许可链多中心动态共识机制

闵新平[1] 李庆忠[1),3)] 孔兰菊[1)] 张世栋[1),3)] 郑永清[1),3)] 肖宗水[2),3)]

[1)](山东大学计算机科学与技术学院 济南 250101)

[2)](山东大学电子商务研究中心 济南 250101)

[3)](山大地纬软件股份有限公司 济南 250101)

摘 要 区块链技术可解决数字化资产可信度低下问题,但大多数解决方案存在交易吞吐量低下、共识延迟过高、通信代价高、难以保证数字化资产全局一致性等方面的限制.许可区块链系统由高可信的节点组成,对特定组织开放,拥有相对良好的网络环境,为区块链的性能扩展提供了新的选择.为支持许可环境中多中心的需求,该文提出许可链多中心动态共识机制,设计两层区块链结构,构建主从多链,通过全局区块链链接多个主体区块链,保证数字化资产的全局一致性,提高区块链性能.通过引入全局区块与主体区块实现交易分流,提高交易吞吐量;通过生成动态验证节点集,设计全局一致性验证模型保证数字化资产的全局一致性;设计多主节点的 PBFT 协议,消除由恶意节点作为主节点带来的交易延迟增加问题.通过安全分析与证明,许可链多中心动态共识机制可保证交易不可篡改、预防 Sybil 攻击等;通过实验验证,许可链多中心动态共识机制可实现秒级交易延迟、十万级交易吞吐量.

关键词 区块链;共识机制;可信度;许可链;数字化资产

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2018.01005

Permissioned Blockchain Dynamic Consensus Mechanism Based Multi-Centers

MIN Xin-Ping[1)] LI Qing-Zhong[1),3)] KONG Lan-Ju[1)] ZHANG Shi-Dong[1),3)]
ZHENG Yong-Qing[1),3)] XIAO Zong-Shui[2),3)]

[1)](*School of Computer Science and Technology, Shandong University, Jinan* 250101)

[2)](*Electronic Commerce Research Center of Shandong University, Jinan* 250101)

[3)](*Dareway Software Co., Ltd., Jinan* 250101)

Abstract Existing solutions leverage blockchain protocols to improve the credibility of digital assets, such as bitcoin blockchain, Ethereum blockchain and Fabric blockchain. Most of blockchain protocols still have significant scalability barriers, such as a higher communication cost, a higher latency, a lower throughput of transaction, a fixed block size and nonsupport of global consistency of digital assets. Permissioned blockchains are made up of highly trusted nodes, open to specific organizations, have a better communication network, and provide new ideas for improving the performance of the blockchain and supporting the global consistency of digital assets. To support the demand of permissioned multi-centers that each center is made up of multi nodes and each user can send any transactions on any centers, by constructing two-layer blockchain and introducing a master-slave blockchain, this paper presents an Permissioned Blockchain Dynamic Consensus Mechanism based Multi-Centers (PBCM), each center has a peer blockchain that keeps itself transactions and global blockchain keeps the abstract of trusted transaction from all centers, PBCM

收稿日期:2017-08-19;在线出版日期:2018-01-22.本课题得到国家自然科学基金(61772316)、泰山产业领军人才专项(tscy20160404)、山东省重点研发计划(2017CXGC0702)资助.**闵新平**,男,1993 年生,博士研究生,主要研究方向为区块链、共识协议.E-mail:minxinping0105@126.com.**李庆忠**(通信作者),男,1965 年生,博士,教授,博士生导师,主要研究领域为数据计算、云计算软件架构、数据科学与智能数据分析.E-mail:lqz@sdu.edu.cn.**孔兰菊**,女,1978 年生,博士,副教授,主要研究方向为大规模数据管理.**张世栋**,男,1969 年生,博士,教授,主要研究领域为云计算软件架构.**郑永清**,男,1965 年生,博士,研究员,主要研究领域为数据计算与云计算软件架构.**肖宗水**,男,1963 年生,硕士,应用研究员,主要研究领域为区块链与业务流程.

《计算机学报》

uses global blockchain to link with multi peer blockchains to improve the performance of permissioned blockchain, and by preventing user from sending multi transactions about the same digital asset at multi centers at the same time, PBCM can guarantee the global consistency of digital assets. By introducing global block and peer block, peer block contains the specific content of transactions and is proposed by each center, global block contains the abstract of trusted transactions and is proposed by global committee, each peer blockchain just keep itself transactions, PBCM can divide transactions into multi peer blockchains to improve the throughput of transactions and reduce the consensus latency of transactions. To guarantee the global consistency of digital assets, this paper presents a Global Transaction Validation Model (GTVM) by constructing dynamic validation group for each peer, the membership of each validation group changes over time to make a trusted validation group, and each validation group validate the global consistency of digital assets according to block header that each peer send, GTVM can solve the double spending problem caused by the user send multi transactions about the same digital asset at different centers at the same time, and GTVM uses the header of peer block to validate the global consistency of digital assets to reduce the communication cost. This paper presents a Multi Primary Node PBFT Protocol (MPBFT) to solve the problem of latency caused by malicious node as primary node, MPBFT selects multi primary node to construct global block on the same time and choose the first illegal block as the finial block. To solve the problem caused by the fixed membership of committee, this paper constructs a dynamic global committee to maintain the global blockchain, the membership of global committer changes over time. By analyzing the credibility assumption, we prove that PBCM can guarantee the credibility of transaction, can resist Sybil Attack and the PBCM is reliable and feasible. The comparison between PBCM and other permissioned blockchains, the throughput can up to 100KTPS and the transaction latency can be controlled under seconds.

Keywords blockchain; consensus mechanism; credibility; permissioned blockchain; digital asset

1 引 言

数字化资产是以电子数据形式存在的各种资产,如数字货币、数字音乐等.目前数字化资产交易管理平台如电子商务平台、物流平台等,所有数据均由单一的中心化平台或单一的数字化资产服务商管理与维护.由于数字化资产交易管理平台由单一的服务商负责管理与维护,数据与平台相对封闭,数据所有权不属于用户;平台内部人员私自篡改数据难以发现,由于数据只属于单一服务商,不与其他平台进行数据交叉验证,被篡改的数据也会被作为真实数据,故目前的数字化资产交易平台提供的数据的可信性难以保证.区块链具有不可篡改、全网集体维护数据等特性,可保证数据不可篡改,保证交易高可信,故可基于区块链重构高可信的数字化资产交易环境.

以比特币[①]为代表的非许可区块链(非许可链)在数字货币、数据存证等领域发挥了巨大作用;但由于以比特币为代表的区块链采用单链模型,所有数字化资产的所有交易混合在一起,影响交易的并发量;采用 POW[1](工作量证明)机制,存在交易吞吐量低下、交易延迟过高等问题;允许节点任意加入,任意用户均可获取任意区块链用户的交易记录,数据的隐私性得不到保障,同时难以支持其他领域(如公共服务领域的证照、健康档案等)的数据安全及高性能需求;以比特币为代表的非许可链采用完全去中心化机制,实现了真正意义上的民主自治,但是非许可链不支持许可管理与监管,难以在数字化资产领域有更多的落地的应用.

许可区块链仅准许具有高信任度的节点来验证交易,对特定的组织或群体开放,每个组织或群体由多个高信任度的节点组成,每一个组织或者群体作为一个中心,每个中心维护本中心的数据,可避免数

① Bitcoin. https://bitcoin.org/en/bitcoin-paper, 2008

据全网透明带来的风险，防止数据泄露，同时可获得较高的性能，由此许可区块链引起了越来越多的关注. 许可链为公共服务、政务服务等领域提供了新的选择，亟需投入更多的资源进行研发.

单链模型中，所有数字化资产的所有交易混合在一条链上会影响交易的并发量、增加数据管理的难度，故许可链一般采用多链模型来提高区块链性能，侧链、联盟链等多链机制在交易吞吐量、交易延迟等方面进行了扩展.

现有联盟链，如小蚁[①]、Hyperledger[②] 等，将整个区块链网络划分为不同的共识群组，每个共识群组维护一条区块链，每个区块链仅存储所属共识群组的交易数据，通过将交易分流到不同区块链的方式实现交易吞吐量的扩展，即将两个中心之间存在多条区块链来存储交易，不同区块链之间相互独立，由此导致用户只能在特定的区块链上发起交易，难以实现不同区块链之间数字化资产的转移，同时难以保证多条链之间数字化资产的一致性；由于每个共识群组的成员相对固定，难以防止恶意节点相互勾连篡改数据；且仍存在交易延迟过高、交易吞吐量低下等限制. 在本文的许可环境中，许可链网络由多个中心的节点组成，数字化资产全局唯一，可在任意的中心上被交易；用户拥有多个数字化资产，用户可在任意的中心上交易所拥有的数字化资产；在上述许可环境下(即许可多中心)，联盟链难以预防跨中心双花问题(即用户同时在不同中心交易同一数字化资产)、难以支持许可多中心、难以保证数字化资产全局一致性.

