Trading in Trust, Tokens, and Stamps

Tim Moreton and Andrew Twigg
Computer Laboratory, Cambridge University, UK

E-mail: firstname.lastname@cl.cam.ac.uk

Abstract

Proposals for providing incentives to increase node participation in peer-to-peer systems can be broadly categorised into token-based and trust-based schemes. This paper aims to relate both models to a variant of stamp trading [6], where nodes produce personalised stamps then trade them to obtain service from each other. By combining features from both trust and token schemes, we present the first trust scheme which gives rise to a bounded-size trust economy and describe its implications for peer-to-peer routing.

1 Introduction

Peer-to-peer systems are typically made up of nodes that are run by individuals and organizations without an out-of-band trust relationship. In such circumstances, it is impossible to verify the validity of peers' software. Trace analysis of such systems [1], supported by game-theoretic modelling [4], has shown that participants will often *free-ride*, not providing resources when it is not in their interest to do so, but continuing to use the service, regardless of the system-wide degradation that results. Such public goods social-dilemmas are well-recognised in economic and political theory literature.

Several techniques have been proposed to increase participation in peer-to-peer systems, by detecting and excluding nodes that refuse to collaborate and by aligning the interests of nodes with those of the service as a whole. These approaches can be broadly categorised into *token-based* and *trust-based* models.

In the former, nodes receive payments for each contribution they make to the service, and in turn use the credit that they have accrued to access the service themselves. In the latter, a trust model transfers nodes' *reputations* measuring their degree of participation: agents grant or refuse each other's requests to use their service on this basis.

The contribution of this paper is to relate both models to the more general scheme of *stamp trading*, a variant of which was proposed by Levien and Dingledine [6], in which each node generates personalised *stamps*. A stamp from a node represents a 'promise' on its behalf to provide a unit of service; nodes trade stamps to obtain service from each other. By varying stamp exchange rates, we show how stamp trading schemes can implement both token and trust schemes. Further, we outline how stamp trading schemes induce economies that relate the production and consumption by nodes in the system.

2 Modelling Incentives

In peer-to-peer applications, each node provides some part of the system-wide service; nodes using this service do so only by interacting with each other. Providing sufficient incentives by limiting or denying service will encourage many free-riders to collaborate as they judge that the service's value outweighs the resource cost necessary to host their portion. Since a peer's requests tend to be scattered across many nodes, a scheme that enforces such service restriction requires that we distribute evidence of participation – either positive or negative – by which nodes can judge others' contributions before offering them services.

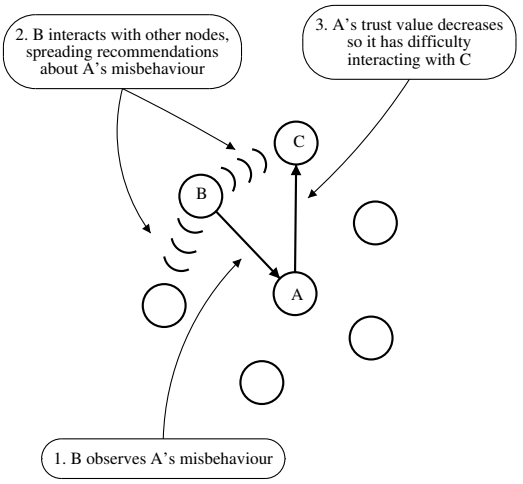

Figure 1. Trust scheme

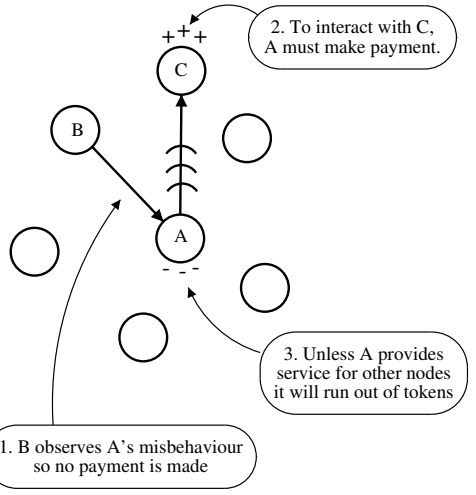

Figure 2. Token scheme

2.1 Trust and Payment Schemes

The key distinctions between trust and payment schemes centre around this dissemination of evidence. In token schemes, nodes must obtain payments from interactions that they have completed succesfully on other nodes' behalfs; this limits the rate at which a node may make requests to others.

