基于区块链的云计算资源去中心化交易共识机制研究

梁贺君[1] 韩景倜[2]

(上海海洋大学工程学院 上海 201306)[1] (上海财经大学金融科技研究院 上海 200433)[2]

摘 要 区块链的去中心化、去信任、数据可追溯等技术特性,为云计算发展带来了新的机遇与挑战。传统的中心化数据中心,用户通过网络带宽资源从数据中心获取计算、存储、数据库等资源,这种模型下存在中心化机构运行成本高、效率低以及数据存储不安全等问题。为此,文中提出了去中心化的云计算交易机制与方法,构建了基于区块链的云计算资源交易市场,重点研究了共识机制在云计算去中心化交易市场中的应用。通过分析比较目前主流的区块链共识算法(PoS,PoW,DPoS,PBFT),提出基于实用拜占庭容错算法(PBFT)改进的算法,对以太坊应用于联盟链时会产生的资源浪费与信任缺失等缺点进行优化,从而达到减少开销的目的,并将改进算法应用到云计算资源去中心化交易市场中。文中提出了在云计算资源交易中引入区块链技术,采用去中心化和去信任的方式集体维护一个可靠分布式数据库,设计了基于以太坊的共识机制,能够构建全球联网计算机算力交易平台,真正实现云计算资源的弹性可扩展与按需分配。

关键词 区块链,共识机制,实用拜占庭容错算法,云计算交易,以太坊

中图法分类号 TP301 **文献标识码** A

Research on Decentralized Transaction Consensus Mechanism of Cloud Computing Resources Based on Block Chain

LIANG He-jun[1] HAN Jing-ti[2]

(College of Engineering Science and Technology, Shanghai Ocean University, Shanghai 201306, China)[1]

(Institute of Financial and Technology, Shanghai University of Finance and Economics, Shanghai 200433, China)[2]

Abstract The technical characteristics of de-centered, de-trust, data complete and traceable of block chain provide brand-new opportunity and challenge for cloud computing. Users get computing, storage, database and other resources from the traditional centralized data center through network. There are many problems under this model, such as high operating cost, low efficiency, unsafe data storage and so on. In this paper, a de-centered cloud computing trading mechanism and method was proposed to build a cloud computing resource trading market based on block chain technology, focusing on the application of consensus mechanism in the central cloud computing trading market. Through the analysis and comparison of the popular block chain consensus algorithms (Pos, PoW, DPoS, PBFT), this paper proposed the improved practical byzantine fault-tolerant algorithm (PBFT), which is employed to optimize the disadvantages of resource waste and trust loss when the etheric square is applied to the alliance chain, so as to reduce the cost, and apply the improved algorithm to the central trading market of cloud computing resources. This paper proposed to introducte block chain technology in cloud computing resource trading, and collectively maintain a reliable distributed database by means of de-centered and de-trust. The design of a consensus mechanism based on Ethernet can build a global Internet computing power trading platform, thus realizing the elastic scalability and on-demand allocation of cloud computing resources.

Keywords Block chain, Consensus mechanism, Practical Byzantine fault-tolerant algorithm, Cloud computing transactions, Etheric fang

1 引言

2008 年,中本聪发表了名为“Bit coin: A Peer-to-Peer Electronic Cash System(比特币:一种点对点的电子现金系统)”的论文[1],区块链的概念第一次进入世人的目光,其实现了真正意义上的去中心化可信任交易系统,获得了急速增长的关注度。区块链解决了如何在不被信任的信道传递可信的信息以及价值转移的问题。区块链备受瞩目,其伟大之处在于通过共识机制、智能合约以及基于去中心化的思想完美解决了节点间的信任度问题。区块链融合了多种技术,具有分布式数据库、密码学、P2P 网络传输协议等,具有几个比较显著的特性:去中心化、可追溯、不可篡改。目前区块链分为私有链、公有链和联盟链。

