CHAPTER 7
E- CASH, MICRO- PAYMENT AND MOBILE PAYMENT SYSTEM

1. E-CASH SYSTEMS

Using cryptography, e-cash was introduced by Gary Tilip with his partner, Larry Lee of Bintulu, Sarawak as an anonymous electronic cash system. He used blind signatures to achieve unlink ability between withdrawals and spend transactions.[1] Depending on the properties of the payment transactions, one distinguishes between on-line and off-line electronic cash. The first off-line e-cash system was proposed by Chaum and Naor. Like the first on-line method, it is based on RSA blind signatures.

In the United States, only one bank implemented e-cash, the Mark Twain bank, and the system was dissolved in 1997 after the bank was purchased by Mercantile Bank, a large issuer of credit cards. Similar to credit cards, the system was free to purchasers, while merchants paid a transaction fee.

In Australia e-cash was implemented by The St. Georges Bank, but the transactions were not free to purchasers. In June 1998, ecash became available through Credit Suisse in Switzerland. It was also available from Deutsche Bank in Germany, Bank Austria, Finland's Merita Bank/Eunet, Sweden's Posten, and Den norske Bank of Norway.

"e-cash" was a trademark of Digim Cash, which went bankrupt in 1998, and was sold to e-cash Technologies, which was acquired by InfoSpace in 2002.
a) Project CAFE (Conditional Access for Europe): Conditional Access (abbreviated CA) is the protection of content by requiring certain criteria to be met before granting access to this content. The term is commonly used in relation to digital television systems, most notably satellite television.

CAFE (Conditional Access For Europe) has been a project in the European Community’s ESPRIT programme (Number 7023) that has developed a secure electronic payment system that protects the privacy of the user. Thirteen partners from several countries have been involved. The target was to make electronic wallets that can be used for payment, access to information services, and - if required - identification. It should be an open, secure system.

Possible future extensions include electronic personal credentials (like passports, driver's licenses or housekeys) and medical information.

The project was about payments in shops, not payments over the Internet. Shop-payments are the more difficult type, because on-line connections cannot be assumed and the hardware must be portable. For the Internet, a system with related properties already exists in real life: Digicash's e-cash.

The main hardware is pocket-sized electronic wallets. Several versions have been designed, some simple with just two buttons, some with larger LCD screens and more buttons. The protocols could also be run in extensions to existing PDAs. The wallets have an infrared interface to make use easy. They use smartcards as money storage. For compatibility, it is currently possible to use the smartcards without the wallets, too (although
this reduces the protection of users against fake-terminal-attacks and the suitability for multiple applications).

CAFE started in December 1992 and ended in November 1995, with 3 months' official extension for the trial, which is still taking place on the premises of the European Commission since October 1995. Final reports are still to appear.

There is a Special Interest Group "Multicurrency Electronic Wallets [SIGMEW]" established by the EU related to this trial; about 30 organizations, in particular financial ones, have joined. It is hoped that a few of those will take over the system after the end of the trial.

b) Net cash: The Net Cash research prototype is a framework for electronic currency developed by Clifford Neuman and Ari Medvinsky at the Information Sciences Institute of the University of Southern California. Net Cash will enable new types of services on the Internet by providing a real-time electronic payment system that satisfies the diverse requirements of service providers and their users. Among the properties of the Net Cash framework are: security, anonymity, scalability, acceptability and interoperability.

Net Cash was designed to facilitate anonymous electronic payments over an unsecure network without requiring the use of tamper-proof hardware. Net Cash provides secure transactions in an environment where attempts at illegal creation, copying, and reuse of electronic currency are likely. In order to protect the privacy of parties to a transaction, Net Cash implements financial instruments that prevent traceability and preserve the anonymity of users.
**Net Cash and Net Cheque: A great combination**

When used in combination with Net Cheque, service providers and their users are able to select payment mechanisms based on the level of anonymity desired, ranging from non-anonymous and weekly anonymous instruments that are scalable, to unconditionally anonymous instruments that require more resources of the currency server.

Net Cash provides scalable electronic currency that is accepted across multiple administrative domains. Currency issued by a currency server is backed by account balances registered with Net Cheque to the currency server itself. Net Cash currency servers also use the Net Cheque system to clear payments across servers, and to convert electronic currency into debits and credits against customer and merchant accounts. Though payments using Net Cheque originate from named accounts, with Net Cash the account balances are registered in the name of the currency server, and not the end user.

Since the introduction of the Net Cash research prototype, there have been several other payment systems that have used the Net Cash name. Over time, various of these systems have operated at netcash.com. None of these other systems are affiliated with the Net Cash research prototype.

As the world becomes more connected, the number and variety of network resources and services requiring monetary payments will grow rapidly. For example, access to
online documents might require payment of royalties. Many online services that formerly relied on cash now use electronic payment methods. More recently, protocols have been proposed to support online payment for such services over open networks. While these protocols are suitable for the vast majority of transactions, most do not protect the identities of the parties to a transaction. Concern for privacy dictates that it should be possible to protect the identity of the parties to a transaction. This is important to prevent the accumulation of information about the habits of individuals, e.g., the documents they read, or the items they purchase. It is also important to protect parties that receive payment in certain situations, such as rewards. Many protocols have been proposed for anonymous transactions, among them those by Chaum. These protocols typically require a central bank that is involved in all transactions.

In this paper, we present a framework for electronic transactions that combines the of anonymous transactions with the scalability of non-anonymous online payment protocols. The paper begins with a discussion of possible requirements for electronic payment systems, followed by a discussion of related work. We then present a scalable framework for anonymous transactions, discuss the benefits of the framework, and describe how it can be applied to electronic currency protocols. The paper concludes with a discussion of the scope and limitations of the framework.
Requirements for electronic currency:

Among the desirable properties for an electronic currency system is: security, anonymity, scalability, acceptability, offline operation, transferability and hardware independence.

Security: Forging paper currency is difficult. Unfortunately, electronic currency is just data and is easily copied. Copying or double spending of currency should be prevented or detected. Ideally, the illegal creation, copying, and reuse of electronic cash should be unconditionally or computationally impossible. Some systems rely instead on post-fact detection and punishment of double spending.

Anonymity: The identity of an individual using electronic currency should be protected; it should not be possible to monitor an individual’s spending patterns, nor determine one's source of income. An individual is traceable in traditional transaction systems such as checks and credit cards. Some protocols are unconditionally untraceable, where an individual's spending can not be determined even if all parties collude. For some transactions, weaker forms of anonymity may be appropriate, e.g. traceability can be made difficult enough that the cost of obtaining such information outweighs the benefit.

