(Originally published in the Los Angeles Times Magazine on February 4, 1996.)

Money is coined liberty, said Dostoyevski, a fact I bear in mind as I climb the impossibly steep stairs to the canal-side "Secret Annex" in Amsterdam, in which Anne Frank and her family hid from the Nazis. Survival in the annex depended on the courage of the family's Gentile helpers, and the cash box from which the Franks drew the coin of their sustenance. I feel spoiled walking through these hushed rooms, gross with freedom and affluence, my pockets full of credit cards and travelers checks, all useless had I been forced to hide with the Franks and their friends. In their situation, what you needed was some divisible unit of exchange that you could hand to someone else with no trace of its provenance attached. What you needed, in other words, was money.

Cash grants its user the cloak of anonymity, which in those days was a tattered cape indeed. Amsterdam is a city historically hospitable to Jews; Sephardim fleeing the Spanish Inquisition helped make this metropolis Europe's diamond center. But the municipal authorities, in an excess of organizational zeal, kept meticulous records at a low-slung brick building in the city's Plantage district. It's still there, next to the zoo, with a plaque on the front. This was the city registry, where they recorded your name, your address and your religion. When the Nazis arrived in 1940, their chores were thus lightened. The registry granted its owners the power of life and death; when it was clear what the data were being used for, resistance fighters tried to destroy the records, which were too tightly packed to burn. Dutch Jewry burned instead.

These lessons are not lost on plump, rabbinical David Chaum, an extraordinarily insightful cryptographer whose little company on the outskirts of Amsterdam is developing a way to carry the tradition of cash onto the frontier of cyberspace, so that purchases on the growing global network of computers known as the Internet can be made securely and privately. Unlike, say, American Express, whose databanks theoretically could be used to assemble detailed dossiers on the lives of its cardholders, Chaum's system would make such elaborate knowledge of an individual's actions, habits and beliefs unobtainable. It sounds harmless enough until you consider the implications in light of the history of money, whose increasing intangibility over the centuries reaches something of an apotheosis in the airy offices of Chaum's company, DigiCash BV.

Chaum is generally agreed to be the father of something called "digital cash," which is like regular cash in that it can be spent with privacy but unlike regular cash in that it has no physical presence. Think of it as the spirit of cash, or maybe even its soul, the essence of the thing without the corporeal shell.

As a concept, Chaumian digital cash has enormous ramifications. Basically, it means that anyone with a personal computer could take on the money-creating functions of a bank--even a central bank, like the Federal Reserve. If I did that, no one would accept my currency, of course. But what if General Motors did it? Or a consortium of Swiss banks? No less than Walter Wriston, the legendary former chairman of Citicorp, has observed that DigiCash is "reviving in modern guise something very close to the old American free-banking system." The system, in other words, that existed before there was a single national currency.

Money is fascinating stuff, and it was to understand this purest new form of the substance I have spent so much of my life worrying about that I'd come to Amsterdam. I wanted to meet the man who had liberated cash from the encumbrance of its body and to find out from the liberator--whose ideas have implications for

commerce, privacy and national sovereignty--precisely what he thinks he is doing.

A Question of Privacy

If David Chaum were motivated solely by making money--receiving income, we should say in this context--he would long ago have signed a deal with some of the major companies rushing into the field of electronic transactions. Like all missionaries, however, Chaum is a man of faith, so profit manifestly is not his primary goal. Chaum is an American, a Jew from Los Angeles with a Ph.D. in cryptography from UC Berkeley. He is a large, soft-spoken man with a graying beard and a ponytail. Although he likes meeting with journalists because his main interest is in selling his ideas, the same spirit that brought forth those ideas keeps him from talking much about himself, which does little to dispel the vague air of cyberspace paranoia that clings to them.

"I'm not paranoid," he insists. "I resist giving out unnecessary information."

