# *Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual*

SKU: 9781482203745-SOLUTIONS

# Key to the Questions of Chapter 2

1. What transactions are excluded in the estimates of nonbanks payments in the US?

Nonbank transactions do not include interbank transfers for the settlement of large-values through CHIPs and Fedwire as well as automated clearing of debit and credit transfers among banks.

2. What factors affect consumer selection of a payment instrument?

- Financial rewards
- Ease of use
- Security

3. What factors affect merchants' adoption of new payment instruments?

- What buyers use
- Payment fees
- Switching costs
- Reduction of fraud and theft
- Increase sales and market share

4. What were the intended and unintended consequences of the approval of the WEB transaction code in 2001?

The code was approved to encourage electronic bill presentation and payment. The unintended consequence was to encourage third-party payment service providers such as PayPal.

5. Compare the use money in open vs. closed payment circuits

The notion of "openness" vs. "closure" relates to the final utilization of the means of payment to make purchases without any a priori restrictions and independently of the issuer. Virtual money is issued by a trusted issuer for a unique usage in a closed circuit to pay for specific goods and services (food, games, transportation, telecommunication). Electronic money, in contrast, is a multipurpose payment mechanism that is recognized in general commercial circuits because it is the electronic version of legal tenders. In closed virtual currency schemes, the service provider sets the exchange rate with the legal



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

tender. If the flow is bidirectional, such as in the case of credit card reward points, there are two exchange rates, a buy rate and a sell rate.

6. What is the difference between the money stored in a transportation card and the money stored in an electronic purse?

The money stored in a transportation card is a token that can be used only to pay for rides on a given bus network. It is often an anonymous payment and is not protected by any user identification or authentication scheme. An electronic purse is a prepaid card that contains money in a given legal currency (U.S. dollars, British pounds, Canadian dollars, etc.) and can be used for any purpose (if acceptable to the seller). An electronic purse is usually protected by security mechanism to identify and authenticate the owner. Finally, an electronic purse is traceable if it points to a bank account; telephone card is not.

7. Why are prepaid cards useful for public transportation systems?

1. Prepaid card: provides up-front revenue collection for the service provider.
2. Easier collection of fare easier
3. Increased revenue from unused, lost, or expired cards.
4. Service provider can enjoy the interest on the prepaid amount before consuming the service
5. Faster service (no need to buy tickets, look for exact change). Contactless cards allow even faster processing.

8. What is the advantage of carrying addenda records with each financial transaction using the CTX Credit Transaction in ACH?

Addenda records up to 9,999 records of up to 80 characters each are used to include remittance data. This makes the payment efficient because in a business-to-business environment, companies pay multiple invoices at once so the addenda include the necessary documentation. These addenda are not standardized, which makes it difficult to automate the processing of account receivables.

9. What are the risks in using debit cards in the US (before the introduction of EMV)?



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

Until the full introduction of chip cards using EMV (Europay, MasterCard, Visa debit cards in the U.S will continue to be of two kinds: signature debit cards and Personal Identification Number (PIN)-authenticated debit cards. With signature debit cards, cardholder authentication relies on the visual comparison of the signature at the point of sale with the signature on the back of the card, which gives a weak protection against counterfeiting or fraud. As the name implies, the user must enter a PIN to authorize the transaction with PIN-authenticated debit cards.

Under the Fair Credit Billing Act (FCBA) of 1974, in the United States, cardholders the maximum liability for unauthorized use of a credit card is $50. Moreover, if the theft of a card is reported before it is used, the cardholder is not responsible for any unauthorized charges. If a credit card number is stolen, but not the card, the cardholder is also not liable for unauthorized use. This rule does not apply for debit cards

10. What are some of the necessary steps to ensure the success of a payment system based on smart cards?

1. An infrastructure to charge and discharge money in and from the smart card
2. A public key infrastructure for certification or a reliable biometric techniques
3. More processing power in the smart card.
4. Standard operating system in the card to allow multiapplications.

11. What is the advantage of carrying addenda records with each financial transaction using the CTX Credit Transaction in ACH?

When the payer sends the remittance information with the payment, the receiver know exactly what they are being paid for. In a business-to-business environment, multiple invoices are typically paid with a single transaction. Without the attached remittance data, the task of posting payments and closing out the account receivables by the receiving company become more elaborate.

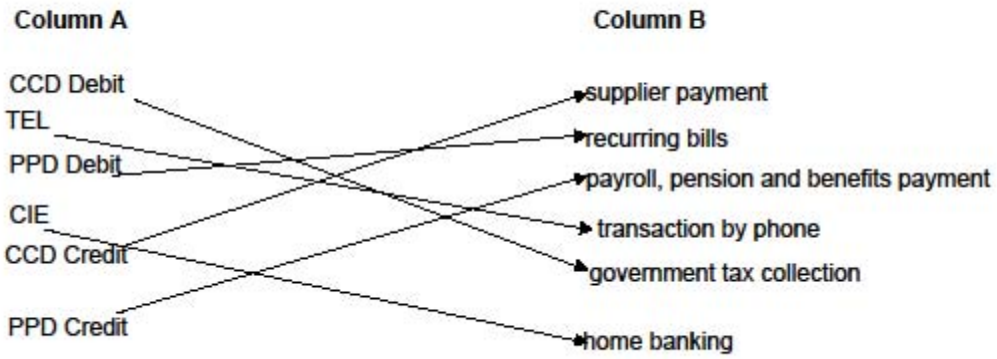
12. Compare client-based and server-based (virtual) wallets.



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

1. In client-based wallets, user must maintain the wallet (updates, patches, etc.), critical data is transmitted for every transaction, wallet can be lost if there is a problem on the disk or a virus, and there is no mobility.
2. In server-based (virtual) wallets, credentials and value are stored on the server, service provider is responsible for maintaining the wallet, and user can access wallet from any terminal (device independence, OS independence

13. Match items from column A with the corresponding item in column B




14. What are the factors that encourage the use of RTGS?

- Improvement in information technology (speed of processing capacity)
- Fee structure that encourages the use of overnight settlement for smaller payments

15. What are the advantages of RTGS for retail payments?

- Reduce the time of settlement for all payments
- Banks will have only payment interface to the clearance and settlement systems.
- Eliminated credit risk

16. Compare credit risk with liquidity risk.

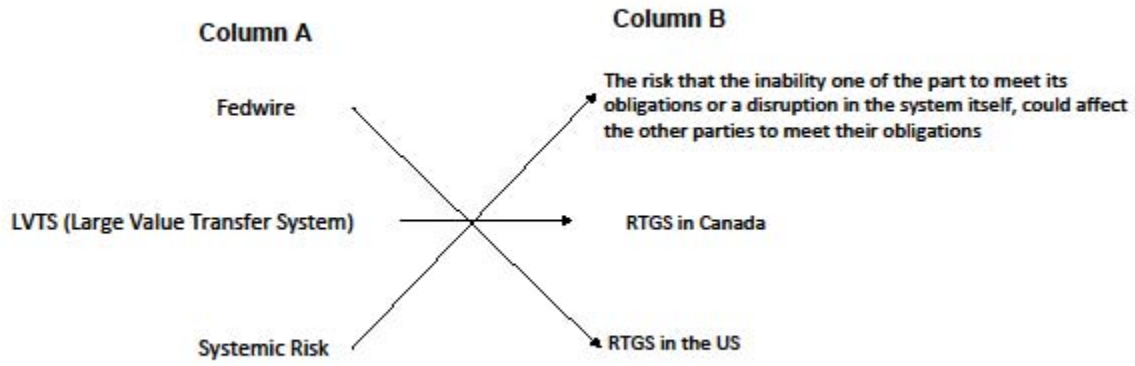
Credit risk, the risk that a counterparty will not settle an obligation for full value, *either due or at any time later*.

Liquidity risk, the risk that a counterparty will not settle an obligation for full value, *when due*.

1. Match items from column A with the corresponding item in column B



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual




17. What are the risks associated with contactless payments?

- Risks that a transaction being carried out without the knowledge of the cardholder

18. What are the risks associated with prepaid cards?

- Card is vulnerable to theft

19. What is the Bank of International Settlements?

The Bank of International Settlements was established in Basle, Switzerland in 1930. Its main tasks are:

- Provide forum for the cooperation for central banks and for stimulating information exchanges among them
- Conduct research on monetary policy and collect and publish statistics international finance.
- Perform traditional banking functions such is reserve management and gold transactions
- Provide and organize emergency actions to shore up the international monetary system in cooperation with other institutions like the IMF (International Monetary Fund).

20. What is the difference between clearance and settlement?

Clearance is the process of transmitting, reconciling and/or confirming payment orders. Settlement is the time at which at the financial obligation is discharged.

21. What is SEPA?



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

SEPA is the process to harmonize the clearance and settlement procedures in Europe by defining common regulations and standards s to increase competition and improve efficient

22. In a push transaction, one party sends a payment to its correspondent. In a pull transaction, one party receives a payment from the other party. Indicate which of the following transactions is a push transaction:

- Wire transfer √
- Credit transfer √
- Check
- ACH debit
- Card

23. What is the main role of NACHA?

Rule making for ACH operations.

24. What is the role of the U.S. Federal Reserve System?

- Regulates the money supply
- Issue regulations for financial institutions
- Operates Fedwire and one of the two ACH systems in the US

25. What is SWIFT?

This is global financial service messaging system frequently used in conjunction with the large-value systems. It also develops internal standards for financial transaction.

26. Evaluate the evolution from magnetic strip cards to smart cards in payments from the point of view of the user, the merchant, the bank, the card manufacturer and for chip manufacturers.

For the end-user and chip manufacturers: it is an incremental innovation

For the bank: it is a new platform innovation to offer existing services but protect the card from counterfeiting.



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

For the merchant and the retailer: it is an architecture innovation because it disrupts the existing operations due to the need to install new terminals and do some training for the associates .

For the card manufacturer: it is an architecture innovation, the need to develop new processes to include the chip in the plastics.

Smart cards are not radical innovations: they do not protection on online transactions.

27. What are the arguments for and against cash?

For individuals: cash is available at no cost and provides anonymity. Also, it is available to those who cannot afford or are not offered other instruments.

For the central bank: The difference between the cost of production and the nominal value is a loan without interest to the central bank (seignorage).

