SURVEY OF ELECTRONIC PAYMENT METHODS AND SYSTEMS

Paul J.M. Havinga, Gerard J.M. Smit, Arne Helme

University of Twente, department of Computer Science
P.O. Box 217, 7500 AE Enschede, the Netherlands
e-mail {havinga,smit,arne}@cs.utwente.nl

Abstract

In this paper an overview of electronic payment methods and systems is given. This survey is done as part of the Moby Dick project[1]. Electronic payment systems can be grouped into three broad classes: traditional money transactions, digital currency and credit-debit payments. Such payment systems have a number of requirements: e.g. security, acceptability, convenience, cost, anonymity, control, traceability and control of encryption methods.
Some requirements appear contradictory and trade-offs have to be made:

- traceability versus anonymity,
- on-line versus off-line,
- use of dedicated tamper-resistance hardware versus software only.

We further present an introduction to the basics of electronic money: encryption, digital signatures, anonymity, and solutions to the double spending problem for digital cash. We give a survey of payment mechanisms, that are either commercially or in a pilot version available today or have been published recently.

1 INTRODUCTION

This survey is conducted as part of the Moby Dick project (Mullender et al. 1995). In this project we develop and define the architecture of a new generation of mobile hand-held computers. The design challenges lie primarily in the creation of a single architecture that allows the integration of security functions (e.g. payment), externally offered services (e.g. airline ticket reservation), 'personality' (i.e. these devices know what their owners want), and communication.
The research issues include: security, power consumption and communication, hybrid networks, data consistency, and environment awareness.
In this paper we will focus on one aspect of the Moby Dick architecture: secure electronic payment systems. An objective of Moby Dick is to find out whether we can provide a plausible and integrated solution for implementing secure payment mechanisms in very personal and relatively resource poor machines. In this survey we give an overview of current trends in electronic payment as was found in the literature; we focus only on the electronic payment mechanism, and not on transactions involved.

1.1 Electronic transactions vs payments

We make a distinction between *electronic transaction* protocols and *electronic payment* protocols. While electronic payment deals with the actual money transfer, electronic transaction protocols deals with the transactions as a whole. This includes: service delivery, service acceptance, confirmation of payment, receipts, etc. Both are of importance for electronic commerce systems.
Electronic transaction protocols group together operations and implement failure atomicity, permanence and serializability. An electronic transaction either fails or all of its operations are carried out (*failure atomicity*). If a transaction fails all partially completed results will be undone. All transactions that complete successfully can not be undone, and the results of these transactions are not lost (*permanence*). The results of transactions that are carried out concurrently will be the same as if they were carried out serially (*serializability*).
Electronic payment protocols transfer trust, either as cryptographically signed promises, or as digital cash. Signed promises prove the authenticity of a sender and the sender's intention to pay for a service. This is, essentially, how credit card systems work. Digital cash is signed messages representing real currencies. These messages do not carry any identification of the sender and are by themselves anonymous.

Electronic transactions and electronic payments are orthogonal issues and solve different problems. A key point is that the payment itself is usually only a small part of the interaction with a service provider, and a system that implements electronic commerce must also implement other ingredients of electronic transactions. For example, if a merchant pays for a service with digital cash, but cannot prove afterwards that the service was actually paid for, the system will not be very secure for individuals.

1. The Moby Dick project is a joint European project (Esprit Long Term Research 20422).

1.2 Electronic payment models

Electronic payment systems can be grouped into three broad classes: traditional money transactions, credit-debit payments and digital currency.

