软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2021,32(1):1−20 [doi: 10.13328/j.cnki.jos.006111]

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

区块链存储可扩展性研究进展*

孙知信[1,2], 张 鑫[1,2], 相 峰[3], 陈 露[1,2]

[1](南京邮电大学 国家邮政局邮政行业技术研发中心(物联网技术),江苏 南京 210003)

[2](宽带无线通信与传感网技术教育部重点实验室(南京邮电大学),江苏 南京 210003)

[3](物流信息互通共享技术及应用国家工程实验室(圆通速递股份有限公司),上海 201705)

通讯作者: 孙知信, E-mail: sunzx@njupt.edu.cn

摘 要: 区块链是一种结合分布式共识、加密、时间戳等方法,在不依赖任何第三方中心化机构的情况下,实现点对点交易、协调以及协作的技术.近几年,区块链技术的不断发展引起了产业界和学术界的极大兴趣.但是,区块链的存储可扩展性问题,提高了区块链设备的门槛,成为了区块链应用落地的瓶颈.介绍了区块链的基本原理和存储模型,分析了当前区块链所面临的存储问题;然后,针对区块链存储可扩展性问题,从链下存储和链上存储这两条技术路线出发,论述了主要的解决方案的原理与思路;最后,总结了提高区块链存储可扩展性的技术研究进展,指出了当前解决方案所面临的问题,为未来的研究工作提供了方向.

关键词: 区块链;比特币;存储可扩展性;存储优化

中图法分类号: TP311

中文引用格式: 孙知信,张鑫,相峰,陈露.区块链存储可扩展性研究进展.软件学报,2021,32(1):1−20. http://www.jos.org.cn/1000-9825/6111.htm

英文引用格式: Sun ZX, Zhang X, Xiang F, Chen L. Survey of storage scalability on blockchain. Ruan Jian Xue Bao/Journal of Software, 2021,32(1):1−20 (in Chinese). http://www.jos.org.cn/1000-9825/6111.htm

Survey of Storage Scalability on Blockchain

SUN Zhi-Xin[1,2], ZHANG Xin[1,2], XIANG Feng[3], CHEN Lu[1,2]

[1](Technology Research and Development Center of Postal Industry of State Post Bureau (Technology of Internet of Things), Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

[2](Key Laboratory of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education (Nanjing University of Posts and Telecommunications), Nanjing 210003, China)

[3](National Engineering Laboratory for Logistics Information Technology, YTO Express Company Ltd., Shanghai 201705, China)

Abstract: Blockchain is a technology that combines distributed consensus, encryption, timestamps, etc., to achieve peer-to-peer trading, coordination, and collaboration without relying on any third-party centralization organization. In recent years, the rapid development of blockchain technology has aroused great interest from industry and academia. However, the problem of storage scalability of blockchain has increased the threshold of blockchain devices and has become a bottleneck for blockchain applications. This paper introduces the basic principle and storage model of blockchain, and analyzes the storage problems faced by current blockchain. Then, for the problem of blockchain storage scalability, from two perspectives of off-chain storage and on-chain storage, the principles and ideas of the existing solutions are discussed. Finally, based on the research progress of the storage scalability of blockchain and the problems of these solutions, directions are provided for future research work.

Key words: blockchain; Bitcoin; storage scalabitity; storage optimization

* 基金项目: 国家自然科学基金(61672299, 61972208); 江苏省研究生科研与实践创新计划(SJCX19_0245)

Foundation item: National Natural Science Foundation of China (61672299, 61972208); Postgraduate Research & Practice Innovation Program of Jiangsu Province (SJCX19_0245)

收稿时间: 2019-10-31; 修改时间: 2020-02-16, 2020-04-19; 采用时间: 2020-06-24; jos 在线出版时间: 2020-07-27

区块链技术起源于 2008 年,由一名叫中本聪(Satoshi Nakamoto)的日本人在《比特币:一个点对点电子现金系统》[1]中首次提出比特币的概念.比特币等数字加密货币的核心技术便是区块链技术.2015 年之前,大家更关注的是比特币的“币”而不是底层的区块链技术.2015 年,以太坊(Ethereum)[2]的出现以及之后的日渐成熟,使得区块链这一概念为更多人所了解和研究,并且朝着更加光明和广泛的应用场景不断发展.

区块链技术的不断发展,给信息共享[3]、版权保护[4]、供应链[5]、物联网[6,7]、医疗[8]、社交[9]以及文件存储[10]等领域提供了更多的可能.但是与传统货币相似,区块链技术同样存在三元悖论,即去中心化、安全性和可扩展性,三者只能得其二.当追求安全性和去中心化时,则无法顾及可扩展性;当追求安全性和可扩展性时,则无法实现去中心化;当追求去中心化和可扩展性时,则需要牺牲安全性.比特币和以太坊都是优先追求去中心化和安全性,而牺牲可扩展性.比特币的吞吐量为每秒处理 7 次交易,以太坊则是每秒 10~20 次.可扩展性已成为区块链应用落地的最大瓶颈.区块链可扩展性可分为性能可扩展性和功能可扩展性,其中,性能可扩展性包含吞吐量扩展、存储扩展以及网络扩展:吞吐量扩展与每个区块中的交易数及产生两个区块的时间间隔有关;存储扩展与区块链生成的数据有关;网络扩展与区块链网络中的数据传输有关[11].

当前,区块链的应用领域[12]可分为:(1) 加密数字货币领域,如比特币、以太币等;(2) 数据记录及管理领域,如数据存储[13]、数据鉴证[14]等;(3) 信息安全领域,如认证技术[15]、访问控制[16]等;(4) 其他领域,如共享经济[17]、智能交通[18]和能源网络[19]等等.区块链在不同场景下的应用,都因高冗余存储(每个节点存储一份完整的数据)增强了数据的公开性、透明性,提高了系统的可用性;但另一方面,每个节点都需要同步最新的账本,这会给区块链带来性能问题和巨大的存储压力.在加密数字货币比特币中,节点需要对全球账本进行同步,才能通过检索本地副本以验证交易的发起者是否拥有足够的“币”发起这笔交易.如图 1 所示,截至 2019 年第 2 季度末,比特币大小约为 221.29GB.潜在的用户如果没有足够的存储空间,那么它将无法加入到区块链网络中作为全节点来验证新交易.当区块链试图解决物联网领域的问题时,会遇到物联网设备作为区块链节点时节点数量增速快、自身体量小以及计算、存储等能力不足[20]的问题.从应用开发的角度看,基于区块链的应用开发需要满足可扩展性要求和一致性要求[21].区块链的一致性是指存储在区块链不同节点中的数据副本的取值必须一致,它通过共识算法、数据的可靠传输、高冗余存储和加密技术来实现[22].由于高冗余存储会增加节点的存储压力,导致存储可扩展性问题.因此,如果需要高一致性,那么就会降低存储可扩展性.综上,从区块链的应用领域和区块链的应用开发角度来看,区块链的存储可扩展性问题已成为制约区块链应用落地的一大问题[23].

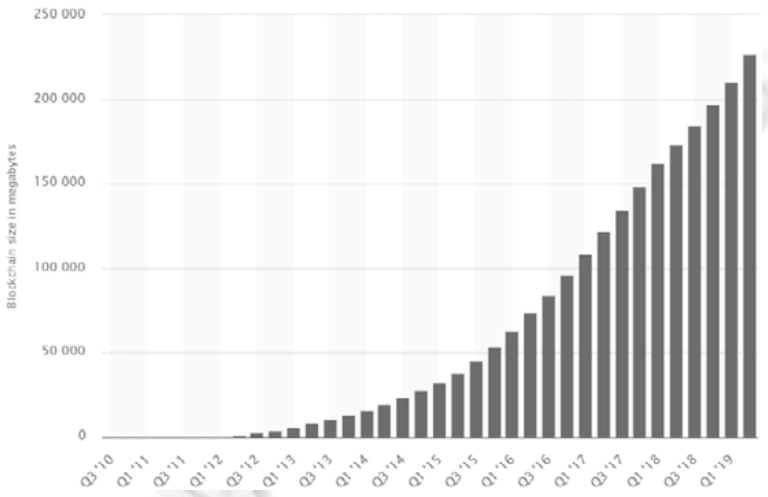

Fig.1 Bitcoin blockchain size from 2010 to 2019 in MBytes

图 1 从 2010 年~2019 年比特币区块链的大小(以 MBytes 为单位)

潘晨等学者[24]从性能扩展和功能扩展两个角度,详细介绍了当前 3 类主流提升区块链吞吐量的技术和 4

类扩展区块链功能的技术.Xie 等学者[11]给出了目前区块链吞吐量、存储以及网络这 3 方面所面临的挑战,并介绍了一些解决办法.Zhang 团队[25]提出了一种低开销的区块链存储架构,架构包含 3 种机制,分别是将原始数据转换为关键词的语义信息模板机制、将区块链账本划分为多个切片的滞后数据切片机制以及将低价值数据存储到中央数据库的历史数据归档机制.Wang 团队[26]建立了关于空间占用率和平均搜索时间之间的数学模式,并设计了一个数据分配策略,以实现在区块链网络中节约存储空间.现有文献一类是应对区块链存储可扩展性问题,提出了相应的解决方案;另一类则是对区块链可扩展性的综述,虽然归纳得较为完整,但更偏重性能、网络、吞吐量等方面的可扩展性.两者都没有对区块链的存储可扩展性问题进行详细、系统的分析,没有体现出在解决存储可扩展性问题时,数据存储方式、节点间的相互关系等角度的差异分析.本文首先介绍区块链所面临的存储可扩展性问题和区块链的存储模型,然后系统性地对链上存储(on-chain storage)和链下[27]存储(off-chain storage)的基本原理、现存问题进行了分析(如图 2 所示),并对未来的发展加以展望,希望能给当前及未来的相关研究工作提供一定的参考与帮助.