Chaum's mission is to save us all from the potentially Orwellian marketplace that the rise of networked computers is about to make possible: a marketplace in which physical cash is replaced by its electronic representative residing on a microchip-embedded card or a computer hard-drive, and in which every petty transaction at a pay phone, toll booth, vending machine, newsstand or donation plate thus is recorded by computer. Not just the sum, mind you, but the time, place and, most important, the identity of the person making the expenditure could be instantly and permanently memorialized.

"This strikes at the heart of our values--democracy, free markets," Chaum says. "It could ruin our whole way of being."

The problem is that while cash still accounts for 80% of the 360 billion transactions that occur in the United States annually, coins and paper money are increasingly passe. Governments dislike cash transactions because currency is hard to track and increasingly easy to counterfeit, thanks to modern computer technology. Big business, which finds it easier to skirt taxes by relying on lobbyists rather than unreported income, doesn't like cash either; bills and coins are bulky, heavy, easy to steal and expensive to process--and they earn no interest.

The ultimate push for a new kind of money arises from the newest kind of market: the Internet, which is growing by leaps and bounds. Many things are possible on the Internet, but many of them aren't happening because existing payment systems are inadequate to the new medium. Clearly, the new paths that commerce will take will not be currency-friendly.

The worry is that if we choose something like the credit and debit cards that are increasingly popular today, we could be giving up much of the personal autonomy we take for granted--the autonomy that comes with cash. Nor is privacy the only thing at stake. As Chaum reminds us, "Credit card organizations are allowed to decide who can get credit cards and who can accept them. Also, you can be disenfranchised. Your money--your credit and money--can be inaccessible at the drop of a hat."

Chaum expressed the situation most powerfully in his seminal article on the subject in the August, 1992, Scientific American: "The choice between keeping information in the hands of individuals or of organizations is being made each time any government or business decides to automate another set of transactions. 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."

He's right, I think to myself. Once the system becomes completely digitized based on the credit- or debit-card model, they'll have us. Then I remember how little I use cash and why. My favorite credit card yields frequent-flier miles, convenient tax receipts and a month of free float. It makes me impervious to muggers and saves trips to the bank. Sure, you can reconstruct my activities from my Visa statement. I've done it. I actually like this capability. What do I care who knows the name of my favorite Italian restaurant? But then I think of Amsterdam's former municipal registry. Isn't it weird the way marketing types who call my home or bug me with junk mail seem to have an unerring sense of what I buy, what I do, who I am? Don't I charge my newspaper and magazine subscriptions? Haven't I used my Visa to make some political donations? Didn't I once use it to purchase a menorah?

Signed, Sealed and Delivered

The crucial thing to understand about Chaumian digital cash is that it differs from the electronic bookkeeping entries that function these days as money, zipping across borders on the wings of computers and telecommunications links. Those aren't cash; those are deposits, numerical representations of cash held in someone's name.

Digital cash, by contrast, is money, only better. It protects the spender's privacy by being untraceable, it cannot be counterfeited, and transaction costs are so low that purchases involving just pennies would make economic sense. It can even provide buyers and sellers with ironclad electronic proof of any transaction, proof superior to any paper receipt because it is unforgeable.

Here's how it works. In Chaum's system, a bank note is nothing more than a randomly generated number, the validation of which depends on the well-established concept of the "digital signature." This signature has two halves, called keys: a public key, available to everyone, and a private key, which an individual would share with no one. Messages can be "signed" by encoding them with the private key and verified as authentic by anyone using the signer's public key.

Imagine now that you present your virtual financial institution, the First Digital Bank, with an electronic bank note in the form of a unique serial number, which you want to represent $20. Like any bank, First Digital will want identification, which it gets in the form of your digital signature on the note. Satisfied that it knows its customer, and having checked that your balance is healthy, the bank replaces your signature with a signature of its own that it reserves for $20 bills and deducts that much from your account. Since it would be easy for the bank to record the serial number and match your identity with that of any vendor depositing the money, in Chaum's view you have no privacy.

