On Digital Money and Card Technologies

Edwin M. Knorr*
Department of Computer Science
University of British Columbia
Vancouver, B.C., V6T 1Z4, Canada

January 20, 1997

Abstract

We survey two related fields: digital money and card technologies (especially smart cards), for possible PhD research topics. We believe that digital money and card technologies will revolutionize life in the 21st century. It will be shown that privacy issues are of serious concern, but that well-designed implementations can have long-term strategic and economic benefits to society. We have been following these two fields for a number of years. It is only very recently that digital money and card technologies have captured the attention of the North American marketplace. We believe that there will be significant research opportunities in these areas for years to come, as evidenced by recent commercial interest in supporting financial transactions via the Internet. This paper examines various aspects of digital money and card technologies, and attempts to provide a comprehensive overview of these fields and their research prospects.

Keywords: digital money, smart cards, Internet commerce, data mining, biometrics, cryptography, HCI, ubiquitous computing, privacy

1 Introduction

Due to recent trends in society and computer technology, we are entering a paradigm shift that will undoubtedly revolutionize the way individuals, corporations, and governments view finance and security. We stand at the crossroads of two worlds: a cash-oriented society, and a cashless society. We believe that it is somewhat academic as to which of the two choices society will embrace in the long run—namely, the cashless one. There are many choices to be made *en route* to a cashless society, and there are many open areas of research. This paper does not attempt to define a specific PhD topic, but rather provides a survey of recent literature and identifies active (or potential) areas of research. It will be

*E-mail address: knorr@cs.ubc.ca and World Wide Web address: http://www.cs.ubc.ca/spider/knorr

shown that card technologies and digital money are inherently linked, and that there are many challenges and opportunities ahead.

1.1 Definitions

This section defines terminology that will be used throughout this paper. Liberal use of examples will help clarify some of the topics addressed by this paper.

Card Technologies This generic term describes integrated circuits and/or storage media that are embedded in plastic cards (typically of credit card size). Card technologies include related hardware, software, and protocols to support applications involving smart cards, optical cards, magnetic stripe cards, bar-code cards, and radio frequency ID (RFID) cards. Some card manufacturers mix properties of these cards, yielding hybrids [20], such as the U.S. government's MARC card [31].

Digital Money Digital money is sometimes called digital cash, electronic cash, or electronic money. A unit of digital money is simply a string of bits representing "real" money that can be used as an electronic medium of exchange [45]. Digital money can serve as a replacement for coins, paper money, cheques, credit cards, debit cards, and many other financial instruments.

Magnetic Stripe Card A narrow magnetic stripe appears on the back of many credit cards, bank cards, security cards, etc. The stripe can hold a small amount of information; however, its storage capacity and the capability for tampering make it unsuitable for secure use [33, 49].

Optical Card An optical memory card is a very durable card that uses WORM (write-once, read-many) technology to hold several megabytes of data, and provides a non-erasable audit trail of information [9, 24].

RFID Cards Radio frequency ID cards [16, 34] are used for contactless transactions. They are often attached to items in retail establishments to help prevent theft. Other uses for RFID technology include the identification and tracking of cargo (e.g., pallets of military supplies); the identification and monitoring of trucks along freeways; fast, automated collection of toll fees from motor vehicle operators (e.g., while a vehicle is travelling at 100 km/h through a toll booth); ubiquitous computing [84, 85]; and, the identification of animals through the use of implantable chips [18].

Smart Card A smart card is a credit card sized plastic card, having a special type of integrated circuit (IC) embedded in it, with visible contacts (in the left hand side of the front of the card) [30]. Including the contacts, a typical smart card IC occupies approximately 25 mm^2 of card real estate.[1] Although memory-only IC cards (e.g., telephone cards) have historically been called "smart" cards, the current trend is to define smart cards as those cards which actually contain microprocessors, RAM, and ROM. Additionally, they may contain EEPROM as well as cryptographic algorithms, operating systems, and facilities for data management. Properties such as cryptographic algorithms, transmission protocols, and physical characteristics of smart cards and related hardware, conform to ISO, ANSI, and CEN standards [74].

1.2 Motivation

Digital money is likely to become a multi-billion—if not multi-trillion—dollar industry in the not-too-distant future. Although smart cards have been popular in Europe for years, they have only recently been introduced to the North American marketplace. As will be shown throughout this paper, there is a direct link between card technologies and digital money. These two areas are attractive because they are capable of solving problems associated with the following motivations and observations:

- It is time-consuming, expensive, and even dangerous to transport, store, handle, insure, and count cash.
- Much crime is directly or indirectly related to cash. This includes theft, robbery, fraud, counterfeiting, etc. For example, society is faced with huge losses due to fraud in social benefits programs (e.g., welfare and unemployment insurance), the underground economy, lost taxation, etc. Furthermore, laser printers, scanning devices, and colour photocopiers can easily reproduce cheques, securities, important documents, gift certificates, etc. Signatures can even be taken from one document, and placed on another. Sections 2.2 and 2.4 show how digital money can significantly reduce these types of crimes.
- Service-oriented transactions can be particularly annoying for the parties involved. For example, it may cost \$10 or more to simply process a claim for a medical appointment. Then, it may take months before the doctor receives payment from the relevant agencies or insurers. The amount of error-prone paperwork can be substantial, especially if signatures, receipts, cross-references, and requests for more documentation are involved. Electronic clearance should provide rapid turnaround time, perhaps overnight. For example, on-line edit checks can be performed, files and messages

[1] The most interesting part of a smart card is the integrated circuit. The plastic card itself is merely a handy and acceptable way of carrying the chip.

can be verified using digital signatures,[2] transaction records can be maintained, and databases can be linked to facilitate or eliminate the complicated accounting and tax reporting procedures that many individuals and organizations face.

- Smart cards facilitate the secure transport, update, and retrieval of medical information. An excellent example of the benefits achieved through smart cards in a medical role is that of dialysis treatment for kidney patients in France [30]. Prior to the implementation of smart cards as a portable database for this medical application, dialysis patients could not leave their hometowns for more than about two days.

