1 Can *Cash* be Digitalised?

Jan Holger Schmidt, Matthias Schunter, Arnd Weber

Abstract

Cash-like payments in electronic commerce and at the traditional point of sale are expected to be beneficial, e.g., because of privacy protection, low transaction costs, and irrevocability. Therefore, we discuss how to design electronic cash in a way that it both mirrors the most important characteristics of traditional cash, but also fulfils the expectations which arise towards electronic means of payment. We analyse the problems and trade-offs between the different characteristics to be implemented. This analysis is based on a user survey and a review of existing technology for electronic payment systems. Finally we argue why existing systems do not fulfil the critical requirements, and point out future work towards electronic payment systems justifying the name "electronic cash".

1.1 Introduction

Electronic cash in our sense is universally usable stored value[1]. Electronic cash is discussed as a means to replace traditional cash in the physical world, and as a means of payment in the virtual world. In both cases, electronic cash could have a number of benefits even compared to future pay-now[2] or post-payment instruments. Examples include that a stored-value payment might be cheaper than a pay-now mechanism, because less on-line connections are required, and that, unlike post-payments, everybody can use it independently of creditworthiness. Furthermore, the payer's privacy can be protected. For these reasons, existing electronic payment instruments do not cover the whole potential market of electronic payments, i.e., a benefit for the issuers of electronic cash will be the possibility of earning fees by conquering a larger share of the electronic payment market.

In order to replace traditional cash, electronic cash should be easily usable and also offer robustness, and off-line transferability. Up to now no electronic cash system offers these characteristics. This leads to the question whether it is possible to develop electronic cash with most characteristics of today's cash, i.e., electronic cash which may eventually replace traditional cash.

1.1.1 Overview

This chapter is structured as follows: Before we describe those characteristics of traditional cash which will need to be mirrored, we will describe the projected benefits

---

[1] Besides electronic cash (i.e., prepaid stored value), we consider debit-card-like pay-now and credit-card-like post-payment schemes.

[2] Note that in all existing debit-card schemes debiting the account is deferred. Therefore, they are post-payment schemes in our sense. This, however, may not hold for future developments.

of electronic cash. Then, we sketch additional requirements, such as loss-tolerance, which are not fulfilled by traditional cash but should be provided by electronic cash. After a short survey over the technological foundations for electronic cash, we discuss the problems which occur if one wants to provide all desirable characteristics.

Note that this is no survey on electronic payment schemes[3]: As we will show, no system exists which offers electronic cash in our sense and only few schemes come close. Therefore, we rather survey existing building blocks, and trade-offs which become important when designing electronic *cash*.

1.2 Projected Benefits of Electronic Cash

Our interviews[4] with the banking industry have shown that electronic cash has not yet turned out to be profitable. New electronic payment schemes seem, however, worth investigating for the following reasons:

- To reduce the costs of cash handling, especially coins,
- to abolish the problem of missing change, and
- to reduce the damage of counterfeit cash.

Using electronic cash as a form of electronic payment has additional benefits:

- Privacy in the sense of untraceable electronic transactions can be achieved.
- Off-line usability of electronic cash reduces costs for networks.
- Issuers can earn fees by "conquering the cash market".
- Interest can be earned from the float, which, e.g., can be used to pay interest to the holders of electronic cash.
- Irrevocability can be guaranteed to the payees, whereas in pay-now or post-pay systems the payer can demand cancellation.

In addition, the benefits of pay-now payment instruments hold:

- Pay-now instruments can be given to less creditworthy individuals.
- By developing alternatives to credit cards and paper cheques, it should be possible to reduce transaction costs.

Some of these benefits can only be earned if traditional cash can be replaced to a substantial degree, and if electronic cash can provide efficient solutions on electronic

---

[3] For such surveys one may look at Asokan, Janson, Steiner, Waidner 1997, Furche and Wrightson 1996, Mahony, Peirce, Tewary 1998, or Wayner 1997. A longer version of this paper has been published as Schmidt et al. 1998.

[4] The requirements and benefits of electronic cash in this paper are based on expert interviews and consumer surveys. The interviews mentioned have been made in the framework of three research projects, which were "Soziale Determinanten der Entwicklung alternativer POS-Zahlungssysteme" funded by Deutsche Forschungsgemeinschaft, CAFE and SEMPER, funded by the Commission of the European Communities. See Furger et al. 1998 for the consumer interviews.

networks. Thus a powerful tool is required, having the advantages of traditional cash, but being transferable across networks as well.

1.3 Which Characteristics Should Electronic Cash Have?

We now sketch characteristics of traditional cash and existing payment system which are desirable for digitalised cash from a user's point of view[5].

1.3.1 Characteristics of Traditional Cash

In order to replace traditional cash it is important to recognise which characteristics traditional cash has: For any payment system named "cash" it is crucial to mirror the expected characteristics. Otherwise, part of the cash market cannot be reached and users may be disappointed if something is called "cash" but cannot fulfil the expected role.

Universal Usability: Universal usability means that everybody can obtain it and pay any payee with it. A user of the world's earliest stored value chip card in Biel, Switzerland, concluded already in 1993: "Cash can be used everywhere, but the card not. You need devices to read it." Also usability by children is not easy to achieve. An aspect of usability is *portability*: Without a device, one cannot use digital cash. Thus, a card reader or an electronic wallet (holding several cards or modules) must fit into existing leather wallets, men said in our surveys, or be of compact shape to be put into pockets (women have less problems with storing such somewhat larger devices).