侧链机制中[③]，每条区块链维护不同的数字化资产，通过将每种数字化资产独立处理的方式来提高交易吞吐量；但由于侧链机制多采用 POW 共识协议或其改进协议，需要在交易速度与安全性之间均衡，由此造成交易延迟较高、交易吞吐量低下；主链与侧链进行数字化资产兑换时需要通过 SPV[1] 技术锁定主链上的账户与数字化资产，降低侧链的交易并发量；在主链资产锁定期间，为保证数字化资产的安全性需要通过长达 1～2 天的工作量计算，由此导致交易延迟过长；同时在资产确认期间，易撤销资产兑换；新增数字化资产需要新增地址类型与一条区块链，增加了系统的维护性；数字化资产全局不唯一，同一数字化资产在不同区块链的含义不同；在许可多中心环境下难以保证主链与侧链数字化资产的一致性、难以支持许可多中心；故需改进区块链以支持许可多中心，实现更高的交易吞吐量、更低的交易延迟、更低的网络通信代价.

许可多中心环境中，每个中心由多个区块链节点组成，各个中心的区块链节点通过共识算法维护本中心的区块链；由于中心由若干个区块链节点组成，中心篡改数据的可能性增大，故需防止中心篡改数据；由于数字化资产全网唯一、不属于任何一个中心，交易双方可以跨中心进行交易数字化资产，故需保证数字化资产在不同中心的全局一致性，防止跨中心双花(Double Spending)问题发生.

本文针对现有区块链性能低下、难以保证数字化资产全局一致性、难以支持许可多中心等问题，构建面向多中心的许可区块链，参与方为不同主体(中心或组织)，每个主体具有唯一的身份标识，每个主体由若干区块链节点组成，各个主体的区块链存储本主体的交易内容；数字化资产全局唯一，可在任意中心被交易；交易双方不属于任何一个主体，交易双方(实体)通过不同主体发起交易，可在任意的主体上交易数字化资产. 基于本文所构建的许可区块链，本文提出许可链多中心动态共识机制(Permissioned Blockchain Dynamic Consensus Mechanism Based Multi-Centers，PBCM)，构建主从多链结构，各主体维护本主体的交易区块链(从链)，所有主体集体维护全局区块链(主链)，从链存储交易内容，主链存储不存在双花问题的交易的摘要，保证交易不可篡改；每个主体的验证群组验证数字化资产的一致性，保证数字化资产在不同的主体中均满足全局一致性，避免双花问题发生. 通过为每个主体构建动态验证群组，分区验证数字化资产一致性，提高交易吞吐量；验证群组随时间动态变化防止主体相互勾结篡改数据；全局区块链采用多主节点的 PBFT 共识算法，由此减少由拜占庭节点作为主节点带来的交易延迟增大问题，降低交易延迟.

本文贡献如下：

(1) 提出一种许可链多中心动态共识机制，支持许可多中心，保证数字化资产及其交易信息不可篡改、提高区块链性能. 设计两层交易区块链，利用主从多链相互锚定，保证交易不可篡改；为主体生成动态验证群组，分区验证数字化资产一致性，提高交易吞吐量、降低交易延迟、降低网络通信代价.

(2) 提出数字化资产一致性验证机制，保证数字化资产在不同主体中不存在的全局一致性问题. 通过全局一致性验证算法，保证数字化资产在不同

① The Antshares. http://www.antshares.org/ 2015
② The Hyperledger. https://www.hyperledger.org/2015
③ Enabling blockchain innovations with pegged sidechains. https://people.xiph.org/~greg/sidechains.pdf 2014

《计算机学报》

的主体中均满足全局一致性，避免双花问题.

(3)提出多主节点的 PBFT(Multi-Primary Node PBFT，MPBFT)协议，减少由拜占庭节点作为主节点带来的交易延迟增大问题，提高全局区块链构建效率，降低交易延迟.

(4)通过安全分析，许可链多中心动态共识机制可实现安全可信的数字化资产交易环境，可保证交易不可篡改.

(5)通过实验验证，许可链多中心动态共识机制可达到十万的交易吞吐量，10 秒以下交易延迟. 在保证数字化资产可信前提下，将许可链网络划分为不同的群组，验证交易一致性，提高易吞吐量；利用全局一致性校验算法验证交易一致性，降低交易延迟；利用主链链接各个从链，扩展区块容量.

本文第 2 节介绍有关区块链性能扩展的研究；第 3 节介绍基本定义及问题描述；第 4 节介绍交易一致性验证共识机制；第 5 节介绍全局区块链共识机制；第 6 节证明许可链多中心动态共识机制可实现可信交易；第 7 节通过实验说明许可链多中心动态共识机制具有更高的性能；第 8 节是对本文共识机制的总结以及未来工作的展望.

2 相关工作

以比特币为代表的区块链存在以下不足：交易延迟较高，每笔交易需经过 1 个小时才能被确认生效；交易吞吐量低下，每秒只能处理 7 笔交易；区块大小受限，每个区块只能存储 1 MB 的数据，而采用 SegWit2x[1] 协议扩容之后每个区块可存储 2 MB 的数据，一个区块最多存储 10 万条左右的数据；数据的隐私性得不到保障，参与节点均可获取全部交易数据. 综上所述，比特币等非许可链区块链技术并不能适应需要即时处理、吞吐量高的数字化资产，因此提高区块链性能刻不容缓.

Blockchain Contract[2] 通过所有节点存储完整区块链，实现可信交易；为提高区块链性能，Bitcoin-NG[3] 通过引入微区块，扩展区块容量和交易吞吐量，但未解决交易延迟过高与区块链分叉问题；SCP[4] 通过将全网节点划分为不同的群组，利用算力扩展吞吐量等；但采用 POW 机制划分群组，增加交易延迟. 在保证交易可信性前提下，大多数解决方案在吞吐量和交易延迟间权衡. 例如：交易吞吐量受区块大小和区块间隔两个因素影响. 增大区块大小，可获得更高的吞吐量，但构建更大的区块，交易验证时间变长；缩短区块间隔，可获得较低的交易延迟，易引发区块链分叉，降低交易可信性[2]. 通常以较高的交易延迟，换取更高的交易吞吐量与交易可信性. 区块链技术的扩展问题主要集中在吞吐量、延迟、区块大小等方面.

在提高交易吞吐量和可信性、降低交易延迟、扩展区块大小等方面的研究已经有很多. Miller 等人[5] 利用可信力较高的节点提高交易吞吐量、降低网络通信代价；但恶意节点可利用可信力较高的节点降低篡改区块被拒绝的概率，从而使篡改的数据生效. Decker 等人[6] 提出链下交易支持即时交易，在不增加区块链网络负担的前提下，利用在任意两个节点之间构建的交易通道，缩短交易延迟；但需提前锁定数字化资产. Miller① 提出一种同步通信模型，利用双向广播机制，降低通信代价，但没有显著提高交易吞吐量. Lewenberg 等人[7] 基于有向无环图的区块构建可扩展的区块链协议来实现更高的交易吞吐量. Bitcoin-NG 通过构建关键区块和微区块，提高交易吞吐量. 关键区块作为索引区块，而微区块包含本时间片段内的具体交易. 每个时间片段内，Bitcoin-NG 仍将所有区块广播给所有节点，因此会导致微区块之间相互依赖问题，同时并未解决区块链分叉问题.

保证交易可信性前提下，上述研究集中在非许可链方面，没有同时解决吞吐量、延迟、区块大小等问题；且依赖算力提高区块链性能，易引发算力越高的节点越可能成功篡改数据等问题；不能满足许可多中心的需求.

许可区块链由可信度较高的节点组成，对特定的组织或群体开放，进一步提高了区块链性能. 许可链在交易吞吐量、交易延迟、区块大小等方面的研究相对较少. Poon② 提出闪电网络，通过在任意两个群组之间建立链下支付通道，仅有少量交易添加到区块链中，提高了交易吞吐量. 链下支付通道尽管显著提高交易吞吐量，但仅支持小额支付，大额支付仍需可靠的加密网络. GHOST[8] 允许并行处理区块，从而降低交易延迟；但仍需将区块广播到所有节点，且无法通过算力扩展吞吐量. 小蚁区块链提高了交易吞吐量，采用 DBFS 机制，易造成事实上的中心；Hyperledger 采用 PBFT 机制，通过将交易分流到多条区块链的策略实现交易吞吐量的扩展，但是难以

① Anonymous byzantine consensus from moderately-hard puzzles: A model for bitcoin. Available on line: http://nakamotoinstitute.org/research/anonymous-byzantine-consensus 2014

② Poon J, Dryja T. The bitcoin lightning network: Scalable off-chain instant payments. Technical Report (draft). https://lightning.network, 2015

《计算机学报》

保证多个区块链之间数字化资产的全局一致性、难以保证数字资产全局唯一等；由于侧链机制多采用POW共识协议，侧链机制需要在交易速度与安全性之间做均衡，数字化资产在主链与从链进行兑换时，存在交易吞吐量低下、交易延迟过高等问题；Tsai等人[9]提出ABC(账户区块链)与TBC(交易区块链)结合的区块链架构，通过采用sharding策略构建多条区块链存储交易，极大地扩展了区块链性能，但并未涉及多条区块链的全局一致性问题.

上述研究虽然解决了交易吞吐量低下与交易延迟过高的问题，但多种类型的数字化资产集中在同一条区块链上，限制性能的进一步扩展；同时难以保证数字化资产在不同主体中均满足全局一致性. 本文提出许可链多中心共识机制，解决交易吞吐量过低、交易延迟过高等问题，支持许可多中心需求，保证交易不可篡改.

3　模型描述

在面向多中心的许可链架构中，数字化资产交易双方可以跨主体进行交易，即在不同主体上同时交易同一数字化资产. 若将同一数字化资产同时跨主体进行交易，或者将已交易的数字化资产再次跨主体进行交易，即同一数字化资产被交易多次，此类情况不满足交易一致性，即存在双花问题. 故需保证交易在所有主体中均不存在双花问题，即数字化资产在所有主体中的状态是一致的.

