计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2023,32(2):13−24 [doi: 10.15888/j.cnki.csa.008938]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于市场证明共识的分布式账本协议: Achain①

薛立德, 徐鑫朋, 桑　耘, 于铭华, 邱　定

(中国电子科技集团公司第三十二研究所, 上海 201808)
通信作者: 薛立德, E-mail: xldxld@mail.ustc.edu.cn

摘　要: 区块链技术给加密货币带来了新的变化, 并得到了广泛的应用. 然而, 它仍面临着高吞吐量、低交易延迟、安全性和去中心化的需求和目标. 此外, 消费节点 (交易提供者) 的意愿难以映射到 leader 中, 区块开采者热衷于挖矿竞赛也导致中心化和能耗的加剧. 为此, 提出了一种不同于传统 PoW (proof-of-work) 共识的新型共识算法——PoM (proof-of-market), 及其第一个实施案例——Achain 协议. PoM 的算法设计使得消费节点进行 PoW 工作, 并投票选出 leader 节点. 这不仅离散化了挖矿的工作, 提升了去中心化, 降低了能耗, 还体现了消费节点的意愿, 只有受到最多支持的节点才能成为 leader. 在性能上, 相较于 PoW 型区块链, Achain 还提升了可扩展性, 此外, 还提供了一种 Achain 节点存储优化方案——FastAchain; 在安全性方面, Achain 辅以一套激励相容的奖惩机制使得恶意节点的收益期望为负, 这保护了诚实节点的利益, 且 Achain 可以容忍至多 1/3 的全网总算力被恶意节点控制. 为了验证 Achain 的性能表现, 实施了一个大规模网络下的 Achain 原型用来评估其相关性能, 结果表明 Achain 达到了预期, 优于一些主流的代表性区块链协议, 且保持了良好的链收敛性和去中心化.

关键词: 区块链; 分布式算法; 分布式共识; 工作量证明; 分布式交易账本

引用格式: 薛立德,徐鑫朋,桑耘,于铭华,邱定.基于市场证明共识的分布式账本协议: Achain.计算机系统应用,2023,32(2):13–24. http://www.c-s-a.org.cn/1003-3254/8938.html

Achain: A Distributed Transaction Ledger Based on Proof-of-market

XUE Li-De, XU Xin-Peng, SANG Yun, YU Ming-Hua, QIU Ding

(The 32nd Research Institute of China Electronics Technology Group Corporation, Shanghai 201808, China)

Abstract: Blockchain technology has brought new changes to cryptocurrencies and has been widely used. However, it still faces the needs and goals of high throughput, low transaction latency, security, and decentralization. In addition, the willingness of consumption nodes (i.e., transaction providers) is difficult to be mapped into leaders, and block miners are keen on mining competitions, which also leads to intensified centralization and energy consumption. To this end, a new consensus algorithm, PoM (proof-of-market), and its first implementation case, the Achain protocol, are proposed. The algorithm is different from the traditional PoW (proof-of-work) consensus, and its design enables consumer nodes to perform PoW and vote for leader nodes, which not only discretizes the mining, improves decentralization, and reduces energy consumption but also reflects the willingness of consumer nodes. In other words, only the node mainly supported can become the leader. In terms of performance, Achain also improves scalability compared with PoW-type blockchains, and it provides a solution for node storage and optimization, which is called FastAchain. In terms of security, Achain is supplemented by a set of incentive-compatible reward and punishment mechanisms to make malicious nodes have negative revenue expectations, which protects the interests of honest nodes, and Achain can tolerate up to 1/3 of the total network computing power being controlled by the malicious nodes. In order to verify Achain's performance, a prototype of Achain under a large-scale network is implemented for evaluation. The results show that Achain has achieved

① 收稿时间: 2022-06-15; 修改时间: 2022-07-18; 采用时间: 2022-08-15; csa 在线出版时间: 2022-11-04
CNKI 网络首发时间: 2022-11-15

expectations, outperformed some mainstream representative blockchain protocols, and maintained positive chain convergence and decentralization.

Key words: Blockchain; distributed algorithm; distributed consensus; proof-of-work (PoW); distributed transaction ledger

比特币 (Bitcoin)[1] 是许多现有分布式账本系统中最典型的例子, 其背后被称作“区块链 (blockchain)”的分布式共识技术也成为了学界及工业界研究的目标. 其核心目的是让用户在没有可信第三方的情况下, 就公共账本信息达成共识. Nakamoto 共识, Bitcoin 的核心共识算法, 使用工作量证明 (PoW) 算法使节点参与 Bitcoin 系统并执行哈希计算操作来确保整个系统共识的安全性. Nakamoto 共识宣称只要系统中恶意矿工的算力不超过全网总算力的 50%, 那么该系统就是有效安全的, 不过后来的工作揭示了 Nakamoto 共识的一些缺点和潜在的攻击方案, 例如, 自私挖矿、顽固挖矿、日蚀攻击等[2−6].

除了这些攻击和漏洞之外, Nakamoto 共识的可用性相较于当前的线上交易需求来说也很差——其平均每秒钟只能处理 7 笔交易, 且平均交易确认延迟高达 1 小时[7]. 另外, PoW 型区块链还面临去中心化的挑战. PoW 的 leader 选举已经显现出明显的“中心化倾向”与“不公平”(例如, 前 4 大 Bitcoin 矿池公司的总算力已超过全网算力的 50%[8]), 过度的中心化也非常容易导致一些安全性问题. 传统的 Byzantine fault tolerance (BFT) 类协议则是完全去中心化的[9], 但它们限制节点自由加入或退出系统, 并且很容易被 distributed denial of service (DDoS) 攻击破坏. 目前, 许多高性能的共识协议都是基于以上两大类共识算法 (PoW 与 BFT), 然而它们都或多或者存在一些缺陷和不足, PoW 类方案则是把系统效率和安全性过度耦合造成性能瓶颈; 而 BFT 则无法适用于大网络多节点共识环境, 且需要额外的节点验证机制才能防止例如 DDoS、Sybil 类型的恶意攻击.

为了解决上述问题, 本文介绍 PoM 共识算法及基于 PoM 的第一个分布式账本协议——Achain. PoM 将 PoW 共识和 leader 选举解耦, 大大削弱了安全性和出块间隔间的相互约束, 提高了系统吞吐量, 降低了交易延迟. 并且在相同的网络环境下, Achain 与 Bitcoin 一样安全.

Achain 的核心算法——PoM 机制主要分为两部分: leader 选举和消费节点 PoW. 在 leader 选举中, 消费节点通过向他支持的候选节点提交合法交易数据来表示他在 leader 选举中支持此候选节点, 其中, 合法交易数据将被视为“选票 (vote)”. 只有收集了预定数量的 vote 的候选节点才能成为 leader 节点. 在消费节点生成 vote 时, 其必须执行相应的消费节点 PoW, 否则此 vote 将是非法的. Achain 协议提供了一组激励机制来匹配 PoM 使得恶意的攻击在统计学意义上是无利可图的. 此外, 即使有不理智的攻击者坚持攻击, 他的攻击也不会比攻击相同设置 (例如, 相同的 PoW 难度和自然分叉率) 下的 PoW 型区块链的难度要小, 因为 PoW 和 PoM 具有相同的防御机制和防御特性. 而且 Achain 协议拥有比 PoW 类区块链更大的可控空间 (例如, 可以通过调整 PoM 的一些参数来抑制自然分叉率). 总的来说, PoM 实现了 PoW 型区块链的安全性, 其还可以有效抑制区块传输延迟对区块间隔和安全性的约束, 进而优化了 Achain 协议的吞吐量、交易延迟、去中心化、公平性以及能耗. 同时体现了消费节点和市场在 leader 选举方面的影响 (而非完全的数学意义上的随机化). 并且我们还提供了一种针对 Achain 的优化方案——FastAchain, 其降低了系统节点的存储成本, 提升了系统的可扩展性和去中心化程度.

