第 46 卷 第 12 期 计 算 机 工 程 2020 年 12 月
Vol. 46 No. 12 Computer Engineering December 2020

·热点与综述· 文章编号:1000-3428(2020)12-0001-11 文献标志码:A 中图分类号:TP302.8

区块链共识机制综述

谭敏生,杨 杰,丁 琳,李行健,夏石莹

(南华大学 计算机学院,湖南 衡阳 421001)

摘 要: 区块链能够有效融合物联网、5G、大数据和人工智能等技术,在新型基础设施建设中具有重要作用。共识机制作为区块链的核心技术,能够保障区块链数据库的一致性和正确性,从而决定区块链的安全性、扩展性、吞吐量等相关性能。根据区块链共识机制的技术路线,将其细分为 3 类单一共识机制和 6 类混合共识机制。从原理实现角度,系统描述共识机制的理论技术,归纳节点达成一致所需的运算操作并评价共识机制的优缺点。从工程应用角度,具体分析共识机制的应用情况,介绍区块链项目并对比共识机制的关键性能。针对现有共识机制研究中存在的能耗与效率问题给出相应的解决方案,并对其奖惩制度、网络分片与存储分片技术等下一步研究方向进行展望。

关键词: 区块链;共识机制;拜占庭容错;分布式系统;一致性

开放科学(资源服务)标志码(OSID):

中文引用格式: 谭敏生,杨杰,丁琳,等. 区块链共识机制综述[J]. 计算机工程,2020,46(12):1-11.

英文引用格式: TAN Minsheng, YANG Jie, DING Lin, et al. Review of consensus mechanism of blockchain[J]. Computer Engineering,2020,46(12):1-11.

Review of Consensus Mechanism of Blockchain

TAN Minsheng, YANG Jie, DING Lin, LI Xingjian, XIA Shiying

(School of Computer, University of South China, Hengyang, Hunan 421001, China)

【Abstract】 Blockchain can effectively connect the Internet of Things, 5G, big data, artificial intelligence and other technologies, playing an important role in new infrastructure construction. As the core of blockchain technology, the consensus mechanism determines the consistency and correctness of the blockchain databases, and thus determines the security, extensibility and throughout of blockchain. This paper categorizes the existing consensus mechanisms of blockchain into three types of single consensus mechanisms and six types of mixed consensus mechanisms. From the perspective of principle realization, it systematically describes the principles of each kind of consensus mechanism, their advantages and disadvantages, and the operations required for the consistency of inductive nodes. From the perspectives of engineering applications, it analyzes the application scenarios of the consensus mechanisms, introduces blockchain projects, and compares the key performance between consensus mechanisms. Finally, it gives the solutions to the problems of energy consumption and efficiency faced by existing consensus mechanism studies, and discusses the further research directions including the reward and punishment mechanism, network slicing and storage slicing.

【Key words】 blockchain; consensus mechanism; Byzantine Fault Tolerance(BFT); distributed system; consistency

DOI: 10.19678/j.issn.1000-3428.0059070

0 概述

比特币(Bitcoin)概念[1]由中本聪在 2008 年 11 月 1 日提出,现已成为市值最大的加密数字货币[2]。区块链作为加密数字货币的底层技术,实际上是一个由所有节点共同维护、共同记账的分布式数据库系统,具有匿名、去中心化、可追溯、不可篡改等特性[3]。区块链架构主要包括分布式记账本、点对点网络、共识机制、智能合约、激励机制和应用程序[4]。记账本由区块构成,区块包含区块头和区块体。区块头包括指

基金项目: 国家自然科学基金(61403183);湖南省教育厅科学研究重点项目(18A230);湖南省财政厅科学研究项目(20191550502);湖南省研究生科研创新项目(CX20200935)。

作者简介: 谭敏生(1965—),男,教授、硕士,主研方向为区块链、可信网络、无线传感器网络;杨 杰(通信作者),硕士研究生;丁 琳,副教授、博士;李行健,硕士研究生;夏石莹,讲师、硕士。

收稿日期: 2020-07-27 **修回日期:** 2020-09-10 **E-mail:** fb12ab@outlook.com

向前一个区块的哈希指针(prev_hash)、版本号(version)、时间戳(ntime)、随机数(nonce)和默克尔树根(Merkle_root),区块体是由交易构成的默克尔树。共识机制[5]是区块链系统达成一致的协议,根据其使用的技术路线分为单一共识机制与混合共识机制。单一共识机制主要分为工作量证明(Proof of Work,PoW)、权益证明(Proof of Stake,PoS)和拜占庭容错(Byzantine Fault Tolerance,BFT)共识机制。

在共识机制中,节点可以分为出块节点、验证节点和记账节点。负责提出区块的节点称为出块节点,也称为出块者、记账者、领导者、主节点或提议者。负责验证区块的节点称为验证节点,也称为验证者或备份节点。验证节点需要验证出块者的合法性、区块的合法性、签名的正确性等。负责维护区块链数据库的节点称为记账节点。记账节点需要存储所有区块和验证区块。出块节点、验证节点和记账节点统称为共识节点。共识机制的主要流程包括选举出块者、提出区块、验证区块和更新区块链。每一轮都先选举新的出块者,再由出块者提出区块(将网络中的合法交易打包进新区块),然后由验证者验证新区块的合法性,最后记账节点将达成共识的新区块写入本地数据库末端来更新区块链。

共识机制主要考虑安全性、扩展性、能耗、吞吐量、交易确认时间和一致性等性能。安全性是指抵抗双花攻击、日蚀攻击等安全威胁的能力[5]。扩展性是指系统支持扩展的能力,主要考虑节点数量和交易数量增加时系统负载和网络通信量的变化。能耗是指每年挖矿消耗的电能。吞吐量是指系统中每秒可以容纳的最大交易量。交易确认时间是指从交易上链到被确认需要的时间。一致性是指系统抵御分叉的能力。

本文总结区块链共识机制,将其分为单一共识机制与混合共识机制,根据技术路线对混合共识机制进行细分,并分析各类共识机制的基本原理及理论依据,同时指出对应的现实世界信任模型。在此基础上,阐述包括选举出块者、提出区块、验证区块和更新区块链的共识机制流程,并从安全性、扩展性、能耗、吞吐量、交易确认时间和一致性等方面分析现有共识机制的相关性能。

1 单一共识机制

1.1 PoW 共识机制

Bitcoin 在没有中心化节点参与的前提下,实现了用户之间的安全自由匿名支付,目前在加密数字货币市场具有较大市值。以 Bitcoin 为代表的莱特币(Litecoin)[6]、Bitcoin-NG[7]、GHOST[8-9]等第一代数字货币系统大多采用 PoW 作为共识机制。PoW 共识机制基于计算机设备进行数学运算的确定性、公平性、可验证性来达成共识,从而保障数据库的一致性,而大部分 PoW 共识机制使用的数学运算为哈希函数。PoW 共识机制相当于自证制度,即自我证明合法性。在 PoW 共识机制中一般使用两次哈希函数,具体共识流程如下:

1)构造默克尔树。矿工收集系统中的交易,使用其认为合法的交易构造默克尔树。

2)选举出块者和提出区块。在 PoW 共识机制中选举出块者和提出区块概念同时进行,矿工通过改变 nonce 的值使 Hash(Hash(version + prev_hash + Merkle_root + ntime + nonce)) < target,找到最先满足要求哈希值的矿工成为出块节点,然后出块节点广播其构造的区块。其中,target 表示目标难度,目标难度每隔一定的时间调整一次,如 Bitcoin 的每 2 016 个区块中所有节点都会按统一公式自动调整目标难度,该公式是将最新 2 016 个区块的实际时长与期望时长进行比较,根据实际时长与期望时长的比值进行相应调整,使得产生区块的平均时间间隔为 10 min。

