

面向物联网的区块链共识机制综述

田志宏, 赵金东*

(烟台大学 计算机与控制工程学院, 山东 烟台 264005)

(* 通信作者电子邮箱 zhjdong@ytu.edu.cn)

摘要:随着数字货币的不断发展,区块链技术引起越来越多人的关注,而对其关键技术共识机制的研究尤为重要。将区块链技术应用在物联网(IoT)中是目前研究的热点问题之一。共识机制是区块链的核心技术之一,其在去中心化程度、交易处理速度、交易确认延迟、安全性以及可扩展性等方面对IoT产生了重要影响。首先对IoT的体系结构特征以及资源受限问题造成的轻量化问题作了阐述,对在IoT中实现区块链所面临的问题作了简要概述,并结合比特币的运行流程对IoT中的区块链需求进行了分析;其次,把共识机制分为证明类、拜占庭类和有向无环图(DAG)类,研究了这些不同类别的共识机制的工作原理,在通信复杂度上分析它们与IoT的适应度,总结它们的优缺点,并对现有的共识机制和IoT结合的架构进行了调研分析;最后,针对IoT面临的中心机构运行成本高、可扩展性差、安全性存在隐患等问题进行了深入研究,分析结果表明,基于DAG技术的埃欧塔(IOTA)和Byteball共识机制在交易数量很多的情况下具有交易处理速度快、可扩展性好、安全性强的优点,是未来IoT领域区块链共识机制的发展方向。

关键词:区块链;共识机制;物联网;适应度;埃欧塔;Byteball

中图分类号:TP391 **文献标志码:**A

Overview of blockchain consensus mechanism for internet of things

TIAN Zhihong, ZHAO Jindong*

(School of Computer and Control Engineering, Yantai University, Yantai Shandong 264005, China)

Abstract: With the continuous development of digital currency, the blockchain technology has attracted more and more attention, and the research on its key technology, consensus mechanism, is particularly important. The application of blockchain technology in the Internet of Things (IoT) is one of the hot issues. Consensus mechanism is one of the core technologies of blockchain, which has an important impact on IoT in terms of decentralization degree, transaction processing speed, transaction confirmation delay, security, and scalability. Firstly, the architecture characteristics of IoT and the lightweight problem caused by resource limitation were described, the problems faced in the implementation of the blockchain in IoT were briefly summarized, and the demands of blockchain in IoT were analyzed by combining the operation flow of bitcoin. Secondly, the consensus mechanisms were divided into proof class, Byzantine class and Directed Acyclic Graph (DAG) class, and the working principles of these various classes of consensus mechanisms were studied, their adaptabilities to IoT were analyzed in terms of communication complexity, their advantages and disadvantages were summarized, and the combination architectures of the existing consensus mechanisms and IoT were investigated and analyzed. Finally, the problems of IoT, such as high operating cost, poor scalability and security risks were deeply studied, the analysis results show that the Internet of Things Application (IOTA) and Byteball consensus mechanisms based on DAG technology have the advantages of fast transaction processing speed, good scalability and strong security in the case of having a large number of transactions, and they are the development directions of blockchain consensus mechanism in the field of IoT in the future.

Key words: blockchain; consensus mechanism; Internet of Things (IoT); adaptability; Internet of Things Application (IOTA); Byteball

0 引言

近年来,物联网(Internet of Things, IoT)设备呈指数级增长,物联网以传统互联网、移动网络、传感器网络为基础,扩展了新的互联网概念,实现万物互联互通,使人类社会更加高效、智能化^[1-2]。但是,物联网设备资源有限,且容易受到安全

攻击^[3]。伴随着区块链在对等网络(Peer to Peer, P2P)传输、分布式存储、共识机制、密码学、智能合约等技术方面的不断运用,将区块链核心技术之一的共识机制应用于物联网场景中,能够解决物联网面临的中心机构运行成本高、可扩展性差、安全性存在隐患等问题,提高物联网的性能和安全性^[4]。

传统的共识机制需要竞争记账权,会造成资源大量浪费

收稿日期:2020-11-05;修回日期:2020-12-17;录用日期:2020-12-21。

作者简介:田志宏(1993—),男,山东临沂人,硕士研究生,CCF会员,主要研究方向:物联网、区块链;赵金东(1974—),男,山东滨州人,副教授,博士,CCF会员,主要研究方向:物联网、区块链。

的现象,不完全适用于资源有限的物联网设备;此外,随着物联网设备的不断增加,交易的处理速度和可扩展性也需要得到提高。而且,区块链分叉^[5]也会导致双花攻击。双花攻击指的是攻击者通过不承认最近的某个交易,并在这个交易之前创建了一条更长的区块链,从而实现一笔交易被花费了两次^[6]。为了解决分叉问题,区块链通常采用最长链原则,但是这样会造成交易高延迟问题^[7]。因此研究各种共识机制优缺点,对物联网和区块链的结合具有重要的意义。

目前,出现了很多种共识机制,有的通过算力竞争来实现,如工作量证明(Proof of Work, PoW)共识机制;有的使用投票选举来实现,如授权股权证明(Delegated Proof of Stake, DPoS)共识机制;还有的利用燃烧硬币来实现,如燃烧证明(Proof of Burn, PoB)共识机制以及其他实现形式的共识机制等。这些共识机制各有各的优势,并且都在相应的场景中得到了运用。但是物联网具有节点密集、资源受限、容量不足等特征,现有共识机制能否直接在物联网场景中得以实现,仍待研究。本文对区块链技术现有的协议、算法和技术进行分析和对比,研究各种共识机制在物联网环境中使用时存在的问题。

本文的主要工作如下:

- 1) 对面向物联网的共识机制进行了分类,分别讨论了各类共识机制的工作原理和优缺点;
- 2) 研究了共识机制在去中心化程度、交易处理速度、交易确认延迟、安全性和可扩展性方面与物联网的适应度;
- 3) 讨论了面向物联网的区块链共识机制现有的挑战,把握了今后研究工作的方向。

1 物联网区块链

1.1 区块链

区块链的概念最开始是由一个笔名为“中本聪”的学者于2008年发表的论文“Bitcoin: a peer-to-peer electronic cash system”中提出的^[8]。区块链中存放了大量的交易信息,相当于一个数据库^[9-12]。文献^[13]提出区块链是一种按照时间顺序将区块从后向前依次链接起来的数据结构,利用非对称加密技术来保证不可篡改和不可伪造的去中心化共享账本。图1是区块链结构图,其中 $a \geq 0$ (当 $a=0$ 时表示创世区块),区块由区块头和区块体构成,区块头包括父区块哈希值、版本号、时间戳、难度目标、*nonce*值以及*merkle*根,区块体保存着大量的交易信息。

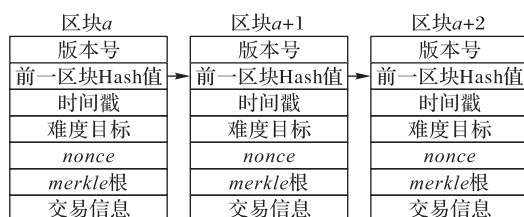


图1 区块链结构

Fig. 1 Blockchain structure

区块链具有去中心化、开放性、共识机制和不可篡改等特点,确保了交易信息的正确性、安全性。

首先,区块链去中心化的特点使每个节点都有权共享交易信息并对信息的正确性进行验证;其次,区块链开放性的特点是每个节点在任何时间都可以加入或者退出;再次,区块链共识机制的特点可以使没有联系的节点,直接依靠共识机制来达成一致协议;最后,区块链不可篡改的特点是基于哈希算法来保证交易信息不会被更改^[14]。此外,根据应用场景和开放程度,区块链可以被划分为公有链、联盟链和私有链^[15-16]。

1.1.1 比特币的运行机制(区块链1.0版本)

比特币是区块链1.0版本的代表,它是一种数字货币,产生于分布式网络结构,区块链1.0版本的系统架构如图2所示。

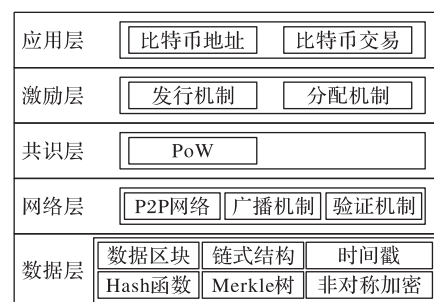


图2 区块链1.0版本架构

Fig. 2 Blockchain version 1.0 architecture

在比特币系统中,每个节点通过P2P网络传输的方式完成交易信息的共享,并且节点可以匿名,保证了网络中交易信息的同步性。此外,为了防止双花攻击,系统采取给交易信息加上时间戳选取计算量最多的链为主链,维护其安全性。图3描述了比特币系统的运行流程^[17]:

- 1) 用户发起一笔新的交易,交易信息在全网中不断被广播;
- 2) 每个节点对接收到的交易进行验证,如果该交易被验证为有效,则将交易存储在交易池中;
- 3) 各节点通过挖矿来产生区块,矿工们需要通过工作量证明来完成哈希计算;
- 4) 当一个节点挖出一个区块,网络中的其他节点将确认该区块的有效性,只需要花费少量的PoW计算即可;
- 5) 如果该区块被确认为有效,则将其链接到区块链中;
- 6) 成功完成一笔交易。

1.1.2 智能合约(区块链2.0版本)

智能合约这一概念最先由Nick Szabo提出,是一套以数字方式定义并被实现的承诺^[18]。区块链去中心化和不可篡改的特点为智能合约赋予了新的涵义,使智能合约能够运行在安全可靠的环境中,图4是区块链2.0版本的基础架构^[13,19]。共识层包含各种共识机制,网络层中P2P网络负责信息的广播,数据层存放数据信息、时间戳等,激励层包含以激励的方式获得收益所采用的机制^[20-22],合约层主要是智能合约,应用层是区块链的应用场景。Ethereum^[23]和Hyperledger^[24]等平台利用智能合约,有效地解决了比特币系统存在的交易处理速度慢和高延迟的问题。

