

基于聚类簇中心的共识跨链交换模型

赵涛^{1,3} 张凌浩² 赵其刚³ 王红军³

(国家电网有限公司大数据中心 北京 100031)¹

(国网四川省电力公司电力科学研究院 成都 610000)²

(西南交通大学信息科学与计算学院 成都 610031)³

摘要 区块链的去中心化、匿名性、不可篡改等特性给金融及其他领域带来了深远影响,但目前区块链系统中仍存在共识计算效率低、单位时间容量受限及不同区块系统之间兼容互通的问题。针对这 3 方面的问题,文中提出了基于聚类簇中心的共识跨链交换模型。该模型在确保区块链系统的开放性、安全性、数据不可篡改性等特征的前提下,实现了用户所发出的交易获得区块链网络的快速确认,并有效地防止同一区块链网络中的单次同步区块数据过大的问题。该模型将区块链中的节点划分为共识服务节点、跨链交换节点和应用节点 3 类。将具有高效计算能力的共识服务节点通过高速网络连接在一起,形成服务于某一业务领域的区块链 P2P 网络,并专为该区块链网络中的应用节点提供共识计算服务;跨链交换节点同时连入不同区块链网络,交换节点之间基于 P2P 协议形成区块链交换网络,为不同区块链网络的应用节点提供跨链访问服务;应用节点可从所属区块链网络共识服务节点同步数据、访问跨链交换节点,以及发送链内或跨链交易。实验证明,通过该模型构建的区块链服务网络大幅度地提升了共识计算效率并增加了单位时间可容纳的交易量。

关键词 区块链,智能合约,共识计算效率,跨链交换,交易量

中图法分类号 TP301.6 **文献标识码** A

Accross Block Chain Consensus Transation Model Based on Cluster Center

ZHAO Tao^{1,3} ZHANG Ling-hao² ZHAO Qi-gang³ WANG Hong-jun³

(State Grid Big Data Center, Beijing 100031, China)¹

(State Grid Sichuan Electric Power Research Institute, Chengdu 610000, China)²

(School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China)³

Abstract The characteristics of blockchain, such as decentralization, anonymity and tampering, have made it exert profound influence on finance and other fields. However, at present, there are still many problems in the block chain system, such as low computing efficiency, limited capacity per unit time, and compatibility and interoperability between different block systems. In view of the above three problems, an efficient blockchain consensus and exchange system was proposed. Under the premise of ensuring the openness, security and tamper ability of the blockchain system and other blockchain features, the system realizes the rapid confirmation of the blockchain network for transactions issued by users, and effectively prevents the problem of excessive single-time synchronous block data in the same blockchain network. The system divide the nodes in the block chain into three types: consensus service nodes, cross-chain switching nodes and application nodes. The consensus service nodes with high computing power are connected together through high-speed network to form a blockchain P2P network serving a certain business field, and provide consensus computing services for application nodes in the blockchain network. Cross-chain switching nodes are connected to different blockchain networks at the same time, and a blockchain switching network is formed between switching nodes based on P2P protocol, providing cross-chain access services for application nodes of different blockchain networks. Application nodes could synchronize data from their respective blockchain network consensus service nodes, access cross-chain switching nodes, and send in-chain or cross-chain transactions. The experimental results show that the blockchain service network built by this system can greatly improve the consensus computing efficiency and increase the volume of transactions per unit time.

Keywords Blockchain, Smart contract, Common computing efficiency, Cross-chain exchange, Volume of transaction

1 引言

作为分布式数据存储、加密算法、共识机制、点对点传输技术的集成应用,区块链被认为是继大型机、个人电脑、互联网之后的计算模式上的颠覆式创新,必将在全球范围内驱动一场新的技术变革和应用变革。区块链技术起源于化名为中本聪的学者于2008年发表的奠基性论文“比特币:一种点对点电子现金系统”^[1]。目前,区块链技术被很多大型机构称为是彻底改变业务乃至机构运作方式的重大突破性技术。同时,类似于云计算、大数据、物联网等新一代信息技术,区块链技术并不是单一信息技术,而是依托于现有技术,加以独创性的组合及创新,从而实现曾经未实现的功能。