3)验证区块并更新区块链。矿工验证哈希值和区块中包含的交易,若哈希值小于给定的难度并且所有交易合法,则将新区块写入到区块链末端,更新区块链,开启下一轮共识;否则直接将其丢弃并继续进行本轮挖矿。

PoW 共识机制保障了系统安全性,能抵抗小于 51% 矿力的双花攻击、自私挖矿攻击和日蚀攻击等安全威胁[10-11],但是中心化矿池使系统安全性下降,如 Bitcoin 中最大的 3 个矿池的算力之和已超过 51%[12],若 3 个矿池勾结,则足以发动 51% 攻击,并拒绝其他矿工的交易及服务攻击等。为保证交易的安全性,PoW 共识机制中的交易不能立即被确认,而是需要等待 6 个区块时间。PoW 共识机制受出块时间和区块大小的限制,吞吐量很低,如 Bitcoin 只有 7 TPS。另外,PoW 共识机制消耗大量电能[13-14],如 2014 年 Bitcoin 挖矿能耗相当于爱尔兰全年用电总量[15-16]。

针对 PoW 共识机制存在的问题,一些解决方案被陆续提出。GHOST 采用最重子树策略生成主链,解决了自私挖矿问题。以太坊(Ethereum)[17-18]使用默克尔前缀树替代默克尔树,引入叔区块结构大幅缩短了出块时间,从而将吞吐量增加至 15 TPS[5]。Bitcoin-NG 改进了区块结构,将其分为关键区块和微区块,关键区块在原 Bitcoin 区块中添加了获得记账权的矿工公钥,微区块由获得记账权的矿工根据需要创建。默认设置为每 10 分钟产生一个关键区块,每 10 秒产生一个微区块。挖矿可以在关键区块上进行,也可以在微区块上进行。Bitcoin-NG 为区块链扩容提供了新思路,降低了交易延迟并提高了吞吐量。文献[13]有效利用了区块链系统的电能。

文献[19]基于区块链的计算能力解决了正交向量、困难性假设等复杂数学计算问题。

1.2　PoS 共识机制

为解决 PoW 共识机制的高能耗问题,文献[20-21]提出 PoS 共识机制,基于用户权益达成区块链数据库一致性[22],并且在点点币(PPcoin)中提出基于币龄的 PoS 共识机制(币龄相当于股权),定义币龄为货币数量乘以时期(coin age = coins × age)。币龄是一个随时间流逝线性增加的未花费货币的权重因子,花费货币或者挖矿后消耗币龄。基于 PoS 共识机制的区块链项目多数是由 PoW 共识机制逐步过渡到 PoS 共识机制,如黑币(Blackcoin)[22]、Ethereum。PoS 共识机制相当于股权制度,所有方案需要持有超过半数股权的用户表决同意才能通过。

PoS 共识机制的具体流程为:

1)选举出块者。用户质押持有的代币来获取币龄,币龄越长,成为区块者的概率越大,挖矿需满足不等式:proofhash < coin age × target,其中 proofhash 表示哈希值,其取决于一个权值修改器、未使用的输出和当前时间。

2)提出区块。出块者收集系统中的交易,将其认为合法的交易打包进区块,然后在系统内广播新区块。

3)验证区块并更新区块链。验证节点对新区块进行验证,若验证成功,则将其添加到区块链末端,更新区块链,开启下一轮共识;否则直接将其丢弃,并重新选举出块者。

PoS 共识机制相比 PoW 共识机制无需计算无意义的哈希值,因此其能耗大幅降低。PoS 共识机制能抵抗小于 51% 权益的攻击,恶意节点控制 51% 权益的概率小于控制 51% 计算能力的概率,安全性高于 PoW 共识机制。Blackcoin 项目指出 PPcoin 中的 PoS 共识机制由于存在币龄攻击和长距离攻击,因此将挖矿需满足的不等式改进为 proofhash < coins × target,其中去掉了 age,节点必须保持在线才能进行权益累积,从而解决币龄攻击。另外,其改进了权益修正因子,通过增加时间戳规则、降低预先计算攻击及减少孤块产生使出块时间控制为 64 s[22],从而提高吞吐量,但仍然存在无危险攻击和长距离攻击[23]。Ouroboros 增加了时期的概念,在每个时期内如果出块者不在线,则该轮不产生区块,解决了长距离攻击,并且选举验证者集合,由验证者验证交易合法性的同时打包合法交易给出块者[24-25]。

1.3　BFT 共识机制

区块链中使用的 BFT 共识机制主要分为实用拜占庭容错(Practical Byzantine Fault Tolerance, PBFT)[26-28]、投机拜占庭容错(Speculative Byzantine Fault Tolerance, SBFT)[29-30]和联邦拜占庭容错(Federal Byzantine Fault Tolerance, FBFT)共识机制[31-32]。BFT 共识机制中不产生无意义的能耗,相比其他单一共识机制能耗较低,其相当于公民投票制度,大部分参与者投票同意方案,投票确认结果才能达成一致性。

1.3.1　PBFT 共识机制

PBFT 共识机制解决了原始拜占庭容错共识机制效率较低的问题,将算法复杂度从指数级降低至多项式级。PBFT 共识机制相当于两轮举手表决,需要对提议进行表决并对结果进行确认。

PBFT 共识机制中每个节点都有一个唯一性编号标识(i),编号逐渐递增。一次共识从开始到结束所使用的数据集合称为视图,每个视图都由一个唯一性编号 v 标识,每次视图变更编号加 1,每个视图中只存在一个主节点,其他节点都为备份节点。PBFT 共识机制执行流程[28]如图 1 所示,具体步骤如下:

1)发出请求。客户机发起请求,并将请求消息发送给所有节点。

2)提出区块。主节点监听到客户机发出结构化的服务请求,进入预准备阶段。主节点对请求消息格式进行检查,若不符合,则直接丢弃;若符合,则在当前视图 v 中分配请求标记序号 n(按序增加),向所有备份节点广播结构化的预准备消息并将此消息写入本地日志。

3)验证区块。备份节点对预准备消息进行检查,若通过,则向其他副本节点广播格式化的准备消息,并将预准备消息和准备消息写入本地日志。

4)更新区块链。节点将接收到的准备消息都写入日志,如果一个节点接收到 $2f+1$ 个来自不同节点(包括其自身)且验证正确的准备消息,则向所有备份节点广播结构化的提交消息。

5)答复。备份节点接收到法定数量的提交消息后执行请求操作,并向客户端发送答复消息。客户端若收到 $f+1$ 个不同备份节点的正确答复时,则认为请求得到执行。

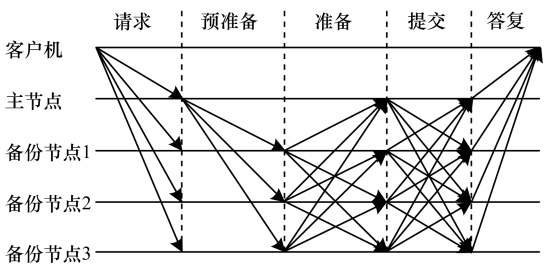

图 1　PBFT 共识机制执行流程

Fig. 1　Execution flow of PBFT consensus mechanism

视图更改协议由备份节点发起,能够解决主节点发生故障的问题。备份节点监测到主节点发生故障时广播视图变更消息并申请成为新的主节点。编号最小(要求此编号比当前发生故障的主节点编

号大)且没有发生故障的备份节点当选为新一轮的主节点。视图变更流程[28]如图 2 所示,具体步骤如下:

1)发起视图变更。备份节点 i 广播视图变更消息,视图变更消息格式为 $\mathrm{Sign}_i(\text{View-change}, v+1, h, C, P, Q)$,其中,$h$ 表示备份节点 i 存储的最新检查点编号,C 表示由备份节点 i 存储的所有检查点编号及对应凭证集合,P 表示由备份节点 i 收集的所有预准备消息集合(对应请求还没有进入提交阶段),Q 表示备份节点 i 接收到的预准备消息集合(对应请求还没有进入准备阶段)。

