Price Waterhouse sees I-commerce growth

Price Waterhouse predicts a massive increase in business conducted via the Internet. Between 1996 and 1997, business-to-business trade doubled every 6 months and this is accelerating to double every 3 to 4 months in 1998. By 2002, the value of goods and services traded via the Internet will increase to $434 billion.' www.pw.com

Digital bearer settlement

by Robert Hettinga

Since the invention of the telegraph, financial transaction settlement has had a problem: how do you transact business at a distance when the simplest way to execute, clear and settle a transaction is with an exchange of bearer certificates?

Our current system of so-called 'book-entry' transaction settlement was invented in order to handle the problems caused by remote transaction execution and the subsequent need to physically exchange bearer certificates for settlement. We now have the means to return to 'digitally encoded' bearer settlement with a three orders of magnitude cost saving.

Soon enough, the era of book-entry settlement, our way of representing money as offsetting debits and credits exchanged between the two parties of a trade through a hierarchy of trusted intermediaries, will be over.

I think that the social and economic impact of the new alternative to book-entry settlement, digital bearer settlement, will be quite large, because, at the root of the status quo's book-entry transaction protocols is the need to involve government and regulation at the most intimate levels. Essentially, '...and then you go to jail' is the penultimate error-handling step in a book entry transaction.

In the old days, before telegraphy, most financial transactions were done by trading bearer certificates, or tokens, of one form or another. Exchanging cash for a bearer bond would be a good 19th century example. Even trading bearer forms of equity was trivial and instantaneous: the offer, the acceptance of the offer, and the settlement of the transaction occurred almost all in one operation.

With the advent of telegraphy and eventually telephony, it was possible to make the offer and accept the offer at a distance, but settlement had to wait until bearer certificates were physically relocated, sometimes over long distances and then exchanged. After all, you couldn't very well send them over a wire.

The solution was to move all the certificates to a central trusted location, called a clearinghouse, and for the trading parties to swap debits and credits between themselves and the clearinghouse. It's pretty apparent that having the certificates physically locked down in the clearinghouse's vault becomes superfluous in such a scheme, because what really matters is the impartial arbitration of the clearinghouse in the case of a transaction dispute. All except for one thing. If someone lies or reneges on a book entry transaction, there isn't much that the other two parties can do except bar them from trading, which, of course, works in bearer certificates, but not nearly as well in book-entry settlement.

So, we need several things to cope with non-repudiation in book-entry settlement. First, we need the ability to determine who physically made what book-entry so we can find them and send them to jail for fraud if necessary. That's because book entries are inherently unstable, insecure, digits sitting in a database somewhere. Many people in Asia are familiar with commodities and derivatives traders who were capable of hiding fraudulent book-entries for long enough periods of time to bring down their respective firms, for instance. In cryptography we call this an authentication problem.

So, besides authentication of the book-entries themselves, we need to secure the links between various charts of database accounts, first by authenticating the users of those electronic links, originally with passwords, then with cryptographic keys and signatures, and now with some combination of biometrics (finger or retinal prints, say) and digital signatures. And, second, by actually encrypting the links themselves so that no one can see what they are even if they can't change the authenticated data without someone noticing.

Sorry for the long-winded explanation, but it's long-winded stuff, as most people who clear trades on the net for a living will tell you. Anyway, for all intents and purposes, you now know everything there is to know about the guts of electronic commerce on the Internet. When you punch your credit card number into a secure web page, pretty much all of the above happens, plus or minus the retinal scan.

However, all this stuff about moving book-entries down encrypted pipes on the internet, including the much-heralded SET protocol for credit cards, is so much financial 'shovelware'.

Fortunately, there is much more that can be done with financial cryptography. There's a whole string of cryptographic protocols out there, beginning with David Chaum's blind digital signature patent in the middle 1980's. You can actually create unique digital objects which can't be forged if you handle them right (if you only exchange them on-line, for instance). You can attach any arbitrary financial value you want to these cryptographically secure objects as long as everyone else agrees with you, and, most important, you honor your agreements concerning their exchangeability into some other financial instrument. So, I call these objects 'digital bearer certificates', after the paper bearer certificates of yore, which I claim these crypto-blobs behave like, more or less.

The fun part comes when you actually start to trade these things. The first thing you notice is that they settle instantly. I give you digital cash certificates, you give me digital bearer bond certificates. Trade over. Elapsed time, thousandths of a second. I can turn right around and take that bearer bond and sell it again, if I want. More to the point, I don't have to wait for my broker work out how to move my money to your broker through the clearinghouse, for their banks to arrange to pay each other, all of which takes days and costs lots of money. The cost of your on-line Schwab or E-trade transaction could move from being measured in dollars to somewhere in the sub-penny range, and probably less over time.

Actually, these aren't account based protocols at all. So there ain't no Schwab, or Merrill Lynch, or Morgan Stanley, required. Well, not completely true. You still need financial intermediaries, no matter how small, to 'rent' reputation to a given transaction.

As far as non-repudiation goes, I know that what you gave me is real because I can test it with the

(Continued on page 15)

(Continued from page 14)

issuer. You can do the same thing. It's so trivial that I equate the act with the physical inspection each of us does, unconsciously or not, when we're handed a piece of cash. If I don't like what I 'see' (determined by the calculation of the cyptographic protocol, of course), I don't trade with you. I'd say it's much better than detecting fraud after the fact, finding who made the offending book-entry, and apprehending, trying, and jailing the miscreant. Frankly, I'd go one further and say book-entry settlement is so complicated and unwieldy that the only reason we have book-entry settlement now is because we couldn't shove paper down a wire back when telegraphy was invented.

Finally, there's no real recordkeeping of transaction logs with digital bearer settlement. Like a pile of cash, you count it up, and that's what you have. There is no need for seven years of audit trails at up to six different transacting parties because you don't have to hunt someone down and send them to jail for reneging on a trade before it settles, and more frequently, to prove you're innocent should you be suspected of something untoward. You don't need a lawyer or an accountant to keep you out of jail at tax time for making the wrong book entry somewhere.

In fact, you don't care who gave you what money as long as they're happy with what you gave them in exchange for it. Reputation becomes the most important thing there is, because damaging someone's reputation is your only recourse in a world where your digital signature is your only identity. The threat of blackballing is in fact a very effective fraud deterrent, and once a digital reputation is trashed, it takes time and higher transaction risk premia to build a new one. To quote J. Pierpoint Morgan on the subject, 'I wouldn't buy anything from a man with no character if he offered me all the bonds in Christendom.'

Once we get to digital bearer bonds, stocks, and derivatives thereof, the world starts to change considerably. However, I still claim that reality is not optional. If you reduce the cost of settling a transaction to effectively zero (okay, past the last basis point but not zero), then the financial markets are going to figure out how to use the technology. Not only is it cheaper, but by being cheaper, it allows for smaller and smaller publically held entities. And automated financial intermediaries. The asset sizes of various trades could get much smaller, but, in addition, I claim, that because trading of financial instruments can happen so quickly, efficiently, and by so many self-interested actors, it'll probably be the way money is raised for very large security issues and for very large projects. Maybe Intel's inevitable $10 billion chip fab, for instance, will be floated into a market 'swarm' of financial intermediaries. Microintermediation, instead of disintermediation, in other words...

Okay. I've now walked you up the edge of the abyss, and pushed you over the cliff, and, you'll notice, you didn't get hurt at all. That's important to think about, because sometimes being quantitatively cheaper has qualitative effects, but, for modern society at least, the future is no different from the past, except that we've figured out how to live better. I expect if we can blow the doors of the cost of financial services with digital bearer settlement, the world will be a much better place to live in, indeed.

Robert Hettinga is the CEO of the Shipwright Development Corporation, in Boston MA
Email: rah@shipwright.com

IN BRIEF

Visa speeds switch to smart cards

Visa International has reorganised its management team in order to speed a massive migration to chip-bearing smart cards over the next five years. According to a Visa source the first Java-based smart cards will hit the market in Europe this summer. Visa's new Central Approval Authority, or CAA, is expected to be fully in operation by midyear. It will provide vendors with a approval process.

E-Finance Forum

Thursday 28th May 1998, 7 pm
London Business School,
Sussex Place,
Regent's Park
London NW1 4SA

Speaker: Guy Knight, Director, Charles Schwab Europe

Guy Knight joined Charles Schwab Europe (formerly ShareLink), the UK's largest execution-only brokerage, at the beginning of 1996 as Marketing Director, subsequently becoming Vice President and Head of European Communications. He is an executive board member of the company.

He will talk about the Schwab e-trading story, the keys to success in this arena, tour parts of the site including web trading and discuss the key issues facing finance companies using the web.

The talk will last for approximately 45 minutes, followed by questions, discussion and a reception with the speaker in the Executive Common Room.

Anyone can attend, but there is a £10 charge. Please register with Tracey Croft at the London Business School (tcroft@lbs.ac.uk), Alumni Office, Sussex Place, Regent's Park, London NW1 4SA.

The E-Finance Forum is organised by Duncan Goldie-Scot of *FT Virtual Finance Report* with support from Emma Caseley, Director, LBS Alumni Association (ecaseley@lbs.ac.uk).

CitX and InsurNet partner

CitX Corporation of Quakertown, PA, has announced a strategic partnership with startup InsurNet Technologies, of Philadelphia, PA. The companies have developed an Insurance Marketing and Management program that enables banks to sell insurance services and products, such as Auto, Home, Health, Long-Term-Care, and Property, to their customers, via the platform called Intrapay.

The Geodesic Market

by Robert Hettinga

This is the first of a series of articles Duncan Goldie-Scot has commissioned me to write on the future of financial technology in an age of ubiquitous internetworks, Moore's law, and strong financial cryptography.

I'm calling this series *The Geodesic Market*, in the spirit of a 'popular' book I've in the works named, oddly enough, *Beyond Civilization: Life in a Geodesic Society*. Actually, the core technology we're going to talk about is a group of financial cryptographic protocols I have termed digital bearer transaction settlement, which is the title of another book I'm working on.

When I was a teenager in the 70's, my best friend Jeff Blanton and I zealously devoured all of Stewart Brands' Whole Earth 'Domebooks'. Back in 1974, when capitalism was the farthest thing from our mildly drug-addled minds, who would have thought that 'Bucky', R Buckminster Fuller, the greatest designer since Leonardo, we thought, had discovered not just an easy way for freaks like us to build cheap housing and squat on someone else's land, but that he had actually discovered the way that society, mapped as always to our communication topologies, would look in the not too distant future.

Buckminster Fuller, for all his latter-day attempts to solve global resource allocation by good old fashioned top-down hierarchical industrial centralism, might not have imagined that the economics of semiconductor switching on telephone networks would eventually create giant, decentralized, capital markets. Markets so powerful that they would make the most out-of-control, rapacious 19th century industrial trust look like the most bucolic feudal guild. On a feast day. With their feet up. Capital markets operating on a network topology almost identical to the geodesic structures my friend and I were all so enamored with back in the days of the Allman Brothers, Levi's Big Bells, and ubiquitous low-yield psychochemicals.

Even more ironic, you and I are going to raucously cheer these new geodesic markets on, as they surfact large concentrations of financial information and capital into fractally smaller and smaller bits, microintermediating it all like so much grease in soapy dishwater, in an instantaneous transnational market for capital. We're going to cheer these new markets on because they're going to make us so damned much money.

Economic inevitability

These market will operate, finally, under the control of economics, instead of the confiscatory 'policies' of aristocrats or nation-states. Nation-states will eventually be as ceremonial as modern-day constitutional monarchs. Like the way physics and philosophy got out from under theology at the end of the dark ages, economics will no longer be the handmaiden of politics in a geodesic market.

The fun part is, it's inevitable. It will come from the collapse of microprocessor prices, the 50% decline every 18 months that is Moore's 'Law', more an observation of the human ability to learn than any physical law. The geodesic market will come from the ubiquitous geodesic internet those prices create, and, in a remarkable reversal of history, a re-emergence of the kinds of transaction settlement methods thought to be killed by the telegraph, and, ironically, mainframe batch computing.

A geodesic market will use digital bearer transaction settlement protocols, perfect pseudonymity, and reputation sanction on ubiquitous public networks, instead of book-entry settlement, audit trails, and la, on the closed, private networks that we now have.

Stunning? Outrageous? Preposterous? Before you click away in disgust, remember we only have what we use now because it was cheaper than what we used to use. Hence you and I don't go down to a bunch of merchants in the City to trade paper cash for paper shares anymore. I am perfectly serious. With financial cryptography and digital bearer transaction settlement, we can do perfectly safe, rational business on the internet without lawyers. Or, for that matter, cops.

In addition to transaction costs three orders of magnitude cheaper than book-entry settlement (yes, past the last basis point: it's time to pick a new measurement unit), you will have perfect financial privacy as a happy accident of the same technology which drastically reduces transaction prices. Just like requiring the privacy-invading physical force of a nation-state in our very transaction clearing processes was an unhappy accident of book-entry settlement.

All of this will happen with more non-repudiation and more asset safety features, including seemingly impossible things like limited liability and shareholder voting.

The reason we have database marketing, book-entry taxes, (like income, capital gains, value added, and sales taxes), and book-entry regulations, (like, well, practically all regulation, these days), is because the book-entries are there.

We need those book-entries in order to prevent non-repudiation of transactions. And, to enforce rules against a transaction's proven repudiation, we need the police. So, if you don't need book-entries, you can't have that other stuff, including, as Doug Barnes of C2NET likes to say '...and then you go to jail' as the error handling step in your transactions protocol.

(Continued on page 15)

Too beautiful not to be real

When I'm working on a problem, I never think about beauty. I think only how to solve the problem. But when I have finished, if the solution is not beautiful, I know it is wrong.

R Buckminster Fuller

(Continued from page 14)

Impossible? If we can do digital bearer transactions, safely and anonymously over the internet for, say, 1000 times cheaper than book-entry settlement, what do you think will happen?

Digital bearer settlement

As a brief preview, let's take a look at the things you can do with digital bearer settlement. Not surprising, it's everything you can do with book-entry settlement, and more.

Consumer Debt: Instead of using a credit card, imagine issuing personal bearer bonds. Whole bond issues, actually. Microintermediated, by, you guessed it, a syndicate of micro-underwriters, living in the ubiquitous internet, all of whom, like underwriters always do, intermediate the market's loan of money to you based upon your reputation for repayment.

Digital Cash: Since most people pay off their credit card purchases within a month after purchase, you will be relieved to know that instead of having to hassle with a credit card bill just to cover your normal monthly purchases, and the lack of privacy which goes with it, you will be able to use digital bearer cash, which will be as safe to use as checks or a credit cards are now, all without interest, or at least annual fees.

The main reason you'll use digital bearer cash is, however, that eventually there'll be no float on your checks or even your credit cards. Notice how debit cards are cheaper already to use than credit cards, and that merchants are starting to see the advantages of getting their money without chargebacks hanging over their head.

This is so fundamental a process that it should be a law of finance or something: the closer an electronic book-entry transaction system gets to instantaneous, the more digital bearer settlement becomes financially necessary. As a friend at a large IT consultancy in Cambridge (Massachusetts) likes to say, 'Real-time gross settlement is digital bearer settlement.'

Capital Markets: Instead of purchasing a stock through a broker with limited, hierarchical, almost oligopolistic access to the capital markets, you'll be able buy your digital bearer bonds or shares in public, or at least privately, using public networks. The internet is the equivalent of the old buttonwood tree on Wall Street, as I once wrote in *Wired*. I show up on the net with cash, you show up with your bearer shares, we exchange the two, and the trade is over. Execution, clearing and settlement, all in one step. Anonymously, because it's cheaper. That's the beauty of digital bearer settlement. You can do this for any financial instrument, debt, equity, or derivative.

Internet Resource Allocation: Also, there are the things you can do with digital bearer settlement that you just can't do any other way. It's easy to imagine very small packets of digital bearer cash 'buying' a message across the internet, with each router buying packet switching low, and selling it high. Look, Ma, no human hands: No 'peering' arrangements, probably no network 'engineering' either, in the long run, as the internet becomes, like any free market, a complex self-adaptive system. I joke about 'picomoney as processor food'. 'Micromoney mitochondria'. Auction markets for bandwidth, certainly. Maybe for the guts of the machine itself, memory and processing time. All you need is Moore's Law, fast enough processors, and, of course, digital bearer financial cryptography protocols.

Utilities: But, wait, it gets worse. You can pay for electricity, in cash, as you use it, down, of course, the same wire you got the electricity from. You can pay for roads as you use them, perhaps every few hundred yards or at every intersection. Like you can on the internet, you can pick the cheapest or fastest route to your destination. So much for 'public' roads. Just about everything you think of as a 'public service', or a 'natural monopoly' may be reduced some day to a continuous cash-settled electronic auction between competing parties. Moore's law creates diseconomies of scale and geodesy. Hierarchy and economies of scale are a function of expensive (human) information switching.

Geodesic Warfare?: Even force can be auctioned off and sold, same as it ever was, only this time to the highest microbidder. Imagine your land covered with semiautonomous landmines, keyed to your digital signature, which only go off when you tell them to. No, don't imagine them taking bribes to change sides. It's real. Someone at the US Army War College wrote a paper on just such a scenario four years ago. Of course, whether we'll need state-funded armies in a world where force has been disintermediated to such an extent or where taxes might be 'optional' is an entertaining proposition.

Price deflation

So, who knows what the future's really going to look like. I may almost have my videophone now, but I have yet to see a (useable!) flying car, for instance. However, there's one thing we can be certain of. Information and knowledge will be developed and sold in much cheaper and smaller bits than we do it now. The prices for industrial goods will fall in a geodesic economy just like agricultural goods and raw materials did in the industrial economy.

