Bitcoin白皮书解读

曾斌 2018-02-27

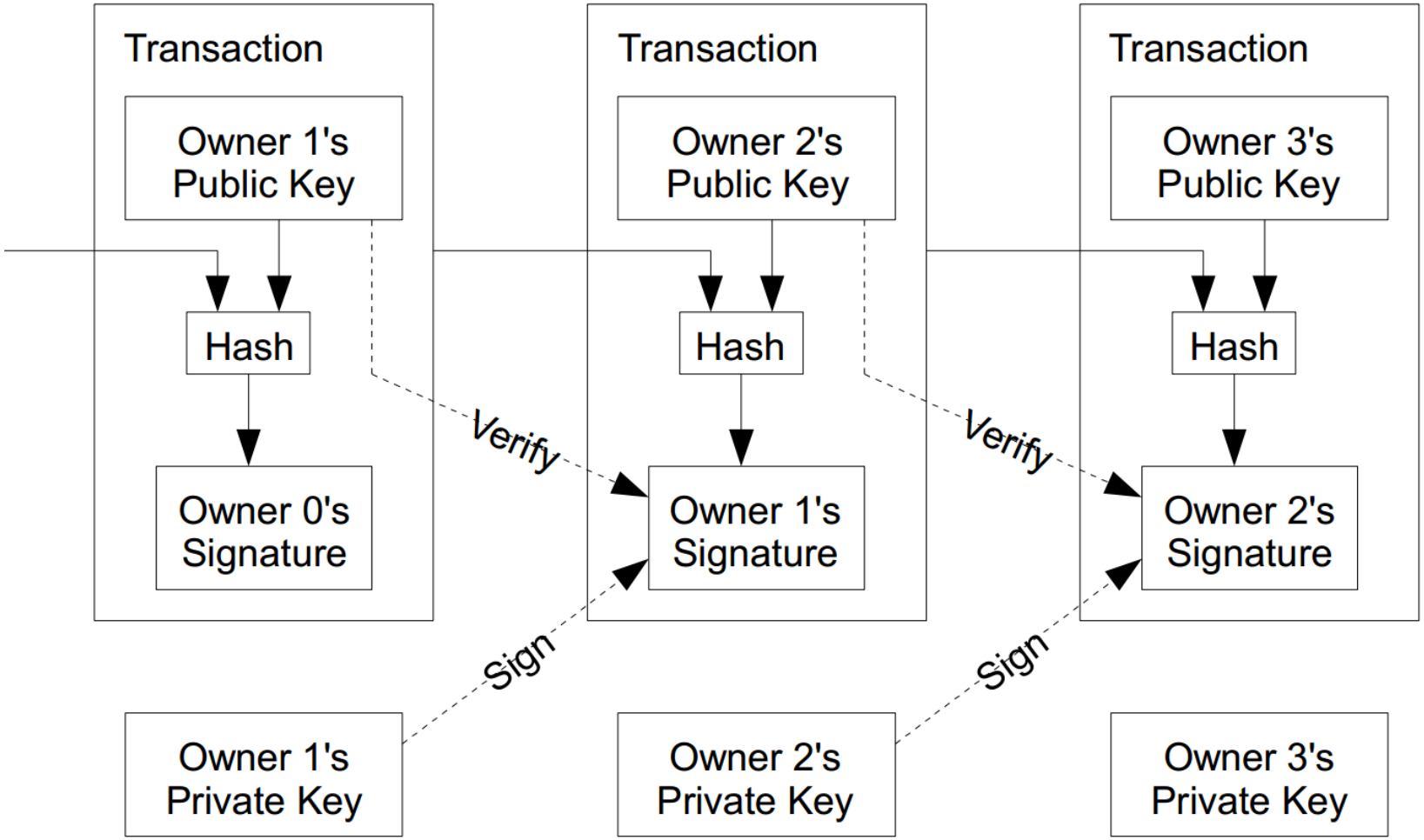
摘 要

- 点对点交易通常需要依赖可信的第三方来阻止双重支付
- BTC – 使用P2P网络解决double-spending问题：
  - 1、对每一笔交易加入timestamp进行hash计算，并将结果保存到一条不断生长的链上
  - 2、各节点进行计算，将一定时间内的交易打包到区块中，除非重新进行计算，否则区块内容不可更改
  - 3、只要网络上绝大多数的算力都是诚实的，他们就能够持续的生成最长链，即：最长链可以信赖
  - 4、网络上所有的信息都会尽可能的广播出去
  - 5、任何一个节点都可以随时离开和加入网络，并选择信赖最长链
