

Wisdom for the Digital Era

Issue One

“Cold Hard Cash”

*DISTRIBUTION RESTRICTED UPON PERMISSION OF LEE FISCHMAN
COPYRIGHT 1996 - LEE FISCHMAN*

Foreword!

Welcome to the future. In this future, there will be little difference between what can be sent over the airwaves, through cable or telephone wire. Everything sent will be digital, and thus as easily transformed into pictures as into text, sound, or anything else which creativity can provide. Today's Internet is only an inkling of what to expect. In the future, digital information will flow over a pervasive, powerful infrastructure. A fascinating new media has arrived.

This series will try to provide wisdom for the Digital Era. Many people are working through the issues and ideas that I will touch upon. However, there have been few neutral sources dealing from a broad perspective with all the consequences of *going digital*. I draw my paycheck from technical work, and yet I am strongly concerned about how machines may affect us. We cannot turn back the clock on the future, but we can understand it and intelligently try to direct its development. In the Digital Era this is especially important - we can march like lemmings into the Information Revolution that the digital era will hasten, or we can understand what we are faced with.

The digital future is something into which we are all heading, and so *Wisdom for the Digital Era* is intended for a broad audience. I will deal more with ideas than facts - too much of today's world is an onslaught of meaningless facts. After all, the goal of this venture is to give you what the first participants in television and radio probably did not have, enough wisdom. For the technically sophisticated reader, bear with me. We will occasionally discuss simple ideas, but hopefully while on the way to something more profound.

Where to start? Money still makes the world go 'round...

Introduction

"Spices could be traded but stories could nary be told."

Why the quote? Imagine the days of yore when traders roamed the continents, connecting one people to another. What could be grown in one region was not easily reproduced in another, and so had a market value. On the other hand, stories did not motivate commerce. Stories were difficult to transport and, even once told, there was no protection against its being retold by others. This is not to say that stories have ever been worthless. As societies have evolved technically, transport mechanisms known as “media” have evolved to carry and commoditize them into something we now call information. Because it moves a valuable commodity, media is valuable.

Media encapsulate information and provide for its distribution. They are extensions of society and yet, because they propagate society's thought processes, media powerfully motivate change. Printed publishing, radio, television, and other media already are fairly well understood, but digital media is not. Because it is so powerful, flexible and immediate, it is chameleon-like, absorbing attributes of all the media that preceded it. But digital media is also a product of emerging technologies that must be dealt with in new ways. The new media is very young, and it faces an unknown future. First principles count.

Ethereal Goods

As digital media takes hold, information increasingly will become physically featureless. Until now, it has been easy to deal with information in our industrial framework because

GALORATH CONSULTING VERSION

it has been captured in tangible goods: a tape, a stage, a book. However, information will increasingly be made available to us as no more than a "bucket of bits."

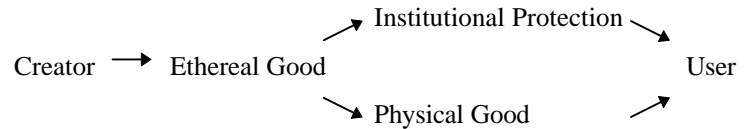
Information that is passed over a *pervasive information infrastructure* such as the Internet can now be copied at no cost and massaged no end. The result? Creators of information have far less control over the distribution of their work.¹ If you are a fan of plenty, then ownership of information was a grand development, because physical media let information blossom: it could be distributed more easily (albeit with some *discrete* limits on distribution) and creators can be rewarded for their labor. However, the transformation from tangible to ethereal media creates fundamental challenges for the protection and distribution of digital information. These may require methods of control that are as revolutionary as the patent laws were in their day. We are heading into a purer relationship with information, one less beholden to things we can feel, see and touch. The era of the "ethereal good"²³ is arriving.

¹This may seem revolutionary, but could it be that a *purer* information regime is emerging? Let me explain: today you can "own" a song or a story, but at some time deep in our history, this was probably a preposterous idea. Along the way, we've learned to use the physical world as a proxy to enforce ownership.