Traditional money transactions

Currently, debit cards are spread widely and deposit transfer via the Internet appears to be coming soon (White 1996). On-line payment by credit card is already available at many commercial web sites today. But these are evolutionary rather than revolutionary changes. What happens behind the scenes - deposit transfer - remains the same. A problem of these type of transactions is that the credit card details must be handled confidential. For secure credit card transactions, a customer's credit card number is encrypted using public key cryptography, so that it can only be read by the merchant. The big advantage of this approach is that the customer does not need to be registered with a network payment service; all that is needed is a credit card number. However, without registration of customers, the encrypted credit card transaction does not constitute a signature, anyone with knowledge of the customer's credit card number can create an order for payment.
Also, because payments processed using this approach are processed as standard credit card charges, the costs are quite high so that this method is not suited for payments whose amounts are on the order of cents.

Credit-debit payments

In payment mechanisms that use the credit-debit model, including CMU's NetBill, First Virtual's InfoCommerce system, and USC-ISI's NetCheque system (Neuman and Medvinksky 1995), customers are registered with accounts on payment servers and authorize charges against those accounts. These systems depend on conversion to/from 'real' currency. With the debit or check approach, the customer maintains a positive balance that is debited when a debit transaction or check is processed. With the credit approach, charges are posted to the customer's account and the customer is billed for or subsequently pays the balance of the account to the payment service.

Electronic credit/debit money can be represented by a *digital cheque*, just like a normal bank cheque. This payment method is by definition not anonymous. In this scheme the bank hands out customer specific blanc cheques to its customers. To pay a merchant the customer fills in the cheque (amount, merchant and date) and puts a digital signature on it. The merchant verifies the origin of the cheque (using the public key of the bank) and the signature of the customer.
An important advantage of the credit-debit model is its auditability. Once a payment has been deposited, the owner of the debited account can determine who authorized the payment. This is important for payments by businesses and desirable by individuals for many of their transactions.

The anonymity can be solved by introducing a trusted third party, sometimes called payment server. With a *direct transfer* payment model the customer and merchant are registered with accounts on a payment server in much the same way as with the credit-debit model. To make a payment, the customer directs the payment server to transfer funds to the merchant's account. The merchant is then notified of the transfer by the payment server or the customer and provides the product or service after verifying that the transfer has occurred. When the payment server is trusted by all parties, it can act as an intermediate between the bank and the customer, hiding the spending pattern of the customer from the bank.

Digital currency

Developments in cryptography has brought a new kind of money: the *digital currency* (e.g. the DigiCash system (Chaum 1992), the CAFE project (Boly et al. 1994) and Mondex). The digital money, an encoded string of digits, can be carried on a smart-card, or stored on a computer disk. Like a traveler's check, a digital coin is a floating claim on a bank or other financial institution that is not linked to any particular account. One cardholder can make a payment to another without bank involvement, by placing both cards in a 'digital wallet' that moves coins from one card to the other. Desktop electronic money transfers can similarly be made by electronic mail. Like paper currency and coins, digital coins are circulating on bearer media. The coins might not have correspondence to 'real' currency.
If personal information is omitted from the coins (unlike current practice in debit- and credit-card transactions), the owner can remain anonymous. An issuing bank only needs to know the total of its outstanding coins, not who holds them at any moment.

A significant aspect of digital currency systems is that digital coins can be given to somebody you do not fully trust, this in contrast to credit-debit payments in which trust between all parties need to exist.

1.3 Size of the transaction

Another classification of electronic payments can be based on the amount of money transferred in a transaction. Even though one may think transactions will eventually be virtually free compared to current transactions, there will still be a noticeable minimum cost of transaction which will depend on its type. Cavarretta and de Silva (Cavarretta and de Silva 1995) identify three classes of typical transactions:

Tiny value transactions: below $1
Medium value transactions: between $1 and $1,000
Large value transactions: above $1,000

Systems that can support tiny value transaction have to

trade-off between convenience of transaction (the major part of a cost in an extremely cheap transaction) vs. the security or durability of transaction. On the other side of the amount range, large value transactions will require highly secure protocols whose implementation are costly: be on-line and/or carry traceability information. Finally, nearly all the system can perform medium value transactions.