- 只要所有诚实节点的算力大于所有攻击节点的算力，系统就是安全的

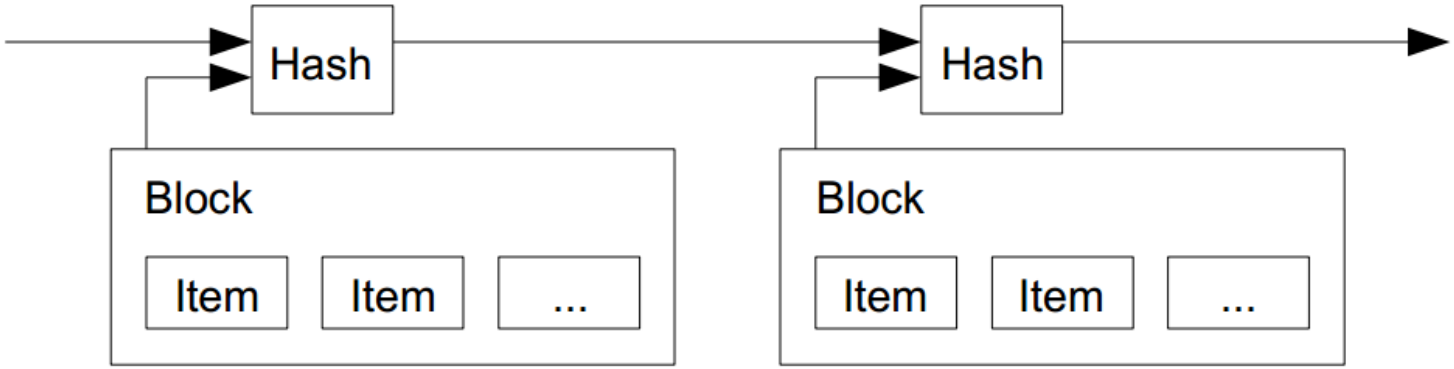
BTC网络工作流程

- step 1. 新交易发生，广播到所有节点
- step 2. 每个节点把一定时间内接收到的所有交易打包到一个区块
- step 3. 每个节点都尝试在自己的区块中找到一个具有足够难度的工作量证明
- step 4. 当一个节点在自己的区块上找到了一个工作量证明，它就向全网进行广播
- step 5. 当且仅当包含在该区块中的所有交易都是有效的且之前未存在过的，其他节点才认同该区块的有效性
- step 6. 如果区块有效，其他节点就跟随该区块的末尾创造新的区块

