设计指导

星云研究院

2019 年 3 月
版本号:0.0.1

目录

1 简介

共识问题 (Consensus Problem) 是研究分布式系统中所有节点达成一致的问题，通常被定义为状态机复制（State Machine Replication），即对于所有节点均以相同顺序执行一个命令序列。而当存在恶意节点的情况下，共识被描述为拜占庭容错问题 (Byzantine Fault Tolerant，BFT）[1]。

在区块链技术出现之前，拜占庭环境下的共识问题并没有得到广泛关注。大多数 BFT 算法实际上在尝试解决拜占庭将军问题（Byzantine Generals Problem，BGP）[2]，即拜占庭容错问题的一个特例。在许多分布式服务中，对于发起状态更变的节点称之为领袖节点（Leader），后者一般由发起请求客户端指定或者按照某种固定算法决定[1]，所有节点对谁是领袖节点很容易达成共识。因此多数已有的共识算法不包括领袖选举或者并未强调其重要性。

区块链技术的出现让共识重新得到关注，2008 年发布的比特币白皮书 [3] 阐述了拜占庭环境下的共识解决思路，但其与传统的 BFT 算法存在较大差异。具体地，比特币中通过算力竞争的方式决定出块权（即领袖节点的选举），并且使用最长链原则实现了大规模节点的状态同步。

区块链共识仍然属于广义上的 BFT 问题，区块链之上的共识算法应该包括**领袖选举（**Leader Election**）和交易验证**（Transaction Verification）两部分 [4, 5]。尽管在一些区块链共识算法中两者没有被严格划分并且存在相关性 [6]，但我们认为将领袖选举和交易验证的解耦思想有助于我们理解区块链共识并且在此基础上设计更加合理的共识算法。

本文旨在简单介绍区块链共识中的领袖选举和交易验证，在此基础上给出相应的分析，从而为后续的共识设计提供指导。

2 相关研究

2.1 领袖选举

相比于传统分布式系统，在匿名和去中心化场景下区块链共识的领袖选举需要应对更多挑战。同时，由于区块链系统对于节点的设定不同，其采领袖选举机制也不

[1]一些算法允许在领袖发生故障时进行领袖重新选举。

尽相同。

以比特币 [3] 和以太坊 [7] 为代表的区块链对于出块节点（即领袖）没有准入限制，参与领袖选举的节点可以随时加入离开整个网络，此类区块链系统称之为无授权区块链（Permissionless Chain）。这类系统通过节点竞争方式选举领袖，其中最为广泛采用的算法是工作量证明（Proof-of-Work，PoW）。需要指出的是，PoW 仅仅实现了领袖选举，而并不是完整的共识协议，这一点在比特币白皮书上已经指出 [3]，而一种普遍的错误是将 PoW 和比特币共识（通常称之为 Nakamoto Consensus）混为一谈。

对于联盟链（Consortium Blockchain）以及部分采用 DPoS 机制的公链 [8]，参与节点需要通过授权并且不能随意加入离开，因此被定义为授权区块链（Permissioned Chain）。在此类系统中，一段时间内所有参与节点集合已知且不变，领袖选举可以采用简单的轮询机制（Round-Robin）[]。从而整个共识问题退化成传统分布式系统中的共识问题，即在领袖选择已经达成共识的情况下（此时领袖仍可以采取恶意行动），所有验证节点如何针对领袖的提案（出块）达成一致。

目前关于授权区块链是否能称之为区块链尚存在争议[2]，但可以肯定的一点是，无授权区块链更符合去中心化思想。不断有研究尝试解决无授权环境下的领袖选举问题。

由于 PoW 会消耗大量电力，权益证明（Proof-of-Stake，PoS）随后被提出，不同于 PoW，后者实现选举往往与链上资产相关而不依赖于物理算力因此都称之为 PoS，但不同基于 PoS 的共识之间通常差别较大。早期的 PoS 仍然是基于 PoW 的变种实现 [9]，即对谜题计算中的目标基于权益（Stake）或币龄（Coin-age）进行加权。作为备受瞩目的以太坊演进方案，Casper[10] 被认为是一种 PoS 协议，但实际上 Casper 是利用 stake 实现链式结构的终结性 (Finality)，并不涉及领袖选举过程，后者仍然可以选择采用 PoW 机制。

无授权区块链对于参与节点没有身份验证，因此对于领袖选取需要引入随机性，以保证安全 [11]。近几年涌现出一些基于随机数生成（Random Number Generation，RNG）的共识机制实现了非 PoW 领袖选举方案 [6, 12, 13]。尽管在出块方式和共识实现上存在区别（例如 Ouroboros 基于弱同步时钟），上述方案均利用伪随机函数（pseudo-random function）实现了领袖的随机选举。

2.2 交易验证

在分布式系统中，状态机复制可以有效解决多服务器之间的数据一致性问题 [14]。最为经典的 Paxos 协议实现了宕机容错（crash-fault tolerant）的一致性算法

[2]EOS is not a blockchain, https://thenextweb.com/hardfork/2018/11/01/eos-blockchain-benchmark/

[15]，其被广泛应用于数据库备份和域名服务等领域 [16, 17]。

随着区块链和数字货币的发展，基于拜占庭容错的一致性算法重新得到关注。在大规模节点网络中，网络通信成为瓶颈。以 Bitcoin 为代表的 permissionless chain 采取了最长链原则（Longest Chain Rule）[3]，[18] 提出了最重子树原则（GHOST Rule）。最长链和 GHOST 协议通常被称之为链式协议（chain-based Protocols），链式协议中节点仅依据接收区块构建链结构实现一致性而不产生额外的状态同步开销。对应地，链式协议仅能保证最终一致性（Eventual Consistency），即保证所有节点最终就共享状态达成一致，但在某个时间段内，共享状态各个节点所存的状态可能不一致。

