

运行于边侧物联网设备的区块链轻型应用研究与实现

衡星辰¹, 普钢², 李零³, 陈达⁴, 张劲松⁴, 周智勋⁴, 姜文喆³

- 南方电网数字电网集团有限公司, 广州 510000
- 云南电网有限责任公司, 昆明 650011
- 云南电网有限责任公司昆明供电局, 昆明 650011
- 云南云电同方科技有限公司, 昆明 650011

摘要 介绍了目前解决区块链存储问题的研究进展及解决方案。结合智慧用电平台边缘侧区块链的部署情况, 在区块链轻型应用方面, 采用分布式哈希表(DHT)分布式区块链存储方式实现边侧区块链数据存储。通过边侧区块链节点历史区块数据定时备份、共识算法多样选择和区块链镜像裁剪等方法配合实现边侧区块链节点的轻量化。指出随着电力物联网技术应用场景的丰富和持续发展, 仍需持续深入研究, 以寻找更加优化的算法模型和解决方案。

关键词 区块链; 边缘节点; 分布式哈希表; 链下存储; 智慧用电

随着物联网技术的快速发展, 万物互联有了越来越多的实际应用, 在物联网设备呈爆炸式增长现状下, 边缘计算的出现实现了物联网设备数据的低时延和高智能化处理, 但是物联网仍然存在安全性和匿名性等隐患。

区块链本质是一种点对点的分布式账本技术, 密码算法是该项技术的基础。自2008年比特币提出以来, 区块链技术首次从技术层面上解决了中心化模型所固有的安全问题, 其中的哈希链、时间戳、共识算法等机制可以有效地保证数据的可追溯、不

可篡改及一致性^[1-3]。在物联网中将区块链的这些特性与边缘计算结合, 可以有效解决隐私和安全问题, 因此边缘计算与区块链技术的融合成为目前研究和应用的热点。

现有物联网系统中, 物联网设备常被用作边缘节点, 其存在增速快、自身体量小、算力和存储不足等诸多问题, 而在物联网边云计算模型中, 原始数据主要由边缘层收集, 因此区块链一般部署在边缘层, 但是边缘层的硬件资源条件相比云端资源, 在资源供给方面受到限制, 部署区块链会给边缘节点

收稿日期: 2023-09-27; 修回日期: 2023-12-29

作者简介: 衡星辰, 教授级高级工程师, 研究方向为电网数字化, 电子邮箱: hengxc@csg.cn

引用格式: 衡星辰, 普钢, 李零, 等. 运行于边侧物联网设备的区块链轻型应用研究与实现[J]. 科技导报, 2024, 42(9): 60-66;

doi: 10.3981/j.issn.1000-7857.2022.07.01103

带来比较大的存储和计算压力,从区块链的应用开发角度看,区块链的存储可扩展性成为区块链应用落地的一大问题^[4]。

1 区块链轻型应用的研究方向

针对区块链面临的存储可扩展性问题,现有研究提出了多种区块链轻型应用的解决方案,其阐述了不同的存储模型及基本原理,从数据存储方式、节点间相互关系等角度进行了差异化分析,总体上,目前提高区块链存储可扩展性的方法有2大类别^[5],链下存储和链上存储(图1)。

