数字货币和区块链 - 简介

山东大学网络空间安全学院

钱宸 2023年10月25日

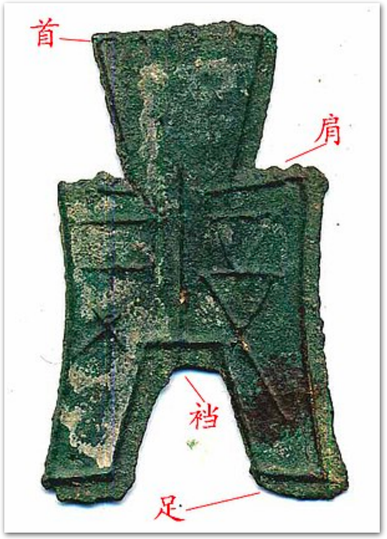
目录

什么是货币?

- 中国古代货币演变

贝币（夏商）

铜贝（西周）



布币（春秋）

飞钱（唐）

以物易物 →信用货币

什么是货币?

- 理想化的货币?
  - 易用性：可以轻易交易
  - 保真性：难以被伪造和复制
  - 匿名性：用途和归属保密
  - 价值：可以被证明价值

什么是货币?

- 矛盾的属性
  - 易用 VS 稀缺 （贝壳/黄金）
  - 能够轻易传递 VS 不可被复制（数字货币/实体货币）
  - 唯一且匿名 VS 可被可靠认证（硬币/信用卡）

什么是货币？（价值）

- 货币价值来源：
  - 是什么 - 现金
    - 贵金属（金银）
  - 能用来做什么 - 信用
    - 信用卡（飞机上刷卡）

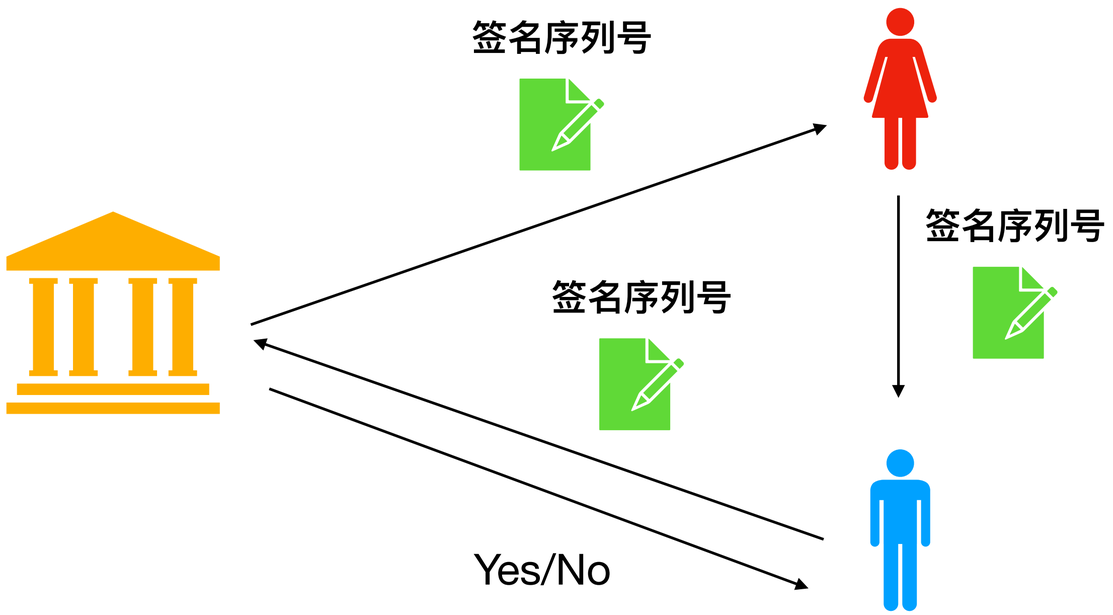
数字货币?

