针对主从多链的区块链集成共识机制研究

李莎莎[1],姬永清[2],罗 盘[3],刘昊哲[1]
(1.南京理工大学 计算机科学与工程学院,江苏 南京 210094;
2.中国电子科技集团公司第28研究所,江苏 南京 210007;
3.海军指挥学院,江苏 南京 211800)

摘 要:区块链技术作为数字货币的基础,实现了去中心化环境下的信任建立与价值传递。随着区块链技术在众多应用领域的深入,区块链所承载的数字资产呈现多元化、复杂化,信息数量的急速增长对区块链的性能提出了更高的要求。采用多链、跨链等技术的主从多链模型,缓解了传统单链模型的性能瓶颈,但现有的共识机制无法适用于主从多链。为此提出一种包含个体共识机制与元共识机制的集成共识机制,确保主从多链模型的区块安全性验证。利用并行的多种共识机制作为个体共识机制,保证了主链在处理从链交易时的高效性。主链中的元共识机制对个体共识的结果进行验证,提高了主链区块的安全性。多种安全性分析与实验结果表明,提出的针对主从多链的集成共识机制较传统的共识机制具备较高的性能与安全性,保证了不同区块链网络节点间自由、安全、有效的数据转换。

关键词:区块链;主从多链;共识机制;集成共识;以太坊
中图分类号:TP311.13 **文献标识码**:A **文章编号**:1673-629X(2021)08-0082-05
doi:10.3969/j.issn.1673-629X.2021.08.014

Research on Blockchain Integrated Consensus Mechanisms of Master and Slave Multi-chain

LI Sha-sha[1],JI Yong-qing[2],LUO Pan[3],LIU Hao-zhe[1]
(1.School of Computer Science and Engineering,Nanjing University of Science and Technology,Nanjing 210094,China;
2.28th Research Institute of China Electronics Technology Group Corporation,Nanjing 210007,China;
3.Naval Command College,Nanjing 211800,China)

Abstract:As the foundation of digital currency,blockchain technology realizes the establishment of trust and the delivery of value in decentralized environment. With the development of blockchain technology in many application areas,the digital assets carried by blockchain are diversified and complicated,and the rapid growth of the amount of information proposes higher requirements for the performance of blockchain. The emergence of master and slave multi-chain model with multi-chain and cross-chain technologies alleviates the performance bottleneck of the traditional single-chain model,but the existing consensus mechanism cannot be applied to master and slave multi-chain. Therefore,an integrated consensus mechanism including individual consensus mechanism and meta-consensus mechanism is proposed to ensure security verification of blocks in master and slave multi-chain model. Multiple concurrent consensus mechanisms are used as individual consensus mechanisms to ensure the high efficiency of master chain in dealing with the transactions in slave chains. The meta-consensus mechanism in the master chain verifies individual consensus results and improves the security of the master chain block. Various security analysis and experimental results show that the proposed integrated consensus mechanism for master and slave multi-chain has higher performance and security than the traditional consensus mechanism,which ensures the free,secure and effective data exchange between different blockchain nodes.

Key words:blockchain;master and slave multi-chain;consensus mechanisms;integrated consensus;Ethereum

0 引 言

区块链由中本聪(Satoshi Nakamoto)在有关比特币的技术论坛[1]上首次提出,作为比特币的底层技术,其安全性经历了历史的考验。区块链技术通过建立信任关系、重构价值体系,从根本上促进了互联网的改变,实现了互联网从信息传递向价值传递的进化。区

收稿日期:2020-09-30 **修回日期**:2021-02-01
基金项目:国家自然科学基金(61472189,61802186);赛尔网络下一代互联网技术创新项目(NGII20180103)
作者简介:李莎莎(1997-),女,CCF会员(B6415G),研究方向为区块链多链与跨链技术、区块链应用。

块链利用去中心化技术,增强人们对匿名交易的信任,降低监管成本,提高数据处理的速度[2-3]。由于具有信息透明、不可篡改、可追溯等特性,区块链技术被广泛应用于金融、物联网、供应链、医疗等众多领域,真正成为具有颠覆性作用的解决方案[4-6]。

