SHARE
SHARE 59
TWEET
COMMENT
EMAIL

STEVEN LEVY 12.01.94 12:00 PM

E-MONEY (THAT'S WHAT I WANT)

The killer application for electronic networks isn't video-on-demand. It's going to hit you where it really matters - in your wallet. It's, not only going to revolutionize the Net, it will change the global economy.

Clouds gather over Amsterdam as I ride into the city center after a day at the headquarters of DigiCash, a company whose mission is to change the world through the introduction of anonymous digital money technology. I have been inundated with talk of smart cards and automated toll takers and tamper-proof observer chips and virtual coinage for anonymous network ftps. I have made photocopies using a digital wallet and would have bought a soda from a DigiCash vending machine, but it was out of order.

My fellow passenger and tour guide is David Chaum, the bearded and ponytailed founder of DigiCash, and the inventor of cryptographic protocols that could catapult our currency system into the 21st century. They may, in the process, shatter the Orwellian predictions of a Big Brother dystopia, replacing them with a world in which the ease of electronic transactions is combined with the elegant anonymity of paying in cash.

He points out the plaza where the Nazis rounded up the Jews for deportation to concentration camps.

This is not idle conversation, but a topic rooted in the Chaum Weltanschauung - state repression extended to the maximum. David Chaum has devoted his life, or at least his life's work, to creating cryptographic technology that liberates individuals from the spooky shadows of those who gather digital profiles. In the process, he has become the central figure in the evolution of electronic money, advocating a form of it that fits neatly into a privacy paradigm, whereby the details of people's lives are shielded from the prying eyes of the state, the corporation, and various unsavory elements.

Fifteen years ago, David Chaum seemed a Don Quixote in Birkenstocks, a stray computer scientist talking of a technology that appeared more rooted in science fiction than high finance. Today, still bearded, but wearing a well-tailored suit, he stands in the thick of a movement that seems unstoppable - the digitization of money. His passion now is to explain that the change need not be oppressive. He travels among bankers and financiers, he runs a company, he proselytizes. And he hopes somebody listens, because the wild card in the era of digital money is anonymity, and David Chaum thinks we're in trouble without it.

Dollar Bills or Bill Dollars

The next great leap of the digital age is, quite literally, going to hit you in the wallet. Those dollar bills you fold up and stash away are headed, with inexorable certainty, toward cryptographically sealed digital streams, stored on a microchip-loaded "smart card" (a plastic card with a microchip), a palm-sized "electronic wallet" (a calculator-sized reader and loader for those cards), or the hard disk of your computer, wired for buying sprees at the virtual mall.

Of course, real money - the trillions of dollars handled each day by banks, other financial institutions, and government clearinghouses - is already digital. No physical tokens are exchanged: all transactions are conducted using streams of bits. But digitizing the final mile of electronic money, where the coin and dollar bill go the way of the vinyl LP, will make all the difference in the world. It will not only change the physical way you spend your money, it will alter the way you view your own economic being. And depending on the manner in which it is implemented, digital money might allow others to view your financial status with a decidedly discomfiting intimacy.

Is e-money really going to happen? Inevitably. Hard currency has been a useful item for a few millennia or so, but now it has simply worn out its welcome. A recent paper by several cryptographers at the Department of Energy's Sandia National Labs in Albuquerque, New Mexico, begins by enumerating what all e-money advocates identify as the fatal flaws of cold hard cash: "The advent of high-quality color copiers threatens the security of paper money. The demands of guarding it make paper money expensive. The hassles of handling it (such as vending machines) make paper money undesirable. The use of credit cards and ATM cards is becoming increasingly popular, but those systems lack adequate privacy or security against fraud, resulting in

MOST POPULAR

SECURITY
How Meltdown and Spectre Were Independently Discovered By Four
ANDY GREENBERG

GEAR
What Is MicroLED and When am I Going to Get It?
BRIAN BARRETT

BUSINESS
James Damore's Lawsuit Is Designed to Embarrass Google
NITASHA TIKU

MORE STORIES

a demand for efficient electronic-money systems to prevent fraud and also to protect user privacy."

"Cash is a nightmare," says Donald Gleason, president of the Smart Card Enterprise unit of Electronic Payment Services Inc. "It costs money handlers in the US alone approximately US$60 billion a year to move the stuff, a line item ripe for drastic pruning. The solution is to cram our currency in burn bags and strike some matches. This won't happen all at once, and paper money will probably never go away (hey, they couldn't even get rid of the penny), but bills and coinage will increasingly be replaced by some sort of electronic equivalent."

The coming of e-money would seem to demand that the governments of the world get together and implement a scheme to make the shift in an orderly fashion. But that's not happening. The US, in particular, is promulgating public cluelessness. When I called a spokesperson for the Federal Reserve to ask about electronic cash, he laughed at me. It was as if I were inquiring about exchange rates with UFOs. I insisted he look into it, and he finally called me several days later with the official word: the Federal Reserve is doing nothing in that area.

Outside the Fed, there are people in government interested in the issue - isolated visionaries in the Department of the Treasury and Congress, in the Office of Technology Assessment - but while they ponder it, plenty of other institutions are devising schemes that will knock our currency preconceptions for a loop. The timetables are short, and as the players look around and see what their potential competitors are doing, those timetables get even shorter, particularly in the race to be first to deliver a plan that offers transactions on computer nets.