On the other hand, the aim of a trust model is not to constrain individuals' usage to their contribution, but rather to observe a node's behaviour (*i.e.* how faithfully it carries out services asked of it) and allow or deny use on that basis.

Trust schemes deal in the dissemination of *reputation* information, according to the success of the interaction. A node's trust is not managed by the node itself: others pass *recommendations* about it, either to nodes who locally compute their own trust values, or to a central trust service. In payment schemes, nodes directly receive tokens which they can use for payment elsewhere.

Incentives in trust schemes. If a node has a low trust value then nodes following the trust protocol will exclude them from the network by not answering their requests. In a similar way, nodes with high trust values will have their requests answered by trustworthy nodes. Figure 1 illustrates this.

Incentives in token schemes. Nodes receive tokens only by successfully completing operations for other nodes. Those that do not offer such services cannot gain the credit that they need to use services themselves. In variable pricing schemes, nodes have incentives to offer the portions of the global service for which there is most demand. Figure 2 illustrates this.

2.2 An Example Trust Scheme

In [8] we present a distributed trust model aimed at enforcing collaboration in the Kademlia [7] routing substrate. Trust values are based on direct observations made by each node about others' returning accurate routing information. Nodes pass recommendations, piggybacked onto routing request replies.

To simplify the presentation, we consider a centralized *sage* that observes each interaction and maintains accurate trust values for each node. Instead of performing local computations to obtain trust values, nodes obtain them from the sage. One can consider recommendations as computing distributed local *approximations* to the sage's trust values.

2.3 Variable Demand and Pricing

In some price-based schemes, agents may set their own prices for providing services. As in

conventional economies, market incentives are intended to dynamically provision for a variable demand for the services provided by different nodes.

Crowcroft et al. [3] propose a scheme to provide incentives for nodes to forward packets for other nodes in mobile ad hoc networks. The system goal is to form the necessary network infrastructure so that transmission energy used in routing is minimized. Each node has two internal resources, battery power and capacity, and a cost asscoiated with each. Nodes experience a variable demand for routing, depending on their location, and set prices based on their internal cost.

In some applications, though, variable demand is inappropriate. DHTs assign nodes and data pseudo-random identifiers, so requests made by each node are evenly distributed. Under variable pricing, nodes attempting to minimise their cost will take less direct paths to that part of the keyspace, contrary to such systems' aims.

2.4 Fair Exchange

Since nodes associate a cost with the internal resources they expend in carrying out a service, a rational node might accept payment for a request and simply not complete it. Although there exist 'fair exchange' schemes to agree on such outcomes [2], they are expensive both computationally and in numbers of interactions.

Further, the nature of many services may prevent nodes from determining exactly whether a service has been (or will be) fulfilled at point of request. One example is distributed storage systems, where a contract to store a block should last much longer than the period of the interaction.

Payment schemes may be complemented by trust models which can penalise nodes by their observed behaviours. The NICE platform [5] advocates setting the price and size of data storage contracts according to an inferred trust value.

3 A General Scheme: Stamp Trading

In the stamp trading scheme (Figure 3), nodes issue *stamps* to their neighbours[1] which can later

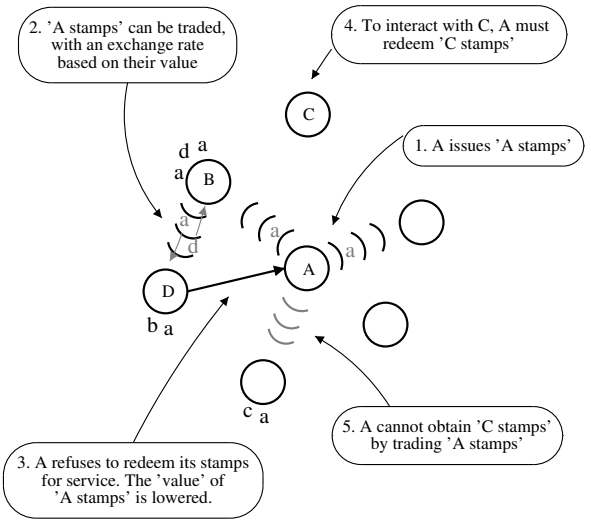

Figure 3. Stamp trading scheme

be *redeemed* at the issuing node for service[2].