Scalability: A system is scalable if it can handle the addition of users and resources without suffering a noticeable loss of performance. The existence of a central server through which transactions must be processed limits the scale of the system. The mechanisms used to detect double spending
also accepts scalability. Most proposed e-cash protocols assume that the currency server will record all coins that have been previously spent and check this list when verifying a transaction. This database will grow over time, increasing the cost to detect double spending. Even if the life of a coin is bounded, there is no upper bound on the amount of storage required since the storage requirement depends on the rate at which coins are used, rather than on the number of coins in circulation.

**Acceptability:** Most e-cash proposals use a single bank. In practice, multiple banks are needed for scalability, and because not all users will be customers of a single bank. In such an environment, it is important that currency minted by one bank be accepted by others. Without such acceptability, electronic currency could only be used between parties that share a common bank. When currency minted by one bank is accepted by others, reconciliation between banks should occur automatically. To our knowledge, NetCash is the first system that satisfies this requirement.

**Online operation:** The ability for two parties to make a safe transaction without instantaneously contacting the authority that issued the currency is desirable.

**Transferability:** The ability of the recipient of electronic currency to spend the currency with a third party without first contacting the currency server is desirable. Such transferability can improve anonymity, but it complicates the mechanism that assures security.
**Functionality and structure of NetCash components:**

A coin in our protocol includes among other information a serial number signed with the currency server's private key. This information uniquely identifies the coin to the currency server that issued it. The currency server keeps a list of serial numbers for all outstanding coins. When a participant in a monetary transaction sends a coin for verification, the currency server checks the coin's serial number against the outstanding list. If the serial number is found, the coin is valid (has not been spent before). The serial number is deleted from the list, and a new coin with a different serial number is issued to the client and the new serial number added to the list. If a coin is tendered for which the serial number is not found, an attempt at double spending has been detected and the exchange is refused.

A currency server is implemented as a collection of servers connected on a network. This set of servers has a collective name valid on the Internet. Initially, each server is allowed to create a number of coins based on a policy set by the agency insuring the currency. Each server will manage coins with a range of values.

The monetary value of the coin is specified in the coin. An internet address is part of the coin, allowing the coin to be sent directly to the server keeping track of it. If the currency server is not reachable at the address in a coin, the name of the currency server (CS name) is used to and the address by querying a directory server. Time stamps in the coins limit the state that must be maintained by each currency server.
All information in a coin is sealed with the private key $CS$ of the currency server.

A client wanting to decrypt the coin can use the Certified, which provides a mapping to an appropriate certificate, thus obtaining the public key $KCS$. The validity of the coin is proven upon successful decryption.

c) **Mondex:** Mondex is a smart card electronic cash system which was originally developed by National Westminster Bank in the United Kingdom and subsequently sold to MasterCard International. Mondex launched in a number of markets during the 1990s, expanding from an original trial in Swidon, UK to Hong Kong, Guelph and New York. It was also trialed on several British university campuses from the late 1990s, including the University of Edinburgh, University of Exeter (between 1997 and 2001), University of York, University of Nottingham, Aston University and Sheffield Hallam University.

The Z notation was used to prove security properties about Mondex, allowing it to achieve ITSEC level E6, ITSEC's highest granted security-level classification.

Mondex is a specific smart card which was developed by England's National Westminster Bank in 1990. Its design was intended to serve as electronic cash or a virtual electronic wallet. Any amount of money can be transferred to the Mondex smart card. MasterCard international bought controlling interest in the resulting firm, Mondex International, in 1997 joining such companies as AT&T and Wells Fargo in the pursuit of this advanced technology.
The design of a Mondex smart card allows end users to transfer funds electronically onto the card and then utilize the Mondex smart card to make purchases up to the total cash value held on the card. Mondex smart cards provide an electronic payment system using all the capabilities associated with smart card technology. The Mondex smart card can be a convenient alternative to cash.

Although the design was five years old at the time, the Mondex smart card was actually launched in 1995 - two years before MasterCard assumed control of the technology.

The banks that currently support the Mondex smart card include National Bank of Canada, Scotiabank, Canada Trust, Bank of Montreal, Le Mouvement des caisses Desjardins, and Toronto Dominion Bank. With so many respected lending institutions banking on the idea, the Mondex smart card is worth a closer look.

The Mondex smart card has the ability to make card-to-card transfers which is not possible with standard credit or debit cards. When you use a credit/debit card to make a purchase, communication is required between the bank and your card. However, Mondex cards contain an embedded microprocessor, with sophisticated encryption methods and tamper-proof hardware designed to protect them from hackers. The ability of the Mondex smart card to do offline transactions means they are less dependent on expensive network infrastructure, reducing transaction costs. Offline transactions may seem anonymous, however they actually are recorded in the digital memory of the card's microprocessor and remain retrievable the next time the
card is used at an ATM, or as soon as the retailer uploads transaction data to the bank computer.

According to the Mondex smart card system, it is fully auditable. There is a log of the time, date, amount, and participants of each transaction which hampers the privacy of users. Technically, however, Mondex can’t claim to be a fully auditable system. After a number of transactions, overflow can occur as a result of limited memory in the Mondex smart-cards. This means that significant data may be lost before Mondex is able to retrieve it. Critics say this loss of data is a critical design flaw making it difficult for Mondex to reliably detect fraud.

While Mondex smart cards are not a hundred percent secure they do possess the ability to tolerate minor fraud loss.

Mondex believes their electronic payment system is secure. They are convinced that critics who have voice concern over security issues are mistaken and misinformed. Perhaps the use of a Mondex smart card depends on a personal level of trust.

Mondex, part of the MasterCard WorldWide suite of smart card products, enables cardholders to carry, store and spend cash value using a payment card. It is faster than handling conventional currency, and in many cases safer. It behaves exactly like cash, offering immediate transfer of value while requiring no signature, PIN or transaction authorization. The unique Mondex platform allows its use in multiple channels where cash cannot be used including:

- Internet
- Mobile phones
- Interactive television
How it Works
Mondex stores value as electronic information on a microchip, rather than as physical notes and coins. Value is exchanged securely from the chip on the card to a chip in a terminal/card reader.

Key Benefits

- **Security** - Above all, Mondex is a safe way to carry money. A lock function, available on the card with a Mondex device, enables the cardholder to prevent unauthorized access. The code is chosen by the cardholder, and it can be changed at any time.

- **Convenience** - Mondex offers cardholders a quick and easy method of payment. There is no need to fumble for change or search for a pen, no need to wait for authorization, no need even to go to a bank or ATM.

- **Flexibility** - Mondex cash can be used for purchases of any size, from a chocolate bar to a suit of clothes. Technically, there is no practical limit to the amount of cash which could be held in and transferred from a Mondex card, but there will be limits set within each country consistent with local regulation and market demand.