For starters, there is CyberCash Inc., sort of an all-star team of pre-digital cash technologies. Headed by Bill Melton, the creator of the Verifone system that handles credit-card transactions between merchants and banks, the principals include Jim Bidzos, president of the cryptography provider, RSA Data Security Inc., Steve Crocker, vice president of Trusted Information Systems Inc. (another prominent crypto-firm), and Dan Lynch is chair and founder of Interop Co. (which produces the largest Internet trade show worldwide). "We will provide cyberspace with financial communications that will be safe and secure and convenient," says Bruce Wilson, CyberCash's chief operating officer. In the first quarter of 1995, CyberCash will offer a network equivalent of debit-card transactions, then expand to credit cards. The next step: cash-like components that support peer-to-peer payments.

Visa has gathered a consortium of financial institutions to design "Electronic Purse," specifications for low-cost purchases at gas stations, convenience stores, grocery stores, fast-food restaurants, and school cafeterias, in addition to such routine items like calls from pay phones, road and bridge tolls, and videogames.

Citibank has been running a prepaid card test in a Long Island facility. There is the aforementioned Smart Card Enterprise of the Electronic Payment Services company, which wants to piggyback spending money on its network of ATMs.

There is the NetCheque project, a debit-card system, developed by the Information Sciences Institute at the University of Southern California. And there is the Information Networking Institute, part of Carnegie Mellon University, whose NetBill is also based on the debit-card model.

Many transit companies envision fare tickets as coinage to buy newspapers and sundries. The phone companies issue phone cards with similar pretensions.

In Denmark, Danmont has distributed over 100,000 cards with money for spending on such things as parking meters and laundromats. Similar systems exist in Portugal and Singapore.

Mondex, a consortium led by two British banks, will roll out its digital-cash system, involving an estimated 40,000 cardholders, to the public in Swindon, England, next year. Its creators envision the system spreading worldwide, as people slip their smart cards into special phones and wallets to conduct cash-like, tamper-proof transactions, even across borders. "It will become ubiquitous - it's the cheapest way of moving money around," says Dave Birch, spokesperson for the project's consultants, Hyperion. "There's the state of Ohio which has in the works a smart-card system for replacing welfare checks with electric money. At Mankato State University in Mankato, Minnesota, students are issued "MavCards," to be used not just for MCI long-distance calls and dining-hall meals but for cash services like photocopying, vending, and laundry.

Finally and inevitably there's Microsoft. For months, it had been quietly organizing a digital money group, presumably to put its own stamp on the emerging phenomena of digital transactions. But things went into overdrive in October, when it laid out $1.5 billion worth of stock to snatch up Intuit, Inc. a financial software company which was determinately moving towards automating money. Along with the buyout, Scott Cook, Intuit's president, became Microsoft's executive vice president of electronic commerce - reporting directly to chairman Gates, begging the question, will dollar bills be replaced by Bill dollars?

As a result of this mad rush, the road to digital cash is not so much a smooth transitional path but a multi-lane cloverleaf with infuriating turnoffs, circles, and dead ends. "A lot of people assume there's going to be a single form of digital money," says Microsoft's chief technical wizard, Nathan Myhrvold. "Today we have a zillion different ways of doing financial transactions. There's cash, checks, credit cards, debit cards, wiring money, traveler's checks ... each of these has a particular point. We're going to see that much diversity in digital money."

Kawika Daguio, a Washington, DC, representative for the American Bankers Association, is familiar with the issue and says, "We may be in a situation analogous to the 1860s - in those days, before our current Federal Reserve system, bank checks backed by different institutions weren't as widely accepted - they circulated and were usually discounted. Chartered banks also printed private-bank notes. Now, we see that some institutions are interested in printing their own versions of electronic money and following their own rules."

Sholom Rosen, a vice president at Citibank, puts it more succinctly: "There are going to be winners and losers, but everybody is going to play." Michael Nash, Visa's senior vice president in charge of the cash-products division, recalls the excitement among executives last June when they witnessed a test of the credit-card consortium's smart-card experiment at a retreat in Cancun, Mexico: "We had senior banking executives lining 70-deep to try this out!"

Considering all these schemes in the aggregate, it is possible to envision the way money will work in the future. But we must distinguish between forms of electronic commerce - including credit cards and bill paying - and electronic cash, in which money is in a fungible, universally accepted, securely backed format and can be passed, peer to peer, through many parties while retaining its value. You know, money.

First of all, imagine that all the uses of credit cards and debit cards are seamlessly integrated into electronic format. Now start to think about real money. Cash will reside in credit-card-sized plastic smart cards which can be stored in palm-sized "electronic wallets." The days of nervously accessing the ATM machine at 2 a.m., looking over your shoulder for muggers, are over. You'll download money from the safety of your electronic cottage. You will use these cards in telephones (including those in the home), as well as electronic wallets, disgorging them whenever you spend money, checking the cards on the spot to confirm that the merchant took only the amount you planned to spend. The sum will be automatically debited from your stash into the merchant's. Cash will be a number, a digitized certificate you'll probably never see.

Commerce on the Net will reproduce the process in cyberspace: you will download money from your bank, put it in a virtual wallet, and spend it online. You will also be able to receive money from your employer, someone who buys something from you, or a friendly soul who lends you a virtual sawbuck until payday.

