区块链作业五

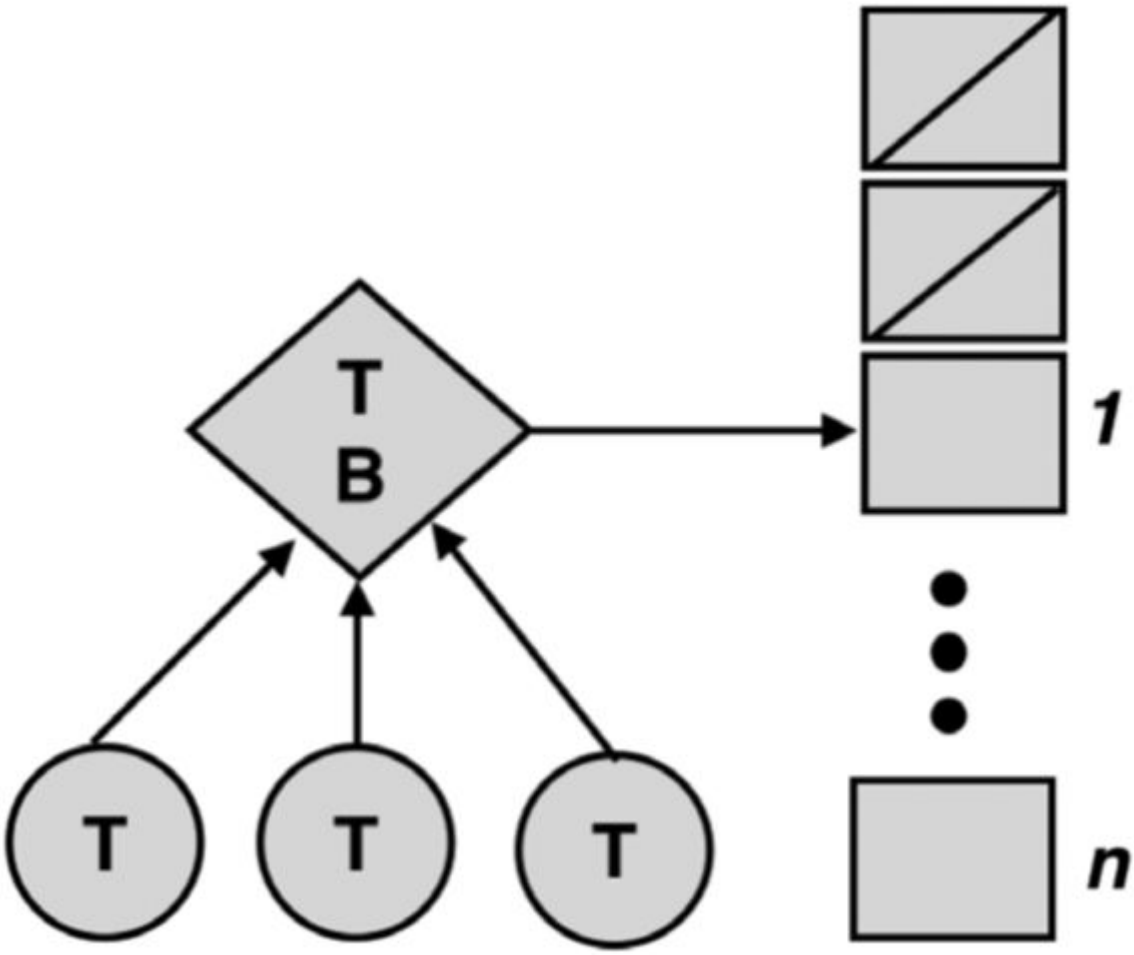
学号：16340023

姓名：陈明亮

一、当前区块链研究中用于提升区块链系统性能与可扩展性的方法总结

1. 区块链系统性能与两个测量指标与区块链扩展性直接相关：交易吞吐量（区块链可以处理交易的最大速率）和延迟（确认交易已包含在区块链中的时间）。比特币的交易吞吐量是其区块大小和块间间隔（时间）的函数。在当前块大小为1MB和10分钟块间间隔的情况下，最大吞吐量限制在每秒约7个交易；而创建交易的客户必须平均等待至少10分钟以确保交易包含在区块链中。目前的研究集中在开发显著提高区块链性能的解决方案，同时保持其去中心化特性。下面介绍几种专门用于提升区块链性能，增加其可扩展性的设计方案。