许可链多中心动态共识机制包括交易一致性动态验证机制与全局区块链共识机制(Mulit Primary Node PBFT，MPBFT). 为保证数字化资产一致性，交易一致性动态验证机制为主体生成动态验证群组，利用多中心协同验证数字化资产的一致性，同时通过分区策略解决现有区块链技术吞吐量低下和交易延迟过高等问题；通过主从链相互锚定，保证交易的不可篡改性；为降低交易延迟，构建群组利用MPBFT构建全局区块，避免拜占庭节点作为主节点时带来的交易延迟增加问题.

如图1所示，许可链多中心动态共识机制中，将时间划分为不同的时间片段，每个时间片段称为一轮. 每个主体均维护本主体的区块链，所有主体集体维护全局区块链；全局区块链存储所有主体认为不存在“双花”问题交易的摘要，每个主体的区块链存储本主体的交易数据. 主体的区块链节点采用PBFT共识协议，每轮选举出一个节点代表本主体，此节点称为主体的代表节点($RNode$)，代表节点负责与其他主体的节点通信；基于随机投票机制，主体的验证群组从全网其他主体的节点中选举产生主体的下轮验证群组；基于随机投票机制，所有主体的验证群组从全网节点中随机选择一组节点作为下轮的全局构建群组；主体的初始验证群组由主体的代表节点从全网节点中选举产生，全局构建群组由所有主体的初始验证群组从全网节点中选举产生. 主体的代表节点将主体区块头数据广播给主体的验证群组；主体的验证群组验证交易是否满足全局一致性；主体的验证节点将将满足全局一致性的交易的摘要发送给构建群组；构建群组利用MPBFT协议构建全局区块. 许可链多中心动态共识机制中相关定义如下.

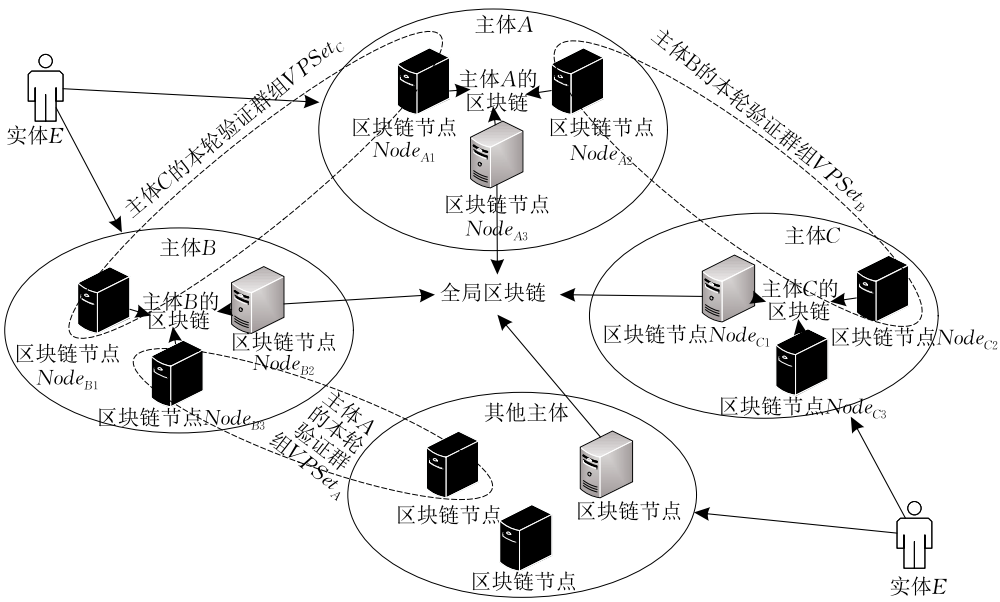

图1　许可链多中心动态共识机制架构

定义 1. 数字化资产 DA. 数字化资产是指企业、组织或个人拥有或控制的,以电子数据的形式存在的,持有以备出售或处在生产过程中的资产. 数字化资产可代表某种数字产品、实体产品或者电子信息等,数字化资产通过 DA_{ID}(数字化资产 ID)全网唯一标识.

定义 2. 交易 T. 交易是指交易双方对数字化资产达成的某种等价约定. $T=(From, To, DA, SigList, TxID)$,$From$ 表示数字化资产供方;To 表示数字化资产需方;DA 表示数字化资产,如金额、电子数据等;$SigList$ 表示交易双方签名列表;$TxID$ 表示交易的 ID(基于哈希算法生成),交易 ID 全网唯一. 交易具有三种状态 $\sigma(T)=\{undefined, valid, invalid\}$,不确定状态 $undefined$、有效状态 $valid$、无效状态 $invalid$. 通过一致性验证算法验证交易是否满足交易一致性,交易的状态由 $undefined$ 转为 $valid$ 或 $invalid$. 可信交易 $\sigma(T)=valid$,即满足交易一致性(不存在双花问题)的交易. 由于交易会触发数字化资产状态的改变,判断数字化资产是否满足一致性,即判断交易是否满足一致性.

定义 3. 主体(Peer) $P_i\in\{P_1,\cdots,P_N\}$,N 表示许可链网络中主体的数量. 主体表示许可链网络中不同的参与方,如电子商务交易平台、物流平台、供应链平台以及政府监管部门等. 主体 P_i 利用公钥地址进行标识,并保存其他主体的身份标识. 每个主体包含多个区块链节点 $Node_{ij}$,$j\leq n_i$,$Node_{ij}$ 表示主体 P_i 的第 j 个节点,n_i 表示主体 P_i 的区块链节点数量. 可信主体是指遵循可信共识机制的、维护许可链网络正常运行的主体,不可信主体是指违背可信共识机制的、扰乱共识过程的主体. 主体分为交易主体和监管主体;交易主体为电子商务交易平台、物流平台、供应链平台等,监管主体主要为政府等监管部门. 交易主体具有发起交易与维护区块链的权利,监管主体仅参与维护区块链,不发起任何交易. 由于监管主体不发起交易,故监管主体的可信度较高,属于可信主体.

定义 4. 节点 $Node_{ij}$ 表示主体 P_i 的第 j 个节点,$\{Node_{ij}, 1\leq i\leq N, 1\leq j\leq n_i\}$. 节点之间通过 P2P(点对点)的异步消息机制进行通信. 节点根据不同的需求拥有不同的身份类型:构建节点 CP、验证节点 VP、普通节点 RP. 每个节点的类型随时间动态改变. 构建节点负责维护全局区块链;验证节点负责验证交易是否满足全局一致性;普通节点仅仅发起交易、维护本主体的交易区块链以及验证交易是否满足局部一致性. 构建节点与验证节点同时也作为普通节点维护本主体的交易区块链以及验证交易是否满足局部一致性. 节点通过公钥地址进行标识,主体 P_i 的所有节点存储主体 P_i 的私钥,利用主体 P_i 的私钥及节点的私钥对区块进行签名. 违背可信共识机制、篡改交易信息、网络通信不畅、扰乱网络正常运行的节点,称为恶意节点[10];恶意节点可以联合起来扰乱共识过程. 诚实节点是指遵循可信共识机制、维护网络正常运行的节点. 可信主体的节点均为诚实节点,不可信主体的节点均为恶意节点. 如图 2 所示,主体 P_i 的验证群组 $VPSet_i$ 由验证节点组成,验证主体 P_i 的交易是否满足一致性;主体 P_i 的验证群组随时间动态变化,主体 P_i 的当前验证群组从全网节点中随机选择一组节点(不属于本主体的节点)作为主体 P_i 的下轮验证节点集 $NextVPSet_i$. 全局构建群组 $CPSet$ 由构建节点组成,全局构建群组由每轮所有主体的验证群组的主节点从全网中随机选择一组节点组成,全局构建群组随时间动态变化.

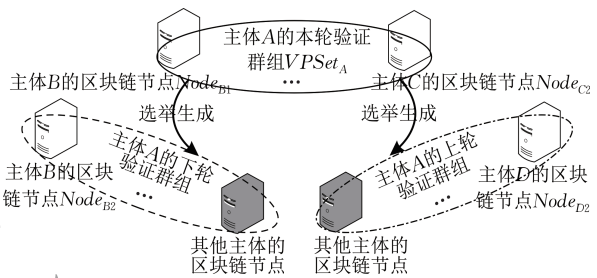

图 2 主体的验证群组

定义 5. 实体表示数字化资产的供方、数字化资产的需方,即 $E=\bigcup_T(From)\cap\bigcup_T(To)$,同时表示数字化资产的交易双方. 实体不属于任何一个主体,实体 ID 作为实体的全网唯一标识. 实体可在任意主体上发起交易.

定义 6. 两层交易区块链. 如图 3 所示,每个主体的区块链节点通过 PBFT 共识协议维护本主体的交易区块链,所有主体集体维护全局区块链;主体交易区块链(从链)通过主体区块 PB(Peer Block)链接而成,主体区块存储本主体的交易数据和主体区块头数据 PBH(Peer Block Header);主体区块头 PBH(Peer Block Header)存储本区块内所有交易的 $TxID$、实体列表、数字化资产 ID 等信息;全局区块 GB(Global Block)将不同主体交易区块链链接起来,构成全局区块链(主链). 全局区块存储满足全局一致性的交易的 $TxID$,全局区块以交易的存储可信交易,每条全局区块的交易中包含多条可信交易,交易格式如下:

$GBTX=\langle GViewID, ChainID, CBlockID, TxList\rangle$,其中 $ChainID$ 表示主体区块链(从链)的标识,

《计算机学报》

CBlockID 表示 *ChainID* 上的主体区块的摘要值，*TxList* 表示可信交易的 *TxID* 列表及对应的数字化资产 ID，*GViewID* 表示当前所属的时间片段序号（轮数），当主体宕机再恢复时，主体可根据 *GViewID* 快速获取当前以及下轮的验证群组、全局构建群组等信息.