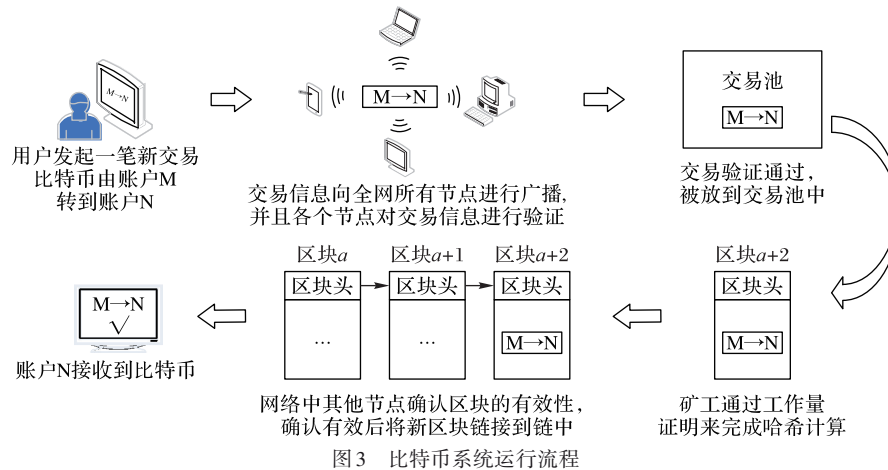


图 3 比特币系统运行流程

Fig. 3 Operation flow of bitcoin system

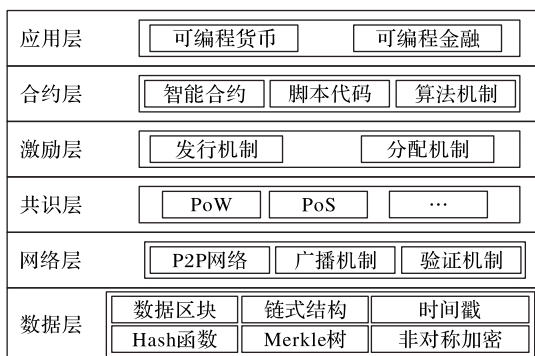


图 4 区块链 2.0 版本架构

Fig. 4 Blockchain version 2.0 architecture

1.2 共识机制

去中心化是区块链中的一个核心要素,每个节点的权力都是一样的,为了保证各个节点之间相互协作需要一套算法,这套算法被称为共识机制^[25-26]。共识机制的研究起源比较早。1982年,Lamport、Shostak和Pease提出了在遭受拜占庭节点的情况下如何达成一致性协议的拜占庭将军问题,推动了共识机制的发展^[27-28]。

区块链核心技术共识机制首先应用于比特币中,随着区块链技术的不断发展与完善,共识机制也越来越成熟。常见的共识机制有工作量证明、权益证明(Proof of Stake, PoS)、授权股权证明、权威证明(Proof of Authority, PoA)、燃烧证明、贡献证明(Proof of Contribution, PoC)、存在证明(Proof of Existence, PoE)^[29]、数据可恢复证明(Proof of Retrievability, PoR)^[30]、存储证明(Proof of Storage)^[31]、拜占庭容错(Byzantine Fault Tolerance, BFT)^[32]、实用拜占庭容错(Practical BFT, PBFT)、简化拜占庭容错(Simplified BFT, SBFT)^[33]、MinBFT^[34]、Honeybadge-BFT^[35]、Algorand、Paxos^[36]、Raft、Tendermint、埃欧塔(Internet of Things Application, IOTA)、Byteball、Hashgraph^[37]、HashNet^[38]、Ouroboros^[39]等。

1.3 物联网

物联网通过连接互联网和信息传感设备,实现智能化控制和处理信息^[40]。图5是物联网层次结构,自底向上可分为三层:感知层、网络层和应用层。感知层能够收集和处理信息;网络层通过网络传输完成信息交互;应用层直接联系具体业务,如智慧城市^[40]、智慧工厂^[41]、智能家居^[42]等。

物联网通常包括资源约束的嵌入式设备,如射频识别

(Radio Frequency Identification, RFID)和传感器节点^[43]。传感器节点作为物联网的重要组成部分,在实际应用中会面临一些技术挑战^[44-46]:第一,由于传感器节点数量多,分布范围广,难以对节点进行集中的管理和维护;第二,由于体积小、功耗低、成本低,传感器节点的能量、计算、存储、通信能力受到限制,影响了网络的扩展能力;第三,由于大多数传感器节点都部署在无人值守的区域,容易出现数据被篡改或遭受攻击,安全性得不到保障;第四,传感器节点容易损坏,一旦出现问题,就无法判断是软件问题、硬件问题还是系统故障,这是由于节点存储空间有限,在节点端很难存储过多的调试信息,没有调试信息就不能够找到错误原因;第五,由于传感器节点在共享信息时,信息容易被泄露,面临隐私泄露威胁。

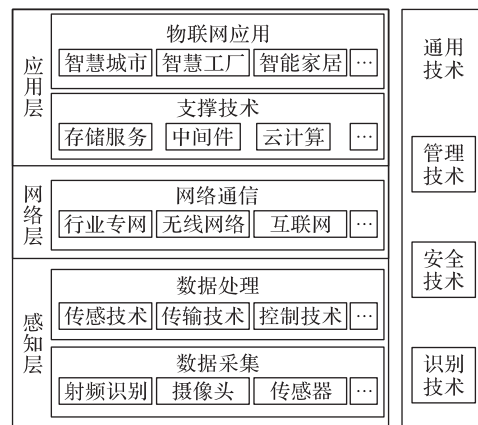


图 5 物联网层次结构

Fig. 5 Hierarchical structure of internet of things

区块链拥有安全可靠的加密技术,并且凭借去中心化、共识机制、不可篡改的特性,能够改善物联网的安全和可扩展性问题^[47]。区块链去中心化的特点使物联网设备不需要中心服务器直接进行信息交互,解决中心机构运行成本高的问题。区块链共识机制的特点能够使物联网设备之间保持信任,增强网络的可靠性^[48]。区块链不可篡改的特点使得数据写入区块链就难以更改,实现物联网设备中数据的追本溯源^[49]。文献^[50]提出利用区块链去中心化的特点解决物联网集中访问控制的问题,实现了去中心化访问控制系统。文献^[51]为解决分布式物联网内的设备之间的信任问题,借助区块链共识机制,提出了一种适用于分布式物联网的信任管理方法,实现了数据共享与数据安全。将区块链共识机制应用于物联网

中,在物联网设备之间实现共识过程,将增强物联网的性能和安全性。

接下来,将详细讨论面向物联网的各种共识机制,并对常见的共识机制进行分类研究,分析共识机制是否适用于物联网场景中。

2 共识算法

物联网设备具有数量多、分布范围广、功耗低、计算能力弱和安全存在隐患的特征,因此分析区块链共识机制的优缺点,对区块链技术能否应用于物联网场景中具有至关重要的作用。随着区块链技术的发展,共识机制的数量与日俱增。本章将介绍在区块链网络中广泛使用的共识机制,并讨论它们的优缺点。

根据生成新区块的方式,可以把共识机制划分为证明类、拜占庭类^[7]和有向无环图(Directed Acyclic Graph, DAG)类。下面将介绍各类共识机制(PoW、PoS、DPoS、PoA、PoC、Ouroboros、PBFT、Algorand、Tendermint、IOTA、Byteball),并对比较分析共识机制在物联网场景中的适应度。

2.1 证明类共识机制

证明类共识需要在共识过程中证明自己满足的特定条件,一般表示为“Proof of X”^[52]。

2.1.1 PoW 共识机制

PoW 共识机制,即工作量证明共识机制。其思想最早出现在 1992 年由 Dwork 和 Naor 发表的论文中,被用来防止垃圾邮件问题^[53]。比特币成功利用 PoW 共识机制在没有中央机构的情况下,使全网每个独立的节点就交易信息的正确性达成一致,实现节点之间的相互信任,同时防止恶意节点制造假身份发起女巫攻击^[54]。

PoW 共识机制用公式 $\text{Hash}(\text{head} \parallel \text{nonce}) < \text{target}$ 来表示,Hash 表示哈希函数,head 表示区块头相关数据,nonce 表示随机数,target 表示难度目标值(网络目标值)。PoW 共识机制的工作原理:矿工首先把所有交易打包生成候选区块,然后通过穷举不断改变 nonce 值,重复计算区块头的哈希值,使得 nonce 值拼接上区块头信息哈希值再进行哈希计算,直到满足区块头哈希小于难度目标值这一条件,才能产生新区块。图 6 是 PoW 共识机制工作原理图,为了找到一个合适的 nonce 值,需要多次进行哈希计算。

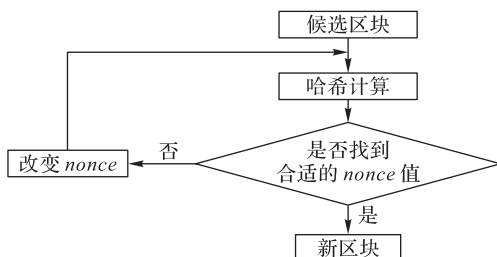


图 6 PoW 共识机制工作原理

Fig. 6 Working principle of PoW consensus mechanism

难度目标值的计算公式^[55]为:

$$\text{newtarget} = \text{oldtarget} * (20160 / \text{totaltime}) \quad (1)$$

其中:newtarget 表示生产新区块的难度目标值;oldtarget 表示生产上一个区块的难度目标值;totaltime 代表生产前 2016 个区块所使用的时间。PoW 难度目标值调整机制:newtarget 变大,生产区块所使用的时间会缩短;newtarget 变小,生产区块

所使用的时间会变长。

SHA256 哈希函数:交易信息被编码为固定长度的由字母和数字组成的字符串后写入区块链^[13]。哈希函数满足三个特性^[17]:1)输入长度不同,但是输出长度却是不变的。2)由输出推导出输入基本上是不可能发生的。对于给定的 b , 找到一个 a , 使 $\text{Hash}(a) = b$, 几乎不可能。3)输入不同,要产生相同的输出是很难的。给定不相同的 a 和 b , 使 $\text{Hash}(a) = \text{Hash}(b)$ 基本上不可能。