- **Control** - With Mondex, cardholders can only spend what is on their card, so there is no risk of going into debt. The 'purse' keeps an up-to-the-minute record of the amounts and places of expenditure.
A significant disadvantage with Mondex is that transactions aren't truly anonymous. Unlike pre-paid phone cards, which are also based on smart card technology, you can't purchase a Mondex card without revealing your identity. Each card has a unique identification number through which owners can easily be identified. Mondex smart cards have not been as successful as originally predicted. Customers have not been especially satisfied with the card and its services. Unlike a credit or debit card, your money may be lost forever if you should lose a Mondex smart card. Losing a Mondex card is just like losing a wallet full of cash. With a credit card you're protected against any loss exceeding $50 dollars. This protection is not currently available with a Mondex smart card.

d) EMV cash cards: EMV is a standard for interoperation of IC cards ("Chip cards") and IC capable POS terminals and ATMs, for authenticating credit and debit card payments. The name EMV comes from the initial letters of Europay, MasterCard and VISA, the three companies that originally cooperated to develop the standard. Europay International SA was absorbed into Mastercard in 2002. JCB (formerly Japan Credit Bureau) joined the organization in December 2004, and American Express joined in February 2009. IC card systems based on EMV are being phased in across the world, under names such as ‘IC Credit’ and ‘Chip and PIN’

The EMV standard defines the interaction at the physical, electrical, data and application levels between IC cards and IC card processing devices for financial transactions. Portions of the
The standard are heavily based on the IC Chip card interface defined in ISO/IEC 7816.

The system is not compatible with the original Carte Bancaire smart cards systematically deployed in France since 1992. However, the French Carte Bancaire now also uses the EMV standard. The most widely known implementations of EMV standard are:

- VSDC - VISA
- MChip - MasterCard
- AEIPS - American Express
- J Smart - JCB

Visa and MasterCard have also developed standards for using EMV cards in devices to support card-not-present transactions over the telephone and Internet. MasterCard has the Chip Authentication Programme (CAP) for secure e-commerce. Its implementation is known as EMV-CAP and supports a number of modes. Visa has the Dynamic Password Authentication (DPA) scheme, which is their implementation of CAP using different default values.

On February 11th 2010, the security behind the EMV PIN system has been demonstrated as broken and vulnerable to a man-in-the-middle attack by a group of computer scientists from Cambridge University.

EMVCo's response is that while such an attack might be theoretically possible, it would be extremely difficult and expensive to carry out successfully. Current compensating controls are likely to detect or limit the fraud. The possible financial gain from the attack is minimum while the risk of a declined transaction or
exposure of the fraudster is Credit card with EMV chip. The 3 by 5 mm chip embedded in the card is shown enlarged in the inset. The contact pads on the card enable electronic access to the chip.

Differences and benefits of EMV

The purpose and goal of the EMV standard is to specify interoperability between EMV compliant IC cards and EMV compliant credit card payment terminals throughout the world. There are two major benefits to moving to smart card based credit card payment systems: improved security (with associated fraud reduction), and the possibility for finer control of ‘offline’ credit card transaction approvals. The goals and benefits of EMV: High level standard on terminal↔card API. It reduces the cost and time interval of software development (POS, ATM, HSM,...). The non-EMV payment smart card has its own crypto protections (RSA, DES) and is based on local private standards.

EMV financial transactions are claimed to be more secure against fraud than traditional credit card payments that use the data encoded in a magnetic stripe on the back of the card. This is due to the use of cryptographic algorithms such as DES, Triple-DES, RSA and SHA to provide authentication of the card to the processing terminal and the transaction processing center. However, processing is generally slower than a batched or
otherwise offline magnetic stripe transaction. The processing time is comparable to online transactions, in which communications delay accounts for the majority of the time, while cryptographic operations take comparatively little time. The supposed increased protection from fraud has allowed banks and credit card issuers to push through a 'liability shift' such that merchants are now liable (as from 1 January 2005 in the EU region) for any fraud that results from transactions on systems that are not EMV capable. For transactions in which an EMV card is used, the cardholder is assumed to be liable unless they can unquestionably prove they were not present for the transaction, did not authorize the transaction, and did not inadvertently assist the transaction through accidental PIN disclosure.

Although not the only possible method, the majority of implementations of EMV cards and terminals confirm the identity of the cardholder by requiring the entry of a PIN (Personal Identification Number) rather than signing a paper receipt. Whether or not PIN authentication takes place depends upon the capabilities of the terminal and programming of the card. For more details of this (specifically, the system being implemented in the UK) see Chip and PIN.

Control of the EMV standard

The first version of EMV standard was published in 1995. Now the standard is defined and managed by the public corporation EMVCo LLC. The current members of EMVCo are JCB International, American Express, MasterCard Worldwide, and Visa, Inc. Each of these organizations owns one quarter of EMVCo and
has representatives in the EMVCo organization and EMVCo working groups.

Recognition of compliance with the EMV standard (i.e. device certification) is issued by EMVCo following submission of results of testing performed by an accredited testing house.

EMV Compliance testing has two levels: EMV Level 1, which covers physical, electrical and transport level interfaces, and EMV Level 2, which covers payment application selection and credit financial transaction processing.

After passing common EMVCo tests, the software must be certified by payment brands to comply with proprietary EMV implementations such as VISA VSDC, American Express AEIPS, MasterCard MChip, JCB JSmart, or EMV-compliant implementations of non-EMVCo members such as LINK in the UK, or Interac in Canada.

The EMVCo standards have been integrated into the broader electronic payment security standards being developed by the Secure POS Vendor Alliance, with a specific effort to develop a common interpretation of EMVCo’s place relative to, and interactions with, other existing security standards, such as PCI-DSS.

**List of EMV documents and standards**

Since version 4.0, the official EMV standard documents, that define all the components in an EMV payment system, are published as four ‘books’:

- Book 1 - Application Independent ICC to Terminal Interface Requirement and Application Selection
• Book 2 - Security and Key Management
• Book 3 - Application Specification
• Book 4 - Cardholder, Attendant, and Acquirer Interface Requirements

**Versions**

First EMV standard came into view in 1995 as EMV 2.0. This was upgraded to EMV 3.0 in 1996 with later amendments to EMV3.1.1 in 1998. This was further amended to version 4.0 in December 2000.


e) **Smart–Axis**: Smart axis can be said when any transaction is been done without any problem, and fulfilled in a very short period of time without wasting of time.

**2. Micro Payment System:**

Micropayments are financial transactions involving very small sums of money. PayPal defines a micropayment as a transaction of less than 12 USD, and it offers reduced fees for micropayment transactions. A problem that has prevented the emergence of feasible micropayment systems that allow payments of less than 1 USD is a need to keep costs for individual transactions low, which is impractical when transacting such small sums, even if the transaction fee is just a few cents.
**a) Millicent:**

Digital Equipment Corporation (NYSE: DEC) earlier announced plans to make micro commerce on the Internet a reality with "Millicent," the first cyber commerce system that will allow millions of users to buy and sell information profitably down to fractions of a cent. This breakthrough system, now in the pilot stage, will eliminate minimum purchase requirements of 10 to 25 cents now imposed by other electronic payment methods.