Off-line Transferability: Traditional cash can be used to pay off-line without involving the bank; similarly this is required from electronic cash, as most payees are not permanently on-line, mostly because of communication costs. With off-line transferability we mean off-line usability where received cash can even be used for another payment without contacting the issuer. Respondents know they need off-line transferability, e.g., for "giving the children pocket money". Someone from Biel said: "But if I have 1,000 sFr on the card, I cannot split them. I cannot transfer them."

Untraceability: In our surveys it has been stated that "monetary affairs are primarily private affairs". Others want to "minimise Big Brother's surveillance of my expenditure". Some French consider that privacy protection is a matter of "liberté personelle", a right to be enforced by the state. Others argued they need privacy protection for paying goods which fell "off the back of a lorry". Thus, it will only be possible to cover certain segments of the cash market when offering a high degree of privacy protection. One should distinguish between "untraceability" (Chaum 1981) and "pseudonymity". "Untraceability" means that the issuer, the acquirer and merchants cannot trace a payer, i.e. cannot tell whether two payments have been made by the same payer. "Pseudonymity" means that all transactions can be linked to pseudo-

[5] A more formal treatment from a technical viewpoint can be found in Pfitzmann, Waidner 1996.

nyms, where the pseudonyms cannot be linked to individuals. Telephone cards that are sold anonymously can be like this. In practice, however, pseudonymous schemes enable identification if the pseudonyms are used too often: Using the phone-card for many calls can lead to identification by examining the destinations of the calls.

Transparency of Financial Status: From a simple look into one's traditional wallet, one can obtain transparency of one's financial status. "With cash, children can see the amount," a respondent said.

Control over Wallets: Traditional wallets remain in one's hands. If a purse on a chip card is used, this chip card may be used for storing other functions as well, such as other payment functions, or a digital signature function to be used in electronic commerce. Therefore, users may not wish to hand over such an important card to a payee.

Long Validity: Issuers of electronic cash usually limit the usability of their cash right from the beginning, in order to prevent long lasting liabilities. Electronic cash may no longer be valid if an issuer goes bankrupt (cf. Japanese Ministry of Finance 1989). The validity of cash may decrease due to inflation. Competition among different electronic currencies could, however, reduce inflation because only those will survive which provide a low rate of inflation (cf. Hayek 1977).

Physical Robustness: High robustness will be required from electronic cash. Users compare it to an embossed credit card, which can be used quite reliably in many countries and climates. Men will bend plastic chip cards when in their hip pockets. Electronic wallets may be stepped upon or dropped.

Cost Efficiency: Merchants are used to paying a disagio when accepting card payments. But individuals will probably find it unacceptable if electronic cash diminishes when transferred between individuals. In any case, a new instrument will have to be either as cheap as traditional cash, or the marginal cost increase must be justified by other benefits.

Security: Security guarantees that the desirable characteristics persist in spite of fraud.

1.3.2 Additional Characteristics of Electronic Cash

We now give an overview of new requirements which are expected from electronic cash. Unlike the characteristics described in Section 1.3.1, a scheme without these new characteristics will not automatically look inferior to traditional cash. So users will not expect all these characteristics. The new characteristics may, however, form an incentive to switch from traditional to electronic cash.

Fungibility: It will be expected that with electronic cash one can pay any particular sum easily, just as one can with post-pay cards, bank transfer orders, etc. This means that if one has the necessary funds available, the system should not tell that the desired payment is impossible. So electronic cash could be better than traditional cash, where one may not be able to pay because the merchant has no appropriate change.

Usability on Networks: From electronic means of payment it will be required that they can be used securely and conveniently with one's PC on networks such as the Internet.

Tolerance Against Loss and Theft: Tolerance against loss, theft and malfunctioning has been a selling argument for post-pay cards, so users will expect it from electronic cash as well. Alternatively, one can try to teach users that regarding loss electronic cash is like traditional cash. The holder, however, will arrive at the conclusion that in case of loss of a card that can only be used by the holder, the issuer still has the real money, and accordingly will expect a refund.

Usability Across Borders: This characteristic may be expected from electronic cash, just as it is available with credit cards. Currently, the issuers of the stored value cards deployed in European countries face the problem that their incompatible systems will not be able to inter-operate even though most of them will soon use "Euros".

Ease of Reloading: If users are required to go to a cash dispenser for withdrawing electronic cash, they may consider withdrawing traditional cash instead, which can be used everywhere. Also, users will require that reloading does not take much longer than withdrawing traditional cash.

User-Friendliness: Systems must be designed in a way that they can be understood and handled easily. Furthermore, users will not develop trust in the system if they believe that the system may not operate in the way they expect it. It might be that a secure and correct system is not used because people just do not trust the system to be secure.

1.4 Technologies for Building Electronic Cash

This section gives an overview of some existing technology which can be used for building electronic cash with the desired characteristics. After sketching some basic technologies, we describe particular kinds of systems as well as their extensions.

