基于树形结构构造的联盟链主从多链共识算法

张文芳[1],孙海锋[1],张晏端[1],唐荣骏[1],王小敏[1],马 征[1],李 暄[2],黄路非[2]
(1. 西南交通大学信息科学与技术学院,四川成都 610031; 2. 成都市第三人民医院,四川成都 610014)

摘 要: 区块链构建了一种价值互联的去中心化网络,是继互联网之后的最具革命性和颠覆性的创新技术.但现有区块链存在性能低下,隐私保护不足,单层链式结构难以支持多种场景下数字资产的分类并发处理,单链共识算法难以实现多链乃至全局的一致性等问题.为解决上述问题,本文基于树形结构设计一种适用于联盟链场景的主从多链架构,可实现不同数字资产的分类、并发处理和达到数据隔离的隐私需求.针对该树形主从多链架构,进一步提出一个基于门限签名的改进拜占庭容错共识算法,可解决多样化数字资产分类并发处理带来的一致性问题.性能分析和仿真结果表明:所提方案在实现隐私数据隔离保护的同时,兼具高并发交易性能,通信复杂度由$O(n^2)$降为$O(n)$,可满足企业多样化业务需求.

关键词: 联盟链;主从多链;树形结构;拜占庭容错共识算法
中图分类号: TP311;TP301 **文献标识码:** A **文章编号:** 0372-2112(2022)02-0257-10
电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20201212

A Consensus Algorithm for Consortium Chain with Tree Based Master-Slave Multi-Chain Architecture

ZHANG Wen-fang[1], SUN Hai-feng[1], ZHANG Yan-duan[1], TANG Rong-jun[1], WANG Xiao-min[1], MA Zheng[1], LI Xuan[2], HUANG Lu-fei[2]
(1. *School of Information Science and Technology, Southwest Jiaotong University, Chengdu, Sichuan* 610031, *China*;
2. *Chengdu Third People's Hospital, Chengdu, Sichuan* 610014, *China*)

Abstract: Blockchain constructs a decentralized network of value interconnection, which is the most revolutionary and subversive innovation technology after the Internet. However, the existing blockchain has some problems, such as low performance, insufficient privacy protection, single-layer chain structure being difficult to support the classification and concurrent processing of digital assets in multiple scenarios, and single-chain consensus algorithm being difficult to achieve multi-chain and even global consistency. In order to solve the above problems, this paper first designs a master-slave multi-chain architecture based on tree structure, which can realize the classification and concurrent processing of different digital assets, and meet the privacy requirement of data isolation. Secondly, a Byzantine fault-tolerant consensus algorithm is designed based on threshold signature to solve the consistency problem in the tree-based master-slave multi-chains. Performance analysis and experimental results show that the the proposed scheme has high concurrency performance and good privacy protection for data isolation, and the communication complexity is reduced from $O(n^2)$ to $O(n)$ which can meet the diversified business needs of enterprises.

Key words: consortium chain; master-slave multi-chain; tree structure; Byzantine fault-tolerant consensus algorithm

1 引言

区块链技术作为去信任化的分布式账本系统,在不依赖于第三方可信机构的前提下,实现点对点的可信价值传递[1].当前,区块链技术已经从作为比特币等数字货币底层技术的1.0时代过渡到智能合约和去中心化应用相结合的2.0时代,并将开启价值互联的3.0时代[2].区块链3.0将解决1.0时代应用范围受限,以及2.0时代性能受限而无法规模化应用等问题,促使越来越多的产业和区块链无缝衔接,其链上承载的资产交易也将从单一的加密货币交易上升到更加复杂和多样

收稿日期:2020-10-29;修回日期:2021-03-30;责任编辑:梅志强
基金项目:国家自然科学基金(No.61872302);四川省科技计划项目(No.2017SZYZF0002,No.2019YFH0097)

化的数字资产交易,多样化的数字资产交易对共识性能提出新的挑战.

以比特币[3]为代表的区块链开创了去中心账本先河,但以比特币为代表的区块链采用单层链式结构,将所有数字资产交易混合在一条链上处理,虽易于维持账本的一致性,但难以平行扩展复杂化和多样化的数字资产交易,也不便于分类管理;采用PoW类单一链上的共识机制,不涉及多链间资产一致性共识,无法满足社会生产多场景协作的应用需求,并且存在效率低下、耗能严重等问题. 因此,单层链式结构下的区块链存在性能、隐私、扩展性方面的技术瓶颈[4]. 为了扩展区块链性能,2015年,Poon等[5]提出闪电网络(Lightning Network),交易双方通过建立线下支付的微支付渠道,将主网承载的交易进行分流处理,大大降低了主网负荷,但链下交易内容未存储到区块链中,使得交易的追溯性受到损害. 2016年,Eyal等[6]通过引入关键区块和微区块提出一种可扩展的区块链协议Bitcoin-NG. 其中,关键区块选举记账人,微区块打包交易,通过选举的记账人在时间片段内创建多个微区块,扩展了区块链的交易处理容量,但Bitcoin-NG在比特币基础上改进,受限于单链结构,难以得到更多的商业应用. 另外,一些学者利用实用拜占庭容错共识算法(Practical Byazntine Fault Tolerant,PBFT)运行效率高、非概率性共识的优点,将PBFT算法与公有链共识算法相结合,构造出高效的混合共识算法(Hybrid Consensus)[7~10],如Tendermint[7]、ByzCoin[9]等,核心思想是先通过PoW、PoS[11]等公有链共识算法选举一定数量的节点作为委员会,委员会内部再依托高效的PBFT算法生产区块,从而扩大公有链交易规模,但不同程度继承了PBFT算法扩展性差以及公链共识算法效率低下、耗能严重等缺点. 2018年,Feng等[12]针对联盟链提出SDMA-PBFT共识算法,引入等级划分和代理人将全网节点分成数个子域,提案区块通过各子域代理人进行共识,减轻了主节点负担,提高了并行处理效率,然而当拜占庭节点成为代理人时,系统安全性将大幅降低. 2019年,Gao等[13]基于信用模型提出T-PBFT共识算法,由信用值高的节点构成共识群组,提升了拜占庭算法的容错率,但通信复杂度高达$O(n^2)$. 2020年,Du等[14]针对联盟链提出MBFT共识算法,利用分层技术将节点划分为两层共识群组,底层群组验证交易,上层群组打包区块,同时将共识群组分片,减少单个群组的负载,提高系统的吞吐量,但分片使得群组规模变小,共识更加趋于中心化. 同年,包振山等[15]针对PBFT算法的扩展性,采用树形拓扑结构对网络进行划分并引入信誉模型以提高安全性,底层子网运行PBFT算法,上层子网运行简化PBFT算法,通信复杂度降至$O(n^k)$(k为底层子网节点数),然而当子网中节点数较大时,通信复杂度仍然较高.

