软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2023,34(1):33−49 [doi: 10.13328/j.cnki.jos.006421]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

轻量级区块链技术综述*

谢晴晴[1,2], 董 凡[1,2]

[1](江苏大学 计算机科学与通信工程学院, 江苏 镇江 212013)

[2](江苏大学 江苏省工业网络安全技术重点实验室, 江苏 镇江 212013)

通信作者: 谢晴晴, E-mail: xieqq@ujs.edu.cn

摘 要: 传统的区块链技术为了保证交易账本的全网共识和不可篡改性, 要求矿工节点具有强大的计算能力和足够的存储空间, 这就限制了资源受限的设备加入区块链. 近几年, 区块链技术已经拓展到金融经济、医疗健康、物联网、供应链等多个领域, 但是这些应用场景存在大量算力弱、存储容量低的设备, 这给区块链的应用带来了巨大挑战. 为此轻量级的区块链技术应运而生. 从轻量级计算和轻量级存储两方面出发, 总结当前轻量级区块链的研究现状, 对比分析各个方案的优缺点. 最后展望未来轻量级区块链的发展.

关键词: 轻量级区块链; 共识机制; 轻量级计算; 轻量级存储

中图法分类号: TP316

中文引用格式: 谢晴晴, 董凡. 轻量级区块链技术综述. 软件学报, 2023, 34(1): 33–49. http://www.jos.org.cn/1000-9825/6421.htm

英文引用格式: Xie QQ, Dong F. Survey on Lightweight Blockchain Technology. Ruan Jian Xue Bao/Journal of Software, 2023, 34(1): 33–49 (in Chinese). http://www.jos.org.cn/1000-9825/6421.htm

Survey on Lightweight Blockchain Technology

XIE Qing-Qing[1,2], DONG Fan[1,2]

[1](School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China)

[2](Jiangsu Key Laboratory for Industrial Network Security Technology, Jiangsu University, Zhenjiang 212013, China)

Abstract: In order to ensure the network-wide consensus and tamper proof of the transaction ledger, the miner nodes are required to possess strong computing and storage resource in the traditional blockchain technology. It greatly limits the resource-constrained devices to join in the blockchain systems. In recent years, blockchain technology has been expanded in many fields, such as financial economy, health care, Internet of Things, supply chain, etc. However, there is a large number of devices with weak computing power and low storage capacity in these application scenarios, which brings great challenges to the application of blockchain. Therefore, lightweight blockchain technology is emerging. This study summarizes some related works of lightweight blockchain from the two aspects of lightweight computing and storage. Their advantages and disadvantages are compared and analyzed. Finally, the future development of the lightweight blockchain systems is prospected.

Key words: lightweight blockchain; consensus mechanism; lightweight computing; lightweight storage

区块链 (blockchain) 技术是近几年最热门的研究领域之一, 国家已将其列入发展战略, 习近平总书记更是亲自参与了区块链的学习研讨会, 并在会上为区块链的未来发展指明了方向. 当前, 区块链技术已经拓展到金融经济[1]、物联网[2,3]、供应链[4]、医疗健康[5]等多个领域, 区块链技术正在经历着发展的黄金时期.

区块链是结合了 P2P (peer to peer) 网络、智能合约、共识机制、密码学等技术的新型的分布式账本技术, 凭借着去中心化和账本数据不可篡改、公开透明等特性, 区块链的出现为解决传统服务架构下存在的安全和信任问

* 基金项目: 国家自然科学基金青年基金 (62002139, 61902157); 江苏省自然科学基金 (BK20200886); 中国博士后科学基金 (2019M651738, 2019M661753)
收稿时间: 2021-05-19; 修改时间: 2021-06-29; 采用时间: 2021-07-28; jos 在线出版时间: 2021-10-20
CNKI 网络首发时间: 2022-11-15

题提供了新思路. 但是, 传统区块链技术存在的高能耗、低效率等缺点严重阻碍了区块链技术的发展. 因此, 亟需一种轻量级的区块链技术. 本文总结分析了当前轻量级区块链技术的研究现状, 旨在推动区块链技术的发展, 为轻量级区块链技术的研究提供参考.

本文第 1 节对区块链技术进行概述, 指出了传统区块链技术在计算和存储上存在的问题. 第 2 节分别从计算、存储以及兼顾计算和存储 3 个方面对当前轻量级区块链技术进行总结分析, 并指出现有方案的优缺点. 第 3 节总结了物联网场景下典型的轻量级区块链架构. 第 4 节对轻量级区块链技术的未来研究进行了展望. 第 5 节对全文进行了总结.

1 引 言

区块链最初作为比特币[6]的底层技术被社会各界人士广泛关注. 在这之后诞生了诸如以太坊 (Ethereum)[7]、超级账本 (Hyperledger Fabric)[8]等开源区块链平台以及大量基于智能合约技术的去中心化应用 (DApp), 加快了区块链技术与更多领域的融合发展. 去中心化的特性使得区块链以更低的成本在不同利益主体参与的无信任场景中构建出信任基础, 有助于推动社会信用体系的创新发展. 最近几年区块链飞速发展, 人们尝试将其应用于金融经济、智能城市、医疗健康、物联网、供应链等领域. 但是, 能耗高、运行效率低等问题制约着区块链的发展, 在资源受限的场景中部署传统区块链面临巨大挑战.

区块链本质是一个集成了 P2P 网络、智能合约、共识机制、密码学等技术的去中心化的分布式数据库. 其整体架构自上到下可以分为应用层、合约层、激励层、共识层、网络层和数据层[9], 如图 1 所示. 区块链凭借去中心化、账本数据不可篡改、可溯源和公开透明等特性[10], 能够有效应对当前互联网环境下存在的安全和信任问题. 但是, 传统区块链技术仍然存在以下问题: 在计算方面, 节点通过共识机制 (如 PoW (proof of work)) 来竞争记账权, 此过程不仅造成大量计算资源的浪费, 同时极大地消耗电力资源. 据统计, 一笔比特币交易的能源消耗可以为一个美国家庭供电 14.46 天[11]; 比特币网络的整体电力需求已飙升至每年 121.36 多太瓦时, 超过了阿根廷整个国家的用电量[11]. 而在存储方面, 节点需要保存完整的区块链副本才能验证区块和交易, 由于数据的不可篡改性, 区块链账本随着时间的推移不断增长. 截至 2021 年 3 月 12 日, 比特币账本大小已经达到 386.70 GB[12], 而以太坊更是高达 632.54 GB[12]. 新加入区块链网络的节点需要下载巨大的账本数据. 这个问题极大地限制了存储容量有限的节点参与维护区块链, 降低了区块链系统的去中心化程度.

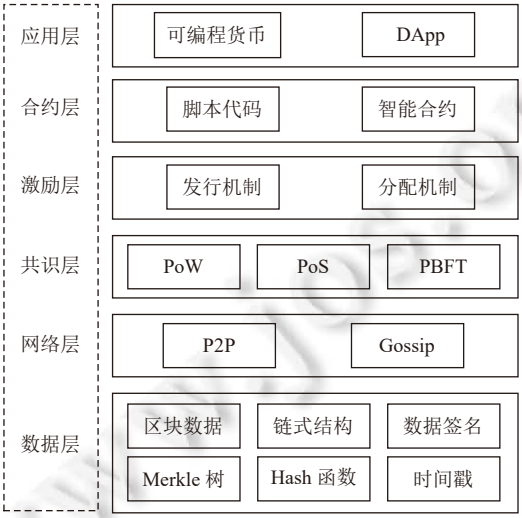

图 1 区块链分层结构

为解决上述挑战, 许多专家和学者根据特定的应用场景对传统区块链技术上进行了优化革新, 提出了轻量级区块链技术. 所谓轻量级主要体现在降低计算和存储消耗两方面. 在计算方面, 通过对传统高能耗的共识算法优

化, 以减轻节点算力消耗; 安全的轻量级密码学工具的研究[13]也有助于提高运算效率. 在存储方面, 通过对账本数据的卸载、压缩, 利用分片技术、云存储等来解决存储压力. 第 2 节将详细介绍这些轻量级技术方案.

2 轻量级区块链技术

在资源受限的场景中应用传统的区块链有诸多限制, 轻量级区块链技术的探索与研究有助于拓展区块链的应用领域. 以下将从轻量级计算、轻量级存储和兼顾计算和存储的轻量级方案 3 个方面阐述当前轻量级区块链技术的研究现状. 图 2 对本文所述的相关轻量级区块链技术进行了分类.

