比特币设计简单却能顺畅运行背后的原因

18308045 谷正阳

1 数据结构

1.1 Hash Pointer

Hash Pointer是一种特殊的指针，记录的是数据块的哈希值。一方面它可以指向数据块，另一方面它可以用于检测数据块有没有被篡改。将数据用哈希指针传承一条链就是区块链。在比特币区块中，区块头部的Previous Block Header Hash就是一个Hash Pointer，它是对上一个区块头部的哈希，在指向上一个区块的同时，又可以可以验证上一个区块头部是否被篡改。

1.2 Merkle Tree

Merkle Tree是另一种用Hash Pointer串联的数据结构，是用Hash Pointer记录左右孩子二叉树。其特点是根部的哈希值可以用于验证整棵树有没有被篡改。在比特币区块中，区块头部中的Merkle Root就是树根的哈希，一段时间内所有的交易作为叶子节点，这样可以用于验证交易有没有被篡改。

1.3 A Bitcoin Block

包含了区块头部和交易记录，交易记录的树根存在Merkle Root中。

2 共识机制

2.1 身份确认：公钥、私钥体系

比特币使用公钥、私钥体系进行身份认证。每笔交易的发起方用他的私钥签名，其他人通过交易发起方的公钥验证公钥的合法性。因而一个公钥私钥对即代表了一个比特币账户。

2.2 交易服务：UTXO交易模型

比特币使用UTXO交易模型提供交易服务。它保证了同一笔资金只出现在一笔交易中。其本质实际上是用交易记录来记录一个人全部的比特币，而非用账户来记录。这样无法实现货币造假，因为它可以追溯到每一笔交易记录是否合法。

2.3 记录管理：链式交易信息记录

交易记录的存储采用分布式存储。每次交易都会进行广播，比特币网络上的每个节点都会存储这些交易。由于每一段时间其中一个节点会生成一个区块，区块里会记录这个时间段内收集的交易记录，而由区块串联而成的区块链便是所谓账本。每个人都有一条近乎相同的区块链，所以每个比特币网络上的节点都存储一个完整的账本，从而实现分布式存储。

2.4 信任规则：工作量证明(POW)

比特币信任规则采用工作量证明。通过修改新区块头部Nonce，计算新区快头部的哈希值，满足哈希值前有若干个0（决定了难度），来表明工作量，第一个计算出Nonce的人有记账权（即可将区块广播）。

3 比特币社区

3.1 比特币安全机制的保障

比特币遵循最长链原则。即出现分叉时优先相信更长的链，将区块接在最长链上。这样就要求算力要在一半以上才能维持分叉，算力在三分之一以上自私挖矿才能获得收益。

3.2 挖矿的激励与策略

对于算出区块的矿工奖励包括出块奖励和上面记载交易的全部手续费，以此激励矿工挖矿和记账。因此为了利益最大，矿工会默认记录那些交易费比较高的交易。另外由于最长链原则，为了规避风险，矿工会默认在最长链上继续挖矿；在同一高度上，也会默认选择最先监听到的区块；在挖出矿的时候，也会默认立刻发布。

4 比特币设计简单却能顺畅运行背后的原因：比特币共识的三个层面

包括规则的共识、历史记录的共识和比特币价值的共识，规则

4.1 规则的共识

规则即确保交易、区块有效的机制，保证了比特币参与者能够进行最基本的交互。

4.2 历史记录的共识

记录即已发生的被记录在区块链传接的Merkle Tree上的交易，保证了去中心化的UTXO的正常运行。

4.3 比特币价值的共识

即与现实货币的汇率，保证所有人想要比特币，所有人可以用比特币交易。

4.4 三者关系

三者相辅相成。规则中如最长链原则，大家优先相信最长的账本，因而规则的共识促成了历史记录的共识。规则中POW决定了挖掘比特币的难度，从而促成了比特币价值的共识。比特币有价值，因而大家会遵守规则促成规则的共识会想要记账促成历史记录的共识。历史记录的UTXO规范了交易过程，从而又促成了比特币的共识。