A node's global trust value is determined by the value of its stamps; the basic idea being that if a node fails to redeem its stamps then the value of its stamps is reduced via a centralized exchange rate mechanism. The node will then have difficulty obtaining other stamps with any value, since few nodes wish to trade *its* stamps. A simple distributed alternative to the exchange rate mechanism is to have the current value 'written' onto the stamp when it is issued.

Stamp trading is closely-related to reputation schemes since nodes there is no enforcement of one-to-one 'consuming-providing' of resources; rather, as long as a node's stamps have sufficient value, it can obtain stamps for other resources.

Incentives. In order to obtain service, nodes need to present stamps, obtained by trading. A node can trade either its own stamps or those it has 'on hand'. By relating the exchange rate of stamps to their issuers' behaviour (in redeeming them), it is in a node's interest to get into a position where it is able to obtain sufficient stamps to do what it wants.

On the downside, stamp trading schemes suffer from a number of practical problems, in particu-

[1] In Kademlia, a node's neighbours are those nodes in its routing table

[2] Though there is no limit on the number of stamps that a node may issue

lar the high overheads of cryptographically signing stamps and maintaining their audit trails, and the latency of obtaining stamps (there is no obvious chain of exchanges for a node to follow, in order to obtain the desired stamps), which is a major restriction to its use in a multi-hop routing service.

3.1 Linking the schemes

We now present our main argument: that stamp trading is a natural generalization of trust and token schemes – it has both a trust and token flavour, in that a node trusts that a stamp will be redeemed, and when a node receives a stamp it issued, this can be thought of as a payment equal to that stamp's value. We first present some terminology.

We say that a stamp trading scheme is *token-compatible* if the total value of stamps in circulation in the network is bounded. This fits our notion of a token scheme, where tokens cannot be forged or minted, and so is closed. We say that a stamp trading scheme is *trust-compatible* if failure by a node to successfully redeem a stamp never increases its stamps' values, *i.e.* stamp value is monotone decreasing with increasing number of failures. This fits our notion of a trust scheme, where nodes cannot gain 'trustworthiness' by misbehaving. An economy emerges from a stamp trading scheme, with many interesting properties such as liquidity and stability, whose investigation remains as further work.

Let us denote the set of stamp trading, trust and token schemes by Stamp, Trust and Token respectively, and we assume there are n nodes in the network, each having three values: i, the total number of stamps issued, r_s, the total number of stamps successfully redeemed, and r_t, the total number of that node's stamps that is has been asked to redeem (so $r_s \leq r_t$). We present some simple stamp trading schemes based on trust and token schemes, then describe two stamp trading schemes which naturally arise as the *intersection of trust and token schemes.*

Theorem 1 *Trust* $\subseteq$ *Stamp,* i.e. *Each trust scheme has an equivalent trust-compatible stamp trading scheme.*

Rather than attempting to prove the general result above, we attempt to justify our intuition by showing how a simple trust scheme can be formulated as a stamp trading scheme. In this case, the stamp value is determined by the proportion of times that a node successfully redeems its stamp, and so represents the trust scheme in [8].

Participation Value (PV). The value of a stamp is r_s/r_t, hence the economy arising from PV is unbounded in size since the total value of stamps in circulation is unbounded. We can view the 'amount of trust in a node' as the total value of its stamps in circulation. If this is unbounded, it means that a node can obtain an unbounded amount of service (*e.g.* in [8], obtaining replies in Kademlia) by 'injecting' trust into the network.

Theorem 2 *Token* $\subseteq$ *Stamp,* i.e. *Each token scheme has an equivalent token-compatible stamp trading scheme.*

Again we attempt to justify our intuition by presenting a simple token scheme as a token-compatible stamp trading scheme.

Fixed Circulation (FC). The value of a stamp is $1/(i - r_t)$, where $i - r_t$ is the number of stamps a node has in circulation. The total value of stamps in circulation at any time is bounded by n, the number of nodes currently in the network. This corresponds to each node having unit credit.

If there is no centralized exchange rate mechanism, we can consider distributed approximation schemes with the aim of approximating the total value of a node's stamps in circulation. One scheme is to mark each stamp with a fixed value when issued, based only on local information. If a stamp is given value $2^{-(i-r_t-1)}$ when issued[3], then the total value of stamps in circulation is $n\sum_{k=0}^{i} 2^{-k} \leq 2n$, and we say this is a 2-approximation scheme to FC.