2)确认视图变更。备份节点 i 收集 $2f+1$ 个(包括其自身)视图变更消息后,给视图 $v+1$ 对应的主节点发送视图变更确认消息,视图变更确认消息格式为 $\mathrm{Sign}_i(\text{View-change-ACK}, v+1, i, j, \mathrm{Hash}(m))$,其中,$j$ 表示发送视图变更消息的备份节点编号集合,m 表示视图变更消息。

3)广播新视图。新的主节点根据存储的信息和日志更新节点数据,发送新视图消息,进入新一轮一致性协议。新视图消息格式为 $\mathrm{Sign}_i(\text{New-view}, v+1, u, \chi)$,其中,$u$ 表示主节点收集到的视图变更证据,χ表示主节点知道的最新检查点、检查点到当前视图中所有已经提交的请求、准备完成的请求和预准备完成的请求。

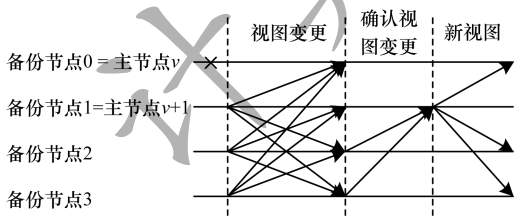

图 2 PBFT 视图变更流程

Fig. 2 Procedure of PBFT view change

PBFT 共识机制可以容忍的最大拜占庭节点数为 $f=\lfloor (R-1)/3 \rfloor$,其中,$R$ 表示共识节点总数。在区块链系统中,采用准入制度增加安全性。当主节点为诚实节点时,共识过程能顺利进行,不会触发视图更换,新产生的区块可以立即确认,系统吞吐量达到 1 000 TPS。由于任意时刻只有一个主节点,因此系统不会发生分叉,并且所有区块需要经过 $2f+1$ 个备份节点(包含主节点)验证,是一种完全去中心化的系统。

由于 PBFT 共识机制采用准入制度,因此节点只有经过认证才能进入系统及广播通信方式,造成了系统扩展性差。共识机制中主节点对请求消息排序并提出区块,然后将预准备消息发送给所有共识节点,时间复杂度为 $O(n)$。在验证时采取多对多的通信模式,每个备份节点都要广播准备消息和提交消息,单个备份节点的时间复杂度为 $O(2n)$,全体备份节点的时间复杂度为 $O(2n)\times O(n)=O(2n^2)$,所以 PBFT 共识机制中一致性协议的时间复杂度为 $O(2n^2+n)\approx O(n^2)$,当节点数量增加时一致性协议性能显著下降。在 PBFT 视图变更过程中,采取多对多的通信模式,每个备份节点都广播一次视图变更消息,时间复杂度为 $O(n)\times O(n)=O(n^2)$,空间复杂度为$O(m)\times O(n)=O(mn)$,且消息包含 C、P、Q 这 3 个集合,所需的存储空间巨大。每个备份节点向新主节点发送一次视图变更确认消息,时间复杂度为 $O(n)$,消息含有备份节点编号集合,空间复杂度相比视图变更消息可以忽略。新主节点向每个备份节点发送一次新视图(t),时间复杂度为 $O(n)$,空间复杂度为 $O(t)\times O(n)=O(tn)$,且消息包含 u、χ两个集合,所需的存储空间巨大。所以 PBFT 视图变更协议的时间复杂度为 $O(2n^2+n)\approx O(n^2)$,空间复杂度为 $O(mn)+O(tn)$。当发生视图变更时,系统时空复杂度为 $O(n^2)\times(O(mn)+O(tn))\approx O((m+t)n^3)$,严重消耗系统资源。

1.3.2 SBFT 共识机制

文献[29]提出 SBFT 共识机制,文献[30]将 SBFT 共识机制应用于区块链。SBFT 共识机制中使用 Collector 技术和收集器通信模式,共识过程中节点将消息发送给收集器,收集器汇总消息后再发送给节点,显著降低了通信量。SBFT 共识机制相当于有专业计票人的投票制度,由计票人统计并公布结果。收集器相当于计票人,可以由客户机担任,也可以由节点担任。SBFT 中备份节点总数为 $3f+2c+1$,其中,c 表示故障节点数量,SBFT 共识机制执行流程[30]如图 3 所示,具体步骤如下:

1)发出请求。客户机向信任的主节点发出请求。

2)提出区块。主节点收集客户机请求,提出区块,然后发送提出区块消息给所有节点。

3)验证区块。所有节点验证从主节点发送过来的预准备消息,如果验证通过,则使用门限聚合签名技术(threshold BLS)[33-35]对验证结果进行数字签名,然后将签名消息发送给收集器 C。

4)统计票数。收集器 C 收集所有节点发送的签名消息并验证合法性。若接收到 $3f+c+1$ 个不同且合法的签名消息,则使用聚合签名技术将消息聚合,然后发送统计票数消息给所有节点。

5)更新区块链。每个节点接收到合法的统计票数消息后,将新区块写入本地数据库并更新区块链,然后发送更新区块链消息给收集器 E。

6)公布执行结果。收集器 E 收集更新区块链消息并对其合法性进行验证。若收集到 $f+1$ 个不同且合法的更新区块链消息,则发送执行结果消息给客户机和所有节点。

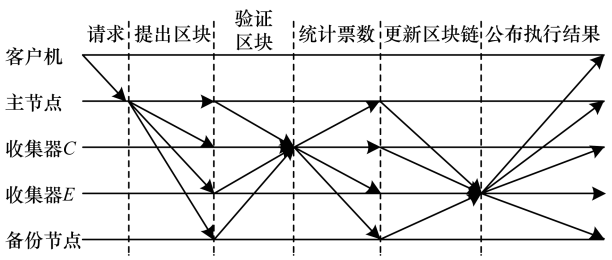

图 3　SBFT 共识机制执行流程

Fig. 3　Execution flow of SBFT consensus mechanism

SBFT 共识机制的视图更改协议也使用 Collector 技术(新的主节点担任收集器),触发条件类似于 PBFT 共识机制,即计时器超时或者收到 $f+1$ 个备份节点发送的主节点出错的证据。SBFT 共识机制能容忍 f 个拜占庭节点和 c 个故障节点。区块能够立即确认,不会产生分叉,并且其不再使用多对多的广播通信模式,降低了通信开销,时间复杂度降至 $O(n)$,显著节省了系统资源。

1.3.3　FBFT 共识机制

FBFT 共识机制弱化了主节点和备份节点的概念,典型的区块链代表项目有瑞波(ripple)[31]、恒星(stellar)[32],每个验证节点在本地维护一个信任节点列表(Unique Node List,UNL),列表中的每个节点都能对交易进行投票。FBFT 共识机制相当于他证制度,每个提案都以他人看法为准。

1)验证请求。每个验证节点不间断监听网络,接收来自客户端的请求信息。经过与本地数据库验证后,如果是不合法的请求,则将其直接丢弃;反之,放入到交易候选集。交易候选集中还包括之前共识过程中无法确认而遗留的交易。

2)提出区块。每个验证节点从自己的交易候选集中取出交易生成提案,并将提案发送给其他节点。

3)验证区块。验证节点在收到其他节点发来的提案后,直接忽略不是来自 UNL 节点的提案,并对比提案中的交易和本地交易候选集,如果有相同交易,则该交易就获得一票。在一定时间内,若交易获得超过 50% 的票数,则该交易进入下一轮;若没有获得超过 50% 的票数,则在下一次共识过程中再次进行确认。