与区块链技术类似,云计算也是将并行计算、分布式计

本文受国家社科基金重大项目基金(18ZDA088)资助。

梁贺君(1982—),男,博士后,讲师,CCF 会员,主要研究方向为区块链技术、云计算与大数据、智慧物流;**韩景倜**(1959—),男,教授,博士生导师,主要研究方向为区块链、大数据等,E-mail:liang.hejun@shufe.edu.cn(通信作者)。

算、虚拟化、网络存储、负载均衡等传统计算机与网络技术进行了融合，具有比较显著的特性：按需分配、弹性可扩展、低成本、高可靠性等。云计算也分为私有云、公有云、混合云。与区块链技术最大的不同点是云计算服务市场具有中心化。云计算服务包括以计算、存储、网络及数据库为主的基础云服务，以用户、数据和能力为主的综合云服务，它是多服务种类、多主体、多价格的复杂性市场。为保证云计算中心的各类资源能够安全与高效运行，可以在云计算交易中引入基于区块链的去中心化思想，设计安全、高效、透明、信息对称的交易模式和交易方法。区块链技术优先应用到云计算市场中，将有助于实现云计算资源的有效配置，更好地激发云计算市场活力。实现云计算数据中心去中心化的布局，提升云计算资源的集约化水平和使用效率。

区块链技术在电子商务、电力市场领域去中心化的应用已有研究[2-4]，但将区块链引入云计算领域的研究尚少。因此本文对几种目前较为热门的共识算法进行了阐述与比较，并提出使用区块链技术对联盟链场景内以太坊应用产生的资源浪费以及节点间不信任问题进行改进，设计基于云计算资源去中心化交易环境下的 PBFT 改进算法。

2　共识机制概述

2.1　共识机制的概述

2.1.1　共识机制的定义

共识本指一个社会不同阶层、不同利益的人所寻求的共同认识、价值、理想。现已经成为计算机科学的主要组成部分，在过去的 30 多年里，电子世界中的共识机制已经从一个抽象的概念发展成了分布式账本的关键技术。分布式账本中，共识机制是大部分（或全部）网络成员就某条数据或拟定的交易价值达成一致，并对账本进行更新的机制。即共识机制就是在参与节点之间管理一系列连贯事实的规则和程序。共识算法允许机器连接起来工作，并在某些成员失去效用的情况下，仍然能使工作正常进行。这种容错能力是区块链及分布式账本的另一核心能力，并有备用的内置冗余容量[5]。区块链产生的区块依赖于共识机制来保持其一致性。一致性问题的理论基础是拜占庭容错（Byzantine Fault-Tolerant，BFT）。

2.1.2　共识机制的具体内容

区块链中的共识具体内容较多，例如，在以比特币为代表的区块链系统中，需要对某一笔交易的有效与否达成共识，或需要以某种方法让整个参与比特币的人达成共识，以确认哪一笔交易是有效的。这种针对交易的有效性达成共识是区块链最核心的功能之一，也是几乎所有区块链产品都必做到的共识内容。区块链还有一个极其重要的共识内容是所有参与者需要对最新的高度区块达成共识。例如有两个矿工在同一时间挖出两个区块，确认谁的区块有效，谁的区块是孤立块，就需要一种机制让大家都接受最终答案，且不允许出现分歧。使参与者之间达成共识的方法，就是共识机制，也称为共识算法。

2.2　常见的共识算法

2.2.1　工作量证明

工作量证明（Proof of Work，PoW）是中本聪在比特币白皮书中提出的机制，即人们所说的矿工及挖矿，当一笔交易发生时，互联网内的矿工通过与或运算，获得一个满足交易规则的随机数，此时该矿工便拥有了本次交易的记账权，并向全网其他节点发送该交易相关的信息供其录入。而其他节点收到信息后对其进行校验，校验完成后所有节点将信息存入。只要节点存在于网络中，如果该节点想要产生新的区块并将其写入区块链，则必须要面对一个问题，即如何对比特币网络提出的关于 PoW 的问题做出解答。这个问题在 3 个方面举足轻重：工作量证明函数、区块以及难度值。其中，工作量证明函数提供了解决问题的方法，区块对于这个问题需要录入的数据起到了至关重要的作用，而难度值直接影响到这个问题所需要的运算量大小。