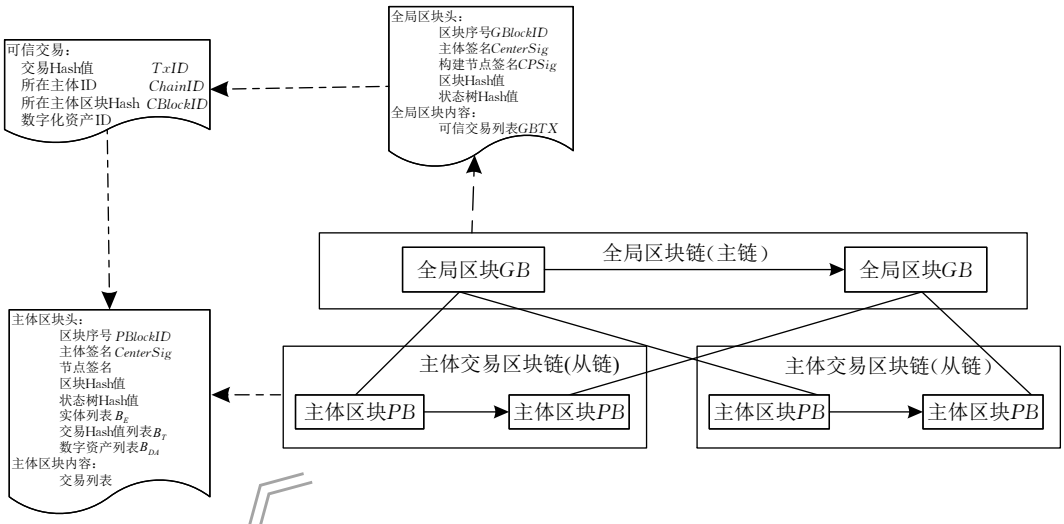

图 3　两层区块链架构

局部一致性是指数字化资产在本主体的主体交易区块链中不存在双花问题；全局一致性是指数字化资产在所有主体交易区块链中均不存在双花问题. 本文通过局部与全局一致性验证算法，防止双花问题的发生. 通过局部一致性验证算法，每个主体保证本主体的交易区块链不存在双花问题；通过全局一致性验证算法，所有主体保证数字化资产满足全局一致性.

4　交易一致性动态验证机制

交易一致性动态验证机制的核心思想是：为主体 P_i 构建可信的验证群组，验证群组利用主体区块头数据验证交易是否满足全局一致性，防止双花问题发生；同时通过分区策略解决现有区块链技术吞吐量低下和交易延迟过高等问题. 如图 4 所示，主体

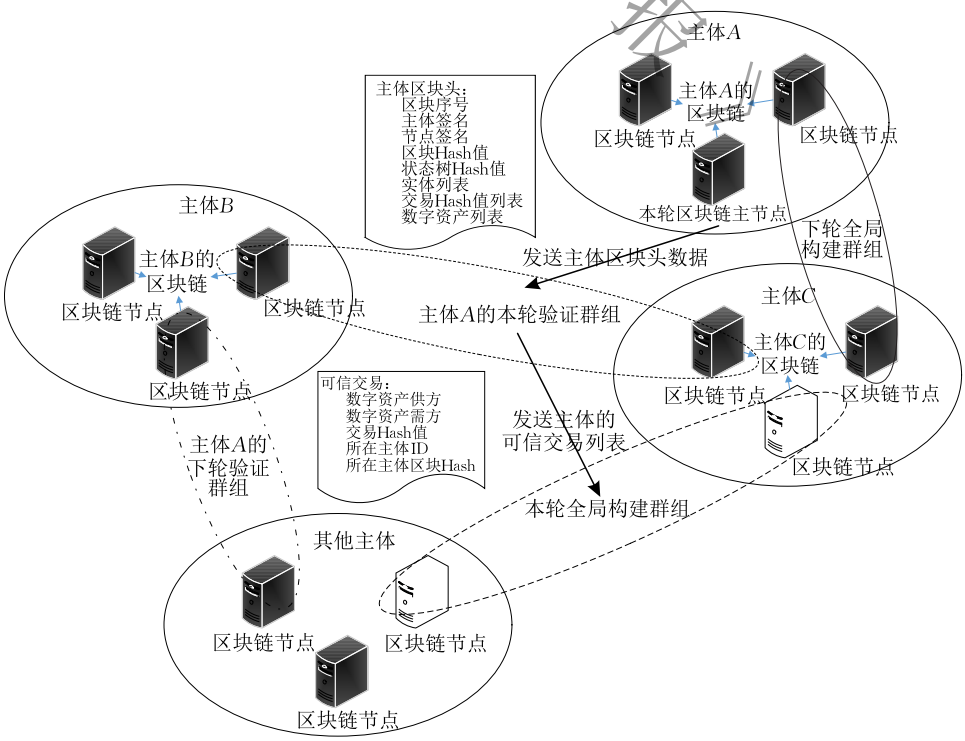

图 4　交易一致性动态验证机制

P_i的区块链节点通过 PBFT 共识算法维护本主体的区块链，主体 P_i的区块链仅存储主体 P_i的交易数据；主体 P_i的验证群组验证主体 P_i的交易是否满足全局一致性，防止跨主体双花问题发生；主体 P_i的验证群组将不存在全局一致性问题的交易的 $TxID$ 发送至全局构建群组；全局构建群组利用 MPBFT 机制构建全局区块链. 只有交易的 $TxID$ 被写入到全局区块链中，该交易才被认定为可信交易.

验证群组生成算法(见 4.1 节)从全网节点中随机选出 K 个验证节点作为主体 P_i的验证群组，主体 P_i的验证群组通过全局一致性验证算法(见 4.2 节)验证主体 P_i的交易是否满足全局一致性；主体 P_i的当前验证群组为主体 P_i构建下轮验证群组.

交易一致性动态验证共识机制如算法 1 所示：主体 P_i的代表节点将本主体的主体区块头数据广播给主体 P_i的当前验证群组 $VPSet_i=\{VP_1,\cdots,VP_K\}$；$VPSet_i$通过全局一致性验证算法来验证交易是否满足全局一致性；验证节点将满足全局一致性的交易的 $TxID$ 广播至构建群组 $CPSet$. 每轮结束之前，主体 P_i验证群组 $VPSet_i$从全网其他主体的节点中选出一组节点作为主体 $VPSet_i$的下轮验证群组 $NextVPSet_i$；所有主体的验证群组从全网节点中选出一组节点作为下轮的全局构建群组 $NextCPSet$.

算法 1. 主体交易一致性验证机制.

```
输入：主体的交易
输出：主体的可信交易
Algorithm ConsistentValidationMechanism
  FOR Pi in {P1,…,PN}
    //所有主体生成自己的验证群组
    VPSeti<—CreateValidtionSet()
    MaintainSelfBlockchain()
    //Pi的代表节点将 PBH 发送给 VPSeti
    RNode.sendPBH(PBH)
  ENDFOR
  FOR primary node of each VPSeti
    //验证群组的主节点发起全局一致性验证
    SendGlobalConsistentValidationRequest(PBH)
  ENDFOR
  FOR each node of each VPSeti
    RecievePBHAndSorted() //按到达的先后顺序排序
    vaidationTxConsistent() //验证交易一致性
    sendTrustedTxt() // 将可信交易发送给 CPSet
  ENDFOR
  CPSet.CreateGlobalBlock() //构建全局区块
  FOR VPSeti of each Peer
    NextVPSeti<— CreateNextVerifictionSet()
  ENDFOR
  NextCPSet<— CreateNextConstructionSet()
END
```

主体 P_i由若干节点组成，采用 PBFT 机制维护主体 P_i的交易区块链，验证交易是否满足局部一致性；每轮选取一个代表节点负责构建主体区块，由代表节点将本主体的主体区块头数据发送给验证群组. 主体 P_i的验证群组基于 PBFT 共识协议验证交易是否满足一致性，防止双花问题发生；验证群组并将满足全局一致性的交易的 $TxID$ 发送给全局构建群组；全局构建群组采用 MPBT 协议构建全局区块. 主体 P_i将主体区块头数据发送给验证群组后，不需等待验证群组的验证结果，继续构建主体 P_i的主体区块.

4.1 验证群组生成算法

群组成员相对固定会引发交易被篡改、节点可信度降低等问题，故本文提出验证群组生成算法为主体 P_i生成可信的动态验证群组，验证群组的成员随时间动态变化. 验证群组生成算法包括验证群组初始化算法和下轮验证群组生成算法. 为保证主体 P_i的初始验证群组中至少存在一半以上的诚实节点，主体 P_i的代表节点随机从全网节点中选择 K 个主体，$K>2N/3$，K 个主体的代表节点在每个主体中随机选择一个节点作为主体 P_i的初始验证节点，且 K 个主体中必须包含监管主体.