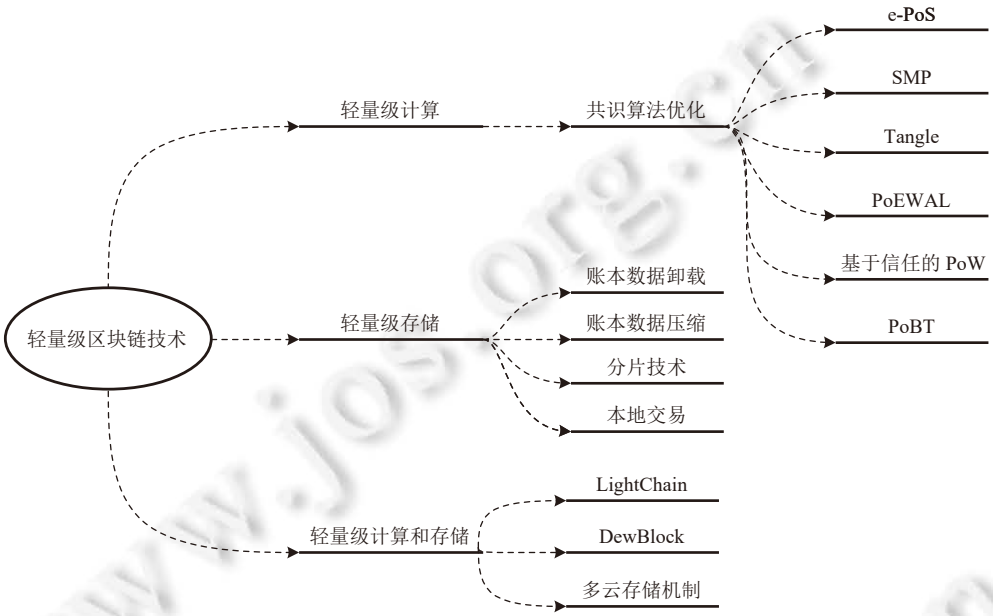

图 2 轻量级区块链技术分类

2.1 轻量级计算

在区块链系统中, 节点通过共识机制实现对区块链账本的一致性维护; 利用加密算法、数字签名和验证机制保证交易数据的正确性和合法性. 区块链的算力消耗主要集中在矿工节点运行共识算法竞争记账权, 因此, 优化传统区块链的共识算法是轻量级计算研究的主要方向. 图 3 展示了本文所列举的轻量级共识机制.

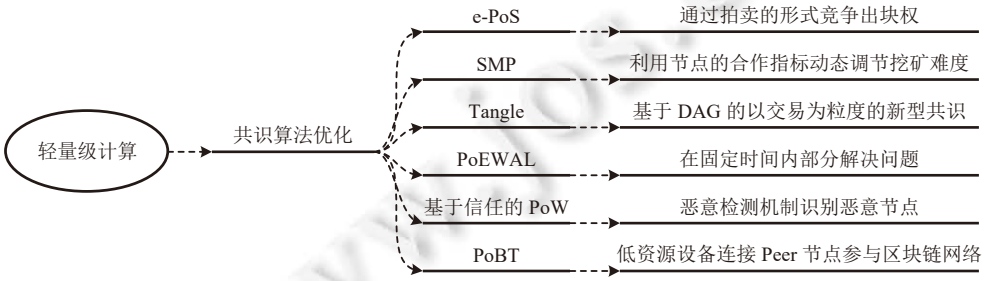

图 3 轻量级计算方案概述

2.1.1 传统区块链共识算法

当前, 区块链中最常用的共识算法有两类, 一种是证明类共识算法, 如 PoW、PoS (proof of stake) 等; 另外一种是拜占庭类共识算法, 如 PBFT (practical byzantine fault tolerance)[14]、Raft[15]等. 由于去中心化程度高, 安全性好,

证明类共识大多应用于公有链中. 而拜占庭类共识主要应用在联盟链中, 由于依赖第三方信任机构, 因此其去中心化程度不高.

(1) PoW

比特币在去中心化的场景中, 实现了用户之间安全的假名化交易, 目前占据了加密数字货币较大的市值份额. 以比特币为代表的 Litecoin[16]、Bitcoin-NG[17]、GHOST[18,19]等第一代加密数字货币所使用共识机制大多是工作量证明机制 (PoW). PoW 共识基于硬件设备进行密码学运算的确定性和可验证性来达成共识. 绝大部分 PoW 共识使用的密码学运算为哈希函数.

PoW 共识的具体过程如下.

① 矿工节点反复试错来改变 *nonce* 值, 直到找到满足公式 (1) 的 *nonce* 值, 最先找到满足要求的 *nonce* 值的矿工节点成为出块节点.

$$SHA256(SHA256(block||nonce)) < target \tag{1}$$

② 出块节点构造新区块, 并在区块链网络中广播新区块.

③ 区块链网络中的其他节点验证区块和交易, 若区块和所有交易均合法, 那么将新区块写入区块链中, 同时进入下一轮共识; 否则忽略该区块并继续本轮共识.

在 PoW 共识中, 节点发动攻击需要控制全网 51% 的算力. 在没有中心化节点的情况下, 节点攻击成功的概率非常低. 因此, PoW 共识能够有效地保障区块链系统的安全性. 但是, PoW 共识存在严重的能耗问题[20], 如 2014 年比特币总体挖矿能耗相当于爱尔兰年用电量[21,22]. 此外, 受出块时间和区块大小的限制, PoW 共识中交易的吞吐量很低, 如比特币每秒处理大约 7 笔交易.

(2) PoS

针对 PoW 共识存在的高能耗问题, 文献 [23,24] 提出权益证明机制 (PoS), 该机制是基于用户权益达成分布式节点间账本数据的一致性[25]. 并在点点币 (PPcoin) 中提出了币龄的概念, 其中定义币龄为节点持有代币的数量与持有时间的乘积 $coinage = coins \times age$. 币龄随时间呈线性增长, 在交易和挖矿过程中被消耗.

PoS 共识的具体过程如下:

① 用户通过质押持有的代币来获取币龄, 币龄越长成为出块节点的概率越大, 挖矿需满足公式 (2).

$$SHA256(SHA256(block||nonce)) < coinage \times target \tag{2}$$

② 出块节点收集合法交易, 打包进新区块中, 并将新区块广播到区块链中.

③ 区块链网络中的其他对等节点对新区块进行验证, 若验证通过, 那么将新区块写入区块链中, 同时进入下一轮共识; 否则忽略该区块并继续本轮共识.

在 PoS 共识中, 节点不需要计算无意义的哈希值, 挖矿过程消耗少量的算力, 因此其能有效缓解 PoW 共识存在的高能耗问题. 此外, 在 PoS 共识中, 节点发动攻击需要控制全网 51% 的权益, 而恶意节点控制 51% 权益的难度高于控制 51% 算力, 因此, PoS 共识安全性更好[23]. 但 PoS 共识仍存在诸如公平性差、容易产生马太效应等缺点.

此外还有一些其他的共识算法, 如: PoB (proof of burn) 是通过销毁基础代币来获得出块奖励的共识机制[26]; PoA (proof of authority) 则是借助声誉高的权威人士来达成共识, 权威人士作为领导者节点[27]; PoC (proof of capacity) 是将节点的剩余存储空间作为竞争记账权的条件, 存储空间大的节点获得记账权的概率高, 如 Permacoin[28]、Spacemint[29]; PoET (proof of elapsed time) 是将硬件执行某个命令的等待时间作为选举出块者的标准, 等待时间最短的节点即为出块节点[30]. 但是, 这些共识都存在能耗高的缺点, 因此并不能直接应用于资源受限的场景.

2.1.2 共识算法优化

传统区块链共识算法要求节点计算无意义的哈希函数, 此过程造成大量资源浪费, 同时不利于在资源受限场景部署区块链. 因此, 许多专家和学者对传统区块链共识算法进行优化, 提出了轻量级共识算法. 表 1 对比分析了传统区块链共识算法和轻量级共识算法的优缺点.

表 1 轻量级计算方案总结分析

分类	共识机制	计算消耗	去中心化程度	安全性	可扩展性	优点	缺点
传统区块链共识方案	PoW	高	完全	强	弱	安全性强, 去中心化程度高	资源消耗大, 可扩展性低
	PoS	低	完全	强	中等	资源消耗低, 安全性强	产生马太效应, 内部共识依赖代币
轻量级共识优化方案	e-PoS	低	完全	强	中等	资源消耗低, 公平性好	需要达成两次共识, 共识依赖代币
	SMP	低	完全	强	中等	资源消耗低, 公平性好	内部共识依赖代币
	Tangle	低	完全	弱	强	资源消耗低, 扩展性强	安全性差, 无全局排序, 实现复杂
	PoEWAL	低	完全	强	强	资源消耗低, 扩展性强	资源受限设备竞争记账权的概率低
	基于信任的 PoW	低	完全	强	中等	资源消耗低, 安全性强	恶意行为识别带来额外的计算开销
	PoBT	低	半中心化	强	强	资源消耗低, 扩展性强	去中心化程度低, 依赖排序节点

(1) e-PoS (extended PoS)

基于股权的 PoS 共识协议容易造成马太效应, 因此, 文献 [31] 提出一种 PoS 的改进协议 e-PoS, 以提高挖矿竞争的公平性. 在 e-PoS 中, 区块周期性产生. 在每个周期内, 矿工通过执行一个不可变的智能合约生成一系列的区块, 如图 4 中的 B_1、B_2、...、B_{l-1}、B_l, 其按区块交易费之和降序排序.