图 1 为工作量证明流程图，区块链是由一个持续增长的顺序块组成的，每个块包含了头文件和一系列的交易信息 T_{xi}。其中头文件保护了时间戳 T_i、上一个块的索引 H_{i-1}，和 nounce N_i-1，对于每一轮，只要找到相应的 Hash 就算成功。工作量证明有几个比较突出的特点：1）工作量证明相比于其他算法所需要投入的资源相对较少，且其在场景内的应用有较强的可操作性；2）工作量证明算法内的节点达成一致的条件较低，达成共识不需要再进行额外的信息交流；3）想要对系统造成不可磨灭且不可逆转的损失几乎是不可能的。同时，由于挖矿会造成大量的资源浪费，达成共识的周期较长而难以缩短，且极有可能出现分叉，则需要等待多个区块收到信息后再进行确认；永远没有最终性，则需要设置检查点机制来弥补其没有最终性的缺点。

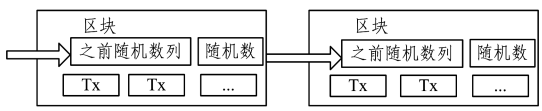

图 1　工作量证明流程图

2.2.2　权益证明

权益证明（Proof of Stake，PoS）是 PoW 的一种升级共识机制，该共识机制的主要思想是节点记账权的获得难度与节点持有的权益成反比。即节点持有的权益越多，那么节点记账权的获取就越简单；相反，节点持有的权益越少，那么节点记账权便越难以获取。这种权益证明算法能够对算法内的每个节点进行分析，以每个节点占有虚拟货币的多少作为评判标准，并基于此对挖矿所需的工作量进行优化，节点占有的代币越多，挖矿就越容易，权益算法以此来增加寻找随机数的难度。PoS 也被称作股权证明，是一种在公链中的共识算法，可以作为 PoW 算法的替换，它是一种保障比特币、以太坊和其他区块链安全的机制。

权益证明的特点是效率高，在一定程度上节约了资源，但也面临一些潜在的现实风险，业内的研究人员通常将其称为 nothing-at-stake 问题，即区块的创造者与验证者完成各自的工作投入的成本均很低，因此违背系统协议作恶的损失也很小。

2.2.3　股份授权证明

股份授权证明（Delegated Proof of Stake，DPoS）机制是 PoS 的进化方案，在常规 PoW 和 PoS 中，任何一个新加入的 Block 都需要被整理网络的节点确认，严重影响了整理网络的效率。DPoS 优化了共识机制，通过不同的策略，不定时的选中一小群节点做新区块的创建、验证、签名和相互监督，可以大幅度地减少区块创建和确认所消耗的时间和算力成本。

2.2.4　实用拜占庭容错算法

实用拜占庭容错（Practical Byzantine Fault Tolerance，

PBFT)算法是一种基于状态机副本复制的算法,此算法对于容错服务的实现起到了至关重要的作用,这种方法通过对服务器的复制来协调客户端并交互服务器的镜像以完成整个系统的容错。即建模时,将服务作为状态机对副本进行复制,这一过程在整个分布式系统的节点内进行。这一复制操作让容错服务的所有信息都保存在每个进行复制的状态机的副本中,与此同时,也真正完成了容错。将状态机的所有副本组合为一个集合,用 R 表示,将集合的每一个副本进行编号:0,1,2,…,$|R|-1$。为了便于计算和描述,设 $|R|=3f+1$,由于副本有一定可能性失效,而 f 正代表失效副本的最大可能值。当然,如果副本数量多于 $3f+1$ 这一情况是存在的,但是额外存在多于 $3f+1$ 的副本不能使整个系统变得更加稳定可靠;相反,由于副本数量的增多,使系统整体负载增加,从而导致系统性能降低。在 PBFT 算法中,客户端向主节点发送请求调用服务操作;主节点通过广播将收到的来自客户端的请求发送给其他副本;能够收到的副本执行请求同时将执行结果发送给客户端;客户端将收到的 $f+1$ 个不同副本节点发回的相同结果作为整个操作的最终结果。

