To appear in *Agoric Systems: Market Based Computation*, edited by Wm. Tulloh, Mark S. Miller and Don Lavoie. This may be found by ftp at netcom.com:pub/joule/DSR1.ps.gz, DSR1.rtf.gz or DSR1.txt

The art of progress is to preserve order amid change
and to preserve change amid order.

Alfred North Whitehead,
Science and the Modern World

The Digital Silk Road

Norman Hardy
norm@netcom.com
Ph: 415 851 2582

Eric Dean Tribble
tribble@netcom.com

Introduction:

Existing and proposed mechanisms for digital money all require large overhead to transfer money between parties. This overhead makes them unsuitable for extremely low cost activities such as delivering and routing packets. We propose a money system with extremely low transaction cost built into the communication protocols. The money introduced by this system is much more like coins than like bank accounts; it supports only small transactions, requires limited trust among the participants, and requires no central bank. With this as a foundation, we then describe elements of an open system that fully supports network resource management, routing, interconnection with the Internet, and other information services, across trust boundaries with competing providers for all services.

The protocol provides incentives for communication and information providers that avoids policy entanglements typical of subsidized systems—cash-and-carry for cyberspace.

We design incentives based on positive reputations and profits in real local currencies. We take inspiration from tales of the silk road by which silk was brought from China to Europe by a series of traders who knew neither.

We use the term *site* here to describe some assemblage of hardware and software operated by an individual or enterprise. We do not distinguish the entities within a site in this paper and we assume that their interests are entirely aligned.

The Money Field = The Packet's Worth

The basic idea is an inter site link level protocol that includes a money field in some packets. This field is not ciphered and is never negative. It is 32 bits long and its value is the *worth* of the packet. It is denominated in units of one thousandth of a cent or less. As such packets pass over an interface between two sites, X and Y, an up-down *accumulator* that is conceptually between X and Y tracks the net money flow. The accumulator is probably implemented at both sites. Conceptually the respective operators of X and Y periodically read the accumulator and pass real money according to the accumulator's value, then reset the accumulator. More realistically this is accomplished by conventional EFT.

Communication is achieved by a network of sites interoperating with this protocol. Some sites specialize in moving data and others in switching while many do both. We call movers and switchers *carriers* here. One simple business for a site is forwarding datagrams. Such sites make a living by accepting packets at an interface, moving them to another interface, deducting a small amount from the packet's worth as toll and then delivering them across the new interface. Such packets include *steering information* in the packet—an indication for each site of the next interface the packet is to be delivered to, with that indication removed from the packet as it is forwarded. This business ensures a net income for such a site at its collective interfaces. Delivery of datagrams requires no tables or records kept by each site. When you send a datagram thru the network you include more money than will likely be required. The excess will arrive with the packet at the destination and can be returned with an acknowledgment. The amount returned is an immediate measure of the cost of the service.

At international interfaces a multiplication of packet wealth converts currency. Any site can set a money field any way it wants but successful sites are constrained as follows. Liabilities (obligations) arise as packets with worth are exported across an interface. The accumulator there records its obligation to the next site operator. The site will thus be careful not to set it higher than the situation warrants. If sets it too low it will soon damage its own reputation and lose business thereby. Prices are set by normal market mechanisms of supply and demand. They may be set for periods of time and advertised to aid planning, or they may be more volatile. The market will decide this too. Since you pay up front you incur no obligation beyond what you pay and you lose at most what you pay.

Link Efficiency

We assume that packets are grouped into blocks and delivered across the physical interface with error control only for the blocks. This reduces the expense of small packets for they need not individually carry error control and acknowledgment information. This detail is necessary for realistic cost estimation. More suggestions on link strategy are in another paper.

Circuits

While datagrams and their incentives are easy to understand we advocate a more complex and efficient mechanism to move data involving persistent *circuits*. Circuits avoid the cost of steering information in each packet. We mark circuit packets across interfaces as belonging to a particular *channel* of that interface and we identify *agents* within sites that act for a particular circuit at that site. Thus a circuit is a data path from origin to destination consisting of channels across interfaces and agents at sites that work for the circuit. Each agent and channel serves just one circuit. The agents may be thought to *own* the interface channels for their circuits. As a circuit packet crosses an interface it is delivered to the agent that owns the channel of the packet. After possible buffering the agent delivers the packet thru its channel on the next interface. Most circuits are symmetric and can carry data in either direction.