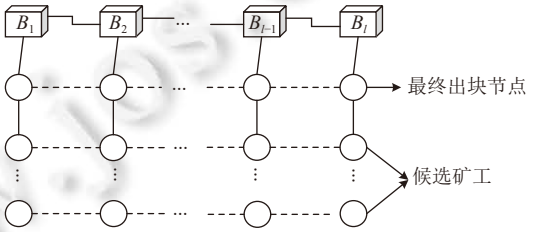

图 4 e-PoS 共识周期

e-PoS 共识的具体过程如下.

① 上一轮周期的出块节点构造区块, 并计算每个区块的基线权益. 节点对一个周期内产生的所有交易按交易费降序排序, 并按顺序用这些交易填充区块, 基线权益表示为区块内所有交易的交易费之和. 节点将产生的一系列新区块及每个区块对应的基线权益广播到区块链系统中 (此过程的节点均指的是上一轮周期的出块节点).

② 通过拍卖竞争记账权. 愿意参与区块拍卖的候选矿工将自身账户余额与区块基线权益进行比较, 当余额大于基线权益时, 则有资格参与该区块拍卖. 候选矿工对当前周期内的所有区块进行出价, 将出价发送到智能合约中, 其中出价以百分比形式表示. 系统按出价最高者选择最终的出块节点, 当出现出价相同时, 实际账户余额高的候选矿工获得记账权. 如图 4 中最上边一层节点获得对应区块的记账权.

③ 最终选定的出块节点将自身余额质押到智能合约中, 同时获得对应区块. 节点验证区块中每笔交易, 如果所有交易均合法, 则对区块签名, 并广播到区块链网络中; 如果有交易违法则将其从区块移除.

④ 区块链网络中的其他对等节点验证新区块及对应出块节点的签名, 若验证成功, 将新区块写入区块链中, 否则将其丢弃.

⑤ 上一轮周期的出块节点执行智能合约, 将控制权转移给本轮周期挑选的出块节点, 同时开启下一轮周期的共识.

在 e-PoS 中, 新区块的产生并不需要运行复杂的密码学算法, 因此能耗相比于 PoS 更低; 此外基于自身资产的百分比来竞争记账权, 整个过程更加公平. 然而, 节点在构造区块前需要对交易池内的交易达成一次共识, 在之后的区块拍卖过程中又需要对区块的所属权达成一次共识, 因此整个过程需要两次共识, 增加了额外的计算开销和通信带宽消耗.

(2) SMP (synergistic multiple proof)

文献 [32−34] 提出一种应用于工业物联网场景下的多重协作证明机制 SMP , 该机制基于物联网设备之间的合作指标来达成区块链账本的一致性. SMP 引入了合作的概念, 定义为物联网设备数据交换的过程, 并用 *CI* (collaboration index) 可视化设备的合作程度. *CI* 本质相当于代币, 用于支付交易产生的数据流. SMP 借鉴了 PoS 中币龄的概念, 将设备持有的 *CI* 及持有时间的乘积定义为“币龄”.

SMP 共识具体过程如下 (涉及的符号及含义见表 2):

表 2 SMP 共识中符号含义

符号	含义
Ω	$\Omega=\sum_{i=1}^{\in} mCI_i\times\Delta t_i$
Φ	$\Phi=\frac{\theta}{200}\times\frac{\psi'}{\psi}$
mCI	CI的最小单位
Δt	mCI 对应的持有时间
$\in$	持有的mCI 总数
θ	近200个块周期内该设备提出的区块数量
ψ'	近200块周期内网络平均吞吐量
ψ	预定义的网络吞吐量阈值

① 节点反复试错来改变 *nonce* 值, 找到满足公式 (3) 的 *nonce* 值. 最先找到满足要求的 *nonce* 值的节点成为出块节点.

$$SHA256(SHA256(block||nonce))<(\Omega+\Phi)\times target \tag{3}$$

② 出块节点负责收集合法交易, 将其打包进区块, 并将新区块广播到区块链网络中.

③ 区块链网络中的其他节点对新区块进行验证, 若验证通过, 那么将新区块写入区块链中, 同时进入下一轮共识; 否则忽略该区块并继续本轮共识.

在 SMP 下的挖矿难度远比 PoW 小, 有效降低了资源消耗. 此外, 为了防止 PoS 带来的马太效应, 定义了两个规则, 一是成功获得记账权的矿工需要初始化自己对应的持有时间 (也就是币龄); 二是获胜者需要等待几个区块之后才能参加下一轮挖矿. 这种机制不仅提高了区块链的公平性, 同时也减少了计算力的浪费.

(3) Tangle (缠绕)

IoTA[35]是一种新颖的交易结算型区块链, 旨在为物联网提供开放、免费的数据和价值转移平台. 不同于传统的链式结构, IoTA 内部采用基于 DAG[36]结构的 Tangle 技术对交易形成共识. 如图 5 所示, 每笔交易都作为图中的一个节点, 用户通过验证两笔历史交易并用哈希指针与自己新产生的交易进行连接的形式将交易插入到区块链中. 没有被验证的交易定义为 *tips*.

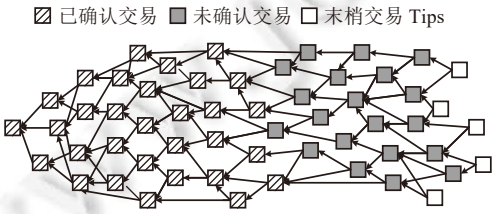

图 5 Tangle 结构图

Tangle 共识的具体过程如下.

① 节点在发起新交易时, 需要在区块链网络中随机寻找两笔 *tips* (此过程采用马尔可夫蒙特卡洛法 (MCMC)),

验证这两笔 *tips* 是否与历史交易有冲突. 若无冲突, 节点利用哈希指针将这两笔交易与新交易进行链接, 然后广播到区块链网络中; 否则寻找其他合法的 *tips*.

② 每笔交易会直接验证两笔前缀交易, 并间接验证这两笔前缀交易直接和间接指向的更早的交易. 当交易被直接或间接验证的次数达到阈值时, 该笔交易就在全网达成共识. 如图 5 中斜杠底纹的交易表示其已被确认并在全网达成共识; 而灰底的交易表示其被验证次数尚未达到阈值, 处于待确认状态.

在 Tangle 中剔除了矿工的角色, 节点不需要竞争记账权, 极大减少了共识的算力消耗; 此外, 交易并行处理, 提高了区块链的运行效率. 然而, 在基于 Tangle 技术的区块链系统中, 攻击者仅需较低的计算成本便能对区块链发动攻击[37], 这严重影响了区块链的安全性和稳定性. 此外, Tangle 中的账本数据无全局排序, 其高效实现较为复杂.

(4) PoEWAL (proof of elapsed work and luck)

在 PoEWAL[38]共识中, 每个参与节点或矿工被分配一个固定的时间范围来解决类似于 PoW 的密码难题, 该机制依赖于给定时间段内执行的工作量, 强调在固定的时间内通过部分解决问题来达成共识而不是在可变的时间内完全解决问题.

PoEWAL 共识的具体过程如下.

① 矿工节点在给定的时间内运行哈希运算, 将其具有最多数量连续零的哈希值的输出广播到区块链网络中. 系统比较所有矿工的输出, 以最多连续作为输出的矿工获得记账权.

② 若多个矿工节点拥有相同的最高数量的连续零, 会产生冲突, 导致区块链分叉. 为了避免分叉, 该机制引入了运气证明, 比较作为哈希运算输入的随机数的值, 拥有较低输入的矿工获得记账权.

③ 获得记账权的矿工节点构造新区块, 并广播到区块链网络中.

④ 区块链网络中的其他节点验证区块和交易, 若验证成功, 将新区块写入区块链中, 同时开启下一轮共识; 否则将其丢弃, 重新竞争记账权.

通过调整给定时间段的大小, 可以有效降低区块开采的资源消耗, 算力低的设备也可以参与挖矿. 但是, 该共识的本质仍然是通过不断地哈希运算以获得更多连续零的哈希值. 类似于 PoW , 拥有高算力的节点成功挖矿的概率更高.

(5) 基于信任的 PoW 机制

文献 [39] 提出了一种基于信任的 PoW 机制, 在保证区块链网络安全性的前提下能有效解决 PoW 共识中的高能耗问题. 该方案引入节点信用值的属性, 信用值越高的节点挖矿难度越低. 如图 6 所示, 利用恶意行为检测机制, 把节点的行为分为积极和消极两方面, 积极行为有助于提高节点的信用值, 而消极行为则会降低节点的信用值. 其中积极方面表现为节点在共识过程中计算和验证的有效交易数量; 而消极方面则由节点的恶意行为时间和惩罚系数决定, 其中恶意行为分为两种, 一种是节点在共识过程中偷懒不作为, 另一种是节点在交易中发动双花攻击. 系统会根据节点的实际恶意行为动态调整惩罚系数.

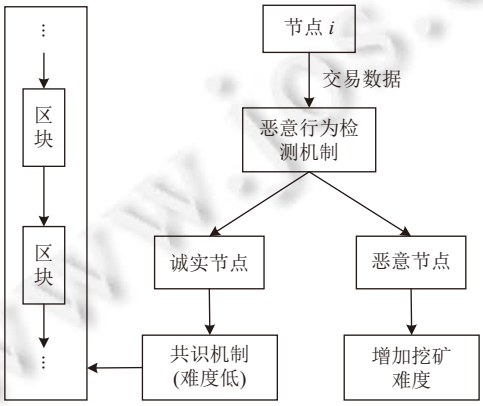

图 6 恶意行为检测共识模型

具体共识过程如下.