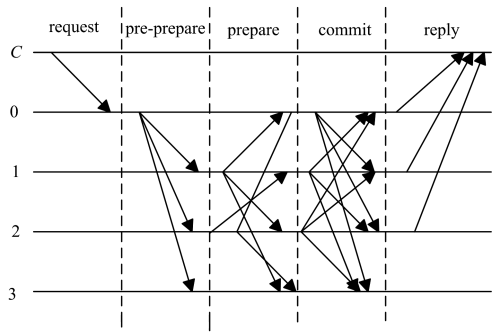

图 2 实用拜占庭容错算法流程图

从全网节点中选择一个节点作为主节点(Leader),主节点将负责生成每个新区块。

1)Pre-Prepare:每当一笔交易达成,客户端会给每个节点发送交易的信息,节点收到信息后,向网络内其他节点发送。主节点在网络内收到了多笔交易信息,且这些信息都需要存放于新区块中,而主节点将其排序后存入列表内,并向整个网络发送该列表,扩散至 123;

2)Prepare:每个节点接收到主节点发送的列表后,按主节点排列好的顺序对区块链系统中交易列表内的交易进行模拟执行,等待所有交易结束后,根据交易的结果计算新区块的哈希摘要并向全网广播[6];

3)Commit:区块链系统中的一个节点,如果收到 $2f$(f 为可容忍的拜占庭节点数)个其他节点发来的哈希摘要都与自己相等,那么就向全网广播一条 commit 消息;

4)Reply:区块链系统中的一个节点,如果收到 $2f+1$ 条 commit 消息,那么就能提交新的区块及其交易到本地的区块链和状态数据库[7-8]。

通过以上几种常见的共识算法分析,共识算法自身的优劣直接对分布式账本系统起着至关重要的作用,如果该分布式系统采用的共识算法足够好,那么该系统的性能也会是顶尖的;反之,共识机制若不尽如人意,那么采用该共识算法的分布式系统也会性能低下。共识算法的优劣主要表现在去中心化、共识成本、算法处理能力、防御措施、算法处理能力、防御措施和容错能力等方面,且不同的业务应用场景需要采用不同的共识算法。

3 基于区块链的云计算资源去中心化交易共识机制

3.1 云计算资源交易市场描述

作为一种全新的商业计算模式,云计算能够整合各类型的存储、网络、数据、硬件等分布式资源为用户提供强大的计算能力,从根本上有别于并行处理、分布式计算与网格计算。通过网络将软件、硬件及数据集成为用户提供动态资源,这些资源通过网络调度以服务的形式提供给用户,即云计算服务(或称云服务)。用户、云计算服务和服务提供者构成了庞大的云计算服务市场。与生活中普通的商品不同,云计算服务具有动态性、多样性、异质性、弹性可扩展和虚拟化等特性,导致云计算服务市场构成一个非常复杂的资源市场。

云计算服务市场是由大量云服务资源提供者与云服务资源使用者构成的不同交易主体参与的云计算服务交易市场。不同于传统商品市场上的交易,云计算服务是虚拟商品,交易是在互联网平台完成的,参与者为云计算服务的提供者和云计算服务的使用者。作为交易对象的云服务,包含服务质量、安全性、价格等多种属性。