2 REQUIREMENTS

In electronic commerce at least two sets of parties (with broadly similar interests within each set) will need to participate: customers and merchants on the one hand, and financial institutions and regulators on the other hand. Arbitrators may be needed in case of a dispute.

2.1 Concerns of customers and merchants

Customers and merchants will have an almost common set of wishes and concerns for electronic commerce mechanisms:

1 *Security.* Electronic currency is just data and is easily copied. It has to be assured that no-one else can divert a payment or impersonate another person in order to steal his funds. Moreover, every party should be protected from a collusion of other parties (multi-party security). No party in the system needs to trust another party - or at least the trust should be as little as possible - to ensure his security. The acclaimed security properties must be publicly verifiable.
2 *Acceptability.* A wide range of parties needs to accept the payment.
3 *Convenience*. To make small purchases, the actions required during a transaction should be minimal. This pertains not only the physical efforts required of a party, but also the speed by which the transaction is processed. This includes: *speed, reliability, fungible* (the 'currency' or payment unit should be divisible), *transferability* (peer-to-peer payments) and *minimal specific hardware*.
4 *Cost*. Preferable no additional cost, hence no effective lower limit to the value of a transaction. Transaction costs include any direct costs, at the customer, merchant and at any intermediary, as well as processing or handling time for all parties.
5 *Privacy.* Today, cash is a more or less anonymous payment mechanism. No external party (individual, company or other authority) can create a historic record of any individual's cash transactions. With electronic money the bank, or any other party should not be able to determine whether two payments were made by the same user.
6 *Durability.* The electronic money should not be easily 'lost': for example, when a system crashes.

2.2 Requirements for financial institutions

The financial institutions, that will provide services to enable these transactions in the marketspace, and regulators will also have a set of requirements for a payment mechanism:

1 *Immediate control*. Financial institutions and regulators will seek a system in which transactions are controlled or cleared individually, so that any breach of security can be identified as soon as possible.
2 *Traceability.* Financial institutions and regulators will seek a system in which transactions are traceable, so that if a crime is detected the culprit can be identified. In particular, traceability will be important to track international funds flows, tax evasion and money laundering.
3 Control over the *spread of encryption* mechanisms. A key concern of the government, and therefore any regulatory body, is to control the spread of encryption mechanisms.

2.3 Trade-offs

The possibility that a large share of the economy transactions will be carried on a new medium raises a lot of regulatory and public concerns described above. Many of those concerns appear contradictory and conflicting, not all the properties of an ideal system can be accomplished at the same time.

Privacy versus traceability

A conflict exists between the wish for privacy and anonymity and the possibility and desire of regulators and intermediaries to be able to trace any transaction in the economy. Traditional intermediaries (credit card companies, banks, etc.) emphasize the desire by consumers to be able to trace their own transactions themselves. Their systems have a low level of anonymity and serve more the objectives of the credit service bureau than those of consumers. Some systems, like David Chaum's DigiCash, have been designed with emphasis on privacy and anonymity.

On-line versus off-line

An other important trade-off to be made is between the centralized and decentralized system, or to put it differently, between the need to verify the transactions on-line vs. the ability to trust a transaction without the presence of an on-line third party. Being able to perform the transactions off-line fulfils many participant requirements and makes electronic money the most alike true physical cash. It is more convenient because it does not require a third party to be constantly functioning. It is cheaper because of the reduced bandwidth and the absence of bottleneck problems. On the other hand, having a transaction processed on-line has advantages to financial institutions and regulators. This is the easiest manner to solve the double spending

problem: a transaction is approved and cleared on the spot. Furthermore, it provides the ability to trace the transactions.