数字签名:共识机制通过数字签名的方式来核对发送者的身份,验证交易信息在传输过程中没有被篡改过,保证交易信息的完整性。数字签名的算法流程^[17]如下:1)密钥生成。首先对交易信息进行加密,并且使用椭圆曲线密码算法来产生公钥和私钥。2)签名算法。接收者使用私钥对接收到的消息进行签名,并且广播出去。3)验证算法。对发送者的身份进行确认,判断身份是否正确。

PoW 共识机制的通信复杂度:通信复杂度是指共识过程中各个节点为了达成一致所需要的通信量。由于工作量证明采用哈希算法,通过寻找 nonce 值,重复计算区块头信息,矿工之间不需要通信,只有在生成区块后才在全网进行广播,其他节点验证区块有效性。因此, PoW 共识机制的通信复杂度为 $O(n)$ 。

PoW 共识机制的优点:

- 1) 去中心化程度高。每个节点享有同等参与的权力,并且对产生的新区块进行验证工作。
- 2) 安全性高。基于最长链原则的 PoW 共识机制,产生区块需要牺牲大量的算力,作恶成本高,避免双花攻击。
- 3) 算法简单,容易实现。生成和验证区块是通过求解哈希函数来解决一个纯粹的数学问题^[56]。

PoW 共识机制的缺点:

- 1) 高延迟。生成一个区块需要花费 10 min,使得区块的确认时间长。
- 2) 可扩展性差。随着交易数量的增加,处理交易的能力有限。
- 3) 成本高。由于挖矿是一个不断进行哈希计算的过程,要以耗费大量的算力为代价,浪费资源。
- 4) 需要特殊的硬件设备,而且对带宽的要求较高。

PoW 共识机制与物联网场景的适应度:

PoW 共识机制应用于物联网场景中,受到四个因素限制:一是,挖矿需要消耗大量的算力资源,而物联网设备由于计算能力弱不适合成为矿工节点^[2];二是,完成共识过程需要消耗大量的能量,而物联网设备具有低功耗的特征,而且大部分物联网终端采用电池供电寿命有限,不能满足能量的供应;三是,由于哈希函数求解的复杂性,解决此难题需要一些时间,使交易处理速度较慢,影响了出块的时间,无法满足物联网应用的低延迟需求;四是,工作量证明共识机制需要特殊的硬件设备来支持以及对带宽有一定的要求,也不适合物联网场景。

2.1.2 PoS 共识机制

PoS 共识机制,即权益证明共识机制,也称股权证明共识机制。其想法来源于 Nick Szabo^[18],之后在 2011 年 bitconitalk 论坛上被 Quantum Mechanic 正式提出^[57],目的是解决 PoW 共识机制存在处理速度慢、高延迟以及计算量大的问题。与 PoW 相比, PoS 是用权益来代替算力,权益也被称为币龄。该算法的中心思想是通过权益大小来获得生成区块的权力,权

益越大的节点越有可能先生成区块,当系统签名一个区块时,其币龄被置为零^[57]。由于通过币龄来产生区块不需要消耗大量的算力,因此能量消耗少。

PoS算法表示: $coinage = coin * time$, $coinage$ 表示该笔交易的币龄, $coin$ 和 $time$ 分别表示持有货币的数量和时间,持有货币的数量越多或者时间越长,则获得产生区块的难度越小。

PoS 共识机制的优点:

1) 节省资源。生产区块不需要进行大量的计算,消耗的能量少。

2) 低延迟。节点挖矿不需要算力竞争,只需要权益证明,提高了确认效率,从交易被打包装入区块到生成新区块的共识过程的确认时间大约是 1 min^[56]。

PoS 共识机制的缺点:

1) 安全性差。由于挖矿成本不高,攻击者可以累积一定量的币龄,发起双花攻击。

2) 可扩展性差。由于交易数量的增加,网络节点处理交易的能力有限。

3) 激励问题。因为 PoS 共识机制在共识过程中不需要消耗大量的算力,相较于 PoW,其激励程度远远不及。

PoS 共识机制与物联网场景的适应度:

PoS 共识机制应用于物联网场景中,受到两个限制:一是, PoS 共识机制生成区块成本低,恶意节点可以发起 51% 攻击,而物联网设备本身就很容易遭受攻击,因此不太适用于物联网场景中^[58];二是,由于其可扩展性差,当物联网设备增加时,网络节点处理能力有限。

2.1.3 DPoS 共识机制

DPoS^[59]共识机制,即授权股份证明机制。DPoS是在 PoS 的基础上改进的一种共识算法,与 PoW 和 PoS 一样,最长的有效区块链即为最佳区块链。相较于 PoW 和 PoS 共识机制, DPoS 共识机制提高了交易处理速度,大约每 3 s 产生一个区块。全网每个拥有权益的节点都具有投票的权力,投票选出一定数量的代表节点,代表节点的职责是生产区块并进行区块的验证,类似于现实中“民主集中”制度的记账方式,可以在短时间内达成共识^[60]。图 7 是 DPoS 共识机制的工作流程:每个拥有权益的用户,投票选出 100 个代表,代表节点以轮流的方式在规定的时间内生产区块,只有验证通过,才能产生有效区块。此外,如果某一个代表节点长时间不在线或者多次产生无效区块,其他节点将投票选出一个新代表节点。

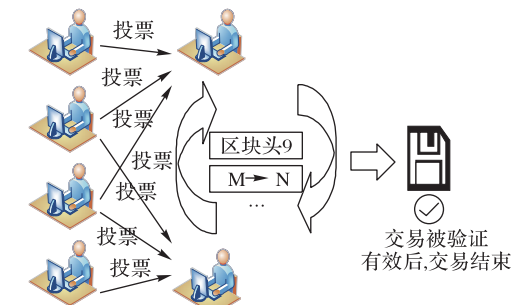


图 7 DPoS 共识机制的工作流程

Fig. 7 Workflow of DPoS consensus mechanism

DPoS 共识机制的优点:

1) 交易确认速度快。代表节点的数量是有限的,使得短

时间内达成共识,产生一个区块仅仅需要大约 3 s,相较于 PoW 共识机制产生一个区块需要 10 min,明显提高了确认速度。

2) 节约资源。在系统中投票选取少量的代表节点,依靠每个代表节点轮流产生区块,不需要消耗大量的算力资源。

3) 可扩展性好。由于代表节点处理交易能力强,提高了节点处理交易的扩展能力^[60]。

4) 抵御双花攻击。因为每个代表节点都拥有生成区块的权力,一旦一个代表节点在规定的时间内没有生成区块或者多次产生无效的区块,那么这个代表节点会被其他代表节点投票剔除。

DPoS 共识机制的缺点:

1) 将一些代表节点的权力中心化。因为多个代表节点能够联合起来共同作恶,影响共识过程。

2) 代表节点可能遭受分布式拒绝服务攻击(Distributed Denial of Service, DDoS)攻击。因为攻击者可以单独对每一个代表节点发起攻击,从而影响代表节点在规定的时间内生产区块。

DPoS 共识机制与物联网场景的适应度:

目前,采用 DPoS 共识机制的区块链应用平台是 EOS 项目。EOS 全称 EOS. IO 软件,通过构建一个类似操作系统的体系结构的应用程序,来实现去中心化应用程序的性能扩展(每秒可以处理百万级交易)^[61]。EOS 项目的物联网应用是 EOSIoT,利用智能合约和射频识别(Radio Frequency Identification, RFID)系统传送的电子标签,实现 EOS 链服务于物联网场景中^[62]。

DPoS 共识机制完全应用于物联网场景中时会受到一些限制: DPoS 共识机制的共识过程虽然简单高效,但是去中心化程度不高,不适用于分布范围广的物联网设备;而且,当物联网设备少时,代表性不强。对 DPoS 共识机制改进的物联网区块链项目是 IoTeX,通过随机选择代表节点发布区块,进一步增强了去中心化和可扩展性方面的能力^[63]。图 8 是 IoTeX 架构,根链负责维护子链,子链直接用来连接物联网设备,当子链出现故障时,根链继续正常运行。

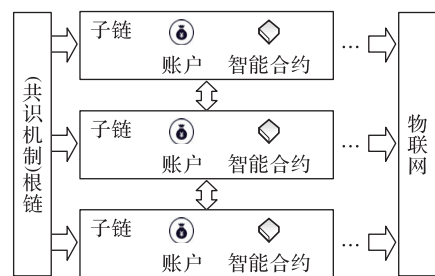


图 8 IoTeX 架构

Fig. 8 IoTeX architecture

2.1.4 PoA 共识机制

PoA 共识机制,即权威证明共识机制,在 PoS 的基础上进一步提高交易处理速度和可扩展性。该机制把节点分为普通节点和验证者,由验证者轮流对区块进行签名来判断是否为验证者。以下是 PoA 共识机制的工作原理^[64]:

1) 系统根据节点信誉选出一定数量的验证者。

2) 用户或者智能合约向系统发起交易请求。

3) 系统中的验证者接收到交易请求后,将交易打包到区

块中。

4) 当一个验证者将交易打包到区块并确认出块,在全网进行广播,验证者对区块进行签名,检查该节点是否为验证者。如果该节点被确认为验证者,则该区块是有效的。

5) 如果普通节点申请成为新的验证者,需要在验证者内部投票决定。验证者将根据投票数量是否大于 1/2,来对该节点进行判断。如果得到超过 1/2 的投票数,该节点将成为新的验证者。

PoA 共识机制的优点:

1) 交易处理速度快。由于计算能力要求低,不需要进行大量的计算,平均只需 5 s 即可生成区块^[65]。

2) 安全性高。由于该机制需要对验证者的身份进行确认,只有确认合格才能发布区块,所以验证者很难作恶,能够有效避免双花攻击。

PoA 共识机制的缺点:

1) 去中心化程度不高。因为参与共识过程的验证者数量较少。

2) 验证者作恶。如果验证者在共识过程中选择作恶,当前有效的解决方法是使用多重签名机制。

3) 隐私威胁。由于验证者身份是公开的,个人信息容易被泄露。

PoA 共识机制与物联网场景的适应度:

PoA 共识机制适用于解决物联网面临的处理能力弱、能量供应有限等问题,但是应用于物联网场景中会受到一个限制:与 DPoS 共识机制类似,由于去中心化程度不高,不适用于分布范围广的物联网设备。

2.1.5 PoC 共识机制

PoC 共识机制,即贡献证明共识机制,最早是由 CyberVein 团队提出的,被用来解决区块链中 51% 攻击问题。PoC 共识机制生产区块是通过贡献算法选择贡献最多的节点,贡献算法的计算公式^[66]:

$$MC = \sum_{n=1}^N \omega_2 * \frac{\Delta T^2}{\omega_1} + (kc)^3 + \sum_{m=1}^M \omega_3 + \omega_4 * (T_1 - T_2 - T_3) \quad (2)$$

其中:MC 代表贡献值; m 和 n 表示节点的数量; ω_1 影响复原的时间; ω_2 与节点的初始状态有关; ω_3 是一个常数值; ω_4 是节点在线时间系数; ΔT 是一个时间差; kc 表示节点状态的相关系数; T_1 代表共识结束时区块的时间戳; T_2 代表初始的时间戳; T_3 代表用户不在线的时间。

PoC 共识机制的优点:

1) 去中心化程度高。贡献证明算法每次选择贡献最高的节点生产区块,节点可以自由参与或者退出。

2) 安全可靠。采用贡献算法,以贡献量最大的节点生产区块,能够有效避免双花攻击。

PoC 共识机制的缺点:

1) 可扩展性差。随着交易量的增加,网络节点处理交易的性能没有改变。

PoC 共识机制与物联网场景的适应度:

PoC 共识机制虽然能够解决物联网存在的安全问题,但是会受到一个限制:随着物联网设备日益增加,扩展能力将受限。

2.1.6 Ouroboros 共识机制

基于 PoS 共识机制的 Ouroboros,被用来防止自私挖矿等攻击,保证系统安全性。在共识过程中,用 slot 表示划分的时间段,相邻的几个 slot 组成一个 epoch。

Ouroboros 共识机制的工作原理^[39]:

1) 获取当前 epoch 的公钥 vk 、权益 s 和初始化随机种子 ρ 的信息。

2) 由随机变量 $F(S, \rho, sl_j)$ 计算出领导者 U_i 负责生产区块的概率,其中: $S = \{(vk_1, s_1), (vk_2, s_2), \dots, (vk_n, s_n)\}$, sl_j 代表第 j 个 slot。如果超过当前 slot 的时间,放弃当前的 slot 进入下一个;同时, MPC 协议会产生一个随机种子 ρ 作为下一个 epoch 过程的函数信息。

3) 当前的 epoch 过程完成。

Ouroboros 共识机制的优点:

1) 安全性高。Ouroboros 对安全性做了严格的数学论证,提出了一种新的激励机制,让诚实节点的行为是一个近似纳什均衡,能够防止恶意攻击。

2) 交易处理速度快。耗费算力资源少,比 PoW 和 PoS 共识机制更高效,大约能够在 20 s 达成共识完成出块。

Ouroboros 共识机制的缺点:

1) 容易遭受 DDoS 攻击。由于 Ouroboros 共识机制能够提前知道谁是下一个出块者,攻击者可以单独发起对某一个出块者的恶意行为。

2) 去中心化程度低。在 Ouroboros 共识机制中,由于节点进行选择出块候选人与代币的分布有关,会影响去中心化程度。

Ouroboros 共识机制与物联网场景的适应度:

Ouroboros 共识机制提高了系统的安全性和交易速度,但由于后期去中心化程度的降低,不太适用于物联网场景中。

2.2 拜占庭类共识机制

拜占庭类共识机制,是以 BFT 为基础发展而来的。

2.2.1 PBFT 共识机制

PBFT 共识算法,即实用拜占庭容错共识机制,最早是由 Castro 和 Liskov 在 1999 年发表的论文中提出的^[67]。节点间为了达成共识需要处理大量的消息,作出决定所需的消息数量取决于拜占庭节点的估计数量,通常用 f 表示拜占庭节点数, n 表示网络中总节点数,使用 n 与 f 的关系在分布式系统中达成共识。比特币中 $n > 2f + 1$,如果拜占庭节点数超过全网总节点数的 1/2,会使区块链分叉,遭受双花攻击。而 PBFT 共识机制采用的是 $n > 3f + 1$,只要系统中正常工作的节点能够达到 2/3 就可以达成共识。PBFT 算法由请求、预准备、准备、提交和回复五个阶段组成,一次共识过程中存在一个主节点和若干个备份节点,如图 9 所示。PBFT 共识机制的工作过程^[67]如下:

1) 请求。网络中的主节点接收客户端发送的请求消息。

2) 预准备。主节点接收到消息后,计算预准备消息为(预准备, v, a, b),其中 v 表示视图编号, a 表示序列号, b 为消息的摘要。

3) 准备。备份节点接收到预准备消息后,计算准备消息为(准备, v, a, b, i), i 为节点编号。同时,每个节点需要检验消息的有效性:如果验证有效,就会把消息写到日志文件中。

4) 提交。每个节点在收到准备消息后,会对准备消息进

行验证,只有通过验证客户端才能收到回复。

5) 回复。若客户端收到的相同回复消息至少是 $f + 1$, 则表示请求结束; 否则, 重新发起请求。

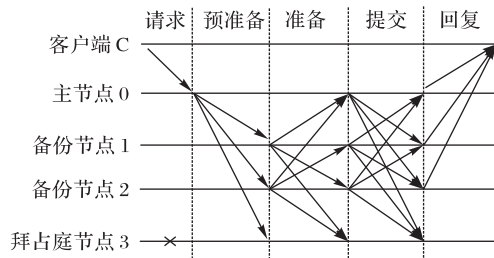


图 9 PBFT 算法流程

Fig. 9 PBFT algorithm flow

文献[68]针对 PBFT 共识过程中需要进行多次交互的问题, 提出了一种基于信用的改进 PBFT 共识机制的高效动态的 CPBFT 共识机制, 该机制能够减少交易确认的时间和节点与节点之间的通信次数, 提高了系统的性能。文献[69]提出采用多主节点的 PBFT 共识机制, 有效地降低了拜占庭节点作为主节点的可能性。

PBFT 共识机制的通信复杂度: 由于算法共识过程的五个阶段需要广播大量的消息, 所以 PBFT 共识机制的通信复杂度为 $O(n^2)$ 。

PBFT 共识机制的优点:

1) 共识效率高。在秒级内就能够生产区块, 效率高。

PBFT 共识机制的缺点:

1) 适用范围有限。PBFT 共识机制不适合采用公有链方式。

2) 可扩展性较差。在节点数增多后, 网络节点处理能力有限。

3) 容错性低。PBFT 共识机制要求节点总数 $n > 3f + 1$, 即系统拜占庭节点数不超过全网节点数的 $1/3$ 。

4) 容易遭受拒绝服务 (Denial of Service, DoS) 攻击。攻击者发起对一笔交易的拒绝服务攻击, 使消息得不到传播, 阻碍成功完成交易。

PBFT 共识机制与物联网场景的适应度:

PBFT 共识机制应用于物联网会受到一个限制: 由于 PBFT 共识机制的安全性会随着节点数量的增多而降低, 而物联网设备数量多, 不能够解决物联网设备的安全威胁问题。

2.2.2 Algorand 共识机制

Algorand 是一种将 PoS 与 BFT 共识机制结合的混合共识机制, 解决了 PoW 和 PoS 共识机制中存在的交易延迟以及 PBFT 共识机制的可扩展性问题^[70]。该共识机制以拜占庭协议为基础, 在共识过程结束时生成一个区块。因此, 交易确认时间比 PoW 和 PoS 共识机制短。而且, 在 Algorand 中会对每个用户分配一个权重, 该权重大小是根据用户所占资金数量决定的, 只要系统中有占 $2/3$ 资金以上的诚实节点, 就可以避免双花和分叉^[43]。此外, 通过随机选择领导者生产区块和委员会成员投票决议 (验证区块) 的方式实现共识过程, 解决了 PBFT 共识机制的可扩展性问题。

Algorand 共识过程^[28]: ①在当前轮中, 计算随机数的数值 $Q^{i-1} = \text{Hash}(SG_{c^{i-1}}(Q^{i-2}), i-1)$, Q^{i-1} 是随机种子, c^{i-1} 是上一轮的领导者, $SG_{c^{i-1}}(Q^{i-2})$ 表示 c^{i-1} 对 Q^{i-2} 的数字签名, $i-1$

表示轮数。②利用可验证随机函数 (Verifiable Random Function, VRF) 选出领导者和委员会成员。③当前被选中的领导者运行委员会内改进的拜占庭共识算法 BA★。

Algorand 共识机制的优点:

1) 交易处理速度快于 PoW 和 PoS 共识机制。Algorand 共识机制通过选取一部分节点完成共识过程, 提高了交易处理的效率; 而且采用改进的拜占庭共识算法 BA★, 以很小的通信量使委员会成员达成一致, 进一步缩短了共识时间。

2) 安全性高。由于采用了随机选取领导者和委员会成员的方式, 不能够确定谁是下一个区块的生产者, 有效地抵御了攻击者的任意行为。

Algorand 共识机制的缺点:

1) 没有激励机制。由于没有额外的奖励, 节点不会积极参与。

2) 安全隐患。网络用户重复使用领导者和委员会成员的私钥, 使私钥容易被泄露; 此外, 当系统中恶意节点占有 $2/3$ 以上资金时, 恶意节点可以发起任何行为的攻击。

3) 缺少惩罚机制。在共识过程中, 如果存在恶意节点, 缺乏惩罚机制将不能阻止恶意行为攻击。

Algorand 共识机制与物联网场景的适应度:

Algorand 共识机制应用于物联网场景中会受到两个限制: 一是隐私泄露问题。由于在共识过程中会重复使用私钥进行签名, 可能会泄露用户信息, 而物联网设备本身就存在隐私泄露问题; 二是当恶意节点掌握系统 $2/3$ 以上资金, 会破坏共识过程, 而物联网设备本身就on容易遭受安全威胁, 这将使 Algorand 共识机制应用于物联网中面临安全挑战。