Against individuals, cash does not bear interest

Against central banks: if a central bank moves interest rates below zero, people will move into cash.

28. Compare the technologies currently used for bank notes, bank cards, paper checks and electronic bill presentment, electronic bill presentment in terms of cost, security, user's convenience. What are the core competencies for each technology? What possible technology transactions are possible?

Bank notes:

Cost: The total cost of banknotes includes the cost of manufacturing, distributing, the recall and destruction of worn-out notes.

Security: Utilization of special paper that cannot be easily reproduced (an issue with high quality scanners and printers). Also, the security aspects include protection of money during transportation in armored vans.



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

User convenience: For small sums ensure ease of use an anonymity. Not useful for large sums. Not customizable.

Core competencies:

1. Counting coins and bills automatically.

2. Inserting metal lines or holograms in the printing process.

3. Design of hard to reproduce bills.

No likely technological transition.

Bank cards

Cost : Manufacturing and distributing the card (by mail). Fraud. Backoffice operation to handle card transactions and follow various regulations. Cost of currency conversions. Cost of security logic on the chip.

Debit vs. credit cards. Debit card transactions cannot be revoked. Credit cards are not given easily. Somewhat customizable.

Security:

1. Authorization centers and adjustment of the security on the basis of the user's profile and the merchant's profile.

2. Holograms in the front side of the card.

3. Adding microprocessors in the card and inserting encryption engines and algorithms.

4. Monitoring of the card network for intrusions.

5. Unreliable or expensive networks.

Core Competencies

1. IC manufacturing



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

2. Database management

3. Risk analysis and data mining

4. Network operations and management.

5. Encryption, remote identification, etc.

Technological transition likely in cryptography, remote identification, etc.

Paper Checks

Cost: Fabrication, security, distribution, return (sorting, identification of the signature, capture of the written data, rejection, etc.) archiving, stolen checks, bad checks.

User convenience: User must know reading and writing. User must be able to balance a checkbook.

Security: Bad checks constitute 1% of total amount of checks.

Core Competencies:

Transportation.

Automated processing for reconciliation and risk analysis.

Settlement systems.

Front office (tellers).

Electronic checks require a new set of skills similar to those for bank cards.

Technology transition likely in networking security.

Electronic bill presentment

Cost: Cost of running a secure and reliable site.

User convenience: Depends on user's familiarity with computers. Access to the Internet.



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

Values for consumers: online payment of bilss.

Security: All the issues associated with the Internet (privacy, distribution of encryption keys).

Security crucial if presentment is linked to payment.

Core competencies

1. Encryption.

2. Customer relation management

3. Backoffice

4. Marketing (cross-selling): billing is a sales- and customer-bonding opportunity.

Technology transition likely in:

Customer relation management system, back office and storage systems, transaction and network security.

Account aggregation

Cost

Security + interfacing with all the billers billing and accounting systems.

User convenience

For end user: All electronic bills from one source (may be).

For billers: delegate the billing to a third party competent in that regard.

Security

All issues related to the Internet + those related to sharing customer's information with the billers.

Core Competencies

1. Encryption.



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

2. Customer relation management

3. Backoffice

Technology transition likely in:

Customer relation management system, back office and storage systems, transaction and network security



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

# Chapter 2

## Money and Payment Systems



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

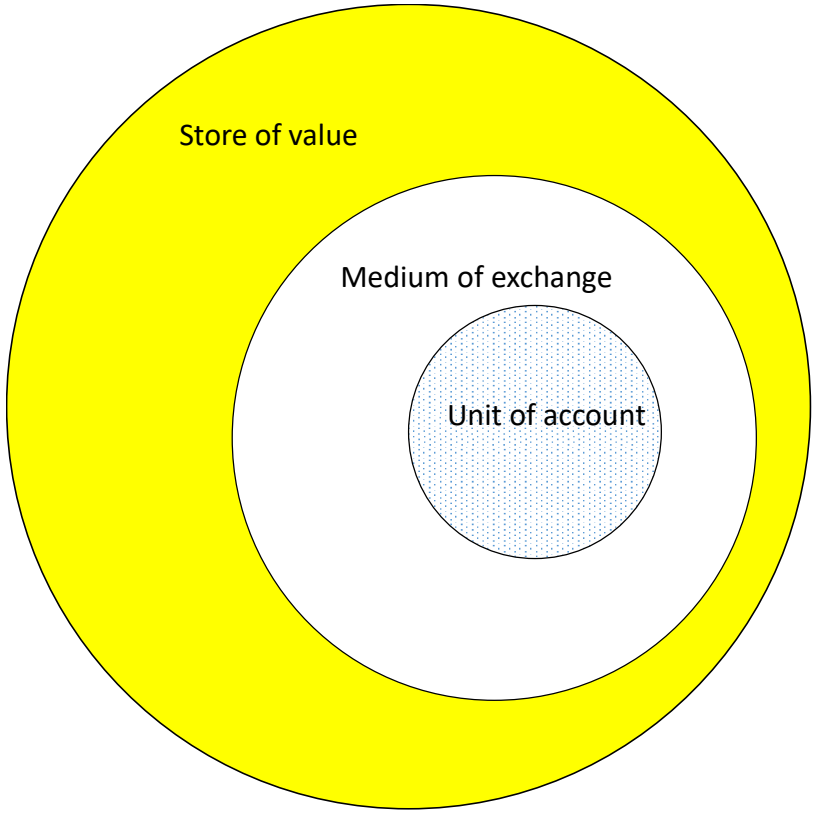
# Outline

- Properties of money
- Instruments of payment and their usage in some countries
- Dematerialized monies
- Purses and holders
- Transactional properties of dematerialized currencies
- The practice of dematerialized money



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

# Functions of Money




- Standard of value (unit of account)
- Medium of exchange
- Store of value



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

# Characteristics of Monetary Units

- It must be divisible to cover a wide range of amounts
- It must be convertible to other means of payment
- It must be recognized by an open community of users
- It must be protected by the coercive power of a state
  - Bitcoin is an exception



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

# Classical Money

- Easily recognizable
- Relatively stable value
- Durable
- Easy to transport
- Easy to use
- Negligible production cost



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

# Types of Monies

- Fiduciary money (coins and notes issued by the Central Bank)
- Scriptural money
  - created by a bank
  - a merchant is free to accept or reject
- Private money
  - Tokens
  - Stocks and shares
- Digital money and cryptocurrencies



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

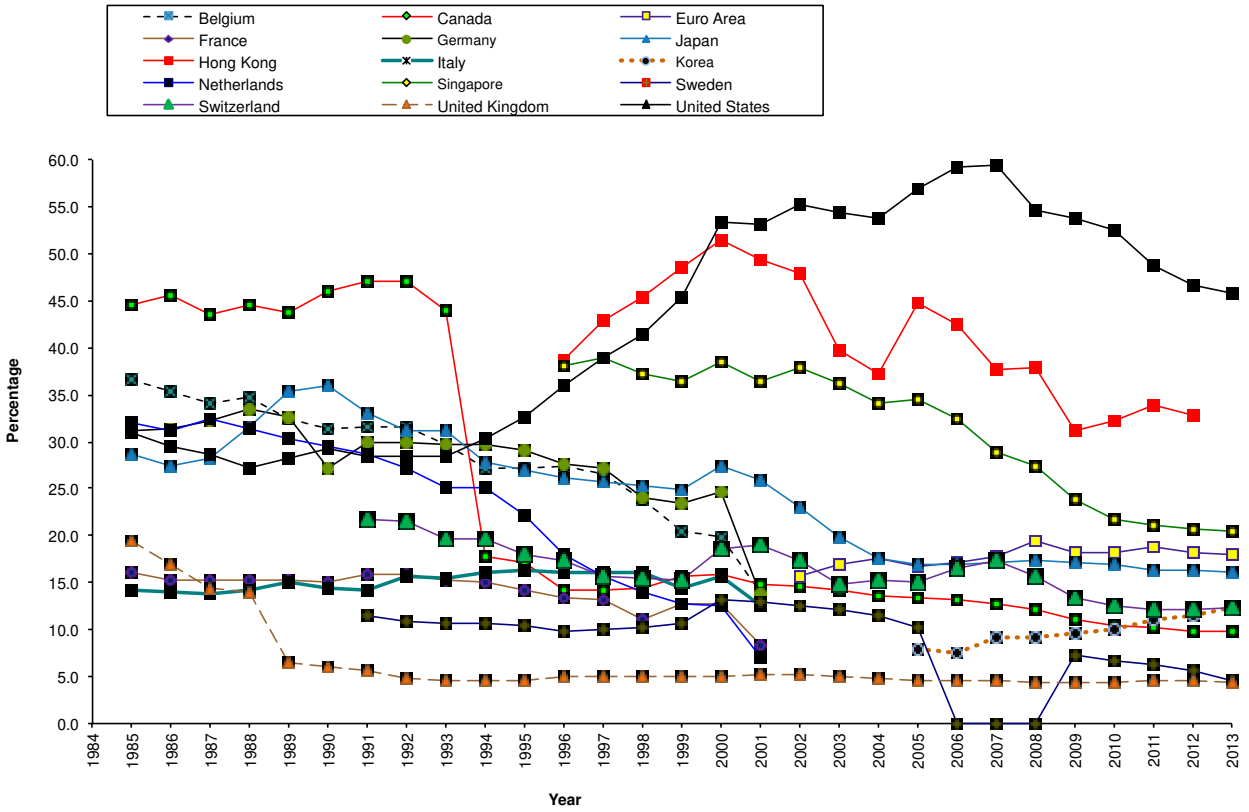
# Classical Instruments of Payment

- Payment instruments are used to transfer the power of money from one economic agent to another - Some have a legal status and some are banking inventions
- Cash
- Checks
- Credit transfer
- Direct debit
- Interbank transfers
- Bills of exchanges
- Payment card