区块链解决的核心问题不是数字货币,而是如何在信息不对称、环境不确定的情况下,建立满足经济活动赖以发生、发展的信任生态体系。而这个问题被称为拜占庭将军问题^[2-4],也可称为拜占庭容错或者两军问题^[5],这是一个在分布式系统中进行信息交互时面临的难题,即在网络中的任意节点都无法信任与之通信的对方时,如何能创建出共识基础来进行安全的信息交互而无需担心数据被篡改^[6]。区块链使用算法证明机制来保证整个网络的安全^[7],借助它,系统中的所有节点能在去信任的环境下自动交换安全的数据,且能与其他领域相融合^[8]以进行分布式应用。区块链与人工智能技术相融合^[9],可以得到更加广泛的应用。在应用过程中,隐私保护^[10]也是一个关键问题。

共识算法是区块链的灵魂^[11],影响系统吞吐量、交易确认时间、应用场景及容错性等。随着区块链技术的风靡,应用于区块链的数字资产日益呈现多样化,而应用从最初的单纯货币、支付经济领域到生活的方方面面,但现有的区块链技术还难以被扩展以支撑多领域的应用,故提升区块链的表达和处理的能力^[12],需要对实现高可信、高速度的价值传递的实现开展深入的研究。

区块链技术发展至今,由于整个网络是基于P2P协议实现数据的同步,并主要采用工作量证明机制实现共识记账;由于节点之间数据传输的时延因素,工作量证明的难度值往往不能设得太低;同时为保证区块的及时同步,区块又不能设的太大,这些因素就限制了区块链单位时间所能容纳的交易数量。如当前以太坊的平均每秒的交易量为20个每秒,每次交易的时延为10~20秒,而比特币网络的平均交易量为5个每秒,每次交易时延10~20分钟。随着技术的发展,跨链的需求越来越广泛^[13],区块链当前的这种低效交易无法适用于具有大规模交易量和低时延需求的诸多应用场景^[14]。

随着区块链技术的发展以及各区块链社区的建立,跨链信息的传递成为了一个非常重要的研究方向。在同一区块链社区内,信息交易的速度不是很高,在跨链信息交易的与传递上,提高跨链交易的速度尤为重要,这也吸引了很多研究者对其进行研究。

鉴于此,本文提出了基于聚类簇中心^[15-16]的共识跨链交换模型,使同一区块链内的数据相关性增强、数据交换量大幅减少;通过对区块链网络计算能力影响较大的共识服务节点之间构建高速互联网络,并根据网络交易需求及时提升共识计算服务节点的计算能力。通过本系统的构建,可在确保

区块链系统的开放性、安全性、数据不可篡改性等特征的前提下,实现用户所发出的交易获得区块链网络的快速确认,并有效地防止同一区块链网络中的单次同步区块数据过大的问题,大幅提升了接入区块链网络应用节点的交易效率。

2 相关研究

区块链系统本质上是一个分布式账本系统。而分布式系统面临的首要问题是如何解决一致性的问题;即如何在多个相对独立的节点之间达成共识的问题;同时保护数据隐私^[10]和安全问题^[15]。共识算法就是用来协调各个节点的一致性,区块链中各节点根据该算法来进行验证,当得到绝大部分节点确认后,数据才被认为是有效的,然后被写入区块链中,成为不可篡改的数据。针对区块链交易吞吐量高、交易延迟低、交易容量大等特性,现有的共识机制大多未同时解决可信性与性能扩展的限制。现有解决方案通常以降低可信度来换取更高的交易吞吐量。

随着区块链技术的发展,跨链交易成为众多研究者的关注重点。跨链通信是当前区块链系统的主要设计之一。目前,区块链像信息孤岛一样运作,无法获取外部数据或自行执行交易,因此跨链通信非常重要。区块链路由器^[17]使区块链能够连接和跨链通信。通过建立一个经济模型,区块链路由器使得网络中的不同区块链能够像互联网一样相互通信。在区块链路由器的网络中,一些区块链起着路由器的作用,根据通信协议,对通信请求进行分析和传输,动态维护区块链网络的拓扑结构。原子化跨链交易^[18]允许在两个不同区块链上的资产持有人直接进行实时交易,并且具有原子性和一致性。跨链共识机制是区块链的灵魂扩展,解决了如何在两个开放的网络中达成共识的问题。Li等^[19]提出了一种基于区块链和边缘计算技术的去中心化框架。该框架由客户层、企业层、应用层、智能层、数据层和基础设施层组成,并通过实例说明了该框架的有效性。他们讨论了制造生态系统正从集成化、集中化系统向共享化、分布式系统转变。该框架融合了区块链和边缘计算的最新发展,能够满足制造生态系统中知识和服务共享的安全和分布式需求。该框架还为共享知识和服务提供了一种更加安全和可控的方式,从而支持公司以更低的成本开发可扩展和灵活的业务,并最终提高了制造服务的整体质量、效率和有效性。

