[Home] [Current Edition] [Compendium] [Forum] [Web Archive]
[Email Archive] [Guestbook] [Subscribe] [Advertising Rates]

The Future of Digital Cash on the Internet

By David C. Stewart
Director, Global Concepts
Email: david@global-concepts.com
URL: http://www.global-concepts.com/

Digital cash for the Internet is a hot topic. A number of viable payment schemes exist. This document reviews a few of these payment schemes and evaluates their respective potential to prosper on the Internet.

Micro-Payments

When most people speak of digital cash, they speak of "micro-payments." In my opinion, a payment mechanism that cannot handle sub-penny payments is not a true "micro-payment" system. I prefer the term "mini-payment" system. We will discuss a number of them shortly. But first, let us look at what we really mean by micro-payment systems.

Micro-payment systems have been touted as the revolutionary agents of the Internet. We are frequently challenged to imagine a day when Internet content providers charge mere cents or even fractions of a cent for information. Your daily dose of Dilbert might cost a tenth of a cent, and the daily update on your stock portfolio might cost you a nickel. Compared to the physical world, where we entertain the notion of eliminating the penny as a relevant payment instrument, micro-payments may seems pretty far-fetched. In my opinion, consumers simply do not want to make micro-payments. After all, we don't like them in the physical world. We top off our gas tanks and leave pennies on the counter for the next change-averse shopper. Nevertheless, the technology exists, so let us assume for the moment that eventually we might have to cope with micro-payments.

Millicent

Millicent is the most promising of these technologies. A thorough description of the technology can be found at the following Web site: http://www.research.digital.com/SRC/personal/stev eg/millicent/millicent.html .

A product of Digital Equipment Corporation, Millicent is based on a scrip model. Unlike a traditional scrip model in which each merchant sells scrip to each consumer, Millicent relies on a scrip broker. The broker, conceivably a bank or bankcard association, is a third party who accepts payments from consumers on the front-end, and scrip credits from merchants on the back-end. The broker issues its own scrip to consumers, eliminating the need for merchants and consumers to have prior relationships before transacting.

To make low-value transactions cost effective, Millicent sacrifices security. Its designers assume that "some" fraud will occur but in such small denominations as to be negligible. Essentially, Millicent was developed as a "lightweight" payment scheme with "lightweight" security for "lightweight" transactions. It could incorporate more powerful encryption or procedural security than it does, but the inherent computing and administrative costs would likely exceed the value of the transactions for which it is intended.

Millicent is pocket change and is expected be treated accordingly. In general, I believe that simply resigning yourself to "some" fraud is a bad idea. If a cyber-crook could pose as a broker and filter a tenth of a cent from each scrip transaction, the exposure could become very real. To quote William Proxmire, "A billion here, a billion there and pretty soon that adds up to real money." That there will be billions of Millicent transactions is presumptuous, but when evaluating risk we need to assume the system might actually succeed. If Millicent takes off, it will undoubtedly need tweaking to address its admittedly high potential for fraud. Mini-Payment Systems A more practical system for payment on the Internet is one that operates in the realm of real denominations.

Mini-payment systems facilitate transactions that fall somewhere between micro-payments and cost-effective credit card transactions for most merchants this is about $.25 to $10.00. A handful of systems exist, but only a few have any real hope of surviving in the near future. Bearer Certificates vs. Notational Systems Digital cash comes in many different flavors; one of which is bearer certificate system. Bearer certificates are "as good as cash;" whoever holds the certificate holds the value. As digital cash changes hands, value ownership is transferred immediately. An alternative to bearer certificates is a notational system, in which transactions between two parties are logged by a third-party processor, but no actual value changes hands until the processor moves funds from one account to another. The systems discussed below fall into one of these two categories.

eCash from DigiCash

DigiCash has system called eCash. It is a bearer certificate system, meaning whoever holds the eCash holds its monetary value. Mark Twain Bank in St. Louis was the first, and still is the only, eCash issuer in the US. However, DigiCash has signed issuing agreements with many large banks overseas. Today eCash constitutes the vast majority of digital cash transactions on the Internet, but its future looks dim in the US market. Why? DigiCash s insistence on privacy. Privacy is the cornerstone of the eCash model. DigiCash does not believe that the issuing bank should necessarily know which customers receive which digital tokens. To accomplish this level of consumer privacy, the system uses "blind signatures" as the way for the issuing bank to certify each token it issues. The process actually requires the customer, not the bank, to generate eCash tokens. Using DigiCash s electronic purse software, the customer creates blank tokens and forwards them (hidden in a digital envelope) to the bank for certification. The bank stamps its signature on on each token, debits the customer's account for the amount of eCash issued and sends the tokens back over the Internet. The bank never sees the actual tokens until they are presented by the payee.