- Due to the growth of the Internet and the World Wide Web, there is a tremendous incentive to provide for Internet commerce. See Section 1.4 for more details.

- Tremendous financial opportunities exist for reduced commissions or transaction costs associated with foreign exchange, stock market trades, etc. For example, if stock market trading were fully automated, efficiencies could be realized. Individuals buying \$5000 worth of stock might only pay a \$5 transaction fee instead of about \$200 at a full-service broker (or perhaps \$50 at a discount broker)[3]. This would open up many domestic and international opportunities which, in conjunction with integrated software packages and full and immediate access to non-confidential corporate information, would finally meet the *efficient markets hypothesis*, that is, that stock prices fully reflect all publicly available information at any given time [82].

- Security is becoming increasingly important in society. This naturally gives rise to the need for reliable, efficient cryptographic algorithms (see Section 2.4). We need to be able to provide identification in on-line systems such as bank machines and computer networks (especially distributed systems that have certain "trusted" components), electronic voting, access control (e.g., unmanned checkpoints such as doors in an office complex), etc. Currently, such facilities allow access using a token (e.g., card, key, password); however, it is vital that the *holder* of the token be the *owner* of the token—mere possession is unsatisfactory for many applications. Furthermore, digital signatures and pseudonyms are essential for carrying out confidential, untraceable, and irrefutable transactions. The notion of allowing an individual to maintain

[2]Digital signatures are well studied in cryptography [63]. A digitally signed message has the property of non-repudiation, that is, an individual cannot deny that he sent certain data, when in fact he did send the data. Digital money is possible because of digital signatures. Signature-creating smart cards use a dedicated co-processor to generate large, random numbers to provide strong security [45].

[3]In March, 1996, Charles Schwab, a major U.S. discount brokerage became the first major investment house to use a real-time trading system on the Internet (using the World Wide Web). A new upstart, E-Trade Group, began its Internet brokerage service during the previous month. *The Financial Post* reports that E-Trade charges only \$14.95 to trade 1000 shares of stock at \$21 per share; Schwab (on-line) charges \$39; and Merrill Lynch & Co., the largest U.S. brokerage, charges \$384 using a full-service broker [66].

digital pseudonyms for different vendors is important for private transactions [45]. For example, one pseudonym might be with a bank, another might be with a stockbroker, and so on. The idea is that a bank cannot link customer information with a stockbroker unless, of course, the customer provides authorization.

One might argue that existing electronic means to process transactions are sufficient to handle society's financial demands. This is not true. Many transactions currently cannot be handled electronically (e.g., small amounts of money for a bus, pay phone, parking meter, vending machine, laundry machine, person-to-person cash transfers, or simply cash transactions at retail establishments). Some of these transactions are becoming problematic because many individuals simply do not carry the large number of coins required for certain transactions. Inflation further complicates the situation. Although Canadians averaged more than 2 credit cards each in 1990, the reality is that cash still represented 89% of the number of financial transactions [8]. In 1993, the amount of money in circulation in the United States was estimated to be between $1200 and $1300 for each man, woman, and child [23]. In fact, it is estimated that 2-5% of the GNP of some countries is consumed by the movement of cash [79].

The costs and profits associated with processing financial transactions are significant. A 1990 estimate of the retailer's cost of handling a cash transaction was about 48 cents, and for a credit card it was about 97 cents [69]. In March, 1991, the commissions on Visa and MasterCard transactions averaged 1-2% of the sale, and American Express transactions averaged 3-5% [26]. In 1993, Automated Teller Machines (ATM's or "bank machines") handled transactions at an overall cost of about 27 cents per transaction (down from 40-60 cents in 1990), debit card transactions cost about 14 cents (down from 32 cents in 1990), and cheques cost about 68 cents (*up* from 50 cents in 1990) [38, 69]. In some cases, financial institutions are waiving or reducing service charges if a customer uses an ATM, PC, or telephone to perform transactions, instead of using a relatively expensive human teller. According to a recent survey by Booz-Allen & Hamilton, the overhead cost for an average Internet banking transaction is 13 cents or less, compared to $1.08 for an average full-service transaction [48]. It is clear that the level of automation in finance is growing, and society is (for the most part) responding quite favourably to financial automation.

One of the most significant catalysts towards the acceptance and implementation of card technologies is *security*. Virtually everyone has been a victim of crime (perhaps many times), either in the form of personal tragedy or loss, or simply dramatically increasing insurance premiums.[4] The reality is that people really do want enhanced security for

[4]It is a very sad commentary on society to see how some law-abiding citizens live in fear, being "caged up" in their homes (with bars on their windows and deadbolts on their doors), while criminals freely walk the streets without shame or loss of rights. A construction worker has indicated to this author that every

themselves, their families, and their possessions.

The loss or theft of a wallet or purse has consequences that far exceed the value of the lost cash. For example, a wallet or purse may contain paper money, coins, credit cards, cheques, a social security card, a driver's license, an automobile club card, a library card, a photocopier card, a video rental card, a bus pass, a voter's card, medical card(s), a dental card, a bank machine card, insurance information, a telephone calling card, a company security card, general ID, etc. If a *single* smart card could replace all of the above, many people would welcome the resulting convenience and peace of mind.[5]

Corporations and governments would welcome smart cards from a cost-benefit point of view. For example, Ontario is considering implementing a \$1B, province-wide, smart card program to integrate many government-related documents (e.g., licenses or documents for obtaining medical services, driving a car, voting, hunting, fishing, and obtaining social assistance) onto a single card [83]. This program is expected to save the province hundreds of millions of dollars each year in fraudulent claims alone. Further savings can be realized due to the reduction in paperwork, and the facilitation of document transfer. For instance, the health ministry could use the card to allow doctors to link hundreds of medical databases, thereby obtaining a patient's complete medical history in a timely fashion. It is believed that overhead costs could be reduced by perhaps as much as 30%, and that the number of deaths and injuries could be significantly reduced through the effective use of card technologies [77].

