Money as IOUs in a Social Trust Network

and

A Proposal for a Secure, Private, Decentralized Digital Currency Protocol

by Ryan Fugger
rafspam@yahoo.ca

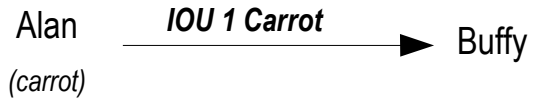
"If I had a million dollars, I'd buy your love."
- Barenaked Ladies

I. Money as IOUs in a Social Trust Network

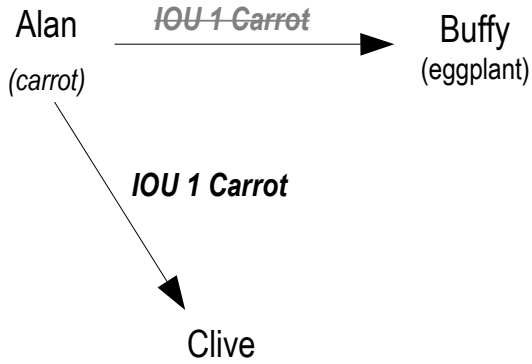
IOUs as Money

All human commerce takes place in more or less sophisticated systems of exchange whose beginnings lie in simple barter: Alan gives Buffy a turnip in exchange for a carrot. This is wonderful if Buffy actually wants turnip, but if she doesn't, Alan needs recourse to a more sophisticated system of exchange to get the carrot. He can write down the promise "IOU one carrot" on a piece of paper, sign it, and if she trusts him to fulfill his promise, she will let him have the carrot in exchange for his IOU. Now they are doing more than just bartering – they are keeping score.

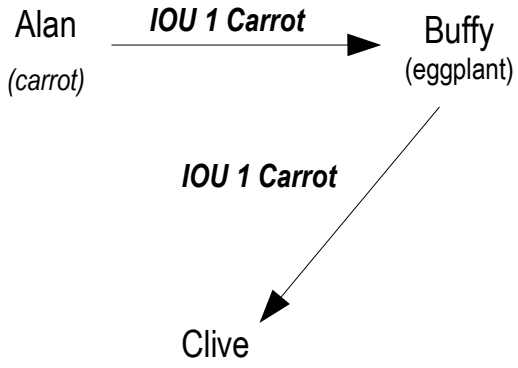
The following diagram describes the situation.



Buffy no longer has an extra carrot to barter, but Alan's IOU, which might be just as good. She might trade Alan's IOU to Clive in exchange for his eggplant, in which case the situation would look like this:



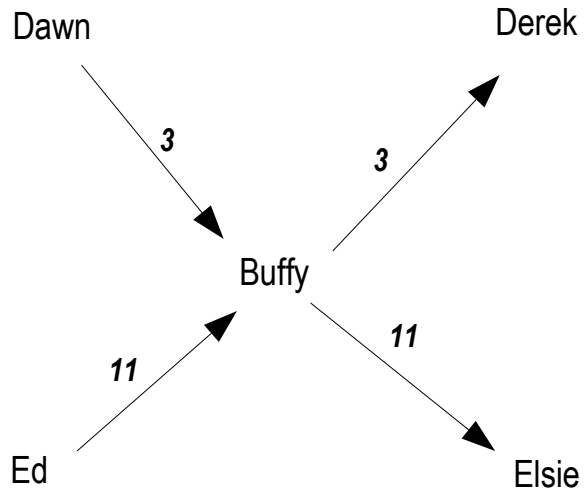
Buffy has used Alan's IOU as "money" to pay for Clive's eggplant. Clive will only accept this arrangement if he trusts Alan to live up to his promise of one carrot. If Clive was tempted by the promise of a carrot, but only trusted Buffy and not Alan, she could write him up her own IOU for one carrot, secure in her knowledge that Alan will come through with Clive's carrot.



The outcome is the same – Alan effectively owes one carrot to Clive, but now Buffy is acting as a trusted intermediary, meaning that if Alan reneges on his promise, she agrees to cough up the carrot out of her own stock.

