Electronic Cash Payment Protocols and Systems

Speaker: Jerry Gao Ph.D.

San Jose State University
email: jerrygao@email.sjsu.edu
URL: http://www.engr.sjsu.edu/gaojerry

May, 2000

Presentation Outline

- ***Overview of electronic cash system***
- ***Ecash (Digital Cash)***
- ***NetCash***
- ***Modex***
- ***Project CAFÉ***
- ***Comparisons and summary***

Overview of Electronic Cash Payment Protocols and Systems

What is cash payment?

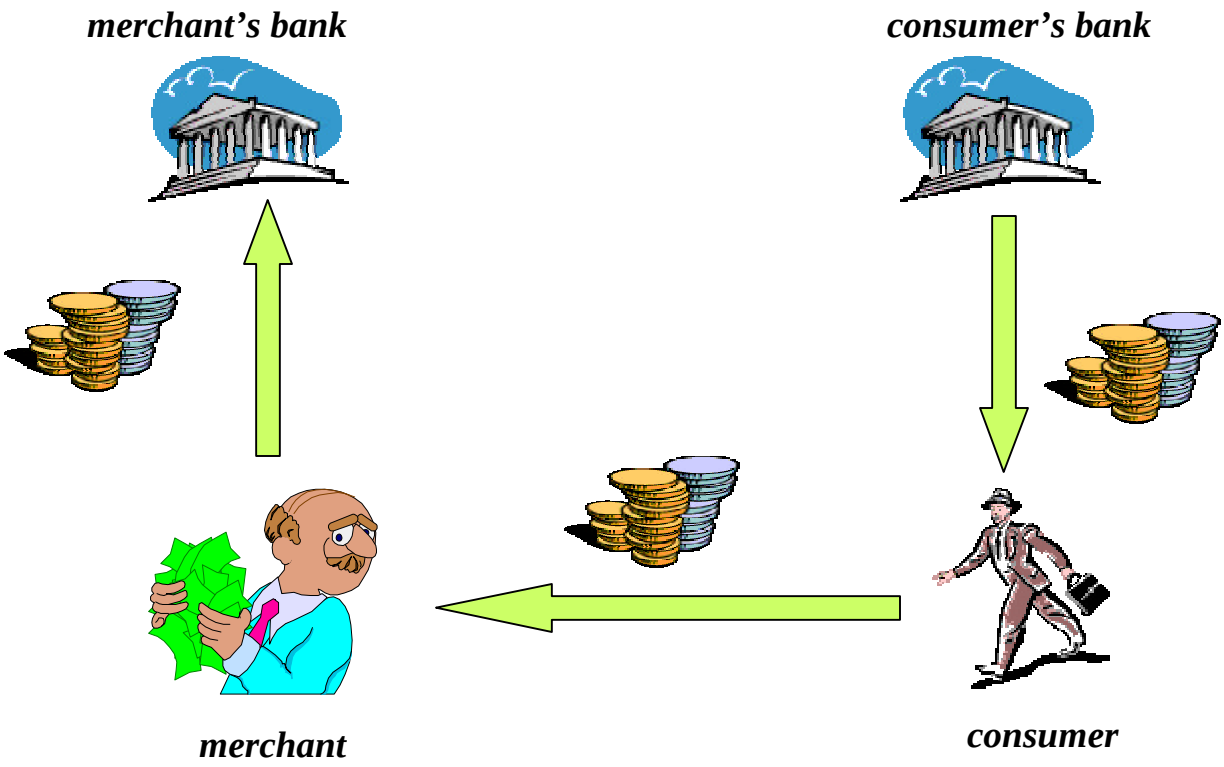
- Cash payment is currently most popular form in conventional payment system in the world.
- Currently cash payment involves 75% - 95% of all transactions are paid in cash..
- Transactions are paid in a cash form (such as $ bill) from a buyer to a seller.

An electronic cash payment system usually is developed based on an electronic payment protocol which supports a series of payment transactions using electronic tokens or coins issued by a third party.

There are three types of users:
- a payer or consumer
- a payee, such as a merchant
- a financial network with whom both payer and payee have accounts.

Jerry Gao Ph.D. 5/2000

Overview of Electronic Cash Payment Protocols and Systems



Jerry Gao Ph.D. 5/2000

Overview of Electronic Cash Payment Protocols and Systems

The basic attributes of cash payment by Donal O'mahony[1]:

- Acceptability: Cash almost universally acceptable as a form of payment, regardless of the transaction amount.

- Guaranteed payment: cash guarantees the payment after the transaction is over. There is no risk of it been rejected or bounced.

- No transaction charges: cash is handled from buyers to sellers with no transaction charges.

- Anonymity: many other forms of payment involve a paper trail linking either or both parties with the transactions. Cash allows transactions take place anonymously.

Jerry Gao Ph.D. 5/2000

Actors Involved in Electronic Cash Payment Systems

- Customers: Customers use the digital cash payment systems to make purchases.

- Dealers: Dealers have to bear the costs of payment transactions.

- Providers for digital payment systems:
Providers are intermediaries between dealers and financial institutions. They provide services and training.

- Development vendors for digital payment systems:

- Financial institutions:
Banking systems or organizations who use electronic payment systems.

- Trust Centers:
They control digital signature keys, and help to secure customer confidence in certain payment systems. They are responsible for the integrity of transmitted data and authenticity of contractors.

Basic Requirements for Electronic Cash Payment Systems

- Digital money:
Payment systems must provide customers and private households with acceptable digital money.

- Security:
Ensure the security of transactions and information privacy of users.

- Scalability:
A large number of customers and concurrent transactions should be handled in a scalable manner.

- Efficient and effective:
Payment systems must support efficient and effective payment processing and accounting services for small payment transactions.

- Simple and lost cost:
Payment systems must provide customers with simple and low cost transparent transactions.

Basic Requirements for Electronic Cash Payment Systems

- Anonymous:
Usually, customers wish to stay anonymous for all involved transactions..

- Double spending:
Digital coins consists of a number of bits. Payment systems must be able to recognize and/or prevent repeated payments with the same digital coin.

- Exchange:
Digital money should be convertible into "real" money whenever necessary.

- Store:
Digital money must be stored locally on hard disks or other media.

- Value:
Digital cash payment systems must provide a large number of digital coins for circulation and perform authentication checking.