2.2.3 Tendermint 共识机制

Tendermint 共识机制是基于 PoS 和 PBFT 的共识机制, 目的是为了解决无利害关系问题^[71]。Tendermint 共识机制受 PBFT SMR 算法和 DLS 算法的启发, 与 DLS 算法类似, Tendermint 以轮为单位进行, 每轮都有一个专用的提议者 (协调者或领导者), 流程进入新一轮, 作为正常处理的一部分^[72]。Tendermint 共识算法中有两个角色: 1) 验证者, 在生产区块阶段拥有投票的权力; 2) 提议者, 提议区块。其共识过程分为三个核心步骤和两个特殊步骤, 也称一轮。三个核心步骤是预投票、预提交、提交, 两个特殊步骤是提议者提议区块、生成新区块并且区块链高度加 1。

图 10 是共识过程^[71]: 首先随机选择一部分节点成为验证者, 然后从验证者中选择一个作为提议者, 当一个提议者完成对区块的提议后, 验证者将以循环的方式产生下一个提议者。提议者开始提议一个区块, 并向全网广播, 验证者在收到这个提议区块后, 验证该区块的有效性, 如果是有效区块, 就进入到投票环节。在投票过程中, 只有获得 $2/3$ 以上验证者同意的票数才能进入到生产区块的下一个阶段。投票过程分为三个阶段: 第一阶段预投票, 如果有 $2/3$ 以上的验证者投票同意则进入到第二阶段预提交。同样, 在预提交阶段如果有 $2/3$ 以上的验证者投票同意则进入到下一个阶段提交。最终, 提交产生一个新区块, 进入下一轮。此外, 如果提议者没有在设置的时间内提议区块, 系统不会等待而会生成一个空块, 进入下一阶段。在预投票阶段, 如果没有获得 $2/3$ 验证者投票的同意, 系统也不会等待会生成一个空块, 进入预提交阶段。在预提交阶段, 如果没有获得 $2/3$ 验证者投票的同意, 直接进入下一

轮,由下一个提议者开始提议区块。空块不含任何交易信息,不是一个真正意义上的区块。

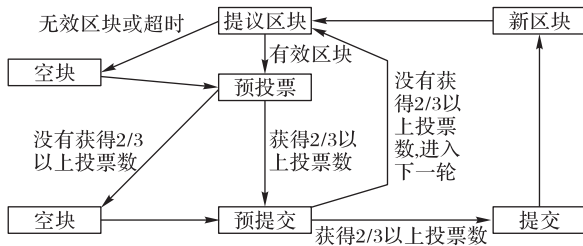


图 10 Tendermint 共识机制工作原理

Fig. 10 Working principle of Tendermint consensus mechanism

Tendermint 共识机制的通信复杂度:因为在投票阶段,需要网络中 2/3 以上的验证者投票同意才可以发送消息,所以,Algorand 共识机制的通信复杂度为 $O(n^2)$ 。

Tendermint 共识机制的优点:

1) 交易处理速度快。因为只要有验证者 2/3 的投票同意就能够生产区块,可以在短时间内处理大量的交易,系统交易吞吐量大^[73]。

2) 安全性高。Tendermint 共识机制对有恶意行为的节点采取罚款的方式,保证了交易信息的正确性。

Tendermint 共识机制的缺点:

1) 可能会遭受 DoS 攻击。由于以循环方式选择提议者,可以针对某一个验证者节点发起攻击,阻止交易完成。

2) 最多能容忍 1/3 拜占庭节点。因为 Tendermint 共识机制在共识过程中需要 2/3 以上验证者投票同意才能进入下一阶段,能够允许的最大拜占庭节点数是不超过全网总节点数的 1/3。

Tendermint 共识机制与物联网场景的适应度:

Tendermint 共识机制的高吞吐和低延迟提高了物联网的性能,特别是通过 Tendermint 实现的 Ethereum 被认为是物联网区块链结合的合适选择^[74]。相较于后面 DAG 类共识机制,当节点数量特别多时其交易处理速度、安全性以及可扩展性不如 IOTA 以及 Byteball 共识机制。

2.3 DAG 类共识机制

如果一个有向图从某个顶点出发,经过若干条边不能够回到原点,则这个图就是一个 DAG, DAG 结构是一种新型区块链技术^[75]。区块链在物联网的运用中存在很多问题,现有的共识机制 PoW 和 PoS 等,无法适用于物联网场景中,因此,提出了面向物联网场景的 DAG (也称为 Tangle) 技术。

2.3.1 IOTA 共识机制

IOTA 是针对物联网场景的应用而提出的一种新型区块链技术,物联网中的设备可以作为区块链的参与节点^[76]。在 IOTA 中,一个区块存放一个交易,图 11 是 IOTA 架构:每个新加入的交易将会被放在后面指向之前的两个交易。相较于链式区块链, IOTA 结构具有较好的可扩展性,同时能够处理大量的交易信息,减少了共识的时间。

为了解 IOTA 的运行过程,需要知道交易的权重和累积权重。 3^n 是权重, n 是非负整数。交易的累积权重是通过该交易的自身权重和其他直接或者间接验证这个交易的所有交易的自身权重相加求和得出的^[77]。图 11 中,一个字母代表一个交易,如 A、B,方框内左上角的数字是交易的累积权重,右下角的数字是交易的自身权重。交易 A 指向交易 B 和 C,那么 A 直

接验证了 B 和 C; 交易 A、B、C、D、E、F、G 最终都指向 H, 则交易 H 的累积权重的计算结果是 16。

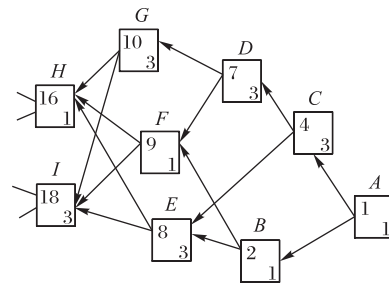


图 11 IOTA 架构

Fig. 11 IOTA architecture

IOTA 共识机制的工作原理:节点发起一个交易,需要验证 Tangle 中先前的两个交易,并将此交易指向他们。然后,通过花费少量的 PoW 计算权重和累积权重验证先前的两个交易。随着这个交易被之后新的交易直接或者间接验证,当交易的累积权重足够大时,则认为这个交易是有效的。利用累积权重大小来验证交易有效性,可能会受到双花攻击(典型的是寄生链攻击)。为此,引入了马尔可夫蒙特卡洛 (Markov Chain Monte Carlo, MCMC) 验证算法,节点先在累积权重 r 和 $2r$ 之间随机选择 m 个交易,然后以式(3)^[77]所示的概率向尖端交易 (tips) 进行离散时间无规行走走到 tips, 找到既定的目标:

$$p_{ij} = \exp(-\alpha(k_i - k_j)) \left(\sum_{z:z \rightarrow i} \exp(-\alpha(k_i - k_z)) \right)^{-1} \quad (3)$$

其中: $\alpha > 0$, $j \rightarrow i$ 代表由 i 转到 j 。

IOTA 共识机制的优点:

1) 高吞吐量。在 DAG 结构下,只需要花费少量的 PoW 来验证先前的两笔交易,从而能够并发处理大量的交易,减少了生成区块的时间。

2) 可扩展性好。随着交易数量的不断增多, IOTA 的处理速度和扩展能力得到相应的提高;而且,交易量越大,系统变得越稳定,安全性也会得到相应的提高。

IOTA 共识机制的缺点:

1) 交易时间不确定。由于 IOTA 的交易验证是通过计算累积权重的方式,在交易量比较少时,容易出现交易长时间得不到确认。

2) 安全性降低。在节点数过少时,容易遭受双花攻击,系统安全性不如链式结构。

IOTA 共识机制与物联网场景的适应度:

IOTA 共识机制应用于物联网需要解决一个技术挑战:由于物联网设备具有分布范围广的特征,当在一定范围内物联网设备比较少而且分散时,需要解决 IOTA 共识机制本身存在的交易时间不确认、容易遭受双花攻击的难题。但是相比前面介绍的几种共识算法,随着物联网设备呈指数级的增长,它在速度、安全、可扩展性方面显然更好,未来会适用于物联网场景中。

2.3.2 Byteball 共识机制

Byteball 是一个去中心化的系统,它可以对货币、股权等数据进行防篡改存储^[78]。单元包括要存储的交易信息,他们之间相互链接,每一个新加入的单元直接或间接地被越来越多的包含哈希值的后续单元所确认。如图 12 所示,顶点表示

单元,一旦一个单元被确认,新的单元随之而来。

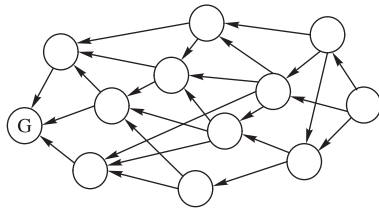


图 12 Byteball 结构

Fig. 12 Byteball Structure

文献[78]介绍了 Byteball 共识算法的原理:在 Byteball 中,引入 12 个见证人,见证人用来记录存储单元。当用户发起交易时,由一个顶端单元开始通过选择算法选择一个最优父单元,直到构成一条到达创世单元的最佳路径称为主链。DAG 的每个顶端单元直接或者间接到达主链,把主链编号为 *MCI*,创世单元的 *MCI* 设置为 0,向后逐渐加 1,主链上最先直接或者间接单元的 *MCI* 是不在主链上的单元的 *MCI*。在发生双重支付时,*MCI* 小的存储单元被认为是有效的。

Byteball 共识机制的优点:

- 1) 安全性强。Byteball 共识机制引入了见证人的方式,并且通过选择算法来创建主链,提高了系统的安全性。
- 2) 可扩展性好。与 IOTA 共识机制类似,交易量越多,系

统越稳定。

Byteball 共识机制的缺点:

- 1) 当存储单元数量比较少时,可能会发生双花问题,因为存储单元太少,使一些交易长期得不到确认,此时攻击者可以发起交易,制造另一条链,并且让其成为主链;而且,交易确认的时间也是不确定的。
- 2) 牺牲了去中心化程度。由于引入了 12 个见证人,没有实现完全去中心化。
- 3) 交易时间不确定。当系统中交易量较少时,会有一些交易长期得不到后续单元的确认。

