Master of Information Technology

Securing Electronic Payments - Introduction

MIT 4204 – E-BUSINESS APPLICATIONS AND STRATEGIES

K.D.C.G KAPUGAMA

University of Colombo School of Computing

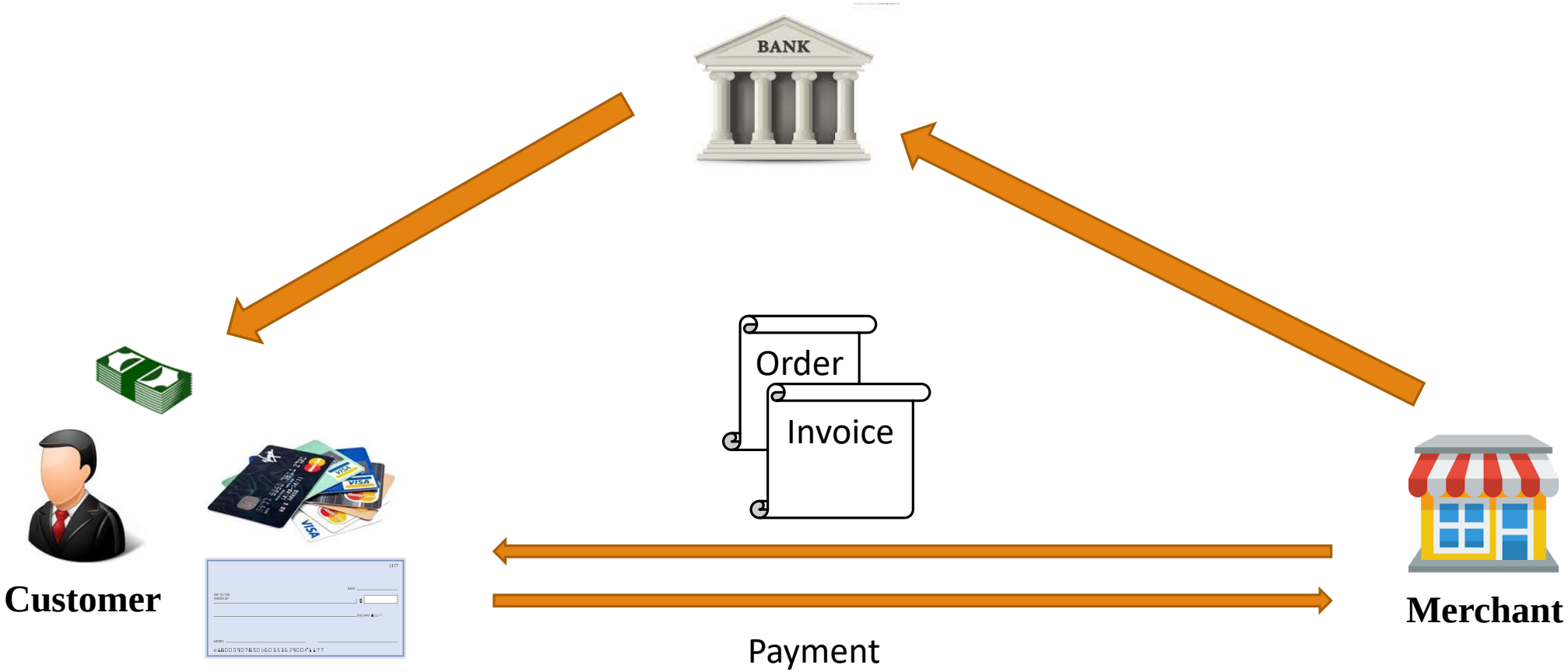
What do people do?

- Types of services:
  - Bill Payments
  - Purchasing items
  - Transfer of money
  - Borrow money
  - Seek information (Inquiries, Statements)
  - Cheat, Steal, and defraud

