

# Electronic Payments: where do we go from here?

Markus Jakobsson<sup>1</sup>, David MRaihi<sup>2</sup>, Yiannis Tsiounis<sup>3</sup> and Moti Yung<sup>4</sup>

<sup>1</sup> Information Sciences Research Center, Bell Labs, Murray Hill, New Jersey 07974.

[www.bell-labs.com/user/markusj](http://www.bell-labs.com/user/markusj)

<sup>2</sup> Gemplus, 3 Lagoon Drive, Suite 300, Redwood City, CA 94065.

[david.mraihi@gemplus.com](mailto:david.mraihi@gemplus.com)

<sup>3</sup> SpendCash.com, Inc., New York, NY. [yiannis@spendcash.com](mailto:yiannis@spendcash.com)

<sup>4</sup> CertCo, Inc., New York, NY. [moti@certco.com](mailto:moti@certco.com)

**Abstract.** Currently, the Internet and the World Wide Web on-line business has boomed, with traffic, advertising and content growing at sustained exponential rates. However, the full potential of on-line commerce has not been possible to realize due to the lack of convenient and secure electronic payment methods (e.g., for buying e-goods and paying with e-money). Although it became clear very early that it is vital for payments to be safe and efficient, and to avoid requiring complicated user intervention, it is still the case that the Internet payment method of choice today is that of traditional credit cards. Despite their widespread use and market penetration, these have a number of significant limitations and shortcomings, including lack of security, lack of anonymity, inability to reach all audiences due to credit requirements, large overhead with respect to payments, and the related inefficiency in processing small payment amounts.

These limitations (some of which are present in the real world) prompted the design of alternative electronic payment systems very early in the Internet age – even before the conception of the World Wide Web. Such designs promised the security, anonymity, efficiency, and universal appeal of cash transactions, but in an electronic form. Some early schemes, such as the one proposed by First Virtual, were built around the credit card structure; others, such as the scheme developed by DigiCash, offered a solution with cryptographic security and payer anonymity. Still others, such as Millicent, introduced micropayment solutions. However, none of these systems managed to proliferate in the marketplace, and most have either ceased to exist or have only reached a limited audience.

This paper is associated with a panel discussion whose purpose is to address the reasons why the international e-commerce market has rejected proposed solutions, and to suggest new ways for electronic payments to be used over the Internet, avoiding the problems inherent in credit card transactions. The purpose of this paper is to set the stage for such a discussion by presenting, in brief, some of the payment schemes currently available and to discuss some of the basic problems in the area.

**Keywords:** anonymity, e-cash, e-commerce, electronic payments, security.

## 1 Introduction

Quite a large number of years had passed from the introduction of Arpanet/Internet until it started to become clear that the Internet would become a vehicle for carrying e-commerce. In the beginning, this network was largely of military interest and used by academics, and traffic was limited to email and file transfers using `ftp`. Large collaborative distributed computing was thought to be an application, but did not materialize. With the introduction of easy to use user interfaces based on `HTML`, access became possible for the masses, causing both the number of users and interest in conducting commerce to grow rapidly. One of the next major steps which promises to bring a large increase in Internet use and effectiveness is an improved payment infrastructure (in a very general sense). One factor commonly believed to have dampened the possibilities for, and interest in electronic commerce has been the lack of such an infrastructure. Thus, practically employable e-commerce has to date been based on existing payment structures, viz. credit cards. These however, have several properties that make them inappropriate for use over the Internet; some of these include their large overhead, risks related to inappropriate use, and inconvenience of use - particularly for small payments.

So, it seems that alternative and more simple methods of payment are required. The lack of such simple schemes can be explained by “the chicken and the egg problem,” namely, without a large existing merchant base, the need for payment schemes is less acute, and without a working payment scheme, merchants are unable to enter the Internet market. Another problem has been that financial institutes traditionally are very conservative, particularly when it comes to trying out new and heretofore unproven payment methods.

All of these problems are, however, gradually fading away: substantial work is being performed on implementing public key infrastructures. Merchants are becoming aware of the strong potential of the Internet marketplace and are making themselves ready to enter it quickly, and some banks are starting to employ cryptographers and security experts, making it easier for them to evaluate technology-related risks.

It seems that it is no longer a question whether there will be Web-based payment schemes. However, a question that remains is what type of scheme(s) will be employed and how soon. To some extent the question of what schemes will be dominant may be resolved not by the consumer, but via government intervention and bank preferences, and by corporate sponsorship. It is likely, though, that many schemes will co-exist at least for a few years, allowing the consumer to state desired preferences.

Cryptographic research has produced several important payment scheme properties over the last few years, including the issues of anonymity, revokable anonymity, micropayments, smart card and PDA based schemes, software-only schemes, among others. It seems that much has been achieved, but it may be the case that there is still a lot of technological work to be done. This is an interesting issue that needs to be discussed and examined. The suitability of the research results to the actual problems faced by financial institutions and

the merchant base is another motivating issue. This gives rise to the following characterization of categories.

### 1.1 Payment categories

At this point we should clarify that electronic payments can be classified according to the acting parties. The parties can be business-to-business, consumer-to-business, business-to-consumer, business-to-government, etc. However, most of these electronic payment needs have been covered. Businesses can transfer funds to each other via ACH or Wire transfers. Similarly, they can transfer funds to governments. Furthermore, even though there is still the possibility of enabling electronic checks among these entities, it is still unclear whether or not this is an enhancement of current possibilities or simply a true business enabler.

It seems to us that the open problem demanding immediate attention in current electronic payment methods is the lack of efficient consumer oriented payment methods (either consumer to business or business to consumer). This paper and discussion is therefore focused on this particular part of the market (of course, this segment of payments has to be connected to other e-payments).

