基于超图和MuSig2聚合签名的联盟链主从多链共识机制

景 旭[1,2],刘滋雨[1,2]
(1. 西北农林科技大学信息工程学院,陕西杨凌 712100;2. 陕西省农业信息智能感知与分析工程技术研究中心,陕西杨凌 712100)

摘 要: 针对多链式区块链采用主链最终共识机制,导致主链负载大,制约从链性能等问题,论文提出一种基于超图和MuSig2聚合签名的联盟链主从多链共识机制. 首先根据超图理论,构建以横贯超图为主链,子超图为从链的联盟链主从多链架构;然后借鉴分治思想,结合“背书-排序-验证”的共识方式,构建分层分类共识机制,通过分类处理交易降低主链负载压力;最后构建基于MuSig2聚合签名的联盟链多方背书签名方法,提升背书签名的验证效率. 性能分析表明:基于MuSig2聚合签名的联盟链多方背书签名安全可靠,基于超图和MuSig2聚合签名的分层分类共识机制具有强一致性和线性时间复杂度. 实验结果表明:基于MuSig2聚合签名的多方背书方法的总效率是椭圆曲线数字签名算法(Elliptic Curve Digital Signature Algorithm,ECDSA)的1.55倍,分层分类共识机制能够提升12.5%的共识效率. 该机制具有较高性能,可满足企业多样化业务需求.

关键词: 区块链;联盟链;主从多链;分层分类共识机制;聚合签名;超图
基金项目: 陕西省重点研发计划(No.2019ZDLNY07-02-01);国家重点研发计划(No.2020YFD1100601)
中图分类号: TP311;TP301 **文献标识码:** A **文章编号:** 0372-2112(2024)03-0803-11
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20220972

Master-Slave Multi-Chain Consensus Mechanism of Consortium Blockchain Based on Hypergraph and MuSig2

JING Xu[1,2], LIU Zi-yu[1,2]
(1. *College of Information Engineering*, *Northwest A&F University*, *Yangling*, *Shaanxi* 712100, *China*;
2. *Shaanxi Engineering Research Center of Agricultural Information Intelligent Perception and Analysis*, *Yangling*, *Shaanxi* 712100, *China*)

Abstract: To solve the problems of multi-chain blockchain using the final consensus mechanism of the main blockchain, resulting in a large load on the main blockchain and restricting the performance of the slave blockchain, a master-slave multi-chain consensus mechanism of the consortium blockchain based on hypergraph and MuSig2 aggregate signature is proposed. Firstly, according to the hypergraph theory, a master-slave multi-chain architecture of the consortium blockchain with the transverse hypergraph as the main blockchain and the sub-hypergraph as the slave blockchain is constructed. Then, drawing on the divide and conquer ideology, combined with the consensus mode of “endorsement-sorting-verification”, a hierarchical classification consensus mechanism is constructed to reduce the load pressure of the main chain through classification processing transactions. Finally, a multi-party endorsement signature method based on MuSig2 aggregate signature is constructed to improve the verification efficiency and performance of endorsement signatures. Performance analysis shows that the multi-party endorsement signature of the consortium blockchain based on MuSig2 aggregate signature is safe and reliable, and the hierarchical classification consensus mechanism based on hypergraph and MuSig2 aggregate signature has strong consistency and linear time complexity. Experimental result shows that the total efficiency of the multi-party endorsement method based on MuSig2 aggregate signature is 1.55 times that of elliptic curve digital signature algorithm(ECDSA), and the hierarchical classification consensus mechanism can improve the consensus efficiency by 12.5%. This mechanism has high performance and can meet the diversified business needs of enterprises.

Key words: blockchain; consortium blcokchain; master-slave multi-chain; hierarchical classification consensus mechanism; aggregate signature; hypergraph

收稿日期:2022-08-18;修回日期:2023-02-09;责任编辑:梅志强

Foundation Item(s): Key Research and Development Program of Shaanxi (No.2019ZDLNY07-02-01); National Key Research and Development Program of China (No.2020YFD1100601)

1 引言

区块链技术是以数据库作为数据存储载体,以对等网络(Peer-to-Peer,P2P)作为通信载体,依赖密码学确定所有权和保障隐私,依靠分布式系统共识框架保障一致性,旨在构建价值交换系统的技术[1]. 当前,区块链技术已经从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,将开启价值互联的3.0时代[2]. 区块链3.0时代将会通过多链技术和跨链技术实现可多链并行和跨链交互的多链式区块链新生态系统[3],以解决1.0时代应用范围受限和2.0时代性能受限而无法规模化应用等问题. 这将促使越来越多的产业和区块链无缝衔接[4],链上共识也将从单一的单链共识上升到更加复杂的多链共识,对共识机制提出了新的挑战.

多链式区块链具有多条并行的链,可实现交易的分片存储和并发执行,能够降低数据处理压力,提高系统性能[5]. 多链式区块链网络中每条区块链可以有多个组织,每个组织可以有多个节点,每个节点可以加入多条区块链,因此它是一个多主体、多种关系的复杂系统. 超级账本hyperledger fabric[6]采用多通道技术实现多链架构,但通道间相互隔离,难以实现多链共识. 为实现多链共识,闵新平等[7]构建主从多链,提出了许可链多中心共识机制. 刘昊哲等[8]构建2层主从多链架构,提出了基于信誉度的多机制融合联合共识机制. Yang等[9]提出了主从链的混合共识算法,提高多域对话交互的效率和可扩展性. 张文芳等[10]构造树形结构的联盟链主从多链架构,提出了基于门限签名的改进拜占庭容错共识算法. Wang等[11]提出了信用证明阈值共识机制,实现有效的信息验证,保证跨链信息的自适应一致性. 可以看出,这些共识机制通过主区块链链接多个从区块链,保证交易的全局一致性,但现有多链式区块链大都采用主链最终共识机制,所有交易均通过主链最终确定,忽略了从链间存在的局部链间交易现象,易造成主链负载大,从而制约从链性能等问题.

超图(hypergraph)是一类一条边可以包含任意节点数量的图结构,对于复杂关系的表达有着天然优势,能够很好地对各类网络、数据结构以及一些对象关系复杂的系统高效建模[12]. 构建多链式区块链时,超图可以从多链式区块链网络中梳理出图和树无法梳理出的关系,能更多地保留多链式区块链网络的高阶结构信息,能够为构建区块链上层架构提供更好的支撑[13].