So imagine that before presenting a serial number to the bank for validation as money, you multiply it by a random factor. It's as if you've slipped the note into a kind of electronic envelope. The bank can't see inside, but thanks to your digital signature on the outside, it can be sure of who is presenting this envelope, and so confidently (and figuratively) punches right through it to validate the contents as worth $20.

Before you go shopping, you keep the cash but discard the envelope--that is, divide by the same factor used earlier to mask your bill. The person with whom you spend this cash might know your identity--from your mailing address, for instance--but doesn't have to know who you are to be sure the money is valid, since the bank has already certified it as such. And when the recipient of your digital cash deposits it in his account at First Digital (or at Second Digital, which can redeem the money at First Digital), the bank has no way to

know who the original spender was, since it never saw the serial number in the first place.

Scale up this system and you begin to get the idea. Although some people call Chaum's new money "crypto-cash," from the perspective of the user there is little cryptic about it. All the blinding and signing occurs invisibly, and you spend the stuff by sitting at your computer and clicking on a picture of a wallet with your mouse. It's easy.

You'll notice that, as described, the system involves banks, both as certifiers of digital bank notes and clearinghouses for redeeming them. But banks are not inherent. For one thing, Chaum acknowledges that digital cash could be made in such a way that it could pass from hand to hand, so to speak, without the intervention of any issuing institution between transactions. What's more, the "banks" in Chaum's system needn't be the institutions we know as banks today (although Chaum himself wants a system based on today's banks). The Postal Service, for example, has long issued money orders in exchange for cash, and is now working on establishing itself on the Internet as an objective authenticator of digital signatures based on the dual-key system. And of course, private financial firms abound.

Where Nobody Knows You're a Dog

The explosive growth of the Internet has provided a big impetus of late in the hunt for alternatives to cash, with some of the most important players in computers and banking rushing to bring commerce to cyberspace. Visa International, Bank of America, Wells Fargo, Microsoft, MCI, Netscape, Electronic Data Systems, First Data Corp., Carnegie-Mellon University, the University of Southern California and others are involved in such efforts. Until now, commerce on the Internet has been hamstrung by the difficulty of conducting secure transactions. You can't safely send your credit card number as electronic mail, for instance, because e-mail messages routinely pass through any number of sites en route to their destination. Hackers, moreover, could steal not just one Mastercard number, for instance, but thousands.

"It is very easy to spot a credit card number," Richard K. Crone, an electronic banking analyst with the KPMG Peat Marwick accounting firm, explained to me via e-mail. "They are standardized. For example, Visa numbers always start with a 4 and Mastercard numbers always start with a 5. Bank-card numbers are generally 16 digits. Envision this: A skillful hacker runs a scoping program on his Internet server looking for 16-digit account numbers that begin with 4 or 5. Is that a needle in a haystack? In this case, the hacking program works when the robber is not working. They don't even have to be there to accumulate the numbers. It can be done remotely."

Even if you could use credit cards securely on the Internet, their transaction costs are too high for much of the business you might want to conduct there. The Internet has been described in its current state as a kind of giant potlatch, in which status derives from how much free information you're willing hurl out into cyberspace, where it tends to replicate itself beyond your control. Glyn Davies, in his "History of Money from Ancient Times to the Present Day" (University of Wales Press, 1994) might just as well have been talking about the Internet when he said that the competitive gift exchange between Solomon and the Queen of Sheba involved "extravagant ostentation, the attempt to outdo each other in the splendor of the exchanges, and above all, the obligations of reciprocity."

Yet much of the information is poor, since providers of quality information tend to supply it only in exchange for payment, or at least for the prospect of payment. But imagine if there was a way to get paid a small sum for some useful piece of information that you supplied on the Internet. Nathaniel Borenstein, a founder of First Virtual Holdings Inc., says that's how his Internet payment company got started. "Our idea

clicked with a 'joke of the day,' " he says. "We'd sell you a joke a day by e-mail for a penny a day. If you get 10% penetration and if the Internet stops growing today, that gives you enough income to hire the entire writing staff of Leno, Letterman and Arsenio. But we had no way to collect the pennies."