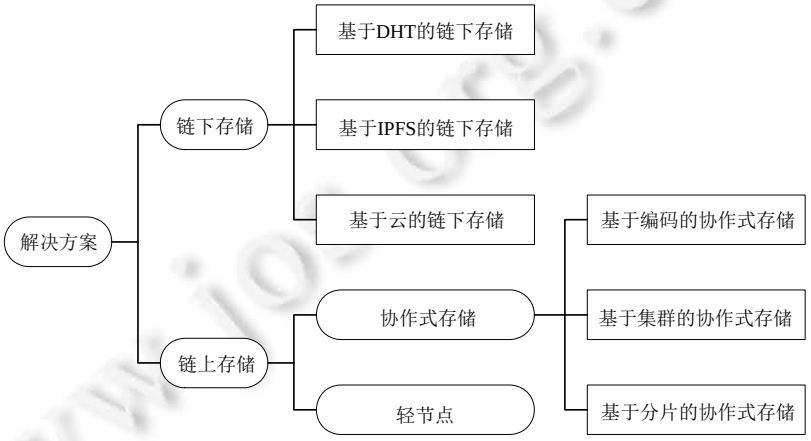

Fig.2 Solutions to improve the storage scalability of blockchain

图 2 提高区块链存储可扩展性方法分类

本文第 1 节概述区块链技术和区块链的存储模型.第 2 节和第 3 节分别综述目前提升区块链存储可扩展性的两大类解决方案——链下存储和链上存储.第 4 节指出当前解决方案所面临的问题,并给出未来可能的研究方向.

1 区块链概述和存储模型

1.1 区块链概述

区块链是一种结合分布式共识、加密、时间戳以及经济激励等方法,在一个完全无信任的环境下,实现去中心化的点对点交易、协调与协作的技术[7].区块链技术有许多优点,例如去中心化、安全性、匿名性、透明性以及自动化等.去中心化的特性解决了在传统中心化场景下成本高昂、效率低下、安全性不可靠等问题[28].区块链将前一块的 hash 值添加至后一区块的区块头中,从而实现链式结构.当经过 6 个区块确认后,这笔交易几乎没有被破解的可能性.通过使用匿名地址并将现实世界地址或标识隐藏,区块链实现了匿名的特性.在中本聪设计的区块链中,任何人都可以查询区块链世界中的每一笔交易信息,从而实现了透明性.区块链技术可以提供灵活的编程特性,支持用户创建可在区块链上自动运行的高级程序,包括智能合约、加密货币及去中心化应用(DApp).通过共识算法[29],区块链中的节点们确保了数据的一致性.

区块链根据其应用场景或开放程度[30]可分为 3 种:公有链(public blockchain)、联盟链(consortium blockchian)和私有链(private blockchain).三者的差异主要体现在网络结构(是否完全去中心化)、共识机制、激

励机制等方面.根据不同场景下的信任构建方式[31],区块链可分为“非许可链(permissionless blockchain)”和“许可链(permissioned blockchain)”.非许可链又称为公有链,是一种完全开放的区块链,彼此间不需要信任;许可链可分为联盟链和私有链,彼此间需要通过一定的方式建立信任关系,具有非完全去中心化的特点.

1.2 区块链存储模型

在区块链系统中,节点作为完全节点存储完整的区块链数据,能够有效地保证区块链的数据安全[32],即,通过高冗余存储机制保证区块链的数据安全.但是,对于具有高冗余存储特点的任何类型的区块链,现在或未来都将有可能遇到存储可扩展性问题.本节将通过结合典型的采用高冗余存储机制的比特币模型来介绍区块链存储的基本模型和关键技术,区块链的存储模型如图 3 所示.区块链存储模型可抽象为两层,分别是数据层和网络共识层[33].区块链网络本质上是一个 P2P 网络[34],节点地位相同.区块在矿工节点计算出正确的 *nonce* 值后,由矿工节点广播至整个区块链网络,其余节点收到区块后验证,通过后将新区块链接至自己存储的区块链之后.

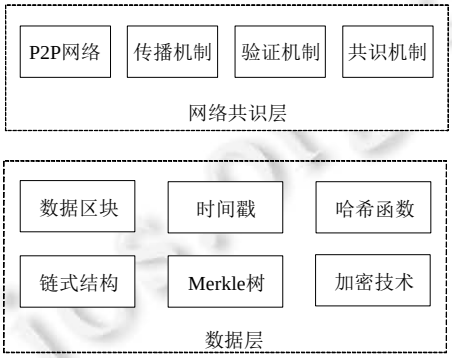

Fig.3 Storage model of blockchain

图 3 区块链存储模型

(1) 数据层

一个完整的区块由区块头和区块体构成.区块头中包含版本号、前一区块的哈希值;当前区块的难度、当前区块经过 PoW 解出的随机值 *Nonce*;当前区块的时间戳以及当前区块所有交易的 Merkle 根.区块体中包含当前区块内的交易数量以及所有经过验证后的交易.区块结构如图 4 所示.

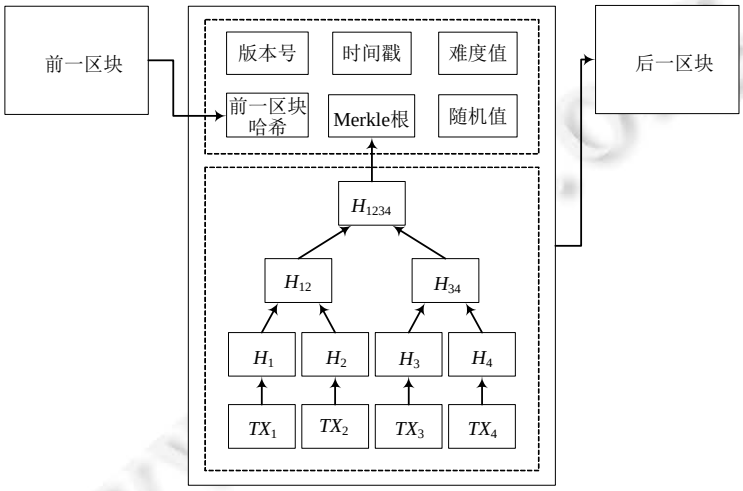

Fig.4 Structure of blocks

图 4 区块结构

链式结构是区块链数据结构的核心.当新区块被生成后,矿工将其添加至区块链的尾端.区块间依次链节,

从而形成完整的区块链数据.当需要访问任意数据时,都可以通过链式结构依次向前溯源.Merkle 根是连接区块头和区块体的重要组件.Merkle 根可以快速归纳和检查区块中交易的存在性和区块的完整性.首先,将区块中所有交易进行分组哈希;然后,将计算出的哈希值插入到 Merkle 树中;接着,对这些哈希值再次分组哈希.如此递归,直至最后生成 Merkle 根并保存至区块头中.时间戳表明当前区块的生成时间,因此,区块链中的所有区块依照时间顺序排列.时间戳可作为区块存在的证明,提高了区块链的不可伪造性和不可篡改性,进而有利于区块链应用到公证、存证等领域.哈希函数具有单向性、易计算性以及抗碰撞性等良好的性质.此外,数据经过哈希函数计算后产生定长的哈希值.这些特性使得哈希函数非常适合应用至区块链中.加密技术,特别是非对称加密,用于保护区块链数据的安全性.

(2) 网络共识层

网络共识层包括区块链网络的组成方式、消息传播机制、数据验证机制和共识机制.比特币等公有链网络中的节点具有分布式以及可自由进出等特点,因此采用 P2P 网络构成区块链网络.P2P 网络中每个节点地位相等,每个节点的功能完全一样,并且不存在任何中心化的机构管理网络.消息传播机制是指当新区块被生成后,将被生成它的矿工广播至区块链网络中的其他节点处验证.数据验证是指任意节点任意时刻都监听区块链网络中广播的交易和新区块.节点在接收到其他节点广播来的交易后,验证其有效性:若交易有效,则将其加入用以存储尚未添加至区块的有效交易的交易池中;若交易无效,则将其删除.共识机制是存储模型中网络共识层的核心,它可以使得区块链网络中的节点高效地达成共识并保持区块链的一致性.在比特币网络中,节点们通过比拼算力,以解决一个计算困难但验证简单的数学问题,最先解答出该问题的节点拥有记账权,并可获得一定的经济奖励.

2 链下存储

链下存储是一种将区块体中数据内容从原区块体转移到链下存储系统,区块体中仅存储指向这些数据的“指针”和其他非数据信息,以解决区块链存储可扩展性问题的方法.当需要存储完整数据时,将原始数据保存至非区块链系统中,同时,按照一定规则生成该数据的唯一标识,并返回给区块链系统;当需要访问完整数据时,通过数据的唯一标识在非区块链存储系统中寻找原始数据,如图 5 所示.

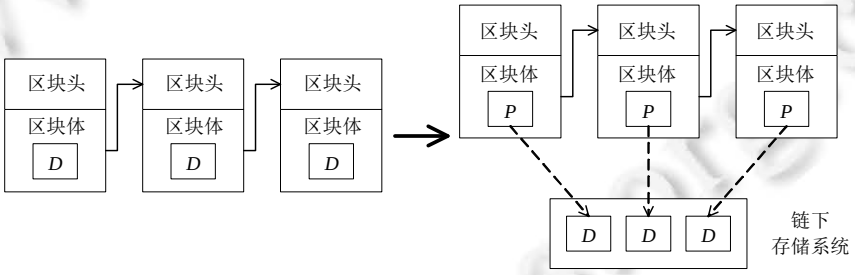

Fig.5 Off-chain storage

图 5 链下存储

定义区块为 *B*,区块头为 *H*,区块体为 *Body*,区块体中的数据为 *D*,*P* 为指向链下存储系统的“指针”,链下存储系统为 *OffChainSS*,则有:

$$location_{before}(D)=Body,$$

$$location_{OffChain}(D)=OffChainSS,$$

$$Body_{before}=\{D\},$$

$$Body_{OffChain}=\{P\}.$$

- 基于 DHT 的链下存储

分布式哈希表(distributed hash table,简称 DHT)是一种分布式存储方法[35].DHT 在不需要中心服务器的情

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.Zyskind 等学者[36]改变了传统区块链网络(例如比特币)存储所有交易的存储模式,将数据与数据引用进行分离式存储,设计了一种使用 DHT 的链下存储模式,其中,DHT 由 Kademlia[37]实现,如图 6 所示.原始数据的引用(即原始数据经 SHA-256 计算后的散列值)保存在区块链中,而原始数据则保存在链下的 DHT 中,如图 6 所示.DHT 由与区块链网络无关的节点维护,这些节点履行经区块链网络批准的读写操作.数据在 DHT 网络中的节点位置足够随机,并且保持一定的重复率,从而确保了高效的可用率.