4)再次验证区块。每个验证节点将超过 50% 票数的交易作为提案发给其他节点,同时提高所需票数的阈值至 60%,重复步骤 3 和步骤 4,直到阈值达到 80%。

5)更新区块链。每个验证节点将超过 80% 的 UNL 节点确认的交易正式写入本地数据库,并更新交易候选集。

FBFT 共识机制可以容忍的最大拜占庭节点数为 $f=\lfloor(R-1)/5\rfloor$。区块的产生不依赖于主节点,因此加快了效率,使得吞吐量达到 1 000 TPS ~ 1 500 TPS[5]。由于每个验证节点自身提出区块、决定信任节点集合,因此去中心效果明显,并且区块产生具有不可逆性,不会产生分叉,在交易上链时就能得到确认,同时用户能够动态加入网络,扩展性高于 PBFT 共识机制,但其时间复杂度为 $O(n^2)$。

2　混合共识机制

2.1　基于 PoW 与 PoS 的共识机制

结合 PoW 与 PoS 的共识机制有两种类型:一种是浅结合,即第一阶段使用 PoW 共识机制,达到预定目标后进入第二阶段使用 PoS 共识机制(不再使用 PoW 共识机制),每次共识过程中只使用一种共识机制(PoW 共识机制或者 PoS 共识机制),如 Ethereum、PPcoin、Blackcoin 等;另一种是深结合,即每次共识过程同时使用 PoW 共识机制和 PoS 共识机制,如活动证明(Proof of Activity,PoA)[36]。浅结合类型的共识机制原理、现实世界模型、流程和性能对应每个阶段的单一共识机制;深结合类型的共识机制流程和性能取决于混合共识机制,但由于深结合类型的共识机制模型比较复杂,因此未对应现实世界模型。

基于 PoW 与 PoS 的共识机制流程具体如下:

1)选举出块者和提出区块头。矿工通过改变 nonce 值(Hash(prev_hash + address + height + nonce) < target,其中,address 表示矿工地址,height 表示新区块的高度),计算新区块头(不含区块体),最先找到新区块头的矿工将成为出块节点,出块节点广播新区块头。

2)验证区块头和选举权益代表。全体矿工验证新区块头,验证成功后选举 N 个权益代表(系统初始化时设定 N)。具体选举协议为:将新区块头的哈希值、前一个区块的哈希值和 N 个固定的后缀连接起来(每次使用一个后缀,共产生 N 个连接体),然后将连接体的哈希值作为输入调用 follow-the-satoshi 算法产生权益代表(一个连接体产生一个权益代表)。

3)提出区块。全体矿工首先判断自己是否成为权益代表人:如果成为前 $N-1$ 个代表中的 1 个,则对新区块头签名并广播签名;如果成为第 N 个代表,则构造新区块体,然后使用新区块头、新区块体和前 $N-1$ 个代表的签名构造新区块并对新区块签名,最后广播新区块。

4)验证区块并更新区块链。所有矿工验证新区块的合法性,将合法新区块写入到区块链末端。

PoA 共识机制采用最长主链原则解决分叉问题,由于攻击者需要同时控制大部分矿力和大部分权益才能攻击成功,因此安全性高于 PoW 共识机制和 PoS 共识机制,但其仍然依靠 PoW 共识机制选举出块者,并且没有有效降低能耗,相比 PoW 共识机制通信时间更长、开销更大,从而造成更低的吞吐量。

2.2　基于 PoS 与委托投票制度的共识机制

比特股(Bitshare)[37]结合委托投票制度对 PoS 共识机制做出重大改进,提出委托权益证明(Delegated Proof of Stake,DPoS)共识机制[38-39]。在 DPoS 共识机制中,代表者称为见证人,由见证人按顺序轮流产

生区块,其他见证人验证区块。DPoS 共识机制相当于人民代表大会制度,由人大代表提出议案并对提案进行投票。

DPoS 共识机制通过选举见证人行使权利,具体流程如下:

1)选举出块者。权益持有者投票选举见证人。见证人在系统中保持中立,每 24 小时更新一次,其收益由权益持有者投票决定。Bitshare 可以有任意数量的见证人,EOS[40] 每轮见证人的数量设置为 21,票数最多的前 20 人自动当选见证人,剩余 1 人随机选出,见证人需要 100% 在线。

2)提出区块。见证人产生区块并对区块签名和添加时间戳,再在系统中广播新产生的区块,如果见证人在某个时隙没有产生区块,则该时隙将被跳过,产生区块的权力交给下一个见证人。Bitshare 中每 2 秒产生一个区块,EOS 中每 3 秒产生一个区块。

3)验证区块并更新区块链。其他见证人负责验证新产生区块的合法性。Bitshare 中 N 个见证人验证通过就可上链(N 个见证人要求代表的投票权之和大于 50%),EOS 中半数以上的见证人验证通过就可以上链。

DPoS 共识机制能够对交易进行秒级验证,并在短时间内提供比现有股权证明系统更高的安全性,抵抗小于 51% 权益的攻击[4]。对系统的任何更改(包括版本更新、添加新功能、对权益的修改等)都必须由大于 51% 权益持有者同意。见证人按顺序产生区块,意味着一笔交易从广播开始直至经过 1/2 区块时间被确认的概率为 99.9%。在通常情况下,有半数以上见证人给出确认后,新区块就为不可逆。在连续丢失 2 个区块后,有 95% 的确认节点处于分叉中,在连续丢失 3 个区块后就有 99% 的确认节点处于分叉中。EOS 的吞吐量理论上可达百万级[5],但是选举见证人需要消耗大量资源,实际应用中吞吐量不理想,且区块的产生依赖于 21 个见证人,从而造成中心化问题。

2.3 基于 PoS、VRF 与公证制度的共识机制

文献[41]结合可验证随机函数(Verifiable Random Function,VRF)[42-44]、PoS 和公证制度提出 Dfinity 共识机制。Dfinity 共识机制中使用 threshold BLS 技术构造 VRF(称为信标),输出一种随时间变化的数据流。Dfinity 共识机制相当于公证制度,提案被任意一个合法的公证人证明后即可认为可信。Dfinity 共识机制执行流程[41]如图 4 所示,具体步骤如下:

1)选举出块者。在每一轮选举开始时,由信标广播随机数,根据随机数确定所有提议者及其排名。

2)提出区块。每个提议者都能提议并广播议案。议案由交易、提议者排名、前一个区块的证书及对新区块的签名组成。系统根据提议者排名,给提案赋予不同的权重。提议者排名越高,权重越大。权重越大的提案越有可能成为新区块。

3)验证区块。每一轮都使用信标随机选举出公证委员会,其中公证人对新区块进行公证。等待一定时间后,每个公证人都将认证成功的消息在区块链系统中进行广播,若有多个区块被公证,则将公证消息全部广播。公证委员会中任意一个公证人公证一个区块后,区块链系统进入新一轮共识。

4)更新区块链。全体记账节点根据公证委员会的认证消息更新区块链。

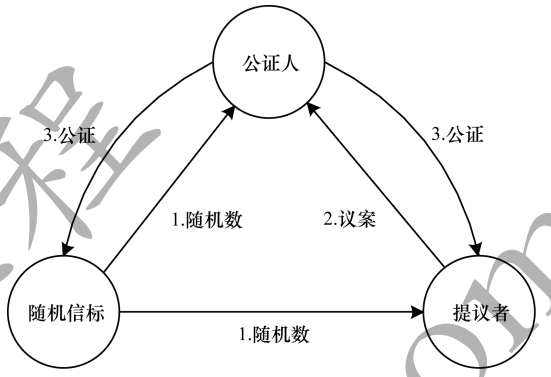

图 4 Dfinity 共识机制执行流程

Fig. 4 Execution flow of Dfinity consensus mechanism

Dfinity 共识机制可以容忍的最大恶意公证人数量为 $f=\lfloor(R-1)/3\rfloor$。由于网络延迟,每一轮都可能有多个区块被认证成功进而产生分叉。为解决分叉,根据协议规定,在任意时间如果所有 B_{k-1} 区块都有共同的先驱 B_{k-2},则提交 B_{k-2} 进区块链;当没有共同的先驱时,提交权重最大的区块。文献[45]证明了当系统诚实用户数量大于 $f+1$ 时,系统最终会达成一致。Dfinity 共识机制中拜占庭节点无法秘密建立和维护被认证的链,所以不会存在双花攻击、自私挖矿攻击、长距离攻击和无危险攻击这些安全威胁,但存在自适应攻击。若采用可验证随机函数产生提议者,虽然解决了提议者身份的问题,提高了系统安全性,但是所有提议者和公证人都使用广播方式进行通信,时间复杂度为 $O(n^2)$。