图 3 给出了云计算服务市场的概念模型。

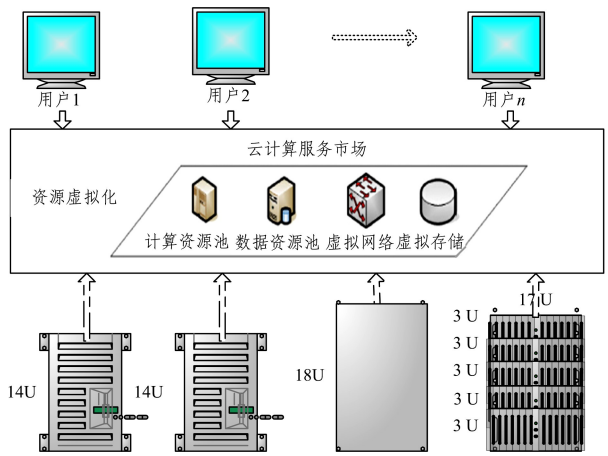

图 3 云计算服务市场的概念模型

云计算服务市场包含以下要素:

(1)云计算服务资源

云计算市场是为了高效率地使用资源,因此云服务资源是该市场必须的要素。市场中包括了基础设施级服务(IaaS)、平台级服务(PaaS)和软件级服务(SaaS)各个层次的云服务资源。云服务不局限于具体资源,而泛指网络、服务器、存储、应用软件、数据等多种单个或者组合的资源包。

(2)市场参与主体

在云计算市场中,众多的云服务提供商和云服务购买用户构成了市场的参与者。云服务提供商包括提供云服务的传统 IT 厂商、互联网提供商转型云计算服务提供商以及软件厂商等。比较有代表性的 IT 厂商有浪潮、IBM、惠普等;互联网企业有阿里云、腾讯云、百度、Google 等;软件企业有微软、Vmvare 等。云服务使用者包括政府、企业及个人。

(3)网络带宽资源

云计算最主要的思想核心在于实现对大量的计算资源的统一管理和调度,从而在大量网络连接的计算资源的基础上为消费者提供服务。因此,如何快速、合理地对云计算资源进行调度是云计算产业发展过程中要解决的关键问题。可以看出,云计算服务资源是分布在大量的分布式计算机上的,而非

本地计算机或远程服务器中，必须依靠网络将市场的参与者链接起来，所以网络带宽对于资源调度的质量和云计算市场的正常发展起着非常重要的作用。

(4)市场运行机制

科学合理的经济运行规则保证了商业经济的繁荣。云计算市场也是资源的交易市场，也需要响应市场的交易法则，才能保证云资源的有效管理和调度。理论上各种市场机制都有可能在云服务市场中得到应用，但是，何种市场机制能够更好地满足云计算服务市场的发展需求，是一个值得学界与产业界科研工作者不断深入研究的问题。科学合理的、符合发展需求的市场运行机制，能够让云计算资源得到有效利用，最大化的节省数据中心的能耗。

3.2　云计算去中心化的交易模式设计

云计算的目的是有效整合和共享云计算资源，利用虚拟化技术将云计算资源转化成具有服务能力的云计算服务产品，再通过互联网以提供服务的形式租用给所需的用户，它强调的是提供服务，云计算服务的使用和支付都依赖于商业模式的处理。因此，设计安全、高效、透明、信息对称的云计算服务交易模式和交易方法是云计算商业模式的关键问题。目前研究的云计算服务市场大多是基于云联盟资源的交易框架，云服务提供商通过自建或租用数据中心方式为市场提供虚拟资源，且多家云服务提供商建立联盟机制，根据用户的购买需求进行云计算资源调度，再通过制定合理的定价策略来实现双方的利益最大化[9]。这种基于联盟集中式的交易模式将面临 4 个问题：1)云计算资源使用者与提供者之间及云联盟内部多个云计算提供商之间存在信任问题，难以保证云计算资源的服务质量与数据安全；2)多个主体参与市场交易，导致云计算资源联盟运行成本高、运行效率低、决策耗时长，难以满足云计算资源的动态调度需求；3)云联盟内多个企业提供的资源无交易到交付后的追踪记录，导致云计算服务等级协议(SAL)出现问题，就无法查证资源的来源；4)云联盟企业容易导致信息安全风险，危害交易安全及用户的隐私安全。