① 恶意行为检测机制对节点行为进行监控, 对于存在恶意行为的节点进行标记, 系统根据积极和消极两方面参数动态调整节点的信用值.

② 节点运行 PoW 共识算法竞争记账权. 节点的挖矿难度由信用值决定, 诚实节点获得较低的挖矿难度; 被标记的恶意节点由于信用值低会产生较高的挖矿难度, 成功挖矿的概率远低于诚实节点.

③ 获得记账权的节点构造区块, 并将新区块广播到区块链网络中. 其他对等节点验证新区块, 并更新区块链账本数据.

大量实验表明, 当模拟节点发起恶意行为时, 节点的信用值出现下降趋势, 会产生较高的挖矿难度, 成功挖矿的概率远低于诚实节点[39]. 通过这种方式, 恶意节点将永远得不到记账权. 能有效减少恶意攻击行为, 增强区块链网络的安全性, 降低诚实节点的算力消耗. 但是, 恶意行为的实时检测以及信用值的实时更新维护会带来额外的计算开销.

(6) PoBT (proof of block and trade)

PoBT[40]是基于 Hyperledger Fabric 框架为物联网设计的一种轻量级共识协议. 如图 7 所示, 物联网设备并不直接参与区块链的维护, 通过连接区块链网络中的对等节点来提交交易提案.

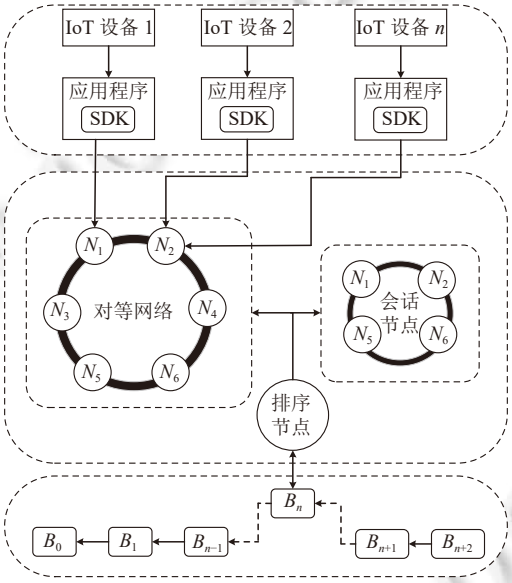

图 7 PoBT 共识模型

PoBT 共识过程如下.

① 物联网设备形成交易提案通过 SDK 发送到与其连接的 Peer 节点. 如图 7 中 IoT 设备 1 通过 SDK 与对等网络中的 N_1 节点进行连接.

② 连接交易双方的 Peer 节点执行交易, 然后发送到排序节点.

③ 交易在排序节点中形成候选区块, 在区块提交前, 由排序节点执行相应算法挑选出参与本区块交易的 Peer 节点形成一个会话, 区块和区块中的交易由这些会话节点进行验证. 如图 7 中参与区块 B_n 中交易的节点有 N_1、N_2、N_5、N_6, 所以这些节点将被挑选成为会话节点参与 B_n 中交易的验证.

④ 排序节点为每个会话节点分配一组交易, 会话节点验证完所有交易后会返回给排序节点一个完成的响应, 当收到超过半数的响应后排序节点批准新区块, 然后将新区块连同排序节点的签名一起发送给网络中所有连接的 Peer 节点. 每个 Peer 节点都会验证签名并将该区块添加到其分类帐中.

在 PoBT 共识中, 新区块由排序节点产生, 剔除了矿工的角色, 节点不需要浪费巨大的算力资源来竞争记账权.

此外, 交易的验证仅限于直接参与交易的 Peer 节点, 这显著减少了信息交换所需的时间以及大量节点参与验证带来的额外计算开销. 缺点就是去中心化程度不高, 共识过程严重依赖于排序节点.

2.2 轻量级存储

由于区块链账本数据的不可篡改性, 随着时间的推移账本数据不断增长, 存储空间受限的节点将无法保存完整的区块链副本, 以至于无法参与区块链的维护, 从而导致去中心化程度的降低. 轻量级存储技术的研究能够有效解决账本数据不断增长带来的问题. 下面将从历史交易数据删除、区块压缩、分片技术、新型架构下的本地交易模型 4 个方面阐述当前区块链中轻量级存储技术的发展. 图 8 展示了本文讨论的轻量级存储方案. 此外, 表 3 总结分析了所讨论的方案的优缺点.

图 8 轻量级存储方案概述

表 3 轻量级存储方案总结分析

分类	概述	优点	缺点
基于UTXO模型的数据卸载	对于不包含UTXO的区块定期执行算法卸载, 以节省空间	缓解节点存储压力, 账本数据卸载达43.35%[32]	破坏账本数据完整性
基于账户模型的数据卸载	交易包含账户状态验证路径, 节点仅需保存最新区块	缓解节点存储压力, 账本数据卸载高达90%以上[41]	破坏账本数据完整性, 节点频繁更新验证路径, 增加计算开销
账本数据压缩算法	当节点自身存储空间不足时, 将历史区块压缩成一个区块	缓解节点存储压力, 减少63%的存储空间消耗[42]	破坏数据完整性, 压缩频率过高, 增加出块和交易处理时延
分片技术	利用分片技术, 节点仅存储自己分片的账本数据	减少存储成本, 提高区块链的可扩展性	跨分片交易处理成本高, 单个分片的安全性和抵御攻击的能力差
本地交易	连接到同一节点的设备产生的交易仅存储在该节点内	在一定程度上能缓解存储压力	去中心化程度低; 节点连接大量设备时, 增加交易处理时延

2.2.1 账本数据卸载

通过分析 UTXO (unspent transaction outputs) 模型和账户模型下的区块链系统的验证机制, 不难发现, UTXO 集合和账户状态都是在不断更新变化的. 对于那些动态存储的内容, 只保存可能由后续交易直接引用的数据, 至于微不足道的部分, 应该在不影响系统正常运行的情况下从本地转移下来. 基于此思想, 一些学者提出通过删除那些“无用”的历史交易数据的方法来缓解节点的存储压力. 下面将具体介绍两种模型下的数据卸载方案.

(1) 基于 UTXO 模型的数据卸载

文献 [32−34] 提出了一种新颖的卸载算法, 称为不相关区块卸载 (unrelated block offloading filter, UBOF), 旨在过滤不相关的区块. 在 UTXO 型区块链系统中, 当 UTXO 集合中的交易输出在之后的交易中被花费时, 这笔输出就会从 UTXO 集合中删除, 存储这笔交易输出的区块中能够被后续交易所引用的 UTXO 数量会减少. 当一个区块中不存在未花费的交易输出时, 就将该区块定义为不相关区块, 在之后的交易验证中不被需要, 因此可以被删除, 以节省空间. 基于此思想设计的 UBOF 算法能够使节点可持续的利用存储空间. 节点定期执行 UBOF 算法, 卸载本地不相关的区块, 同时将完整的区块链副本存储到云端. 实验表明, UBOF 算法可以卸载高达 43.35% 的历史数据[32].

(2) 基于账户模型的数据卸载

同样考虑对账本数据删除的方案, 文献 [41] 提出一种基于以太坊账户模型的财产证明 PoP (proof of property)

方案, 其基本思想是在每笔交易中包括一个财产证明 (证明某笔交易的输入账户拥有足够的硬币来完成所述交易). 节点通过最新区块的状态树提取自己账户的验证路径, 每当有新的区块产生时, 节点都需要更新自己账户的验证路径, 并在所提交的交易中包含最新的验证路径. 在验证过程中, 节点仅需最新区块头就可以验证交易合法性. 节点将最新区块头中状态树根的哈希与验证路径中状态树根的哈希进行比较, 若相同则证明验证路径是正确的, 然后再根据验证路径检验账户是否有足够的硬币来满足交易.

在 PoP 方案中, 验证交易不需要历史区块, 节点可以在存储空间不足时删除历史区块, 以缓解存储压力. 对于新参与者允许先下载最新区块参与竞争记账权, 完整区块链可以在后台下载, 这就减少了参与者的等待时间. 但是, 节点频繁更新验证路径会带来额外计算开销.

2.2.2 账本数据压缩

文献 [42] 提出一种账本数据压缩方案. 通过与共识机制有机结合, 将历史区块数据进行压缩处理, 充分提高节点存储空间利用率. 在所提议的方案中, 节点加入区块链网络后, 需要在区块链网络中同步自身的存储能力. 如图 9 所示, 通过 PBFT 共识的有机结合, 在选择 Leader 节点时, 节点检测自身剩余存储空间; 当存储空间充足时, 则正常执行 PBFT 共识; 当存储空间不足时, 则启动数据压缩程序. 将历史区块作为叶子节点构造 Merkle 树, Merkle 树根节点的哈希值存储在压缩区块中, 新区块的哈希指针指向压缩区块, 最后在区块链网络中同步压缩后的区块数据. 实验表明, 与传统区块链相比, 基于数据压缩程序的区块链系统能有效节省节点的存储空间, 缓解节点的存储压力. 当系统趋于稳定时, 压缩程序能减少节点约 63% 的存储空间[42]. 但是, 随着大量节点的加入, 压缩程序调用的频率会升高, 同时会增加出块时延.