**Organization:** The paper is organized as follows. Section 2 discusses credit cards, which are by far, the most prominent method for electronic payments. Section 3 discusses electronic checks, and how they fit in the on-line payment arena. Section 4 categorizes the various proposed “cash-like” methods. Section 5 gives representative examples of a variety of payment systems. We obviously are not exhaustive in covering the many various suggested schemes and apologize for omitting many interesting designs. Section 6 then touches on some likely future scenarios. Section 7 concludes the paper.

## 2 Credit card payments

The most common type of payment used on-line are credit card payments. The main reasons for this is of course convenience, ease of use, and because they are ubiquitous and omnipresent. However, as noted above, they are insecure, offer no anonymity, and do not allow small payments.

- **High costs and inability to allow small payments.** Each credit card payment has a fixed cost of 20-40 cents, plus a variable cost of 2-20%, depending on the method used and the negotiated contract.

The fixed costs originate from the cost of performing a transaction, since transactions usually involve some type of paperwork, and the traversal of a proprietary network rented by Visa, Mastercard, or some other credit card provider. US banking regulations exist which mandate that users' accounts be maintained so as to enable a mechanism for disputing payments. This makes relatively high fixed costs unavoidable.

The variable costs are a reflection of the security problems associated with credit cards. In other words, the credit card issuers recover their costs from

fraud by charging the merchants a percentage on their customers' purchases. For this reason this fee is variable, and is much higher for, say, Internet or telephone purchases than it is for purchases where the physical card is presented. It also varies by industry sector, with certain high-fraud businesses being penalized with higher fees. For Internet purchases the variable fees are typically higher, ranging from 5 to 20% of the purchase price.

In short, the main reason for these high fees is the insecurity of the original credit card design, which allows merchants to view (and copy, and reuse) all of the customer's private information.

As a result of these high fees, payments of less than \$10 cannot be made with credit cards with a reasonable profit being made by the merchants (especially for on-line merchants, who incur higher charges). Aggregating small payments into one reasonably sized amount before charging one's credit card is the solution currently used, but this poses too many unnecessary restrictions on both users and merchants.

- **All purchases are traceable.** Despite the convenience of a full history of one's purchases, as well as the ability to dispute payments made with a credit card (especially in the US), the fact that credit card issuers have all the users' spending information available poses serious privacy concerns. This information is sold to advertisers, and is utilized internally by credit card issuers to target advertisements to their audience. From both an ethical as well as a practical perspective, giving someone the ability to conduct payments should not go hand-in-hand with knowing their whereabouts, their spending patterns, and their personal preferences.
- **Security problems for the customers.** One of the bigger problems with credit card payments is that all the user's private information is exposed to the merchants. This allows merchants to effectively steal and use their customers' credit cards. Obviously, this is a much greater threat over the Internet, where the merchant can be located anywhere in the world. This security problem is manifested in two different ways, depending on where the credit card has been issued:

- For credit cards issued outside the US, the end-customer is held liable for all purchases. Thus, a stolen credit card number has a direct impact on the consumer. Clearly, this is a serious security problem, especially since the customers have little or no control whatsoever over the merchants' handling of their credit card information.
- For US-issued credit cards, there is a regulatory limit of \$50 on the consumer's liability in case of a lost or stolen card number. In addition, most credit cards will typically refund the whole amount from a fraudulent purchase, so more likely than not the customer's liability is nil. Credit card issuers often take advantage of the fact that consumers are afraid of losing their credit cards by offering them additional "security guard" features. In essence, this is an insurance against theft or loss of one's credit card; the problem is that the fee for this insurance is extremely high, typically 0.5 to 1% of all the customers' purchases.

Thus, in either case consumers are unfairly penalized for the credit cards' own inappropriate security design.

*SET*: VISA and MASTERCARD's analog to a credit-card setting which incorporates legally-binding signatures, implements digital signatures as a tool for authenticating users, merchants, and banks. This reduces the possibility of fraudulent transactions, thus bringing on-line transactions on par with physical-card solutions. Note however, that the complexity of SET has, so far, hampered its full-scale deployment. It is, in fact, too expensive for most merchants to implement, and it also requires end-users to download specific software and to participate in a public key infrastructure –which is not yet firmly in place. Also, even SET does not raise credit cards to a sufficiently high security standard to completely overcome fraud, hence credit cards still charge merchant fees which makes micropayments prohibitive.

### 3 Electronic checks

Following the model of physical payments, where credit cards, cash, and checks combine to dominate the market, a logical step for payments are electronic checks. Described in an abstract fashion, these are sequences of bits that encode a value, and using either digital signatures or other cryptographic constructions allows a receiver to distinguish between valid and invalid bit sequences.

Some methods have indeed been put to practice, but there has been no large-scale adoption to date. The biggest missing link for these schemes is to put in place legislation governing the use of digital signatures and other cryptographic functions, so that the types of digital agreements which can be seen as binding can be determined. This is therefore an adaptation of the interpretation of how written signatures are binding. Even though digital signatures have been put to practice many years ago, and even though they are much harder to forge than hand written signatures, they are not yet legally binding to the same extent that hand written signatures are (except in places where laws were put in place). This point creates a severe problem for issuing banks: lack of a clear regulation framework.

One of the largest components in the cost of checks is the physical delivery into and out of the clearing houses. Attempts to mimic checks electronically by presenting an electronic image of checks causes a large traffic over electronic networks, so it solves the cost problem only partially (whereas digital signature based checks have the potential for being much cheaper to implement).