聚合签名是一种支持聚合特性的数字签名变体,可以把多个用户的签名压缩成一个签名,使得多个签名的验证简化到一次验证,能够有效减小签名的存储空间和签名验证的工作量[14]. MuSig2[15]聚合签名是一种新型两轮通信的Schnorr[16]聚合签名算法,提升了Schnorr聚合签名的安全性能,且复杂度低于三轮通信的MuSig1[17]聚合签名,没有BLS(Boneh-Lynn-Shacham)[18]聚合签名配对函数复杂不友好、验证时间长等缺点.

本文提出一种基于超图和MuSig2聚合签名的联盟链主从多链共识机制. 首先,设计一种基于超图的联盟链主从多链架构,基于子超图和横贯超图切分共识群组,使得每一个子超图和横贯超图分别组成一个通道,每个通道维护一条链,以横贯超图为主链,子超图为从链;然后,借鉴分治思想,结合“背书-排序-验证”的分工并行方式,构建包含单通道共识、多通道共识、全局共识的分层分类共识机制,避免所有交易均通过主链最终共识确定,以减轻主链负载,提升从链的性能;最后,构建基于MuSig2聚合签名的联盟链多方背书签名方法,进一步提升交易签名的验证效率. 本文所提方案能够对多链优化提供一定借鉴,对促进区块链落地具有一定意义.

2 基于超图的联盟链主从多链架构

联盟链是指由多个地位平等且利益相关的组织(机构)共同参与和维护的区块链,是一个广泛的共同体. 在这个共同体中,各个组织在深度合作时会做更深的收敛,形成多个相互协作的小集体. 在生产实践中,为了符合实际场景,通常会以一个小集体收敛为一条区块链,通过跨链技术使多个小集体形成多条可跨链交互的区块链. 区块链中继技术是一种最常用的跨链技术,具有易扩展、高性能、适用场景广泛等特性. 考虑到多链间需要支持多场景下跨链交互的业务需求,多层中继跨链会导致系统性能下降的问题,以及联盟链中各组织地位平等的客观条件,本文采用单层中继模式. 根据超图理论,构建以横贯超图为主链,子超图为从链的联盟链主从多链架构. 要保证主从链能够跨链交互,则主从链必然连通;要保证联盟链中各组织地位平等的客观条件,各组织应不依赖其他组织可以直接参与和维护主链,所以主链至少应包含各组织的一个代表节点. 若将联盟链抽象为一个超图结构,以联盟链的节点为超图的点,组织为超图的超边,则一条从链构成子超图;根据超图的连通性和横贯超图等特性,超边至少有一个节点相交,因此从链中每个组织提供一个代表节点至主链充当中继节点,这些中继节点构成了

横贯超图. 这样,既能保证各从链能够通过主链连通,又能以最小的节点数使主链包含所有组织,保证联盟链中各组织地位平等. 基于超图的联盟主从多链架构如图1所示(图中保留超图结构信息便于展示节点之间的通信联系).

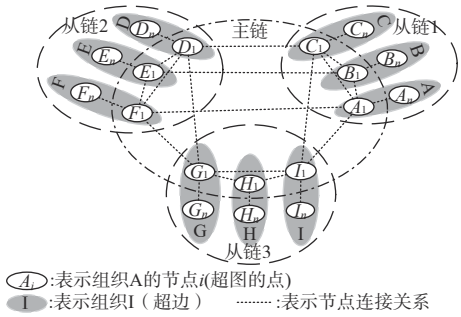

图1　基于超图的联盟链主从多链架构

在图1中,通过多通道构建多链,基于子超图和横贯超图划分共识群组,形成由组织A、B、C组成的从链共识系统1;由组织D、E、F组成的从链共识系统2;由组织G、H、I组成的从链共识系统3;由组织A、B、C、D、E、F、G、H、I的代表节点A_1、B_1、C_1、D_1、E_1、F_1、G_1、H_1、I_1组成主链共识系统. 主链共识系统负责构建主链,从链共识系统负责维护主链以及各自从链.

在联盟链主从多链架构中,交易不仅可以在通道内部进行,还可以跨通道,能够实现多链之间的价值互联. 相关定义如下:

定义1　组织(Organization, Org):区块链网络中的企业、机构等实体.

定义2　通道(Channel):多个特定网络成员之间的专用通信链路.

定义3　节点(Node):区块链的通信实体. 按照功能可分为锚节点、背书节点、排序节点、主节点、记账节点、中继节点. 锚节点负责跨组织通信. 通道中每个组织都有一个锚节点,便于同一通道中不同组织的节点发现通道内所有节点. 背书节点负责交易提案的背书签名. 排序节点负责将未打包的交易排序、生成区块并广播给主节点. 主节点负责把接收到的区块转发给其他节点. 记账节点负责验证交易的有效性和将区块保存到通道账本. 中继节点是从链中选择的代表节点,负责将从链的投票结果反馈给主链,并从主链获取区块信息,以实现主从链间的协作. 一个节点可能同时具有不同的功能,但为了以并行方式提高系统性能,一般节点不同时担任多种功能.

定义4　背书策略(Endorsement Policy, EP):背书一个交易的规则.

定义5　交易(Transaction, Tx):一次对账本的操作,只有满足背书策略的交易才有效.

定义6　单通道共识(Single-Channel Consensus, SCC):单个通道内节点执行共识协议,得到一个合法通道内的区块.

定义7　多通道共识(Multi-Channel Consensus, MCC):多个通道间节点执行共识协议,得到多个合法的通道内的区块.

定义8　全局共识(Global Consensus, GC):各组织的代表节点,对单通道共识进行二次共识过程,得到最终全局合法的区块.

定义9　主从多链(Master-Slave Multiple Chain, MSMC):1条主链+N条从链构成的"1+N"主从链群,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. 基于超图的联盟链主从多链的区块结构如图2所示.

主链的数据区块称为主链区块(Master Block, MB). 从链的数据区块称为从链区块(Slave Block, SB). 主、从链区块(Block, B)格式一致为:

B=<Header<Number, Pre_Hash, DataHash>, Data<Envelope<Payload,…,>>, MetaData>

其中,Header表示区块头,包含区块序号Number,前一区块头哈希值Pre_Hash,当前区块数据体哈希值DataHash;Data表示区块数据体,包含排序后的交易列表Envelope;Envelope包括交易数据载荷Payload等;Metadata表示元数据,记录一些辅助信息,如通道的排序服务信息、区块的提交时间哈希等.