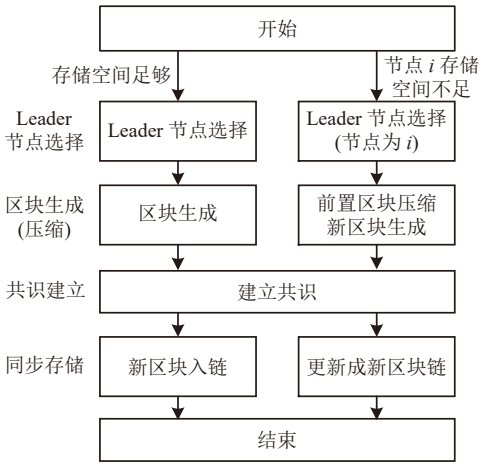

图 9 区块压缩模型

2.2.3 分片技术

分片技术是数据库中常用的手段, 其通过将大型数据库分割为大量小而易管理的数据碎片, 以提高数据的处理效率. 在区块链中, Luu 等人[43]将分片技术与共识协议有机结合, 提出了分片共识协议. 利用分片技术的思想将区块链网络分割为许多更小的网络分片, 每个网络分片只需要运行更小范围的共识, 处理更少的交易, 存储更少的账本数据. 当前分片技术按难度递进分为网络分片、交易分片和状态分片 3 个层级. 网络分片是基础, 状态分片实现最为复杂. 其中状态分片通过将完整的状态信息分散地存储到各个分片中, 从而使得每个分片可以独自处理交易, 节点仅需维护自己分片内的账本数据. 分片技术不仅能提高区块链的可扩展性, 同时很大程度上解决了区块链巨额存储成本问题. 典型的分片方案有 RapidChain[44]、Omniledger[45]等.

文献 [46] 是利用分片思想, 在主子链架构中融入有向无环图, 提出一种新颖的交叉链解决方案. 该方案采用分片共识, 每个分片内的节点独立的维护一个子链账本, 每个子链通过联盟链连接到主链. 与传统区块链相比, 在此方案下, 每个子链可以独立并行地处理交易, 有效提高区块链系统的吞吐量; 此外, 子链只存储特定分片内的账

本数据, 有助缓解节点的存储压力, 降低账本数据在大范围同步过程中所带来的网络消耗.

2.2.4 本地交易

文献 [40] 提出了一种本地交易的概念. 在物联网场景中, 每个物联网设备通过连接区块链网络中的节点来发起交易, 一个节点可以连接多个物联网设备. 连接到同一节点的设备之间的交易被称为本地交易. 本地交易的处理流程如图 10 所示, 源设备 D_s 发起交易 M, 与之连接的节点 N_{sd} 在此过程中被定义为本地节点. 一旦本地节点确定交易请求的目标设备 D_d 也和自己相连, 那么本地节点就验证源设备 D_s 和目标设备 D_d 的签名, 并请求排序节点选择一个随机节点 N_i 来验证交易 M. 当交易 M 通过验证之后被发送到排序节点, 排序节点收集本地节点 N_{sd} 的本地交易, 构造新区块并签名, 该本地节点 N_{sd} 保存新区块. 在此方法中, 本地交易仅存储在该本地节点中. 当交易双方连接不同的节点时, 交易才会被上传到区块链, 存储在所有节点中. 通过这种本地交易的形式能够有效降低区块链账本的增长速度, 有助于缓解节点的存储压力. 但本地交易依赖于特定的系统框架, 无法推广到其他类型的区块链系统中.

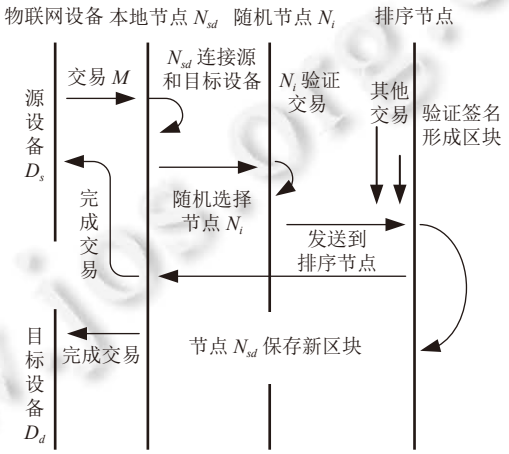

图 10 本地交易流程

2.3 兼顾计算和存储的轻量级方案

不同于第 2.1、2.2 节所阐述的单一优化的轻量级方案, 本节讨论的方案能够有效兼顾计算和存储优化, 解决资源受限场景下无法部署区块链的问题. 图 11 展示了本文讨论的兼顾计算和存储的轻量级方案. 此外, 表 4 总结分析了所讨论的方案的优缺点.

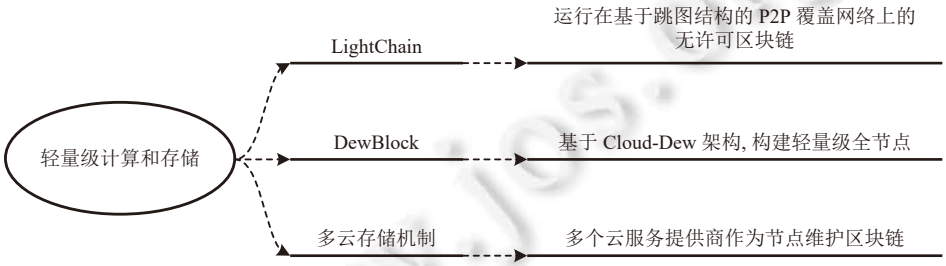

图 11 兼顾计算和存储的轻量级方案概述

(1) LightChain

LightChain[47]是运行在基于跳图 (skip graph)[48]结构的 P2P 覆盖网络上的无许可区块链. 跳图是一种基于 DHT (分布式哈希表) 的分布式数据结构[49], 每个跳图节点具有数字 ID、名称 ID 和 IP 地址 3 种属性, 其中数字 ID 和名称 ID 被称为节点的标识符. 节点通过检索标识符访问其所需要的数据. 在区块链的交易生成过程中, 节点需要收集一定数量的对等节点对交易的验证签名, 才能调用跳图的插入算法将交易插入跳图中. 而在区块生成过

程中, 节点需要收集跳图中的交易, 并构造区块, 然后在跳图中随机检索节点, 并请求其验证区块并签名, 最先集齐一定数量的节点的验证签名的节点将新区块插入跳图中. 当交易被包含在新区块并被插入到跳图中时, 交易的发起者会将该交易从跳图中删除以提高检索效率.

在 LightChain 中, 节点不需要存储完整区块链账本, 通过检索跳图按需访问交易和区块; 在基于跳图的验证证明 (proof-of-validation, PoV) 共识机制下, 节点能够平等的参与竞争记账权, 而不受算力和资产的影响. 该方案不仅能有效缓解节点的存储压力, 同时减少了共识过程中计算资源的消耗, 提高共识公平性, 解决了资源受限设备无法参与区块链的问题. 但是节点频繁地查找、插入、删除操作增加了网络消耗.

表 4 兼顾计算和存储的轻量级方案总结分析

分类	概述	优点	缺点
LightChain	运行在基于跳图结构的P2P覆盖网络上的无许可区块链	减少了共识过程中计算资源的消耗, 提高共识公平性, 缓解节点存储压力	节点频繁地查找、插入、删除操作增加了网络消耗
Dewblock	基于Cloud-Dew架构, 构建轻量级全节点	缓解个人设备的计算和存储压力, 云提供更高效的计算处理能力	部署成本高, 云存储安全性低
多云存储机制	云服务提供商作为节点维护区块链	提高区块链运行效率, 能够解决个人设备资源限制的问题	物联网设备产生大量的、时效性低的数据存储在云端, 造成资源浪费, 增加部署成本

(2) DewBlock

DewBlock[50]是基于 Cloud-Dew 架构[51]的区块链平台, 将 Dew 计算与云计算有机结合, 构建具有全节点功能的轻量级节点. 其中 Dew 计算[52]是云计算环境中的一种本地计算机软件-硬件组织模式, 本地计算机提供独立于云服务的功能, 并与云服务协作.

在 DewBlock 中, 节点由 Dew 服务器和云服务器组成. Dew 服务器部署在个人计算机或移动设备中, 与云服务器连接, 构成一个全节点. 云服务器和 Dew 服务器可以充当区块链客户端. 当 Dew 客户端独立运行时, 其功能类似于轻节点, 不存储区块数据, 同时无法参与验证和挖矿. 当 Dew 客户端与云客户端连接时, 其具有全节点的功能, 云客户端通过特定的通信协议与 Dew 客户端通信, 以提供计算和存储服务, 在此状态下的 Dew 客户端可以参与区块链的维护工作. DewBlock 将区块链的存储和计算工作都集中在云服务器中, 以此来缓解个人设备的计算和存储压力. 利用云服务能够有效地解决在资源受限场景中无法部署区块链的问题, 但同时也给区块链带来了隐私泄露和数据安全等问题.