Furthermore, because the whole system is software-based, duplicating certified eCash tokens is a trivial event. After all, digital cash is a just a string of bits. There is nothing stopping a consumer from creating ten copies of the same token. This loss of control on the issuing side must be made up for on the clearing side of the transaction. Therefore, during each eCash transaction, the merchant must make a real-time online connection to the issuing bank to be sure the tokens presented by the consumer haven t been redeemed already by another payee. Each token is matched against a redeemed tokens file. If the customer has played by the rules, the query finds no matches and the transaction is okayed. If the customer has made and already spent duplicates of those tokens, the transaction bombs.

The fact that eCash requires online verification of each token exchanged during a transaction severely limits its application in the US market. This process requires both the merchant that accepts eCash on the Internet and the consumer who spends it to have account relationships with the same institution. Today that institution is Mark Twain Bank. Obviously, this is highly impractical for most US merchants and consumers. DigiCash's model is much better suited for markets with a more centralized banking system, where clearing and settlement are less encumbered by single-bank issuance.

Another major fault with eCash is that it is software-based. Unless a bearer-certificate system can be used in the physical world in addition to the Internet, I believe it will fail on the Internet. Consumers will find little value in a bearer-certificate system reserved exclusively for the Internet. Without migrating its system to chip-cards that can function on and off-line, DigiCash will find eCash to be short-lived in the US.

CyberCoin from CyberCash

CyberCash rolled out its own version of digital cash in October 1996. The product, CyberCoin, relies on a notational system rather than a bearer certificate model. As with any other digital cash scheme, the consumer prepays for CyberCoins. A key difference between CyberCoin and other models is that value is not actually transferred to the consumer's PC, chip card, or in this case the CyberCash Wallet. Funds are held in escrow in a proxy account set aside for that consumer at CyberCash s bank in Virginia. The consumer need not have an account at that bank. When the consumer makes a transaction with a merchant, CyberCoins are transferred from the consumer's CyberCash Wallet to the merchant's CashRegister, using CyberCash as the central processor for the transaction. CyberCash simply keeps track of which consumer is paying which merchant and in what amount.

Essentially it is a book entry transfer system. CyberCash then transfers funds from the consumer s proxy account to the merchant s proxy account. The merchant, like the consumer, does not need an actual account at CyberCash s bank. If the merchant wants to deposit CyberCoins in its own deposit account, it must request that CyberCash initiate an ACH transfer to the merchant s bank. There are fees associated with the transfer. Therefore, it behooves the merchant to make transfers only when enough funds have accumulated in its CashRegister to be cost effective.

The fact that each transaction does not require inter-bank clearing and settlement, allows CyberCash to accommodate low dollar transactions cost-effectively. CyberCash designed its system to handle transactions as small as $0.25. The CyberCash system offers a low-risk solution to financial institutions. Neither consumers nor merchants can effectively counterfeit CyberCoins, because the system does not rely on bearer certificates. No one can introduce value into the system. CyberCash knows exactly how much CyberCoin has been bought or transferred, and it controls the funds.

The greatest fraud risk is to the consumer in the event that someone gets access to his or her PC and makes CyberCoin purchases. But such is the risk with any software-based system. The greatest downfall of the CyberCash model is not its security, but its lack of application to physical world transactions. When dual-purpose digital cash is readily available, CyberCoin will probably feel the same squeeze as eCash. However, the threat will not be as great to CyberCoin for a number of reasons.

CyberCash is working very hard (and successfully) to distribute its Wallet software via software products like the Netscape browsers. The Wallet's broad distribution base will help solidify CyberCash's position as the payment processor of choice for Internet transactions whether via credit cards, digital cash or other schemes. Furthermore, because CyberCoin relies on the existing payment system infrastructure, it will proliferate easily without resistance from the banking industry neither the consumer's nor the merchant s bank need even be aware that CyberCoin transactions have occurred.

Despite its strong points, however, I believe CyberCoin will eventually concede market share to more versatile bearer certificate systems like Mondex or Visa Cash. Either way, CyberCash stands to do very well as a transaction processor. It announced in September 1996 that was integrating Mondex processing capabilities into its software. When Mondex hits the Net, CyberCash will be ready.

Mondex

Unlike the systems discussed above, Mondex was born off-line and is migrating toward the Internet. Mondex is entirely chip card-based, and it is unique in that it can accommodate card-to-card transfers. Like the eCash system, Mondex uses bearer certificates; funds are stored remotely on the user s actual card. Unlike eCash, however, Mondex funds can be transferred from one card to another indefinitely without requiring central clearing or verification by a bank or processor. Therefore, Mondex is the closest of all the digital cash systems to real cash.

The key difference between Mondex and cash is the audit trail that Mondex provides. Mondex cards record each transaction with a unique identifier that can be used to track funds if necessary. The key to Mondex is its security, which exists in two primary aspects of the system: the hardware of the card, and the value transfer process. Mondex banks on the security of its chip card system. The notion behind Mondex's hardware security is that funds cannot exist anywhere but on a Mondex card. Even the central issuing facilities rely on racks of high-dollar Mondex cards to store and write value to the cards that are issued for public use.

