信陵神州
www.payunion.net

区块链与数字货币技术解析

王建新 2017年1月20日

区块链及数字货币现象

- 比特币的火热局面
  - 比特币：截止2016年12月29日10:15，共挖出16069862.5比特币，按当天价格价值约156亿美元。
  - 最新消息：区块链被列入《“十三五”国家信息化计划》

物联网、云计算、大数据、人工智能、机器深度学习、**区块链**、生物基因工程

区块链及数字货币现象

- 围绕区块链的光环

区块链及数字货币现象

- 各国对比特币的态度
  - **肯定:**

    德国金融部认可比特币是一种“货币单位”和“私有资产”

    加拿大承认比特币的“货币地位”
  - **否定:**

    泰国是全球首个封杀比特币的国家

    俄罗斯和韩国也是反对态度强硬

    中国在2013年底比特币价格峰值时期由中国人民银行等五部委联合发布《关于防范比特币风险的通知》，认为比特币“不具有货币属性，不是真正意义的货币”，基本上是持否定态度的
  - **放任:**

    美国、英国、日本

区块链及数字货币现象

- 针对区块链的不同观点
  - 区块链技术被认为是互联网发明以来最具颠覆性的技术创新，它依靠密码学和数学分布式算法，在无法建立信任关系的互联网上，无需借助任何第三方中心的介入就可以使参与者达成共识，以极低的成本解决了信任与价值的可靠传递难题。区块链技术的重要应用——区块链金融，被认为是传统金融的颠覆者。
  - 一群高智商的骗子（“伪创业者”），编个故事、拼凑个白皮书，披上“区块链的外衣”，布下的庞氏骗局。

区块链及数字货币现象

- 典型的疑惑
  - 程序员人为造出的一串数字价值能超过黄金，价值从何而来?
  - 区块链技术是否具备颠覆性?
  - 基于区块链的数字货币与传统货币相比优势在哪?
  - 数字货币能否取代当前货币?
  - ……

基于区块链的数字货币

- 区块链是什么？
  - 区块链是实现比特币等虚拟货币的核心技术；
  - 比特币是目前区块链最成功的应用。

区块链与数字货币技术

1. 比特币的货币特征
2. 比特币与传统货币对比优劣
3. 区块链技术

基于区块链的数字货币

- 比特币发展历程
  - 2008年10月31日 中本聪 《比特币：一种点对点的电子现金系统》
  - 2009年1月3日 创世块

    “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks”

    财政大臣正站在第二轮救助银行业的边缘
  - 170块：2009年1月12日：第一笔虚拟交易
  - 57035块：2010年5月22日，第一笔现实交易10000比特币买价值25美元披萨代金券，10000比特币的最高价值超过1200万美元。因为披萨味道好，这个人又买了几次，共花费40000比特币。

基于区块链的数字货币

- 比特币发展历程
  - 2010年8月17日，比特币最早的交易所价格出现，0.0769美分
  - 2013年11月29日，比特币在热门交易平台Mt.Gox的交易价格创下1242美元的最高价，超过一盎司黄金价格。
  - 2013年12月5日，中国人民银行联合五部委共同发布《关于防范比特币风险的通知》，比特币价格应声而落，12月18日跌至522美元，之后一直 在震荡中下行。直到2015年1月14日，比特币价格迎来本次泡沫的历史低点，114美元。
  - 当前价格可在各个比特币交易平台查看（2016年9月约600美元）。