- 如何赋予数字信息价值？？
  - 易用性✔（Easy）
  - 保真性✘（Hard）
  - 匿名性✔（Easy）
  - 价值✘（Hard）

基于信用的货币初次探索

- 点对点分布式文件分享系统（Peer-to-Peer：P2P）
  - 每个用户在下载文件的同时，也作为分布式分享文件的节点提供他人下载
  - 然而，分享文件完全基于信用原则。只下载不分享的行为使得整个系统无法正常运转。
  - 解决方式：引入现金的概念（Mojo nation/Karma/百度文库）
    - 分享的用户获取虚拟代币作为回报
    - 下载需要通过支付虚拟代币进行

信用数字货币探索（一）



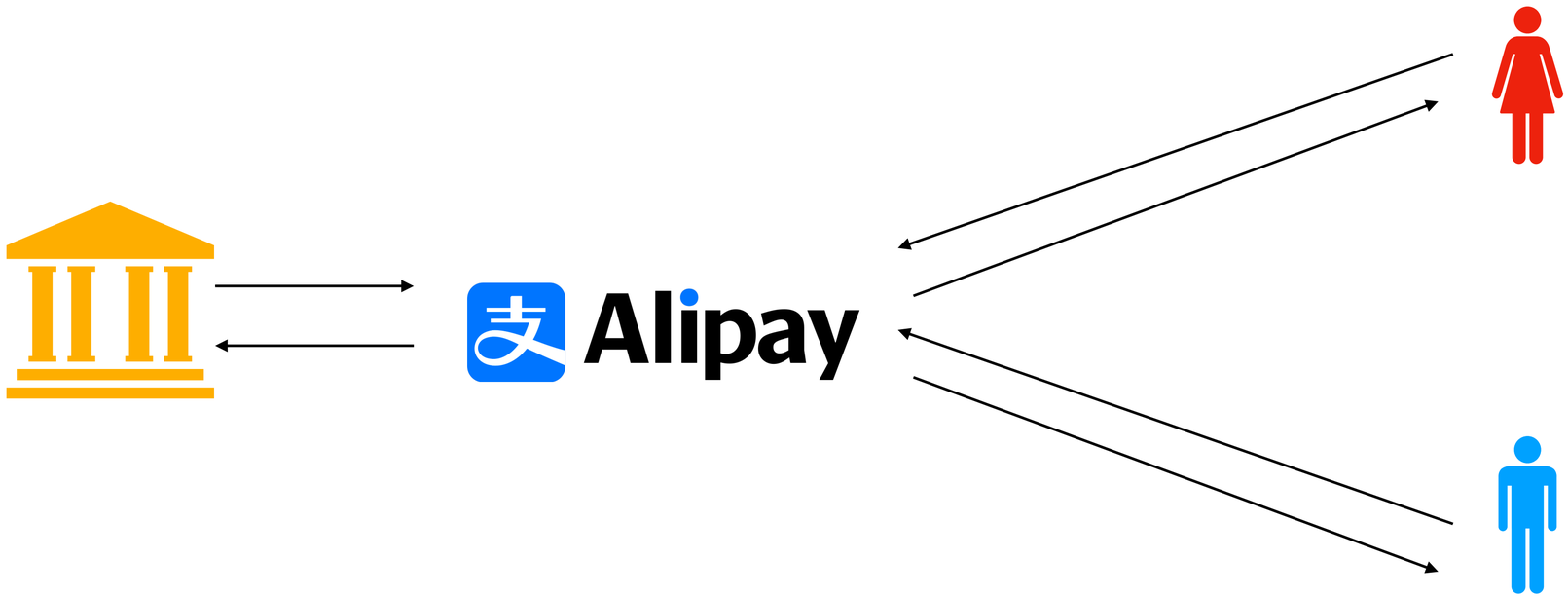
- 银行首先查询Alice有足够的余额
- 生成唯一的序列号并签名
- 银行将签名与序列号发送给Alice
- Alice将签名与序列号发送给Bob
- Bob询问银行签名与序列号是否使用过
- 如果序列号没有被使用过银行交易完成

信用数字货币探索（一）

- 签名序列号带来的问题：对应之前数字货币提到的性质
  - 易用性：数字文件✔
  - 保真性：数字签名保证序列号的真实性/收到后必须立即联系银行，否则可以复制数字签名✔ and ✘
  - 匿名性：完全不匿名，交易的人员和交易金额都要告知商户和银行才可以✘
  - 价值：银行信用背书✔