1.4.1 Basic Technologies

Tamper-Resistant Hardware

To prevent criminals from copying electronic cash, one possibility is to use tamper resistant chip cards. Chips can, however, be attacked with sophisticated laboratory equipment (Anderson, Kuhn, 1996). More powerful intrusion detection systems are becoming available, but they result in modules thicker than chip cards.

Trustworthy User Devices

The users should trust the device protecting its assets but should not be forced to trust modules from other parties (Pfitzmann et al. 1997). One way to control what a payment module from the bank communicates by using a "wallet with observer" (Chaum 1992): The idea is that the user has a trusted wallet of his choice. Each issuer then provides a plug-in module which protects the issuer (Pfitzmann et al. 1997). For transparency, the user's wallet also needs a display and keypad in order to enable control over the amount, and for entering the PIN. Another advantage of such a wallet is that contact-less interfaces could be used, which enables cheap and robust terminals.

Authentication, Digital Signature Functions, and Blind Signatures

Authentication schemes are used to guarantee that communication is done with the right *persons* or *devices*. In contrast, digital signatures allow to prove the authenticity of *messages* (Diffie, Hellman 1976). An issuer can use a digital signature to sign electronic coins. Chaum suggested to "blind" the signatures for making untraceable payments. Blinding means that some blinding factor is calculated into the electronic coin to be signed by the issuer. After signing, the blinding factor is removed by the holder. Thus the coin remains signed, but the issuer has not seen the signature which is deposited after payment (Chaum 1983, Chaum 1989).

Connection Anonymity

If a payment is made on a network, the network operators can trace the transaction, whether blinding is used or not. A remedy are anonymous terminals or network anonymity services (e.g., Chaum 1981).

Loss Tolerance Mechanisms

To build loss-tolerant systems, backups of electronic cash can be kept by the issuer. In case of untraceable electronic cash, loss tolerance can be provided if the user stores back-up information (Pfitzmann, Waidner 1997).

1.4.2 Technologies for Coin-based Payment Systems

We distinguish between coin-based and counter-based payment systems. Like traditional coins, electronic coins are of a fixed value. To assure that coins can only be created by the issuer, the coins are digitally signed. In order to offer untraceability blind signature schemes can be used. Such coins can be very secure, but they come with the problem of low fungibility. Some improvements can solve or reduce these problems, but first some general extensions are shown.

Double-Spender Detection

There exists no software solution that protects electronic cash from being copied and used twice. This is the reason why on-line verification or tamper-resistant hardware is typically required for secure off-line use. But security needs not depend on tamper resistance only, as there are solutions to identify a criminal who spent a value more than once: Even if blind signatures are used, double spenders can be identified if an identity is encrypted into electronic coins (Chaum, Fiat, Naor 1990) so that the identity can only be decrypted if the coin was double-spent.

Value-less Coins for Transferability

A value-less coin can be used to authenticate a message once while staying untraceable. Double-use leads to identification. This technique (van Antwerpen 1990) is used to allow off-line transferability for untraceable electronic cash. The recipient of a transferred coin needs a value-less coin which is then linked to the received coin during the payment. For paying, the recipient forwards the received coin and then "pays" the value-less coin. The recipient verifies the link to the coin with value. In all following transfers the coin together with a growing list of linked value-less coins will be forwarded. After deposit, the coin together with the linked chain[6] of value-less coins can be used to identify double users with the usual mechanisms.

Paying Interest with Coins

For paying interest on coins Chaum (1989) introduced two methods: time-stamps and receipts. Another proposal uses coins with a dynamic value that increases due to the interest paid.

Coin-Extensions for Fungibility

Change: Coins are of a fixed value. This leads to the problem of a lack of coins in the appropriate denominations. In traditional systems payers and payees have a reservoir of change for this reason. This solution cannot be used in untraceable systems without payee untraceability. If, for example, an anonymous buyer pays a merchant, the problem is that the merchant knows which change (s)he gives to the buyer. If no transferability is offered the buyer has to give the change to the acquirer. In co-operation with the acquirer the merchant can then find out the identity of the buyer, because the buyer is now in the payee-role, for which no anonymity is offered.

Divisibility: Okamoto and Ohta (1992, cf. Chan, Frankel, Tsiounis 1998) suggested divisible coins, where each coin can be spent incrementally up to its monetary value. So one can pay $1 using a $10 coin and keeping $9 for other payments of different values. A drawback is that fragments of one coin can be linked, which reduces untraceability.

Refund: Cheques have the advantage that the payer can write the amount the payee wants to have into it while paying. Chaum, Fiat and Naor (1990) describe such a system with pre-paid coins. The user withdraws „high-value" coins from the issuer and can decide what amount up to the coin value they would like to spend. After having paid the user requests the issuer to pay the refund of the difference between the coin value and the paid amount. Even if there are a number of payments and deposits of the same amount, issuer and acquirer cannot link them.

---

[6] The size of the transferred coins must grow because each transfer adds one value-less coin encoding a new identity (Chaum, Pedersen 1993).

Another possibility to increase fungibility is to combine coins with counter-based systems, as shown below.

1.4.3 Technologies for Counter-Based Payment Systems

In counter-based payment systems, the electronic cash a person owns is represented by a counter. Tamper resistance is required to keep the users from manipulating the counter. Also authentication schemes are required to prevent illegitimate communication with the counter in order to change its value. Untraceability may be provided if all payment modules use the same key which must be kept secret using tamper-resistant hardware. If, for security reasons, different keys are used, the keys can be used as pseudonyms which results in a pseudonymous scheme.