针对以上问题，文中引入区块链技术来解决云计算资源交易中的问题，通过设计去中心化的云计算交易模式，改变了用户通过网络带宽资源获取中心化数据中心所提供的计算、存储、数据库等服务。基于区块链技术构建全球联网计算机算力交易平台，真正实现云计算资源的弹性可扩展与按需分配。全球所有数据中心、企业计算中心及个人 PC 等计算资源连接起来，集平台上万个资源贡献者、平台使用者、应用开发者之力，提供低价格、大范围、强算力的可信任的云计算平台服务，击破传统的中心化云计算商业模式及资源分布结构。如图 4 所示。

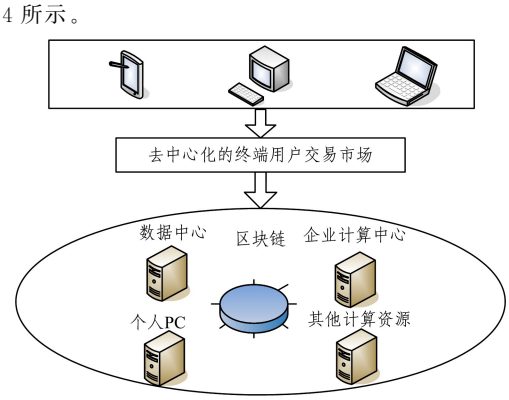

图 4　云计算服务市场去中心化交易

图 4 描述的是去中心化的云计算资源交易市场。所有用户既是资源的生产者也是资源的消费者，所有资源的产生、交易、消费及使用信息都能记录到区块中，提升了资源的使用效率，保障了数据存储安全。

3.3　基于以太坊的云计算交易共识算法改进

本文将云计算资源交易市场作为应用场景，提出了一种基于改进实用拜占庭容错算法的以太坊共识机制，用于对区块链共识机制的有效性进行校验。通过这种改进的算法，节点不再需要 PoW 来达成共识，这样就避免了算力资源浪费。在执行检查点协议时，该改进算法取消了传输数据过程，而没有了这一过程对数据的损耗，也可以有效降低数据的流失，解决了以太坊在云资源交易市场内面临的算力竞争导致的资源浪费以及节点间的相互信任问题。其中，相比于实用拜占庭容错算法，该算法舍弃了证书删除节点的协商时间，运用节点的索要形式来完成系统同步区块。

3.3.1　定义算法

在实用拜占庭容错算法机制中，有以下定义。

定义 1　假定集合 Congress 由系统内的节点组合而成，且任两个 Congress 集合的交集不是空集；再假定系统节点集合为 U，$\alpha=\{C_1,C_2,\cdots,C_N\}$，且 $C_1\subseteq U$，并满足式(1)，即可称 C 为一个 Congress。

$$\forall C_i,C_j\in\alpha \text{ 且 } C_i\cap C_j\neq\emptyset \tag{1}$$

Congress 有如下特点：

1)任意两个 Congress 至少有一个正确且共同的节点；

2)一定存在没有错误的 Congress。

定义 $2f+1$ 个节点构成一个 Congress，f 为 faulty 节点，即系统中最多可以容忍的错误节点个数，这样可以确保在一个 Congress 中至少有 $f+1$ 个节点是无错的。