多层链式结构下的区块链不仅能对多样化的数字资产进行分类处理,还能提升系统并发处理能力,提高交易吞吐量. 2016年,Tsai等[16]将传统单层链式结构一分为二,提出账户区块链(ABC)和交易区块链(TBC)相结合的区块链架构. ABC负责查询、存储账户,TBC负责建块、执行交易,利用上述方法可实现负载均衡,但并未实现多样化数字资产的分类处理. 文献[17,18]通过楔入式侧链技术实现了链与链之间的资产交互,但侧链技术只是一种双向锚定协议,并非独立的区块链架构,并且该技术通常用于基于PoW共识的区块链,需要在交易速度与安全性之间做权衡. 2017年,IBM提出许可的商业区块链超级账本(Hyperledger Fabric)[19],采用多通道技术实现多链架构,每个通道各自维护一条链,不同通道间相互独立与隔离,然而通道间难以实现资产的转移和一致性. 2018年,闵新平等[20]提出许可链多中心架构,该架构中各中心主体维护交易区块链,所有中心主体维护全局区块链,全局区块链与交易区块链通过哈希值锚定保证数字资产交易的全局一致性,但该架构不能防止双花问题,并且其采用的PBFT共识算法会随着链的增多,性能急剧下降.

针对现有区块链性能低下,难以支持多种场景下数字资产的分类并发处理,难以实现多链共识等问题,本文首先面向联盟链设计一种树形主从多链架构,该架构基于树形结构对群组进行切分,使得树中的每一个父节点和其子节点组成一个通道,达到数据隔离的隐私需求;通过每个通道维护一条从链,所有通道共同维护一条主链,实现不同数字资产的分类处理;通过从链存储多样化交易内容,主链存储交易摘要,主从链通过哈希锁定的方式达到不可篡改和便于审计的目的;利用多个通道并行处理交易,解决现有区块链吞吐量低下和交易延迟过高等问题. 然后,针对树形结构的主从多链架构,设计基于门限签名的拜占庭容错共识算法来解决多样化数字资产分类并发处理带来的一致性问题,以及设计视图转换协议将失效或作恶的父节点向底层叶子节点位置调动,并将底层叶子节点替换到父节点位置,以获得强有力的系统活性保障. 分析表明,本文提出的主从多链结构突破了单链的功能和性能束缚,具有良好的高并发交易性能,同时兼顾隐私数据的隔离保护,满足企业多样化业务需求.

2 联盟链主从多链系统架构

联盟链是指由多个利益相关的机构共同参与和维护的区块链,其网络中的节点来自不同组织,互相缺乏信任且可能是拜占庭节点. 为了使系统能够容忍拜占庭错误,本方案采取树形结构来构造主从多链架构,树

中每一个父节点i对应的子节点数量$T_i \geqslant 3f_i$,f_i为父节点i及其子节点构成的通道中所能容忍的拜占庭节点数量. 主从多链架构按照T_i叉树对联盟链共识群组进行划分,得到树中每个父节点(除根节点)和其副本节点组成的下层通道,以及根节点和其副本节点组成的上层通道,并且其数量之和满足构成拜占庭容错系统要求,即每个通道内副本总数量$n \geqslant 3f_i+1$;父节点(除根节点)为各自下层通道的主节点,维护各自通道内的从链和主链,根节点为上层通道的主节点,负责构建主链;通道之间相互隔离,实现对不同数字资产的隐私保护,并以多通道并发处理数字资产交易的方式解决现有区块链技术吞吐量低和交易延迟高等问题.

考虑到实际的业务需求以及树过深会导致系统性能的下降,本方案采用深度为2的T_i叉树. 如图1所示,基于深度为2的T_i叉树对共识群组进行划分,形成相互独立、相互隔离的主从多链;树中每个父节点和其子节点都构成拜占庭容错系统,即ABCD、BEFG、CHIJKLM和DNOPQ组成的4个拜占庭容错系统. 其中ABCD构成上层拜占庭容错系统,负责构建主链;BEFG、CHIJKLM和DNOPQ构成下层拜占庭容错系统,负责维护主链以及各自通道内的从链.

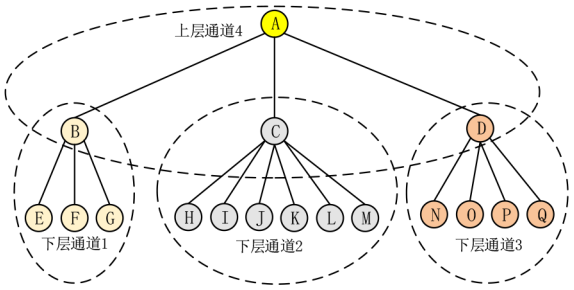


图1　主从多链系统架构

为实现主从多链之间的价值互联,在本文所构造的联盟链主从多链架构中,数字资产不仅可以在通道内部交易,还可以跨通道进行交易,实现链与链之间的互操作性,例如用户可以用某项资产交换不同机构的理财产品,不同的资产就需要在多条链上做转移、交换操作. 当进行链与链之间的互操作时,若将同一数字资产分别与不同的通道主体进行交易,同一资产将完成两次或者多次支付,则此类交易不满足全局一致性,故在联盟链主从多链架构中,不仅要保证通道内部交易的一致性,还要保证数字资产在跨通道交易时的一致性. 为了保证主从链的一致性,本文采用基于门限签名改进的拜占庭容错共识算法进行全网共识,由树中父节点收集其副本节点的投票信息(投票基于门限签名),当收集到的合法签名数量达到门限值t_i($t_i=2f_i+1$)时,父节点对投票信息进行聚合,然后向上层节点递归提交每个通道的门限签名状态,上层节点通过验证门限签名的合法性确认各通道交易的有效性以及状态是否达成一致,继而构建主链并广播给各下层通道,下层通道收到合法的主链区块后,将主链区块持久化写入到主链,同时更新本地的从链;主从链通过哈希相互锁定,保证交易的一致性和不可篡改性. 由此,针对联盟链主从多链架构下难以维护全局资产一致性问题,构建了高可信度的数字资产交易共识算法,保证数字资产的全局一致性,提高了区块链性能.

联盟链多链模型相关定义如下.

定义1　数字资产(Digital Assets,DA). 数字资产是指企业拥有或控制的,以电子数据的形式存在,或可被数字化的资产,比如:付费音乐、虚拟积分、房产等. 不同数字资产可被不同通道分类处理,数字资产通过全网唯一标识的数字身份进行转让、质押、租赁等各种交易操作.