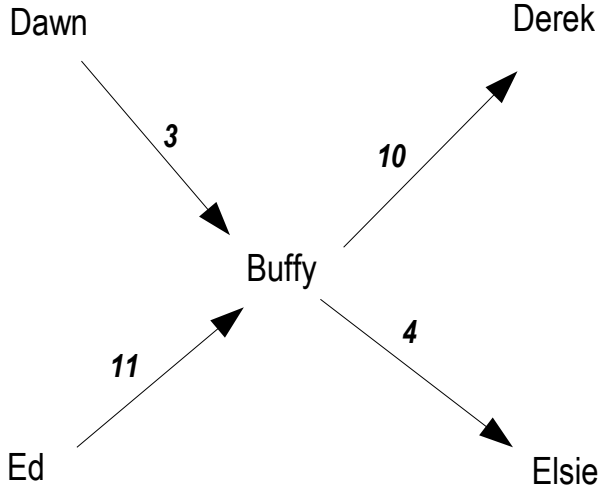
The Trusted Intermediary

If several people know and trust Buffy, they can use her as an intermediary in order to accept each other's IOUs without needing to actually know each other. (They can also use any standard of value they wish: dollars, ounces of gold, stones. They are not restricted to carrots...)



Despite the fact that she does not know or trust Derek, Dawn has managed to transcend simple bartering by exploiting Buffy's trust in her and Derek's trust in Buffy. Similarly, Ed and Elsie have exploited their common relationship with Buffy to enable a transaction that might have not been possible otherwise.

Since Elsie and Derek both trust Buffy, they can use Buffy's IOUs for keeping track of exchange between them, without needing to rely on mutual trust. If Elsie wanted to pay Derek 7 units for services rendered, she could sign over to him 7 of Buffy's IOUs. The graphical scorechart would then look like:

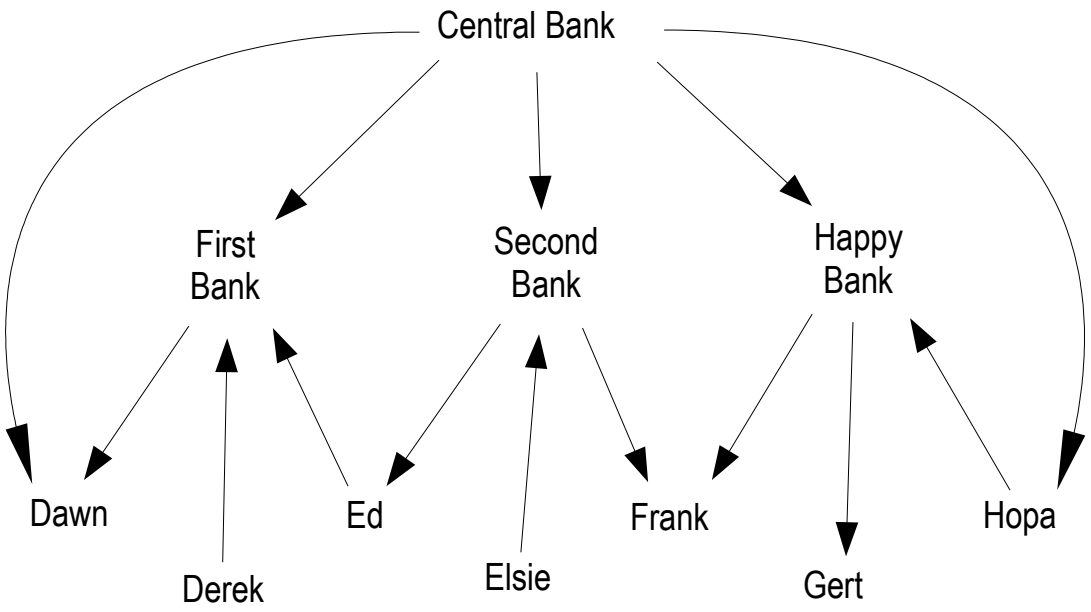


Notice that Buffy's ledger stays even, with 14 units owed to her, and 14 owing to others. The transaction between Elsie and Derek doesn't affect Dawn or Ed in the slightest, despite the fact that they are in a sense the source of and backing for Buffy's IOUs.

Banks

The fact that many people will accept Buffy's IOUs in payment makes them very useful. In our familiar monetary system, Buffy's role is played by a bank. In the diagram above, we would normally say that Buffy the Banker has loaned $3 and $11 to Dawn and Ed, respectively, and holds deposits of $10 for Derek and $4 for Elsie. Buffy may demand property as collateral for loaning out her valuable IOUs. Account holders exchange Buffy's IOUs by cheque, and Buffy keeps her accounts updated accordingly.

In reality, the modern banking system has much more to it than this. A very simplified version might look something like this:



Remember, in these diagrams, arrows represent IOUs. Arrows leaving the central bank represent cash in the form of national currency. Arrows leaving a private bank represent a deposit at that bank, and arrows going into a bank represent a loan granted by that bank.

Modern banking is complicated system that aims to allow everyone transacting business in the nation access to the IOUs of a single trusted authority, an agent of the government called the central bank, via a panoply of private banks. The central bank IOUs take the form of national currency. The private banks act as intermediaries between the public and the central bank, doing the dirty work of deciding how much credit to extend to any individual, and the central bank sets rules and props up well-behaving banks by providing them with currency when they need it to keep the system stable.