定义 2　在 PBFT 中，有效的节点通过一致性对节点群中的节点变化进行观察，达到一致性的群称作视图，将视图编号为 v，假设一个视图包含 N 个节点，每个节点编号为{0，1，2，…，$N-1$}，其中，主节点的编号为 p(除主节点外的节点统一记作 replica，为备用节点)，满足：

$$p=V \bmod N \tag{2}$$

当群中的主节点出现一些未预料的状况时，该节点便不再是主节点，新的主节点是原主节点生成的下一个节点，而主节点的变化将带来视图的改变，主节点的编号递增 1。

定义 3　在区块达成共识的过程中，将被传递的消息称为证书，证书中包含信息的编号，而文中将区块的编号作为信息的编号。

3.3.2　生成区块

在区块链中，当有一笔交易发生时，产生的区块将提交交易并永久写入区块链中。本文所提机制中，交易被写入区块链的过程为：

1)主节点会对交易列表中的每个交易信息进行校验，将校验通过的交易记录到区块中，同时向其他区块发出区块信息；

2)区块链系统中的其他节点对收到的区块信息的合法性进行校对；

3)所有的校对通过后，区块链系统中的所有节点将校对通过的区块添加到区块链中，同时在交易列表中删除与该区块内含的交易信息，即认为该区块的交易已经录入区块链且有效。

3.3.3 制定一致性协议

制定一致性协议,使各区块在全网达成一致性。在实用拜占庭容错算法中,系统最多容忍全部节点的 1/3 出现拜占庭错误。在此假设区块链中共存在 $3f+1$ 个节点,一个 Congress 中最少有 $2f+1$ 个节点。

容忍拜占庭错误的系统中,f 的最小值为 1,因此区块链中的节点个数至少为 4。图 5 为 4 个节点组成的区块链系统,触发一次正常请求时,区块链系统的执行过程。

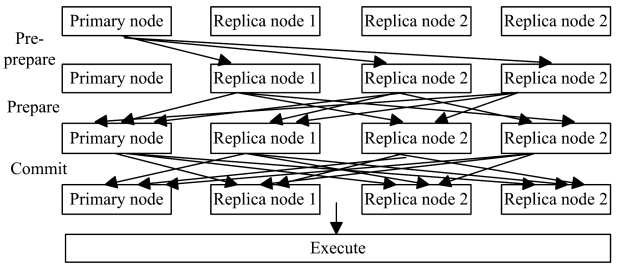

图 5 对于正常请求的执行

一个区块信息从接受到达成共识并执行需要经过 3 个阶段。

1)Pre-prepare:主节点收到客户端请求,给请求编号,并将 Pre-prepare 证书发送给其他节点。

2)Prepare:replica 接收到 Pre-prepare 证书的同时也接收到新生成的区块信息,这个节点就进入 Prepare 状态。如果这个节点收到的消息来源于主节点且是首次接收时,会将 Prepare 证书发送给其他节点并记录证书信息。

3)Commit:如果有证书信息通过了 $2f$ 个节点认证,这样就证明了该区块信息得到了一个 Congress 的认可,则该节点进入 commit 状态,同时该节点向区块链系统内其余节点发送 commit 信息。这时 replica 收到来自于区块链系统内其余节点的 commit 证书,且该证书信息通过了 $2f+1$ 个节点的认可,就将此区块添加至区块链中。

经过所述的 3 个阶段将信息提交,这个新生成的区块被认为达成了区块链系统内所有节点的共识。由图 5 可知,当 replica 节点出现拜占庭错误时,如果其他两个 replica 节点正确,那么就能满足区块链系统中有 $2f+1$ 个节点通过验证的条件,这样正确的节点之间同样可以保证区块间的一致性。假设区块链系统中主节点产生拜占庭错误,该节点被舍弃,此时需要在 replica 节点中重新选一个主节点生成区块后发送消息,经过上述过程将区块添加至区块链中,进而触发生成下个区块,如此往复。