信用数字货币探索（二）

- 如何解决数字货币的匿名性问题?
  - 尝试：中介式服务（Paypal/支付宝）

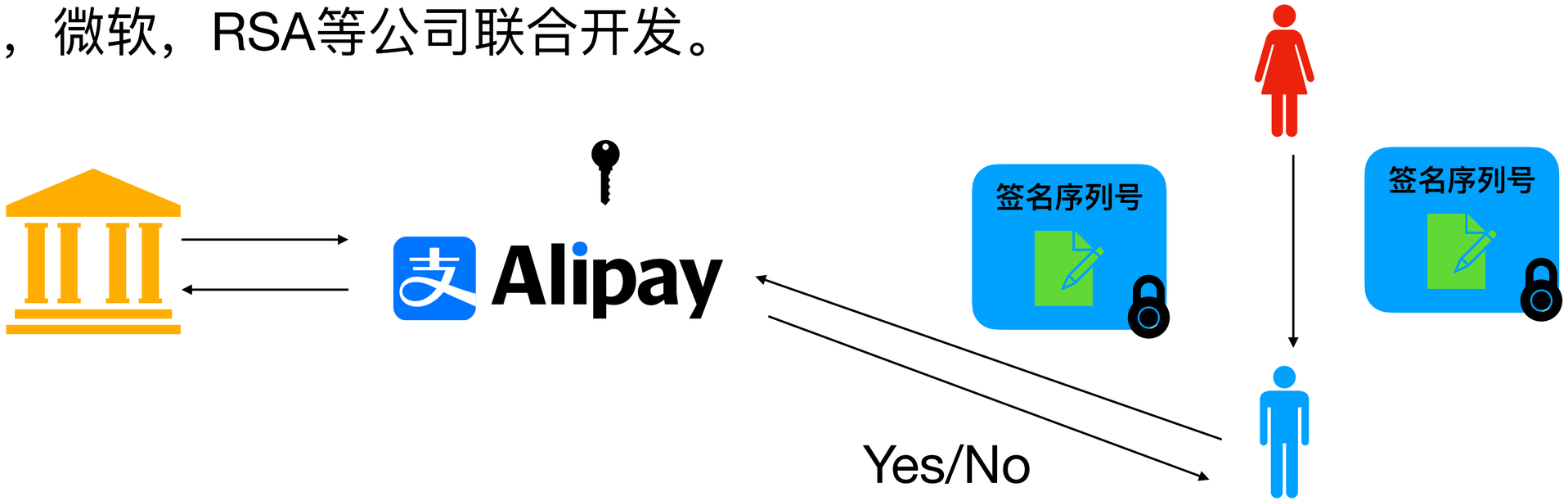


信用数字货币探索（二）

- 引入中介的好处：
  - 银行信息不需要直接告知个体商户
  - 银行信息交给可信度较高的知名企业
- 坏处：
  - 用户和商户都需要通过中介进行沟通
  - 交易过程增加了复杂性（1994年刚开始有https，整个过程需要通过电子邮件无法实时）

信用数字货币探索（三）

- 为了解决商家与用户之间的交流不畅的缺陷 →引入加密算法
- 将银行信息加密后发送给商户→只有中介可以解密
- 90年代中期，SET （Secure Electronic Transaction）由VISA，MasterCard，IBM，微软，RSA等公司联合开发。



信用数字货币探索（三）

- 几个小趣事：
  - SET本身是信用货币，1994年建立的CyberCash公司采用了SET体系，但是也引入了网络币（CyberCoin）的数字币用于小额支付
  - 90年代，加密算法在美国被当作武器严格管制，严禁从美国出口。但是信用货币被特殊批准可以让海外用户使用 →理由：从软件中提取加密技术比重新开发一套更难。。
  - 历史：CyberCoin等公司被怀疑收到千禧虫漏洞攻击→2001年破产→知识产权被维瑞信（Verisign）收购 →转卖给Paypal