基于区块链的数字货币

- 比特币的货币特征
  - 参与方
  - 发行规则
  - 价值怎么产生
  - 如何交易
  - 怎么记账
  - 交易安全性

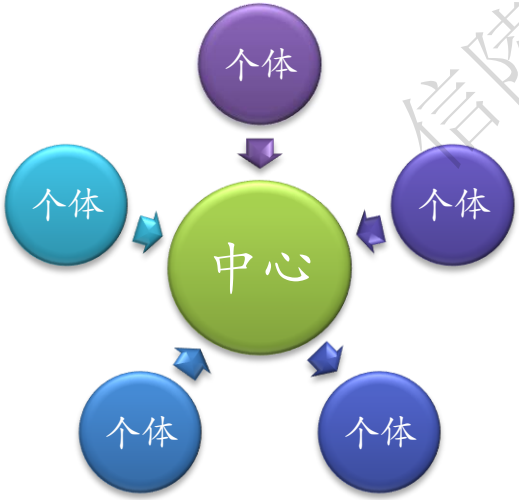
基于区块链的数字货币

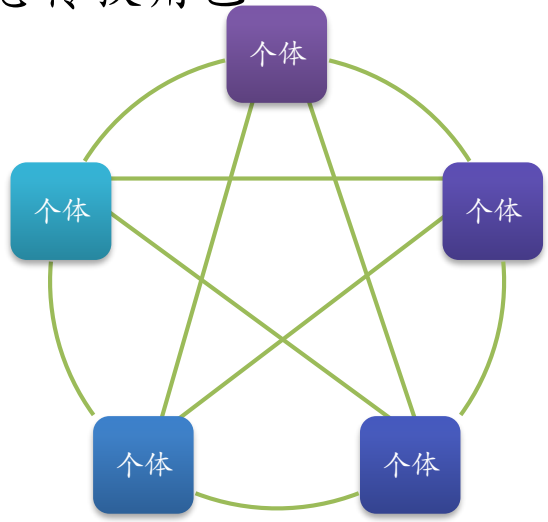
- 比特币的货币特征

比特币的参与方：

- 矿工
- 普通交易者

二者关系：完全平等，可随意转换角色

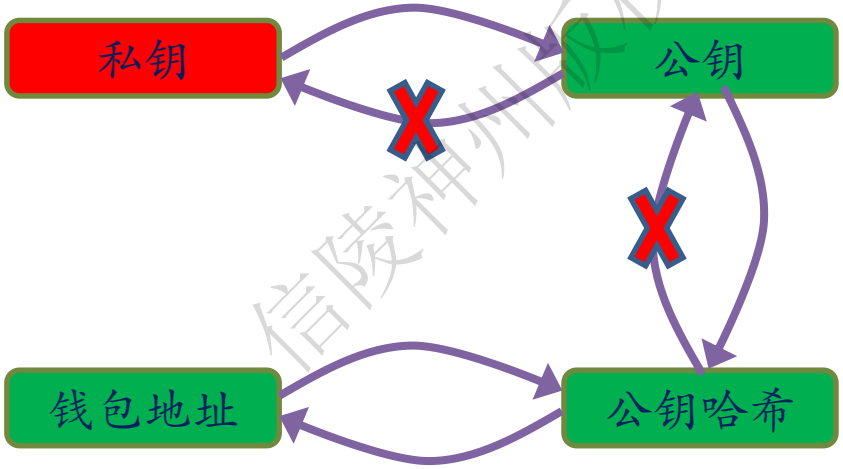




基于区块链的数字货币

- 比特币的货币特征

比特币的参与方——身份认证：



基于区块链的数字货币

- 比特币的货币特征

比特币的参与方——身份认证：

钱包地址 ≈ 银行卡号

私钥 ≈ 密码

基于区块链的数字货币

- 比特币的货币特征

发行规则：

- 挖矿

挖矿规则：

① 约10分钟挖矿成功一次；

② 初始挖矿成功奖励50比特币，每4年减半，直到到达最小单位聪；

基于区块链的数字货币

- 比特币的货币特征

发行规则：

- 挖矿

挖矿的实质是解一道数学难题，对规定的数据进行HASH256运算，找到符合难度值要求的结果，对于每个找到正确结果的矿工，给予比特币奖励。

算法：HASH256（x） = SHA256（SHA256（x））

SHA256算法的特点：结果是32字节（256bits）的十六进制字符串，算法不可逆。

每找到一个符合要求的结果，区块链增加一个区块。

基于区块链的数字货币

- 比特币的货币特征

发行规则：

- 挖矿

难度值：必须小于某个值的HASH256结果才满足要求，靠难度值限制整个系统平均10分钟找到一个正确结果，即挖矿成功一次。

目标值=最大目标值/难度值

最大目标值：0x00000000FF.....FF（32字节）

新难度值 = 旧难度值 /（过去2016个区块花费时长 / 20160 分钟）

基于区块链的数字货币

- 比特币的货币特征

发行规则：

- 挖矿

挖矿奖励规则：挖矿成功奖励50比特币，每210000块（约4年）后，奖励的比特币数减半，直到2140年减半后小于1聪（聪：比特币最小单位，1聪=0.00000001BTC）