So, while we believe that “check based” payments are viable, and that they will turn out to be important once they are successfully introduced, this is not likely to occur before more specific legislative structures are in place. Similarly, these payment methods depend on a comprehensive public key infrastructure to be in place before they can become common and widespread. While this is on the way of happening, it has not materialized yet.

It is important to note that banks and financial institutions are relatively conservative due to the heavily regulated nature of their industry. Therefore,

e-payment implementations to date are a very close reflection of payments in the physical world, and do not incorporate features that would normally come to mind in an electronic scenario. For example, there is no real-time clearing method for electronic checks, which although impractical in the physical-check world, would make perfect sense electronically. One possible reason for this is that banks have built their business models around a particular way of handling checks, which would be invalidated with the availability of real-time clearing. However, as technology progresses the banks will have to catch up or they are at risk of being bypassed.

## 4 Types of Cash-like Schemes

In this section, we will discuss some different types of cryptographically based payment schemes, broadly referred to as “e-cash” or “cash-like” schemes. This categorization is necessary due to the multitude of proposed systems and the differences between their approaches.

### 4.1 Privacy

As highlighted in section 2, consumer privacy is a major consideration, considering the ease with which data mining can be performed electronically. Therefore a significant portion of electronic payment systems afford some level of consumer privacy. We briefly outline the levels of available privacy in this section.

**Schemes with Perfect Privacy.** Information which can be considered personal can be gathered at several stages in a payment process. To begin with, for every Internet connection the IP address of the consumer is exposed; this can be used for various types of tracing and is certainly private information. On the other end, the merchant may explicitly request personal user information in order to complete a purchase. Clearly, a payment mechanism cannot deal with these “out of band” information leaks. Therefore in our context “perfect privacy” means that the payment mechanism itself hides all consumer-specific information.

Perfect privacy, frequently also referred to as “user anonymity” can be achieved in many ways. Anonymity may be established at the time of acquisition of some type of bearer instrument, similar to the way physical cash provide anonymity. Or, anonymity may be established at the time of payment, with the use of cryptographic techniques; in this case, the consumer can “convince” a merchant that the payment information supplied is correct, without revealing any information that could link this payment to the acquisition process, and therefore her/his identity. These types of techniques are called “zero-knowledge proofs”. From a cryptographic perspective, these were the initial schemes (based on off-line coins) and they were based on “blind signature techniques” which is more efficient than generic zero-knowledge proofs. The notion was put forth by Chaum [C82] and was investigated in the initial papers in the cryptographic literature [CFN88,OO89,OO91,FY93,B93,F93,O95].

**Schemes with Revokable Privacy.** Privacy, no matter how desirable, may cause problems in the regulatory and legal levels. In particular since a bearer instrument is, by definition, valid for payments in an open environment, there exists the potential for money laundering, buying illegal goods, blackmailing, and other attacks [vSN92]. To prevent against these, some anonymous systems allow an administrative party or a collection of parties to revoke the consumer's anonymity under certain circumstances, such as a court order. Such revocation is usually made possible by forcing the consumer to encrypt their private information under the key(s) of the administrative authority(ies). When revocation is ordered, the encrypted data are given to the authority(ies) which can then decrypt to obtain the consumer's identity. An alternative to revocation which has been recently proposed, is public auditing file of coins and access to revoke coins within this context.

**Schemes without Privacy or with limited Privacy mechanisms.** There are also systems which do not employ anonymity, usually in the interest of simplicity. Despite the obvious consumer advantage of the availability of personalized dispute mechanism, complete lack of anonymity usually limits consumer appeal.

Thus, some systems employ a mid-way for privacy. Usually this is performed by the entity issuing the bearer instrument (the "bank") possessing the consumer's private information, but preventing disclosure to third parties, including merchants. Some of these types of schemes are frequently confused with "perfect privacy" schemes, but the fact remains that the bank can still perform data mining on users' personal information; furthermore, the bank *is* the most likely party to perform such mining anyway, since it possesses the largest database of customer data.

## 4.2 Size of Payment

In principle a payment mechanism should be able to handle arbitrary size payments. However, there are technical as well as regulatory reasons which prevent a single scheme from covering all possible payment types.

**Schemes for Large and Medium Payments.** Generally when a large single payment is involved there exist regulatory requirements to record the payment amounts, or potentially to allow dispute of payments. But even in the absence of regulation, consumers are unlikely to use a payment mechanism for large or medium value payments if they cannot (a) easily obtain transaction records and dispute payments, (b) be assured that the security of the mechanism is adequate to protect the transmitted funds. On the other hand, processing costs, as well as time to complete a purchase are of lesser importance, since large payments are conducted with relatively small frequency from the consumer's side. Also, anonymity is of lesser importance, since a payment trail is usually desirable by the (lawful) consumers to allow for transaction records and potential disputes.

**Schemes for Small Payments.** In contrast to the requirements for large payments, the priorities for schemes that can be used with small payment denominations are (a) efficiency, (b) anonymity, and (c) simplicity. Accountability, recording of transactions and dispute resolution are of lesser importance –except for when payments are aggregated to larger amounts, but this can be seen as a form of a large payment and treated accordingly. To this effect, a special category of schemes has been developed, traditionally called “micropayments” since they allow payments as low as cents or fractions of cents. It is important to note that the micropayment computational cost cannot be too large and resource consuming (which will increase their cost and will defeat their purpose). Thus, technology like blind signature which could have provided anonymity for small payments is not useful due to its computational cost.

### 4.3 Use of Randomness (Probabilistic Schemes)

In the majority of cases, payment mechanisms employ deterministic techniques during the payment verification process. This type of assurances are traditional in the banking industry. However, there are systems which can obtain (computational and otherwise) efficiency advantages by performing some payment-related functions in a probabilistic way, thus spreading the effective “cost” of an operation throughout multiple transactions and consequently achieving higher overall efficiency.