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

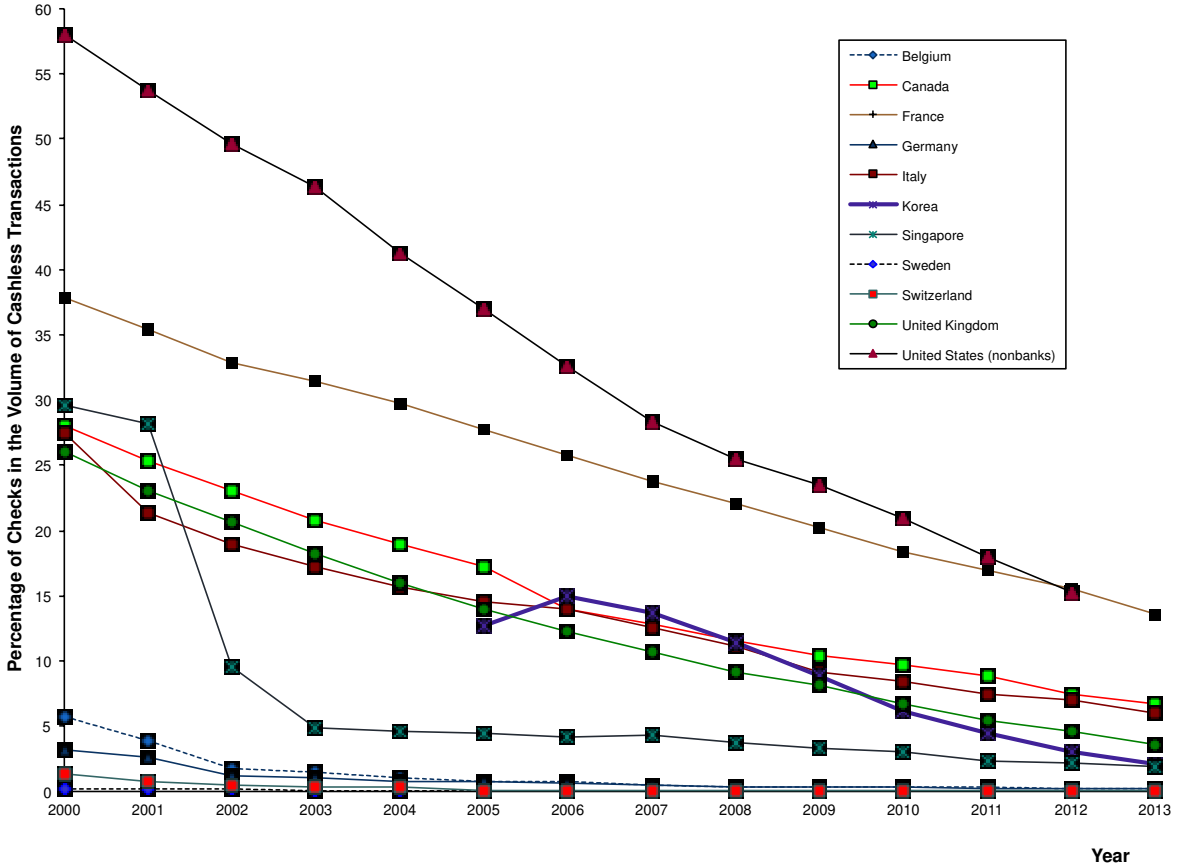
# Patterns of Cash Usage in percentage of in the Narrow Money for Selected Countries






Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

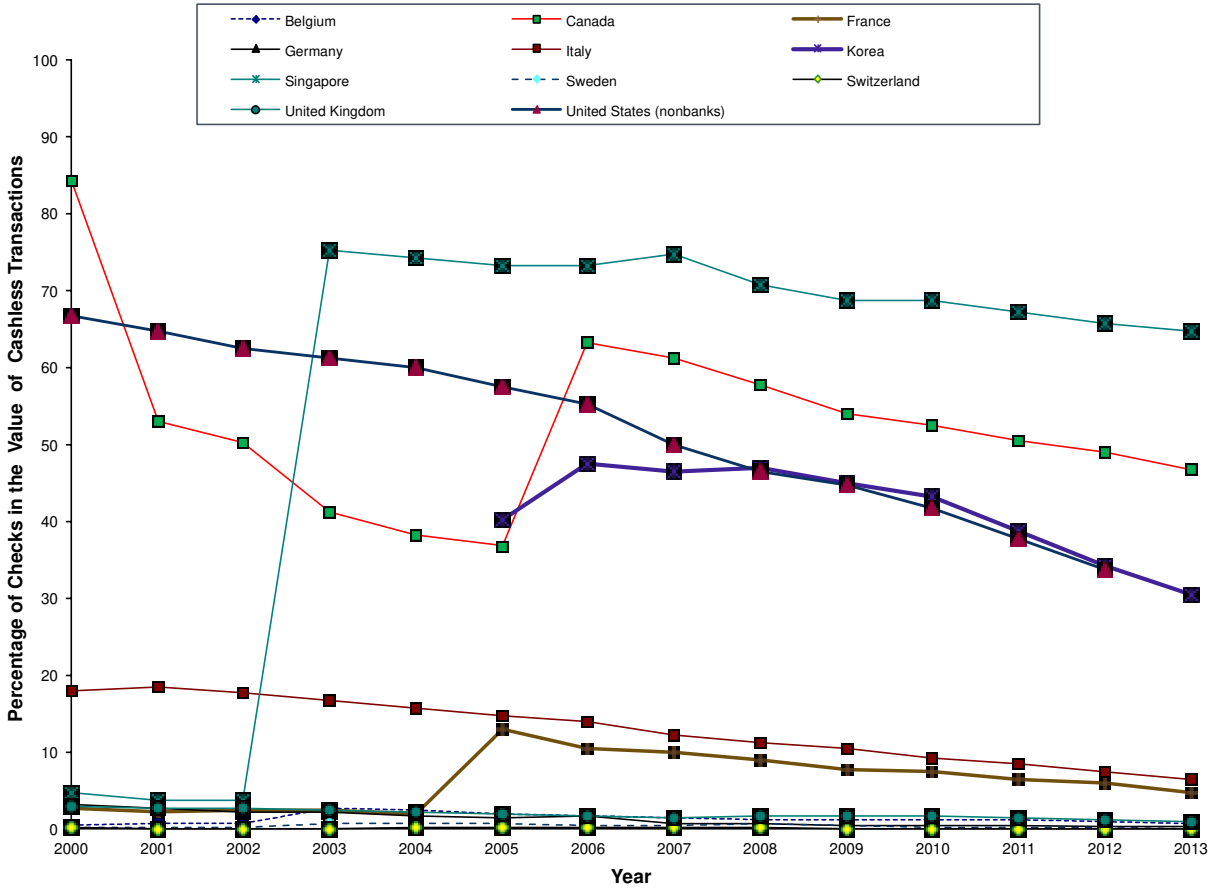
# Percentage of Checks in the Volume of Scriptural transactions






Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

# Percentage of Checks in the Value of Scriptural transactions

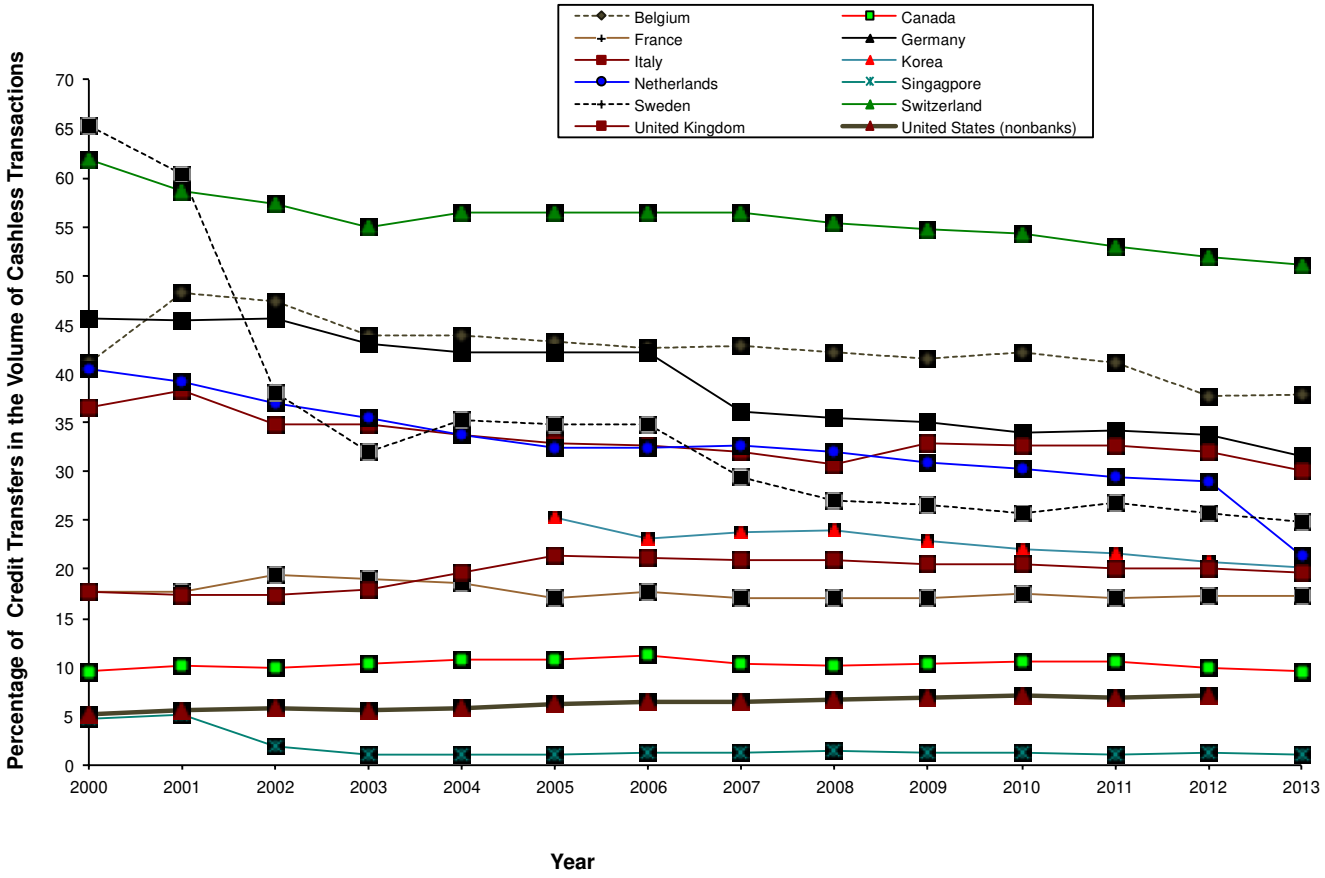





Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

# Percentage of Credit transfers in the Volume of Scriptural Transactions

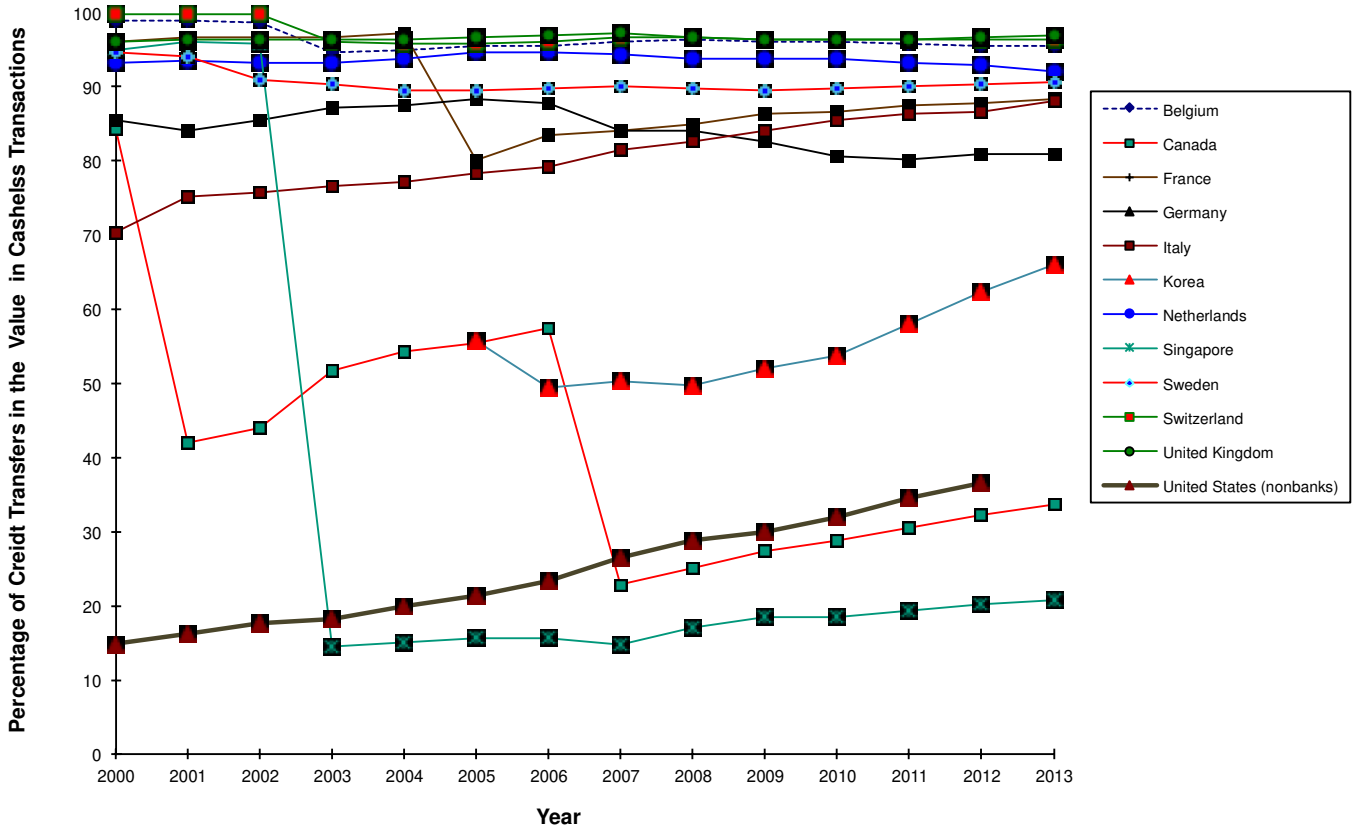
Since 1/1/99, all payments by the U.S. federal government are credit transfers except for tax refunds






Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

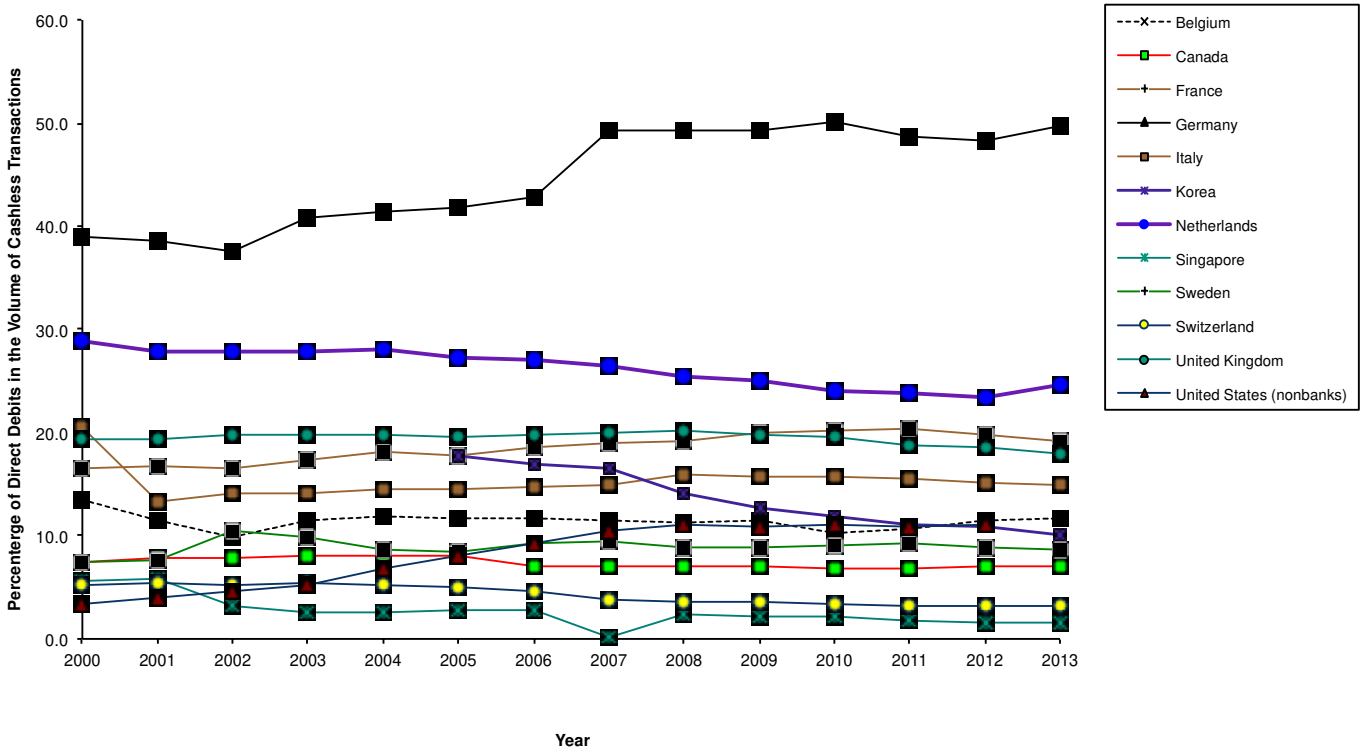
# Percentage of Credit transfers in the Value of Scriptural Transactions






Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

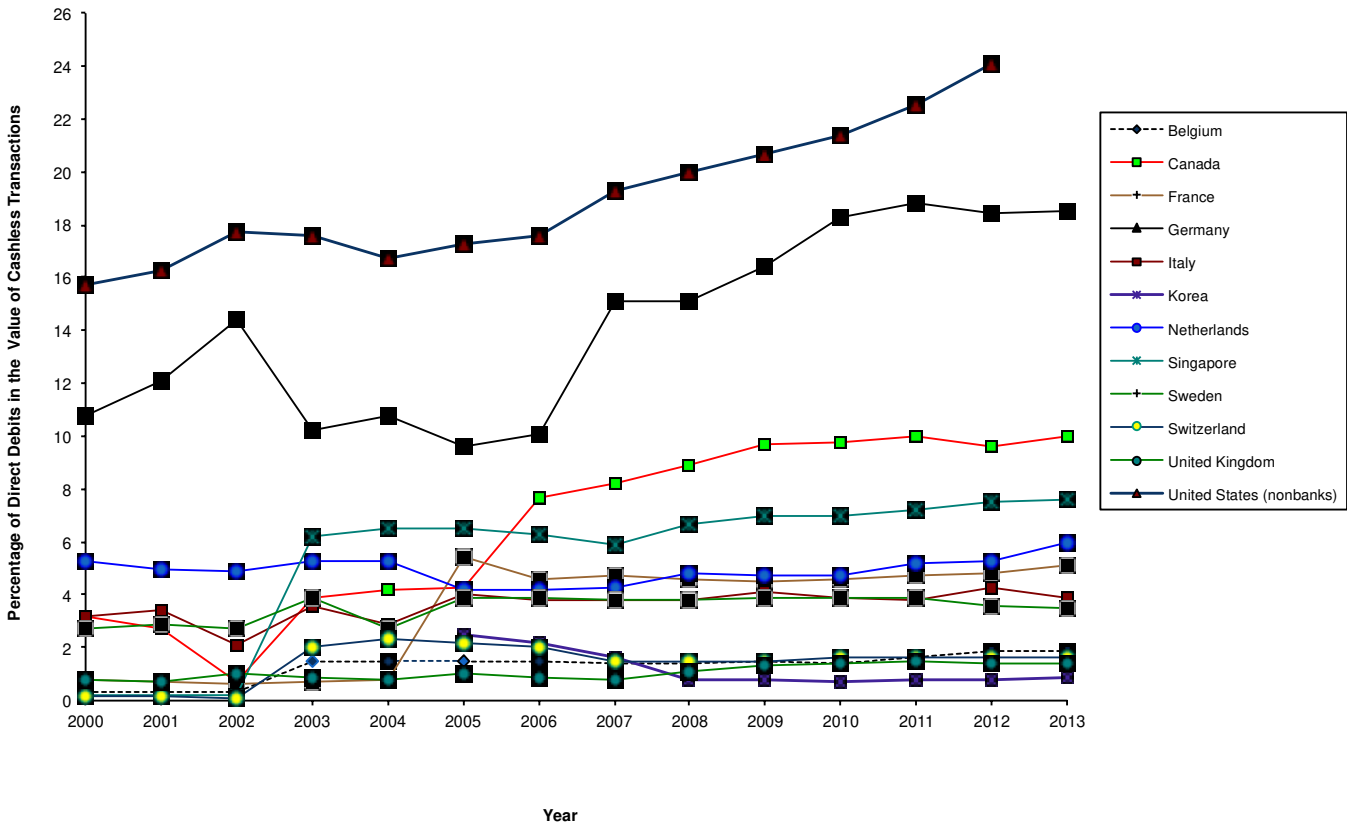
# Percentage of Debit Transfers in the Volume of Scriptural Transactions






Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

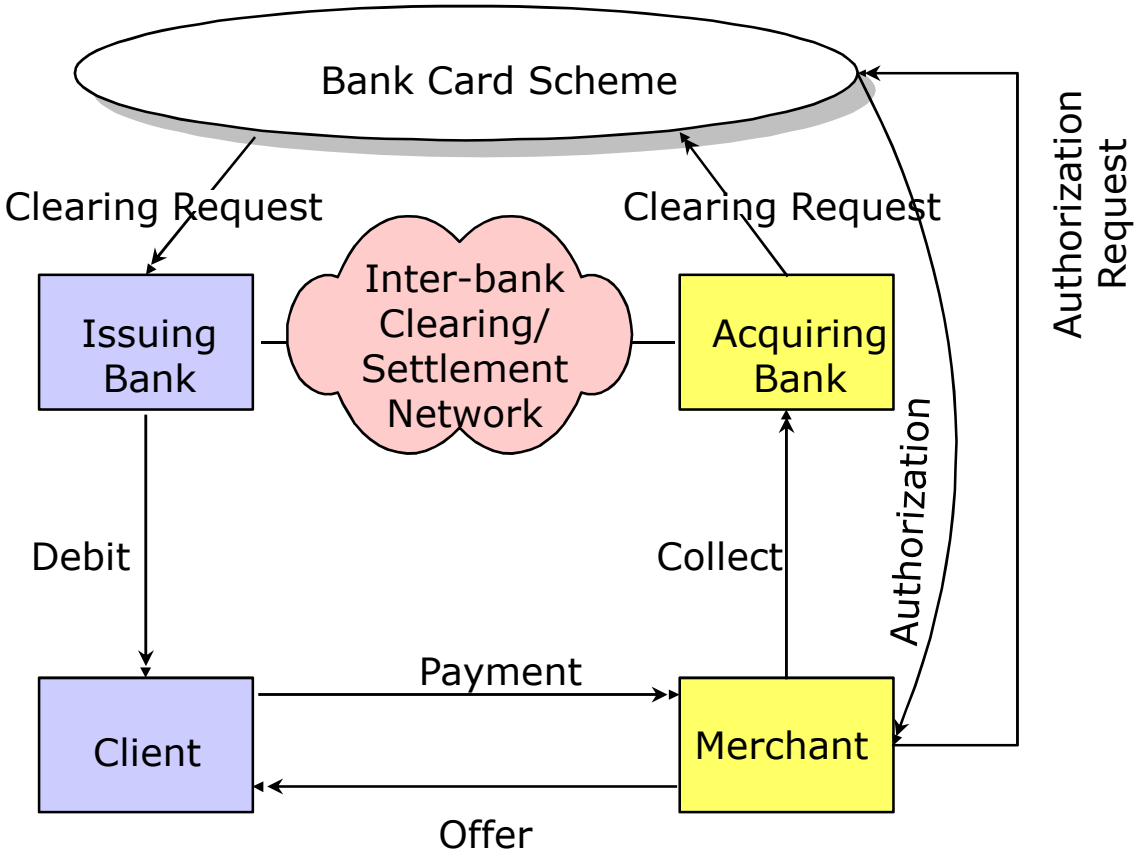
# Percentage of Debit Transfers in the Value of Scriptural Transactions






Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

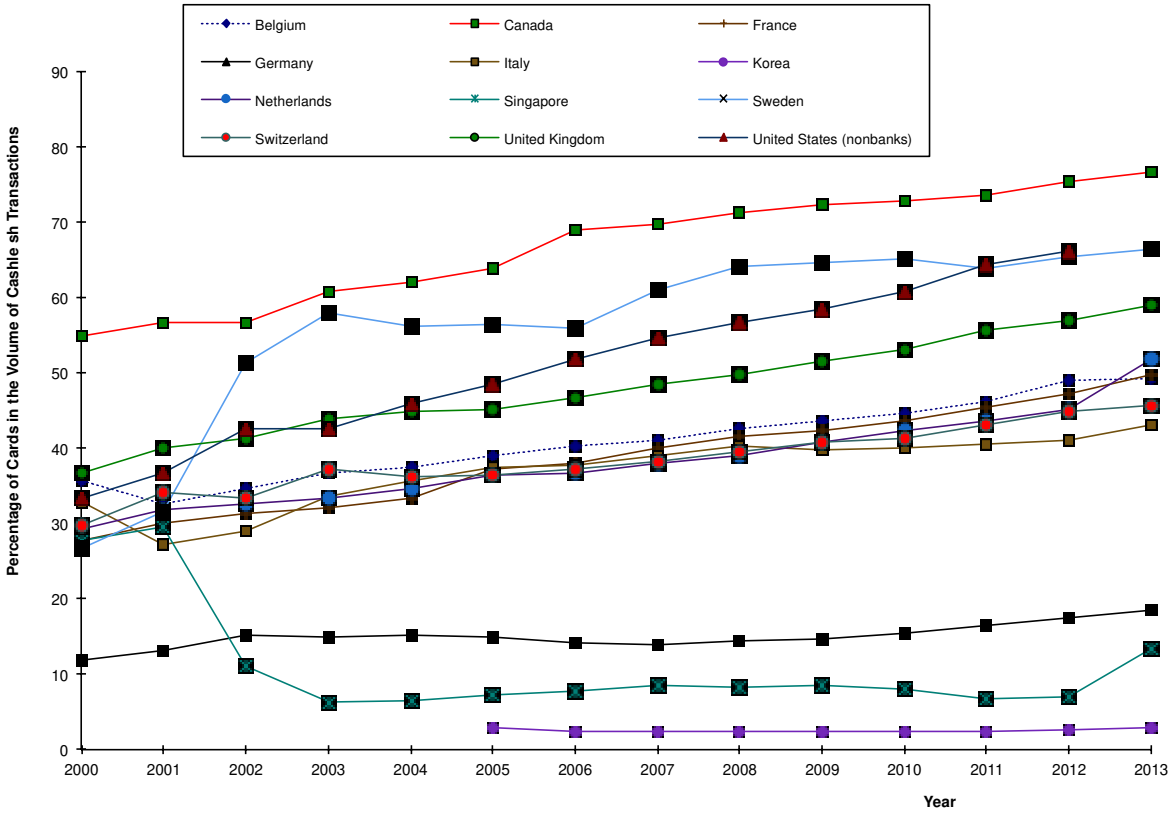
# Exchanges during Bank Card Transactions






Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

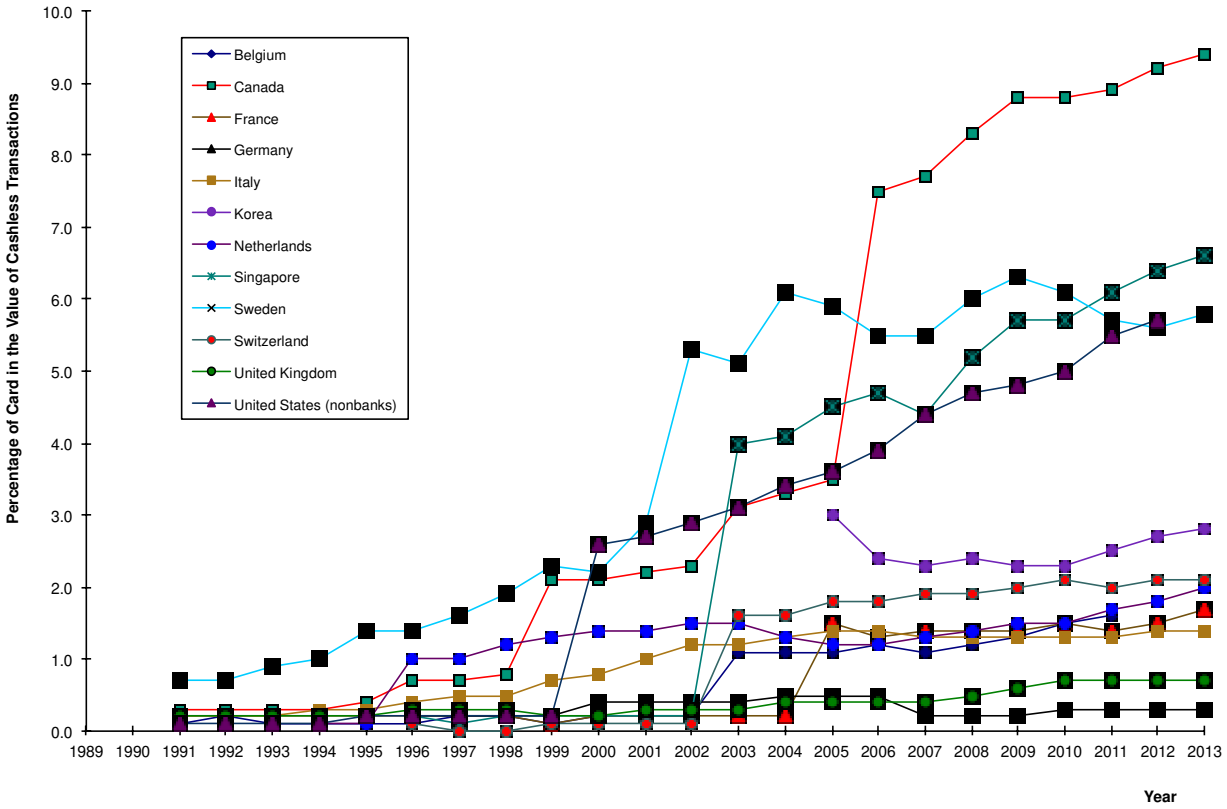
# Percentage of Bank Card Transactions in the Volume of Scriptural Transactions






Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

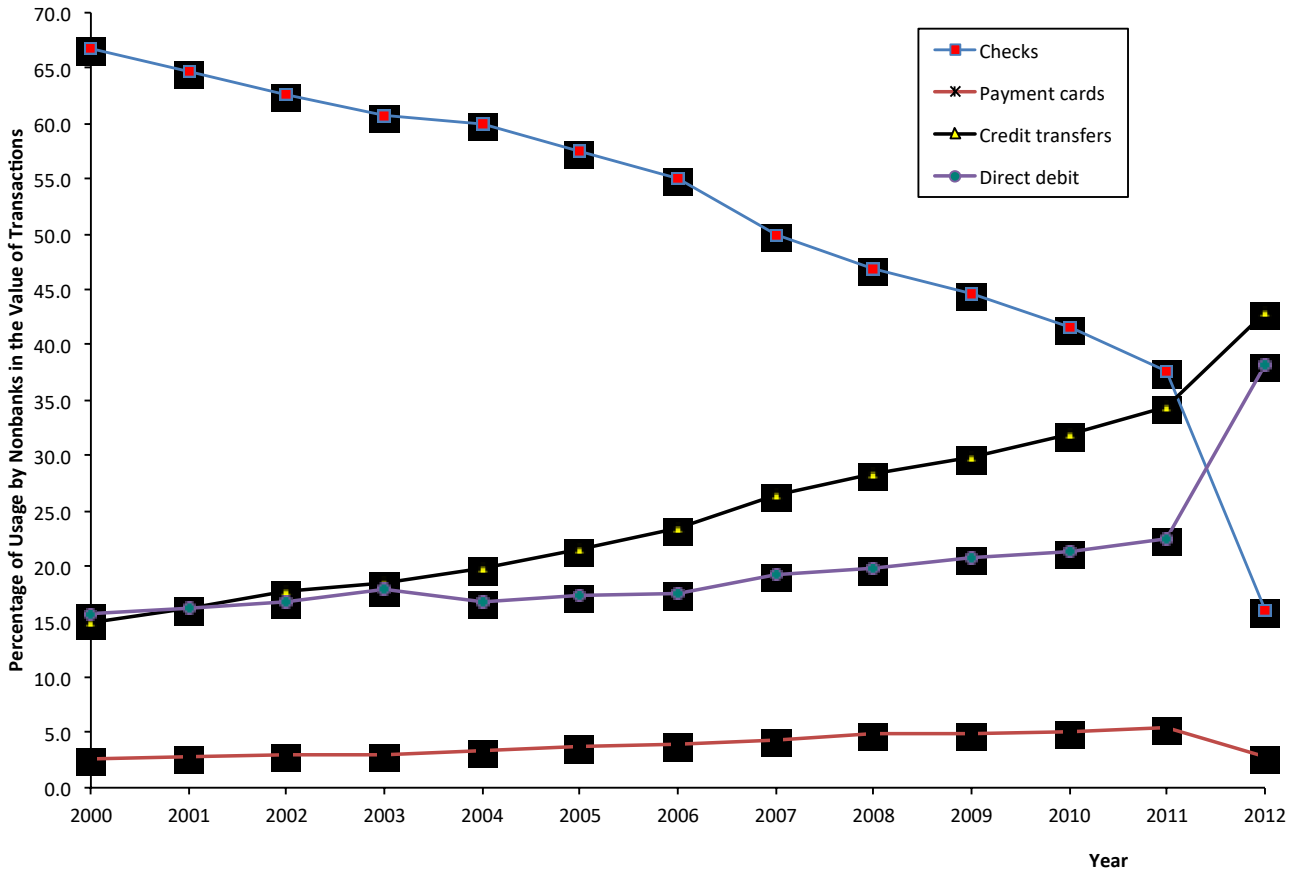
# Percentage of Bank Card Transactions in the Value of Scriptural Transactions






Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

# Evolution of Payment Instruments by Non-Banks in the U.S. By Value






Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

# Emerging Payment Types - Dematerialized Monies

- Electronic money
  - fiduciary money stored in electronic forms
- Virtual money
  - fiduciary money
  - token (jeton)
  - QQ coins (Tencent) or Facebook Credits
- Digital Money (DigiCash, Bitcoins)
  - value stored in the form of algorithms
  - Minted by a client software
- Private money (stock options and shares)



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

# Electronic Purses and Electronic Jeton (token) Holders

- Electronic Money within physical support
  - Electronic Purses (Mondex)
  - Electronic Token (Jeton) Holders (Telephone Cards, transportation cards)
- Virtual Money stored in software programs
  - Cloud-based payment systems
  - Virtual Purses (ExxonMobil's SpeedPass, WebMoney)
  - Virtual Jeton Holders (Millicent)



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

# Electronic Purses and Electronic Jeton Holders

| Characteristic | Electronic Purse | Electronic Jeton Holder |
|---|---|---|
| Expression of purchasing power | Legal tender | Consumption unit |
| Unit of payment | Universal: can settle any payment in a defined territory | Specific to transactions involving the issuer |
| Guarantor of purchasing power | Bank | Service provider |
| Charging of value | By a bank or its agent | Unregulated |
| Circuit of financial services | Open | Closed |



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

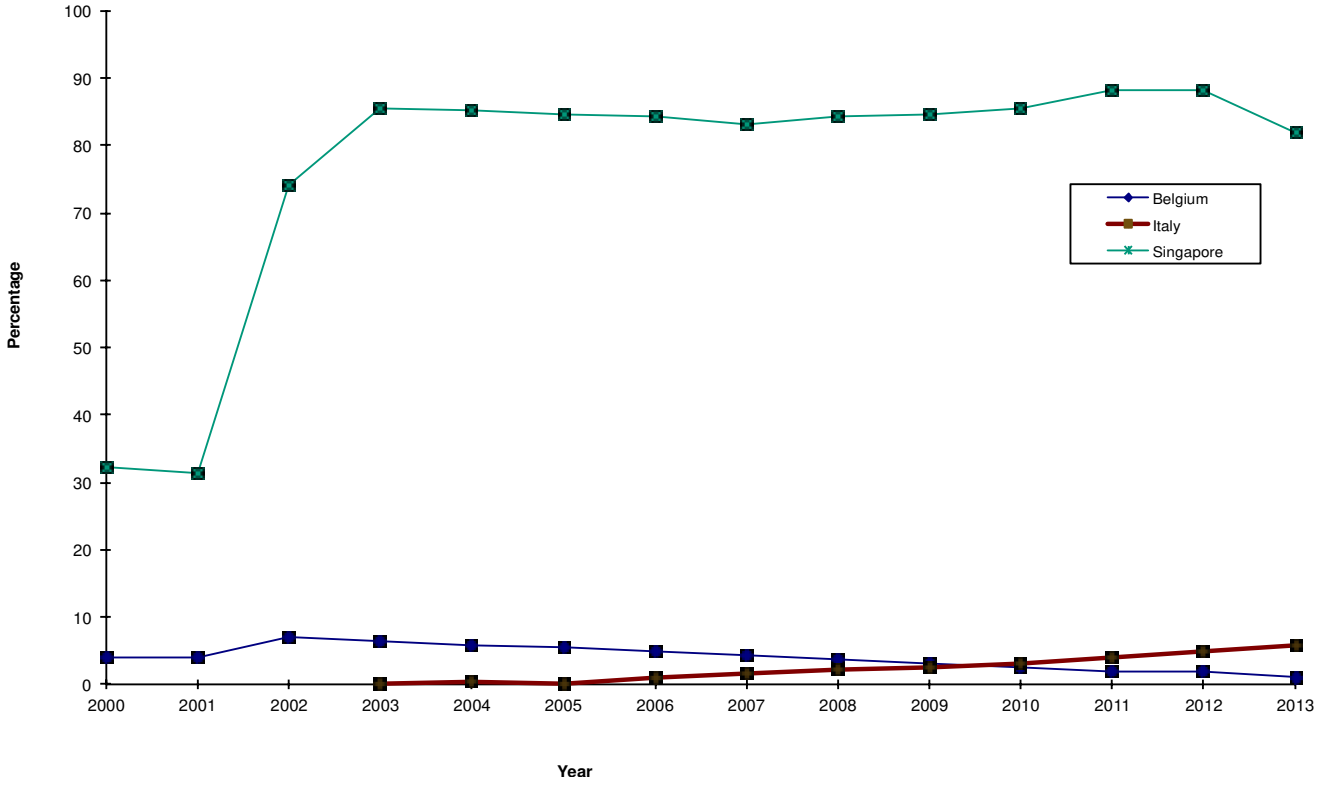
# Digital Wallets

- A digital wallet is a software on a desktop, a mobile terminal or a network server
- A mobile wallet is an app to store, access, manage and used identification and payment instruments in a secure way
- A mobile wallet can be linked to an account on a server
- Examples of mobile wallets: Google Wallet, Softcard, Apple Passbook, GoPago, QuickTap, Osaifu-Keitai, etc.