使用区块链技术将不同部门、不同组织联系在一起,Fridgen等^[20]将区块链技术和业务流程管理相结合,设计、实施和评估用于跨组织工作流管理的区块链原型。防止篡改的过程可以提高可审计性、自动化过程和系统的分散性,这是区块链解决方案用于跨组织工作流管理的主要优势。

Li等^[21]提出了一种新的区块链架构,其专为满足工业标准而设计,利用了卫星链的概念。卫星链可以私下并行运行不同的共识协议,因此大大提高了系统的可扩展性,并且设计了跨链交易算法及基于超级账本的框架实现了该算法。

针对跨链交易吞吐量高、交易延迟低、隐私保护、交易容量大等特性,现有的共识机制都难以同时解决。解决方案通常以降低可信性来换取更高的交易吞吐量。国内外学术界都积极开展对于区块链技术的研究,现有机制存在计算资源

浪费的问题,且性能过于低下,无法支持应用需求。

本文构建了一种高效的跨链共识与交换系统,该系统实现用户所发出的交易获得区块链网络的快速确认,并有效防止同一区块链网络中的单次同步区块数据过大的问题。

3 基于聚类簇中心的共识跨链交换模型

随着区块链承载的数字资产日益呈现多样化,交易内容逐渐呈现富类型,这对区块链的共识性能提出了新的挑战。区块链系统存在共识计算效率低、单位时间交易容量受限以及不同区块链系统之间兼容与互通等问题。尽管很多学者在区块链共识机制问题上提出了许多模型,但却无法同时解决不同区块链系统之间的兼容互通问题。

针对目前已有的区块链系统存在的问题。本文提出了基于聚类簇中心的共识跨链交换模型,主要是基于密度峰值^[16]

的共识结点竞争模型,共识结点达成之后,设计了相应的链内交易、访问及跨链访问算法。

3.1 基于密度峰值的共识结点竞争模型

该系统将区块链系统中的节点划分为共识服务节点、跨链交换节点和应用节点 3 类不同节点。将具有高效计算能力的共识服务节点通过高速网络连接在一起,形成服务于某一业务领域的区块链 P2P 网络,专为该区块链网络中的应用节点提供共识计算服务;将跨链交换节点同时连入不同区块链网络,并同步不同区块链的区块数据,在该节点上形成不同区块链网络的状态数据库,交换节点之间基于 P2P 协议形成区块链交换网络,为不同区块链网络的应用节点提供跨链访问服务;应用节点可从所属区块链网络共识服务节点同步数据、访问跨链交换节点,以及发送链内或跨链交易,如图 1 所示。

