8.3 区块链与电子化隐私

01 可控匿名

- **常见运用场景：**电子货币
- **保障方式：**形成去中心化体系，无中心化机构收集管理用户数据，保障数据私密性
- **技术目标：**保障货币使用者的信息隐私
- **存在的问题：**允许永久的第三方匿名，可能变相鼓励如逃税、恐怖融资和洗钱等犯罪行为
- **解决办法：**实现**可控的匿名性**，只向特定的组织和机构披露必要的数据

02 可控匿名的实现方式

货币或资产的一个重要的因素是**流通**。

通过流通实现和真实世界的**交互**，丰富信息，使交易者**身份立体化**，使得匿名可控。

匿名是一种设计，**“基于密钥”**而非“基于身份”。

交易过程中不透露交易双方个人信息，但最终保证每笔交易**有迹可循**。

03 达世币

- 是一种**匿名性良好**的虚拟货币
- 匿名程度高，交易**无法被追踪和查询**
- 适用于**不想暴露交易记录和财政隐私**的用户
- 由想进行匿名交易的交易者发起匿名申请，通过**主节点进行混币**后，随机分发混合后货币

04 PrivateData技术

- **应用：**Hyperledger 和 Fabric1.2.0
- **目标：**增强用户之间数据的私密性
- **实现方式：**
  - 实际的隐私数据+隐私数据的哈希值=隐私数据集合（private data collection）
  - 实际的隐私数据通过gossip协议传播，有权限看到这些数据的节点收到数据
  - 隐私数据被保存在本地的private state database数据库中，orderer无法看到数据本身
  - 链上仅记录隐私数据的hash，真正的隐私数据通过gossip协议在节点之间广播
- **意义：**定义隐私分享策略，使得机构组织可以**选择性分享**隐私数据

05 身份混合（Identify Mixer）

- **实质：**加密协议套件
- **应用：**Fabric 1.3版本
- **价值：**
  - 强大的身份验证及隐私保护功能，如：无需披露交易身份即可进行交易
  - 不可追踪性，如：单个身份发送多个交易不会泄露交易是通过相同的身份发送的能力
- **实现方式：**
  - 发行者将证明一组用户的属性以数字证书的形式发布，叫做“凭证”
  - 用户稍后生成拥有凭证的“零知识证明”，并且还选择性地仅公开用户选择显示的属性
  - 该证明不会向出发布的用户以外的任何验证者、发行者或任何其他人显示其他信息

06 区块链在隐私保护中的不足

- 1、区块链技术处于发展初期，技术更新快，技术细节存在不完善
- 2、由于区块链技术日益普及和推广，涉及的用户和资产数量也不断上升而带来的隐私保护的难度和风险的提升