²My use of this term, and the kernel of this concept, comes from an article by Gordon B. Thompson, "Ethereal Goods: The Economic Atom of the Information Society", in Information Technology: Impact on the way of life***

³Can we even think of ethereal goods as *goods*? Some people have not. The Free Software Foundation was an early reaction to the extension of property rights into the ethereal realm. Its solution was to devote brains and sweat towards creating software free for the taking. The FSF people asked how an ethereal good, intended for ethereal purposes, could be owned. They had been brought up in an environment of academic volunteerism marked by tremendous unrewarded achievement, and so this was not a crazy idea to them. The FSF people also felt that with control of software

Our society has *already* extended property rights into the ethereal realm to some extent.⁴ If you create something unique, even just a "look and feel", it is intellectual property and you can own it. Creators of information have used two essential methods to enforce ownership:



Above are two basic means of intellectual property protection. For an example, imagine a musician's work. Persons who want to listen to it at any time can purchase his or her LP. This is a form of physical protection, a way of encapsulating information into something that can be grasped and reckoned with as a saleable object. If in contrast a business wants to play the music in its elevators, the musician would be owed a fee. Protections of this sort do not impose physical burdens but instead reckon with ethereal goods in their own realm, with institutional protections provided by contracts or legal rules. This can be an advantage: physical goods provide more clear-cut protection, but they are inefficient because they carry physical distribution costs.

So far, each set of controls has been *general*. Print publishing provides impartial protection to whatever is being written, just as patent laws can protect many different ideas. A new class of controls is emerging that is neither institutional nor physical. These controls are also not general but highly specific, varied according to the nature of the information itself.

property would come inhibition of use, and a lack of progress. The paradoxical tradition of the FSF delivered a vast and amazingly good world of software, upon which much of the UNIX tradition rests.

⁴*Our* society is a relative thing. Intellectual property protections vary depending on the legal system. Illegal use of software in the United States is in the 30-40% range; in nearly all other countries it is higher. Source: Wall Street Journal, week of May 19.

Defining and Controlling Information

The Land of the Untamed Bandwidth, today's Internet and tomorrow's Matrix⁵, inhabits an underlying physical infrastructure yet replicates information almost costlessly. Once *owned* information gets loose in the Digital Realm, it is available for anyone's taking, and so the schemes that are used to release information into the world must be devised cleverly if creators' rights are to be protected.

By understanding information can we devise schemes for its distribution? The philosopher Pears has described information according to the following criteria:⁶

- **Stock.** Information can be accumulated, compiled and stored.
- **Flow.** Information flows from a source, and it can be released at a controlled rate.
- **Scarcity.** The less information available, the greater the worth of what remains.
- **Quality.** Information can vary in quality, where quality is determined by content. Quality in a music recording is could be a lack of static, in a story it could be the editing.
- **Production.** Information can be created almost from scratch, and there are an infinite number of ideas that can be generated from every real event. Once generated, information is subject to the semi-physical laws described above.

Let's connect all of the above with that economically relevant term, *market value*. This is how much people care that you are exercising rights over something. If you can control the essentials of information, you can influence its value. Stock market information is a very pure example. Once published in the local paper, the price of IBM is nearly worthless since it can be copied costlessly - "Say, Bob, did you know that

IBM closed at so-and-so yesterday?" However, under other circumstances, the price of IBM might be pretty valuable information. For example, people *will* pay for very timely prices, and stock listing services know this. Some will artificially delay your receipt of quotes or speed them up, because the delay itself determines value. If you can control the release of information, exploiting its uniqueness, timeliness and connectedness, then you can exercise rights over it.

Truly valued ethereal goods will be policed by a new sort of cop. The digital cop will be a fluid beast patrolling a world that is completely fluid, for the only relative constant in the digital world is its physical layer. As we already are starting to see, and in some cases as has existed for some time,⁷ information will largely police itself, because it can do so more effectively and at less cost than calling in the FBI. Protections may increasingly be integrated *into the object*. One-shot affairs such as movies on demand may be super-packaged in encrypto-readers that access information but that effectively prevent you from copying it, while software-on-demand might be downloaded in parcels that maintain open lines of verification with providers, but also obfuscate code beyond recognition until just before use. Some information objects, already sitting on your desk (or in your head?), may have to be plugged into the "information utility" in order for them to work, just as you rely on the electric company to keep the fridge humming. Its usage will be clocked elsewhere.

Many of the above ideas, such as movies or software on demand, make intimate use of the *pay-per-use* model, and so those ideas won't work unless pay-per-use also makes sense.⁸ In fact, the rationale for pay-per-use is so strong that some people predict 'full publishing' has seen its day. Knowledge engineers M.S. Miller and K.E. Drexler at Xerox explain the rationale behind pay-per-use:

⁵The Matrix is an emergent term for the "super" Internet, the network of networks of which the Internet is still only a part.