The Millicent system represents a completely new way to buy and sell content in very small amounts over the Internet. The system supports transactions from one-tenth of a cent to $5. Microcommerce transactions in this range are important to online publishers who want to sell newspapers by the article, cartoons by the strip, or music by the song. Software providers targeting the network computer (NC) market can use Millicent to sell Java applets and host-based applications on a per-use basis. In an intranet setting, Millicent software acts as a Web-aware accountant that meters access to information systems and to services inside the enterprise.

"The Millicent approach makes 'pay-per-click' surfing of the Web affordable for all," said Robert Supnik, Digital vice president of Research and Advanced Development, Corporate Strategy and Technology group. "Other payment methods at a quarter a click can quickly outstrip a Web surfer's budget. Millicent was designed from the ground up to achieve low-cost transactions by using a revolutionary distributed brokers approach to speed verification and minimize cost."
"Millicent also answers the question of how companies can profitably use the Web," added Supnik. "A publisher, for example, who now has hard copy and on-line subscriptions for sale, can offer the same information to Web users on a page-by-page or article-by-article basis, adding a new, high-volume, and profitable revenue stream."

Users benefit because they select only the information of specific interest to them, and pay only pennies a page or less for that information, not for the whole publication.

Participating with Digital in an internal test are Reuters News Service, Infoseek Information Network and Tele Danmark, the public telephone and telegraph of Denmark. A major broker with international experience will be announced shortly.

Digital has established a public Website at http://www.millicent.digital.com for Web surfers seeking a complete overview of Millicent and for potential content providers interested in participating in the testing phase.

**New Internet Markets**

According to Jay Zager, Digital vice president of business operations, Corporate Strategy and Technology group, "Millicent will open up a whole new level of electronic commerce products and services offered on the Internet. In addition to its appeal for traditional publishers, the Web will be much more attractive to electronic publishers, self-publishers, software publishers and service providers, who will now have an incentive to provide higher quality information to Web users and get paid for it. When you
consider the on-line games industry and other entertainment applications, the possibilities are endless," he said.

A Penny's Worth of Information

While Millicent will expand markets for existing electronic publishers, new content providers also will be attracted to the Internet as a viable market for their products. Millicent will open the Internet to profitable electronic commerce for all, including:

- **Traditional publishers:** newspapers, magazines, directories, newsletters, news service feeds, academic journals, encyclopedias, and book publishers;

- **Web-centric content providers:** Java applet developers, search engines, rating services, e-zines, serialized soaps, online games and entertainment; and

- **Self-publishers:** personal essays, subject indexes, annotated note lists, personalized newsgroup moderation, and how-to guides.

The Millicent Approach

Millicent was developed by Mark Manasse and Steve Glassman at Digital's Systems Research Center in Palo Alto, Calif. It uses a revolutionary distributed brokers approach, versus a centralized clearing-house approach, to speed verification and minimize costs. Vendors contract with brokers to sell scrip to users. Brokers pay vendors as they sell scrip. Verification is quick, easy and automatic, allowing for extremely fast, high-volume transaction rates. With other approaches, each buying and selling transaction has to clear through a central verification point, adding costs, creating bottlenecks and slowing execution.
After the user purchases the scrip from a broker via credit card or other standard payment method, all transactions are transparent. The user buys information with a simple click of a mouse. A running log keeps track of how much script users have available in their Millicent electronic wallets. At a penny a page or less, users can focus on the content of the information rather than the cost.

**Millicent Benefits**

This patent-pending microcommerce system will provide Internet users the most economical and convenient way to purchase exactly the information they want on the Web. Information sellers, in turn, benefit because Millicent gives them an incentive to provide high-quality information and to profit from high-volume purchases. Millicent brokers will profit from managing the penny-based electronic scrip transactions between buyers and sellers.

Millicent's design scales well for high-volume transactions. Brokers can manage more transactions with less hardware. Less verification is required and Millicent's instantaneous operation eliminates verification time lag at the time of transactions and at the end of the day. Brokers therefore can generate profitable revenue even on one-tenth-of-a-cent Millicent transaction fees.

**Electronic Fraud Unprofitable**

Millicent makes electronic fraud unattractive and very difficult. The system was designed to make it virtually impossible to double-spend, counterfeit, or change the value of the script. Millicent transactions, typically a few cents or less, provide little
incentive and a high likelihood of detection for those attempting to steal large amounts of penny-based script.

Digital Equipment Corporation is a world leader in open client/server solutions from personal computing to integrated worldwide information systems. Digital's scalable Alpha and Intel platforms, storage, networking, software and services, together with industry-focused solutions from business partners, help organizations compete and win in today's global marketplace.

**b) Subscript:**

A subscript or superscript is a number, figure, symbol, or indicator that appears smaller than the normal line of type and is set slightly below or above it – subscripts appear at or below the baseline, while superscripts are above. Subscripts and superscripts are perhaps best known for their use in formulas, mathematical expressions, and descriptions of chemical compounds or isotopes, but have many other uses as well.

In professional typography, subscript and superscript characters are not simply ordinary characters reduced in size; to keep them visually similar to the rest of the font, typeface designers make them slightly heavier than a reduced-size character would be. Likewise, the amount that sub or superscripted text is moved from the original baseline varies by typeface and by use.

**Uses**

A single typeface may contain sub- and super-script glyphs at different positions for different uses. The four most common positions are listed here. Because each position is
used in different contexts, not all alphanumerics may be available in all positions. For example, subscript letters on the baseline are quite rare, and many typefaces only provide a limited number of superscripted letters. Despite these differences, all reduced-sized glyphs go by the same generic name of subscript and superscript. Note that the terms subscript and superscript are synonymous with the terms inferior letter (or number) and superior letter (or number), respectively.

**Subscripts which are dropped below the baseline**

Perhaps the most familiar example of subscripts is in chemical formulas. For example, the formula for glucose is C6H12O6 (meaning that it is a molecule with 6 carbon atoms, 12 hydrogen atoms and 6 oxygen atoms).

A subscript can also distinguish between different versions of a subatomic particle. Thus electron, muon, and tau neutrions are denoted $\nu_e$, $\nu_\mu$ and $\nu_\tau$. A particle may be distinguished by multiple subscripts, such as $\Omega^{--b\!b\!b}$ for the triple bottom omega particle.

Similarly, subscripts are also used frequently in mathematics to define different versions of the same variable; for example, in an equation $x_0$ and $x_f$ may indicate the initial and final value of $x$, while $v_{rocket}$ and $v_{observer}$ would stand for the velocities of a rocket and an observer. Commonly, variables with a zero in the subscript are referred to as the variable name followed by "naught". (e.g. $v_0$ would be read, "v-naught")

Subscripts are often used to refer to members in a mathematical sequence or set. For example, in the sequence $O =$
(45, -2, 800), O3 refers to the third member of sequence O, which is 800.