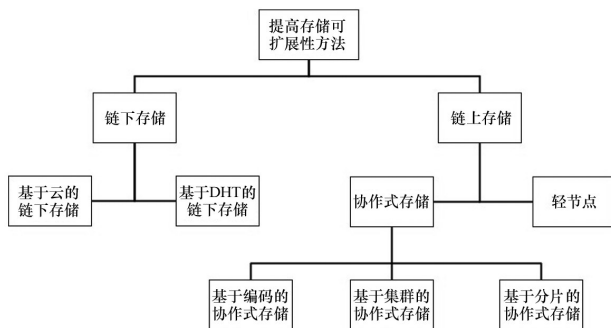


图1 提高区块链存储可扩展性的方法

1.1 链上协作式存储

根据使用技术的不同,链上协作式存储可分为基于编码的协作式存储、基于集群的协作式存储和基于分片的协作式存储。Dai等^[6]提出的分布式存储框架基于网络编码,通过对多个数据包的编码进行融合从而提高单次传输的信息量;也有研究人员基于纠错码提出一种降低节点存储负担的LS(low storage)节点,在不需存储完整区块链的情况下,仍然可以验证完整区块链^[7]。Xu等^[8]为解决区块链存储挑战,引入一个称为共识单元(CU)的新概念,将不同的节点组织成一个单元,并让它们在系统中存储至少1个区块链数据的副本。基于这一思想,进一步定义块分配优化(BAO)问题,该问题确定块的最佳分配,以充分利用存储空间并最小化查询成本。分片协作式存储的技术基础是将节点分成更小的单位并对其进行并行地处理和维持,Elastico是第1个基于分片的公有链共识协议,其分片后的

每个节点仍然需要存储完整的账本^[9],后续OmniLedger进行改进提出定期改组分片策略^[10],Yoo等^[11]提出了静态分片区块链模型。针对分片技术难以保证跨片交易安全性的问题,Zamani等^[12]使用RandHound和VRF协议将验证者随机分配到不同的分片中,每个分片中的验证者验证了分片的有效性且保证了跨分片交易的安全性。Yu等^[13]提出了基于智能合约的区块链分片方案Chainspace。总体来说,以上方式各有特点,但实际应用于不同场景时仍然面临存储膨胀的问题。

1.2 轻节点

轻节点与全节点是一对相反的概念,轻节点不需要存储完整账本,在新的区块出现时,只需要下载区块头信息。传统的Simplified Payment Verification(SPV)轻节点^[14]需要存储每个区块的区块头,并且需要信赖全节点验证支付和交易,因此很多研究人员从不同角度对传统轻节点做了改进,例如,EPBC轻节点在需要完整区块时才会请求全节点,其他情况只需存储大小定长的区块总结值^[15];SCC用Merkle树的方式对最新区块的前一区块链进行压缩,使其与完整的账本保持一致性,当没有空闲空间存储完整账本时,可以删除旧区块,存储和压缩最新区块^[16]。

1.3 基于云的链下存储

基于云的链下存储是通过把实际数据存储到云端,而把数据的散列值保存在区块链中,从而解决区块链的存储扩展性问题。私有链Chameleon架构^[17]就是一种典型的基于云的链下存储架构,原理是将最近一段时期的数据存储在区块链中,以前的数据存储在网上,为实现数据的一致性,会将最新的一个区块的散列值保存至区块链中。Yu等^[18]提出了一个分层边缘云区块链结构LayerChain。LayerChain考虑到不同类型节点的计算能力和存储空间具有较大差异,将来自工业物联网(IIoT)设备的区块链交易数据分别存储在云区块链层、边缘区块链层和IIoT设备层3层结构中。

1.4 基于分布式哈希表的链下存储

分布式哈希表(distributed hash table, DHT)是一种分布式存储方法^[19],原理是在无中心服务器的

情况下,每个节点负责一个小范围内的路由,同时存储一小部分数据,从而实现 DHT 网络的寻址和存储。Li 等^[20]利用以上理论,开展了针对物联网大规模数据存储的研究,提出了一种适用于大规模物联网数据的存储与保护方案。该方案将数据转发到链下的 DHT 存储系统中,当边缘端实体需要访问数据时,在区块链中广播带公钥的数据请求,并由区块链节点负责对实体的认证工作(图 2)。

2 智慧用电平台边侧区块链轻型应用

2.1 边侧区块链部署方式

在智慧用电平台中,边缘侧面临网络环境和物理存储的限制,可能存在台区间物理距离远,且台区间组网成本过高等问题,导致孤立台区存在,此时可在 1 个台区上虚拟多个节点,以满足区块链运行;对于台区相对集中的区域,可以采用多个台区组网的方式,进行区块链部署,在每个台区部署 1 个节点。