定义2　通道(Channel). 类似发布-订阅模式消息传递通道,树中每一个父节点和其子节点都构成一个通道,通道之间数据隔离. 如图1所示,ABCD构成上层通道,负责构建主链,其中A是根节点,可为政府部门部署的监管节点,通过维护主链达到监管审计的目的. BEFG、CHIJKLM和DNOPQ构成下层通道,负责维护主链以及各通道内的从链.

定义3　节点(Node). 按照节点的职责,可以分为普通副本和主节点. 普通副本负责对提案进行投票;主节点可以进一步分为上层通道主节点和下层通道主节点,下层通道主节点一方面负责将所属通道的投票结果反馈给上层通道,另一方面负责从上层通道主节点获取最新的主链区块并在通道内部广播与同步. 上层通道主节点负责收集下层通道投票结果并构建主链区块.

定义4　背书群组(Endorsement Group,EG). 当涉及链之间的互操作时,为保证数字资产交易在各个通道中的状态保持一致,需要为相应的数字资产交易生成动态背书群组,由背书群组负责对其数字资产交易进行背书.

定义5　交易(Transaction,TX). 交易是指双方对数字资产进行价值的交换,一般包括两种交易方式:通道内数字资产交易和通道间数字资产交易. 通道内数字资产交易属于通道内部资产交易,由通道内交易发起人对其进行签名(如椭圆曲线签名算法)后在通道内部进行广播,然后由通道内成员对其进行基于门限签名的投票,父节点收集投票结果,将其提交到上层通道以写入到主区块链. 通道间数字资产交易涉及链之间的互操作,需由相应的背书群组对其背书,并将背书结果提交到上层通道以写入到主区块链.

定义6　主从多链(Master-slave Multiple Chain,MSMC). 如图2所示,相对"一链治所有"的单层链式结

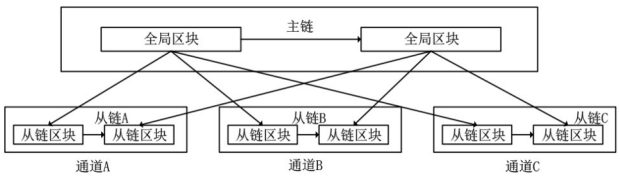


图2 主从多链模型

构,主从多链包括一条主链和多条从链,主从链均是按照时间戳顺序将数据区块以首尾相连的方式构成的独立区块链.从链存储通道内相关的数字资产交易内容,保证通道内局部一致性,由各自通道成员维护;主链存储所有通道内不存在双花交易的哈希值,保证数字资产全局一致且不可篡改,由全体成员共同维护.只有当从链交易的哈希值被写进主链,该从链交易才生效.主链的数据区块称为主链区块(Master Block,MB),也叫作全局区块,主链区块格式为

$$MB=<MB\_PBHash,MB\_Hight,MB\_MerkleTree,SB\_Hight> \quad (1)$$

其中,MB_PBHash为前一区块哈希值,MB_Hight为区块高度,MB_MerkleTree为交易的哈希值按照Merkle树方式组织的一种数据结构,SB_Hight为数字资产交易对应的从链标识,用于快速定位到相应的从链所在的区块高度.从链的数据区块称为从链区块(Slave Block,SB),从链区块格式为

$$SB=<SB\_PBhash,SB\_Hight,SB\_MerkleTree,MB\_Hight> \quad (2)$$

其中,SB_PBhash为前一区块哈希,SB_Hight为区块高度,SB_MerkleTree为交易的哈希值按照Merkle树方式组织的一种数据结构,MB_Hight为数字资产交易对应的主链标识,用于快速定位到相应的主链所在的区块高度.

3 门限签名

(t,n)门限签名[21]是指群体的签名密钥被n个成员以门限方式共享,任意大于等于t个成员的子集可以代表这个群体产生签名,而任意少于t个成员的子集则不能.在基于门限签名的拜占庭容错的共识算法中,将群体的签名权利以门限方式分散给各副本,各个副本采用门限的方式进行投票,投票达到门限值t时,才能生成决议的有效签名.这样的方法既保证了共识结果得到大多数副本的许可,又可在最小连通性的网络环境中实现低延迟、高鲁棒性的拜占庭容错共识算法.根据子密钥分发方式的不同,门限签名可分为两种类型:由可信任中心分发子密钥的门限签名方案和分布式分发子密钥的门限签名方案.本文采用分布式分发子密钥的门限签名方案,适合联盟成员互不信任的网络环境.门限签名的一般模型如下:

密钥生成Gen:输入安全参数k,输出系统公钥PK以及每个成员的私钥SK_i.

签名Sign:输入安全参数k、消息m以及成员私钥SK_i,产生部分签名σ_i,然后再由指定成员将达到门限值t的部分签名σ_i合成门限签名σ.

验证Verify:输入安全参数k、消息m、系统公钥PK和门限签名σ后,输出判断值"接受"或者"拒绝".

4 基于树形结构的联盟链主从多链共识算法

本文基于T_i叉树提出一种联盟链主从多链架构,该架构中每一个父节点和其子节点都构成一个通道,利用多通道并发处理数字资产交易,解决单链架构下数字资产交易混合处理导致的性能低下问题.但多通道并发处理可能导致数字资产不一致,并且现有以PoW、PBFT为主的共识算法均是以单链架构为背景,在多链架构下难以处理多样化数字资产并发交易.因此,本节针对树形结构的联盟链主从多链提出一种基于门限签名的改进拜占庭容错共识算法,通过上层通道与下层通道协作共识完成数字资产的验证与记链操作,主要包括通道内数字资产交易一致性共识算法和通道间数字资产交易一致性共识算法.

假设每个通道及背书群组已经预分发门限签名的秘密份额,每个成员拥有各自通道的群签名私钥,群公钥全网公开,设门限签名的门限值$t_i=2f_i+1$,设一般签名表示为Sig、门限签名表示为ThresholdSig以及门限签名中的部分签名表示为PartSig.

4.1 主从多链架构下通道内数字资产交易一致性共识算法

假设每个通道至多存在f个拜占庭节点,即满足$f\leqslant\lfloor(n-1)/3\rfloor$,并且假设拜占庭节点的行为可以是任意的,可以通过合谋方式欺骗诚实节点,破坏系统一致性,但是拜占庭节点计算能力有限,无法在多项式时间内突破密码机制,如签名算法.以图1主从多链架构为例,图中存在ABCD、BEFG、CHIJKLM和DNOPQ这4个最小拜占庭容错系统.其中ABCD属于上层拜占庭容错系统,BEFG、CHIJKLM和DNOPQ属于下层拜占庭容错系统,A、B、C和D为相应拜占庭容错系统的主节点.则在主从多链架构下的通道内数字资产交易一致性共识算法中,整体流程如图3所示,具体过程描述如下.