联盟链以及部分公链通过缩小节点规模，实现了更强的一致性保证。节点针对每个提案进行投票，通常基于 PBFT[19] 或者更为宽松的投机 BFT 算法 [20]，此类机制被称之为投票协议（vote-based Protocols）。相比于链式协议，投票协议对系统要求更为严格，PBFT 和最差情况下的投机 BFT 网络通信开销为 $O(n^2)$，因此采用此类协议的网络往往规模较小。

基于 PBFT 机制，ByzCoin[5] 利用集体签名 (collective signing) 以及群签名 (CoSi) 实现了投票节点规模可扩展，因而在一些分片技术（sharding）中也被采用 [21]。

采用投票协议的区块链会针对每个出块进行一致性确认，因此每个区块状态不可能被扭转，从而实现终结性（Finality）。相比之下，基于链式结构的区块链在达到最终一致性前任何区块状态都可能发生改变（例如某个区块在某个时间后不再属于最长链），通常这种改变概率随着链式结构增长单调递减 [3]，因此链式结构共识无法保证终结性，或者仅提供概率终结性（Probabilistic Finality）。较为特殊地，Casper[10] 在检查点（checkpoints）内部采用最长链原则，而不同检查点间则通过投票保证终结性。

需要指出的是，通常认为采用链式协议的系统吞吐量（Throughput）低于基于投票协议的系统，实际上在仅满足最终一致性条件以及同等节点规模和网络环境下，链式协议实现状态同步开销更低。

3 系统模型

3.1 网络模型

分布式系统中，节点之间的通信方式主要为消息传递（Message Passing）。在同步网络（Synchronous Network）模型下，所有节点的消息传输延迟不会超过某个阈值；而在异步网络（Asynchronous Network）模型下，节点间的消息传输延迟可以是任意值。根据 FLP 定理 []，异步网络环境下，只要存在一个拜占庭节点则 BGP 问题

无解。

目前所有拜占庭容错的共识算法均是基于同步网络模型，一些更为宽松的模型允许网络中除领袖以外节点之间的通信可以为异步网络，后者称之为“弱终止假设”（或“半异步网络”）[19]。在本文中，我们基于同步网络模型讨论共识算法。

由于网络传输延时的存在，网络中的节点无法实现完美同步时钟（Perfectly Synchronized Clock）[3]，一种更严谨的描述方法是逻辑时钟（Logical Clocks）[22]。

在后文中，若没有特殊说明，t 均表示节点的本地时间。

3.2 数据模型

在区块链中，最基本的数据结构是交易（Transaction）和账户（Account），这里给出相关定义。

定义 1. （账户）一个账户 i 拥有一个私钥（Secret Key）sk_i 和基于私钥构建的公钥（Public Key）pk_i。一个账户 i 可以表示为多元组 $\langle pk_i, sk_i, s_i \rangle$，其中 s_i 表示用户 i 状态[4]。

以 Bitcoin 为代表的交易网络主要采用了未交易输出模型（Unspent Transaction Outputs Model，UTXO Model）；而以 Ethereum 为代表的区块链系统采用了账户模型（Account Model）。通常来说，账户模型设计更接近于传统记账系统（例如银行），并且支持图灵完备智能合约（Turing-complete Smart Contract），因此这里我们基于账户模型给出相关定义，需要指出的是，UTXO 模型理论上同样适用于我们的共识设计。

定义 2. （系统状态）系统状态定义为系统中所有账户的状态，即 $S = \{s_1, ..., s_n\}$。

定义 3. （交易）交易描述了一次系统的状态更变，一个交易包含交易发起账户 i 和接受账户 j 的状态更变，即 $tx_k = \langle s_i, s_i', s_j, s_j' \rangle$，其中 s_i，s_j 表示交易发生前账户的状态，s_i'，s_j’ 表示交易发生后账户的状态[5]。交易也可能使账户状态不发生变化，即 $s_i = s_i'$ 或者 $s_j = s_j'$。

在此基础之上，我们给出区块的定义。

[3]或者说节点间的时钟同步本质上也是一个共识问题。

[4]在交易网络中，用户状态即用户余额，随着智能合约和用户行为的多样化，这里统一称之为用户状态

[5]这里假设交易发生在一对账户间，对于多对多的交易可以转换为多笔交易

定义 4. （区块）区块是一个数据结构，一个区块 B 包含了一组交易 $Tx_B = \{tx_1, \ldots, tx_n\}$，一个指向上一个区块的引用 $h(B^{\prec})$，出块者的证明 φ_B 和时间戳 t_B，其中 $B^{\prec}$ 表示 B 所指向的前置区块，$h(\cdot)$ 为某种哈希函数。

4 领袖选举

4.1 基础

在传统分布式系统 [15, 19] 中负责发起状态更变请求的节点被定义为主节点 (Primary)，接受并验证请求的为副本节点（Backup）。而在区块链系统中，所有参与打包区块以及验证区块的节点，统称为矿工（Miner）[6]。为不引起混淆，后文统一将执行领袖选举协议的节点称之为提案者（Proposal），而选举具有出块权限的节点称之为领袖（Leader）。

首先，我们给出领袖选举的相关定义。

定义 5. （提案）对于提案者 i，其提案操作表示为函数 $M_i(Tx, B', \zeta_i)$，其中 Tx 为待验证交易集合，B' 为某已有区块，ζ_i 为提案参数。$M_i(Tx, \zeta_i) \in \{B, \perp\}$。

定义 6. （验证）对于提案者 i，其验证操作表示为函数 $V_i(B, t_i)$，其中 B 为待验证区块，t_i 为提案者 i 的本地时间。$V_i(B, t_i) \in \{0, 1\}$。

定义 7. （领袖选举协议 Π）对于提案者集合 N[7]，提案者 $i \in N$ 在 Tx 和 B' 不为空的情况下，执行提案操作 M_i，若输出为 B 则将其广播；同时提案者 $j \in N$ 在收到区块 B 后执行验证操作 V_j。对于提案者 $i \in N$，满足 $\exists j \in N, M_i = B \wedge V_j = 1$ 时，提案者 i 成为领袖。