Advantages of Electronic Cash Payment Systems

- ***Saved time:***
  - ***Reduce transaction process time***
  - ***Speed up transaction processes***

- ***Reduced costs:***
  - ***Reduce transaction costs***
  - ***Reduce cash distribution costs***

- ***Flexibility:***
  - ***Digital cash can take many forms, including prepaid cards***
  - ***Digital cash can be converted into different currencies***

- ***Reduce cash distribution risk:***
  - ***Reduce the regular cash distribution risk***

- ***Error free and efficient:***
  - ***Reduce transaction errors***

Special Features of Electronic Payment Protocols

Features of electronic cashes:

- Portable, divisible, recognizable, untraceable, and independent from physical locations.

Important features of electronic cash payment protocols and systems:

- Anonymity: *This ensure that no detailed cash transactions for customer are traceable. Even sellers do not know the identity of customers involved in the purchases.*

- Liquidity: *Digital cash have to be accepted by all concerned economic agents as a payment method.*

- Prepaid cards:
Buyers can buy prepaid cards that are accepted by special sellers.

- Electronic payment processing: all transactions are processed electronically.

Transactions Types in Electronic Cash Payment Systems

Three types of transactions:

- Withdrawal: the payer transfers some of money from the bank account to his or her payment card.

- Payment: the payer transfers the money from the card to the payee.

- Deposit: the payee transfers the money received to the bank account.

Two types of implementations:

- On-line payment: --> the merchant calls the bank and verifies the validity of consumer's token or electronic coin before accepting the payment and delivering the merchandise.

- Off-line payment: --> the merchant submits consumer's payment for verification and deposit sometime after the payment transaction is completed.

Electronic Cash Payment Protocol: ECash

What is Ecash?

Ecash was developed to allow fully anonymous secure electronic cash to be used on the Internet to support online trading between buyers and sellers.

Overview of Ecash:

- Ecash is a payment protocol for anonymous digital money on the Internet.

- It is developed by DigiCash Co, of Amsterdam, The Netherlands.

- It is currently implemented and offered by Mark Twain Bank, St. Louis since 1995.

- DeutscheBank Ag, Frankfurt (Main) offers Ecash as a pilot project to its customers since October 1997.

Electronic Cash Payment Protocol: Ecash

Ecash model:

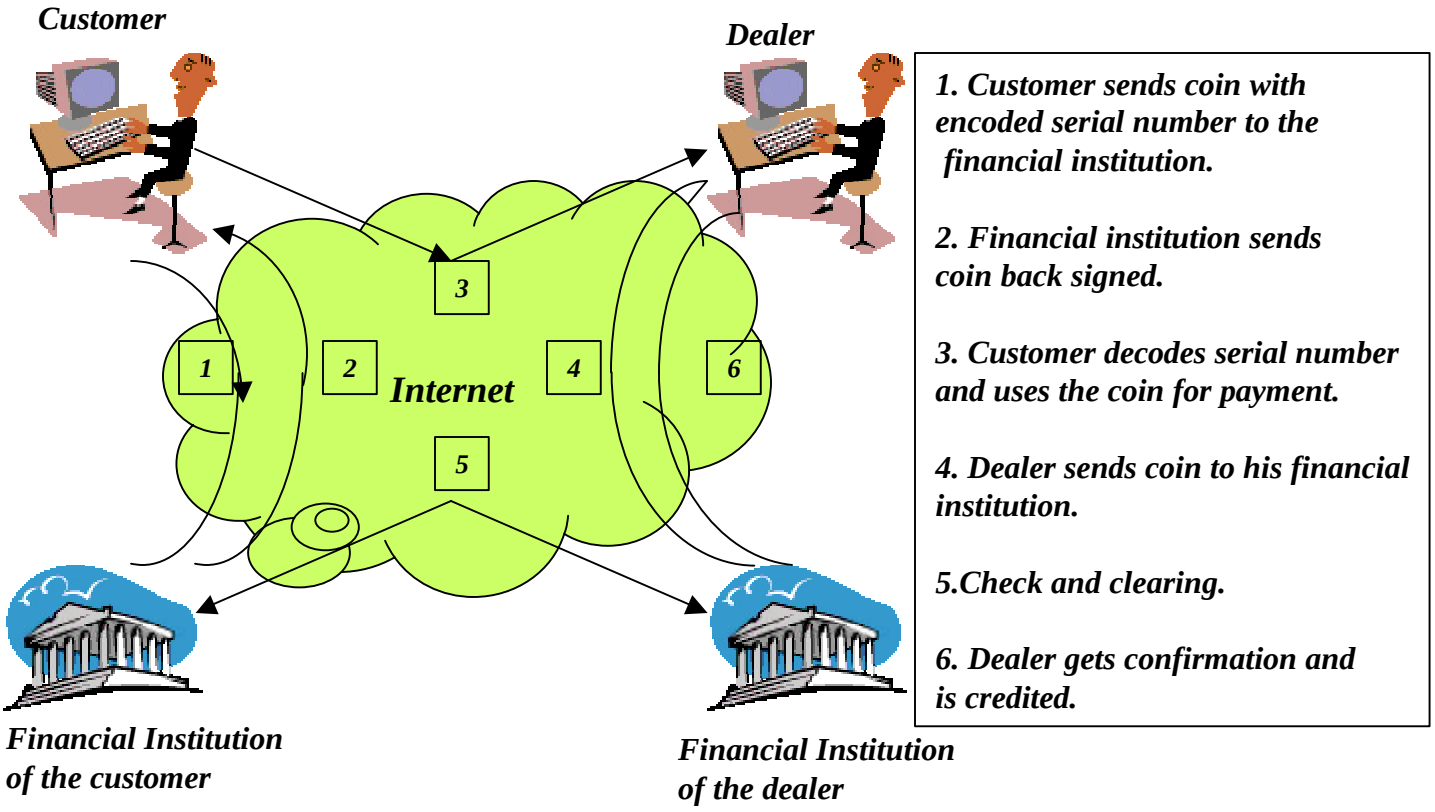
Three participants are involved in Ecash payment model:
clients, merchants and banks.

-- Client wallet software:
- clients have Ecash wallet software (cyberwllet) on their computers.
- they can use Ecoins in their wallet to make purchases from merchants.
- withdraw coins from their accounts in a Ecash bank.
- store and manage client's coins, track all transactions.

-- Merchant software:
- accept and process payments
- interact with Ecash bank to perform validation and authentication
- sell items and generate receipts.