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

# Percentage of Electronic Purse Transactions in the Volume of Scriptural Transactions






Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

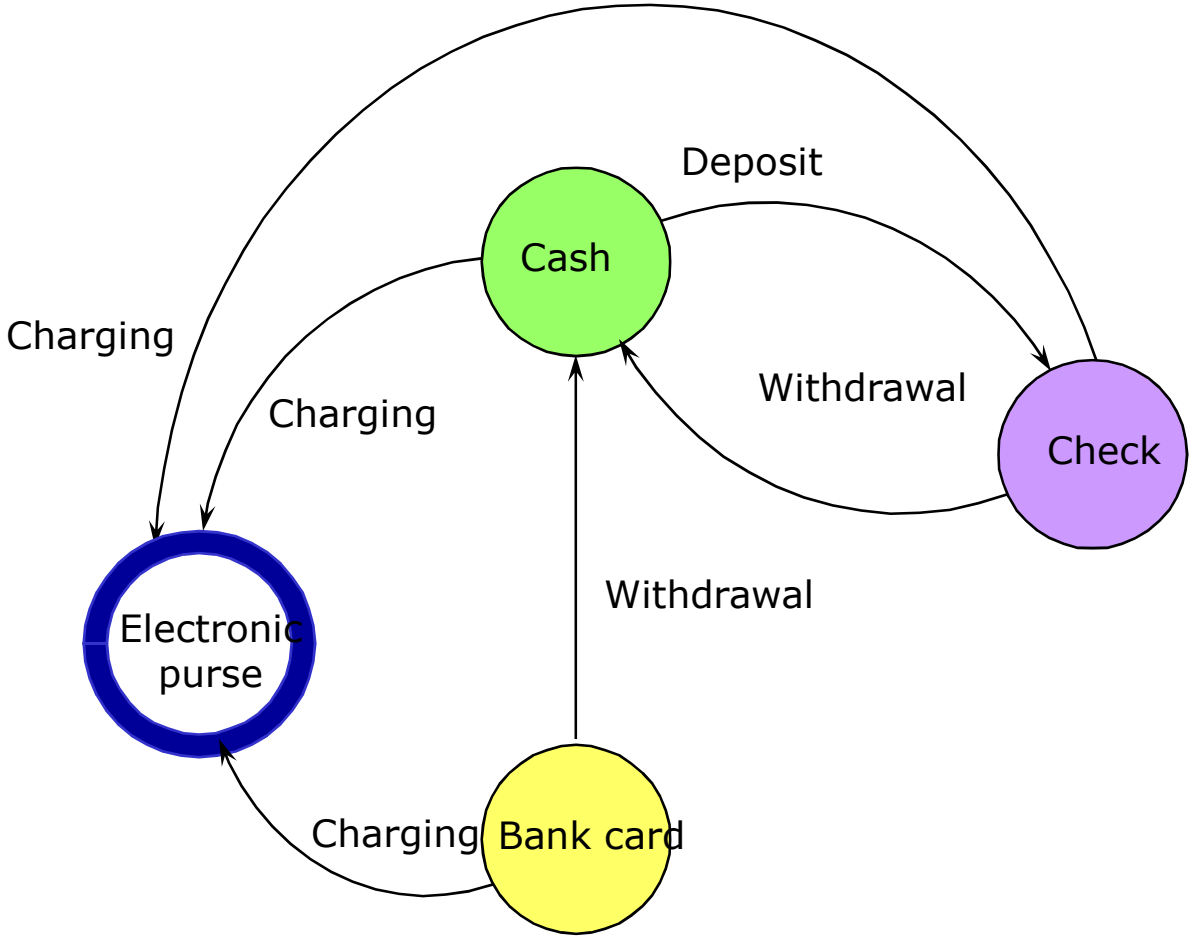
# Transactional Properties of Dematerialized Currencies

- Atomicity
- Consistency
- Isolation (no interference among transactions)
- Durability (resilience to errors)
- Anonymity (not always)
- Non-traceability: anonymity + two payments by the same person cannot be linked



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

# Monetary Flow among Payment Instruments






Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

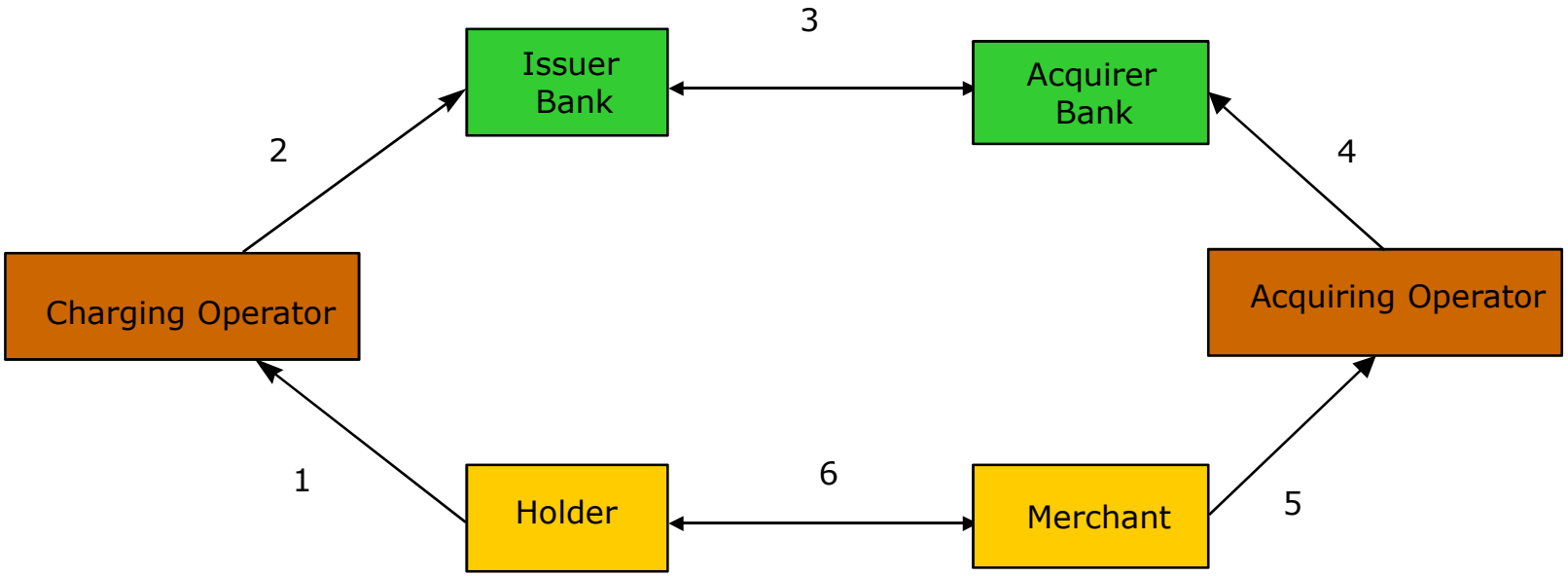
# Comparison of Monies

| Type of Money | Nature of Money | Support (the Container) | Value Store | Value Representation | Mode of Payment | Means of Payments (Instrument) |
|---|---|---|---|---|---|---|
| Fiduciary | Concrete, material | Paper, piece of metal | Safe, wallet, purse | Bank notes, coins | Face-to-face transaction | Bank notes, coins |
| Scriptural | Immaterial (an account maintained by a credit institution) | Magnetic, optical, electronic | Account maintained by a credit institution | Numerical value | Remote, face-to-face (retail automatic machines) | Check, debit card, credit card credit transfer |
| | | Integrated circuit card | Electronic purse | | | |
| | | Computer/Smart phone | Virtual purse (memory allocated by an intermediary) | | | Electronic fund transfer |



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

# Flows in a Transaction by Dematerialized Money




- Charging and discharging of the dematerialized money
- Purchasing and payment protocols
- Verification protocols (on line, off line, semi-online)

- Protocols for collection, acquisition and clearance
- Peer-to-peer transfer protocol



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

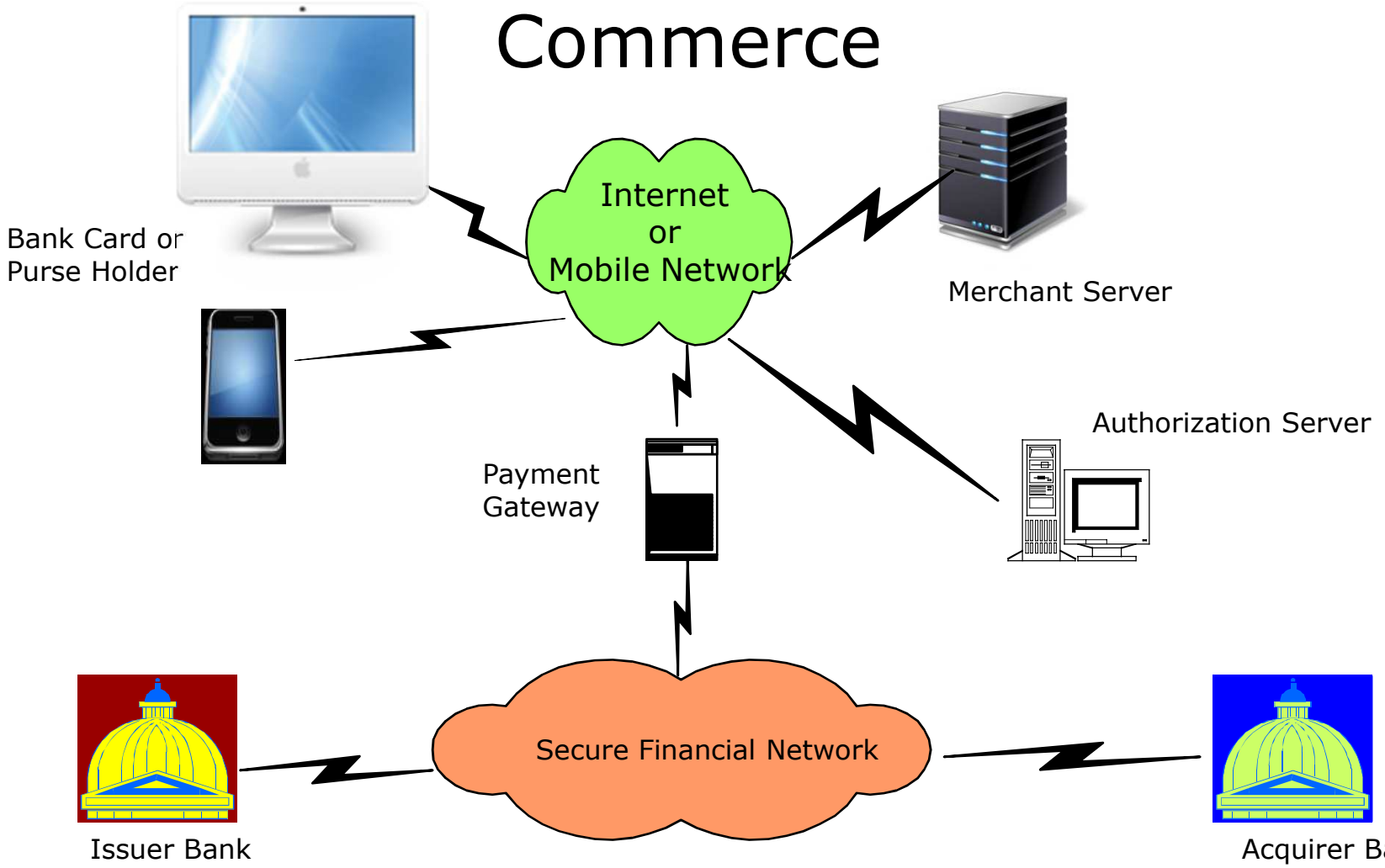
# Security Requirements of Charging Protocols

- The protocols must resist attacks from outside the system:
  - Must resist misappropriation by any one of the participants
  - A 3rd-party non-participant must not be able to intercept the message to manipulate the content, modify orders, or resend valid but old messages.
  - Must resist false charges such as
    - Attributing the charge to a client other than the one identified
    - Attributing an amount different from the requested one
    - Repaying a previously authenticated charge
    - Repudiating a previously correctly executed charge
- Must be robust to return to previous state if there is an error.