通常而言，我们认为领袖选举机制需要满足以下性质：

- 随机性：提案者在执行提案操作前无法预知自己或者他人是否会成为领袖。
- 可验证：TBC

不难发现选举协议 Π 的随机性来自于提案操作 M 的随机性，这里我们首先给出 Π 随机性的数学描述。我们将时间表示为有序的离散[8]集合 T，因此提案者 i 的提案

[6]对于只参与同步并验证区块而不进行出块的节点，也称之为全量节点。
[7]N 可以为有限或者无限集合。
[8]当 T 为连续集合时，该定义仍然可描述，这里简单采用离散集合描述。

可以表示为随机过程 $\mathbb{X} = \{X(i,t), t \in T\}$。其中 $X(i,t)$ 表示为在 t 内 M_i 输出不为 $\perp$ 的概率。根据数学定义 [23]，如果一个随机过程在某个时刻的取值在这个时刻之前就可能可以知道（可测），则此随机过程称之为可预测过程（Predictable Process）。

定义 8. （提案 n 阶可预测性）在 t 时刻，如果已知 Tx, B', ζ_i，可确定 $t+1$ 至 $t+n$ 时刻 M_i 的取值，但无法确定 $t+n+1$ 时刻 M_i 的取值，则 M 具有 n 阶可预测性。

对应地，我们给出不可预测性的定义。

定义 9. （提案不可预测性）在 t 时刻，如果已知 Tx, B', ζ_i，不可确定 $t+1$ 时刻 M_i 的取值，则 M 具有不可预测性。

当选举协议可预测时，会出现若干潜在问题。例如自私挖矿（Selfish Mining）[24] 不需要承担风险因而变得更加普遍 []，并且节点在成为领袖前可能存在消极运行的问题（"last actor" problem）[13]。更进一步地，目前许多链上 DApp（例如博彩）的随机性来自于出块随机性，当出块可预测时，此类 DApp 则会有被操控风险。

此外，网络中的节点在接受到区块时需要首先验证区块的有效性，因此合法的区块需要具有有效性的特征。

特征 1. 基于区块 B 本身即可验证其有效性，即区块 B 的有效性仅与交易组 Tx_B、$B^{\prec}$ 和 φ_B 相关。

对于 UTXO 模型和 Account 模型，交易组的有效性验证方式不同，这里不做过多展开。对于 φ_B，根据领袖选举协议的不同其有效性验证方式也有所不同，具体分析见后续章节。在保证 Tx_B 和 $B \prec$ 有效性的情况下，区块 B 的有效性依赖于其出块证明 φ_B 的有效性。

4.2 PoW 协议

我们首先给出基于 PoW 的领袖选举机制相关分析。

定义 10. (选举协议 Π_w)基于 PoW 机制的领袖选举协议，有 $\epsilon = \langle d, t, nonce, Mr(Tx), \tau \rangle$，且：

$$M(Tx, B', \epsilon) = \begin{cases} B & \text{if } h(d, t, h(B'), nonce, Mr(Tx)) < \tau \\ \perp & \text{otherwise} \end{cases} \tag{1}$$

其中 $d \in N^+$ 表示困难程度，通常会随着时间动态调整,τ 表示目标值，$nonce$ 为一个临时随机数，t 为时间戳，$h(\cdot)$ 表示某种哈希函数，例如 Bitcoin 中采用的 SHA-256。对于提案区块 B，有 $t_B = t$，$Tx_B = Tx$，$Pre(B) = h(B')$ 以及 $V(B) = \epsilon$。

推论 1. Π_w 满足伪随机性。

证明. 根据公式1，$\Pr(M(Tx, B', \epsilon) = B)$ =$\Pr(h(d, t, h(B')|nonce, Mr(Tx)) < \tau)$，$h(\cdot)$ 具有伪随机性[9]，TBC □

推论 2. Π_w 具有可验证性。

证明. 对于提案区块 B，有 $V(B) = \epsilon$，对于其他提案者已知 $nonce$ TBC □

4.3 非 PoW 协议

目前基于非 PoW 的领袖选举协议主要是基于权益的领袖选举，在此我们给出几种具有代表性的非 PoW 选举协议。

定义 11. （选举协议 $\Pi^{\alpha}_{\bar{w}}$）对于提案函数 $M_i(Tx, B', \zeta_i)$，有 $\zeta_i = \langle s_i, t_i, \delta \rangle$，其中 s_i 表示提案者 i 的状态（即权益），t_i 为 i 的本地时间，δ 表示某个伪随机数，并且

$$M_i(Tx, B', \zeta_i) = \begin{cases} B & \text{if } g(s_i, \delta, t_i) = 0 \\ \perp & \text{otherwise} \end{cases} \tag{2}$$

$g(\cdot)$ 表示某种函数。对于提案区块 B，$Tx_B = Tx$，$B^{\prec} = B'$（即 $h(B^{\prec}) = h(B')$），$\varphi_B = \langle t_B, s_i, sig_i, \delta \rangle$，其中 $t_B = t_i|_{M_i=B}$，sig。

对于验证操作 V_j，具体地：

$$V_j(B, t_j) = \begin{cases} 1 & \text{if } V(B^{\prec}, t_j) = 1, t_j > t_B, g(s_i, \delta, t_B) = 0, sig_i ... \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

可以看出，执行协议 $\Pi^{\alpha}_{\bar{w}}$ 的提案者需要提供某个账户的权益证明（即 s_i），当提案者的当前时间满足条件 $g(s_i, \delta, t_B) = 0$ 时，则可以成为领袖出块。

[9]在给定 y 情况下，目前没有比穷举更好的算法来寻找 x 使其满足 $h(y|x) < c$。

推论 3. $\Pi_{\bar{w}}^{\alpha}$ 具有 1 阶可预测性。

证明. 对提案者 i，在 $t=n$ 时刻，已知 Tx，B' 和 $\zeta_i=\langle s_i,t,\delta\rangle$，$X(i,t)$=$\Pr(g(s_i,\delta,n)=0)\rightarrow[0,1]$。因为 g 为确定性函数，令 $t=n+1$，可以求得 $g(s_i,\delta,n+1)$，即在 t 时刻给定输入 Tx，B' 和 ζ_i，可以预测 $X(i,t+1)$。 □