此外, 本文通过 omnetpp 模拟了一个 p2p 实验网络, 其具有 30 Mb/s 的带宽和 100 ms 的平均延迟, 并包含超过 1 000 个分布式对等节点. 实验检测了协议的各个参数对 Achain 性能的影响. 结果表明, 在大多数参数设置下, Achain 可以实现出色的吞吐量和交易延迟 (超过 4 000 TPS 以及 10–40 s 的交易延迟). 在相似的网络环境下, Achain 的吞吐量达到了 10 倍于 Bitcoin-NG[7]、5 倍于 ByzCoin[10] 以及 4 倍于 Algorand[11] 的水平, 交易延迟也达到了与 Algorand 相同的水平, 并且只有 Bitcoin-NG 和 ByzCoin 的一半. Achain 系统中上链的交易在等待 3 个区块后的回滚率为 0%, 且几乎没有高度超过 1 的分叉, 这说明该方案具有较高的安全性和可靠性. 并且 Achain 在所有参数设置下都保持了出色的去中心化水平.

1 相关工作及与 Achain 的对比

不可否认, 当前的区块链设计还存在诸多难题, 其中讨论最多的便是可扩展性 (scalability) 问题. 为此, 学界和工业界还提出了许多解决方案, 例如 Bitcoin-NG[7] 和 ByzCoin[10]. Bitcoin-NG 引入了“key block”和“micro-block”的概念, key block 使用经典 PoW 算法进行 leader 选举, microblock 用于存储交易. 并且为了防止双花攻击, Bitcoin-NG 引入了“毒药交易”机制. ByzCoin 则是基于 Bitcoin-NG 和 practical Byzantine fault tolerance (PBFT) 协议[9] 的进一步改进. 它将 leader 选举和交易确认分开, 并使用 PBFT 委员会的认证来立即确认交易. ByzCoin 实现了与 Paypal 相当的吞吐量, 确认延迟为 15–20 s. 然而, 它们仍然将 PoW与 leader 选举联系耦合起来, 并且引入了除 PoW 外的复杂共识机制 (例如, PBFT), 这将在极端情况下大大降低系统效率. 此外, 对 PoW 的一些修改 (例如, proof-of-stake (PoS)、delegated proof-of-stake (DPoS)[12]) 并没有改变 PoW 的本质. 相反, Achain 的 PoM 机制虽然仍然需要执行 PoW 操作, 但 PoM 将 PoW 操作分散到消费节点级别, 这解耦了系统的安全性和效率, 使两者均得到了提升.

Algorand[11] 中则首次采用了 VRF&BFT 机制, 它使用可验证的随机数来确保 leader 节点选举的数学公平性. 类似地, 随后也有很多混合共识协议被提出[13–15], 它们大都基于 PBFT 算法, 并融合了 RAFT[16]、分片 (sharding) 等技术, 以此实现扩展性的提升. 与上述协议不同的是, 本文的 PoM 并未使用复杂的混合共识机制, 而是基于新型 PoW 算法辅以激励策略在候选节点之间实现了激励相容, 并考虑到市场因素和消费节点的偏好.

还有许多学者提出了完全不同于 PoW 的新型共识算法设计, 例如 PoB (proof-of-burn)[17] 和 PoR (proof-of-reputation)[18]. 虽然两者都实现了可观的性能表现, 但前者要求节点将代币 (token) 发送到一个“不可使用的 (unspendable)”交易地质进行“销毁”, 这浪费了太多的算力和虚拟代币, 后者则以中心化为代价实现了对于“超过 51% 恶意算力攻击”的抵御.

区块链可扩展性的最终目标是“无限扩展 (scale-out)”——网络规模扩大到任何程度都不会影响系统的性能, 甚至系统性能可以随着验证节点的增加而提升. 目前有两种主要类型的解决方案: 链下解决方案和分片[19–23]. 前者是利用区块链的特性, 提出不同应用场景下可行的链下解决方案. 然而, 这样的解决方案本质上超出了共识算法的控制范围, 且其安全性不受到共识算法的保护. 分片技术源于分布式数据库的思想, 它通过牺牲部分一致性来提升可扩展性. 因此, 这两种方案也都没有完全突破性能、安全性和去中心化的三角.

2 模型与问题定义

在本节中, 首先对系统模型进行描述, 然后对要解决的问题进行定义.

2.1 模型

(1) 系统模型: 本文假设 hash 函数作为随机预言机 (oracle), 任何节点都可以进行 PoW 操作, 并且这个过程在单位时间内的所有消耗 (例如电力消耗、设备折旧、时间成本等) 对于任何节点都是均等的, 任何节点都可以用同样的资金购买获得同等质量的“PoW 计算服务”. 本文的系统具有标准密码学假设 (例如, 公钥签名、集体签名等). 任何节点都可以获得正确且合法的创世区块. 系统中的任何节点都有一个固定的身份: 消费者 (或称消费节点) 或候选者 (或称候选节点). 消费节点产生交易并提交给候选节点, leader 选举将在候选节点中选出一个当前轮的 leader (如果没有分叉). 然后 leader 节点打包并广播合法区块. 此外, 所有节点也根据属性 (诚实和恶意) 分为诚实节点和恶意节点.

(2) 网络模型: 网络中共有N个节点 (n个候选和m个消费节点, $N=n+m$). 所有诚实节点形成了一个连接良好的同步点对点 (p2p) 覆盖网络. 当一个诚实节点广播或传输消息时, 任何其他诚实节点接收此消息的延迟存在一个常数上限, 记为Δ. 且所有消息都通过 Gossip 协议在诚实节点之间传输.

(3) 威胁模型: 协议容忍所有恶意节点的计算能力不到全网的1/3. 恶意节点的行为可以任意地偏离本文的协议. 此外, 恶意节点可以破坏任意的诚实候选节点, 但它们不能破坏消费节点. 然而, 恶意节点可以创建任意数量的恶意消费节点 (例如, 通过女巫攻击). 此外, 他们不能在多项式时间内破解本文的标准密码学假设.

(4) 消费节点偏好模型: 消费节点对于候选节点的选择都有一定的偏好 (这是其他区块链协议没有考虑的). 并记CP_i^j为消费节点$i\in[m]$对候选节点$j\in[n]$的偏好程度 (其中, 偏好程度表示i希望将他的交易数据提交给j的程度, 例如: $n=10$, x是i的最偏好的候选节点, y是i的第二顺位偏好的候选节点, 那么$CP_i^x=10, CP_i^y=9$), 则$CP_i^j>CP_i^k$表示i偏好j多于k. 并记LCP_i为i根据他的

偏好对所有候选节点进行排序的列表.

2.2 问题定义

在第 2.1 节的模型下, 本文的协议方案需要实现高吞吐量、低交易延迟、一定的可扩展性、低候选阈值(利于去中心化)、简单性、有效性和安全性, 具体说明如下.

(1) 有效性和安全性: 诚实消费节点的交易最终会得到 Achain 区块链的确认; Achain 可以抵御双花攻击(又称 51% 攻击)、Sybil 攻击以及 single point of failure (SPOF) 类攻击.

(2) 吞吐量: 当网络的规模 (即节点数)、带宽等系统参数确定后, 将单位时间内系统确认的平均交易数定义为系统的吞吐量. Achain 的目标则需要最大限度地提高系统吞吐量.

(3) 交易延迟: 当网络的规模、带宽等系统参数确定后, 交易延迟定义为从交易产生 (即消费节点发起交易) 起直到交易最终在区块链上被确认所经过的时间. Achain 的目标则需要尽可能地减少交易延迟.