⁶The mathematically inclined might be interested in pure *information theory*, created by Claude Shannon at Bell Labs in the early 50s.

⁷The Software Industries Association, the recording industry's ASCAP, and the cable industry are all invested with substantial powers of surveillance and self-enforcement.

⁸Alternative approaches will abound. Among these will be the 'peep show' approach: "a browse costs some, and a nibble costs more".

"Consider the current [market]. Producers... put up with extensive illegal copying. Occasional users must pay as much for software as intense users. Software priced for intense users is expensive enough to discourage purchase by occasional users - even if their uses would be of substantial value to them. Further, high purchase prices discourage many potentially frequent users from trying the software in the first place."⁹

In fact, pay-per-use has always been with us, from the first puppet show to the library, to that indispensable modern institution, the video rental store. In deciding whether pay-per-use (vs. a one-time sale of limited perpetual rights) can work, the media, the transience of lending, and the method of compensation matter:

- **The traditional media for a given information object.** You watch movies on a screen, with a signal that might as well come from Mars. However, you grasp a novel and curl up on the couch with it. Lending conventional books out is one thing, however, just try a Digital Age tactic... such as renting out books on a phosphorescent screen. Certain information objects are more culturally amenable to pay-per-use than others. It will be easier to replace movies with a new distribution package than it will be to wean people off of story books.
- **Hoarding.** Ever met anyone with a shelf full of videos? How about a shelf full of books? They'd rather own just a few than rent them all. The more this is true for a given information/media combination, the harder it is to sell pay-per-use.
- **Economic incentives.** People buy videos because their children will watch them so often that the purchase price is cheaper than the rental price. Pay-per-use rates must be structured to discourage the purchase of perpetual rights.¹⁰ Further economics are at play. Publishers price products based on

the consumer's perception of their use and benefit, and higher margins may be easier to defend through outright sales. This is why tax programs cost less than \$50 while layout software can cost \$700, although the former may actually have cost more than the latter to create. If pay-per-use charges are set at a flat rate, they are also less appropriate for informational objects whose value increases only with use, be it complex software, because of its extended learning curve, or a jazz recording, due to its hidden aesthetic.¹¹

The key to much of the above discussion will be encryption, because just like cable, signals will still be vulnerable to interception. Encryption will make tapped information worthless unless the correct keys are available. Ah, says the skeptic, "cable redux, black market decrypters and the like!" This is not likely for several reasons. First, the industry is now more sophisticated, and so encryption schemes will have far more panache, including unique keys for each intended recipient. It used to be that anyone could hook up the same cable box and expect unlimited HBO, but the encryption of the future may be far more personalized, and so cryptographic attacks will have to hit much narrower targets. The second reason for confidence in cryptographic protection is that the new world is "bidirectional".

Bidirectional means that communications between you and your information provider will flow in both directions, a radical departure from the truncated dialogue between you and the local TV station. Bidirectional means that sophisticated, active interrogation schemes will prevail, an idea that is called "skepticism". The reverse of skepticism is the honor system and till now that has been tolerated by information providers because anything else is too expensive. Skepticism of remote elements will prevail in

¹¹What happens when information has a tangible element? Picture these three cases: the electronics for a new car, word processing software that comes with reference cards, manuals, etc., and a special headset for viewing 3D simulations. In each case, as the hardware becomes less specific to the software, pay-per-use becomes more realistic.

⁹"Markets and Computation: Agoric Open Systems" in *The Ecology of Computation*

¹⁰The expected cost of an outright purchase must exceed the discounted cost of rental payments.

this digital future because it will be cheap to implement, and many trap doors effectively will be closed.

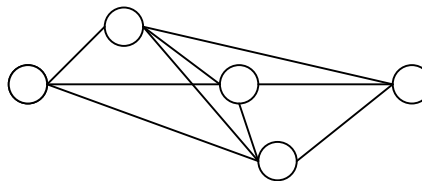
Information's Infrastructure

All of the preceding discussion of information content and pricing overlooks the physical layers beneath, but the supporting infrastructure of the Digital Future plays a key role. For the time being, our digital sights are dominated by that living cliché, the Internet. At its most atomic level the Internet in turn is dominated by a wondrous artifact of nuclear survivability - not the urban cockroach, but the *packet*. Packets are smaller units of information into which network communications are decomposed.¹² The more packets that you can send through a network, the higher is that network's *bandwidth*.

