数字货币和区块链

- 中心化数字货币

山东大学网络空间安全学院

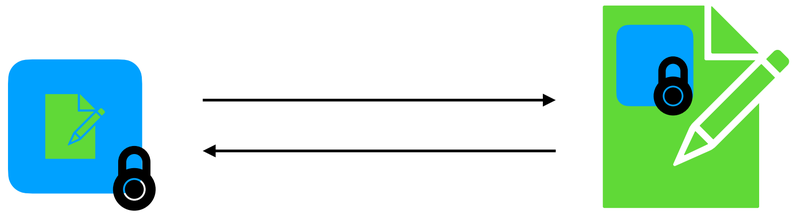
钱宸 2023年11月13日

数字货币

- 中心化数字货币定义与安全性
- 基于离散对数的数字货币
- 可传递数字货币定义
- 可传递数字货币构造

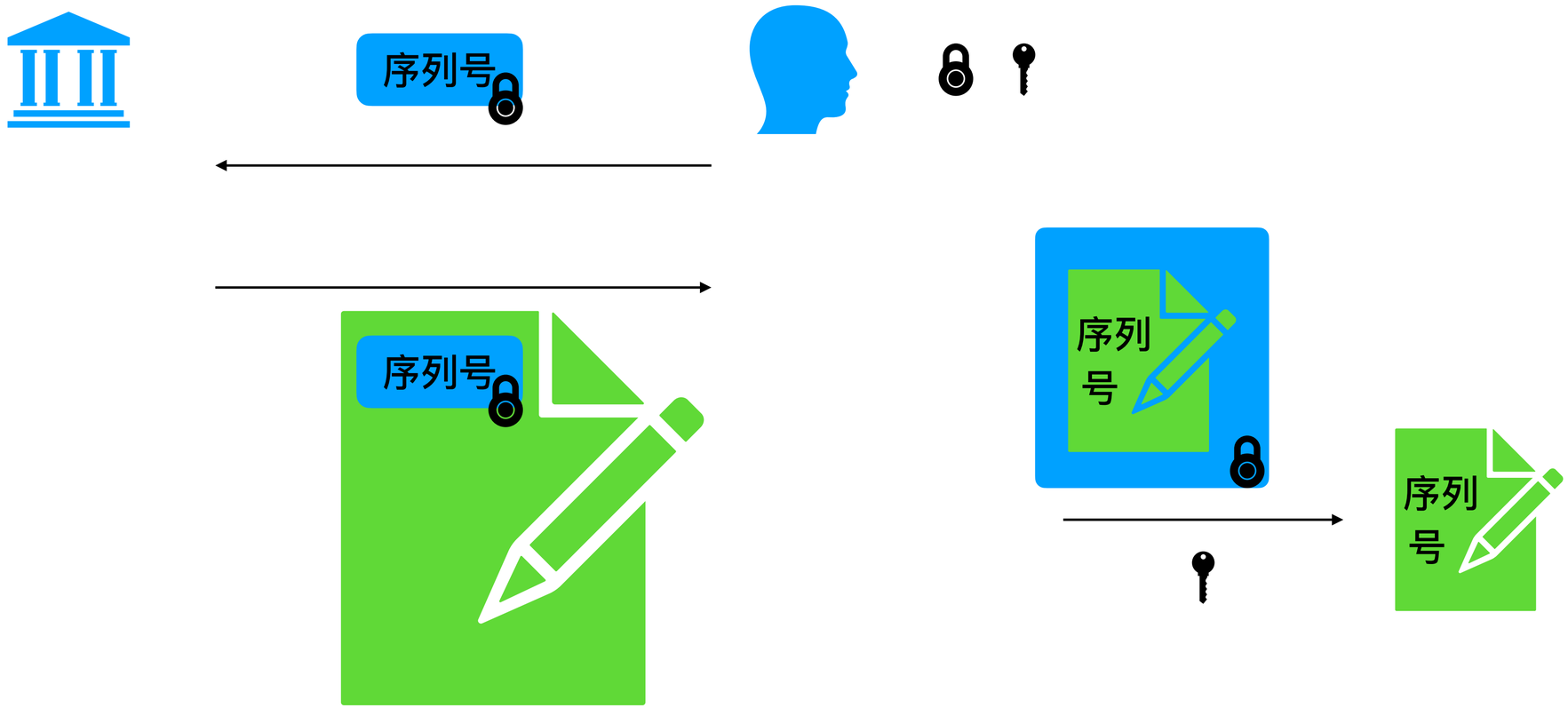
现金数字货币探索（二）

- 1988年David Chaum提出利用盲签名的方式来同时解决匿名性和双支付攻击
- 盲签名的重要特性：



现金数字货币探索（二）

- 如何利用盲签名的性质设计数字现金?