比特币总数：20999999.97690000

当前矿工每次挖矿成功得到12.5比特币。

基于区块链的数字货币

- 比特币的货币特征

  怎么发行：

  - 挖矿

  挖矿规则的影响：

  当前阶段：人为造成物以稀为贵的效果；

  长期影响：通缩性货币

基于区块链的数字货币

- 比特币的货币特征

  发行规则：

  - 挖矿

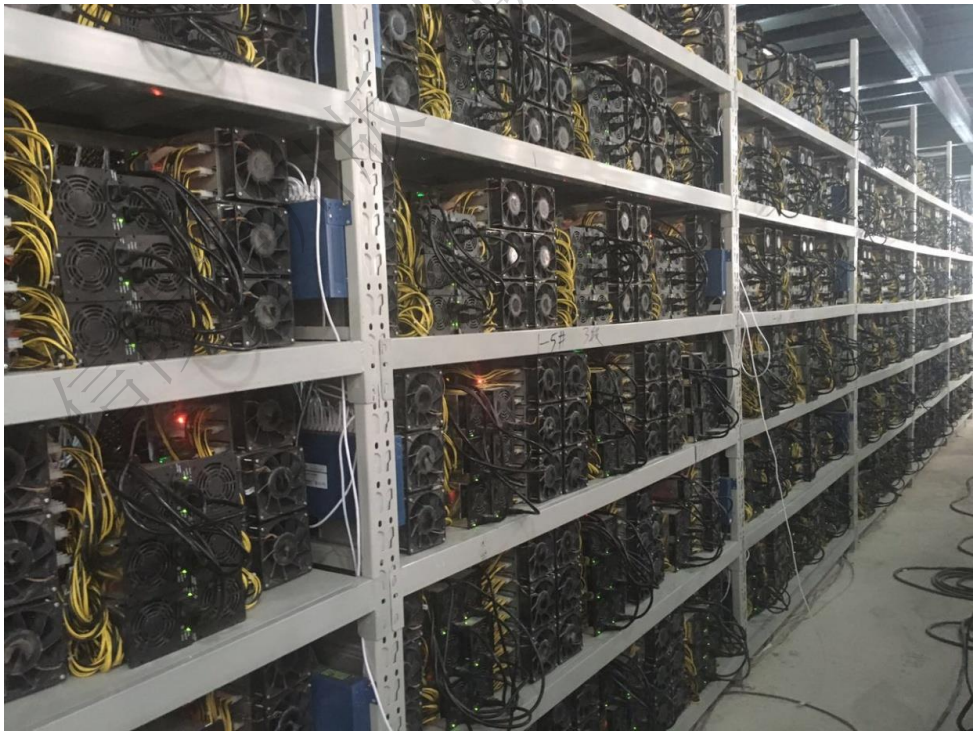
  共识机制： 工作量证明（pow）

基于区块链的数字货币

- 比特币的货币特征

发行规则：

- 挖矿



基于区块链的数字货币

- 比特币的货币特征

  如何交易：

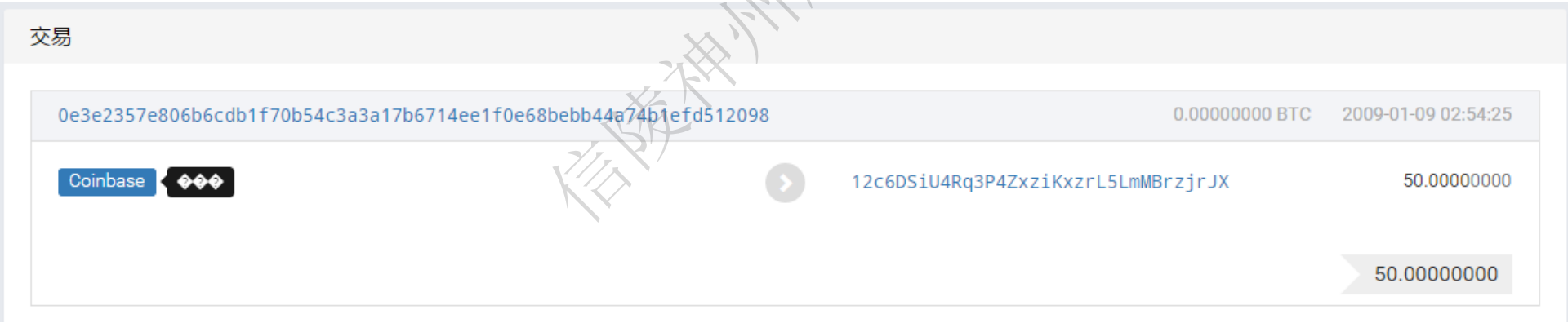
  - 生产交易
  - 转账交易

基于区块链的数字货币

- 比特币的货币特征

  如何交易：

  - 生产交易



基于区块链的数字货币

- 比特币的货币特征

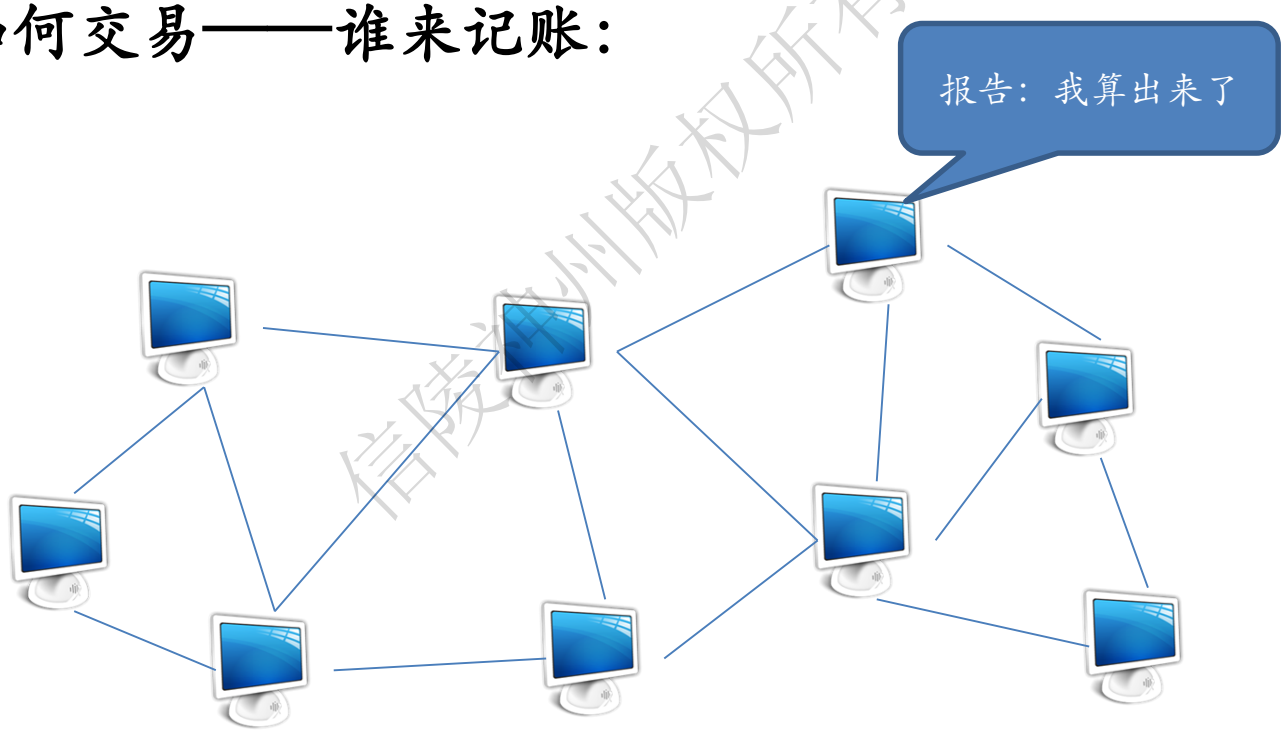
  如何交易：

  - 转账交易

基于区块链的数字货币

- 比特币的货币特征

如何交易——谁来记账：



计算数学题中。。。

基于区块链的数字货币

- 比特币的货币特征

  如何交易——账本：

账本

区块头：
版本号
前一区块头HASH
交易Merkle Root
时间戳
难度值
随机数

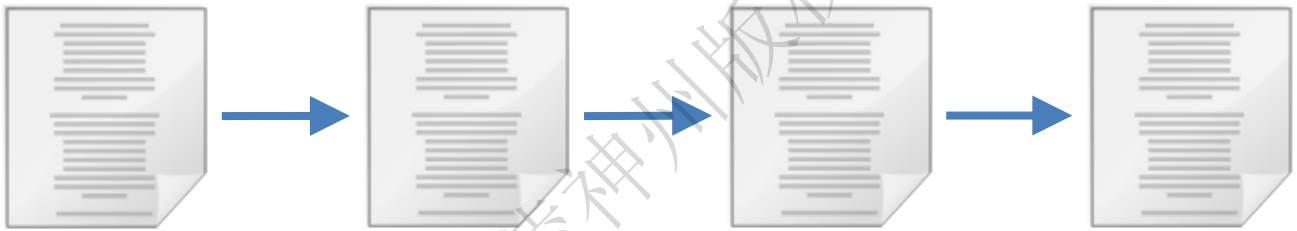
交易记录：
交易1
交易2
……
交易n

Block
区 块

基于区块链的数字货币

- 比特币的货币特征

  如何交易——账本：



BlockChain 区块链

基于区块链的数字货币

- 比特币的货币特征

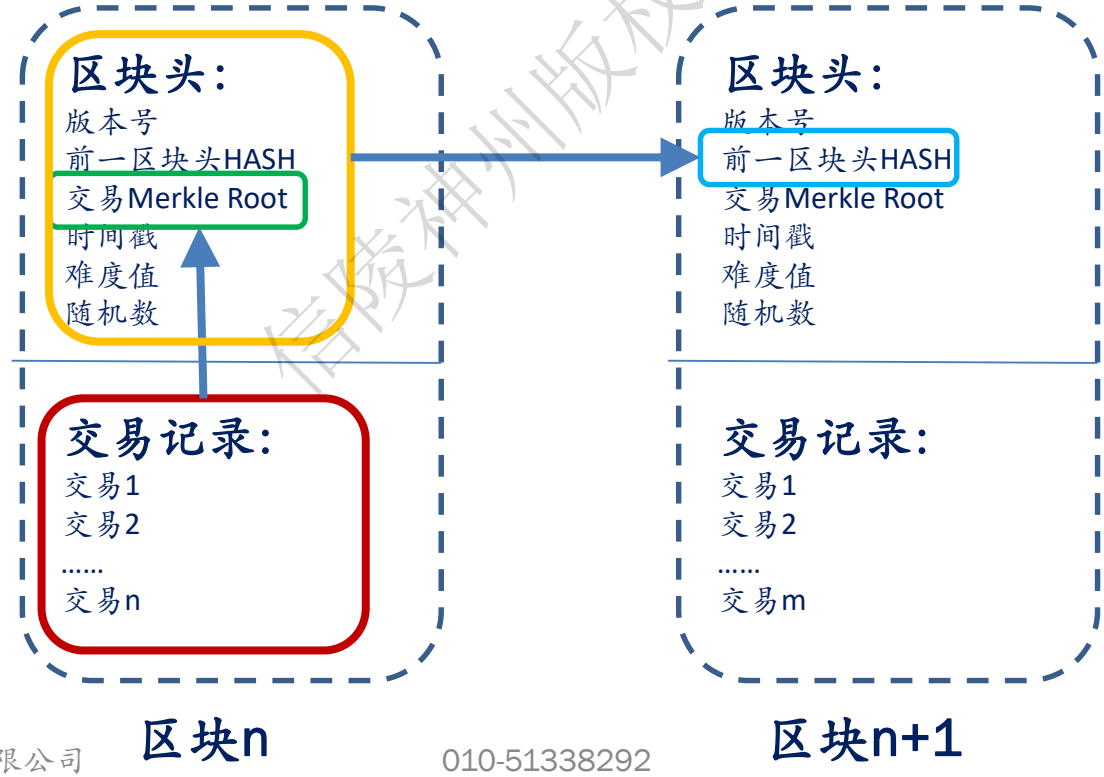