A Hierarchical System

Modern Banking is a hierarchical system resting entirely on people's trust in the government and its agent, the central bank. This is why the central bank works hard to stabilize the system: to maintain people's faith in their IOUs. Actually, faith in government currency is mainly centered around the fact that it is required to pay taxes, leaving people feeling confident that as long as there are taxes, there will be demand for government currency. But the central bank must work hard to balance the task of maintaining an adequate supply of its currency while at the same time avoiding inflation. This is a terribly complicated game, for many reasons, and it is not entirely clear that it is a game that any central bank can win in the long run under the current system. The Great Depression is an example of a spectacular failure of our type of monetary system.

Why must we have such a hierarchical system? Why must we all agree on the same trusted authority to issue our IOUs? Finding a new trusted intermediary to faciliate every transaction is tedious and costly, and so an agreement within the community to use the IOUs of a single, centralized authority saves everyone time and energy. However, in many ways, the costs involved in forming and maintaining trust relationships have simply shifted onto the banks' shoulders, but are still paid for by us all, through user fees and interest charges on loans.

In what follows, I propose that current technology allows for automation of the previously tedious and costly task of finding alternative trusted intermediaries. Such a system could work to stabilize the monetary system in the case of a potentially catastrophic loss of faith in the centralized authorities.

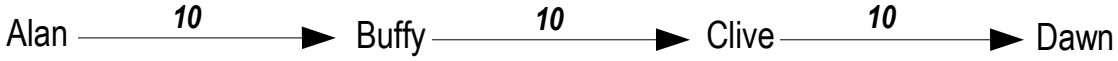
II. A Proposal for a Secure, Private, Decentralized Digital Currency Protocol

Using computer networks we can automate the process of finding trusted intermediaries for any transaction, and in the process build a more efficient and stable monetary system.

Decentralization

The risk of a centralized, hierarchical system is that it is vulnerable at the root. If trust in the government central bank wanes, the system fails. If the internet ran like our monetary system, every data communication would be dependent on the functioning of one central computer that supervised the whole network. If the central computer were to crash, the whole network would break down. The internet, however, was built to withstand a nuclear attack – any part of it can fail without paralyzing the rest. It accomplishes this by decentralizing authority in the system with a set of common protocols that allows networked computers to flexibly negotiate data transactions amongst themselves with no centralized supervision. A similar paradigm can be applied to the monetary system.

Imagine a large piece of paper with the name of every person (human or legal) written on it. Then every person is given the chance to draw lines connecting them to every person they trust, and to write a number next to the connection signifying the amount of money they would be comfortable lending that person. Payment between trusted parties is made by passing an IOU, up to the credit limit that the recipient has assigned to the payer. Payment between strangers is made by finding a sequence of trust connections that joins them, and daisy-chaining the passing of IOUs between trusted parties as in the following diagram:



Here, Alan pays Dawn 10 via Buffy and Clive. Alan now owes 10 to Buffy, who stays even by owing 10 to Clive, who further owes 10 to Dawn. Alan has found someone who will accept his IOUs, and Dawn receives IOUs from someone she trusts. Alan's overall account is at -10, Buffy's and Clive's are at zero, and Dawn is at +10. No one need accept an IOU from someone they haven't already decided to trust, or go beyond the level of trust they have assigned to anyone.

It is exactly the difficulty of finding Buffy and Clive to act as intermediaries that necessitates a centralized banking system. But when the whole graph of people and trust connections is stored in a computer network, that task becomes routine. What is required is a protocol to allow such path-finding to happen in a consistent way.

The analogy to computer networks is as follows: every person is like a node on the network, social trust is the basis for network connections, credit offered to a trusted connection is like available bandwidth, and passing IOUs is like transferring a stream of data, using some of the available bandwidth. This analogy is not perfect, however, since passing IOUs in one direction raises the credit available in the other direction, while passing data never increases the available bandwidth in the other direction.

Compatibility and Flexibility

This model of decentralized trust network currencies is completely compatible with the current banking system, as is shown in the modern banking diagram in Part I. Cash represents an IOU of the central bank, and holding cash is a trust connection to the central bank. Implicit in the system is that the central bank's credit with each individual is essentially unlimited, while the individual has no credit in the relationship. Depositing cash in a bank account amounts to accepting the bank as an intermediary in your relationship with the central bank. A bank loan is a trust connection with the bank where the bank grants the recipient credit at interest.