Once in use, no other chip card or hardware device posing as a Mondex card could interface with a real Mondex card. Mondex cards detect spoofs and refuse to transfer money to them. The system relies on the fact that each card is certified by a Mondex digital signature. The transfer process itself is also extremely secure. When a transfer occurs between a consumer and a merchant, for example, the two cards not only verify each other s authenticity, but the transfer occurs in a sequential process so that funds cannot possibly exist in two places at once. Funds are deducted from the consumer s card before they are written to the merchant s card. It doesn't work any other way.

Because Mondex is a card-dependent system, one of its biggest stumbling block is that it requires card readers in the hands of consumers. This is no trivial requirement. It makes one wonder whether DigiCash might have been right to have introduced eCash as a software-only system for the Internet. Nonetheless, Mondex will do all right. Devices like the VeriFone VeriSmart card reader are available for around $100, and the prices will fall over time. For around $60 a user could buy one of the new card readers from InteliData that are built into standard 3.5" floppy diskettes. These devices will need to be formatted so they can interact with Mondex cards, but that will happen soon enough.

I think the Fall trial of Mondex on the Internet, using AT&T employees as a beta market, will show that Mondex is a secure and cost-effective Internet payment system. With the proliferation of card readers from companies like VeriFone, InteliData, GemPlus and others, the technical barriers will fall.

A more significant barrier to Mondex is an economic barrier: it is not clear how banks are going to make money on it. To begin with, the issuing institution does not profit from any float. To issue Mondex money involves buying it up front from Mondex. Only then can a financial institution issue Mondex funds to its customers. Once funds are in the market, the financial institution likely will not collect transaction processing fees, because the system does not necessarily require bank involvement unless a user wanted to make a deposit/withdrawal or just exchange the Mondex card for cash. Economic barriers aside, I think Mondex is the best of the digital cash schemes in terms of long-term viability. It's a cool system.

Visa Cash

Visa Cash answers some of the tough economic questions presented by Mondex, in that the issuing financial institution earns float on Visa Cash. A bearer certificate product from Visa, Visa Cash is chip card-based. Any Visa bank can issue Visa cash, and earn float income and, in the case of disposable Visa Cash cards, residual value that gets forgotten or discarded by consumers.

The system made a splash at the Atlanta Olympics, but the trial has since settled down to just a trickle of transactions. It is not clear when Visa will announce a trial of Visa Cash on the Internet. Considering the recent Internet trial announcement by Mondex, of which MasterCard is a majority owner, Visa will likely introduce something soon.

While Visa Cash is an easier sell to the banking industry from a financial perspective, it lacks some of Mondex's versatility. With Mondex, users can transfer money from card to card indefinitely. The bank need only be involved if a deposit is made. With Visa Cash, consumers don't have that luxury. One reason is that banks would have to forego the current processing fee they charge for each merchant deposit. Another is the perceive security threats from having digital cash "out there" where banks can't keep an eye on it.

A third reason is the float. Imagine if consumers could make card-to-card transfers? For example, Bank A, Bank B and Bank C issue Visa Cash to consumers A, B and C respectively. If consumer A pays $30 to consumer B, then consumer B now has a card with Visa Cash issued from both Bank A and Bank B. If consumer B now pays $20 to consumer C, how should the chip cards determine which bank's Visa Cash to transfer? It may seem immaterial, but if consumer C were to make a deposit, the banks that issued the deposited Visa Cash are going to loose float. Arbitration rules are needed, like first in/first out or last in/first out, but no such rules exist for Visa Cash. Until they do, Visa Cash will have less flexibility than Mondex.

Conclusions

So what does it all mean? I think the market today is dominated by eCash, because it has been the only thing available. Nonetheless, the number of transactions is probably minuscule. CyberCoin is in the ring now and will quickly surpass eCash, because it is more versatile and better suited to the US payments industry.

Ultimately, however, CyberCoin will lose market share to multi-purpose systems like Mondex. A system that can exist online and off-line will be more valuable to the digital consumer than an Internet-only solution like CyberCoin. And while Mondex may get an early lead on Visa Cash or its Internet equivalent, it s a harder sell to the banking industry.

More banks will issue Visa Cash than Mondex. Visa also tends to be more aggressive in its marketing campaigns than MasterCard, so Visa Cash will catch up quickly.

I see the whole thing shaking out in about seven or eight years. By then, Mondex, Visa Cash, CyberCoin and a few other emerging systems, will have the lion s share of the market. If I had to guess at the future market share distribution for digital cash transactions on the Internet, I would estimate the following:

Year:	2001	2005
CyberCoin	51%	21%
Mondex	20%	32%
Visa Cash	20%	36%
eCash	5%	1%
Other	4%	10%

As far as overall sales, I would estimate that by 2001 we will see over $10 billion in digital cash transactions. This will be due in large part to booms in pornography, gambling, video games and Internet phone services all off which are greatly enabled by the mere existence of digital cash. Other information services like news and commercial information will further push the transaction volume and total sales associated with digital cash. In the end, digital cash will be a real part of the digital economy over the next 5-10 years and beyond.