With their power to say yes or no in all kinds of important ways, banks can be intimidating, but the truth is that their place in a world of instant, cashless transactions is far from secure. In 1950, banks held two thirds of the total assets of American financial firms, but today banks hold just one third. Nearly 80% of the credit card processing business is held by non-banks such as First Data Resources Inc. At a recent convocation on financial institutions, a managing director at Montgomery Securities named J. Richard Fredericks put it succinctly. "Banking is essential to a modern economy," he told the group. "But banks are not."

Visa International hopes to reverse the twilight of the banks by moving beyond credit and even debit cards into a brave new world of electronic information exchange. This is a bold undertaking for an organization that can strike the casual visitor as wary; Visa's address is a post office box in San Francisco, but as I learned when a PR man picked me up at the airport, headquarters is an unmarked building in the suburbs. Partly, this reflects concerns about terrorism, but more mundanely, it reflects the general misunderstanding of what Visa is, which is essentially a marketing and clearing organization. Visa doesn't want you coming down to headquarters to try and pay your bill or make a complaint, because you are the customer of your bank, whose name is also on your card.

My visit to Visa began with a video depicting the organization's vision of the future. "The world's relationship with money and information is undergoing a revolution," the announcer says. "Visa and its members are leading this change."

In the video, a self-assured young woman, walking past a street-corner saxophone player, makes a donation by picking up a hand-held input device and inserting a plastic card. A worried young man pulled over for speeding decides to pay his ticket on the spot, handing the helmeted officer a card that carries not just value but also his driver's license. A young French woman, visiting a physician somewhere in Asia, is stymied by the language barrier at first but hands over her Visa card. The receptionist pops it into a computer and the patient's medical records appear, instantly translated into Chinese ideograms.

Visa's plan is for these know-it-all cards to be issued by your bank. Since a microchip on the card would have plenty of room for other kinds of data, it seems inevitable that such cards would soon be indispensable, almost like a drivers license, and might similarly devolve into a de facto identity card--at least until a better technology comes along. "In 15 years, it may not be a card at all," says Carl F. Pascarella, president of Visa USA. "It could be your palm."

Visa also intends to make the Internet safe for the 700 million or so bank cards in the world. Visa and Microsoft have joined forces to develop "a secure method for executing electronic bank-card transactions across global public and private networks." Mastercard, a similar consortium of banks, later agreed to join Visa in developing a standard for conducting secure transactions in cyberspace. The goal is to capture more and more transactions for bank cards, which have already made inroads against cash in supermarkets and elsewhere.

The great frontier for the banks, both on and off the Internet, is transactions of less than $10. Visa, Mastercard and the like aren't terribly economical for such transactions, yet these small purchases are a tempting target, and later in the day I am taken to meet an energetic young Visa senior vice president named Todd C. Chaffee, who explains why: Worldwide transactions of less than $10 each amount to more than $8

trillion a year.

Visa is dedicated to replacing cash wherever possible, but its executives are divided about the extent to which currency will persist into the future. Their views on this may be generational. Chaffee has little doubt: "The chip is going to hit cash like a freight train. Cash is just a stupid, antiquated old medium."

Chaffee understands the threat to banks exceedingly well. "Bank branches will largely disappear," he says. "Banks will have to compete in a whole new electronic realm." In that realm they will face new competitors such as Microsoft and AT&T, and the question "friend or foe?" will bring an unsettling answer: both. But the banks, Chaffee assures, won't take this threat lying down. "We're not going to let another payment system emerge that threatens the Visa payment system," he says matter-of-factly. "The large Visa banks aren't going to sit idly by."