Classical Forms of Payments

- Involving Parties
  1. Customer
  2. Bank
  3. Merchant

Classical Forms of Payments



Instruments of Payments

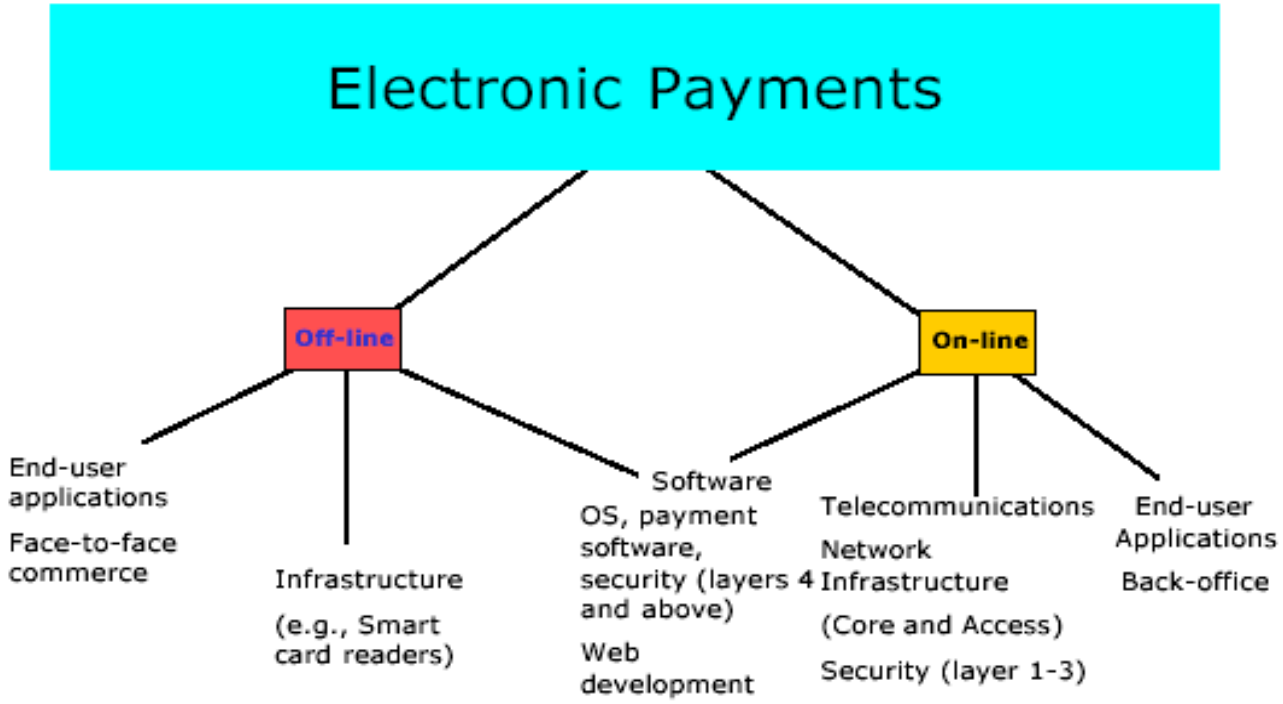
- Payment instruments are used to transfer the power of money from one economic agent to another. Some have a legal status, and some are banking inventions. E.g.

1. Cash
2. Checks
3. Credit transfers
4. Direct Debit
5. Inter-banks transfers
6. Bills of exchanges
7. Payment cards

Electronic Payments

- **Offline Payments**
  - Transactions that can be completed *without* an online connection.
- **Online Payments**
  - Transactions that need *real-time online connectivity*.

Electronic Payments



Requirements

- **Security**
  - Two people should be able to exchange digital cash without any part being able to alter or reproduce the electronic token.
  - The transaction protocol must ensure high-level security with sophisticated encryption techniques.
    - This involves using private key encryption
    - The authentication of sender and receiver involves digital signatures.
  - Online verification can prevent double spending, or other offline techniques must be used.

Requirements

- **User-Friendliness**
  - User *should not* have to understand the cryptographic techniques involved in the exchange.
  - The operation of the payment protocol should be transparent to the users
  - Digital cash should be simple to use
  - It should be easy to use from spending perspective and to accept as a form of payment.

  - Complicated systems are difficult to administer and raise the failure rate due to the errors of the user.
  - Simplicity leads to the acceptance by a large number of users.

Requirements

- **Portability**
  - People should be able to easily carry their digital cash and exchange it within alternative delivery systems.
  - Non-computer-network delivery channels should be able to handle digital money.
  - The security and use of digital cash should not depend on any physical location.
  - The cash can be transferred through computer networks and off the computer networks into other storage devices.
  - Digital wealth should not be restricted to a unique, proprietary computer network.

Requirements

- **Transferability**
  - Digital cash should be transferable to others users.
  - If I pay a bill for three friends, they should be able to easily transfer their share of the bill to me.
  - Peer-to-peer payments should be possible without a third party.
  - Neither party should be required to have registered merchant status.
  - Neither party should have to be online to do this
  - Digital money can then be used for gifts, charity, or tips
  - Other person-to-person payments become possible, like payments to children, friends or colleagues

Requirements

- **Anonymity**
  - Anonymous digital cash allows personal financial privacy.
  - It is untraceable.
  - A digital cash withdrawal cannot be associated with its subsequent deposit
  - Transactions made with it are unlinkable.
  - It is impossible to associate two different digital cash transactions made by the same person with each other

Requirements

- **Cost**
  - Depends on the complexity of information infrastructure.
  - Expenses of maintenance and quality assurance.
  - Outsourcing needs to be managed.

Requirements

- **Trust**
  - *Issue:* Customers do not trust an unknown faceless seller, paperless transactions, and electronic money. Thus, switching from a physical to a virtual store may be difficult.
  - Many unresolved legal issues on a global basis (e.g. lack of consumer protection or privacy protection)