A way to increase security in pseudonymous counter-based systems and to detect spending of value which was not withdrawn is to track the value of each counter at the issuer. In systems, which can be used off-line, this might not always be the actual value, but it can be updated from time to time and used to detect if the counter stored on the smart card has been manipulated, i.e., if its shadow shows a negative amount. Such shadow counters can also be seen as backups to provide tolerance against loss, theft and malfunctioning. In most existing systems, however, loss tolerance is not communicated to the holders in order to keep costs for help-desks low ("Yesterday the Coke machine did not work, I want my money back").

1.4.4 Hybrid Schemes: In Between Coins and Counters

Counters with Value-Less Coins

A way to provide untraceability while using asymmetric authentication techniques is to use value-less coins for the authentication of payments: To increase the security in counter-based systems, one can combine counters with electronic cheques (Bos, Chaum 1990). For each payment an electronic cheque with the issuer's signature is needed. Because each cheque can only be used up to a maximum amount, in case a counter is broken, it will not be possible to spend an unlimited amount of money without contacting the issuer (CAFE 1996).

Multi-Use: To save storage space on smart cards there are techniques for using the same value-less coin multiple times (CAFE 1996[7]). Thus, depending on how often a cheque can be used, the system provides something in between untraceability with coin-level security if the cheque can only be used once and pseudonymity with counter-level security if the cheque can be used arbitrarily often.

Tick payment: If all payments are to be made to the same payee, such as per tick with a telecom provider, one single value-less coin (signature) needs to be used. After initialisation, one can pay subsequent ticks quickly (Pedersen 1997).

---

[7] In CAFE, the cheques could be spent twice. Thus it was possible to have 70 payments on a card chip.

Adding Value to Value-Less Coins: If one replaces the value-less coins with coins with an upper and lower value limit, one can slightly increase the security of the scheme since one has to pay the lower limit of the range for withdrawing the coins which can then, depending on the value of the counter, be used up to the maximum amount. Consider, for example, that the minimum and maximum amount only differ by 10 cents, then, the gain of breaking tamper resistance is limited to 10 cents per payment.

Coin Pools with Counter

A solution for providing fungibility, unlinkability, and security is to equip the users with a large pool of digital coins of different denominations and track the spendable portion with a counter.[8] If tamper resistance is broken, the user can spend all coins in the pool once without being identified. For the coins the user reloads, (s)he has to pay. So the possible damage by breaking the tamper resistance is limited to the amount in the coin pool.

1.5 Trade-offs in Designing Electronic Cash

Now we examine the most important trade-offs when implementing different characteristics in one system.

1.5.1 Trade-offs with Costs

An electronic cash system will be only acceptable if costs are lower than the benefits it offers. So in all cases where the fulfilment of characteristics costs money, such as for comfortable user-devices, the players should be willing to bear the costs if the benefits of using this kind of money are large enough. Another possibility would be that the issuer expects other benefits from the customer relationship and therefore is willing to bear the costs. We believe that at the time of writing it has not been sufficiently investigated whether the users are willing to pay for powerful systems having many useful characteristics. It is not even clear how much a secure system offering many characteristics will cost and whether these costs will be higher than the full costs of traditional cash or other payment schemes.

For all values in use, issuers have to store information about them[9], and the values have to be transferred, even if the value is only one penny. Characteristics like off-line transferability require complex protocols which make transaction times longer. Also additional trustworthy hardware will increase costs, like displays for achieving transparency.

---

[8]Personal communication with David Chaum.

[9]Except in systems where only counters on user devices are used. But in such systems issuers might not even recognise fraud.

Untraceability makes everything more complicated: Untraceability comes with the overhead for blinding and more complex protocols. Untraceability in networks requires anonymous connections.

The more convenient a system gets, the more it costs: To achieve convenient reloading for users, many withdrawal terminals will be required. It would even be better if phone and computers could be used for reloading as well. This, however, requires techniques for managing passwords securely and approval on secure displays.

Robustness and reliability are costly and always limited: To achieve reliability will cost money. Electronic cash stored on portable devices will never reach the robustness of traditional coins. Water, heat and strong magnetism will quite likely destroy electronic coins stored on user devices. Chip cards are known to be well portable, but they may break when stored close to coins in traditional wallets. Displays for achieving transparency need particular protection. By spending more money, one can design more robust devices. On the other hand users might accept non-robust electronic cash if the devices are not too expensive and convenient loss- and fault-tolerance is offered.

Fungibility for secure untraceable coin-based systems is difficult to achieve: A payment should not be impossible because one ran out of appropriate coins. A solution not requiring change is to use coins of the smallest denomination, e.g., 1 cent. This, however, will lead to considerable memory and computing requirements, which in turn will lead to problems with portability and ease of use. Storing, e.g., cents for 100 Euros means 10Mbits of coin data. Even with wallets having more storage than cards[10], spending, e.g., 2500 coins will still surpass its computational power or lead to unacceptable reloading times. A remedy would be to use multi-spendable or divisible coins which reduces untraceability.