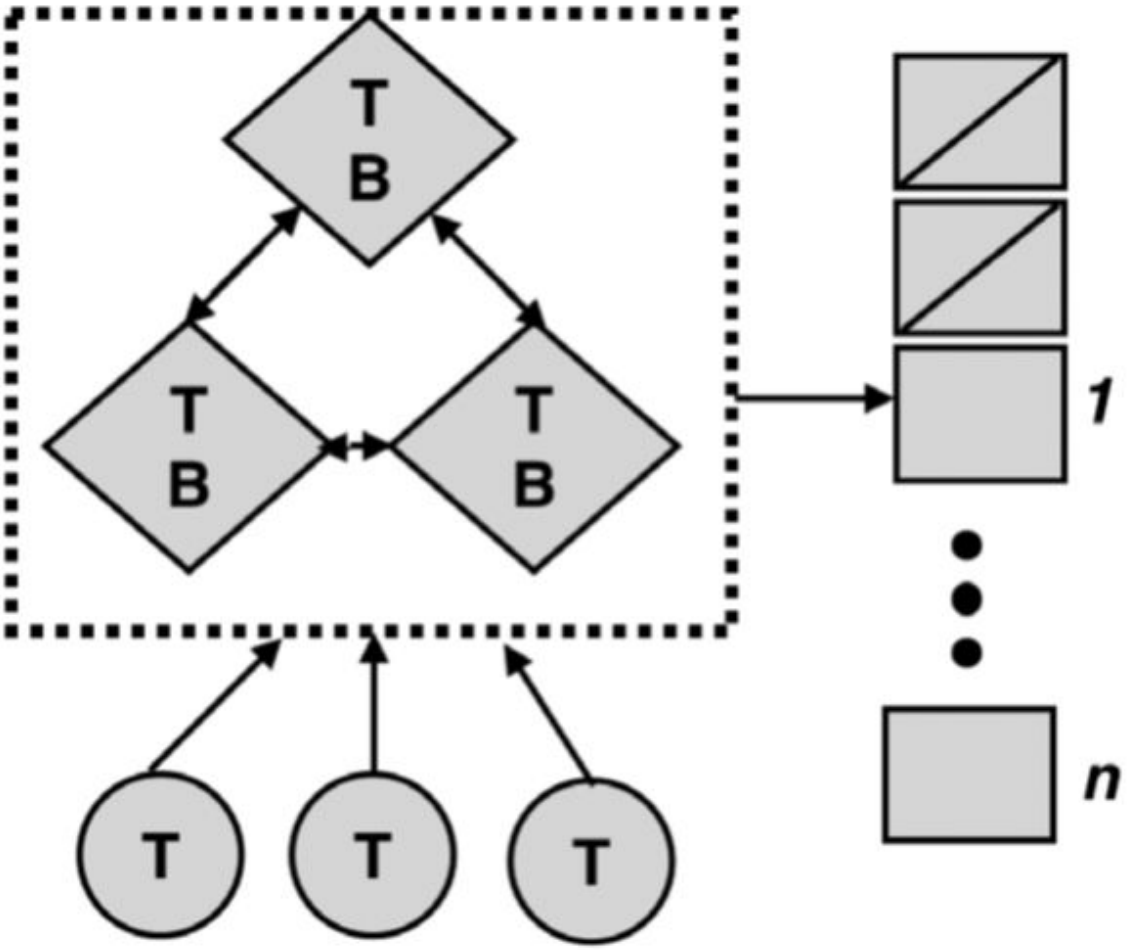
2. 多区块单一领导`Multiple Blocks per Leader`
    - Bitcoin-NG分享了比特币的信任模型，但将领导者选举（通过工作量证明随机且偶尔执行）与交易序列化解耦。然而，与比特币不同的是（比特币领导者节点只能提出一个区块来追加区块链），Bitcoin-NG将时间划分为epoch，领导者节点可以在其epoch期间单方面向区块链追加多笔交易，直到新领导者节点被选出。 Bitcoin-NG中有两种区块：密钥区块和微区块。 密钥区块包含一个难题答案，用于领导者选举。密钥区块还包含一个公钥，用于签署由领导者节点生成的后续微区块。每个区块都包含对前一个微区块和密钥区块的引用。费用会在当前领导者（40%）和下一个领导者（60%）之间分配。
    - 与比特币类似，通过增长（聚合所有密钥区块的）最长分支来解决分叉问题。请注意，由于这些微块不包含工作量证明，所以微区块不会影响分支的长度。为了对微区块中创建分叉的领导者节点进行惩罚，后续的领导者节点可以在其关键块（包含被剪枝分叉中的第一个块的头部）之后插入特殊的有毒交易作为欺诈证据。这使恶意领导者节点的报酬无效，报酬的一小部分支付给告发领导者。当一位新领导者选出但前任领导者还没有收到，并继续产生微区块时，分叉也会出现。然而，一旦新领导者选举的宣布达到所有节点，这些分叉就会得到解决。