据美国高德纳公司之前的估计,到 2020 年,世界上有约 200 亿个设备互联到物联网中.这些设备数量巨大,给数据的安全存储带来了挑战.为了有效地存储大规模的物联网数据,Li 等学者[38]提出了一种适用于大规模物联网数据的存储与保护方案,如图 7 所示.该方案利用边缘计算技术克服了物联网设备计算能力不足的问题,并且将数据转发到链下的 DHT 存储系统中.当实体需要访问数据时,在区块链中广播已添加由无证书密码体制[39]生成的公钥的数据请求,并由区块链的矿工节点负责对实体的认证工作.

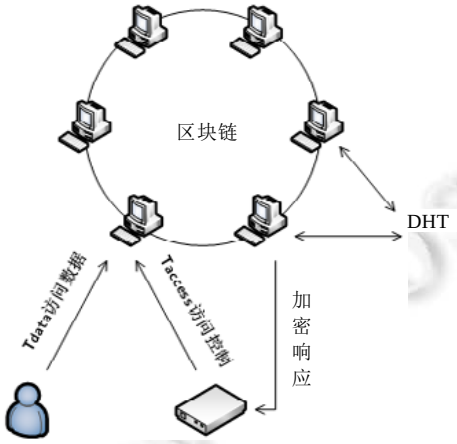

Fig.6 Overview of the decentralized platform

图 6 平台结构示意图

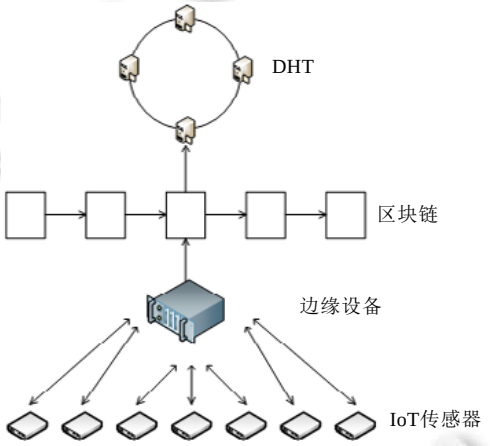

Fig.7 Structure of data storage scheme with blockchain

图 7 基于区块链和边缘计算的物联网数据的存储方案

- 基于 IPFS 的链下存储

星际文件系统(inter planetary file system,简称 IFPS)是一种旨在将所有计算设备与相同文件系统连接起来的点对点分布式文件系统[40].IPFS 是内容寻址的,即内容本身决定了内容的位置[41].文件存储到 IPFS 后,将会得到一个 IPFS hash.IPFS hash 既可以作为访问文件的索引,又可以检验文件内容是否被篡改.基于 IPFS 的这一特性,IPFS 作为区块链的存储方案(即区块中只保存 IPFS hash)是目前链下存储中使用较多的一种方案.

Zheng 等学者[42]设计了一种基于 IPFS 的区块链存储模型,矿工检查待验证的交易是否有效:如果有效,则将其存入 IPFS 中,并将 IPFS 返回的哈希加入至交易池.当新区块产生后,其他节点验证新区块:如果新区块中的交易哈希与本地交易池中的交易哈希相同,则代表这些节点同样验证过这笔交易;如果本地交易池中没有,则通过哈希从 IPFS 中下载并确认.Ali 等学者[43]针对物联网数据隐私问题提出了一种基于区块链和 IPFS 的“模块化联盟架构”,既解决了传统区块链网络无法存储海量数据的缺点,又消除了 IoT 数据的中心化管理模式.Desema[44]是一个基于 Ethereum 和 IPFS 的分布式服务市场系统.在 Desema 中,服务的元数据和大型数据都存储在 IPFS 中,而区块链中仅存储这些数据的散列值.Xu 团队[45]提出了一种基于 Ethereum 和 IPFS 的社交媒体应用,其中,Ethereum 用于保存用户数据,IPFS 用于保存大型文件数据.这既保证了用户数据的完整性和真实性,又解决了文件存储的冗余.以太坊创建智能合约时,需要将智能合约代码保存至以太坊中.这意味着老旧的或者不再使用的智能合约都保存在以太坊中,从而极大地增加了创建智能合约时的存储消耗.Norvill 等学者[46]在创建智能合约时,把智能合约源码存储到 IPFS 中,从而显著地减少了这类存储消耗.

- 基于 DHT 和 IPFS 的链下存储

PingER(ping end-to-end reporting)是一个由 SLAC 国家加速器实验室美国开发和管理的全球端到端互联网性能测量框架[47].PingER 由遍布全球 20 个国家的 50 个 MA(monitoring agent)组成.每个 MA 每天将 ping 统计信息存储到本地 MA 上,然后 SLAC 再将每个 MA 的数据归档至中心服务器.为了防止未来 SLAC 支持的消失,文献[48]提出了一种基于区块链和 DHT 的去中心化的数据存储和访问框架.MA 的身份由客户端转变为节点,因此,MA 的作用不再仅限于收集数据,而是成为数据存储、处理的节点.区块链中存储数据文件的元数据信息以管理身份和访问控制,数据文件的引用存储在链下的 DHT 中,而数据文件本身则存储在 IPFS 中,如图 8 所示.

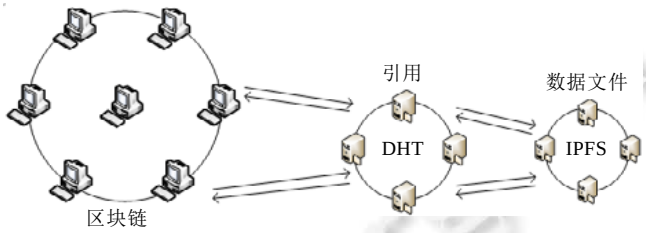

Fig.8 Off-chain storage pattern using DHT and IPFS

图 8 DHT 与 IPFS 共同作为链下存储

- 基于云的链下存储

Ali[49]提出了一种方法,通过把实际数据存储到云端,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.Chameleon[50]是一个动态适应、可扩展的私有链架构.Chameleon 架构由控制和认证层、云存储层、共识和处理层以及访问层组成.与文献[49]不同,Chameleon 不是将所有的数据都存储在云上,而是将数据的散列值存储在区块链中.而 Chameleon 认为:在一些场景下,数据与之前的数据几乎是没有关联的.因此,它将最近一段时期(一天或者一周)的数据存储在区块链中,以前的数据存储到云上.存储在云上的以前的数据中,最新的一个区块的散列值将被保存至区块链中,从而实现数据的一致性(见表 1).

Table 1 Comparison of off-chain storage patterns

表 1 链下存储对比

文献	链下存储系统	公有链/私有链	应用场景	链下数据的安全性
[36]	DHT	私有链	数据隐私保护	依赖于 Kademlia 协议
[38]	DHT	私有链	IOT 设备数据管理	依赖于无证书加密体制
[42]	IPFS	公有链	改进比特币存储模型	依赖于 IPFS 协议
[43]	IPFS	私有链	数据隐私保护	依赖于 IPFS 协议
[44]	IPFS	公有链	去中心化服务市场	依赖于 IPFS 协议
[45]	IPFS	公有链	社交媒体	依赖于 IPFS 协议和智能合约
[46]	IPFS	公有链	智能合约存储	依赖于 IPFS 协议
[48]	DHT+IPFS	私有链	数据管理	依赖于 IPFS 协议和 DHT 协议
[49]	云存储	公有链	去中心化浏览器	依赖于云存储服务
[50]	云存储	私有链	可扩展的私有链架构	依赖于云存储服务

在链下存储方式中,区块头或重要数据依然保存至区块链账本中,原始区块体以及其他数据由链下存储系统负责存储.新区块体中可存储访问链下存储系统的访问记录等信息,而指向链下存储系统的“指针”信息可存储于新区块体中,也可存储于区块头中.由比特币区块的结构可知:一个区块所占的大小约为 1M,而一个区块的区块头的大小为 80byte[1].因此,从存储效率的角度看,链下存储可以大幅度地减轻区块存储的压力.

从所使用的技术角度来看,现阶段链下存储方式主要可分为基于 DHT 的链下存储、基于 IPFS 的链下存储以及基于云的链下存储.基于 DHT 或 IPFS 的链下存储与传统分布式存储相似,同样需要考虑存储冗余的问题,以提高位于链下的数据的安全性.但与比特币网络中每个节点保存完整账本的方式不同,这两种改进的链下存储缓解了区块链网络中节点的存储压力,将一部分数据存储的工作量转移到一个与区块链网络并行的分布式

存储系统中.该系统节点既可以由区块链网络中的节点,也可以由不在区块链网络中的节点组成.若链下的分布式系统全部由区块链网络中的节点组成,这样仅仅减轻了那些在区块链网络中但不在链下分布式存储系统的节点的存储压力.因此,通常的做法是链下分布式存储节点由两部分构成:一部分是区块链网络中的节点,另一部分是非区块链网络中的节点.这种做法缓解了大部分区块链网络中节点的存储压力,由一些具有足够存储能力的节点同时负责链下的分布式存储系统.然而,这种做法也并不是完美的:一方面,在需要考虑如何挑选具有足够存储能力节点的同时维护链下存储系统,但又要保证这些节点不是恶意节点而控制区块链的数据真实性;另一方面,需要考虑如何确定链下分布式存储系统中的区块链节点和非区块链节点之间的比例,以确保存储系统的安全.基于云的链下存储将存储压力转移到云,区块链的去中心化属性将被减弱.基于云的链下存储方案与前两者的不同在于,区块链节点无法参与到云存储中.云存储服务往往都由大型的服务商提供,依赖于中心化机构的服务.此时,区块链仅能验证数据是否被篡改,而不能保证数据的真实性.另一方面,从经济角度来看,云存储所产生的成本由谁承担,以及如何控制减轻区块链节点存储压力所带来的收益大于云存储所需要的额外经济成本,都是需要慎重考虑的.链下存储可以显著减轻区块链节点的存储压力,但需要考虑新的安全问题.