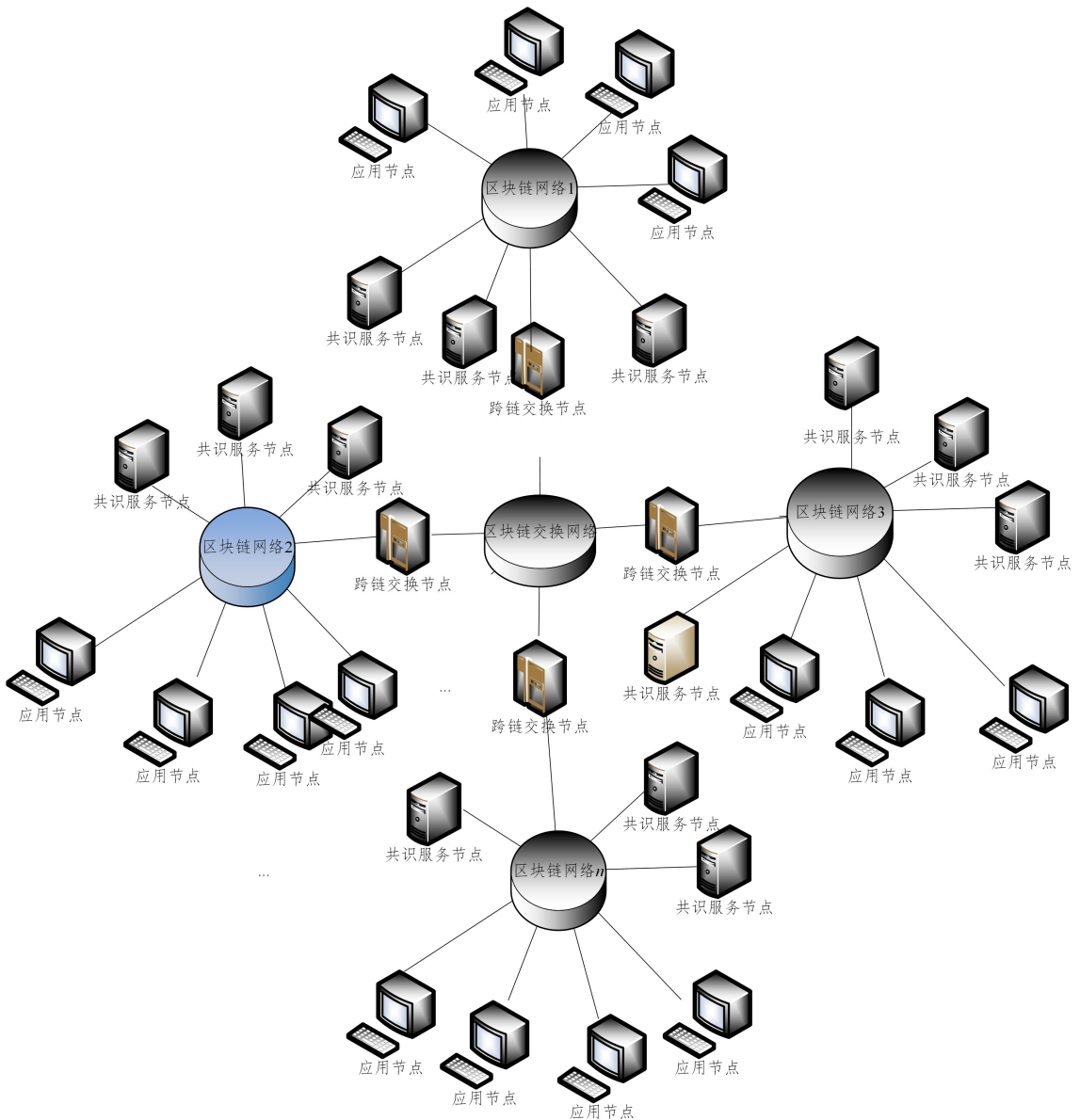


图 1 基于聚类簇中心的跨链交换模型

在图 1 中,区块链网络按所服务或应用的领域、业务不同,划分为不同的专门区块链网络;不同区块链网络,根据服务容量、交易效率的需求不同,接纳具有相应计算能力并能高速连入该区块链主网络的计算节点作为共识服务节点,由共

识服务节点之间通过计算能力竞争向该区块链网络应用节点提供共识计算服务。如图 1 所示,跨链交换节点分别接入不同的区块链网络,并同步不同区块链区块数据,并在该节点上形成不同区块链网络的状态数据库。图 1 的部署围绕着共识

服务节点和跨链交换节点进行,这实际上是一个优化问题。

给定样本应用节点 $D = \{x_1, x_2, \dots, x_m\}$, k 为共识服务节点数,共识服务节点集合为 $C = \{C_1, C_2, \dots, C_k\}$, 共识跨链交换:

$$E = \sum_{i=1}^k \sum_{x \in C_i} \|x - \mu_i\|_2^2 \quad (1)$$

其中, $\mu_i = \frac{1}{|C_i|} \sum_{x \in C_i} x$ 是簇 c_i 的均值向量。直观来看,式(1)在一定程度上刻画了跨链交换的网络传输代价, E 值越小则代价越小,在应用节点固定的情况下,合理的共识与跨链交换节点的设置可以使网络传输代价最小,达到最优的情况,这样交易和共识的效率将达到最高。