Hardware versus software

A dedicated hardware solution might look to be the ideal technical solution in many senses, but raises some economical and technical issues. On the one hand, the smart card, a tamper resistant piece of hardware with security functions, can help to solve the double spending problem in an off-line environment. It is very flexible at a very low cost per transaction. It is therefore perfectly adapted to tiny and medium value transactions, but not to high valuable transactions because of its non durability.
On the negative side, it requires the spread of specific pieces of hardware (card readers) and its acceptance by consumers. It therefore requires a broad agreement among participants. Also, this kind of card can be loaded with unidentifiable tokens (ideal anonymous cash system) and used without password. This implies that, if a customer declares the card lost, stolen or destroyed, the cash is lost. This property makes the smartcard a non-durable system, and therefore not adapted to large transactions.
New technologies may make tamper-resistant devices more vulnerable to attacks. For this reason, the security of a system should only partly be dependent on the tamper-resistance of the user-devices.

Transparency versus explicitness

On the one hand users may want transparent money transaction algorithms, the real money transactions are hidden from the user. But on the other hand the users want to be in the control-loop of all the money transactions. They want to be sure that they only pay what they have asked for and they do not want to spend any money without being notified.

3 BASICS OF ELECTRONIC MONEY

There are a number of technical options to implement electronic money: asymmetric keys vs. public key system; on-line versus off-line system; hardware specific (smart card) vs. hardware independent, etc. See (Schneier 1996) for an overview.
In this section we will describe the main techniques that are used to implement parts of the electronic money mechanisms.

The simplest electronic version of money can be text, created with a word processor or e-mail package, asking your bank to pay someone a specific sum. However sending this ‘money’ over an electronic network creates several security problems (Computer Active 1996, Chaum 1992): confidentiality, authentication, non-repudiation, integrity, anonymity and detection or prevention of double spending.

First, as the money is sent over the network it must be unreadable for unauthorized persons. Therefore, the electronic money must be *encrypted*. Encryption can be done by using a mathematical transformation with a key. Both secret key as well as public key encryption can be used.

To prevent that somebody else creates similar money we need authentication. The purpose of *digital signatures* is to authenticate both the sender and the message; i.e. to provide proof to the recipient that the message stems from the sender, and that the message’s contents have not been altered since leaving the signatory. Cryptography has produced a number of different methods for proving and verifying the authenticity of electronic documents, messages and transactions using a digital signature.
The sender produces a digital signature by applying certain calculations to a message. This process is called the *signature function*. The resulting signature, which looks like random data, only has meaning when read in conjunction with the message used to create it. The recipient of the message checks the digital signature by performing another set of calculations on the signature and the message. This is called the *verification function*. The result of these calculations reveals whether or not the signature is a genuine authentication of both sender and message. To guarantee that the public-key list (used by everyone to verify signatures) has not been tampered with the public directory entries are digitally signed by a certification authority trusted by all parties. Using the authority’s public key anyone can verify that the directory entry is genuine. The signed directory entry is known as a ‘*certificate*’.

The system described above is secure, but it is not *anonymous*. If the bank keeps track of note numbers, it can link each shop’s deposit to the corresponding withdrawal and so determine precisely where and when a client (or any other account holder) spends his/her money. The resulting dossier is far more intrusive than those now being compiled. Chaum has developed an application of digital signatures, called blind signatures, that can restore privacy. There are other solutions that partially solve the anonymity problem, for example (Brands 1995), or using an anonymous intermediate (e.g. ACC) (Low et al. 1994).

Since electronic money is just a bunch of bits, a piece of electronic money is very easy to duplicate. Obviously, real electronic money systems must be able to prevent or detect *double spending*.
On-line electronic money systems prevent double spending by requiring merchants to contact the bank’s computer with every sale. The bank computer maintains a database of all the spent pieces of electronic money and can easily indicate to the merchant if a given piece of electronic money is still spendable. If the bank computer says the electronic money has already been spent, the merchant refuses the sale.
Off-line electronic money systems detect double

spending in a couple of different ways. One way is to create a special smart card containing a tamper-proof chip called an 'Observer' or 'Guardian'. Both the user and the bank have to trust the observer chip. The observer chip keeps a mini database of all the pieces of electronic money spent by that smart card. If the owner of the smart card attempts to copy some electronic money and spend it twice, the Observer chip would detect the attempt and would not allow the transaction. Since the Observer chip is tamper-proof, the owner cannot erase the mini-database without permanently damaging the smart card. The other way off-line electronic money systems handle double spending is to structure the electronic money and cryptographic protocols to reveal the identity of the double spender by the time the piece of electronic money makes it back to the bank. This is sometimes called *one-show blinding* (Chaum 1992). If users of the off-line electronic money know they will get caught, the incidents of double spending will be minimized. The advantage of these kinds of off-line systems is that they do not require special tamper-proof chips.