  总结：

  - 参与方：矿工和普通交易者
  - 怎么发行：挖矿奖励
  - 如何交易：使用未花费的交易
  - 怎么记账：区块链

基于区块链的数字货币

- 比特币的货币特征

交易安全性：



基于区块链的数字货币

- 比特币的货币特征

  交易安全性：

？ = 2:1 ..... (n-1) :1

基于区块链的数字货币

- 比特币的货币特征

  交易安全性：

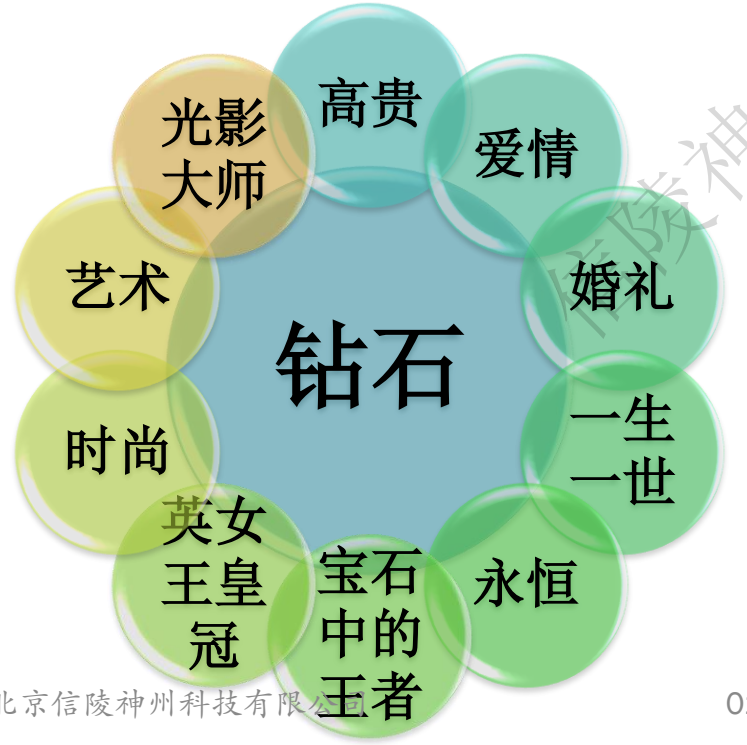
  - 交易记录由ECDSA数字签名保证真实性；
  - 区块内交易记录由merkle root防篡改；
  - 区块头由后一区块记录的前一区块头HASH值防篡改；
  - 通过分布式记账确保整个区块链不能被篡改。

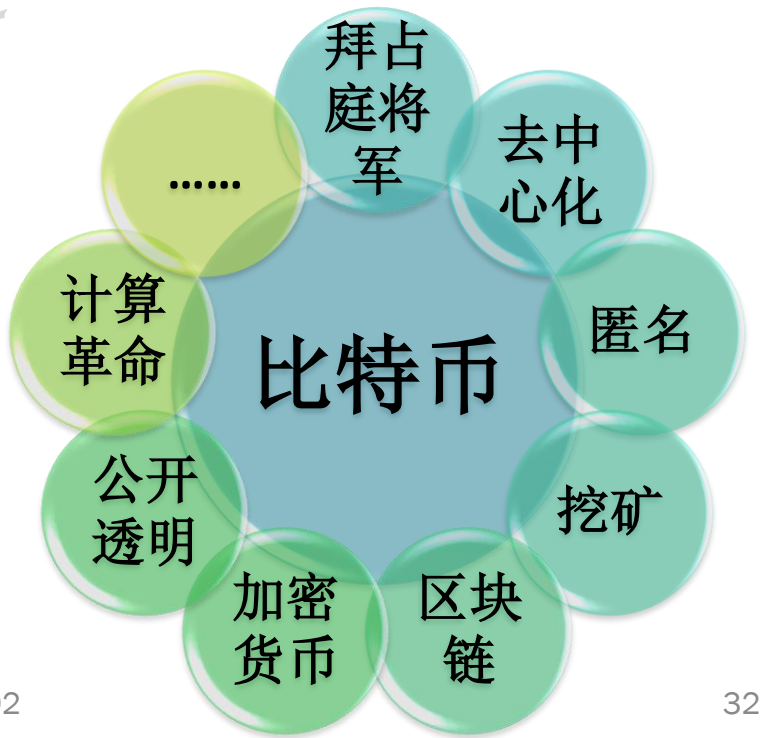
基于区块链的数字货币

- 比特币的货币特征

  价值怎么产生：

  - 围绕比特币和区块链的各种光环





基于区块链的数字货币

- 比特币的货币特征

  价值怎么产生：

  ① 挖矿规则人为造成物以稀为贵的效果；

  ② 围绕比特币和区块链的各种光环。

区块链与数字货币技术

1. 比特币的货币特征
2. 比特币与传统货币对比优劣
3. 区块链技术

基于区块链的数字货币

- 比特币与传统货币对比优劣
  - 功能
  - 性能
  - 资源占用
  - 安全性等方面

基于区块链的数字货币

- 2.4 比特币与传统货币对比优劣

功能：

- 当前货币：完善的生态环境，实现所有功能。

  比特币：基本的货币发行及交易。
- 比特币限定总量约2100万个（通缩型货币）
- 交易时间模糊：
- 挖矿成本：
- 可复制性：

基于区块链的数字货币

- 比特币与传统货币对比优劣

性能：

比特币：

- 约每秒7笔（区块最大长度1M字节）
