Money as IOUs in Social Trust Networks &
A Proposal for a Decentralized Currency Network Protocol

Version 2
(Version 1 at http://www.practicalmetaphors.com/decentralizedcurrency_orig.pdf)

by Ryan Fugger
rafspam@yahoo.ca
April 18, 2004

I. Money as IOUs in Social Trust Networks

Money as IOUs

I can an IOU for payment, with three restrictions:

1. My IOU will only be accepted by my friends who trust me. I cannot pay strangers.
2. Each of my friends will only accept an IOU from me up to a certain amount, depending on how much each one trusts me (measured by how much credit each will offer me).
3. If my friends accept my IOU, they cannot use it as currency outside the circle of my trusted friends.

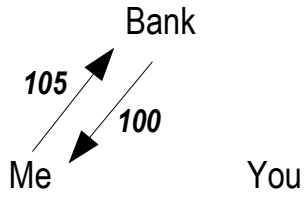
These are severe restrictions. But consider this:

- National currency notes are essentially IOUs from the government good for the payment of taxes.
- Everyone will accept a nearly unlimited amount of government IOUs, which, if we consider the government like a person, means we trust it a lot, since we give it nearly unlimited credit.
- A bank account is an IOU from a bank, a promise to redeem the account for a certain number of government IOUs on demand.
- A bank loan is an exchange of a personal IOU, the loan agreement which the bank accepts, for a bank IOU, at a fee. Loaning is the mechanism for the creation of bank IOUs.
- We need access to bank IOUs and government IOUs to pay each other, since we do not trust each other's IOUs.
- Government and bank IOUs are valuable because they are universally trusted.

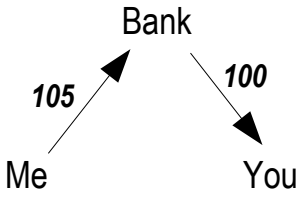
So if I want to pay you, instead of giving you my IOU, I give you government IOUs (cash) or a bank IOU (via cheque). Well over 90% of the money supply is bank IOUs, which are created out of thin air when a bank vouches for someone's personal IOU (i.e., when it gives them a loan).

Trusted Intermediaries: Banks and the Government

One way of thinking about this is that the bank, or the government in the case of cash payment, acts as a trusted intermediary in the payment. I give my IOU to the bank in exchange for its IOU, and I pay you with the bank IOU. These diagrams represent the situation, with arrows representing IOUs.



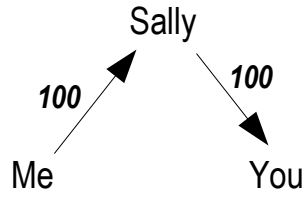
First, I've taken a loan of $100 out from the bank at 5% simple interest, meaning I owe back $105. (I may already have had some money in a bank account to pay you, but for over 90% of the money in circulation, someone had to do this initially to create that money.)



Next, I've passed the $100 in bank IOU to you in payment. Notice how I don't owe you anything, just the bank does. That's fine with the bank, because I owe it just as much (plus 5%), and it has decided to trust my IOU, because I have a good credit rating or offered them collateral.

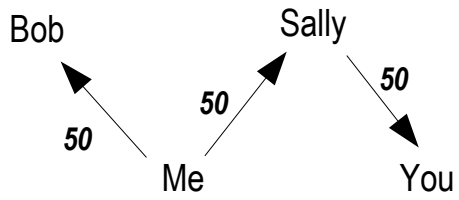
A Different Trusted Intermediary

Wouldn't it be nice to find someone other than the bank who trusted me, whom you trusted and who would be cheaper to deal with? If we spent some time talking about it, we might find a mutual friend, Sally, who could be a trusted intermediary for our transaction.



I've given Sally an IOU for $100 in exchange for her IOU, which I pass along to you. The problem is Sally's IOU isn't nearly as valuable as the bank's IOU, because you can only use it to pay people who trust Sally, as well people who owe her, such as me.

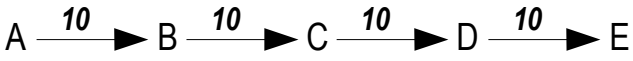
But if my IOU can be used to pay a stranger through a trusted intermediary, then Sally's IOU can too. Suppose you needed to pay Bob $50, and you discovered that Bob knew and trusted me. You could arrange to give Bob $50 of Sally's IOU, which he could give to me in exchange for my IOU, and I could settle $50 of my debt with Sally:



Notice how I still owe $100, and Sally is still even, but the arrows have rearranged since you paid half of your $100 balance to Bob, who gains a credit of $50.

You could pay anyone this way, as long as you could find a chain of trusted intermediaries connecting you to the payment's recipient, and as long as those intermediaries had enough available credit between them to make your payment.

In general, if everyone started at even, here's how A would pay $10 to E via trusted intermediaries B, C, and D:



In this arrangemtne, no one ever has to accept an IOU from anyone they don't trust. The problem is finding a chain of trusted intermediaries for each transaction...

II. A Proposal for a Decentralized Currency Network Protocol

To facilitate decentralized payment via non-bank and non-governmental intermediaries, we need to maintain a social network in which connections between parties are defined by granting credit. A computer will do the work of finding IOU payment paths through the network.

Here are questions that will need to be answered to define how payments occur over such a network, along with some of my tentative answers.