Visa's vision for extending the payment system is a range of debit and credit transactions conducted electronically. "Our goal is to bring the existing payment system into the new realm," Chaffee says. For transactions conducted in person, "smart cards" would be used. If I buy a shirt, I hand over the card and the price is transferred from my account to the retailer's. Or it is charged to my smart card's credit function. If I don't want my wife to know about the purchase, I pay in "cash," meaning the store deducts from the card some of the cash I loaded into its memory at my personal computer, or at a vending machine. In that case, the store's computer won't even know who bought the shirt.

But if I buy something on the Internet, something like information, which doesn't require a shipping address, the store will know me. And the bank behind my credit or debit card will know my identity as well, because the banks plan to extend their hegemony over the payment system onto the Internet, and in all likelihood there will be little room for anonymity. Visa and its 20,000 member banks would no doubt do the same solid job of protecting confidentiality that they do today. Yet although there is a technological alternative, the Internet transactions Visa envisions would leave a never-ending trail of electronic bread crumbs behind every American fortunate enough to have the wherewithal to be a part of the system. The system is David Chaum's worst nightmare.

Uh-Oh!

Like many of us, Chaum bears some responsibility for his own bad dreams. Besides developing a solution to the problem of exchanging money in cyberspace, Chaum is noteworthy, in the stampede to commercialize cyberspace, for something else: his absence among the major players entering the field. "The problem with his system," says one key figure, "is that it requires a new monetary system. Some things are better accomplished through evolution than revolution."

Digital cash does raise a host of unsettling questions. Consider, for instance, the circumstances under which I met Marcel van der Peijl, a DigiCash systems developer, in Amsterdam. Using some of the cyberbucks created by Chaum's organization for an Internet digital cash experiment, van der Peijl sat in a roomful of casually dressed, bilingual young men like himself, playing poker with a computer in Australia. As I sat down, he was drawing cards to a bad hand. He ended up with a pair of queens, not good enough to beat the machine down under, and lost a cyberbuck. He will not be the last. Given how much people like to gamble (Americans wagered $394 billion in 1994, according to the trade journal International Gaming & Wagering Business), virtual casinos could become a major destination on any future information highway. After all, if gambling is illegal where you live, how will anyone stop you from connecting to a machine in some far off place where it is permitted? If you're dealing in cash, they can't.

But that's nothing when you consider the implications for governments. By removing many of the liabilities associated with cash transactions, digital cash could become a preferred medium of exchange. Taxes may indeed be what we pay for a civilized society, as Oliver Wendell Holmes Jr. said, but how do you collect them if everybody does business in cryptocash?

"That's what I'm worried about," says Don Alexander, a Washington attorney who served as commissioner of the Internal Revenue Service under Presidents Nixon, Ford and Carter. To the IRS, cash is the enemy, and the ball and chain of its corporeal nature are what keep people using the banking system, where the government can see what they're doing. With a laugh, Alexander recalls suggesting that $100 bills be printed in pink instead of green, on paper three times the size of regular bills. The idea was to make cash harder to hide. "Cash transactions lead to massive tax evasion," he explains. "Anything that makes cash transactions possible where you don't even have to have cash"--meaning thick, grubby old greenbacks--"makes it even more difficult."

Chaum's critics worry that his invention might open the door to international terrorism. Kidnapping, the argument goes, will become more attractive because the risks associated with collecting the money will be eliminated. What with the spread of nuclear weapons, you could hold up an entire nation for digital cash that couldn't be traced. Chaum insists that his implementation would make this impossible. Even lacking an intelligible digital receipt, the payer of any ransom would simply tell the bank the serial number of any digital bank notes paid over, and those notes would become unspendable.

The Treasury Department is among those worried. Its Financial Crimes Enforcement Network, for instance, offers a statement summarizing its major concerns; among these, cash cards are much easier to conceal than bank notes, since one card could conceivably hold billions of dollars. The government is also worried about the prospect of financial criminals no longer needing to have any human contact with a financial institution, or of lawbreakers making deposits and withdrawals without anyone knowing their whereabouts. One of the government's worries--that digital cash could make money laundering much easier--may be unfounded. Actually, depending on how it was implemented, digital cash could make money laundering unnecessary.