Based upon the examples presented so far, it should be clear that there are numerous motivating factors for moving towards digital money and card technologies. Here is a summary of the kinds of applications that card technologies can support:

- prepaid, closed, stored value systems for a specific application (e.g., transit, photocopying, and telephones [37, 68])

- an "electronic purse" that can be used for multiple applications. Instead of "units of value" in the form of some number of prepaid telephone calls, for example, an amount of digital money is loaded onto the card, and is properly decremented (or incremented) by each participating application, thus facilitating speed and convenience [61, 79].

new home that he has worked on has a built-in security (alarm) system. Ironically, this author recently received a baffling letter from the provincial government indicating that British Columbia has received an award for its "low" crime rate and for the tremendous "progress" that the government has made over the past few years with respect to crime control [46].

[5]Some people no longer want their addresses to appear on their driver's licences and other documents, due to stalking and other invasive crimes. In this regard, it is likely that more and more addresses will be replaced by Post Office box numbers [78]. Card technologies have the ability to encode and restrict access to such documents. Furthermore, some individuals want their cards to display "different personalities", depending on the nature of the transaction or relationship [77].

More details are provided in Section 1.3.

- Internet commerce [45]
- pay-TV [76]
- identification [18, 51]
- portable data files [58]
- security (i.e., physical and logical access to locations, machines, and networks [29]). A single smart card can be used in place of numerous keys for access to homes, businesses, automobiles, etc.[60] Smart cards can manage access privileges and support personal preferences when logging on to a local machine (e.g., while travelling overseas), in order to access files on one's "home" computer [36, 64], thus facilitating global connectivity.
- government services such as Electronic Benefits Transfer (EBT) [31, 52, 62, 72, 86]
- mass transit [67]
- telecommunications (e.g., GSM cellular) [50, 76]

1.3 Electronic Purse

The problem with prepaid "tickets" or stored value cards is that they are typically restricted to a specific application. This means that consumers may have to carry separate cards for buses, vending machines, cafeterias, etc. This does not solve the problem of carrying around multiple cards, and this approach may not necessarily be more convenient or safer.

At this point, it is useful to draw distinctions between a stored value card and an electronic purse. A stored value card is typically of some fixed denomination, and it is transferable, disposable, non-refundable, and part of a closed, prepaid system. For example, a stored value card for public telephones might contain 25 units of value, thus enabling the holder to make a total of 25 local telephone calls. The card would be decremented by one unit for each call, and there would be no need for a microprocessor on the card.[6] An electronic purse, on the other hand, is a smart card, and is issued empty of value, with the user deciding how much money to download onto the card. It is typically reloadable, personalized, and may be linked to a bank account for subsequent "downloads" of cash [79]. The card can be used to transfer a given amount of money to any application accepting the purse card—provided the required funds exist on the card.

[6] Many stored value cards have traditionally been called smart cards because of the presence of an integrated circuit on the card, but these cards are really memory-only "smart" cards.

The Mondex card [32, 79] is a good example of an electronic purse. A Mondex information leaflet [47] highlights the following features:

> "Mondex has all the core features of cash but with added convenience and security. Unlike cash, Mondex value can be loaded from the comfort of your home using a Mondex-compatible telephone. Thank of it as an ABM [Automated Banking Machine] in your home."
>
> "Purchases are made by slipping the Mondex card into a Mondex sales terminal. Transactions take approximately 3 seconds and no signature or authorization is required."

Users can even perform person-to-person (i.e., purse-to-purse) cash transfers via a small, optional hardware device called an "electronic wallet". A Mondex card keeps a record of transactions. Multiple currencies can be managed on a single card, making it suitable for international use, especially in Europe where there are many countries within a short distance of one another, and where it is very easy for members of the European Community to cross borders and transact business.

Mondex trials are ongoing in Swindon, England, where over 10,000 individuals have signed up for the pilot. Mondex's major North American pilot will begin in early 1997, in Guelph, Ontario. Bell Canada, the Canadian Imperial Bank of Commerce, and the Royal Bank of Canada are partners in the venture.

1.4 Internet Commerce

One of the most exciting aspects of digital money involves Internet commerce. Besides some of the major banks and credit card companies, the current key players in the digital money field are companies such as CyberCash, Open Market, DigiCash, First Virtual, and Mondex [32, 45].

Internet commerce is more than just paying bills over the Internet, or moving funds from one account to another. Internet commerce involves the exchange of goods or services for money using the capabilities of the Internet. Global Internet sales totalled US$500 million in 1995. KPMG predicts that this amount will balloon to $1 *trillion* by the year 2000 [48].

Consider on-line shopping by PC. Selection, ordering, and payment can take place over a PC, and goods can be delivered directly to the customer. Furthermore, sales know no geographic boundaries. This means that a small business that previously could only afford a small advertisement in the Yellow Pages or in the local newspaper can now advertise its services to the entire world. Many Internet businesses do not need to acquire expensive real estate and retail furnishings to attract customers. For example, *Amazon.com* Books claims to be "Earth's biggest bookstore" [3]. Its entire business is on-line, and its motto is: "If it's in print, it's in stock". *Amazon.com* provides discount prices, a search facility, and on-line reviews of books by customers, authors, and publishers. Unlike many bookstores, turnaround time is fast, and books are delivered directly to the customer's address. Customer response has been very positive, as evidenced by numerous on-line testimonials.

Consider also the tremendous money-making potential for selling *information* over the Internet. Perhaps a single, real-time stock quote might cost 5 cents, a delayed stock quote might cost 2 cents, and a download of hundreds of historical quotes might cost 1/10 cent each; the latest sports scores might be sold for a nickel; video might be broadcast at a few cents per minute; keyword searches in databases might be performed for a few cents; documents could be downloaded for a dollar; and so on. Users surfing the web may wish to view/download articles, pictures, etc., after agreeing to pay a small fee. The owner of the work would get a percentage of that fee, and could make a lot of money if the number of transactions is large. This offers the potential of significant profits attainable through volume sales at low cost (in conjunction with small overhead costs).