(4) 可扩展性: Achain 目标需要解决 PoW 型共识中安全性和可扩展性之间的冲突和耦合, 并保证在不牺牲安全性的情况下尽可能提高可扩展性. 此外, 方案应该能够嵌入其他分片协议和第 2 层协议 (例如闪电网络[24]).

(5) 候选节点门槛和去中心化: 在 Achain 中, 候选节点承担验证者的义务, 这里的候选节点的门槛意味着加入共识机制的条件 (例如, 加入许可的区块链需要所有其他成员的批准). Achain 需要尽可能降低此门槛以实现更高度的去中心化, 同时确保不牺牲安全性.

(6) 消费节点偏好: 令 $\sum_{i\in[m]} CP_i^j$ 为候选节点 j 的受欢迎程度, 那么 Achain 协议需要满足: "j 节点成为 leader 节点"的概率与 j 的受欢迎程度呈现正相关关系.

3 Achain 方案设计

本节详细介绍 Achain 协议方案的设计内容, 图 1 展示了 Achain 的分层系统架构. 在数据层, Achain 的区块链的数据结构和传统的 Bitcoin 类似, 但原本的交易信息被 vote 信息替代. Achain 区块链由一个个 Achain 区块构成, Achain 区块则包括 vote 信息、候选节点 deposit 信息、leader 数字签名等, 其中 vote 信息还包括: unspent transaction outputs (UTXO) 交易信息、消费节点 PoW 证明、消费节点数字签名、前块哈希指针等. 在网络层, Achain 采用了 Gossip 传输协议, 保证消息在分布式网络中的可靠广播. 在共识和激励层, PoM 机制作为 Achain 的核心共识算法被提出, 并辅以基于博弈论的激励策略以及冷热候选节点机制完成了共识激励的任务.

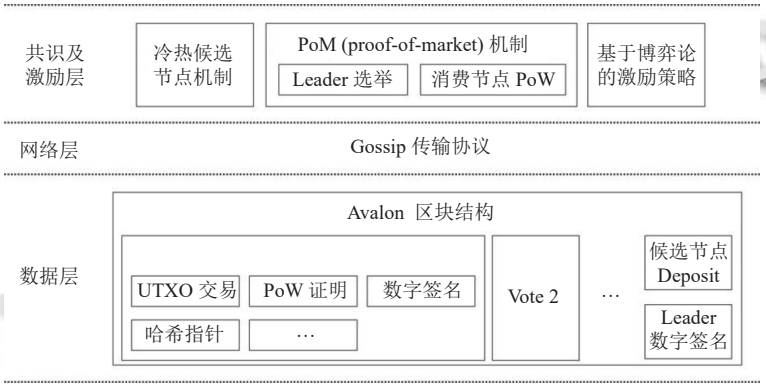

图 1 Achain 系统架构图

各层级模块之间的关系如下, 系统中的所有候选节点运行 Achain 的 leader 选举模块; 同时消费节点执行消费节点 PoW 模块, 消费节点 PoW 需要输入 UTXO 交易信息, 其可输出合法的 vote 信息, 消费节点将合法的 vote 信息提交给相应的候选节点 (此过程中, 博弈论激励模块和冷热候选节点机制也在同时起作用, 激励节点执行完成上述步骤); leader 选举结束后成为 leader 的节点, 将收集到的 vote 信息整合为合法的 Achain 区块数据, 并调用 Gossip 传输协议广播此区块. 至此, 一个新的合法 Achain 区块在系统中被各节点达成共识.

3.1 市场证明 (PoM) 机制

本节将介绍 PoM 共识机制, 它包括 vote 机制、leader 选举和区块广播. 消费节点的 PoW 构成了 vote

机制. 与经典的 leader 选举不同, 这里采用了“一票多投 (one voter for multiple investments, OVMI)”机制, 其消除了 PoW 机制对于系统吞吐量的限制并简化了 Achain 协议. 消费节点使用他们提交的交易数据作为 vote 来选择他们最喜欢的候选节点作为 leader 节点, 而消费节点 PoW 产生的成本可以过滤掉恶意节点.

3.1.1 候选节点的 leader 选举

图 2 展示了 Achain 系统中的选举过程, 具体内容如下.

1) 首先, 在一轮 leader 选举中, 所有参加选举的候选节点“冻结”其本地账本中的一定数量的数字资产 S_d 作为“押金 (deposit)”, 然后将此信息附上其的数字签名并广播. 收到此 deposit 消息的消费节点可以根据 S_d 的数值及其他因素选择他们支持的候选节点并将本地的交易数据提交给他 (或他们). 注意, S_d 是暂时从候选节点的账本中冻结的, 除非 leader 竞选失败, 否则候选节点不能使用、转移此 deposit. 如果候选节点成为 leader, 那么 S_d 将被分发给此前提交过交易信息给他的消费节点, 具体的分发金额数目则是与消费节点提交的交易的金额成正比.

2) 候选节点可以在前一轮 leader 节点广播区块后立即进行下一轮 leader 选举, 并将其 deposit 的 S_d 值广播到网络中. 当候选节点 i 本轮收集的总交易额 ta_i 达到某个阈值 (该阈值与前任 leader 节点收集的总交易额有关) 后, 他将立即验证所有收集到的交易. 如果没有其他候选节点早于 i 节点达到阈值 (即, 在这一轮中 i 没有收到任何其他节点广播的新块), 那么 i 将立即打包并广播所有合法交易. 收到区块的候选节点知道自己在本轮选举中失败, 便可立即加入下一轮选举.

在 leader 选举中隐藏了很多细节, 这里, 首先描述候选节点需要收集的交易金额阈值, 记其为 TAT. 如果前一个 leader 节点 l 收集的交易金额为 ta_l (即, l 收集到的 vote 中包含的金额总和为 ta_l), 则下一位 leader 的交易金额至少为 $TAT = \lambda ta_l$. 系数 λ 在某种程度上相当于 Bitcoin 系统中的挖矿难度, λ 受此期间市场的交易量和趋势控制, 例如, 前任领先者的交易额为 $ta_l = 100$, 当前市场的需求在上升阶段, 可设置 $\lambda = 1.07$, 那么下一个 leader 收集的交易额一定大于 107. λ 的主要作用是控制区块的间隙. 其他细节内容将延后至第 3.1.2 节和第 3.2 节中.

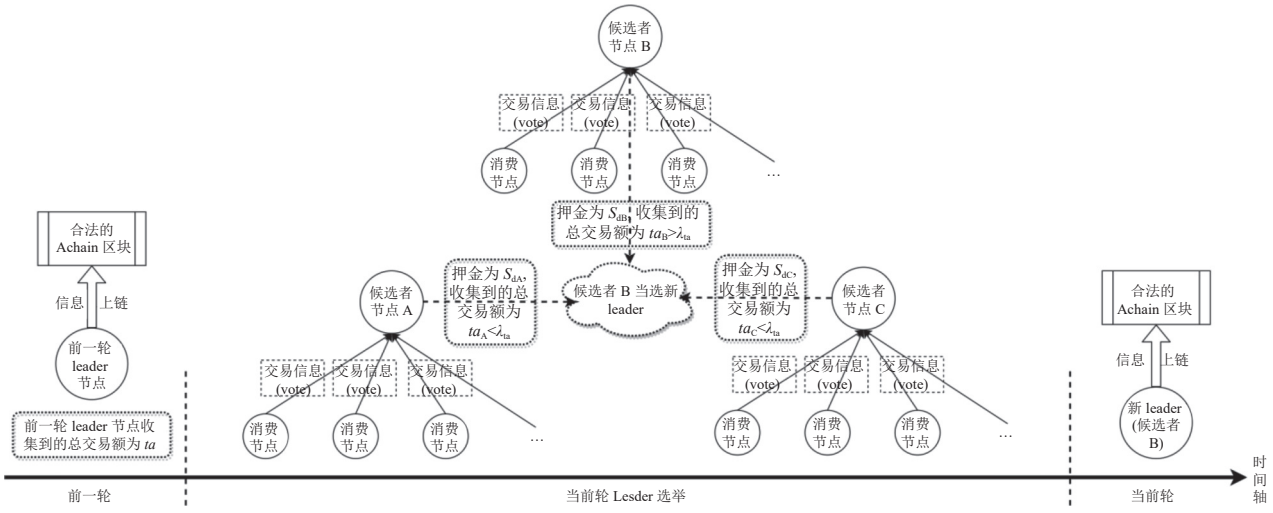

图 2 Achain 的 leader 选举过程示意图

3.1.2 消费节点 PoW 方案

当候选节点在执行 leader 选举时, 消费节点则需要通过消费节点 PoW 输出相应的 vote 数据, 并在 leader 选举中提交给特定的候选节点, 以此保证 Achain 系统中 leader 选举过程的正常执行. 具体内容如下.