4 CURRENT SYSTEMS

In this chapter we show some payment mechanisms that are either commercially or in a pilot version available today or have been published recently. Many systems are similar, and differ only in some minor details. The following analysis does not cover an exhaustive list of all available mechanisms, but illustrates the main options and their associated features.

4.1 Traditional money transactions

These systems have the characteristics normally associated with credit card and bank card transactions. They are mainly used for identification of the user, so they are not anonymous since the credit card company or the bank has a record of all transactions. Since there is likely to be on-line verification of transactions on a real-time basis, there is immediate control. As a result of the on-line clearing, total cost is fairly high. In most cases, credit cards are only accepted above certain amounts. Peer to peer transactions are not possible. Without any encryption, sending credit card details over a network such as the Internet is not secure: the details can be pulled off by anyone 'listening' on the open network. There are several systems that facilitate secured credit card transactions over the Internet, we will mention just a few.

SET

IBM, Netscape, GTE, CyberCash, MasterCard, Microsoft and Visa have cooperatively developed the Secure Electronic Transactions Protocol (SET) for securing on-line transactions. This protocol will facilitate credit card transactions on the Internet. SET secures cardholder account and payment information as it travels across the network, preventing interception of account numbers and expiration dates by unauthorized individuals. Payment information and authentication is ensured by the use of digital signatures.

PCT

The Private Communication Technology (PCT) protocol, defined by Microsoft, provides privacy between two communicating applications, and authenticates at least one of the two to the other. A higher level application (e.g. HTTP, FTP, etc.) can layer on top of the PCT protocol. PCT uses a symmetric session key for the encryption of messages during a connection, and performs the requested authentications based on asymmetric public keys.

iKP

iKP is an IBM proposal for a family of public key protocols supporting secure presentation of credit card information (Bellare et al. 1995). The iKP technology is designed to allow customers to order goods, services, or information over the Internet, while relying on existing secure financial networks to implement the necessary payments. The iKP technology is based on RSA public-key cryptography.

First Virtual's InfoCommerce System

In this system the credit card information is given to First Virtual via phone only when the account is opened. Thereafter, purchases are made using user account ID. During purchase, the client gives the vendor his client's ID. The vendor sends a transaction report to First Virtual, on which it e-mails a report to the client for confirmation. If the client confirms, the client's credit card order is processed.

4.2 Credit-debit payments

Millicent

Millicent (Glassman et al. 1995) aims at small-scale commercial transactions over electronic networks. Typical schemes for performing commercial transactions require at least a digital signature per transaction. Unfortunately, reasonably unforgeable digital signatures are slow: contemporary machines can sign one to four dozen messages per second, depending on key length, while decryption runs about an order of magnitude faster. Millicent seeks to reduce the costs, increase the transaction rate, and provide on-line levels of certainty to vendors. It does this by introducing the notion of vendor-specific *digital scrip*: vendor-specific to make it easy to verify that it hasn't been doubly-spent, and generated according to local criteria, so that it can be easily verified for authenticity. A typical method for generation might be to use a secret key to encrypt a serial number; the encrypted value and index of the key form the scrip. When the scrip is received by the vendor, it is decrypted in order to verify that it encodes a valid, previously unspent index. *Brokers*

mediate between vendors and customers to provide sufficient amortization opportunity for the scrip. While customers may take months or years to spend enough at a single vendor to cover the cost of a standard financial transaction, we can expect that they will spend enough in total to justify a financial transaction with the broker that supplies all of their scrip needs.