单台区孤链这种方式适用于台区较为孤立,周围没有相邻台区,与台区的组网成本较高,为了满足边缘设备采集数据的可信存储,以及计算过程的

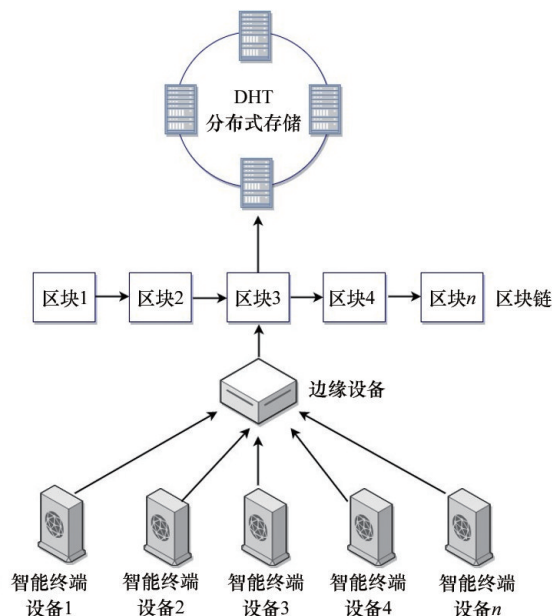


图 2 基于边缘计算和区块链的物联网数据存储方案

可信,需要将区块链部署到台区的 1 台设备上,并在同一台设备上组链和共识。多台区组网方式适用于台区之间物理距离相隔较近,组网难度不大,组网成本低的台区之间。智慧用电平台边缘侧区块链的部署方案如图 3 所示。