(1) 消费节点提交给候选节点的消息结构为: 消费节点的数字签名、交易信息、最新区块的哈希信息 (用于防止节点预先执行消费节点 PoW)、支持的候选数量和随机数 x. 这种类型的消息称为消费节点的 vote, 如图 3 所示.

(2) 消费节点必须对其 vote 进行 PoW 操作, 具体地, 调整随机数 x, 使整个消费节点的 vote 的哈希值、

交易金额等数据满足当前的消费节点难度条件 (此过程类似于 Bitcoin 的“挖矿”出块过程). 只有在规定的消费节点难度下完成 PoW 的 vote 才是合法的.

(3) 一票多投 (OVMI): Achain 系统允许消费节点在一轮选举中将不同的 vote 提交给多位候选节点, 只要他们提交的 vote 是合法的.

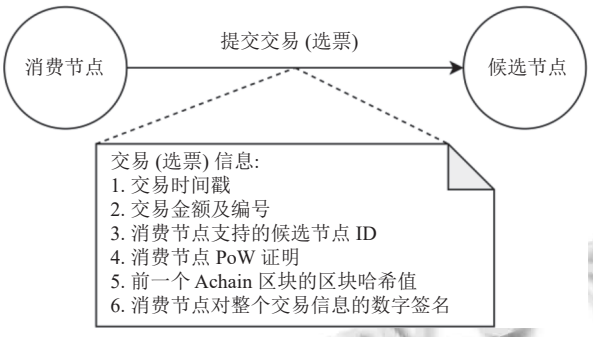

图 3 消费节点的合法 vote 结构图

这里解释一下消费节点 PoW 难度, 记其为d_c. 类似于 Bitcoin 的挖矿难度, d_c就是消费节点进行 PoW 操作的难度. d_c与当前所有消费节点的总哈希能力相关, 且与消费节点提交的交易金额相关. 但是, 不同于 Bitcoin 挖矿难度的定义, 这里从一个新的角度 (经济学角度) 在定义 1 中对消费节点难度d_c和消费节点 PoW、交易金额等的关系进行定义, 具体如下.

定义 1. 消费节点 PoW 难度, 记为d_c. 基于第 2.1 节中的系统模型假设, 若节点花费了S_{PoW}额度的资金用于消费节点 PoW (主要用于例如: 挖矿的电力、设备租借、人力成本等), 且当前消费节点难度为d_c, 那么他可以合法化的交易金额的期望值为$d_c S_{\text{PoW}}$.

例如, 如果一笔交易的金额是 10 单位代币, 并且$d_c = 100$, 那么消费节点需要花费 0.1 单位代币来完成消费节点 PoW 所产生的成本才能使该交易合法.

与 PoW 型区块链一样, Achain 中消费节点的算力也会不断变化, 因此d_c需要根据网络的总算力做出相应的变化, 以保持计算时间的稳定. 此外, 消费节点 PoW 还需要保证消费节点 PoW 的成本线性, 即当一笔交易tx被拆分为两部分tx_1和tx_2时, tx的消费节点 PoW 的成本期望值应该等于完成tx_1和tx_2的 PoW 的期望成本之和. 并且这很容易实现: 假设在一次哈希函数调用中, 完成 1 单位代币交易的消费节点 PoW 的概率为p, 那么在一次哈希函数调用中, 完成s个单位代币交易的消费节点 PoW 的概率应为p/s.

实际上, PoM 机制将挖矿与 leader 节点选举脱钩, 避免了算力的中心化和恶性的挖矿竞争.

3.2 激励机制

消费节点 PoM 不足以使 Achain 系统是激励相容的, 因此需要引入配套的激励机制. 运用博弈论是设置合理的激励机制的关键, 本节介绍 Achain 协议的整体激励机制.

除了前面提到的交易金额的阈值TAT和消费节点 PoW 难度d_c, 如图 4 所示, Achain 还有以下两个主要的系统参数.

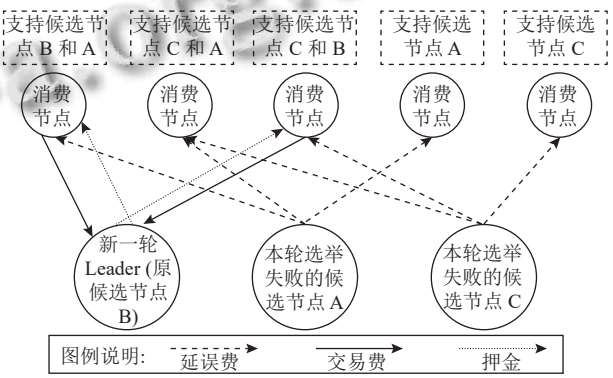

图 4 Achain 的激励机制示意图

(1) 交易费率k_t: 当 leader 成功上链金额为S的交易时, 消费节点应该给 leader 一定比例的交易金额作为“交易费”——$k_t S$, 在 Bitcoin 中也有类似的机制.

(2) 延误费率k_d: 如果候选节点在选举中失败, 他应该向在本轮选举中支持他的消费节点支付$k_d S$作为交易的延误费, 这里的S为消费节点本轮 leader 选举中提交给此失败候选节点的交易总额. 延误费是对选举失败造成的交易延迟的一种“补偿”, 其可以防止一些恶意攻击, 这在后面会进行详细分析.

(3) 这里的k_t和k_d应满足以下关系 (基于博弈论策略):

$$(n-1)k_d + \frac{S_0}{f(S_0)} < k_t < \frac{n(n+1)}{n-1}k_d + \frac{S_0}{f(S_0)}$$

以及:

$$k_d < \frac{1}{d_c}$$

其中, n表示系统内节点数; S_0表示 deposit 数额; $f(S_0)$表示当一个候选节点广播S_0数额的 deposit 时, 可以获得的消费节点提交的 vote 数额的数学期望; d_c表示消费节点 PoW 难度.

交易费和延误费按照以下规则支付.

(1) Achain 协议要求候选节点在决定参加选举时向全网广播带有签名的 deposit 信息. 如果候选节点获胜, 则立即将收集到的交易打包, 并按交易金额的比例向每个支持此 leader 的消费节点支付相应的 deposit, 否则此交易集被视为非法的.

(2) 由于全网对失败候选节点收集的交易并不会达成共识, Achain 协议采用“索赔”机制来分配延误费. 合法 vote 本身可以被视为一种“支票”, 当此“支票”在未来被用于支付时, 相应的金额将从相应的失败候选帐户中自动扣除.

(3) 为防止候选节点资金短缺而无法支付延误费, Achain 协议规定候选节点在每次选举中必须冻结一定数额的“预付延误费”. 如果候选节点获胜, 则解冻, 否则等待几轮后自动解冻. 但只要候选节点处于选举状态, 那么就必须保持一定数额的“预付延误费”.