Even software could be advertised, sold, registered, distributed, and installed over a network—perhaps for only tens of dollars. Alternatively, the cost could be determined dynamically, based on the number of invocations of the executable program, assuming that chargeback facilities are in place. If the software to be licensed is a high-performance, transaction-oriented database system, then perhaps a fraction of a cent per transaction would be sufficient to reimburse the owner of the program. The small transaction fee would encourage individuals or organizations to use the services immediately, instead of having to worry about justifying the up-front cost of possibly many thousands of dollars for the acquisition and support of software. In distributed systems, some CPU or I/O bound tasks can be performed at remote sites, with appropriate chargeback systems in place.

Currently, Internet commerce deals largely with credit card style transactions, yet it makes little sense to deal with credit cards for small monetary amounts, and it certainly makes no sense to devote computational resources to encrypting and logging individual transactions that involve only a few cents, or perhaps a fraction of a cent. It would be too slow and expensive to facilitate such transfers, unless purchases were aggregated. On a larger scale, Internet commerce can process financial transactions involving thousands or millions of dollars. This is where cryptography and identification are crucial.

Henry Dreifus indicates that in the not-too-distant future, telecommunications costs will be almost zero [21]. He adds that dedicated networks over leased lines will be unsatisfactory because organizations want the ability to connect to any other organization. Routers will become increasingly sophisticated. Point of Sale (POS) devices will change, perhaps in some form of Internet-ready PC. Organizations such as Verifone and Hypercom are actively exploring such technologies. Security contines to be a "better mousetrap" game, and will continue to play a critical role in telecommunications technology. Dreifus believes that some form of convergence in network technologies is unlikely to occur. Heterogeneity will be an ongoing characteristic of telecommunications networks. All of these topics are directly related to digital money and card technologies.

We now examine some potential areas of research, some of which are already receiving considerable attention. We limit our discussion to non-hardware issues.

2 Potential Areas of Research

2.1 Data Management

Data storage is important in card applications because of the relatively small on-board storage (e.g., 32 KB for smart cards, less than 1 KB for magnetic stripe cards, but several MB for optical cards).[7] The limited storage capacity of smart cards means that algorithms, compression, security, and management of applications are critical. Different applications or "accounts" (e.g., medical information, bus "money", telephone "money", and personal identification) can reside on a single smart card. In fact, there could be hundreds of applications on the same card. Even within an Electronic Benefits Transfer application, there could be many sub-classes [62]. The implementation of a special-purpose, limited function DBMS on the card seems useful [36, 42]. Smart card operating systems have also generated research interest [42, 56].

2.2 Biometrics

Biometry is the study of mathematical or statistical properties in biology, specifically physical or behavioural characteristics. Biometrics are important to card technologies because biometrics can verify that the holder of the token (e.g., the smart card) is in fact the owner of the token. This is important for remote computer access, access control to physical sites, transaction authorization, etc. Smart cards containing biometric information (and hosts that store biometric data) are capable of providing excellent security [11, 75]. For example, Westinghouse's Hanover nuclear plant uses fingerprints and hand geometry techniques, in conjunction with smart cards, to handle security at unmanned checkpoints [17].

Here are some biometrics that have application to smart cards and digital money. Other

[7] Optical cards use WORM technology and do not contain a microprocessor, thereby limiting their functionality. Some hybrid smart cards possess optical storage. Advances in microelectronics will continue to add storage capacity (e.g., EEPROM) to smart cards.

biometrics include keystroke behaviour, DNA, retinal patterns, iris images, and even body odours [11].

Facial Recognition This form of image recognition is receiving considerable attention [28, 65, 87], and is particularly attractive in security applications because it is a "hands off" and unobtrusive approach to security. For example, in hospitals, a medical worker must frequently depart from a central work area, possibly leaving a terminal unattended. Logging off and on repeatedly is not a satisfactory solution to security. Good facial recognition systems are of value to many applications.

Fingerprints Fingerprints have long been recognized as a positive means of identification, and have found particular interest in card based security systems [57, 71]. Organizations such as Identix develop fingerprint-based access and control mechanisms to safeguard databases and networks [70].

Hand Geometry The skeletal structure of an individual's hand can be used, in conjunction with possession of a smart card, to provide a high degree of confidence that a person actually is who he claims to be [11, 39].

Vein Patterns The vein network in the back of one's hand forms a personal "bar code", sufficient to provide a degree of confidence in security applications [60].

Voice Verification Research in auditory systems has shown some promise [75], although much more work is required.

Signature Dynamics An individual's signature is sufficient to provide a fairly high degree of confidence in moderate security applications. Studies have shown that signature dynamics systems can properly authorize individuals whose signatures vary somewhat from signature to signature, but can reject forged signatures that a human might recognize as being perfectly valid [44].

The number of false positive hits and false negative hits needs to approach zero before biometric applications gain universal acceptance in digital money and card technologies. Thus, research into biometric technology will continue to receive serious interest.

2.3 Human-Computer Interaction (HCI)

It has been said that the best form of computer interface is the self-effacing one, that is, one in which an individual does not recognize the presence of a computer [85]. This leads to the notion of ubiquitous computing. The combination of a contactless smart card (or RFID card) and a facial recognition system falls into this category.

Easy-to-use interfaces lie at the heart of HCI. Much work needs to be done in this area since there can be many types of hardware devices that accept smart cards. Given the competition among vendors and the diversity of applications, it is unlikely that there will be a single standard for card technologies and digital money—at least in the foreseeable future. Consider banking machines. Regardless of the financial institution, most ATM's perform similar functions; however, the implementation of some types of transactions may vary considerably from one institution to another. Bill payments and account transfers are examples of this.[8] Some people refuse to use ATM's, or cannot use ATM's; instead, they perform their banking the old fashioned way: face-to-face with a human teller. Senior citizens, handicapped people, those needing assistance to carry out transactions, individuals who are leery of technology, and people who have had unpleasant experiences with ATM's fall into this category. We need to realize that regardless of the level of automation, there will still be a human element in financial services.