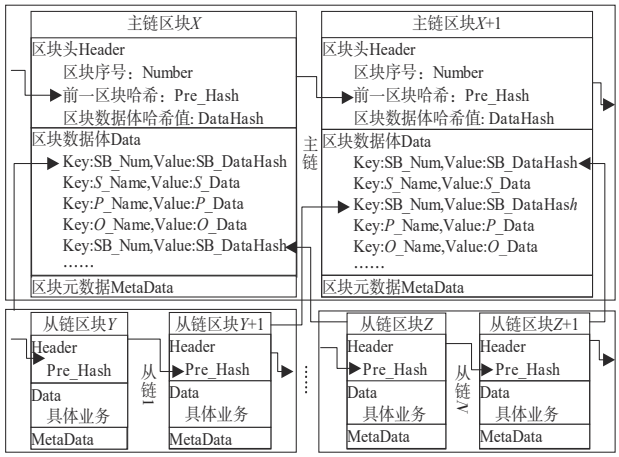

图2　基于超图的联盟链主从多链的区块结构

交易数据载荷以(Key,Value)键值对形式存储,其中,Key是每条数据地址的唯一关键字,Value是实际存储的数据. 从链区块中的交易数据载荷用于实现具体业务. 主链区块中的交易数据载荷(Payload, P)根据用途可分为基础性交易数据载荷和业务性交易数据载荷.

主链区块中的基础性交易数据载荷(Basic Payload, BP)用于验证从链交易的合法性,载荷内容为:

MB_BP=<MB_BP_S, MB_BP_O, MB_BP_P>

其中,MB_BP_S=<Key:*S*_Name, Value:*S*_Data>,*S*_Name表示从链名称,*S*_Data表示从链信息结构体;MB_BP_O=<Key:*O*_Name, Value:*O*_Data>,*O*_Name表示组织名称,*O*_Data表示组织信息结构体;MB_BP_P=<Key:*P*_Name,Value:*P*_Data>,*P*_Name表示节点名称,*P*_Data表示节点信息结构体,共同支撑主链验证从链交易的功能.

主链区块的业务性交易数据载荷(Operational Payload, OP)用于实现主从链关联,载荷内容为:

MB_OP=<Key:SB_Num, Value:SB_DataHash>

其中,SB_Num表示从链区块序号,可将主从链区块关联;SB_DataHash表示从链区块数据体哈希值,可保证从链交易难以篡改.

3 联盟链主从多链分层分类共识机制

现有主从多链的共识机制主要通过主链最终共识保证交易一致性,所有交易均会在主链最终共识后存储在主链上,造成主链负载压力大,影响从链性能. 传统区块链中区块的打包、共识以及交易执行等都是在单一节点上完成的,限制了区块链的交易执行速率,制约了系统整体性能[19]. 为使基于超图的联盟链主从多链具有更高的性能,本研究采用Hyperledger fabric“背书-排序-验证”分工并行的方式来达成共识. 共识过程分为交易内容合法性验证和交易顺序一致性保证两个步骤. 背书和验证保证交易内容的合法性. 排序保证交易顺序的一致性. 通过将共识解耦,可以实现多节点并行处理以提升性能,也便于智能合约的开发者设计更为灵活的信任模型[20]. 结合联盟链网络在宏观上有“小世界”,中观上有“群聚特性”,微观上有“聚类性”等特征,以及业务节点的交互和数据存储可能存在局部现象,借鉴分治思想,对共识一致性进一步细分,在基于超图的联盟链主从多链上构建分层分类共识机制,实现对主从多链更加细致的共识管理. 基于超图的联盟链主从多链分层分类共识机制如图3所示.

在图3中,共有4条通道,分别是通道1、2、3和中继通道. 通道1中包含三个实体组织A、B、C和一个排序组织O. 组织A、B、C中分别有两个节点. 为了便于叙述,每个节点同时担任多种角色. 以组织A为例,A_1节点同时是锚节点、中继节点、主节点,A_n同时是背书节点、记账节点. 排序组织O中的节点O_A由组织A提供,其他组织依此类推. 通道1、2、3结构相似,依此类推. 中继通道包含所有组织,每个组织的1号节点加入中继通道充当中继节点. 基于超图结构的联盟链主从多链分层分类共识机制分为单通道共识、多通道共识、全局共识三类.

各类共识的主要工作流程如下:

(1) 单通道共识

单通道共识用于交易只涉及通道i内成员,不涉及其他通道成员且不影响全局的应用场景,由下层通道共识保证即可,优先级最低. 每一个通道是一条独立的链,单通道共识可在多链中并发执行,如图3的单通道共识所示.

在图3的单通道共识中,客户端连接主节点A_1,通过锚节点向通道内其他组织的背书节点发送交易背书请求;背书节点B_n、C_n接收到背书请求后执行背书过程,将结果返回给客户端;客户端再将携带背书签名的交易请求发送给主排序节点O_A;主排序节点广播给其他排序节点,排序后将结果发送给主节点;由主节点广播至记账节点,记账节点验证后存储交易,完成共识过程.

(2) 多通道共识

面对复杂多样化的场景需求,交易不仅在单个通道发生,还可能跨多个通道. 当交易涉及多个通道但不涉及全部通道时,需要保证通道间的一致性. 多通道共识首先通过中继通道上存储各通道的背书策略和成员证书等信息实现对跨链交易自行验证;再通过多次共识保证通道间交易一致性,优先级高于单通道共识. 某一笔交易若需要多个链共识,则需要与多个链分别交互,通过跨链多次共识保证通道间的一致性. 以通道1与2间的多通道共识为例,如图3的多通道共识所示,共识流程如下:

(*a*)客户端连接A_1节点,通过锚节点向通道内其他组织的背书节点发送交易背书请求;同时通过中继节点向通道2的中继节点D_1发送交易背书请求,并行执行通道1共识和通道2共识,得到共识结果S_1和S_2;中继节点A_1和D_1互相交换共识结果,通道1和2可相互获得交易背书结果,具有不可抵赖性.

(*b*)中继节点A_1和D_1根据中继通道上存储的基础性交易数据载荷分别验证共识结果S_2是否满足通道2的共识策略和S_1是否满足通道1的共识策略. 若满足,则将共识结果S_2提交至通道1,共识结果S_1提交至通道2,再次共识存证即可;若不满足,则分别对通道1和通道2的第一次交易进行冲账操作.