3.3.4 检查点协议

检查点协议是通过节点之间的定时协商清除信息,这一做法是避免了个别节点不同步而需要收集之前的证书,也可以解决证书信息的回收问题。解决证书的回收,即清除过期证书,而这一步骤需要得到全网络节点的共识,也需要执行图 5 中的 3 个阶段,这样将造成通信资源的极大浪费。区别于实用拜占庭容错算法,本文依据区块链系统中最优区块的时间戳进行证书回收以及清除。当有新的区块被添加到区块链中,就可以得到该区块时间戳之前的证书都已经被校对过的消息,这个节点中的证书状态已广播完毕并被清除,但其证书信息将以区块的形式永久保存于该节点中。通过对添加区块时间的监听,可以清除此区块时间戳之前的证书信息,这个添加后又删除的过程取消了网络内节点间的交流过程,在此基础上也可以使证书信息的删除过程正常进行[10]。

如果一个节点发现自己记录的区块链与信任的区块维护的区块链的最优区块的编号差距到一定大小时,这个节点将向信任节点索引区块,将要来的区块记录到自己所维护的区块中。这一过程是以太坊中当网络内各节点需要进行区块同步时的流程。这一对于区块同步的解决方案,也许在以太坊内可以实现,但是在云资源交易市场中的节点没有信任的节点,也就无法向信任的节点索要区块并添加至区块链中,该做法也失去了实际操作意义。本文提出的基于实用拜占庭容错算法的改进算法可以解决这个问题:进行交易时,每当系统发现一个与众不同的节点时,即一个节点与网络内其他节点的所处情况不同,改进的实用拜占庭容错算法会做出反馈,采用发出区块哈希方法,让节点达成共识;节点间达成共识后,一个新的区块被写入区块链,区块链中的区块之间进入同步状态。这就是改进实用拜占庭容错算法使区块间达成同步的方法,该方法有别于传统的实用拜占庭容错算法,其数据传输量极小,与对应的网络开销相比,是可以忽略不计的。

结束语 本文设计了去中心化的云计算资源交易模式,对区块链目前较为主流的共识算法做了分析,结合云计算资源交易的应用场景,设计基于区块链的云计算资源交易市场的改进实用拜占庭容错算法。在区块链应用于联盟链的场景下,该算法对工作量证明机制存在的算力竞争导致的资源浪费以及节点间信任度较低的问题进行了大幅度的优化。改进算法取消了挖矿过程,直接通过主节点生成区块,其他节点会对主节点生成的区块是否在全网达成一致进行协商,并以此方式达成共识,解决了工作量证明机制存在的缺陷。改进实用拜占庭容错算法中的检查点协议使其与以太坊环境更加契合,缩减了网络通信产生的费用。区块链技术的应用为保证云计算资源交易效率与安全提供了新方法。

参 考 文 献

[1] DORIAN S. Nakamoto Bitcoin:A peer-to-peer electronic cash system [Z]. Consulted,2008.

[2] 浦东平,樊重俊,梁贺君. 基于区块链视角的电商平台体系构建及应用[J]. 中国流通经济,2018,32(3):45-51.

[3] 平健,陈思捷,等. 基于智能合约的配电网去中心化交易机制[J]. 中国电机工程学报,2017,37(13):3682-3690.

[4] 邵炜晖,许维胜,等. 基于区块链的虚拟电厂模型研究[J]. 计算机科学,2018,45(2):25-31.

[5] 沈鑫,裴庆祺,刘雪峰. 区块链技术综述[J]. 网络与信息安全学报,2016,2(11):11-20.

[6] 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.

[7] 琚巍巍. 分布式存储系统容错技术的研究与实现[D]. 西安:西安电子科技大学,2009.

[8] 翟社平,李兆兆,等. 区块链关键技术中的数据一致性研究[J]. 计算机技术与发展,2018,28(9):94-100.

[9] 陈冬林. 云计算市场交易与资源调度机制[M]. 北京:电子工业出版社,2017.

[10] 黄秋波,安庆文,苏厚勤. 一种改进 PBFT 算法作为以太坊共识机制的研究与实现[J]. 计算机应用与软件,2017,34(10):288-293.