3. 集体领导`Collective Leaders`

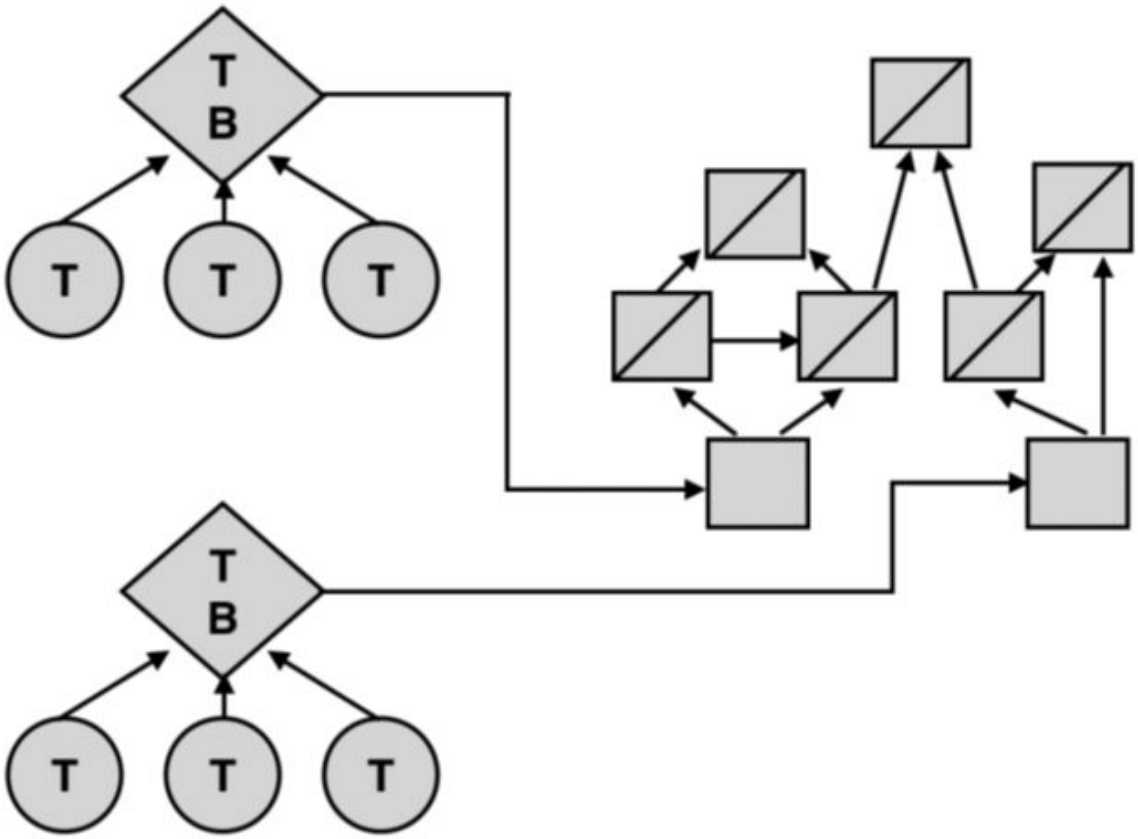
- 该方案采用多个领导者共同快速决定是否应该将区块添加到区块链中。ByzCoin通过扩展Bitcoin-NG取代比特币的概率性交易一致性保证（具有强一致性），以实现高交易吞吐量。这有一个好处，即客户提交的交易将被添加到区块链中，区块链仍然是无分叉的，因为所有领导者都立即就区块有效性达成一致。 ByzCoin修改了Bitcoin-NG的密钥区块生成机制：一组领导者，而不是单个领导者，产生一个密钥区块，然后是微区块。领导者小组由近期时间窗口的矿工动态组成。每个矿工的投票能力与其在当前时间窗口的挖矿区块数量成正比，这是其哈希能力。当一位新矿工解决难题之后，它将成为现任领导小组的一员，更进一步，替换出最老的矿工。 ByzCoin使用与比特币相同的激励模式，但报酬由领导者小组成员按其比例分摊。