Exactly what goes on inside smart cards, wallets, and computers won't be apparent. But the protocols chosen by the lords of e-money are all-important. Depending on how they work, the various systems of electronic money will prove to be boons or disasters, bastions of individual privacy or violators of individual freedom. At the worst, a faulty or crackable system of electronic money could lead to an economic Chernobyl. Imagine the dark side: cryptocash hackers who figure out how to spoof an e-money system. A desktop mint! The resulting flood of bad digits would make the hyperinflationary Weimar Republic - where people carted wheelbarrows full of marks to pay for groceries - look like a stable monetary system.

A privately circulated paper written by Kawika Daguio sketches out some of the problems in the form of questions:

Who is going to create the monetary value?

In other words, who will back up the money, assuring trust. Will it be government? Banks? Visa? The New York City Transit Authority?

"A dollar bill is a piece of paper - what's the difference between that and another piece of paper?" asks Sholom Rosen of Citibank. "It is the ability to present that piece of paper and get assurance of a return. It's not backed. There was a time when it was backed, but those times are gone. What gives it value? The banking system. The paper is the liability of the banking system. The supply of money is grown and disappears in the banking system."

Yet others seem to think that, if universally trusted, a digital currency system can, in effect, float on its own momentum. "If you have money on the network, you can make private money on the network," says Eric Hughes, a co-founder of the privacy champions, the Cypherpunks. He is now exploring the possibility of setting up a cyberspace bank. "It's easiest not to turn the money into paper if you don't have to."

What security features will be included?

How will these systems protect against fraud? Can they be hacked or counterfeited? What will be the trade-offs between ease-of-use and security?

"People get sticky fingers," says Rosen. "The most honest guy in the world will find some cash and stick it in his pocket. When outsiders hear about digital-cash schemes, the first thing they say is, 'I'm going to break in.' "

Of course, smart cards have to be tamper-proof so people can't reverse engineer them and double-spend. The prime protection is cryptography. "The bits in a container have to move from one to the other," explains Rosen. "When you're done, you have to have less in one container and more in the other. Also, your transaction can't be intercepted. Crypto can secure the transition. How strong the crypto is depends on who's going to try to break in - if it's the Mafia or a national government, they'll have plenty of resources."

David Chaum thinks, for instance, that some canny dark-side entrepreneurs can crack the Mondex system now being tested in England. Though its mathematical protocols are strong, he says, too much depends on the tamper-proofing of the cards. "One device can say, 'OK, I'm transferring $100,000 to you,' and the other one says, 'Oh, fine, I believe you.' So if you break either one of those open (defeating the tamper-proof technology) and tell it you've got a zillion dollars, the whole system just dies." (Mondex insists its scheme cannot be cracked, but will not provide further details. "Suffice it to say we're betting the shop on it," says Dave Birch.)

Will they work so the value will be restored if they're lost?

Everybody seems to agree that smart cards holding digital cash should provide an option to punch in a Personal Identification Number before buying something; but there is also a consensus that most people won't use that option. "The consumer won't bother with that," says Visa's Michael Nash. "The key here is that we imagine this as expanding what you do with credit cards. We do not think the electronic purse is appropriate for people buying jewelry or automobiles." In many systems - Mondex is a good example - losing your stored-value smart card is like losing a wad of bills. Don't carry more than you can afford to lose.

Who's going to regulate electronic money?

At the moment, all the players are proceeding as if no one is. They extrapolate a regulatory system growing out of the current one, while they are aware that as the digital economy becomes pervasive there may be calls for new limits and regulation. As for now, the rush is to get everything in place, and no traffic cops seem to be slowing anybody down.

Who's going to pay for it?

"I don't believe that it's sound policy to charge somebody royalties for engaging in the virtual world's equivalent of putting your hand in your pocket, pulling out a bill, and handing it to somebody," says Kawika Daguio. He is particularly perturbed by the claims of Online Resources & Communications Corporation, a company in Virginia that insists that it holds a patent (US # 5,220,501) giving it "exclusive rights to process real-time electronic transactions of consumers who use any in-home terminal to purchase goods and services, pay bills, and bank through a debit network, including the automated teller machine networks." Online Resources further claims that "the patent covers all in-home terminals, including telephones, computers." (The patent may be challenged by banks and ATM processors.)

On the other hand, Microsoft's Myhrvold, perhaps anticipating a licensing revenue that would make DOS look like a drop in the bucket, challenges Daguio's assertion, claiming that we already pay the equivalent of such a fee. "Of course you do," he says. "Explicitly or implicitly there's a fee involved. Even in a pure-cash transaction, you pay for those costs. Cash is an expensive thing to move around. You have to hire guards from Brinks with guns and all that bullshit. That's all included in the price of things you buy."

The bottom line is that nothing is free, especially when it comes to money. You will pay for e-money, either in transaction fees or, as in the CyberCash model, by allowing others to earn interest on your electronic cash - even as it sits in your virtual wallet.

In short, the various systems have implicitly or explicitly postulated tentative answers to some of these questions, and the answers to others, such as the regulatory structure, will have to evolve as the idea catches on. But one question remains open: the dichotomy between privacy and traceability.