Loss tolerance comes with additional overhead: If loss tolerance is used, one needs backup information, so this information needs to be handled. Even if this backup has only to be done once at the creation of the electronic purse it will make usage less convenient: One has to keep a printout, a memory card, or remember the passphrase for decrypting a backup stored at the issuer.

1.5.2 Trade-offs with Security

Perfect security is not possible: Apart from the risk that someone manages to break the system with much effort and special equipment requiring considerable costs, there will be always the risk that someone steals secret information like private keys for “minting” coins or circuit layouts to break tamper-resistance. If electronic cash is generally used, breaking the system is not only a risk for the issuer. Imagine a whole nation that is not able to do payments anymore because criminals produced lots of

---

[10] The storage capacity of chip cards which is largely limited by the fact that men tend to sit on the cards and therefore the chips must not surpass 25mm^2.

counterfeit money. It could already be problematic if there are only rumours that the system has been broken. People might wish to exchange their electronic cash into other values. This can lead to a cascading default by the inability of participants to pay off a close-of-day deficit (Bonorris 1997).

Trust in the system is required: People will only use new systems if they trust them. The new protocols are difficult to understand, so it may take considerable time and effort until trust has been established (Pfitzmann et al. 1997).

Untraceability means more costs for fighting fraud: In untraceable systems users cannot be linked to transactions. This means that criminals may still be untraceable, if they manage to break the system: Untraceable coin systems use blind signature schemes where the issuer does not know which coins are used. For the issuer it would be very difficult to detect criminals who "mint" their own coins. Only when more coins have been received than issued fraud will become obvious.

More security results in more complex systems: A simple counter system that only relies on tamper resistance will not cause any difficulties but in security. It can be seen as a question of time until a given system with a certain technology for providing tamper resistance is broken. Updating systems with the latest tamper-resistance technology comes with regular costs and the management overhead for expiring old user devices. If one enables the users of a counter-based system to transfer amounts offline, the issuer might not even detect that counterfeit money is in use and it will be hardly possible to accuse someone of fraud. If tamper resistance is not used alone, protocols become more complex to allow for security and other characteristics. This results in longer transaction times and the need for more powerful devices. Coin-based systems can be designed in a very secure way and essentially only the risks remain that the underlying cryptographic schemes are broken or that the issuer loses control over his secret key. However, paying the proper amount efficiently is a challenge. It also takes longer to load coins, as opposed to just updating a balance of a counter. In a system of value-less coins with counters, one will be in between.

The more characteristics a system offers, the more risky is its security: It is a general fact that the more complex a system is, the more possible weak points may have been overlooked during development. So a paradox situation is reached. Secure systems are getting more complex and may need additional features like divisible coins in order to be fungible, what again leads to risks with security due to the complexity of the resulting system.

Full control over the wallet leads to a trade-off with security of the issuer: In contrast to the users, who don't want that the devices obtained from the issuer (e.g., a card) can be withdrawn, the issuer might wish to have them withdrawn by a terminal if they are suspect. Such blacklisting will help only in pseudonymous systems.

Unlimited validity will not be offered by issuers: It is unknown how future fraud with a given system will develop. Issuers will not wish to have liabilities in terms of value in the hand of holders for many years because criminals may have broken the system and the damage may continue for years. To keep this risk manageable, issuers limit the validity of cash or systems to a few years. This is inconvenient as one may not be able to pay or as outdated value has to be exchanged in an on-line connection with the issuer. Another disadvantage of long validity is that the issuer has to store more information for double spending detection or for loss tolerance.

1.5.3 Trade-offs with Convenience

*Convenience is a trade-off in itself***:** Offering additional features for a convenient use of the system often leads to inconvenience elsewhere in the system. Allowing for example users to transfer electronic cash will lead to more complex protocols and in the case of coin-systems to growing coins and thus larger devices having more memory. As one expert put it in our interviews: “And then you need a little carriage to drag it behind you.” The more computational power and special features are required the bigger the devices become. A possible solution which doesn’t require the user to carry an additional bigger device is to integrate payment functions in mobile phones or watches[11]. But still some people like children might not wish to carry expensive phones or watches with them all the time, thus a payment could be impossible.

Unlimited off-line transferability using double-spending detection in an untraceable system is not possible: In addition to the problems of off-line usability alone, off-line transferability will always be limited by the amount of available memory. Alternatively, one would have to force holders to give certain pieces of value which reached a limit of transfers back, i.e. differentiate between transferable and unspendable money. The latter is not in line with today's rules of handling traditional cash, but not absurd, as received credit card payments or cheques cannot immediately be used for payments either. However, it would have to be displayed to the holder if money is unspendable.

Usability is always limited: It will be very difficult to make electronic cash as usable as traditional cash. There are devices needed to store and pay. Electricity will always be required. So electronic cash systems will always suffer from an operational risk that payments are impossible because parts of the systems are down. Some characteristics will make electronic cash more difficult to handle than coins or credit cards. Think of electronic cash which cannot be spent since unlimited transferability is not possible or of the need to handle one’s electronic device carefully.

An off-line usable, loss-tolerant system doesn’t allow long validity: With off-line use, an issuer can only refund lost money after it is no longer valid. Otherwise, the cash of a legitimate owner may be invalidated. Therefore, there is a conflict between loss-tolerance requiring short validity and off-line use requiring long validity.