随着区块链技术在不同应用领域的逐渐深入,区块链技术应用从单一的数字货币转向人类社会的方方面面,区块链所承载的数字资产也呈现多元化、复杂化,信息数量的急速增长对区块链的性能提出更高的要求。全球区块链数量日益增多,链与链之间不可避免地需要进行数字资产转移、跨链通信[7-9]。为解决共识机制的性能瓶颈,打破不同区块链之间的隔阂,各种多链、跨链、侧链技术应运而生,对区块链性能的扩展起到了推动作用[10]。区块链的跨链技术是区块链实现互联互通、提升扩展性的重要技术手段。随着区块链应用场景不断趋于丰富化和复杂化,越来越多的区块链项目给出跨链的解决方案,使得跨链技术逐步得到发展。

2013 年 5 月,NoLan 在 BitcoinTalk 论坛提出了原子转移(atomic transfers)[11]思路,是实现原子式跨链数字资产交易的最初基础技术方案。Nolan 的技术方案经过改进升级后被称为哈希锁定,成为跨链的一种主要技术手段。比特币核心开发者加入的 Blockstream 公司于 2014 年 10 月发布的白皮书中提出了楔入式侧链(pegged side chains)[12]的概念,目的是实现不同区块链资产的跨链转移及在不影响主链的情况下实施更多的技术创新。2016 年 5 月,美国区块链软件技术公司 ConsenSys 设计了 BTCRelay[13],实现了以太坊对比特币区块链数据的跨链访问。2016 年 11 月,Wood 在 Polkadot 白皮书[14]中介绍了一种异构的多链架构,支持不同共识系统去中心化、去信任地进行交互操作、访问。2016 年 12 月,Blockstream 公司进一步提出强联邦侧链(sidechains with strong federations)的概念[15],在资产交换中引入由多方控制的多重签名地址,以减少延迟并提升互操作性。

Zcash 团队开发出交叉链原子交易(cross chain atomic trades,XCAT)工具,实现了 ZEC 和 BTC 之间的跨链原子交易;Bancor 基于智能合约构建了一套跨链的去中心化流动性网络,实现没有对手方的区块链资产的自动估值和兑换;OneLedger 提供一套企业系统与区块链系统联通的解决方案,通过侧链接入各类私有链、联盟链和公有链,并通过中间协议层与企业级系统通信。

现有的多链跨链技术从形态上来看,有些是在已有区块链项目基础上的改进,实现了有限数据互联;有些提出了一套通信协议,以实现区块链间的通信;有些通过新的系统架构和运行模式,支持不同区块链的接入。总的来看,跨链技术仍处于初期发展过程中,跨链的推广应用需要达成更广泛的共识,尤其是设计多区块链架构下的共识机制。

对于共识机制性能的扩展,许多学者对其展开了研究。Joseph 等人[16]提出闪电网络的概念,通过建立直接或间接的支付通道,实现链上交易资金与链下交易过程管理,提高了比特币区块链交易的吞吐量,但无法保证线下交易的真实性,破坏了区块链可追溯的优势。Yoad 等人[17]实现一种利用有向无环图(directed acyclic graph,DAG)建立区块的方式,以提高区块链交易的吞吐量,但该方案只适用于单链架构,对于多数字资产的混合型交易处理模式并不适用。Elastico 等人[18]利用分片技术实现网络分割,每个部分并行地进行交易处理,但在进行复杂交易时,由于难以验证容易达到性能瓶颈。

文中重在研究一种主从多链架构下的集成共识机制,集成共识机制运行在主链网络中,包含个体共识机制与元共识机制。个体共识机制负责对从链区块进行共识,元共识机制则是对多个个体共识的结果进行共识。集成共识机制实现了多条从链区块中数据的并行验证,提高了数据的处理速度,保证主链区块的生成效率。

文中提出的针对主从多链的集成共识机制从以下两方面看具有创新性与优势:

(1)统计方面:由于从链上传的区块信息十分庞大,使用单一共识机制会导致性能不佳。多个共识机制并行处理可以加快信息处理速度,保证交易信息的及时处理;

(2)安全性:经集成共识机制验证后的数据较单一共识而言具备更高的可信度,修改区块历史的难度更大,大幅度提高了区块链的安全性。

1　主从多链集成共识机制

1.1　主从多链结构

文中研究的主从多链结构,现给出如下定义:

主链:系统生成的第一条链,负责从链的确认工作,保证从链能够良好运行。

从链:利用侧链技术对主链进行延伸创建的区块链。若链为主链的延伸,则被称为一级从链;若为一级从链的延伸,则被称为二级从链,以此类推。被延伸的链称为父链,延伸的侧链称为子链。一条父链可以拥有多个子链,而一条子链只会拥有一个父链。

命名空间:用于唯一区分每条链的字符串。

主从多链模型采用一条主链、多条从链的方式完成主从多链的搭建,每条从链按照命名空间进行分类。

在同一命名空间中,从链节点处理相同类型的交易;不同命名空间的从链将区块上传至主链,由主链节点进行验证。主从多链结构如图 1 所示。

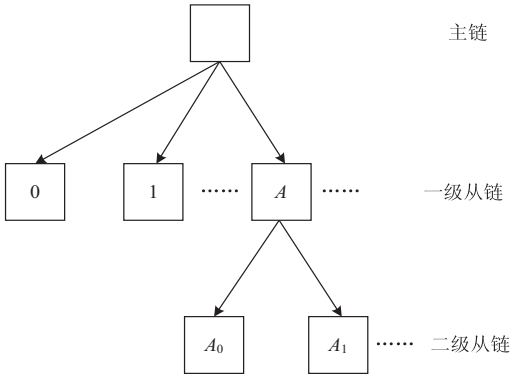

图 1 主从多链树形结构

1.2 集成共识机制

集成共识机制运行在主链网络中,采用先经多种共识机制的共识后,对共识的结果再次进行一轮共识的方式。首先进行的共识称为“个体共识机制”,对共识结果进行共识称为“元共识机制”。集成共识通过构建并结合多种共识机制共同完成共识任务,可获得比单一共识机制更优越的处理性能和安全性。利用并行的多种共识机制作为个体共识机制,保证了主链在处理从链交易时的高效性。主链中的元共识机制对个体共识的结果进行验证,提高了主链区块的安全性。集成共识机制能够组合各种不同的共识结果,且不限于特定的链结构。

1.2.1 集成共识 DAG 结构

主从多链中的从链采用 PoS 共识机制产生区块,从链产生区块之后,选择代表节点将其上传至主链中。主链首先利用“个体共识机制”对从链区块进行认证,产生微区块。微区块指向多个从链的区块。经过“元共识机制”认证后,主链区块中产生一个区块对指向多个微区块。如图 2 所示,从链区块、微区块、主链区块组成金字塔形的有向无环图(DAG)结构。

1.2.2 多签名上传区块算法

从链在上传区块信息时,需要让多个代表节点多重签名后再进行上传。主链中的节点在接受到从链信息后,对从链中的多重签名进行验证。

从链区块生成后,区块生成者利用所有代表节点的公钥生成待签名区块,并将其发送给所有代表节点,具体的节点使用多重签名上传区块的步骤如算法 1 所示。若超过半数的代表节点进行签名后,区块生成者将已签名的区块发送至从链网络中,代表节点在接收到这个区块后,将该区块发送至主链中。

算法 1:多重签名上传算法。

输入:周期内的最新区块 B,未打包的交易集合 TX,区块生产者 U,代表节点的集合 $S = \{U_1, U_2, \cdots, U_n\}$

输出:需要上传给父链的区块 B'

1:U 产生未签名信息 $B_0 \leftarrow \{B, \mathrm{TX}\}$;

2:U 统计代表节点公钥,产生待签名信息 $B_1 \leftarrow \mathrm{Block}\{B_0, S\}$;

3:U 将待签名信息 B_1 发送给所有代表节点 $\{U_1, U_2, \cdots, U_n\}$;

4:各个代表节点 U_i 收到 B_1 后用私钥 SK_i 签名,$B_i \leftarrow \mathrm{Sign}\{B_1, \mathrm{SK}_i\}$;

5:代表节点 U_i 将签名结果 B_i 发送给节点 U;

6:U 等待接收的签名数量大于 $n/2$ 后,生成区块 $B' \leftarrow \mathrm{Pack}\{B_1, B_2, \cdots, B_n\}$。