(1)下层通道的主节点(如B、C、D)收集本通道一段时间内发生的数字资产交易,统一检查并打包进区块,签名后向各自通道内的副本广播提案消息,其消息格式为$<Sig_{ip}(Proposal,v_i,h_i,Hash(Block_i)),Block_i>$,其中$Sig_{ip}$是通道$i$的主节点$p$签名,$v_i$是通道$i$的视图编号,$h_i$是通道$i$的提案区块高度,$Hash(Block_i)$是对通道$i$提

案区块$Block_i$的消息摘要.

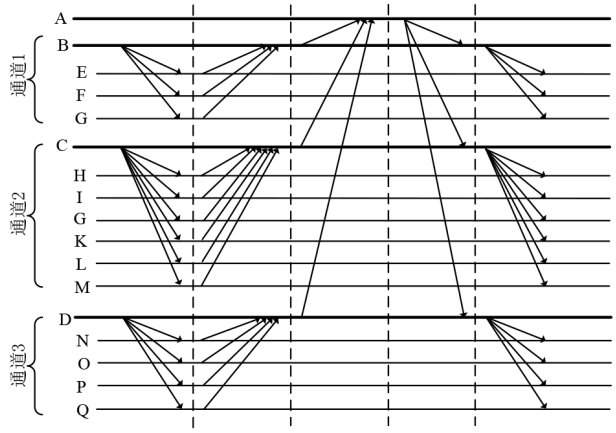


图3　基于门限签名的主从多链共识算法

(2)各通道内的副本收到各自主节点发来的提案消息后,检查消息签名是否正确、视图编号是否一致.如果通过验证,则向各自主节点发送基于门限签名的投票消息,具体消息格式为<$PartSig_{ij}$(VoteMsg, v_i, h_i, Hash($Block_i$), sk_{ij})>. 其中v_i是通道i的视图编号,h_i是通道i的区块高度,Hash($Block_i$)是对区块$Block_i$的消息摘要,sk_{ij}是通道i所属副本P_j的门限签名子密钥.

(3)当下层通道的主节点收到大于等于t_i-1(门限值t_i=2f_i+1)个来自所在通道不同副本发来的对同一个区块$Block_i$的部分签名投票消息后,首先验证部分签名是否正确、视图编号是否一致.如果验证通过,则连同自己的一条投票消息,对区块$Block_i$的投票数达到预期门限值t_i.此时,下层通道主节点合成门限签名ThresholdSig$_i$=ThresholdSig($PartSig_{i1}$, $PartSig_{i2}$, …, $PartSig_{it}$),向上层通道主节点(如A)发送投票结果并在本通道内广播,具体消息格式为<Sig_{ip}(VoteResult, v_i, h_i, ThresholdSig$_i$, Hash($Block_i$))>. 其中v_i是通道i的视图编号,h_i是通道i的区块高度,ThresholdSig$_i$是对区块哈希值Hash($Block_i$)的门限签名.

(4)上层通道的主节点收集到各通道的投票结果后,首先验证门限签名是否正确、视图编号是否一致,如果验证通过,对下层通道主节点发来的交易(区块哈希值Hash($Block_i$))按照一定规则进行排序,构造主链区块MB,之后将主链区块MB广播给与其通信的下层通道主节点,消息格式为<Sig_m(MasterBlockMsg, h, Hash(MB), ThresholdSig$_l$(l=1, 2, …, d)), MB>. 其中Sig_m是上层通道主节点的签名,h为主链区块高度,MB为主链区块,包含下层通道所提交区块哈希值的集合,ThresholdSig$_l$(l=1, 2, …, d)是下层通道对Hash($Block_l$)的门限签名,d为下层通道提交的门限签名个数.

(5)下层通道主节点收到上层通道的主节点发来的主链区块消息后,在通道内部进行广播与同步.当各通道副本收到主链区块消息后,首先验证上层通道的主节点的签名是否正确,以及主链区块中所包含的每一个通道区块哈希值对应的门限签名是否正确.如果验证通过,将主链区块持久化写入到全局区块链,同时更新本地的从链区块链.

4.2　主从多链架构下通道间数字资产交易一致性共识算法

在基于树形构造的联盟链多链架构中,数字资产不仅可以在通道内部进行交易,还可以在通道间进行交易.由于通道间交易的数字资产涉及多个通道,当同一数字资产在不同通道同时进行交易时,易造成双花问题.为保证跨通道间资产交易在各个通道中的状态保持一致,首先从交易相关通道中选取背书群组,由背书群组负责对跨通道交易进行背书,并将背书结果反馈到上层通道进行全局共识.

假设通道间交易的数字资产涉及k个通道,为保证背书群组中至少存在三分之二的诚实背书节点,需要从k个通道中选取$r>\sum_{i=1}^{k}3f_i+1$个背书节点,且每个通道至少选择$3f_i$名节点作为背书节点.背书群组内部选择一名背书节点作为背书群组主节点.

(1)各通道主节点收集本通道一段时间内发生的跨通道交易,统一检查并打包进区块,签名后发送至背书群组,其消息格式为<Sig_{ip}(Proposal, v_i, h_i, Hash($Block_i$)), $Block_i$>. 其中Sig_{ip}是通道i的主节点p的签名,v_i是通道i的视图编号,h_i是通道i的提案区块高度,Hash($Block_i$)是对通道i提案区块$Block_i$的消息摘要.

(2)背书群组接收到通道间交易后,验证区块中的每一笔交易是否满足全局一致性,即同一时刻对同一数字资产的交易只允许出现一次.如果通过验证,则背书群组成员进行基于门限签名的背书签名,并向背书群组主节点发送背书签名消息,其消息格式为<$PartSig_{ij}$(Endorsement, v_i, h_i, Hash($Block_i$), sk_j)>. 其中v_i是通道i的视图编号,h_i是通道i的区块高度,Hash($Block_i$)是对区块$Block_i$的消息摘要,sk_j是背书群组所属成员P_j的门限签名子密钥.

(3)当背书群组主节点收到大于等于t_i-1(门限值$t_i=\sum_{i=1}^{k}2f_i+1$)个背书群组成员发来的对同一个区块$Block_i$的背书签名消息后,首先验证部分签名是否正确、视图编号是否一致.如果验证通过,则连同自己的一条背书签名消息,对区块$Block_i$的投票数达到预期门限值t_i,此时背书群组主节点合成门限签名ThresholdSig$_i$=ThresholdSig($PartSig_{i1}$, $PartSig_{i2}$, …, $PartSig_{it}$)作为背书结果,将背书结果附在提案消息后转发至上层通道主节点并在背书群组内广播,具体消息格式为<Sig_{ip}(Propos-

al, v_i, h_i, Hash(Block$_i$)), ThresholdSig$_i$>. 其中 v_i 是通道 i 的视图编号, h_i 是通道 i 的区块高度, Hash(Block$_i$)是对区块 Block$_i$ 的消息摘要, ThresholdSig$_i$ 是对提案区块 Block$_i$ 的背书签名.