-- Banks: clients and merchants have accounts at an Ecash bank.
- manage and maintain accounts of clients and merchants

Electronic Cash Payment Process with Ecash



1. Customer sends coin with encoded serial number to the financial institution.

2. Financial institution sends coin back signed.

3. Customer decodes serial number and uses the coin for payment.

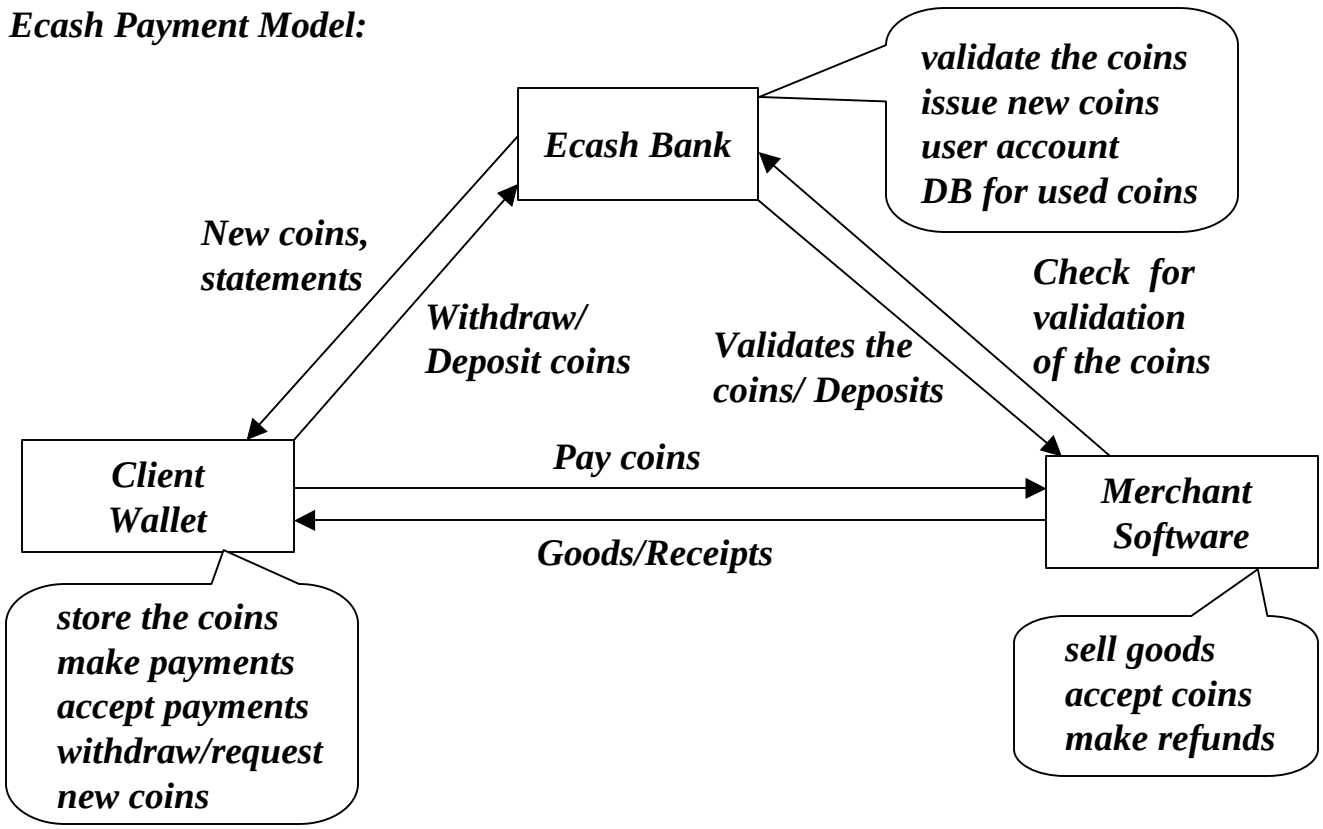
4. Dealer sends coin to his financial institution.

5.Check and clearing.

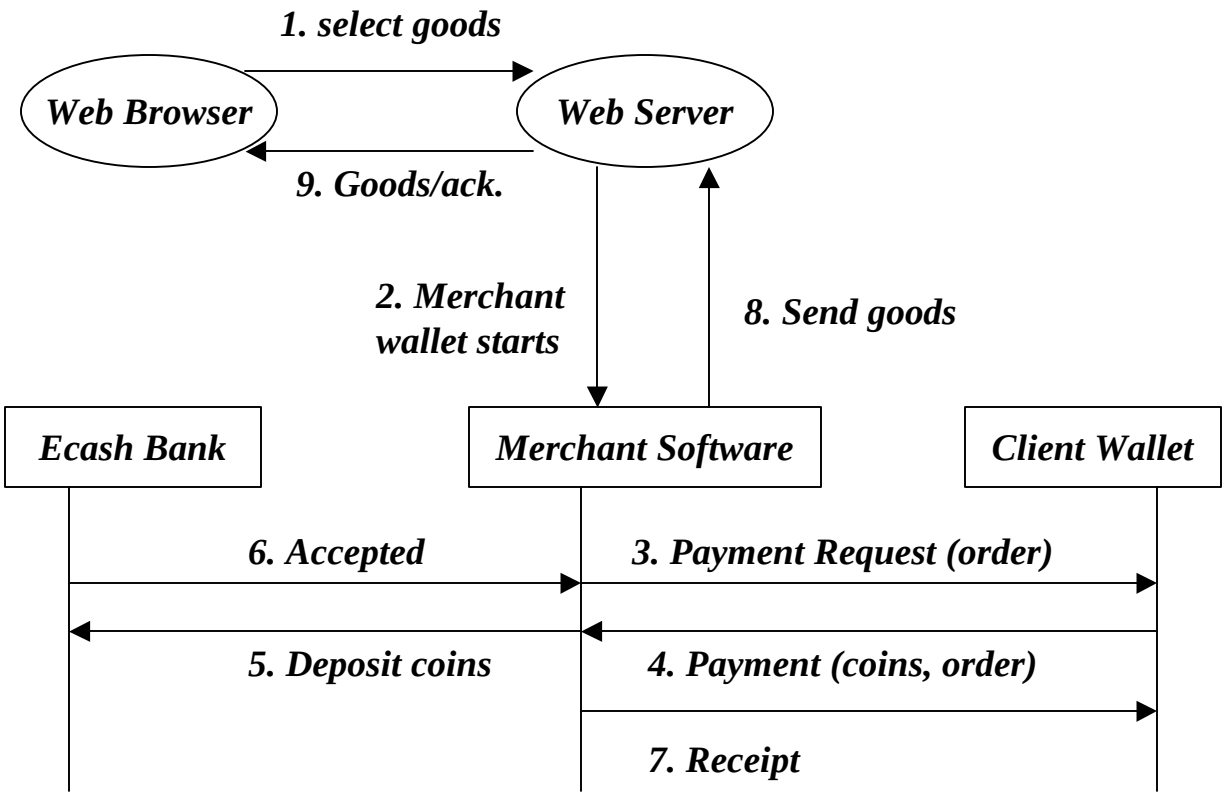
6. Dealer gets confirmation and is credited.

