Payment as a Routing Problem

An introduction to the Ripple project

by Ryan Fugger
ryan@ripplepay.com
http://ripple.sourceforge.net/.

Payment as a routing problem

Modern currencies are issued in the form of abstract obligations to provide value of some form, be it banks' obligations to redeem account balances for government notes, governments' obligations to redeem those notes as credit toward taxes due, or e-gold's obligations to store gold in trust for account holders. A decision to accept a certain currency* is a decision to trust the issuer to fulfill its obligations. From this perspective, a loan repayment agreement is currency issued by the borrower and accepted by the lender.

Payment is the transfer of obligations from one entity, the payer, to another, the recipient, in a form the recipient will accept. In other words, to make payment, the payer must present obligations from a currency issuer that is trusted by the recipient. The payer is faced with the problem of *how to route the payment:* how to convert obligations that it holds or can readily obtain (for example, via a line of credit) into obligations from an issuer that the recipient considers trustworthy.

In a closed village setting, where everyone is known to everyone else, personal obligations (IOUs) are acceptable as currency. As the number of people in the economy grows, *trusted intermediaries* such as banks arise to enable payments between strangers. Banks issue and accept obligations just like anyone else, but their obligations are accepted by so many people they become a payment hub. Instead of using personal obligations directly, people make payment by transferring bank obligations backed by personal obligations.

Bank-type intermediaries succeed to the degree that they can acquire a reputation as trustworthy within the economy that they serve. But no single consumer bank is going to have a monopoly on trust in an industrial-sized economy. There is a need for payments to be routed from one bank to another. If the two banks in question are known to each other and trust the value of each other's obligations, then this is simply a matter of each keeping an account of payments between them that may be settled from time to time as needed, in whatever fashion the banks normally settle accounts.

However, as the number of banks in the economy multiplies, it becomes impossible for all banks to know and trust each other individually. At this point, a government usually steps in to regulate banking practices, thereby ensuring bank obligations have value, and creates a central bank to provide a single, known *path of trust* for routing payments between account holders at any of the regulated institutions. As the number of central banks around the world grows, yet another layer is required to connect them together.

In this type of hierarchical currency network, payments are *simple to route*, but there is a cost for this simplicity.

* *Currency* here is defined as obligations from a certain issuer, as considered separately from the units of value in which those obligations are accounted.

Analogy to computer networks

Computer networks are built to route information from one computer to another. The evolution of computer networks follows a similar course to that of currency networks. For a small network, computers can be directly connected to each other as needed using wires. As the number of computers grows, this soon becomes unwieldy, and it is easier to connect all the computers to a special intermediary computer called a router, which relays information between computers in the network. Routers accept and transmit data like any other computer, but act as a hub for messages between computers because they are highly connected.

Eventually, it is desirable to send information between networks, and to accomplish this, several routers can be connected to a super-router, and these in turn can be connected to an even higher router, and so on in a hierarchical fashion as needed.

Since there is only a single route between any two points, routing messages in strictly hierarchical networks is simple. But this is also the Achilles heel of hierarchical networks: every part of the network has a single point of failure, and thus a single point of control.

Thankfully, the designers of the Internet did not build it as a strict hierarchical network – primarily because to withstand a nuclear attack, it couldn't have any single points of failure. As a side effect, the Internet can operate as the most democratic forum for communication ever known, because it does not require, and is in fact resistant to, control by special groups. (The aspects of the Internet that are the most controversial, such as the domain name system, actually are hierarchical in nature and controlled by special groups.)

The task of implementing the decentralized, open Internet we know and love boiled down to developing protocols for routing messages through an arbitrary computer network. The continually-evolving Internet Protocol standards have been an unqualified success.

Applying the lessons of the Internet to monetary systems

The payment systems we have today are designed as hierarchical trust networks for easy payment routing and rely heavily on active regulation to protect the delicate points of failure inherent in this type of structure. Regulation has been at best only moderately successful – destabilizing “attacks” on national currencies by speculators are a regular occurrence – and always controversial, as various interest groups compete to use single points of control as levers for advancing their agendas.

There are alternatives to the present arrangement. The Internet demonstrates the feasibility of routing information in an arbitrary network, by developing a standard protocol. Payments are nothing but information about obligations – if paths can be found to route information, paths can be found to route payments. The difference is that while information is routed along “best-effort” paths through physical data networks, payments must be routed along reserved paths through abstract trust networks. Billions of trust relationships that exist outside the tightly-regulated global hierarchical currency network could be integrated into that network, removing single points of failure without harming the value of existing obligations. The resulting network would be more stable, and therefore require less regulation and be less expensive to use, while at the same time being more democratic and responsive to local concerns.

Ripple is the project to develop an open, standard protocol to route payments in an arbitrary currency network. The Ripple project's website is http://ripple.sourceforge.net/.

May 2006