(4)上层通道主节点收到附有背书签名的提案消息后,首先验证背书签名是否正确、视图编号是否一致. 如果验证通过,构造主链区块 MB,并将主链区块 MB 广播给与其通信的下层通道主节点,具体消息格式为<Sig$_m$(MasterBlockMsg, h, Hash(MB), ThresholdSig$_l$(l=1,2,⋯,d)), MB>. 其中 h 为全局区块高度, MB 为主链区块,包含了下层通道提交的区块哈希值, ThresholdSig$_l$(l=1,2,⋯,d)是背书群组对 Hash(Block$_l$)提交的门限签名, d 为背书群组提交的门限签名个数.

(5)下层通道主节点收到上层通道的主节点发来的主链区块消息后,在通道内部进行广播与同步. 当各通道副本收到全局区块消息后,首先验证上层通道的主节点的签名是否正确,以及全局区块中所包含的门限签名是否正确. 如果验证通过,将全局区块持久化写入到主区块链,同时更新本地的从区块链.

4.3 视图转换

设 delay(t)表示副本发送基于门限签名的投票消息到副本最终接受到主链区块的时间间隔. 因为只有交易的哈希值被写进主链,该交易才会生效,所以当某通道副本等待时间超过预设值 delay(t)时仍然没有收到主链区块,启动视图转换协议,更换通道主节点,以避免陷入无限等待. 视图转换流程如下.

(1)当通道 i 的副本 P_j 进入视图转换协议后,令视图编号 $v_{new}=v+1$,其中 v 是通道 i 的当前视图编号,向其他副本广播 View-Change 消息,其消息格式为<Sig$_j$(View-Change, v_{new}, h, Hash(Block$_i$))>. 其中 h 为区块高度, Hash(Block$_i$)为通道 i 的主节点在高度 h 提交的从链区块哈希值. 如果副本 P_j 在高度 h 没有收到提案区块则为 null.

(2)其他副本 P_u 在收到 View-Change 消息后,同样令视图编号 $v_{new}=v+1$,广播 View-Change 消息,其消息格式为<Sig$_u$(View-Change, v_{new}, h, Hash(Block$_i$), Hash(MB), PartSig$_u$, ThresholdSig$_l$(l=1, 2, ⋯, d))>. 其中, Hash(Block$_i$)为通道 i 的主节点在高度 h 提交的从链区块哈希值, Hash(MB)为全局主链区块的哈希值, PartSig$_u$ 为副本 P_u 对 Hash(Block$_i$)进行投票的部分签名, ThresholdSig$_l$(l=1,2,⋯,d)是对包含在全局区块中的从链区块哈希值的门限签名, d 为下层通道提交的门限签名个数. 如果副本 P_u 没有收到对应字段信息则为 null.

(3)新视图 v_{new} 的主节点 P_{new} 利用收到的 View-Change 消息中的 PartSig 和 ThresholdSig 字段,构造 New-View 消息:

1)如果 P_{new} 收到的 View-Change 消息中至少有一条包含合法 ThresholdSig$_l$(l=1,2,⋯,d),则向其他副本广播 New-View 消息,其消息格式为<Sig$_{P_{new}}$(New-View, v_{new}, h, Hash(Block$_i$), Hash(MB), ThresholdSig$_l$(l=1,2,⋯,d))>;

2)如果 P_{new} 收到的 View-Change 消息中有 t_i 条对 Hash(Block$_i$)的部分签名 PartSig,则合成门限签名 ThresholdSig$_i$,并向上层通道主节点发送 New-View 消息,其消息格式为<Sig$_{P_{new}}$(New-View, v_{new}, h, ThresholdSig$_i$, Hash(Block$_i$))>;

3)如果 P_{new} 没有收到一条消息包含合法的 ThresholdSig$_l$(l=1,2,⋯,d),也没有收到对 Hash(Block$_i$)的 t_i 条部分签名 PartSig,则选择新的提案 Block$_{new}$,并向其他副本广播新的提案消息,其消息格式为<Sig$_{P_{new}}$(New-View, v_{new}, h, Hash(Block$_{new}$), Block$_{new}$)>.

如果是上述第一种情况,将 New-View 消息在通道内部进行广播同步即可. 如果是上述第二种情况,上层通道主节点收到 New-View 消息后,首先验证门限签名是否正确、视图编号是否一致;如果验证通过,重新构造主链区块 MB,并将主链区块 MB 广播给与其通信的下层通道主节点,具体消息格式为<Sig$_m$(MasterBlockMsg, h, Hash(MB), ThresholdSig$_l$(l=1,2,⋯,d)), MB>,下层通道主节点收到新的全局区块后在通道内部进行广播,其他副本同步更新主从链. 如果是上述第三种情况,先由主节点 P_{new} 收集与合成门限签名,再向上层通道主节点提交 New-View 消息,后续过程与第二种情况类似,此处不再赘述.

5 性能分析

5.1 安全性、活性、一致性证明

假定每个通道中至多存在 $f_i\left\lfloor\left(n_i-1\right)/3\right\rfloor$ 个拜占庭节点(f_i 为通道 i 内的拜占庭节点数, n_i 为通道 i 内的总节点数).

引理 1 每个通道对通道内资产交易的投票结果是可信的.

证明 由拜占庭系统定理可知,当拜占庭容错系统中有 f 个拜占庭节点时,若系统总节点数 $n\geq 3f+1$,系统总能达成一致[22]. 本方案基于 T_i 叉树构建主从多链,使得每个通道内的副本数量总和满足 $n\geq 3f_i+1$,即每个通道都构成拜占庭容错系统.

假设下层通道 i 的主节点 p 为拜占庭节点,在收集本通道内产生的数字资产交易后, p 将错误交易信息打包进区块 Block$_i$,并将其在通道 i 内广播. 根据系统条件,通道 i 内至多存在 $f_i\left\lfloor\left(n_i-1\right)/3\right\rfloor$ 个拜占庭节点,最后 p 收到的同意投票数最多为 f_i-1 个(小于 $t_i-1=2f_i$ 个),因此无法合成合法的门限签名 ThresholdSig$_i$.