- 交易确认速度约10分钟。

当前货币：

- VISA峰值每秒1.4万笔交易。
- 今年双11，支付宝峰值每秒12万笔，全天10.5亿笔交易

基于区块链的数字货币

- 比特币与传统货币对比优劣

  性能：

基于区块链的数字货币

- 比特币与传统货币对比优劣

  资源占用：

  - 存储资源：目前区块链大小约100G（2016年9月）

    每个矿工节点100G，存储资源

  - 算力：2014年某矿厂2500台挖矿机，每月40万电费

    算力并未产生现实财富。

基于区块链的数字货币

- 比特币与传统货币对比优劣

  安全性：

  1. 货币持有者需要的安全性
  2. 比特币宣称的安全性
  3. 比特币的安全能否满足货币持有者的需要?

基于区块链的数字货币

- 比特币与传统货币对比优劣

安全性：

1. 货币持有者需要的安全性：

我的货币完全按照我的意愿支付。

别人冒充我的身份花我的钱不行——伪卡交易

交易的数据与我的意愿一致——交易篡改

需要两方面保护：身份认证信息的保护和交易数据防篡改。

基于区块链的数字货币

- 比特币与传统货币对比优劣

安全性：

2. 比特币宣称的安全性
   - 不可篡改
   - 匿名性
   - 加密货币
   - 敏感信息保护
   - ……

基于区块链的数字货币

- 比特币与传统货币对比优劣

安全性：

2. 比特币宣称的安全性

- 不可篡改

交易记录通过ECDSA签名；

所有的交易计算Merkel Root HASH；

Merkel Root HASH作为区块头的一部分，区块头篡改会被后一区块发现；

通过分布式记账确保对区块的篡改不会被系统接受。

基于区块链的数字货币

- 比特币与传统货币对比优劣

安全性：

基于区块链的数字货币

- 比特币与传统货币对比优劣

安全性：

3. 比特币的安全能否满足货币持有者的需要?