3 链上存储

链上存储,不需要每个节点都存储完整的区块链账本,也不依赖于额外的链下存储系统,只需要每个节点根据预先约定的规则存储对应的部分账本即可.链上存储与前一节所述链下存储的不同在于:数据仍然存储在区块链上,而不是非区块链存储系统中.根据预先约定的规则中节点间的相互关系,链上存储可分为协作式存储模式和轻节点模式.定义区块体中的数据为 D,$Body_{i-1}$ 为第 i 至第 j 个节点同一区块的区块体,其中,$j \geqslant i$, $\tilde{D}$ 为原数据根据链上存储规则确定的存储内容, $\tilde{D} \leqslant D$. 那么,链上存储可表达为

$$location_{before}(D) = Body,$$
$$location_{OnChain}(D) = \{Body_{i-j}\},$$
$$Body_{before} = \{D\},$$
$$Body_{OnChain} = \{\tilde{D}\}.$$

3.1 协作式存储

与比特币的经典存储模式相比,链上协作式存储模式不再需要每个节点都保存一份完整的区块链数据备份.节点协作是指若干个不同的节点进行合作,从而使这些节点具有与“全节点”一样的功能.协作式存储根据使用技术的不同,合作的方式也有很多种形式,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.

- 基于编码的协作式存储

Dai 等学者[51]提出了一种基于网络编码的分布式存储框架(network coding-based distributed storage,简称 NC-DS).网络编码是一种将编码和路由信息交换的技术,可以对接收的多个数据包进行编码信息融合,从而提高单次传输的信息量,进而提升网络整体性能[52].NC-DS 有两种实现:一种是码率确定的 NC-DRDS,另一种是码率非确定的 NC-RLDS.

(1) NC-DRDS 机制取代同时输出数据包的形式,采用顺序输出的形式输出编码后的包.将大小为 x 的区块(或多个区块)切分成 k 个包,对其进行 Reed-Solomn 编码,得到 n 个编码包,存放至 n 个节点中(即一个节点保存至一个包).倘若仍有节点未保存,则继续将 k 个数据包编码成 $2n$ 个编码包,存放至 $2n$ 个节点中.重复上述操作,直至区块链网络中所有节点均保存了一个编码包,如图 9 所示.任意 k 个编码包都可恢复原始数据包;

(2) 而 NC-RLDS 机制则采用了一种二进制域随机偏移编码,将数据包右移随机位的比特然后按位的方式组合,同样以 NC-DRDS 的方式分发至区块链网络中的每个节点.

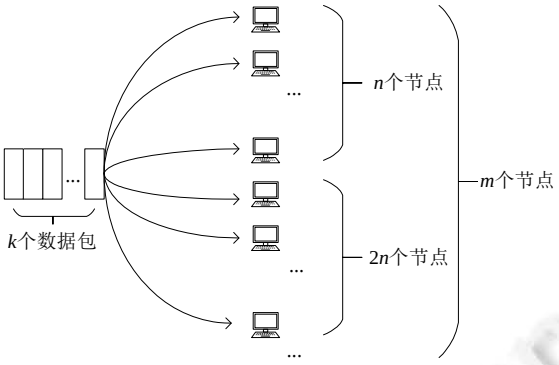

Fig.9 NC-DRDS

图 9 NC-DRDS 示意图

Perard 等学者[53]基于纠删码(erasure code)提出了一种降低节点存储负担的 LS(low storage)节点.区块首先被切分成 k 个片段,再使用伪随机数生成器生成的系数对原始片段进行线性组合,生成编码片段并发送至节点.当节点需要恢复区块时,只需从其他节点下载超过 k 个编码片段.对这些编码片段进行逆线性变换,便可恢复出原始区块.当有新节点加入区块链网络中时,首先从全节点或者其他 LS 节点处下载完整区块链,然后对每个区块进行验证,并生成编码片段.新节点将完整的区块删除,同时保留区块的哈希和编码片段.因此,LS 节点在不需要存储完整区块链的情况下,仍然可以验证完整区块链.

- 基于集群的协作式存储

文献[54]中提出了一种基于 DHT 集群的存储负载均衡方案,DHT 由 Chord 协议[55]实现.在该方案中,区块链网络中的节点划分成若干个 DHT 集群,一个 DHT 集群中的若干个节点共同维护一份完整的区块链数据.区块链中的节点通常需要保存两部分内容,分别是区块数据和区块链状态.在该方案中,DHT 集群中的一个节点只需保存完整区块链副本中区块数据的一部分,而区块链状态部分则需要区块链网络中每个节点都存储.新区块产生后,根据区块的散列值映射到 Chord 环的对应位置.根据哈希函数的特性来确定 DHT 集群内每个节点存储多少个区块会满足均匀分布的要求.在 DHT 集群内,如果需要重复存储 R 次,则在 Chord 环中的节点后面的 R 个节点同样存储 1 次.如果一个区块在 DHT 集群内的所有节点都重复存储,那么此时 DHT 集群的节点就像全节点一样.

Kaneko 等学者[56]设计了一种基于 DHT 集群的负载平衡方法,其中,DHT 由 Kademlia[37]实现.在这一方法中,区块链中的节点分为两类:第 1 类在纯 P2P 网络中挖矿,称为挖矿节点;另一类在 DHT 网络中验证新交易和新区块以及保存区块链数据,成为数据节点.当数据节点产生了一个新交易,则首先广播至该节点所在的 DHT 集群中;然后,集群中的其他节点将该交易广播至其他集群中.所有数据节点对交易进行验证,如果交易有效,将其广播至 P2P 网络中,挖矿节点收集交易,并重复该过程直至挖出新区块.根据新区块的哈希得到该区块的 ID,与节点 ID 进行 XOR 运算,得到与区块 ID 距离最近的节点所属的 DHT 集群.挖矿节点将新生成的区块广播至该集群,集群的节点对区块进行验证,并添加至区块链中.

文献[57]引入了“共识单元”这一概念,共识单元是指一起工作并维护至少一份完整区块链的一组节点.根据前一个单位时间内的区块访问频率,将需要访问的区块优先存储到共识单元内的节点,并考虑一定的冗余.再将所有在前一个单位时间内未被访问的区块分配至相应的节点.至此,共识单元内的存储空间已全部被使用.当共识单元内有新区块需要存储时,需要占用一部分旧区块的空间.根据最优原则,将新区块存储到某个节点上有备份存储的某个或某些区块占用的空间.当有新节点加入共识单元时,分配一定的区块给新节点,从而降低共识单元内的查询消耗.当共识单元内有节点离开时,若该节点存储的区块也存储在其他节点处,那么只需通知查询者更新查询目的地;若该节点存储的区块在其他节点处没有备份,则只需将这些新区块作为需要存储的新节点对待即可.

- 基于分片的协作式存储

分片技术最早被应用于分布式数据库领域,数据库被分割成多个部分并存储到不同的服务器中.在区块链领域中,分片是指节点被分成若干个更小的单元并行地处理交易或维护不相交的区块链账本,前者称为交易分片,后者称为状态分片.Elastico[58]是第一个基于分片的公有链共识协议,Elastico 的思想是交易分片,因此,区块链即使分片后,每个节点仍然需要存储完整的账本.

OmniLedger[59]意识到了 Elastico 存在的问题,并做出了改进.OmniLedger 由身份链和多个分片组成,通过 RandHound 协议,将节点自动地分配到不同的分片.为了减轻节点的存储消耗,OmniLedger 引入了状态块的概念.当一个共识时代结束时,分片的领导者将 UTxO 存储在有序的 Merkle 树中,并将 Merkle 的根哈希存入状态块的头部.状态块经过验证后,将作为下一个共识时代的创世块.但是,OmniLedger 采用的是分片定期改组策略,所以存在大量的数据迁移消耗.

SSChain[60]将区块链网络划分为根链网络和分片网络.市场激励机制会动态地调整根链网络和区块链网络中的哈希算力,使得哈希算力均匀地分布在不同分片中.节点可以自主选择加入收益较高的分片.一个节点可以同时属于根链网络和分片网络.根链网络负责验证一段时间内的分片区块并生成根区块,同时保存完整的分片区块和根区块.SSchain 采用市场激励机制,因而不需要定期改组分片网络,避免了数据迁移.为了减轻分片内的存储负担,SSChain 将前一时期内的 UTxO 保存至有序 Merkle 树中,然后将 Merkle 树的根哈希保存至检查点的头部中,检查点前的区块便无需再存储.

不同于前两种动态划分分片的方式,Yoo等学者[61]提出了一种基于域的静态分片区块链模型.该模型将区块链网络分为区域分片和全局分片,如图 10 所示.区域分片内存在由 PoW 决定的委员会,并动态调整.委员会内的节点通过 PBFT 验证交易并生成区块.全局分片的委员会同样由 PoW 决定,委员会通过 PBFT 验证交易.交易通过验证后被传输到相关的区域分片中.区域分片内的节点负责生成区块并保存至区域区块链中.

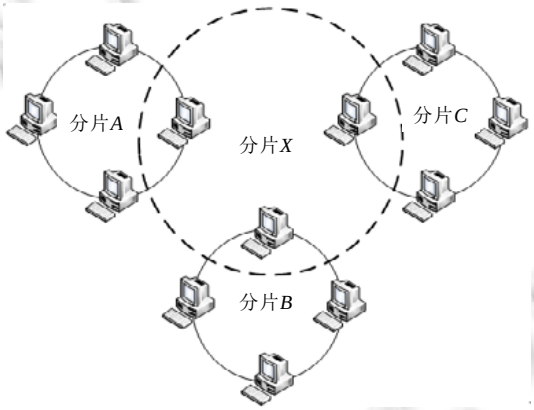

Fig.10 Collaborative storage pattern based on sharding

图 10 基于分片的协作式存储示意图

为了方便比较和总结 3 类协作式存储的区别,下面对一些概念进行定义.

定义 1(区域). 区块链网络可由若干个区域组成,区域之间可以相互交叉.集群、分片等都可视为一个区域.

定义 2(静态区域划分). 对于节点 n_i,根据节点分配机制,当 $t=t_1$ 时,n_i 被分配到区域 A_{j1};当 $t=t_2$ 时,n_i 被分配到区域 A_{j2}.若 $\forall t_2\neq t_1$,都有 $A_{j1}=A_{j2}$,则称区域划分是静态的;反之,则称为动态.