Here we describe systems in which consumers pay according to a probabilistic model, either honor-based (you have to pay each time, and if you are caught not paying in a random “check” you are charged a multiple of the purchase price) or lottery based (you only pay infrequently, but you pay multiple times the purchase amount). Some examples of such schemes are:

- **Probabilistic Polling.** The idea behind probabilistic polling construction is to integrate a probabilistic function defining the frequency for sending payment to the bank. These schemes propose a probabilistic deposit at the time of the transaction, correlating the risk of overspending to the frequency of on-line verification of payments. Drawbacks of the method are the need for on-line verification of users solvability and black-listing (which requires to maintain black-list and keep informed vendors of any new revoked user).
- **Probabilistic Auditing.** In this setting, a hardware-based deterministic scheme is combined with a probabilistic auditing of spending records (to detect overspending).
- **Probabilistic Paying.** The idea is to let users send bids and pick randomly a transaction as a “contract” (or several transactions depending on the scheme setting) that is (are) declared as payments. The user committed to the contract must finalize the transaction and actually pay the merchant.

### 4.4 Implementation

**Hardware based Schemes.** Many schemes rely to some extent on hardware implementations and assumptions. These schemes are of two major types:

- **Security relies on hardware.** Some schemes, such as [Mon], derive their security entirely from the hardware used. In [Mon], users carry hardware, and in the hardware a state corresponding to the balance is kept. When a transaction is performed, this balance is altered correspondingly. Clearly, such a scheme would not be a good idea if implemented in software, as it would allow users to either increase their balance by increasing the counter, or even simpler, by “rewinding” to a previous state after a payment is performed. In schemes like the above a probabilistic approach can be employed to limit the cost of the check, by only performing on-line verification for a certain fraction of the transactions, as discussed above.
- **Security improved by hardware.** In other schemes, such as off-line coin-based schemes, the hardware is used to prevent overspending. Even though these schemes have mechanisms in place to detect and trace overspending, and some schemes allow the bank to block other coins issued to the fraudulent user, the use of hardware can reduce the amount of litigation, blacklisting, and complicated cases involving more than one country.

**Software-only schemes.** There are many proposed schemes that do not rely on hardware. Two different categories can easily be distinguished:

- **Fraud is impossible.** In on-line schemes, the bank or a clearing agency gets involved in every transaction, and verifies that funds are available. Therefore, preventing users from overspending funds they are not entitled to. The bank can verify that a user is entitled to spend an amount either by verifying that he has a coin (or similar) bearing a valid signature, and also verifying that this coin has not been previously spent. Alternatively, the transaction may be account-based, allowing users only to access funds by identifying themselves as having access to an account that the bank keeps. In the latter case, the bank determines the presence of the account, as opposed to the absence of a previously spent coin with the label in question. Both of these approaches have the drawback of the slowdown of the transaction due to the online connection with the bank, and the increased cost due to on-line availability requirements.
- **Fraud is unprofitable.** In micro-payment schemes, each unit of funds is so small that there is no significant risk of fraud, as the amount to be gained is not substantial. Also, this type of payment scheme is likely only to be used in situations where there is no clear benefit associated with a tremendous overspending (such as access to home pages, etc.). It is important to design the supporting architecture to prevent accumulation of vast amounts of small payments to be used for something of high value that can be delivered before the bank detects overspending. (This type of delay is an important but little studied tool for reducing the incentive of misbehavior.)

## 4.5 Infrastructure

**Phone based.** Specialized companies have been proposing for more than 10 years payment by phones<sup>1</sup> of your monthly bills. Bills you can pay include your utilities, telephone bills, cable TV, credit cards and even selected company accounts. The main idea is to simplify the processing of regular payments on user's side.

**Internet based.** The next wave of payment schemes integrating privacy protection, non-repudiation features and enlarging the customer base of electronic commerce is obviously based on the Internet revolution. The example of e-commerce services like amazon or eBay demonstrates the impact of Internet setting on the old trade model, enabling any customer to chose and decide knowing better and better the relative value of goods and services. Direct PC and other equipment purchasing is yet another novel business model that the Internet enables. The direct access to customers and reduction of supply chains are expected to further enhance the economic value of the Internet. Payments within this new economic arena are of prime importance.

## 5 Examples of Schemes

Will now mention a few schemes, categorize them given the above payment scheme morphology, and briefly discuss what types of situations they appear to be best suited for.

### 5.1 Credit Card Setting and On-line Schemes

- **NetBill** : This scheme [CTS95] is based on the on-line paradigm, including some nice variants such as atomicity of payments (a fault tolerance feature whereby a user pays only for transactions he receives) and anonymity by usage of pseudonyms. The drawbacks may be the number of message to process (8) for a transaction and the mandatory on-line communication with the intermediary NETBILL server. We comment that the issue of fault tolerance raised by the atomicity concern is real and important in deployed systems (see also [BBC94,CHTY96,T96,XYZZ99]).
- **NetCheque and NetCash** : This project [NM95] managed by the University of Southern California is another on-line scheme where users issue checks using a secret key (shared between a user and the bank) as a certificate of validity. A weakness may be the need of users to register at the banks, and the on-line verification of check correctness and fund availability which is required for each payment. Off-line verification is a technical possibility, but at the cost of possible frauds (non detection of bad checks). This

---

<sup>1</sup> one might notice that most of these companies propose also an extension of their service through computer-based solutions, using either Internet options or simply modem connection and dedicated software

project is an extension of NETCASH [MN94] which implemented electronic currency like the Digicash scheme but the system keeps only tracks of tokens in circulation, i.e., those issued but not already spent.