Electronic Cash Payment Protocol: Ecash

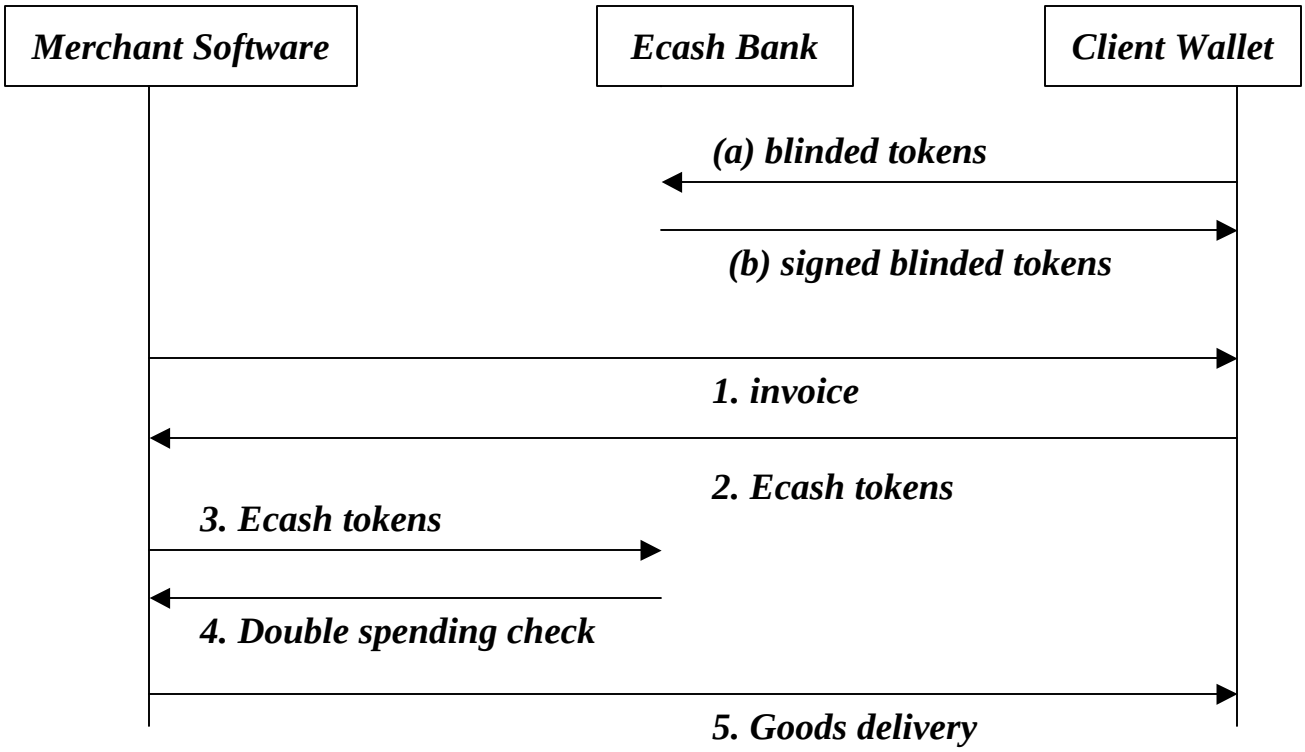
Ecash Payment Model:



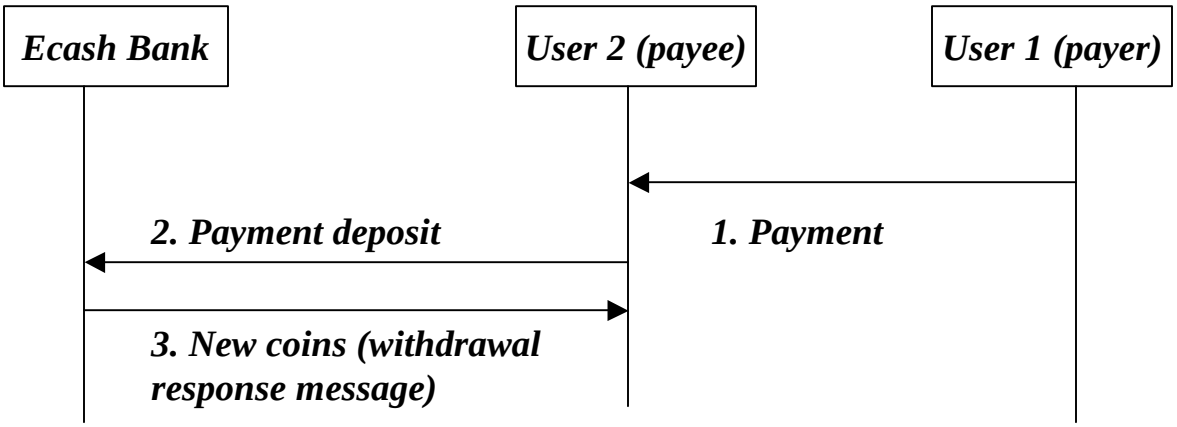
Electronic Cash Payment Protocol: ECash



Electronic Cash Payment Protocol: ECash



Electronic Cash Payment Protocol: ECash



Electronic Cash Payment Protocol: ECash

- Ecash Coins:

- Ecash coins are pieces of data that can be copied.

- The value of Ecash coins cannot be included with the serial number in the fields of the coin.

- Use a different signature key for each coin denomination.

Example: $1 Coin = Serial#, keyversion, {Serial#} SK Bank's $1 Key

- Security mechanisms:

- using RSA public-key cryptography.

- 'blind signature' is the foundation of Ecash privacy feature.

- Every user in the system has their own public/private key pair.

- Double-spending prevention:

- To ensure that a serial number is not spent twice, the minting bank must record every coin that is deposited back to that bank.