信用数字货币探索（三）

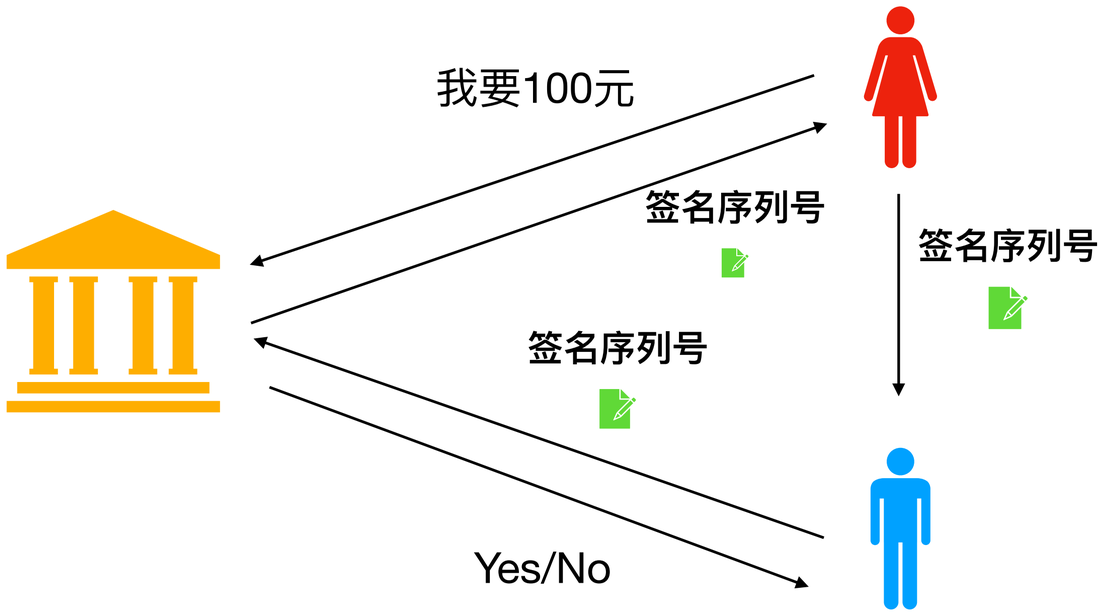
- SET信用货币体系的优劣势
- 优势：
  - 在https尚未普及的年代里，SET体系中的认证（签名算法）保证了交易的安全性
- 劣势：
  - SET体系中要求商家和用户都进行认证，绝大多数用户不愿意进行复杂的个人认证操作

现金数字货币

- 现金数字货币 VS 信用数字货币
- 现金：
  - 需要大众认可现金的价值✘
  - 避免了用户拒不还钱的风险✔
  - 用户的匿名性✔
  - 支持线下交易✔

现金数字货币探索（一）

- 和最初的想法很类似：不包含用户个人信息

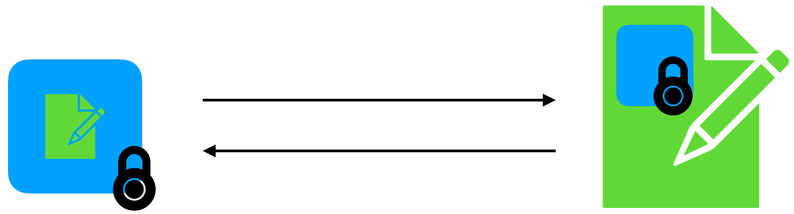


现金数字货币探索（一）

- 双重支付（double spending）
  - Alice可以将数字货币直接复制给第三人
  - 简单的解决方法：
    - 每一次交易，接收方都要和银行进行核对
    - 即使不包含个人信息，但是所有的交易流程都被银行掌握