现金数字货币探索（二）

- Chuam电子货币的优缺点：
  - 匿名性：发送给银行的是加密信息，银行无法知道具体序列号✔
  - 中心服务器需要参与每一笔交易✘
  - 无法离线进行交易✘

现金数字货币探索（三）

- 1988年David Chaum, Amos Fiat & Moni Naor：离线双支付检测
- 不可思议！
  - 传统货币的不可复制性来源于特殊的纸张，油墨，水印的难复制特性
  - 数字货币是数字信息，可以实现完美复制（每个比特都相同）

现金数字货币探索（三）

- 解决方案?
  - 从信用货币中汲取灵感
  - 为了保证信用卡支付的安全性，每一笔信用卡支付实际需要经过联网认证
  - 那飞机上的信用卡如何支付?
    - 基于信用的支付方式
    - 支付结束后对双支付的检测

现金数字货币探索（三）

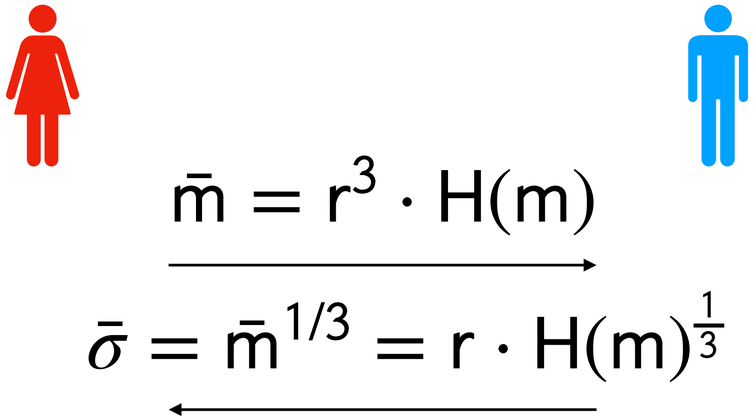
- David Chaum, Amos Fiat & Moni Naor 共同设计了一种加密算法
  - 电子货币中加密了身份信息
    - 即使银行也无法解密
  - 每次支付的时候，接受随机人让你解密一部分信息
  - 双支付发生了以后，两个不同的电子支付可以让银行追踪到个人信息

中心化的数字货币

- 盲签名系统
  - 解决数字货币的匿名性问题
- 抵御双支付攻击
  - 解决数字货币的伪造重用问题

数字货币 - Chaum-RSA-FDH

- 我们从盲签名算法开始：
  - RSA-FDH（RSA- Full Domain Hash）
    - $\mathrm{pk} = \mathrm{N}, 3, \mathrm{sk} = 1/3 \mod \phi(\mathrm{n})$
    - 信息盲化：$\bar{\mathrm{m}} = \mathrm{r}^3 \cdot \mathrm{H}(\mathrm{m})$
    - 盲签名：$\bar{\sigma} = \mathrm{r} \cdot \mathrm{H}(\mathrm{m})^{\frac{1}{3}}$



数字货币 - 抵御双支付攻击

- 如何生成可以抵抗双支付攻击的序列号?
- $f_{\mathsf{SN}}(id, n_s, n_r)$满足：（其中$n_s$是发送者的随机数，$n_r$是接收者的随机数）
  - 没有n_s的情况下算不出$f_{\mathsf{SN}}(id, n_s, n_r)$ - 货币安全性
  - 给出$f_{\mathsf{SN}}(id, n_s, n_r)$和$f_{\mathsf{SN}}(id, n_s, n_r')$且$n_r \neq n_r'$的时候，能算出$id$。
- $f_{\mathsf{SN}}(id, n_s, n_r) = pk_s^{n_r}\mathsf{H}(n_s)$
  - 货币安全性 → 哈希函数的随机性
  - 抗碰撞性 →$pk_s = (f_{\mathsf{SN}}(id, n_s, n_r) \cdot f_{\mathsf{SN}}(id, n_s, n_r)^{-1})^{1/(n_r - n_r')}$

中心化数字货币数字货币

- Alice通过与Bob的交互产生$f_{\mathsf{SN}}(pk_A, n_a, n_b)$
- Alice向银行获取$f_{\mathsf{SN}}(pk_A, n_a, n_b)$的盲签名$\sigma$，并将$(f_{\mathsf{SN}}(pk_A, n_a, n_b), \sigma)$发送给Bob
- Bob验证签名安全性，将钱存入银行