Smart cards and digital money will have a profound impact on the way individuals and companies transmit personal and financial information between one another. Human-computer interfaces will draw significant attention in these areas for many years to come. Section 2.2 dealt with biometrics and it is clear that many HCI studies need to be done before the implementation of biometric techniques becomes widespread.

2.4 Cryptography

One of the most active research areas in card technologies and digital money is cryptography [4, 6, 7, 55, 63, 73, 80]. There are three phases of authentication for transactions using smart cards: authentication of the host by the card (to prevent a bogus host from illegally obtaining or changing information), authentication of the card by the host, and authentication of the user by the card [19].

One area that promises to be a good research area is that of being able to quickly find trusted certifiers across organizational boundaries (i.e., generalized notaries) [22]. For example, in many corporations, there are one or more individuals who manage security for corporate-wide datasets. The individuals responsible for setting up accounts and passwords need to be trusted, and their integrity is crucial to data security in the organization. Suppose now that 2 organizations enter a joint venture and agree to share certain data resources. Again, we need the notion of a general certifier who is known to (and trusted by) both organizations. This problem becomes more complex as the number of organizations

[8] As a new customer of a major Canadian bank, this author became quite confused as to how to perform payments on an ATM, and on two separate occasions, he had to abort the transactions and appeal to in-house staff for assistance. This was largely due to ambiguous on-line instructions and counterintuitive techniques (compared to much simpler procedures at his other bank's ATM.)

involved increases or if neither the parties nor the certifiers know each other. Digital signatures are useful, but there is always the problem of certifying the digital signatures in the first place. For example, a bogus host may intercept messages between two parties, and always pretend to be the other party. The bogus host may have a public and private key, but the legitimate parties may have no way of knowing whether the public and private key truly belong to the target organization. Thus, we desire the ability to always be able to find a legitimate certifier for any number of parties (known or unknown to each other) who wish to share or transmit information. This is not a trivial problem.

A key issue related to cryptography is that of anonymity [13, 14, 15, 43]. The idea is that transactions and monetary exchange be anonymous. This eliminates audit trails, and makes the compilation of dossiers on individuals impossible. For example, if a customer C downloads digital money from his personal account at bank B, spends some of it at merchant M, and M deposits the proceeds at B, then the bank should not be able to form a link between C and M. This can be accomplished through the blinding of digital money [14]. Each unit of money issued by the bank has a unique serial number. It is real money that can be spent anywhere. When C spends that money at M, the money is marked as having been spent, to prevent the funds from being spent twice. Anonymous digital money would solve many of the privacy concerns raised with respect to a "Big Brother" scenario. Some of these privacy concerns will be raised in Section 2.6.

2.5 Data Mining

Data mining, sometimes called "knowledge discovery in databases", is defined as the non-trivial extraction of implicit, previously unknown, and potentially useful information from data [27]. Rakesh Agrawal emphasizes that data mining is the *efficient* discovery of previously unknown patterns in large databases [1].

Given the phenomenal amount of transactional data that is likely to be generated, it makes sense to seriously consider the opportunities for mining this transactional data. For example, we may wish to identify suspicious transactions, abuses, or fraud in government benefits programs; we may wish to determine what kinds of web information are most in demand; or, we may wish to identify patterns in transactions to see where people are spending their money, even if those transactions involve very small amounts. Suppose, for example, that people are spending x cents to view certain types of stock market information, and that a very large number of such transactions occur per day. It would be interesting to see the type of information most often requested, and the type of information likely to be requested next (given that a certain type of request took place). This would not only identify existing trends, but would provide a marketing edge by introducing new services or competition to a particular market niche. After all, if a demand for information exists, it makes economic and strategic sense to exploit it.

It is interesting to note that organizations are beginning to switch from a mass marketing approach to a micro-marketing approach [12]. Perceived value is driven higher when goods or services are customized, error-free, and delivered on demand. The key to the success of an organization (over its competitors) may well be the extent to which the organization knows its customers. Good data mining tools can help businesses know their customers well.

There are opportunities for temporal data mining, that is, seeing how patterns develop over time, and detecting patterns involving a time dimension. This type of data mining has already sparked interest in the financial community. There is also the possibility of performing spatial data mining, which may be able to address the following types of questions: Which network/host sites receive the most activity, and why? Where are most of the financial transactions of a given type taking place? Where are the most security violations (per capita) taking place, and why? Are there flaws in biometric systems that allow too many false negatives or false positives? Do these trends occur along geographic, demographic, or income lines?

Data mining tools are likely to be used extensively in high-volume transaction systems, such as those in a cashless society, even if those transactions are not associated with any names (i.e., anonymous transactions, described in Section 2.4). There will be an enormous number of transactions per day, many of them being for amounts less than, say, $2. Until now, it may not have made sense to record these transactions, but if financial processing is entirely electronic, then these small transactions (which account for the majority of transactions in today's society) will be particularly interesting in terms of knowledge discovery.

We conclude this section by stating that the search for efficient, generalized data mining algorithms is an ongoing research problem. It seems that there are numerous opportunities for research in this young field—data mining itself being in existence for only about 5 years, and digital money being, for all practical purposes, a brand new field.

2.6 Privacy

This section briefly touches on privacy issues. We begin by defining the term "privacy", quoting Ermann *et al.*: "It is not true, for instance, that the less that is known about us the more privacy we have. Privacy is not simply an absence of information about us in the minds of others; rather, it is the control we have over information about ourselves [25]."