All is not so simple. Today's world is dominated by flat-rate connection pricing that is unresponsive to how much bandwidth is being used. The result is what economists call a 'commons problem'.¹³ To picture the commons problem imagine (as is now the case) that the capacity of the Internet is finite and that a number of people choose to use applications that quickly eat up a lot of that capacity. These people don't have to pay an extra amount for slowing down the whole network, so why should they care that they are making everyone else miserable? In a sense, the Internet is common property that is free to be abused, hence the "tragedy of the commons".

Resources across the present-day Internet are allocated very inefficiently because a mechanism is not yet in place that will keep everyone in line. Many people think that such a mechanism

will be based on *network* usage levies. To understand pricing issues, we need to understand how the Internet is set up. Imagine first that mythical Ma Bell owned the whole network, all the little lines below:



If this were so, pricing network usage would be simple: the packet is a convenient, standard measure of how much informational juice you are drawing,¹⁴ and so you could be charged by how many packets you are sending and receiving. There are three problems with this scenario:

Ma Bell does not own the whole network.

The digital realm is composed of many autonomous networks, and a single "TCP/IP" conversation may pursue several different paths across multiple networks. By contrast, in the established world of telephony conversations do not pass through too many networks, a single conversation pursues a single path, and billing systems have existed from the beginning, providing an early incentive for networks to coordinate. The bottom line is that when a digital conversation crosses several networks, the costs that each network incurs to bear that conversation cannot yet be recouped. However, there are certain strongly central Internet coordinating bodies and the computer industry is amenable to adopting standards, and so successful pricing coordination is entirely likely.¹⁵

¹² Perhaps things will change and packets will become an outmoded paradigm, but for technical reasons there are compelling reasons for them to remain the same - packets are robust and efficient. A communications method known as "statistical multiplexing" allows packets from diverse conversations to be pooled and thrust forward together, while failures to get through can be corrected at the packet level without endangering the whole conversation.

¹³This is what happens when everyone wants as much as they can get of something, there isn't enough to go around, and so everyone suffers.

¹⁴When you decompose information into bits and send them as packets, no matter what the information, a bit is a bit, and a packet is a packet. Because of this sameness, the packet is as general a measure as the kilowatt hour. However, just as kilowatt hour costs vary according to certain factors, including time of day, packets should also not always cost the same!

¹⁵ Telephone companies are devolving into a freer market, while the digital realm is becoming more orderly. In the end, similar mechanisms might be employed to conduct

Ma Bell does not necessarily control the whole 'conversation'. Information not only is decomposed into packets, the packets that compose a single "conversation" currently are routed independently, so that the conversation itself may flow across many different paths by the time it is completed.¹⁶ This may be true even though specific sub-networks (networks under unified control that are components of the whole) may choose to lock in specific conversational paths .

Neither party controls the length of the conversation. Remember that the digital future is bidirectional, that is, packets flow effortlessly in both directions. One recipient thus could be unexpectedly drenched with packets. This is very different from a phone conversation, where either party can control the duration of the call by simply hanging up (or not picking up), thereby limiting the bill. If charges are being levied by the packet, and it costs as much to send as to receive, are you charged when you unexpectedly receive a lot of packets from someone else?

In this brave new world, first principles are again a great place to start. We can build from these to discover the technical and economic regimes that may emerge. From the end-user's

business and to pass communications between proprietary networks. This is made even more likely because the telephone networks are often also the digital information networks - these networks can physically carry both flavors of information concurrently.

¹⁶Remember that the Internet was originally a military undertaking. Packet-level path routing was implemented to fortify the network against attack. For example, if during a conversation one of the paths (routers or lines) for that conversation were to be vaporized, network geography would adapt and the conversation could naturally find its way through by another path. However, this set-up may change. New protocols such as asynchronous transfer mode (ATM) set up virtual circuits that are maintained for the duration of a conversation. Although this method is less robust in the face of nuclear attack, because it requires less routing overhead, it is a more efficient choice in times of peace.

standpoint there are three basic considerations behind pricing: quantity, quality, share.