定义 3(区域定期改组). 区域定期改组是指节点 n_i 一旦被分配到区域 A_{j1} 内,任意时间后都不会被系统重新分配到区域 A_{j2},其中,$A_{j1}\neq A_{j2}$.

定义 4. 区域账本是指仅记录该区域内交易的区块链账本,记为 BC_{area}.

定义 5. 对于区块 B_k, $B_k=\bigcup_{i=0}^{m}B_{k_i}$, 则称 B_{k_i} 为区块 B_k 的子集,称 $\sum_{i=0}^{m}\lambda_{k_i}B_{k_i}$ 为区块子集的线性组合;对于区

块 B_k,$\bigcup_{k=0}^{n}\lambda_k B_k$ 称为区块的集合.

定义 6. 当新节点加入区域时,区域内的原节点若需要调整已存储的数据,则称该模型具有自动调整性.

定义 7(区块的原子性). 若区块完整地存储在一个节点中,则称该存储方式保留了区块的原子性;反之,若一个区块经过切分存储在不同的节点中,则称该存储方式破坏了区块的原子性.

集群是指一组共同工作的节点,而分片则指将账本切分成粒度更小的部分.本文中,集群是从节点的角度切分区块链,分片是从账本的角度切分区块链.因此,本文将集群和分片均看作是区域.基于编码的协作式存储模式没有显式的区域划分,但可以将源于同一个数据包的若干个子包所在的节点看作是一个区域,满足定义 1.如果下一个数据包划分成若干个子包后,这些子包所处的节点集与前一数据包时不同,则可看作为区域定期改组,周期为产生一个新区块的时间.

表 2 从区域划分思想、划分形式、定期改组、区域存储内容、区块原子性、区域自动调整性、是否有节点存储完整账本以及节点存储大小的角度,详细地对比了 8 种不同的协作式存储.动态划分区域有利于防止恶意节点控制某一区域,从而影响整个区块链的网络性能.定期改组区域能够提高一定的安全性,但与此同时,也会存在大量的数据迁移工作.对于文献[54]和文献[57]中的方案,当有新节点加入区域后,模型会自动地调整曾经存储在原节点上的数据,重新分配到新节点上.这种自动的调整方式会占用区域内的通信带宽,增加通信成本.从存储效率的角度看,对于基于编码的协作式存储,编码时切分的数据子包个数越多,节点所需的存储空间越小.对于基于动态分片的协作式存储,区块链分片数越多,节点所需存储空间越少.这两种方式所需的存储空间和比特币存储模型所需存储空间呈线性关系.对于基于集群的协作式存储,节点所需存储空间与集群内节点数量相关,集群内节点数量越多,每个节点所需存储空间越小.对于基于静态分片的协作式存储,当进行初始化划分时,若某一分片规模明显大于其他分片,则日后同样也将面临存储膨胀的问题.

Table 2 Comparison of collaborative storage patterns

表 2 协作式存储比较

文献	区域划分思想	区域划分形式	区域定期改组	区域存储内容	区块原子性	自动调整性	存在节点保存完整账本	节点存储大小	符号
[51]	编码	动态	Y	单一区块	N	N	N	区块子集	$set(\bigcup_{i=0}^{n}B_{i,j})$
[53]	编码	–	Y	单一区块	N	N	N	区块子集线性组合	$set(L(B_{i,j}))$
[54]	集群	静态	N	完整账本	Y	Y	N	区块集合	$set(\bigcup_{i=0}^{n}B_i)$
[56]	集群	静态	N	区块集合	Y	N	N	区块集合	$set(\bigcup_{i=0}^{n}B_i)$
[57]	集群	–	N	完整账本	Y	Y	N	区块集合	$set(\bigcup_{i=0}^{n}B_i)$
[59]	分片	动态	Y	区域账本	Y	N	N	区域账本	$\bigcup_{i=0}^{n}B_{A_k,i}$
[60]	分片	动态	N	区域账本	Y	N	Y	区域账本	$\bigcup_{i=0}^{n}B_{A_k,i}$
[61]	分片	静态	N	区域账本	Y	N	N	区域账本	$\bigcup_{i=0}^{n}B_{A_k,i}$

注:B_i 表示第 i 个区块,$B_{i,j}$ 表示第 i 个区块的第 j 个部分,$B_{A_k,i}$ 表示区域 A_k 内的第 i 个区块,$L(\cdot)$表示线性组合,$set(\cdot)$表示集合,$\bigcup_{i=0}^{n}(\cdot)$ 表示并集

3.2 轻节点

3.2.1 SPV 轻节点

在比特币网络中,大部分用户是普通用户(没有矿机并且只消费比特币的用户).如果这些用户运行一个完整的比特币客户端,那么需要准备大约 200G 的空余硬盘.对于比特币手机钱包来说,存储完整的比特币账本是不现实的,因此便有了适用于运行在小型设备的轻量型节点.

全节点是一种存储完整账本、需要同步所有区块链数据、能够独立校验区块链上的所有交易并实时更新区块链的节点.轻节点是一种不需要存储完整账本,每当有新区块出现时,只需要下载区块头的节点类型.SPV 协

议(simple payment verification protocol)[1]是最早的轻节点协议,该协议指出:不运行全节点也可验证支付,用户只需要保存所有的区块头即可,如图11所示.SPV轻节点只需从区块链网络中下载所有区块的区块头.SPV轻节点由于自身并不存储区块链中区块的区块体,因此不能独立验证交易,需依赖于全节点.当需要验证支付时,向区块链网络发出请求,进而查找用于支付的那笔交易所在的区块,再根据Merkle根哈希验证这笔交易是否有效.

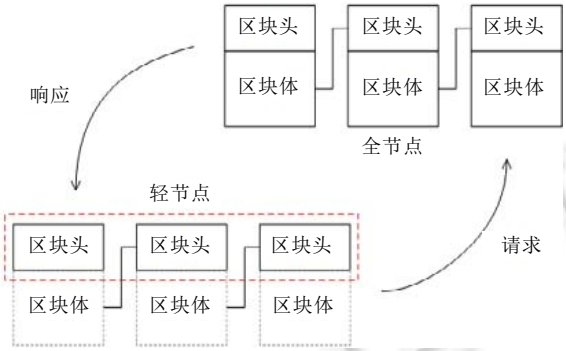

Fig.11 SPV scheme of light node

图 11 SPV 轻节点协议

第 3.2 节所述的轻节点模式与第 3.1 节所述的协作式存储模式的区别与联系可见表 3.

Table 3 Difference and relation between light node mode and collaborative storage mode

表 3 轻节点模式与协作式存储模式的区别

存储模式	区别	联系
协作式存储	节点们之间是一种对等与合作的关系;恢复完整的原始区块链账本需要这些节点相互合作	两者都属于链上存储模式,相比全节点模式,两者都不需要存储完整的区块链账本,可通过一定的方式实现全节点模式的功能
轻节点	存在轻节点的区块链网络中,必然存在全节点;恢复完整的原始区块链账本需要全节点的帮助	

3.2.2 改进型轻节点

SPV 轻节点需要存储每个区块的区块头,意味着节点的本地存储上限仍与区块链中区块的数量成正比例关系;另一方面,轻节点需要信赖全节点验证支付或交易,减弱了区块链无需信赖第三方的特质.因此,很多学者从不同的角度对传统的轻节点作了改进.

Xu 等学者[62]提出了一种公有链客户端协议,称为 EPBC.这种客户端适用于物联网设备或手机等存储资源有限的设备.与 SPV 协议不同,它不用存储所有区块的区块头,而只需存储一个大小定长的数据,并且与区块链账本的大小无关.EPBC 在每个区块的区块头中添加了一个对当前区块链的总结 S,但无需参与挖矿的过程.S 的生成过程与 RSA 类似,需要选取两个质数 p 和 q,生成 N.在创世区块的区块头中,添加 N 和一个随机数 g.当轻节点需要验证时,全节点生成一个元组 $(p_i^{(0)}, p_i^{(1)})$ 返回给轻节点.轻节点只需验证 $p_i^{(0)}$ 和一个关于 S_n 的等式即可.当加入区块链时,轻节点从区块链网络中选取 u 个节点,并获取 $S^{(u)}$.轻节点随机选取一些区块,并与这些节点交互以验证 $S^{(u)}$的有效性.最后选取由最多节点返回的 $S^{(u)}$作为区块链总结.

文献[63]提出了一种存储压缩协议 SCC(storage compression consensus).SCC 是一种基于 PBFT 的改进协议.当物联网节点申请加入区块链时,首先要通知自己的存储容量和存储上限系数,以便其他节点验证其存储能力.存储能力最小的节点可作为一轮 SCC 中的领导者,因其执行压缩的过程表明,它忠诚地维护和紧跟区块链系统.在 SCC 中,每轮除了需要处理正常生成的最新区块外,还需要通过 Merkle 树的方法生成一个由区块链中所有区块组成的压缩块.压缩块中存储最新区块的 hash,最新区块中存储压缩块的 hash,如图 12 所示.当这两个区块通过验证后,每个节点根据其自身情况进行存储.存储资源受限的轻节点存储最新区块和压缩块,并将之前的区块全部移除.每轮共识结束后,执行相同的过程.