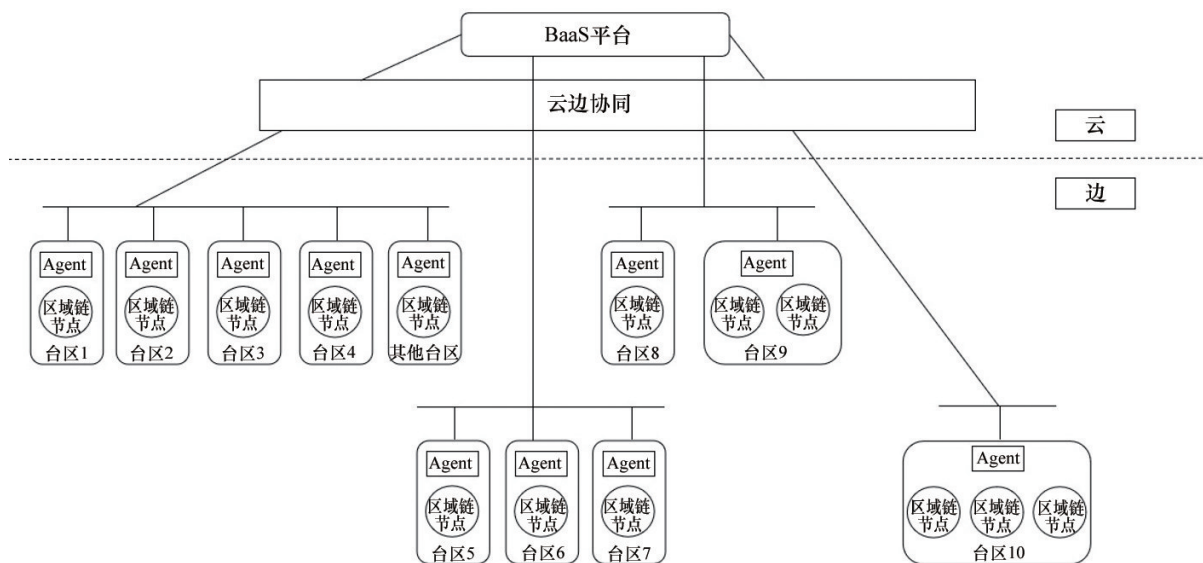


图 3 边缘侧区块链部署方案

2.2 轻型应用的实现

目前,主流台区智能设备的配置普遍较低,CPU(中央处理器)主频为1 G左右,内存为1~3 G,默认存储空间为8 G左右。与传统的部署在云端服务器的区块链网络不同,部署在低配边缘侧终端上的区块链网络存在显而易见的存储瓶颈,由于边侧终端的默认存储容量较小,需要外部插卡扩展,主流扩展只支持存储容量为16、64、128 GB的存储卡,实际可用于存储区块数据存储的空间分别为10、58、122 GB左右,因此必须从应用层面尽可能节省存储空间。

当前的轻量化研究,主要针对算法、存储、操作系统镜像其中一项进行优化。采用联合优化方案,

不仅可以大幅度提高系统的工作效率,同时也可以提高链上存储的存储利用率。首先,通过对共识算法的选择,采取算法更加便捷、产生数据量更少的算法,并通过DHT实现链上存储,降低单个节点存储压力;其次,对各边缘侧节点的存储数据采取数据裁剪,定期上传和清理节点内部数据的措施,降低所需要的存储空间,从而实现数据和算法双方轻量化。

本研究根据智慧用电平台边缘侧区块链的部署情况,在区块链轻型应用方面,选择基于DHT的链下存储,结合数据裁剪、镜像裁剪并选择适合的共识算法,实现边侧物联网设备的区块链轻型应用(图4)。

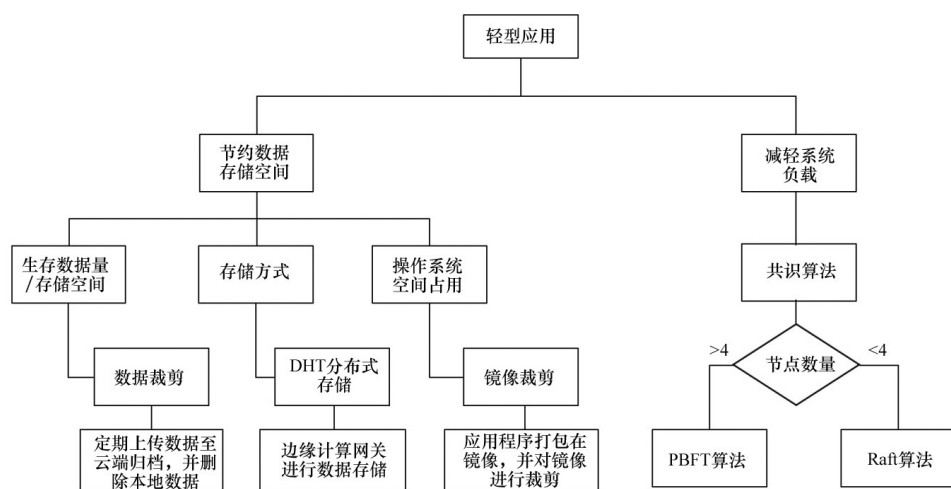


图4 轻型应用实现流程

2.2.1 DHT存储实现

每个台区即是所属边缘侧链的区块链节点,而多个台区通过所属的边缘计算网关,构成了DHT分布式存储的基础节点单元。处于DHT分布节点位置的边缘计算网关,存储着下属台区所对应边缘侧链的区块数据。相应地,边缘侧链就是依靠 n 个边缘计算网关的支撑,实现了DHT存储的架构(图3)。

每个边缘计算网关,将从台区采集的数据进行结构化处理,并完成上链和存储。具体地,采用元数据链上存储,原始数据链下存储的方式,即DHT存储方式。原始数据通过一些字段对其特征进行描述,形成元数据,其中包含数据类型、原始存储节

点、签名等信息。

2.2.2 边侧区块链数据裁剪

对于存储空间有限的边缘台区设备,存量很快便会达到存储峰值,因此平台中将采用边缘区块链节点数据定期归档的方式,通过将边侧区块链节点中的历史区块数据归档至云端数据归档仓库,并完成已归档数据的删除,从而达到轻量化边侧区块链节点的目的(图5)。

