2019~2020 学年冬学期《区块链与数字货币》课程作业 1

应承峻 3170103456

1. 说明比特币区块链中区块的组装生成过程和验证入链过程。

在区块链生成区块之前，先要通过工作量证明（Proof of work）来决定哪个节点拥有记账权。胜出的节点将下图所示信息写入区块中，并更新 Merkle 树，然后通过广播告知全网的其他节点。

大小	字段	描述
4字节	版本	版本号，用于跟踪软件/协议的更新
32字节	父区块哈希值	引用区块链中父区块的哈希值
32字节	Merkle根	该区块中交易的merkle树根的哈希值
4字节	时间戳	该区块产生的近似时间（精确到秒的Unix时间戳）
4字节	难度目标	该区块工作量证明算法的难度目标
4字节	Nonce	用于工作量证明算法的计数器

当全网中其他节点接收到广播后，会对这个区块进行验证，具体的验证方式包括①检验区块数据结构是否完整，比如通过 SHA256 算法验证区块头信息是否有效②包含了足够的工作量从而使得区块头的哈希值小于难度目标值③区块链时间戳是否正确④区块大小是否在长度限制内⑤检验 Merkle 树是否完整等等。当验证通过后将其装入自己的链中，并向其他节点继续传播，否则直接将其抛弃。

将区块装入自己的链时，需要通过父区块的 Hash 值来判断该区块应该被连接到主链上还是分叉中还是孤立区块。最常见的情况就是新区块验证通过后，直接将新区块链接到当前区块链的最后一个区块后面，然后将主链高度增 1。但是考虑到区块链由于网络传输的原因，每个节点收到其他节点产生的新区块在时间上存在差异。比如假设有两个区块 A 和 B 在相近的时间内完成了计算，然后在相近的时间内将区块广播道网络中（且此时 AB 均未收到其他区块的广播），即这时会出现一些节点先接收到 A 区块而另一些节点先接收到 B 区块的情况，这些节点会选择把先收到的区块加入到自己的主链之中，然后把后收到的区块加入主链产生的分支链上形成分叉。而节点最终会选择工作量最大的（即高度最高）的链作为自己的主链。最后一种情况是当新区块的父节点并未被找到时（即有可能先收到了子区块而后收到父区块），该区块会成为孤立区块，后续当收到父区块后，孤立区块才会被链接到父区块后面。