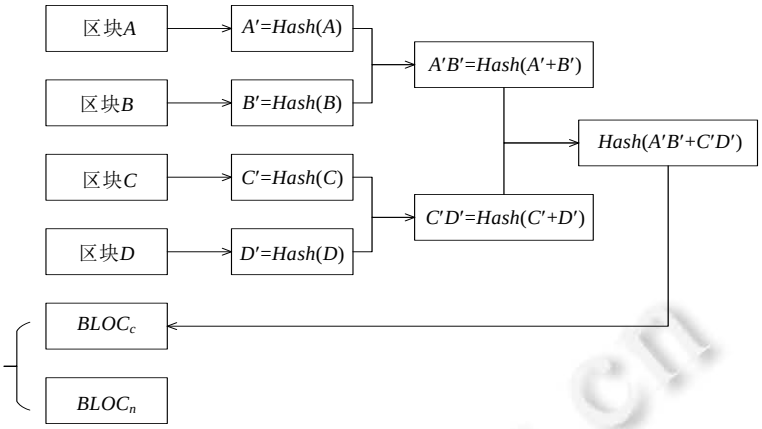

Fig.12 Compression block and next block

图 12 压缩块和最新区块

传统轻节点依赖于区块链网络中的全节点,同时,这也是轻节点的局限之一.Frey 团队[64]提出了一种模型,这种模型中的轻节点在验证交易时无需依赖于全节点.模型将节点分为 5 类角色,分别是挖矿节点、全节点、安全轻节点、传统轻节点和 DHT 节点.一个物理节点可以同时是多种角色.为了实现安全轻节点不存储完整账本的目的,区块结构进行了改进.在区块头中额外添加两个值,H_{UTxO} 和 H_{index},如图 13 所示.根据输出地址的前 k 位,将 UTxO 集分割成 $2k$ 个分片,对它们进行哈希运算,然后再对这些哈希值进行一次哈希,得到 H_{UTxO}.对由所有区块的 hash 构成的数组进行哈希运算得到 H_{index}.区块链中的节点以及与区块链无关的节点共同组成 DHT. DHT 保存 UTxO 集的分片和最近 h 个完整区块.在安全轻节点加入区块链网络时,只需下载最近 6 个区块、UTxO 分片哈希列表和区块哈希列表.当安全轻节点验证一笔新交易时,首先从 DHT 中找到对应的 UTxO 分片.若该 UTxO 分片 hash 与先前下载的 hash 相同,则该交易是有效的.这种方式将原先依赖于全节点的数据转移至若干节点共同维护的 DHT 中.对于存储资源充足的全节点,存储负担仅增加了一点点;但对于对于存储资源受限的轻节点来说,减轻了存储负担并不再依赖于全节点.

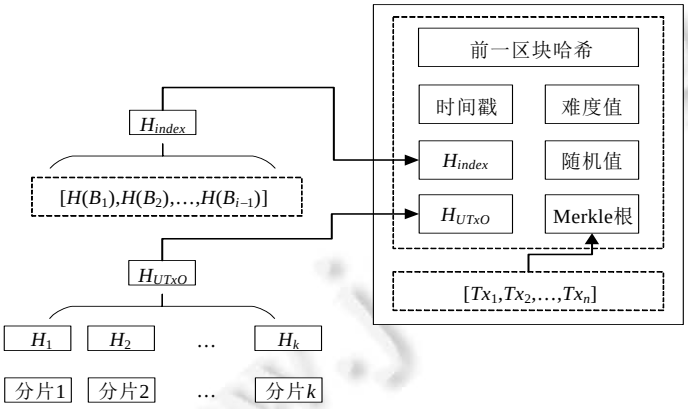

Fig.13 Block index hash and the UTxO hash are added to the block header

图 13 添加 H_{UTxO} 和 H_{index} 的区块结构

Palai 团队[65]提出一种称为区块总结的方法,该方法既可以获得比 SPV 更多的权限,又不需要像全节点那样保存完整账本.区块总结方法将 l 个原始区块总结成一个新区块,称为总结区块.总结区块中交易的输入与其所

包含的原始块中的交易输入一样,输入同理.如果一笔交易的输出是另外一笔交易的输出,那么将根据净效果合并这些交易.总结区块也会包括原始区块的哈希.直接总结区块同样会造成区块链账本大小问题.Palai 使用递归的方式对区块序列进行总结,即对总结区块进行总结.该方法引入了总结深度的概念,原始区块的总结深度为 0,原始区块直接总结区块的总结深度为 1,以此类推.一个区块长度为 n 的区块链经过区块递归总结后,将变成先是 o 个原始区块,再是 m 个总结深度为 1 的总结区块,之后再是 m 个总结深度为 2 的总结区块,以此类推.经过区块总结后的区块链如图 14 所示.Nadiya[66]在 Palai 团队研究的基础上,使用 Deflate 压缩算法对总结区块进行数据压缩,进一步减小了区块链所占用的存储空间.

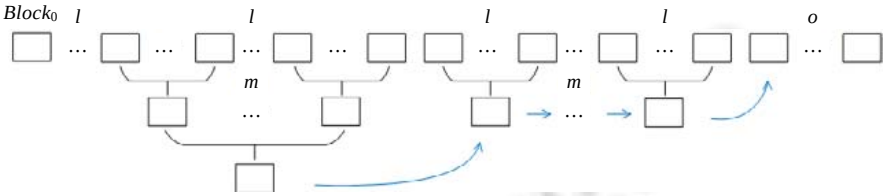

Fig.14 Block summarization

图 14 区块总结示意图

表 4 从轻节点是否依赖全节点以及轻节点存储内容的角度,对比了 6 种典型的轻节点协议或模型.根据是否依赖全节点,可将轻节点协议或模型分为两种:一种是依赖于全节点,另一种是不依赖于全节点.与比特币原始存储模型不同的是,SVP 轻节点只需要存储区块链账本中的区块头,因此,当需要区块体时,向全节点请求.同样地,EPBC 轻节点仅存储大小定长的区块总结值,当需要完整区块时,即请求全节点,并通过区块总结值判断全节点返回的区块是否有效.SCC 通过对最新区块前的区块链按照 Merkle 树的方式进行压缩,以与完整的区块链账本保持一致性.当全节点不再有空余空间存储完整区块链账本时,可以简单地去除旧区块,仅存储压缩区块和最新区块.另一类不依赖于全节点的轻节点模型,对区块进行总结或者压缩,使这些原始区块合并或组合成一个新区块,新区块远小于原始区块集合的大小.对于使用 UTxO 模型而不是余额模型的区块链来讲,一笔交易的输出有可能是另一笔交易的输入,净变化是没有区别的.所谓总结是指,将原始区块集合中交易集进行合并.但这种方式具有局限性,只适合区块体中仅保存金额、数字变化的场景.对于存证、溯源等区块体中存储非数字型数据的领域,区块总结的方式是无法使用的.

Table 4 Comparison of light node patterns

表 4 轻节点对比

文献	公有链/私有链	是否依赖全节点	能否独立验证交易	节点存储大小	符号	适用情况限制
[1]	公有链	Y	N	所有区块头	$\bigcup_{i=1}^{n} H_i$	–
[62]	公有链	Y	Y	区块总结值	S_n	–
[63]	私有链	Y	N	压缩区块和最新区块	$B_{compression}+B_n$	–
[64]	公有链	N	Y	最新 6 个区块 UTxO 哈希列表 区块哈希列表	$\bigcup_{i=n-5}^{n} B_i$ + $List(\{H(utxo\ shard)\})$+ $List(\{H(Block)\})$	非 UtxO 模型
[65]	–	N	Y	所有总结区块	$\bigcup_{i=1}^{a} B_{summary_i}$	非 UtxO 模型
[66]	–	N	Y	压缩后的 所有总结区块	$C(\bigcup_{i=1}^{a} B_{summary_i})$	非 UtxO 模型

注:B_i 表示第 i 个区块,H_i 表示第 i 个区块的区块头,$Body_i$ 表示第 i 个区块的区块体,$List(\cdot)$表示列表,$C(\cdot)$表示压缩函数

4 总结与展望

本文从区块链账本存储位置的角度,综述了链下存储和链上存储两种用于提高存储可扩展性方法的研究

进展.本节将指出两大类方法目前所面临的挑战,并为未来的研究工作提供一些可能的方向.

4.1 当前解决方案所面临的挑战

(1) 应用场景

区块链可分为公有链和非公有链,后者包括联盟链和私有链.公有链是完全去中心化的,任何节点都可以随时加入或退出区块链网络.联盟链是一种部分去中心化的区块链,它由联盟或企业构成组织负责维护.而私有链则是一种中心化的区块链,适合特定的中心化机构控制.

在链下存储的模式中,数据转移至第三方可信赖的存储系统,或由公有链节点负责维护链下存储系统存储.后者易出现提供额外存储空间的超级节点,两者都会破坏公有链的去中心化特质.在非公有链场景下,节点的写入受中心化的机构或联盟控制,并且数据规模较小.此时,链下的存储系统可由负责非公有链的中心化机构或联盟以及非公有链的节点来维护.

链上存储更适合节点众多的公有链、联盟链场景.在协作式存储模式中,节点间的关系不是单向依赖的,而是相互依赖、相互合作.轻节点模式适合存储容量小的智能设备,如手机、PC 以及传感器等.许多学者也提出了不依赖于全节点的轻节点方案,一定程度上提高了轻节点的独立性和安全性,但轻节点仍无法实现全节点的所有功能.利用区块总结方式的轻节点可以节省大量空间,但同时在应用场景上也存在一定的局限性,这些轻节点仅适合于区块体存储货币转移的场景,而无法应用到存证、溯源等领域.

(2) 安全性

区块链迄今为止面临的最大挑战便是安全问题,即便是完全去中心化的比特币,对于链下存储模式,如何确保链下的存储系统安全、可靠也仍是一个难点.一种解决方案是维护链下存储系统的都是区块链节点,另一种方案是维护链下存储系统的节点一部分是区块链节点一部分是非区块链节点.前者增加了区块链节点的负担,后者牺牲了公有链的去中心化特性.区块链与链下存储系统之间的通信安全同样需要考虑.

对于协作式存储,如何确保区域中即使存在恶意节点,但不会影响区域内节点的协作或区域间的协作,是设计协作式存储方案首先需要考虑的问题.协作式存储需要考虑一定的数据冗余以确保数据的安全.而轻节点与全节点的关系是轻节点安全性的根本,负责与轻节点通信的全节点如果是恶意节点,那么至少在一个时期内,该轻节点都被恶意节点所欺骗.因此,轻节点应该要么依赖尽可能多的全节点,要么应该依赖区块链整体网络.

无论是链下存储还是链上存储,原先完整的区块链账本都会被拆分.那么当节点需要完整账本时,从链下存储系统或其他节点处获取自身不存储的账本部分后,账本将会被整合.整合后的账本与区块链网络中所存储的账本必须保持完全一致.因此,必须考虑一定的冗余策略和补救策略以保证区块链的一致性在链下存储和链上存储不受影响.