- **Quantity.** This is the most basic characteristic of the information being relayed. Depending on what is being transferred, size tends to vary by orders of magnitude. Most textual e-mail messages consume a few hundred bytes at most which, when sent over a network, constitutes scarcely more than a few packets. Graphics and file transfers rapidly ascend the size ladder, consuming at least tens of thousands of bytes. Transmissions with a time dimension, such as Internet radio or audiovisual conferencing, will further telescope size requirements.
- **Quality.** When you send an e-mail message, you usually don't care if it takes either one second or ten minutes to reach its recipient. However, an online audiovisual conference or a remote terminal session must perform in near real-time. By the same token, network problems that merely cause some static on Internet radio are ruinous during a file transfer, which cannot tolerate even a few corrupt bits. Speed and data integrity thus are both issues of transmission quality.
- **Share.** If you were to be charged for incoming packets, you probably would not be thrilled having to pay for someone else's junk e-mail. However, if you are receiving movies on demand, paying for their receipt is more reasonable. What about accessing Coca-Cola's Web page to sign up for a contest, or pointing to the IRS for tax information? Here the issue clouds a bit, for you are voluntarily accessing something, and yet it may also be in a provider's interest to offer that something to you for free. As with toll-free numbers, there should be a way to determine which party foots transmission costs, or if both parties should pay a share.

This section has discussed considerations leading up to pricing, the next will discuss actual mechanics. The Internet relies on humans for animation, and this is the reason pricing could be favored over other methods. However, engineering anything with a "human in the loop" will lead to results that are simply not predictable.

Pricing Issues

Many network veterans believe that charging for basic network use could be the Holy Grail of the digital world, the mechanism behind a final rationalizing of resources. With pricing, the digital landscape could undergo such fundamental changes that the result might best be described as a new era, "After Pricing". Such sweeping paradigm shifts could occur that this section's ideas need a caveat: they could end up being way off the mark. However, certain issues are still worth exploring.

Accounting issues. The current problem with pricing digital conversations on the basis of {quantity, quality, share} is that this must be done on a per-packet basis, but the decentralized nature of the Internet makes this difficult. Because each packet sent today is essentially autonomous, network providers must account for usage on a packet-by-packet basis. Because even modest digital transactions generate thousands of packets, this is a horrendous accounting problem, although not unsolvable. First, even large numbers of packets are a tractable, finite number. Second, the digital future will inherit DNA from existing components such as the cable, telephone, and cellular industries, all of which levy usage fees - it's a successful model!

To enable {quantity, quality, share} pricing each packet must also carry sufficient information. Packet headers currently identify the sender and recipient. An additional quality rating would prioritize and set pricing for the transmission,¹⁷ while a 'bill to' flag would determine who pays.

¹⁷If charges are levied on a per-packet basis, digital bandwidth providers should be as profitable as telephone companies now are. According to this logic, won't they provide as much capacity as the market generally needs? Not necessarily, because of the fact that especially 'bursty' applications, events, or times of day could suddenly bring even the most capable network to its knees. Just as electric utilities cannot prevent peak season brownouts, it does not make economic sense to build a digital network that can handle *any* level of use. Rather, the network should be capable of performing digital triage during emergencies, so that the most time-critical applications get priority.

Enhanced packet headers would mean real money and so would need protection. Because simply encrypting headers renders them unreadable to the network routers that must process them,¹⁸ a somewhat more sophisticated arrangement would be required. The alternative to adding this pricing "baggage" to each packet header is to identify the whole message instead. Given the current mode of transmitting messages, packet by autonomous packet, this is not practicable. However, future digital communications may not be many-pathed as they are today but instead carried over a single 'virtual circuit'. Packets would then be part of a complete stream, handleable in total.

With many networks levying use charges, how will they bill? If each charged end-users directly, the result would be a voluminous, piecemeal statement. One alternative would be trickle-down pricing, where charges are billed on a provider-to-provider basis, until accumulated at the *terminal* provider, who deals with the consumer. However, this idea is likely to be complicated and inefficient. An alternative is to forward charges to a central fee processor, who could then send a unified bill to the consumer. The shortcoming of this idea? Having everyone send their business to a single processor would be a hard sell. If network billing ever comes about, reconciling those bills is certain to be a very difficult issue.

As an aside, radio and television do not have to handle levies across several networks, but they do teach us something about pricing. These technologies produce public goods which are accessible to all the public and thus impossible to *explicitly* charge for. Instead, television and radio stations have inserted advertising to cover their costs.¹⁹ Because Internet content until now also has been largely public, it has favored advertising. However, its necessity should

¹⁸As the name implies, this hardware directs or "routes" network transmissions.

