

区块链技术共识算法综述

王晓光

(北京吉利学院, 北京 102202)

摘要: 基于区块链技术的去中心化等技术特点, 及比特币平台的平稳运行, 该技术已成为目前金融领域的热点。其技术框架中重要的一点就是它的共识机制, 在去中心化的原则上解决了节点间互相信任的问题。区块链能在众多节点中达到一种较为平衡的状态, 也是因为共识机制。笔者重点介绍了部分流行共识算法, 具体包括 PoW、PoS、DPoS、PBFT, 并提出了共识算法的分析标准。

关键词: 区块链; 共识机制; 比特币; 金融创新

中图分类号: TP311.13 **文献标识码:** A **文章编号:** 1003-9767 (2017) 09-072-03

Summary of the Consensus Algorithm of Block Chain Technology

Wang Xiaoguang

(Beijing Geely College, Beijing 102202, China)

Abstract: Based on decentralization technical characteristic, and the running smooth of Bitcoin platform, the block chain technology has become the hotspot of financial technology. The important point of block chain technical framework is the consensus mechanism, it solves the problem of the mutual trust between the nodes. The block chain technique makes the nodes achieve a more balanced state by means of the consensus mechanism. The author mainly introduces some popular consensus algorithm, including PoW, PoS, DPoS, PBFT, and puts forward the basic standard of consensus algorithm.

Key words: block chain; consensus mechanism; Bitcoin; financial innovation

区块链首次出现在中本聪发表的《比特币：一种点对点的电子现金系统》论文中。它的可实现性已由运行至今的比特币所证明。其突出优势在于去中心化设计的分布式数据库, 通过运用时间戳、Merkle 树形结构、不对称密钥加密算法、共识算法和奖励机制, 使用对等式网络——P2P 网络实现去中心化信用的交易, 为解决中心化模式存在的可靠性差、低效率等问题提出新的计算范式。

1 区块链技术在我国的金融领域的应用

为了紧跟技术发展趋势, 世界各大金融机构都积极参与到区块链的研发中来, 争取竞争主动权, 其中最为著名的是 R3CEV 区块链联盟。作为区块链创业公司, 其发起了 R3 区块链联盟, 目前已有 42 家大银行加入, 具体包括美国银行、纽约梅隆银行、花旗银行等。我国金融机构也积极进行相关的研究, 并已取得具体成果。2016 年 4 月 19 日, 中国分布

式总账基础协议联盟, 即 China Ledger 联盟, 宣告成立。该联盟成员包括中证机构间报价系统股份有限公司、浙江股权交易中心、中钞信用卡产业发展有限公司、北京智能卡技术研究院等十一个成员。

在 2016 年, 微众银行和华瑞银行率先将区块链技术应用于联合贷款业务中的备付金管理及对账流程, 搭载在核心产品“微粒贷”上。

2017 年 1 月, 邮储银行联合 IBM 公司开发了基于区块链技术的资产托管业务系统。这是第一次在核心业务系统中使用区块链技术。该系统的使用减少了业务环节, 提高了风险管理水平。

2017 年 2 月, 作为 R3 联盟成员的招商银行宣布在总行、香港分行和永隆银行两岸三地间将区块链技术应用到直连清算系统, 以缩短交易时间, 减少查询对账操作程序。

作者简介: 王晓光 (1962-), 男, 黑龙江哈尔滨人, 硕士研究生, 教授。研究方向: 金融信息化。



2 重要的共识算法

分布式网络的核心难题是如何高效达成共识。中心化程度低的、决策权分散的社会更难达成一致。如何平衡一致性和可用性,在不影响实际使用体验的前提下还能保证相对可靠的一致性,是研究共识机制的目标。

下面对 PoW、PoS、DPoS、PBFT 算法进行介绍。

2.1 PoW (工作量证明)

PoW (Proof of Work) 机制是适用于比特币系统的共识机制。通过设计与引入分布式网络节点的算力竞争,保证数据一致性和共识。所有参与“挖矿”的网络节点都在遍历寻找一个随机数,保证使当前区块的区块头的双 SHA256 运算结果小于或等于某个值。一旦某个节点找到符合要求的随机数,该节点就获得当前区块的记账权,并获得一定数额的比特币作为奖励。此外,还引入动态难度值,目前求解该数学问题所花费的时间在 10 分钟左右。PoW 共识机制将比特币的发行、交易和记录联系起来,还保证了记账权的随机性,实现比特币系统的安全和去中心化。

该算法的优点是易实现,节点间无需交换额外的信息即可达成共识,破坏系统需要投入极大的成本。缺点是浪费能源,区块的确认时间难以缩短。

2.2 PoS (权益证明)

PoS (Proof of Stake) 本质上是采用权益证明来代替 PoW 的算力证明,记账权由最高权益的节点获得,而不是最高算力的节点。权益代表节点对特定数量的货币的所有权,称作币龄或币天数。币龄等于货币数量乘最后一次交易时间长度。例如,在交易中某人收到 10 个币,持有 10 天,则获得 100 币龄,如果又花去 5 个币,则消耗掉 50 币龄。采用 PoS 共识机制的系统在特定时间点的币龄是有限的,长期持币者有更长的币龄,所以币龄可以视为其在系统中的权益。共识过程的难度与币龄成反比,这样累计消耗币龄最高的区块将被链接到主链。仅依靠内部币龄和权益而不再需要大量消耗外部算力和资源,解决了 PoW 消耗算力的问题。

PoS 的优点是不像 Pow 那么消耗算力。缺点是拥有权益的参与者未必希望参与记账,还是需要挖矿。

2.3 DPoS (股份授权证明机制)

DPoS 在 PoS 的基础上,将记账人的角色专业化。先以

权益作为选票来选出记账人,然后记账人之间再轮流记账。所有持币者投票选出一定数量的节点。被选中的节点代理他们进行验证和记账,记账人必须保证 90% 在线。该共识机制中每个节点都能够自主决定其信任的授权节点,且由这些节点轮流记账生成新的区块。