对于共识节点和交换节点的选择,可以采用贪婪算法找到最优的共识服务和交换节点,但算法复杂度太高,因此采用密度峰值的算法^[16]来进行选择,该算法主要是根据应用节点的密集程度而选择共识服务和交换节点。区块链结点的密度计算如式(2)所示:

$$\rho_i = \sum_j x(d_{ij} - d_c) \quad (2)$$

其中, ρ_i 表示每个结点的密度, d_{ij} 是结点 i 到结点 j 之间的距离, d_c 是一个截断距离。根据区块链网络结点规模进行参数的设置。然后计算当前结点到其他候选交换结点的距离,计算如式(3)所示:

$$\delta_i = \min_{j: \rho_j > \rho_j} (d_{ij}) \quad (3)$$

其中, δ_i 表示当前结点到比当前结点密度高的结点的最小距离。通过这两个公式可以计算出图 1 中的最优交换结点,而计算出的结点会使其他结点与交换结点交换数据的代价和是最小的,能够使式(1)达到最小值。

3.2 基于区块链共识与交换系统的实施过程

3.2.1 应用节点的交易过程

在区块链中,一笔新的交易产生时,首先被广播到网络中的其他参与节点;然后,每个节点会将很多笔未验证的交易放入区块中,每个区块包含数百或上千笔交易;接着,每个节点进行工作量证明来决定谁来验证交易,而谁最快算出结果,就由谁来验证,最快的节点会把自己的区块广播给其他节点,其他节点确认这个交易是否有效,无误后,接受该区块;最后,所有节点完成接受后,各节点会重新开始建立下一个区块。

在区块链的共识与交换系统中,应用节点在链内的交易过程与上诉过程大同小异,具体交易过程如图 2 所示。



图 2 应用节点链内交易流程图

节点在链内的交易如算法 1 所示。

算法 1 链内交易算法

输入:交易记录 T_i

输出:交易结果

1. 应用节点向区块链网络发送交易 T_i ;
2. 区块链网络中共识服务节点将该交易纳入交易池 $T_i \rightarrow T_{pool}$ 中;
3. 共识节点之间基于激励机制获取区块记账权;
4. 竞争获胜的共识服务节点使用从其交易池中的交易生成新区块;
5. 生成区块的共识服务节点向网络广播新区块;

6. 其余共识服务节点验证新区块,若正确则进行第 7 步,若不正确则进行第 3 步;

7. 应用节点从共识服务节点同步新区块,纳入本地区块链并更新其状态库。

3.2.2 应用节点的跨链过程

在区块链所面临的众多问题中,区块链之间的兼容互通问题在很大程度上限制了区块链的应用空间。而跨链技术就是实现互联网价值的关键所在。跨链是各区块链的桥梁,以实现链与链之间的价值转换和信息交互等。信息交互就是信息传递,是在不改变原始链的结构前提下,实现将信息从一条链传递到另一条链的过程。

文中构建的区块链共识与交换系统需要应用节点的跨链过程,来实现信息的传递,进而提高共识计算效率和增加单位时间可容纳交易量。而在该系统中,应用节点的跨链交易发送过程如图 3 所示。

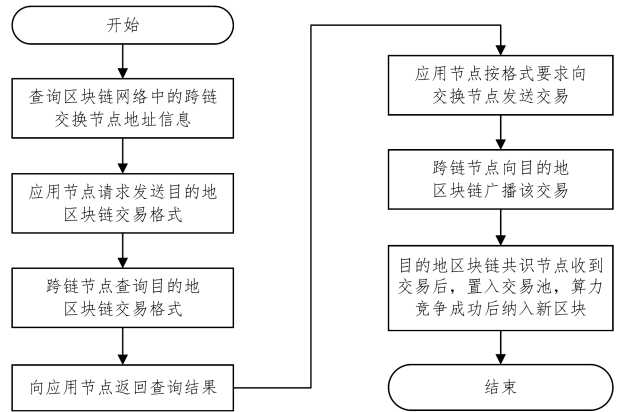


图 3 应用节点跨链交易发送流程图

应用节点的跨链交易过程中,跨链访问过程如算法 2 所示。

算法 2 跨链访问交易算法

输入:跨链交换节点的地址队列 $Aline$

输出:交易状态标志,交易地址

1. 应用节点从所获区块链网络中获得 1 个或多个跨链交换节点的地址;
2. 应用节点向该跨链节点发送待发送交易区块链数据的格式请求;
3. 跨链节点根据该请求查询交易发送目的地区块链交易格式;
4. 跨链节点将该查询结果返回应用节点;
5. 应用节点按该格式要求将跨链交易封装并发送跨链交换节点;
6. 跨链交换节点收到跨链交易后,在目的地区块链内广播该交易;
7. 目的地区块链共识服务节点收到交易后,置入交易池,并在算力竞争成功后将该交易纳入目的地区块链网络的新区块。