推论 4. $\Pi_{\bar{w}}^{\alpha}$ 具有 ∞ 阶可预测性。

证明. 对提案者 i，在 $t=n$ 时刻，已知 Tx，B' 和 $\zeta_i=\langle s_i,t,\delta\rangle$，$X(i,t)$=$\Pr(g(s_i,\delta,n)=0)\rightarrow[0,1]$。令 $t=n+m$，可以求得 $lim\Pr(g(s_i,\delta,n)=0)$。即在 t 时刻给定输入 Tx，B' 和 ζ_i，可以预测 $X(i,t+m)_{m\rightarrow\infty}$。 □

可以发现最原始的协议不具备不可预测性，我们基于此做部分改动。

定义 12. （领袖选举协议 $\Pi_{\bar{w}}^{\beta}$）对于提案函数 $M_i(Tx,B',\zeta_i)$，有 $\zeta_i=\langle s_i,t_i,\delta\rangle$，其中 s_i 表示提案者 i 的状态（即权益），t_i 为 i 的本地时间，δ 表示某个伪随机数，并且 δ 更新周期为 Δ。

推论 5. $\Pi_{\bar{w}}^{\beta}$ 具有 Δ 阶可预测性。

5 交易验证

5.1 基础

基于第4章，在已选举出提案者的情况下，交易验证对出块进行验证。首先给出拜占庭环境下交易验证的相关定义和特性。

定义 13. （交易验证）对于验证者集合 V[10]，包含 n 个节点，其中最多有 f 个拜占庭节点，即最少有 $n-f$ 个诚实节点。所有节点必须从提案中最终做出决策，并且满足下述条件：

- 一致性（Agreement）：所有诚实节点的决策必定相同。
- 可终止性（Termination）：所有诚实节点在有限的时间内结束决策过程。

[10]类似于定义7，此处 V 可为有限或无限集合。

- 有效性（Validity）：选择出的决策值必须来自某个有效的提案。

在同步网络环境下，任何交易验证协议，都需要满足上述条件[11]。

如2.2小节介绍，交易确认机制根据块是否具有终结性划分为链式协议和基于投票协议。投票式交易验证满足终结性，即交易一旦完成验证则不可能发生改变。对应地，链式交易验证则仅满足概率终结性，即随着链结构的增长交易发生改变逐渐降低，但无法为 0。需要指出的是，即便是类似 PBFT 的投票协议，其数据结构仍可以采用链式区块结构。

从安全性角度，我们不希望已经验证的交易会存在修改的可能，即出现长距离攻击（Long-Range Attack）。同时，随着数据的不断增长，一些普通节点可能无法负担庞大的数据量，因此确定性的终结性可以减少数据的存储。最后，考虑到未来的分片设计，数据分片需要终结性作为基础。因此我们采用基于投票机制的设计，保证交易的终结性。

5.2 已有投票策略分析

首先我们对目前基于投票的验证策略进行简单分析。根据是否需要验证节点进行身份验证，我们将投票策略分为授权投票和无授权投票，通常来说分别适用于联盟链和公链。

5.2.1 授权投票策略：PBFT

PBFT 协议 [19] 中在已经指定主节点（Primary）的情况下，验证过程包括下面 3 步：

- PRE-PREPARE（预准备阶段）：主节点在收到请求后向所有副本节点广播与准备消息，其格式为 $\langle\langle PRE-PREPARE, v, n, d\rangle_{\sigma p}, m\rangle$，其中 v 是视图编号，n 是消息序号，d 是消息摘要，m 为请求消息，σp 为主节点 p 的签名；
- PREPARE（准备阶段）：一旦副本节点 i 接受预准备消息则进入准备阶段，同时该节点向所有副本节点发送准备消息 $\langle PREPARE, v, n, d, i\rangle_{\sigma i}$。当节点 i 收到 $2f$ 个从不同副本节点发来与 $PRE-PREPARE$ 相匹配的 $PREPARE$ 消息，则定义 $prepared(m, v, n, i)$ 为真；
- COMMIT(确认阶段):当 $prepared(m, v, n, i)$ 为真时，副本节点 i 将 $\langle COMMIT, v, n, D(m), i\rangle$ 广播至其他副本节点，进入确认阶段。对节点 i 而言，$prepared(m, v, n, i)$ 为真

[11]部分研究中将可终止性和有效性描述为活性（Liveness）。

且 i 已经接受了 $2f+1$ 个 $COMMIT$ 消息与 $PRE-PREPARE$ 消息一致则定义 $committed-local(m,v,n,i)$ 为真。而存在 $f+1$ 个正常副本节点集合使得其中所有副本节点 i 的 $prepared(m,v,n,i)$ 为真，则定义 $committed(m,v,n)$ 为真。

预准备阶段和准备阶段确保所有正常节点对同一个视图中的请求序号达成一致。而确认阶段保证了所有正常阶段对本地确认的请求序号达成一致，及时这些请求在每个节点的确认处于不同的视图。

不难发现，在 PBFT 策略中，验证节点 i 集合固定并且身份公开，在其发布 PREPARE 消息后其决策也公开可见，因而在其发布正常 COMMIT 消息前存在被攻击或者贿赂可能。所以对于采用 PBFT 算法的系统，无法适用于 Permissionless 环境。

5.2.2 无授权投票：Algorand

不同于 PBFT，Algorand[6] 针对 Permissionless 场景，其在领袖选举和交易验证中均采用了基于 VRF 的随机抽取策略，这里重点分析其交易验证部分。

Algorand 验证核心算法 BA★ 如下：

- Reduction：该步骤的目标是将需要达成共识的多个区块转化为对某一特定区块或者空块二选一达成共识；
- BinaryBA★：基于 Reduction 的输出，在特定区块和空块之间达成共识。在 $Maxstep$ 轮中没有达成共识则认为网络状况出现问题。