2.4 基于 PoS、BFT 与委托投票制度的共识机制

小蚁链(NEO)中结合委托投票制度、PoS 共识机制和 PBFT 共识机制提出委托拜占庭容错(delegated Byzantine Fault Tolerance,dBFT)共识机制[46],参与者依据所持有的代币数量进行投票,选举出记账人,由全体记账人运行 BFT 算法达成共识生成新区块。dBFT 共识机制相当于人民代表大会制度,记账人相当于人大代表。dBFT 共识机制中新产生的区块可以立即确认,每 15 秒 ~ 每 20 秒产生一个新区块,吞吐量实测可达 1 000 TPS,可以容忍的最大拜占庭节点数为 $f=\lfloor(R-1)/3\rfloor$,但在 NEO 项目[46]中,需要 NEO 项目方同意才能成为共识节点,其目前只有 7 个共识节点,其中 6 个由项目方控制,接近于完全中心化系统。

2.5　基于 PoS、BFT 与 VRF 的共识机制

2.5.1　VBFT 共识机制

在 Ontology 项目中,结合 PoS、BFT 和 VRF 提出基于可验证随机函数的拜占庭共识机制(VBFT)[47],实现了网络的快速共识。每个区块的 VRF 值根据前一个区块计算得到,具体过程为提取前一个区块中的交易事务,计算 1 024 bit 的哈希值并将该哈希值作为输出。系统中将网络分为共识网络和公共网络。用户通过质押代币后参与到共识网络,共识合约自动更新共识节点列表和相应权益(PoS 表),每产生一个区块更新一次。共识节点分为出块者、验证者、确认者,所有验证者组成验证者集合,所有确认者组成确认者集合。VBFT 共识机制相当于选举制度,合法的选民都具有投票权、被投票权,由可验证随机函数验证选民身份的合法性。

VBFT 共识机制运行时依据 VRF 值作为索引,从 PoS 表中选举共识节点,具体流程如下:

1)选举出块者和提出区块。每一轮依据 VRF 值从共识网络中选举潜在出块者集合,每个潜在出块者提出一个区块。

2)验证区块。每一轮依据 VRF 值从共识网络中选举出验证者集合,每个验证者从共识网络中收集被提出的区块进行执行验证,并投票给具有最高优先级的区块,广播投票消息。

3)确认区块。每一轮依据 VRF 值从共识网络中选举出确认者集合,确认者统计验证者的投票,最后确认达成共识的区块并广播确认消息。

4)更新区块链。共识网络中所有的节点复制确认者认可的区块,只有结束一轮共识,才开启新一轮共识。

每一个区块决定了 VRF 函数的一个输出,由 VRF 函数确定共识节点序列,根据节点序列分配优先级,然后通过节点优先级加权决定区块优先级,最后投票给优先级最高的区块,从而解决分叉问题。VBFT 共识机制中随机选择出块节点、验证节点、确认节点,能够抵抗恶意攻击,去中心化程度和安全性高,吞吐量达到 3 000 TPS,交易确认时间为 5 s ~ 10 s。另外,VBFT 共识机制由共识节点执行 BFT 共识机制,资源消耗低,可以容忍的最大拜占庭节点数为 $f=\lfloor (R-1)/3 \rfloor$,时间复杂度为 $O(n^2)$,扩展性随共识节点的增加而降低。

2.5.2　Algorand 共识机制

文献[48]结合 PoS、BFT 和 VRF 提出 Algorand 共识机制,实现同步网络的快速共识。VRF 由可验证概率函数构造. $\mathrm{Hash}(\mathrm{Sign}_i(r,s,Q^r))$,其中,$r$ 表示节点对共识轮数,s 表示共识步数,Q^r 表示随机数种子,. 表示小于 1 的小数且其后面是小数位,i 表示节点数。Algorand 共识机制[49-50]相当于多委员会制度,包括出块节点委员会和验证节点委员会。

在每轮共识中,当选为潜在出块节点的证据($\sigma_i^r=\mathrm{Sign}_i(r,1,Q^r)$)和新区块分开广播,具体流程如下:

1)选举出块节点和区块验证节点。在第 $r-k$ 轮中的每个验证节点运行 VRF 函数判断自身身份:若在 $r-k$ 轮中没有当选为验证节点,则不参与本轮共识;若. $\mathrm{Hash}(\mathrm{Sign}_i(r,s,Q^r))<p$,其中 p 表示概率,则当选为潜在出块节点并广播证据 σ_i^r;若. $\mathrm{Hash}(\mathrm{Sign}_i(r,s,Q^r))<p'$,其中 p'表示概率,则当选为区块验证节点,成为委员会成员。

2)提出区块。每个潜在出块节点生成 B^r并将其在区块链系统中广播。区块形式为 $B^r=(r,\mathrm{PAY}^r,\mathrm{Sign}_i(Q^r),\mathrm{Hash}(B^{r-1}))$,其中 PAY^r表示区块 B^r中包含的交易集合,若 $\mathrm{PAY}^r\neq\varnothing$,则 $Q^r=\mathrm{Hash}(Q^{R-1},s)$;否则,$Q^r=\mathrm{Hash}(\mathrm{Sign}(Q^{R-1},s))$。

3)验证区块。委员会成员运行 BA * 共识机制验证本轮区块的合法性,其是一种新的拜占庭一致性共识机制。BA * 共识机制包含分级共识(Graded Consensus,GC)算法和改进型二元拜占庭一致性(Binary Byzantine Agreement,BBA)算法,委员会成员验证潜在出块节点的合法性,找出概率值最小的潜在出块节点并选举为出块节点,同时阻止传播概率值较大的潜在出块节点提出区块,并验证其提出区块的合法性,广播验证消息。

4)更新区块链。参与记账的用户根据委员会的验证消息更新区块链。

Algorand 共识机制随机选举出块节点和验证节点,能够抵抗恶意攻击,去中心化程度和安全性高,吞吐量高于 Bitcoin,交易确认时间低于 1 min。BA * 共识机制类似 PBFT 共识机制,资源消耗低,每个步骤都要求拜占庭节点数少于 $f=\lfloor (R-1)/3 \rfloor$,算法时间复杂度为 $O(n^2)$,但其至少需进行 6 轮通信,通信开销高于 PBFT 共识机制。

2.5.3　Omniledger 共识机制

文献[51]结合 VRF、PoS、BFT 和锁机制提出 Omniledger 共识机制,从未花费币池(Unspent Transaction Output,UTXO)的角度实现跨分片链交易的原子性,每条分片链都拥有并维护自身的 UTXO。Omniledger 共识机制使用 PoS 共识机制挑选出验证节点,利用 VRF 将验证节点分配到分片链,每个分片链内部使用 BFT 共识机制达成一致,并通过锁机制保证跨分片链操作时的原子性和正确性。Omniledger 共识机制较复杂,没有对应的现实世界信任模型,具体流程如下:

1)初始化。客户端创建跨分片链交易(cross-TX)。cross-TX 被广播给所有花费 UTXO 的分片链(ISs)。

2)加锁。所有 ISs 与 cross-TX 关联,每个 ISs 锁定自身 UTXO 并检查交易合法性。若验证通过,则先写日志,分片链领导者提交接收证明;若验证失败,分片链领导者提交拒绝证明。