(3) 多云存储机制

文献 [53] 提出一种基于区块链的多云存储机制, 旨在为物联网设备产生的数据提供一个安全的存储方案. 该方案采用多个云服务提供商节点取代单个云服务. 如图 12 所示, 智能设备, 家庭信息管理员和云服务提供商共同组成区块链系统. 在以家庭为单位的边缘网络中, 多个智能设备通过蓝牙、WiFi、ZigBee 等方式相会连接, 这些设备收集数据, 以提供更好的服务; 同时家庭信息管理员负责收集智能设备产生的数据, 定期上传到云端存储, 并通过区块链网络将存储记录以交易的形式记录到区块链中. 云服务提供商作为区块链网络中的对等节点负责维护区块链, 每个云服务提供商都保存完整的区块链副本. 为了保证上传到云上的数据的完整性和正确性, 采用基于身份的代理聚合签名 IBPAS (ID-based proxy aggregation signature) 方案, 每个智能设备生成一个唯一的身份 ID (identity document), 设备生成的数据都需要签名以保证数据完整性. 该方案采用多个云服务提供商节点来运行维护区块链, 能够解决资源受限的物联网设备无法部署区块链的问题; 同时 IBPAS 签名方案能够提高验证速度, 压缩区块存储空间, 减少通信带宽.

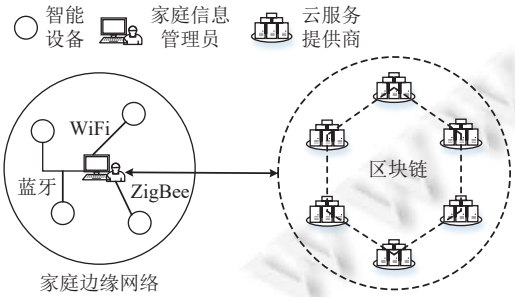

图 12 多云存储机制

3 物联网中轻量级区块链应用架构

物联网环境中存在海量异构、轻量级的智能设备, 这些设备收集的大量数据暴露在网络中, 时刻面临着数据安全等问题, 传统集中式的数据处理策略存在性能瓶颈以及单点故障的问题. 区块链凭借其分布式架构、去中心化以及不可篡改的特性为解决物联网数据存在的安全问题提供了新思路. 但传统的区块链技术存在的能耗高、扩展性差等问题, 这使得区块链与物联网的结合存在巨大挑战. 为解决上述问题, 许多专家和学者展开了物联网场景下的轻量级区块链技术研究. 本节将一些轻量级区块链应用架构分为以下 3 种类型: 1) 物联网设备以全节点身份参与区块链; 2) 物联网设备以轻节点身份参与区块链; 3) 物联网设备以轻节点-全节点身份参与区块链.

3.1 物联网设备以全节点身份参与区块链

这类架构不需要额外部署其他资源强大的设备, 通过研究轻量级的共识机制与数据存储, 试图让资源受限的物联网设备以全节点的身份参与共识过程、区块数据存储、交易验证与区块挖掘的工作. “时态区块链”[54]就是基于此类架构的一种解决方案, 其建议从区块链中删除所有超过预设时间段的块, 以使资源受限设备可以维护区块链. 又如第 2.2.2 节中提到的压缩方案[42], 通过结合 PBFT 共识, 在选择 Leader 节点时会根据节点剩余存储情况执行压缩程序, 使区块链系统处于资源受限设备的可控范围内, 从而使其可以参与共识过程. 文献 [55] 提出了一种传感链的解决方案, 试图使传感器存储区块链账本并参与共识. 该方案的思想类似于第 2.2.3 节中提到的分片技术, 即将一个完整的区域划分为多个子区域, 每个子区域中的传感器节点形成本地网络并维护本地账本. 为了管理区块链的大小, 定期删除历史区块. 而区块则由子区域中的传感器节点以协商的方式挑选出的一个节点进行创建.

此类架构虽然可以使资源受限的物联网设备作为全节点直接管理区块链, 但该类研究忽略了一个重要的细节就是物联网设备的主要工作是收集数据、处理数据以及交换数据, 而这些工作将占据物联网设备的绝大多数资源. 将物联网设备作为全节点管理区块链势必会影响其收集、处理数据的效率, 同时也不利于区块链的扩展. 因此, 目前将物联网设备作为全节点的方案效果不佳.

3.2 物联网设备以轻节点身份参与区块链

在这类架构下, 通过额外部署其他资源强大的设备充当全节点维护区块链, 而资源受限的物联网设备以轻节点的身份参与区块链, 不需要存储完整的区块链账本. 如基于 Hyperledger Fabric 框架 PoBT[40]模型, 物联网设备通过连接 peer 节点发起交易, 不需要存储账本数据; 区块的生成依赖排序节点, 交易验证以及账本数据存储由 peer 节点承担. 在该模型下, 区块链的可扩展性得到了改善, 同时也解决了物联网与区块链结合存在的挑战. 但是, 节点加入区块链网络需要向第三方信任机构进行身份认证, 去中心化程度低. 此外, 区块链的性能依赖排序节点生成区块的效率. 文献 [38] 通过集群的形式组织物联网设备, 每个集群中部署一个资源强大的设备作为集群头, 由集群头执行轻量级的 PoEWAL 共识协议维护区块链. 文献 [53] 结合云计算, 以云服务提供商作为全节点, 但云服务器远离物联网终端, 交易的处理以及传输天然存在一定延迟. 而文献 [33,34] 则利用边缘计算, 将全节点部署在靠近物联网终端的边缘节点处, 以解决云计算带来的处理时延问题.

此类架构能有效解决区块链与物联网融合问题, 在一定程度上提高了物联网区块链的可扩展性, 但未充分利用物联网设备资源, 忽视物联网不同层的设备之间的差异性.

3.3 物联网设备以轻节点-全节点的身份参与区块链

不同于上述两类架构, 本节讨论的架构充分考虑了物联网的分层结构, 使区块链与物联网的不同层有机结合形成新的架构[56]. 将资源严重受限的感知层设备设为轻节点, 考虑到物联网的网络层和应用层的终端设备具有一定的计算和存储能力, 因此可以选择轻量级的共识算法以及数据存储方式, 使得这部分的终端设备可以以全节点的身份维护区块链, 从而减少额外部署全节点的成本消耗. 文献 [32] 为工业互联网设计了一种轻量级的区块链系统, 该方案将全节点部署在物联网应用层中的个人计算机中, 而感知层的传感器节点作为轻节点参与区块链. 采用轻量级的共识算法 SMP 以及不相关区块卸载算法 UBOF 来缓解全节点的资源消耗和存储压力, 提高交易处理效率. 文献 [50] 利用 Cloud-Dew 架构, 将个人终端设备与云计算结合, 利用云计算提供的计算和存储服务, 使个人终

端设备可以作为全节点维护区块链. 而文献 [39] 是利用网络层的网关设备作为全节点, 利用恶意行为检测策略增强网络安全性, 降低网关设备挖掘工作的能耗.

文献 [57–60] 在轻节点-全节点架构下进行优化以集群的形式组织节点, 提出了轻量级可扩展的区块链架构 (lightweight scalable blockchain, LSB). 整体架构如图 13 所示, 利用覆盖网络将物联网设备进行互联, 将全节点部署在物联网的网络层和应用层. 系统通过随机的方式选择一个全节点作为集群头, 集群头负责维护区块链, 并通过基于时间的分布式共识算法 (distributed time-based consensus, DTC)[57]与其他集群头建立共识, 同步区块链账本. 物联网设备通过与集群头建立连接从而发起交易, 物联网设备相当于轻节点, 不需要存储区块链账本. 在所提议的框架中, 交易流和数据流分离. 交易被定义为用于在节点之间交换控制信息的基本通信原语, 是描述物联网设备之间交互的一种记录消息; 数据流即物联网设备交换的数据. 交易流是以广播的形式在集群头之间传播, 并存储到区块链上; 而数据流以单播的形式直接路由到交互的双方, 物联网设备产生的数据并不存储到区块链上, 而保存在本地或云端, 以减少内存占用.

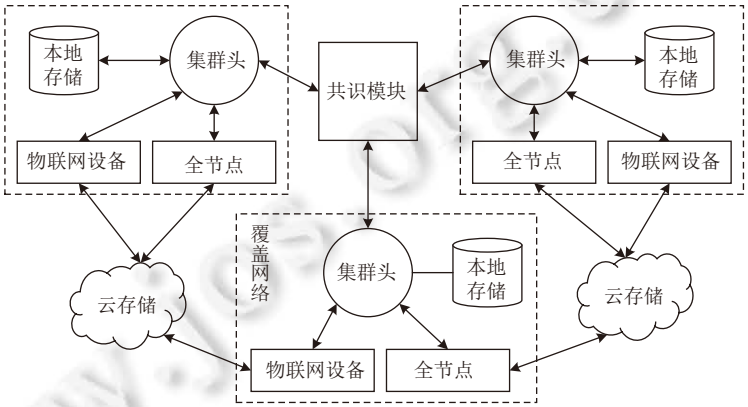

图 13 LSB 架构

本节所介绍的区块链架构能有机的结合物联网各层设备, 并利用轻量级区块链技术能有效解决低资源设备无法满足传统区块链的高算力要求以及无法存储完整区块链账本的问题, 更好地促进了区块链与物联网等资源受限场景的融合发展.