交易 - Transactions



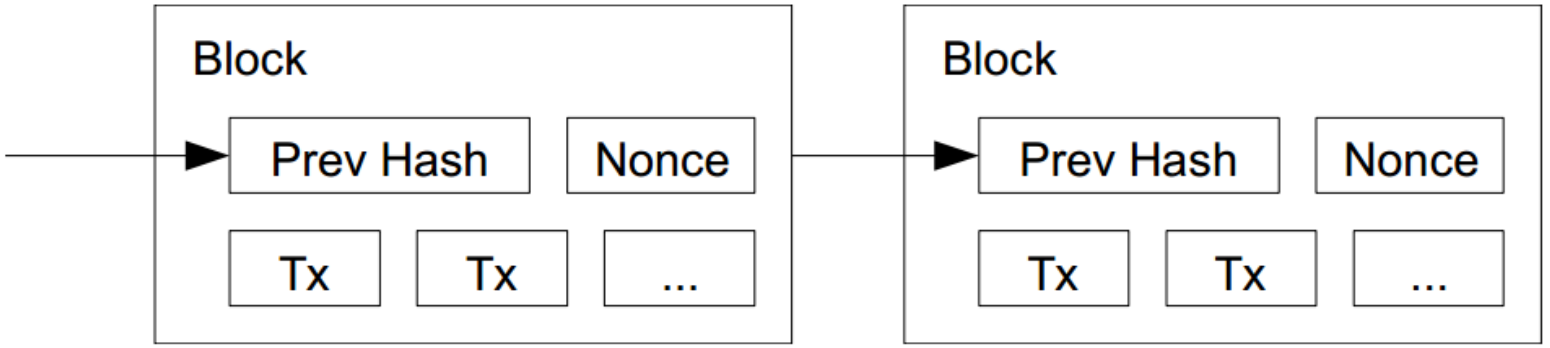
时间戳服务器 - Timestamp Server



1、时间戳服务器通过对以区块(block)形式存在的一组数据实施随机散列而加上时间戳

2、时间戳服务器应当是分布式的

工作量证明 - Proof-of-Work



1、工作量证明机制是分布式时间戳服务器的组成部分之一
2、打包一个区块需要完成一定难度的计算任务
3、如果区块生成的速度过快，那么计算任务的难度就会提高，以此控制区块的生成速度

