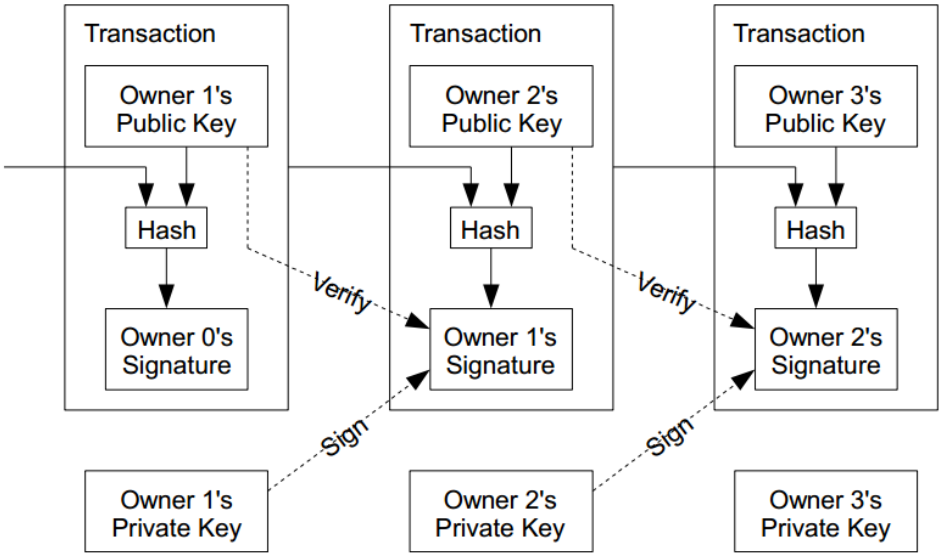
比特币白皮书

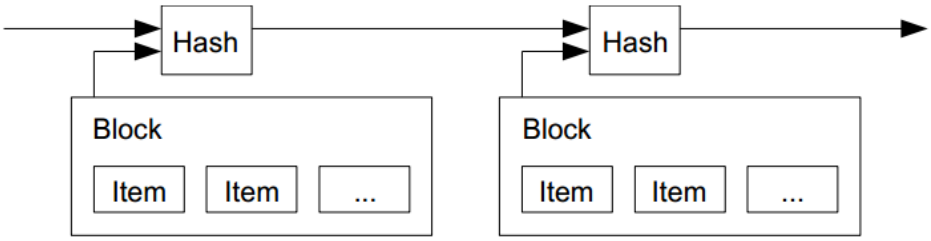
笔记本: 区块链
创建时间: 2019/10/10 10:22 **更新时间:** 2019/10/13 16:22
作者: jyyhermance@163.com

摘要
去中心化的p2p支付系统
通过基于时间戳的随机散列形成的前后相关的序列，解决双重花费问题
优/缺点？-> 回滚交易代价很大，记录难以更改

1 简介
阐述可更改交易（通过第三方中介中心实现）的弱点
比特币用密码学代替中心化中介信用 -> 实际上相比中介中心，更相信交易对方的信用
提供不可更改的交易 -> 强卖家保护

2 交易


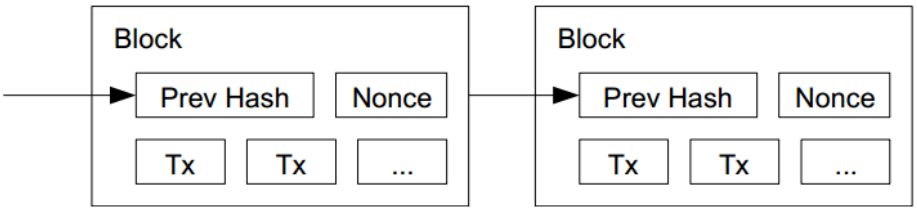
付款人：将收款人的公钥和上一笔交易记录HASH，在最后用付款人的私钥签名
收款人：收到之后，用收款人的私钥解密，用付款人的公钥验证其签名
问题在于，收款人无法验证之前是否有付款人双重支付了该货币 -> 公布交易信息，被多数节点认可的是有效交易

3 时间戳服务器


如何取得时间：来自连接的其他节点的中位数，且与本机时间相差不超过70分钟，否则提醒更新

每个时间戳的哈希值中都包含前一个时间戳 -> 形成链条chain -> 区块链按时间先后顺序组织起来（存在安全隐患？）

4 工作量证明



设计思想：提高作恶成本
投票权：one CPU one vote（比one IP one vote更为安全）
弊端：后期大矿场很多，个人用户难以参与

5 网络

1. 向所有节点广播交易
2. 节点将交易存入区块
3. 分别找pow
4. 最先找到的向其他节点广播自己的区块
5. 其他节点收到区块，验证交易的合法性后，接受区块 （接受后，本节点不再接受其他节点广播的同一个区块，也放弃自己之前进行的计算
6. 接受区块的表现为，在这个区块的基础上创建下一个新的区块

发生同时广播：在一个上工作，记录下另一个备用（分叉），直到下一次pow出现，某个分支变得更长，则再次合并

6 激励

每个区块的第一笔交易，会创建一枚新的比特币，由本区块的创建者获得。
交易费（交易的确认也占用了节点
如果后期，比特币停止发行，但是没有大规模商业应用，很可能交易量过低，带来计算节点萎缩，交易时间过长，交易费上涨，甚至崩盘

7 回收磁盘空间

丢弃旧事务中的数据：剪枝Merkle树

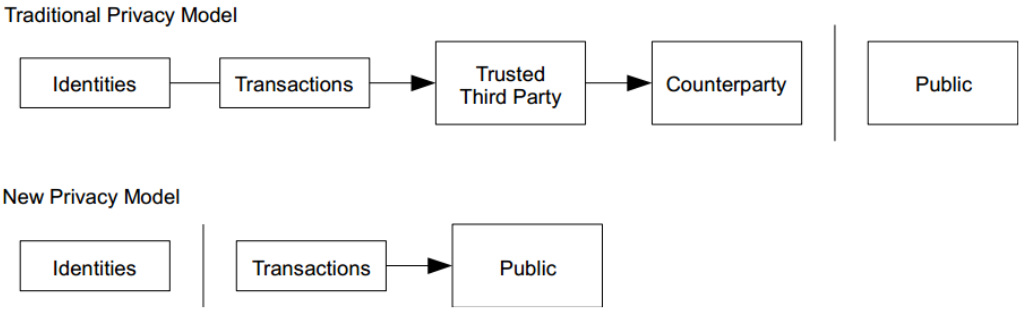
8 简化支付验证

保存最长链的区块头，获取相关交易的Merkle分支，最后检查此交易是否被节点接受 --> 诚实节点控制下有效
抵御攻击：一旦节点发现无效区块，发出警告
对于业务频繁的公司：使用私链/联盟链（更为高效和安全）

9 合并和分割交易额

交易可以包含多个输入和两个输出（付款+找钱）

10 隐私



保护用户隐私 --> 阻断信息流：公钥匿名

11 计算

攻击者只能拿走已经支付的钱
随着需要赶上的区块数增加，攻击成功概率呈指数下降
为防止攻击者提前准备，交易前收款人重新生成一对密钥