Byteball 共识机制与物联网场景的适应度:

Byteball 和 IOTA 共识机制相较于链式数据结构来说,能够并发处理大量的交易,同时提高了扩展能力,更适用于物联网场景中。

2.3.3 DAG 类共识机制分析对比

IOTA 和 Byteball 共识机制,有很多的共性,同时也会有很多的区别。表 1 是 DAG 类共识机制对比,Byteball 与 IOTA 的主要区别是:①Byteball 比 IOTA 多了交易费用;②IOTA 相较于 Byteball 用到了少量的 PoW 来进行验证工作;③IOTA 新发起的交易指向先前的两个交易,而 Byteball 能够指向先前的三个交易。

表 1 DAG 类共识机制对比

Tab. 1 Comparison of DAG consensus mechanisms

DAG 类共识机制	共识方式	共性	区别
Byteball	使用选择算法	交易吞吐量大,可扩展性好。当交易量较少时,去中心化程度低于链式结构区块链,会遭受双花攻击以及交易时间不确定等问题,这些是制约 DAG 应用于物联网的重要因素	需要交易费用,同时引入见证人牺牲一定程度的去中心化
IOTA	花费少量的 PoW 来计算累积权重		利用协调器进行交易信息安全确认,而协调器执行效率低

2.4 共识机制分析

研究区块链共识机制,需要对影响区块链共识机制的因素进行分析并做一些相应的比较。其影响因素如下:

- 1) 去中心化程度。去中心化程度决定了参与共识节点的权力是掌握在少数人手里还是多数人手里。
- 2) 交易处理速度。也叫交易吞吐量,是指在给定的时间段内处理交易的数量。
- 3) 交易确认延迟是指交易从发起到生成区块的时间也就是交易的响应时间^[79]。
- 4) 安全性。共识机制中的安全性指的是在共识过程中,其所能够承受恶意节点发起任意行为攻击的能力。
- 5) 可扩展性是指网络节点处理交易的能力,评价可扩展性好坏的标准是随着交易数量的增加,系统中节点处理交易的能力能否得到相应的提高^[80]。

表 2 列出了各种共识机制的算法种类、提出年份、吞吐量、响应时间、容错性和应用平台。表 3 展示了各种共识机制在是否容易分叉、交易处理速度、交易确认延迟、安全性以及可扩展性上的优缺点。通过表 2 和表 3 直观的对各种共识机制进行对比,分析面向物联网应用的共识机制。

PoW 共识机制采用公有链,每个节点都可以参与,因而去中心化程度高。表 3 表明 PoW 共识机制容易产生分叉,进而如果攻击者掌握了全网 51% 的算力,会发起 51% 攻击;并且, PoW 共识机制也会遭受其他类型的攻击,如日蚀攻击、自私挖矿攻击等。通常情况下, PoW 共识机制产生一个区块需要花费 10 min,会带来高延迟问题,而对于本身要求低延迟的物联

网设备显然是不适用的。

相较于 PoW 共识机制, PoS 共识机制的出块时间为 1 min,而且依靠币龄来产生区块,不需要消耗大量的能量;但由于 PoS 共识机制容易遭受 51% 攻击以及无利害关系问题攻击,使系统安全性得不到保障。PoS 共识机制虽然提高了交易处理的速度,但是在安全性和可扩展性上没有任何的优势,不能解决物联网面临的现状问题。

DPoS 共识机制交易处理速度比 PoW 和 PoS 更快,不容易产生分叉,安全性比 PoW 和 PoS 更好;缺点是只有少量的代表节点参与共识过程,而物联网设备具有分布范围广的特点,节点太少不具有代表性。因此, DPoS 共识机制不能够直接应用于物联网设备,只能通过改进 DPoS 共识机制使其适用于物联网设备。

PoA 共识机制具有交易处理速度快、共识时间短、扩展性好的特点;但算法实现起来比较困难,而且还存在隐私泄露问题,给物联网与区块链的结合带来困扰。

PoC 共识机制不容易产生分叉,其安全性高;但是由于可扩展性比较差很难适合数量不断增加的物联网设备。

Ouroboros 是一个可证明其安全性高的共识机制,其交易处理速度比 PoW 和 PoS 共识机制快;但由于后期去中心化程度的降低,会影响其在物联网场景中的使用。

PBFT 共识机制的优点是不容易产生分叉,交易处理速度快。但是,这种共识机制容易遭受 DoS 的攻击;而且, PBFT 共识机制只能容忍不超过 1/3 的拜占庭节点,随着节点数量的增

加,在安全性上得不到保障,不能解决物联网的安全问题。

Algorand 共识机制具有交易处理速度快的优点。但是,容易遭受系统中占有 2/3 资金以上的不诚实节点攻击;而且,当物联网设备的数量特别多时,可扩展性方面存在不足,会给物联网和区块链的结合带来麻烦。

Tendermint 共识机制具有低延迟和可扩展性好的优点,对于物联网区块链结合来说是适合的。但是,如果故障节点或恶意节点数超过 1/3 以上时,安全性则得不到保证;而且,随着物联网设备的大量增多,在交易处理速度和可扩展性上不如 IOTA 和 Byteball 共识机制。

IOTA 和 Byteball 共识机制是一种新型加密技术,其在交易吞吐量和可扩展性上比传统的区块链共识机制有了很大的改进;但是在交易数量过少的情况下,IOTA 和 Byteball 的安全性低,而且容易发生交易长时间得不到确认等问题。

根据共识机制在去中心化程度、交易处理速度、交易确认延迟、安全性和可扩展性方面对物联网产生的影响,要因地制宜地选择适用于物联网场景的共识机制。在大多数情况下,PoW、PoS 共识机制不适合于物联网场景中;DPoS 由于节点数量太少,不适用于分布范围广的物联网体系;PBFT 在安全性要求低的物联网场景中可以使用。随着物联网设备的增多,PoC、Ouroboros、Algorand、Tendermint、POA 和 PoC 在吞吐量和可扩展性上不如 IOTA 和 Byteball,IOTA 和 Byteball 所具有的特点更适用于物联网场景。文献[81]研究了 PoW、PoS 共识机制和利用 DAG 技术的共识机制,根据生成区块的平均时间、交易确认的延迟、每秒处理交易的数量(Transaction Per Second, TPS)和确认失败的概率评估共识算法的性能,结果表明 PoW 和 PoS 对网络资源的变化更敏感,而 DAG 对网络负载条件更为敏感。

表 2 共识机制对比

Tab. 2 Comparison of consensus mechanisms

共识机制分类	算法种类	提出年份	吞吐量	响应时间	容错性	应用平台	
证明类	PoW	PoW	1999	≈7 TPS	10 min	1/2	Bitcoin
	PoS	PoS	2011	≥25 TPS	1 min	1/2	Peercoin
	DPoS	PoS	2014	≥300 TPS	≈3 s	1/2	EOS
	PoA	PoS	2017	/	5 s	1/2	PoA. Network
	PoC	PoC	2017	/	/	1/2	CyberVein
	Ouroboros	PoS	2017	/	≈20 s	1/2	Cardano
拜占庭类	PBFT	BFT	1999	数千 TPS	秒级	1/3	Hyperledger Fabric
	Algorand	PoS+BFT	2017	≈900 TPS	<1 min	1/3	Algorand
	Tendermint	PoS+PBFT	2014	/	/	1/3	Ethermint
DAG 类	IOTA	PoW	2018	7~12 TPS	几分钟到几小时	1/2	IOTA
	Byteball	/	2016	/	/	1/2	Byteball

表 3 共识机制优缺点对比

Tab. 3 Comparison of advantages and disadvantages of consensus mechanisms

共识机制分类	是否容易分叉	交易处理速度	交易确认延迟	安全性	可扩展性	
证明类	PoW	是	慢	高	容易遭受 51% 攻击、日蚀攻击、自私挖矿攻击	差
	PoS	是	快	低	容易遭受 51% 攻击、无利害关系问题攻击	差
	DPoS	否	快	低	存在权力中心化问题,容易遭受 DDoS 攻击	好
	PoA	是	快	低	存在验证者节点作恶、隐私泄露问题	好
	PoC	否	快	低	强	差
	Ouroboros	/	快	低	容易遭受 DDoS 攻击	好
拜占庭类	PBFT	否	快	低	容易遭受超过 1/3 拜占庭节点攻击、容易遭受 DoS 攻击	差
	Algorand	否	快	低	容易遭受系统中有 2/3 资金以上的恶意节点攻击	较好
	Tendermint	否	快	低	容易遭受 DoS 攻击	好
DAG 类	IOTA	是	快	/	节点数比较少时容易遭受双花攻击	好
	Byteball	是	快	/	节点数比较少时容易遭受双花攻击	好

3 结语

物联网技术实现了物与物之间的互联,推动了生产力的发展。但是,物联网存在中心机构运行成本高、可扩展性差和安全性低等缺陷,限制了物联网的发展。而区块链具有去中心化、开放性、共识机制和不可篡改等特点,刚好弥补了物联网的缺陷。在区块链架构中,物联网设备利用区块链的特点,实现数据的安全存储^[82],将区块链应用于物联网场景中,被认为是区块链 3.0 版本^[83]。文献[84]提出物联网能够实现物与物之间相互通信,但在数据隐私和安全方面还存在缺陷,利用区块链去中心化的特点,提供可靠的数据共享环境,实现物联网系统的透明性、安全性和隐私性等。共识机制是区块链技术的核心要素,将影响物联网的发展。文献[85]针对物联网

面临的设备数量多、结构复杂、计算能力弱等问题,提出利用区块链的去中心化和共识机制的特点,实现物联网与区块链的有效结合。本文通过对各种共识机制的优缺点进行对比,发现当需要处理大量交易时,IOTA 和 Byteball 比其他共识机制在交易处理速度和可扩展性等方面更有优势,更适用于物联网场景中。虽然 IOTA 和 Byteball 已经开始应用于物联网场景,但是仍然存在很多的问题:

1) 去中心化程度不彻底。IOTA 共识机制采用协调器来控制和处理信息,而 Byteball 共识机制引入见证人来维护网络信息,因此他们都没有实现完全去中心化。

2) 安全问题。当交易数量较少时,IOTA 和 Byteball 共识机制容易遭受双花攻击,而且交易可能长时间得不到确认,将他们应用于物联网场景,需要解决这一问题。

3)信息存储。由于物联网设备的存储能力有限,在IOTA和Byteball共识机制应用于物联网设备时,需要解决存储问题。本文通过分析区块链共识机制的工作原理与优缺点以及与物联网的适应度,希望给未来物联网区块链的融合带来一些启示。

参考文献 (References)

- [1] LI S, XU L D, ZHAO S. 5G Internet of things: a survey [J]. *Journal of Industrial Information Integration*, 2018, 10: 1-9.
- [2] 何正源,段田田,张颖,等. 物联网中区块链技术的应用与挑战 [J]. *应用科学学报*, 2020, 38(1): 22-33. (HE Z Y, DUAN T T, ZHANG Y, et al. Blockchain in internet of things: application and challenges [J]. *Journal of Applied Sciences*, 2020, 38 (1) : 22-33.)
- [3] HUANG J, KONG L, CHEN G, et al. B-IoT: blockchain driven internet of things with credit-based consensus mechanism [C]// *Proceedings of the 39th International Conference on Distributed Computing Systems*. Piscataway: IEEE, 2019: 1348-1357.
- [4] CHRISTIDIS K, DEVETSIKIOTIS M. Blockchains and smart contracts for the internet of things [J]. *IEEE Access*, 2016, 4: 2292-2303.
- [5] COUTO DA SILVA F J, DAMSGAARD S B, MOUSING SORENSEN M A, et al. Analysis of blockchain forking on an Ethereum network [C]// *Proceedings of the 25th European Wireless Conference*. Berlin: VDE Verlag GMBH, 2019: 1-6.
- [6] ANTONOPOULOS A M. 精通区块链编程:加密货币原理、方法和应用开发(第2版) [M]. 郭理靖,李国鹏,李卓,译. 北京:机械工业出版社, 2019: 156. (ANTONOPOULOS A M. *Mastering Bitcoin* (2nd ed) [M]. GUO L J, LI G P, LI Z, translated. Beijing: China Machine Press, 2019: 156.)
- [7] 朱岩,王巧石,秦博涵,等. 区块链技术及其研究进展 [J]. *工程科学学报*, 2019, 41(11): 1361-1373. (ZHU Y, WANG Q S, QIN B H, et al. Survey of blockchain technology and its advances [J]. *Chinese Journal of Engineering*, 2019, 41(11): 1361-1373.)
- [8] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. [2019-12-02]. <https://bitcoin.org/bitcoin.pdf>.
- [9] YU S, LV K, SHAO Z, et al. A high performance blockchain platform for intelligent devices [C]// *Proceedings of the 1st IEEE International Conference on Hot Information-Centric Networking*. Piscataway: IEEE, 2018: 260-261.
- [10] UPADHYAY N. Demystifying blockchain: a critical analysis of challenges, applications and opportunities [J]. *International Journal of Information Management*, 2020, 54: No. 102120.
- [11] ZHENG Z, XIE S, DAI H, et al. An overview of blockchain technology: architecture, consensus, and future trends [C]// *Proceedings of the 6th IEEE International Congress on Big Data*. Piscataway: IEEE, 2017: 557-564.
- [12] MÜNSING E, MATHER J, MOURA S. Blockchains for decentralized optimization of energy resources in microgrid networks [C]// *Proceedings of the 2017 IEEE Conference on Control Technology and Applications*. Piscataway: IEEE, 2017: 2164-2171.
- [13] 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. (YUAN Y, WANG F Y. Blockchain: the state of the art and future trends [J]. *Acta Automatica Sinica*, 2016, 42(4): 481-494.)
- [14] WALSH C, O'REILLY P, GLEASURE R, et al. Understanding manager resistance to blockchain systems [J/OL]. *European Management Journal* [2020-12-02]. <https://doi.org/10.1016/j.emj.2020.10.001>.
- [15] 于戈,聂铁铮,李晓华,等. 区块链系统中的分布式数据管理技术——挑战与展望 [J]. *计算机学报*, 2021, 44(1): 28-54. (YU G, NIE T Z, LI X H, et al. The challenge and prospect of distributed data management techniques in blockchain systems [J]. *Chinese Journal of Computers*, 2021, 44(1): 28-54.)
- [16] PILKINGTON M. Blockchain technology: principles and applications [M]// OLLEROS F X, ZHEGU M. *Research Handbook on Digital Transformations*. Northampton, MA: Edward Elgar Publishing, 2016: 225-253.
- [17] 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. Blockchain principle and its core technology [J]. *Chinese Journal of Computers*, 2021, 44(1): 84-131.)
- [18] SZABO N. Formalizing and securing relationships on public networks [J]. *First Monday*, 1997, 2(9): No. 548.
- [19] AGGARWAL S, KUMAR N. Blockchain 2.0: smart contracts [J/OL]. *Advances in Computers* [2020-12-02]. <https://doi.org/10.1016/bs.adcom.2020.08.015>.
- [20] WANG Y, GAO Y, LI Y, et al. A worker-selection incentive mechanism for optimizing platform-centric mobile crowdsourcing systems [J]. *Computer Networks*, 2020, 171: No. 107144.
- [21] WANG Y, CAI Z, ZHAN Z, et al. Walrasian equilibrium-based multiobjective optimization for task allocation in mobile crowdsourcing [J]. *IEEE Transactions on Computational Social Systems*, 2020, 7(4): 1033-1046.
- [22] WANG Y, CAI Z, ZHAN Z, et al. An optimization and auction-based incentive mechanism to maximize social welfare for mobile crowdsourcing [J]. *IEEE Transactions on Computational Social Systems*, 2019, 6(3): 414-429.
- [23] BUTERIN V. A next-generation smart contract and decentralized application platform [EB/OL]. [2020-01-02]. <https://whitepaperdatabase.com/wp-content/uploads/2017/09/Ethereum-ETH-whitepaper.pdf>.
- [24] CACHIN C. Architecture of the Hyperledger blockchain Fabric [EB/OL]. [2020-01-09]. https://www.zurich.ibm.com/dcc/papers/cachin_dcc.pdf.
- [25] WANG B, HU Y, LI S, et al. A blockchain consensus mechanism for educational administration system [C]// *Proceedings of the 2nd International Conference on Electronics Technology*. Piscataway: IEEE, 2019: 603-608.
- [26] 冯翔,刘涛,吴寿鹤,等. 区块链开发实战: Hyperledger Fabric 关键技术与案例分析 [M]. 北京:机械工业出版社, 2018: 42-46. (FENG X, LIU T, WU S H, et al. Blockchain in action: key technology and case analysis for Hyperledger Fabric [M]. Beijing: China Machine Press, 2018: 42-46.)
- [27] LAMPORT L, SHOSTAK R, PEASE M. The Byzantine generals problem [J]. *ACM Transactions on Programming Languages and Systems*, 1982, 4(3): 382-401.
- [28] 刘懿中,刘建伟,张宗洋,等. 区块链共识机制研究综述 [J]. *密码学报*, 2019, 6(4): 395-432. (LIU Y Z, LIU J W, ZHANG Z Y, et al. Overview on blockchain consensus mechanisms [J]. *Journal of Cryptologic Research*, 2019, 6(4): 395-432.)
- [29] CROSBY M, NACHIAPPAN, PATTANAYAK P, et al. Blockchain technology: beyond bitcoin [J]. *Applied Innovation Review*, 2016(2): 6-19.