Just how far it goes is limited by Moore's Law. Moore's Law also enables the ubiquitous use of cryptographic financial protocols, like Chaum's original blind signature algorithm for digital bearer certificates, or the one for Rivest's MicroMint micropayment protocol.

This series of articles is about how those markets, well capital markets, will come to be, how they will operate, and what actors will probably succeed in those markets.

Next month I'll discuss geodesic networks and why I think they create geodesic social institutions like geodesic markets, how trade and money, how human society itself looks when viewed historically through the lens of their communications architectures. Then, I'm going to talk in laymen's terms about the financial cryptography underpinning digital bearer transaction settlement, and then survey some of the different kinds of digital bearer settlement protocols on the market and in the labs at the moment.

After that, I'm going to apply these different protocols to different pieces of the capital markets we now have, and show you what the world looks like in a geodesic market for capital.

Robert Hettinga is the CEO of the Shipwright Development Corporation, in Boston MA
Email: rah @shipwright.com

IN BRIEF

Sumitomo Bank to use 128-bit

Sumitomo Bank plans to adopt 128-bit encryption security for its Internet banking system, which is scheduled for launch in June.

The bank plans to procure an authentication system that uses 128-bit encryption from VeriSign Japan KK, the Japanese arm of US firm VeriSign.

Sumitomo is the first Japanese financial institution to implement 128-bit encryption.

Net banking services for Japan

Bank of Tokyo-Mitsubishi (BTM) is to introduce a new internet banking service for private clients in collaboration with Microsoft. A BTM spokesman said the bank will use software based on the Microsoft Money personal financial management product to enable clients to make financial transactions and access financial information through the internet.

How to underwrite a digital bearer security

by Robert Hettinga

In this second instalment of the Geodesic Market, I'm going to show how to underwrite digital bearer securities, using cash as an example.

The business model I'm using should be familiar to anyone who's been in the securities business for more than 20 years, and especially to anyone who's studied financial history. There's no surprise in that. We have 5,000 years of experience with bearer transactions. There's nothing new, except the cryptographic protocol, to worry about, and we're not going to talk about cryptography here in any detail.

Another nice thing about this model as applied to cash is that it will be possible for people to convert their money to digital cash in and out of their own bank accounts, just like they can for paper cash. The underwriter, as I call the issuer of digital cash, becomes the internet equivalent of a third-party ATM machine, something everyone's familiar with.

Because of this modular plug-and-play approach, it's pretty simple to obey all the rules we currently have about handling cash, while dramatically reducing the cost of cash transactions in the process.

So, let's get started with a look at the players in this market.

Consumers and merchants

A consumer is someone who buys a piece of digital cash from a financial intermediary, an underwriter, in exchange for some other kind of money, a change in a bank account balance in this case, in order to effect a transaction on the net.

A merchant is someone who accepts a digital bearer certificate in payment for something else.

Of course, I hate the use of the words consumer and merchant because they don't describe geodesic peer-to-peer transactions very well, but the banking world understands them perfectly, like they do underwriter or trustee or custodian, so I use them here.

Underwriter

The underwriter issues digital bearer certificates, and is fiduciarily responsible for exchanging them into other forms of money, again a bank account balance change, held by a custodian in a reserve account. Someday, of course, the reserve assets collateralising an issue of digital cash could be some other digital bearer asset.

The second most important thing an underwriter does is to verify, at every transaction, that a given digital bearer cash certificate hasn't been double spent, copied by someone and spent twice. After that, the underwriter issues a brand new signature-blinded certificate to the person accepting the cash in payment. If the exchange fails at any point, so does the transaction, and the person offering the cash is prevented from double spending it, thus preventing repudiation of the transaction at execution time. Cheques, credit cards, or any book-entry transaction can't offer that security. Even with on-line validation for fraud, the merchant is still at risk of stopped checks or chargebacks.

Finally, the most important thing an underwriter does is to market its certificates to the world. Which, if you look at an underwriter in the capital markets, is exactly what they do for both primary and secondary transactions, and that's why I use the label here.

The original DigiCash ecash mint at Mark Twain Bank was a used 486 machine, just to give you an example of the hardware cost of being an underwriter. Eventually underwriting may be automated to the point of processor husbandry in the same way that one tends a web or router farm today, but it should always be done by a separate financial entity other than the trustee.

Trustee/custodian

A trustee, or custodian, holds the money reserving an issue of digital cash, on behalf of the cash certificate holders, in a bank account, though someday the reserve assets could be held in bearer form under the trustee's control. Like bond trustees or mutual fund custodians, the trustee operates according to an agreement, like a bond debenture, between the underwriter and the certificate holders. This agreement could specify fees and, most important in the early adoption process, reserve ratios.

So, while the underwriter is the direct financial intermediary, and keeps the interest which accrues on the reserve account, the trustee risks their reputation by holding the reserves, is compensated for it, and controls that risk by making sure that the reserve agreement is adhered to.

Put simply, there is no way to to get exchangeability of digital bearer securities into book-entry assets without a genuine, fully regulated trustee/custodial bank, which, in my opinion, is why we don't have internet digital bearer settlement today.

The holders of the blind signature patent, and other protocol inventors, have a hard time understanding this. DigiCash, as the canonical example, will only license their patent to a single bank in a single country, and not to any one else, forcing the trustee and underwriter to be the same entity, creating a very brittle and not very robust network of financial entities. The result has been market failure, for the most part. Having a competitive, many-to-many, underwriter/trustee market system fixes that problem completely, as we'll see in a bit.

Inventors and developers

For all intents and purposes, the consumer, merchant, underwriter and trustee are really all the financial entities necessary in a market for a digital bearer instrument.

There are other entities required to make this work, of course. There are developers of the software for that market and, most important, the inventors of the financial cryptography protocols, like David Chaum, Mark Manasse, Stephan Brands, Ron Rivest or Ian Goldberg.

Developers can either sell their software directly to customers or merchants, or they can sell servers to the underwriters and the underwriters can give away clients to their users.

Inventors can license their protocol to the market as a whole through the trustee. This way, trustees can take royalties out of a percentage of the under-

writers' interest earnings on the reserve account, or from the fees charged when some other asset is converted into the bearer instrument in question, or some combination of both.

With book-entry or bearer-collateralised trustees, this rewards innovation cheaply and easily. You don't even need patents to do it. Even with bearer-collateralised trustees, the inventor of the protocol still gets paid, no matter who or where he is. This, among other things, is part of the judge role I was talking about above. The trustee, who's in business to be fair and impartial, loses reputation capital otherwise.

A market for digital cash

The consumer buys, from a software developer, or is given, by an underwriter, a wallet: a client application which allows the storage and disbursement of digital bearer certificates. Wallets will probably be specific to the cash-protocol used, and not to the underwriter using the protocol.

With a wallet installed, maybe as a browser plug-in, the consumer goes to the underwriter's secure web page. The consumer enters, either by swiping a card or emitting stored information on her hard drive, the account and PIN number for her bank account just like she would at an ATM. The consumer's account information is probably blinded, so that not even the underwriter, or even the trustee, sees it as it goes through the trustee and onto the ATM network for authorisation.

The consumer's bank sends an authorisation message back to the trustee, who notifies the underwriter of the reserve account change, who in turn disburses digital cash certificates to the customer in the amount of her request. With the exception of the issuance of digital bearer cash instead of paper cash, this is roughly what happens with a private ATM machine.

This is all done for whatever fee the underwriter charges, in the same way traveller's checks are sold at a premium at the time of sale, or that a foreign ATM machine charges for non-customer transactions. In fact, redeeming it off the net at par like a traveller's cheque, and exchanging it free for other digital bearer cash online is probably fundamental for merchant acceptance.

Purchases on the net

The consumer then uses the new cash to buy something from a merchant on the net. In theory, a merchant could do offline transactions, without involving a direct exchange and replacement of certificates from the underwriter, but they're ridiculously insecure from the standpoint of double spending.

This exchange of certificates, this printing of new certificates at the time of each transaction, is still orders of magnitude cheaper than book-entry payment methods, and, since it's blinded by cryptographic protocol, the transaction retains its bearer quality. That is, the asset changes hands anonymously (on the net at least), it exists in only one place at one time, and the only proof required for non-repudiation is the certificate itself. Just like dollar bills, only three orders of magnitude cheaper than an internet debit or a credit card transaction.

With the transaction over, the merchant can instantly spend his newly minted cash certificate somewhere else, this time for free, because the longer it stays on the net, the more interest it earns in the underwriter's reserve account, all at minimal cost to the underwriter.

Or, the merchant can turn around and redeem the certificate at par through the underwriter, who in turn has the trustee clear the money through the ATM system to the merchant's bank in the exact reverse of the process which got the money onto the net in the first place.

Notice, for the first time, it is technically possible to use the ATM system for a cash deposit from a foreign bank, in this case, from the trustee, on behalf of the underwriter, to the merchant's bank account. Finally, notice that, since the wallets will probably be free, anyone can get paid in cash over the internet. They only need a bank account to put money on the net or take it off, important in the early stages, but not nearly so as time goes on.

Observations on this market model

It should be obvious by now that we're looking at a classic case of Metcalfe's Law. The more entities there are in this market's network the more robust and valuable it is.

The model gives us a many-to-many universe of interdependent underwriters, trustees, software developers and protocols, all in competition with their peers to offer the best price, collateral, reputation, quality of execution, and so on. The idea is to create a ubiquitous geodesic capital market composed of efficient, instantaneously cash-settled auctions of fungible, non-branded, risk-graded, digital bearer financial instruments.

The other thing the model creates is something I call microintermediation. Because of the information processing diseconomies of scale in Moore's law, we have lots of small, automated financial intermediaries, each one operating directly between a given buyer and seller. This, I believe, is the logical outcome of financial disintermediation, which, until now, has been about removing multiple intermediaries between a buyer and seller. As we're starting to see in the internet search engine market, we'll start to see a speciation of financial intermediaries, by financial instrument, risk, etcetera, all brought about by Moore's law. After all, no single processor in a geodesic network can handle all the traffic.

Note also that everyone who puts money on to the net or takes it off is identified to the complete satisfaction of government regulators everywhere. Digital bearer cash is treated just like physical cash in the eyes of regulators, and is subject to the same regulations. There is no functional difference between a digital cash underwriter and an ATM machine. And, yet, on the net itself, transactions are perfectly anonymous.

This is the ultimate paradox of digital bearer settlement. The transaction protocols are so strong cryptographically that you don't need identity to keep your trades from breaking. More to the point, you don't even need biometric identity to prevent fraud. A digital signature is persistent enough to actually attach a reputation to.

We'll talk more about this, and about digital bearer bonds, next month.

Robert Hettinga is the CEO of the Shipwright Development Corporation, in Boston MA
Email: rah@shipwright.com

IN BRIEF

Legal and General mortgage plan

Legal & General's first internet-based offering, Flexible Reserve Mortgage InterPlan, has attracted around 23% of its customer base since its launch in November 1997 according to Neeta Patel, head of the emerging media unit. Figures from L&G show that Flexible Reserve customers are using the online service on average three times a month to increase monthly payments and transfer money.
www.LandG.com

‘All the bonds in Christendom’: Digital Bearer Bonds

by Robert Hettinga

If you read the last instalment of The Geodesic Market, you now know how to put digital bearer cash on to the net. Of course, you can put every type of financial instrument into digital bearer form, and this month we’re going to look at debt, which is the simplest extension of the cash model I showed you last time.

Of course, to issue debt, the borrower (or any other market actor, of course, except secondary buyers and sellers) needs a good reputation, and we’re going to talk about that first.

With much fanfare, I now trot out my favourite quote from J Pierpoint Morgan, the last major denizen of the bearer-settled financial universe.

At the time he uttered this pearl of financial wisdom, Morgan was more or less on his deathbed, and was literally hauled in front of the US Congress to testify before he died.

So, imagine yourself there, in a congressional committee-room in 1913, (one year after 1912, the year libertarian columnist Vin Suprynowicz says was the high water mark in American liberty) and there you are, looking at the only man in history to refill Fort Knox with the proceeds of a typically-oversubscribed European bond issue on the strength of his signature alone, after this very same Congress had spent that treasury empty in the first place.

A man who single-handedly stopped several bank panics, one of them by while playing solitaire in one room of the Morgan Library, with a roomful of bank presidents arguing in the room across the hall, shuttling occasional proposals to him for his hoped-for approval over the course of a few days, all while Wall Street held its breath.

A very old man, now. An old man, being commanded, upon contempt of the best Congress money could ever buy before or since, to tell them the ultimate secret of banking. The most important thing a banker had to have to succeed.

Is it the right, um, ‘family background?’ they seem to ask this paradigm of New England WASPiness. The right school tie? Never mind that Morgan was tutored for the most part. The right secret society membership? Of course, Morgan wasn’t much of a joiner, except that he ran the board of trustees of his church, and that of the Metropolitan Museum of Art, like he did the rest of his enterprises, with an iron fist.

Morgan just scowls at them. His answer is very simple:

‘Character.’

Our would-be congressional inquisitor was probably dumbstruck. He was surely some loutish turn-of-the-twentieth-century urban machine politician, or maybe a rural silver-shoes-on-yellow-goldbrick-road bimetal free-silver populist in extreme Dorothy-Gone-to-Oz Mode.

Whatever he was, he was almost certainly hoping for a financial conspiracy story of Bilderburg proportions to put into the next day’s muckraking headlines. And, I bet, this modern Torquemada couldn’t believe his ears.

‘Character?’, he sputters. Like he’d never heard the word before.

Morgan puffs himself up to his full 5-foot-rotund-something, gives the man one of those famous withering glares over a rosacea-mangled nose.

‘Sir, I wouldn’t buy anything from a man with no character if he offered me all the bonds in Christendom.’

Parsing that language to account for, um, ‘late nineteenth-century Episcopalian sexism’, we get as clear a definition of the enforcement power of reputation as has ever been stated this side of ‘Caveat Emptor’.

In other words, if you lie, I don’t do business with you again. Ever.

And, in the world Morgan found himself in, that kind of financial shunning was pretty much all anyone really could do.

It was really ever thus, throughout the history of money, much less finance. Sure, you could go to your friendly local force monopoly, be they monarchical, tyrannical, empirical (in the manner of Napoleon, not Hume), or oligarchal (or, even, democratic, on extremely rare occasions), and you could try to get them to beat up someone who ripped you off. But, usually, that was way too much work. Said regional force monopoly had to actually find this person, and then apprehend, try and convict him, and, frankly, more likely than not, he’s changed his name and venue and spent the cash you paid him for those bogus bearer bonds you’re now holding, and, well, so sorry, sir, but them’s the breaks.

And so, to sanitise and paraphrase the immortal Bluto Blutarski of ‘Animal House’ fame, it was actually you who screwed up: you trusted this brigand to begin with. You believed he had character, a good reputation, in other words, and it turned out that he didn’t, at all.

This was true up to and including J Pierpoint Morgan’s day, where, although you could use a telegraph to execute a trade on the New York Stock Exchange floor, you still had to bring in actual paper and swap it for some other actual paper to clear and settle the trade.

Yet, oddly enough, reputation sanction, plain old fashioned shunning, worked just fine for over 5,000 years. Marvellously well, in fact.

Though, we now know what happened to J Pierpoint Morgan’s tidy little financial universe of men with good character. Tabulators and comptometers begat computers, and, next thing we know, we’re all using wires and computers to move accounting entries around, my debits for your credits, and bang, financial transactions execute, clear and settle more or less electronically, modulo a tape swap and a batch job or two.

And, now, all I need to buy something over the internet is to give you a credit card account to take the money out of, and, maybe, but not necessarily, a cryptographic authentication (obviously, I hate the current misuse of ‘signature’, much less ‘certificate’) to prove that it was I who told you where the account

(Continued on page 12)

IN BRIEF

Intuit to give software to poor
Intuit, the maker of Quicken and TurboTax, is establishing the Quicken Tax Freedom Project, a program to donate web-based online tax preparation and electronic tax filing to lower income families and individuals.

Intuit expands card insurance
Intuit's personal insurance web site, QuickenInsure Market, has signed an agreement with AutoConnect, a second-hand car service, to provide real-time car insurance quotes, policies and information to shoppers.

(Continued from page 11)
with the money in it was.

Yet, there's a little problem with book entry settlement and clearing, and it involves that force monopoly I was talking about.

When we have to make copies of our transactions and give them to a 'trusted' third party to keep us from lying to each other, that's pretty awful, and not only from the standpoint of simple privacy.

More important, there's something particularly insidious to freedom itself about just shoving around debits and credits, instead of physical objects, or, now, digital objects, when you pay for things or convert one asset into another.

With book entry settlement, you have to keep a virtually perpetual audit trail, so that on a 'syntactic' level, you can prove the trade happened some indeterminant date in the future, and so you can prevent the other party from denying (that famous legal double-negative, 'non-repudiation') the trade ever took place. And, once you've done that, it's real easy to use those records to call a cop and send that person to jail. Actually, you're forced to, for any of a number of reasons, not the least because the clearing/settlement lag is such that someone might have absconded before you knew what happened to your money, and giving the clearing house physical enforcement capabilities in meatspace would make cause undue competitive pressure on the sovereign's monopoly on force.

Now you can see why book-entry transaction settlement requires very strict biometric identification for anyone who changes the book-entries themselves, or even those who order book-entries to be changed. Everyone else (us customers, in other words) must deposit in advance of any significant financial activity, as sort of hostage capital to whatever transactions we execute.