需要注意的是，在 Reduction 和 BinaryBA★ 中，都需要多次执行 $CommitteeVote()$ 和 $CountVotes()$ 操作，即投票和计票。这里重点分析前者，$CommitteeVote()$ 输入包括 $(ctx, round, step, \tau, value)$，其中 ctx 为环境变量（包括当前账本信息以及当前种子等等），$round$ 表示当前轮数，$step$ 表示执行当前计票操作的步骤（例如 Reduction-1），τ 表示抽签比例参数，$value$ 表示投票区块。

验证节点执行 $CommitteeVote()$ 时需要先执行 $Sortition()$ 即通过抽签判断自己是否有资格参与投票，不难发现，在给定 $round$ 和随机种子（$ctx.seed$）情况下，每个验证节点每次执行 $Sortition()$ 的结果固定。因此实际上在 Reduction 和 BinaryBA★ 过程中，仍然是同一批节点在参与投票，并且在 Reduction 中的第一次 $CommitteeVote()$ 之后，所有投票的节点身份已经曝光，因此也存在被攻击或者贿赂的风险。

Algorand 假设在整个 BA★ 过程中所有验证节点不会改变投票选择，在保证三

分之二诚实节点的情况下，如果收不到足够的投票则问题一定出在网络上[12]。但由于诚实节点仍可能会被攻击或者贿赂，我们认为该算法仍然存在问题。

5.3 投票模型

目前关于电子投票（Electronic Voting）的研究中 [25]，除去传统的隐私性（Privacy）、公平性（Fairness）和健壮性（Robustness）需求，理想的电子投票还需要满足如下要求：

- 可校验性（Universal-Verifiability）：任何第三方都可以验证最后的投票结果是否正确统计了合法选票[13]；
- 无收据性（Receipt-Freeness）：投票者无法向第三方证明其所投的选票内容；
- 无争议性（Dispute-Freeness）：任何第三方都可以验证协议的参与方是否正确执行了协议；
- 自计票性（Self-Tallying）：任何第三方可以进行计票，而不需要可信第三方或者投票者的参与；
- 完善保密性（Perfect Ballot Secrecy）：假设存在 n 个选民，任何 t 个（$t < n$）投票者的投票结果只有剩余 $n - t$ 个投票者串通起来才能知道。

而对于共识机制中的投票系统，由于不存在可信的第三方机构，每个验证节点既是投票者也是计票者(即所谓的"all voters are talliers")，因此其必须满足可校验性和自计票性。论文 [25] 指出在大规模的投票系统中，并不需要满足完善保密性。

现有大多数基于投票的共识机制都无法满足无收据性和无争议性，具体地来说，对于拜占庭验证节点，虽然无法伪造或篡改其他人的消息[14]，但仍可能出现如下恶意行为：

- 恶意投票：恶意验证者不发布任何投票或者对其他验证者发布不同的投票，例如对部分验证者发布 $\langle pk_i, sign_{sk_i}(t, h(B_1), \pi_i)\rangle$，而对另一部分验证者发布 $\langle pk_i, sign_{sk_i}(t, h(B_2), \pi_i)\rangle$，$B_1 \neq B_2$。
- 割裂网络：在采用 Gossip 协议传输的网络中，恶意节点可能在收到其他节点的投票后不向其他节点转发该信息，导致原有投票信息无法广播到所有节点。

[12] Algorand 假设网络最终会收敛于同步模型
[13] 另有原子可校验性描述仅投票者可以验证投票结果是否正确统计了合法选票。
[14] 通常而言，我们认为现有的签名算法可以保证信息无法篡改或者伪造。

- 共谋：恶意节点在投票前或者投票过程中得知其他验证者身份，从而贿赂其他验证者使其投票决策发生变化。

作为分布式系统，区块链中所有验证节点通过 P2P 方式进行通信，因此任何节点在投票过程中都无法检验其他节点是否正确执行协议，即在投票过程中无争议性无法保证。[15]在这种情况下，恶意投票和割裂网络将变得可行。这两种行为会导致决策无法收敛，从而影响共识的活性。

共谋行为则违背了无收据性，现有大部分投票共识都没有考虑拜占庭节点的共谋行为并且假设系统中拜占庭节点比例低于某个阈值（例如三分之一），而实际上，由于共谋行为的存在，系统中拜占庭节点比例会更高。

我们认为理想的投票机制应该抵抗上述三种恶意行为。首先，我们给出投票流程中的相关定义：

定义 14. （注册）对于任何期望参与验证过程的节点 i，执行操作 $R(s_i, \varepsilon)$，s_i 为节点 i 的状态，ε 为额外证明输入（通常为某个随机数），R 输出为

定义 15. （投票）对于验证节点 i，在接受某提案区块 B 后，满足 $V(B,t)=1$ 的情况下，对所有验证节点广播消息 $\langle pk_i, sign_{sk_i}(h(B), \pi_i)\rangle$。其中 $sign_{sk_i}(\cdot)$ 表示基于节点 i 私钥的签名，$h(B)$ 表示提案区块 B 的哈希值，π_i 表示验证节点 i 的投票效益证明。

定义 16. （验票）

定义 17. （计票）对于验证节点 j，对所有验证节点广播消息 $\langle pk_i, sign_{sk_i}(h(B), \pi_i)\rangle$。其中 $sign_{sk_i}(\cdot)$ 表示基于节点 i 私钥的签名，$h(B)$ 表示提案区块 B 的哈希值，π_i 表示验证节点 i 的投票效益证明。