Hard cash, of course, is anonymous - you can spend your printed bills with the assurance that no one can trace your expenditures or compile a dossier on your lifetime spending records. But electronic cash has no such assurances. Its computer-mediated nature makes traceability the course of least resistance. This gives rise to a provocative question: Can digital cash become anonymous, as real-world money is? And if so, should it be?

And these questions lead us back to Amsterdam - headquarters of DigiCash, the company formed by David Chaum.

Digital Money Man

In the world of digital cash, David Chaum is the marked penny that keeps reappearing. His ideas circulate as freely as cash itself. He is indisputably the pioneer of the field, the one who shifted it from the ether of science fiction to the solid footing of mathematical truth. But the man himself is the center of controversy. All of those involved in the daring attempt to shred dollar bills into arcane mathematical formulae know of Chaum, and almost all admire his work. But when they talk of their dealings with him, they immediately go off the record. It turns out that at one point they considered licensing Chaum's patents or at least recruiting Chaum's participation in their projects. These processes seemed to end in fruitless standoffs, sometimes acrimonious ones. Then, inevitably, more negotiations. Chaum cannot be ignored even by those who disparage him off the record.

Why are all these people so worked up about David Chaum?

I get a hint the day after my ride with Chaum through Amsterdam. We have made plans to meet at a coffeehouse off the Keizersgracht.

Our plan is to spend the entire day talking about digital money and his work. But before the tape recorder goes on, Chaum takes pains to make one thing clear to me: he is not, as some people derisively call him, some sort of privacy nut. He is by no means a paranoiac, but merely someone who has made some remarkable discoveries that people should know about before they make irrevocable choices about the traceability of their finances.

Fine, I say, and begin the interview. Tape recorder on. "How old are you?" I ask. "I don't tell that to people," he says.

At heart, David Chaum is driven by ideals. Indisputably the brains behind making digital cash work, he holds the key patents in the field, particularly in the area of anonymous, untraceable cash. He is therefore in a position to become a very rich and powerful person. Yet he avoids the path of least resistance and largest revenues - cashing in by licensing his schemes - because he is passionate about the potential of anonymous cash and wants the news of its viability spread far and wide.

He says that if, after knowing that the possibility of private, digital-monetary transactions exists, people opt to spend their money with the same traceability as credit cards, he will accept the decision. But he doesn't think that will happen. His guess is that once people are aware of the issues, they will agree that traceable routes are the evil of all money.

From a very early age, David Chaum had an interest in the hardware of privacy. "What's important to realize is that there is a strong driving force for me," he says. "My interest in computer security and encryption came from my fascination with security technologies in general - things like locks and burglar alarms and safes," he says. (As a graduate student, he devised two new designs for locks and came close to selling both to major manufacturers.) And, of course, he was very much fascinated with computers. In high school and college, he did typical hacker sorts of things: password cracking, dumpster diving, and such. But he was also picking up some serious background in mathematics. And late in his college career, he came to cryptography, a discovery that in retrospect seems inevitable.

Chaum's first major papers, published in 1979 when he was a graduate student at the University of California at Berkeley, are indicative of his strong focus in his work: devising cryptographic means of assuring privacy. His ideas build upon the concept of public-key cryptography, the technique devised by Whitfield Diffie and Martin Hellman in the mid-'70s that established cryptography as a mass technology. Specifically what excited Chaum was the use of digital signatures - a way of establishing the authenticity of a message sender. "I got interested in those particular techniques because I wanted to make [anonymous] voting protocols," he says. "Then I realized that you could use them more generally as sort of untraceable communication protocols." The trail led to anonymous, untraceable digital cash.

Dining with the Cryptographer

For Chaum, the politics and the technology reinforce each other. He believes that as far as privacy is concerned, society stands at a crossroads. Proceeding in our current direction, we will arrive at a place where Orwell's worst prophecies are fulfilled. He delineated the problem in an essay called "Numbers Can Be a Better Form of Cash Than Paper." "We are fast approaching a moment of crucial and perhaps irreversible decision, not merely between two kinds of technological systems, but between two kinds of society," says the article, published in 1991. "Current developments in applying technology are rendering hollow both the remaining safeguards on privacy and the right to access and correct personal data. If these developments continue, their enormous surveillance potential will leave individuals' lives vulnerable to an unprecedented concentration of scrutiny and authority."

In the early 1980s, Chaum conducted a quest for the seemingly impossible answer to a problem that many people didn't consider problematic in the first place: how can the domain of electronic life be extended without further compromising our privacy? Or - more daring - can we do this and increase privacy?

In the process, he figured out how cryptography could produce an electronic version of the dollar bill.

In order to appreciate this, you have to consider the apparent obstacles to such a task. The most immediate concern of anyone attempting to produce a digital form of currency is copying. As anyone who has copied a program from a disk to a hard drive knows, it is totally trivial to produce an exact duplicate of anything in the digital medium. What's to stop me from taking my one Digi-Buck and making a million, or a billion, copies? If I can do this, my laptop, and every other computer, becomes a mint, and infinite hyperinflation makes this form of currency worthless.

The answer to the problem of digital duplication lies in using digital signatures to verify the authenticity of bills. Only one serial number would be assigned to a given "bill" - the number itself would be the bill - and when the unique number was presented to a merchant or a bank, it could be scanned to see if the virtual bill was authentic and had not been previously spent. This would be fairly easy to do if every electronic unit of currency was traced through the system at every point - but that would bring about exactly the kind of surveillance nightmare that gives Chaum the chills. How could you do this and unconditionally protect one's anonymity?