优点是大幅缩小参与验证和记账节点的数量,可以达到秒级的共识验证。缺点是整个共识机制还是依赖于代币,很多商业应用是不需要代币存在的。

2.4 Ripple Consensus

瑞波共识算法,使一组节点能够基于特殊节点列表达成共识。初始特殊节点列表就像一个俱乐部,要接纳一个新成员,必须由 51% 的该俱乐部会员投票通过。共识遵循这核心成员的 51% 权力,外部人员则没有影响力。由于该俱乐部由“中心化”开始,它将一直是“中心化的”,而如果它开始腐化,股东们什么也做不了。

2.5 PBFT 机制

这是一种基于消息传递的一致性算法,算法经过三个阶段达成一致,这些阶段可能因为失败而重复进行。

在 $N \geq 3F+1$ 的情况下一致性是可能解决的。其中, N 为计算机总数, F 为有问题计算机总数。信息在计算机间互相交换后,各计算机列出所有得到的信息,以大多数的结果作为解决办法。只要系统中有 $2/3$ 的节点是正常工作的,就可以保证一致性。

PBFT 算法的过程如下。

客户端向主节点发送请求调用服务。客户端 c 向主节点发送 $\langle \text{REQUEST}, o, t, c \rangle$ 请求执行操作 o , 这里时间戳 t 用来保证客户端请求只会执行一次。每个由副本节点发给客户端的消息都包含了当前的视图编号,使得客户端能够跟踪视图编号,从而进一步推算出当前主节点的编号。客户端通过对点消息向它自己认为的主节点发送请求,然后主节点自动将该请求向所有备份节点进行广播。

视图是连续编号的整数。主节点由公式 $p = v \bmod |R|$ 计算得到,这里 v 是视图编号, p 是副本编号, $|R|$ 是副本集合的个数。

副本发给客户端的响应为 $\langle \text{REPLY}, v, t, c, i, r \rangle$, v 是视图编号, t 是时间戳, i 是副本的编号, r 是请求执行的结果。

主节点通过广播将请求发送给其他副本,然后就开始执行三个阶段的任务。



(1) 预准备阶段。主节点给收到的请求分配一个序列号 n ，然后向所有备份节点群发预准备消息，预准备消息的格式为 $\langle\langle\text{PRE-PREPARE},v,n,d\rangle,m\rangle$ ，这里 v 是视图编号， m 是客户端发送的请求消息， d 是请求消息 m 的摘要。

(2) 准备阶段。如果备份节点 i 接受了预准备消息 $\langle\langle\text{PRE-PREPARE},v,n,d\rangle,m\rangle$ ，则进入准备阶段。在准备阶段时，该节点向所有副本节点发送准备消息 $\langle\text{PREPARE},v,n,d,i\rangle$ ，并且将预准备消息和准备消息写入自己的消息日志。如果看预准备消息不顺眼，就什么都不做。

(3) 确认阶段。当 (m,v,n,i) 条件为真时，副本 i 将 $\langle\text{COMMIT},v,n,D(m),i\rangle$ 向其他副本节点进行广播，于是就进入了确认阶段。所有副本都执行请求并将结果发回客户端。客户端需要等待 $f+1$ 个不同副本节点发回相同的结果，作为整个操作的最终结果。

如果客户端没有在有限时间内收到回复，请求将向所有副本节点进行广播。如果请求已在副本节点处理过了，副本就向客户端重发一遍执行结果。如果请求没有在副本节点处理过，该副本节点将把请求转发给主节点。如果主节点没有将该请求进行广播，那么就有认为主节点失效，如果有足够的副本节点认为主节点失效，则会触发一次视图变更。

3 共识算法的分析标准

共识算法的优劣对于分布式系统的性能影响很大，具体可以从以下几个方面加以考虑。

3.1 安全机制和容错能力

安全机制首要防止可能的攻击，而攻击主要考虑 5 点：攻击的类型（DoS 攻击，盗取和 Double-Spending）、攻击使用的成本多大、攻击的范围和目标的损害程度、攻击的持续性和网络修复反应的速度、算法机制的总体攻击的可能性。其次就要考虑算法的容错能力，一般来讲，如果采用分布式模块化分层应用设计方式，容错的能力就能得到极大提升。

3.2 算法处理能力

在实际消费过程中，客户不可能忍受 10 分钟以上的交易确认时间。目前主流的数字货币交易确认时间均超过 10 分钟，所以如何在兼顾系统安全的前提下，缩短交易确认时间是重要的课题。

3.3 共识成本

目前比特币系统需要通过“挖矿”，即算力竞争来获得记账权，这带来算力的巨大浪费。其他共识算法在一定程度上减少了算力损耗，但又存在其他问题。因此，需要根据需要简化算法。

3.4 去中心化的算法

区块链技术的特点之一就是去中心化。共识算法设计如何贯穿这一思想，是需要深入研究的问题。

4 结 语

共识机制解决了区块链如何在分布式场景下达成一致性的问题。可以从去中心化、网络成本、扩展性、安全机制和容错能力来评估共识算法。未来创新之处在于降级共识算法的复杂度。基于工作证明的共识算法会逐步缓慢退出市场，而那些不消耗能源的共识算法会进一步发展，这是一种长期的发展趋势。

参考文献

- [1] 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.
- [2] 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).
- [3] 张宁,王毅,康重庆,等.能源互联网中的区块链技术:研究框架与典型应用初探[J].中国电机工程学报,2016,36(15):4011-4022.