5.4 补充：投票效益

除了投票过程中可能出现的攻击，对于投票效益的计算，我们认为也可能存在如下潜在的安全问题：

- 女巫攻击：投票过程必须能够抵抗女巫攻击（Sybil Attack），解决方法可以是通过设置准入门槛或者将投票效益与参与者的资产挂钩。

[15]尽管 Casper 通过 Slash 机制实现了检点的互相监督，但恶意行为被发现是基于交易已经上链的前提。

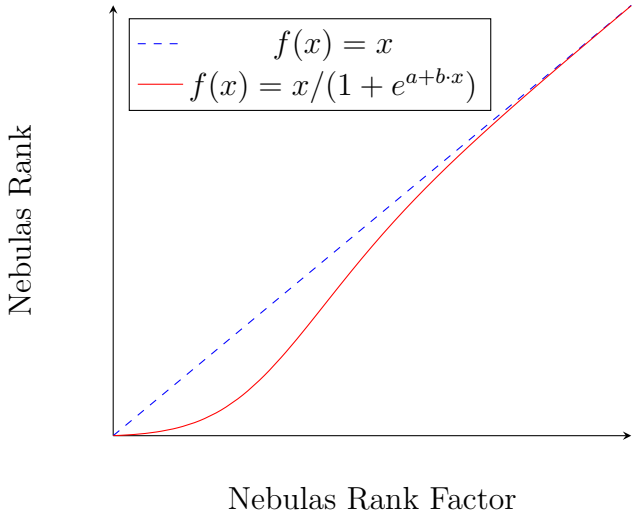

图 1: The curve of the Nebulas Rank function

- Nothing-at-Stake：通常而言区块链共识的投票是根据参与者的持有（或抵押）的资产计算所得，在没有投票成本的情况下，验证者更倾向分散其投票效益。一种解决方法是引入投票成本，或者对于分散投票行为作出惩罚 [10]。

A 对 PoW 的进攻方式

自比特币被提出同时成为最具影响力的区块链项目以来，对其核心的 PoW 协议的种种进攻方式的提出，以及相应的对策，相应安全性的分析从未停止过。目前大家熟知的就有“51% 攻击”（主要能实现“双花攻击”），以及 2015 年 Eyal 等人提出的“私自挖矿”攻击等等，同时还存在着鲜为人知甚至潜在的尚未被发掘的进攻方式。作为共识的设计者，深入了解此类进攻方式的工作原理及影响，并分析相应的对抗策略，无疑能为所设计共识的安全性提供极大帮助。

近期，Ren Zhang 等人关于 PoW 进攻方式的研究的论文发表在安全领域顶级会议 2019S&P 上（暂无引用链接）。这里我们以这篇论文为基础，简要概述其结论，并为本设计指导提出一些对 PoW 进攻方式见解与思考。

就目前而言最为广泛的进攻方式可大致分为两大类

- 分叉攻击

  这类攻击方式就包括我们熟知的**双花攻击**：在攻击者 a 支付数字货币的交易 $a \to b$ 被区块 B 打包，并且攻击者 A 获得实际（如线下收货）收益后，以 B 区块的父区块为根进行分叉产生新区块 B'，同时 B' 包含攻击者将同一笔数字货币支付给其小号的交易 $a \to a'$，进而达到否定区块 B 及其中交易 $a \to b$ 的目的。结果 b 没能收到款但 a 收到了货。

  通常认为双花攻击需要攻击者达到全网 50% 以上算力。

  同时也包括所谓的**私自挖矿攻击**。当攻击者挖出新区块后，并不选择立即公布这个区块，而是私自在新区块上继续挖矿并不断加长更新，即，维护自己的一条“私链”。当私链长度大于主链长度时，攻击者选择一直在私链挖矿。只有当私链长度等于主链长度时，攻击者才选择公布其私链并期望私链能赢得之后的算力竞争。结论表明只要攻击者算力大于全网的 1/3，私自挖矿即可以让攻击者有利可图。具体分析见原论文 [24]。

  私自挖矿可以和双花攻击进行结合，即先在主链进行交易后再公布私链用以否定主链交易。

- 定点攻击

  这类攻击有个专业名称叫 feather-fork，最早见于比特币论坛上[16]。

  此类攻击允许攻击者在拥有即使小于 50% 算力的情况下完全隔绝任何来自某特定地址（即所谓黑名单，如 Alice）的交易。具体操作如下：

[16]https://bitcointalk.org/index.php?topic=312668.0

攻击者事先做出一个承诺（commitment[17]）：我永远不会在任何包含来自 Alice 的交易的区块上进行挖矿。攻击者会一直遵循他所做的承诺。

作为一个普通矿工，当他听到攻击者的承诺后，作为一个利益最大化的个体，他在打包交易的时候也不会包含任何来自于 Alice 的交易：如果他的区块包含了 Alice 的交易，那么在攻击者拥有算力为 α（全网百分比）的情况下，至少有 α^2 的概率攻击者连续挖到两个区块，这两个区块将接在该矿工区块的父区块上，使该矿工挖出的区块成为孤块而丧失奖励。而矿工不打包 Alice 的交易仅仅损失少量交易费。其结果是，所有理性矿工都会隔绝 Alice 的交易，达成所谓定点攻击。一般而言 α 越大能拉拢的普通矿工越多。

造成定点攻击的原因在于理性矿工与协议矿工（reference miner）的区别：理性矿工总会最大化自己的利益，而协议矿工会至始至终按协议运作。定点攻击只有在协议矿工的比例少于 50% 时才作效。

- 其他攻击（跳链，矿池）。

  跳链严格来说不是一种攻击：因为比特币的挖矿难度是根据 2 周内平均挖矿时间动态调整的，那么，很多大矿工大矿池可以选择在比特币难度较高的时候转去其他 PoW 公链挖矿，待比特币难度降下来（必然结果。因为矿工跳槽了，总算力减少）之后再回归比特币。来源见于 Bitcoin-NG [4]

  所谓矿池相关攻击不属于共识层面，是因为矿池的引入导致各式矿工行为。这里稍微介绍下仅供参考。

  Pool-hopping [26]: 类似，有的矿池是根据单位时间收益（出块奖励/挖矿时间）来分配奖励。那么，矿工可以在某矿池挖了一段时间没挖出矿后跳到别的矿池去挖矿，因为在原矿池继续挖即使挖出来了因时间太长收益也低。一般为达到平均时间的 43.5% 即跳槽。