Everyone under the jurisdiction of the SEC has their fingerprints on file, for a reason, not to mention their current name and address. Enough information to drive a totalitarian tyranny through, frankly.

And, so, the real reason governments have grown to control such an increasingly huge part of our lives, through book-entry taxes (sales, VAT, capital gains, income) and regulation (think of a regulation which doesn't eventually rely on transaction audit trails), is because, we require government intervention in our economic processes, our very transactions themselves, or those selfsame transactions wouldn't occur at all. Book-entry settlement and the ad baculum argument at the core of the very idea of the modern industrial nation-state are intimately related. A tax on income is easy to enforce because you need force to make the income transactions execute to begin with. One hand washes the other. Pay packets with paper cash cost too much to handle when you can just issue cheques for people to deposit into mainframe-enabled chequing accounts.

Seen from a network perspective, a book-entry transaction is about shoving a very insecure piece of data, a positive or negative integer, a debit or credit, down a very secure pipe. And, to get access to that pipe, you have to be physically, um, obtainable, to law enforcement at any point in time before, during, and after the fact, should you lie about it.

With digital bearer settlement, we have turned that last paragraph completely on its head. With a blind signature cryptographic protocol, for instance, we can send a secure transaction, a strongly encrypted and cryptographically authenticated token (a digital bearer certificate, if you will), down an insecure pipe, the internet, in other words, and with the right software, that's the end of the transaction.

We don't need biometrically authenticated access control to a proprietary secure network in order to shove an inherently insecure book entry back and forth out of someone's database of transactions and, by extension, their chart of accounts. We actually don't need to keep audit trails at all anymore, much less for years at at time, and, more dramatically, we don't even need cops to hunt down miscreants who 'break' our trades, either in execution, settlement, or clearing.

Instead, with a simple exchange of digital bearer certificates, we can execute, clear, and settle the transaction all at once, and the cryptographic financial protocol, executed in software, simply won't operate unless all conditions are met for the transaction to occur.

Which, oddly enough, is exactly the way a physical bearer certificate works: I show up with my cash, you show up with your paper bonds, we agree on a price, we inspect and swap our various pieces of paper, and we walk away. I know the bonds are good by inspecting them, you know the cash is good by inspecting that, and, frankly, we don't care who each other is. Ever.

Now, with digital bearer certificates, we can do exactly the same thing on the net. That 'inspection' step now occurs when we test and redeem our cash or bond certificates with their issuers online, and, if the certificates can't be redeemed, the trade can't even execute.

It stops before it starts. Nobody gets burned, frankly, except the criminals who want to double spend the certificates. The only people who even need a reputation in the transaction itself are the issuers of the respective digital bearer certificates involved, and not the buyers and sellers of those certificates in the secondary markets.

And, of course, that 'reputation' we're talking about here is the past behaviour, on the net, of a public-private keypair used in the authentication and issuance of a given digital bearer certificate. Or in the sale of anything else, for that matter. Just by using the public key and the signature on the certificate, anyone in the market can validate that the certificate was issued by the entity issuing or underwriting it. And, in the course of a transaction, as we said, the issuer itself can validate the 'semantic' part of the transaction, that the certificate is in fact unique and exchangeable at no cost for another unique set of bits representing the same value.

So, a digital bearer certificate is authenticated by the issuer of that certificate, in the same way that the intaglio printing, special paper, serial numbers and signatures on a given paper bearer bond make it unique and non-replicable.

That makes not only for a more secure, and completely private, transaction, but it also makes for a radically cheaper transaction, which is really the whole point. As we all know by now, the reason we have book-entry settlement to begin with is because it's radically cheaper than the physical delivery of paper bearer certificates, not so the government, or anyone else, can surveil us in our very grocery purchases.

On the net, we talk about accumulating and quantifying reputation in some imaginary future denomination and we call that stuff 'reputation capital'. Which immediately leads to the cypherpunk inside-joke about permanent shunning being 'reputation capital punishment'. And, actually, that's pretty understandable. Instead of going off to San Francisco in the 1850's to change your name and venue after screwing up, you just delete your private/public key pair, and start a new reputation over from scratch. In a bearer settled world, of course, it happened all the time.

I expect, like corporations today, reputations will be sold, and the variance between the market value of the assets controlled by that reputation, and the market value of the reputation itself will be our imaginary reputation 'capital', something we call 'goodwill' today.

Now, to quote Bill Cosby, 'I told you that story to tell you this one.'

With digital bearer settlement, and the sanction of reputation against public keys which have bad character, as Morgan called it (reputation, to you and me) it is now possible to create digital bearer bonds.

Actually, last time, in my underwriting model for digital cash, I cheated. When you think about it, a bank note, cash in other words, is an instantly callable, perpetually issued bond which pays no interest. It represents a claim, in the old days, at least, on some principal amount of a given debt, and not its interest, redeemable upon demand in the asset the note is reserved against and denominated in.

So, to issue a digital bearer bond with a simple coupon, you just issue a digital bearer certificate for the principal amount, redeemable at the end of the life of the bond, and you bundle a bunch of coupons with that certificate for the redemption of principal, one for each interest period, and redeemable at the end of that interest period, and sell them all together as a unit.

To do a zero-coupon bond, simply issue a certificate payable at expiration and sell it for the net present value of that amount given some fixed interest rate.

Strips are just that. Strip the coupon certificates from the principal one and sell them all as individual certificates with their own prices. Notice that we bump into the old fixed income analysis chestnut about a bond being a series of options on cash flow, which, of course, I'll muck around with a bit more, when we get to derivatives.

Convertible bonds should be redeemable either in cash or stock. Bearer stock, of course, which we'll talk about next time.

Money market instruments, for the most part, are just bonds with extremely short lifespans.

It's even conceivable to have microbonds, issued by individuals. After all, the size of an individual underwriter, and the resulting syndicates of underwriters, to boot, is probably completely driven by Moore's law. I joked in Wired a few years ago about a syndicate of microbond 'bots' loaning me the money for lunch, payable at the end of the month.

If you can have microbonds, macrobonds are also possible. I expect that digital bearer settlement will be a universal phenomenon, just like book-entry settlement is today.

Secured bonds, like equipment mortgage bonds, can use various trusted entities to validate the worth of the assets securing the bond, just like a trustee/custodian does for a bond or cash issue.

And, of course, you can add all kinds of call provisions, redemption exclusions, and anything else you can think of, to a digital bearer bond, only this time, you're writing software, and not law, as the old cypherpunk mantra goes.

Finally, any of the above bonds will be rated, just like bonds are today, yielding the same market we have now, with fungible graded commodities, in perfect competition, only, now the velocity of those markets can be greatly accelerated. After all, you are executing, settling, and clearing, instantly, and for cash.

Notice several things here. First, the language of bearer settlement completely underlays our very discussion of bonds even today. The word 'coupon', for interest, 'holding' a bond, all of that. Digital bearer settlement makes it that more relevant. Back to the future, and all that. It says to me that we're not going to have too much conceptual trouble thinking about a world of digital bearer settlement, which is one of the principal attractions, besides reducing transaction cost by three orders of magnitude, of course.

Second, and probably more important, by creating actual digital financial objects, objects which make electrons behave in certain ways online, just like the mouseprint covering those huge paper bearer bonds of yore caused lawyers and judges to behave in certain ways in meatspace, you have freed finance from a huge chunk of legal cycle-time itself, and you get a genuine financial ecology on the net, on top of that geodesic economy I talk so much about. In fact, most of the time it seems to me that they're part of the same thing. The geodesic network being the substrate upon which this bestiary of financial entities and objects are born, live, and die. It gets worse when I talk about the idea of 'micromoney mitochondria' at the end of this series, but I'll soften you up a bit before we get that far out over the edge of the cliff, into cartoon physics, as it were.

Anyway, in this new financial ecosystem, financial theory and practice become one and the same thing, the behaviour of financial software and digital bearer objects on a ubiquitous global internetwork. It may be that, after years of using mathematics and physical analogs to describe financial economics, the ultimate anathema to mathematical finance will occur, and finance will become an observational science again.

Frankly, I think we're looking at some combination of the two, where mathematical finance will propose, and the genetic behaviour of the market will dispose. Which, when you think about it, is exactly what happens today.

Back to the future, and all that.

Next month, we'll talk about digital bearer stock, and, implicit in that, how to achieve limited liability in 'cypherspace'.

Robert Hettinga is the CEO of Philodox, in Boston MA
Email: rah@philodox.com

IN BRIEF

Ecommerce to boom in India
Electronic commerce in India will climb sharply to $160 million by calendar 2001 from a negligible $2.8 million in 1997, market research firm International Data Corporation said. 'Our research shows that electronic commerce in India is largely between businesses and consumers, and not business to business,' said Ravi Sangal, president of IDC India. He was speaking at India Internet World '98, a four-day conference and exhibition.

Russell's Revenge: Digital Bearer Equity

by Robert Hettinga

Since law attempts to be as logical as possible, and software is nothing but mathematics, I'm about to show you how to turn common law, or some of it, anyway, into software. We're going to do it all, of course, by talking about digital bearer equity.

One of my favourite people in philosophical history is Bertrand Russell. Most people familiar with the history of computational logic know that not only did Russell discover a paradox that eventually undermined the foundations of logic when Goedel solved it a few decades later, that consistent systems could never be complete and complete systems could never be consistent, but also that Russell and his partner Alfred North Whitehead quite literally broke their brains proving, logically, that 1+1 was 2 using symbolic logic alone, unifying maths and logic for the first time.

The idea of joint control of an enterprise is as old as western civilisation. Before the time of the Greeks, hierarchy and property rights had gotten so evolved that everyone belonged to someone else. Ministers of the pharaohs used to routinely sign their correspondence to their superiors, 'Your Slave'. Hydraulic monopoly has a weird effect on people that way. Certainly the Chinese, Brahmins, and, to a lesser degree, the Mesopotamians, refined hierarchical lifetime control of their subjects to a fine art.

It's questionable whether the Greeks were the sole inventors of democracy, small hunter-gatherer bands like the Australian aborigines had a more egalitarian society than most larger agricultural societies, for instance. Nonetheless, the Greeks are certainly the people we like to remember as the originators of the practice of voting as a 'protocol' for group decision-making. Especially since they actually had agriculture and actually kept written records of the votes they took.

The Roman republic, literally, 're publica', the public thing, abstracted direct voting up one level by electing representatives who in turn did the actual voting, proxies, if you will. This allowed a much greater span of control than a simple city state, Delian League or not. First 'pecunia', then 're publica'. Those Romans got to invent all the fun words, didn't they?

Notice that neither democracies or republics are necessarily stable or even representative. Greece and Rome, or any of their early modern replicas including the one I'm fond of, excluded most of their populations from actual voting control, but, as communication technology and industrial requirements for education increased in prevalence, suffrage tended to become universal, and, ironically, slavery itself has been shown to be a peculiarly agricultural institution, all of Marx's protestations to the contrary.

Another way to think about it comes from an old college logic professor of mine. We all have the same information and intelligence, and the future is uncertain, so we might as well vote about what to do next.

Of course, joint ownership is not new either, and neither is proportional voting control of businesses, or anything else. The corporation, peculiar this time to industrialism and the modern nation-state, has direct antecedents in other common-law business forms not requiring the force of that nation-state for their very existence, something important to anyone trying to code up erst-corporate behaviour in software instead of law.

You don't even need the legal sanction of a nation state to have limited liability. Common law created limited partnership long before corporations. Britain had fully functioning non-corporate limited liability entities at least until the end of the nineteenth century. Lloyds not withstanding, of course.

So, the point is, can you make all this fun stuff happen in software?

Let's look at the cryptography for a bit. For starters, you can store multiple 'hashes' of the same data in such a fashion that with any m of n pieces, you can reconstruct the whole dataset. That is useful for storing, say, your digital bearer bonds, in various blinded cryptographic storage areas all over the net, for a fee of course, but it also provides a pointer to controlling a business entity as well.

Why? Remember that 'identity' directly maps to 'key-pair' in cypherspace. With an m-of-n reconstruction scheme, any m members of a board could vote to control the 'root' key of a virtual corporation, for instance, you could actually control that key. There's considerable doubt whether hierarchies make sense in this context at all. In fact, most global name-space schemes based on key-management hierarchies bump right into Russell's Paradox and Goedel's Result as if their designers never took logic at all.

Anyway, this form of m-of-n key-control works best for simple partnerships, but you still have the problem of voting control of larger entities, particularly if you want lots of shareholders. Fortunately, there are cryptographic protocols for anonymous voting, as well. I'll spare you the gory cryptographic details, but there are ways to elect a board, and for boards to vote control of a key, which can then be used to authenticate the actions of as large a business entity that you want. The creation of voting proxies, in other words.

So, we've taken care of common stock, and, because we know about digital bearer bonds, we can get a hint about how to do dividends: just present some token at the time of the dividend and collect cash. But, what kind of token do we use when all we have is a stock certificate? Clearly we don't want to redeem that at dividend time, do we?

No, we don't have to. There is yet another class of cryptographic protocol called, weirdly enough, zero-knowledge proofs of knowledge. Using these methods, it is possible to hash a given bit of information and use that hash to prove to someone that you have

(continued on page 14)

IN BRIEF

Wells Fargo pilots smart card on net
A group of Wells Fargo employees are taking part in a new smart card pilot in which participants log onto the internet, transfer funds from their banking accounts on to their Mondex cards and use their cards to shop online. Wells Fargo allowed customers to load cash on to the Mondex cards over the internet last April. It is now working to sign up merchants. Pilot merchants include www.greeting-card.com, and www.ticketweb.com.

New Jersey plans smart cards for drivers

New Jersey plans to issue smart cards to its nearly six million drivers in a scheme dubbed AccessNJ. The plan also envisions the possible addition of other government applications, such as electronic benefits, firearms permitting, as well as possible private sector applications, such as electronic purses..

(continued from page 13)

that information in its entirety. No, it's not magic, it's mathematics. Using zero knowledge proofs on a stock certificate, you can prove not only that you are entitled to vote, but that you are entitled to collect dividends as well. In fact, you can use it to prove that you are a preferred stockholder, or that you are a holder of Class B instead of A, or anything else. Finally, the issuer can use these proofs to show that you have already collected a dividend, voted a stock, whatever.

Oh. One other thing. Want to authenticate the books of a corporation for a given price earnings ratio without seeing the entire set? Want to authenticate an actual cashflow or asset holding for a debtor? Use the same zero-knowledge proof cryptography. Eric Hughes even claims to have invented a way to publish completely 'open', publicly available files, cryptographically munged, of course, which, when, a business entity wanted to prove a certain figure or set of line-items was in that otherwise encrypted information, they could use their unique key pair and a zero knowledge proof to show that the expenditure was in fact there. This could even be audited by a trusted third party, whose signature would be on the encrypted data. It just keeps getting weirder.

Frankly, the reason we don't use zero knowledge proofs for bond payments is because bonds have finite duration. They all, with one exception proving the financial rule called a 'perpetuity', expire sooner or later. It'll probably be cheaper to just issue all the digital bearer certificates, principal and interest, en masse. It'll certainly be more financially reasonable from the standpoint of calculating the value of those certificates, as any student of fixed income mathematics will tell you. Simply issue all the certificates at once, and let them each be priced, and traded, accordingly.

But getting back to equity, what about limited liability? Well, think about this for a minute. If, for instance, you have anonymous control of information, then the only thing you can do to the holder of that information in any meaningful sense is to discount the value of that information in the market. Remember, when we talked about reputation, we talked about reputation 'capital punishment', where a given cryptographic key pair is shunned, its economic value effectively zero.

These days we do it with laws which say that a shareholder of a corporation is only liable for whatever money he invested into it, and, when the market says a stock is worthless, there isn't anything such thing as negative value.

But, again, in cypherspace, we try to replace law with strong cryptographic software, and, most of the time, we get the same result. Funny how symbolic logic works that way. Call it Russell's revenge.

In other words, if a shareholder spends money on a digital bearer certificate signifying partial ownership in an enterprise, and that bearer certificate, for whatever reason, is worth nothing, that's all the shareholder has lost. Since he's holding a certificate normally, his key is completely blinded, and he is thus anonymous. Only if he double spends the certificate is he unmasked. So, on a 'semantic' level, there's no other 'recourse' the market has but to the value of the equity certificates he holds. And, as any person who's holding shares of a fraudulently accounted company can tell you, that penalty is a good enough proxy for limited liability.

Issuing digital bearer equity, or debt and cash, of course, is different, in that the key issuing the certificate must be known to have a good reputation, and have proven asset value in the case of collateralised debt. The holders of the certificates, though, don't need to be known at all for the system to work.

Pretty cool, huh? With digital bearer equity, you can have publicly held business entities whose size limits are only driven by transaction cost, just as Coase's theorem says it should be, and, the shareholders can be completely anonymous.

And, of course, as we all know by now, I claim, at least three times before breakfast every day, that digital bearer settlement will drop transaction costs by at least three orders of magnitude, which is why you have anonymous shareholders, and not though any desire for privacy per se. The reason we have registered stock ownership, remember, is because we have book-entry settlement. If we could do digital bearer settled equity, there would be no need to register securities from an economic standpoint, and, as I'm also fond of saying, physics begets economics, which begets common law, which begets legislation and 'policy'. You cannot run the causation movie backwards and get any money.

So, no, I don't think that absolute deregulation of equities markets will be the only component of that cost reduction, though it may one of the most interesting effects of that cost reduction, no matter what its magnitude.