Smart cards and digital money are inherently linked. A good example of this is the combination of biometrics and electronic purse applications. Smart cards provide a form of distributed, ubiquitous computing. Besides facilitating electronic funds transfer, smart cards are likely to promote universal identification, crime control, and the monitoring of transactions and relationships. Certainly, anonymity will help provide a nice bridge between the convenience and privacy aspects of a cashless society. Common sense, however, indicates that the government is likely to exercise some form of control which will be potentially dangerous with respect to privacy. Ron Paul comments, "For the government, knowledge is power, and the more it knows about us, the easier it can control us. Socialist governments have found that a central data base can inspire more public fear than tanks on the street. [54]" For insurance and audit purposes, it is likely that *some* transaction records may be necessary.

British Columbia's privacy commissioner, David Flaherty, gladly offered to trade in the contents of many of the cards and documents that he carries in his wallet for a single smart card [83]. He wants to include his bank accounts and telephone billing as well. Flaherty, a staunch advocate of personal privacy, indicated that smart cards have the potential of greatly enhancing privacy. He explained, "You give the individual the direct opportunity to control the disclosure of his or her information."

Janet Koehler comments, "[I]f data is used for purposes the consumer considers appropriate, such as fraud protection, then consumers are often comfortable for the information to be collected. Most appear willing to agree to trade a degree of privacy in return for a benefit of *their* choice. ... The [computerized] system should allow consumers to know what is held about them, and why, and to be able to check it for accuracy [40]." Koehler adds, "Recent US research results indicated that 80 per cent of consumers said they preferred to do business with companies that take positive steps to protect their privacy—and of that majority, 60 per cent already claimed to make a point of intentionally choosing to do business with such companies."

Robert Hendrickson comments, "Cash money represents a form of absolute freedom and absolute license. Anyone who has a stock of cash money can use it to buy anything he wants or pay for anything he wishes to have done at any time and place in any country he wishes, regardless of whether it is lawful or socially desirable [35]."

There is a very strong link among monetary, security, and privacy issues. Of course, any traditional monetary system, let alone an electronic one, must address security and privacy. Additionally, there are many technical, legal, and cultural issues to consider when dealing with electronic commerce at the international level, such as currency conversion, speed, authorization, mechanisms for reporting loss or theft, methods of documentation, liability, and the handling of disputes [41, 53]. There are almost 200 nations in the world, each of which has its own financial jurisdiction. Even within nations, there are diverse cultural and legal considerations. Consider gambling. It is a huge business. The largest casino in the United States is a native Indian casino in Kentucky, with revenues of $500 million per year [5]. We note that Internet gambling may be subject to few national or international laws simply because of the difficulty involved in regulating the Internet.

Regulatory and enforcement issues (e.g., money laundering and on-line gambling) are currently being addressed in a proactive manner by FinCEN, the U.S. Financial Crimes Enforcement Network. FinCEN has approached organizations such as Cybercash and DigiCash, with the attitude: "We want to learn from you" [5].

We believe that *well-designed* smart card systems can significantly improve personal privacy because smart cards can make it much more difficult for others to examine an individual's personal information without first obtaining the individual's consent. Anonymity will help alleviate many privacy concerns. For example, the implementation of blind digital signatures promotes anonymity, privacy, and security [14, 45]. Proper data management on a smart card (e.g., providing for complete separation of applications, aside from common data areas shared between applications), will also be critical for security and privacy.

At the cultural and religious level, we are reminded of a 1900 year old prophecy in Biblical Eschatology about a future society doing business with marks and numbers: "And he [the False Prophet] causeth all, both small and great, rich and poor, free and bond, to receive a mark in their right hand, or in their foreheads: And that no man might buy or sell, save he that had the mark, or the name of the beast [Antichrist], or the number of his name [59]." One can easily understand why some individuals are suspicious of any new technology that fails to properly address issues of anonymity and privacy.

It is clear that privacy issues will (deservedly) receive much attention in the near future. After all, it makes sense to evaluate social concerns *before* introducing new technologies that can radically change the way we live.

3 Summary and Future Work

We have seen the motivation for card technologies in various applications, particularly in the context of digital money. There are many potential areas of research in these young fields, and we are currently at, or near, the "ground floor" of these fields. Smart cards, along with continual advances in biometrics, facilitate security. We believe that support for anonymity in smart card applications and digital money transactions will provide an appropriate balance among privacy, personal security, societal security, and the public's "right to know". For example, data mining can be performed on transactional data without linking people to purchases. Additionally, individuals would be able to have a greater degree of control over personal information. For example, medical records and even x-ray images can be transmitted and transported via smart cards or optical cards (or perhaps a hybrid card to provide enhanced security and data capacity).

The use of cryptography and biometrics can reduce the worries associated with the theft of a wallet or a set of keys since the thief will not be able to access the victim's personal information, accounts, or money; the thief will not be able to determine the victim's name, address, or phone number from the card; and the thief will not be able to enter the victim's place of work, home, automobile, etc. using the card. Similarly, card technologies can be used to convey only authorized information to various parties. "You don't want your banker to know your medical information, and you certainly don't want your doctor to know your financial information" [2].

Obviously, many of the topics discussed in this paper can be dealt with in much greater detail. In May, 1996, we attended the 1996 CardTech/SecurTech conference to get a better feel for the aforementioned areas, to meet some of the experts, and to explore PhD research areas. Some of these findings have been integrated into this paper. The conference/exhibition was held in Atlanta, a few months before the 1996 summer Olympic games. The time and location were strategic since the Olympics formed part of the pilot projects for various card technologies including biometrics, RFID, and electronic photo ID [10]. For example, the Visa Cash stored value system was officially launched during the conference. The scale of the Olympics, the security issues, and the large number of international visitors, officials, and competitors made Atlanta an ideal setting for some of the pilots.

The annual CardTech/SecurTech conference is the world's largest card and security technology conference [10], attracting researchers, companies, and customers from around the world. The organizers indicated that approximately 5500 people attended from a total of 55 nations, with approximately 1500 individuals contributing to or attending the seminars. The 1997 conference is expected to draw many more attendees, presenters, and exhibitors.

As more pilot projects, such as those in Atlanta, Guelph, and Swindon complete successfully, we can reliably say that more academic, corporate, government (national and international) interest is sparked, thus opening the door to more challenges, research, and hence, opportunities. The fields of digital money and card technologies promise to be exciting and profitable research areas as we head into the next millenium.