A) be signed, with any denominational signature, by the bank.
B) Have an expiry date associated with it that is later than the present date.
C) Not appear in the DB of spent coins.

Electronic Cash Payment Protocol: ECash

Scrip Message Structure

Vendor	*Value*	*Scrip-id*	*customer-id*	*expiration-date*	*info*	*certificate*

Electronic Cash Payment Protocol: NetCash

What is NetCash?

- Netcash is an online electronic cash system, for open networks.
- It was developed at Information Sciences Institute of the University of Southern California.

Overview of NetCash:

- Users can make and accept payments using NetCash.

- Both asymmetric and symmetric cryptography are used to provide the network security of the system to limit fraud.

- The system use multiple currency servers that mint and issue electronic coins to the users of the system, accepting electronic checks in payment for them.

Electronic Cash Payment Protocol: NetCash

NetCash model:

Three participants are involved in NetCash payment model:
tbuyers (or clients), merchants, and currency servers.

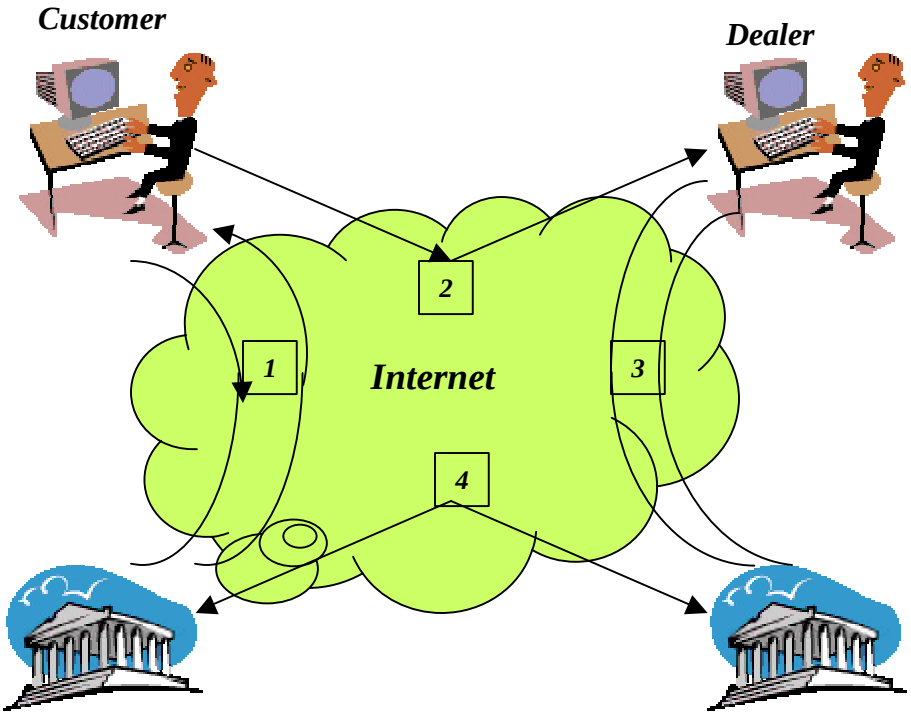
Four services are provided:

- Verifying coins, to prevent double spending.
- Issuing coins in return for payment by electronic check.
- Buying back coins, giving an electronic check in return.
- Exchanging valid coins for new ones with some anonymity.

NetCheque is proposed to provide the electronic check infrastructure required to bring monetary value into and out of the NetCash system.

- Clients can buy and sell NetCash coins in exchange for electronic checks.
- NetCash servers can use electronic checks to settle debts between themselves,

Electronic Cash Payment Process with NetCash



1. Customer gets coin by payment (e.g. by credit card, check)

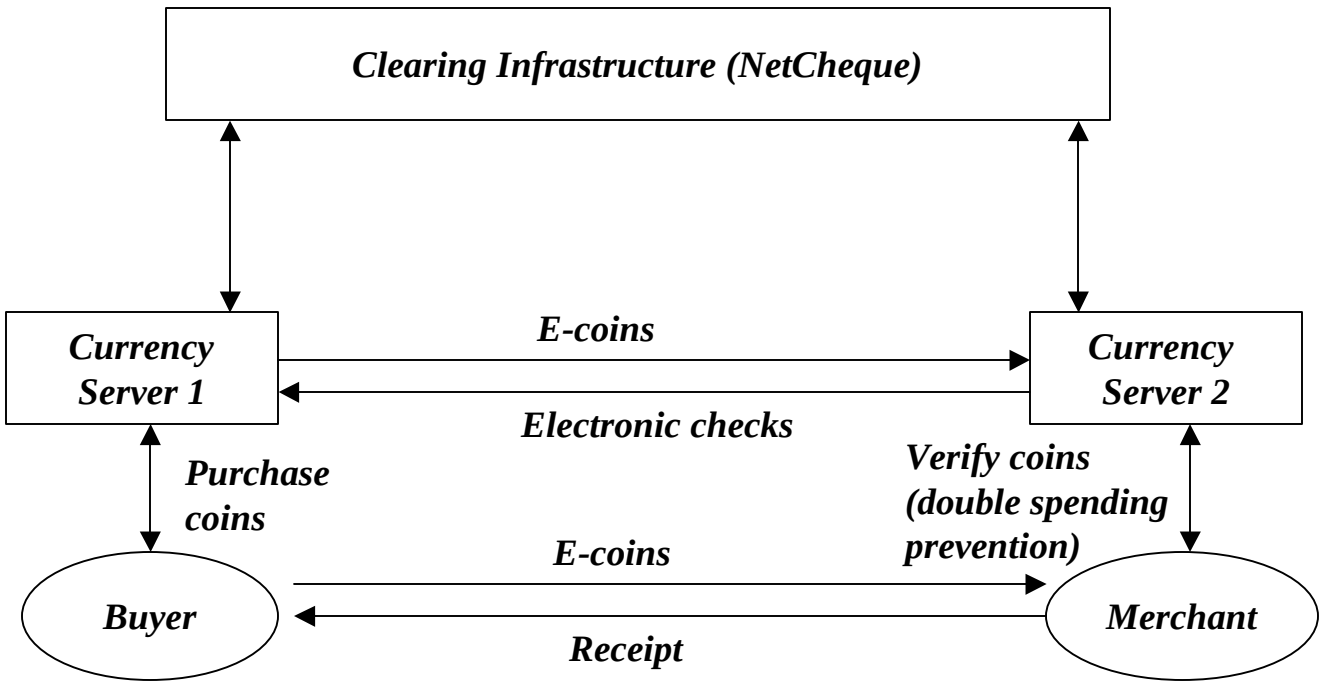
2. Customer sends coins encoded in an asymmetric way to the dealer.