Some circuits may provide flow-control or backpressure. This is done thru signals flowing between agents thru channels against the data flow indicating when more data can be accepted. Backpressure may arise at the destination or some intermediate point in the circuit. Circuits that don't do backpressure discard data when unable to deliver it. We will mention numerous other potential circuit qualities in a later paper.

An agent holds some money to rent buffers and pay for transmission across interfaces. Occasional packets thru the circuit carry money to replenish the agent's money.

Building circuits

Building a circuit occurs with a needle moving thru the network with steering information like a datagram but leaving a path of channels and agents behind it. To delete a circuit a destruct signal travels along the circuit that deletes the agents and frees the channels. By convention a zero in the needle as interface number signifies end-of-circuit and the current site is the target of the circuit. Messages thru the circuit are interpreted locally.

Note that it is possible to send a datagram using the circuit primitives: Send the needle, the data, then the destruct signal.

Routing Services, or Scouts and Guides

A scout program situated at some site in the network can explore available routes. It does this by launching circuits in all directions. As each site is reached the scout asks the site its name. The response is returned over the circuit. When the scout has not seen the name before, it adds the site to its map. The scout asks the site what it does for a living. When a site responds that it moves or switches data and the scout has seen the name before it adds a link to its map. Other responses are entered into an information service data base. At new sites the scout asks how many interfaces there are. The scout continues while there are unexplored interfaces in its map. The scout contracts with each site to be informed of any new interfaces that should arise or expire.

The scout's data base is available to affiliated guide programs that advise how to travel between sites. It is natural for guides to deal in the reputations of the carriers that they select for their customers. Sites that claim to move data but do so unreliably are not long recommended by guides.

What's in a Name?

We wish to impose few standards here. It seems, however, that some standard internal way for programs to name sites would be widely convenient if not necessary. We propose that a public crypto key is suitable for fundamental site names. We propose that one simply generate a public-private key pair and use the public key as a name. Only the real owner is able to process messages meant for him. Others, seeing X's public key, could claim to be X, but could not reply to any messages meant for X. The first 32, 48 or 64 bits of an RSA public key form suitably unique and short nick-names for many purposes.

Name Servers

Naming seems to be a natural monopoly but it need not be. Hierarchical naming schemes ala the Internet serve many purposes. Names that a person could carry with her would also be useful. Naming services are closely allied with guide services.

A given name server can sell alphabetic names. There might be a US name server that manages to convince most people in the US that his is the only important name server and registering "L. Jones" there is to effectively own that name. One service of this server would be to map alphabetic names to public key names. It is interesting to imagine competing between name sellers. We have thought out this to a few levels of gaming and it seems stable. A possible plan is to sell name-key pairs at $1 each. More likely is to charge $\$10^{8-n}$ where n is the length of the name. This is only a crude estimate of the market price.

Other Services

Carriers, guides and reputation systems are all information services. They all work for cash. Data base operators, computers and all sorts of other traditional information services fit in this same mold. We imagine here a few more specific services that might arise.

I want to integrate a function or factor a polynomial. I send the problem to a Mathematica server together with $.05 and get the response in a few seconds. I probably get the answer but the response may be that $.05 of computing yielded no answer but more might do the trick. For a while it will preserve the state of the computation for resumption if I wish to send more money. The response might alternatively be that it knows the answer but will only reveal it for $.25.

There may be an interface to a real bank thru which you can deposit and withdraw small sums of cash from your account; a CyberATM, or better, CyberTeller.

I have a document in TeX format but I can only print Post Script files. There is a service that does the conversion for $.005 per page.

Anonymous Forwarders: Some sites will advertise a public crypto. They will expect all or some of their input packets to be ciphered. If such ciphered packets request some delay before forwarding, the site serves as a *mix*. (David Chaum introduced the term mix to describe a network service that forwards mail after removing standard indications of the source, thus providing anonymous mail.) The amount of money allows statistical tracing but this may be alleviated by establishing a small account at the mix. (Anonymous mail is a complex social issue and the operator of such a mix may be subject to social pressures.)