3)解锁。客户端根据阶段 2 的结果发出提交交易信息或者取消交易消息。若所有 ISs 都验证通过,则发出提交消息;若其中有任意一个 ISs 提交了拒绝

证明,则发出取消交易消息。ISs 接收并验证提交消息后,将交易写入分片链,并在 UTXO 中使用对应的代币并解锁交易;接收 UTXO 的分片链(OSs)并在 UTXO 创造对应的代币。

Omniledger 共识机制利用 PoS 共识机制抵抗女巫攻击,可容忍的最大拜占庭节点数为 $f=\lfloor(R-1)/4\rfloor$。吞吐量随分片链数量线性增加。

2.6 基于 BFT 与锁机制的共识机制

2.6.1 Tendermint 共识机制

文献[52]提出的 Tendermint 共识机制使用锁机制深度改进 PBFT 共识机制而得到,具体流程如图 5 所示,包含预投票、预提交和提交 3 个步骤,其中提交包含得到区块和等待超过 2/3 节点提交两个步骤。任何共识节点不论处于哪个阶段,只要接收到合法的提交消息,都进入提交阶段。Tendermint 共识过程中对预投票消息进行加锁,保证了数据正确性和一致性,无需视图变更协议和错误恢复协议,减少了系统资源消耗,但是一致性协议的时间复杂度为 $O(n^2)$。由于 Tendermint 共识机制较复杂,因此没有对应的现实世界信任模型,目前其已应用于 Cita[53] 项目。

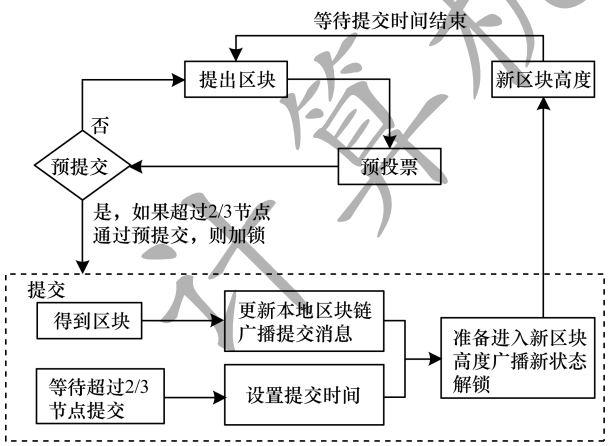

图 5 Tendermint 共识机制执行流程

Fig. 5 Execution flow of Tendermint consensus mechanism

2.6.2 Chainspace 共识机制

文献[54]结合 BFT 与锁机制在 Chainspace 中提出 S-BAC 共识机制,保证了存储分片中智能合约的正确性和安全性。S-BAC 分片链内部和分片链之间都使用 BFT 共识机制,区别在于对拜占庭节点数量要求不同。S-BAC 分片链内部相当于公民投票制度,分片链之间相当于否决权制度。

共识机制中的分片链和诚实节点均指与交易相关的分片链和诚实节点,跨链通信由分片链领导者发起,Chainspace 共识机制执行流程[54] 如图 6 所示,具体步骤如下:

1)初始化。一个用户初始化交易,将准备消息至少发送给一个诚实节点。为保证至少一个诚实节点接收到准备消息,需要在一条分片链中将消息发送给 $f+1$ 个节点,或者在每条分片链中都将消息发送给 $f+1$ 个节点。

2)分配序号。接收到准备消息,分片链进入活动状态,内部使用 BFT 共识机制给准备消息分配序号。

3)验证消息和加锁。分片链内部使用 BFT 共识机制验证交易,若超过 f 个节点验证通过,则进入锁定状态并广播准备提交消息和证据;否则广播拒绝准备消息和证据。如果节点处于锁定状态时,则不接收其他交易并广播拒绝其他交易消息。

4)接收。每条分片链都监听网络,如果收到一条拒绝准备消息,则广播拒绝提交消息和证据;反之,广播接收提交消息和证据。

5)提交和解锁。若分片链接收到提交消息,则将其与交易相关的对象设置为不活跃状态并提交交易,同时更新分片链及解锁交易。若接收到拒绝提交消息,则释放相应的锁,将相关的对象设置为活跃状态,等待下一次共识。

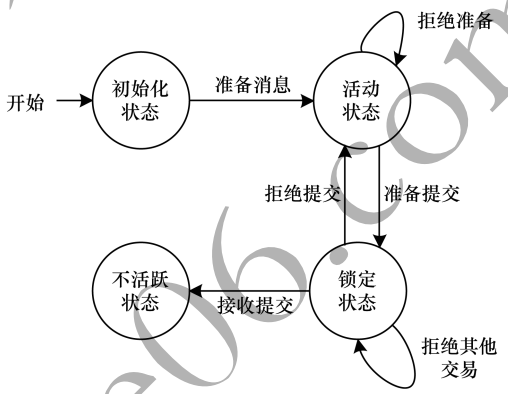

图 6 Chainspace 共识机制执行流程

Fig. 6 Execution flow of Chainspace consensus mechanism

分片链中可以容忍的最大拜占庭节点数为 $f=\lfloor(R-1)/3\rfloor$,分片链之间不能容忍拜占庭节点。如果不同交易涉及的节点不同,则共识操作可以并发进行。分片链内部和分片链之间的交易可以立即确认,但是 S-BAC 只解决了分片链的一致性问题,而没有解决 Chainspace 全局一致性问题。

3 其他共识机制

能力证明(Proof of Capacity,PoC)是根据参与者的计算机硬盘空闲空间作为标准选举出块者的共识机制,如 Permacoin[55]、Spacemint[56]。消逝时间证明(Proof of Elapsed Time,PoET)是根据可信硬件芯片执行某个命令的等待时间作为标准选举出块者的共识机制,等待时间最短的用户即为出块节点[57]。权威证明(Proof of Authority,PoA)是基于权威人士声誉的共识机制,由声誉高的权威人士证明交易的合法性[58]。燃烧证明(Proof of Burn,PoB)是通过可验证的方式销毁基础代币来获得奖励的共识机制[59]。

4 共识机制分析

目前,区块链已经发展到第三代,第一代和第二代为公链,主要使用 PoW 共识机制、PoS 共识机制

和混合共识机制;第三代为联盟链,主要使用 PBFT 共识机制。本节将从能耗、安全性、生成区块时间、交易确认时间、是否存在代币和是否需要专业记账人等方面对单一共识机制进行分析比较,如表 1 所示。同时,对现有典型的区块链项目进行比较,如表 2 所示,其中"—"表示没有对应数据。

表 1　单一共识机制性能比较

Table 1　Performance comparison of single consensus mechanisms

性能	PoW 共识机制	PoS 共识机制	PBFT 和 SBFT 共识机制	FBFT 共识机制
能耗	高	较低	低	低
安全性	<51% 计算能力	<51% 权益	<33.33% 共识节点	<20% 共识节点
生成区块时间	出块时间长,不能满足高频次交易要求	出块时间较短	出块时间较短,能满足高频次交易要求	出块时间较短,能满足高频次交易要求
交易确认时间	确认时间长,一般需要经过 6 个区块后才能确认	确认时间较短	立即确认	立即确认
吞吐量	低	较高	高	高
一致性	概率性	概率性	高	高
是否需要代币	是	是	否	是
是否需要专业记账人	否	否	是	否