---

[11]As PIN-pads on watches would have to be very small and thus difficult to use, a solution would be to enter an amount elsewhere, transmit it to the watch, display it and have approval on the watch with a small fingerprint reader.

Transparency of financial status versus size: Instead of carrying around a "terminal" of one's own with a PIN-pad and a display, roughly the size of a small pocket-calculator, it might be more convenient to just hand over the card or simply insert it in a terminal.

1.6 Existing Systems

If one wishes to replace traditional cash, our surveys came to the conclusion that one needs at least off-line transferability and untraceability. Of course we cannot estimate how big the share of traditional cash is one could replace if these two characteristics are not fulfilled in total. But we believe the reader will agree that these two are important characteristics. Today, there is not a single implemented prototype fulfilling them all. All Internet payment schemes, such as ecash[12], cannot be used off-line. All current smart-card purses neither provide untraceability nor transferability. Among all off-line usable systems ever built, only Mondex provides transferability, and only the CAFE prototype provides untraceability but only limited transferability to "sibling" cards (e.g., for paying from parents to children to the merchant).

1.7 Consequences

In the European deployments of stored value cards it became apparent that it is very difficult to replace traditional cash. Except with Mondex, holders were not put into a position to directly transfer value to anybody who participates. Some issuers tried to provide for transparency by distributing card readers. Also usability restricted to a nation seemed odd at times other cards are increasingly accepted abroad. Usability of cards for payments over networks still is very seldomly seen.[13] From our own surveys we know that users are aware of the lack of functionality as compared to traditional cash. Accordingly, Tim Jones, then CEO of Mondex, said "Cash is a great product" (Financial Times of December 11/12, 1993). If one selects only some of the characteristics required one can sell in certain niches. But such issuers should not expect that they can replace traditional cash in general. It appears some have been trapped by their own sales promotion telling that their brand is a better form of traditional cash, with subsequent disappointment among holders, merchants and issuers when it was not usable, did not provide privacy, was not transparent, etc.

Wallets

Future electronic cash systems could, however, to a higher degree justify their name. Electronic wallets could have several megabytes of E^2PROM, a display, and a keyboard, which solves several problems at once: One can provide transferability. One

---

[12] Digicash's ecash requires on-line verification and, like all Internet payment mechanisms, does not really provide untraceability since they do not provide connection anonymity as the payer needs a TCP/IP address to establish a connection with the payee.

[13] The Dutch Telecom "KPN" trialled their Chipper stored value card in the EU-project SEMPER for payments over the Internet. See <http://www.semper.org>.

can store many coins. One can display how much funds one has and enter a PIN on one's own device. It would be possible to use the wallet-observer concept. One could also put the initiative for paying into the wallet, so that untrusted terminals cannot take money out. As compared to other payment instruments, immediate, off-line, irrevocable, untraceable payments would be possible. With low terminal costs thanks to a contact-less interface, they can even be cost-effective for small sums.

Unfortunately very little experience has so far been made with wallet-like devices because the semiconductor, plastic-card, and banking industries were locked into the direction of using chip cards. The question arises if users are willing to use larger devices and pay for them. First in-depth interviews with 300 frequent card users in five European countries indicate that these are willing to pay Euros 15-50 for devices which replace several cards (Furger et al. 1998). Feedback from people who were demonstrated mock-ups was quite encouraging:

> *"That's quite snazzy."*
>
> *"If I had a super gadget like this in my hands, of course I'd use it for a whole variety of things."*
>
> *"It's obvious that something like this is going to come eventually."*
>
> *"Could be something like a Swatch, the latest trend to have."*
>
> *"That's the future, this kind of thing."*

However, no large trial has been made so far[14]. The willingness to own such devices may increase once users will wish to make digital signatures securely, i.e., see what they sign, and enter approval on their own machines instead of on an untrusted machine, potentially infected by malicious code (cf. the German Digital Signature Law, Bundesregierung 1997). This would render the usability of digital signatures at different places possible, thus also at the point of sale. In order to reduce the marginal costs of wallets, one could incorporate the payment and signature functions into other devices, such as pocket calculators, phone sets, car locks, digital cameras and organisers (see Pfitzmann et al. 1997, Weber 1998). With biometric verification, in case only approval must be given, one would not need a keyboard and then even watches could be used.

[14] In CAFE only few transactions were made using the infra-red interface, and in the UBS St. Moritz trial of 1990, also using a stored-value card with a wallet, the radio interface was not very robust.