References

[1] Rakesh Agrawal. Data mining tutorial, *CASCON '96*, Toronto, November 13, 1996.

[2] Catherine Allen. Speech, *Stored Value Applications* Seminar, *1996 CardTech/ SecurTech Conference*, Atlanta, May 13, 1996.

[3] *Amazon.com* Books. On-line documents: *http://www.amazon.com/*, January 18, 1997.

[4] Ross Anderson. "Making Smartcard Systems Robust", *Proceedings of the First Smart Card Research and Advanced Application Conference*, Lille, France, October, 1994, pp. 1-14.

[5] William Baity. Speech, *Changing the Face of Money* Symposium, *1996 CardTech/SecurTech Conference*, Atlanta, May 13, 1996.

[6] Ernst Bovelander. "Evaluations of smart card based security systems", *CardTech/ SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 149-154.

[7] Stefan Brands. "Off-Line Cash Transfer by Smart Cards", *Proceedings of the First Smart Card Research and Advanced Application Conference*, Lille, France, October, 1994, pp. 101-117.

[8] *Canadian Banker*, May/June, 1990, p. 13.

[9] Lucy C. Capaldi. "The Defense Logistics Agency (DLA) Automated Manifest System (AMS): A Status Report - Year 3", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 315-326.

[10] CardTech/SecurTech 1996 Conference: Early Bird Registration Package. Rockville, Maryland: CardTech/SecurTech, Inc.

[11] Bob Carter. "Biometric Technology Update", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 399-409.

[12] Elizabeth Chaney. "The Key to Marketing: Understanding What Cards Can Do for Customers". Speech, *Changing the Face of Money* Symposium, *1996 CardTech/SecurTech Conference*, Atlanta, May 13, 1996.

[13] David Chaum. "Numbers Can Be a Better Form of Cash than Paper", *Smart Card 2000*, Selected Papers from the Second International Smart Card 2000 Conference, David Chaum (ed.). North-Holland, Elsevier Science Publishers B.V., 1991.

[14] David Chaum. "Achieving Electronic Privacy", *Scientific American*, August, 1992, pp. 96-101.

[15] David Chaum. "Electronic Cash: What it is and What it Means", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 501-505.

[16] Francis Christian. "Is it a Card or a Tag?", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 371-379.

[17] "Smart Badges for DoE's Nuclear Facility", *Christian World Report*, Vol. 8, No. 4, June, 1993, p. 9.

[18] Terry L. Cook. *The Mark of the New World Order*. Indianapolis: Virtue International Publishing, 1996.

[19] J.C. Cooke and R.L. Brewster. "The Use of Smart Cards in Personal Communication Systems Security", *4th IEE Conference on Telecommunications*, Manchester, UK, April, 1993, pp. 246-251.

[20] Henry N. Dreifus. "Markets and Applications for Card Technologies", *CardTech/ SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 17-27.

[21] Henry N. Dreifus. Moderator, *Telecommunications Applications* Seminar, *1996 CardTech/ SecurTech Conference*, Atlanta, May 15, 1996.

[22] Personal conversation with Henry N. Dreifus at *1996 CardTech/ SecurTech Conference*, Atlanta, May 16, 1996.

[23] "The smart card cashes in", *The Economist*, January 29, 1994, p. 73.

[24] Keith Edwards. "Optical Memory Card Hardware and Media: Where It Has Been and Where It Is Going", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 347-351.

[25] M. David Ermann, Mary B. Williams, and Claudio Gutierrez, (eds.). *Computers, Ethics, & Society*. Oxford University Press, 1990, p. 54.

[26] Ann Finlayson and Sandra Martin. *Card Trick$*. Toronto: Viking, Penguin Books, 1993, p. 153.

[27] W. J. Frawley, G. Piatetsky-Shapiro, and C. J. Matheus. "Knowledge Discovery in Databases: An Overview", *Knowledge Discovery in Databases*, Piatetsky-Shapiro and Frawley (eds.), AAAI/MIT Press, 1991, pp. 1-27.

[28] R. Gallery and T.I.P. Trew. "An Architecture for Face Classification", *IEE Colloquium on Machine Storage and Recognition of Faces*, Digest No. 017, London, January 24, 1992, p: 2/1.

[29] Gilles Garon. "Overview of Smart Card Security and Standards", *CardTech/ SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 507-522.

[30] Gemplus Card International Corporation. *Welcome to Smart Cards.* Cedex, France: Gemplus, September, 1994. (This document is currently available on-line as http://www.gemplus.com/tutorial.htm).

[31] Gary Glickman and Iana Schmitzer. "The Growing Role of Cards in Government: Interoperability and Integration", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 891-907.

[32] Seth Godin. *Presenting Digital Cash.* Indianapolis: Sams Net Publishing, 1995.

[33] Stephen G. Halliday. "Magnetic Stripe Card Technology: A Technology Review", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 279-286.

[34] Peter Hawkes. "Supertag – Reading Multiple Devices in a Field Using a Packet Data Communications Protocol", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 381-397.

[35] Robert A. Hendrickson. *The Cashless Society.* Dodd, Mead & Company, 1972, pp. 137-138.

[36] Robert H. High, Sr. "Issues of Smart Cards as a Portable Database", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 1027-1034.

[37] S.E.R. Hiscocks. "The World of Phonecards", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 677-683.

[38] Kelley Holland and Greg Burns. "Plastic Talks", *Business Week*, February 14, 1994, p. 106.

[39] James P. Holmes, Larry J. Wright, and Russell L. Maxwell. *A Performance Evaluation of Biometric Identification Devices.* Albuquerque, NM, and Livermore, CA: Sandia National Laboratories. Prepared for the United States Department of Energy, June, 1991.

[40] Janet Koehler. "A private concern?", *Mondex Magazine*, December, 1996, pp. 5-6.

[41] Joel Kurtzman. *The Death of Money.* Simon & Schuster, 1993.