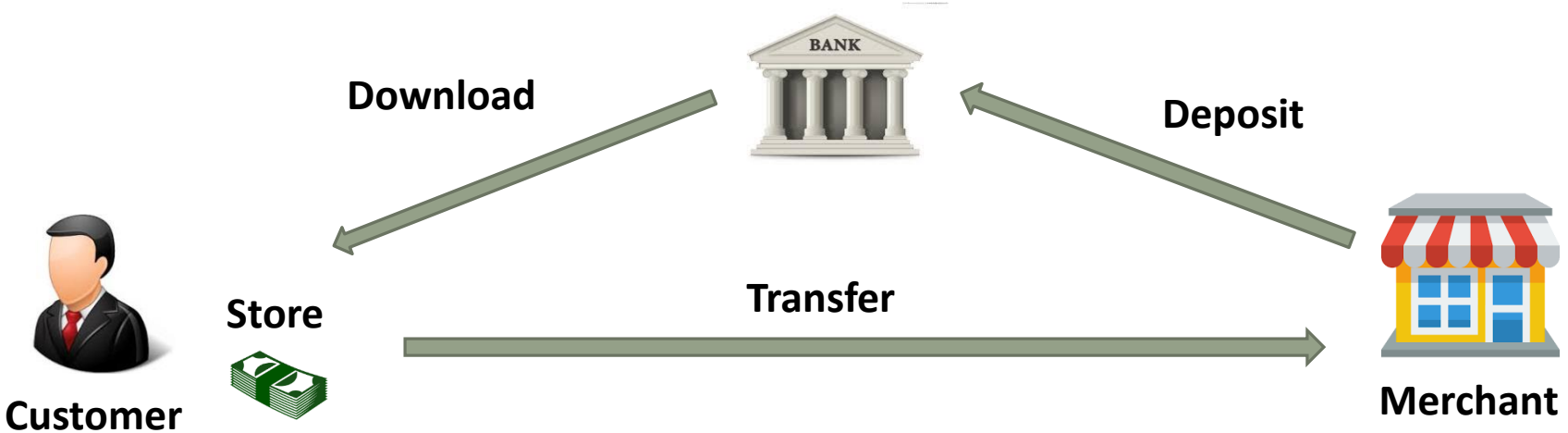
Characteristics of Payments

- **Characteristics:**
  - Where is the money (authorization)
  - Time of payment vs. time of order/shopping
- **Characteristics of payment methods.**

Type of payment	Money	Time
Cash	With Customer	At Purchase
Debit card	In Bank	At Purchase
Credit card	In Bank	After Purchase
Invoice	In Bank	After Purchase
Pre-paid	With Merchant	Before Purchase
Subscription	With Merchant	Before Purchase

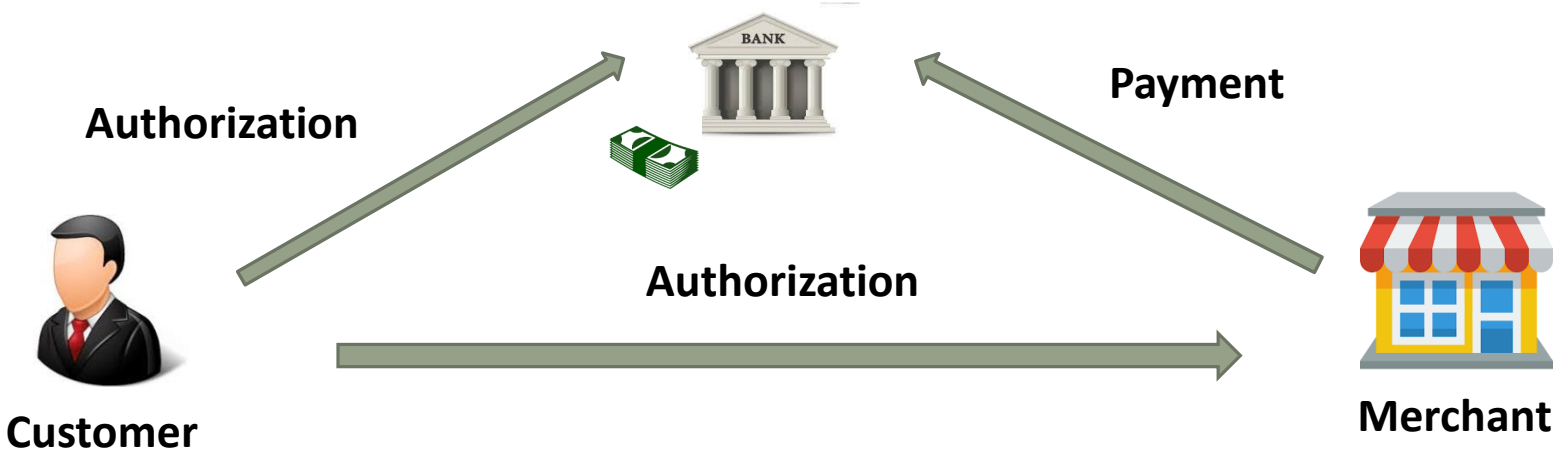
Internet Transactions

Type of payment	Money	Time
Cash	**With Customer**	At Purchase
Debit card	In Bank	At Purchase
Credit card	In Bank	After Purchase
Invoice	In Bank	After Purchase
Pre-paid	With Merchant	Before Purchase
Subscription	With Merchant	Before Purchase