Also in mathematics and computing, subscript can be used to represent the radix, or base, of a written number, especially where multiple bases are used alongside each other. For example, comparing values in hexadecimal, denary, and octal one might write Chex = 12dec = 14oct.

Subscripted numbers dropped below the baseline are also used for the denominators of stacked fractions, like this: 67/68

**Subscripts which are aligned with the baseline**

The only common use of these subscripts is for the denominators of diagonal fractions, like ½ or the signs for percent %, permille ‰, and basis point ‱. Certain standard abbreviations are also composed as diagonal fractions, such as % (care of), % (account of), % (addressed to the subject), or in Spanish % (cada uno/a, "each one").

**Superscripts which typically do not extend above the ascender line**

These superscripts typically share a baseline with numerator digits, the top of which are aligned with the top of the full-height numerals of the base font; lower-case ascenders may extend above

Ordinal indicators are sometimes written as superscripts (1st, 2nd, 3rd rather than 1st, 2nd, 3rd), although many English-language style guides recommend against this use. Other languages use a similar convention, such as 1er or 2e in French, or 4ª and 4º in Italian, Portuguese, and Spanish.
Many abbreviations use superscripts, especially historically. Examples in English include Jos and Wm (for Joseph and William), ye (for the, originally þe), tht or yt (that), yr (your), or maty (majesty). In handwritten shorthand, many abbreviations are still written this way, such as defn (definition), expt (experiment), or govt (government). In French, superscript abbreviations are still quite common, such as Mlle (for Mademoiselle) and Gie (for générale). The standard abbreviation for “number,” №, also uses a superscript. In early modern writing, two-letter abbreviations were sometimes written with the superscript directly above the base letter, as in ſ or ſ.

In early Middle High German, umlauts and other modifications to pronunciation would be indicated by superscript letters placed directly above the letter they modified. Thus the modern umlaut ü was written as û; both vowel and consonants were used in this way, as in ûhéezze or bõsen. In modern typefaces, these letters are usually smaller than other superscripts, and their baseline is slightly above the base font’s midline, making them extend no higher than a typical ordinal indicator.

Superscripts are used for the standard abbreviations for service mark™ and trademark™. The signs for copyright © and registered trademark ® are also sometimes superscripted, depending on the use or the typeface.

On hand-written documents and signs, a monetary amount may be written with the cents value superscripted, as in $8\textsuperscript{00} or 8€\textsuperscript{50}. Often the superscripted numbers will be underlined: $8\textsuperscript{00}, 8€\textsuperscript{50}. The currency sign itself may also be superscripted, as in $80 or 6¢.
Superscripted numerals are used for the numerators of diagonal fractions, like \( \frac{3}{4} \) or the signs for percent %, permille %, and basis point %. Certain standard abbreviations are also composed as diagonal fractions, such as % (care of), \( \% \) (account of), \( \% \) (addressed to the subject), or in Spanish \( \% \) (cada uno/a, "each one").

**Superscripts which typically extend above the ascender line**

Both low and high superscripts can be used to indicate the presence of a footnote in a document, like this or this.\(^{xi}\) Any combination of characters can be used for this purpose; in technical writing footnotes are sometimes composed of letters and numbers together, like this.A.2 The choice of low or high alignment depends on one’s taste, but high-set footnotes tend to be more common, as they stand out more from the text.

In mathematics, high superscripts are used to indicate that one number or variable is raised to the power of another number or variable. Thus \( y^4 \) is \( y \) raised to the fourth power, \( 2x \) is \( 2 \) raised to the power of \( x \), and the famous equation \( E = mc^2 \) includes a term for the speed of light squared.

The charges of ions and subatomic particles are also denoted with superscripts. \( \text{Cl}^- \) is a negatively charged chlorine atom, \( \text{Pb}^{4+} \) is an atom of lead with a charge of positive four, \( e^- \) is an electron, \( e^+ \) is a positron, and \( \mu^+ \) is an antimuon.

Atomic isotopes are written using superscripts. In symbolic form, the number of nucleons is denoted as a superscripted prefix to the chemical symbol (for example \( ^3\text{He} \), \( ^{12}\text{C} \), \( ^{13}\text{C} \), \( ^{131}\text{I} \) and \( ^{238}\text{U} \)). The letters \( m \) or \( f \) may follow the number to indicate metastable or fission isomers, as in \( ^{58}\text{mCo} \) or \( ^{240}\text{fPu} \).
Subscripts and superscripts can also be used together to give more specific information about nuclides. For example, $^{92}\text{U}$ denotes an atom of uranium with 235 nucleons, 92 of which are protons. A chemical symbol can be completely surrounded: $^{6}\text{C}{}^{8}$ is an ion of carbon with 14 nucleons, of which six are protons and 8 are neutrons.

The numerators of stacked fractions (such as $^{34}/^{35}$) usually use high-set superscripts, although some specially designed glyphs keep the top of the numerator aligned with the top of the full-height numerals.

**Software support**

**Desktop publishing**

Many text editing and word processing programs have automatic subscripting and superscripting features, although these programs usually simply use ordinary characters reduced in size and moved up or down – they are not true subscript or superscript glyphs. Professional typesetting programs such as QuarkXPress or Adobe InDesign also have similar features for automatically converting regular type to subscript or superscript. These programs, however, may also offer native OpenType support for the special subscript and superscript glyphs included in many professional typeface packages.
### Comparison of software support

<table>
<thead>
<tr>
<th>Software</th>
<th>OpenType support for professional glyphs?</th>
<th>Default values for glyph transformation (non-professional glyphs)</th>
<th>Keyboard Shortcuts</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>size</td>
<td>subscript position</td>
</tr>
<tr>
<td>OpenOffice 2.3</td>
<td>no</td>
<td>58%</td>
<td>-33%</td>
</tr>
<tr>
<td>Microsoft Word 2002</td>
<td>no</td>
<td>65%</td>
<td>-14.1%</td>
</tr>
<tr>
<td>Adobe Illustrator CS3</td>
<td>yes</td>
<td>58.3%</td>
<td>-33.3%</td>
</tr>
<tr>
<td>Adobe Photoshop CS3</td>
<td>ordinal letters only</td>
<td>58.3%</td>
<td>-33.3%</td>
</tr>
</tbody>
</table>

**HTML**

In HTML and Wiki syntax, subscript text is produced by putting it inside the tags `<sub>` and `</sub>`. Similarly, superscripts are produced with `<sup>` and `</sup>`. The exact size and position of the resulting characters will vary by font and browser, but are usually reduced to around 75% original size. Note that superscripts are usually placed too high for many typographic purposes.