激励 - Incentive

- 一定的激励能够促使节点保持诚实

- 激励分为两类：

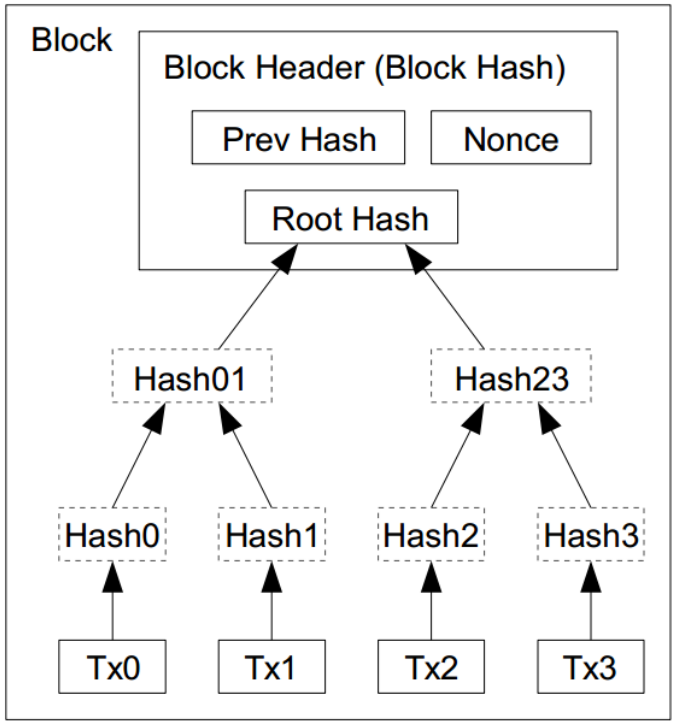
  1）挖矿奖励

  每个区块的第一笔交易是奖励给区块创建者的新币；

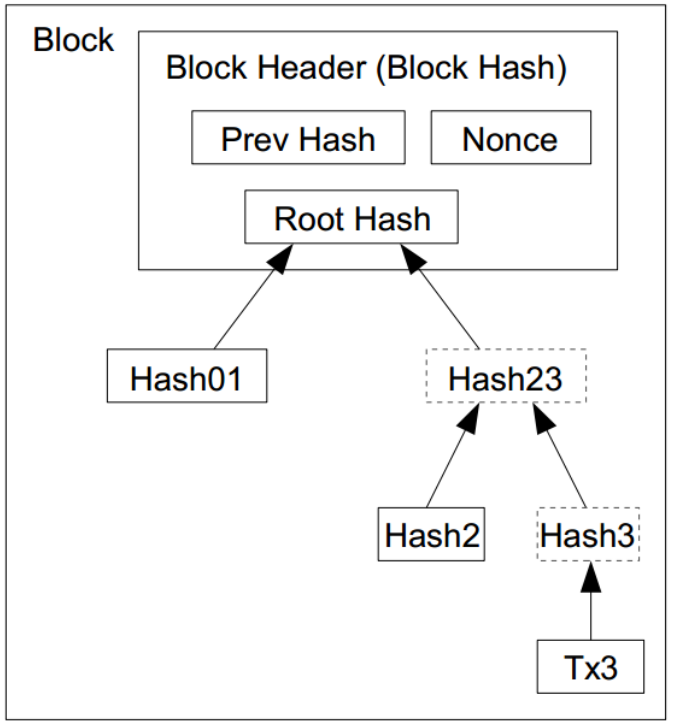
  2）交易费

  每一笔交易的输入金额比输出金额多出来的部分作为交易费支付给旷工。

Merkle Hash Tree



Transactions Hashed in a Merkle Tree

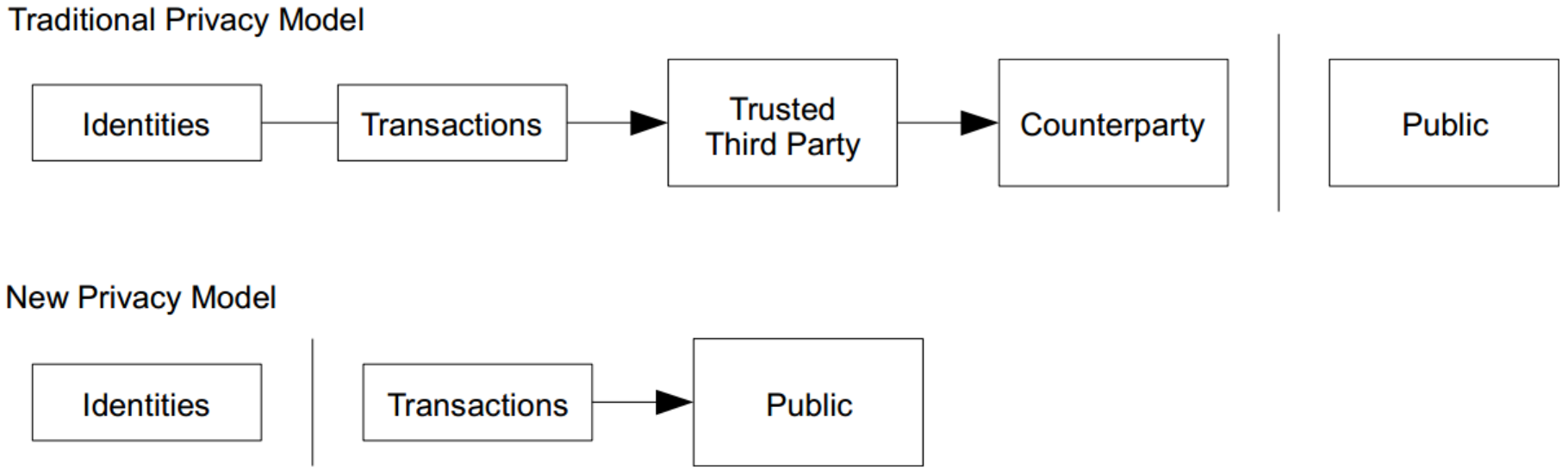


After Pruning Tx0-2 from the Block

- 借助Merkle Tree，每一个区块仅需要保留root hash就能知道区块内的交易是否被篡改

隐私保护 - Privacy

- 相比于中心化系统的隐私保护方法，Bitcoin能够更好的保护用户隐私信息。



参考资料

- Bitcoin: A Peer-to-Peer Electronic Cash System
- 精读比特币白皮书（大鱼）
- A simple Blockchain in Python
- Python 从零开始构建自己的比特币区块链系统