Next time, we'll talk about digital bearer derivatives, but, after that, we'll come back to equity, and Coase's Theorem, and talk about micromoney, and its impact on the size of the firm. Stay tuned.

Robert Hettinga is the CEO of Philodox, in Boston MA
Email: rah@philodox.com

E-Finance Forum 7pm Monday 23rd November, London Business School
Sussex Place, Regent's Park, London NW1 4SA

Speaker: Robert Hettinga will explain how new financial technology will allow digital cash, digital stock certificates and digital bearer bonds to replace the existing payments and clearing and settlement infrastructure, allow dispersed stock trading on multiple exchanges, reduce costs and improve market security.

The talk will last for approximately 45 minutes, followed by questions, discussion and a reception with the speaker in the Executive Common Room. Anyone can attend, but there is a £10 charge. Please register with Tracey Croft at the London Business School (tcroft@lbs.ac.uk), Alumni Office, Sussex Place, Regent's Park, London NW1 4SA.

Lycos buys Wired Digital
Cambridge, Mass based Lycos is buying Wired Digital ending Wired's ambitions to build an online property that leveraged the offline brand. Lycos boss Bob Davis is reported to have claimed that adding Wired Digital, in particular HotBot, would effectively give Lycos access to 40 percent of all Web traffic.

Digital bearer derivatives - mathematics of polite fiction

by Robert Hettinga

Digital bearer derivatives are possible and, at the margin, digital bearer settlement is probably the technology most suited for the execution, clearing and settlement of derivatives.

With the free-falling price of microprocessing, we're going to get more, and more complicated, derivatives, whether we want them or not, and, with ubiquitous internetworks, they're going to be digital bearer derivatives, because that's going to be the cheapest way to do them.

So, before we start, let's review my (and Russell's) mantra that reality starts with physics and economics and ends with law, 'policy', and philosophy. Trying to legislate economics and finance, for instance, is one of the sillier things any sovereign, much less any religion, can do.

I say religion here because, at some point in Christian theology, probably in deference to the Temple money-changing episode, interest was declared immoral, and, from that now-curious beginning, we get modern derivative transactions.

Christian monarchs, in trying to outlaw interest, found that, no matter how hard they tried, they just couldn't, really. Eventually, in the late middle ages, they let religious undesirables, like Jews, be the money lenders and charge interest, but only after a ridiculous amount of creative denial.

Muslim countries still outlaw interest today, for instance, and they go through an amazing amount of gyrations to keep their banks in business as a result. But, as Joe McCarthy used to say about communism, no one in, say, Saudi Arabia, dare call it 'interest', even today.

Nonetheless, buried, deep in the glosses, palimpsests and marginalia, among all the shucks and jives that mediaeval sovereigns did to avoid the 'i' word, were some very interesting residents of the then-hand-illuminated financial bestiary. These critters really did look an awful lot like bonds, and, even, derivatives. Of course, they couldn't possibly be those unholy chimera, because they would be, quite literally, an abomination, a sin unto God Himself.

Yet, in England, for instance, there was the ever-ubiquitous tally-stick, which started out being a poor man's depository receipt for taxes, with big notches for big money, and small notches for small, and split between the two counterparties to keep everyone honest. These sticks ended up, in rather short order, representing 'fictitious' transactions, and, more important, contingent claims, on some other asset, usually, bullion. The king would, instead of paying creditors in gold, pay them with tally-sticks, which would then 'mature' sometime later at the time of the bullion's eventual arrival in the treasury. These discounts were, of course, representing the, um, opportunity cost, of the money involved. Certainly not interest. That would be evil, of course.

In fact, the considerable fortunes of the Knights Templar, and Hospitalar, too, were built on bills of exchange, issued to crusading nobility, who could, magically, deposit money in one place in Europe, and take it out of somewhere else upon their arrival in the Holy Land. 'Of course, Sire. Interest would be a sin. We can, however, sell you this bill of exchange at a discount, if you would should desire it...'

You can account for a multitude of risks, if not sins, in the discounted price of that bill of exchange, including the obvious one of said Sovereign getting lost, bill and all, at sea on occasion.

Not to mention creating bills of exchange for assets which never leave a country at all, thus avoiding taxes, even for the sovereign, at least in countries like England where the sovereign was accountable, even marginally, to the law. Bills of exchange were even created representing assets which might never exist, except if some contingency occurred. Guess what **those** were?

Of course, most reasonably clueful bond folks will gladly haul out a trusty Fabozzi book or two and show you that, yes, a bond is, in fact, an option on some future cashflow that the bond promises, or, more precisely, that a bond is a **bundle** of options (interest coupons, remember?) on that future cashflow, the granularity of the option's settlement date being either every quarter, if you feel discrete, or infinite, if you feel continuous and remember that most bonds are quite liquid assets. And this tide of financial calculus floats all boats, even a crusader's fleet mired in the middle ages, modulo the occasional Mediterranean storm.

So, just like quarks, it seems that options and other derivatives are the very conceptual building blocks of the financial universe, and to ignore or restrict them is to do so at one's own economic peril, if not one's mortal soul.

Thought about in those terms, of course, derivatives become as old as civilisation itself. Thales of Meletes (who was the world's first philosopher if you're in a medieval mood, and believe in the infallibility of Aristotle), answered the world's oldest taunt, 'if you're so smart, how come you aren't rich', by cornering the local olive oil-pressing futures market, monopolising those presses at harvest time. It not only made him rich, but famous, too, especially to everyone who's taken the nickel tour at the Chicago Board of Trade and walked away dreaming of being latter-day Hunt Brothers. Doing that ill-fated silver corner **right**, of course...

Even before Hellenic Asia Minor, the owners of various grain depositories in Egypt, and even Babylon, raked it in one haircut at a time, purchasing grain before it was even planted, and flipping that imaginary grain, over and over again, until the harvest actually came in.

This kept people from dumping grain in the streets at harvest time, certainly, because the prices were too low then, which is exactly the apocryphal event precipitating modern futures exchanges in places like Chicago, sans hydraulic monopoly. Those who forget history, and so forth.

At the root of every derivative is a polite, and frequently mathematical, fiction. A fiction, which, if it turns to real prophecy, makes money. And, if you've ever listened to any entrepreneur in heat

spouting his latest funding pitch, you'll notice that predictions are pretty cheap to make. Moreover, an awful lot of of those predictions exist about any one event at any one point in time. Putting a value on that vast quantity of fiction might have been worth a Nobel Prize to some people who should now know better than to hang out with the likes of Mr Merriwether, but, more important, the process is driven by supply and demand. The initial price of futures, options, and other contingent claims, relative to the assets they make claims on, are, like talk, cheap for the most part.

In addition, if the underlying asset of a class of contingent claims is volatile, it's a very good idea to settle and clear the purchase and sale of those claims as soon as possible, so people won't forget their sometimes large obligations, or can collect on their occasionally formidable returns. Which, oddly enough, is exactly what happens at options exchanges all over the world. Chicago, for instance, now has next day settlement, if I remember, and the trend has been towards even shorter settlement times, wherever possible.

And digital bearer transactions settle fastest and cheapest.

We need to look at something else about a derivative. All those conditions under which the contingent claim will be executed make things **very** complicated. You simply cannot have a modern derivative without computers and online real-time information. You need even more computational horsepower to model the damn things to see if they do what you want them to.

This complexity, and the corresponding computational modelling requirements, has always been seen to be a bug. It's really a feature, though. The more you automate the process the better it works, and now, it can be automated up to and including settlement, scaring the wits out even the hardiest of souls.

Already I can hear quite a few disgusted 'harumphs' out there, particularly from those of you who have seen formerly boring equity exchanges go limit-down like some CBOT pork-belly pit. You've seen 'portfolio insurance' contracts blow up like so many World War I barrage balloons under the tracer bullets of illiquidity, causing markets to crash around the world.

More to the point, we've seen countless portfolio managers who claimed to be using derivatives, but who were doing nothing but speculation with large amounts of other people's money as if it were just another game of liar's poker.

So, what does digital bearer settlement bring to the party? For starters, increased automation, of course. You can build an actual **object**, which lives out there on the network all by itself, waiting for the proper market conditions to be met before it executes. Furthermore, because of those extremely reduced transaction costs, you can do transactions at extremely small sizes. Well, sizes considerably less than the hundred-million, or even billion, dollar transactions required to make institutional-scale money in derivatives today.

Because of this small transaction cost, you could actually create a bunch of micro-derivatives, set them loose, and see if they work. Nothing like small-scale working models to see what really works, certainly. You could even create, abomination of abominations, auto-mutating derivatives, following genetic algorithms, spawning slightly altered copies of themselves at settlement time with some of the proceeds. Fast, cheap, and out of control, indeed. It's enough to send you scurrying back to the monastery, sandals flying every which way...

Dragging us back to the human universe, with this kind of granularity you could also create a whole array of derivatives, representing a whole spectrum of possible positions, in smaller transaction sizes, allowing you much more flexibility in your financial plans. That's why derivatives exist, after all, to hedge your purchase or sale of something else against the unforeseen. At the expense of Godless speculators, of course.

But, the primary problem with modern derivatives is that nobody is there on the other side of a desired trade at crunch time. Nobody there in the specific volume desired, and so, most hedging transactions, like the limit orders they are, go unanswered until the price is much lower, defeating the purpose of the derivative in the first place. Being able to execute a score of smaller transactions, instead of one giant one, at some intermediate prices in an avalanche of continuously falling prices gives a portfolio manager at least some comfort of dollar-cost averaging on the way down. Frankly, I expect that it will tame volatility as a result. It is precisely these precipitous free-falls with no answering bid, which cause the volatility problem in the first place.

Oh. Right. Before I forget, the transactions are all anonymous, of course.

So, how do you do all this fun stuff? Well, if you couple some bit of autoexecutable code with a digital bearer instrument, or a bundle of digital bearer instruments, you can execute all the pricing, and other financial data, requirements you want. Certainly a bit of XML, or Java, done right and properly authenticated, could do the trick, but, like most problems in financial cryptography, that trick is usually harder than it looks.

Fortunately, what looks like an initial solution to the problem was presented at the 1998 International Conference on Financial Cryptography, FC98 to its friends, held this past February in Anguilla.

X-Cash, a new transaction protocol by Markus Jakobsson of Bell Labs and Ari Juels of RSA Labs, is a bundle of digital bearer instruments which look for the terms they want, and when those terms meet with an acceptable offer, they execute, clear, and settle the transaction, all at once. If you're interested in this paper, and a whole bunch of others on the cutting edge of Financial Cryptography, you might want to look at the conference's proceedings, which are now available from Springer-Verlag. See www.fc98.ai for details.

Of course, figuring out how, and doing it, are two entirely different things, and, frankly, X-Cash is only the first of what will necessarily be many attempts at solving the problem of autoexecutable, digitable bearer, derivatives.

It's the same problem financial cryptographers fight every day: the problem of turning law and legal agreement into something much better: running software. Turning law, and apparently, thrill-addiction, into economic, literally physical, objects.

Objects beyond the control of gamblers and, apparently, experts at liar's poker.

Robert Hettinga is the CEO of Philodox, in Boston MA Email: rah@philodox.com

IN BRIEF

Visa buys into CyberSource

Credit card giant Visa has made a 'significant' equity investment in credit card screening startup CyberSource. The CyberSource bypasses the SET protocol. Visa and CyberSource will now work together to build products that 'shield Web merchants and their banks from internet credit card fraud.' Both deny the investment signals a move away from SET, but analysts say they see it as a sign that adoption of the protocol has lost all momentum.

The Geodesic Market
by Robert Hettinga

One-Way Hash and Micromoney Mitochondria: Digital Bearer Micropayment

December 1, 1998

"When the going gets weird, the weird turn pro", as Hunter S. Thompson once said, and the going, for this article, is going to get pretty weird, and in hurry.

I've taken you from digital bearer cash, through bonds and equity, and, last month, we ended up with derivatives, showing you could get as weird as you wanted, financially, and still use digital bearer settlement technology to make transaction settlement cheaper to use than book-entry methods. Probably by several orders of magnitude, or a thousand times, cheaper.

Now we're going back to cash, microcash, to be exact, and, in the weird spirit of Mr. Thompson, we're going to talk not about Yage, or Ibogaine, or various reptilian pineal extracts, but about different kinds of hash.

Well, okay, not *hashish*, exactly. Hash*es*, actually. And not anything even vaguely psychochemical, though the consequences of hashes might get pseudobiological sooner than you might imagine, and simply mind-bending to contemplate when we get there.

The technology I'm talking about here is that venerated mathematical algorithm and staple of computer science, the hash function.

A hash function is something they teach you in your first year of computer science. Properly defined, a hash is a usually smaller, mechanically derived, fixed-length sample, subset, or just plain correlated bunch of bits related to usually a larger, and variable-length, bunch of other bits. A hash is something that allows you to mechanically check the integrity of data without actually examining the data itself. I can send you a hash of some computer program I've written, so that you can run a hash of your copy, compare the hash you have to the hash I gave you, and, if they're identical, it's highly unlikely that your copy is different than mine.

It's that "highly unlikely" bit that's important, here. For instance, if I hash a given bit of information and the result is 2^128 bits in size, and the hash method is a one-way function which gives me a more or less random output, I have a 1 in 2^128 chance of getting the same hash from some other bunch of data. Nice large number, that. Longer than the number of seconds the universe has been alive, even. Longer the total age of the universe if Mr. Hawking, and, more recently, experimental data, were both wrong and the universe is in fact closed.

However, like all large numbers, including infinity, you can control

those, um, astronomical probabilities if you want, and that control is at the heart of micromoney.

If you reduce the output size of a one-way random hash function which uses a key (a "cryptographic" hash, in other words) you can control how much computation (money, in other words) is spent in the generation of a hash "collision", which is the name for happens when two entirely different blobs of data generate exactly the same hash value. Finally, if you use the right kind of hash function this way, and you find a hash collision, you can use that information to generate as many collisions like it as you want, with very little extra computation at all. Each one of those hashes are as hard to forge as the first one is.

What you get is exactly the economics of minting a penny, only with bits, which are much cheaper to mint with. To mint a penny you have to literally build a factory, because that's what a modern mint really is. But, the next penny after the first one is barely noticible in terms of marginal cost, and, so, it behooves you to mint as many pennies as possible to earn back the investment in your mint. That is, if you were selling pennies for a living, which governments claim they really don't do, though they book it on their balance sheets as seignorage income, nonetheless...

Using hash collisions, as found in various the various micromoney algorithms out there including MicroMint from Ron Rivest and it's several progeny, and in Millicent by Mark Manasse, and in HashCash, a simple anti-spam protocol by Adam Back, that's exactly what you can do. You can take in people's money in one form or another and quite literally print them a positively huge amount of extremely low-value cryptographic hash-collision tokens, all while still turning a tidy profit. Seignorage for the rest of us, to paraphrase Mr. Jobs.

The disparity in cost between the cost of "minting" the first token and minting the second is enormous, much greater than that required to mint the second penny in our example above. Remember, again, how long it takes to "brute-force" a hash-string the size of 16 bytes, the size of this one: "1234567812345678". That is, 128 bits divided by 8 bits per byte.

Those 16 bytes, if handled properly, are certainly small enough to stick onto the most mundane events in cyberspace and pay directly for some service at the time it's rendered. All without an invoice, or clearing a check, or authenticating a credit card. and, without, of course, the finance and accounting departments backing them up.

You can use those 16 bytes to pay for sending a piece of email. Or downloading a web page. Or, even, with enough 18-month turns of Moore's law and a stiff tailwind, routing a group of packets from here to there across the net.

Imagine every router on the net buying bandwith low and selling it high in a continuous, digital-bearer, microcash-settled, cash-on-the-routerhead auction for internet switching. In such a world, you don't even need network engineering, at least as we've

defined it today, because the market, and not some grand top-down design, will determine where the next router will go, without any human intervention in the purchase at all.

...Good. I see you've drunk the Electric Kool-Aid, and the visuals are just starting to kick in. Great stuff, huh? Remember, I did warn you this was going to get weird in a hurry, and now, I believe, it's time for the weird to turn pro. Hold on...

But, wait, as they say in the more manic infomercials, there's more. As the internet becomes more and more ubiquitous, and microprocessors become cheaper and cheaper to make, the internet, defined as the TCP/IP protocol (or it's progeny, whatever that will be), it interlinks the most amazing places into a unified geodesic network, reachable through the air from local antennas, or sattellite antennas, or just physically, by connecting you to the network with a wire or fiber optic cable. With an increasingly ubiquitous internetwork, you can sell even more and more mundane things this way. In the ultimate throes of this anarchocapitalist madness, *everything* can be for sale.

Let's start with the obvious one first. Electricity. Already, they have demonstrated IP over electric lines in Britain. It is mostly trivial to do, especially over higher voltage power lines. Now, if you squint, you can see, with your newly dialated pupils, the very electrical *appliances* in your house, your microwave oven, your toaster, your teakettle, paying for their very electricty as they use it. With microcash.

It's not that hard to do. I just showed you how, right? All you need is a hash-handling chip in the toaster a little smarter than the chip in that expensive "gourmet" toaster sitting right there, right now, on the shelf in the gourmet kitchen store down the street. I call these imaginary chips micromoney mitochondria, and with them you get the quasibiological effect of picomoney as processor food.

If you remember the history of this century, and the first article in this series, it wasn't until checking accounts and hierarchical industrial networks became prevalent that lots of working folks *stopped* paying for their flat's electricity with actual coins in a meter somewhere on the premises. As we'll find out in the next article, that kind of "unwinding" of history is a very quick and dirty way to figure out how a bearer settled geodesic economy looks, if not how to implement it from scratch.