(3) 全局共识

全局共识用于需要保证交易全局性一致的场景. 先在从链执行单通道共识,再由中继节点提交至主链,并通过中继通道上存储各通道的背书策略和成员证书等信息验证交易是否满足单通道共识. 满足后进行全局一致性共识,通过从链存储交易内容,主链存储区块

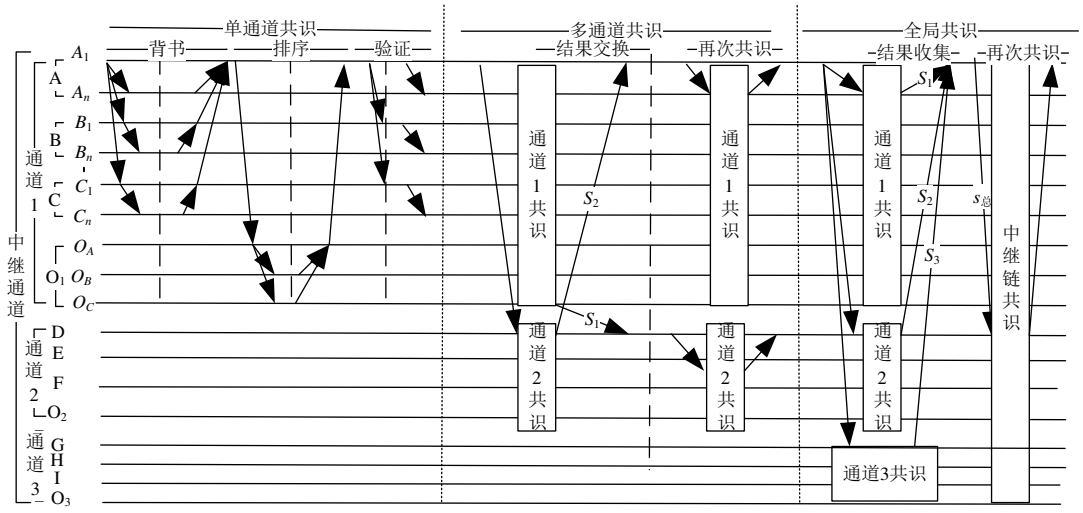

图3　基于超图的联盟链主从多链分层分类共识机制

编号和数据体哈希,保证主从链一致和从链不可篡改,优先级最高. 全局一致性共识流程如图3的全局共识所示.

在图3的全局共识中,客户端连接A_1节点,通过锚节点向通道内其他组织的背书节点发送交易背书请求;同时通过中继节点向通道2的中继节点D_1和通道3的中继节点G_1发送交易背书请求;并行执行通道1、2、3的共识,得到共识结果S_1、S_2和S_3;将结果汇聚到中继节点A_1,再提交至中继通道上;中继通道依次验证S_i是否满足该通道的共识策略. 若满足,则在中继链进行再次共识;若不满足,则对通道1、2、3的本次交易冲账.

由上述共识流程可知,多通道共识、全局共识是在单通道共识基础上进行的二次共识,因此单通道共识是否具有确定性就变得尤为重要. 根据共识结果是否确定,区块链共识可分为概率性共识和确定性共识[21,22]. 概率性共识中区块数据以一定概率达成一致,随着时间推移概率逐渐提高,但不能保证区块数据将来不可更改,称为弱一致性,如工作量证明(Proof of Work,PoW)、权益证明(Proof of Stake,PoS)等. 确定性共识中一旦区块数据达成一致便不可更改,称为强一致性,如paxos、raft、实用拜占庭容错(Practical Byzantine Fault Tolerance,PBFT)等.

在分层分类共识机制中,各个链可以采用不同的共识算法,但必须是确定性共识. 因为概率性共识存在回退的可能,会使得多通道共识结果和全局共识结果因单通道共识回退变得不正确. 在采用不同确定性共识算法时,根据验证策略分别验证即可,如Raft要求满足1/2以上节点同意,PBFT需要满足2/3以上节点同意. 主链中存储各从链的背书策略,以及节点公钥等信息,便于实现从链交易的验证,进而实现不同共识融合.

4　基于MuSig2聚合签名的联盟链多方背书签名方法

在多链环境下,多通道共识需要多次跨链交互,交易验证速率对共识效率有着重要影响. Hyperledger fabric采用椭圆曲线数字签名算法(elliptic curve digital signature algorithm,ECDSA)[23]进行背书签名,若用n个私钥签名,则验证时需要对n个签名各自验证,需要n次取模和$2n$次点乘运算. MuSig2聚合签名生成的多签验证时,只需要$2n$次加法运算和n+1次点乘运算. 加法运算所占用的资源极低,且在验证时仅需一次验证即可,时间复杂度$T(n)=O(n)$,因此能够提升交易验证效率. MuSig2聚合签名的第一轮可以提前执行,使得对签名请求实时处理时,只须进行一轮并发通信. 这种仅一轮并发通信的特性可以提高多重签名响应速度,而且略加改造就可以与Hyperledger fabric的交易背书机制良好融合,使多个背书签名聚合为一个标准Schnorr签名.

为了更好地结合MuSig2聚合签名与背书机制,借鉴SBFT(Simple Byzantine Fault Tolerance)[24]共识中收集器(collector)的线性通信模式,在共识过程中引入一个协作中心专门用于收集和分发背书消息,以降低通信复杂度;借鉴raft[25]心跳思想,协作中心需要间断性向背书节点发送一个活性消息,以保证协作中心具有活性,避免签名过程陷入死等待. 这种优化一方面可以提高MuSig2聚合签名速度,同时还可以使得MuSig2的第二轮次更容易与背书签名收集方式融合. 基于MuSig2聚合签名的联盟链多方背书签名过程如图4所示.

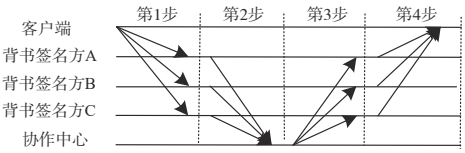

图4 基于MuSig2聚合签名的联盟链多方背书签名过程

在图4中,签名过程如下:

第1步:客户端构建交易提案并用MuSig2签名(用于身份验证,不需要聚合)后,它们一起作为交易提案请求发送给背书策略指定的背书签名方,如图4中的第1步所示.

第2步:背书签名方接收到交易提案请求后,验证交易提案签名;验证成功后模拟执行交易,生成交易结果和用于MuSig2聚合签名中聚合该笔交易背书签名的随机数(nonce1);然后将交易提案、交易结果、背书签名方公钥、随机数(nonce1)封装,并用MuSig2签名(用于验证消息,不需要聚合)后一起作为交易提案结果发送给协作中心,如图4中的第2步所示.