- **Digicash :** Digicash Blue Mask exists in three different versions, depending on memory size required by applications. The small version (6K ROM, 1K EEPROM and 128 RAM) does not support Fast Debit functionality due to lack of RAM space. Fast Debit is possible on medium card (3K EEPROM) but without packing option (without signature compression, scheme efficiency is drastically reduced). The large version (10 K ROM, 8K EEPROM and 256 RAM) implements the optimal Fast Debit command with compression, enabling many fast payments for transaction time around 20 ms. (We note that Digicash as a company is not any more in operation.)

## 5.2 Probabilistic Payment Schemes

- **Polling Schemes.** Gabber and Silberschatz [GS96] and then Jarecki and Odlyzko [JO97], proposed schemes where:

1. users register by giving a first payment, which is a signed note including a bank certificate;
2. subsequent payments sent by users (depending on the underlying payment scheme) are received by the vendor and probabilistically sent to the bank for deposit at the time of the transaction.

The overspending risk can be limited to a known value by defining the probabilistic checking as a function of the transaction size (making large payments more likely to be checked.)

- **Yacobi’s Auditing Scheme.** In [Yac97] a hardware-based deterministic scheme with a probabilistic auditing of spending records (to detect overspending) is proposed. This project at Microsoft Research includes the following features:

- smart-card id-based wallet (tamper-resistant device)
- e-coins signed by the bank and stored in the smart-card
- duplication (double-spending prevention) controlled by probabilistic checking in the device

- **Rivest’s Lottery.** In this lottery based scheme [Riv97a], the idea is to use a chain of values as a book of lottery tickets. The user pays with the next value (or pre-image) in the book (as will be described in the coupon section 5.5) but with the twist that the bank later announces one of the tickets as a winning ticket. If the user spent the corresponding ticket, then he is responsible for paying the vendor with the ticket value. The lottery must be held after the book (of the day, of the week) is not in use anymore to prevent cheating users from trying to never spend a winning ticket.

In a variation of the scheme in [Riv97b], the decision to perform a payment is done by both the payer and merchant who execute a standard coin-flipping protocol (merchant commits a random number, payer sends a guess and vendor de-commits) to decide jointly if the user should pay or not.

### 5.3 Hardware-based schemes

- **Small Value Payments** : Stern and Vaudenay’s scheme SVP [SV97] proposed to deliver to each vendor a smart-card containing a MAC master key. Users buy tokens certified by the bank using the private-key MAC scheme; they perform a payment by sending a token to the vendor’s device which checks the certificate in order to validate the transaction. The idea is that only the bank knows the secret key while any vendor can verify properly the tag authenticity. The main security issue is related of the master key storage on each individual card since breaking a card is equivalent to getting the scheme’s master key.
- **Micro-Mint** : Rivest and Shamir proposed to run (using huge off-line computation) schemes which find collisions of (properly tuned) hard to find collisions of (somewhat hard to find) collision free hash-functions to be used instead of signatures. This setting guarantees that forging e-coins is hard (the demonstration is based on classical birthday-paradox arguments: if the output of  $h$  is  $\log n$  bits, then finding a collision require to perform approximately  $\sqrt{n}$  hashings) but not replication.
- **Hybrid Schemes** : The advantage of having a unified scheme which works in software and hardware (assuming card reader in the PC) is advocated in [BGJY98].

### 5.4 Phone based Payment

TelPay [Tel], for instance, enables you to pay most of your regular monthly bills using either your telephone or your computer 24 hours per day, 7 days per week. Bills you can pay include your utilities, telephone bills, cable TV, credit cards, charge cards (The Bay, Eaton’s, Esso, etc.) and many other accounts. Using the system requires to complete a registration form that enables TelPay to store user information and provide users with registration number associated to a personal identification number (PIN). Users can send additional details regarding bills already registered or add more bills after set up phase.

### 5.5 Coupon-based Schemes

- **Lamport-signature based schemes** : Various schemes rely on an idea from Lamport: Rivest and Shamir’s PAYWORD, Anderson’s et al. NETCARD [AMS96], Pedersen’s Scheme [Ped95], Jutla and Yung’s PAYTREE [JY96b] and Hauser’s et al. MICRO-IKP [HSW96]. The idea is the following : take a one-way permutation  $f$  (or a hash function), pick a random input  $x$  and iterates  $f$  a large number  $n$  of times to produce  $y = f^n(x) = f(f..(f(x)))$  and authenticate  $y$  with a public-key signature scheme. The chain of values  $y, f^{-1}(x), f^{-1}(f^{-1}(x)), \dots x$  has the property that given any element of the chain, it is hard to compute the pre-image (due to the one-wayness property) but easy to verify that this chain leads to  $y$ , authenticated by the bank. The general construction of a payment scheme based on this idea is to deliver

to users triples of the form  $(x, y, \text{sign}(y))$ ; when users want to pay, they spend an inverse as a micro-payment unit. Jutla and Yung generalized the chain idea to trees. The drawback is again the double-spending attack; prevention against this attack is to check on-line (which is expensive) or to blacklist malevolent users (but user's identity must be properly built so that forge/change identity is hard to do).