To continue the weirdness, think about a world where an internet router can save enough retained cash out of operations to buy a new line to a less busy router. Or copy of itself. Or to sell itself off into "slavery"(?) to another router (which is buying a copy of itself, remember?) after losing too much money to stay in business anymore. Transported. Mr. Macawber, thy name is "cypherspace". More time, running backwards, on Moore's law.

Great acid, yes?

But wait, there's more. If you can really do this with roads, paying at every intersection to get through it (money's cheap and small, remember?), does a, um, hierarchically organized force monopoly, a nation-state or it's smaller hierarchical subdivisions, need to "own" that road anymore? Shades of a favella in Sao Paulo, where the "property" lines extend into the middle of the street. Actually, not so "property" anymore, as the favella dwellers, along with their private piece of concrete to the middle of the street, now have secured real property rights to that concrete and the now-legally recognized road under it. So, are *they* charge you to drive over their little piece of micro-road? Stop this trip. Now. Please, make it go away...

What's next? Paying microcash for water as it comes out of the tap? No, let's not think about the inverse of *that* particular plumbing operation, as it's fraught with images of misers, Gordon Gecko (as someone likened me to, after I started thinking too hard about this in public on the net), and of couse, Scrooge himself, speaking of unwinding the clock to a more Dickensian universe.

Paying auction prices for *force*? Landmines which won't blow up if you have the right key? And keep paying them? Mama told me not to come...

Okay. Let's abstract our selves back a level or two, and think about actual micro-economics for a while, both to cool off our blazing neurons, and to honor a promise I made last time. Early in this decade, Ronald Coase, formerly of the LSE -- and now, I believe, at the University of Chicago, where all good Nobel laureates go to die -- won, you guessed it, a Nobel prize in economics. Coase won the Nobel by hypothecating (without actual mathematics, a boon and comfort to innumerates like me everywhere), that firm size is directly related to transaction costs.

That is, the cheaper the transaction cost, the smaller the firm can be. This has been proven, with actual data, to as much certainty as a fact of physics itself in the decades since the 1920's when Coase made this prediction.

Well? Notice something? Some digital bearer protocols are *really* cheap to use. Some get us to efficient transaction *spreads* in milli-to-microcent range. That makes for *really* small "firms". Market actors. Proprietors, in other words.

More to the point, if Moore's law reduces the price of switching enough to bearer-settle even the smallest conceivable purchases, like bandwidth, or road passage, or electricity, you end up a very strange

universe, populated with a swarm of extremely competitive, dumb, randomly-behaving business entities motivated *only* by, as Dickens' Mr. Macawber said, "keeping income over expenditures". Curioser and curioser, to mix my Victorian fiction a bit.

You don't just have an invisible hand, anymore.

To steal the name of the Cato Institute's football team, you have an invisible *foot*. Something which can kick the pants off any large, vertically-integrated, hierarchically-organized industrial-era business now trying to combat its transfer pricing problems in order to compete with a market which, these days, values that business in pieces *much* more than it does the entire business, because, of course, the transaction costs are now low enough for those pieces of the old firm to sell their services directly to the market instead of doing it behind the "firewall" of a company's chart of accounts.

*Dis*economies of scale, in other words. The world turned upside down. "Cats and dogs", as Bill Murray (who played Mr. Thompson once), "living together."

The weird have indeed turned pro.

Cheers,
Robert Hettinga

E-Commerce results
A spate of earnings reports from e-tailers and online payment firms confirms much of the pre-holiday hype internet shopping went mainstream in the autumn. Amazon.com reported $252.9 million in book, music, and video sales in the final three months of 1998, outstripping in a single quarter all of its sales for 1997, when revenues totalled $147.7 million.

'Hit 'em where they ain't': deploying digital bearer transactions

by Robert Hettinga

In the final part of his series on the use of digital bearer financial instruments, Robert Hettinga moves on from the theory to explain how we can actually deploy these instruments.

You couldn't have gotten through the capital market upheavals of the 1980's, much less Oliver Stone's movie *Wall Street*, without bumping into Sun Tsu, the ancient Chinese military thinker who, for our purposes, is best summed up by the Stonewall Jackson maxim, 'Hit 'em where they ain't'.

Among other things, Sun said that a small army should look large, a large army small, that one should attack when the enemy retreated, and retreat when the enemy attacked. You can almost hear P.T. Barnum muttering, somewhere, 'Never give a sucker an even break.' Mao, accommodating his intended audience with many simple single-worded exhortations and lots of exclamation points, recapitulated Sun's logic and won his wars in much the same way.

I propose, in less florid terms here, to think about the deployment of digital bearer transactions in that same spirit. That is, start where book-entry settlement ain't, and move on from there. With that fulcrum, we can lever complexity of digital bearer settlement against itself, and start 'surfacting' the existing glops of book-entry markets into smaller, more geodesic ones.

If you think about it, we face almost the same task that Copernicus, Kepler, and Gallileo did when they removed the earth from the centre of the universe. Like Kepler, we're going to use the simple mathematical ellipses of financial cryptography to replace the financial and legal Ptolomaic epicycles industrial economies had to build on top of their electronic, but still human-switched, information networks. We want to move money across these new geodesic networks we've built in cypherspace without the financial shovelware that currently passes for internet transaction settlement. If, of course, that's what you can call the out of band settlement of internet-executed transactions, which is what internet credit card and even check transactions really are.

I've already spent the last six months telling you, with a broad brush, how to apply digital bearer transaction technology to every security imaginable. This article is about specific applications of digital bearer transaction technology to problems people have told me about. It's an effort to jump-start your own thinking about digital bearer settlement in your own business.

Last November I went to to London, where, when I wasn't speaking to the E-Finance Forum, or to someone in the City, and, ultimately, to the Adam Smith Institute's conference on internet trading, all thanks to Duncan Goldie-Scot, I spent two evenings in a Kensington Australian wine bar, thinking about a couple of capital market bearer-settlement ideas with a few of the conference's participants.

After we're through with those two, I'd like to talk about micromoney mitochondria some, and an effort underway at DARPA to make the internet 'smarter'.

A Swiss fund

The first example, and the easiest to think about, is an already existing *bearer*-held Swiss hedge fund. Of course, *bearer* in Switzerland (or the BVI's, or wherever else) is quite different from the *bearer* I've been talking about the past few months. *Bearer* shares are typically registered with a trustee of some kind, but that registration is blinded from the portfolio manager. So, imagine, in the spirit of my previous 'Bill and Ted's excellent mutual fund' scenario, we created Bill and Ted's excellent bearer hedge fund.

That is, this existing hedge fund puts up a blind-signature certificate mint, right in the same room with their existing web server. When people pay the server digital cash, they are issued a digital bearer certificate representing assets in the fund. Right. What's digital cash? Okay, so we don't have digital cash. So we use checks, or bank wires. Somebody goes to a web page, is issued a non-transferable provisional certificate right off the bat, and, when the wire or cheque clears, they can come back and get real bearer certificates in exchange for the provisional one.

If done right, such an automated customer service scheme will probably be much cheaper the way it's done now, even with the added complication of transaction latency, which is there right now, anyway. Whenever digital bearer cash is available, handling shareholder exchanges will be even that much cheaper. Again, as a portfolio manager, you don't ever know who your customers are, anyway. The trustee administers your customer's money in the logical opposite of an American blind trust. Instead of the customers not knowing what the portfolio's invested in, though, the portfolio manager doesn't know, legally, who's invested in his fund. Which is the rub.

Notice my use of the word *legally*. There's this whole industry of fund trustees in Switzerland, using lots of lawyers no doubt, all devoted to administering those blinded lists of shareholders in *bearer* funds. I would even venture to guess that my digital bearer version of Bill and Ted's excellent Swiss bearer hedge fund is illegal, in order to perpetuate this cottage industry, though it might be fun to push the legal envelope a bit, to see how strong it is. We're still figuring it out.

However, I would bet that if using digital bearer certificate servers lowered the trustee's customer service by three orders of magnitude, they would have to adopt the technology, and that's exactly how to sell this idea in Switzerland. Portfolio managers would much rather just run their money, without having to think about such things for the time being. Save that box in Bill and Ted's machine room for

(Continued on page 11)

(continued from page 10)
some later regulatory regime and a few more iterations of Moore's law.

Which brings me, again, to the most important point I've been making throughout this series of articles. There's not a cryptoanarchist cypherpunk in the world who wouldn't jump at doing this particular contract. If the blind signature patent was clear, which we'll talk about in a bit. But, unfortunately, those people are jumping at this kind of work for entirely the wrong reasons. It's almost as if they think that just because they can put up a digital bearer-settled fund, that in and of itself will sell the fund to investors.

Remember again, slipping the surly bounds of earth is all well and good, but it's coach fare from Kitty Hawk to Dayton which put people into the air. Nobody's going to invest in 'Bill and Ted's' excellent Swiss bearer hedge fund at all unless they can make more money there than they can at home. Part of that present advantage, is, of course, taxes, and, probably, more than one case of investing ill-gotten gains, defined how you will in the jurisdiction of the money's origin.

However, the market for financial privacy is infinitesimally, ludicrously, small when compared to the market for cheaper transactions in general. And, frankly, the Swiss trustee, much less Bill and Ted themselves, are profitable enough already with the legislated privacy they already have, or they wouldn't be in business as it were.

No, what will sell this contract to some lucky financial cryptography systems integrator is lowered cost of customer service, pure and simple. Again, I claim, issuing bearer certificates to the net is the way to do this, even if those certificates are purchased the old fashioned way, with cheques, bank wires, or, given the location in question, suitcases full of cash. Again, we're eventually looking at a world where digital cash will be involved, and, when that's possible, the whole idea of safe jurisdictions like Switzerland may end up an interesting footnote in financial history. If they don't do it in Switzerland first, of course, and get a technological jump on the rest of the world...

EuroClear

Now, lets look at the second deployment idea. This one is one where you'd least expect it, in the heart of the institutional clearing system, literally under EuroClear's nose. Big institutions in Europe decided they needed a place to function for the myriad European exchanges in the same way that the Depository Trust Company does for the New York Stock Exchange. They hired J.P. Morgan to play that role, and called the system EuroClear. The problem is that the costs of the system are such that smaller institutions can't really afford to clear their trades there. A bunch of us figured, over some nice Australian Cabernet (and, um, kangaroo), that if you applied the model of digital bearer underwriting we talked about in July, and used Morgan as the institutional custodian for a jointly-held aggregate account, you could underwrite a bunch of closed-system bearer certificates against those shares and money, which a 'club' of smaller institutions could use to instantaneously clear trades against each other. Since this 'club' of smaller institutions would all be known to each other in the aggregate, all of the 'know your customer' rules could be adhered to, and, yet, the system could still, paradoxically, settle trades anonymously between club members.

The result would be extremely lowered transaction costs between the club's members, and, of course, instantaneous clearing and settlement. Something which might even be interesting to the much larger members of EuroClear to use someday, we figured. Maybe, someday, anonymity in settlement could translate to anonymity in execution itself... This rather insidious application of digital bearer technology, at the very place where one would expect the next generation of book-entry technology to be deployed, is exactly what Sun Tsu, Stonewall Jackson, and I mean by 'hit 'em where they ain't'.

In other words, deploy digital bearer settlement where book-entry settlement, well, ain't, yet, and don't fool around with attacking the Maginot Line of the existing book-entry-settled capital market infrastructure until the battle's already over. Dropping a few geodesic smart-mines on their escape routes, like we did in the two examples above, would work perfectly.

Router code

For the final deployment example, I've just learned about a project which which leads me to believe that the era of cash-settled switching-level auctions of internet bandwidth is not too far off after all. DARPA, the Defense Research Projects Agency, the very agency which funded the original internet, has hired firewall/security/spook-crypto company Trusted Information Systems (now part of McAffee's and PGP's parent, Network Associates, Inc.), to build a so-called Active Network, a technology where internet packets include code which tells the router where they want to go.

This is instead of a router needing increasingly larger route-lookup tables, requiring, you guessed it, hierarchical networks with big fast routers at the top-level 'backbone'. Moreover, these packets will be cryptographically signed, to prevent their execution instructions from being tampered with.

All of this is so the network can be more, you guessed it again, geodesic in structure and thus cheaper to use. Will wonders ever cease? So, avoiding geek-vs-spy conspiracy theories and the odd technological ad hominae against TIS in the expectation that the market requirement for cryptographic open source code solves the cypher-paranoia problem, this executable-as-network-packet idea looks like exactly like a running-code proof of my assertion that attaching micromoney to the information at the packet level is completely within technological reason. Welcome, one final time, to the future.

So let's play with DigiCash

Which brings me to a final hobbyhorse. Most of the problems, I think, with the deployment of digital bearer transactions are legal ones. Oddly enough, it's not even laws and regulation against bearer transactions themselves, which, on the face of it, are quite considerable. Even these regulations are com-

(Continued on page 12)

IN BRIEF

IP telephony soon

More than 80 percent of those in the high tech industry believe IP telephony, or phone calls over the Internet, will be widely used within five years, a new study shows. Of nearly 700 people surveyed, about 29 percent believe businesses and consumers will embrace voice-over IP within two years, while 54 percent said adoption will occur within three to five years.

Offline merchants left behind

Traditional real-world merchants who do not provide an ecommerce channel to their customers risk losing market share to their competitors, according to a new series of research reports from International Data Corp. (IDC). With the online population looking more like the overall U.S. population, companies must serve their customers online or their competitors will do it for them, the reports conclude.

(Continued from page 11)

pletely surmountable given enough cost-reductions and increased profit margins. Law follows economics, in other words.

The primary problem, as I see it, is the effective control, by the nation-state, of intellectual property. I tend to be extremely Coasian when it comes to my definition of private property. I believe that once information is on my hard drive, decrypted, and in a form useful to me, that's about as private as property can possibly be. It's mine. I can do anything I want to with it including sell it. Furthermore, as the internet becomes more and more location independent, you can't keep me from selling it.

I challenge anyone to enforce an intellectual property patent against me in an environment where anything, encrypted or not, watermarked or not, can be auctioned to the highest bidder, in usable digital form, for digital bearer cash. Cryptolopes, or electronic software distribution, or stenographic watermarks, even custom-compiled executable code and escrowed funds, do not add a whit of value in such a world. As an inventor, much less a seller, of digital goods, there is simply no reason to increase your transaction costs, and, correspondingly, reduce your profit, in order to control your digital product once it has been sold to someone. Just auction your product off to the highest bidder and be done with it.

The economics of the geodesic auction market says that if you have the first information of a specific type, you will make more money on that information than anyone else. Yet, before we can get there from here, there is a rather juicy irony involved. Because you need to cash digital bearer certificates into book-entry money sooner or later, the patents for digital bearer certificate technology are completely enforceable at the point of conversion, the gateways between the cypherspace and meatspace.

As I'm fond of saying, bankers and corporation presidents, as very creatures of the law itself, don't like to get sued for patent infringement anymore than they like to go to jail for financial crime in general. In fact, I think that patents on digital bearer transaction technology are so enforceable that they are completely obstructing progress in digital bearer settlement right now.

I would even go so far as to say that none of the current holders of digital bearer patents, (and, frankly, most of the current crop of people who want to control those patents in the future) know the least thing about financial markets and about how to market digital bearer transaction settlement to the financial community.

Well, actually, there is one person who might be the exception to that rule, and that's Scott Loftesness, the recently appointed President of DigiCash, Inc. DigiCash, you will remember, was founded by David Chaum, the father of modern financial cryptography, and is the company which holds the blind signature patent, the original patent on anonymously-transferable digital bearer certificates.

Unfortunately, after finally getting control of his company's intellectual property, Mr Loftesness now has to pay down a mountain of debt, mostly in failed bridge loans to venture capitalists, all of which are secured by those patents.

In my opinion, this debt may already exceed the estimated experimental licensing revenue remaining in the useful lifetime of the patents involved. And, given DigiCash's failure to find a market for their digital bearer certificates, licenses for experimental purposes is about the only alternative left.

DigiCash is already in Chapter 11, and, unless someone can see a way to market for that technology that others haven't seen already, the firm may not re-emerge.

And so, a group of us are looking at putting together a research-based syndicate to hold the DigiCash patents, or at least the most important internet-only pieces of that portfolio, in order to keep it from being tied up for the rest of its usable lifetime. The idea would be to license it for research purposes to all comers, and only when bearer certificates using the patented technology were exchanged into book-entry assets would a modest royalty accrue to the syndicate membership, payable at the gateway between the internet and the proprietary financial networks.

Syndicate members would get unlimited use of the patent, or at least a reduced royalty rate, as further remuneration for their investment. As much as I hate the idea of path dependency, I think that there are only so many neurones which any one company can apply to the problem of digital bearer settlement. If one company controls a critical bit of technology, the chances are too great, in a still incredibly experimental marketplace, of a dog in the manger preventing anyone else from making something happen.

Internet years are too short for the rules on patent duration as it is without financial cryptographers trying to be software developers, or banks, or anything else; something I've railed about on the net many times in the past few years. Since invalidating the very idea of software patents anytime soon is not reasonable (to the contrary, even business processes seem patentable at the moment, one look at the Walker Digital patent farm tells you that much), it might be worth figuring out a way for cryptographic protocol inventors to get paid for their intellectual property without holding up research in the field for everyone else.

While I think forming a syndicate to hold those patents, or a royalty association, something like what ASCAP does for songwriters, is the way to solve the problem, I'm certainly open to other suggestions.