边缘侧链由多个台区智能设备组成,由于区块链的去中心化特点,每个台区的区块链节点都将存储其他台区节点采集的数据,假设4个台区组成边缘侧链,每个台区下存在200户电表,则每次电量

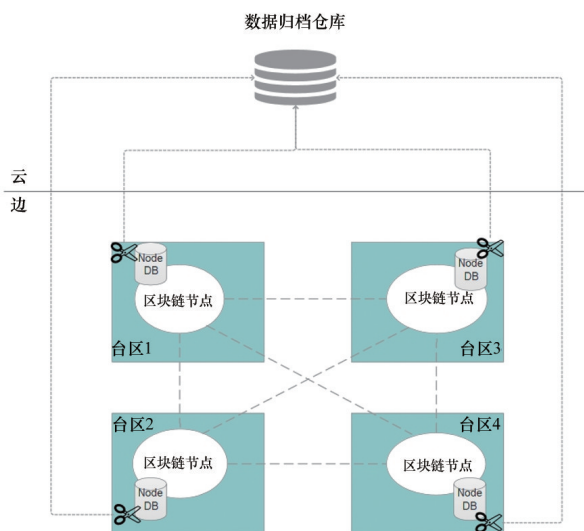


图5 数据裁剪归档图

采集,单个区块链节点上将存储800条电费计算数据。表1展示了台区终端全量数据存储所占空间和所能存储时间信息。

从表1可以看出,通过增加边侧区块链数据裁剪方法,可以大幅度减少边缘节点的存储压力,其中日存储量在归档频率增加后,分别为原来的1/5和1/12,单个节点上所能存储的信息时间也明显增加。

2.2.3 共识算法选择

现有研究发现共识算法也是制约物联网设备能耗开销的最主要问题,在一般的物联网应用场景下,采用轻量级的共识协议可以有效降低物联网设备计算、通信和存储的负担。理论上,区块链网络中的节点越多,则区块链网络的健壮性越强,即允许的出错节点数越多。智慧用电平台将采用Raft

表1 台区终端全量数据存储空间及时间信息

归档频率	日存储使用	所能存储时间(16 GB)	所能存储时间(64 GB)	所能存储时间(128 GB)
1 d	3.29 GB	最近3天	最近17天	最近35天
5 h	673.92 MB	最近15天	最近85天	最近175天
2 h	224.64 MB	最近45天	最近255天	最近525天

共识和PBFT共识2种共识算法。Raft共识其实是一种分布式一致性算法,只允许节点宕机而不允许存在恶意节点;PBFT算法允许存在恶意节点和宕机节点,PBFT算法最少需要4个节点才能完成共识。

由于边端设备的计算资源和存储资源有限,并且不可随时进行扩容,边缘端需要削减区块链共识的成本和部署资源的成本。根据区块链多账本、多备份、分布式存储的特点,每个节点存储的数据量是(单个账本大小×节点数),所以在多个台区组网场景下,将采用4节点组成的PBFT算法进行共识,防止恶意节点对系统破坏的同时,降低存储成本;在单台区孤链部署方式下,平台将采用Raft共识,部署3节点的区块链,这种共识机制消耗计算资源相对PBFT共识较少。

2.2.4 基础镜像裁剪

由于区块链应用程序打包在Docker镜像中,对区块链镜像进行裁剪也能有效降低存储空间,智能用电平台使用Ubuntu 18.04 ARM架构系统,基

于裁剪后的Ubuntu18.04操作系统制作区块链镜像,有效地将镜像从400 M+裁剪到了200 M左右,较大程度上节省了边端设备的有限存储空间。

2.3 轻型化效果

将所提出的区块链轻型应用试验于南方电网智能电网试验平台约3个月,并与未采用轻型应用的智能电网进行对比。该试验平台拥有100个边缘台区(即区块链节点),平均每个台区下辖300台电表。采用的轻型应用在采用数据裁剪时,会对边缘节点产生的每个月的数据进行数据归档和删除。通过表2和表3可以看出,在系统能耗不明显增加的情况下,采用区块链轻型应用的智能电网在云端数据存储量、边缘节点平均数据存储量和系统存储数据总量上表现均优于传统智能电网;并且随时间增加,传统智能电网边缘节点存储的数据量逐渐增加,存储压力增大,而采用区块链轻型应用的智能电网由于会对边缘节点存储的数据量进行归档和删除,所以存储压力明显减小。