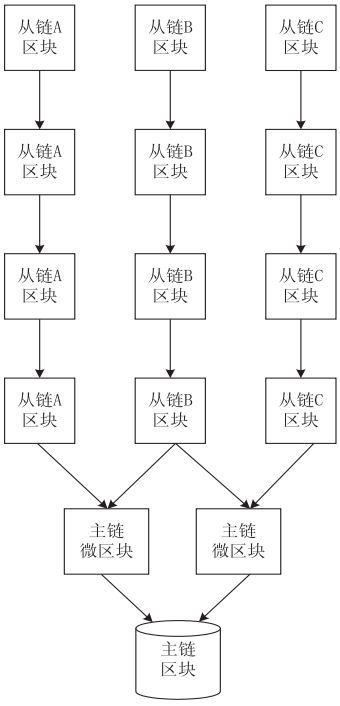

图 2 主从多链区块 DAG 结构

1.2.3 个体共识机制

主链上的节点首先对一级从链上传的区块信息进行个体共识,每个节点会创建一个区块,这种经过个体共识机制产生的区块命名为微区块,区块中包含多个一级从链上传的区块信息。微区块中还包含多种 PoW(proof of work)计算的结果,不同的 PoW 计算采用不同的哈希算法,如 SHA256,ETHASH、X11 等。节点基于自己拥有的算力等资源自主选择几种哈希算法进行 PoW 计算,并将计算成功的结果加入到微区块当中,具体如算法 2 所示。

算法 2:微区块生成算法。

输入:多个从链区块的集合 $\mathrm{BlockSet} = [B_1, B_2, \cdots, B_n]$ 点公钥 Pub,节点选择的算法组 $\mathrm{HashSet} = [H_1, H_2, \cdots, H_X]$

输出:主链微区块 W

1. $W_0 = \mathrm{Genrate}(\mathrm{BlockSet}, \mathrm{Pub})$

2. foreach H_i in HashSet

3. $r \leftarrow$ random number

4. while $H_i(W_0, r) > \text{target}$
5. do $r \leftarrow r + 1$
6. end
7. $\text{proof}_i \leftarrow r$
8. end
9. $W \leftarrow \text{Pack}(W_0, \text{proof}_1, \text{proof}_2, \cdots, \text{proof}_X\}$
10. return W

节点要求微区块需要完成多个 PoW 共识之后才会接受。节点接收到微区块后,会验证微区块是否完成了节点要求的全部 PoW 算法,若完成,则作为元共识机制的输入进行下一步操作。若未完成,则拒绝该微区块。个体共识算法要求生成区块的节点和验证区块的节点均选择多种算法。若区块中完成共识的数量较多,则更多的节点愿意接受该区块,但哈希的计算时间会比较长,晚于其他节点发布区块。若完成数量少,则区块生成时间较短,但生成的区块满足验证节点算法要求的几率较低。

1.2.4　元共识机制

节点在接收到所有的微区块,验证微区块满足算法要求后,会对微区块进行拆包,提取出包含的从链区块的信息。超过半数个体区块打包过的从链区块信息会被打包进该节点生成的主链区块中。假定主链网络中包含了 T 个节点进行个体共识机制 $\{h_1, h_2, \cdots, h_T\}$ 于 N 个一级从链上传的从链区块信息的集合 $\{c_1, c_2, \cdots, c_N\}$ 个体 c_j 来说,有:

$$H(c_j)\begin{cases}\text{accept}, \text{if } \sum_{i=1}^{T} h_i^j(x) > 0.5\ T \\ \text{reject}, \text{otherwise}\end{cases}$$

其中, $H(c_j)$ 表示系统是否接收区块信息 c_j , $h_i^j(x)$ 表示对于个体共识 h_i 中是否包含区块信息 c_j ,若包含则为 1,否则为 0。所有 $H(c_j) = \text{accept}$ 的 c_j 会被打包入主区块中。