No More Fed?

Back in Amsterdam, I notice an interesting thing about the cryptocash that van der Peijl has been losing playing poker, which is that it is unbacked. The cyberbuck, in other words, represents no sum of gold or known currency on deposit anywhere and carries nobody's promise to pay anything. It is not unlike the dollar in that respect or the money issued by other advanced industrial nations, whose currencies float against one another, bobbing up and down in a sea of supply and demand, euphoria and despair. I ask what will happen if van der Peijl should gamble away all 1 million of the cyberbucks Chaum's organization has created for its experiment. I am assured on all sides that DigiCash won't just "print" more. The cyberbuck is not to be inflated.

Well, not yet, anyway. Often backed at first by gold or some other commodity, currencies have a historical tendency to break free of their earthly moorings and become fiat money. Sooner or later they start to lose value. Governments find it hard to resist printing more or pursuing fiscal and monetary policies that have a similar effect. The result, typically, is inflation, with its corrrosive social and economic consequences. The Nobel economist and free-market avatar Friederich A. von Hayek proposed a novel remedy for this problem: governments could print as much money as they want, so long as they abandon their monopoly in that department. Hayek figured that merchants, workers and so forth would naturally tend to demand the

strongest currency, whether issued by the government or (his preference) some private party, which could maintain the currency's value by pegging it to an index of commodities and strictly controlling its expansion. By voting with their purchases, individuals and firms would make it impossible for a nation to inflate its currency, lest such debased money find itself without a constituency.

The idea is not as farfetched as it seems. When I was in the Netherlands, I paid for things as easily in guilders as I do in dollars, simply by whipping out my credit card. Hayek wrote that computers would facilitate local currency competition, and, in fact, somebody's computer, located God-knows-where, did all the arithmetic during my travels. Many chaotic countries have already stumbled into Hayekian commerce; in Bosnia, for instance, you need Deutschemarks or dollars to get anything done.

Hayek and Chaum have something in common: Their ideas, carried to their logical conclusion, would mean the end of monetary policy as it is known today. The market would take over that role, ruthlessly casting aside currencies that didn't hold their value. Hayek, in fact, pictured free-market money causing the disappearance of central banks--an interesting echo, from the other side of the spectrum, of Marx's prediction that Communism would cause the disappearance of governments.

Tiring of the waiting room, Chaum and I walk around outside, along the empty spaces abutting his office building, and talk in the freezing wind. I ask where things stand, and he seems serenely confident, which worries me. Others are forging ahead with Internet payment systems while Chaum claims perennially to be in negotiations with major players of all kinds. Central bankers have invited him to meet, he says. His Internet cash experiment, meanwhile, isn't terribly impressive. I checked out some of the "shops" and thought one vendor, Judy Paul, was selling T-shirts for e-cash, but she turned out to want dollars for them. She'll take e-cash for bumper stickers, though, and is thinking of giving away the e-cash she gets this way to Internet denizens who look at her World Wide Web pages. "Like if you're the 4005th person who has visited our pages in April, you'll get five e-cashes." she explained by e-mail. "Or we may buy an e-house on the e-lake. Send our kids to e-university."

On the other hand, even Visa's Chaffee admits that "unquestionably, there's a real market for extremely private payment systems." If necessary, I suspect, such systems will bubble up out of cyberspace on their own; if the emerging electronic payment system isn't sufficiently private, the marketplace will provide the privacy missing from it. Just as certain island nations provide a measure of banking secrecy today, we can expect the emergence of more comprehensive digital secrecy havens tomorrow. There is no shortage of national sovereignty, after all. Hungry little countries are popping up all the time, and computing power only gets cheaper.

Daniel Akst writes the weekly "Postcard From Cyberspace" column in The Times. His last article for the magazine was on the 1980s.