Chaum began his solution by coming up with something called a "blind signature," a process by which a bank, or any other authorizing agency, can authenticate a number so that it can act as a unit of currency - yet the bank itself does not know who has the bill, and therefore cannot trace it. This way, when the bank issues you a stream of numbers designed to be accepted as cash, you have a way of changing the numbers while maintaining the bank's imprimatur.

One of Chaum's most dramatic break-throughs occurred when he managed to come up with a proof - though for a different application - that this sort of anonymity could be provided unconditionally, with all the assurance of mathematical proof that no one could violate it. The idea came when he was driving his Volkswagen van from Berkeley to his home in Santa Barbara, where he taught computer science at the University of California in the early '80s. "I was just turning this idea over and over in my head, and I went through all kinds of solutions. I kept riding through it, and finally by the time I got there I knew exactly how to do it in an elegant way."

He presented his theory with a vivid example: a scenario of three cryptographers awaiting the check after finishing their meal at a restaurant. The waiter appears. Your dinner, he tells the cryptographers, has been prepaid. The question is, by whom? Has one of the diners decided to anonymously treat his colleagues - or has the National Security Agency paid for the meal? The dilemma was whether this information could be gleaned without compromising the anonymity of the cryptographer who might have paid for the dinner.

The answer was fairly simple. It involved coin tosses hidden from certain parties. For example, A and B could flip a quarter behind a menu so C couldn't see it - and then each write down the result and pass it to him. The key stipulation would be that if one of them was the culprit who paid for the meal, that person would write down the opposite result of the coin toss. Thus if C received contradictory reports of the coin toss - one heads, one tails - he would know that one of his fellow diners paid for the meal. But without further collusion, he would have no way of knowing which one. By a collection of coin tosses and combined messages, any number of diners could play this game. The idea could scale to a currency system.

"It was really important, because it meant that untraceability could be unconditional," he says. Meaning mathematically bulletproof. "It doesn't matter how much computer power the NSA has to break codes - they can't figure it out, and you can prove that."

Chaum's subsequent work, as well as the patents he successfully applied for, continued to build upon those ideas, addressing problems like preventing double-spending while preserving anonymity. In a particularly clever mathematical twist, he came up with a scheme whereby one's anonymity would always be preserved, with a single exception: when someone attempted to double-spend a unit that he or she had already spent somewhere else. At that point the second bit of information would allow a trace to be revealed. In other words, only cheaters would be identified - indeed, they would be providing evidence to law enforcement of their attempt to commit fraud.

This was exciting work, but Chaum received little encouragement for pursuing it. "For many years, it was very difficult for me to have to work on this sort of subject within the field, because people were not at all receptive to it," Chaum says. For several years in the early 1980s, Chaum attempted to personally contact the leading lights in privacy policy and share his ideas with them.

"The uniform reaction was negative," he says. "And I couldn't understand this. It made it all the harder for me to keep pushing on this, because my academic advisors were saying, 'Oh, that's political, that's social - you're out of line.' Even the department head at Berkeley said, 'Don't work on this, because you can never tell the effects of a new idea on society.' I acknowledged him in my dissertation, saying it was the rethinking and finally the rejection of this principle that caused me to do this work."

Eventually, Chaum decided that the best way to spread the ideas would be to start his own company. By then he was living in Amsterdam. On a visit with his Dutch girlfriend, he had fortuitously met up with some academics at CWI, Centrum voor Wiskunde en Informatica, the nationally funded Dutch Center for Mathematics and Computer Science in Amsterdam, where he subsequently formed the cryptography research group. So, in 1990, he launched DigiCash b.v., a subsidiary of the US company DigiCash Inc., with his own capital and a contract from the Dutch government to build and test technology to support anonymous toll payments on highways. Chaum developed a prototype by which smart cards holding a certain amount of verified cash value could be slipped into a gadget affixed to the windshield, and high-speed scanning devices would subtract the tolls as the cars whizzed by. The cards could also be used to pay for public transportation and eventually other items. Of course, the payments would be anonymous. After completing that contract (the system has not yet been implemented), Chaum kept his company active in smart-card applications; some of the projects focused on cash systems that would be used in a building or complex of buildings. The DigiCash headquarters, along with several businesses and agencies around the Netherlands, use the system currently. But to date, the company's operations have been relatively small-scale, even as the world has now come around to seeing the significance of the ideas Chaum hatched in isolation. DigiCash remains independent, without a close alliance with a large partner in banking or financial services. Chaum feels that in time such partners, at least licensees of DigiCash technology, will emerge; if so, his paradigm will be a crucial factor in maintaining privacy in the age of e-money. This is an idea Chaum believes is worth holding out for.

Some people interpret this as stubbornness, or at the least poor business practice. "People wanted to buy David's patents but he asked for too much - he wanted control," says a former DigiCash employee. "The real problem is that privacy isn't what the banks want, it isn't what the stores want. They want something easy to use, fast, and very cheap." (Still, this source guesses that Chaum "has hung on for so long that he will probably succeed.")