3.2.3 共识与交换系统的特征

在区块链共识与交换系统中,共识服务节点、应用节点中均设置有一个跨链交换节点状态数据库,跨链交换节点将定时向各区块链网络广播节点地址信息,该节点地址信息将被各区块链共识服务节点、应用节点接收并更新跨链交换节点库,超出一定时间未能收到广播信息的跨链节点信息将被共识服务节点、应用服务节点从跨链交换节点库中删除。

在该系统中,共识服务节点、应用节点与跨链交换节点,均为开放式接入,任何符合相应计算条件、网络条件的节点均可以在获得相应区块链软件(共识服务节点软件、应用节点软件或跨链交换节点软件)后自由加入或退出。

4 基于区块链共识与交换系统的实现

文中以目前广泛使用的以太坊 go 语言客户端为例,详细描述该系统的实现。

4.1 实验步骤及模拟实验实现

目前的以太坊 go 语言客户端既包括有用于区块数据同步、状态数据库生成、状态数据库查询、交易发送的以太坊客户端功能,又包括有用于交易数据归结、基于 POW 进行挖矿竞争、新区块生成与验证的服务端功能。由于网络中每个节点的功能均是相同的,任何节点既可仅作为客户端,又可作为提供共识计算的服务端,为了保证网络中的数据能保持同步和算力竞争尽可能公平,挖矿难度一般自动调节在每 15 秒生成一个区块。具体的实验参数如表 1 所列。由于上述机制,由该客户端所构建的以太坊网络,交易数大概在 20 个每秒左右,每个交易被确认的时延平均在 90 秒以上,一个交易要被正式确认,一般要在第六区块之后才能被确认已进入主链。基于上述对以太坊 go 语言客户端的介绍,并按照本文所描述的系统和方法,对以太坊 go 客户端进行了改造,具体如图 4 所示。将 go 客户端中的挖矿功能与应用访问功能分离,分别形成挖矿节点软件,即共识服务节点软件和应用节点软件;修改挖矿节点的挖矿难度调节函数,使每个区块的生成时间缩短至 100 毫秒到 1 秒之间;将挖矿节点软件部署在网络时延较小且处于高速互联的云节点上,节点之间的时延控制在 50 毫秒以内,挖矿节点的算力根据网络业务量动态提升;应用节点则无时延与算力限制,由应用用户根据自身应用情况决定应用节点的算力及网络接入带宽。

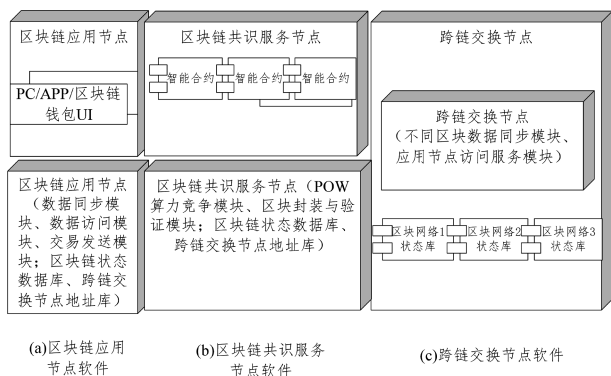


图 4 基于 Go 语言客户端的系统软件实现图

表 1 实验环境参数表

编程语言	版本	环境	模拟节点
go	1.9.2	Ubuntu	2 200
python	3.6	Pycharm	2 200

另外,基于应用节点软件改造形成了支持多区块链网络数据同步的跨链交换节点软件。该节点软件可同时运行多个区块数据的区块链同步进程,分别同步相应区块数据,并更新本地区块链的状态数据库。按前述方法设计应用节点与跨链交换节点之间的跨链数据访问和交易发送协议及软件功能。

4.2 实验结果分析

基于上述方法即可将当前低效的以太坊系统改造为一个可适用于大交易量的高效区块链系统。模拟系统设置交易节点的数量从 2 逐渐变化到 2 048,所花费的时间如图 5 所示,红色的曲线是本文所提模型。蓝色曲线是未改造的以太坊模

型。在交易结点参与比较少的情况下,两个模型所花费的时间差不多,以太坊模型还稍微的具有一点优势,但是随着交易结点数量增加,本文模型的优势逐渐爆发出来,且所花费的时间差距很大。由图 5 可以看出,在交易结点大于 150 时,本文模型在交易效率上有极大的优势,因此本文模型适合大规模的区块链部署的应用场景。