所有节点生成主区块后,将区块在网络中进行广播。利用 PoS 共识机制作为主链的共识机制,决定主链区块的生成。假定主链网络中包含了 N 个节点进行元共识机制 $\{m_1, m_2, \cdots, m_N\}$ 中 m_i 从链交易的集合 x 的判断结果为 $m_i(x)$,最终结果 $M(x)$ 为:

$$M(x) = m\left(^{\text{argmax}(w_i)}_{i \in S}\right)(x)$$

其中, S 表示主链网络中随机挑选的 10% 的节点集合, w_i 表示 h_i 在主链网络中的权益。

$$w_i \geqslant 0, \sum_{i=1}^{T} w_i = 1$$

w_i 取决于节点对于主链网络的贡献度。节点在主链网络中最终被接受的区块越多, w_i 越大。

2　安全性分析

在主从多链集成共识中,结合了 PoW 共识机制和 PoS 共识机制,现分析针对 PoW 共识机制与 PoS 共识机制的多种攻击方式对文中提出的主从多链集成共识机制的影响。

(1)自私挖矿攻击。

自私挖矿攻击的主要手段是攻击者成功挖到区块后不进行广播,而是继续进行挖矿,之后通过有选择性地公布区块,构造一条由攻击者自己控制的分叉。在主从多链集成共识机制中,区块生成操作每周期进行一次。每次生成一个区块,节点即使隐藏新块,在真正确立主链区块之前,无法进行下一步操作。攻击者隐藏区块会使其他节点产生的区块被区块链网络所接受,从而失去挖矿奖励。因此,攻击者无法通过自私挖矿攻击获利,反而会减少其收益。

(2)无利害关系攻击。

无利害关系攻击会导致多条分叉并驾齐驱,链中节点无法对主链达成共识,极大地影响区块链的可用性。在主从多链集成共识的元共识机制中,节点使用 PoS 共识机制选择一个节点进行主链区块的生成。主链区块可以指向多个微区块,元共识机制中的节点可以选择让从链区块包含所有的微区块并获取所有微区块的奖励,不需要进行分叉以保持优势。

(3)双重支付攻击。

攻击者进行双重支付攻击的目的是为取消其先前发布的交易信息。在主从多链中,主链只进行从链区块的验证,没有权益或通证的存在,因此攻击者不会对主链采取双重支付攻击。

(4)长程攻击。

长程攻击能够实施的主要原因是在 PoS 共识机制中,节点在生成区块时可以几乎不耗费资源。而主从多链集成共识中,节点需要进行哈希算法生成微区块。因此,节点无法立刻创建出超过正常链长度的分叉链,长程攻击无法实施。

3　实验与分析

3.1　实验环境搭建

文中使用以太坊代码并对其进行修改以搭建主从多链模型。采用 go-ethereum1.11 版本,执行环境为 Ubuntu 16.04LTS。实验运行在 4 台电脑组成的局域网中,具体配置为内存>4 GB、硬盘>30 GB、Intel i5、主频>2.9 GHz。每台电脑中运行了 5 个节点,总计 20 个节点组成主从多链网络。实验为测试主从多链架构中事务的处理速度,尽可能多地向节点发送交易,验证节点能否快速进行交易打包。

3.2　TPS 测试

由于区块链网络采用分布式架构,每个节点会单独进行区块生成,节点的数量不会对网络整体的 TPS

产生较大影响,因此网络的出块速度不会由于节点数量的改变产生较大变化。一共进行了 100 轮共识,实验结果如图 3 所示。对于使用 PoW 共识机制的以太坊而言,TPS 平均值在 35 左右。在主从多链的共识机制中,单条从链的 TPS 在 52 附近上下波动,而主链集成共识机制在饱和的情况下,TPS 能够达到 40。由于主链中只保存了从链区块的信息摘要,信息处理需求小于从链,因而主链的共识机制不会对从链的事务处理速度造成大幅度影响。