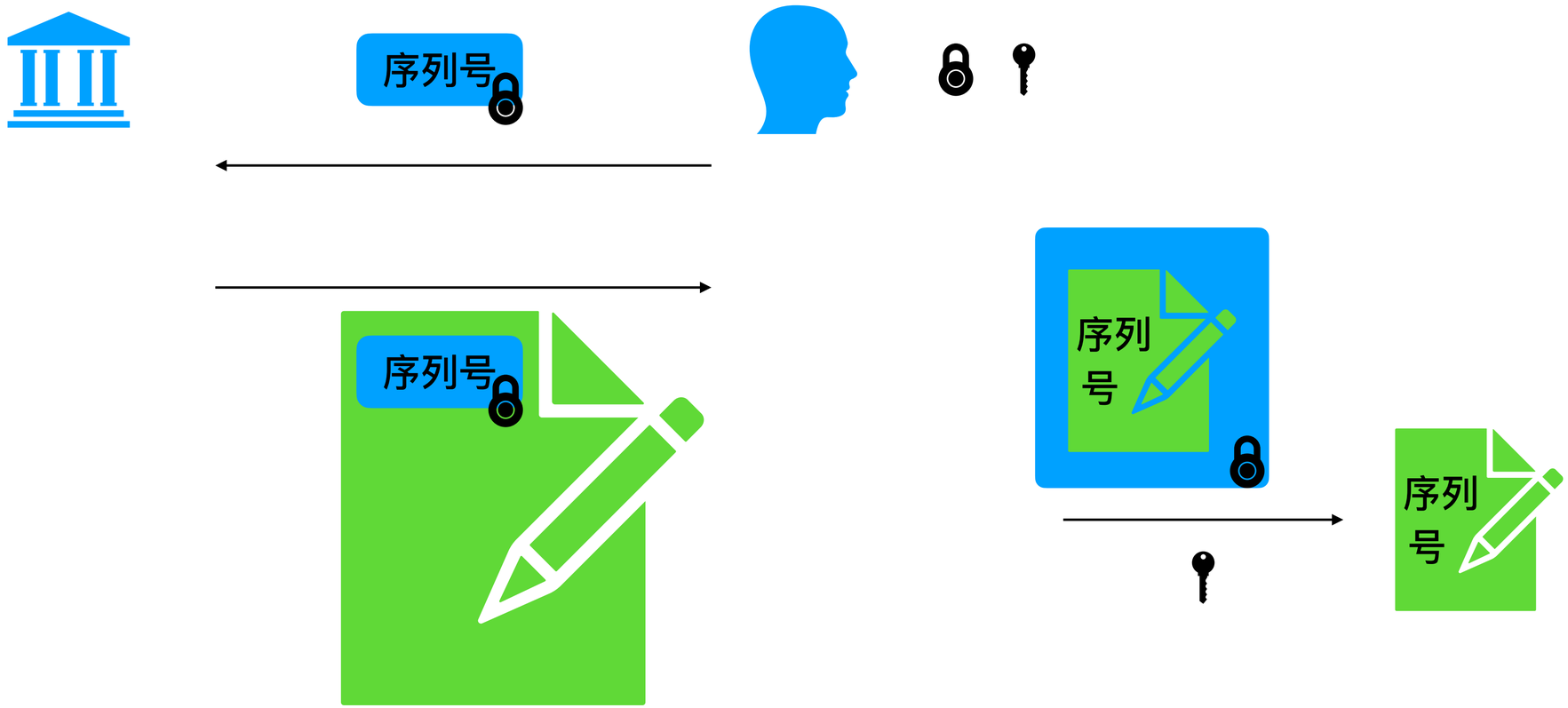
现金数字货币探索（二）

- 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）

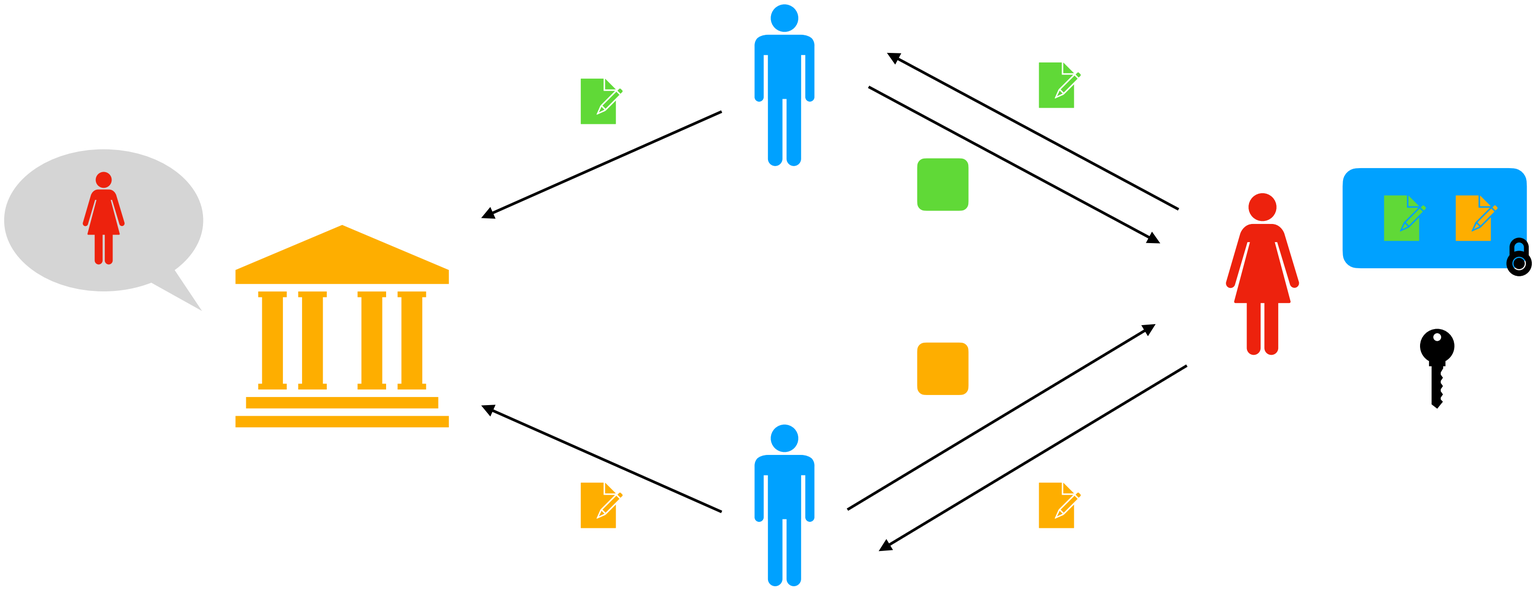
现金数字货币探索（三）

- 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

现金数字货币探索（三）



- 几个关键点：
  - Alice如果没有进行双支付的操作的情况下，银行不知道密钥。所以无法知道身份信息
  - 无法诬陷，Alice同一个人解密的相同的区域。

现金数字货币探索（四）

- 现金数字货币的一些问题：
  - 每一次支付过程中都要通过服务器和银行，无法将收到的货币付给他人
  - 无法进行分割
- 后续的一些解决方案：
  - Okamoto,Ohta（1991，可分割，可传递，低安全性）
  - Blazy等人（2011，可传递，高安全性，低效率）
  - Bauer, Fuchsbauer, Qian（2021，可分割，高安全性，高效率）

现金数字货币探索（五）

- 商业化以及遇到的一些困难：
  - 1989年就创建了DigiCash，并用于欧美相关银行业
  - David Chaum将盲签名等数字货币相关技术进行了专利化
  - 规模推广难，商家和用户没有充足的动力将信用卡系统替换为新的现金数字货币系统。
  - 后续，为了避免时候追责的漏洞，产生了用硬件避免双支付的设计。（我们并不涉及这方面的内容）

从数字货币到区块链

- 数字货币的下一个浪潮是由区块链技术带来的。
- 数字货币：基于银行发行的现金来保证货币的价值
- 凭空发行货币?
  - 思想来源于现代对于货币的新的认识
  - 早期：货币 == 贵金属 （金、银）
  - 现代：货币只是信用体系，1971年美国尼克森宣布美元与黄金脱钩

区块链-给数据赋予价值

- 寻找黄金的替代物：
  - 解决数学难题所花费的时间、能源
- 历史来源：
  - 从算力中提取稀缺物
  - 1992年，Dwork和Naor为了解决垃圾邮件的问题，首次提出类似的方案
  - 每一封电子邮件发出的时候，发件人都要解决一个数学难题，只有解决了难题的信件才会被接收。