  派间谍（Miners' dilemma [27]）：简单而言，矿池 A 可以派一部分矿工，所谓间谍，去矿池 B 挖矿，但是间谍挖到真正的矿不会提交给 B 矿池，只提交挖矿的证明。（提交 share，难度为矿的千分之一）。相当于，间谍从 B 矿池领工资但不真正挖矿，工资分给 A 矿池的人。（当然 B 矿池也会向 A 矿池派间谍，形成一个类似囚徒困境的局面）。

文章接下来分析了某些著名的 PoW 项目针对这些攻击的安全性，同时提出了几项评价指标。这里不详细介绍。其重点结论在于，针对上述进攻安全性不能同时满足：存在一个安全性悖论："rewarding the bad and punish the good"。具体而言，对于区块链分叉，一般存在两种处理方式：

[17]commitment 是博弈论中一个重要概念。见 https://en.wikipedia.org/wiki/Stackelberg_competition

- 对所有分叉同给予同样奖励，所谓“reward-all”。举例包括 fruitchain，EthPoW（叔块）等。此类项目由于分叉没有损失，会加剧分叉攻击。
- 对分叉进行惩罚，所谓“punishment”，如将出块奖励均匀分发给各个分叉。举例包括 DECOR+，Bahack‘s idea。此类项目由于分叉损失过大，理性矿工会更加担心自己挖出的块成为孤块，进而加剧定点攻击。
- 还有一类叫做“reward lucky”。此类协议奖励某些区块，定义比较模糊。举例如 Subchains,Botail。但是文章认为 lucy 不等于 good，也不能达到效果。

所以，该论文给我们的思考在于，设计共识应达成上述安全性的一个平衡。

文章最后给出的共识参考建议也值得一提：

- 设计的协议不应该太复杂。
- 不应只针对特定的攻击来进行安全性分析。(应全面考虑)
- 不应针对特定攻击者奖励进行安全性分析。(应全面考虑)

另外，文章指出安全性能基于下面几项要素得到提高

- 网络环境更好
- （弱）全局时钟的存在
- 可信赖的第三方
- 责任外包制度
- 基于“Layer 2”的抗攻击手段。

B 谜题选择

谜题（puzzle）在 PoW 协议中扮演重要角色。通常，PoW 协议规定只有解决给定谜题的矿工拥有出块权，是一种抵抗女巫攻击的有效手段。有文章指出 PoW 本质是通过谜题实现一个分布式时钟[18]。

谜题的选择同样也面临各式各样的取舍：

[18]https://grisha.org/blog/2018/01/23/explaining-proof-of-work/

- 谜题固然需要一定的难度来防止女巫攻击，但另一方面，有研究表明对于任何算力竞赛模型，高难度的谜题存在马太效应，更容易造成大户垄断(51%dominance)。

- 谜题的难度固然需要动态调整以适应不断升级的算力，但另一方面，动态难度会造成跳链现象（见章节A)。同时，动态难度也会遭受所谓长程攻击（long-range attack)，即攻击者从某远古区块开始一直以极低算力挖一条私链，因难度是动态的私链增长速率可以和主链一致，然后攻击者一定时间段突然加大算力，使私链长度大于主链。通常解决长程攻击的方式为矿工检测到分叉时，除简单的采取最长链原则外同时也要检测区块难度，以摒弃难度过低的链。

鉴于谜题在 PoW 协议中的重要作用，作为区块链共识设计者，了解包括比特币在内的多个 PoW 所采用的谜题及工作原理，优势劣势等，也是设计合理的 PoW 共识必不可少的一部分。

本章节主要针对 Mimblewimble 共识协议（Grin 项目）所采取的谜题进行介绍并展开思考。该谜题名称叫 cuckoo，发表在 2015 年 FC 上 [28]。

比特币的挖矿工具经历了 CPU，GPU，FPGA，ASIC 四个阶段。现今有比特大陆等矿机公司已经本质上实现了比特币的算力垄断。而 cuckoo 旨在提出一种新的谜题，使得挖矿工具的更新停留在 GPU 这一步——只有 1060 以上显卡才能进行挖矿。

谜题的本质是验证（verification）与探索（proof attempt）的不对称性。比特币所采取的 SHA256 由于哈希函数的难逆性无疑符合条件。cuckoo 采取的是随机图找环算法，通过引入内存带宽限制构建谜题的难度。具体步骤如下:

- 图的生成。

  二部图的 N 个点已经给定，通过哈希函数随机生成二部图的 M 条边（大约 $N/2$)。生成边的方式要满足一定的要求，可以理解为每条边是根据 $(k, nonce)$ 的 SHA512 值决定，其中 k 为编号，$nonce$ 为矿工尝试的数字。验证时，一旦给出 nonce 则可还原出图中所有的边。

- 谜题目标。

  给定一个图，矿工需要给出一个长为 L 的环。验证时，一旦给出图以及 L 个点的编号，可以轻易验证环是否能形成。

  值得一提的是，从一个图里面寻找长为 L 的环是多项式时间可解的[19]。然而由于图的生成是完全随机的，且每个图大概率不存在长为 L 的环，故矿工仍然需要暴力搜索。

[19] L 为偶数时，时间复杂度为 n^2。L 为奇数时，时间复杂度为 $M(n)$，其中 $M(n)$ 为计算矩阵乘法所需的时间复杂度。

- 找环推荐算法。

  文章推荐算法包含两部分。

  - 减支部分

    所谓减支本质上是完成一个拓扑排序问题：去掉所有度数为 1 的以及相邻的边，重复上述过程直到所有点的度数 ≥ 2。由于上述减支过程需要存储每个点的度数，故需要进行大量内存读取。这就是该谜题能引入内存带宽限制的原因。

    文章同时也提出了其他的减支算法，$BFS(L)$ 和 $BFS(L/2)$，能避免对每个点都记录信息，但会消耗更多的时间，是一种时间和存储的平衡（TMTO，time-memory trade-off）

