


第三讲 电子商务支付工具

北京大学计算机系电子商务实验室

- 
- 5.1 电子支付的概念及发展
 - 5.2 电子交易模型
 - 5.3 信用卡支付方式
 - 5.4 数字现金支付方式
 - 5.5 电子支票支付方式
 - 5.6 网上银行



5.1 电子支付的概念及发展

■ 5.1.1 电子货币


● 1. 电子货币的定义

所谓电子货币是指一种表示现金的加密序列数，它可以用来表示现实中各种金额的币值(就像人民币元一样，人民币只是一些用各类图像标记加以区分的特殊的纸张)。

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

3



使用电子货币具有很多优点

- 人们通过网络可以迅速地将其送至远处，以完成支付过程
- 可确保支付过程的匿名性和准确性
- 具有比现金支付高得多的安全性

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

4



2002-3-23

● 2.电子货币存在的问题

- 观念上：从传统纸币到 0 和 1 构成的数字货币
- 技术上：纠错、校验能力
- 法规上：制定法律
- 安全上：遗失、电磁攻击、黑客攻击、删改
- 应用上：环境支持，包括人员和设备

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

5




2002-3-23

● 3.电子货币的发展策略

- 严格管理
- 明确可靠的法律准备
- 技术安全保障
- 防止犯罪活动
- 货币统计报告
- 可回购
- 储备要求
- 加强国际性合作

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

6




2002-3-23

■ 5.1.2 电子支付的定义及特点

- 1989年美国法律学会的《统一商业法》中定义：电子支付是支付命令发送方把存放于商业银行的资金，通过一条线路划入收益方开户银行，以支付给收益方的一系列转移过程。
- 电子支付是以金融电子化网络为基础，以商用电子化机具和各类交易卡为媒介，以计算机技术和通信技术为手段，以电子数据(二进制数据)形式存储在银行的计算机系统中，并通过计算机网络系统以电子信息传递形式实现流通和支付。

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

7



2002-3-23

电子支付具有以下特点：

- 以计算机技术为支撑，进行储存、支付和流通
- 集储蓄、信贷和非现金结算等多种功能为一体
- 可广泛应用于生产、交换、分配和消费领域
- 使用简便、安全、迅速、可靠
- 电子支付通常要经过银行专用网络

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

8

■ 5.1.3 电子支付的发展

- 第一阶段是银行利用计算机处理银行之间的业务，办理结算
- 第二阶段是银行计算机与其他机构计算机之间资金的结算
- 第三阶段是利用网络终端向客户提供各项银行服务
- 第四阶段是利用银行销售点终端(POS)向客户提供自动的扣款服务
- 第五阶段是最新发展阶段，电子支付可随时随地通过互联网络进行直接转账结算，形成电子商务环境。

2002-3-23

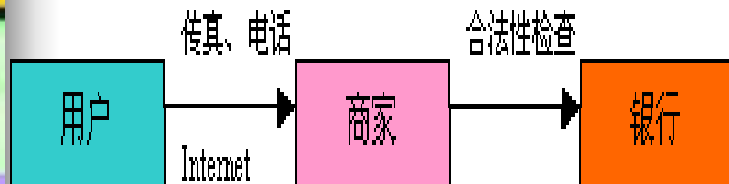
北京大学计算机科学技术系(版权所有，未经许可，不得转载)

9

5.2 电子交易模型

■ 5.2.1 支付系统无安全措施模型


- 1. 流程



2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

10




- 2.特点
 - 风险由商家承担
 - 商家完全掌握用户的信用卡信息
 - 信用卡信息的传递无安全保障

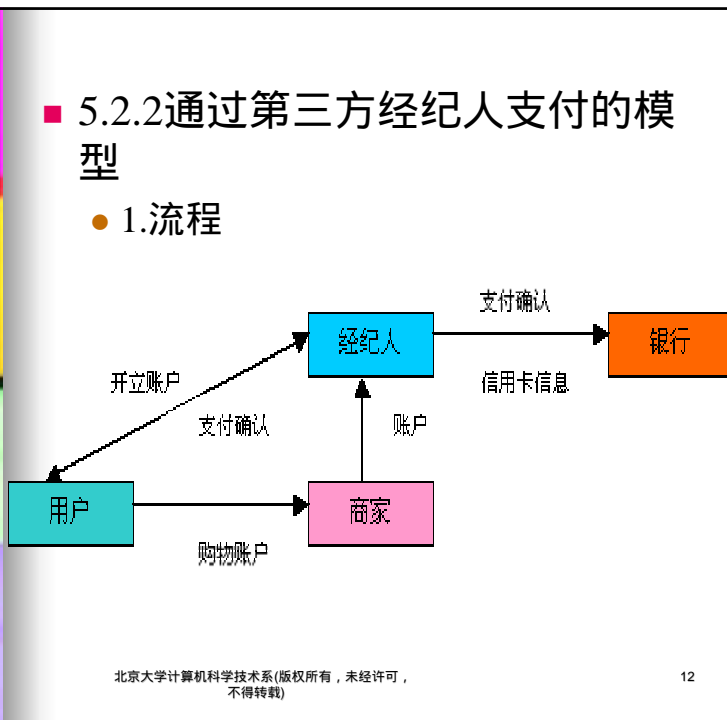
2002-3-23

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

11



- 5.2.2通过第三方经纪人支付的模型
 - 1.流程



```
graph LR; User[用户] -- 开户 --> Broker[经纪人]; User -- 支付确认 --> Broker; User -- 购物账户 --> Merchant[商家]; Merchant -- 账户 --> Broker; Broker -- 支付确认 --> Bank[银行]; Bank -- 信用卡信息 --> Broker;
```

