# Numbers Can Be a Better Form of Cash Than Paper

David Chaum

Centre for Mathematics and Computer Science
Kruislaan 413, NL-1098 SJ Amsterdam, The Netherlands

Soon, by accessing a computerized network from almost anywhere, you may be able to pay for a purchase, change your insurance coverage, or perhaps even send an electronic "letter" to a friend. Although a single system integrating all these functions is still some way off, its piecemeal construction is already underway. Automatic cash dispensers and electronic payment devices at shops, for instance, are in use in many countries and are planned in many more. The technology underlying all this does have enormous potential for cutting organizations' costs and increasing their security, as well as for enhancing consumer convenience. The prevailing approach to applying the technology, however, brings with it some quite serious dangers.

This current approach requires individuals to identify themselves to the system each time they use it. All the various identifying techniques–like tamper-resistant plastic cards, memorized secret numbers, and fingerprints–are essentially equivalent to universal ID numbers, such as the ones used for social insurance or passports. These identifiers allow computerized linking of all manner of personal information, from school, medical, and employment records to purchase details captured in electronic payments. Faced with how easily such data can be tapped, exchanged, and modified, legal mechanisms seem powerless to protect individuals from errors and data misuse. Moreover, "automatic pattern recognition" techniques could be applied by anyone tapping into the large-scale systems currently being planned. Individuals might thus be categorized by their transaction patterns–everywhere they pay, every relationship they have with organizations, and everyone they communicate with–in a form of invisible mass surveillance.

All these problems can be avoided by a new approach to using so-called smart cards–plastic cards containing microcomputer chips. The most technically advanced of these, the "supersmart" card made by Toshiba for Visa, is no bigger or thicker than the familiar credit card, yet includes a battery, character display, and buttons like a pocket calculator. As with all current- approach cards, though, the organization that owns and issues it must make it tamper-resistant to prevent anyone else from accessing its internal structure. By contrast, the new-approach card computer is all yours. You can choose one just as you would any pocket-sized calculator or personal computer, and can even access or customize its inner workings to suit your convenience. Tamper resistance, with its inflexibility, expense, and low security, has been made unnecessary by more advanced coding techniques.

## 1 Shopping With Your Electronic Wallet

When you buy something with your new-approach card computer, the clerk's electronic cash register transmits to your card the cost and description of the purchase. If you agree to these details as displayed by your card, all you do is enter on its keyboard your single secret authorizing number. Your card then completes the transaction by transmitting to the cash register a one-time-use number of several hundred digits–a number that is money.

Such a card not only improves on the personal convenience and security of credit cards, but the coding it uses ensures privacy. Even paper cash is traceable in principle, since the bank could record the serial numbers of the notes you withdraw. Conceptually, the inherent traceability of pre-printed notes could be avoided by instead, during withdrawal, having the bank validate and return envelopes that you supply. A plain slip within such an envelope would get, say, a carbon-paper image of the bank's "worth-one-dollar" validating signature stamp. You could then discard the envelope and spend your validated yet untraceable slip just like cash. The actual digital system works essentially the same way: your card randomly codes a number that it chooses to serve like the slip, obtains the bank's coded validating signature on it during a withdrawal, and removes the random coding before spending the resulting validated numeric note. A simple mathematical proof shows that the bank can't trace such a numeric note to its withdrawal, no matter how extensive or ingenious the computerized analysis. If you need to, though, you can reveal information that lets any one of your payments be traced incontestably.

Security for banks and merchants is also improved. The bank's coded signature, which lets a numeric note's validity be tested by any card or cash register, is far harder to counterfeit than printed money. But because numbers are easy to copy exactly, retailers need protection against someone spending a note number more than once. For high-value payments, the bank's list of already spent notes is electronically consulted while you wait. For low-value transactions, shops avoid this expense by requiring a random selection of additional numeric information from the payer. The amount of such information revealed in spending a note once is absolutely useless in tracing the payer. But enough additional information is revealed in spending a note twice so that, after the day-end deposit of notes, the bank gets from each "double spender" the equivalent of a signed confession.

## 2 Showing Credentials Without Identification

Business and government organizations sometimes do legitimately need to see statements that other organizations have issued about individuals. Such credentials have in the past taken the form of identifying paper certificates, like passports, driver's licenses, and membership cards. The original purpose of most of these documents was to securely authenticate individuals' qualifications, such as an economic or age bracket, a license, or an academic degree. Identification was a means to that end. But in today's computerized imitation of paper-based

methods, identification allows organizations to match with or directly access other organizations' computerized files. This has created in effect a single huge database on individuals, although it remains slow, incomplete, and prone to error. Yet a comprehensive and centralized system, even if it were acceptable to the public, would be prohibitively expensive.