Frustrated by not being able to use Chaum's patents, some companies have devised their own schemes for anonymity, which may or may not infringe on Chaum's. More recently, Stefan Brands, formerly at CWI, has come up with an alternative scheme that has drawn considerable interest. Brands contends the system absolutely does not infringe Chaum's patents; Chaum's carefully worded response is, "He's not convinced me that it doesn't."

The topic of patents is touchy; Chaum bridles at any talk that equates him with the robber-baron set. In his mind, the revenues are secondary to the potential effect on society. "It's my mission to do this, because I had this vision that stuff like this might be possible, and felt it was my responsibility to do it. No one was working on this for the good half-dozen years I was; they all thought I was nuts. They gave me a hard time. We couldn't license, really, without the patents; the whole purpose of them is to get this stuff out there."

Hidden Values

Does anonymity really matter when it comes to electronic money? Some people dismiss its significance - or argue that anonymity is a bad thing.

"Speaking for myself, it would be dangerous and unsound public policy to allow fully untraceable, unlimited value digital currency to be produced," says Kawika Daguio of the American Bankers Association. "It opens up opportunities for abuse that aren't available to criminals now. In the physical world, money is bulky. In the physical world, it is possible to follow people, so a kidnapper can potentially be caught if the currency is marked, if the money was being observed on location, or if the serial numbers were recorded. Fully anonymous cash might allow opportunities for counterfeiting and fraud."

Nathan Myhrvold of Microsoft concurs. "There's a role for untraceable transactions. But it's not a panacea. Some people get very worked up about it. But there's been a very steady trend away from untraceable cash. There are cases where explicit traceability is a good thing. Like in my business expenses. I want them to trace it! All these things are there for a reason. They're not there as part of a plan by nefarious Big Brother. Look, I understand Chaum's concern to a certain degree. There's a lot of concern for privacy today. But I do worry about the idea of saving people from themselves. Just because I sign up for a traceable form of money doesn't mean I want my next-door neighbor to see my transactions."

Chaum says he has never argued for total untraceability, but sort of a constrained anonymity. "My work has been trying to establish a whole space of possibilities, bounded by pure perfect anonymity on one side and a perfect identification on the other side."

Chaum is not the only person working this turf: building on his ideas, researchers at Sandia Labs have been working on a scheme that attempts to balance anonymity with law enforcement's need to trace criminal transactions. Sort of an anonymous, digital-cash Clipper Chip. "I was concerned about some of the effects electronic cash could have on criminal activity," says Ernie Brickell, a Sandia cryptographer. "It could make it very easy for people to undertake kidnappings and extortion. It might be possible for a person to do a kidnapping and ask for money to be exchanged in a way in which there was no physical exchange - you would have no idea what country the person was in. There was also the potential that new types of criminal activity would emerge. So we looked at whether it would be possible to develop electronic cash schemes in which people could have much of the privacy that Chaum talks about, but with hooks in it, so that if law enforcement had the need to look into a transaction, it could."

Yet it is not at all clear that even this sort of limited anonymity will gain, er, currency. Users of electronic cash - the general public - will probably never be polled on whether they prefer it to be anonymous. Brickell admits that anonymity will be a hard sell. "There's going to be so much information about individuals floating around, that we want to protect privacy as much as we can," he says. "But some of the bankers feel that an anonymous system is never going to make it, or even be something that they can get behind." In fact, says Niels Ferguson, a cryptographer who works for DigiCash, "the people who decide actually often have an interest in not protecting people's privacy because they are among the potential benefactors of gathering the information."

But what of the Nathan Myhvolds, who seem to argue that they want traceability? Ferguson sighs. "Oh, the number of times I've had to argue with people that they need privacy! They'll say, 'I don't care if you know where I spend my money.' I usually tell them, 'What if I hire a private investigator to follow you around all day? Would you get mad?' And the answer always is, 'Yes, of course I would get mad.' And then my argument is, 'If we have no privacy in our transaction systems, I can see every payment - every cup of coffee you drink, every Mars bar you get, every glass of Coke you drink, every door you open, every telephone call - you make. If I can see those, I don't need a private investigator. I can just sit behind my terminal and follow you around all day.' And then people start to realize that, yes, privacy is in fact something important. Any one part of the information is probably unimportant. But the collection of the information, that is important."

Which is exactly why certain officials are licking their chops at the prospect of traceable cash. These include, of course, law-enforcement agencies, who are more than eager to see hard cash phased out. What would the drug dealers do? The money launderers? The underground economy? They will argue that granting anonymity to digital cash would provide a bonanza for kidnappers, muggers ... criminals of every stripe. But consider a world where all money is electronic and traceable, and you have the most potent crime-fighting weapon in history.

The institution with the most to gain is the Internal Revenue Service. The computer age has been very good to the IRS, which now has access to any number of databases that yield reality checks on any given citizen's tax returns. Traceable cash would accelerate this process, and the tax-collection agency can't wait to take advantage of it. In a recent speech - presented on April 15, no less! - Coleta Brueck, the project manager for the IRS's Document Processing System, described some of the IRS's plans. These include the so-called "Golden Eagle" return, in which the government automatically gathers all relevant aspects of a person's finances, sorts them into appropriate categories and then tallies the tax due. "One-stop service," as Brueck puts it. This information would be fed to other government agencies, as well as states and municipalities, which would draw upon it for their own purposes. She vows "absolutely" that this will happen, assuming that Americans will be grateful to be relieved of the burden of filing any taxes. The government will simply take its due.