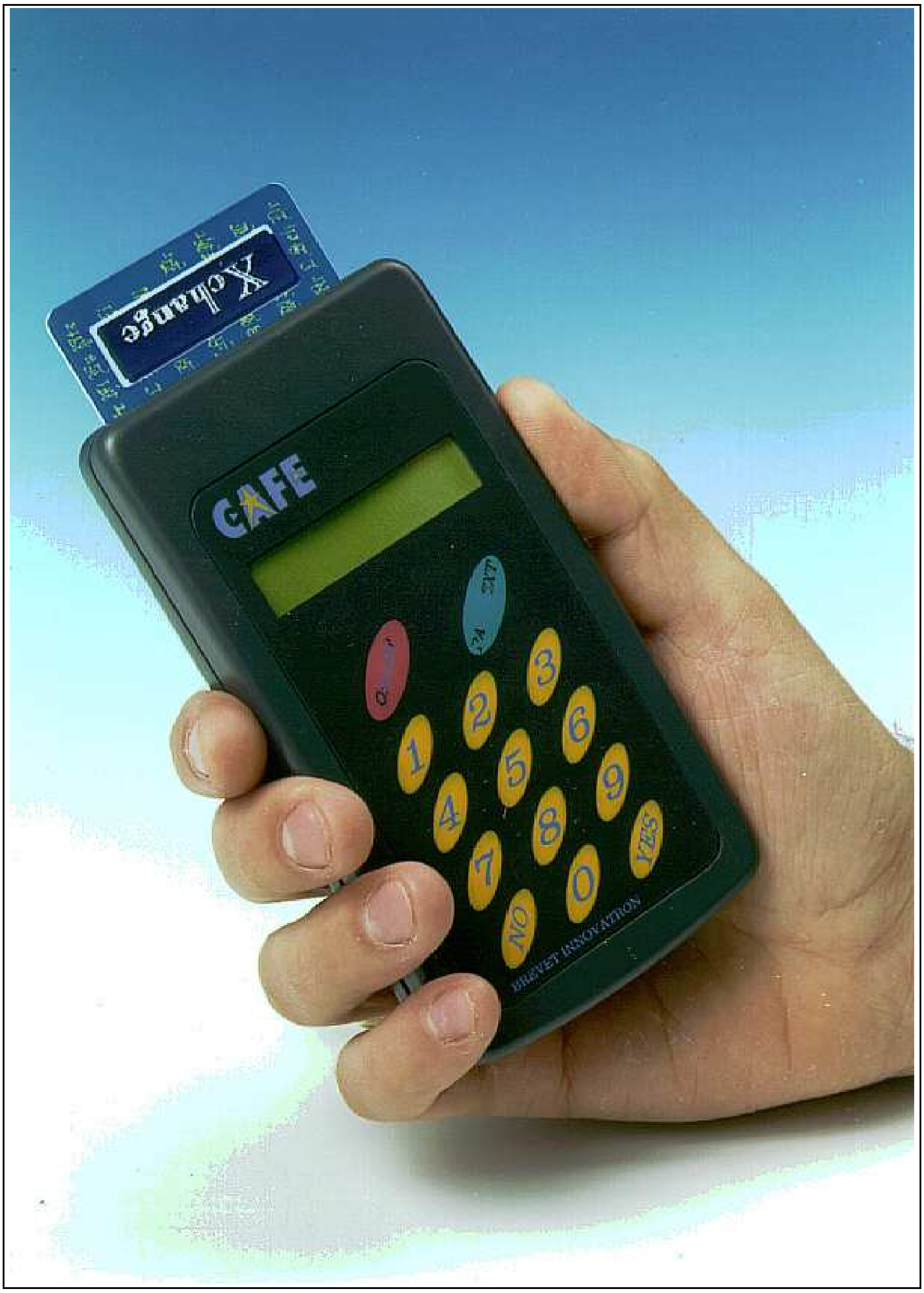

Figure 1: CAFE-Wallet, with infra-red and normal chip card interfaces.

Figure 2: Backside of a multi-functional wallet with drawer for security modules from railway company, bank, etc. (Özalp 1996).

Coins in Cards

As the banking industry focuses on cards, one could attempt to put untraceable electronic cash into a smart card, but without a counter. It might be possible to design a coin system based on blind signatures using card chips. To minimise storage space one can use divisible or multi-spendable coins. Privacy will suffer somewhat because some payments will become linkable. Robustness, transparency and loss tolerance, however, will be as difficult to achieve as in any other card system. Still, this could be a system with fairly low costs for the device on the side of the holder. However, for usability balance readers will need to be supplied, so why not build wallets in the first place?

Other Approaches

Besides the two approaches sketched, a third approach is to use more powerful intrusion detection mechanisms for tamper-resistant modules and thus rely less on signatures. Systems exist with battery-powered RAM, against some of which no attack is known (e.g., crypto boards manufactured by IBM). Today such carriers are thicker than normal card chips and, as produced in small batches, very expensive. But issuers could rely more on tamper resistance than they do today. A forth possibility might be to search for new cryptographic techniques.

Can *Cash* be Digitalised?

Even with today's techniques it is be possible to bring more characteristics, like off-line usability, transparency or untraceability, into new electronic payment systems. Untraceable systems, e.g., would be much closer to our traditional cash than existing card payment schemes. Such systems could also be cost efficient for small values. However, as the trade-offs have shown, building an electronic payment system justifying the name “Electronic Cash” remains a research challenge.

1.8 Acknowledgements

The authors wish to thank David Chaum, Franco Furger, Tatsuaki Okamoto, Birgit Pfitzmann, Ingo Pippow, Jan Reichert, and Michael Waidner for many valuable discussions. The consumer surveys have been made for the CAFE project. The authors wish to thank our interviewers and more than 300 respondents (see Furger et al. 1998, Weber 1995, Weber 1997 for the results). This work was partially supported by the ACTS SEMPER project; however, it represents the view of the authors only.