¹⁹It has been said that in places like Britain, people actually come in from the kitchen when the *commercials* come on, so I hesitate to call this implicit pricing!

decline as content pricing increasingly becomes an option.²⁰

Pricing issues and effects of pricing. Pricing may have a dramatic effect on consumer behavior. Although network use is very efficient and therefore will always be cheap, with network pricing it will cost something more than zero. On the information consumer's side, "surfing" will become less fashionable when the costs start adding up. While this will discourage casual discovery, it will spur the development of increasingly sophisticated search engines, directories and content programming.

The parties who actually may take the biggest hit are information providers who plan on subsidizing content, such as air freight shippers providing package tracking or online shopping malls. Till now these providers have faced fixed setup costs for servers, software and communications lines, but in the future they may pay a cost for each "hit" they take. Because of this, much stricter business criteria are likely to be applied to the establishment of "sites" (Internet or otherwise), including more disciplined payoff analyses. There are already concerted attempts at tracking usage, and even at capturing detailed user (read: "consumer") profiles.

And what prices should be set? Currently, packets from diverse sources and applications do not compete to get through to their destinations but rather are treated equally. When the communications lines and routers that comprise the Internet (and the future digital realm) are operating at less than capacity, there really is no need for competition because nothing needs to be sidelined to make way for anything more critical. Under these circumstances, no one ought to complain because the information queue moves at maximal capacity for all comers. However, when things do jam up, certain applications (and even certain personality types)

²⁰"Other factors aside" is a big loophole in this case. What really will happen is the equivalent of Tom Cruise drinking a can of Dr. Pepper in a movie. Especially with the level of content sophistication we are seeing, no one will abandon advertising; advertising will be seamlessly folded into content. As in the movies, content often will be just a sophisticated vehicle for advertising.

will suffer more than others. In the classic capitalist sense, those who want better service at times of stress just might be asked to pay more for the privilege. In economics this practice, called 'pricing at the margin', is known to yield an efficient outcome for all involved .

Marginal pricing is a *class* of schemes. It can range from an on-the-fly, automatic auction as packets pass through routers, to pre-arranged prices that attempt to pre-ration usage, to triage-style pricing schemes that allocate quality on the basis of how much any given packet announces it is *willing* to pay. To the consumer, pricing levels might be automatically associated with certain activities (e-mail is cheap, remote logins are moderate, "radio" is high) and there may also be an adjustable metre which consumers can set ("I'm feeling cheap today, I'll wait", or "I'm in a hurry, I'll pay"). Even with prioritization pricing, consumers may see *no difference in pricing* no matter what they are doing - quality may instead become a competitive issue between service providers. The big operators especially could opt to provide consumers with flat rate pricing, while having the internal capacity to implement their own, sophisticated triage schemes to control upstream bandwidth costs (the costs of providing outside network access to their users). Remember Sprint's "dropping pin" ads? Quality is certain to be a complicated and contentious issue.

Cold Hard Cash?

Up till now we've been going about this cyber world engaged in a discussion of how cold hard cash is intertwined with bits, networks and digital whatnot. However, the promise of the digital realm, a nearly effortless transport of information, has also been the challenge confronting monetized commerce. The ultimate paradox is that, in cyberspace, there is no such thing as cold hard cash.

The monetization of the digital realm will be its ultimate empowerment. Money will bring the development of cyberspace full circle, by connecting it with the world at large. Letting *trusted representations of value* flow through the networks will be very much like letting the genie out of the bottle and because of this the online community - opportunistic business, fascinated cyber travelers, wary government, and the consumer hordes - is uncorking very

GALORATH CONSULTING VERSION

carefully. The challenge is to find representations of value that can pass through an ethereal realm while remaining, paradoxically, anything but ethereal.

Proxies for cold hard cash abound, but let us first adopt the right frame of mind - what is *money*? Money is a general, divisible unit of exchange that makes it possible to buy goods of different value. It is also storable, so that it can be accumulated and spent when convenient. True money is anonymous and thus easily transferrable, letting it exchange hands in a wealth-increasing chain of economic transactions. Money must also be backed, i.e., some authority's imprimature must christen it legitimate, or else it would not be an accepted proxy for real goods. Will, can and should digital money be all this?