由以上分析可知,每个通道对通道内资产交易的

投票结果是可信的. 证毕

引理 2 背书群组对跨通道资产交易的背书结果是可信的.

证明 由4.2节可知背书群组节点数N满足

$$N>\sum_{i=1}^{k}3f_i+1 \tag{3}$$

在最坏的情况下,与跨通道资产交易相关通道中的拜占庭节点全被选为背书节点,这些拜占庭节点试图通过合谋来破坏系统一致性. 但由系统条件知,每个下层通道i中存在的拜占庭节点数f_i满足

$$f_i\leqslant\left\lfloor\left(n_i-1\right)/3\right\rfloor \tag{4}$$

由式(3)和式(4)可以推出,背书群组中存在的拜占庭节点数N_f满足

$$N_f\leqslant\sum_{i=1}^{k}f_i \tag{5}$$

即背书群组中的拜占庭节点数至多为$\sum_{i=1}^{k}f_i$.

由式(3)和式(4)可得,背书群组中至少存在$\sum_{i=1}^{k}3f_i+1-\sum_{i=1}^{k}f_i=\sum_{i=1}^{k}2f_i+1$个诚实节点,则在背书群组中的诚实节点数至少占总节点数的三分之二. 根据拜占庭容错系统原理,背书群组满足拜占庭容错性,即背书群组对跨通道资产交易的背书结果是可信的. 证毕

定理 1 本文构建的主从多链架构是安全的.

证明 本文构建的主从多链架构主要涉及通道内资产交易和通道间资产交易,由引理1和引理2可知,当通道i内至多存在$f_i\leqslant\left\lfloor\left(n_i-1\right)/3\right\rfloor$个拜占庭节点时,通道内资产交易和通道间资产交易均是可信的,故本文构建的主从多链架构是安全可信的. 证毕

定理 2 本文采用基于门限签名改进的拜占庭容错共识算法是安全可靠的.

证明 在基于门限签名改进的拜占庭容错共识算法中,群体的签名权利以门限方式(门限值$t_i=2f_i+1$)分散给通道内各副本,通道内各副本采用门限签名的方式进行投票达成共识,当通道内对某一区块提案的投票数达到门限值t_i时,才能生成通道内决议有效的投票结果,并由通道主节点将此投票结果发送至上层通道构建全局区块,即全局区块包含了各通道代表法定人数投票意愿的门限签名,所有通道节点收到全局区块后只需验证该门限签名的合法性,即可对该通道的投票结果以及全局区块的有效性进行安全验证,故本文采用基于门限签名改进的拜占庭容错共识算法是安全可靠的. 证毕

定理 3 本文构建的主从多链架构具有较强的不可篡改特性.

证明 在基于POW共识算法构造的公有链中,每一个区块都获得一定的算力保障,攻击者想要篡改某一区块,需要掌握全网51%的算力,篡改难度大. 在基于PBFT共识算法构造的联盟链中,失去算力保障的区块仅依靠分布式存储来保证不可篡改,难以防止节点之间相互合谋篡改数据,篡改成本低. 在本文构造的主从多链架构中,主链保存交易哈希值,从链保存交易内容,主从链通过哈希值的方式相互锁定. 假设某通道成员以合谋的方式篡改通道内部的从链交易,若要使篡改的区块生效,则同时需要篡改全网成员保存的主链交易,篡改的代价相对较大,故本文构建的主从多链模型具有较强的不可篡改特性. 证毕

定理 4 系统共识进程不会因为拜占庭节点的作恶行为而中断,即本文方案具有活性.

证明 根据区块链架构设定,每个通道内至多存在$f\leqslant\left\lfloor(n-1)/3\right\rfloor$个拜占庭节点. 由引理1、引理2和定理1可知,下层通道内的数字资产交易以及跨通道资产交易的背书结果均是可信. 如果主节点p作恶,未发送门限签名投票结果至上层通道,或由于网络问题宕机,使共识进程处于停滞状态,由4.3节可知,系统将根据视图切换协议,开启新的共识进程,避免陷入无限等待,进而使主从多链架构保持了活性. 证毕

引理 3 若下层通道i上传提案区块Block_i,则主链中一定会包含Block_i.

证明 当下层通道i的主节点p收到大于等于t_i-1(门限值$t_i=2f_i+1$)个所在通道不同副本对Block_i的投票消息,验证通过后合成门限签名$\mathrm{ThresholdSig}_i$,并向上层通道主节点m发送投票结果.

上层通道主节点m按一定顺序收集各下层通道上传的提案区块且对提案的投票结果验证通过后,m将各通道发送的提案区块的哈希值按一定顺序构造主链区块MB并签名,广播给下层通道主节点,下层通道主节点收到主链区块消息后在各自通道内广播. 由4.1节可知,通道i内各副本通过验证Block_i的哈希值、$\mathrm{ThresholdSig}_l(l=1,2,\cdots,d)$以及$\mathrm{Sig}_m$的正确性,即可就主链区块达成共识,进而使提案区块$\mathrm{Block}_i$上链. 证毕

引理 4 若背书群组上传提案区块Block_i,则主链中一定会包含Block_i.

证明 假设通道间交易的数字资产涉及k个通道,则需要从k个通道中选取$r>\sum_{i=1}^{k}3f_i+1$个背书节点,且每个通道至少选择$3f_i$名节点作为背书节点. 由4.2节易知,若背书群组上传提案区块Block_i,则主链中一定会包含Block_i,证明过程与引理3类似,此处不再赘述. 证毕

定理 5 本文方案具有一致性.

证明 由引理3和引理4易知,本文方案具有一致

性. 证毕

5.2 性能对比

本节将从区块链架构和共识算法两方面与现有主流方案进行比较,进而得出本方案的综合评价结果,详见表1.

由表1可知,Bitcoin[3],Bitcoin-NG[6],Ethereum和MBFT[14]采用单层链式结构,将所有交易混合在一条链上处理,难以实现数据之间的隔离. Bitcoin,Bitcoin-NG和Ethereum采用PoW共识算法,其去中心化程度较高、容错率较高,并且每一区块获得算力保障,数据篡改难度大,但采用的PoW共识算法存在吞吐量低、延迟高等问题,影响系统的可扩展性,尽管Bitcoin-NG通过引入关键区块和微区块解决了可扩展性问题,但仍然需要"挖矿",效率没有得到质的提升.