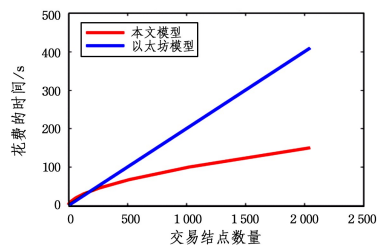


图 5 交易结点及其对应的时耗图

5 总结与展望

5.1 总结

在区块链性能解决方案的探究过程中,如何提高交易吞吐量,减少交易延迟仍然是区块链性能的热点问题。虽然在区块链性能方面,诸多学者对区块链架构以及区块链共识机制已经有了一些研究成果,然而针对不同区块链系统之间兼容与互通问题对区块链性能影响的探索少之又少。本文通过构建区块链共识与交换系统,实现用户所发出的交易能获得区块链网络的快速确认,并有效防止同一区块链网络中的单次同步区块数据过大的问题,大幅提升了接入区块链网络应用节点的交易效率。

第 4 节中,通过本文的构建实现基于聚类簇中心的共识跨链交换模型,根据区块链所服务领域或业务的不同,可构建不同的区块链服务网络,区块链服务网络之间通过跨链交换节点以实现不同链之间的数据交换,使同一区块链内数据相关性增强、数据交换量大幅减少;通过对区块链网络计算能力影响较大的共识服务节点之间构建高速互连网络,并根据网络交易需求及时提升了共识计算服务节点的计算能力,从而大幅提升共识计算效率和增加单位时间可容纳交易量。

5.2 研究展望

对于区块链的性能研究,构建了一种高效的区块链共识交换系统,减少同一区块链内数据交换量,为对区块链网络计算能力影响较大的共识服务节点之间构建高速互连网络,从而大幅提升共识计算效率和增加单位时间可容纳交易量。区块链的共识性能是目前的研究热点,是具有价值与挑战的研究领域,还存在诸多问题需进一步探索。未来研究需解决的问题:(1)应用场景需要进一步明确,区块链分为公有链和许可链,不同场景具有各自的特色和优势,必须在明确应用场景的前提下,才能进一步改进区块链共识计算效率。(2)隐私保护需求,区块链是去中心化系统,在共识协商等过程中,数据需要在不同节点上进行验证,这将导致数据泄露。因此,区块链需要保护用户隐私,同时满足监管需求。

参考文献

- [1] NAKAMOTO. Bitcoin: A Peer-to-Peer Electronic Cash System [EB]. <https://www.bitcoin.org/bitcoin.pdf>.

- [7] KIM C G, KIM J G, LEE D H. Optimizing image processing on multi-core CPUs with Intel parallel programming technologies [J]. *Multimedia Tools & Applications*, 2014, 68(2): 237-251.
- [8] CHAPMAN B M. Shared Memory Parallel Programming with Open MP [M]. *International Workshop on OpenMP Applications and Tools*, Springer Berlin Heidelberg, 2005.
- [9] CHAPMAN B, JOST G, VAN D P R. Using OpenMP: Portable Shared Memory Parallel Programming [J]. *Journal of Computer Science & Technology*, 2010, 10(3).
- [10] YAMAZAKI I, KURZAK J, WU P, et al. Symmetric Indefinite Linear Solver using OpenMP Task on Multicore Architecture [J]. *IEEE Transactions on Parallel and Distributed Systems*, 2018; 1-1.
- [11] WU G, CHEN Q, CAO F, et al. Parallel hybrid genetic algorithm for sat problems based on OpenMP [C] // *International Conference on Intelligent Systems & Knowledge Engineering*. IEEE, 2018.
- [12] ZHANG Q, ZHAO Q. Application of Parallel Computing with OpenMP in Global Ionosphere Mapping [J]. *Geomatics & Information Science of Wuhan University*, 2018, 43(2): 227-233, 240.
- [13] 柳建, 孙胜军, 毛国平, 等. 蒙特卡洛模拟的并行实现及并行效率研究 [J]. *计算机应用与软件*, 2018, 35(1): 301-303, 339.
- [14] 崔树林, 张旭, 张树清, 等. 基于 GPU 的大规模栅格数据分块并行处理方法 [J]. *计算机技术与发展*, 2015(3): 19-22.
- [15] LIU Y, YU F. Automatic inspection system of surface defect son optical IR-CUT filter based on machine vision [J]. *Optics & Lasers in Engineering*, 2014, 55(7): 243-257.
- [16] 房玮睿, 王春露. 基于缓冲池和多线程的智能交通短信平台设计与实现 [C] // *中国通信学会学术年会*. 2009; 7-11.
- [17] 刘振安, 章守信, 刘胜璞. 并行图像处理算法的设计与实现 [J]. *测控技术*, 2003, 22(5): 5-6.
- [18] 耿晓中. 基于多核分布式环境下的任务调度关键技术研究 [D]. 长春: 吉林大学, 2013.
- [19] 胡海兵, 薛源, 徐挺, 等. ITO 导电薄膜表面缺陷的图像特征分析 [J]. *计算机应用*, 2017, 37(S1): 198-200.