Specialized computing facilities could sell their service this way. If I have a computation that takes 10^9 bytes of real ram for $2 \bullet 10^{10}$ operations, some Cray machine could run my code in 20 seconds for $3. If the Cray were kept busy with such business it would provide a 100% profit for the operator. Note that I need not be deemed a researcher by the government.

Even if 10^9 bytes of storage are not required I may prefer to spend $50 for 30 seconds of a big Cray to do ray tracing than 3 hours of delay on my own CPU.

Guides may offer datagram forwarding service to avoid computing an optimal path from source to destination. Perhaps specialized forwarding services would make more sense in this case but guides already have full time circuits to each site.

Incentives and Reputations

> It is not from the benevolence of the butcher, the brewer, or the baker, that we expect our diner, but from their regard to their own self-interest. We address ourselves, not to their humanity but to their self-love, and never talk to them of our necessities but of their own advantages.
>
> Adam Smith, *An Inquiry into the Nature and Causes of theWealth of Nations,* 1776

A site in this world can default, but when one buys an information service it is almost always caveat emptor. We do not request our money back when a magazine proves uninteresting. There is seldom a way for a third party to judge whether the service satisfied some contract. We rely thus on the positive reputation of the vendor.

Communication links fail which will cause interfaces to go down. A site may use a circuit as a detour for the interface. It might build the circuit in advance as a precaution. It might take a loss to maintain its reputation. Alternatively it is remarkably inexpensive to build two circuits between the same two endpoints, the second to serve as a hot standby. Since no data moves over the standby the cost is probably negligible. Circuits with a standby could arrange for their site agents to return the buffered data at the several sites to be retransmitted over the standby circuit.

When a neighboring site itself goes down it is harder to play fair. Only the failed site can properly interpret packets that were meant for it. It behooves a site X to arrange for at least one of its neighbors to notify routing services when X dies. This minimizes damage to X's reputation. It is in the neighbors interest to do so because, to an extent, their reputations rise and fall together. The whole neighborhood's reputation can suffer.

The concept of liability helps think about how systems like these work. When a site accepts a packet requesting forwarding to another interface it has acquired a liability or obligation. If it loses the packet it has defaulted but gains the amount of money in the lost packet. The site guards the packets to guard its reputation. We specifically reject mechanisms that would create an externally registered liability for each packet as that would likely cost more than the transaction itself. In particular there would be no legal liability. In the presence of real time automatic reputation systems it is enough that reputations can be lost in minutes.

Reputation Systems

Reputation systems can be built to provide current information on the performance of a site as observed by its customers. Examples of reputation services are Dun&Bradstreet, the local Better Business Bureau and Consumer's Union. Reputation systems are complex. We do not anticipate automating them completely. They must gain the trust of their customers and the only way to do this is to provide useful guidance to those customers. Indeed a reputation system must protect its own reputation.

Examples of such services are Dun&Bradstreet, the local Better Business Bureau and Consumer's Union.

Reputation systems are in a natural position to provide Yellow Page service.

Reputation systems can evaluate and rate a service by anonymously subscribing to it. Usually, however, they must evaluate complaints that come from customers of the rated services because the service is too expensive or it requires subjective judgment, or judgment by experts, who are, after all, the customers. The reputation service must thus judge the veracity and incentives of its reporters, namely the very customers of the reputation service. This requires the difficult skills of a diplomat, but ultimately incentives pull in the right directions.

There is an economy of scale in reputation systems. A user learns of the reliability of a service from other users thru reputation systems. He does business with many vendors according to their reputations as reported by the reputation system. He does business with only a few reputation systems and can thus directly judge these familiar systems.

Standards

This whole exercise is at attempt to avoid standards as if standards were bad. Actually standards are good but systems are sometimes bad because they cannot adapt to new standards. When we describe standards it is in part to establish that standards are possible in a world such as we suggest. Our main effort is to show possibilities if money is included in low level protocols. Behind each protocol description there is the suppressed comment that it could work some other way and work at the same time in the same network albeit with resulting inconvenience.