第3步:协作中心接收到各背书签名方的交易提案结果后验证签名,检验交易提案和交易结果是否一致,完成后存储各背书签名方交易提案结果;当获取到满足背书策略数量的交易提案结果时,将各背书签名方的交易提案结果合并成MuSig2聚合签名的第一轮消息,并通过事件机制发送给背书策略指定的背书签名方,如图4中的第3步所示.

第4步:通过事件监听机制,背书签名方及时获取MuSig2聚合签名的第一轮消息;通过MuSig2聚合签名的第一轮消息中其他背书参与方的公钥和随机数(nonce1),直接计算共同的随机数(nonce2)以及各自的签名碎片,将交易提案、交易结果、背书签名方签名碎片、共同的随机数(nonce2)封装成MuSig2聚合签名的第二轮消息,发送给客户端;根据MuSig2聚合签名,由客户端将签名碎片聚合成一个MuSig2聚合签名,如图4中的第4步所示.

由图4可知,基于MuSig2聚合签名的联盟链多方背书签名过程有4轮广播. 假设第i轮时间复杂度为$T_i(n)$,可以看出,对于n个背书签名方,在每一轮中只发送n个背书消息,即$T_1(n)=n$,$T_2(n)=n$,$T_3(n)=n$,$T_4(n)=n$,则总时间复杂度$T(n)=T_1+T_2+T_3+T_4=4n$,即基于MuSig2聚合签名的联盟链多方背书签名的时间复杂度为$T(n)=O(n)$. 具体如算法1所示.

验证MuSig2聚合签名时,向验证函数VerifySignature传入签名方公钥序列、聚合签名sig以及交易提案,即可完成交易提案的签名验证.

算法1 基于MuSig聚合签名的联盟链多方背书签名

输入:客户端Client,背书签名方A、B、C,协作中心CooCenter

输出:签名:sig

Proposal,err := Client.CreatTransaction Proposal()//客户端生成交易提案

err := Client.Broadcasted(Proposal)//客户端广播交易提案

NonceA := A.GetRound1Nonce(Proposal)//背书签名方A针对交易提案生成随机数,其他签名方同理

round1MsgA , err := A.GetRound1Msg(NonceA,Proposal)//背书签名方A生成交易提案结果,其他签名方同理

err := A.Send(round1MsgA,CooCenter)//背书签名方A发送交易提案结果到协作中心,其他签名方同理

round1TotalMsg , err := CooCenter.Merge(round1MsgA , round1MsgB)//协作中心生成第1轮消息

err := CooCenter.Broadcasted(round1TotalMsg)//协作中心广播第1轮消息

round2MsgA, err = A.GetRound2Msg(Proposal, round1TotalMsg)// 背书签名方A根据第1轮消息生成含签名碎片的第2轮消息,其他签名方同理

err := A.Send(round2TotalMsg,client) // 背书签名方A发送第2轮消息到客户端

sig, err := Client.GetAggSignature(Proposal,round2MsgA, round2MsgB, round2MsgC,…)//客户端聚合各背书签名方的签名碎片,并对交易提案签名

5 安全性分析与方案对比

5.1 安全性分析

考虑到许可制联盟链使用数字证书等安全机制增强安全性,存在恶意节点的可能性很小,以及容忍拜占庭故障的共识机制会使系统中节点数量过多导致系统变复杂和性能大幅下降,因此以raft协议为例,分析分层分类共识机制中的排序阶段,背书策略为超过半数通道成员背书.

假设通道i有m_i个背书节点和n_i个排序节点,至多存在g_i个故障背书节点和f_i个故障排序节点,则g_i满足$g_i-\lfloor(m_i-1)/2\rfloor$,$f_i$满足$f_i-\lfloor(n_i-1)/2\rfloor$.

引理1 通道内交易、通道间交易以及全局交易的背书结果是可信的.

证明 当交易仅发生在通道i内时,根据$g_i-\lfloor(m_i-1)/2\rfloor$可得$m_i\geqslant 2g_i+1$;因为有效背书节点数等于总背书节点数减去无效背书节点数,即$h_i=m_i-g_i$,所以通道i的有效背书节点数h_i满足式(1).

$$h_i\geqslant g_i+1 \tag{1}$$

由式(1)可知,通道i的有效背书节点数超过总背书节点数的1/2,满足背书策略,因此通道内交易背书结果是可信的.

当交易发生在k个通道间时,k个通道的总背书节

点数等于k个通道背书节点数之和,即$T_k=\sum_{i=1}^{k}m_i$;根据$m_i\geqslant 2g_i+1$可得)$\sum_{i=1}^{k}m_i\geqslant\sum_{i=1}^{k}2g_i+1$,所以$k$个通道的总背书节点数$T_K$满足式(2).

$$T_k\geqslant\sum_{i=1}^{k}2g_i+1 \tag{2}$$

k个通道的总故障背书节点数M_g满足式(3).

$$M_g=\sum_{i=1}^{k}g_i \tag{3}$$

k个通道的总有效背书节点数等于k个通道总背书节点数减去总故障节点数如式(4)所示.

$$M_h=T_K-M_g \tag{4}$$

将式(2)和式(3)代入式(4)可得$M_h\geqslant\sum_{i=1}^{k}2g_i+1-\sum_{i=1}^{k}g_i$,所以$k$个通道的总有效背书节点数$M_h$满足式(5).

$$M_h\geqslant\sum_{i=1}^{k}g_i+1 \tag{5}$$

由式(5)可知,k个通道的总有效背书节点数超过总背书节点的1/2,满足背书策略,因此通道间交易的背书结果是可信的.

当交易发生在全局通道时,全局通道上的背书节点是各组织的代表节点,满足式(1)和式(5),总有效背书节点数超过总背书节点的1/2,满足背书策略,因此全局交易的背书结果是可信的.

综上,通道内交易、通道间交易以及全局交易的背书结果是可信的.

引理2　每个通道内区块的排序结果是一致的.

证明　通道i的排序节点数n_i、故障排序节点数f_i满足式(6).

$$n_i>2f_i+1 \tag{6}$$

由式(6)可知,通道i内有效排序节点数超过总排序节点数的1/2,有限状态机能够将区块排序结果复制到足够数量的排序节点,实现强一致性,因此每个通道内区块的排序结果是一致的.

定理1　基于MuSig2聚合签名的联盟链多方背书签名方法是安全可靠的.