表2 系统存储表现对比

时长/月	云端数据存储量/GB		边缘节点平均数据存储量/GB		系统存储数据总量/GB	
	传统智能 电网	采用区块链轻型 应用的智能电网	传统智能 电网	采用区块链轻型 应用的智能电网	传统智能 电网	采用区块链轻型 应用的智能电网
1	2318	1831	23	18	4636	3662
2	4844	3729	48	19	9688	7458
3	7247	5644	72	18	14494	11288

表3 系统负载对比

时长/月	平均每天系统计算、通信、存储能耗/kW	
	传统智能电网	采用区块链轻型 应用的智能电网
1	7987	8136
2	8239	8417
3	8056	8185

3 结论

通过对比目前已有的区块链轻型应用研究成果及解决方案,对链上协作式存储,轻节点,基于云的链下存储和基于DHT的链下存储的基本原理、特点和优缺点进行了分析。结合本智慧用电平台边缘侧区块链的部署情况,在区块链轻型应用方面,采用元数据链上存储,原始数据链下存储的方式,即DHT存储方式实现边侧区块链数据存储;同时还通过边侧区块链节点历史区块数据定时备份至云端、删除已归档数据的方式达到轻量化边侧区块链节点的目的;此外考虑到不同台区组网方式的不同,在共识算法的选择上灵活应用Raft共识和PBFT共识2种共识算法,减少边侧计算资源消耗;最后利用区块链镜像进行裁剪也有效地降低了存储空间。

通过上述方法实现了智慧用电平台边侧物联网设备的区块链轻型应用,目前该应用已经在云南电网昆明市下辖500个台区开展试点应用,各项指标与试验指标相当,数据访问响应时间降低,数据安全性得到了保障,但是随着电力物联网技术应用场景的丰富和持续发展,边侧区块链和边缘计算融合时所遇到的存储挑战将持续存在,因此本课题仍需持续深入研究,以寻找更加优化的算法模型和解决方案。

参考文献 (References)

- [1] 邵奇峰, 金澈清, 张召, 等. 区块链技术: 架构及进展[J]. 计算机学报, 2018, 41(5): 969-988.
- [2] Karagiannis T, Broido A, Faloutsos M, et al. Transport layer identification of P2P traffic[C]//Proceedings of the 4th ACM SIGCOMM Conference on Internet Measurement. New York: ACM, 2004: 121-134.
- [3] 夏清, 窦文生, 郭凯文, 等. 区块链共识协议综述[J]. 软件学报, 2021, 32(2): 277-299.
- [4] Yang W L, Aghasian E, Garg S, et al. A survey on blockchain-based Internet service architecture: Requirements, challenges, trends, and future[J]. IEEE Access, 2019, 7: 75845-75872.
- [5] 孙知信, 张鑫, 相峰, 等. 区块链存储可扩展性研究进展[J]. 软件学报, 2021, 32(1): 1-20.
- [6] Dai M J, Zhang S L, Wang H, et al. A low storage requirement framework for distributed ledger in blockchain[J]. IEEE Access, 2018, 6: 22970-22975.
- [7] Perard D, Lacan J, Bachy Y, et al. Erasure code-based low storage blockchain node[C]//Proceedings of IEEE International Conference 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). Piscataway, NJ: IEEE, 2018: 251-257.
- [8] Xu Z H, Han S Y, Chen L. CUB, a consensus unit-based storage scheme for blockchain system[C]//Proceedings of IEEE 34th International Conference on Data Engineering (ICDE). Piscataway, NJ: IEEE, 2018: 25-36.
- [9] Luu L, Narayanan V, Zheng C D, et al. A secure sharding protocol for open blockchains[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2016: 17-30.
- [10] Kokoris-Kogias E, Jovanovic P, Gasser L, et al. OmniLedger: A secure, scale-out, decentralized ledger via sharding[C]//Proceedings of IEEE Symposium on Security and Privacy. New York: ACM, 2016: 1-16.