3. Dealer presents coins and gets new coins or is credited. Dealer sends confirmation to the customer.

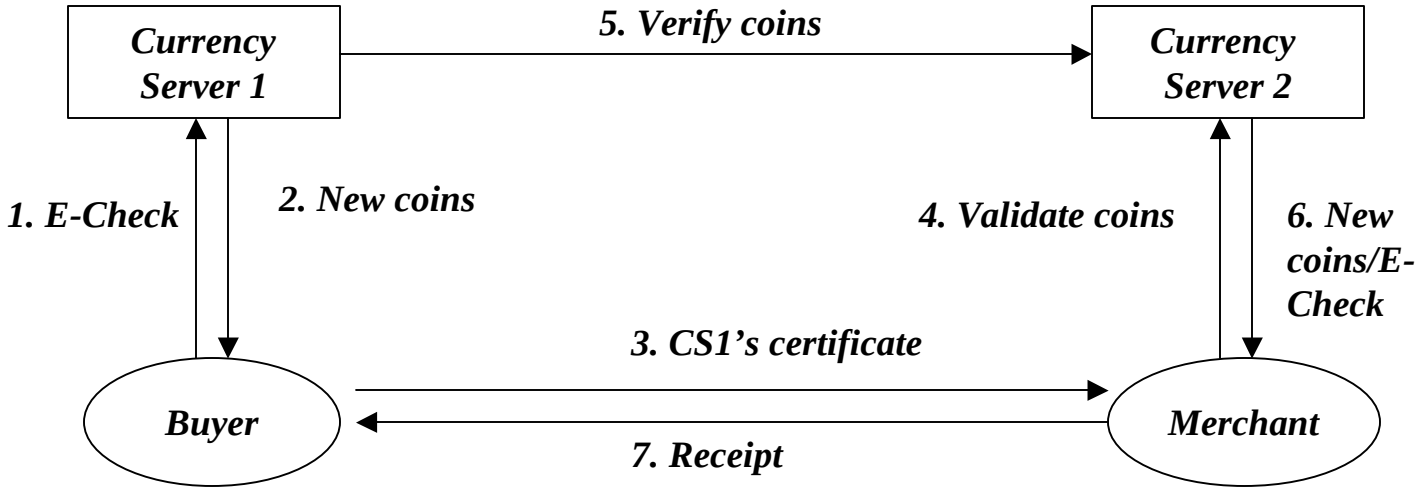
4.Clearing by financial institution.

Electronic Cash Payment Protocol: NetCash

NetCash Payment System:



Electronic Cash Payment Protocol: NetCash



Making a purchase with NetCash

Electronic Cash Payment Protocol: NetCash

A NetCash coin has the following form:

- CS_name: - name of the minting currency server.

- CS addr: - network address of the minting currency server.

- Expiry: - the date on which the coin becomes invalid..

- Serial #: - a unique identifier of the coin to the minting currency server.

- Value: - the amount of the coin is worth

Each coin is encrypted with currency server's secret key (SKcs), which becomes a digital signature to show that the coin is authentic.

Electronic Cash Payment System: Mondex

What is Mondex?

- Mondex is a payment scheme that was initially funded by a major banking organization called National Westminster (NateWest) in U.K. in 1990.

In June 1996, Mondex International became a separate company to promote technology around the world.

Overview of Mondex:

- Mondex uses electronic smart cards that is loaded with money from an account. It is an integrated circuit card (ICC). It plays as an "electronic purse".
- No online verification is needed.
- Security: --> Two levels of security are provided in Mondex:
- the chip used on Mondex cards has in-built risk management system.
- a PIN number is used by Merchants to lock the Value Transfer Terminal so that only authorized personnel can remove value from the Mondex merchant's terminal, or allow refunds.
- the system will close down the card when unusual card behaviors (like transfer of huge funds) occur.

Electronic Cash Payment System: Mondex

- Mondex involves six different entities:

- Franchisees: grant the right and obligations to manage and promote and exploit Mondex in their geographic territory.

- Originators: issue, control, and redeem electronic cash denominated in a currency.

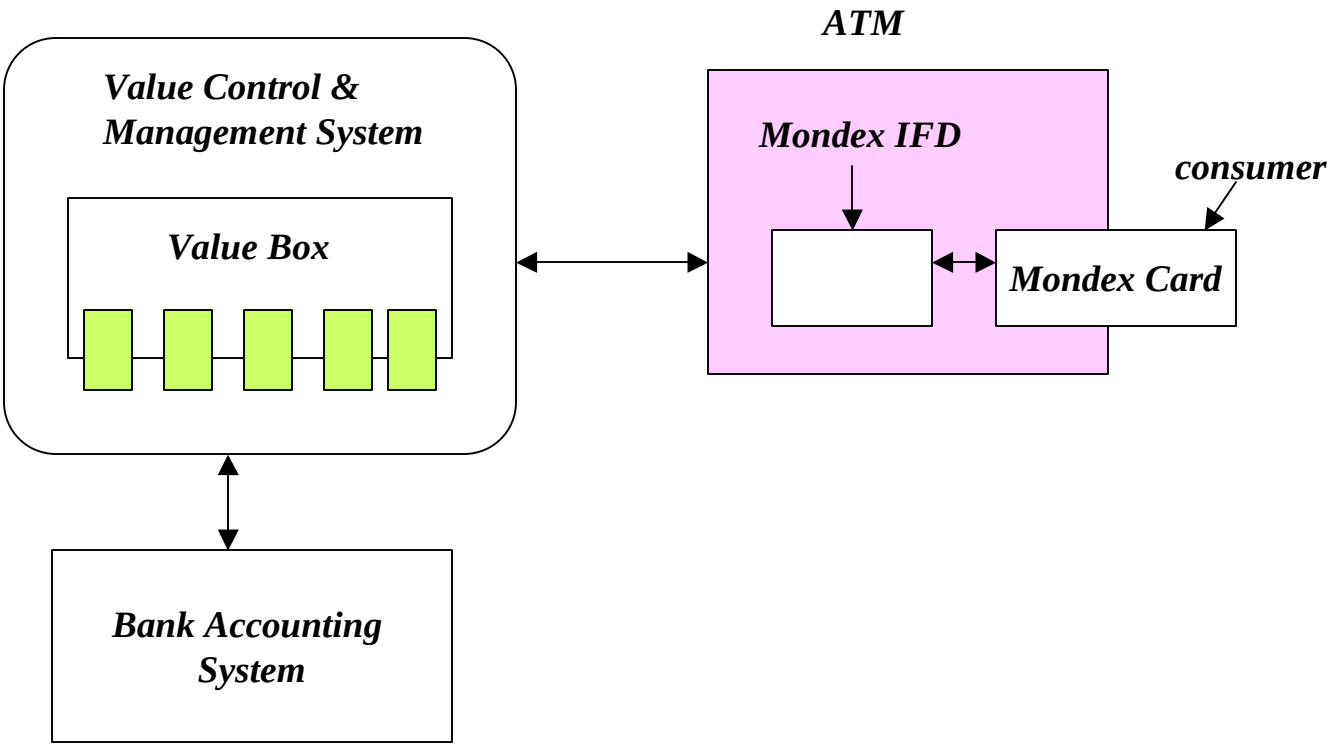
- Manufacturers: produce the hardware to process Mondex Card.