证明　MuSig2聚合签名的验证函数满足$sG=R+eP$;心跳机制可以保证协作中心的活性;随机数和交易提案等关联,一定程度上可避免随机数重用和私钥泄露;消息签名验证,可以保证消息的合法性. 综上,基于MuSig2聚合签名的联盟链多方背书签名方法是安全可靠的.

定理2　基于超图的联盟链主从多链分层分类共识机制有线性级时间复杂度.

证明　本文采用“背书-排序-验证”的共识方式且多链可并行. 在背书阶段,基于MuSig2聚合签名的联盟链多方背书签名方法的时间复杂度$T_{背书}(n)=O(n)$. 在排序阶段,本文采用raft排序协议,时间复杂度$T_{排序}(n)=O(n)$. 在验证阶段,MuSig2聚合签名验证时间复杂度$T_{验证}(n)=O(n)$. $T_{总}(n)=T_{背书}(n)+T_{排序}(n)+T_{验证}(n)=O(n)$,故基于超图的联盟链主从多链分层分类共识机制有线性级时间复杂度.

定理3　基于超图的联盟链主从多链分层分类共识机制具有强一致性.

证明　由引理1可知,当通道i内至多存在g_i个背书故障节点和f_i个排序故障节点时,通道内交易、通道间交易以及全局交易的背书结果是可信的;由引理2可知,每个通道内区块的排序结果是一致的,故基于超图的联盟链主从多链分层分类共识机制具有强一致性.

定理4　基于超图和Musig2聚合签名的联盟链主从多链分层分类共识机制是安全可靠的.

证明　由定理1可知,基于MuSig2聚合签名的联盟链多方背书签名方法是安全可靠的;由定理3可知,基于超图的联盟链主从多链分层分类共识机制具有强一致性;故基于超图和Musig2聚合签名的联盟链主从多链分层分类共识机制是安全可靠的.

定理5　基于超图的联盟链主从多链架构具有不可篡改特性.

证明　在基于超图的联盟链主从多链架构中,单通道交易由通道内成员共同存储. 若要篡改区块,需要篡改通道内半数以上成员的账本. 多通道交易由多个通道成员共同存储,若要篡改区块,需要篡改多个通道内半数以上成员的账本. 全局交易由从链保存交易内容,主链保存从链对应的区块编号和数据体哈希值,主从链通过区块编号和数据体哈希值的方式相互锁定. 若要篡改区块,需要篡改全网半数以上成员的账本. 故基于超图的联盟链主从多链架构具有较强的不可篡改特性.

定理6　基于超图的联盟链主从多链架构是安全可信的.

证明　基于超图的联盟链主从多链架构主要涉及通道内交易、通道间交易、全局交易. 由引理1~3可知,当通道i内至多存在g_i个背书故障节点和f_i个排序故障节点时,通道内、通道间、全局的交易均是有效、安全、可信的. 由定理4,可知,基于超图的联盟链主从多链架构具有不可篡改特性,故基于超图的联盟链主从多链架构是安全可信的.

5.2　方案对比

从链式结构和共识机制方面,与现有主流方案的比较如表1所示.

由表1可见，Bitcoin[26]、Ethereum[27]、文献[28]采用单层链式结构，难以并发处理交易，存在吞吐量低、延迟高、可扩展性低等问题. Hyperledger fabric[6]采用多链结构，只支持跨链可读操作，存在一定的局限性. 文献[7,10]支持跨链处理，采用PBFT共识，具有强一致性、不容易出现分叉、效率较高等特点，但通信复杂度较高，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. 本方案构建的主从多链架构，主从链通过区块序号和数据体哈希值相互锁定，保证交易难以被篡改，从链可通过主链的中继节点实现跨链通信，通过主链上的基础性交易数据载荷实现跨链验证，进而实现跨链交互. 本方案采用“背书-排序-验证”分工并行的共识方式，可实现多节点并行处理；构建的分层分类共识机制可根据场景需求选择不同层次的共识，避免所有交易都通过主链最终确定，降低主链负载压力；基于MuSig2聚合签名的联盟链多方背书签名，可提升签名验证效率和性能.

表1 方案对比

方案	架构	共识机制	容错类型	容错率	去中心化	分叉	跨链	抗双花	通信复杂度
Bitcoin[26]	单链	PoW	作恶	50%	完全	有	无	无	—
Ethereum[27]									
文献[28]		PBFT			部分	无			$O(n^2)$
Fabric[6]	多链	raft	故障	50%	部分	无	无	有	$O(n)$
文献[7]		PBFT	作恶	33%		无	有	无	$O(n^2)$
文献[10]						无		有	
本方案		确定性	故障	50%					$O(n)$

6 实验仿真

6.1 实验环境

本文以传统区块链ECDSA签名和多链架构下的主链最终共识机制作为参照，实现相关实验. 实验环境如下：

(1)硬件环境：16 GB内存、1 TB硬盘及Intel(R)i5-6300HQ处理器.

(2)测试工具：Caliper区块链性能测试工具.

(3)依赖包：ECDSA依赖包：crypto/ecdsa、crypto/elliptic、crypto/x509、encoding/pem；MuSig2依赖包：sammyne/musig2.

(4)区块链网络：Hyperledger fabric联盟链框架，1条主链ChainS，3条从链ChainA、ChainB、ChainC，每条链都构成一个独立的raft排序系统；每条从链有3个组织，每个组织提供两个peer节点和1个order排序节点；从链中每个组织提供一个节点至主链充当中继节点，每条链提供1个排序节点至主链充当排序节点.

(5)测试配置：3个测试链码如表2所示，交易数量设为1 000.

(6)背书签名测试用例：三个背书签名方、一个协作中心.

表2 测试链码

链码名称	链码功能	共识类型
SingleLoad	单通道上链	单通道共识
CrossLoad	跨通道上链	多通道共识
GlobalLoad	全局上链	全局共识(主链最终共识)

6.2 实验结果

(1) 背书签名

借助MuSig2依赖包，实现基于MuSig2聚合签名的多方背书签名. 根据背书签名测试用例得到背书签名结果图如图5、图6所示.