为了让延误费对 Achain 有正向的激励作用, 恶意节点不能从延误费中获利, 这就要求节点在消费节点 PoW 上的成本 (投资) 的数学期望大于他可以获得的延误费, 即, $k_d < 1/d_c$.

3.3 冷热候选节点机制

在前面对 Achain 的描述中, 所有候选节点都可以同时参与 leader 选举. 但是, 这种方法分散了消费节点的计算能力, 并可能削弱 Achain 的安全性. 因此, Achain 协议引入热冷候选节点机制.

(1) Achain 系统的运行过程按照时间T进行分割, 并分为若干个长度相等的周期.

(2) 在每个周期T内, Achain 系统从所有候选节点中随机选择 3 个特殊候选节点 (通过 Algorand[11] 的选举方案, 一种基于 VRF 的 leader 选举方案), 被称为“热候选节点”, 其他候选节点则被称为“冷候选节点”.

(3) 消费节点只能向热候选节点提交合法交易, 除非消费节点判断热候选节点是恶意的或离线的.

(4) 当消费节点判断热门候选节点是恶意的或离线时, 消费节点可以提交合法 vote 给冷候选节点.

这里解释一下冷热候选方案的一些细节. 首先, 每轮只选出 3 个热门候选, 以确保所有消费节点 PoW 算力都集中在这 3 个候选上. 因此, 只要恶意节点的算力不超过全网算力 (所有消费节点算力) 的 1/3, 他就无法进行双花攻击. 随机选择热门候选节点的过程在 Algorand[11] 的委员会选举方案中有详细说明, 该方案使用全局不可伪造且可验证的随机数来防止作弊. 关于消费节点发现候选离线的方法: 由于消费节点 PoW 的完成时间满足指数分布, 随着时间的增加, 热候选节点出块的概率会不断接近 1. 如果等待足够长的时间还没有热候选节点发布新块, 则消费节点可以确定热候选节点均已离线.

3.4 Gossip 传输协议

Achain 协议在网络传输层采用的 Gossip 协议是一种典型的分布式消息传输协议, 其底层一般采用 UDP 协议, 其可以同时实现低负载, 高可靠和可扩展性等性能, 且简单而易于实现. Gossip 协议内容大致如下: 首先消息传输由一个种子节点发起, 此种子节点先随机挑选出若干个邻居节点, 并将需要同步的消息发送给它们. 收到消息的节点则成为新的种子节点并重复上述过程, 直到网络中的所有节点均接收到此消息. Gossip 协议具有最终一致性, 因此, 在理论上, 总会存在一个时间节点, 系统内所有节点在此节点之后均收到了需要同步的消息.

3.5 分叉

本节首先介绍 Achain 区块链的链接规则: 一个区块内的所有交易必须指向同一个父区块. 因此, 当分叉发生时, 所有消费节点都需要选择合适的父区块, 而候选节点也必须选择合适的消费节点 (以确保其区块内的交易指向同一个父区块, 否则区块将被视为非法的).

当系统中产生分叉, 并且不同的网络分区产生不同的共识时, Achain 使用与 Bitcoin 相同的解决方案——选择最长的链. 区块间隔的缩短可能会导致分叉的增加. 并且由于 PoM 的机制, 分叉的概率在更大程度上取决于市场情况. 例如, 如果有一个“超级候选节点”, 具有很强的吸引 vote 的能力 (通过优惠策略、优质服务等), 那么分叉的概率非常低, 因为其他候选节点很难与他几乎同时发布合法块. 在最坏的期间下, 如果有多个相同受欢迎的候选节点, 那么分叉的概率会增加.

尽管如此, 与 Bitcoin 不同的是, 在这种情况下, Achain 仍然可以通过调整参数来影响分叉率. 例如, 可以调整d_c、TAT或限制 OVMI (这使得消费节点只选择单一的候选节点, 从而降低分叉率).

3.6 Achain 伪代码

本节在算法 1 中使用伪代码来阐明 Achain 的运行过程.

算法1. Achain主算法

输入: 交易金额阈值TAT、消费节点PoW难度d_c、交易费率k_t、延误费率k_d

输出: 无

(1) 对于任意候选节点j

步骤1. 开始新一轮的leader选举, j广播自己的deposit信息S_d; j收集消费节点的交易并验证其合法性 (例如: 消费节点PoW、数字签名、UTXO记录等); 将所有合法交易添加到本轮j收集的交易集TX中. 执行步骤2.

步骤2. 若$\sum_{tx\in TX} S_{tx}>TAT$且没有任何候选节点广播一个新的合法区块, 其中$S_{tx}$代表$tx$的金额, 则执行步骤3, 反之执行步骤4.

步骤3. j立即签署、打包和广播所有交易; j向消费节点支付相应deposit, 即S_d, 这些交易包含在TX中, 并向消费节点收取交易税k_t. 执行步骤5.

步骤4. 若已有其他候选节点广播新的合法块, 则j向本轮中所有提交vote给他的消费节点支付延误费k_d. 执行步骤5.

步骤5. 若j继续参加leader节点选举, 则进入下一轮选举并执行步骤1, 反之退出.

(2)对于任意消费节点i

步骤1. 若接收到新的合法区块b, i停止正在进行的操作并执行以下操作: i根据最新的区块链更新自己的未提交交易列表UTX_i; i收集候选节点的deposit信息并调整LCP_i(根据每个候选节点的S_d和i的偏好). 进入步骤2.

步骤2. 若从高到低遍历所有的候选节点$j\in LCP_i$且j是热候选节点, 则i从UTX_i中选择最早的交易tx; i执行$CPoW$函数 (详见算法2)得到合法交易$ltx=CPoW(i,j,b,tx,d_c)$. i将ltx提交给j. 同时, i监听网络, 是否收到新的合法区块, 若收到则进入步骤1, 反之继续执行步骤2.

算法 1 中的 $CPoW$ 函数 (即消费节点 PoW 操作)的内容如算法 2 中所示.

算法2. 函数$CPoW$ (消费节点PoW)

输入: 消费节点i, 候选节点j, 前一个区块b, 交易内容tx, 消费节点PoW难度d_c

输出: 合法交易ltx

步骤1. 产生随机数x; 计算$H=HASH(i,j,HASH(b),tx,x)$, 其中$HASH(\cdot)$表示散列函数; 如果H满足金额为S_{tx}的交易对应的消费节点PoW难度d_c, 则执行步骤2, 反之执行步骤1.

步骤2. 函数返回$ltx=sig_i(<i,j,HASH(b),tx,x>)$, 其中$sig_i(\cdot)$表示$i$的数字签名.

3.7 优化方案 FastAchain

为了进一步优化 Achain 的性能, 我们提出了 FastAchain, 其提供一种基于默克尔树的新型链结构并采用账户模式记录交易信息, 帮助节点节省存储空间, 提升系统的可扩展性和去中心化程度. 详细内容如下.

Achain 节点存储的块信息中包含了自创世块以来的所有交易记录, 这是因为 UTXO 交易结构需要对每笔交易进行溯源. Achain 节点会随着系统的运行而不断地存储更多的交易, 这会造成区块链可扩展性的瓶颈, 并且高昂的存储成本也必然会导致中心化的加剧. 为此, FastAchain 允许 Achain 节点对稳定的 Achian 块进行“快照”处理, 具体地, Achain 节点只保存稳定的 Achian 块中的块头、所有交易的哈希信息、节点签名、交易金额这些主要数据, 而并不存储 UTXO 交易的主体内容. 并且采用账户 (account) 模式记录每个消费节点的当前余额状态. 其中, 所有交易的哈希信息采用默克尔树 (Merkle trees) 结构进行存储, 如图 5 所示. FastAchain 中交易的默克尔树结构主要分为 3 层: 根哈希、节点哈希和交易哈希, 根哈希是此 Achain 块的所有交易的总哈希, 节点哈希是此 Achain 块中某个消费节点提交的所有交易的哈希, 每个交易哈希则对应着具体的某个 UTXO 交易.