表1 方案性能对比

方案	架构	共识机制	容错率	去中心化程度	分叉	数据隔离	跨链处理	抗双花	通信复杂度
Bitcoin[3]	单链	PoW	50%	完全	有	×	×	√	
Bitcoin-NG[6]	单链	PoW	50%	完全	有	×	×	√	
Ethereum[23]	单链	PoW	50%	完全	有	×	×	√	
T-PBFT[13]	单链	PBFT	50%	半去中心化	无	×	×	×	$O(n^2)$
MBFT[14]	单链	MBFT	33%	半去中心化	无	×	×	√	$O(n)$
文献[15]	单链	TTNPBFT	33%	半去中心化	无	×	×	√	$O(n^k)$
Fabric[19]	多链	PBFT	33%	半去中心化	无	√	×	√	$O(n^2)$
文献[20]	多链	PBFT	33%	半去中心化	无	√	√	×	$O(n^2)$
本方案	多链	*	33%	半去中心化	无	√	√	√	$O(n)$

注:×表示不支持该性能,√表示支持该性能,*表示本方案采用的共识

基于PBFT的共识方案,具有强一致性、不容易出现分叉、效率较高等特点,但往往通信复杂度较高. 如,T-PBFT[13]根据信用评价模型选出高信用共识群组以提升系统容错率,但其通信复杂度仍高达$O(n^2)$,随着节点的增多,系统性能会大幅降低,并且不适用于多链架构. MBFT[14]通过分片和分层技术,提高了交易速度,但由于分片使得共识群组越来越小,中心化程度加深,并且也不适用于多链架构. 文献[15]引入树形拓扑结构提高系统可扩展性,但由于其各层子网使用PBFT共识算法,在子网规模较大的情况下仍然无法有效地降低通信复杂度,且信誉模型的引入会使整个系统趋于中心化,同时也不适用于多链架构. Fabric[19]和文献[20]采用多层链式结构,实现交易的并发与隔离处理,但由于采用了PBFT共识算法,面临着可扩展性不足等问题,系统性能随着节点数的增多而急剧下降. 此外,Fabric不支持跨链操作,难以满足现实生活多协作场景应用需求,通道成员数量有限且相对固定,数据易被合谋篡改. 文献[20]采用基于交易哈希值的动态验证算法以防止双花问题,但基于交易哈希值的动态验证算法只能识别具有相同交易哈希值的双花交易,若同一时刻同一数字资产与不同主体发生交易,不同主体间的交易哈希值不同,使得基于交易哈希值的动态验证算法难以识别交易的输入是否来自同一数字资产.

本方案基于T_i叉树构造主从多链架构,主从链通过哈希值相互锁定,难以篡改交易内容;通过从链并发处理交易,在提升交易速度的同时实现交易的隔离处理;同时采用基于门限签名改进的拜占庭容错算法避免了两两交互,从而将通信复杂度降为$O(n)$. 另外,门限签名包含法定人数投票意愿,其他副本只需验证一条门限签名即可对投票结果的一致性进行安全验证,有效降低了签名验证复杂度.

6 实验仿真

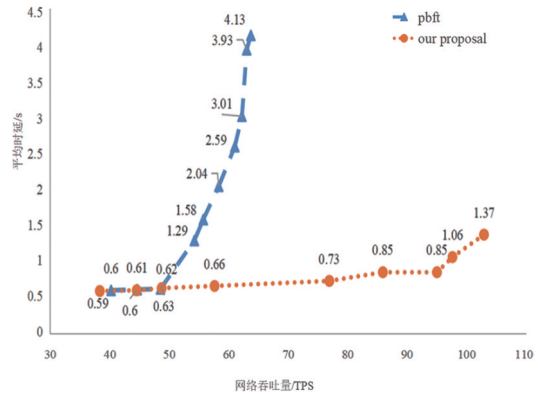
本文参考联盟链框架Hyperledger Fabric,利用其多通道及可插拔共识模块实现树形主从多链的架构及其共识算法,同时选用单链架构下的PBFT算法作为参照,在同等硬件条件下采用区块链性能测试工具Caliper进行测试,分别得到本文多链共识算法和PBFT算法的网络时延和吞吐量,以此来对比分析算法的性能优劣. 所做实验采用4 GB内存、50 GB硬盘及Intel(R) i5-6300HQ处理器的硬件平台. 由于硬件条件限制,设置网络结构为最小拜占庭系统,即每个通道为最小拜占庭系统,PBFT算法和本文算法设置为同样大小的网络架构,均包含13个orderer共识节点和一个peer节点. 本次实验用到的3个测试链码如表2所示.

表2 链码接口

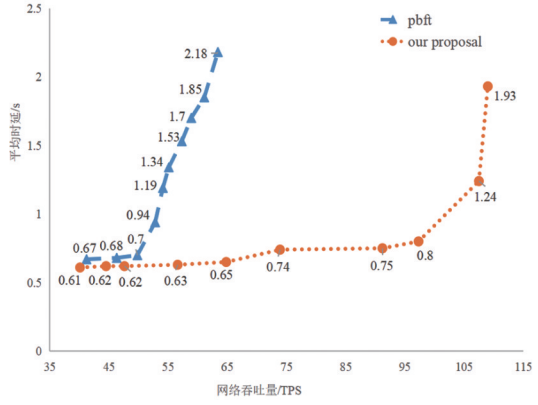
SDK接口名	接口功能	接口接收参数
open	开户	账户名、金额
transfer	转账	账户名、账户名、金额
delete	销户	账户名

实验采用区块链性能测试工具Caliper对3个测试链码进行测试,系统交易数量设为500(考虑测试效率,transfer.js的交易数设为250),通过调整交易发送速率,来观察时延和吞吐量的变化. 将交易发送速率从

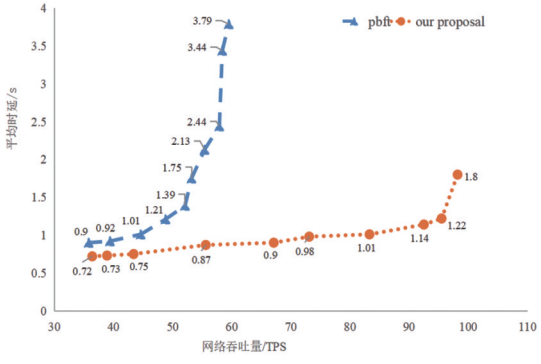
50 TPS(交易/秒)递增到100 TPS的网络吞吐量和时延结果制图(每间隔5 TPS绘制一个点),横坐标为网络吞吐量,纵坐标为时延,得到测试链码open.js,transfer.js,delete.js的吞吐量(Throughput)-时延(Latency)图,如图4所示.