- ty and Privacy (SP). Piscataway, NJ: IEEE, 2018: 451–467.
- [11] Yoo H, Yim J, Kim S. The blockchain for domain based static sharding[C]//Proceedings of 17th IEEE International Conference on Trust, Security and Privacy In Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE). Piscataway, NJ: IEEE, 2018: 1689–1692.
- [12] Zamani M, Movahedi M, Raykova M. RapidChain: Scaling blockchain via full sharding[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2018: 931–948.
- [13] Yu B, Li X F, Zhao H. Virtual block group: A scalable blockchain model with partial node storage and distributed hash table[J]. The Computer Journal, 2020, 63(10): 1524–1536.
- [14] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. (2009-03-16) [2023-05-12]. <http://bitcoin.org/bitcoin.pdf>.
- [15] Xu L, Chen L, Gao Z M, et al. EPBC: Efficient Public Blockchain Client for lightweight users[C]//Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers. New York: ACM, 2017: 1–6.
- [16] Kim T, Noh J, Cho S. SCC: Storage compression consensus for blockchain in lightweight IoT network[C]//Proceedings of IEEE International Conference on Consumer Electronics (ICCE). Piscataway, NJ: IEEE, 2019: 512–523.
- [17] He G B, Su W, Gao S. Chameleon: A scalable and adaptive permissioned blockchain architecture[C]//Proceedings of 1st IEEE International Conference on Hot Information-Centric Networking (HotICN). Piscataway, NJ: IEEE, 2018: 186–193.
- [18] Yu Y, Liu S M, Yeoh P L, et al. LayerChain: A hierarchical edge-cloud blockchain for large-scale low-delay industrial Internet of Things applications[J]. IEEE Transactions on Industrial Informatics, 2021, 17(7): 5077–5086.
- [19] Androutsellis-Theotokis S, Spinellis D. A survey of peer-to-peer content distribution technologies[J]. ACM Computing Surveys, 2004, 36(4): 335–371.
- [20] Li R N, Song T Y, Mei B, et al. Blockchain for large-scale Internet of Things data storage and protection[J]. IEEE Transactions on Services Computing, 2019, 12(5): 762–771.

Blockchain lightweight application research and implementation as applied to edge IoT devices

HENG Xingchen¹, PU Gang², LI Ling³, CHEN Da⁴, ZHANG Jinsong⁴, ZHOU Zhixun⁴, JIANG Wenzhe³

1. China Southern Power Grid Digital Power Grid Group Co., Ltd., Guangzhou 510000, China

2. Yunnan Power Grid Co., Ltd., Kunming 650011, China

3. Kunming Power Supply Bureau of Yunnan Power Grid Co., Ltd., Kunming 650011, China

4. Yunnan Yundian Tongfang Technology Co., Ltd., Kunming 650011, China

Abstract This paper first introduces various researches and solutions to solve the problem of blockchain storage at present. Secondly, combined with the deployment of blockchain on the edge side of the intelligent electricity platform, DHT distributed blockchain storage is adopted. At the same time, regular backup of historical side block data, multiple selection of consensus algorithms, and blockchain mirror cutting are used to realize the lightweight of side blockchain nodes. Finally, it is pointed out that with the enrichment and continuous development of application scenarios of the electricity internet of things, this topic still needs further research to find more optimized algorithm models and solutions.

Keywords blockchain; edge node; distributed hash table; off-chain storage; intelligent electricity platform ●



(责任编辑 傅雪)