**TeX**

In TeX’s mathematics mode (as used in MediaWiki), subscripts are typeset with the underscore, while superscripts are made with the caret. Thus `$X_{ab}$` produces Xab, and `$X^{ab}$` produces Xab.

**Unicode**

Unicode defines subscript and superscript characters in
several areas. Note, however, that fonts which include these characters may align them quite differently: subscripts may be at or below the baseline, while superscripts may stop at the cap line or extend above it. The same font may even align letters and numbers in different ways. Because of these inconsistencies, these glyphs may not be suitable for some purposes.

**Unicode includes subscript and superscript characters in the following blocks:**

- The Latin-1 Supplement block contains the feminine and masculine ordinal indicators 脩 and _EOF, superscript numerals ¹, ², and ³, the permille sign ‰, and the precomposed diagonal fractions ½, ¼, and ¾. The copyright © and registered trademark signs ® are also in this block.

- The General Punctuation block contains the permille sign ‰ and the per-ten-thousand sign ′.

- The Number Forms block contains several pre-composed diagonal fractions: ⅓ ⅔ ⅕ ⅖ ⅗ ⅘ ⅙ ⅚ ⅛ ⅜ ⅝ ⅞ ⅟.

- The Combining Diacritical Marks block contains medieval superscript letter diacritics. These letters are written directly above other letters appearing in medieval Germanic manuscripts, and so these glyphs do not include spacing, foreexample û. They are shown here over a long string of periods: ..................

- The Subscripts and Superscripts block contains superscripts of numbers, mathematical symbols, and a few letters: ⁰ ¹ ² ³ ⁴ ⁵ ⁶ ⁷ ⁸ ⁹ + − = ( ) ₀ ₁ ₂ ₃ ₄ ₅ ₆ ₇ ₈ ⁹ + − = ( )

433
• The Letterlike Symbols block contains a few symbols composed of subscript and superscript characters: % % % %

• The Spacing Modifier Letters block has superscripted letters and symbols used for phonetic transcription: ʰ ʱ ʲ ʳ ʴ ʵ ʶ ʷ ʸ ˠ ˡ ˢ ˣ ˤ

• The Phonetic Extensions block has several sub- and superscripted letters and symbols:

• The Phonetic Extensions Supplement block has a few more:

Consolidated for cut-and-pasting purposes, the Unicode standard defines complete sub- and super-scripts for numbers and common mathematical symbols (₀ ₁ ₂ ₃ ₄ ₅ ₆ ₇ ₈ ₉ + − = () − = ( ) ), a full superscript latin lowercase alphabet except q (можно взять из нижнего списка), a limited uppercase latin alphabet (можно взять из нижнего списка), a few subscripted lowercase letters (можно взять из нижнего списка), and some greek letters (можно взять из нижнего списка). Note that since these glyphs come from different ranges, they may not be of the same size and position, depending on the typeface.

Open Type

One of the advanced features of OpenType typefaces is support for professionally designed subscript and superscript
glyphs. Exactly which glyphs are included varies by typeface; some have only basic support for numerals, while others contain a full set of letters, numerals, and punctuation. Since many of these glyphs are not included in Unicode, they are typically placed in the Unicode Private Use Area.

c) pay world:

The payward micropayment system was proposed by Ron Rivest and Adi Shamir in the Same paper that they proposed Micro Mint. In Payward users generate their on ‘coins’ or paywards, which are sent to vendors and then verified by brokers. Each user has a certificate “a block containing the user’s identity and public key, digitally signed by a broker. When a user wishes to make a purchase at a vendor for the first time a day. She First randomly picks a payword "seed". \( w_n \), where is a reasonable estimation of purchase a user would make at a typical vendor in a day. The user then computes payword "chain", by reputedly hashing \( w_n \) \( w_{i-1} = h(w_i) \), where \( i = 1, \ldots, n \). Before making a purchase, the user sends the vendor a digitally signed commitment to \( w_0 \), the "root" of the payword chain. The user then send the vendor \( w_i \) through \( w_m' \) where \( m \) is the number of coins the user wishes to spend. The vendor can easily verify this chain by hashing \( w_m \) \( m \) times until be reaches \( w_0 \). At the end of each day the vendor sends the broker the user’s commitment to \( w_0 \) along \( w_m' \) which the broker uses to credit the vendor’s account for \( m \) coins.

d) hash chain trees:

CoinMint is designed to be hash function independent, however for this implementation, we will use the DES encryption system to generate coins.
To use DES as a MicroMint hash function, we use a fixed plaintext initialization and iterate the keys as the inputs. The represents our output.

e) micro-mint:

The MicroMint micropayment scheme is designed to be small and efficient without using and public-key cryptography. Since public-key cryptography can present a significant computational burden, this scheme does without it and relies on other mechanisms to accomplish authentication. Like many micropayment schemes, MicroMint is token-based a ‘digital coin’ is purchased by consumers from a central authority, spent at a vendor, and finally redeemed by the same central authority for currency.

g) Others: There are a number of other micropayment systems in various stages of development, from proposals in academic literature to systems currently in commercial trials. While most micropayment systems share same goal, the manner in which they achieve those goals can vary considerably.

3. Mobile payments:

Mobile payment is a new and rapidly-adopting alternative payment method–especially in Asia and Europe. Instead of paying with cash, cheque or credit cards, a consumer can use a mobile phone to pay for a wide range of services and digital or hard goods such as:

- Music, videos, ringtones, online game subscription or items, wallapers and other digital goods.
- Transportation fare (bus, subway or train), parking meters and other services.
• Books, magazines, tickets and other hard goods.

There are four primary models for mobile payments:

• Premium SMS based transactional payments
• Direct Mobile Billing
• Mobile web payments (WAP)
• Contactless NFC (Near Field Communication)

Mobile payment has been well adopted in many parts of Europe and Asia. Combined market for all types of mobile payments is expected to reach more than $600B globally by 2013, while mobile payment market for goods and services, excluding contactless NFC transactions and money transfers, is expected to exceed $300B globally by 2013.

Mobile payment (MP) is that type of payment transaction processing in the course of which - within an electronic procedure - (at least) the payer employs mobile communication techniques in conjunction with mobile devices for initiation, authorization or realization of payment

a) Mobile Internet Architectures:

There are two main issues that can be identified regarding the formal structure of the network over which mobile and transient devices must currently operate:

1. The current implementation of the Internet is based on location and association aware communication that in effect resembles a virtual circuit path communication.

   The problem is that in high latency, variable and mobile networks both ends of the circuit are frequently changing
which in turn results in extensive retransmission and delays as well as communication failures.

2. The current network communication schema links the identification of the communication devices to a particular location at the physical level by means of the IP association and distribution. Real migration and mobility are therefore hard to fit in a rigid primarily static hierarchical structure.