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

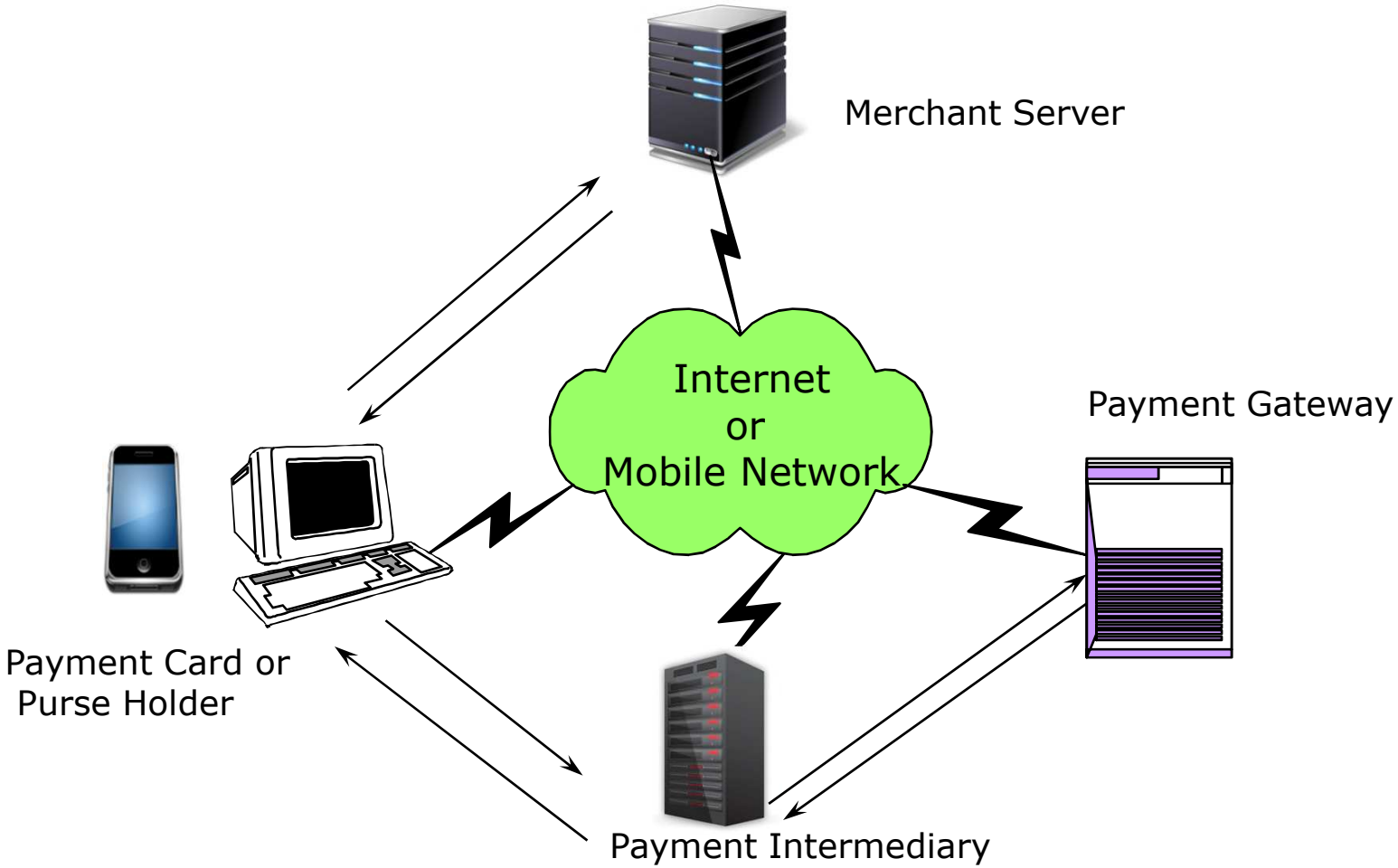
# Payment Gateways in Electronic Commerce






Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

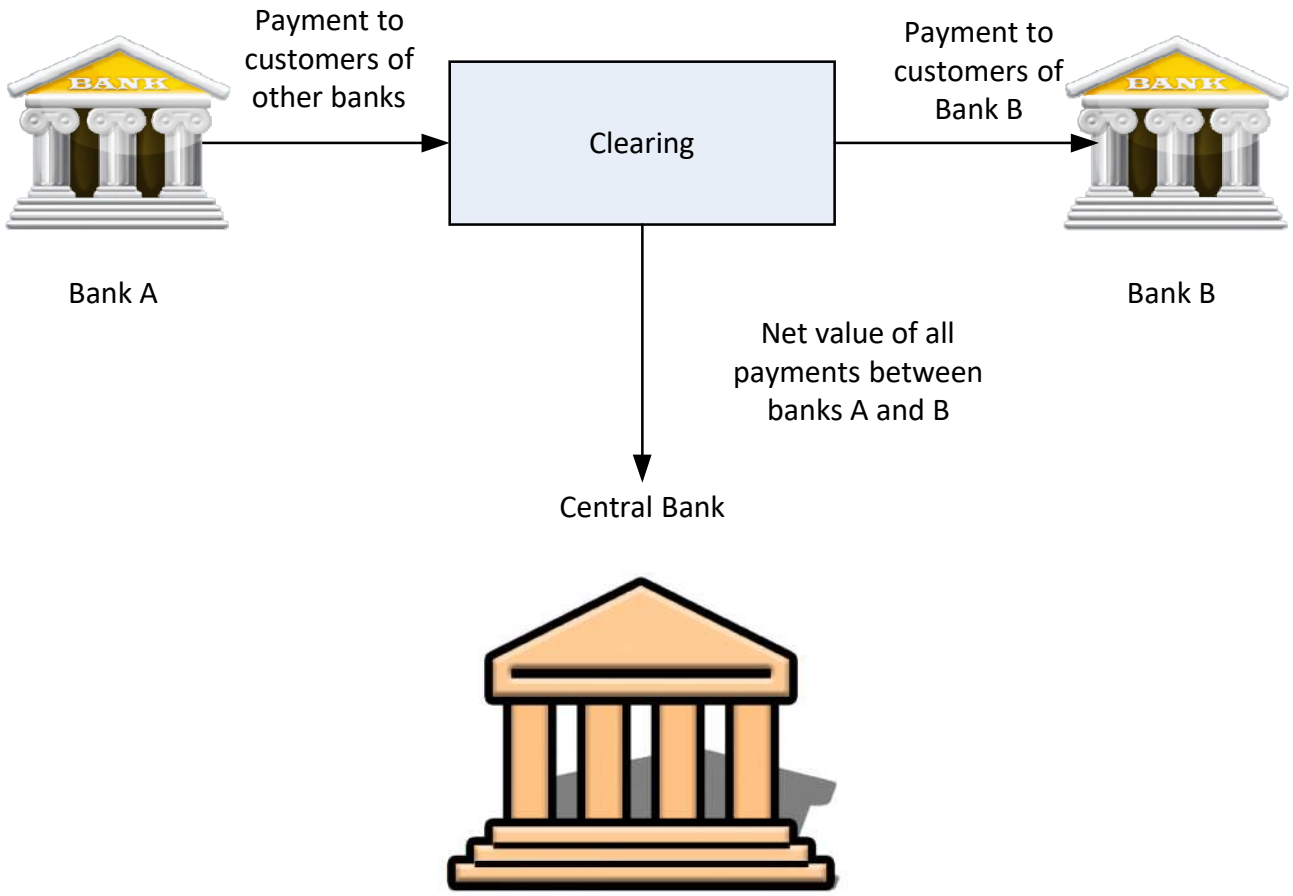
# Payment Intermediaries in Electronic Commerce






Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

# Settlement Systems






Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

# Clearing and Settlement

- Clearing & Settlement refers to the process where banks settle their accounts by exchanging money.
- All bank representatives usually meet every working day in a special *clearing house* and
  - Compare their respective credits in various financial instruments
  - Settle the account by exchanging money
- In electronic Clearing & Settlement, this process is done over computer networks.



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

# Classification of Settlement Networks

- Nature of the processing
  - large value systems
  - mass systems (many transactions of relatively small value)
- Ownership and management of the network
  - public network owned by the central bank
  - private network owned by members of a group of banks
  - private network leased to the banks on a use basis
- The way the settlement is done
  - real-time gross settlement (the same day)
  - netting (consolidation of various transactions to avoid paying settlement charges)



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

# United States

- Federal Reserve System
  - Central bank
  - Regulator
  - Operates the Fedwire service for large-value settlements
  - One of two large scale automated clearing house (ACH) networks
- Large-value Settlement Systems
  - Fedwire
  - CHIPS managed by the Clearing House Payments Company



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

# ACH (Automated Clearing House)

- Two operators
  - Electronics Payments Network (EPN)
  - Federal Reserve System
- Codes defined by the Electronic Payment Association
- WEB transaction codes for web transaction
  - Online-initiated ACH credit payments
  - Person to person (P2P) payments



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

# United Kingdom

- Clearing House Automated Payment System (CHAPS)
  - Euro component with the TARGET system
- Retail payments
  - Cheque & Credit Clearing Company Ltd. for paper credits and checks
  - BACS (Banker's Automated Clearing Service)
  - Faster Payment Service clears Internet and telephone payments up to £10,000 in 2 hours.



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

# France

- Large-value payments: TARGET2-Banque de France
- PNS
- Retail payment System



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual

# Drivers for Innovations in Banking and Payments

- Technical developments
- Business needs
- User preferences
- Legislations and regulations
- Standards
- Ideology



Protocols for Secure Electronic Commerce 3rd edition Sherif Solutions Manual