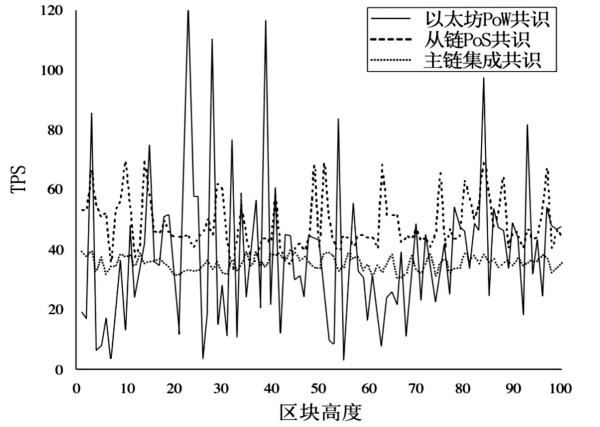

图 3 从链与以太坊 TPS 对比

4 结束语

文中提出了一种区块链集成共识机制,为主从多链模型提供区块安全性验证。利用并行计算的多种共识机制作为个体共识机制,保证了主链在处理从链事务时的效率和完整性。主链中的元共识机制对个体共识机制进行认证,提高了主链区块的安全性。通过多种安全性分析,证明了提出的针对主从多链的集成共识机制较单一共识机制具有更高的安全性。实验结果证明,提出的主从多链集成共识机制相较于单一 PoW 共识的以太坊具有良好的交易处理性能。未来工作将着重于设计合理的从链代表节点选举算法,实现安全可靠的主从链通信过程。

参考文献:

[1] NAKAMOTOS S. Bitcoin:a peer to peer electronic cash system[R/OL]. 2008. https://bitcoin. org/bitcoin. pdf.

[2] 袁 勇,王飞跃. 区块链技术发展现状与展望[J]. 自动化学报,2016,42(4):481-494.

[3] 韩 璇,袁 勇,王飞跃. 区块链安全问题:研究现状与展望[J]. 自动化学报,2019,45(1):206-225.

[4] 何 蒲,于 戈,张岩峰,等. 区块链技术与应用前瞻综述[J]. 计算机科学,2017,44(4):1-7.

[5] MORKUNAS V J,JEANNETTE P,BOON E. How blockchain technologies impact your business model[J]. Business Horizons,2019,62(3):295-306.

[6] 章 峰,史博轩,蒋文保. 区块链关键技术及应用研究综述[J]. 网络与信息安全学报,2018,4(4):22-29.

[7] 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.

[8] 郭 朝,郭帅印,张胜利,等. 区块链跨链技术分析[J]. 物联网学报,2020,4(2):35-48.

[9] LI D,LIU J,TANG Z,et al. AgentChain:a decentralized cross-chain exchange system[C]//18th IEEE international conference on trust,security and privacy in computing and communications/13th IEEE international conference on big data science and engineering. Rotorua,New Zealand:IEEE,2019:491-498.

[10] 李 芳,李卓然,赵 赫. 区块链跨链技术进展研究[J]. 软件学报,2019,30(6):1649-1660.

[11] SCHULTE S,SIGWART M,FRAUENTHALER P,et al. Towards blockchain interoperability[C]//International conference on business process management. Vienna,Austria:Springer,2019:3-10.

[12] BACK A,MAXWELL G,CORALLO M,et al. Transferring ledger assets between blockchains via pegged sidechains:U. S. ,10812274[P]. 2020-10-20.

[13] QI M,WANG Z,LIU D,et al. ACCTP:cross chain transaction platform for high-value assets[C]//International conference on blockchain. Rhode Island,Greece:Springer,2020:154-168.

[14] QASSE I A,ABU T M,NASIRQ. Inter blockchain communication:a survey[C]//6th annual international conference on research track. Rabat,Morocco:Association for Computer Machinery,2019:1-6.

[15] DARISI M,SAVLA J,SHIROLE M,et al. STEM:secure token exchange mechanisms[C]//International conference on advances in cyber security. Penang,Malaysia:Springer,2019:206-219.

[16] GUO Y,TONG J,FENG C. A measurement study of bitcoin lightning network[C]//2019 IEEE international conference on blockchain. Atlanta,USA:IEEE,2019:202-211.

[17] LEWENBERG Y,SOMPOLINSKY Y,ZOHAR A. Inclusive block chain protocols[C]//International conference on financial cryptography and data security. Berlin,Heidelberg:Springer,2015:528-547.

[18] LUU L,NARAYANAN V,ZHENG C,et al. A secure sharding protocol for open blockchains[C]//ACM SIGSAC conference on computer and communications security. Vienna,Austria:ACM,2016:17-30.