◆ 伪卡交易

账户信息和密码泄露导致伪卡交易

比特币钱包地址是公开的；

私钥保存在客户端（PC或手机），私钥的安全取决于客户端的安全。

钱包地址 ≈ 账户信息

私钥 ≈ 密码

基于区块链的数字货币

- 比特币与传统货币对比优劣

安全性：

3. 比特币的安全能否满足货币持有者的需要?

◆ 交易篡改

区块链总账具有防篡改功能

交易记录计入总账之前是否能够防止篡改，依然取决于客户端的安全性。

基于区块链的数字货币

- 比特币与传统货币对比优劣

安全性——比特币安全事件：

1. 2010年8月，黑客利用大整数溢出漏洞分两笔交易“挖”出了1844亿个比特币，导致开发人员迅速升级软件并启动了硬分叉处理漏洞；
2. 2011年6月，Allinvain（bitcointalk论坛成员）25000个比特币被盗；
3. 2011.6.19，Mt GOX平台（曾经占据世界交易总额 80% 的世界第一大比特币交易平台）6万用户数据泄露，约50万比特币被以极低价格卖出（每单0.01美元）使得比特币的价格从32美元降到了1美分的价格；
4. 2011年7月，位于波兰的第三大比特币在线交易所Bitomat宣布丢失1.7万比特；

基于区块链的数字货币

- 比特币与传统货币对比优劣

安全性——比特币安全事件：

5. 2011年8月，作为常用比特币交易的处理中心之一的MyBitcoin宣布遭到黑客攻击，并导致关机。超过78000比特币丢失；
6. 2012年3月和5月Bitcoinica的交易平台连续两次遭到黑客攻击，损失超过4.3比特币，直接导致网站关闭；
7. 2012年9月，比特币交易平台Bitfloor服务器遭入侵，黑客窃取了2.4万比特币；
8. 2014.2.25，Mt GOX平台约85万比特币被盗（占当时全部比特币的7%），整个平台余额仅剩2000，平台破产；
9. 2016.6.17，价值5000万美元的360万以太币被盗，导致以太币的硬分叉（ETH和ETC）

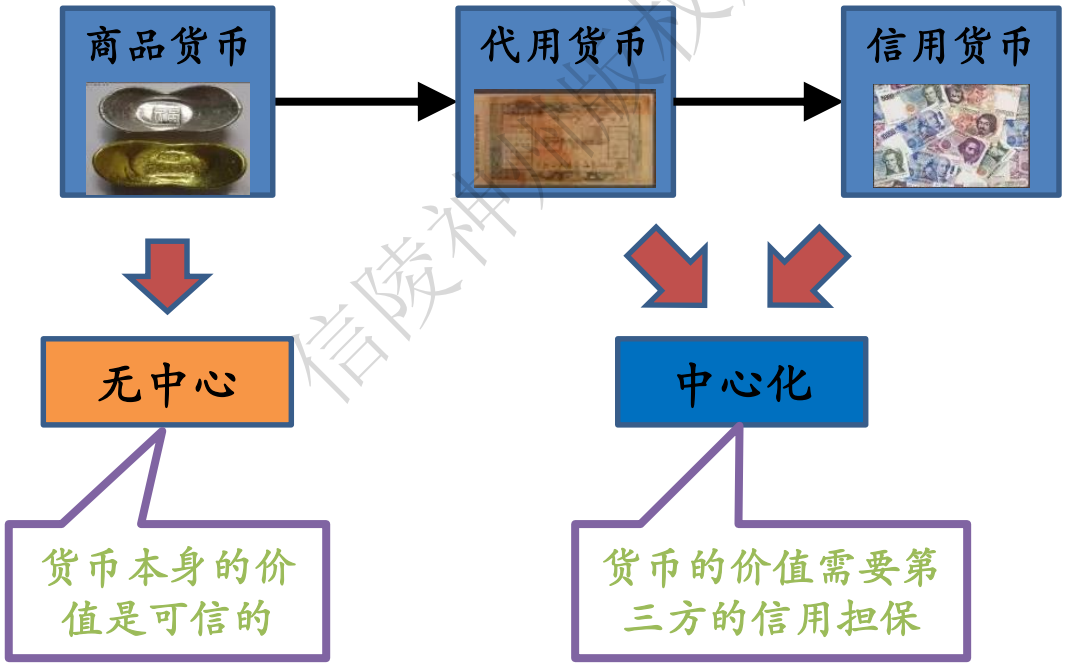
基于区块链的数字货币

- 比特币与传统货币对比优劣
  - 功能
  - 性能
  - 资源占用
  - 安全性等方面

基于区块链的数字货币

- 比特币与传统货币对比优劣

去中心化：



基于区块链的数字货币

- 比特币与传统货币对比优劣

  去中心化（续1）：

  - 解决了单点故障

    某一个人或组织无法影响最终结果

    代价是交易的冗余，牺牲了效率

基于区块链的数字货币

- 比特币与传统货币对比优劣

  去中心化（续2）：

  货币发行中心化：

  - 中心是否代表所有人的利益？

基于区块链的数字货币

- 比特币与传统货币对比优劣

  去中心化（续3）：

  - 当前世界金融秩序的最大矛盾：美元是世界货币，而美联储是美国的央行。
  - 解决矛盾的思路
  - 颠覆性意义

基于区块链的数字货币

- 比特币与传统货币对比优劣

  是否可能替代现在的货币系统?