Questions

1. *Should the social network be maintained on a single server or distributed among several servers?*

It makes sense to store a system for decentralizing payment intermediaries in a decentralized fashion, among as many servers as wish to participate in the system. Thus the need for a protocol for servers to communicate. Servers might store only one account.

2. *Should there be one currency or many?*

There's no reason why many mutual credit networks in different denominations couldn't operate simulaneously on the same servers. Payments can only be made by finding credit paths in a single denomination, however. Currency exchange is possible by trading IOUs in one denomination for

IOUs of another.

3. *Should an account (node on a social network) be stored on and accessible exclusively from a single server, or could an account be a more nebulous entity, stored redundantly in the computer network of servers, and accessible from any given server? Or some mix of both approaches?*

For privacy and security, an account would likely have to be stored only one server, their "home" server. A server would be accessible from anywhere on the internet, regardless. And any server could implement its own data redundancy schemes internally.

4. *If accounts are stored on single servers only, should servers share information about how their internal nodes are connected, or could they communicate and work with each other blindly?*

For the sake of privacy, servers should probably share a minimum amount of account information with other servers. Servers might be able to interoperate by simply sharing the node IDs of the accounts which accounts they manage.

5. *If accounts are distributed redundantly throughout the computer network, how is data consistency maintained?*

6. *How would servers need to cooperate in finding payment paths in the social network?*

Two servers would each have full information on connections between their account nodes, including available credit each way. To make a payment between nodes on different servers, each would have to find a path or paths with sufficient available credit from the payment source/recipient to the other server, and then negotiate the process of matching up these paths.

To make a payment between accounts on servers with no connections between them, one or more intermediary servers must be enlisted.

7. *How secure is it?*

Public key encryption could be used for secure communication, and digital signatures for authentication. The payment protocols will have to be carefully thought out to prevent abuse, especially by intermediary servers. The fact that all credit is granted only between trusted private parties should be exploited to make abuse unlikely.

8. *How private?*

Presumably only the servers you use, those you trust as social network connections, and possibly anyone who pays you will be able to know who owns your account. Servers might allow anonymous accounts identified only by a node ID on the social network, and possibly also by nickname identifiers, much like email addresses: <node_nickname@server.com>.

9. *Should servers be allowed to charge for their services?*

Why not? However, the protocol should be if possible designed so that one or two servers are not motivated to attempt to monopolize all the accounts by not cooperating with other servers to provide payment intermediaries. Servers might decide to charge other servers (in whatever currency they wish) for access to their nodes for payment or as intermediaries, and the costs would be passed along to the user. However, this should hopefully be as fruitless as an email provider attempting to charge other servers for sending email to its users.

10. If each account is stored exclusively on one server, should it be able to be moved?

The protocol could include an XML or some other specification for account data so accounts could easily migrate from one server to another.

11. How could a merchant accept this type of payment?

The merchant could grant credit to a well-connected intermediary who might charge for the service (as a bank does), and then clients would have to find a path that connects through this intermediary to pay. A business could also grant unlimited credit to its owners, and payment would funnel through them.

Various technologies, such as smart cards, could be used, or new technologies invented to faciliate face-to-face payments.

12. What are the rules for gaining credit with another account?

There are no rules. Two users may come to any kind of credit arrangement, including charging interest, requiring collateral, or offering redemption of IOUs in government currency. Their credit agreement may be written, verbal, or implicit. At a minimum, the arrangement needs to specify the denomination of the credit. Usually credit limits will be specified at each end as well. The currency protocol could include specifications for a standard basic credit arrangement (denomination and credit limits) and and specifications for defining custom credit arrangements between nodes that might be on different servers.

Servers will no doubt provide client software that enables the formation of all sorts of credit agreements between nodes. Servers will be able to restrict what types of arrangements they will enable in software, but it will be difficult or impossible for servers to restrict what types of agreements two users may form on their own. However, enabling certain types of agreements in software could make the system more flexible and user-friendly.

One type of credit agreement that might be useful is a percentage fee for acting as an intermediary, charged by well-connected nodes, similar to an interest fee at a bank. If the payment protocols were aware of this type of arrangement, the extra charge could be automatically passed back to the original payer. Payers could instruct the network to attempt to avoid intermediary fees if desired, but the transaction may be slower.

Servers will likely expedite transactions routed through charging intermediaries for a cut. If a server A begins to refuse non-paying transactions outright, however, other servers might start refusing transactions from server A, reducing the usefulness of its charging intermediaries, and causing them to switch servers. If the problem got bad enough, some servers could refuse to process paying transactions entirely, effectively creating two separate currencies of the same denomination, one allowing paying transactions, and one requiring all transactions be free.

In any case, the protocol should be flexible enough allow each user and server to make independent decisions on ideological questions such as charging interest and fees. What will result no one can predict.

13. Will transactions be fast enough?

Hopefully. Enabling well-connected intermediaries to charge fees if they wish might help speed up transactions for those willing to pay, while hopefully not restricting free transactions for those willing to wait a little longer.

The longer, significantly different first version of this document is at http://www.practicalmetaphors.com/decentralizedcurrency_orig.pdf . It may explain some points better than this version.

Comments and suggestions are appreciated. Email Ryan Fugger, rafspam@yahoo.ca .