区块链原理与技术 第二次作业

19335286 郑有为

题目：重点阅读 “Monoxide: Scale Out Blockchain with Asynchronized Consensus Zones”，思考以下问题

- 比特币设计简单，但是它能顺畅运行，背后有什么原因?
- Monoxide 提出的共识机制 与 比特币的共识机制有哪些不一样?
- 思考：连弩挖矿机制存在什么样的潜在问题?

比特币设计简单，但是它能顺畅运行，背后有什么原因?

- 安全机制：
    - 密码学原理：比特币使用哈希和数字签名。比特币使用哈希表示大量数据的唯一摘要值，作为数据的验证凭据，来保证数据的完整性和正确性；数字签名是信息发送者产生的一种无法伪造的数字串，他人可通过发送者的公钥来对信息来源进行验证，实现所有者确权。
    - 使用UTXO模型（未花费交易输出）来确保每个用户的比特币账户难以被伪造。
    - 使用默克尔树表示大量交易的摘要，使用前向哈希维护区块链链状结构，二者使比特币能够支持防篡改。
- 共识机制：比特币使用PoW（工作量证明）来实现共识，PoW难题不容易完成、容易验证、工作过程公平、具有随机性。对矿工而言是公平的，对交易而言是安全的。
- 激励机制：PoW规则中，成功挖到矿并提交的人可以获得系统一定数量的比特币的奖励以及用户附加到交易上的支付服务费用，矿工能在这个过程中获利，因此会自发地参与挖矿。
- 博弈结果：区块链的顺畅运行时多方博弈的结果。
    - 在共识模型中，基于纳什均衡和帕累托最优，拥有记账权的人更倾向在维护整个体系过程中获利；使用网络的人需要付出一定的成本以免滥用，少数人作恶的成功几率很低，只有极端势力才有可能不顾一切的颠覆这个体系 。
    - 在软分叉发生的过程中，没有升级的节点会因为不知道新共识规则下，而生产不合法的区块，就会产生临时性分叉。此时老节点挖到无效块，这些块不会被新节点接收，强迫老节点更新协议、规则，转而扩展最长的链 ，分叉自动消失，比特币的单链区块结构得以保持。
- 社区的健康生态：比特币社区成员形成网络，规模的扩大能增强比特币的安全性和可靠性，比特币的安全性，生态健康程度与比特币的币值相互影响。

Monoxide 提出的共识机制 与 比特币的共识机制有哪些不一样?

共识机制是区块链中的大多数或所有节点为同意建议的状态或值而采取的一组步骤。

- 比特币的共识机制：基于工作量证明（PoW）的挖矿，参与者需要通过消耗资源暴力解决一个问题来获得记账资格。
    - 具体的挖矿过程就是：参与者综合上一区块的哈希值，上一个区块生成之后的新的验证过的交易内容的Markle Root值，加上猜测的一个随机数Nonce，和时间，一起打包到一个候选新区块，让新区块的哈希值小于比特币网络中给定的一个数。
- Monoxide中提出的共识机制：本质上同样采用PoW。
    - Monoxide利用分片（Zone）的思想把区块划分为多个共识组来提升区块的可扩展性。不同共识组相互独立形成子系统，以线性地提升整个系统的交易处理速度（TPS）和吞吐量。
    - 通过[区号，分片规模，区块链的高度]三元组来标识一个区块，每一个用户给定一个地址，对地址进行计算来实现区域的划分。

- 划分群（Swarm），一个群内的成员享有对同一份数据集的拷贝，群内通过协议实现消息的传播。
- 使用最终原子性（Eventual Atomicity）来处理跨区的交易，简单理解就是把一个交易划分为两个阶段：取钱（Withdraw）和存钱（Deposit）。两个阶段形成发起方和收取方所在的两个分区内独立的挖矿。
- 通过连弩采矿，矿工可以通过解决一个证明工作的难题，在不同的区域创建多个区块。对于PoW目标值，连弩挖矿可以采用不同区相同目标值和不同目标值两种策略，不管是哪一种策略，都能充分利用物理算力，提高矿工挖矿的效率。

连弩挖矿机制存在什么样的潜在问题?

连弩挖矿机制允许矿工使用单个PoW解决方案在不同的区域同时创建多个块，但每个区域不能超过一个块。

- 在这个挖矿过程中，连弩挖矿机制趋于让算力平均分布在各个分区，但不使用连弩挖矿的一部分算力只在单个分区挖矿，这一部分算力可能会造成算力分布的不平均，导致它不完全公平。

  每个区的有效算力：$m_s = \frac{m_d}{2^k} + m_p$，$m_d$为连弩挖矿总算力，$m_p$为该区域非连弩挖矿算力。
- 连弩挖矿使得矿工效率更高，如果不能合理的调控区块的生成速度，将会导致Orphan rate升高，TPS下降。
- 跨区域的交易能从一个区块传输到另一个区块是必要的，但负责这个过程的一方没有收益，而是自愿进行。此过程缺乏激励机制。（但作者也有建议跨区域交易发行者设置两倍甚至三倍的交易费用金额）（Section 6.2）
- 最终原子性模型不适用于多对多支付的应用场景。（对于一个复杂的支付场景，最终原子性不适用，因而需要讲复杂支付分解一次次简单的Withdraw-Deposit过程）（Section 6.3）
- 冗杂：数据重复，由于最终原子性，一次跨区域交易将划分为两份子交易，分别加入到不同区块，使得实际处理的交易过程是不分区区块链系统的两倍。（Section 7.2）
  - 随着区块数目的增加，跨区域交易在所有交易中的比例会向100%趋近，固有讨论的意义。
  - 虽然交易内容不会变成原来两倍，但会产生两倍的Chaining Block（相当于比特币系统的区块头），在分区数目增多的情况下，这部分冗余所占用的空间更加明显。