  - 理论上的可行性
  - 技术上的瓶颈
  - 非技术的瓶颈

基于区块链的数字货币

- 比特币与传统货币对比优劣

人行对数字货币的研究

人行成立专门的数字货币研究团队，就数字货币的发展方向、原型构想、技术路径选择、法律依据以及对货币政策的影响等关键问题进行分析和探讨。

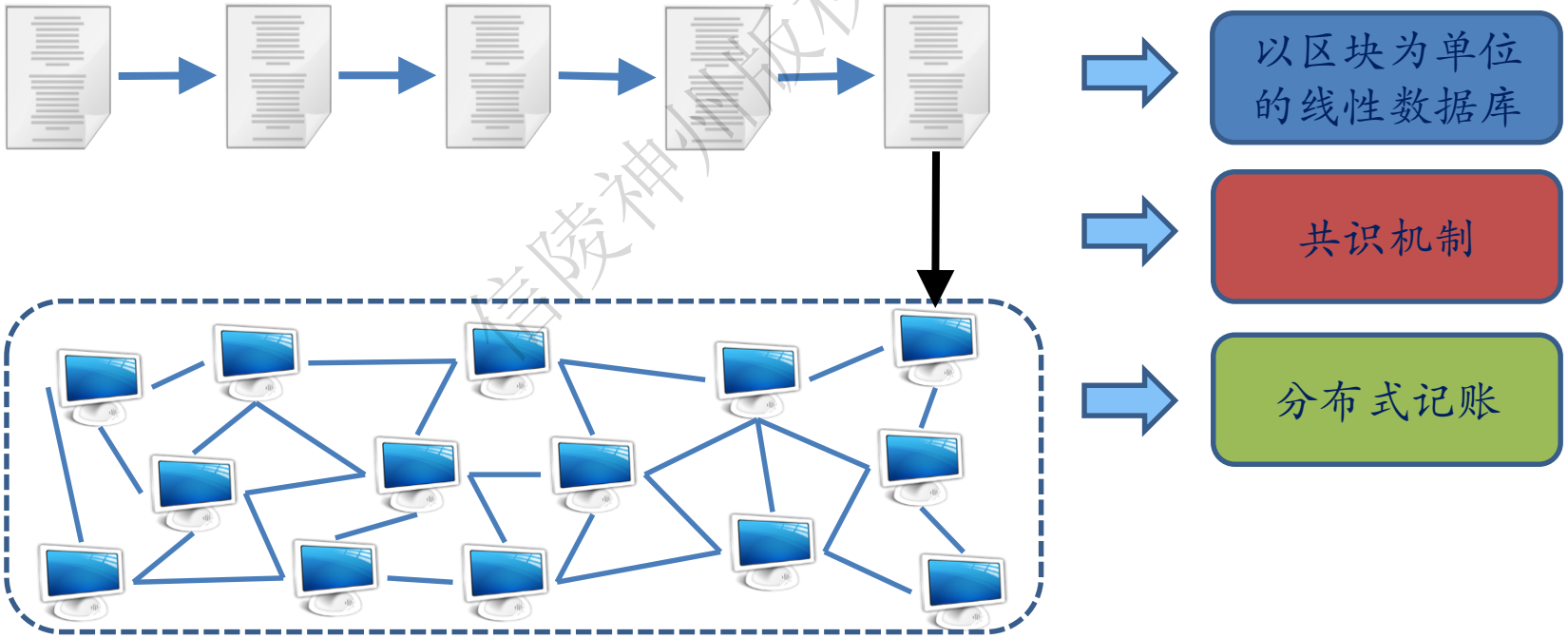
区块链与数字货币技术

1. 比特币的货币特征
2. 比特币与传统货币对比优劣
3. 区块链技术

区块链技术

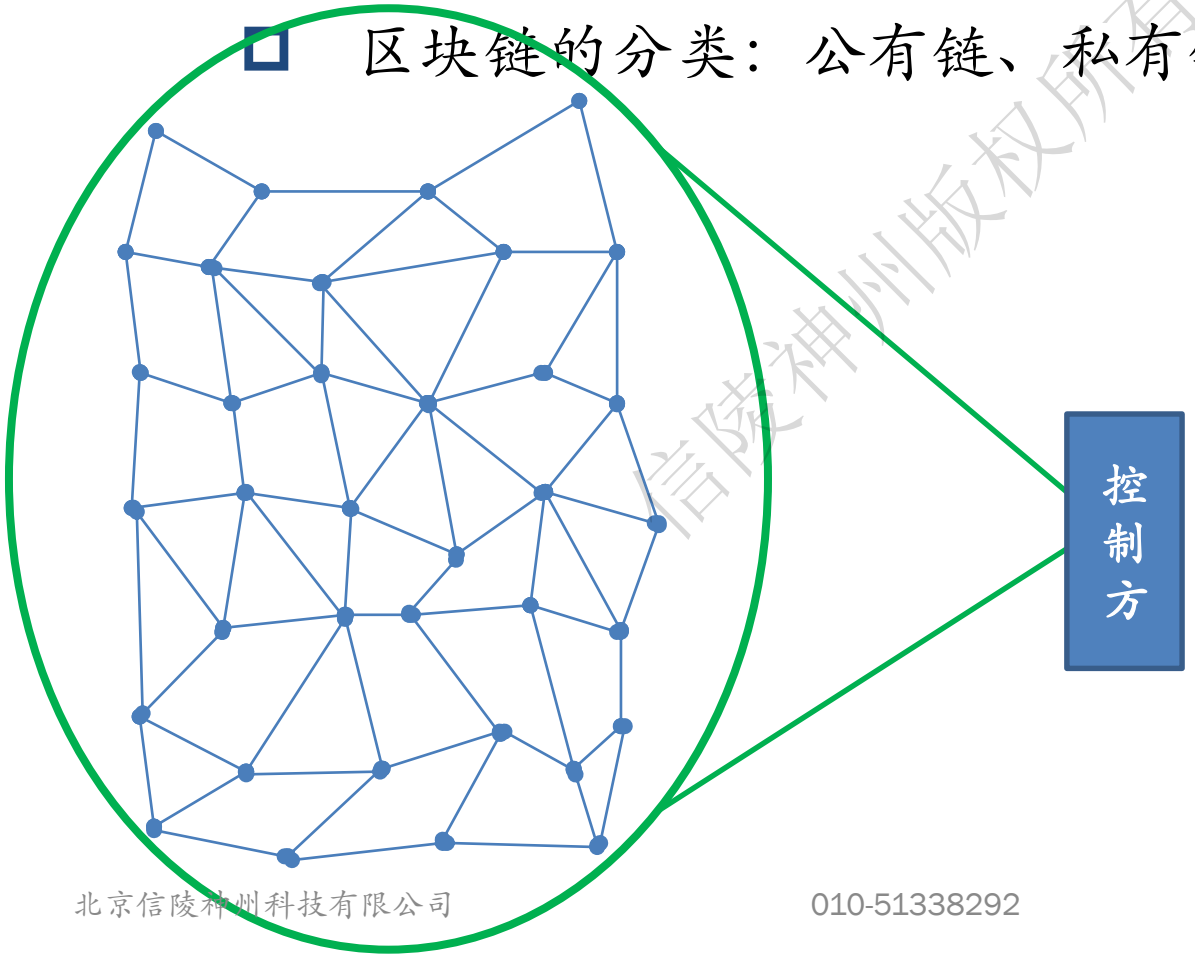
- 区块链的本质

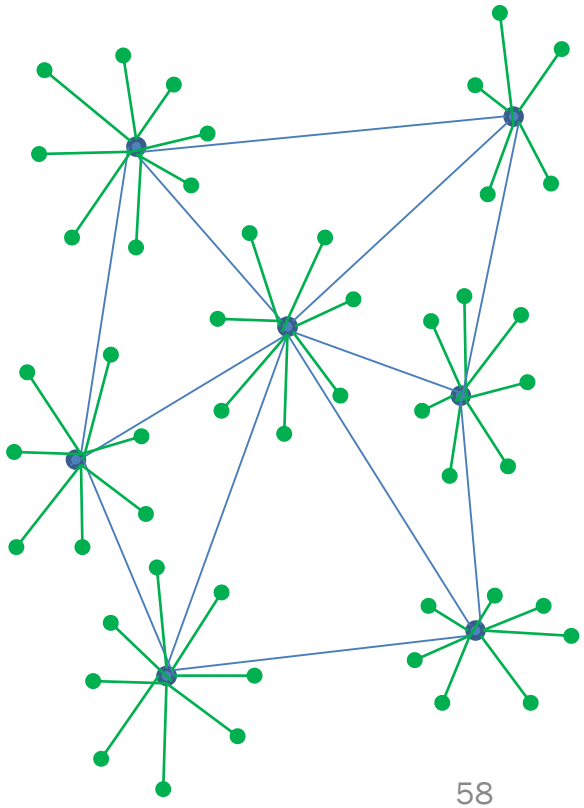
  比特币的哪些技术属于区块链



区块链技术

- 区块链的本质
  - 区块链的分类：公有链、私有链、联盟链





区块链技术

- 区块链的本质

  区块链与传统数据库对比：

  - 不可篡改
  - 公开透明
  - 记录不能update、delete、insert，只能append、select
  - 解决了单点故障

区块链技术

- 区块链应用

  理论上数据库可记录任何数据，区块链可用于任何应用；实际上应记录适合自己特点的数据，以及发挥区块链优势的应用