- **QC Technology** : N-count solution is based on the chain value idea. The card contains a key index  $k$  and the terminal a N-counter denoted  $x_n$ . The payment protocol looks like this :

1. Card sends the key index  $k$  to the Terminal
2. Terminal replies with the following data:
  - chain parameters  $(N, TID, CID, u)$
  - amount to be paid  $m$
  - current counter value  $(x_n)$
3. Card computes  $x_0 = G(S_k, TID, CID, N, u)$  and  $x_1, x_2, \dots, x_{n-m}$  where  $x_i = F^i(x_n)$
4. Card computes  $x_{n-m}$  and decreases balance by value  $m * u$
5. Terminal checks if  $F^m(x_{n-m}) = x_n$

$S_k$  is a secret key,  $F$  and  $G$  two one-way functions (typically SHA or MD5). The length of the chain depends on the road pricing configuration. A two beacon setting gives enough time to prepare the transaction, time requirement being less critical. On the contrary, in a one beacon situation, the total transaction must be processed in less than 20 ms. In this case, the chain is minimal (length 1) and the empty N-counter at terminal is  $x_1 = F(x_0)$ . The card will simply compute and send  $x_0$ .

- **MilliCent** : Digital's scheme MILICENT [GMA<sup>+</sup>95] is a private-key solution where brokers, connected to a certain subset of vendors, are in charge of selling e-coins related to a vendor. These vendor-specific coins can only be authenticated by the vendor, using his private key. The brokers must be trusted and have agreements with vendors (certification).

## 5.6 Schemes with revocability

The anonymity coming with the unrestricted usage of blind signature mechanisms could lead to attacks from large-scale criminal organizations. In order to reduce such risks and improve control and reliability of anonymous payment schemes, the concept of revocable privacy was introduced. In such a setting, privacy can be removed to identify malevolent users or trace improperly withdrawn coins. Escrowed cash scheme introduced in [vSN92] as schemes based on the fair blind signature primitive [CPS95] give a good flavor of the concept but required the Trustees to get involved during withdrawals (also [BGK95]), decreasing drastically overall performance of the scheme. Recent works introduced the first revocable off-line (w.r.t to the Trustees) schemes, based on publicly verifiable secret sharing techniques [CMS96, Sta96] or on indirect discourse proofs [FTY96].

An interesting model from Jakobsson and Yung [JY96a] introduced the notion of Ombudsman (a government official in charge of the customers defense

against abuses) yielding an efficient electronic money system where tracing does not only depend on the bank but requires the combined endeavors of the bank and the Ombudsman in the tracing process. Furthermore, the paper introduced new type of attacks, including bank robbery attack corresponding to an adversary able to access to secret pieces of information, and ways of protecting users and issuers against these.

Several implementations such as [CPS96] based on the fair blind signature primitive or [M'R96], sub-contracting the blinding to a trustee and using an Identity-based piece of information to achieve provable privacy and security, were performed on smart-cards, proving the practical validity of such concepts.

is or where descriptive names,

## 6 Future Directions

In this section, we will briefly treat some potential scenarios, and discuss what potential implications they may have on e-commerce. By the nature of the discussion, it is impossible to be exhaustive in this exposé, and we focus only on a few potential events, and do not consider the implication of combinations of these.

### 6.1 Legal Restrictions on “Financial Cryptography”

In the light of the current debate, it is not unlikely that some countries will impose restrictions on the type of cryptography used by their citizens. Currently such limitation are on bulk encryption from national security perspective. However, this may change with the likely growth of e-commerce in terms of its impact on local economies. In this case, the flow of money becomes as important to control as the flow of information. Therefore, even if payment schemes not easily abused for use for secret communication are put in place, local governments are likely to want to control the flow of services and funds, much in the sense of what customs does for its physical counterpart. This desire may further limit what kinds of payment schemes are employed, and may, for example, force privacy to become more of a legislative measure than a technical measure. Alternatively, it may create markets for local payment schemes (for which users enjoy privacy, but taxes are automatically charged by the local government as a part of any transaction), and global schemes mainly employed for exchange of currencies between local schemes. These, in turn, would work as the interfaces between different legislative and tax domains, and would have taxation as a main objective. In such a situation, “black market” exchange of funds may become a problem much resembling what piracy is today, and would have to be battled with a combination of legislative and technical measures.

Another limitation may prevent ore restrict certain types of cryptographic tools to be employed, such as public key cryptography, either globally or in particular countries. This in itself may cause different schemes to be employed, as will local requirements on the functionality of the schemes (something we can

already witness today with the divide between European cash cards and U.S. credit cards.) Additionally, and as we will discuss in the next section, a multitude of different schemes may evolve and be employed in the same market.

## **6.2 Many Parallel Standards**

Payment schemes today give the impression of being on the way of becoming a niche market in which we have a few leaders for common types of payments, and special schemes used only in particular situations. There are many reasons, ranging from corporate interests to varying requirements on payment schemes based on their usage, that such a variety of schemes may be deployed, either symbiotically or in competition with each other. One example of the symbiotic use was given in the previous section; others could arise to give users better functionality, and to cover a variety of situations. For example, fast and low-overhead schemes are useful for situations like paying for daily commuting tolls, while frequent-flier programs and the like require no speed of transactions, and may put restrictions on how funds are transferred and used (or taxed when doing so.) Still, incorporating schemes to allow for a consolidated presentation to the user, and allowing for (potentially automatic) transfer possibilities give rise to a much more versatile construction. Whereas much of the problem remaining to be solved is that of building an appropriate infrastructure, it is also important to implement mechanisms for monitoring (by law enforcement, customs, arbiters, and others.) It is interesting to notice the tradeoff between monitoring and privacy here, giving rise to a much more severe potential privacy intrusion than what has previously been considered.

## **6.3 Advances in Cryptanalysis**

Advances in cryptanalysis has the same potential to change the payment scene by limiting what types of operations as legislation does, and may limit the use of certain schemes or types of schemes. It is noteworthy to point out that a vast majority of payment schemes discussed in the cryptographic community are based on public key cryptography. In the perhaps unlikely event that public key cryptography ceases to exist (e.g., by the development of inexpensive quantum computers, and a lack of public key algorithms to withstand the related attacks) a new approach has to be taken in many situations. This, along with concerns of legal restrictions, calls for careful studies on how to implement desirable payment schemes relying plainly on secret key cryptography, or on other methods to ensure correctness of payments.