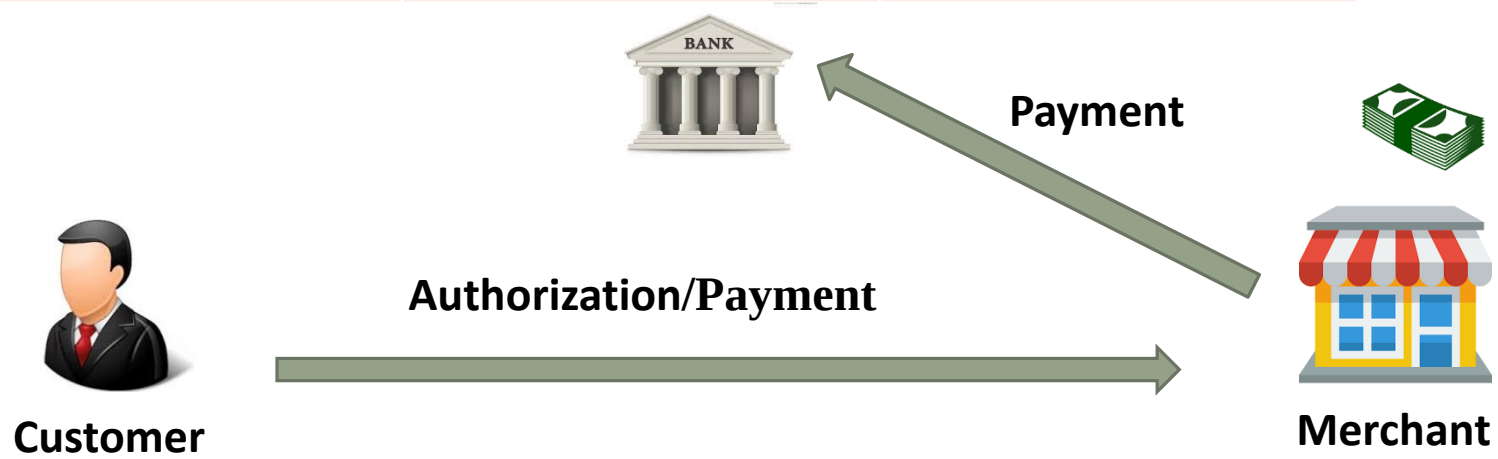
Internet Transactions

Type of payment	Money	Time
Cash	With Customer	At Purchase
Debit card	**In Bank**	At Purchase
Credit card	**In Bank**	After Purchase
Invoice	**In Bank**	After Purchase
Pre-paid	With Merchant	Before Purchase
Subscription	With Merchant	Before Purchase



Internet Transactions

Type of payment	Money	Time
Cash	With Customer	At Purchase
Debit card	In Bank	At Purchase
Credit card	In Bank	After Purchase
Invoice	In Bank	After Purchase
Pre-paid	**With Merchant**	Before Purchase
Subscription	**With Merchant**	Before Purchase