4 研究展望

针对目前区块链存在算力消耗大、扩展性差以及账本数据不断增大等问题, 大规模应用区块链还有许多工作需要开展和完善. 如何解决资源受限场景中部署区块链的问题, 还需要继续深入研究. 轻量级区块链技术的研究仍具有重要现实意义, 未来可以从以下 4 个方面展开研究.

(1) 多级共识机制研究

对大型区块链系统进行合理化的分层处理, 建立多级共识, 先在低层次节点之间建立共识, 再向上层传递, 直到所有节点之间达成共识. 以此来缓解区块链中的算力消耗和网络带宽消耗.

(2) 共识融合分片技术

将共识机制与分片技术结合, 利用状态分片的思想, 合理解决跨分片交易问题, 实现区块链性能的扩展以及可持续存储.

(3) 账本数据的合理优化

现有的一些数据优化方案如删除历史数据、压缩区块等破坏了交易数据的完整性, 如何在保证交易数据完整性的前提下对区块链账本进行瘦身仍需要深入研究.

(4) 安全性和隐私保护

大多数的轻量级区块链方案着重于解决能耗问题, 对于区块链中隐私保护方面缺乏关注. 因此, 在轻量级区块

链技术的研究过程中更应该注重对隐私问题的关注.

5 结束语

区块链凭借其去中心化, 账本数据不可篡改, 公开透明以及可溯源等特点, 能够有效应对当前互联网环境下存在的安全和信任问题, 现已拓展到多个应用领域. 但是, 能耗高、运行效率低等问题制约着区块链的发展, 在资源受限的场景中部署传统区块链仍存在巨大挑战. 本文总结了部分典型的应用在资源受限的场景中的轻量级区块链方案, 通过对比分析, 这些方案虽然在一定程度上能够缓解传统区块链的弊端, 但仍然存在一些缺点, 如安全性不高, 缺乏隐私保护等. 因此, 需要更加深入的研究轻量级区块链技术, 推动区块链的融合发展.

References:

[1] Si XM, Chen WG. Introduction to blockchain and digital currency technology. Ruan Jian Xue Bao/Journal of Software, 2019, 30(6): 1575–1576 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5747.htm [doi: 10.13328/j.cnki.jos.005747]

[2] Casado-Vara R, de la Prieta F, Prieto J, Corchado JM. Blockchain framework for IoT data quality via edge computing. In: Proc. of the 1st Workshop on Blockchain-enabled Networked Sensor Systems. Shenzhen: ACM, 2018. 19–24. [doi: 10.1145/3282278.3282282]

[3] Wang X, Zha X, Ni W, Liu RP, Guo YJ, Niu XX, Zheng KF. Survey on blockchain for Internet of Things. Computer Communications, 2019, 136: 10–29. [doi: 10.1016/j.comcom.2019.01.006]

[4] Toyoda K, Mathiopoulos PT, Sasase I, Ohtsuki T. A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain. IEEE Access, 2017, 5: 17465–17477. [doi: 10.1109/ACCESS.2017.2720760]

[5] Xia Q, Sifah EB, Asamoah KO, Gao JB, Du XJ, Guizani M. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE Access, 2017, 5: 14757–14767. [doi: 10.1109/ACCESS.2017.2730843]

[6] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008. https://bitcoin.org/bitcoin.pdf

[7] Wood G. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 2014, 151(12): 1–32.

[8] Androulaki E, Barger A, Bortnikov V, *et al*. Hyperledger fabric: A distributed operating system for permissioned blockchains. In: Proc. of the 13th EuroSys Conf. Porto: ACM, 2018. 30. [doi: 10.1145/3190508.3190538]

[9] Li D, Wei JW. Theory, application fields and challenge of the blockchain technology. Telecommunications Science, 2016, 32(12): 20–25 (in Chinese with English abstract).

[10] Zhang L, Liu BX, Zhang RY, Jiang BX, Liu YJ. Overview of blockchain technology. Computer Engineering, 2019, 45(5): 1–12 (in Chinese with English abstract). [doi: 10.19678/j.issn.1000-3428.0053554]

[11] Digiconomist. Bitcoin energy consumption index. 2021. https://digiconomist.net/bitcoin-energy-consumption

[12] Bitinfocharts. Blockchain size. 2021. https://bitinfocharts.com/

[13] Wu CK. An overview on the security techniques and challenges of the internet of things. Journal of Cryptologic Research, 2015, 2(1): 40–53 (in Chinese with English abstract). [doi: 10.13686/j.cnki.jcr.000059]

[14] Castro M, Liskov B. Practical Byzantine fault tolerance and proactive recovery. ACM Trans. on Computer Systems, 2002, 20(4): 398–461. [doi: 10.1145/571637.571640]

[15] Ongaro D, Ousterhout J. In search of an understandable consensus algorithm. In: Proc. of the 2014 USENIX Annual Technical Conf. (ATC). Philadelphia: ACM, 2014. 305–320.

[16] Clarke S, Craig I, Wyszynski M. Litecoin cash: The best of all worlds SHA256 cryptocurrency. 2018. https://litecoinca.sh/downloads/lcc_whitepaper.pdf

[17] Eyal I, Gencer AE, Sirer EG, Van Renesse R. Bitcoin-NG: A scalable blockchain protocol. In: Proc. of the 13th USENIX Conf. on Networked Systems Design and Implementation (NSDI). Santa Clara: ACM, 2016. 45–59.

[18] Sompolinsky Y, Zohar A. Secure high-rate transaction processing in bitcoin. In: Proc. of the 19th Int'l Conf. on Financial Cryptography and Data Security. San Juan: Springer, 2015. 507–527. [doi: 10.1007/978-3-662-47854-7_32]

[19] Kiayias A, Panagiotakos G. On trees, chains and fast transactions in the blockchain. In: Proc. of the 5th Int'l Conf. on Cryptology and Information Security in Latin America. Havana: Springer, 2017. 327–351. [doi: 10.1007/978-3-030-25283-0_18]

[20] King S. Primecoin: Cryptocurrency with prime number proof-of-work. 2013. http://launch.primecoin.org/static/primecoin-paper.pdf

[21] Shoker A. Sustainable blockchain through proof of exercise. In: Proc. of the 16th Int'l Symp. on Network Computing and Applications. Cambridge: IEEE, 2017. 1–9. [doi: 10.1109/NCA.2017.8171383]

[22] O'Dwyer J, Malone D. Bitcoin mining and its energy footprint. In: Proc. of the 25th IET Irish Signals & Systems Conf. and the 2014

China-Ireland Int'l Conf. on Information and Communications Technologies. Limerick: IEEE, 2014. 280–285. [doi: 10.1049/cp.2014.0699]

[23] King S, Nadal S. PPcoin: Peer-to-peer crypto-currency with proof-of-stake. 2012. https://bitcoin.peryaudo.org/vendor/peercoin-paper.pdf

[24] Peerchemist. PeerAssets whitepaper. 2016. https://www.Peercoin.net/

[25] Vasin P. Blackcoin's proof-of-stake protocol V2. 2014. https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf

[26] Karantias K, Kiayias A, Zindros D. Proof-of-burn. In: Proc. of the 24th Int'l Conf. on Financial Cryptography and Data Security. Kota Kinabalu: Springer, 2020. 523–540. [doi: 10.1007/978-3-030-51280-4_28]

[27] De Angelis D, Aniello L, Baldoni R, Lombardi F, Margheri A, Sassone V. PBFT vs. proof-of-authority: Applying the CAP theorem to permissioned blockchain. In: Proc. of the 2nd Italian Conf. on Cyber Security. Milan: CEUR-WS, 2018.