So, there, after about six months, you have it. Not only have I discussed the enormous possibilities of the emerging world of digital bearer transaction settlement, but I've shown you how to do every financial instrument you can ever imagine in digital bearer form, using ubiquitous geodesic internetworks as your marketplace. All of this, hopefully, for significantly less cost than it would be to drag all those book-entry audit trails behind you all over the internet. I certainly enjoyed this series of articles, and I hope you did, too.

Robert Hettinga is the CEO of Philodox, in Boston MA
Email: rah@philodox.com

IN BRIEF

Waterhouse plans IPO this spring

Waterhouse is the latest brokerage planning to go public, in a long-expected move by its owner to cash in on investor infatuation with the Internet. Waterhouse's parent, Canada's Toronto-Dominion Bank, said it plans to sell a 10 percent stake in its discount brokerage operations to the public this spring. The stock offering could value Waterhouse alone at up to $10 billion.

Internet bearer underwriting: it's time

by Robert Hettinga

The weeks running up to this year's Financial Cryptography Conference (FC99) were really amazing, especially if you're a fan of digital bearer transaction settlement.

First, there was a lot of excitement about the forthcoming disposal, out of bankruptcy, of the DigiCash patent portfolio. This includes David Chaum's blind signatures, which are useful, as you remember, for macro-scale cash, bonds, and even equity.

Mark Briceno, a former DigiCash employee now turned dealmeister, said at FC99 that he has put together a syndicate which includes all of DigiCash's former licensees, and that upon acquisition, the patents will be royalty-free for open source and experimental use. Unfortunately, two of his promised closing days since have come and gone, however.

Yet, I recently talked to Nicholas Negroponte at the joint MIT Media Lab/USENIX Things that Think / Embedded Systems Workshops. Negroponte, the Media Lab's founder, is also, hopefully, the final Chairman of DigiCash, and has arrows in his back to prove it. He was talking to me quite nicely about Zero Knowlege Systems, the primary sponsor of Briceno's syndicate effort, so maybe something is in the offing. Finally.

Another wierd thing happened to me the week before the conference, when I got a query from a local investment banker, representing a public corporation with $5 million in cash and $7 million in market value. He proposed creating a company by buying both DigiCash and DEC/Compaq's Millicent technology. I went downtown to visit him, and said no, that wasn't a good idea, but that doing some kind of publically-held financial cryptography patent royal trust, a cross between an oil-patch deal and Buffet's Berkshire Hathaway, might be a fun thing to try. His firm didn't like the idea, but I still think it's a good one, and, upon leaving, I felt like I was resigned to evangelizing this stuff to deaf ears forever.

But, that very night, things changed enormously. I got an email message that night from Ron Rivest, sent to John Gilmore and Paul Kocher and cc'd to me and Adi Shamir. Rare company, indeed.

Ron Rivest and Adi Shamir are, of course, the R and S of RSA, the DC3 of the public key cryptography business. Rivest, himself of MIT, is responsible for RC4, the cipher behind the lock that appears on your browser when you encrypt your credit card number to Amazon and purchase a book.

In addition to co-inventing RSA with Rivest, Adi Shamir, from the Weisman Institute in Israel, has blown up more ciphers, more smart-card hardware, more supposedly secure commercial cryptosystems than practically any other man alive.

John Gilmore is one of the founders of Sun Microsystems, one of the founding board members of the Electronic Frontier Foundation, and a founding cypherpunk. For someone who's stirred up so much trouble, and with all the right people, he's one of the kindest folks I've ever met.

Gilmore's also the man who funded, for $250,000 of his own money, a special-purpose cryptographic supercomputer humorously called 'Deep Crack', which broke the US Government-mandated 56-bit Data Encryption Standard, or DES. In less than 3 days. At an amortized cost per key of about $360.

Paul Kocher, a well-respected cryptographer with several famous cryptosystem attacks of his own to his credit, was the man who designed and built 'Deep Crack' for Gilmore, and who now runs it occasionally, on behalf of the EFF, under whose auspices the DES effort was undertaken to begin with.

DES is ubiquitous in finance: $3 trillion a day in currency transactions are encrypted using DES, for instance. Breaking DES, in so short a time, and especially for so little money, was an act which sent shivers up the spine of bank security professionals everywhere.

It's even worse than that. 56 bits, the largest keysize possible with DES, is also the largest keysize allowed for export by the US government. Not a good place for the financial community to be in, technology-delaying 'exemptions' for financial cryptography aside.

So, into my email inbox arrives a message by and for the aforementioned cryptographic pantheon. The message says, quite simply, that just by designing and building a special-purpose machine to brute-force-search the DES keyspace, Kocher and Gilmore had inadvertently constructed a prototype MicroMint machine. They had, without knowing it, built a machine which would mint money in very, very, small denominations. A production machine would start at one thousandth of a dollar and go down from there.

I just sat there, stunned. I thought it would be years before something like this was going to happen. Digital bearer microcash has always been my 'way out there in left field' scenario, something I used to scare old people, children and politician with. I joked about routers that would use micromoney to buy bandwidth low and sell it high, saving enough out of operations to buy a copy of themselves. Or about toasters which would buy their electricity out of the wall. Or cars which pay tolls to use neighborhood streets and roads. Privately owned streets and roads, much to the joy of libertarians everywhere.

Rivest apparently cc'd me on this amazing email message because I had talked to him over lunch, almost two years ago, about commercializing MicroMint someday.

So, in my reply to this email message from cryptographic Olympus, I effused, at typical great length, about my underwriting model for digital bearer settlement, and how, since the prototype was already there in the form of 'Deep Crack', it was probably time to talk about building a production version of a MicroMint machine. Somehow. An actual financial cryptography supercomputer, probably costing several million dollars or more. Somehow.

Since everyone but Gilmore was going to Anguilla the next week for FC99 anyway, something I'm sure Rivest knew when he'd sent the email, I proposed that all of us talk about it there.

Immediately, I started emailing all the other people I thought I needed to make this work. Fortu-

(Continued on page 15)

(Continued from page 14)
nately, they, too, were almost all going to Anguilla for FC99.

The very first person I wanted sitting on my shoulder for a reality check, Jiminy to my Pinnochio, was Paul Guthrie, VP of Advanced Technology at VISA. Paul has been a long-time subscriber to my all digital commerce and financial cryptography lists, and has gone to every one of my Financial Cryptography conferences since the beginning.

Paul and I have talked extensively in the past about what it takes to effect a withdrawal of digital bearer cash from the automated teller network on to the internet, instead of a mere purchase of digital bearer cash with a credit card. Even more important was solving the problem of deposits from the net, which, oddly enough, is not intractable at all. Since VISA has it's hand in practically all funds-transfer and payment-systems networks, especially, for my purposes, the PLUS ATM network (Cirrus is owned by MasterCard), Paul's a very good person to know, and we have a lot of fun talking about this stuff.

It dawned on me, as we approached the conference, that the only two people I really needed to talk to to see if this was technologically possible, better, to have talk to each other, was Paul Kocher, the builder of 'Deep Crack', and Paul Guthrie, who could figure out in detail what integrating a MicroMint machine with the rest of book-entry financial system meant. Everyone else was just window dressing.

Did I get some amazing window dressing. I ended up with a dinner, for 17 people, at a nice French resturaunt just down the beach from FC99's first-night cocktail reception. I just went around the room towards the end of the reception, grabbing everyone I thought I needed and hauling them down the beach to dinner.

Besides Duncan Goldie-Scot, of this newsletter, this crypto-herding exercise included people like Nicko van Someren, the founder and CTO of nCipher, a British company which makes cryptographic accellerator hardware for internet commerce; Adam Shostack, cypherpunk turned CTO of Netect, a network security software company; Fearghas McKay, former British Internet Society chairman and now CTO of MIDS, an internet traffic-analysis company; Derek Atkins, of PGP 3.0 fame and now of Lucent; and Jason Cronk, owner of a large Florida web-hosting firm, and a big advocate of cash-settled geodesic recursive markets for intellectual property.

I didn't grab Ron Rivest himself and shove him down the beach towards dinner like I did the rest, because as someone with lots of people wanting his attention I figured he would be busy. But, to my surprise, after we had all sat down to dinner, Rivest and his wife wandered in for dinner on their own, and they came and sat with the rest of us. I was very happy.

So, after sitting all the right people together so they could talk to each other afterward, I banged on a glass for attention and got everyone caught up on Rivest's email message about the possibility of 'Deep Crack' being used to run MicroMint, kicking off an excellent dinner conversation on how to make an internet bearer microcash system happen.

It turns out that while it may be a little complicated to make changes to the ATM system to allow deposits from a third-party machine in much the same way that you can make withdrawls now, you can use other systems like ACH to get the same result, and, in fact, most of the problems faced by a nacent MicroMint are regulatory. People like Paul Guthrie kept beating me over the head with Federal Reserve Regulation E, which, as currently written, prevents digital bearer cash from being treated the same way as paper bearer cash is.

At this point I said something fateful. I said, 'If you guys can design a system which allows me to withdraw money, in microcash, from my bank account over the internet, and to deposit it later the same way, I'll get you guys, Ron (Rivest), Paul (Kocher), Paul (Guthrie), and Nicko (van Someren) in front of Alan Greenspan himself if I have to, demo it, and get Reg E changed.'

Dead silence. Followed by skeptical laughter all around.

Fortunately, I'm still immune to this stuff. I'd been there before, and I consoled myself with my favorite Schoppenhauer quote, the one about how new ideas are first rediculed, then fought violently, and then declared obvious.

Yet, Greenspan, a not-so-closet libertarian, if not a closet 'Austrian' economist, loves the idea of private currencies like we would be doing with this MicroMint box, and, if talked to in the right way, he would probably become an advocate for a revision of Reg E to account for digital bearer cash.

So, for the next day or so, I couldn't get this idea out of my mind. It was dawning on me that, because of developments with the DigiCash patents, and especially with this news about MicroMint, that there was simply no scientific or technological obstacle whatsoever to the underwriting of internet-based digital bearer instruments, not just microcash, not just 'macro'cash, but, someday soon, debt, equity, and any derivative thereof.

It's time to do some actual finance with all the financial cryptography. Later in the conference II came up with a company name for an internet bearer underwriting corporation. I called it, oddly enough, the Internet Bearer Underwriting Corporation. The fact that the corporation's initials sound like 'I-Buck' never entered into my mind.

Two weeks ago, I went downtown to the lawyers who incorporated my last company and got the ball rolling. We registered the Internet Bearer Underwriting Corporation in Delaware a week later, and I'm actively seeking officers, a board of directors, and, of course, shareholders. I have signed the incorporation papers, so I guess it's official.

I'm hoping to turn the key on all of this, to go live to the net, by the first week of July, 2000. That should allow whatever Y2K hysteria is left to transpire, certainly, but it's mostly because I don't think I can raise money and get anything built faster than that, anyway. And, frankly, it will probably be later, 'internet years' or no.

I want IBUC to underwrite, after 5 years, $30 billion a year in internet microcash, in bearer form, at an average front-end load of 85 basis points. That's how the investment hockey-stick looks, anyway. $30 billion is a scary number in the technology business, but it's not too scary in finance remember that $3 trillion-a-day currency market.

So, wish me luck, everyone.

Robert Hettinga IS the Internet Bearer Underwriting Corporation of Delaware
Email: rah@shipwright.com

IN BRIEF

CBA launches US share trading service

The Commonwealth Bank of Australia has launched a US share trading service for retail investors. Commonwealth Securities' new facility is the third initiative that it has announced so far this year, following the January launch of both its margin lending business and its internet-based FundsDirect service. The margin loan business has already generated significant income.

Endpiece:How to build a bearer underwriting revenue model

At the end of last month I began building the revenue model for IBUC, the Internet Bearer Underwriting Corporation, which I founded here in Boston, and wrote about in the last issue. You can 'back' into some pretty interesting numbers without doing a market test at all, something which is, frankly, impossible anyway, given the mostly unknown, and not insignificant capital cost of building the MicroMint box, for instance. Frst, you need an adoption curve. Typically, people in marketing use the logistics equation's curve. In our case, however, we had some real data, the historical and estimated future dollar volume of internet retail transactions, which, of course, are mostly credit card transactions. We got some from a fairly reliable source. These adoption curves start in the small hundreds of millions in 1995 or so, and, from 1996, they grow at a compound annual growth rate of about 100% or so over the last four years, into the tens of billions for this year. Using this time series, we now have as good a guess for an adoption curve as any for a proposed digital bearer payment technology. If something proves useful, it'll probably be adopted this fast, and if done right, probably won't be complementary or competitive with existing transaction types, thus increasing the dollar volume of internet transactions over time. So, we can take this normalised curve and tweak it for all transactions executed by mulitiplying the credit card number by some factor, or, we can use it fractionally, like we did, to gin up some numbers for a specific product. Again, you can back into a fairly nice approximation with actual data. Every year, the Bank for International Settlement publishes a report showing the global transaction counts and dollar volumes by each payment method, cash, credit cards, checks, wire, ACH, and so forth. Since virtually all transactions on the internet are executed with credit cards, if an meatspace-equivalent-risk digital form existed in digital bearer form, it's safe to assume that we might apply the meatspace ratio of that method to credit cards to the cypherspace credit card number. Of course, that doesn't work so good for MicroMint-based microcash, which doesn't have a meatspace equivalent, but it's a good start. So, use that factor times whatever market penetration number you think you can justify, and you have, voila, a revenue curve. So, now, we need an upper bound to all this unbounded enthusiasm. My CFO and I were wondering how we were going to do this, when, we remembered that we were in the underwriting business. After rooting around a bit, it dawned on us that Goldman Sachs had just filed a shelf offering for their IPO, so we went to the Securities and Exchange Commission's EDGAR website to go look at it. Right up there, on a metaphorical movie screen, was about a megabyte of information on how to be an underwriter, including the size of the global capital markets, Goldman's underwriting revenue and profits, and a whole host of other goodies. When we got through reading this, we were swinging from the lamp posts. *Cheers, Robert Hettinga Email: rah@shipwright.com*

How will regulators work in the new net economy?

by Bob Hettinga

Regulators have not even started to get to grips with the challenges they will face in the wired world.

In the summer of 1996, about a year after a bunch of us started the Digital Commerce Society of Boston, friend and fellow ex-cypherpunk Perry Metzger, formerly of Bellcore and Morgan Stanley and now owner of Piermont Systems *(www.piermont.com)*, a well-regarded financial computer security integrator, came up from New York to talk to us about how financial cryptography would allow the issue, on to the net in digital bearer form, of any financial instrument we could conceive of. Perry discussed some whimsical 'gold-denominated Burmese opium futures', for which he named his talk that day.

Implicit in that title, of course, was the point that government financial regulation, and, someday, governments themselves, were somehow ' optional' in a world of totally anonymous, but still non-repudiable transactions.

Eric Hughes, one of the co-founders of the cypherpunk cryptography enthusiasts' list, went even further in his thinking. He liked to say that, in imagining a world with ubiquitous internetworks and strong cryptography, it helped to 'think like an illegal actor'. Imagine, in other words, a world of ubiquitous recreational vices, murder-for-hire, and all the other staples of any good mob novel: all of it available, with impunity, everywhere, all the time, on the net, for a price. A frankly romantic vision, now, in hindsight.

If anything, recent history seems to show otherwise: all law seems to be enforceable everywhere, all at once.

For instance, several years ago a gentleman was extradited to Tennessee and convicted for the pornographic contents of his California computer bulletin board.

Within the last few years, two members of the cypherpunks list themselves have been convicted, and sent to jail, for making public threats to specific federal judges and officials, both involving completely hypothetical digital-cash-settled assassination auctions. Hypothetical, of course, because there isn't a working digital cash system, among other things. One of those convictions seemed, to me at least, more for a form of tacky political performance art than any physical threat to a judge, though the judge apparently thought otherwise.

And, of course, we should expect equivalent international incidents of these kinds, sans theatrics, sooner or later. After all, almost all countries have extradition treaties with each other for violent crime, and most at least for fraud, if not necessarily for other financial or tax crimes. If the aforementioned gold-denominated Burmese opium futures were illegal in one place at all, current legal opinion holds, cyberspace makes them extraditable, and thus illegal, everywhere, no matter the server' s physical jurisdiction.

Yet, cryptography itself, the thing which could so romantically change this state of affairs, is still being ' decriminalized' , and, recently, it has been done so an astonishing rate. Within the last month alone, Canada, Germany, and Britain, even France, who virtually outlawed cryptography of any strength whatsoever, have all seen the writing on the digital commerce wall, and have announced, grudgingly, that they will explicitly 'decontrol' cryptography in some fashion or another.

As people on the net have known for years, nation-states can now see that digital commerce means financial cryptography, and that financial cryptography must, of necessity, be the strongest possible cryptography available if it is to be of any use at all.

In other words, nation-states understand one of Hettinga's many 'laws' of digital commerce: Financial cryptography is the *only* cryptography that matters.

Even national security is taking a back seat to commercial 'signals intelligence'. Last month, the US Congress found itself the scene of the most amazing spectacle, with the National Security Agency claiming, of all things, attorney-client privilege in order to keep from discussing Echelon, a 40-year-old 'I'll spy on your people if you spy on mine' co-operative eavesdropping arrangement between the intelligence services of most developed nations.

Yet, the primary reason for such sunshine in dark places is not politics at all: it is business.

In the ultimate swords-to-ploughshares exercise, Echelon data, obtained at enormous taxpayer cost, is now being used, evidently, to give US companies an economic advantage in their international business negotiations. Why? Because, of course, other countries do it for *their* citizens. France, with its ironically strict cryptography controls, has been repeatedly caught informing companies like Bull and Airbus about the results of its operations against companies like IBM and Boeing.