图5 协作中心

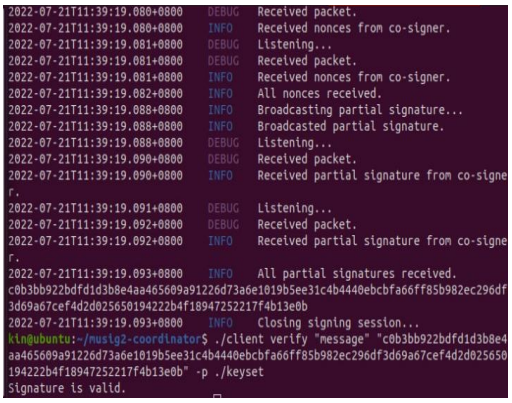

图6 基于MuSig2的多方背书签名

在图5中，协作中心接收到了三个背书签名方的nonces1、签名碎片等信息. 在图6中，背书签名方在协

作中心的协助下,生成了MuSig2聚合签名即c0b…eob;签名验证成功后得到结果valid,表明签名是有效的.

(2) 背书签名效率

借助ECDSA依赖包,实现ECDSA签名的多方背书签名. 根据背书签名测试用例,取10次测试结果的均值,分别对比MuSig2聚合签名与ECDSA的签名与验签时长如表3所示.

由表3可以看出,在单通道共识中,MuSig2聚合签名的时长分别为签名415.584 μs,验签465.548 μs,总时长881.132 μs;ECDSA的时长分别为签名225.854 μs,验签720.569 μs,总时长946.423 μs. MuSig2聚合签名效率是ECDSA签名的1.07倍. 在多通道共识和全局共识中,多通道可以并行. 假设共有n个子通道,各子通道背书节点数均为3个,MuSig2聚合签名的时长分别为签名415.584 μs,验签最大为465.548n μs,总时长最大为415.584+465.548n μs;ECDSA的时长分别为签名225.854 μs,验签最大为720.569n μs,总时长最大为225.854+720.569n μs. MuSig2聚合签名的总效率是ECDSA签名的1.55倍. 所以基于MuSig2聚合签名的联盟链多方背书签名在多链环境中效率优势明显.

表3　签名与验签时长　　单位:μs

签名算法	时长
三个签名方生成一个MuSig2聚合签名	415.584
三个签名方并行生成三个ECDSA签名	225.854
验证三个签名方生成MuSig2聚合签名	465.548
依次验证三个签名方的ECDSA签名	720.569

(3) 吞吐量与时延

利用多通道和可插拔共识模块实现主从多链的架构及分层分类共识机制. 测试过程中,分别调用测试链码SingleLoad.js、CrossLoad.js、GlobalLoad.js. 通过调整交易发送速率,观察时延和吞吐量的变化. 当交易吞吐量按照10 TPS(transactions per second)从50 TPS递增到150 TPS时,网络时延和吞吐量的趋势如图7所示.

由图7可以看出,单通道共识仅在通道内进行,时延最低;多通道共识为两条链间共识,如从链chainA与chainB、chainA与chainC,需要跨链,因此时延高于单通道共识;全局共识首先在从链共识后提交至主链,由主链最终共识,最后发送至从链,时延较高. 当网络吞吐量到达120 TPS后,时延趋向稳定,若取三轮测试均采用全局共识,则总时延约为4.79×3 = 14.37 s;若平均分布在全局共识、单通道共识、多通道共识之间时,则总时延约为4.79 s +4.34 s +3.44 s=12.57 s,提升效率为(14.37−12.57)/14.37= 12.5%. 本文将共识分层分类,根据不同场景需要选择不同共识类型,避免所有交易都需要主链最终共识,降低了主链负载压力,提升了效率.

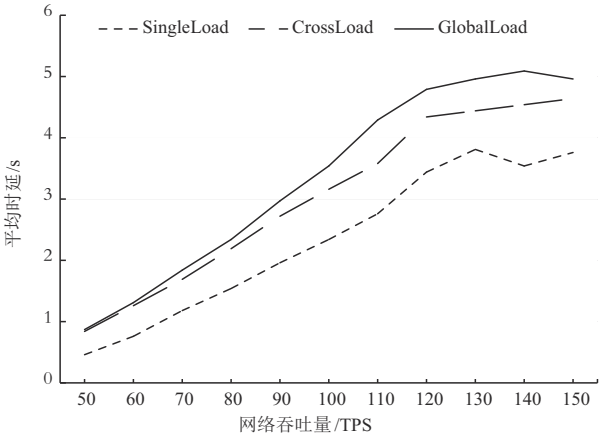

图7　网络吞吐量与时延的趋势

7　结论

针对主从多链共识机制采用主链最终共识机制,导致的主链负载压力大,制约从链性能等问题,本研究提出了一种基于超图和MuSig2聚合签名的联盟链主从多链共识机制. 首先面向联盟链提出一种超图结构的主从多链架构,根据子超图和横贯超图将群组切分成一条主链和多条子链;其次针对超图结构的主从多链架构,设计分层分类共识机制,根据不同场景需要,灵活选择共识类型,避免所有交易均通过主链最终共识确定,降低主链负载压力;最后提出基于MuSig2聚合签名的联盟链多方背书签名方法,提升交易签名的验证效率,进而提升共识效率,提升系统性能. 理论分析表明:基于MuSig2聚合签名的联盟链多方背书签名方法是安全可靠的,基于超图和MuSig2聚合签名的分层分类共识机制具有强一致性和线性时间复杂度,基于超图的联盟链主从多链架构具有不可篡改特性. 实验结果表明:基于MuSig2聚合签名的多方背书方法的总效率是ECDSA的1.55倍,分层分类共识机制提升了12.5%的共识效率. 该机制具有高并发交易性能,可满足企业多样化业务需求.

参考文献

[1] 蔡晓晴, 邓尧, 张亮, 等. 区块链原理及其核心技术[J]. 计算机学报, 2021, 44(1): 84-131.
CAI X Q, DENG Y, ZHANG L, et al. The principle and core technology of blockchain[J]. Chinese Journal of Computers, 2021, 44(1): 84-131. (in Chinese)

[2] LU Y. The blockchain: State-of-the-art and research challenges[J]. Journal of Industrial Information Integration, 2019, 15: 80-90.

[3] JIN H, XIAO J. Towards trustworthy blockchain systems in the era of “Internet of value”: Development, challenges, and future trends[J]. Science China Information Sciences,

2021, 65(5): 153101.

[4] DI FRANCESCO MAESA D, MORI P. Blockchain 3.0 applications survey[J]. Journal of Parallel and Distributed Computing, 2020, 138(C): 99-114.