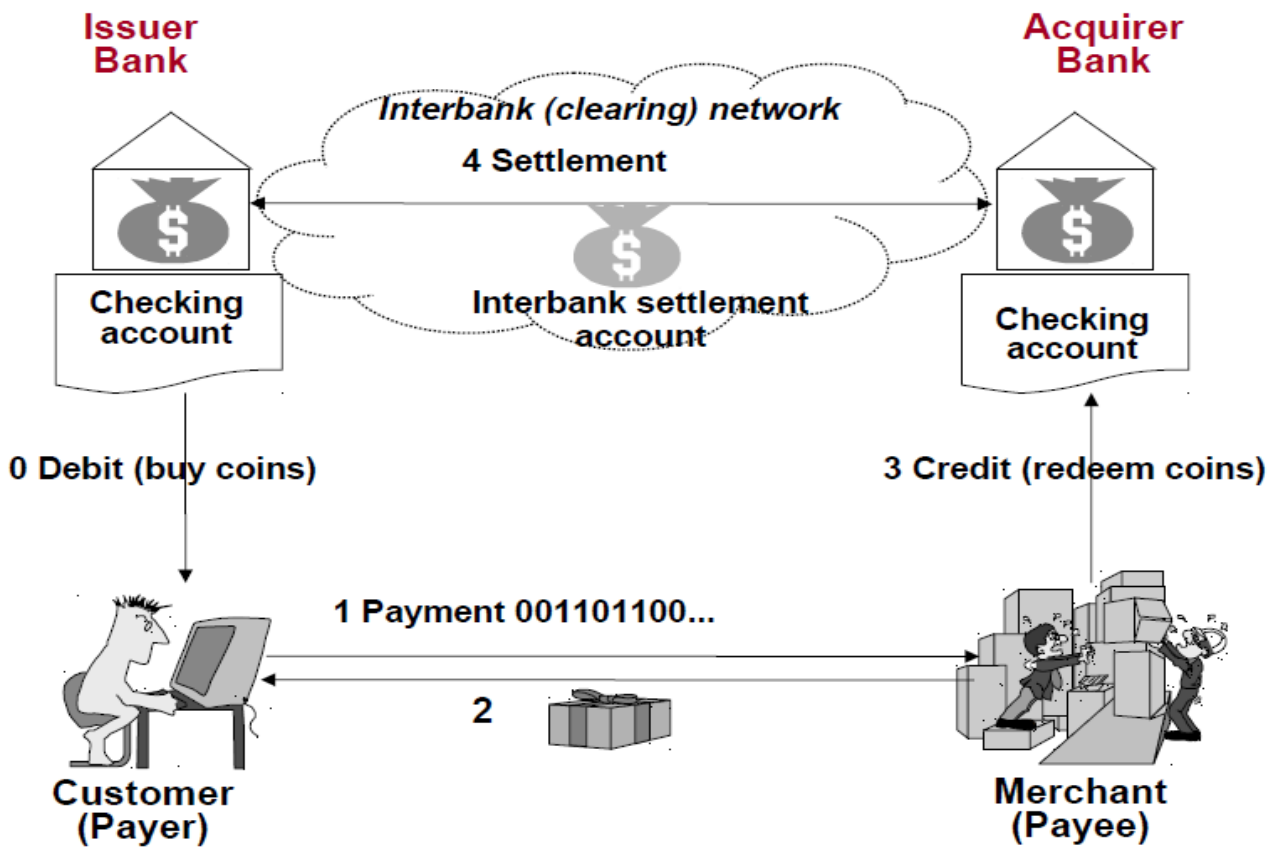
Types of Digital Payments

1. Digital Cash
2. Stored Money (Micropayments)
3. eCheck
4. eMoney Order
5. Debit Payment
6. Credit Payment
7. Invoice / Payment order
8. At delivery (Pay-per-view)
9. Subscription
10. Cryptocurrency

Digital Cash

- Amount of money in digital cash accounts
- Useful for those who are without credit cards
- Small amount of cash in the account
- Fewer security problems compared to credit cards