(a) open.js



(b) transfer.js



(c) delete.js

图4　吞吐量-时延图

从图4可看出,本文算法有着较高的峰值吞吐量以及较低的时延,而PBFT算法峰值吞吐量较低、时延较高,具体而言:

(1)本文多链系统的峰值吞吐量比PBFT系统的峰值吞吐量大约高了57%,并且当交易发送速率接近70 TPS的时候,PBFT系统基本达到了峰值吞吐量,而本系统的吞吐量在交易发送速率接近110 TPS时才会逐渐达到峰值;

(2)Caliper测试工具的输出结果Avgrage Latency表示一个交易从进入系统到最终写入区块的时间.从图中可以看出,两个系统的时延都会随着吞吐量的增加而增加,但本文多链系统的时延增长较慢,而PBFT系统的时延会随着吞吐量的增加急剧增加.

从上述仿真结果可以看出,本系统在多节点高发送率高交易量的情况下,吞吐量和时延优于传统的PBFT方案.

7　结论

本文针对现有区块链性能低下,难以支持多种场景下数字资产的分类并发处理、难以实现多链共识等问题,首先面向联盟链提出了一种树形主从多链架构,该架构通过树形结构将群组切分成多条子链,利用子链分类并行处理多样化数字资产交易,有效解决了现有区块链吞吐量低下和交易延迟过高等问题.其次针对树形结构的主从多链架构,设计基于门限签名的拜占庭容错共识算法解决多样化数字资产分类并发处理带来的一致性问题,同时设计视图转换协议实现强有力的系统活性保障.

参考文献

[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.
SHAO Q F, JIN C Q, ZHANG Z, et al. Blockchain: Architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(5): 969-988. (in Chinese)

[2] EFANOV D, ROSCHIN P. The all-pervasiveness of the blockchain technology[J]. Procedia Computer Science, 2018, 123: 116-121.

[3] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. (2008-11-01) [2022-01-17]. http://bitcoin.org/bitcoin.pdf.

[4] 蔡维德, 郁莲, 王荣, 等. 基于区块链的应用系统开发方法研究[J]. 软件学报, 2017, 28(6): 1474-1487.
TSAI W D, YU L, WANG R, et al. Blockchain application development techniques[J]. Journal of Software, 2017, 28 (6): 1474-1487. (in Chinese)

[5] POON J, DRYJA T. The bitcoin lightning network: Scalable off-chain instant payments[R/OL]. (2016-01-14) [2022-01-17]. https://lightning.network/lightning-network-paper.pdf.

[6] EYAL I, GENER A E, SIRER E G. et al. Bitcoin-NG: A

scalable blockchain protocol[C]//13th USENIX Symposium on Networked Systems Design and Implementation. Santa Clara, USA: USENIX, 2016: 45-59.

[7] JAE K. Tendermint: Consensus without mining[R/OL]. (2014)[2022-01-17]. https://tendermint.com/static/docs/tendermint.pdf.

[8] PASS, RAFAEL, ELAINE S. Hybrid consensus: Efficient consensus in the permissionless model[C]//31st International Symposium on Distributed Computing(DISC 2017). Vienna, Austria: Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2017: 39-55.

[9] KOGIAS E K, JOVANOVIC P, GAILLY N, et al. Enhancing bitcoin security and performance with strong consistency via collective signing[C]//25th USENIX Security Symposium(USENIX Security 16). Austin, USA: USENIX ASSOC, 2016: 279-296.

[10] PASS R, SHI E. Thunderella: Blockchains with optimistic instant confirmation[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. New York, USA: Springer, 2018: 3-33.

[11] VASIN P. Blackcoin's proof-of-stake protocol v2 [R/OL]. (2014-07-01)[2022-01-17]. https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf.

[12] FENG L B, ZHANG H, CHEN Y, et al. Scalable dynamic multi-agent practical Byzantine fault-tolerant consensus in permissioned blockchain[J]. Applied Sciences, 2018, 8 (10): 1919.

[13] GAO S, YU T Y, ZHU J M, et al. T-PBFT: An EigenTrust-based practical Byzantine fault tolerance consensus algorithm[J]. China Communications, 2019, 16(12): 111-123.

[14] DU M X, CHEN Q J, MA X F. MBFT: A new consensus algorithm for consortium blockchain[J]. IEEE Access, 2020, 8: 87665-87675.

[15] 包振山, 王凯旋, 张文博. 基于树形拓扑网络的实用拜占庭容错共识算法[J]. 应用科学学报, 2020, 38(1): 34-50.
BAO Z S, WANG K X, ZHANG W B. A practical Byzantine fault tolerance consensus algorithm based on tree topological network[J]. Journal of Applied Sciences, 2020, 38(1): 34-50. (in Chinese)

[16] TSAI W T, BLOWER R, ZHU Y, et al. A system view of financial blockchains[C]//2016 IEEE Symposium on Service-Oriented System Engineering(SOSE). Oxford, UK: IEEE, 2016: 450-457.

[17] BACKA A, CORALLO M, DASHJRET L, et al. Enabling blockchain innovations with pegged sidechains [R/OL]. (2014-10-22) [2022-01-17]. https://www.blockstream.com/sidechains.pdf.

[18] ROOTSTOCK. Sidechains, drivechains and RSK 2-way peg designs[EB/OL]. (2015) [2022-01-17]. https://blog.rsk.co/noticia/sidechains-drivechains-and-rsk-2-way-peg-design/.

[19] SOUSA J, BESSANI A, VUKOLIC M. A Byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform[C]//Proceedings of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers. Las Vegas, Nevada, USA: ACM, 2017, 6: 1-2.

[20] 闵新平, 李庆忠, 孔兰菊, 等. 许可链多中心动态共识机制[J]. 计算机学报, 2018, 41(5): 1005-1020.
MIN X P, LI Q Z, KONG L J, et al. Permissioned blockchain dynamic consensus mechanism based multi-centers [J]. Chinese Journal of Computers, 2018, 41(5): 1005-1020. (in Chinese)

[21] PARK C, KUROSAWA K. New Elgamal type threshold digital signature scheme[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 1996, 79(1): 86-93.

[22] LESLIE L, ROBERT S, MARSHALL P. The Byzantine generals problem[J]. ACM Transactions on Programming Languages and Systems(TOPLAS), 1982, 4(3): 382-401.

[23] GAVIN WOOD. Ethereum: A secure decentralised generalised transaction ledger[EB/OL]. (2014-01-14) [2022-01-17]. http://gavwood.com/Paper.pdf.

作者简介

张文芳 女, 1978 年出生于山西省太原市. 博士, 西南交通大学副教授, 硕士生导师. 主要研究方向为密码学和信息安全.
E-mail: wfzhang@swjtu.edu.cn

王小敏(通讯作者) 男, 1974 年出生于江西省萍乡市. 博士, 西南交通大学教授, 博士生导师. 主要研究方向为信息安全和轨道交通安全工程.
E-mail: xmwang@swjtu.edu.cn