- Members are licensed by Franchisees to issue Mondex Cards to consumers and merchants.

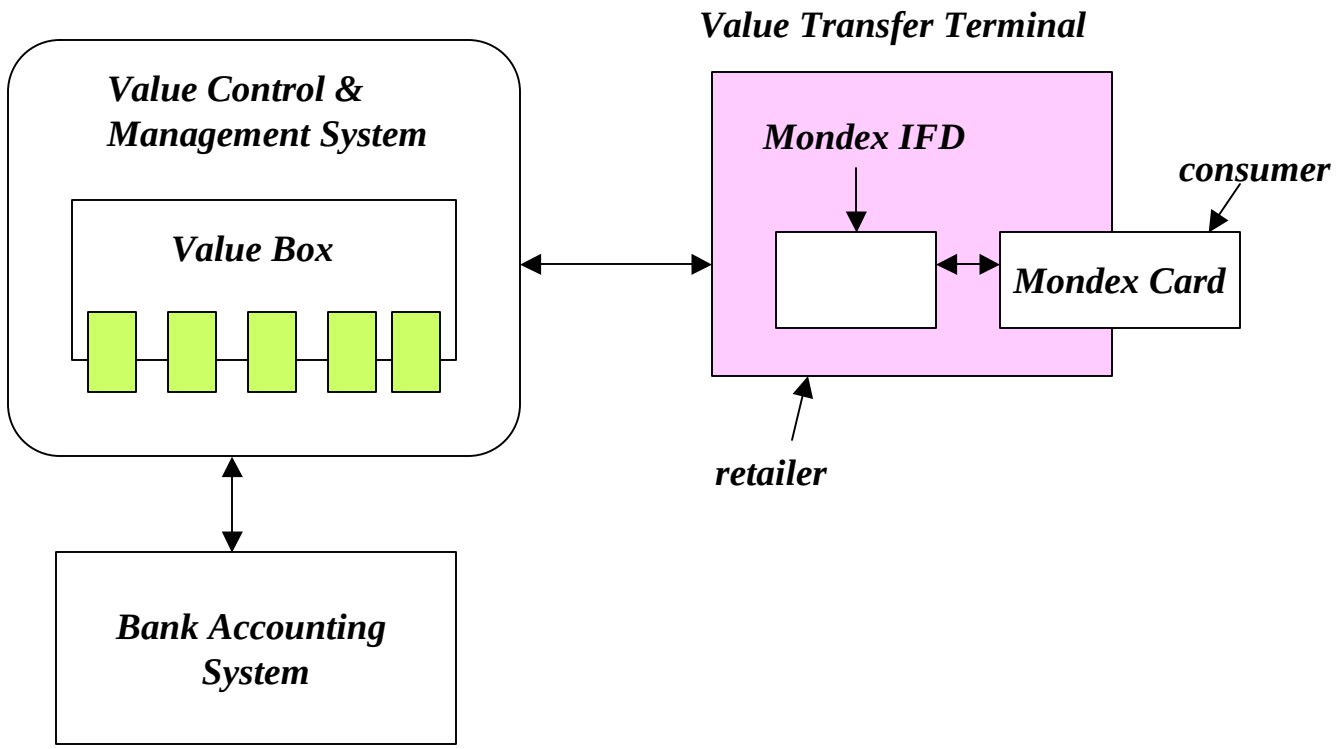
- Merchants: enter into an agreement with Members to enable them to accept Mondex electronic cash as payment for goods and services.

- CardHolders: consumers with Mondex card from Members, and use the card to pay the goods and services from the merchant

Electronic Cash Payment System: Mondex



Electronic Cash Payment System: Mondex



Electronic Cash Payment System: CAFE

- Overview of CAFÉ Project:

- CAFÉ(Conditional Access for Europe) was a project funded under the Europe Community's ESPRIT program.

- It began in 1992, and lasted for three years. The major outcome of this project was the development of an advanced electronic cash payment system.