  - 不适合记录随时更改的数据，适合记录按时间顺序长期保存且需要防篡改的数据
  - 不适合记录隐私数据，适合记录需要公开透明的数据
  - 适合无信任基础的场景
  - ……

区块链技术

- 3.3 区块链应用

  区块链的应用场景：

  - 投票
  - 慈善
  - 股权分配
  - 学历登记
  - ……

区块链技术

- 当前区块链应用的问题

为使用区块链而使用区块链!

区块链技术

- 总结

  区块链技术的发展取决于两方面：

  - 区块链能做什么？
  - 与传统技术对比优势在哪？

信陵神州技术培训

- 1. 区块链与数字货币技术解析
- 2. 条码支付技术
- 3. 移动支付
- 4. 电信诈骗风险与风范
- 5. 银行卡类相关内容培训
- 6. 银行卡交易流程及风险控制
- 7. 银行卡受理终端功能及安全
- 8. 金融信息系统安全及风险控制
- 9. 加密算法在金融交易各个环节的应用及密钥管理
- 10. 网上银行系统
- 11. 跨境支付
- 12. 第三方支付
- 13. 金融信息系统安全
- 14. 互联网金融
- 15. 金融相关的新业务形式以及新技术分析

联系人：老孟

手机号：13601260375

邮　箱：pay@payunion.net

Thanks!

谢谢观赏！