(3) 效率

在链下存储方式中,区块链仅需存储区块头和一些重要数据,而区块体或一些普通数据则存储在链下存储系统中.区块链存储负担明显减轻.在许多协作式存储中,节点所需的存储空间往往与区域内节点数量无关,因此与比特币存储模型所需空间近似呈线性关系.当区块不断地增加至区块链的尾端时,这些协作式存储方案慢慢地同样会遇到存储瓶颈.轻节点通常存储区块头或经过总结后的区块链账本.研究者需要考虑如何使得改进后的存储模型所需空间日后不会面临同样的存储问题.

链下存储和链上存储都在一定程度上增加了通信成本,即以时间换取空间.在链下存储模式中,节点需要花费额外的通信成本从链下的存储系统获取区块链数据.对于链上存储模式,当节点需要完整的区块链账本时,则要向区块链网络中的节点或区域内的节点请求自己没有存储的账本部分.因此,研究者们需要考虑区域的划分与时间成本和存储成本之间的关系.对于轻节点而言,当需要完整数据时,无法从本地找到对应区块,而需要请求区块链网络中的全节点或整个区块链网络.在解决存储扩展性问题的同时,需要考虑与通信成本之间的关系,从而做到在可承受范围内,增加一定的通信成本以获得较小的存储压力.

4.2 未来研究方向

第 4.1 节提到了区块链存储可扩展性技术主要面临的一些问题,在这些问题的基础上,本文给出了几个未来的研究方向.

(1) 研究可节省存储空间的共识机制

目前,大部分提高区块链存储可扩展性的解决方案都是对经过共识后产生的新区块进行处理,以达到减轻节点存储压力的目的.这些解决方案是从区块链基础架构模型的网络层进行改进,不涉及改变区块链的共识机制.未来可从区块链基础架构模型的共识层入手,研究可节省存储空间的共识机制;区块链节点在达成共识的过程中同时考虑如何协作存储区块数据,以解决区块链存储日益膨胀的问题.此外,在公有链场景中,存在经济激励手段鼓励节点参与共识.因此在可节省存储空间的共识机制中,需要在共识机制中添加合理的经济激励措施,奖励付出更多存储资源的节点.

(2) 研究与初始节点数量相关联的动态区域划分方法

链上协作式存储模式通过将区块链网络划分成若干个区域,区域内的节点协作地维护区块链账本.目前的链上协作式存储模式中的区域划分方法可分为动态和静态两种方式.然而无论是动态划分还是静态划分,均与初始时节点数量无关.这就导致在区域划分前,区块链网络中的节点即使存在数量的差异,划分方法仍然相同,进而可能导致区域节点间的通信成本增加.未来可从区块链节点数量与通信成本和存储成本之间的关系来加以思考,建立相应的数学模型,实现访问本地和区域内其他节点的区块链数据所花费的时间之和最优,进而实现通信成本和存储成本的最优化.

(3) 研究存储定长数据的轻节点模式

随着物联网技术的不断发展,未来物联网与区块链的整合非常重要.链上协作式存储模式会增加物联网节点间的相互依赖,因此,轻节点模式更适合物联网中的轻量级设备.按照当前主流的轻节点协议,这些轻节点所存储的数据大小与完整区块链账本大小之间大致呈线性关系.以这种存储方式,轻节点未来依然会遇到存储瓶颈.因此,研究存储定长数据的轻节点模型是一个值得研究的方向.

(4) 研究不同存储模式下的安全机制

目前提高区块链可扩展性的两类解决方案——链下存储和链上存储,仍存在着一定的安全性问题,包括链下存储系统与区块链间的交互安全问题、链上协作式中区域内的恶意节点问题、轻节点与全节点间的信任问题以及区块拆分后重构时的安全问题等.属性加密、同态加密以及零知识证明等技术为提高链下存储和链上存储的安全性提供了方向.未来可研究基于属性加密、同态加密或零知识证明等技术的安全机制,进而提高链下存储及链上存储模式的整体安全性.

5 结束语

区块链存储的可扩展性已成为制约区块链应用落地的一大问题.巨大的存储压力,一方面使得已有的节点可能无法继续参与区块链;另一方面,使得存储能力差的轻型设备无法加入区块链网络.因此,研究提高区块链存储可扩展性的技术具有非常重要的意义.本文首先介绍了区块链所面临的存储可扩展性问题以及区块链的存储模型,其次分析了两大类提高存储可扩展性技术的研究进展,最后对提高存储可扩展性技术所面临的问题和研究方向给出了我们的思考和总结.

References:

[1] Nakamoto S. Bitcoin: A peer-to-peer eletronic cash system. 2009. http://bitcoin.org/bitcoin.pdf

[2] Wood G. Ethereum: A secure decentralised generalised transaction ledger. 2015. http://gavwood.com/Paper.pdf

[3] Wang L, Liu WY, Han XW. Blockchain-based government information resource sharing. In: Proc. of the 23rd IEEE Int'l Conf. on Parallel and Distributed Systems (ICPADS). 2017. 804−809.

[4] Zhang XW, Yin YJ. Research on digital copyright management system based on blockchain technology. In: Proc. of the 3rd IEEE Information Technology, Networking, Electronic and Automation Control Conf. (ITNEC). 2019. 2093−2097.

[5] 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.

[6] Casado-Vara R, 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. 2018. 19−24.

[7] 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.

[8] 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.

[9] Li C, Palanisamy B. Incentivized blockchain-based social media platforms: A case study of steemit. In: Proc. of the 10th ACM Conf. on Web Science (WebSci 2019). 2019. 145−154.

[10] Chen YL, Li H, Li KJ, Zhang JY. An improved P2P file system scheme based on IPFS and blockchain. In: Proc. of the 2017 IEEE Int'l Conf. on Big Data. 2017. 2652−2657.

[11] Xie JF, Yu FR, Huang T, Xie R, Liu J, Liu YJ. A survey on the scalability of blockchain systems. IEEE Network, 2019,33(5): 166−173.

[12] Liu AD, Du XH, Wang N, Li SZ. Research progress of blockchain technology and its application in information security. Ruan Jian Xue Bao/Journal of Software, 2018,29(7):2092−2115 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5589.htm [doi: 10.13328/j.cnki.jos.005589]

[13] Vo HT, Kundu A, Mohania M. Research directions in blockchain data management and analytics. In: Proc. of the 21st Int'l Conf. on Extending Database Technology. 2018. 445−448.

[14] Tian JF, Jing X, Guo RF. Public audit scheme of shared data based on blockchain. In: Proc. of the 2nd Int'l Conf. on Frontiers in Cyber Security, Vol. 1105. 2019. 327−344.

[15] Cheng X, Chen FL, Xie D, Sun H, Huang C, Qi ZY. Blockchain-based secure authentication scheme for medical data sharing. In: Proc. of the 5th Int'l Conf. of Pioneering Computer Scientists, Engineers and Educators, Vol. 1058. 2019. 396−411.

[16] Yao ZY, Pan H, Si XM, Zhu WH. Decentralized access control encryption in public blockchain. In: Proc. of the 1st Int'l Conf. (BlockSys 2019), Vol. 1156. 2020. 240−257.

[17] Pazaitis A, De FP, Kostakis V. Blockchain and value systems in the sharing economy: The illustrative case of backfeed. Technological Forecasting and Social Change, 2017,125:105−115.

[18] Li L, Liu JQ, Cheng LC, Qiu S, Wang W, Zhang XL, Zhang ZH. CreditCoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. IEEE Trans. on Intelligent Transportation Systems, 2018,19(7): 2204−2220.

[19] Baza M, Nabil M, Ismail M, Mahmoud M, Serpedin E, Ashiqur MR. Blockchain-based charging coordination mechanism for smart grid energy storage units. In: Proc. of the 2019 IEEE Int'l Conf. on Blockchain (Blockchain). 2019. 504−509.

[20] Shi JS, Li R. Survey of blockchain access control in Internet of things. Ruan Jian Xue Bao/Journal of Software, 2019,30(6): 1632−1648 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5740.htm [doi: 10.13328/j.cnki.jos.005740]

[21] Tsai WT, Yu L, Wang R, Liu N, Deng EY. Blockchain application development techniques. Ruan Jian Xue Bao/Journal of Software, 2017,28(6):1474−1487 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5232.htm [doi: 10.13328/j.cnki.jos.005232]

[22] Zhai SP, Li ZZ, Duan HY, Gao S. Research on data consistency of key technologies of blockchain. Computer Technology and Development, 2018,28(9):94−100 (in Chinese with English abstract).

[23] Yang WL, Aghasian E, Garg S, Herbert D, Disiuta L, Kang B. A survey on blockchain-based Internet service architecture: Requirements, challenges, trends, and future. IEEE Access, 2019,7:75845−75872.

[24] Pan C, Liu ZQ, Liu Z, Long Y. Research on scalability of blockchain technology: Problems and methods. Journal of Computer Research and Development, 2018,55(10):2099−2110 (in Chinese with English abstract).

[25] Zhang XH, Wang HM, Shi PC, Fu X. LS4BUCC: A low overhead storage architecture for blockchain based unmanned collaborative cognition system. In: Proc. of the 2019 IEEE Int'l Conf. on Service-oriented System Engineering (SOSE). 2019. 221−226.

[26] Wang QS, Wang HZ, Zheng B. An efficient distributed storage strategy for blockchain. In: Proc. of the ACM Turing Celebration Conf. 2019. 1−5.

[27] Poon J, Dryja T. The Bitcoin lightning network: Scalable offchain instant payments. 2016. https://lightning.network/lightning-network-paper.pdf

[28] Salman T, Zolanvari M, Erbad A, Jain R, Samaka M. Security services using blockchains: A state of the art survey. IEEE Communications Surveys & Tutorials, 2019,21(1):858−880.

[29] Wang WB, Hoang DT, Hu PZ, Xiong ZH, Niyato D, Wang P, Wen YG, Kim DI. A survey on consensus mechanisms and mining strategy management in blockchain networks. IEEE Access, 2019,7:22328−22370.

[30] Yu G, Nie TZ, Li XH, Zhang YF, Shen DR, Bao YB. The challenge and prospect of distributed data management techniques in blockchain systems. Chinese Journal of Computers, 2019,42:1−27 (in Chinese with English abstract).