An extension of the card-computer payment technique can solve these problems. All credential transactions are conducted through your card, using a different numeric alias or "digital pseudonym" with each organization. Credentials are issued in the form of unforgeable coded signatures on these pseudonyms, which your card handles much as it does numeric notes. If you authorize it to, your card can transmit convincing numeric proof that you hold at least one combination of credential signatures meeting an organization's requirement–without revealing anything more. The way the pseudonyms are created assures organizations that you can't lend, modify, or escape accountability for your credentials. And because of the way your card codes "blank" credentials in "envelopes" before they are signed by organizations, your pseudonyms cannot be linked any more than your payments can. You retain complete control over your personal information, just as if all the computerized records that organizations maintain on you today were stored only in your card computer.

## 3 Protecting Electronic Mail

Once electronic payment becomes commonplace, electronic mail may be next. The widespread use of "e-mail" may raise a number of problems: keeping message content confidential, preventing users from falsely denying that they have sent or received particular messages, and forestalling automated "traffic analysis" that could trace the patterns of users' relationships.

The new approach's solution broadcasts messages to all electronic mail computers in the network. This prevents tracing to the intended recipient, and it ensures that receipt of messages cannot be denied. Also, a novel kind of coding permits each person's e-mail computer to conceal unconditionally which messages it sends. Other coding keeps message content confidential and lets recipients be sure–and convince others if necessary–of the message originator's digital pseudonym. This solution naturally facilitates payment and credential transactions from home, with all the convenience and protection offered by card computers.

## 4 The Moment of Decision

Lower cost and higher security will serve as strong motivation for organizations to adopt the new approach. As more people become aware both of the dangers posed by the current approach and of the improved personal convenience and security offered by the alternative, organizations may be further motivated by consumer preference, public opinion, and even legislation.

At the moment, however, the centralized-data approach is gaining momentum. Automatic cash dispensers and other current electronic payment techniques, with the tracing they allow, are just the tip of the massive investment iceberg required by such large-scale systems.

We are fast approaching a moment of crucial and perhaps irreversible decision, not merely between two kinds of technological system, but between two kinds of society. 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. If, on the other hand, the new approach prevails, the erosion of our informational rights can be reversed and new rights added–notably the right, realizeable through personal card computers, to reveal only necessary information in transactions. As we move into an age of pervasive computerization, control over information becomes the key to social, economic, and political power. Card computers can restore balance by putting part of that key, both literally and figuratively, back in the hands of private citizens.

## References


1. D. Chaum, "Blind Signatures for Untraceable Payments," *Advances in Cryptology, Proc. Crypto'82*, D. Chaum, R.L. Rivest, and A.T. Sherman, Eds., Plenum Press, New York, 1983, pp. 199–203.
2. D. Chaum, "Security Without Identification: Transaction Systems to Make Big Brother Obsolete," *Communications of the ACM*, Vol. 28, No. 10, 1985, pp. 1030–1044.
3. D. Chaum and J.-H. Evertse, "A Secure and Privacy-Protecting Protocol for Transmitting Personal Information Between Organizations," *Advances in Cryptology, Proc. Crypto'86, LNCS 263*, A.M. Odlyzko, Ed., Springer-Verlag, 1987, pp. 118–167.
4. D. Chaum, "Blinding for Unanticipated Signatures," *Advances in Cryptology, Proc. Eurocrypt'87, LNCS 304*, D. Chaum and W.L. Price, Eds., Springer-Verlag, 1988, pp. 227–233.
5. D. Chaum, "Privacy Protected Payments: Unconditional Payer and/or Payee Untraceability," *SMART CARD 2000: The Future of IC Cards, Proceedings of the IFIP WG 11.6 International Conference, Laxenburg (Austria), October 19–20, 1987*, North-Holland, Amsterdam 1989, pp. 69–93.
6. D. Chaum, A. Fiat, and M. Naor, "Untraceable Electronic Cash," *Advances in Cryptology, Proc. Crypto'88, LNCS 403*, S. Goldwasser, Ed., Springer-Verlag, 1990, pp. 319–327..
7. D. Chaum, "Online Cash Checks", *Advances in Cryptology, Proc. Eurocrypt'89, LNCS 434*, J.-J. Quisquater and J. Vandewalle, Eds., Springer-Verlag, 1990, pp. 288–293.
8. D. Chaum, B. den Boer, E. van Heyst, S. Mjølsnes, and A. Steenbeek, "Efficient Offline Electronic Checks," *Advances in Cryptology, Proc. Eurocrypt'88, LNCS 330*, C.G. Günther, Ed., Springer-Verlag, 1988, pp. 294–301.
9. D. Chaum, "Achieving Electronic Privacy", *Scientific American*, August 1992, pp. 96–101.

10. D. Chaum and T.P. Pedersen, "Wallet Databases with Observers," *Advances in Cryptology, Proc. Crypto'92, LNCS*, E.F. Brickell, Ed., Springer-Verlag, to appear.