## **6.4 Social and Technical Changes**

Clearly, social changes can be expected to have a major impact on the field. For example, if PDA's become as common as credit cards are, it this drastically simplifies the building of a new infrastructure for payments. Similarly, technical

changes, such as a substantial increase of the available communication bandwidth (and the price for it) may affect what types of schemes are employed. As an example, it makes little sense to implement off-line payment schemes if the cost for communication drastically falls, given the higher costs and complexity of such schemes. There is a trend towards both of these changes. However, at the same time as such changes simplify the employment of payment schemes, they also increase the security concerns, as should be evident in the light of viruses. So far, these have not started to surface on PDA's, but that is likely to only be a matter of time; likewise, due to the lack of electronic payment schemes in common use, they have also not started to target the wallets of users. This, too, may simply be a question of time. From a technical point of view, that should prompt more secure operating systems to be constructed for these devices, and of recovery mechanisms for payment schemes. These may be based on automatic arbitration, supported by tracing mechanisms and detection mechanisms controlling "unusual" flow patterns. The latter, in turn, forces categorization, which may be questionable in terms of privacy concerns if not performed by the user himself, or made non-interpretable to a third party looking for differences in behavior.

### **6.5 Technology and the Business/Politics issues**

In order to appeal to mainstream customers, have large merchant base, and get many involved in the payment systems, technology and other business and political factors have to be reconciled. While the richness of available schemes is justified technically (and has to be pursued by scientists), the mainstream solution has to account for many concerns. The integration of the solutions, especially the global large scale one requires a lot of understanding of the regulatory, financial, social and other aspects of the user base (clients, merchants, financial institute (old and new) and governments and global markets).

Integrating payment technology with other technologies (fault tolerance, distributed systems, Internet interfaces/API's, other e-commerce infrastructure, etc.) is still challenging since cryptography is merely a component of the entire system. Some open issues are in [W98].

Large scale studies of comprehensive technological solution has not been done yet. The issue of economic stability assurances that new currencies should maintain (technically and otherwise) is an important issue. The development of stable and well recognized business models will help in integrating payment schemes into them. The issue of education of the user base and the integration of payments as an infrastructure component with emerging e-commerce applications is an interesting challenge.

## **7 Conclusion**

We have presented some of the past issues with the technology of electronic payments. This area is challenging and promising. We believe that the need

for it is inherent, though the difficulties in achieving it are extensive and interrelated to many more general e-commerce and secure infrastructure issues. We have surveyed some prototypical examples from the past and the present. We categorize the technical solutions. We further related the technology to many non-technological constraints and discussed possible future needs, directions and possibilities. While we could not have possibly cover all areas and systems in this very prolific field, we hope we have presented the basic technological developments (with omissions, of course). We think that we have pointed to various interesting and challenging issues for further activities. These activities are needed in numerous areas: research, business development, technical research and development, social, legal and political studies and other interdisciplinary issues related to e-commerce and payment mechanisms.

## References

- [AMS96] R. Anderson, C. Manifavas, and C. Sutherland. Netcard - a practical electronic cash system. In *Fourth Cambridge Workshop on Security Protocols*. Springer-Verlag, 1996. Available at <http://www.cl.cam.ac.uk/users/rja14>.
- [B93] S. Brands, Untraceable Off-Line Cash in Wallets with Observers, Crypto'93
- [BBC94] J. Boly, A. Bosselaers, R. Cramer et al., The ESPRIT Project CAFE: High Security Digital Payment Systems, ESORICS'94
- [BGJY98] M. Bellare, J. Garay, C. Jutla, and M. Yung, *VarietyCash: A Multi-Purpose Electronic Payment System* (Extended Abstract), Usenix Workshop on Electronic Commerce'98
- [BGK95] E. F. Brickell, P. Gemmel, and D. Kravitz, Trustee-Based Tracing Extensions to Anonymous Cash and the Making of Anonymous Change, SODA'95
- [BP89] H. Burk and A. Pfitzmann, Digital Payment Systems Enabling Security and Unobserability, *Computer & Security*, 8/5, 1989, 399-416
- [C82] D. Chaum, Blind Signatures for Untraceable Payments, Crypto'82
- [CFN88] D. Chaum, A. Fiat, and M. Naor, Untraceable Electronic Cash, Crypto'88
- [CFT98] A. Chan, Y. Frankel, and Y. Tsiounis, Easy Come-Easy Go Divisible Cash, Eurocrypt'98
- [CHTY96] J. Camp, M. Harkavy, J. D. Tygar, and B. Yee, Anonymous Atomic Transactions, 2nd Usenix on Electronic Commerce, 1996
- [CMS96] J. Camenisch, U. Maurer, and M. Stadler. Digital Payment Systems with Passive Anonymity-Revoking Trustees. In *ESORICS '96*, LNCS 1146. Springer-Verlag, 1996.
- [CPS95] J. Camenisch, J.-M. Piveteau, and M. Stadler. Fair Blind Signatures. In *Eurocrypt '95*, LNCS 921, pages 209–219. Springer-Verlag, 1995.
- [CPS96] J. Camenisch, J.-M. Piveteau, and M. Stadler. An Efficient Fair Payment System. In *Proc. of the 3rd CCCS*, pages 88–94. ACM press, 1996.
- [CTS95] B. Cox, D. Tygar, and M. Sirbu. Netbill security and transactions protocol. In *First USENIX Workshop on Electronic Commerce*, 1995. Available at <http://www.ini.cmu.NETBILL/home.html>.
- [DFTY97] G. Davida, Y. Frankel, Y. Tsiounis, and M. Yung, Anonymity Control in e-cash. In the 1-st Financial Cryptography, LNCS 1318 Springer.