Digital Cash

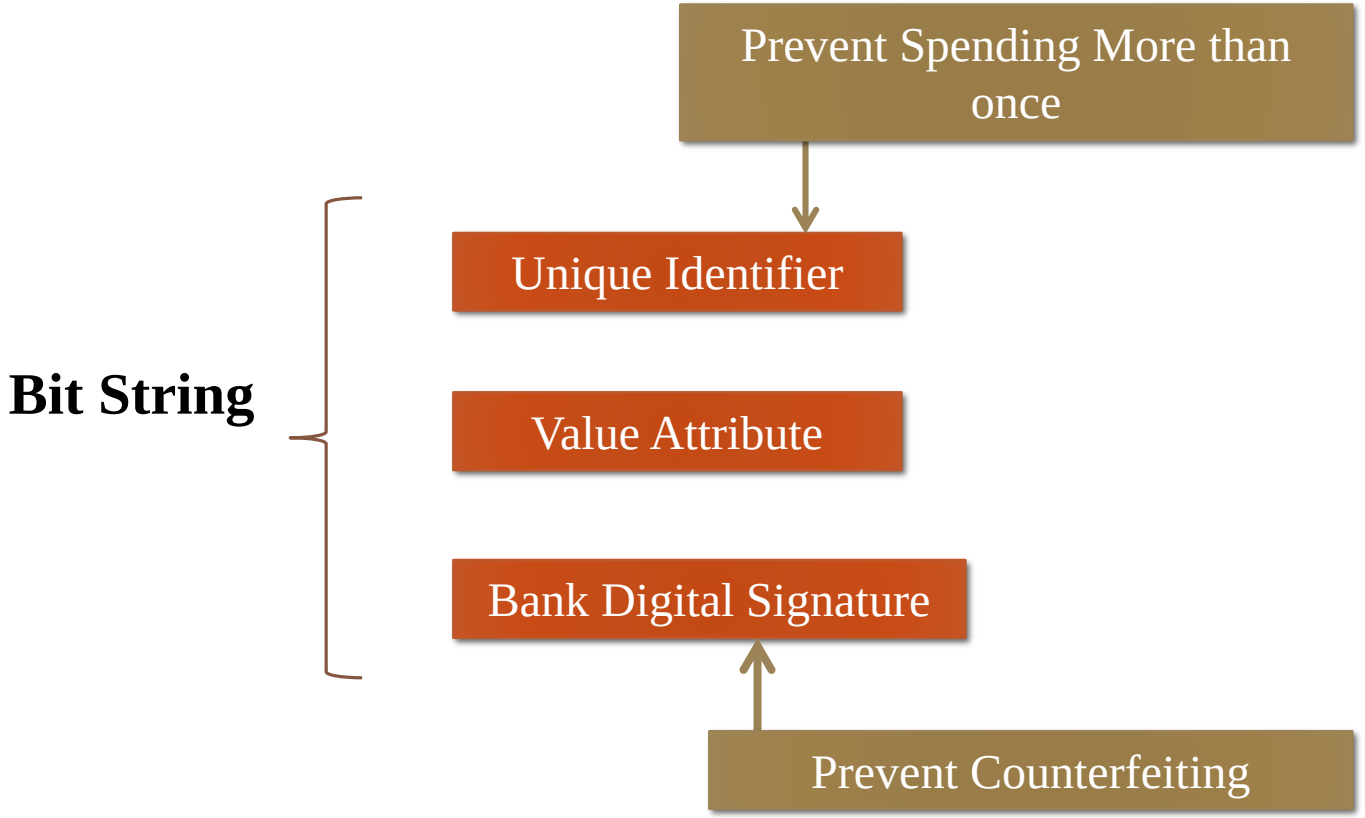


Digital Cash

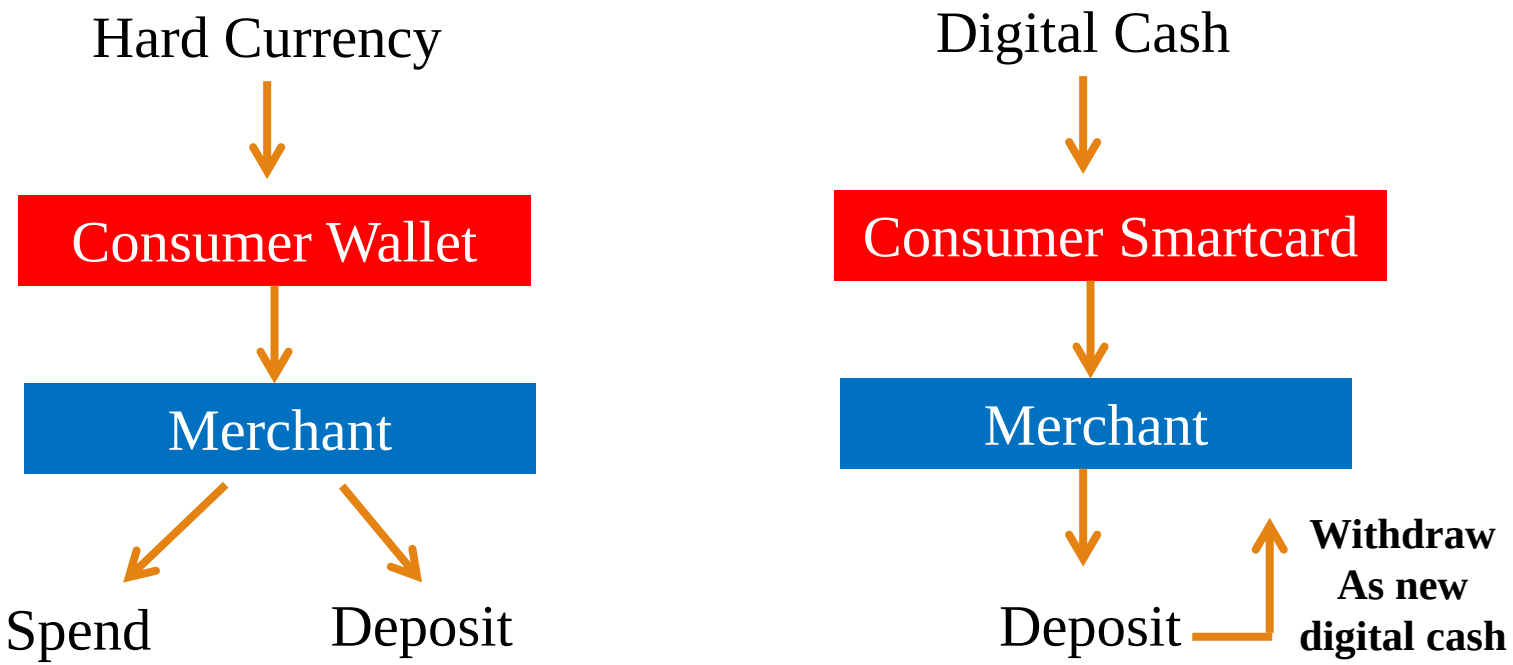
- Digital cash is represented by data. Hence, how do we prevent:
  - **Counterfeiting?**
  - **Multiple spending?**

1111100001101001111
1000111001100001110
1111001010100111011
0111010101110110011

What is a Digital Cash Token ?



Digital Cash must be deposited



Possible Characteristics of Digital Cash

- Anonymity of Consumer
  - Merchant knows who paid, but that information is not inherent to the digital cash itself.
  - Financial institution knows what merchant deposited.
- Attribution of Cheating
  - Double spending
- Authorized Traces

David Chaum and Anonymous eCash

- “The difference between a bad electronic cash system and well-developed cash system will determine whether we will have a dictatorship or a real democracy. “