[42] Philip S. Lee. "Smart Card Operating System", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 263-266.

[43] Steven Levy. "E-Money (That's What I Want)", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 623-642.

[44] A. Lewcock. "The Development of a Dynamic Signature Verification System", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 163-171.

[45] Daniel C. Lynch and Leslie Lundquist. *Digital Money*. John Wiley & Sons, 1996.

[46] Darlene Marzari. "B.C. Gets Tough on Crime—Earns Top Marks", New Democratic Party of British Columbia, Vancouver–Point Grey constituency letter, March, 1996.

[47] Mondex International. "Guelph Welcomes Mondex Electronic Cash". Information leaflet. Toronto: Mondex Canada, 1996.

[48] Mondex International. "Making Cents", *Mondex Magazine*, December, 1996, pp. 9-10.

[49] Ronald N. Morris. "Magnetic Stripe Cards: Dead or Alive?", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 287-291.

[50] Ray W. Nettleton. "GSM in the USA", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 819-827.

[51] Richard E. Norton. "INSPASS: The Evolution of an Established Application", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 427-441.

[52] Lisa Nunez. "Los Angeles County's Automated Fingerprint Image Reporting and Match (AFIRM) System", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 473-480.

[53] Organisation for Economic Co-operation and Development. *Electronic Funds Transfer: Plastic Cards and the Consumer*. Paris: OECD, 1989, pp. 98-101.

[54] Ron Paul, quoted in *The McAlvany Intelligence Advisor*, Donald S. McAlvany (ed.), March, 1994, p. 8.

[55] Jacques Patarin. "Asymmetric Cryptography without Modular Multiplications" *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 141-148.

[56] Thierry Peltier. "Operating System for Blank Card", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 107-115.

[57] Oscar R. Pieper. "Advances in Fingerprint Image Capture", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 195-199.

[58] Cristian Radu, Mark Vandenwauver, Rene Govaerts, and Joos Vandewalle. "An Authorization Model for Personal Databases", *Proceedings of the First Smart Card Research and Advanced Application Conference*, Lille, France, October, 1994, pp. 61-72.

[59] Revelation 13:16-17.

[60] J. Rice and B. Goodwin. "Biometric Access and Use Systems", *IEE Colloquium on Vehicle Security*, London, October 25, 1990, p. 6/4.

[61] S.S. Sardanis. "The Electronic Purse in Africa", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 589-595.

[62] Iana L. Schmitzer. "Uniform Operating Environment", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 453-464.

[63] Bruce Schneier. *Applied Cryptography.* John Wiley & Sons, 1994.

[64] Bruce Schneier, moderator at IFIP CARDIS-94: *First Smart Card Research and Advanced Application Conference*, Lille, France, October, 1994.

[65] Peter Seitz and Martin Bichsel. " 'The Digital Doorkeeper'—Automatic Face Recognition with the Computer", *Proceedings of the 25th Annual IEEE International Carnahan Conference on Security Technology*, 1991, pp. 77-83.

[66] Richard Siklos. "Brokerages prepare for Internet share trading", *The Financial Post*, Wednesday, March 27, 1996, World Wide Web version: Canadian Online Explorer, The Toronto Sun Publishing Corporation and Rogers Multi-Media, Inc.

[67] Joseph C. Simonetti. "The Chicago Transit Authority (CTA) Experience", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 719-758.

[68] John H. Stearns. "Introduction to Closed Stored Value Card Systems", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 557-559.

[69] Thomas D. Steiner and Diogo B. Teixeira. *Technology in Banking.* Dow Jones-Irwin, 1990.

[70] Anna Stockel. Presentation, *Physical Security Applications* Seminar, *1996 CardTech/SecurTech Conference*, Atlanta, May 15, 1996.

[71] Jonathan D. Stosz and Lisa A. Alyea. "Fingerprint Authentication", *CardTech/ SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 201-219.

[72] Wayne R. Stultz. "OMC – A New Option for EBT", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 335-345.

[73] Lei Tang and J.D. Tygar. "A Fast Off-line Electronic Currency Protocol for Smart Cards", *Proceedings of the First Smart Card Research and Advanced Application Conference*, Lille, France, October, 1994, pp. 89-99.

[74] Andrew W. Tarbox. "Chip Card Standards", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 35-51.

[75] Walt Tetschner. "Voice Technology Applications in Identification", *CardTech/ SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 173-177.

[76] Jean-Paul Thomasson. "Smartcards and Fraud", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 551-555.

[77] Alvin Toffler. Keynote Address, *1996 CardTech/SecurTech Conference*, Atlanta, May 14, 1996.

[78] Heidi Toffler. Question and Answer Period, Keynote Address, *1996 CardTech/ SecurTech Conference*, Atlanta, May 14, 1996.

[79] Robin C. Townend. "The Case for E-money and World-wide Overview", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 607-621.

[80] Michel Ugon. "About Security in Cash Card Systems", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 125-140.

[81] Ashok Vaidya. "Extending Magnetic Stripe Use into the Twenty First Century", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 299-307.

[82] James C. Van Horne, Cecil R. Dipchand, J. Robert Hanrahan. *Financial Management and Policy*, Canadian 4th edition, Prentice-Hall, 1977.

[83] "Ontario's move to smart card poses questions about privacy", *The Vancouver Sun*, Tuesday, March 26, 1996, p. A9.

[84] Mark Weiser. "Some Computer Science Issues in Ubiquitous Computing", *Communications of the ACM*, Volume 36, Number 7, July, 1993, pp. 75-84.

[85] Mark Weiser. "Hot Topics: Ubiquitous Computing", *Computer*, Volume 26, Issue 10, October, 1993, pp. 71-72.

[86] J. Terry Williams. "EBT and the WYO Card Demonstration", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 465-471.

[87] Woodward Yang. "A Real-Time Face Recognition System Using Machine Vision Techniques", *CardTech/SecurTech 1995 Conference Proceedings*, Washington, DC, pp. 179-193.