Digital money may be revolutionary not because it is electronic, but because it will be exchanged across the evolving information infrastructure. Without being "commerce-enabled", information could only be offered across public networks to satisfy non-monetary, or else only commercially strategic goals. Digital money changes all this, in a manner akin to opening a gateway in the sky between the ethereal world and the world of real goods... and cold hard cash. The only limit to the phenomenon of information is creativity, and networks of autonomous agents essentially supercharge this phenomenon.²¹ Letting those agents interact with money is like letting kids play with matches - things can happen with a multiplied effect to what is possible in the physical world alone.

The basic problem with digital money is that it must flow across the same insecure, digital pipelines as everything else. In fact, electronic wire transfers have been available to large institutions for some time. With prearrangement between established parties, including private networks, standard formats, encryption, trusted staff, etc., such transactions are relatively easy. Digital money evolves wire transfers down to a more egalitarian form, where any two parties can transfer funds under a wide variety of circumstances, outstripping the

physical and financial capabilities of current methods.

Just as there are several 'value products' in our wallets and pocket books, the digital realm will be equally diverse. The product used will depend on a number of factors, some detailed below:

- **Security.** Every transaction should be one to which the revealed buyer and seller agree, one that passes real value, which can also be authenticated.
- **Convenience.** Digital value products should enable transactions that can be as seamlessly and invisibly integrated into the existing application framework as possible.
- **Amount Spent.** Because informational content can be meted out in very small amounts, transaction charges may sometimes be measured in "micro cents". If so, processing costs must be even lower or else the profit will be negative. At other times, huge amounts may be transferred, requiring potentially cumbersome security²².
- **Anonymity.** This helps more than the pornography market. Particularly in a realm where records can be easily kept, if every transaction you commit to identifies you, then your precise purchasing profile can be compiled and exploited. Some people think this is scary.

Perhaps because transactional models are general enough to apply in any media, some value products in the digital ether will be analogous to those in physical use. However, they may be very technically different and supercharged with new functionality. Some possibilities:

Cash. Unique, encrypted units of value that are backed by real money and can be exchanged freely. Digital cash is the closest thing to physical money, for it can be bought, stored and *anonymously* transferred. To use digital cash, you literally buy some, hold onto it until you're willing to spend it, and then trade some of it; whomever receives the cash is then free to spend

²¹ This sentence hints at a potential, future section titled *Systemics*.

²²As they are now, largely over private networks, using the Electronic Data Interchange format.

GALORATH CONSULTING VERSION

or save it. By definition, digital "cash" must be self-authenticating, a feat that is achieved either through an internal algorithm or through storage on tamper-proof hardware.

Credit. Transactions that are tied into the conventional credit card infrastructure. Buyers transmit their encrypted credit card numbers, which are then processed conventionally. With credit card purchases, additional information can be passed, automatically defeating simple copying attacks. The encrypted transaction can state an amount, what is being bought, the time of purchase, a *digital signature* and who the intended recipient is. The danger to credit transactions is not copying, but cryptographic attacks. If a message can be decrypted, then your credit card account number lies naked to nefarious purposes.

Check. Personal guarantees of payment, redeemable through a variety of means including interbank transfers. Digital checks would rely on digital signatures, against which only cryptographic attacks would present a serious threat. Checks can be written for any amount, although processing costs are too high for very small transactions. In addition, there is no ceiling to the financial loss against a fraudulent check.

PIN. Using this system, buyers give sellers a personal identification number to pay for a transaction. The seller contacts a clearing house, which then sends a message back to the buyer asking whether the trade was valid. This system was used first by Internet bankers First Virtual, who completely dispensed with encryption, choosing instead to send followup confirmations of transactions via e-mail. Buyers must pre-register with First Virtual, which charges transactions to the buyer's credit card account. Although processing costs place the minimum feasible charge well into the multiple-cent range, PIN systems permit "divisible" micro cent charges. Sellers can simply accumulate charges in micro cents until they meet First Virtual's feasible minimum, and then send the fee on.

All communications in the First Virtual system are open and thus subject to spying, but would-be felons would have to intercept the PIN number when sent, then intercept First Virtual's confirming e-mail back to the buyer. While each of these things is easily done, combined

they are more difficult and easily detected, while the loss for any given transaction is limited by credit card laws. By the way, even if credit cards are being used, PIN systems can be designed for anonymity.