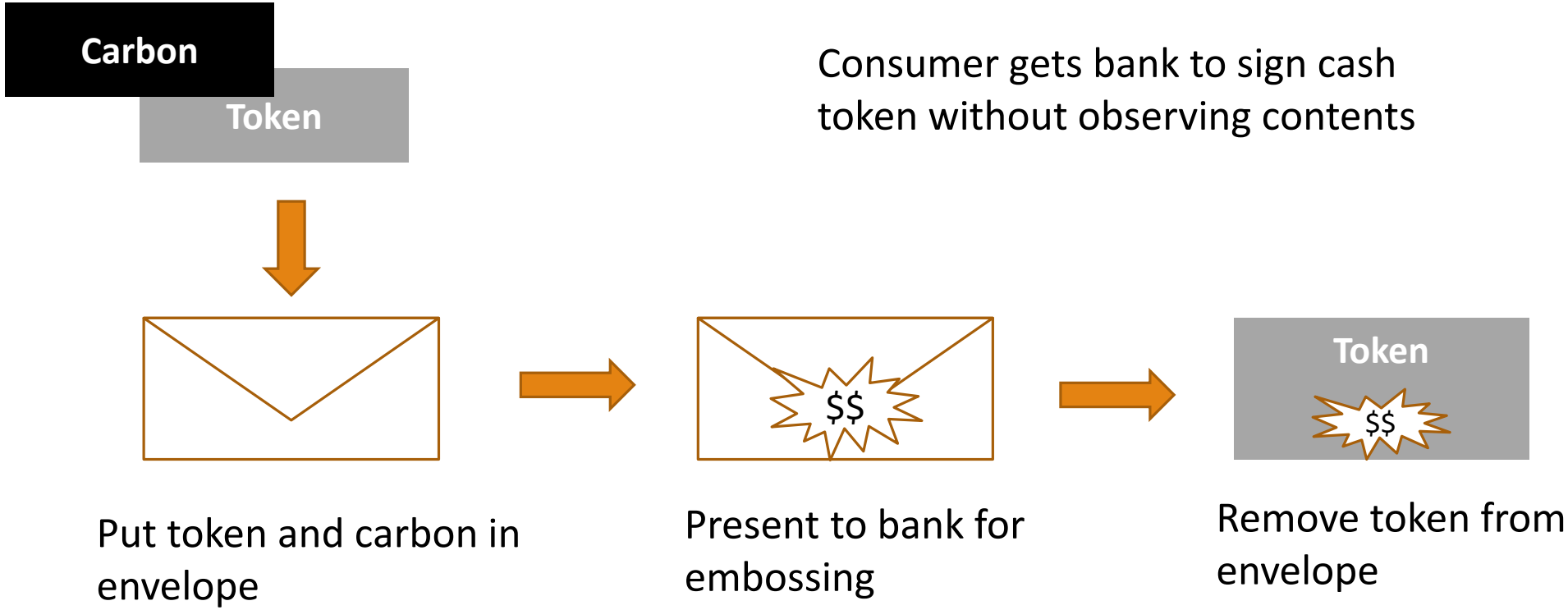
-attributed to Chaum-

Blind Signature

- Blind signature scheme is a protocol that allows the provider to obtain a valid signature for a message ***m*** from the signer without seeing the message and its signature
- If the signer sees the message ***m*** and its signature later, he can verify that the signature is genuine. However, he is unable to link the message-signature pair to the particular instance of the signing protocol which has led to this pair.

