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

Many peer-to-peer networks rely on cooperation between nodes. Reputation and payment protocols are two methods of introducing incentives to participate in systems such as Mojo Nation [10] and Free Haven [3]. We are interested in the relationship between reputation and payment protocols, in particular the types and properties of the economies and incentives they induce. Our work reveals some interesting parallels. It turns out that both types of protocol induce similar incentive schemes, in that there exists a more general protocol – stamp trading – which captures the essence of both. Our analysis and results have implications for many peer-to-peer systems including spam-resistant networks, file-sharing and routing.

1 Introduction

A major problem in current peer-to-peer systems is the mutual distrust between peers. Internet-scale systems contain many pseudonymous entities (nodes), which are running under multiple administrative domains, and by agents without an out-of-band trust relationship. This often gives rise to the problem of free-riding, where nodes make use of the resources provided by the service without participating and contributing themselves. Free-riding is such a significant problem for peer-to-peer networks such as Gnutella [1, 5] that they have been predicted to collapse 'under their own weight'.

In this paper, we are interested in two main ways of providing incentives to nodes in peer-to-peer networks – reputation and payment protocols – and how they relate to one another, in particular in the economies they induce. A reputation protocol operates by nodes granting service to other nodes based on their reputation within the network, and a payment protocol operates by having the requesting node make a payment to the node providing the service. In a simple sense, the former deals in the transfer of reputation whilst the latter deals in the the transfer of tokens.

We show similarities between the nature of the incentives provided by schemes from both types of protocol and introduce a more general protocol known as stamp trading, an early variant of which was proposed by Levien [6]. We show that stamp trading protocols capture the essence of both reputation and payment protocols, and demonstrate that a number of well-known examples including Mojo Nation and Free Haven can be easily expressed as stamp trading schemes. We are able to formulate new schemes which provide a number of desirable properties, and describe their implications for peer-to-peer routing protocols such as Kademlia [7].

2 Modelling Incentives

In peer-to-peer systems, 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.

2.1 Reputation and Payment Protocols

The notions of reputation and payment protocols refer to how this evidence is disseminated within the network. Payment protocols operate using a form of currency or token, whereby nodes obtain payments from interactions that they have completed successfully, and use these tokens for payment elsewhere – this limits the rate at which a node may make requests to others, since nodes cannot mint arbitrary amounts of currency.

On the other hand, a reputation protocol allows the provider of a service to accept requests based on the requesting node's 'reputation' within the network. A node's reputation is not managed by the node itself; others circulate *recommendations* about the node to establish its trust value. Hence reputation protocols deal in the dissemination of reputation information.

Incentives in reputation protocols. Nodes with low reputation will find it difficult to obtain service in the network. In general, a reputation protocol should ensure that nodes need to successfully contribute to the network in order to have a high reputation, hence providing suitably strong incentives for nodes. Figure 1 illustrates this.

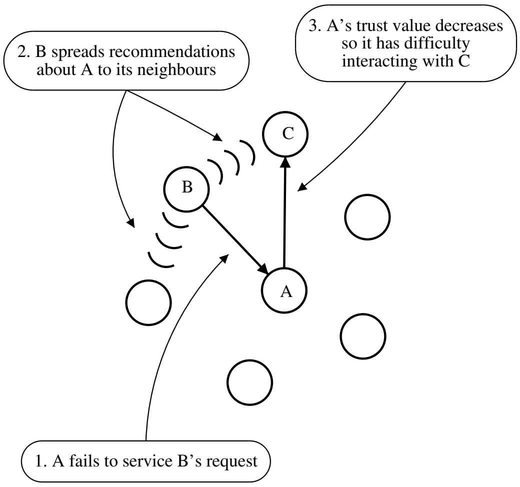
2. B spreads recommendations about A to its neighbours
3. A's trust value decreases so it has difficulty interacting with C
C
B
A
1. A fails to service B's request

Figure 1. Reputation protocol

Incentives in payment protocols. Nodes receive tokens only by successfully providing service for other nodes. Those that do not perform such services cannot gain the credit that they need to use the services themselves. In variable pricing schemes (where nodes may demand several tokens for an interaction), nodes have incentives to offer the portions of the global service for which there is most excess demand. Figure 2 illustrates how these incentives arise in payment protocols.