NetCheque (Neuman and Medvinsky 1995)

NetCheque is a distributed accounting service supporting the credit-debit model of payment. Users of NetCheque maintain accounts on accounting servers of their choice. A NetCheque account works in much the same way as a conventional checking account: account holders write electronic documents that include the name of the payer, the name of the financial institution, the payer's account identifier, the name of the payee, and the amount of the check. A NetCheque payment bears a signature, and must be endorsed by the payee, using another signature, before the cheque will be paid. The system is based on the Kerberos system.

UEPS

UEPS, the Universal Electronic Payment System (Anderson 1992), is an electronic funds transfer product based on off-line operation. It is designed around smartcard based electronic wallet and chequebook functions. A customer loads her card with money from a card held by a bank teller or installed in an ATM; she then makes purchases by transferring value to a merchant card; and the merchant in turn uploads his takings to his bank via an ATM or terminal.
The security of UEPS is based on two levels of authentication. The core is an electronic cheque which caries two digital signatures: one generated with a key known only to the issuing bank's security module and the customer card, and one generated with a key which is controlled by the clearing house and loaded by them to the card before it is supplied to the bank. The former signature will only be checked in the event of a dispute. Both signatures are standard message authentication codes, calculated on amount, payee and date. Only the cards embedded in bank and merchant terminals possess a set of universal secrets, and the customer cards have keys derived from their serial numbers using these master keys. The payment protocols implement both message chaining and double encryption.

Others

There are many systems in this category e.g. First Virtual Holdings, FSTC's Electronic Check project, NetBill.

4.3 Digital currency

DigiCash

The DigiCash system (Chaum 1992) involves the creation of 'electronic coins' in the form of digitally signed numbers in exchange for real money from the user's bank account. Each of these coins can be spent, once and only once, with a service provider who accepts them. When the coin is spent it is immediately sent by the recipient to the issuing bank for on-line verification and logging (to ensure it is not spent again) before confirming receipt to the payer, who then discards the used coins. The appropriate amount is credited to the recipient's bank account. This system uses 'blinding' techniques to ensure that the coin can be verified without revealing the identity of the payer to the payee or the bank.

NetCash

NetCash (Neuman and Medvinsky 1995) is an electronic currency service that supports real-time electronic payments with some provision of anonymity across multiple administrative domains on an unsecured network. NetCash tries to find a balance between unconditionally anonymous electronic currency, and signed instruments analogous to checks that are more scalable but identify the principals in a transaction. Currency issued by a currency server is backed by account balances registered with NetCheque to the currency server itself and the NetCheque system is used to clear payments across servers and to convert electronic currency into debits and credits against customer and merchant accounts. Though payments using NetCheque originate from named accounts, with NetCash the account balances are registered in the name of the currency server, and not the end user.

CAFE

CAFE (Boly et al. 1994) provides a high security of all parties concerned without being forced to trust other parties (so-called multi-party security). This should give legal certainty to everybody at all times. Moreover, both the electronic money issuer and the individual users are less dependent on the tamper-resistance of devices than in usual digital payment systems. It uses a combination of tamper-resistance devices extended with Chaum's protocol. As long as the smartcard is tamper resistant, it is impossible to spend money more than once. If tamper-resistance of the device is broken, users who spend electronic money more than once are identified, and the fraud can be proven to them. Since CAFE aims at the market of small everyday payments that is currently dominated by cash, payments are off-line, and privacy is an important issue.

Mondex

The Mondex system is based on a tamper-proof smart card that holds the cash (in multiple currencies) and the software to make and receive payments. The system preserves anonymity in that only the chip on the card has a complete record of transactions, and therefore only the cardholder has access to this information.