Unique Tokens. As discussed, digital cash is designed to literally self-authenticate when interrogated. This may be a dangerous tactic because the cash is relying upon the sanctity of its encapsulated algorithm, and anything that is protected can eventually be broken. However, there is an alternative approach to digital cash which does not involve self-authentication. In fact, it's elegance is such that it needn't involve encryption. Imagine that "tokens" are sent out to buyers, each with a uniquely identifying code. Upon redemption of the token, its code - and thus the token itself - immediately can be authenticated against a list of released codes. When a token is redeemed the code is struck from the list, and so forgeries (which must arrive later) are instantly detected. The token system relies on the buyer's protection of unclaimed tokens, and on the issuer's ability to produce codes that cannot be appropriated fraudulently.²³ Depending on how they are designed and implemented, tokens may allow both anonymity and divisibility.

If the Digital Realm is to allow unbounded amounts of value to flow, then there is a serious security challenge ahead. We're talking *money*. Relentless and serious attack awaits such a system, using methods that include *sniffing* (listening in), *spoofing* (impersonation) and *cryptanalysis* (code-breaking). With the statelessness, anonymity, newness and special characteristics of the media, limitless fraud is imaginable. On this note, the advice of the cyber-commerce team at *First Virtual Holdings Co* is worthwhile: design a transaction system as any good engineer might. First, transaction systems should be redundant; if any protection is compromised, further protection awaits. Second, systems should limit loss; they should be partitioned, alarmed, and limited by design, so that real catastrophes are always averted.

What will be the impact of having a parallel universe of digital value which exists apart from

²³ Among other protections, codes could be randomized, spaced far apart, encrypted, and would probably have an expiration date.

the traditional money supply?²⁴ The answer depends on how far apart from that supply it exists, which in turn depends on the value product that is used. The more closely digital transactions are linked to the conventional financial infrastructure, the less uncertainty there is. Digital checks will transfer real money stored in real banks, so there will be no impact whatsoever. Digital credit cards will be linked fully to conventional credit cards, and although credit cards do have a positive impact on the extended money supply, this has already been going on for years.

Digital cash is where the real money supply questions arise. An issuer of digital cash has an incentive not to back its value product with real cash on a one-to-one basis. After all, not everyone will ask to redeem their digital money at once and, if not being asked for, money is an expensive thing to just hold onto. If the minting of digital money is not backed fully with real cash, then what happens is similar to banks' practice of *fractional lending*. Fractional lending lets an institution lend out much more cash than it really has; it holds onto only enough so that the fraction of its customers who ask for money on any given day will get paid. This is now something that only banks are allowed to do. The government will have to decide whether it wants to extend fractional lending to *digital cash*. If it does allow fractional lending, and the use of digital cash booms proportionate to the overall economy, then the money supply will increase noticeably.

There is at least another possibility which will lead to digital money becoming totally disengaged from the conventional money supply. Imagine a system based on barter, but instead of two parties actually exchanging goods and services, they receive storeable points whenever they give away something. These points can then be redeemed for other goods and services. Appropriately enough, these points

can be called *money!* If all of this happens digitally, then a parallel money supply emerges.

What of other demons? The key attribute of digital value will be spatial and temporal *fluidity*. Witness the workings of fluidity thus far - foreign exchange traders lay siege to economies, drug money flows to safe havens, illicit transactions are enabled. Under certain conditions and for certain value products, digital value will have a worsening effect. However, all may not be lost. Currently, if you use your credit card to buy items in another state, you pay state tax. If you put a lot of money into a personal account, you attract notice. If you deliver a false set of goods, you commit mail fraud. As much as it is thought of the other way around, digital cash represents an extension of the real world into the ethereal world, including the checks and balances (adequate or not) that have evolved against financial abuse.

Stay Tuned to Wisdom for the Digital Era?

Depending on feedback, the following sequels to *Cold Hard Cash* are planned:

The Systemic View. What systems theory has to say about the Digital Revolution.

Warfare. To conventional, nuclear, bacteriological and chemical warfare, add information.

Media Redux. Digital media examined from the perspective of media past and present, including a dose of media theory.

Infodigitalia. Wild and conventional thoughts about digital information.

Neo-Luddites. Man against machine, Part Deux.

The Revolution May Not Be Digitized. Revolutions can only be judged so once they're over. Don't put this one to bed yet.

²⁴ This is a useful question because economies depend on such things as the money supply. Although economists themselves disagree on how important the money supply really is, changes in it may at least effect inflation, and also the government's ability to manage the economy.