[5] 张亮, 刘百祥, 张如意, 等. 区块链技术综述[J]. 计算机工程, 2019, 45(5): 1-12.
ZHANG L, LIU B X, ZHANG R Y, et al. Overview of blockchain technology[J]. Computer Engineering, 2019, 45(5): 1-12. (in Chinese)

[6] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger fabric: A distributed operating system for permissioned blockchains[C]//Proceedings of the Thirteenth EuroSys Conference. New York: ACM, 2018: 1-15.

[7] 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)

[8] 刘昊哲, 李莎莎, 吕伟龙, 等. 基于信誉度的主从多链区块链共识机制[J]. 南京理工大学学报, 2020, 44(3): 325-331.
LIU H Z, LI S S, LV W L, et al. Master-slave multiple-blockchain consensus based on credibility[J]. Journal of Nanjing University of Science and Technology, 2020, 44(3): 325-331. (in Chinese)

[9] YANG W L, GARG S, HUANG Z Q, et al. A hybrid consensus algorithm for master—Slave blockchain in a multi-domain conversation system[J]. Expert Systems with Applications, 2022, 204: 117300.

[10] 张文芳, 孙海锋, 张晏端, 等. 基于树形结构构造的联盟链主从多链共识算法[J]. 电子学报, 2022, 50(2): 257-266.
ZHANG W F, SUN H F, ZHANG Y D, et al. A consensus algorithm for consortium chain with tree based master-slave multi-chain architecture[J]. Acta Electronica Sinica, 2022, 50(2): 257-266. (in Chinese)

[11] WANG L Z, WU J, YUAN R F, et al. Dynamic adaptive cross-chain trading mode for multi-microgrid joint operation[J]. Sensors, 2020, 20(21): 6096.

[12] 胡秉德, 王新根, 王新宇, 等. 超图学习综述: 算法分类与应用分析[J]. 软件学报, 2022, 33(2): 498-523.
HU B D, WANG X G, WANG X Y, et al. Survey on hypergraph learning: Algorithm classification and application analysis[J]. Journal of Software, 2022, 33(2): 498-523. (in Chinese)

[13] 索琪, 郭进利. 基于超图的超网络: 结构及演化机制[J]. 系统工程理论与实践, 2017, 37(3): 720-734.
SUO Q, GUO J L. The structure and dynamics of hyper-networks[J]. Systems Engineering-Theory & Practice, 2017, 37(3): 720-734. (in Chinese)

[14] 杨涛, 孔令波, 胡建斌, 等. 聚合签名及其应用研究综述[J]. 计算机研究与发展, 2012, 49(S2): 192-199.
YANG T, KONG L B, HU J B, et al. Survey on aggregation signature and its application[J]. Journal of Computer Research and Development, 2012, 49(S2): 192-199. (in Chinese)

[15] SCHNORR C P. Efficient identification and signatures for smart cards[C]//CRYPTO'89: Proceedings on Advances in cryptology. Berlin: Springer, 1989: 239-252.

[16] MAXWELL G, POELSTRA A, SEURIN Y, et al. Simple Schnorr multi-signatures with applications to Bitcoin[J]. Designs, Codes and Cryptography, 2019, 87(9): 2139-2164.

[17] NICK J, RUFFING T, SEURIN Y. MuSig2: Simple two-round Schnorr multi-signatures[C]//Advances in Cryptology—CRYPTO 2021. Cham: Springer International Publishing, 2021: 189-221.

[18] 杨坤伟, 杨波, 周彦伟. 群智网络中基于区块链的有序聚合签名认证方案[J]. 电子学报, 2022, 50(2): 358-365.
YANG K W, YANG B, ZHOU Y W. A sequential aggregate signature authentication scheme based on blockchain for crowdsensing system[J]. Acta Electronica Sinica, 2022, 50(2): 358-365. (in Chinese)

[19] 刘明达, 陈左宁, 拾以娟, 等. 区块链在数据安全领域的研究进展[J]. 计算机学报, 2021, 44(1): 1-27.
LIU M D, CHEN Z N, SHI Y J, et al. Research progress of blockchain in data security[J]. Chinese Journal of Computers, 2021, 44(1): 1-27. (in Chinese)

[20] 孟吴同, 张大伟. Hyperledger Fabric共识机制优化方案[J]. 自动化学报, 2021, 47(8): 1885-1898.
MENG W T, ZHANG D W. Optimization scheme for hyperledger fabric consensus mechanism[J]. Acta Automatica Sinica, 2021, 47(8): 1885-1898. (in Chinese)

[21] 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.
XIA Q, DOU W S, GUO K W, et al. Survey on blockchain consensus protocol[J]. Journal of Software, 2021, 32(2): 277-299. (in Chinese)

[22] 袁勇, 倪晓春, 曾帅, 等. 区块链共识算法的发展现状与展望[J]. 自动化学报, 2018, 44(11): 2011-2022.
YUAN Y, NI X C, ZENG S, et al. Blockchain consensus

algorithms: The state of the art and future trends[J]. Acta Automatica Sinica, 2018, 44(11): 2011-2022. (in Chinese)
[23] JOHNSON D, MENEZES A, VANSTONE S. The elliptic curve digital signature algorithm (ECDSA)[J]. International Journal of Information Security, 2001, 1(1): 36-63.
[24] GOLAN GUETA G, ABRAHAM I, GROSSMAN S, et al. SBFT: A scalable and decentralized trust infrastructure [C]//2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). Piscataway: IEEE, 2019: 568-580.
[25] ONGARO D, OUSTERHOUT J. In search of an understandable consensus algorithm[C]//Proceedings of the 2014 USENIX Conference on USENIX Annual Technical Conference. Berkeley: USENIX Association, 2014: 305-320.
[26] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. (2008-11-01)[2022-08-18]. http://bitcoin.org/bitcoin.pdf.
[27] WOODG.Ethereum:Asecuredecentralisedgeneralisedtransaction ledger[EB/OL]. (2014-01-14) [2022-08-18]. http://gavwood.com/Paper.pdf.
[28] GAO S, YU T Y, ZHU J M, et al. T-PBFT: An eigen trust-based practical byzantine fault tolerance consensus algorithm[J]. China Communications, 2019, 16(12): 111-123.

作者简介

景　旭　男,1971年生于陕西礼泉. 现为西北农林科技大学信息工程学院副教授、硕士研究生导师. 主要研究方向为区块链技术、隐私保护、信息系统安全等.
E-mail: jingxu@nwsuaf.edu.cn

刘滋雨　男,1998年生于贵州晴隆. 现为西北农林科技大学在读硕士研究生,主要研究方向为区块链技术.
E-mail: 2020056010@nwsuaf.edu.cn