Access to Echelon data seems to have even been offered by David Aaron, the Clinton administration's erstwhile roving cryptography ambassador, as an inducement for countries like Australia to sign on to the Wassanar ' arrangement', an 'informal' agreement among a large number of industrial nations to promote so-called 'key-escrow' encryption,

(continued on page 14)

IN BRIEF

UK tipped as Europe's e-commerce hub

Britain is poised to lead Europe in the exploding electronic commerce market, boosted by its advanced technology and status as a major financial centre. 'By taking advantage of its high international bandwidth capability, the UK can act as the European gateway for international transactions and exchanges over the internet,' Intel Chief Executive Craig Barrett told a CEO conference on technology.

Mondex expands in Asia; Proton enters Africa

MasterCard International's Mondex subsidiary, which made a breakthrough into Japan four months ago, has announced the formation of a franchise for South Korea. And Proton World International, which is partly owned by Visa International, made its first landing in Africa-a potentially extensive electronic purse system to be managed by Securecard Trust Company Ltd. of Lagos, Nigeria.

(continued from page 13)

a form of cryptography where the government has a copy of everyone's encryption keys. Key-escrow, or Government Access to Keys (GAK) to its foes, is, of course, mutually exclusive from digital commerce, and GAK's various US legislative incarnations have been steamrollered accordingly.

My guess is that the Jospin government finally figured out that 'infowar', when it happens, will occur not between nation-states, but between businesses, and that the best way for France to protect her businesses, and thus her tax base, is to allow their use of the strongest possible financial cryptography available. Which, given the eventual use of financial cryptography on the internet to hide private financial assets from confiscation by nation-states, makes for a marvelous paradox indeed.

So, what about that romantic vision of ' cryptoanarchy' , as Tim May, another founding cypherpunk, called it?

Remember, most of the acts that we call criminal today, especially those involving violence and property, still happen in 'meatspace', the abode of humans, and not 'cypherspace', the abode of encrypted electrons.

Meatspace, as anyone who has seen (or suspected) a surveillance camera knows, is becoming more and more supervised with every iteration of Moore' s Law. A digital CCD video camera, ready to be plugged into the internet as a web-cam, sells for less than $100 these days. Thus, it' s no surprise that an overwhelming majority of this surveillance is the completely private supervision of completely private property to prevent that property's theft or damage. Yet, people don't complain about this ubiquitous videography nearly as much as they would if a government did it. In fact, except for ostensibly personal spaces like restrooms or employee locker rooms, people don' t complain at all about private supervision of private property.

Do you see a pattern emerging, here?

As we encrypt our digital property to protect it in 'cypherspace', making it more invisible to nation-states, we increasingly supervise our physical property to protect it in meatspace, making it more *visible* if you will, all without requiring a nation-state to do it for us.

More important, we increasingly enforce those property rights with private means: security guards, for example, armed or otherwise. That's because, like everything else we buy, it is increasingly *cheaper* to buy private goods and services than 'public' ones, even force.

Put another way, direct payments, priced in auction markets, are increasingly cheaper than transfer payments, at a calculated price, between various accounts on a firm's, or a country's, books. Professor Von Mises and his calculation argument against socialism strikes one more time.

Moore's law accelerates this by dramatically reducing transaction costs, both in obtaining and processing necessary market information, first with cheap telephony, personal computers and faxes, and now with email and the web, but also in reducing the execution cost of those transactions themselves, with SSL and digital signatures for credit cards and checks, and, eventually, the clearing and settlement cost of those transactions as well, with digital bearer financial cryptography.

The result of lower transaction costs, as Coase tells us, is smaller, and more autonomous, 'firms': private, public, or otherwise. The fractal disintegration of large hierarchical empires like the former Soviet Union, or Yugoslavia, is a case in point, but so too is the peaceful 'devolution' of centralized power to smaller governmental units in both the US and Britain. Or, even, when one thinks about it, the apparent commercialisation of the Chinese People's Liberation Army.

Nation-states, like their aristo/theocratic predecessors did with industrialism, will have to stand back and let the geodesic train go by. And, like aristocrats and theologians before them, politicians will increasingly become mere ceremonial appendages to a larger, more geodesic, economy and society. The nation-state as entertainment, if you will.

So, we might actually have gold-denominated Burmese opium futures someday. Financial cryptography allows anything to be bought and sold, of course, as long as it can be represented on a wire with bits. Getting delivery of physical goods in some eventually private ' jurisdictions' may be another thing altogether.

We might even have, heaven forbid, auction markets for private-sponsored assassination itself, just as Hughes and May predicted, so long ago, at least in net-years. Certainly the death penalty is a type of state-sponsored assassination, and lots of countries still have that. Commercial assassination, ala 'The Godfather' is a, um, horse, of a different colour entirely, though.

War is, of course, murder on a grand scale, and something the more centrally-controlled nation-states have been particularly good at in this century.

But, I think, on the whole, with enough private supervision of private property, physical crimes, especially violent ones, will decline over time, and maybe even dramatically.

War and murder, are, after all, seriously bad for business - ask any Serbian shopkeeper these days - and the best way to prevent vandalism and the destruction of property, even on a large scale, is to identify the people doing it and then physically prevent them from doing so. This process would start from the ground up, it would seem to me, just by securely broadcasting criminal actions to a geodesic network, and warning others nearby to secure their property, and by force, if necessary.

So, even if, over time, most financial assets will migrate to the net, and the ability for an individual to act remotely to effect a physical outcome - even a violent one - increases, this action-at-a-distance can only occur within the bounds of someone else's private surveillance and protection scheme.

Your freedom to act ends where my nose begins, in other words.

That is not an intolerable state of affairs at all.

Robert Hettinga is the CEO of the Internet Bearer Underwriting Corporation of Delaware
Email: rah@ibuc.com

Divine Providence
Internet content without transfer pricing

by Bob Hettinga

Bob Hettinga continues his series about his start-up Internet Bearer Underwriting Corporation – IBUC

I started IBUC, my new internet bearer underwriting venture, because bearer micropayments, a technology I had left for the distant future of internet commerce, had come out of nowhere to be the easiest technology to implement first?

The same kind of unexpected, amazing thing happened on the demand side of the equation last month, when internet advertising revenue began to decline precipitously.

It was only within the past year that advertising revenue was overtaken by commerce revenue as the mainstay of the internet economy. First with brochure sites for companies such as AT&T made by companies with names such as net. genesis and RazorFish, and then with internet gold-rush sites such as Pathfinder, HotWired, Yahoo, Lycos, and Excite, it seemed that the only way to make money on the net was to either construct a brochure site, which itself was nothing but an advertisement, or own a content site, which was itself supported by advertising. Even better, obviously, was selling equipment and services to those who did one or the other of the above. Gold pans and blue jeans to the miners.

The realisation that inventory databases could be linked with financial cryptography on a web-server means that commerce for things normally stored in warehouses and sold by salesmen has exploded on the net. Companies such as Dell and Cisco get a majority of their multi-billion-dollar revenues straight from the web, for instance. The total amount of internet commerce is expected by several sources to top a trillion dollars by 2002. With the very sizeable exception of financial assets (a majority of all individual stock trades will soon be originated from the internet, for instance), and travel services, most of that projected internet commerce revenue will still be for items you can physically touch, things which are delivered later, instead of now, things which you'll keep after you purchase them and not literally throw away after a single use.

But it isn't that commerce for books, computers, and other actual stuff is just getting bigger than that for advertiser-paid content. Not at all. Advertisements on the web have shown themselves to be eminently ignorable by the web-browsing public, and, as a result, advertising revenue has actually fallen, and considerably so. Every large web-content site you have ever heard of has a huge budget for advertising outside the net, print, magazine, television, even radio, because ads on the internet itself just aren't that effective. And, yet, what these very firms sell, ostensibly, is internet advertising, and not the actual content of their websites. So, while things haven't reached panic proportions yet in the content business, it will be interesting to see how content providers are going to react to all this.

The very definition of industrial-age mass media is that it is produced on something cheap enough that it can thrown away after consumption. Of course, geodesic media has the same or cheaper delivery cost. Furthermore, Moore's Law on a ubiquitous internetwork allows the size of a 'production run', or 'audience size', to approach one. Or, at least, you could do it that way, if you could lower your transaction costs far enough. In other words, in a geodesic medium such as the net, it will probably turn out cheaper to actually pay the content's creator directly for custom content with digital bearer microcash than it is to 'target' advertising through one or more industrially-organised 'infomediaries' (or whatever McKinsey's buzz-word-du-jour is these days).

That'll be true no matter how big, or fast, your customer datamines can be. The market is your database, in other words. Database marketing, just like database transaction settlement, will choke on the sheer volume of 'targeted impressions' it has to monitor, and, more important, transfer prices it has calculate to pay for those impressions. A geodesic market sees such information choke points as damage, and routes around them.

Advertising supported mass-media, is, of course, the quintessential transfer-priced command economy. That is, accountants, not markets, attempt to calculate the value of whatever content an advertiser purchases on behalf of that content's consumers, using not-always-accurate heuristics like cost per thousand impressions, say, or percentage audience share. As most serious students of finance already know, it was the demonstration of the near-impossibility calculating a transfer price which resulted in most of the Nobel prises in economics given out in the last few decades. And so, as I've said about financial cryptography and cryptography itself, financial economics is the only economics that matters these days. In fact, the only time transfer pricing is even attempted is when transaction costs outside the firm were too high, for one reason or another, to get a market price. This is, of course, Coase's theorem, the fundamental theorem of microeconomics, and that theorem, in turn, is the very definition of what is, or isn't, a firm. More to the point, transaction cost determines exactly how large any firm can be.

The very concept of economy of scale comes from this. Since we at IBUC have sworn ourselves the equivalent of a barbarian blood-oath against transfer pricing on the internet, we have always considered web-page advertising as an almost unitary proxy for the potential content segment of digital bearer microcash market, and thus completely fair game when we go 'viking' in that direction. However, it now appears, the market for that unitary proxy has fallen. Does mean that there'll be no more content on the internet, especially at very low cost? Hardly. It only means that transfer pricing doesn't work as a way to pay for internet content. It's only really a problem for industrial-style distribution hierarchies, not the people who actually produce new content. As the technology of internet content delivery keeps exploding, and the price of distribution itself collapses accordingly.

MP3 audio files proliferate, much to the conster-

(continued on page 14)

IN BRIEF

Bank of America takes net to its Military Bank

Bank of America announced that it has launched an addition to its Military Bank through the introduction of an internet banking service (www.bankofamerica.com/military) that allows military and government customers worldwide access 24-hours a day to their account relationships.

Intuit adds another 61 OFX firms

Intuit has announced that 61 more financial services companies are offering customers the ability to connect their financial data with their Quicken software via Intuit's Open Financial Exchange-based web connect technology. Web Connect allows users to download updated account information from their financial institutions directly into Quicken. Intuit now provides online data connectivity to 745 finance firms.

(continued from page 13)

nation of record company executives everywhere. And much to the delight of those artists getting heard by more people just by disintermediating those very same record companies. And, it's getting cheaper.

All this new networked content business needs is a new way to pay for it all at that exponentially falling delivery price. (Shhhh. If you listen very carefully, you can hear a Norse rowing song coming up the river.) So, while most industrial content 'infomediaries' may be hiding behind their castle walls of lawyers, professional managers and strategic consultants, the smarter ones are investing a little danegeld to get involved in these new markets for content and get along with their new barbarian neighbours. After all, artists just want to be seen and heard, not sell to themselves.

Intermediation doesn't go away in this new world: it atomises into smaller and smaller bits with each iteration of Moore's law. So there is a way to pay for micro-cost content, and that is digital bearer micropayment. It's simple to imagine a protocol where a content client keeps putting pennies into a server's coinbox for a certain number of megabytes or seconds of additional streamed content. It's even easier to see some kind of XML function for doing things with each web page we see. The problem is, most of this potentially valuable content is still, for all practical intents and purposes, buried deep inside the transfer-priced cost of other things, like advertising, and even internet access. Internet access which, itself, is buried in the cost of telephony in certain tariff-mandated transfer-priced markets such as Great Britain. It's 'free', in other words. That the word 'free' actually means a redirected payment and a transfer price makes no difference to an uninformed, and, frankly, innumerate, public. They are 'paying' all that they want to for using the web, for internet access, and especially for telephony and, they expect the price to fall as time goes on.

It's what Michael Eisner likes to call the financial 'box' we have to operate in. As long as a customer's cost to use the net falls over time, he's happy, whether he pays cash to every website he sees, or he pays for it by the month to an ISP, or he pays what amounts to a tax on his phone calls, to get it.

How does a content provider bootstrap this? Easy. Damn the torpedoes, sell stuff for cash anyway, and let the market sort it out. Transfer-priced content is going to go away, one way or another, and clinging to the sinking ship of advertiser revenue and other equivalents won't help matters.

What will happen in the content market is what always happens when revenue dries up: a shakeout. If it's not currently underway, that is. Pathfinder, for instance, is gone, subsumed by a separate site for each Time Warner's media properties. The people who do things for free will continue to do so until their expenditures, or their opportunity cost, causes them to quit. The people who do really valuable things will continue to do so as well, and get paid for it somehow. For the rest, it's really a question of either being the lowest cost producer/distributor, or finding new revenue streams, or some combination of both.

My claim is that those in the last group will be people who focus on aggregating and distributing content instead of creating it, that everyone's going to be the lowest cost producer/distributor, that the transfer-priced revenue they were invented for will dry up. Any good market eats it's young, and all that.

That brings me to something I've called a geodesic recursive auction. I've actually talked about the idea here in this column before, but this new 'emergency' in internet content revenue dictates a little more detail in the discussion.

The idea itself is pretty simple. I create new content. I sell it to you for the most I can get for it, and I keep doing that until nobody else wants to buy it anymore. If people are deluging my server with purchase requests, I raise my prices until the load goes down to something manageable. If I have no traffic, then I'm charging too much. Buy low, sell high; charge all that the market will bear. Darwin rules. By the same token, if I download something from you, I can turn right around and sell it again to anyone who wants to buy it, thus maybe recoup my costs, and even make a profit. The assumption is that on the net, things like copyright and other intellectual 'property' controls simply cost too much to enforce. It's hard to reach out and arrest somebody over the net, particularly if functionally anonymous bearer transactions are the cheapest possible transactions. Also, the additional cost of copy-control mechanisms such as 'watermarks', 'cryptolopes' and so on is simply too high for whatever extra value they might provide.

Before the advent of ubiquitous geodesic internetworks, much less auction-priced digital bearer transactions, huge amounts of profit were eaten up in the inefficient transfer-pricing of production assets, or, more important, the information about that assets, up and down the organisation chart and its corresponding chart of accounts. Industrial-era record companies, publishers, and entertainment networks are all still fairly hierarchical entities today, even though the economics of Moore's law has changed their business considerably over the last thirty or forty years. It's not without a reason that the most important person in the movie business these days is the artist's agent, and not the studio head, for instance. Digital bearer cash, at sufficiently small denominations, probably the $10^-3 (a tenth of a penny) range, or maybe lower, enables the direct purchase, and, more important, the immediate disposal of content after its use.

In so doing, it solves precisely the problem that advertising does by batching impressions and transfer-pricing the cost of delivering the content responsible for those impressions. More to the point, it uses economics and software to solve the problem of copyright infringement, because storage cost should vastly exceed purchase price. (By the way, we at IBUC call $10^-3 a 'minidollar' because 'millidollar' sounds too close to 'Millicent' a proprietary trade-name belonging to Digital, now Compaq. Another transfer pricing problem, yes?)

In other words, digital bearer minidollars give us the exact industrial definition of 'mass-media' -- use it once and throw it away -- but without the transfer-pricing overhead of hierarchically organised markets. Toffler's 'mass-customisation', indeed. Only there's no industrial-era 'mass' to any of it. Every single bit is paid for directly by the user of those bits, in a hyper-efficient, auction-priced, cash settled, geodesic, market. The customer, and the producer, get exactly what they want, and more of it, for less money. Sounds like progress, instead of disaster, to me. And, of course, for us at IBUC, it's almost divine providence.

Bob Hettinga is CEO of IBUC
Email: rah@ibuc.com

The Geodesic Economy

Robert A. Hettinga

"Who needs money anyway?": The New Monetary Economics, Monetary Separation, and Digital Bearer Settlement

Economic Government Group

Top

Introduction

Features

Interact!

About EGG

One of my best friends in the whole world is Mark Tenney of Mathematical Finance in Alexandria, Virginia. The best man at my wedding, I met Mark during my mostly sad attempt to go to the University of Chicago as a "Student-at-Large", where I snuck in the back door and hung out for almost a year before they threw me out -- though, to my credit, or lack there of, it was for impecuniosity, more than anything else. "First thing you do, you get the money", and all that.

It was fun, though, and I ***did*** manage to transfer enough credit from Chicago to finish my undergraduate philosophy degree at Missouri. Up until the last five years or so, when I discovered the "University of the Internet", I'd always wished I could afford to go back some day and play some more, especially in finance and economics.

Anyway, Mark was one of those scary mathematical prodigies who finished both high-school and college in three years apiece, finished all-but-a-doctoral-dissertation in Physics at Brandeis in three years, hedging himself with an Master's, then turned on a dime and did the same thing in Finance at Chicago, hedging again with an MBA in Finance. All this before wading into the fray of quantitative fixed-income analytics-for-hire, swinging that claymore-sized intellect of his with both hands.