- [dST98] A. de Solages and J. Traore, An Efficient Fair off-line electronic cash with extensions to checks and wallets with observers, In the 2-d Financial Cryptography.
- [F93] N. Ferguson, Extensions of Single-Term Coins, Crypto'93
- [FTY96] Y. Frankel, Y. Tsiounis, and M. Yung, Indirect Discourse Proofs: Achieving Fair Off-Line E-Cash, Asiacypt'96.
- [FTY96] Y. Frankel, Y. Tsiounis, and M. Yung. Indirect Discourse Proof: Achieving Efficient Fair Off-Line E-Cash. In *Asiacypt '96*, LNCS 1163, pages 286–300. Springer-Verlag, 1996.
- [FY93] M.K. Franklin and M. Yung, Secure and Efficient Off-line Digital Money, ICALP'93 LNCS 700, Springer Verlag. 1993.
- [GMA<sup>+</sup>95] S. Glassman, M. Manasse, M. Abadai, P. Gauthier, and P. Sobalvarro. The Milicent Protocol for Inexpensive Electronic Commerce. In *Fourth International World Wide Web Conference*, 1995. Available at <http://www.research.digital.com/SRC/milicent>.
- [GS96] E. Gabber and A. Silberschatz. Agora: A Minimal Distributed Protocol for Electronic Commerce. In *USENIX Workshop on Electronic Commerce*, 1996.
- [HSW96] R. Hauser, M. Steiner, and M. Waidner. Micro-Payments based on IKP. In *Worldwide Congress on Computer and Communications Security Protocol*, 1996. Available at <http://www.zurich.ibm.com/Technology/Security/publications/1996/HSW96-new.ps.gz>.
- [J95] M. Jakobsson, Ripping Coins for a Fair Exchange, Eurocrypt'95
- [JM98] M. Jakobsson and D. M'Raihi, Mix-based Electronic Payments, Workshop on Selected Areas in Cryptography, 1998
- [JY96a] M. Jakobsson and M. Yung. Revokable and Versatile Electronic Money. In *Proc. of the 3rd CCCS*, pages 76–87. ACM press, 1996.
- [JO97] S. Jarecki and A. Odlyzko. An Efficient Micropayment Scheme based on Probabilistic Polling. In *Financial Cryptography '97*, LNCS 1318. Springer-Verlag, 1997.
- [JY96b] C. S. Jutla and M. Yung. PayTree: “Amortized-Signature” for Flexible MicroPayments. In *Second USENIX Workshop on Electronic Commerce*, 1996.
- [MN94] G. Medvinsky and C. Neuman. Netcash: A Design for Ppractical Electronic Currency on the Internet. In *Second ACM Conference on Computer and Communication Security*, 1994.
- [Mon] Mondex. <http://www.mondex.com>.
- [M'R96] D. M'Raihi. Cost-Effective Payment Schemes with Privacy Regulation. In *Asiacypt '96*, LNCS 1163, pages 266–275. Springer-Verlag, 1996.
- [NM95] C. Neuman and G. Medvinsky. Requirements for Network Payment: The Netcheque Prospective. In *IEEE COMCON*, 1995. Available at <ftp://prospero.isi.edu/pub/papers/security/>.
- [O95] T. Okamoto, An Efficient Divisible Electronic Cash Scheme, Crypto'95
- [OO89] T. Okamoto and K. Ohta, Disposable Zero-Knowledge Authentication and Their Applications to Untraceable Electronic Cash, Crypto'89
- [OO91] T. Okamoto and K. Ohta, Universal Electronic Cash, Crypto'91
- [Ped95] T. Pedersen. Electronic Payments of Small Amounts. Technical report, Aarhus University, Computer Science Department, 1995. DAIMI PB-495.
- [Riv97a] R. Rivest. Electronic Lottery Tickets as Micro-Cash. In *Financial Cryptography '97*, LNCS 1318. Springer-Verlag, 1997.

- [Riv97b] R. Rivest. Lottery Tickets as Micro-Cash, 1997. Financial Cryptography '97 Rump Session.
- [Sta96] M. Stadler. Publicly verifiable secret sharing. In *Eurocrypt '96*, LNCS 1070, pages 190–199. Springer-Verlag, 1996.
- [SPC95] M. Stadler, J. M. Piveteau, and J. Canmenisch, Fair Blind Signature, Eurocrypt'95
- [SV97] J. Stern and S. Vaudenay. Small-value payment: a flexible micropayment scheme. In *Financial Cryptography '97*, LNCS 1318. Springer-Verlag, 1997.
- [T96] J. D. Tygar, Atomicity in Electronic Commerce, ACM Symposium on Principles of Distributed Computing, 1996
- [Tel] TelPay. <http://www.telpay.ca>.
- [vSN92] S. von Solms and D. Naccache. On Blind Signatures and Perfect Crimes. *Computers & Security*, 11:581–583, 1992.
- [W98] M. Waidner, Open Issues in Secure Electronic Commerce, 1998
- [XYZZ99] S. Xu, M. Yung, G. Zhang and H. Zhu, Money Conservation via Atomicity in Fair Off-Line E-Cash. In *ISW'99*. Kuala Lumpur, Malaysia, Springer-Verlag, 1999.
- [Yac97] Y. Yacobi. On the continuum between on-line and off-line e-cash systems. In *Financial Cryptography '97*. Springer-Verlag, 1997.