验证群组初始化算法描述如下：主体 P_i的代表节点随机从全网中选择 K 个主体，K 个主体的代表节点在每个主体中选择一个节点作为主体 P_i验证群组的候选节点 GP_i；K 个主体的代表节点将选择(投票)结果发送给其他 $K-1$ 个主体的代表节点和主体 P_i的代表节点；主体 P_i的代表节点和 K 个主体的代表节点将出现次数最多的 K 个节点作为主体 P_i的验证群组 $VPSet_i$；各个主体的代表节点将统计结果($VPSet_i$的成员信息)广播给本主体内的节点，$VPSet_i$中的每个验证节点相互通信，由此验证节点之间建立连接.

下轮验证群组生成算法描述如算法 2 所示：主体 P_i的当前验证群组 $VPSet_i$随机选择 K 个主体，在每个主体选择一个节点作为主体 P_i的下轮验证群组 $NextVPSet_i$，满足 $VPSet_i\cap NextVPSet_i=\varnothing$(即某一节点不允许连续两轮作为某一主体的验证节点，且 $K>2N/3$；VP 将本节点的投票结果发送给其他 $K-1$ 个验证节点和主体 P_i的代表节点；验证节点 VP 和主体 P_i的代表节点统计出现次数最

多的 K 个节点作为 $NextVPSet_i$，并将最终投票结果 $CNextVPSet_i$（下轮候选验证群组）发送给构建群组.

算法 2.　下轮验证群组生成算法.

```
输入：主体的本轮验证群组，全网节点
输出：主体的下轮验证群组
Algorithm CreateNextVerifictionSet
  FOR each VP in VPSet_i
    candidateList<— selectCandidataNode()//选取候选节点
    //将本节点的投票结果发送给其他验证节点
    sendSelfVoteToOther(candidataList)
    result<— CalVoteFromAllVP()//计算投票结果
    //将投票结果发送给构建群组
    sendMsgToCPSet(result)
  ENDFOR
  CPSet. DO {
    //计算每个主体的下轮验证群组
    NextVPSet_i<—CalPeerVPSet()
    //CPSet 其他节点共识结果
    Consensus(NextVPSet_i)
    IF AllPeerNextSetCaled()
      sendinfoToAllPeer(NextVPSet_i)
    ENDIF
  }
  FOR each node in NextVPSet_i
    //接受构建节点的消息，获取成员列表
    VlidateGroupMember=getFromCPMessage()
    //验证节点之间建立通信
    CommunicationMember(ValidationGroupMember)
  ENDFOR
END
```

构建群组将 $K+1$ 个中 $CNextVPSet_i$（主体 P_i 的下轮候选群组）出现次数最多的 $CNextVPSet_i$ 作为主体 P_i 的下轮验证群组 $NextVPSet_i$. 当构建群组计算出所有主体的下轮验证群组时，将每个主体的下轮验证群组的成员列表，发送给每个主体的当前以及下轮验证节点、代表节点. 构建节点 CP 将每个主体的 $NextVPSet_i$ 成员列表广播给 $K/3$ 个主体的代表节点，每个主体的代表节点将下轮群组消息发送给本主体的节点，每个节点由此获得本节点下轮的节点类型. 基于以上机制，可保证下轮验证节点接收到正确的验证群组的成员列表信息.

在主体 P_i 下轮验证群组构建过程中，本轮验证节点之间相互发送投票信息的通信代价为 $O(K^2)$；验证节点将本节点统计出的下轮验证群组成员信息发送给全局构建群组的通信代价为 $O(K\times CK)$，CK 表示全局构建节点的数量；全局构建群组统计出主体 P_i 的下轮验证群组成员信息的通信代价为 $O(CK)$；全局构建群组将主体 P_i 的下轮验证群组成员信息发送给本轮验证群组、所有主体的代表节点、下轮验证群组的通信代价为 $O([(2K+N)/3]\times CK)$；下轮验证节点之间相互通信的代价为 $O((K/2)\times(K-1))$；故主体 P_i 的下轮验证群组的构建代价为 $O\left(K^2+(K+1)\times CK+\frac{(2K+N)}{3}\times CK+\frac{K}{2}\times(K-1)\right)$，由于 $2N/3\leq K$，$CK\leq N$，故主体 P_i 的下轮验证群组的构建代价为 $O(N^2)$.

4.2　全局一致性验证算法

主体 P_i 的验证群组通过全局一致性验证算法来保证数字化资产在不同的主体中均满足全局一致性，即同一时刻只允许同一数字化资产在一个主体中被交易，由此避免跨主体双花问题发生；每个主体的验证群组仅验证本主体的数字化资产是否满足全局一致性，通过分区验证数字化资产的全局一致性来提高交易吞吐量.

交易一致性动态验证机制中，主体 P_i 的代表节点需要将交易的某些关键信息广播给 P_i 的验证节点，以便验证群组验证交易是否满足全局一致性；若主体 P_i 将每笔交易广播给全网所有节点，全网通信代价为 $\sum_{i=1}^{n}N_T_{ij}\times n^2$，$n$ 表示全网节点数，N_T_{ij} 表示第 i 个主体第 j 个区块中包含交易的数量；若主体 P_i 将具体的交易内容发送给其他主体的节点，易引发隐私信息泄露问题. 若主体 P_i 将区块内容广播至全网，由于区块较大，交易一致性验证时间会变长，增加区块链存储与维护成本；故本文提出一种基于区块头数据的全局一致性验证算法，降低网络通信代价，提高交易吞吐量.

由于主体 P_i 的验证群组由至少全网 $2N/3$ 个主体的节点组成，根据容氏原理，故任意两个主体的验证群组中至少存在 $N/3$ 的个节点来着相同的主体；由于属于同一个主体的节点共享所有信息，故主体 P_i 的验证群组中至少存在一半以上的验证节点可获取全网其他主体的主体区块头数据；故全局一致性验证算法如算法 3 所示：主体 P_i 的代表节点将主体区块头数据广播给本主体所有验证节点；验证节点按照 PBH 到来的先后顺序验证交易是否满足全局一致性；验证节点按照以下规则进行该主体区块的

《计算机学报》

一致性验证:同一时刻同一数字化资产至多允许交易一次,即同一全局区块链高度下,同一数字化资产不允许出现在全网其他主体的主体区块头数据中.

主体区块的区块头 PBH 结构如下:

$$PBH=(B_E,B_T,B_p,B_{DA},CBlockID),$$

$$B_T=\{\bigcup_{T_i\in PB}(TxID)\},$$

$$B_E=\{\bigcup_{T_i\in PB}E\}.$$

主体区块头包含以下信息:本主体区块所有交易的 $TxID$ 列表 B_T,所关联实体列表 B_E,主体签名,创建时间,前一区块的哈希值 B_p,数字化资产 ID 列表 B_{DA},$GBlockID$ 代表当前全局区块的 ID.

主体 P_i 的验证群组将本群组认为不存在全局一致性问题的交易 $TxID$ 的以消息的形式发送给全局构建群组,消息格式如下:$Msg=\langle ChainID,CBlockID,TxID,DA,GBlockID,Sig\rangle$,$GBlockID$、$ChainID$ 等表示同上,Sig 表示节点的签名;全局构建群组根据以下规则保证交易满足全局一致性:同一全局区块链高度下,同一数字化资产只能出现一次.

算法 3. 全局一致性验证算法.

```
输入:主体的验证群组,主体区块头数据
输出:主体的可信交易列表
Algorithm GlobalConsistentValidation(PBH)
  FOR each node of VPSet_i
    sorted(PBH) //按照时间先后对收到的 PBH 排序
    IF primary node //如果是主节点
      //主节点发起 PBH 交易一致性验证
      SendPBHValidationRequest(PBH)
    ENDIF
    IF PreparePBHValidationed //准备验证
      FOR each ⟨TxID,DA⟩ in PBH
        //该数字化资产是否双花
        PS<—checkParallSpending(TxID,DA)
        IF PS==false
          append(ConsistentTX,TxID)
        ENDIF
      ENDFOR
      sendConsistentTX()
      IF Consistent(TX) //可信交易
        SendToCPSet(TX)
      ENDIF
    ENDIF
  ENDFOR
END
```

当本轮验证过程结束时,存在未处理的主体区块头、正在验证的主体区块头.对于此类情况,当本轮时间结束时,当前验证节点 VP 终止所有主体区块头数据验证过程,并删除未处理的主体区块头数据.主体 P_i 将主体区块头数据广播给验证群组 $VPSet_i$,在一定的时间 $vali_time$ 之内,若主体 P_i 没有收到验证结果,主体 P_i 再次发送该主体区块头数据.以上机制,对于被中止验证的主体区块头数据,交易延迟最大为 $vali_time$.

5 全局区块链共识协议 MPBFT

全局构建群组通过全局区块链共识协议将每个主体的可信交易的 $TxID$ 存储到全局区块链上;每轮所有主体的验证群组的主节点从全网中选出一组节点作为下轮的全局构建群组,全局构建群组成员随时间动态变化.第一轮所有主体的验证群组的主节点从每个主体中选择一个节点作为初始构建群组;每个时间片段内,所有主体的验证群组的主节点随机从全网中选择 CK 个主体,然后从每个主体中选出一个节点作为下轮构建群组,其中 $CK\geq 2N/3$,且不允许某个区块链节点连续两轮作为构建节点;所有主体的验证群组的主节点将投票信息发送给当前构建群组,由当前构建群组统计出投票数 topCK 的节点,并将其作为下轮构建群组,同时每个验证节点将下轮构建群组信息采用组播的方式发送给所有主体的代表节点以及下轮构建群组成员,即每个构建节点将消息广播给全网 1/3 主体的代表节点与下轮构建节点.

