and Presence Protocol (XMPP): Core*, October 2004. RFC 3920.

[6] P. S.-A. (Ed). *Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence*, November 2004. RFC 3921.

[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] S. Gesell. *The Natural Economic Order*. The Free Economy Publishing Co., 1934. Translated from the sixth German edition (originally published in 1913). Also available as a hypertext document in English, translated by Phillip Pye, at http://www.systemfehler.de/en/neo/.

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

[10] Maebashi Artists Association. MAAS (Maebashi Artists ASsociation). Hypertext document. Available electronically at http://www.watsystems.net/users/maassite/.

[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. In *IEICE TRANSACTIONS on Communication*. The Institute of Electronics, Information and Communication Engineers, April 2005.

[13] K. Saito, E. Morino, and J. Murai. Reduction over time: Easing the burden of peer-to-peer barter relationships to facilitate mutual help. In *Proceedings of the Second International Workshop on Computer Supported Activity Coordination (CSAC 2005)*, May 2005 (to appear).

[14] 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)*.

[15] 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.

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