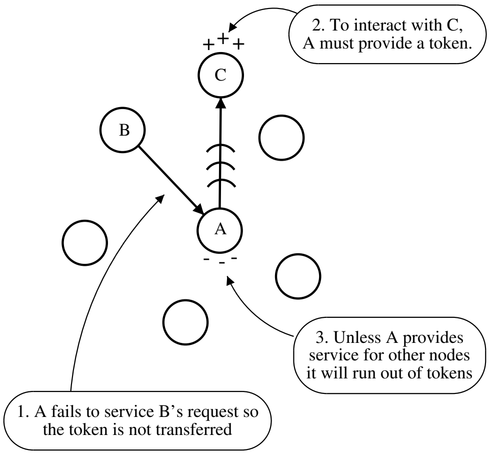
2. To interact with C, A must provide a token.
+++
C
B
A
- - -
3. Unless A provides service for other nodes it will run out of tokens
1. A fails to service B's request so the token is not transferred

Figure 2. Payment protocol

In order to motivate our work, we consider a number of reputation and payment procotols which will serve as examples. As example reputation protocols, we consider the simplified trust model in [8] which aims to enforce collaboration in the Kademlia [7] DHT routing substrate. As a more complex example, we consider the Free Haven [3] reputation protocol.

Mojo Nation [10] was one of the earliest peer-to-peer systems to use a payment protocol (although it required a centralized trusted third party to resolve double-spending issues). As an example of a variable-demand payment protocol, we use the model of Crowcroft et al. [2], which provides incentives for nodes to forward traffic 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 associated with each. Nodes

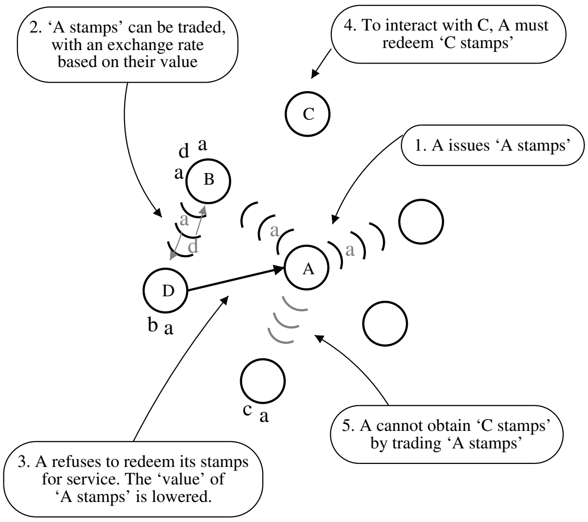
2. 'A stamps' can be traded, with an exchange rate based on their value
4. To interact with C, A must redeem 'C stamps'
C
1. A issues 'A stamps'
d a
a
B
a
d
a
a
A
D
b a
c a
5. A cannot obtain 'C stamps' by trading 'A stamps'
3. A refuses to redeem its stamps for service. The 'value' of 'A stamps' is lowered.

Figure 3. Stamp trading protocol

experience a variable demand for routing, depending on their location, and set prices based on their internal cost.

3 Stamp Trading Protocols

In the stamp trading protocol (Figure 3), nodes issue or trade personalised *stamps* with their neighbours[1] which can later be *redeemed* at the issuing node for service. There is no limit to the number of stamps that a node may issue (other than that imposed by bandwidth and processing requirements), and stamps can be traded between nodes.

Trading of stamps is dependent on their *value*, which we initially assume to be controlled by a centralized exchange rate mechanism which can observe all interactions between nodes, and hence provide perfect valuations. The value of a node's stamps is key to its ability to use the network. If its stamps devalue it will have difficulty obtaining other stamps with any value, as rational nodes will not wish to purchase its stamps. Stamp trading is closely related to trust schemes since 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 others' services.

Incentives. In order to obtain service, nodes need to present stamps originally issued by that node. A node can trade either its own stamps or those it has received from other nodes. By relating the exchange rate of stamps to their issuers' behaviour, 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. The exact nature of the incentives arises in the method used to determine the stamp exchange rates.