在全局构建群组构建过程中,本轮所有主体的代表节点之间相互发送投票信息的通信代价为 $O(N^2)$;主体的代表节点将本节点统计出的下轮全局构建群组成员信息发送给本轮全局构建群组的通信代价为 $O(N\times CK)$;全局构建群组统计出下轮全局构建群组成员信息的通信代价为 $O(CK)$;全局构建群组将下轮全局构建群组成员信息发送给所有主体的代表节点、下轮全局构建群组的通信代价为 $O([(CK+N)/3]\times CK)$;下轮全局构建节点之间相互通信的代价为 $O(CK\times[(CK-1)/2])$;故主体 P_i 的下轮验证群组的构建代价为 $O\left(N^2+N\times CK+\frac{CK\times(CK+N)}{3}+\frac{CK\times(CK-1)}{2}\right)$,由于 $2N/3\leq CK\leq N$,故下轮全局构建群组的构建代价为 $O(N^2)$.

本文中所有主体的验证群组以及全局构建群组

的轮转由全局构建群组统一协调，全局验证群组收集到所有主体的下轮验证群组成员信息以及下轮构建群组成员信息，然后由当前的全局构建群组采用组播的方式将每个群组的下轮成员信息广播给所有主体的代表节点，然后由主体的代表节点广播给本主体内的所有节点，由此本轮、下轮群组的节点均可获取相关信息；当前全局构建群组发送一条群组轮转消息，表示在未来某个全局区块之后发起群组轮转.

在全局区块构建过程中，若所有节点通过 POW 机制竞争生成全局区块，易造成交易延迟过高、算力浪费、交易吞吐量低下等问题，故本文利用改进的 PBFT 机制(MPBFT)生成全局区块，降低交易延迟，提高交易吞吐量；在构建区块时需要根据交易更新 Merkle 树，现有区块链模型采用顺序构建 Merkle 树的方式会影响交易吞吐量的提升，故本文采用并行分支的方式构建 Merkle 树，通过独立更新每个分支的方式提升交易吞吐量. 如算法 4 所示，MPBFT 每轮选举多个主节点同时构建全局区块，按照时间顺序验证每个主节点构建的全局区块，构建群组将最先验证通过的全局区块广播至所有主体的代表节点，同时删除其他主节点构建的全局区块. MPBFT 通过每轮选举多个主节点同时构建区块来降低传统 PBFT 算法中恶意节点作为主节点带来的交易延迟增加的问题.

算法 4.　全局区块链构建算法.

```
输入：每个主体的可信交易列表
输出：全局区块
Algorithm CreateGlobalBlock()
  FOR each primary node of CPSet
    sendGB() //发送本节点构建的全局区块
  ENDFOR
  FOR each node of CPSet
    receive GB coming from each primary node
    checkGB() //检测 GB 是否正确
    //将 GB 的检测结果发送给其他构建节点
    sendCheckResult(GB)
    //大多数构建节点认为该 GB 有效
    if checked(GB)
      //向其他节点发送停止检查消息
      SendStopMessage(GBNum)
      deleteOtherGB()
    ENDIF
    //将全局区块广播至全网
    sendGBTONetwork(GB)
  ENDFOR
END
```

每个构建节点基于时间戳判断最先共识通过的全局区块，并将此全局区块广播给 w 个主体的代表节点，$N/3<w<2N/3$；由于每个节点接收到多次全局区块，故可保证节点接收到正确的全局区块.

6　安全分析与证明

定理 1.　主体 P_i 的每轮验证群组中至少存在一半以上的诚实节点，故主体 P_i 的验证群组是可信的.

证明.　主体 P_i 每轮的验证群组从全网 $K\geq 2N/3$ 个主体中每个主体选择一个节点作为主体 P_i 的验证节点；由拜占庭定理可知，全网中至少存在 $2N/3$ 以上的可信主体，且组成可信主体的节点均为诚实节点，由此可知 K 个主体中最多存在 $N/3$ 个不可信的主体，故主体每轮的验证群组中至少包含 $(K+1)/2$ 个诚实节点，所以主体的每轮验证群组时可信的.

定理 2.　全局构建群组中至少存在一半以上的诚实节点，故全局构建群组是可信的.

证明.　全局构建群组从全网 $CK\geq 2N/3$ 个主体中每个主体选择一个节点作为全局构建节点；由拜占庭定理可知，全网中至少存在 $2N/3$ 以上的可信主体，且组成可信主体的节点均为诚实节点，由此可知 CK 个主体中最多存在 $N/3$ 个不可信的主体，故全局构建群组中至少包含 $(CK+1)/2$ 个诚实节点，所以全局构建群组是可信的.

定理 3.　本文所构建的许可区块链网络是可信的.

证明.　许可区块链网络由每个主体的验证群组以及全局构建群组组成，由定理 1 和 2 可知，主体的验证群组与全局构建群组均是可信的，故许可区块链网络是可信的.

定理 4.　恶意主体 P_j 篡改的交易数据以及相关区块不会生效.

证明.　假设恶意主体 P_j 篡改本主体中交易数据以及相关区块，篡改的交易及区块必须从全局区块链中检索到才被认定为生效. 恶意主体 P_j 篡改的区块若想生效，需将篡改后的全局区块发送给所有节点；且恶意主体 P_j 需将篡改区块之后的所有全局区块篡改；同时恶意主体 P_j 需篡改所有主体的交易区块链，篡改的代价比较大；故恶意主体篡改的数据难以生效.

《计算机学报》

定理 5. 两层交易区块链不存在分叉问题.

证明. 主体 P_i 的区块链节点采用 PBFT 机制构建主体区块. 同一时刻,主体 P_i 仅生成一个主体区块,同时每个主体区块必须由构建者签名,其他节点通过签名校验与 Merkle 树校验等验证区块是否合法,故主体交易区块链不存在分叉问题. 构建群组采用 MPBFT 机制构建全局区块,每个全局区块必须由构建节点签名,其他节点通过签名校验与 Merkle 树校验等验证区块是否合法. 同一时刻,构建群组仅验证一个全局区块的有效性,故两层交易区块链不存在分叉问题.

分析 1. 本文所构建的许可区块链网络可以有效地防止 Sybil 攻击等.

由于本文所构建的区块链是许可链,故每个实体、主体必须通过批准才可加入网络;每个实体主体均拥有自己的公私钥,任何区块、交易与消息均需私钥签名;当主体接受到任何消息或交易、区块时,首先校验签名是否正确、对应的公钥地址是否在许可列表中,签名不正确的、不在许可列表中的实体与主体发送的消息将不会生效;基于以上机制,可以有效地防止 Sybil 攻击.

分析 2. 本文所提出的许可链多中心动态共识机制可以有效地预防重放攻击.

每条消息与交易均包含一个哈希摘要,每个节点根据摘要判断该消息或交易是否已经接收过;故节点不会重复接收消息,可以有效地防止重放攻击.

分析 3. 本文所构建的许可链网络是可靠稳定的.

由于本文所构建的许可区块链采用的是 PBFT 共识协议或改进的 PBFT 共识协议,根据 PBFT 协议,每个主体至少需要拥有 4 个节点即可正常维护主体的交易区块链;全局至少需要 4 个主体即可正常维护全局区块链.

当一个节点存在网络通信不畅问题时,则其他节点认为该节点为不诚实的节点,在任何一个验证群组或全局构建群组中,至少存在 2/3 以上网络通信良好的节点即可保证共识机制正常工作;在许可环境中网络状况相对良好,每个群组至少存在 2/3 以上网络通信良好的节点,故本文所构建的许可区块链网络是可靠稳定的.

分析 4. 每个主体的存储本主体的交易区块链与全局区块链是可行的.

全局区块链中仅包含可信交易的 ID 等可信信息,信息量相对较少,全局区块链的容量不会远大于主体交易区块链的容量;在许可环境中,每个主体均拥有较大的存储空间,故每个主体存储本主体的交易区块链与全局区块链是可行的.

分析 5. 由全局构建群组统一负责所有主体的验证群组以及构建群组的轮转是稳定、可靠的.

在本文所构建的许可链多中心动态共识机制中,所有群组的统一轮转消息与全局区块并不是由全局构建节点直接广播给全网所有节点,而是由全局构建节点广播给所有主体的代表节点,由主体的代表节点再将消息或者全局区块广播给本主体的节点;由于一个主体的所有节点基本上是物理聚集的,主体内的节点之间网络状况良好;故基于以上机制可以消除由直接广播给全网节点引发网络堵塞造成的消息超期或者延迟过长等问题;加之许可链网络中主体的代表节点之间通信相对良好,且一个全局构建节点将消息广播给所有主体的代表节点,可以保证消息的即时到达.

若主体发生宕机或者网络暂时中断的情况,即无法接受到任何全局构建群组发生的消息,在这段时间内,该主体无法进行任何交易;当主体再次恢复通信时,主体会接受到新的全局区块,全局区块中包含当前全局的时间片段序号,主体根据当前的全局时间片段序号判断本主体是否拥有当前的验证群组信息,向其他主体的请求当前本主体的验证群组信息以及当前全局构建群组信息等,由此继续本主体的交易,故由全局构建群组统一负责所有主体的验证群组以及构建群组的轮转是稳定、可靠的.