- 领导者小组被组织成一个消息通信树，其中最新的矿工（领导者）在树的根部。领导者运行一个具有线性消息传递复杂度的实用拜占庭容错协议的修改版本，以生成一个集体签名，证明至少三分之二的共识小组成员见证并验证了该微区块。网络中的节点可以以O(1)时间复杂度验证该微区块已被共识小组验证为有效。这种设计解决了Bitcoin-NG的限制——恶意领导者节点可以创建微区块分叉：在ByzCoin中，这要求领导者小组成员的三分之二多数为恶意节点。此外，Bitcoin-NG遭受竞争条件困扰：一位尚未收到新领导者的老领导者节点可能会继续错误地在较早的微区块上进行挖矿。在ByzCoin中，领导者小组成员确保新领导者建立在最新的微区块之上。



4. 并行区块链增长`Parallel Blockchain Extension`
    - 如图6所示，在这种方法中，多个领导者并行增长区块链的不同部分（例如，交易图）。比特币具有增长区块链的线性过程：矿工尝试解决难题，找到答案的矿工追加下一个区块。由Boyen，Carr和Haines提出的框架通过放弃“区块”和“链”的概念来并行化这个过程（支持交易的图式交叉验证，而不是线性，可以理解为“区块图”）。每笔交易确认两笔交易（其双亲）并包含一些有效负荷（例如，加密货币）和工作量证明。

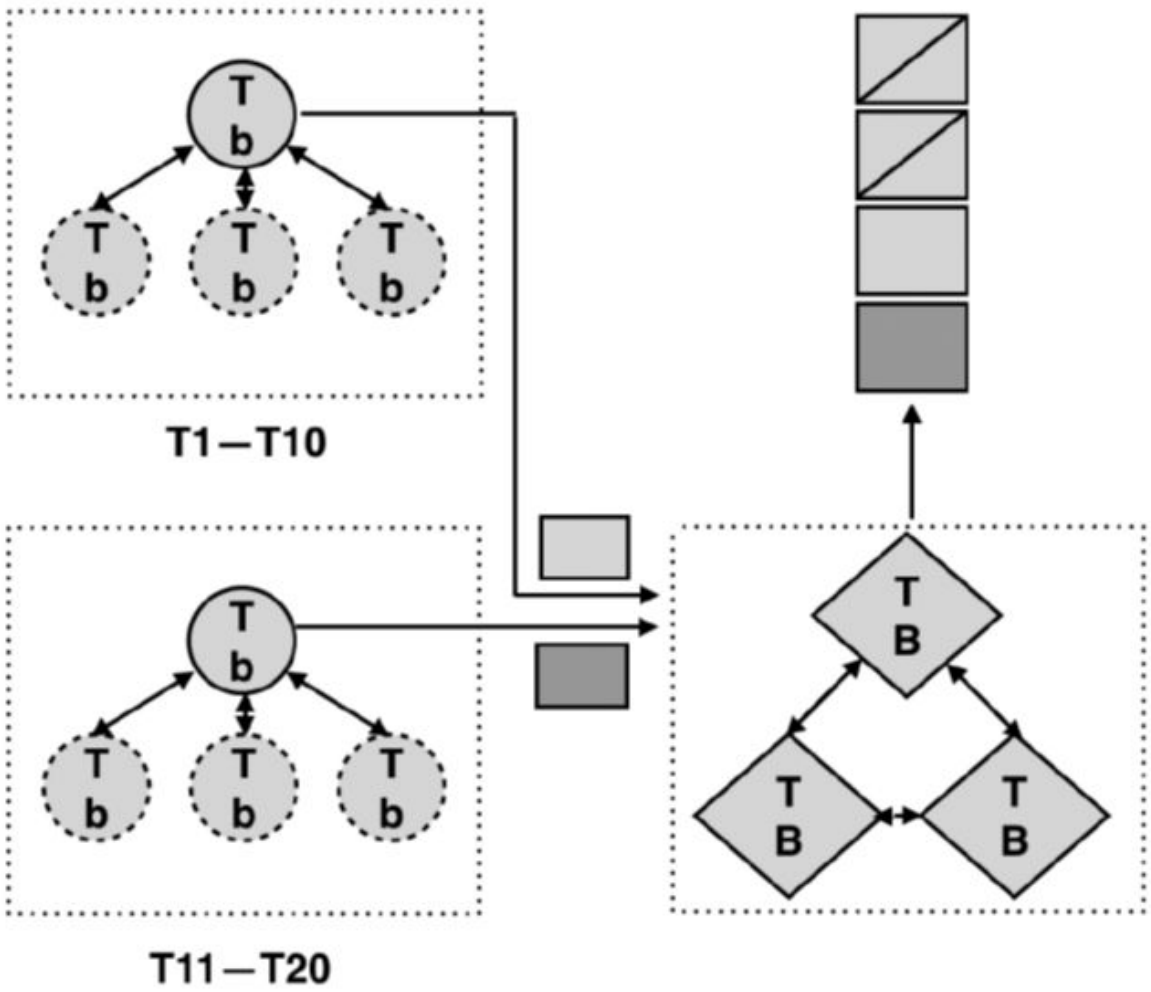
    - 交易可以由多个子节点进行潜在的验证。此外，每次交易还会包含一笔报酬，这笔报酬由验证该交易的交易收取。随着更多的节点直接或间接地验证它，报酬值会降低，因此新节点有更多的动机来验证最新的交易。该系统已被证明是收敛的，这意味着在某一时刻有一个交易连接到（并且因此隐式地验证）之前的所有交易。作为这种图结构的结果，矿工可以并行地增长交易图的不同分支。系统中的正常（非矿工）节点在收到交易时验证它们。除了对交易及其双薪的工作量证明正确性和结构有效性进行标准检查之外，节点还验证该交易不是双重支出（通过接受附加有最大工作量的良好格式的交易验证）。