1.9 References

Anderson, Ross; Kuhn, Markus: Tamper Resistance - a Cautionary Note. The Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, California, November 18-21, 1996, pp. 1-11

Antwerpen, C. van: Electronic Cash. Master's thesis, Centre for Mathematics and Computer Science (CWI), Amsterdam 1990

Asokan, N.; Janson, Phillipe; Steiner, Michael; Waidner, Michael: The State of the Art in Electronic Payment Systems, IEEE Computer 30/9 (1997), pp. 28-35

Bonorris, Steven; Digital Money: Industry and Public Policy Issues; Institute for Technology Assessment; Washington, 1997

Bos, Jurjen; Chaum, David; SmartCash: A Practical Electronic Payment System. Report CS-R9035, Centrum voor Wiskunde en Informatica, Amsterdam 1990

Bundesregierung, die: Verordnung zur digitalen Signatur (Signaturverordnung - SigV), in der Fassung des Beschlusses der Bundesregierung vom 8. Oktober 1997. Available at <http://www.bsi.de>

CAFE: The CAFE Consortium: Technical Specifications: Architecture and Protocols - Final Report Volume IIA, CAFE (Esprit 7023) Deliverable PTS9364, April 1996

Chan, Agnes; Frankel, Yair; Tsiounis, Yiannis: Easy Come - Easy Go Divisible Cash. Eurocrypt' 98, LNCS 1403, Springer-Verlag, Berlin 1998, pp. 561-575

Chaum, David: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 1981, pp. 84-88

Chaum, David: Blind Signatures for Untraceable Payments. Advances in Cryptology, Proceedings of Crypto' 82, New York 1983, pp. 199-205

Chaum, David: Privacy Protected Payments – Unconditional Payer and/or Payee Untraceability; SMART CARD 2000, Laxenburg (Austria), 19.-20. 10. 1987, North-Holland, Amsterdam 1989, pp. 69-93

Chaum, David; Fiat, Amos; Naor, Moni: Untraceable Electronic Cash. Crypto '88, LNCS 403, Springer-Verlag, Berlin 1990, pp. 319-327

Chaum, David: Achieving Electronic Privacy. In: Scientific American (August 1992), pp. 96-101

Chaum, David, Pedersen, Torben: Transferred Cash Grows in Size; Eurocrypt '92, LNCS 658, Springer-Verlag, Berlin 1993, pp. 390-407

Diffie, Whitfield; Hellman, Martin: New Directions in Cryptography. IEEE Transactions on Information Theory, 1976, pp. 644-654

Furger, Franco; Paul, Gerd; Weber, Arnd: Survey Results. Paper, 1998 (Project CAFE). Available at <http:/www.iig.uni-freiburg.de/~aweber/>

Furche, Andreas; Wrightson, Graham: Computer Money: a systematic overview of electronic payment systems, dpunkt Verlag, Heidelberg 1996

Hayek, Friedrich von: Entnationalisierung des Geldes. Eine Analyse der Theorie und Praxis konkurrierender Umlaufsmittel. Mohr, Tübingen 1977

Japanese Ministry of Finance: Problems Related to the Circulation of Prepaid Cards. Report from the Research Group. Tokyo 1989 (in Japanese)

Okamoto, Tasuaki; Ohta, Kazuo: Universal Electronic Cash. Crypto '91, LNCS 576, Springer-Verlag, Berlin 1992, pp. 324-337

O'Mahony, Donal; Peirce, Michael; Tewari, Hitesh: Electronic Payment Systems, Artech House, 1998

Özalp, Nilgün: Entwurf von Benutzerendgeräten für elektronische Zahlungssysteme. Master's thesis, Fachhochschule Hildesheim/Holzminden 1996

Pedersen, Torben: Electronic Payments of Small Amounts. Security Protocols 1996, LNCS 1189, Springer-Verlag, Berlin 1997, pp. 59-68

Pfitzmann, Birgit; Waidner, Michael: Properties of Payment Systems - General Definition Sketch and Classification; IBM Research Report RZ 2823 (#90126) 05/06/96, IBM Research Division, Zurich, May 1996

Pfitzmann, Birgit; Waidner, Michael: Strong Loss Tolerance of Electronic Coin Systems. ACM Transactions on Computer Systems 15/2 (1997), pp. 194-213

Pfitzmann, Andreas; Pfitzmann, Birgit; Schunter, Matthias; Waidner, Michael: Trusting Mobile User Devices and Security Modules. Computer 30/2 (1997), pp. 61-68[15]

Schmidt, Max; Schunter, Matthias; Weber, Arnd: Is Electronic Cash Possible? Universität des Saarlandes, Fachbereich Informatik. Techn. Bericht Nr. A/03/98, 1998

Weber, Arnd: See What You Sign. Secure Implementations of Digital Signatures. Trigala Sebastiano et al. (eds.): Intelligence in Services and Networks: Technology for Ubiquitous Telecom Services. Springer-Verlag, Berlin 1998, pp. 509-520

Weber, Arnd; Carter, Bob; Pfitzmann, Birgit; Schunter, Matthias; Stanford, Chris; Waidner, Michael: Secure International Payment and Information Transfer. Towards a Multi-Currency Electronic Wallet. Frankfurt 1995 (Project CAFE)

Weber, Arnd: Soziale Alternativen in Zahlungsnetzen. Campus, Frankfurt, New York 1997

[15] See chapter "Trustworthy User Devices" in this publication for a revised version.