7 实验分析

本文参考以太坊、Fabric 开发实现本文所提出的许可链多中心动态共识机制,修改了以太坊的交易格式、状态树、共识算法、节点类型、交易入池规则等,同时参考 Fabric 实现多链架构.

许可环境中网络状况相对较好,节点之间通过异步消息机制进行通信,当一个节点存在网络通信不畅问题时,则其他节点认为该节点为不诚实的节点,在任何一个验证群组或全局构建群组中,至少存在 2/3 以上网络通信良好的节点,故可保证共识机制正常工作. 本文的实验环境为 20 台 128 GB 内存、32 核 CPU、10 T 存储空间的服务器,服务器之间使用千兆网络通信. 本实验通过 Docker 虚拟化技术部署许可链节点,每个 Docker 容器代表一个许可链节点;通过 Kubernetes 管理整个 Docker 集群;通过

flannel 技术实现容器之间的通信，即许可链节点之间的通信.

在本实验中，每个主体均拥有一个 *NodeDB* 节点(以太坊节点类型)，*NodeDB* 节点负责管理与维护本主体所有节点的链接信息以及每轮的主节点信息等. 通过 *NodeDB*，每个主体的节点可以相互链接. 如图 5、图 6 所示，通过 *NodeDB* 节点，主体中的每个节点与其他节点相互链接.

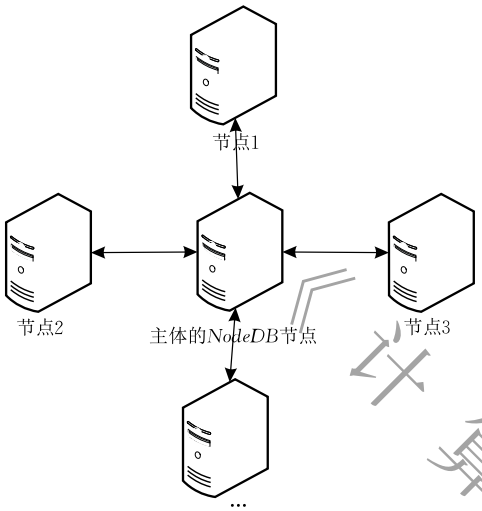

图 5　主体的 *NodeDB* 节点架构

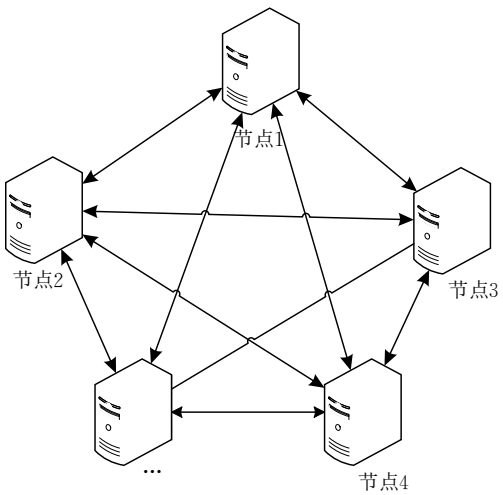

图 6　主体网络架构

如图 7 所示，每个主体的 *NodeDB* 节点之间相互链接，每个主体的 *NodeDB* 节点可以获取其他主体 *NodeDB* 上的节点信息，每一个节点可以和全网其他节点相互链接通信.

本文实验构建 20 个主体，每个主体大约有 10 个节点组成，全网有 300 个节点组成. 采用 POW 共识机制的区块链，当区块构建频率较高时，交易传播和区块大小成为影响区块链性能的主要因素. 本文采用广播区块头数据的方式，同时采用全局区块压缩传输的方法，减少传播量，并且在区块中添加额外信息，以便验证主体区块所包含的交易是否满足全局一致性. 本文将许可链多中心动态共识机制与 Fabric 在交易吞吐量 TPS、通信代价、交易延迟 TL 三个方面对比. 在相同的安全假设下，许可链多中心动态共识机制，可获得更高交易吞吐量、更低的交易延迟、动态可变的区块大小.

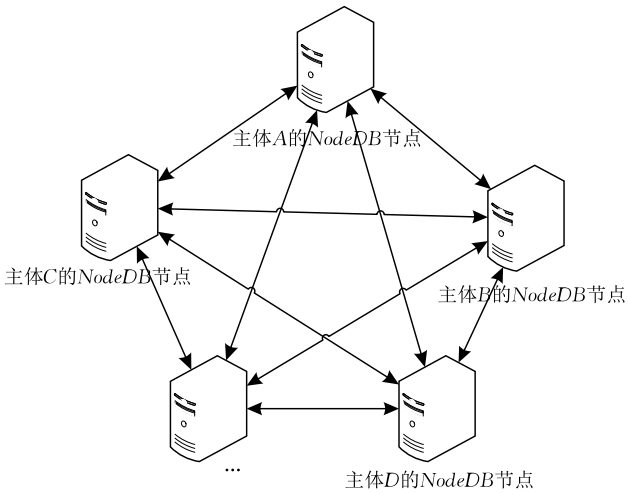

图 7　全网 *NodeDB* 架构

交易吞吐量

本文所构建的许可链多中心动态共识机制，每个主体仅将本主体的主体区块头数据发送给其他主体，其他主体根据主体区块头数据验证交易是否存在跨主体的双花问题；本主体不需等待验证结果返回，可继续构建本主体交易区块链；主体之间数据传输时采用压缩机制，扩展了全局区块包括的交易数量上限；由于构建节点将全局区块广播给每个主体的构建节点即可实现全局区块的全网传输，降低区块构建过程中的传输延迟，由此提高交易吞吐量. 图 8 表示，许可链多中心动态共识机制中，由于采用 MPBFT 共识协议，全局区块链每秒可以达到万笔交易.

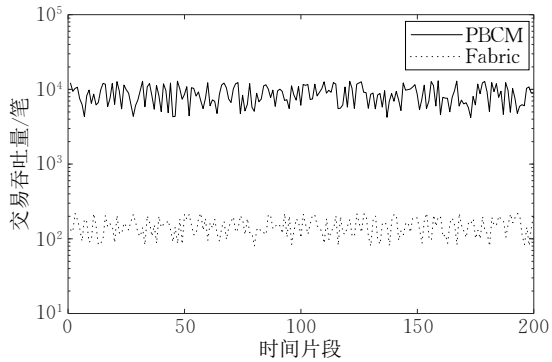

图 8　全局区块链交易吞吐量

《计算机学报》

如图 9、图 10 所示，在每秒 1 万笔交易的条件下，比较在全局区块每条交易中包含不同的可信交易的 $TxID$ 的情况下，GZIP、LZO、Snappy 等不同压缩算法的效率. 在 2 MB 的区块大小限制下，在全局区块每笔交易包含 10 笔可信交易的 $TxID$ 情况下，经压缩之后的全局区块大小的为 2 MB 左右；由于 GZIP 解压缩耗时较长（1 秒左右），LZO 与 Snappy 解压缩总共在 0.1 秒内完成，对系统整体影响比较小，时间可以忽略不计；故采用 LZO 或 Snappy 压缩机制. 由于每秒中全局构建群组的平均交易吞吐量为 10 000TPS，故每秒可信交易数量为十万（10000×10）.

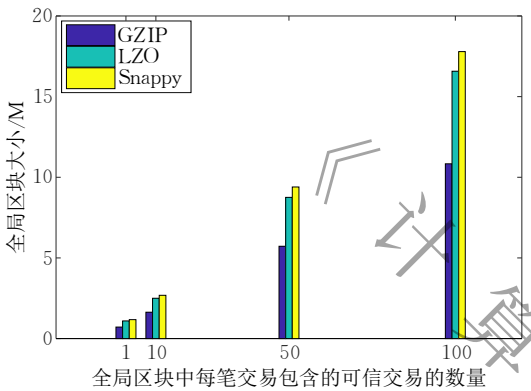

图 9 全局区块链压缩量对比

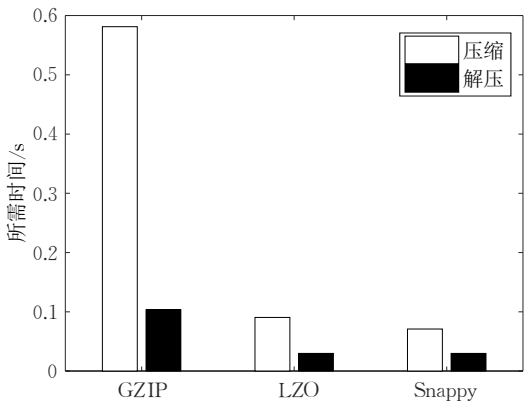

图 10 压缩算法解压、压缩效率

交易延迟

在许可链多中心动态共识机制中，普通节点只构建自己的交易和区块；验证节点仅将可信交易的 ID 写入到本主体交易区块链中，并不影响主体本身的交易和区块处理；同理构建节点生成全局区块，并不影响本主体的交易和区块处理. 所以，在主体内部不存在交易延迟，交易延迟仅仅与一致性验证过程相关.

在许可链中，主链的共识群组采用 MPBFT 协议进行全局区块的构建；MPBFT 协议可支持批量共识，即共识消息中包含多条需要共识的交易的 $TxID$，批量共识机制降低了共识延迟；由于构建节点将全局区块广播给每个主体的构建节点即可实现全局区块的全网传输，减少了数据传输延迟；在许可环境中，节点之间的消息传输可在毫秒级完成，最多经过 5 轮消息传输即可完成共识消息的确认的，再加上共识消息的解压缩过程（0.5 秒内）以及判断过程与区块构建过程，全局区块的构建过程可控制在 10 秒内完成. 图 11 表示，每个主体区块的平均验证时间在 8～12 秒左右，Fabric 的交易延迟在 20 秒左右.