- [30] JUELS A, KALISKI B S. PORs: proofs of retrievability for large files [C]// Proceedings of the 14th ACM Conference on Computer and Communications Security. New York: ACM, 2007: 584-597.
- [31] ATENIESE G, KAMARA S, KATZ J. Proofs of storage from homomorphic identification protocols [C]// Proceedings of the 15th International Conference on the Theory and Application of Cryptology and Information Security, LNCS 5912. Berlin: Springer, 2009: 319-333.
- [32] LAMPORT L. Time, clocks, and the ordering of events in a distributed system [J]. Communications of the ACM, 1978, 21(7): 558-565.
- [33] GUETA G G, ABRAHAM I, GROSSMAN S, et al. SBFT: a scalable and decentralized trust infrastructure [EB/OL]. [2020-02-06]. <https://arxiv.org/pdf/1804.01626.pdf>.
- [34] VERONESE G S, CORREIA M, BESSANI A N, et al. Efficient byzantine fault-tolerance [J]. IEEE Transactions on Computers, 2013, 62(1): 16-30.
- [35] MILLER A, XIA Y, CROMAN K, et al. The honey badger of BFT protocols [C]// Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2016: 31-42.
- [36] LAMPORT L. The part-time parliament [J]. ACM Transactions on Computer Systems, 1998, 16(2): 133-169.
- [37] LEMON B, MANCE H, PAUL M. Hedera: a governing council and public hashgraph network [EB/OL]. [2020-02-12]. <https://www.hedera.com/hh-whitepaper-v1.4-181017.pdf>.
- [38] CAO Z, LONG M, WANG J, et al. HashNet: deep learning to Hash by continuation [C]// Proceedings of the 2017 IEEE International Conference on Computer Vision. Piscataway: IEEE, 2017: 5609-5618.
- [39] KIAYIAS A, RUSSELL A, DAVID B, et al. Ouroboros: a provably secure proof-of-stake blockchain protocol [C]// Proceedings of the 2017 Annual International Cryptology Conference, LNCS 10401. Cham: Springer, 2017: 357-388.
- [40] JIANG D. The construction of smart city information system based on the internet of things and cloud computing [J]. Computer Communications, 2020, 150: 158-166.
- [41] SHARIATZADEH N, LUNDHOLM T, LINDBERG L, et al. Integration of digital factory with smart factory based on internet of things [J]. Procedia CIRP, 2016, 50: 512-517.
- [42] ALAA M, ZAIDAN A A, ZAIDAN B B, et al. A review of smart home applications based on internet of things [J]. Journal of Network and Computer Applications, 2017, 97: 48-65.
- [43] MAKHDOOM I, ABOLHASAN M, ABBAS H, et al. Blockchain's adoption in IoT: the challenges, and a way forward [J]. Journal of Network and Computer Applications, 2019, 125: 251-279.
- [44] 孙利民, 张书钦, 李志, 等. 无线传感器网络理论及应用 [M]. 北京: 清华大学出版社, 2018: 18-22. (SUN L M, ZHANG S Q, LI Z, et al. of Wireless Sensor Networks: Theory and Application [M]. Beijing: Tsinghua University Press, 2018: 18-22.)
- [45] LIU T, WANG Y, LI Y, et al. Privacy protection based on stream cipher for spatiotemporal data in IoT [J]. IEEE Internet of Things Journal, 2020, 7(9): 7928-7940.
- [46] 史锦山, 李茹. 物联网下的区块链访问控制综述 [J]. 软件学报, 2019, 30(6): 1632-1648. (SHI J S, LI R. Survey of blockchain access control in internet of things [J]. Journal of Software, 2019, 30(6): 1632-1648.)
- [47] MACKENZIE B, FERGUSON R I, BELLEKENS X. An assessment of blockchain consensus protocols for the internet of things [C]// Proceedings of the 2018 International Conference on Internet of Things, Embedded Systems and Communications. Piscataway: IEEE, 2018: 183-190.
- [48] PAN J, YANG Z. Cybersecurity challenges and opportunities in the new edge computing+ IoT world [C]// Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization. New York: ACM, 2018: 29-32.
- [49] 中国通信标准化协会物联网技术委员会发布《“物联网+区块链”应用与发展白皮书》[J]. 电信工程技术与标准化, 2019, 32(11): 11. (White paper on application and development of "internet of things + blockchain" issued by internet of things Technical Committee of China Communications Standardization Association [J]. Telecommunication Engineering Technology and Standardization, 2019, 32(11): 11.)
- [50] NOVO O. Blockchain meets IoT: an architecture for scalable access management in IoT [J]. IEEE Internet of Things Journal, 2018, 5(2): 1184-1195.
- [51] 任彦冰, 李兴华, 刘海, 等. 基于区块链的分布式物联网信任管理方法研究 [J]. 计算机研究与发展, 2018, 55(7): 1462-1478. (REN Y B, LI X H, LIU H, et al. Blockchain-based trust management framework for distributed internet of things [J]. Journal of Computer Research and Development, 2018, 55(7): 1462-1478.)
- [52] 朱建明, 张沁楠, 高胜. 区块链关键技术及其应用研究进展 [J]. 太原理工大学学报, 2020, 51(3): 321-330. (ZHU J M, ZHANG Q N, GAO S. Research progress of blockchain key technologies and their application [J]. Journal of Taiyuan University of Technology, 2020, 51(3): 321-330.)
- [53] DWORK C, NAOR M. Pricing via processing or combatting junk mail [C]// Proceedings of the 12th Annual International Cryptology Conference, LNCS 740. Berlin: Springer, 1992: 139-147.
- [54] DOUCEUR J R. The sybil attack [C]// Proceedings of the 2002 International Workshop on Peer-To-Peer Systems, LNCS 2429. Berlin: Springer, 2002: 251-260.
- [55] 吴梦宇, 朱国胜, 吴善超. 基于工作量证明和权益证明改进的区块链共识机制 [J]. 计算机应用, 2020, 40(8): 2274-2278. (WU M Y, ZHU G S, WU S C. Improved consensus mechanism of blockchain based on proof-of-work and proof-of-stake [J]. Journal of Computer Applications, 2020, 40(8): 2274-2278.)
- [56] WANG Q, HUANG J, WANG S, et al. A comparative study of blockchain consensus algorithms [J]. Journal of Physics: Conference Series, 2020, 1437: No. 012007.
- [57] Bitcoin Wiki. Proof of stake [EB/OL]. [2020-02-18]. https://en.bitcoin.it/wiki/Proof_of_Stake.
- [58] BAMAKAN S M H, MOTAVALI A, BONDARTI A B. A survey of blockchain consensus algorithms performance evaluation criteria [J]. Expert Systems with Applications, 2020, 154: No. 113385.
- [59] LARIMER D. DPoS consensus algorithm-the missing white paper

- [R/OL]. [2020-02-19]. <https://hivean.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper>.
- [60] 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.)
- [61] Block. one. EOS. IO technical white paper [R/OL]. [2020-02-20]. <https://cdn.bitturk.com/whitepaper/eos.pdf>.
- [62] 宋琪杰,陈铁明,陈园,等. 面向物联网区块链的共识机制优化研究[J]. 电信科学, 2020, 36(2): 1-12. (SONG Q J, CHEN T M, CHEN Y, et al. Research on consensus mechanism optimization for IoT blockchain [J]. Telecommunication Science, 2020, 36(2): 1-12.)
- [63] FAN X, CHAI Q. Roll-DPoS: a randomized delegated proof of stake scheme for scalable blockchain-based internet of things systems [C]// Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services. New York: ACM, 2018: 482-484.
- [64] 李国,张洁慧,臧金梅. 面向解决民航虚占座位的改进PoA共识机制区块链系统研究[J]. 计算机应用研究, 2020, 37(11): 3368-3372, 3377. (LI G, ZHANG J H, ZANG J M. Research on improved POA consensus mechanism blockchain system for solving empty seats in civil aviation [J]. Application Research of Computers, 2020, 37(11): 3368-3372, 3377.)
- [65] ALGHAMDI T A, ALI I, JAVAID N, et al. Secure service provisioning scheme for lightweight IoT devices with a fair payment system and an incentive mechanism based on blockchain [J]. IEEE Access, 2020, 8: 1048-1061.
- [66] 王建宇. 基于区块链的数据保全系统设计与实现[D]. 北京:北京工业大学, 2019: 48-52. (WANG J Y. Design and implementation of data preservation system based on blockchain [D]. Beijing: Beijing University of Technology, 2019: 48-52.)
- [67] CASTRO M, LISKOV B. Practical Byzantine fault tolerance [C]// Proceedings of the 3rd Symposium on Operating Systems Design and Implementation. Berkeley: USENIX Association, 1999: 173-186.
- [68] 徐治理,封化民,刘飏. 一种基于信用的改进PBFT高效共识机制[J]. 计算机应用研究, 2019, 36(9): 2788-2791. (XU Z L, FENG H M, LIU B. Improved PBFT efficient consensus mechanism based on credit [J]. Application Research of Computers, 2019, 36(9): 2788-2791.)
- [69] 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.)
- [70] GILAD Y, HEMO R, MICALI S, et al. Algorand: scaling Byzantine agreements for cryptocurrencies [C]// Proceedings of the ACM SIGOPS 26th Symposium on Operating Systems Principles. New York: ACM, 2017: 51-68.
- [71] BUCHMAN E. Tendermint: Byzantine fault tolerance in the age of blockchains [D]. Ontario: University of Guelph, 2016: 18-34.
- [72] BUCHMAN E, KWON J, MILOSEVICZ Z. The latest gossip on BFT consensus [EB/OL]. [2020-03-20]. <https://arxiv.org/pdf/1807.04938.pdf>.
- [73] FERDOUS M S, CHOWDHURY M J M, COLMAN A, et al. Blockchain consensus algorithms: a survey [EB/OL]. [2020-03-21]. <https://arxiv.org/pdf/2001.07091.pdf>.
- [74] JIANG Y, WANG C, WANG Y, et al. A cross-chain solution to integrating multiple blockchains for IoT data management [J]. Sensors, 2019, 19(9): No. 2042.
- [75] BAI C. State-of-the-art and future trends of blockchain based on DAG structure [C]// Proceedings of the 2018 International Workshop on Structured Object-oriented Formal Language and Method, LNCS 11392. Cham: Springer, 2018: 183-196.
- [76] 高政风,郑继来,汤舒扬,等. 基于DAG的分布式账本共识机制研究[J]. 软件学报, 2020, 31(4): 1124-1142. (GAO Z F, ZHENG J F, TANG S Y, et al. State-of-the-art survey of consensus mechanisms on DAG-based distributed ledger [J]. Journal of Software, 2020, 31(4): 1124-1142.)
- [77] POPOV S. The tangle [EB/OL]. [2020-03-25]. https://assets.ctfassets.net/r1dr6vzfhev/214uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf.
- [78] CHURYUMOV A. Byteball: a decentralized system for storage and transfer of value [EB/OL]. [2020-03-28]. <https://byteball.org/Byteball.pdf>.
- [79] 喻辉,张宗洋,刘建伟. 比特币区块链扩容技术研究[J]. 计算机研究与发展, 2017, 54(10): 2390-2403. (YU H, ZHANG Z Y, LIU J W. Research on scaling technology of bitcoin blockchain [J]. Journal of Computer Research and Development, 2017, 54(10): 2390-2403.)
- [80] CROMAN K, DECKER C, EVAL I, et al. On scaling decentralized blockchains [C]// Proceedings of the 2016 International Conference on Financial Cryptography and Data Security, LNCS 9604. Berlin: Springer, 2016, : 106-125.
- [81] CAO B, ZHANG Z, FENG D, et al. Performance analysis and comparison of PoW, PoS and DAG based blockchains [J]. Digital Communications and Networks, 2020, 6(4): 480-485.
- [82] CHI J, LI Y, HUANG J, et al. A secure and efficient data sharing scheme based on blockchain in industrial internet of things [J]. Journal of Network and Computer Applications, 2020, 167: No. 102710.
- [83] DI FRANCESCO MAESA D, MORI P. Blockchain 3.0 applications survey [J]. Journal of Parallel and Distributed Computing, 2020, 138: 99-114.
- [84] THAKORE R, VAGHASHIYA R, PATEL C, et al. Blockchain-based IoT: a survey [J]. Procedia Computer Science, 2019, 155: 704-709.
- [85] WANG X, ZHA X, NI W, et al. Survey on blockchain for internet of things [J]. Computer Communications, 2019, 136: 10-29.
- TIAN Zhihong**, born in 1993, M. S, candidate. His research interests include internet of things, blockchain.
- ZHAO Jindong**, born in 1974, Ph. D., associate professor. His research interests include internet of things, blockchain.