[28] Miller A, Juels A, Shi E, Parno B, Katz J. Permacoin: Repurposing bitcoin work for data preservation. In: Proc. of the 2014 IEEE Symp. on Security and Privacy. Berkeley: IEEE, 2014. 475–490. [doi: 10.1109/SP.2014.37]

[29] Park S, Kwon A, Fuchsbauer G, Gaži P, Alwen J, Pietrzak K. SpaceMint: A cryptocurrency based on proofs of space. In: Proc. of the 22nd Int'l Conf. on Financial Cryptography and Data Security. Nieuwpoort: Springer, 2018. 480–499. [doi: 10.1007/978-3-662-58387-6_26]

[30] Chen L, Xu L, Shah N, Gao ZM, Lu Y, Shi WD. On security analysis of proof-of-elapsed-time (PoET). In: Proc. of the 19th Int'l Symp. on Stabilization, Safety, and Security of Distributed Systems. Boston: Springer, 2017. 282–297. [doi: 10.1007/978-3-319-69084-1_19]

[31] Saad M, Qin Z, Ren K, Nyang D, Mohaisen D. e-PoS: Making proof-of-stake decentralized and fair. IEEE Trans. on Parallel and Distributed Systems, 2021, 32(8): 1961–1973. [doi: 10.1109/TPDS.2020.3048853]

[32] Liu YQ, Wang K, Lin Y, Xu WY. LightChain: A lightweight blockchain system for industrial Internet of Things. IEEE Trans. on Industrial Informatics, 2019, 15(6): 3571–3581. [doi: 10.1109/TII.2019.2904049]

[33] Xu CH, Wang K, Xu GL, Li P, Guo S, Luo JT. Making big data open in collaborative edges: A blockchain-based framework with reduced resource requirements. In: Proc. of the 2018 IEEE Int'l Conf. on Communications (ICC). Kansas City: IEEE, 2018. 1–6. [doi: 10.1109/ICC.2018.8422561]

[34] Xu CH, Wang K, Li P, Guo S, Luo JT, Ye BL, Guo MY. Making big data open in edges: A resource-efficient blockchain-based approach. IEEE Trans. on Parallel and Distributed Systems, 2019, 30(4): 870–882. [doi: 10.1109/TPDS.2018.2871449]

[35] Popov S. The tangle. White Paper, 2018, 1(3).

[36] Benčić FM, Žarko IP. Distributed ledger technology: Blockchain compared to directed acyclic graph. In: Proc. of the 38th IEEE Int'l Conf. on Distributed Computing Systems (ICDCS). Vienna: IEEE, 2018. 1569–1570. [doi: 10.1109/ICDCS.2018.00171]

[37] Lathif MRA, Nasirifard P, Jacobsen HA. CIDDS: A configurable and distributed DAG-based distributed ledger simulation framework. In: Proc. of the 19th Int'l Middleware Conf. (Posters). Rennes: ACM, 2018. 7–8. [doi: 10.1145/3284014.3284018]

[38] Raghav, Andola N, Venkatesan S, Verma S. PoEWAL: A lightweight consensus mechanism for blockchain in IoT. Pervasive and Mobile Computing, 2020, 69: 101291. [doi: 10.1016/j.pmcj.2020.101291]

[39] Huang JQ, Kong LH, Chen GH, Wu MY, Liu X, Zeng P. Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism. IEEE Trans. on Industrial Informatics, 2019, 15(6): 3680–3689. [doi: 10.1109/TII.2019.2903342]

[40] Biswas S, Sharif K, Li F, Maharjan S, Mohanty SP, Wang Y. PoBT: A lightweight consensus algorithm for scalable IoT business blockchain. IEEE Internet of Things Journal, 2020, 7(3): 2343–2355. [doi: 10.1109/JIOT.2019.2958077]

[41] Ehmke C, Wessling F, Friedrich CM. Proof-of-property: A lightweight and scalable blockchain protocol. In: Proc. of the 1st Int'l Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB). Gothenburg: ACM, 2018. 48–51. [doi: 10.1145/3194113.3194122]

[42] Kim T, Noh J, Cho S. SCC: Storage compression consensus for blockchain in lightweight IoT network. In: Proc. of the 2019 IEEE Int'l Conf. on Consumer Electronics (ICCE). Las Vegas: IEEE, 2019. 1–4. [doi: 10.1109/ICCE.2019.8662032]

[43] Luu L, Narayanan V, Zheng CD, Baweja K, Gilbert S, Saxena P. A secure sharding protocol for open Blockchains. In: Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security (CCS). Vienna: ACM, 2016. 17–30. [doi: 10.1145/2976749.2978389]

[44] Zamani M, Movahedi M, Raykova M. RapidChain: Scaling blockchain via full sharding. In: Proc. of the 2018 ACM SIGSAC Conf. on Computer and Communications Security (CCS). Toronto: ACM, 2018. 931–948. [doi: 10.1145/3243734.3243853]

[45] Kokoris-kogias E, Jovanovic P, Gasser L, Gailly N, Syta E, Ford B. OmniLedger: A secure, scale-out, decentralized ledger via sharding. In: Proc. of the 2018 IEEE Symp. on Security and Privacy (SP). San Francisco: IEEE, 2018. 583–598. [doi: 10.1109/SP.2018.000-5]

[46] Jiang YM, Wang CX, Huang Y, Long SY, Huo YL. A cross-chain solution to integration of IoT tangle for data access management. In: Proc. of the 2018 IEEE Int'l Conf. on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). Halifax: IEEE, 2018. 1035–1041. [doi: 10.

1109/Cybermatics_2018.2018.00192]
[47] Hassanzadeh-Nazarabadi Y, Küpçü A, Özkasap Ö. LightChain: A DHT-based blockchain for resource constrained environments. arXiv: 1904.00375, 2019.
[48] Aspnes J, Shah G. Skip graphs. ACM Trans. on Algorithms, 2007, 3(4): 37-es. [doi: 10.1145/1290672.1290674]
[49] Androutsellis-Theotokis S, Spinellis D. A survey of peer-to-peer content distribution technologies. ACM Computing Surveys, 2004, 36(4): 335–371. [doi: 10.1145/1041680.1041681]
[50] Wang YW. A blockchain system with lightweight full node based on dew computing. Internet of Things, 2020, 11: 100184. [doi: 10.1016/j.iot.2020.100184]
[51] Wang YW. Cloud-dew architecture. Int'l Journal of Cloud Computing, 2015, 4(3): 199–210. [doi: 10.1504/IJCC.2015.071717]
[52] Wang YW. Definition and categorization of dew computing. Open Journal of Cloud Computing, 2016, 3(1): 1–7. [doi: 10.1109/MCC.2016.12]
[53] Ren YJ, Yan L, Jian Q, Leng Y, Qi J, Sharma PK, Wang J, Almakhadmeh Z, Tolba A. Multiple cloud storage mechanism based on blockchain in smart homes. Future Generation Computer Systems, 2021, 115: 304–313. [doi: 10.1016/j.future.2020.09.019]
[54] Dennis R, Owenson G, Aziz B. A temporal blockchain: A formal analysis. In: Proc. of the 2016 Int'l Conf. on Collaboration Technologies and Systems (CTS). Orlando: IEEE, 2016. 430–437. [doi: 10.1109/CTS.2016.0082]
[55] Shahid AR, Pissinou N, Staier C, Kwan R. Sensor-chain: A lightweight scalable blockchain framework for Internet of Things. In: Proc. of the 2019 Int'l Conf. on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). Atlanta: IEEE, 2019. 1154–1161. [doi: 10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00195]
[56] Sagirlar G, Carminati B, Ferrari E, Sheehan JD, Ragnoli E. Hybrid-IoT: Hybrid blockchain architecture for Internet of Things—PoW Sub-blockchains. In: Proc. of the 2018 IEEE Int'l Conf. on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). Halifax: IEEE, 2018. 1007–1016. [doi: 10.1109/Cybermatics_2018.2018.00189]
[57] Dorri A, Kanhere SS, Jurdak R, Gauravaram P. LSB: A lightweight scalable blockchain for IoT security and anonymity. Journal of Parallel and Distributed Computing, 2019, 134: 180–197. [doi: 10.1016/j.jpdc.2019.08.005]
[58] Dorri A, Kanhere SS, Jurdak R. Towards an optimized blockchain for IoT. In: Proc. of the 2nd IEEE/ACM Int'l Conf. on Internet-of-Things Design and Implementation (IoTDI). Pittsburgh: IEEE, 2017. 173–178.
[59] Dorri A, Kanhere SS, Jurdak R, Gauravaram P. Blockchain for IoT security and privacy: The case study of a smart home. In: Proc. of the 2017 IEEE Int'l Conf. on Pervasive Computing and Communications Workshops (PerCom workshops). Kona: IEEE, 2017. 618–623. [doi: 10.1109/PERCOMW.2017.7917634]
[60] Dorri A, Kanhere SS, Jurdak R. Blockchain in Internet of Things: Challenges and solutions. arXiv:1608.05187, 2016.

附中文参考文献:

[1] 斯雪明, 陈文光. 区块链与数字货币技术专题前言. 软件学报, 2019, 30(6): 1575−1576. http://www.jos.org.cn/1000-9825/5747.htm [doi: 10.13328/j.cnki.jos.005747]
[9] 李董, 魏进武. 区块链技术原理、应用领域及挑战. 电信科学, 2016, 32(12): 20–25.
[10] 张亮, 刘百祥, 张如意, 江斌鑫, 刘一江. 区块链技术综述. 计算机工程, 2019, 45(5): 1–12. [doi: 10.19678/j.issn.1000-3428.0053554]
[13] 武传坤. 物联网安全关键技术与挑战. 密码学报, 2015, 2(1): 40–53. [doi: 10.13686/j.cnki.jcr.000059]

谢晴晴(1990－), 女, 博士, 讲师, CCF 专业会员, 主要研究领域为应用密码学, 区块链技术.

董凡(1995－), 男, 硕士生, 主要研究领域为轻量级区块链技术.