Nevertheless, if it were necessary to reconstruct a customer's trace for reasons of justice, the information could be accessed with the customer's permission or by collecting information from merchants. The chip on the card provides immediate control at the time of any transaction. Peer to peer transactions are possible, providing both parties have access to the necessary hardware. The system can be used for any amount, and should be relatively fast and reliable.

Brands' off-line electronic cash system

In this system a tamper-resistant smart card, issued by the bank and trusted by the user, controls a counter that represents the amount of electronic cash carried by the user (Brands 1994). The use of a counter ensures that the computation and communication complexity for paying an amount are independent of the specific amount due, and that conversions between multiple currencies can be made at payment time. Smart cards can transfer electronic cash to POS terminals that need not be physically secured by the bank without needing on-line verification. Cryptographic software in the user controlled computer ensures that payments are untraceable and unlinkable. A build in mechanism for tracing of double spent transaction data ensures that the cost of breaking the smartcard in practice will significantly exceed the expected financial profit that the attackers can make from this.

Others

Other systems in this category are currently in test or actually in use (e.g. Chipknip and Chipper in the Netherlands)

5 CONCLUDING REMARKS

Our study for this survey revealed many electronic payment systems. However, some systems are quite similar, and differ only in some minor details. We distinguish three categories i.e. traditional money transactions, credit-debit payments and digital currency. Such payment systems have different strengths and weaknesses with respect to their requirements: security, acceptability, ease of use, transaction cost, additional cost (e.g. point of sale hardware), privacy/ traceability, durability and immediate control.
Table 1 shows a quick overview of typical electronic payment models. The digital cash systems are described in more detail, because they were most promising for our project and they are the least traditional. Digicash, CAFE and Mondex were chosen because they represent typical classes of digital cash.

Many of the concerns of the parties involved in electronic payment appear contradictory and trade-offs have to be made. Therefore it is hardly possible to draw a definitive conclusion which approach is best. One approach might work in one application, whereas it would fail in another. A contradiction exists between

	Tradi-tional.	Debit/ Credit	Digital cash Digicash	CAFE	Mondex
security	+	+	++	++	+
acceptance	++	o	o	o	+
ease of use	+	o	+	++	++
transact.cost	--	+	-	++	++
extra cost	++	++	++	-	-
privacy	--	-[a]	++	++	o
durability	++	++	+	+	--
control	++	++	++	++	o
transaction size	medium large	small medium	medium	small medium	small medium
on/off-line	on	on[b]	on	off	off
smartcard	no	no	no	yes	yes

Table 1: Quick overview of some studied systems

a. Millicent protocol has privacy via trusted third party
b. UEPS is off-line and uses a smartcard

the right of privacy/anonymity and the possibility and desire of regulators and intermediaries to be able to trace any transaction in the economy, whereas the customer may want anonymous transactions. An other important trade-off to be made is between the need to verify the transactions on-line versus the ability to trust a transaction without the presence of a third party. A dedicated hardware solution might look to be the ideal technical solution in many senses, but raises some serious market and technical issues. On the one hand, the smart card, a secured piece of hardware, can help to solve the double spending problem in an off-line environment.

Most payment systems have been proposed by technologists and concentrate on overcoming the insecurity of communication networks to enable applying traditional payment mechanisms. Although this is a first step towards electronic commerce, it imposes constraints and therefore the mechanism is not suited for all types of payment. Another often used payment method is credit-debit transactions. An important advantage of the credit-debit model is its auditability. However, this model does not typically provide anonymity, though it may be extended to do so. The third type is electronic currency. If personal information is omitted from the balance transfer information (unlike current practice in debit- and credit-card transactions), the bearer can remain anonymous.

Another classification of electronic payments can be based on the amount of money transferred in a transaction. There will be a noticeable variable cost of trans-

action which will depend on its type. Systems that can support transactions of small amounts of money have to trade-off between convenience of transaction (the major part of a cost in an extremely cheap transaction) versus the security or durability of transaction. On the other side of the amount range, transactions incurring large amounts of money will require highly secure protocols whose implementation are costly: be on-line and/or carry traceability information.