  - 找环部分。

    文章推荐的找环算法维护一个有向图森林，以类似并查集的方式将边逐条加入。一开始，所有孤立点各自都是一座森林。一旦一条边加入，如果两个端点属于两个不同森林，则将两个森林合并，通过维护森林中边的指向与每个节点的 root 值。当且仅当新加入边的两个端点属于同一森林时，则必存在一个环，可根据有向图路径找到该环并确定长度。

    值得一提的是，如果找出来环的长度不为 L，则忽略该条边继续上述操作。这样虽然可能导致有的长为 L 的环被漏掉，但这种情形概率不高，作为一种概率性的算法仍能保证高效性[20]。

文章推荐的数据规模 $N = 2^{25} + 2^{25}$，$L = 42$

文章接下来给出了很多实验图表。这里不一一列出，仅简要介绍结论。

- 计算哈希函数的时间开销随着节点规模增大而减小，最终低于 15%。（大部分时间用于找环）
- 存在 42 环的概率在 $M/N > 1/2$ 时剧烈增长。
- 内存的读开销随着已尝试 nonce 的百分比指数级上升，但写开销持平。
- 存在环的概率与 L 大约成反比。

总结：就目前而言 cuckoo 能限制矿机，但同时也需要考虑到新型矿机的可能性（如基于路由器的大带宽）。

[20]高效概率性算法在实际运作中比比皆是。一个经典的例子是质数判定问题 $Prime()$。有研究已经证明该问题是多项式时间可解，但时间复杂度仍然很高。实际运行时人们仍然选择用费马小定理进行判断。后者不能保证 100% 正确但更快。另一个例子是线性规划问题，虽然已被证明椭圆算法能在多项式时间解决，但人们更多的还是采用单纯形法，后者不能保证多项式时间解决，但实际平均运行时间往往更低。

参考文献

[1] M. Pease, R. Shostak, and L. Lamport, "Reaching agreement in the presence of faults," Journal of the ACM (JACM), vol. 27, no. 2, pp. 228–234, 1980.

[2] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 4, no. 3, pp. 382–401, 1982.

[3] S. Nakamoto et al., "Bitcoin: A peer-to-peer electronic cash system," 2008.

[4] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, "Bitcoin-ng: A scalable blockchain protocol," in 13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16), pp. 45–59, 2016.

[5] E. K. Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford, "Enhancing bitcoin security and performance with strong consistency via collective signing," in 25th {USENIX} Security Symposium ({USENIX} Security 16), pp. 279–296, 2016.

[6] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling byzantine agreements for cryptocurrencies," in Proceedings of the 26th Symposium on Operating Systems Principles, pp. 51–68, ACM, 2017.

[7] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum project yellow paper, vol. 151, pp. 1–32, 2014.

[8] I. Grigg, "Eos-an introduction," Whitepaper) iang. org/papers/EOS_An_Introduction. pdf, 2017.

[9] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," self-published paper, August, vol. 19, 2012.

[10] V. Buterin and V. Griffith, "Casper the friendly finality gadget," arXiv preprint arXiv:1710.09437, 2017.

[11] R. Pass and E. Shi, "Rethinking large-scale consensus," in 2017 IEEE 30th Computer Security Foundations Symposium (CSF), pp. 115–129, IEEE, 2017.

[12] B. David, P. Gaži, A. Kiayias, and A. Russell, "Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain," in Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 66–98, Springer, 2018.

[13] T. Hanke, M. Movahedi, and D. Williams, "Difinity technology overview series–consensus system (rev. 1)," 2018.

[14] F. B. Schneider, "Implementing fault-tolerant services using the state machine approach: A tutorial," ACM Computing Surveys (CSUR), vol. 22, no. 4, pp. 299–319, 1990.

[15] L. Lamport et al., "Paxos made simple," ACM Sigact News, vol. 32, no. 4, pp. 18–25, 2001.

[16] M. Burrows, "The chubby lock service for loosely-coupled distributed systems," in Proceedings of the 7th symposium on Operating systems design and implementation, pp. 335–350, USENIX Association, 2006.

[17] F. Chang, J. Dean, S. Ghemawat, W. C. Hsieh, D. A. Wallach, M. Burrows, T. Chandra, A. Fikes, and R. E. Gruber, "Bigtable: A distributed storage system for structured data," ACM Transactions on Computer Systems (TOCS), vol. 26, no. 2, p. 4, 2008.

[18] Y. Sompolinsky and A. Zohar, "Secure high-rate transaction processing in bitcoin," in International Conference on Financial Cryptography and Data Security, pp. 507–527, Springer, 2015.

[19] M. Castro, B. Liskov, et al., "Practical byzantine fault tolerance," in OSDI, vol. 99, pp. 173–186, 1999.

[20] R. Kotla, L. Alvisi, M. Dahlin, A. Clement, and E. Wong, "Zyzzyva: speculative byzantine fault tolerance," in ACM SIGOPS Operating Systems Review, vol. 41, pp. 45–58, ACM, 2007.

[21] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "Omniledger: A secure, scale-out, decentralized ledger via sharding," in 2018 IEEE Symposium on Security and Privacy (SP), pp. 583–598, IEEE, 2018.

[22] L. Lamport, "Time, clocks, and the ordering of events in a distributed system," Communications of the ACM, vol. 21, no. 7, pp. 558–565, 1978.

[23] H. van Zanten, "An introduction to stochastic processes in continuous time," Lecture notes, 2013.

[24] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," Communications of the ACM, vol. 61, no. 7, pp. 95–102, 2018.

[25] A. Kiayias and M. Yung, "Self-tallying elections and perfect ballot secrecy," in International Workshop on Public Key Cryptography, pp. 141–158, Springer, 2002.

[26] M. Rosenfeld, "Analysis of bitcoin pooled mining reward systems," arXiv preprint arXiv:1112.4980, 2011.

[27] I. Eyal, "The miner's dilemma," in 2015 IEEE Symposium on Security and Privacy, pp. 89–103, IEEE, 2015.

[28] J. Tromp, "Cuckoo cycle: a memory bound graph-theoretic proof-of-work," in International Conference on Financial Cryptography and Data Security, pp. 49–62, Springer, 2015.