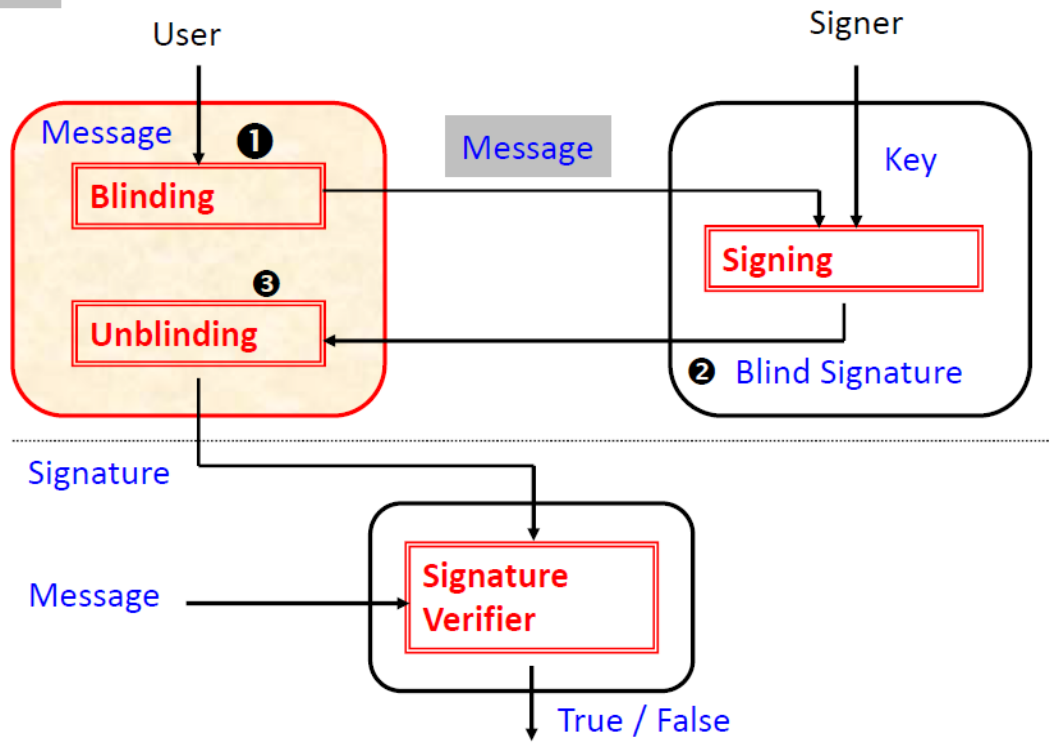
Blind Signature

- Analogy



Blind Signature

❶ "Message" : the **blinded** message



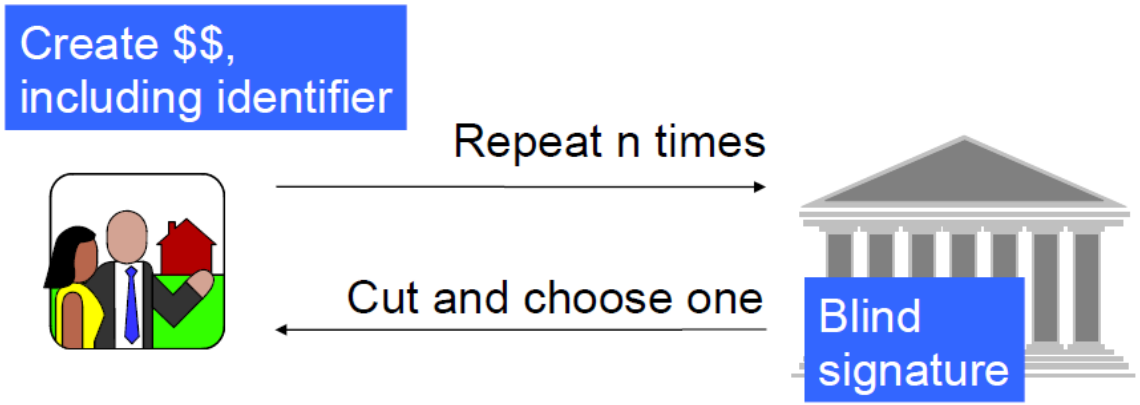
❸ Signature on "Message": to be obtained after **unblinding**

❷ Signature on "Message" : the **blind** signature

★ *Unlinkability*: it is intractable for the signer to link ❸ to ❷

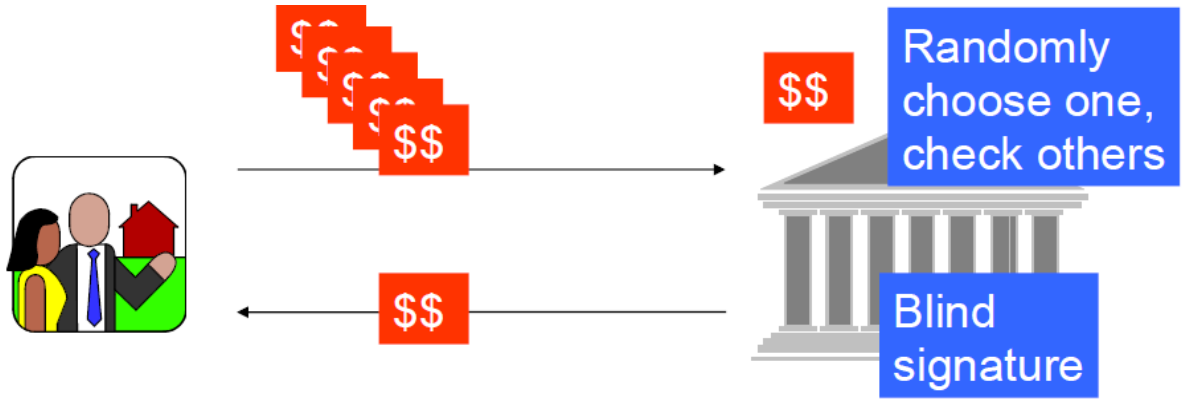
E.g.: https://en.wikipedia.org/wiki/Blind_signature

Spending Anonymity



If the consumer's software creates the digital cash, and the bank signs it blindly, the bank will not see the identifier. The **cut and choose protocol** assures the bank the $$ is genuine.

Cut and Choose Protocol



Although the bank cannot see what is being signed, with the cut and choose, the incentive of the consumer is to generate legitimate instances of digital cash.

Chaum's Anonymous eCash

- **Anonymous**
- **Secure** (no-double spending)
- Only **transfer** (no creation/storage)

DiGi CASH
NEXT GENERATION MOBILE PAYMENT

…and **bankrupted** in 1999

Micropayment

- A payment small enough that processing it is relatively costly. Note: processing one credit-card payment costs about 3%.
- A payment in the range 0.1¢ to $10
- Processing cost is the key issue for micropayment schemes. (There are of course other issues common to all payment schemes)

The Need of Micropayments

- “Pay-per-click” purchases on Web
  - Streaming music and video
- Mobile Commerce
  - Geographically based info services
  - Gaming
  - Small “real world” purchases
- Infrastructure accounting:
  - Paying for bandwidth

Digital Wallets

- Allows customer to store name, address, credit card information on an electronic device or software.
  - Benefit is that the customer enters information just once.
- **Sever-side digital wallet** stores information on remote sever of merchant or wallet publisher.
  - A security breach can reveal thousands of users' personal information to unauthorized parties – Google wallet, Microsoft Windows Live ID, Yahoo! Wallet
- **Client-side digital wallet** stores information on consumers computers.
  - Must download wallet software onto every computer.

Stored Money (EMV) – Chip Card

In 1994
Europay International,
MasterCard International
Visa

Merchants

Hardware Digital Wallets

- Implemented using smart phones or tablets.
- Store owner's identity credentials (driver's license, medical insurance card, store loyalty cards, etc)
- Transmit portions of information using Bluetooth or wireless transmission to nearby terminal.
- Near field communication (NFC) technology can be used if equipped with NFC chip
- E.g. Google Wallet, Android Pay and Apple Pay.
- Security and privacy are major concerns (Must prevent unauthorized access)

The Failure of Digital Cash

- There have been several proposals for digital money. Until a few years ago, all had failed.
- No gain over existing systems:
  - Still need a central point of trust.
  - Privacy: Who monitors the system?
  - Can we entrust a bank with managing an entire currency.
- **Note the difference:**
  - **Digital cash**: Electronic version of existing currency (USD)
  - **Digital currency:** Entirely new currency (i.e. Bitcoin)