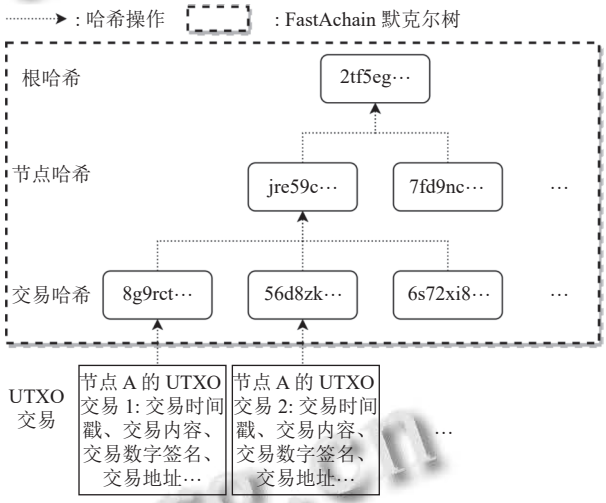

图 5 FastAchain 中交易的默克尔树结构示意图

采用 FastAchain 方案, 节点则无需存储绝大多数 Achain 块中的具体交易信息, 只需存储它们的默克尔树并维护一个消费节点的 account 列表即可. 在对热候选者节点广播的新块中的交易进行验证时也仅需验证其余额的合法性, 即, 此节点是否有足够的余额支付此笔交易.

FastAchain 方案使得节点只需花费远小于 Achain 方案的存储空间就可以达到同样的共识效率, 由于默克尔树的存储成本极低且固定, 因此, FastAchain 的链上数据容量增长是非常缓慢的, 且受网络规模扩大交易数量增多等因素的影响较小. 这进一步提升了 Achain 协议的可扩展性. 此外, 随着节点存储成本的减少, 系统的准入门槛也会降低, 这也有助于提升 Achain 协议的去中心化程度.

4 Achain 有效性及安全性分析

4.1 有效性分析

Achain 的有效性分析在本质上与 Bitcoin 是一样的, 因为 PoM 本质上也是一种 PoW 机制. 换句话说, 文献 [25] 中对于 Bitcoin 主干协议的分析中的许多属性, 例如公共前缀 (common prefix) 和链质量 (chain quality), 都可以“移植”到 Achain. 下面我们尝试通过比较 Bitcoin 和 Achain 的一个变体来说明其有效性.

在前面的描述中, Achain 的每一个消费节点似乎都是一个矿工, 他们需要不断地“挖矿”来使自己的交易合法化以提交给候选节点. 考虑另一种类似的情况 (即 Achain 的变体): 消费节点不是“挖矿”的实际执行者, “挖矿”过程是交给候选节点的 (例如: 消费节点不具备挖矿的硬件条件, 但是候选节点具有强大的计算能力). 消费节点仍然需要支付挖矿的消耗和成本, 他们可以自己选择委托哪个候选节点进行挖矿. 在这种情况下, Achain 和 Bitcoin 已经非常相似, 仅有的区别是以下两点: 挖矿成本由不同方承担 (在 Bitcoin 中, 由矿池承担; 在 Achain 中, 由消费节点承担); 挖矿工作是离散的, 但总工作量保持不变 (在 Bitcoin 中, 挖矿工作是一个整体; 在 Achain 中, 挖矿工作根据交易离散化).

这里一个可能的疑问是: Achain 挖矿的获胜条件看起来和 Bitcoin 不同. 但其实它们本质上是一样的: 因为 Achain 挖矿的获胜条件是达到一定交易金额, 而 Achain 的挖矿难度是成正比与金额门槛的. 因此, 两者的综合效果与 Bitcoin 的挖矿难度相同. Achain 的变体和 Bitcoin 之间的差异不影响在 Bitcoin 主干协议[25] 中获得的关于安全性和有效性的结论. 并且对于 Achain 变体的分析也适用于原始 Achain. 因此, Bitcoin 的有效性和安全性结论同样适用于 Achain.

4.2 安全性分析

本节主要讨论 Achain 在主流区块链攻击下的安全性.

(1) 双花攻击 (51% Attack): 双花攻击是指攻击者使用相同的 UTXO 在不同的交易中花费. 当攻击者拥有全网 50% 以上的算力时, 他可以创建一个高度大于原链的新链来回滚旧链上的交易 (即, 创建一个分叉), 从而删除之前已被确认的交易, 达到双花的目的.

根据第 4.1 节的有效性分析, 当恶意节点控制的算力不超过总算力的 50% 时, Achain 区块链与 Bitcoin 区块链相同, 确认上链的区块是不可篡改的. 唯一可能存在的问题是, Achain 的分叉率可能会高于 Bitcoin, 这需要消费节点等待更多的区块来确认他的交易. 幸运的是, 与 Bitcoin 相比, Achain 有更高的自由度通过设置系统参数 (例如: TAT 和 d_c) 来抑制分叉率 (这将在实验部分详细讨论).

(2) 女巫攻击 (Sybil attack): Sybil 攻击是指具有多个身份的节点通过控制系统内的大部分其他节点来削弱冗余备份的作用. 在没有身份验证的 p2p 网络中, Sybil 攻击很容易使数据备份失效并破坏共识. 因此, 大多数共识算法需要对加入系统的节点进行身份验证, 以确保它们不是 Sybil 节点.

Achain 与 Bitcoin 一样, 允许节点自由进出系统, 这使其暴露在女巫攻击的威胁之下. 然而, Achain 也有像 Bitcoin 一样防止 Sybil 攻击的机制. 当一个恶意节点打算制作多个恶意候选节点副本时, 他将面临延迟费的“惩罚”; 当一个恶意节点打算制作多个恶意消费节点副本时, 他将面临消费节点 PoW 的成本和消耗. Achain 通过合理的系统参数设置使得这两种作恶的收益在数学期望上都是小于零的. 因此, Achain 具有良好的抗 Sybil 攻击的能力.

(3) SPOF 攻击: SPOF 是指如果系统中的某个特定节点发生故障 (例如, 遭受 DDoS 攻击), 系统将无法继续运行. 在分布式共识算法中, 如果 leader 选举是有规律且可预测的, 那么攻击者就可以连续不断地破坏这些 leader 节点, 从而导致整个系统完全瘫痪.

然而, Achain 的领导者选举是随机的. 即使攻击者使用 SPOF 瘫痪了几个热门候选节点, 其他候选节点仍然可以正常运行并产生区块, 并且它们成为 leader 的顺序是不可预测的.

5 Achain 原型实验及结果分析

本节将评估 Achain 的性能, 包括: 交易的吞吐量、交易的确认延迟、交易的回滚率、链的收敛性和去中心化 (详细解释见表 1). 此外, 两个重要的变量是领导人选举的阈值 TAT 和消费节点 PoW 挖矿难度 d_c. 注意, 为了便于理解, 这里重新定义 d_c 为: 消费节点在一单位时间内 (1 s) 可以通过消费节点 PoW 合法化的一单位金额的交易的次数, 因此, d_c 越大, 节点的挖矿效率越高 (这与定义 1 不同, 但并不影响性能分析, 此设置只是为了方便试验参数的设置). 此外, 原型实验指定 TAT 和 d_c 的缺省值是 80 000 和 6.