2002-3-23

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

12




- 2.特点
 - 用户账户的开设不通过网络
 - 信用卡信息不在开放的网路上传送
 - 通过电子邮件来确认用户身份
 - 商家自由度大，风险小
 - 支付是通过双方都信任的第三方(经纪人)完成的

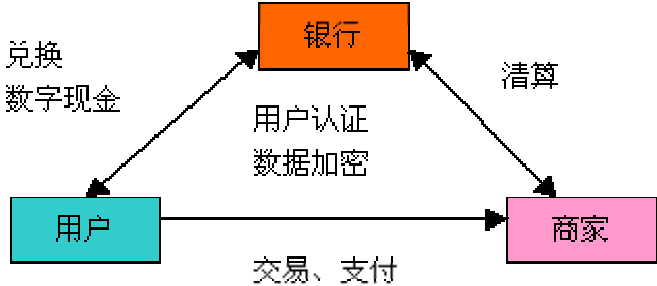
2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

13



- 5.2.3数字现金支付模型
 - 1.流程



2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

14




● 2.特点

- 银行和商家之间应有协议和授权关系
- 用户、商家和数字现金的发行都需要使用数字现金软件
- 适用于小额交易
- 身份验证是由数字现金本身完成的
- 数字现金的发行负责用户和商家之间实际资金的转移
- 数字现金与普通现金一样，可以存、取和转让

2002-3-23

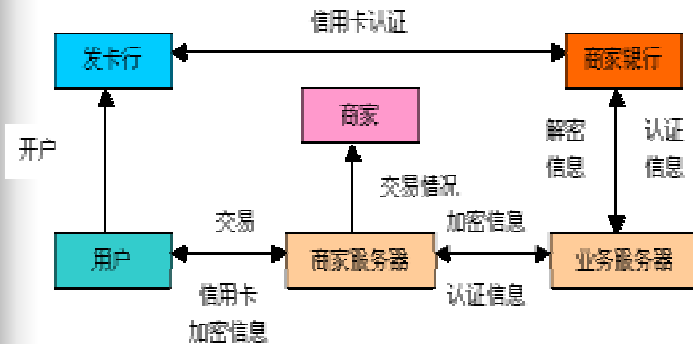
北京大学计算机科学技术系(版权所有，未经许可，不得转载)

15



■ 5.2.4简单加密支付系统模型

● 1.流程



```

graph TD
    User[用户] -- 开户 --> Issuer[发卡行]
    Issuer -- 信用卡认证 --> MerchantBank[商家银行]
    MerchantBank -- 认证信息 --> BusinessServer[业务服务器]
    BusinessServer -- 解密信息 --> MerchantBank
    MerchantBank -- 交易情况 --> Merchant[商家]
    Merchant -- 交易 --> User
    User -- 信用卡 --> MerchantServer[商家服务器]
    MerchantServer -- 加密信息 --> BusinessServer
    BusinessServer -- 认证信息 --> MerchantServer
  
```

The flowchart illustrates the process of a simple encrypted payment system. It involves several entities: the User (用户), Issuer (发卡行), Merchant Bank (商家银行), Business Server (业务服务器), Merchant Server (商家服务器), and Merchant (商家). The process starts with the User opening an account (开户) with the Issuer. The Issuer then performs a credit card authentication (信用卡认证) with the Merchant Bank. The Merchant Bank sends authentication information (认证信息) to the Business Server, which in turn sends decryption information (解密信息) back to the Merchant Bank. The Merchant Bank then provides transaction status (交易情况) to the Merchant. The User makes a transaction (交易) with the Merchant. The User also sends a credit card (信用卡) to the Merchant Server, which sends encrypted information (加密信息) to the Business Server. The Business Server then sends authentication information (认证信息) back to the Merchant Server.

2002-3-23

北京大学计算机科学技术系(版权所有，未经许可，不得转载)

16



2002-3-23

- 2.特点
 - 信用卡等关键信息需要加密
 - 使用对称和非对称加密技术
 - 可能要启用身份认证系统
 - 以数字签名确认信息的真实性
 - 需要业务服务器和服务软件的支持

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

17



2002-3-23

- 5.2.5SET (Security Electronic Transaction) 模型
 - 1.SET的目标
 - 信息在互联网上安全传输, 不能被窃听或篡改
 - 用户资料要妥善保护, 商家只能看到订货信息, 看不到用户的账户信息
 - 持卡人和商家相互认证, 以确定对方身份
 - 软件遵循相同的协议和消息格式, 具有兼容性和互操作性

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

18

● 2.SET标准的内容

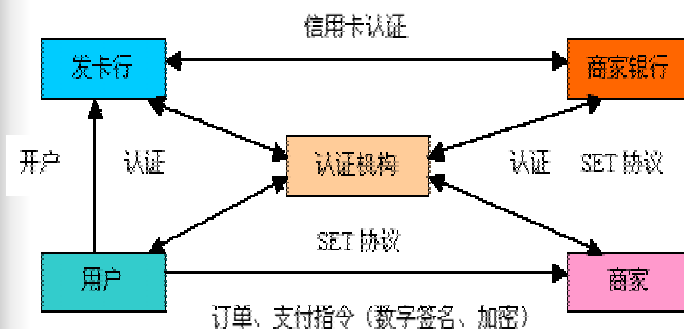
- 加密算法
- 证书信息及格式
- 购买信息及格式
- 认可信息及格式
- 划账信息及格式
- 实体之间消息的传输协议

2002-3-23

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

19

● 3.流程



2002-3-23

北京大学计算机科学技术系(版权所有, 未经许可, 不得转载)

20



2002-3-23

● 4.SET协议的安全措施

- 加密技术：同时使用公钥与私钥
- 数字签名技术
- 电子认证
- 电子信封