(上接第 561 页)

- [2] STOLZ D, WATTENHOFER R. Byzantine agreement with median validity [C] // *19th International Conference on Principles of Distributed Systems*, 2015.
- [3] CASTRO M, LISKOV B. Practical Byzantine fault tolerance and proactive recovery [J]. *ACM Transactions on Computer Systems*, 2002, 20(4): 398-461.
- [4] CASTRO M, LISKOV B. Practical byzantine fault tolerance [C] // *The Third Symposium on Operating Systems Design and Implementation*. Berkeley: USA, 1999; 173-186.
- [5] 范捷, 易乐天, 舒继武. 拜占庭系统技术研究综述 [J]. *软件学报*, 2013, 24(6): 1346-1360.
- [6] 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.
- [7] 王继业, 高灵超, 董爱强, 等. 基于区块链的数据安全共享网络体系研究 [J]. *计算机研究与发展*, 2017, 54(4): 742-749.
- [8] 张俊, 高文忠, 张应晨, 等. 运行于区块链上的智能分布式电力能源系统: 需求、概念、方法以及展望 [J]. *自动化学报*, 2017, 43(9): 1544-1554.
- [9] 袁勇, 周涛, 周傲英, 等. 区块链技术: 从数据智能到知识自动化 [J]. *自动化学报*, 2017, 43(9): 1485-1490.
- [10] 祝烈煌, 高峰, 沈蒙, 等. 区块链隐私保护研究综述 [J]. *计算机研究与发展*, 2017, 54(10): 2170-2186.
- [11] CONG L W, HE Z. Blockchain Disruption and Smart Contracts [C] // *Nber Working Paper Series*. Social Science Electronic Publishing, 2018; 1-41.
- [12] YUAN Y, WANG F Y. Development status and prospect of block chain technology [J]. *Journal of Automation*, 2016, 42(4): 481-494.
- [13] BEHL J. Scalable BFT for Multi-Cores: Actor-Based Decomposition and Consensus-Oriented Parallelization [C] // *10th Workshop on Hot Topics in System Dependability*. Broomfield, Co, 2014; 1-6.
- [14] 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.
- [15] FREY B J, DUECK D. Clustering by passing messages between data points [J]. *Science*, 2007, 315(5814): 972-976.
- [16] RODRIGUEZ A, LAIO A. Machine learning. Clustering by fast search and find of density peaks [J]. *Science*, 2014, 344(6191): 1492-1496.
- [17] WANG H, CEN Y, LI X. Blockchain router: A cross-chain communication protocol [C] // *The 6th International Conference on Informatics, Environment, Energy and Applications*. ACM, 2017; 94-97.
- [18] HERLIHY M. Atomic cross-chain swaps [C] // *Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing*. ACM, 2018; 245-254.
- [19] LI Z, WANG W M, LIU G, et al. Toward open manufacturing: A cross-enterprises knowledge and services exchange framework based on blockchain and edge computing [J]. *Industrial Management & Data Systems*, 2018, 118(1): 303-320.
- [20] FRIDGEN G, RADSZUWILL S, URBACH N, et al. Cross-Organizational Workflow Management Using Blockchain Technology-Towards Applicability, Auditability, and Automation [C] // *51st Annual Hawaii International Conference on System Sciences*. 2018. 3507-3516.
- [21] LI W, SFORZIN A, FEDOROV S, et al. Towards scalable and private industrial blockchains [C] // *Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts*. ACM, 2017; 9-14.