表 1 Achain 实验参数及其说明表

参数	解释说明
交易吞吐量 (TT)	Achain系统每秒确认的平均交易数
交易确认延迟 (TCD)	交易自出现到被Achain系统上链确认所经历的平均时长
交易的回滚率 (TRR)	在若干区块后, 交易因发送分叉而被回滚的概率
区块链的收敛性 (CC)	发生分叉时Achain区块链需要等待收敛的块数
去中心化	每个候选节点成功生产一个区块的概率

5.1 Achain 原型实验设置

本实验通过 omnetpp 在模拟的 p2p 网络中实现了 Achain 的原型. 为了模拟真实的全局分布式网络, 节点之间所有连接的带宽被限制为 30 Mb/s, 并在所有通信链路上施加 100 ms 的延迟 (这一设置类似于之前协议的实验[10,19]). 并且为了模拟消费节点的交易, 本实验的交易池收集了 Bitcoin 区块链中所有真实交易的集合, 其来自高度从 500 000 到 505 000 的区块, 且每笔交易的容量大小也根据采集到的真实数据进行模拟 (在 150 KB 到 250 KB 之间). 本实验原型共模拟了 1 003 个消费节点, 每轮的热候选者节点也将随机地从这 1 003 个节点中产生. 每个消费节点每秒产生 5 个原始交易 (为了平衡实验的性能, 网络规模被控制为 1 003 个节点, 但这已经可以接近很多了经典的区块链原型, 例如 Bitcoin-NG、ByzCoin 等).

5.2 交易吞吐量 (TT)

本节研究了 TAT 和 d_c 对 Achain 系统吞吐量的影响. 具体实验结果如图 6 和图 7 所示. TAT 和 d_c 的增加都对 Achain 的吞吐量有积极的调节作用, 但并不是很明显. Achain 在大多数参数设置下可以达到 4 000 TPS 以上, 这与 Visa 的平均吞吐量相当, 在相同条件下远高于 ByzCoin (几乎是 ByzCoin 吞吐量的 4 倍).

5.3 交易确认延迟 (TCD)

Achain 的平均 TCD 实验结果如图 8 和图 9 所示. 注意这里的 TCD 是基于等待 6 个区块确认交易的时间, 即, 使用与 Bitcoin 相同的标准交易确认模型. TAT 与 TCD 呈明显正相关性, 而 d_c 对 TCD 几乎没有影响 (实际上是弱负相关). 其潜在的原因是阈值的上升需要更多的交易, 然而消费节点产生的交易频率是固定的, 因此需要等待更长的时间. 当 $d_c \geq 3$ 时, 消费节点基本可以向所有 3 个热门候选节点提交交易, 所以继续增加 d_c 只能带来 TCD 的小幅提升. 在大多数情况下, Achain 的 TCD 不会超过 40 s, 在最好的情况下, 交易可以在 10 s 内得到确认, 且交易不会被回滚.

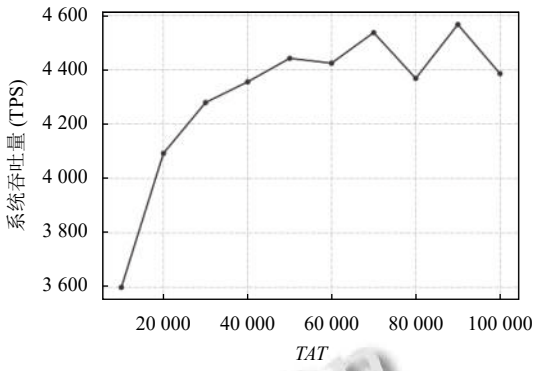

图 6 参数 TAT 与 Achain 系统的吞吐量之间的关系实验图

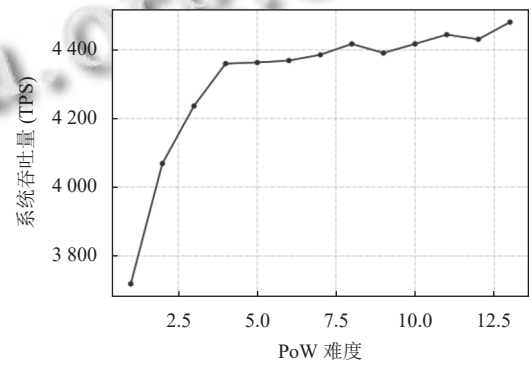

图 7 参数 d_c 与 Achain 系统的吞吐量之间的关系实验图

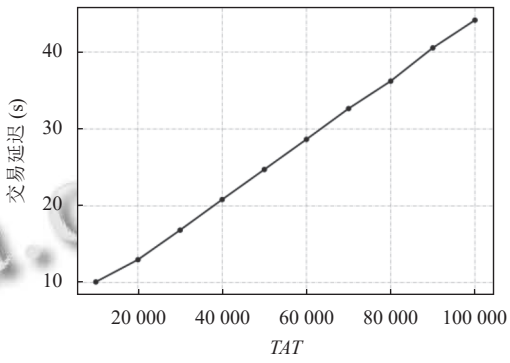

图 8 TAT 与交易确认延迟的关系实验图

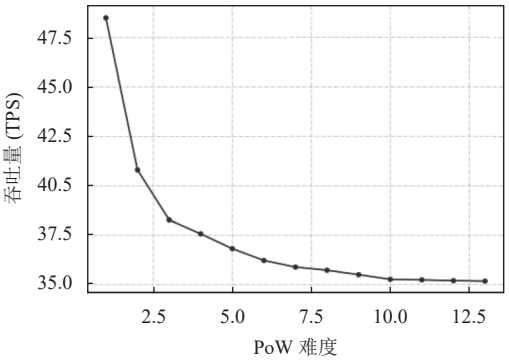

图 9 d_c 与交易确认延迟的关系实验图

总的来说, Achain 的 TCD 远远超过了 Bitcoin 区块链的水平, 与目前主流的区块链协议相当, 这说明 Achain 在达到了高实用性的同时, 其延迟也是完全可以接受的.

5.4 交易回滚率 (TRR)

回滚率是衡量区块链协议的重要指标, 直接关系到系统的安全性. PoM 本质上是一种 PoW 型共识, 因此 Achain 具有 PoW 型区块链的收敛性, 这使得提交的交易在被确认后是不可变的. 表 2 和表 3 为相关实验结果, 其中数据均取自高度超 100 的区块链. TAT 和 d_c 的增加可以有效抑制 TRR. 当等待超过 3 个区块后再确认交易, Achain 系统中就不存在回滚现象. Achain 和 Bitcoin 一样保守地等待 6 个区块来确认交易, 因此它的安全性非常高.

表 2 TAT 与交易回滚率的关系实验表

TAT	快速确认 (%)	等待3个块 (%)	TAT	快速确认 (%)	等待3个块 (%)
10000	26.50	0	60000	7.71	0
20000	16.94	0	70000	6.95	0
30000	12.73	0	80000	5.98	0
40000	10.51	0	90000	5.99	0
50000	8.80	0	100000	4.99	0

5.5 区块链的收敛性 (CC)

Achain 链的收敛实验通过记录分叉的数量和高度来判断区块链的安全性. 实验结果如表 4 和表 5 所示. 一般情况下, 大多数分叉的高度为 1, 只有少数分叉达到高度 2. 增加TAT可以有效抑制分叉. 比较表 3 和表 5 可以发现, 合理地增加d_c可以抑制 TRR 且不影响分叉率. 这是因为d_c的增加允许消费节点将相同的交易提交给更多的候选节点, 即使有回滚, 交易也可以被其他候选节点的区块确认.