3.1 Generalising Reputations and Payments

We now present our main argument: that stamp trading is a natural generalization of reputation and payment protocols – it has both a reputation and payment flavour, in that a node trusts that a stamp will be redeemed (and a node's reputation is the aggregation of these trust values), and when a node receives a stamp (issued by another node or by redemption of its own stamps), this can be thought of as a payment equal to that stamp's value. To make this more precise, we first present some terminology.

A stamp trading *scheme* is a stamp trading protocol along with a method for valuing the stamps. The stamps that a node has in circulation represent the amount of service it has 'committed to'. We say that a node's *credit* is the total value of stamps it has *on hand* (stamps not issued by itself) plus the total value of stamps that it has yet to issue. Because nodes can give stamps away to neighbouring nodes, the total credit in the network equals the total value of stamps in circulation (stamps issued by a node are held on hand by others in the network).

We say that a scheme is *token-compatible* if the total credit (value of stamps in circulation) in the network is bounded. This fits our notion of a payment protocol, where tokens cannot be forged or minted, and so the economy is bounded. We say that a scheme is *trust-compatible* if failure by a node to successfully redeem a stamp never increases its credit, *i.e.* stamp value is monotone de-

[1] We do not assume the existence of a manually-configured trust graph, in contrast to Levien [6]; *e.g.* in Kademlia, a node's neighbours are those nodes in its routing table

creasing with increasing number of failures. This fits our notion of a (non-trivial) reputation protocol, where nodes cannot gain 'trustworthiness' by misbehaving.

Let us denote the set of stamp trading and trust- and token-compatible schemes by Stamp, Trust and Token respectively, and 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 by that node, and r_t, the total number of that node's stamps that have been presented for redemption (so $r_s \leq r_t$).[2] We now describe how schemes based on reputation and payment protocols give rise to simple stamp trading schemes.

Theorem 1 Trust $\subseteq$ Stamp*, i.e. Each trust-compatible scheme (whether implemented via a reputation or payment protocol) has an equivalent trust-compatible stamp trading scheme.*

Rather than attempting to prove the general result above, we justify our intuition by showing how the theorem holds for the Kademlia trust protocol [8].

Participation Value (PV). This trust-compatible stamp-trading scheme represents the Kademlia trust protocol in [8]. The value of a stamp is $(r_s + 1)/(r_t + 1)$ and represents the probability that it will be successfully redeemed by its issuer. The total value of stamps in circulation is unbounded, hence we say that the economy induced by this scheme is also unbounded in size. Since one can view the global trust value or 'reputation' of a node as its credit, PV corresponds to a trust economy where nodes can 'mint' arbitrarily large amounts of trust. In the context of Kademlia [8], if a node's stamps have value v (corresponding to its trust value) then it need send out $1/v$ requests to receive a single reply, on average. Hence nodes with high bandwidth are relatively unaffected by application of this scheme.

Redemption Rate (RR). The value of a stamp is given by $(r_s + 1)/i$, which represents the proportion of stamps issued which have been successfully redeemed. Without an exchange protocol, stamps are lost when presented for redmeption, therefore the total value of a node's stamps in circulation is given by $(i - r_t) \cdot \frac{r_s+1}{i} = (r_s + 1) \cdot (1 - \frac{r_t}{i}) \leq r_s + 1$. It turns out that this maximum value is obtained by flooding the network with stamps, since

$$\lim_{m \to \infty} m \cdot \frac{r_s + 1}{i + m} = r_s + 1.$$

i.e. this limit describes a node's credit when flooding the network with its stamps, irrespective of its previous behaviour. RR $\in$ Trust, since stamp values never increase if a stamp is not successfully redeemed, and RR $\in$ Token since the circulation value is still 'bounded' by the number of successful redemptions (and so does not allow 'minting' of arbitrary credit). This leads to the property that non-pseudospoofing is a weak Nash equilibrium, *i.e.* an agent cannot control any more circulation value by using multiple nodes than by using a single node.

Since Free Haven (FH) forces nodes to donate an equal amount of resources as they consume, and does not rely on an exchange protocol, RR is an equivalent stamp-trading scheme to FH.