6 REFERENCES

Anderson R.J.: "UEPS - a second generation electronic wallet", *Computer Security - ESORICS 92*, Springer LNCS v 648, pp 411-418. (see also ftp://ftp.cl.cam.uk/users/rja14/smartcards.ps.Z)

Brands S.: "Off-line cash transfer by smart cards", Centrum voor Wiskunde en Informatica (CWI), *Technical report CS-R9455*, September 1994. This is a revision of: Proceedings of the First Smart Card Research and Advanced Application Conference, Lille, France, Oct. 1994, pp. 101-117. (see also: http://www.cwi.nl/~brands/cash.html)

Brands S.: "Electronic cash on the Internet", *proceedings of the Internet Society 1995, symposium on network and distributed system security*, San Diego, February 1995, pp 64-84.

Boly, J.P. et al.: "The ESPRIT project CAFE - high security digital payment systems", *ESORICS 94, third European Symposium on Research in Computer Security*, Brighton, LNCS 875, Springer-Verlag, Berlin, pp 217-230 (see also / http://www.zurich.ibm.ch/Technology/Security/sirene//publ/BBCM1_94CafeEsorics.ps.gz)

Cavarretta F., de Silva J.: "Market Overview of payments mechanisms for the Internet commerce", http://www.mba96.hbs.edu/fcavarretta/money.html

Chaum D.: "Achieving electronic privacy", *Scientific American*, August 1992, pp 96-101 (see also: http://digicash.support.nl/publish/sciam.html)

Computer Active: information can be browsed on http://www.computeractive.on.ca/cAi/security/primer.html

Electronic Check: information can be browsed on http://www.fstc.org/projects/echeck/index.shtml

Glassman S. et al.: "The Millicent Protocol for Inexpensive Electronic Commerce", *proceedings of the 4th International World Wide Web Conference*. December, 1995. (see also: http://www.research.digital.com:80/SRC/millicent/)

FirstVirtual: information can be browsed on http://www.firstvirtual.com/

Bellare M., et al.: "iKP -- A Family of Secure Electronic Payment Protocols", IBM T.J. Watson Research Centre and IBM Zürich Research Lab, *proceedings of the First USENIX Workshop on Electronic Commerce*, New York, July 1995 (see also: http://www.zurich.ibm.com/Technology/Security/extern/ecommerce/iKP_overview.html)

Low S.H., Maxemchuk N.F., Paul S.: "Anonymous Credit Cards", *proceedings of the 2nd ACM conference on Computer and communication security*, Fairfax, Virginia, November 1994 (see also ftp://ftp.research.att.com/dist/anoncc/anoncc.ps.Z)

Mullender S.J., Corsini P., Hartvigsen G. "Moby Dick - The Mobile Digital Companion", LTR 20422, Annex I - Project Programme, December 1995 (see also http://www.cs.utwente.nl/~havinga/pp.html)

Mondex: information can be browsed on http://www.mondex.com.

NetBill: information can be browsed on http://www.ini.cmu.edu/NETBILL/publications

Neuman B.C., Medvinsky G.: "Requirements for network payment: the Netcheque perspective", *Proceedings of IEEE Compcon 95*, March 1995. (see also ftp://prospero.isi.edu/pub/papers/security/netcheque-requirements-compcon95.ps.Z)

PCT 96: Microsoft Corporation's PCT Protocol, Internet draft, April 1996

Schneier B.: "*Applied cryptography, second edition: protocols, algorithms, and source code in C*", Wiley, ISBN 0-471-11709-9

Secure Electronic Transaction (SET) Specification., Visa and MasterCard.

White L.H.: "The technology revolution and monetary evolution", *The future of money in the information age, Cato Institute's 14th Annual Monetary Conference*, May 23, 1996, Washington D.C. (see also: http://www.cato.org/moneyconf/14mc-7.html)