表 3 d_c与交易回滚率的关系实验表

d_c	快速确认 (%)	等待3个块 (%)	d_c	快速确认 (%)	等待3个块 (%)
1	16.00	0	6	5.98	0
2	10.80	0	7	6.06	0
3	8.33	0	8	5.41	0
4	7.29	0	9	5.29	0
5	6.92	0	10	5.23	0

表 4 TAT 与分叉数量和高度的关系实验表

TAT	高度1的分叉	高度2的分叉	TAT	高度1的分叉	高度2的分叉
10000	269	1	60000	49	0
20000	154	1	70000	49	1
30000	107	1	80000	35	0
40000	84	0	90000	40	0
50000	67	1	100000	31	1

表 5 d_c与分叉数量和高度的关系实验表

d_c	高度1的分叉	高度2的分叉	d_c	高度1的分叉	高度2的分叉
1	31	1	6	35	0
2	31	0	7	35	0
3	33	0	8	35	1
4	38	0	9	33	1
5	37	0	10	35	0

5.6 去中心化

去中心化实验检验了 Achain 的公平性和安全性. 如果区块间隔的过度缩小会使得节点每轮开始 PoW 操作的时间不同, 那么系统的安全性将受到极大威胁. 实验结果如表 6 和表 7 所示, 其中所有实验数据均至少稳定运行 3 次获得, 结果表明 Achain 在不同的TAT和d_c设置下保持良好的去中心化. 热门候选人的胜率基本维持在 25%–40% 的区间内, TAT和d_c的变化并没有带来明显的胜率波动. 在与 Achain 的 TCD (10–40 s) 和带宽 (30 Mb/s) 的同等设置条件下, 传统 PoW 型区块链会有严重的拥塞和中心化 (这也是 PoW 型区块链无法增加出块容量或减少出块间隔的根本原因), 但是 Achain 却可以保证系统的正常运行.

表 6 热候选节点的胜率 (出块率) 与阈值 TAT 的关系表

热候选节点	TAT			
	20000	40000	60000	80000
节点1 (%)	30.20	28.60	29.50	25.60
节点2 (%)	34.00	30.70	31.10	43.30
节点3 (%)	35.80	40.70	39.40	31.10

表 7 热候选节点的胜率 (出块率) 与消费节点 PoW 难度 d_c的关系表

热候选节点	d_c			
	4	6	8	10
节点1 (%)	23.90	25.60	26.40	26.70
节点2 (%)	37.50	43.30	34.10	33.30
节点3 (%)	38.60	31.10	39.50	40.00

6 结论与展望

总结来说, 本文提出了一种基于新型 PoM 共识的区块链协议——Achain, 它综合考虑了效率、公平性、去中心化和节能, 并试图打破经典区块链面临的诸多限制. PoM 本质上是一种新型的 PoW 共识, 但它将“挖矿”操作从区块生产者转移到消费节点上. 再加上合理的激励机制, Achain 使得恶意节点的攻击无利可图. 在理性攻击者的假设下, Achain 具有更好的性能和去中心化性, 并充分考虑了消费节点的意愿. 由于目前的 Achain 只是分布式账本系统, 并不是图灵完备的

(turing completeness), 因此进一步的研究将拓展 PoM 共识机制的适用范围, 研制基于 PoM 的智能合约系统.

致谢

感谢中国科学技术大学苏州高等研究院陈蔚林博士、陈柄任博士对本文 Achain 协议设计及实验的讨论和帮助.

参考文献

1 Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 2008: 21260.
2 Eyal I, Sirer EG. Majority is not enough: Bitcoin mining is vulnerable. Proceedings of the 18th International Conference on Financial Cryptography and Data Security. Christ Church: Springer, 2014. 436–454.
3 Gervais A, Ritzdorf H, Karame GO, *et al*. Tampering with the delivery of blocks and transactions in Bitcoin. Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. Denver: ACM, 2015. 692–705.
4 Heilman E, Kendler A, Zohar A, *et al*. Eclipse attacks on Bitcoin's peer-to-peer network. Proceedings of the 24th USENIX Conference on Security Symposium. Washington: USENIX Association, 2015. 129–144.
5 Karame GO, Androulaki E, Capkun S. Double-spending fast payments in Bitcoin. Proceedings of 2012 ACM Conference on Computer and Communications Security. Raleigh: ACM, 2012. 906–917.
6 Nayak K, Kumar S, Miller A, *et al*. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. Proceedings of 2016 IEEE European Symposium on Security and Privacy. Saarbruecken: IEEE, 2016. 305–320.
7 Eyal I, Gencer AE, Sirer EG, *et al*. Bitcoin-NG: A scalable blockchain protocol. Proceedings of the 13th USENIX Conference on Networked Systems Design and Implementation. Santa Clara: USENIX Association, 2016. 45–59.
8 BTC. https://explorer.btc.com/zh-CN/btc/insights-pools.
9 Castro M, Liskov B. Practical byzantine fault tolerance. Proceedings of the 3rd Symposium on Operating Systems Design and Implementation. New Orleans: USENIX Association, 1999. 173–186.
10 Kokoris-Kogias E, Jovanovic P, Gailly N, *et al*. Enhancing Bitcoin security and performance with strong consistency via collective signing. Proceedings of the 25th USENIX Conference on Security Symposium. Austin: USENIX Association, 2016. 279–296.
11 Gilad Y, Hemo R, Micali S, *et al*. Algorand: Scaling byzantine agreements for cryptocurrencies. Proceedings of the 26th Symposium on Operating Systems Principles. Shanghai: ACM, 2017. 51–68.
12 Wood G. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 2014, 151(2014): 1–32.
13 Crain T, Natoli C, Gramoli V. Red belly: A secure, fair and scalable open blockchain. Proceedings of 2021 IEEE Symposium on Security and Privacy. San Francisco: IEEE, 2021. 466–483.
14 Li CL, Zhang J, Yang XM. Scalable blockchain storage mechanism based on two-layer structure and improved distributed consensus. The Journal of Supercomputing, 2022, 78(4): 4850–4881. [doi: 10.1007/s11227-021-04061-3]
15 Yang J, Jia ZH, Su RG, *et al*. Improved fault-tolerant consensus based on the PBFT algorithm. IEEE Access, 2022, 10: 30274–30283. [doi: 10.1109/ACCESS.2022.3153701]
16 Ongaro D, Ousterhout J. In search of an understandable consensus algorithm. Proceedings of the 2014 USENIX Conference on USENIX Annual Technical Conference. Philadelphia: USENIX Association, 2014. 305–320.
17 Karantias K, Kiayias A, Zindros D. Proof-of-burn. Proceedings of the 24th International Conference on Financial Cryptography and Data Security. Kota Kinabalu: Springer, 2020. 523–540.
18 Yu JS, Kozhaya D, Decouchant J, *et al*. RepuCoin: Your reputation is your power. IEEE Transactions on Computers, 2019, 68(8): 1225–1237. [doi: 10.1109/TC.2019.2900648]
19 Kokoris-Kogias E, Jovanovic P, Gasser L, *et al*. OmniLedger: A secure, scale-out, decentralized ledger via sharding. Proceedings of 2018 IEEE Symposium on Security and Privacy. San Francisco: IEEE, 2018. 583–598.
20 Liu CC, Guo HC, Xu MH, *et al*. Extending on-chain trust to off-chain—Trustworthy blockchain data collection using trusted execution environment (TEE). IEEE Transactions on Computers, 2022. [doi: 10.1109/TC.2022.3148379]
21 Zheng PL, Xu QQ, Luo XP, *et al*. Aeolus: Distributed execution of permissioned blockchain transactions via state sharding. IEEE Transactions on Industrial Informatics, 2022. [doi: 10.1109/TII.2022.3164433]
22 Zamani M, Movahedi M, Raykova M. RapidChain: Scaling blockchain via full sharding. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. Toronto: ACM, 2018. 931–948.
23 Kiayias A, Russell A, David B, *et al*. Ouroboros: A provably secure proof-of-stake blockchain protocol. Proceedings of the 37th Annual International Cryptology Conference on Advances in Cryptology. Santa Barbara: Springer, 2017. 357–388.
24 Poon J, Dryja T. The Bitcoin lightning network: Scalable off-chain instant payments. https://lightning.network/lightning-network-paper.pdf.
25 Garay J, Kiayias A, Leonardos N. The Bitcoin backbone protocol: Analysis and applications. Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology. Sofia: Springer, 2015. 281–310.

(校对责编: 牛欣悦)