The decentralized model is also compatible with commodity-backed currencies. This just means that the central bank's IOUs can theoretically be cashed in for tangible assets, as opposed to just used for payment of taxes.

By drawing an IOU diagram of LETSystems or another complementary currency, we can see that it is compatible with the trust-network IOU model. However, all of these currencies (that I've seen) rely on a single trusted intermediary to accomplish all transactions. The terms of credit may vary, but they are still centralized models.

A decentralized currency protocol allows for replication, if desired, of existing currency structures, but in addition offers the capability of choosing alternative trusted intermediaries to enable transactions.

Protocol Requirements

The protocol must provide a set of consistent behaviours for each node. The vital behaviour for the feasibility of this system is that each node agree to accept incoming IOUs from trusted connections in exchange for passing an IOU to the next node down the transaction chain. This is analogous to the agreement by internet nodes to transmit data received from neighbouring nodes to other neighbouring nodes, regardless of the ultimate source or destination.

It is worth noting that different currencies would operate on their own separate networks: Each currency would have its own graph of people and trust connections. People might take part in several different currency networks, but they would never have to accept an incoming IOU of 10 of one currency and pass along 10 of another. Exchanging currencies is always possible, but involves a completely separate transaction on each currency network.

If two people wanted to set up mutual credit, but didn't want it used to relay others' transactions in “regular” currency, then they must use their own private currency, so their connection doesn't appear on the graph of regular currency connections. In fact, in a currency network such as the one I describe, allowing or disallowing “through” transactions defines a currency.

There is no reason why a payment must occur along a single path. One transaction might combine several paths, if there is insufficient bandwidth along one single path, or if no single path is found fast enough.

Negotiating Social Trust Connections

The protocol must allow flexibility in people's ability to negotiate trust connections as they see fit. This includes the ability to set and change limits on the credit granted to the other party at any time. Questions such as whether interest or fees will be charged, or collateral required, should remain between the two parties, and not affect the external behaviour of those nodes.

Data Storage

The strength of a decentralized monetary system is that it does not require centralized data storage. The status of a social trust connection, including credit limits on either end, and IOU balances, can be stored separately at each end wherever and however the parties choose, as long as such storage allows for proper behaviour when interacting with other nodes on the currency network.

The authoritative data on credit limits will always be with the granter. In case of disagreement about the IOU balance, the protocol should behave conservatively, by calculating available credit for each party based on the other's balance data, until the two parties can come to a resolution.

Security and Privacy

Leaving storage of data for each trust connection in the hands of the parties involved means that it can be as secure as the two parties wish to make it. The question is, how much of this data must be revealed in order to achieve fast transactions? I am not an expert in computer networking, but I suggest that decisions about how much data to share for the sake of efficiency be left to the individual.

It is possible, but possibly inefficient, to complete a transaction in which no intermediate node is ever aware of the identity of the original source or ultimate recipient of IOUs, or the amount of the transaction. This might involve giving the transaction a unique ID and dispatching blind crawlers along the trust network from one or both ends to find each other. Or, both parties could agree on a well-known intermediary as a destination where their crawlers would meet and complete the transaction without having to divulge any information to any third party.

It should also be possible to complete a transaction without either initiating party needing to know the identites or trust connection details of any of the intermediaries except those they are directly connected to.

The protocol I propose should be flexible enough to accommodate the desired privacy of any two parties to a transaction.

Public-key encryption and authentication might be required where appropriate.

Flow Considerations

Optimal transaction paths are likely the ones with some available credit that can be found most quickly. It should not matter which path is chosen, since if there are multiple viable paths, intermediaries along the chosen path will not be significantly inconvenienced. They can use the

other paths to make payments that may no longer be possible along the chosen path due to its now-possibly-restricted bandwidth.

Of more importance is the fact that various well-connected intermediaries may decide to charge fees for their service, which would be passed back to the transaction initiator. Transaction parties must be able to decide whether to accept these fees or not, and transaction messages should be able to include instructions to avoid these fees if possible, or to prefer such paths if they speed up the transaction.

Peer-to-peer file-sharing protocols might provide a useful model for some aspects of the currency protocol.

Conclusions

I will not speculate on what a decentralized currency network would look like. That will depend on the people involved. But I highly suspect that, given appropriate common protocols, as a monetary system it will be extremely robust and a great improvement over current systems.

This paper has only presented a basic outline and touched on some issues that may need to be addressed for implementation of a decentralized currency. I hope that it has struck a chord and that readers will share and expand upon these ideas.

I would like to thank and recommend the writings of Bernard Lietaer (www.transaction.net) and Michael Linton (www.openmoney.org).

Comments and suggestions are welcome. Please email rafspam@yahoo.ca. Thank you.