Last year, I told Mark that I had decided to concentrate on digital bearer transactions full-time, and he asked a bunch of questions like he always does when I reveal my latest off-the-wall idea. And not saying much in reply, which he also always does, being one of the most laconic people I've ever met. That's okay, I suppose. I talk enough for both of us.

Anyway, a few days later, Mark calls me up, all excited. Well, as excited as Mark gets, anyway. "You could issue digital bearer certificates backed up by an S&P 500 portfolio," Mark says with not much affect, followed by dead air, which is my cue to talk.

"Yup," says I, chattering away, "That's easy. Old hat. We talked about stuff like that on cypherpunks ***years*** ago. The only problem is, it's illegal in the US for various reasons, and proving that you're ***only*** issuing to and redeeming from foreign nationals is ***really*** too complicated. We don't call it 'digital bearer settlement' for nothing. Of course, that doesn't keep several smash-the-state cryptoanarchists out there from daydreaming, in color, about that idea pretty much full time. Expressions like 'tax-evasion' and 'money-laundering' only make them work harder, after all. Me, I'm only in it to reduce transaction costs. Illegal business is chump change compared to putting the entire global economy onto the net in digital bearer form.

"Steve Schear and I even figured that you could do it with just about ***any*** stock, anywhere, from anywhere, as long as it was legal in the jurisdiction you did it ***from*** . Sort of an "Unsponsored Network Depository Receipt", UNDRs, for short..." and then, I proceeded to go into an entire rant on ***that*** . In four-part harmony. Arlo Guthrie would have been proud...

Finally, I run out of gas, like I always do, and Mark says, "If you issue digital bearer certificates collateralized by the S&P 500, you won't need cash anymore." More dead air.

"Well," I said, jumping back in, "maybe, maybe not. I mean, the dollar's pretty much pecunia franca right now, yes? Anyway, you wanna write something up about it, and we'll zing it out onto some of my mail lists for comment?"

I figure that if Mark was excited enough, ***he*** could bash on the mathematical finance of this idea much better than I ever could, being mostly innumerate myself, with my undergraduate philosophy degree from a midwestern state-school, and leftover student-at-large credit from UofC.

I mean, the closest thing I ever got to a genuine financial education was sneaking out of the University of Chicago Bookstore Graduate School of Business textbook section with books like Brealy & Meyers' "Corporate Finance", and Sharpe's "Investments". Needless to say, reading stuff like that, and hanging around people like Mark at a place like Chicago pretty much set my "if there's not a market for it, it really doesn't matter" view of reality into steel-reinforced concrete. It's kind of the core of my anti-state bias as well, I suppose.

Mark is, of course, a pro at this kind of stuff, having figured ways to use Green's functions to kill off lots of Monte-Carlo modeling, building closed-form solutions for various security prices, and so forth. His asset-liability models sit in the guts of several very large insurance companies, and there are questions about his asset-value calculation methods on the US actuarial exam. One of his latest projects is building the analytical core of start-up e-finance company in an as-yet undisclosed European country, and his client before that was one of the largest financial services firms in the world, owning well-known insurance and mutual fund companies everywhere you would care to name.

So, I didn't hear much from Mark about this idea of his anymore, probably because most of his "wetware" bandwidth is paid for these days, with real money, and he doesn't have much time to spare for actual fun -- much less writing a non-reviewed finance paper that I would just pass around the net for free. And so that's the last I heard of it for a while.

Then, a few months ago, after I'd started up my new company, IBUC.COM, to actually issue digital bearer cash and other stuff some day, some newbie on the cypherpunks list talked about trying to do yet another internet currency, a smallish rant with a whole bunch of, well, ***wrong*** stuff in it. So wrong, in fact, I can't even remember most of it. As is unfortunately usual in these circumstances, I ended up writing my own rant in reply. It centered around my own favorite point on the subject, that unless any "internet currency" was exchangeable into ***dollars*** , or some other standard unit of exchange, nobody was going to pay any attention to it.

There have been several efforts on cypherpunks and elsewhere to think about synthetic currencies based on attention, or

machine cycles, for instance, and, while using machine cycles to prevent ***forgery*** is at the core of most decent micromoney protocols like MicroMint, but you have to denominate your digital bearer cash in something ***financial*** , or it will be of no real use to normal people. Not that most cypherpunks care about being normal, you understand, but there it is.

Nonetheless, I did toss off some nice words in the direction of the e-gold guys, who, at the time, were issuing a kind of gold-backed "internet currency", albeit in book-entry form. They had been having some success with it, mostly among the anarcho-survivalist gold-bug crowd. Meaning that a lot of very bright erst- and proto-cypherpunks have been playing with e-gold, for reasons of politics, paranoia, or both. Or at least so I figured at the time, anyway.

Dr. Douglas Jackson, the oncologist-turned-founder of e-gold, is quite a bit more phlegmatic about these things himself, though certainly never a fan of fiat currency. He understands, for instance, that storage costs can make gold-backed account balances actually depreciate over time. But, in implementing the e-gold payment system, he and several thousand e-gold users have ended up with quite a bit more experience in non-credit-card internet payments than anyone else has to date, mostly because they didn't try to do anything too complicated in the early stages.

More to the point, all of Doug's competition (like First Virtual, CyberCash, and DigiCash, to name a few) have killed themselves off going for the main chance. They kept trying to conquer the world, trying to be some kind of ***sole*** transactor of business on the web, without understanding that finance is a business of herds and swarms and that ***nobody*** trusts anyone who's the sole ***anything*** .

Meanwhile, Doug's still doing a tidy, if not land-office, business, precisely because he's ***not*** trying to take over the world. In fact, I'd say that anyone who's interested in internet payment should pay more than a little attention to e-gold, or, as their evangelist Jim Ray likes to call it, "The little internet payment system that could."

Anyway, Ian Grigg, an expatriate Australian who I can't really call a cypherpunk -- more of a "moneypunk", maybe, since he's spent a lot of time lately down in Anguilla building things for e-gold, among other people -- sees this cypherpunks rant of mine about internet currency after I forwarded it to dbs, the digital bearer settlement discussion list that I run. Ian observed there that if transaction speed was fast enough, the market would probably converge to a world without cash at all. Shades of Mark Tenney.

Since I respect Ian's opinion, because Ian seems to have read every "Austrian" economist there ever was, and is a great fan of Scottish free banking, not to mention because of all his work for e-gold, which now runs on his "Ricardo" web-market-making system, I thought to myself, "Okay. Maybe. Someday. In the meantime, I want IBUC to do cash, dollars preferably, thank you very much, and after that, other ***actual*** securities, and, after ***that*** , we'll see if the dollar really does evaporate as the world's primary exchange currency." And having said so to the list in reply, I left the discussion there for the time being.

Which brings me to a little while ago, when I was half-to-three-quarters of the way through with a nice rant for this column on something else entirely, and ended up throwing it all in the trash.

That was because of something I got in email from ***another*** friend of mine, one of the best internet transaction lawyers in the business, John Muller, a partner at Bobreck, Fleger and Harrison, in San Francisco. Among other things, John is Chair of the Web Site Working Group of the American Bar Association Joint Subcommittee on Electronic Financial Services (say ***that*** ten times fast), and Co-chair of the Automated Transactions and Electronic Agents project of the ABA Cyberspace Law Committee.

What John sent me was the most recent Electronic Financial Services Update, the back issues of which can be seen at http://www.abanet.org/buslaw/efss/whatsnew.html, and in that update was "Towards a Moneyless World?", a paper by Malte Krueger, of the University of Cologne and the University of Western Ontario, for the International Atlantic Economic Conference, which was held in Vienna this past March. Apparently, this paper was also presented in different form to the Second Berlin Conference on Internet Economics a little while later.

And, there, after converting PDF to PostScript, and then PDF to ASCII text so I could read it faster, ***there*** was a pointer to where my friend Mark Tenney -- and, I bet, Ian Grigg -- got the idea that as transaction latency and transaction costs go to zero, the value function of currency converges to that of more "financial" assets: They were quoting, whether they knew it or not, the so-called "New Monetary Economics" (NME), a phrase coined by Robert Hall, but conceived, in the early 1980's, by no less a pair of financial luminaries than Eugene Fama, of the Efficient Market Hypothesis, and Fischer Black, of the Black-Sholes option equation. Others, like Krueger, apparently, call this the "BFH system", in their honor -- or for other reasons, it's hard for me to tell.

Krueger says, of NME/BFH,

> In the current system money (cash and deposits) is used as medium of exchange and unit of account. In the BFH system there would be no common medium of exchange with a fixed nominal value in terms of the unit of account. Instead, assets with variable prices are used. This implies that, in principle, any asset could serve as a medium of exchange. An example that is often used to illustrate 'moneyless' payments are mutual funds shares. The value of mutual funds' shares varies with the value of the funds' assets and within certain limits they can be used for making payments. So, the medium of payment 'mutual fund share' has a value that is not fixed in terms of the commonly used unit of account. Eugene Fama (1980) argues that monetary separation is efficient because the financial system (Fama uses the term 'banks') serves two functions that are independent of each other: the accounting function and the portfolio management function. Banks could fulfill the accounting function without holding assets or using any medium of payment. It would be sufficient to have a unit of account. As an uninvolved third party, banks could just keep records of transactions. The issue of liabilities and the purchase of assets is derived from the second function, the portfolio management function. In this function banks help individuals to hold their wealth in a form they desire.

What the above means to me is pretty much what Tenney and Grigg said, that Moore's law creates an increasingly

geodesic, ubiquitous, public internetwork, which, coupled with the financial cryptography of digital bearer settlement, "surfacts" currency into its constituent parts. Why keep something which doesn't earn you money, in other words? Why not use something which is as risk-free as possible but still earns money while it's in your possession? Furthermore, the longer money's going to be in your possession, the more incentive you have to invest in something where short-term volatility isn't a problem. We'll leave discussion of my opinion on the "accounting" function as an exercise for the reader.

Anyway, Macroeconomists call this division of unit of exchange from unit of account, monetary separation. And, as a result, we get more and more different kinds of exchange with decreasing transaction cost. Banks go back to being "counting houses" instead of fiduciaries, trustees, keeping track of who owes what to whom, and the returns on money are higher for the users of that money. The advent of the money-market mutual fund, was, of course, a step down this road.

As to whether this means the death of currency, Krueger comes down on the side of network effects -- unfortunately conflating them with path-dependency; network effects being cool, and path dependency being balderdash -- and says that the opportunity costs of keeping track of various different asset classes, and, more importantly, exchanging those different asset classes with others just to effect any trade whatsoever in a virtual re-emergence of barter, still costs too darn much, and thus, the internet gives us monetary integration, and not separation. As someone said of Mozart, "too many notes".

I'm personally not so sure, Moore's law being what it is. It might be easy enough with with enough bandwidth and processing power to do all those exchanges and re-balance one's "portfolio" of money-equivalents, paying people in whatever asset class they want, and still make more money than parking money as dollars in a bank somewhere, or, worse, keeping cash on hand.

However, I also think that it'll be a while, just yet, for that world to emerge, and, frankly, I want to buy things with ***dollars*** , and right now.

By way of some even ***more*** twisted synchronicity, Krueger's paper then points to my friend Tatsuo Tanaka's paper on the macroeconomic consequences of internet free banking. Which, oddly enough, I edited and recommended for publication in the peer-reviewed internet journal First Monday four or so years ago. I even invited Tanaka to come up and present the paper at a Digital Commerce Society of Boston luncheon shortly after the paper came out.

Tanaka says, first of all, that internet free-banking is like the expatriate-cash Eurodollar market on steroids. Internet free-banking drives the final nail in the coffin of central bank control of any nation's currency, because, if a currency is stable enough, and maybe even if it isn't, sooner or later more of the currency is "issued" on a fiduciary basis outside a country, collateralized by foreign-held dollar-denominated accounts, for instance, than is issued by the central bank itself. And the net makes ***where*** the money is, heh, immaterial.

Unfortunately, Tanaka also says that competition for underwriting cash to the net causes the eventual fractional reservation of digital cash against its denominated currency, and that, sooner or later, crises of confidence in all those different issues, and their various partial reserves, force the creation of, you guessed it, monetary union of some kind. Tanaka liked to wax about the eventual creation of a central bank of cyberspace, thus setting most cypherpunks' and other free-money advocates' teeth on edge, mine included, skyward-rolling eyes and all.

But the story gets weirder than that. Recently, Douglas Jackson and his crew at e-gold have been taking their association with "moneypunks" like Mr. Grigg (and, um, others :-)), to heart lately. They split themselves into a trustee-underwriter relationship of several firms, and, in the process, have created an offshore subsidiary, based in, where else, Anguilla, to, you guessed it, offer fractionally-reserved, (but non-blinded) gold-denominated digital bearer certificates, called, oddly enough, DigiGold.

The idea behind DigiGold is to fractionally reserve gold denominated transactions, loaning out the reserve's other fraction to offset the cost of gold storage, which, as we noted above, at a percent or more a year, is a considerable one if you're trying to create a currency which is supposed to hold its value. In fact, Ian went so far as to start buying and selling notes denominated in gold recently, apparently as part of his work with DigiGold.

"Gold-denominated Burmese opium futures", indeed.

For one final bit of weirdness, I eventually got around to reading Glassman and Hassett's Dow 36,000 article in the Atlantic Monthly, which, at the core of its analysis, notes that among other things and contrary to received wisdom, equities held in the long term are much ***less*** risky than even long-term government bonds are, and how the market has been compensating for that for the last few decades or so by driving equity prices slowly upward to their risk-adjusted "reasonable" price. Like their title says, they say that the Dow could be at 36,000 and still be "reasonable", whatever that means. Mercy.

A splendid read nonetheless, whether you agree with them or not, and the bit about the risk of the equity market certainly makes a compelling argument for a very, very, interesting result for us, in light of all of the above.

At the core of all modern financial analysis is the proposition that government bonds, especially short-term ones, are the safest investment. They're safe because, for instance, the chance of the US government defaulting on any given 90-day T-Bill on any given day is virtually non-existent. T-Bills are literally risk free, and all other investment is calculated against them for riskiness. The Net Present Value equation, for instance, says that if the returns of a proposed investment are less than you would get from a T-Bill, you should forget the investment and keep your money in T-Bills instead.

And, at every year of bond maturity, the government bond sits at the lowest point of the risk "well" for that maturity. Or so I thought, until I saw Glassman and Hassett's description of what all financial theorists knew already for a fact, that the long-term risk of the overall equity market is much less than that of even government bonds.

So. Can we back that "zero" equity-market risk down the maturity curve to the present? Maybe, with a derivative or two. I haven't gone looking for the answer, and it's press time already. I wouldn't be surprised, though, and to walk out on a very

thin limb, I'm going to assume it to be true.

Certainly the idea of, say an S&P 500, or maybe a larger-index-based "cash" starts to make sense, if we can do it. After all, Ian Grigg and his friends are trying, for all intents and purposes, to do roughly the same kind of thing with gold. Gold hops around a bunch, and volatility is probably not a good thing for a currency to have. So any financial engineering you can do to at least take the volatility down a bit would be good. And you'd want to do the same thing with equity indices, because, as a functional perpetuity, a stock can be just as volatile as a 30-year bond might be.

What we get, if we do create a low-volatility equity-based currency, is really very interesting.

We get what Gene Fama and Fisher Black must have been thinking about back in early eighties heyday of the "New Monetary Economics": a completely private form of "riskless" return.

Think about that for a minute. Not only do we have digital bearer settlement, so we don't need the nation-state to provide force and ensure the non-repudiation of our transactions, but we don't even need another kind of force either: the confiscatory force of a nation's tax system, making for "riskless" government securities, which, in turn, undergird our very concept of what risk is.

What we get is truly ***private*** money. That is, someday we can create a completely synthetic currency based upon a commonly-referenced ***equity*** market index.

Look, Ma, no currency board, much less a central bank. No guns. No sovereign. And we still get money. Amazing.

So now, instead of stepping ***back*** to a commodity economy to avoid state control of the monetary supply, using something like gold to anchor value on the net, we can step ***forward*** into the information economy, the geodesic economy: All we need to collateralize our transactions is a sufficiently representative and publicly known equity index, with the volatility hedged for short term use using ***other*** publicly known derivatives. Presto change-o, a synthetic internet security. And, of course, this works with bearer held stocks, if we ever get those, as well.

Finally, anyone who wants to can do this -- well, if their reputation's good enough. This is finance, after all.

Of course, the sticking point all this fun is the state itself, as I said to Mark Tenney more than a year ago. Remember all the book-entry taxes and regulations about bearer ownership of bonds, TEFRA, et. al., here in the U.S., and then exponentiate that number to get the regulatory barriers for bearer equity.

It'll certainly be easier, for the time being, to issue cash denominated in dollars than it would be to try to climb an enormous ziggurat of regulators and legislators, telling all of them that issuing bearer-form equity-index-denominated money would be a good thing, even if it completely removed ***their*** central banks, much less ***their*** very government bonds, from the center of the financial universe. A lead balloon, indeed. Almost makes you want to believe in path-dependency, that does.

But don't despair. Remember that if digital bearer transactions really ***do*** something I'm betting my company on, sooner or later an equity index-based "internet currency" will in fact emerge as the best way to buy things.

Even more interesting, if we're right, government-extorted revenue will cease to be the foundation upon which the concept of "riskless" return -- and all of finance itself -- rests.

But that's probably what Fama and Black had in mind, right?

Robert A. Hettinga is with the Internet Bearer Underwriting Corporation.

Return to the Articles and Essays page, or the Articles and Essays by Date page.