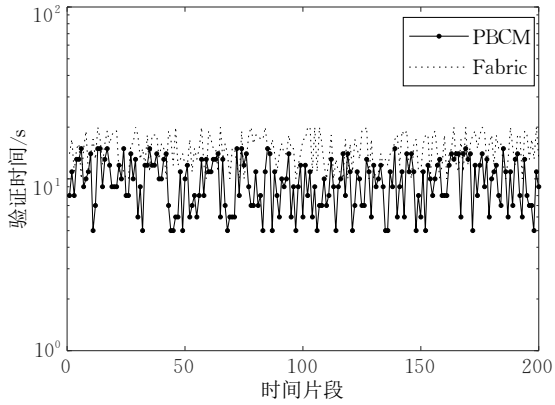

图 11 交易延迟

通信代价

本文所构建的许可区块链网络中，构建节点不需将全局区块广播至所有的节点，仅需广播给每个主体的代表节点即可，降低了网络的通信代价. Fabric 等区块链网络中，每个节点需要将区块广播给所有其他节点，且当一个节点已经接收到区块时，其他节点仍会继续向其广播区块，造成网络资源的浪费，且大的区块需要的传播时间更长. 图 12 所示，全局区块的大小仅仅为 1 M～1.5 M 左右.

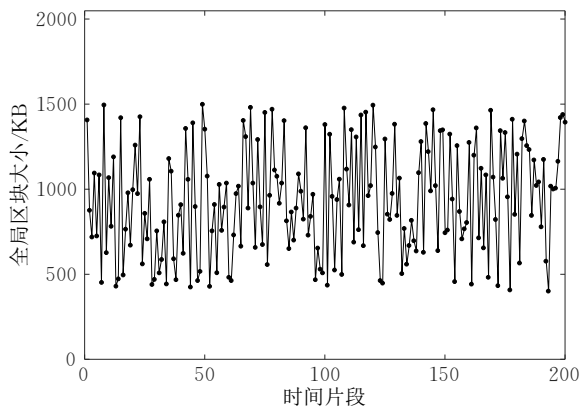

图 12 全局区块容量

投票通过率对性能的影响

在本文中，共识群组或验证群组在共识过程中，群组内一半以上的节点认为某个交易是可信交易，

则该交易即为可信交易.投票通过率是指确定某一交易为可信交易所需的有效投票数占总投票数的比例;在每个群组的拜占庭容错率为 1/2 的情况下,对比投票通过率为 51%、55%、60%、65%下交易延迟与交易吞吐量的变化.投票通过率越大表示需要的有效投票数越多,即需要越多的节点投有效票,由于恶意节点的存在会导致在时间阈值内难以收集到足够到的有效投票,从而导致交易延迟变长,同时交易吞吐量也会受到降低.如图 13 所示,随着投票通过率的提高,交易延迟逐渐增大,交易吞吐量逐渐下降,故投票通过率为 51%是合适的.

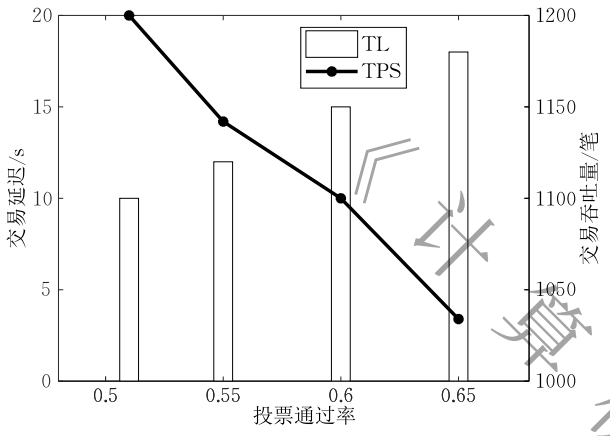

图 13　共识通过率对比

8　结论与展望

本文通过设计主体区块与全局区块,构建两层交易区块链;通过为每个主体生成动态验证群组,利用主从多链相互锚定,提出许可链多中心动态共识机制.通过证明,许可链多中心动态共识机制可构建高可信度的数字化资产交易环境.在保证高可信度交易的前提下,许可链多中心动态共识机制实现了更高的交易吞吐量、更低的交易延迟、动态可变的区块大小.本文的未来工作是:如何利用多区块链技术提高交易可信度;如何进一步降低网络通信代价;如何利用数据库索引技术,构建区块链 no-sql 快速检索机制.

参　考　文　献

[1] Yuan Yong, Wang Fei-Yue. Blockchain: The state of the art and future trends. Acta Automatica Sinica, 2016, 42(4): 481-494(in Chinese)
(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)

[2] Watanabe H, Fujimura S, Nakadaira A, Kishigami J. Blockchain contract: A complete consensus using blockchain//Proceedings of the 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE). Shanghai, China, 2015: 577-578

[3] Eyal I, Gencer A E, Sirer E G, Renesse R V. Bitcoin-NG: A scalable blockchain protocol//Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation, Santa Clara, USA, 2016: 45-59

[4] Luu L, Narayanan V, Baweja K, et al. SCP: A computationally-scalable Byzantine consensus protocol for blockchains. Cryptology ePrint Archive, Report 2015/1168

[5] Miller A, Litton J, Pachulski A, et al. Discovering Bitcoin's public topology and influential nodes//Proceedings of the ACM Symposium on Applied Computing. Coimbra, Portugal, 2013: 121-128

[6] Decker C, Wattenhofer R. A fast and scalable payment network with bitcoin duplex micropayment channels//Proceedings of the Symposium on Self-Stabilizing Systems. New York, USA, 2015, 9212, 3-18

[7] Lewenberg Y, Sompolinsky Y, Zohar A. Inclusive block chain protocols. Financial Cryptography and Data Security. Berlin, Germany: Springer, 2015: 528-547

[8] Sompolinsky Y, Zohar A. Secure high-rate transaction processing in bitcoin//Proceedings of the International Conference on Financial Cryptography and Data Security. Berlin, Germany, 2015: 507-527

[9] Tsai W T, Blower R, Zhu Y, et al. A system view of financial blockchains//Proceedings of the Service-Oriented System Engineering (SOSE), San Francisco, USA, 2016: 450-457

[10] Lamport L, Shostak R, Pease M. The Byzantine generals problem. ACM Transactions on Programming Languages and Systems, 1982, 4(3): 382-401

MIN Xin-Ping, born in 1993, Ph. D. candidate. His main research interests include blockchain and consensus mechanism.

LI Qing-Zhong, born in 1965, Ph. D., professor, Ph. D. supervisor. His main research interests include data computing, cloud computing software architecture, data science and data analysis.

KONG Lan-Ju, born in 1978, Ph. D., associate professor. Her main research interest is large-scale data management.

ZHANG Shi-Dong, born in 1969, Ph. D., professor. His main research interest is cloud computing software architecture.

《计算机学报》

ZHENG Yong-Qing, born in 1965, Ph. D., professor. His main research interests include data computing, cloud computing software architecture.

XIAO Zong-Shui, born in 1963, M. S., professor. His main research interests include blockchain and business process.

Background

A blockchain is a transaction database shared by all nodes participating in a network based on a consensus protocol. With this mechanism, existing solution leverage blockchain protocol to improve the credibility of digital assets. Existing blockchain protocols still have many scalability barrier, such as a higher communication cost, a higher latency, a lower throughput of transaction, a fixed block size and nonsupport of global consistency of digital assets on permissioned multi-centers. For example, the maximum rate at which these systems can process transactions is capped by the choice of two parameters: block size and block interval. There is a lot of work that to improve throughput, reduce latency and communication cost. Unfortunately, the throughput of transactions just up to 1000/TPS, and the latency still up to 20 s.

By allowing higher trusted node to verify transaction and opening to specific organizations or groups, Permissioned Blockchain can prevent privacy data and suggest better performance on latency and throughput. There is a lot of work to improve the performance of permissioned blockchain, most of those cannot improve the throughput, latency and credibility of transactions at the same time. And most of those sacrifice the privacy of transactions and throughput. And existing permissioned blockchains don't support permissioned multi-centers that each center is made up of multi nodes and each user can send any transactions at any centers on the same time.

By partitioning the network into subcommittees and constructing two-layer blockchain, this paper presents Permissioned Blockchain Dynamic Consensus Mechanism based multi-centers (PBCM) to improve the performance of permissioned blockchain and guarantee the global consistency of digital assets. By constructing master-salve blockchain, PBCM can divide transactions into multi peer blockchains to improve the throughput of transactions and reduce the consensus latency of transactions. By constructing dynamic validation group for each center, Global Transaction Validation Model (GTVM) can guarantee consistent of digital assets and improve the throughput of transaction. Based on multi-primary node, Multi Primary Node PBFT (MPBFT) can reduce the latency caused by malicious node as primary node. PBCM can achieve 100K/TPS, and the max latency is 10 s.

This work is partially supported by the grants from the National Nature Science Foundation of China (No. 61772316), the Science, Taishan Industrial Experts Programme of Shandong Province (No. tscy20160404) and the Technology Development Plan Project of Shandong Province (No. 2017CXGC0702).

《计算机学报》