3. The current internet does not natively provide any off-line communication mechanisms for transient users moving across multiple networks with intermediate disconnections.

We propose a new paradigm to transient communication networks. We essentially contend that mobile and transient devices should be part of a "Green Network", a transient mobile architecture that treats nodes and traffic as Digital Entities. The Digital Entities are identified with unique and persistent identifiers. Traffic is treated as data pools being exchanged between distinct entities by means of a replicating self propagating self adjusting network. The Green Network effectively isolates the data exchange and delivery from the communicating parties. Rather than having the end-points coordinate and adjust the communication by retransmitting and controlling the flow of their traffic; these nodes are now part of a network of dual purpose entities uniquely identified with location independent identifiers, that produce and route pools of data (pods). These PODs are in turn identified by persistent identifiers as well. Once a certain POD has been deposited into the Green Network, it (the network) will
assume the responsibility of routing the traffic to fit the end nodes movement given the current characteristics of the network.

Data is not moved towards a particular destination but rather routed into the Area of Influence of a particular device. The Area of Influence (AoI) is expressed in terms of the general area of communication that a particular ad-hoc node is known to be associated with. This way a roaming node will have the data delivered to it through its current AoI. This paper reports on current status of our work, describes the full scope of the architecture and outlines our future research path to complete a fully distributed implementation of this architecture. Areas of Influence are composed by a set of nodes that form an ever expanding and growing network that merges several layers and levels. These nodes and the Aolis they form are part of the network core and edge. They are in fact capable to expand this edge seamlessly to incorporate even more nodes into the network.

The overall Mobile Transient Network builds on the original logical model of the internet to form a logical network that allows the effective merging of heterogeneous networks without forcing them to modify their communication protocol but rather their logical coordination mechanism.

b) Mobile network operator as bankers: As the RBI (Reserve Bank of India) act as a banker’s bank, and operates the working of other banks. Same as mobile network operator works to mobile customers. It takes responsibility of all the processing of the network, so that the network process can work properly without any disturbance. Mobile network operator takes care of all the customers sake and gives a good services to their customers.
e) Credit card based system:

A credit card is a small plastic card issued to users of a system of payment. It allows its holder to buy goods and services based on the holder's promise to pay for these goods and services. The issuer of the card grants a line of credit to the consumer (or the user) from which the user can borrow money for payment to a merchant or as a cash advance to the user. Usage of the term "credit card" to imply a credit card account is a metonym.

A credit card is different from a charge card: a charge card requires the balance to be paid in full each month. In contrast, credit cards allow the consumers a continuing balance of debt, subject to interest being charged. Most credit cards are issued by banks or credit unions, and are the shape and size specified by the ISO/IEC 7810 standard as ID-1. This is defined as 85.60 × 53.98 mm (33/8 × 21/8 in) in size.

How credit cards work

Credit cards are issued after an account has been approved by the credit provider, after which cardholders can use it to make purchases at merchants accepting that card.

When a purchase is made, the credit card user agrees to pay the card issuer. The cardholder indicates consent to pay by signing a receipt with a record of the card details and indicating the amount to be paid or by entering a personal identification number (PIN). Also, many merchants now accept verbal authorizations via telephone and electronic authorization using the Internet, known as a 'Card/Cardholder Not Present' (CNP) transaction.
Electronic verification systems allow merchants to verify in a few seconds that the card is valid and the credit card customer has sufficient credit to cover the purchase, allowing the verification to happen at time of purchase. The verification is performed using a credit card payment terminal or Point of Sale (POS) system with a communications link to the merchant's acquiring bank. Data from the card is obtained from a magnetic stripe or chip on the card; the latter system is called Chip and PIN in the United Kingdom and Ireland, and is implemented as an EMV card.

For transactions at which the buyer is not present and the card not shown (e.g., e-commerce, mail order, and telephone sales), merchants additionally verify that the customer is in physical possession of the card and is the authorised user by asking for additional information such as the security code printed on the back of the card, date of expiry, and billing address.

Each month, the credit card user is sent a statement indicating the purchases undertaken with the card, any outstanding fees, and the total amount owed. After receiving the statement, the cardholder may dispute any charges that he or she thinks are incorrect (see Fair Credit Billing Act for details of the US regulations). Otherwise, the cardholder must pay a defined minimum proportion of the bill by a due date, or may choose to pay a higher amount up to the entire amount owed. The credit issuer charges interest on the amount owed if the balance is not paid in full (typically at a much higher rate than most other forms of debt). Some
financial institutions can arrange for automatic payments to be deducted from the user’s bank accounts, thus avoiding late payment altogether as long as the cardholder has sufficient funds.

Interest charges

Credit card issuers usually waive interest charges if the balance is paid in full each month, but typically will charge full interest on the entire outstanding balance from the date of each purchase if the total balance is not paid.

For example, if a user had a $1,000 transaction and repaid it in full within this grace period, there would be no interest charged. If, however, even $1.00 of the total amount remained unpaid, interest would be charged on the $1,000 from the date of purchase until the payment is received. The precise manner in which interest is charged is usually detailed in a cardholder agreement which may be summarized on the back of the monthly statement. The general calculation formula most financial institutions use to
determine the amount of interest to be charged is APR/100 x ADB/365 x number of days revolved. Take the Annual percentage rate (APR) and divide by 100 then multiply to the amount of the average daily balance (ADB) divided by 365 and then take this total and multiply by the total number of days the amount revolved before payment was made on the account. Financial institutions refer to interest charged back to the original time of the transaction and up to the time a payment was made, if not in full, as RRFC or residual retail finance charge. Thus after an amount has revolved and a payment has been made, the user of the card will still receive interest charges on their statement after paying the next statement in full (in fact the statement may only have a charge for interest that collected up until the date the full balance was paid...i.e. when the balance stopped revolving).

The credit card may simply serve as a form of revolving credit, or it may become a complicated financial instrument with multiple balance segments each at a different interest rate, possibly with a single umbrella credit limit, or with separate credit limits applicable to the various balance segments. Usually this compartmentalization is the result of special incentive offers from the issuing bank, to encourage balance transfers from cards of other issuers. In the event that several interest rates apply to various balance segments, payment allocation is generally at the discretion of the issuing bank, and payments will therefore usually be allocated towards the lowest rate balances until paid in full before any money is paid towards higher rate balances.
Interest rates can vary considerably from card to card, and the interest rate on a particular card may jump dramatically if the card user is late with a payment on that card or any other credit instrument, or even if the issuing bank decides to raise its revenue.

Benefits to customers

The main benefit to each customer is convenience. Compared to debit cards and checks, a credit card allows small short-term loans to be quickly made to a customer who need not calculate a balance remaining before every transaction, provided the total charges do not exceed the maximum credit line for the card. Credit cards also provide more fraud protection than debit cards. In the UK for example, the bank is jointly liable with the merchant for purchases of defective products over £100.