表 2　典型的区块链项目性能比较

Table 2　Performance comparison of typical blockchain projects

项目	核心共识机制	能耗	安全性	吞吐量/TPS	生成区块时间/s	交易确认时间/s
Bitcoin	PoW	高	<51% 计算能力	7	600	3 600
Litecoin	PoW	高	<51% 计算能力	56	300	1 800
Bitcoin-NG	PoW	高	<51% 计算能力	400	600(关键区块) 10(微区块)	600
GHOST	PoW	高	<51% 计算能力	200	—	—
Ethereum	PoW	高	<51% 计算能力	15	15	60
Blackcoin	PoS	较低	<51% 权益	—	64	—
PPcoin	PoS	较低	<51% 权益	—	—	—
Hyperledger fabric	BFT	低	<33.33% 共识节点	$>10^3$	—	立即确认
Cita	BFT	低	<33.33% 共识节点	—	—	立即确认
ripple	BFT	低	<20% 共识节点	1 500	—	立即确认
Bitshare	DPoS	低	<51% 见证人	—	2	—
EOS	DPoS	低	<51% 见证人	10^6	3	—
NEO	dBFT	低	<33.33% 共识节点	10^3	15 ~ 20	立即确认
Ontology	VBFT	低	<33.33% 共识节点	>3 000	—	5 ~ 10
Dfinity	Dfinity	低	<33.33% 公证人	10^3	—	—
Algorand	Algorand	低	<33.33% 共识节点	875	—	60

5　研究展望

在区块链共识机制的设计过程中主要考虑能耗、效率、一致性和安全性等性能,现有区块链技术是在效率、安全性和去中心化之间进行有侧重的取舍。共识机制作为区块链的核心技术,未来的研究方向主要包括以下 4 个方面:

1)研究被委托人不遵守规则时对委托人赔偿的共识机制。在基于委托的共识机制中,目前研究的重点是减少委托人不遵守规则时的惩罚,因此下一步将研究被委托人不遵守规则时如何对委托人进行赔偿。

2)研究结合 VRF 与 Bitcoin-NG 的共识机制。将 VRF 应用于 Bitcoin-NG 中可以极大提高关键区块的产生效率,从而降低能耗并提高资源利用率。

3)研究结合 VRF 与网络分片技术的共识机制。将 VRF 应用于网络分片中可以提高共识机制效率并降低验证区块时间,从而增加吞吐量。

4)研究基于高效 Rollup 方法的共识机制。在储存分片中,目前主要研究基于 ZK-Rollup 和 Optimistic Rollup 方法的共识机制,但由于 ZK-Rollup 方法使用 ZK-SNARK 技术,计算过程复杂,计算时间长达 10 min,因此可以通过基于其他零知识证明技术的 Rollup 方法降低计算时间,提高共识机制效率,加快区块产生速度。在 Optimistic Rollup 方法中,新产生的区块需要等待 1 周到 2 周的审查期才能被确认,因此可将其与 BFT 共识机制相结合,使新区块能够立即被确认,从而提高共识机制的执行效率。

6 结束语

区块链技术发展至今,受到各行各业的广泛关注。共识机制作为区块链的核心技术,能够保障区块链数据库的一致性和正确性,从而决定区块链的安全性、扩展性、能耗等相关性能。本文从一致性、容错性等角度归纳现有区块链共识机制,分类介绍区块链共识机制的技术路线。基于现实世界的信任模型,分析各种共识机制的原理,阐述包括选举出块者、提出区块、验证区块和更新区块链的共识机制流程,并从安全性、能耗、吞吐量和区块确认时间等方面对现有共识机制的相关性能进行对比总结。随着区块链技术在新型基础设施建设中发挥愈加重要的作用,大规模、跨领域的区块链会得到更加广泛的应用和发展,因此后续将对具有完善的奖惩制度且高容量、高效率的共识机制做进一步研究。

参考文献

[1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. [2020-06-14]. https://bitcoin.org/en/bitcoin-paper.

[2] BitInfo Charts. Cryptocurrency statistics[EB/OL]. [2020-06-14]. https://bitinfocharts.com/cryptocurrency-prices/.

[3] ZHANG Liang, LIU Baixiang, ZHANG Ruyi, et al. Overview of blockchain technology[J]. Computer Engineering, 2019, 45(5): 1-12. (in Chinese)
张亮,刘百祥,张如意,等. 区块链技术综述[J]. 计算机工程,2019,45(5):1-12.

[4] ZHENG Zibin, XIE Shaoan, DAI Hongning, et al. An overview of blockchain technology: architecture, consensus, and future trends[C]//Proceedings of 2017 IEEE International Congress on Big Data. Washington D. C., USA: IEEE Press, 2017: 557-564.

[5] BACH L M, MIHALJEVIC B, ZAGAR M. Comparative analysis of blockchain consensus algorithms[C]// Proceedings of the 41st International Convention on Information and Communication Technology, Electronics and Microelectronics. Washington D. C., USA: IEEE Press, 2018: 1545-1550.

[6] CLARKE S, CRAIG I, WYSZYNSKI M. Litecoin cash: the best of all worlds SHA256 cryptocurrency[EB/OL]. [2020-06-14]. https://litecoinca.sh/downloads/lcc_whitepaper.pdf.

[7] EYAL I, GENCER A E, SIRER E G, et al. Bitcoin-NG: a scalable blockchain protocol[C]//Proceedings of the 13th Symposium on Networked Systems Design and Implementation. Santa Clara, USA: USENIX Association, 2016: 45-59.

[8] SOMPOLINSKY Y, ZOHAR A. Secure high-rate transaction processing in bitcoin[M]. Berlin, Germany: Springer, 2015.

[9] KIAYIAS A, PANAGIOTAKOS G. On trees, chains and fast transactions in the blockchain[C]//Proceedings of International Conference on Cryptology and Information Security in Latin America. Berlin, Germany: Springer, 2017: 327-351.

[10] CHEN L, XU L, SHAH N, et al. Unraveling blockchain based crypto-currency system supporting oblivious transactions: a formalized approach[C]//Proceedings of ACM Workshop on Blockchain, Cryptocurrencies and Contracts. New York, USA: ACM Press, 2017: 23-28.

[11] FENG Q, HE D B, ZEADALLY S, et al. A survey on privacy protection in blockchain system[J]. Journal of Network and Computer Applications, 2019, 126: 45-58.

[12] Bitcoin mining pools[EB/OL]. [2020-06-14]. https://www.buybitcoinworldwide.com/mining/pools/.

[13] KING S. Primecoin: cryptocurrency with prime number proof-of-work[EB/OL]. [2020-06-14]. http://launch.primecoin.org/static/primecoin-paper.pdf.

[14] SHOKER A. Sustainable blockchain through proof of exercise[C]//Proceedings of the 16th International Symposium on Network Computing and Applications. Washington D. C., USA: IEEE Press, 2017: 1-9.

[15] O'DWYER K J, MALONE D. Bitcoin mining and its energy footprint[C]//Proceedings of the 25th IET Irish Signals & Systems Conference. Washington D. C., USA: IEEE Press, 2014: 280-285.

[16] Digiconomist. Bitcoin sustainability[EB/OL]. [2020-06-14]. https://digiconomist.net/bitcoin-energy-consumption.

[17] BUTERIN V. A next-generation smart contract and decentralized application platform[EB/OL]. [2020-06-14]. https://cryptorum.com/resources/ethereum-whitepaper-smart-contracts-and-decentralized-application-platform.2/.

[18] Ethereum Project. Eth2.0[EB/OL]. [2020-06-14]. https://github.com/ethereum/eth2.0-specs.

[19] BALDOMINOS A, SAEZ Y. Coin.AI: a proof-of-useful-work scheme for blockchain-based distributed deep learning[J]. Entropy, 2019, 21(8): 723.

[20] KING S, NADAL S. PPcoin: peer-to-peer crypto-currency with proof-of-stake[C]//Proceedings of 2016 ACM SIGSAC Conference on Computer and Communications Security. New York, USA: ACM Press, 2016: 1-27.

[21] Peerchemist. Peer assets whitepaper[EB/OL]. [2020-06-14]. https://www.peercoin.net/.

[22] VASIN P. Blackcoin's proof-of-stake protocol V2[EB/OL]. [2020-06-14]. https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf.

[23] XIA Changlin, SONG Yurong, JIANG Guoping. An optimized proof of stake consensus strategy[J]. Computer Engineering, 2019, 45(5): 25-28, 34. (in Chinese)
夏昌琳,宋玉蓉,蒋国平. 一种优化的权益证明共识策略[J]. 计算机工程,2019,45(5):25-28,34.