Bridges

To connect with classic networks we propose bridging sites that conforms to both worlds. The bridge keeps accounts for whoever needs to access CashNet from the Internet. If someone in the Internet needs to build a circuit to Y in CashNet then she must have an account with a bridge operator. She may then build a circuit to the bridge, identify herself somehow, and build a cash net circuit from there to Y. Her bridge account supplies money for packets going into CashNet and accumulates money for packets of hers coming back out.

There might be a collect call service where the bridge on its own speculative expense calls someone in CashNet in response to a query by an Internet citizen unknown to the bridge. The bridge asks if the CashNet citizen is willing to accept a collect call.

Calls from CashNet are easier. No account is needed for connection service to the Internet which can be paid for immediately.

Advantages

Decentralization affords diversity. Diversity fosters evolution. The protocol is simple and makes it possible to start up small businesses without the normal high cost of locating customers and arranging contracts.

Many one person companies. Many people already make a living indirectly thru the Internet. To do so requires finding some sponsor that will hire you with an motivation to provide some information service for free. The sponsor may indirectly be some government with a charter to provide service, or it may be an enterprise that supports collaborative research. Most information commerce cannot conform to these patterns.

Wide variety of services. Most current Internet services are currently free to the end user. This may be changing already but the Internet provides no integrated way of charging for such service. It is thus infeasible to sell some service whose intrinsic worth is only a few cents. When I wander into a book store and choose a book and pay for it with cash I need not learn the name of the owner of the book store nor need he learn mine. It is even easier when I buy something from a vending machine.

No Junk Mail! One could protect himself in a satisfying way if one advertised his reading tariff along with his net-name and directed his mail deamon to discard mail with insufficient tariff, then at least one would be compensated for reading such mail. More politely one's mail deamon could return the excess postage with a note that the message was automatically discarded since the worth was insufficient to justify reading the mail. One would surely get off of most junk mail lists that way! People with 900 series phone numbers get few solicitations! We don't mean this suggestion in all seriousness but we do hint at some social issues that are not exclusively electronic. Some "junk mail" may be desired by the recipient. We may want to see colloquium announcements or movie reviews. I instruct my deamon to watch for such announcements and return postage to the distributor sufficient to deliver the next package.

Availability of trivial services. I once got a total stranger to convert a TeX file to a PostScript file for me. The Internet is friendly place but I cannot continue to impose on strangers. If the converter were paid a penny a page he might find it worth his while to automate this service.

Communication systems have long been thought to be natural monopolies. To the technical obstacles to progress are thereby added bureaucratic and political obstacles. Technical progress has eliminated most of the original reasons for viewing the phone business as a natural monopoly, especially as cable companies install high bandwidth service to the home. When government operates phone systems as in many countries today, it has the political mandate, or feels it has, to establish policies that limit the uses to which lines may be put. Some of these policies are in fact to protect the established system from competition. Some countries were a decade or so late in digital communications because such service threatened conventional revenues. This is characteristic of monopolistic behavior. Government regulation is supposed to limit monopolistic manifestations. This is very difficult, perhaps impossible, even for intelligent uncorrupt non-political regulators.

Perceived Problems

Potential problems arise when we make fundamental changes to any working system. We examine several here and tend to argue that they will be transient.

Without central administration there is more opportunity for substandard service. Indeed there are no centrally mandated standards. This system would naturally encourage voluntary and de facto standards. Reputation systems would report compliance with such standards. Mandated standards are often unachieved. Competition even solves the problem of what the standards should be—How good is good enough?