"If I know what you've made during the year, if I know what your withholding is, if I know what your spending pattern is, I should be able to generate for you a tax return," she says. "I am an excellent advocate of return-free filing. We know everything about you that we need to know. Your employer tells us everything about you that we need to know. Your activity records on your credit cards tell us everything about you that we need to know. Through interface with Social Security, with the DMV, with your banking institutions, we really have a lot of information, so why ... at the end of the year or on April 15, do we ask the Post Office to encumber itself with massive numbers of people out there, with picking up pieces of paper that you are required to file? ... I don't know why. We could literally file a return for you. This is the future we'd like to go to."

It isn't the future that David Chaum would like to go to, though, and in hopes of preventing that degree of openness in an individual's affairs, he continues doggedly in his crusade for privacy.

Megabucks on the Net

Cyberspace is destined to be the first battleground of the digital money wars. While it will take years, perhaps decades, for e-money to replace hard currency in the physical world, the virtual world not only can't accommodate the current system, but is desperate for immediate implementation of the digital equivalent. Everyone agrees that the Internet is the staging ground for the first true boom in electronic commerce, but it's a transactional wasteland. You can't buy anything without a credit card. You can't even collect on a $2 bet with a friend.

It is here that the difference between electronic money and electronic cash will become most apparent. The network equivalent of some of the current forms of electronic commerce - traceable credit cards and debit cards - are already well under way. One of the prime movers in this initiative is the CommerceNet consortium, which intends to deliver an infrastructure for, among other transactions, encrypted credit-card payments through the Net. These will work exactly like regular credit-card transactions, except that the actual account numbers will be scrambled so eavesdroppers, known as packet sniffers, can't intercept them and make illegal charges. Sort of the electronic equivalent of crumpling up the carbons.

Of course, these transactions are officially traceable - "When you buy something, the seller is identified to the buyer," says Cathy Medich, executive director of CommerceNet.

While this is undoubtedly useful, the open structure of the Net begs for a more cash-like system. Why should only those businesses pre-approved as official merchants be able to sell things? Why can't people transfer money to one another? "If I owe you $25 and say, 'I'm good for it, I have a credit card in my wallet,' what can you do?" asks Bruce Wilson, chief operating officer of CyberCash. "You can't do anything. You're not a merchant. That's the situation in the online world, with virtual storefronts and countless potential entrepreneurs who can't process credit cards. There are millions of college students who want space on a server to sell things. Poets who want to sell a limerick of the day. Weather servers with satellite images. They need a cash-like methodology. For those people, anonymity is not an issue. It's simply the problem of doing peer-to-peer payments. You to me, you to a relative. That's why we have a requirement for cash. So if Wired magazine has an archive of articles on a server, and a researcher is sitting somewhere at 2 a.m. searching the Net, he can say, 'Oh, here's five articles by this expert Steven Levy.' And he can download those articles. For a dollar, a dollar-fifty, two-fifty an article. He's happy to have it!"

CyberCash, of course, is planning to offer a system that will do network cash, but is reserving judgment on the degree of anonymity it will use. "If the marketplace is looking for anonymity, our service will not be used if it is not offering it to a sufficient degree," says Bruce Wilson. "If it never becomes an issue, it will not need to be there. For our cash services, we plan a middle-of-the-road approach."

Meanwhile, there is "e-cash," offered by David Chaum's DigiCash. Anonymity is at the center of e-cash, which works with Windows, Mac, and Unix clients. I played with a beta version in Amsterdam and found it easy to use - as simple as reaching in a pocket and buying something but leaving no digital trace. This ease is indicative of all e-money schemes, really: mundane on the surface but either repressive or subversive underneath. A simple example: if Chaum's scheme could be used for downloading the thousands of documents available on the World Wide Web, then anyone could start a cottage business by selling files for low prices - say 10 cents, 25 cents apiece. (Chaum says that the cost for a transaction would eventually be infinitesimal, maybe one-tenth of a cent.) Eventually, as bandwidth increases, information in all sorts of formats - like audio and video - could be offered for cash. And no trail would follow the buyers - the sellers could not automatically stick your buying preferences on a mailing list. The government could never track your reading preferences. Or, to be honest, your lack of tax payments. Whereas in the alternative, everything might be traced.

E-cash rolled out on an experimental basis early this fall (http://www.digicash.com/). Each user, upon enrollment, gets $100 in token CyberBucks. This can be e-mailed to friends and acquaintances or spent in coins, simply by tapping a mouse.

How anticlimactic - clicking on "OK" to fork over funds! But unseen to the user, something miraculous is going on. Computer cycles are furiously crunching cryptography that represents the very best of David Chaum's dream. Secure money, accurately accounted for, unconditionally untraceable. It is a proof of concept that the future need not be one where purchases are tied to spenders.

At press time, DigiCash counted 15 businesses and organizations around the globe, including Encyclopaedia Britannica, getting ready to set up "shops" that will sell info for e-cash. Presumably, these new virtual storefronts will raise the sophistication level of the system from its initial state, which is, considering that e-cash is the vanguard of a new financial system, rather casual. Of the first few places to spend CyberBucks, one was the DigiCash store (where you could buy a reprint of a Chaum article, "Achieving Electronic Privacy," Scientific American, 1992, for $2.84 in digital cash). Another was something called Big Mac's Monty Python Archive Shop, offering homegrown transcriptions of Monty Python movies and routines for various increments of CyberBucks. A disclaimer cheerfully admitted a direct approach to the copyright question: it read, "I basically just stole these texts."