Many credit cards offer rewards and benefits packages, such as offering enhanced product warranties at no cost, free loss/damage coverage on new purchases, and points which may be redeemed for cash, products, or airline tickets. Additionally, carrying a credit card may be a convenience to some customers as it eliminates the need to carry any cash for most purposes.

Parties involved

- **Cardholder**: The holder of the card used to make a purchase; the consumer.

- **Card-issuing bank**: The financial institution or other organization that issued the credit card to the cardholder.
This bank bills the consumer for repayment and bears the risk that the card is used fraudulently. American Express and Discover were previously the only card-issuing banks for their respective brands, but as of 2007, this is no longer the case. Cards issued by banks to cardholders in a different country are known as offshore credit cards.

- **Merchant**: The individual or business accepting credit card payments for products or services sold to the cardholder.

- **Acquiring bank**: The financial institution accepting payment for the products or services on behalf of the merchant.

- **Independent sales organization**: Resellers (to merchants) of the services of the acquiring bank.

- **Merchant account**: This could refer to the acquiring bank or the independent sales organization, but in general is the organization that the merchant deals with.

- **Credit Card association**: An association of card-issuing banks such as Visa, MasterCard, Discover, American Express, etc. that set transaction terms for merchants, card-issuing banks, and acquiring banks.

- **Transaction network**: The system that implements the mechanics of the electronic transactions. May be operated by an independent company, and one company may operate multiple networks.

- **Affinity partner**: Some institutions lend their names to an issuer to attract customers that have a strong relationship
with that institution, and get paid a fee or a percentage of the balance for each card issued using their name. Examples of typical affinity partners are sports teams, universities, charities, professional organizations and major retailers.

Transaction steps

- **Authorization**: The cardholder pays for the purchase and the merchant submits the transaction to the acquirer (acquiring bank). The acquirer verifies the credit card number, the transaction type and the amount with the issuer (Card-issuing bank) and reserves that amount of the cardholder's credit limit for the merchant. An authorization will generate an approval code, which the merchant stores with the transaction.

- **Batching**: Authorized transactions are stored in "batches", which are sent to the acquirer. Batches are typically submitted once per day at the end of the business day. If a transaction is not submitted in the batch, the authorization will stay valid for a period determined by the issuer, after which the held amount will be returned back to the cardholder's available credit (see authorization hold). Some transactions may be submitted in the batch without prior authorizations; these are either transactions falling under the merchant's floor limit or ones where the authorization was unsuccessful but the merchant still attempts to force the transaction through. (Such may be the case when the cardholder is not
present but owes the merchant additional money, such as extending a hotel stay or car rental.)

- **Clearing and Settlement:** The acquirer sends the batch transactions through the credit card association, which debits the issuers for payment and credits the acquirer. Essentially, the issuer pays the acquirer for the transaction.

- **Funding:** Once the acquirer has been paid, the acquirer pays the merchant. The merchant receives the amount totaling the funds in the batch minus either the "discount rate," "mid-qualified rate", or "non-qualified rate" which are tiers of fees the merchant pays the acquirer for processing the transactions.

- **Chargebacks:** A chargeback is an event in which money in a merchant account is held due to a dispute relating to the transaction. Chargebacks are typically initiated by the cardholder. In the event of a chargeback, the issuer returns the transaction to the acquirer for resolution. The acquirer then forwards the chargeback to the merchant, who must either accept the chargeback or contest it. A merchant is responsible for the chargeback only if she has violated the card acceptance procedures as per the merchant agreement with card acquirers.

**Secured credit cards**

A secured credit card is a type of credit card secured by a deposit account owned by the cardholder. Typically, the cardholder must deposit between 100% and 200% of the
total amount of credit desired. Thus if the cardholder puts down $1000, they will be given credit in the range of $500–$1000. In some cases, credit card issuers will offer incentives even on their secured card portfolios. In these cases, the deposit required may be significantly less than the required credit limit, and can be as low as 10% of the desired credit limit. This deposit is held in a special savings account. Credit card issuers offer this because they have noticed that delinquencies were notably reduced when the customer perceives something to lose if the balance is not repaid.

The cardholder of a secured credit card is still expected to make regular payments, as with a regular credit card, but should they default on a payment, the card issuer has the option of recovering the cost of the purchases paid to the merchants out of the deposit. The advantage of the secured card for an individual with negative or no credit history is that most companies report regularly to the major credit bureaus. This allows for building of positive credit history.

Although the deposit is in the hands of the credit card issuer as security in the event of default by the consumer, the deposit will not be debited simply for missing one or two payments. Usually the deposit is only used as an offset when the account is closed, either at the request of the customer or due to severe delinquency (150 to 180 days). This means that an account which is less than 150 days delinquent will continue to accrue interest and fees, and could result in a balance which is much higher than the actual credit limit on the card. In these cases the total debt may far exceed the
original deposit and the cardholder not only forfeits their deposit but is left with an additional debt.

Most of these conditions are usually described in a cardholder agreement which the cardholder signs when their account is opened.

Secured credit cards are an option to allow a person with a poor credit history or no credit history to have a credit card which might not otherwise be available. They are often offered as a means of rebuilding one’s credit. Fees and service charges for secured credit cards often exceed those charged for ordinary non-secured credit cards, however, for people in certain situations, (for example, after charging off on other credit cards, or people with a long history of delinquency on various forms of debt), secured cards can often be less expensive in total cost than unsecured credit cards, even including the security deposit.

Sometimes a credit card will be secured by the equity in the borrower's home.

**Prepaid "credit" cards**

A prepaid credit card is not a true credit card, since no credit is offered by the card issuer: the card-holder spends money which has been "stored" via a prior deposit by the card-holder or someone else, such as a parent or employer. However, it carries a credit-card brand (Visa, MasterCard, American Express or Discover) and can be used in similar ways just as though it were a regular credit card. Unlike debit cards, prepaid credit cards do not require a PIN.
After purchasing the card, the cardholder loads the account with any amount of money, up to the predetermined card limit and then uses the card to make purchases the same way as a typical credit card. Prepaid cards can be issued to minors (above 13) since there is no credit line involved. The main advantage over secured credit cards (see above section) is that you are not required to come up with $500 or more to open an account. With prepaid credit cards you are not charged any interest but you are often charged a purchasing fee plus monthly fees after an arbitrary time period. Many other fees also usually apply to a prepaid card.

Prepaid credit cards are sometimes marketed to teenagers for shopping online without having their parents complete the transaction.

Because of the many fees that apply to obtaining and using credit-card-branded prepaid cards, the Financial Consumer Agency of Canada describes them as "an expensive way to spend your own money". The agency publishes a booklet, "Pre-paid cards", which explains the advantages and disadvantages of this type of prepaid card.