5. 分片交易`Sharding Transactions`

- Elastico 将节点分成称为“委员会”的组，每个委员会管理交易的一个子集（分片）。在图7中，上部分片处理前10个交易，而下部分片处理后续10个交易。在委员会内，节点运行拜占庭一致性协议以协定交易区块。如果该区块已被足够的节点签名，委员会将其发送给最终委员会。最终委员会将从委员会收到的一系列交易整理到一个最终区块中，然后在其成员之间运行拜占庭一致协议以增长区块链，并将附加区块广播给其他委员会。

- 系统按epoch运行：分配给委员会的节点仅在epoch期间内有效。在这个epoch结束时，这些节点解决当前最终委员会产生的随机字符串难题，并将求解答案发送给下一个最终委员会。因此，在每个epoch，一个节点与委员会中的不同节点搭档，管理一组不同的交易。委员会数量与系统中可用算力成线性比例关系，但一个委员会内的节点数量是固定的。因此，随着更多节点加入网络，交易吞吐量增加而延迟不会增加，因为这里有一个解耦：一致性协议所需的消息与添加到区块链的最终区块的计算和广播之间的解耦。



三、区块链侧链技术，以及以太坊构建侧链方法

1. 侧链（SideChains）因为最早是由比特币提出，所以这个概念后期也更多的是在描述比特币相关的扩容，它的定义是：可以让比特币安全地从比特币主链转移到其他区块链，又可以从其他区块链安全地返回比特币主链的一种协议。

   比特币的闪电网络也可以认为是一种侧链，因为它允许用户A和用户B不在主链上直接交易，而是在“侧链”上进行频繁地进行了N笔交易之后，再把最后的交易结果同步到主链上。

   侧链的本质是，首先把你的一部分比特币（或者以太坊）锁定在主链上，并且在侧链上对你的货币进行操作，当操作周期结束之后再在主链上结算。闪电网络是比特币的第二层协议，很多人说闪电网络上的币和主链上的币是两种币，这是因为当你的比特币在主链上锚定的时候，你在闪电网络上操作的那些币，其实是已经脱离了比特币的存在，闪电网络的币之于主链上的比特币，就像是美元锚定在黄金（主链）上一样。

2. 关于如何通过以太坊构建侧链的方法，可以通过Loom Network使用侧链的技术来扩展以太坊。想要在Loom上开发DApp，可以使用Loom SDK为每个DApp生成一个侧链，它是以以太坊作为基础层的第二层区块链。Loom Network是以太坊应用程序特定的侧链网络，开发人员可以在其中大规模地运行分散的应用程序。Loom Network旨在成为一个平台，社区可以在侧链上运行软件，在平台上拥有既得利益的公平透明的既得利益，同时能够根据需求调整安全限制。