In a sense, that sophomoric admission gets to the heart of e-money. If anonymity becomes a standard in cyberspace cash systems, we have to accept its potential abuse - as in copyright violations, fraud, and money laundering. Innovative new crypto schemes have the potential for mitigating these abuses, but the fact of anonymity guarantees that some skullduggery will be easier to pull off. On the other hand, the lack of anonymity means that every move you make, and every file you take, will be traceable. That opens the door to surveillance like we've never seen.

"You have to let your readers know how important this is," Chaum tells me when discussing online anonymous cash. "The choice can only be made once." He thinks that if an economic system that tracks all transactions comes to cyberspace, the result would be much worse than the situation in the physical world. "Cyberspace doesn't have all the physical constraints," he says. "There are no walls ... it's a different, scary, weird place, and with identification it's a panopticon nightmare. Right? Everything you do could be known to anyone else, could be recorded forever. It's antithetical to the basic principle underlying the mechanisms of democracy."

David Chaum believes, as he wrote in an article in 1992, that "in one direction lies unprecedented scrutiny and control of people's lives; in the other, secure parity between individuals and organizations. The shape of society in the next century may depend on which approach predominates."

How Anonymous Electronic Money Works

Smart cards

1. Alice wants to fill her empty smart card with untraceable e-money taken from her bank. She inserts her card into an ATM-like slot in a machine at home or on the street. The gold computer chip on the card sends a random key to the bank in a digital "envelope." The bank signs the envelope with its signature, ensuring that the "money" inside can be trusted. Think of the envelope as having carbon-paper innards. The signature outside will transfer to the note inside without the bank knowing the destination of the money. The bank then sends the envelope back to Alice's smart card, which strips away the envelope,leaving a complex numerical code. Alice now has anonymous cash.

2. Alice can venture into the world and spend her e-money anyway she wants - as bus fare, at a mall store, in parking meters, or even to lend money to a friend, slipping the card into her friend's "digital wallet."

3. The recipient of anonymous e-money copies the math-money from Alice's smart-card chip and then has its computer add its own account ID number to it. This aggregate number (the money) is sent to the bank. (For added security, the bank might send an acknowledgment back to the recipient, but it's not essential.) The bank then credits the recipient - bus company, store, city, or friend - with the specific amount of money. However the bank cannot trace the money to Alice.

Network

The entire process can run on a network as well. Instead of the calculations hap-pening on a gold microchip inlaid on a credit card, the transactions take place on the motherboard chip of any computer logged on the Net.

1. Alice's computer communicates with the bank, loading up with anonymous money.

2. She can send her e-money anywhere an e-mail message can go, and just as fast - to a mail-order outfit, a bill-collection agency, her mortgage company, or some kids publishing a brash electronic magazine.

3. Recipients then e-mail the money to their bank accounts, where the amount is ready to be made into e-money again.

Both smart card and networks meld into one system. Computers' slot readers will enable them to spend money from smart cards, or fill up smart cards with money earned on the Net.

#MAGAZINE-2.12

VIEW COMMENTS

HACK BRIEF

Russian Hackers Release Apparent IOC Emails in Wake of Ban

LOUISE MATSAKIS

GROUNDED

Inside the 4-Day Disaster that Nearly Broke JFK Airport

ALEX DAVIES

TAKEOFF

Climb Inside Bell's (Theoretical) Flying Taxi of the Future

JACK STEWART

ROBOTICS

A Robot That Tugs on Pig Organs Could Save Human

MATT SIMON

INTERNET CULTURE

Meme's Best Friend: The Rise of 'Doggo'

ANDREA VALDEZ

PHYSICS

CAN AN ARROW FIRED STRAIGHT UP FALL FAST ENOUGH TO KILL YOU?

RHETT ALLAIN

WE RECOMMEND

POWERED BY OUTBRAIN

KLINT FINLEY

When Wi-Fi Won't Work, Let Sound Carry Your Data

WIRED STAFF

Liveblog Day 3: Watch Us Touch All of the Gadgets at CES

ADAM ROGERS

Softwear: How an Underground Fashion Label for Nerds Got Cool

WIRED STAFF

CES 2018: More Gadgets We're Drooling Over

ANDY GREENBERG

WhatsApp Security Flaws Could Allow Snoops to Slide Into Group Chats

GET WIRED MAGAZINE
Don't Let the Future Leave You Behind
SUBSCRIBE NOW

GET WIRED MAGAZINE
Don't Let the Future Leave You Behind
SUBSCRIBE NOW

GET OUR NEWSLETTER
WIRED's biggest stories delivered to your inbox.
Enter your email
SUBMIT

FOLLOW US ON YOUTUBE
Don't miss out on WIRED's latest videos.
FOLLOW

CNMN Collection

Use of this site constitutes acceptance of our user agreement (effective 3/21/12) and privacy policy (effective 3/21/12). Affiliate link policy. Your California privacy rights. The material on this site may not be reproduced, distributed, transmitted, cached or otherwise used, except with the prior written permission of Condé Nast.