[24] KIAYIAS A, RUSSELL A, DAVID B, et al. Ouroboros: a provably secure proof-of-stake blockchain protocol[C]//Proceedings of Annual International Cryptology Conference. Berlin, Germany: Springer, 2017: 357-388.

[25] DAVID B, GAŽI P, KIAYIAS A, et al. Ouroboros praos: an adaptively-secure, semi-synchronous proof-of-stake blockchain[C]//Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Germany: Springer, 2018: 66-98.

[26] CACHIN C. Architecture of the hyperledger blockchain fabric[EB/OL]. [2020-06-14]. https://pdfs.semanticscholar.org/f852/c5f3fe649f8a17ded391df0796677a59927f.pdf.

[27] SUN Jiahao, MENG Xiangsi, ZHANG Haoyun, et al. Hierarchical consensus optimization of blockchain based

on trust delegation[J/OL]. Computer Engineering:1-11 [2020-06-14]. https://doi.org/10.19678/j.issn.1000-3428.0056097. (in Chinese)
孙嘉豪,孟翔斯,张浩运,等.基于改进 PBFT 的区块链知识产权保护模型[J/OL].计算机工程:1-11[2020-06-14]. https://doi.org/10.19678/j.issn.1000-3428.0056097.
[28] CASTRO M, LISKOV B. Practical Byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems,2002,20(4):398-461.
[29] KOTLA R, ALVISI L, DAHLIN M, et al. Zyzzyva: speculative Byzantine fault tolerance[C]//Proceedings of the 21st ACM SIGOPS Symposium on Operating Systems Principles. Washington D. C., USA: IEEE Press,2007:45-58.
[30] GUETA G G,ABRAHAM I,GROSSMAN S,et al. SBFT:a scalable and decentralized trust infrastructure [C]// Proceedings of the 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. Washington D.C.,USA:IEEE Press,2019:568-580.
[31] SCHWARTZ D, YOUNGS N, BRITTO A. The ripple protocol consensus algorithm [C]//Proceedings of Annual International Cryptology Conference. Berlin, Germany:Springer,2017:357-388.
[32] MAZIERES D. The stellar consensus protocol: a federated model for Internet-level consensus[EB/OL]. [2020-06-14]. https://tools.ietf.org/html/draft-mazieres-dinrg-scp-04.
[33] HODEL P, CACHIN C. Integrating BLS signatures in PROTECT [EB/OL]. [2020-10-22]. https://crypto.unibe.ch/archive/theses/2020.msc.patrick.hodel.pdf.
[34] LIBERT B, JOYE M, YUNG M. Born and raised distributively:fully distributed non-interactive adaptively-secure threshold signatures with short shares [J]. Theoretical Computer Science,2016,645:1-24.
[35] WANG Y. A review of threshold digital signature schemes[EB/OL]. [2020-06-14]. https://webpages.uncc.edu/yonwang/papers/reviewTSS.pdf.
[36] BENTOV I,LEE C,MIZRAHI A,et al. Proof of activity: extending bitcoin's proof of work via proof of stake [J]. ACM SIGMETRICS Performance Evaluation Review, 2014,42(3):34-37.
[37] SCHUH F,LARIMER D. Bitshares 2.0:financial smart contract platform [EB/OL]. [2020-06-14]. https://www.weusecoins.com/assets/pdf/library/Bitshares%20Financial%20Platform.pdf.
[38] Bitshare Project. Delegated proof-of-stake consensus [EB/OL]. [2020-06-14]. https://bitshares.org/technology/delegated-proof-of-stake-consensus/.
[39] SCHUH F,LARIMER D. Bitshares 2.0:general overview [EB/OL]. [2020-06-14]. https://cryptorating.eu/whitepapers/BitShares/bitshares-general.pdf.
[40] EOS Project. EOS.IO technical white paper[EB/OL]. [2020-06-14]. https://github.com/EOSIO/Documentation/blob/master/Technical WhiterPaper.md.
[41] HANKE T, MOVAHEDI M, WILLIAMS D. DFINITY technology overview series, consensus system[EB/OL]. [2020-06-14]. https://arxiv.org/abs/1805.04548.
[42] JAGER T. Verifiable random functions from weaker assumptions[C]//Proceedings of Theory of Cryptography Conference. Berlin,Germany:Springer,2015:121-143.
[43] HOHENBERGER S, WATERS B. Constructing verifiable random functions with large input spaces[C]//Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin,Germany: Springer,2010:656-672.
[44] MICALI S,RABIN M,VADHAN S. Verifiable random functions[C]//Proceedings of the 40th Annual Symposium on Foundations of Computer Science. Washington D. C.,USA: IEEE Press,1999:120-130.
[45] ABRAHAM I, MALKHI D, NAYAK K, et al. Dfinity consensus, explored[EB/OL]. [2020-06-14]. https://eprint.iacr.org/2018/1153.pdf.
[46] NEO Project. NEO whitepaper[EB/OL]. [2020-06-14]. https://docs.neo.org/docs/zh-cn/basic/whitepaper.html.
[47] Ontology Project. Consensus mechanism [EB/OL]. [2020-06-14]. https://docs.ont.io/ontology-elements/consensus-mechanism.
[48] GILAD Y,HEMO R,MICALI S,et al. Algorand:scaling Byzantine agreements for cryptocurrencies[C]//Proceedings of the 26th Symposium on Operating Systems Principles. Washington D.C.,USA:IEEE Press,2017:51-68.
[49] CHEN J, MICALI S. Algorand: a secure and efficient distributed ledger[J]. Theoretical Computer Science, 2019,777:155-183.
[50] LEUNG D, SUHL A, GILAD Y, et al. Vault: fast bootstrapping for the Algorand cryptocurrency[EB/OL]. [2020-06-14]. https://people.csail.mit.edu/nickolai/papers/leung-vault.pdf.
[51] KOKORIS-KOGIAS E,JOVANOVIC P,GASSER L,et al. Omniledger:a secure, scale-out, decentralized ledger via sharding[C]//Proceedings of 2018 IEEE Symposium on Security and Privacy. Washington D.C.,USA:IEEE Press, 2018:583-598.
[52] KWON J. Tendermint:consensus without mining[EB/OL]. [2020-06-14]. http://diyhpl.us/~bryan/papers2/bitcoin/tendermint_v03.pdf.
[53] Cita Project. Cita-whitepaper[EB/OL]. [2020-06-14]. https://github.com/citahub/cita-whitepaper.
[54] AL-BASSAM M,SONNINO A,BANO S,et al. Chainspace:a sharded smart contracts platform[EB/OL]. [2020-06-14]. https://arxiv.org/abs/1708.03778.
[55] MILLER A,JUELS A,SHI E,et al. Permacoin:repurposing bitcoin work for data preservation[C]//Proceedings of 2014 IEEE Symposium on Security and Privacy. Washington D.C.,USA:IEEE Press,2014:475-490.
[56] PARK S,KWON A,FUCHSBAUER G,et al. Spacemint:a cryptocurrency based on proofs of space[M]. Berlin, Germany:Springer,2018:480-499.
[57] CHEN L,XU L,SHAH N,et al. On security analysis of Proof-of-Elapsed-Time (PoET) [C]//Proceedings of International Symposium on Stabilization, Safety, and Security of Distributed Systems. Berlin, Germany: Springer,2017:282-297.
[58] ANGELIS D S,ANIELLO L,BALDONI R,et al. PBFT vs proof-of-authority: applying the cap theorem to permissioned blockchain [EB/OL]. [2020-06-14]. https://eprints.soton.ac.uk/415083/.
[59] KARANTIAS K, KIAYIAS A, ZINDROS D. Proof-of-burn[C]//Proceedings of International Conference on Financial Cryptography and Data Security. Berlin, Germany:Springer,2020:523-540.

编辑　陆燕菲