区块链-给数据赋予价值

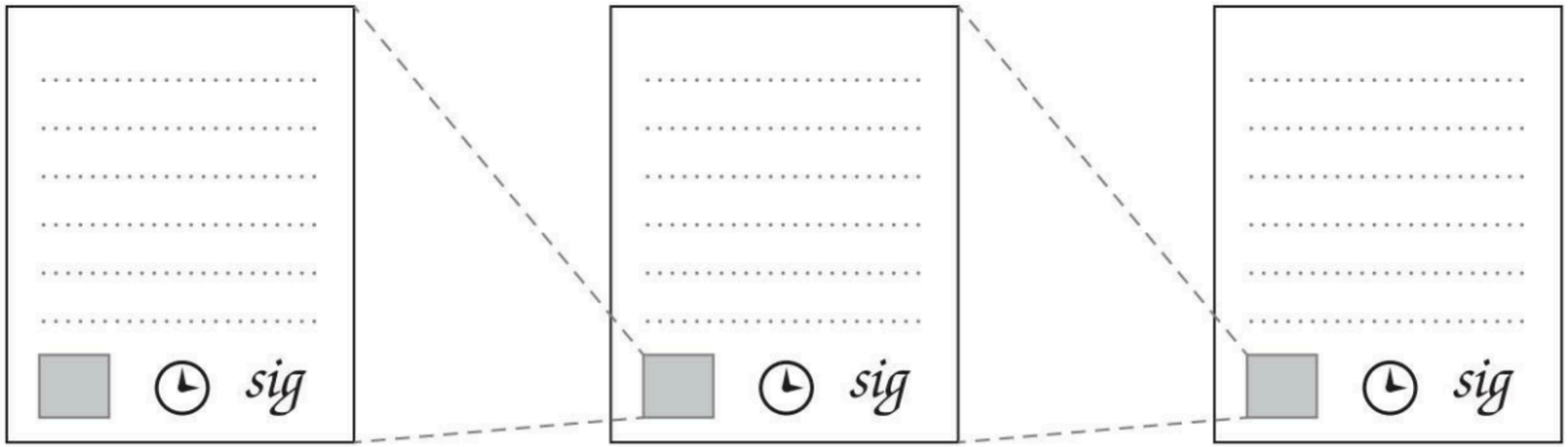
- 什么样的数学难题?
  - 发件人不能将同样的难题/答案附在不同的邮件中
  - 收件人可以高效的验证这些答案
  - 解决n个问题的难度应该随着题目的数量线性增加
  - 硬件不断发展→ 题目的难度可以由收件人来灵活设置

区块链-给数据赋予价值

- 哈希现金已经出现了比特币的雏形了
  - 将数据的价值与算力挂钩的思路
  - 具体的计算方法
  - 都使用计算哈希函数的方式（后续详细介绍）
- 哈希现金有着重要的理论意义，但实际中。。。
  - 垃圾邮件的问题并没有足够的严重
  - 无法作为真正的货币，没有解决发行的问题

区块链-给数据赋予价值

- 区块链技术：
  - 分布式账本
- 哈希现金的技术痛点：
  - 没有办法避免随意发行导致的通货膨胀 →分布式共享账本
  - 通过哈希和签名算法保证账本的内容和时间戳不可篡改性



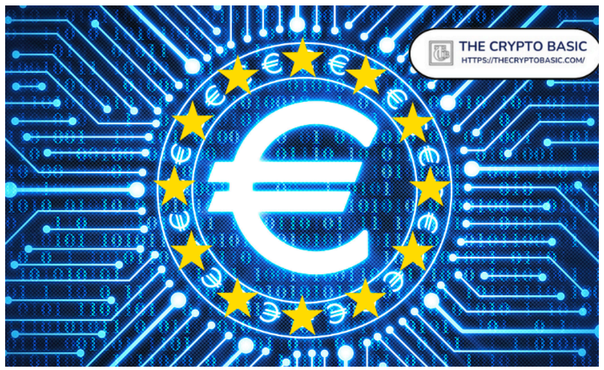
区块链-给数据赋予价值

- 比特币给区块链技术带来的影响
- 分布式账本：
  - 上述的方式需要中心认证的服务器
  - 通过添加类似哈希现金的方式，保证分布式共享账本的唯一性
- 有了分布式共享账本：
  - 交易信息被记录在账本上，无法被篡改也就无法产生双支付攻击
  - 但是匿名性无法保证 → 零知识证明

区块链-给数据赋予价值

- 故事并没有到此结束：
  - 区块链货币的去中心化保证了匿名性，但是被广泛用于逃脱监管。
  - 可控，隐私保护，高效，安全的数字货币始终正在路上！

数字人民币
e-CNY



总结：数字货币的发展历史

- 信用类数字货币
- 现金类数字货币
- 分布式记账
- 所关注的焦点：
  - 易用性：可以轻易交易
  - 保真性：难以被伪造和复制
  - 匿名性：用途和归属保密
  - 价值：可以被证明价值

课程后续的安排

- 密码学基础知识回顾
  - 哈希函数、签名算法、加密算法、零知识证明等
- 现金类数字货币技术
  - 理论构造、安全模型与证明等
- 区块链技术
  - 区块链结构、多方安全计算、共识协议