Without central administration there are greater opportunities for fraud. It will bother some that forwarding sites have neither accountability nor legal liability. Operators of such sites must plan to make their living from repeat business. Just as a restaurant must provide food acceptable to its customers to ever make a profit, so must such sites play largely by the "rules". One type of fraud is especially egregious—"losing" packets and pocketing the money. This is especially tempting since one may be able to blame the loss on your neighbor. Indeed this aspect bars application of CyberCash from transfers of large sums. Just as one normally does not carry $10,000 as he wanders through strange neighborhoods, neither does one send $10,000 packets thru most sites. (This is another justification of the 32 bit money field denominated in $.00001) Repeated packets, with acknowledgments, could move large sums but this may run up against limits imposed at interface accumulators where the credit of one site operator may be insufficient in the eyes of the downstream operator. It all boils down to the fact that big money is a big deal, even for banks! Incidentally this problem with big money is better handled with schemes such as Chaum's digital money which involves a bank and does provide accountability and perhaps legal liability.

Protection against gridlock may require some distributed logic. Gridlock occurs when some set of sites are unable to accept new packets for lack of storage and all of the packets that they need to deliver (to relieve their congestion) are directed to members of the set, none of whom are receiving. We have not thought out an incentive based solution to this yet. Circuits alleviate but do not eliminate this problem. This difficult exercise is left for the reader

Operator Credit

These concerns involve both the individual end user whose personal computer implements this protocol or some huge communications carrier.

If the credit of one of the site operators at an interface is insufficient for the other operator then the latter may establish a limit on the accumulator beyond which traffic is not accepted. This would likely be the case for end-users that would thus be limited in the bills they could run up. The credit limit may be zero, thus requiring prepayment. Conversely the same limit protects the user from running up unlimited bills thru misunderstanding of the software that handles his cybercash.

Perhaps such interfaces would make EFT (Electronic Funds Transfer) arrangements with normal financial institutions when some economic amount of net money is involved or credit becomes stretched. This is an ideal application for Chaum's DigiCash.

Other Issues

Several ideas have been omitted from this paper that concern how a network of this sort can provide a degree of security and reliability beyond what is possible to achieve based on the Internet protocols. These issues are somewhat orthogonal but may, nonetheless, be strategic to each other. We expect to produce another paper covering these ideas soon. We hope to speculate in another paper about prices that might be achieved if there is free entry by communications providers into this market.

Conclusion

Much of the charm of the Internet is the informality of access. One can learn of a program thru netnews, fetch it via FTP and run the program in the span of an hour with no bureaucrats or clerks involved and certainly no lawyers. This is as much a matter of Internet culture as charter. But what has more charm and informality than a flea-market where cash and anonymity prevail?

Bibliography

Braun, Hans-Werner, and Claffy, Kimberly C., and Polyzos, George C.,
"*A Framework for Flow-based Accounting,*"
to appear in Proc. Singapore International Conference on Networks (SICON'93), Singapore, September 1993.
(Also available by anonymous ftp from ftp.sdsc.edu:pub/sdsc/anr/papers/accting.sg.ps.Z)

Brands, Stefan, *An Efficient Off-Line Electronic Cash System Based On The Representation Problem.* Anonymous ftp at: ftp.cwi.nl:/pub/CWIreports/AA/CS-R9323.ps.Z

Chaum, David. Achieving Electronic Privacy, (blind signature technology) *Scientific American* v267, n2 (August, 1992)

Dukach, Semyon, SNPP: A Simple Network Payment Protocol. *Proceedings of the Eighth Annual Computer Security Applications Conference*, december 92. Anonymous ftp at: ana.lcs.mit.edu:pub/snpp.

Ferguson, Niels, *Single Term Off-Line Coins*, in "Proceedings of EuroCrypt'93", 1994, To appear. (Anonymous ftp at: ftp.cwi.nl:/pub/CWIreports/AA/CS-R9318.ps.Z)

Huberman, B.A., editor, *The Ecology of Computation* (North-Holland, New York, 1988).

MacKie-Mason, Jeffrey K., and Varian, Hal R.(1993). *Some Economics of the Internet.* gopher: gopher.econ.lsa.umich.edu

MacKie-Mason, Jeffrey K., and Varian, Hal R.(1993).*Pricing the Internet.* gopher: gopher.econ.lsa.umich.edu

Pool , Ithiel de Sola, *Technologies of Freedom*, (Belknap Harvard, Cambridge MA).

Temin, Peter with Louis Galambos. *The Fall of the Bell System, a study in Prices and Politics.* Cambridge, Cambridge University Press, 1987