Nex, e give a stamp trading scheme which arises naturally from trust and token schemes, and represents a natural derivation of Levien's original scheme [6] (which we refer to as Redemption Rate,

[3]So stamps' values decrease exponentially as they are issued but not redeemed–this can be calculated by other nodes, using local information about the issuing node

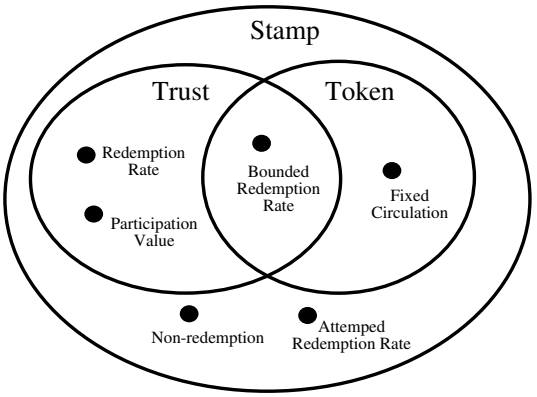

Figure 4. The various metrics and schemes

RR). Our scheme below is similar, though modified so that the total value of stamps in circulation is bounded.

Bounded Redemption Rate (BRR). The value of a stamp is r_s/i^2, so the maximum value of each stamp is $1/i$, and the total value of a node's stamps in circulation is given by $(i - r_t) \cdot \frac{r_s}{i^2} = \frac{r_s}{i} \cdot (1 - \frac{r_t}{i})$. Therefore, a node obtains maximum value of its stamps in circulation when it sets $i = 2r_t$, having the same number of stamps in circulation as have been returned to it. The total value of stamps in circulation is $\frac{1}{4}\sum_{i=1}^{n} r_s/r_t \leq n/4$, since a node cannot successfully redeem more than stamps than asked to. This maximum value for a node is obtained, regardless of nodes' behaviour in redeeming stamps, r_s.

BRR $\in$ Trust since the value of a stamp clearly never increases if it is not successfully redeemed, and BRR $\in$ Token since it provides a trust economy of bounded size (unlike RR). What this means is that, in the context of [8], rather than each request having a constant probability of succeeding (as for PV), BRR bounds the probability that an *unbounded* number of requests will succeed in obtaining a single reply, so avoids packet-flooding of requests. Furthermore, newly-joined nodes only worsen their low initial trust value by flooding requests. An interesting area for further work is modelling the rates in this scheme using queuing theory.

Finally, we present two theorems which represent answers to interesting questions which arose in writing this paper, and provide in Figure 4 an attempt to classify the schemes discussed, taking into account the various theorems.

Theorem 3 *Trust* $\cap$ *Token* $\neq \emptyset$

There is a trust- and token-compatible scheme – BRR, which provides a bounded trust economy.

Theorem 4 *Stamp* $\supset$ *(Trust* $\cup$ *Token)*

That is, the set of trust- and token-compatible schemes does not exactly cover the set of stamp trading schemes. A simple counter-example is a scheme which rewards nodes for poor behaviour, such as $(r_t - r_s)$ (Non-redemption, NR) or even a version of RR which ignores successful redemptions, such as r_t/i (Attempted Redemption Rate, ARR). Both are in Stamp but are neither trust- nor token-compatible.

4 Conclusion

We have argued that trust and token schemes are essentially the same, and provided equivalent schemes based on stamp trading schemes. We also presented the first scheme combining features of trust and token schemes to provide a bounded trust economy, with some promise for use in peer-to-peer networks such as Kademlia.

References

[1] E. Adar and B. Huberman. Free riding on gnutella.

[2] N. Asokan, V. Shoup, and M. Waidner. Asynchronous protocols for optimistic fair exchange. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 86–99, 1998.

[3] J. Crowcroft, R. Gibbens, F. Kelly, and S. string. Modelling incentives for collaboration in mobile ad hoc networks. In *Proceedings WiOpt'03*, 2003.

[4] P. Golle, K. Leyton-Brown, I. Mironov, and M. Lillibridge. Incentives for sharing in peer-to-peer networks. *Lecture Notes in Computer Science*, 2232.

[5] S. Lee, R. Sherwood, and B. Bhattacharjee. Cooperative peer groups in nice. In *In Proc. IEEE Infocom.*

[6] R. Levien. Stamp trading networks. Available at www.levien.com/thesis, 2001.

[7] P. Maymounkov and D. Mazieres. Kademlia: A peer-to-peer information system based on the xor metric, 2002.

[8] T. Moreton and A. Twigg. Enforcing collaboration in peer-to-peer routing services. In *Proc 1st International Conference on Trust Management.*