Theorem 2 Token $\subseteq$ Stamp*, i.e. Each token-compatible scheme (whether implemented via a reputation or payment protocol) 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) (without exchange). 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 exactly equal to n, the number of nodes currently in the network. FC represents an economy of constant size, corresponding to each node having unit credit. Hence it is equivalent to the example payment protocol scheme with no exchange protocol since nodes lose stamps they present for redemption, regardless of the outcome.

Fixed Circulation (FCex) (with rational exchange). Consider the scheme FC with an exchange protocol, such that if a stamp is not redeemed, neither party has control of it, *i.e.* it is destroyed. The

[2] It will be obvious which node these values refer to

number of stamps that a node has in circulation remains $i - r_t$ but the stamp value is now $1/(i - r_s)$. Hence the total credit in the network is bounded from above by n (rather than a constant). In addition, FCex $\in$ Trust since failure to successfully redeem a stamp causes the value of a node's stamps to strictly decrease. Therefore, combining FC with a rational exchange protocol for exchanging tokens gives a trust- and token-compatible stamp trading scheme. This is equivalent to Mojo Nation (MJ).

Since both RR and MJ favour nodes with a higher bandwidth[3], the next scheme aims to remove this bias and bound the circulation value in the network, regardless of nodes' abilities to issue stamps.

Bounded Redemption Rate (BRR). The value of a stamp is $\left(\frac{2(r_s+1)}{i}\right)^2$, so the maximum value of each stamp is ≤ 4, and the total value of a node's stamps in circulation is given by $4(i - r_t) \cdot \left(\frac{r_s+1}{i}\right)^2 = 4\frac{(r_s+1)^2}{i} \cdot (1 - \frac{r_t}{i})$. Flooding the network with stamps causes a node's credit to approach zero, as described by the limit

$$\lim_{m\to\infty} 4m \cdot \left(\frac{r_s+1}{i+m}\right)^2 = \lim_{m\to\infty} \frac{(r_s+1)^2}{i^2/m + 2i + m} = 0.$$

hence BRR resists flooding attacks by providing a strong incentive for rational nodes (which aim to maximize their credit) not to flood the network with their stamps.

It turns out that a node obtains maximum circulation value when it ensures that $i = 2r_t$, *i.e.* having the same number of stamps in circulation as have been presented for redemption (hence a node's maximum value is obtained regardless of whether the stamps are actually redeemed successfully or not). The size of the economy is thus bounded from above by

$$\begin{aligned} \frac{2n\,(r_s+1)^2}{r_t} \cdot \left(1 - \frac{r_t}{2r_t}\right) &= n \cdot \frac{(r_s+1)^2}{r_t} \\ &\leq n \cdot \left(r_s + O\left(\frac{1}{r_t}\right)\right) \end{aligned}$$

which asymptotically approaches that of RR, and so resists pseudospoofing as long as the cost of creating the pseudonym is $\Omega(1/r_t)$ where r_t is the number of stamps presented for redemption at that particular pseudonym. Hence BRR will resist pseudospoofing in practice.

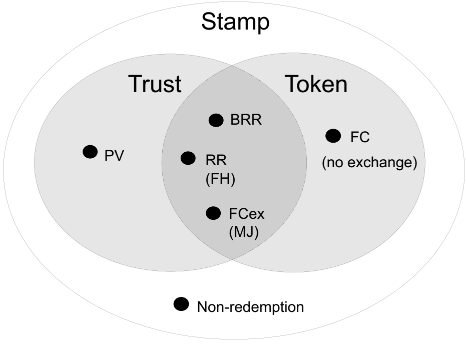

Figure 4. A simple classification of stamp trading schemes

Like RR, BRR is both trust- and token-compatible. However, BRR goes beyond RR by removing the bias towards nodes which can flood the network with stamps. BRR has interesting implications for applications such as spam-resistant networks, file-sharing and routing. As an example, in Kademlia [7, 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 avoiding packet-flooding of requests. Furthermore, newly-joined nodes only worsen their low initial reputation by flooding the network with requests.