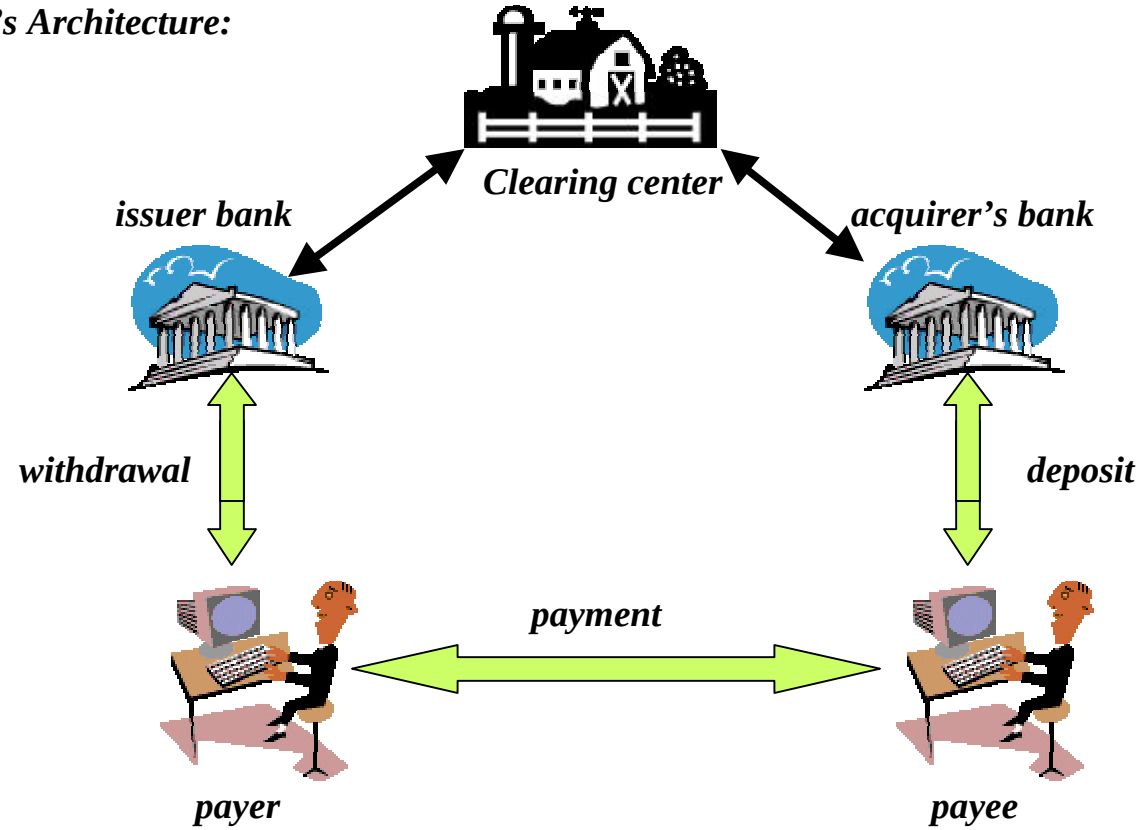
- The payment system used CAFÉ protocol, which use a hybrid payment scheme that based on the concepts of electronic cash and electronic check.

- CAFÉ's goals:

- ***Multiparty security***
- ***Offline payments***
- ***Detection of double spending***
- ***Untraceable payments***

Electronic Cash Payment System: CAFE

CAFÉ's Architecture:



Electronic Cash Payment System: CAFE

- CAFÉ devices:

- There are various tamper resistant electronic devices available in the CAFÉ system, which are used to store money, perform cryptographic operations, and make money to the merchants.

- CAFÉ's devices:

(a) Smart card or Alpha system:

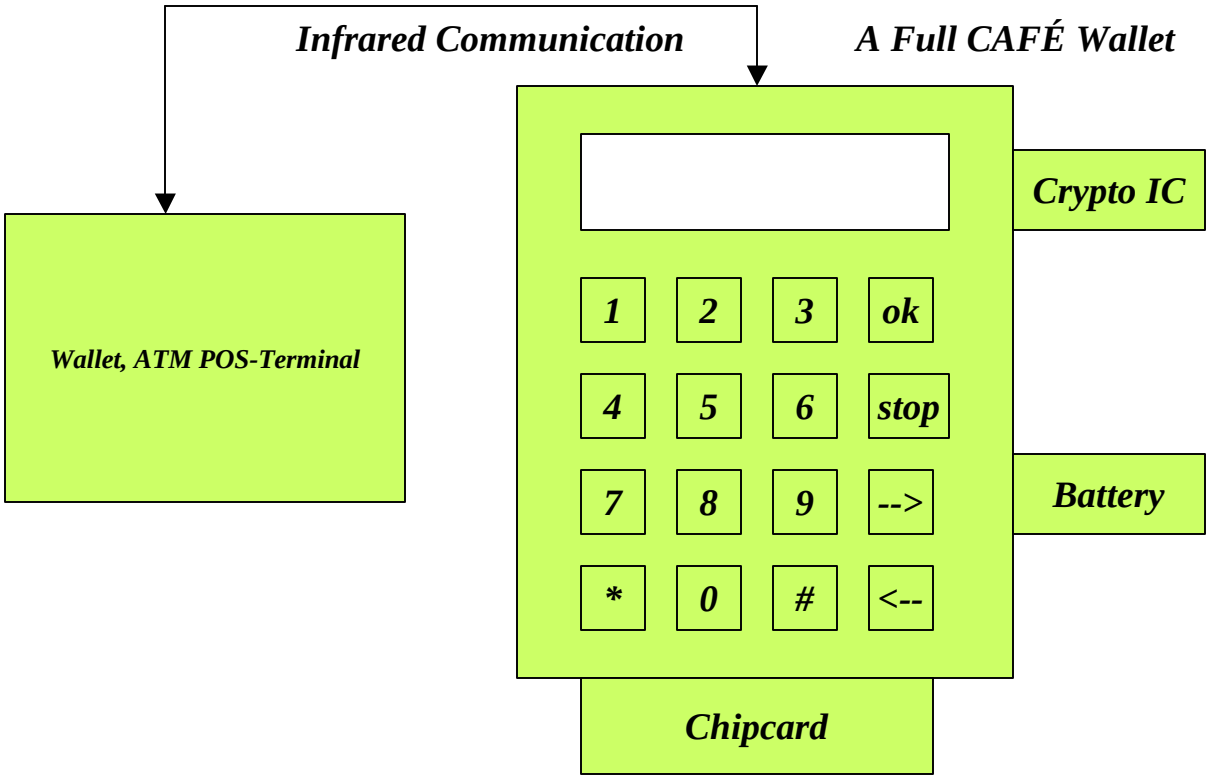
It is an electronic credit card with an embedded microprocessor. It can store coins and transaction information, and perform security and cryptographic operations.

(b) Wallet: --> it consists of two parts:

- Observer - protects the bank's interests

- Purse with a keyboard and a display. It protects user's interests, and allows users to enter PIN number and communicate with outside world.

Electronic Cash Payment System: CAFE



Electronic Cash Payment System: CAFE

CAFÉ security:

CAFÉ use two types of security mechanisms to project the system:

- use of "tamper-resistant devices" to store cryptographic keys and to perform all cryptographic transactions.

- use a cryptographic fallback mechanism that allows the financial institutions to detect double spending of electronic currency.

CAFE's fallback mechanism --> "offline digital coins":

-offline digital coin encoded the identity of the payer into the coin number:
There are two parts in the coin number- PART I + PART II

- When the coin is used only once in a payment transaction, PART I will be revealed.
- Whenever the coin is used more than once, both Part I and II will be revealed to find the payer.