[31] Zeng SQ, Huo R, Huang T, Liu J, Wang S, Feng W. Survey of blockchain: Principle, progress and application. Journal on Communications, 2020,41(1):134−151 (in Chinese with English abstract).

[32] Jia DY, Xin JC, Wang ZQ, Guo W, Wang GR. ElasticQM: A query model for storage capacity scalable blockchain system. Ruan Jian Xue Bao/Journal of Software, 2019,30(9):2655−2670 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5774.htm [doi: 10.13328/j.cnki.jos.005774]

[33] Yuan Y, Wang FY. Blockchain: The state of the art and future trends. Acta Automatica Sinica, 2016,42(4):481−494 (in Chinese with English abstract).

[34] Yu ZY, Liu XG, Wang G. A survey of consensus and incentive mechanism in blockchain derived from P2P. In: Proc. of the 2018 IEEE 24th Int'l Conf. on Parallel and Distributed Systems. 2018. 1010−1015.

[35] Theotokis SA, Spinellis D. A survey of peer-to-peer content distribution technologies. ACM Computing Surveys, 2004,36(4): 335−371.

[36] Zyskind G, Nathan O, Pentland AS. Decentralizing privacy: Using blockchain to protect personal data. In: Proc. of the 2015 IEEE Security and Privacy Workshops. 2015. 180−184.

[37] Maymounkov P, Mazières D. Kademlia: A peer-to-peer information system based on the XOR metric. In: Proc. of the IPTPS. 2002. 253−65.

[38] Li RN, Song TY, Mei B, Li H, Cheng XZ, Sun LM. Blockchain for large-scale Internet of things data storage and protection. IEEE Trans. on Services Computing, 2019,12(5):762−771.

[39] Zhang FT, Sun YX, Zhang L, Geng MM, Li SJ. Research on certificateless public key cryptography. Ruan Jian Xue Bao/Journal of Software, 2011,22(6):1316−1332 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4007.htm [doi: 10.3724/SP.J.1001.2011.04007]

[40] Benet J. IPFS—Content addressed, versioned, P2P file system. 2014. https://github.com/ipfs/ipfs/blob/master/papers/ipfs-cap2pfs/ipfs-p2p-file-system.pdf

[41] Hasan SS, Sultan NH, Barbhuiya FA. Cloud data provenance using IPFS and blockchain technology. In: Proc. of the 7th Int'l Workshop on Security in Cloud Computing. 2019. 5−12.

[42] Zheng QH, Li Y, Chen P, Dong XH. An innovative IPFS-based storage model for blockchain. In: Proc. of the 2018 IEEE/WIC/ACM Int'l Conf. on Web Intelligence (WI). 2018. 704−708.

[43] Ali MS, Dolui K, Antonelli F. IoT data privacy via blockchains and IPFS. In: Proc. of the 7th Int'l Conf. on the Internet of Things (IoT 2017). 2017. 1−7.

[44] Klems M, Eberhardt J, Tai S, Härtlein S, Buchholz S, Tidjani A. Trustless intermediation in blockchain-based decentralized service marketplaces. In: Proc. of the 15th Int'l Conf. on Service-Oriented Computing. 2017. 731−739.

[45] Xu QQ, Song ZW, Mong Goh RS, Li YJ. Building an Ethereum and IPFS-based decentralized social network system. In: Proc. of the 24th IEEE Int'l Conf. on Parallel and Distributed Systems. 2018. 1−6.

[46] Norvill R, Fiz Pontiveros BB, State R, Cullen A. IPFS for reduction of chain size in Ethereum. 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). 2018. 1121−1128.

[47] Matthews W, Cottrell L. The PingER project: Active Internet performance monitoring for the HENP community. IEEE Communications Magazine, 2000,38(5):130−136.

[48] Ali S, Wang GJ, White B, Cottrell RL. A blockchain-based decentralized data storage and access framework for PingER. In: Proc. of the 17th IEEE Int'l Conf. on Trust, Security and Privacy in Computing and Communications/12th IEEE Int'l Conf. on Big Data Science and Engineering. 2018. 1303−1308.

[49] Ali M. Trust-to-trust design of a new Internet [Ph.D. Thesis]. Princeton: Princeton University, 2017.

[50] He GB, Su W, Gao S. Chameleon: A scalable and adaptive permissioned blockchain architecture. In: Proc. of the 1st IEEE Int'l Conf. on Hot Information-Centric Networking (HotICN). 2018. 87−93.

[51] Dai MJ, Zhang SL, Wang H, Jin S. A low storage room requirement framework for distributed ledger in blockchain. IEEE Access, 2018,6:22970−22975.

[52] Chen C, Dong C, Mao YF, Chen GH, Wang H. Survey on network-coding-aware routing in wireless network. Ruan Jian Xue Bao/ Journal of Software, 2015,26(1):82−97 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4696.htm [doi: 10.13328/j.cnki.jos.004696]

[53] Perard D, Lacan J, Bachy Y, Detchart J. Erasure code-based low storage blockchain node. 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). 2018. 1622−1627.

[54] Abe R, Suzuki S, Murai J. Mitigating bitcoin node storage size by DHT. In: Proc. of the Asian Internet Engineering Conf. 2018. 17−23.

[55] Stoica I, Morris R, Liben-Nowell D, Karger DR, Kaashoek MF, Dabek F, Balakrishnan H. Chord: A scalable peer-to-peer lookup protocol for Internet applications. IEEE/ACM Trans. on Networking, 2003,11(1):17−32.

[56] Kaneko Y, Asaka T. DHT clustering for load balancing considering blockchain data size. In: Proc. of the 6th Int'l Symp. on Computing and Networking Workshops (CANDARW). 2018. 71−74.

[57] Xu ZH, Han SY, Chen L. CUB, a consensus unit-based storage scheme for blockchain system. In: Proc. of the 34th IEEE Int'l Conf. on Data Engineering (ICDE). 2018. 173−184.

[58] 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 2016). 2016. 17−30.

[59] 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). 2018. 583−598.

[60] Chen H, WangYJ. SSChain: A full sharding protocol for public blockchain without data migration overhead. Pervasive and Mobile Computing, 2019,59:1−15.

[61] Yoo H, Yim J, Kim S. The blockchain for domain based static sharding. In: Proc. of the 17th IEEE Int'l Conf. on Trust, Security and Privacy in Computing and Communications/12th IEEE Int'l Conf. on Big Data Science and Engineering (TrustCom/ BigDataSE). 2018. 1689−1692.

[62] Xu L, Chen L, Gao ZM, Xu SH, Shi WD. EPBC: Efficient public blockchain client for lightweight users. In: Proc. of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers (SERIAL 2017). 2017. 1−6.

[63] 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). 2019. 1−4.

[64] Frey D, Makkes MX, Roman PL, Taïani F, Voulgaris S. Bringing secure Bitcoin transactions to your smartphone. In: Proc. of the 15th Int'l Workshop on Adaptive and Reflective Middleware (ARM 2016). 2016. 1−6.

[65] Palai A, Vora M, Shah A. Empowering light nodes in blockchains with block summarization. In: Proc. of the 9th IFIP Int'l Conf. on New Technologies, Mobility and Security (NTMS). 2018. 1−5.

[66] Nadiya U, Mutijarsa K, Rizqi CY. Block summarization and compression in bitcoin blockchain. In: Proc. of the 2018 Int'l Symp. on Electronics and Smart Devices (ISESD). 2018. 1−4.

附中文参考文献:

[12] 刘敖迪,杜学绘,王娜,李少卓.区块链技术及其在信息安全领域的研究进展.软件学报,2018,29(7):2092−2115. http://www.jos.org.cn/1000-9825/5589.htm [doi: 10.13328/j.cnki.jos.005589]

[20] 史锦山,李茹.物联网下的区块链访问控制综述.软件学报,2019,30(6):1632−1648. http://www.jos.org.cn/1000-9825/5740.htm [doi: 10.13328/j.cnki.jos.005740]

[21] 蔡维德,郁莲,王荣,刘娜,邓恩艳.基于区块链的应用系统开发方法研究.软件学报,2017,28(6):1474−1487. http://www.jos.org.cn/1000-9825/5232.htm [doi: 10.13328/j.cnki.jos.005232]

[22] 翟社平,李兆兆,段宏宇,高山.区块链关键技术中的数据一致性研究.计算机技术与发展,2018,28(9):94−100.

[24] 潘晨,刘志强,刘振,龙宇.区块链可扩展性研究:问题与方法.计算机研究与发展,2018,55(10):2099−2110.

[30] 于戈,聂铁铮,李晓华,张岩峰,申德荣,鲍玉斌.区块链系统中的分布式数据管理技术——挑战与展望.计算机学报,2019,42:1−27.

[31] 曾诗钦,霍如,黄韬,刘江,汪硕,冯伟.区块链技术研究综述:原理、进展与应用.通信学报,2020,41(1):134−151.

[32] 贾大宇,信俊昌,王之琼,郭薇,王国仁.存储容量可扩展区块链系统的高效查询模型.软件学报,2019,30(9):2655−2670. http://www.jos.org.cn/1000-9825/5774.htm [doi: 10.13328/j.cnki.jos.005774]

[33] 袁勇,王飞跃.区块链技术发展现状与展望.自动化学报,2016,42(4):481−494.

[39] 张福泰,孙银霞,张磊,耿曼曼,李素娟.无证书公钥密码体制研究.软件学报,2011,22(6):1316−1332. http://www.jos.org.cn/1000-9825/4007.htm [doi: 10.3724/SP.J.1001.2011.04007]

[52] 陈晨,董超,茅娅菲,陈贵海,王海.无线网络编码感知路由综述.软件学报,2015,26(1):82−97. http://www.jos.org.cn/1000-9825/4696.htm [doi: 10.13328/j.cnki.jos.004696]

孙知信(1964−),男,博士,教授,博士生导师,主要研究领域为网络通信的理论与技术,计算机网络及安全.

相峰(1967−),男,硕士,主要研究领域为物流工程,企业管理.

张鑫(1996−),男,硕士生,主要研究领域为区块链存储技术与应用.

陈露(1995−),女,博士生,主要研究领域为网络安全技术,区块链技术.