Finally, we present two theorems which answer interesting questions which arose in writing this paper, and provide in Figure 4 an attempt to classify the schemes discussed.

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

Proof. There do exist trust- and token-compatible schemes, *e.g.* MJ, RR and BRR. □

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

Proof. That is, stamp trading is strictly more general than trust- and token-compatibility. Simple counter-examples are schemes which reward poor behaviour such as $(r_t - r_s)$ (Non-redemption, NR),

[3] Low-bandwidth Mojo Nation nodes often have to consolidate their limited resources to acquire sufficient Mojo

which is in Stamp but is neither trust- nor token-compatible. □

4 Open Problems

Since we first discussed the ideas in this paper, a number of interesting problems have arisen, or been brought to our attention. Here are what we consider to be the the most important, or relevant.

Practical implementations. An implementation of a stamp-trading protocol would allow real-world analysis of its performance. Practical problems associated with stamp-trading networks include proving that a stamp was not successfully redeemed, handling double-spending and the overheads of cryptographically signing stamps and maintaining their audit trails (as in [4]).

In Figure 2, node B does not wish to give the token to A unless A actually provides service. Likewise, A will not provide the service unless it knows that B will give it a token in return. This *exchange problem* arises in stamp trading, to accurately estimate r_s and r_t. A rational exchange protocol ensures that a misbehaving party cannot gain any advantage, *e.g.* Syverson's protocol [9].

Properties of stamp-trading economies. We considered simple properties of stamp-trading economies such as size, but a more thorough economic analysis could include liquidity and stability, and how the economic properties of a scheme (*e.g.* bounded vs. constant-size) influence one's ability to approximate it.

Better quantification of attack-resistance. Although we have shown how RR and BRR are resistant to an attacker forging others' stamps, flooding the network with its own stamps and a node failing to redeem stamps, other attacks include failing to delete stamps after trading, and collusion to increase the stamp price of a partner.

5 Conclusion

Reputation and payment protocols are two methods of introducing incentives to participate in collaborative peer-to-peer systems such as Mojo Nation and Free Haven. We have shown that both protocols have a great deal in common, in two senses. Firstly, there exists a more general protocol – stamp trading – which captures the notions of trust- and token-compatibility. Secondly, there exist stamp trading schemes which combine desirable properties of both.

One interesting question is whether reputation is a indeed a currency. The best answer we can give is 'yes', in that it can be traded to induce an economy, but 'no', in that it is earned and lost rather than bought and sold. The stamp trading scheme BRR has a number of interesting implications for real peer-to-peer systems such as spam-resistant networks, file-sharing and routing. We are working to better understand the economic principles underlying stamp trading, and to apply the ideas to real peer-to-peer systems.

References

[1] E. Adar and B. Huberman. Free riding on Gnutella. Technical report, Xerox PARC, 2000.

[2] J. Crowcroft, R. Gibbens, F. Kelly, and S. Östring. Modelling incentives for collaboration in mobile ad hoc networks. In *Proc. WiOpt'03*.

[3] R. Dingledine, M. J. Freedman, and D. Molnar. The free haven project: Distributed anonymous storage service. *LNCS*, 2009, 2001.

[4] R. Dingledine and P. Syverson. Reliable MIX cascade networks through reputation. In *Proc. Financial Cryptography*, 2002.

[5] P. Golle, K. Leyton-Brown, I. Mironov, and M. Lillibridge. Incentives for sharing in peer-to-peer networks. *LNCS*, 2232, 2001.

[6] R. Levien. Attack-resistant trust metrics. *PhD Thesis*, www.levien.com/thesis/, 2001.

[7] P. Maymounkov and D. Mazieres. Kademlia: A peer-to-peer information system based on the xor metric. In *Proc. IPTPS'02*, 2002.

[8] T. Moreton and A. Twigg. Enforcing collaboration in peer-to-peer routing services. In *1st International Conference on Trust Management*, 2003.

[9] P. Syverson. Weakly secret bit commitment: Applications to lotteries and fair exchange. In *11th Computer Security Foundations Workshop*, 1998.

[10] B. Wilcox-O'Hearn. Experiences deploying a large-scale emergent network. In *Proc. IPTPS'02.*