区块链共识算法的发展现状与展望

袁 勇 [1, 2] 倪晓春 [1, 2] 曾 帅 [1, 2] 王飞跃 [1, 3, 4]

摘 要 共识算法是区块链技术的核心要素, 也是近年来分布式系统研究的热点. 本文系统性地梳理和讨论了区块链发展过程中的 32 种重要共识算法, 介绍了传统分布式一致性算法以及分布式共识领域的里程碑式的重要研究和结论, 提出了区块链共识算法的一种基础模型和分类方法, 并总结了现有共识算法的发展脉络和若干性能指标, 以期为未来共识算法的创新和区块链技术的发展提供参考.

关键词 区块链, 共识算法, 分布式系统, 拜占庭容错, P2P 网络

引用格式 袁勇, 倪晓春, 曾帅, 王飞跃. 区块链共识算法的发展现状与展望. 自动化学报, 2018, **44**(11): 2011−2022

DOI 10.16383/j.aas.2018.c180268

Blockchain Consensus Algorithms: The State of the Art and Future Trends

YUAN Yong[1, 2] NI Xiao-Chun[1, 2] ZENG Shuai[1, 2] WANG Fei-Yue[1, 3, 4]

Abstract Consensus algorithm is a key component of the blockchain technology, and also a hot topic in distributed systems research. In this paper, we systematically review and discuss 32 mainstream consensus algorithms emerged in the development process of blockchain. We introduce the classic distributed consistency algorithms, as well as the milestone research efforts and the key conclusions of distributed consensus algorithms. We also propose a novel model and classification approach of blockchain consensus algorithms. In the end, we summarize the consensus algorithms and their performance measures using an evolutionary tree. This is our preliminary research effort towards the blockchain consensus algorithm, aiming at offering useful guidance and reference for future innovation of novel consensus algorithms and the development of blockchain technology.

Key words Blockchain, consensus algorithms, distributed systems, Byzantine fault tolerance, peer-to-peer network (P2P)

Citation Yuan Yong, Ni Xiao-Chun, Zeng Shuai, Wang Fei-Yue. Blockchain consensus algorithms: the state of the art and future trends. *Acta Automatica Sinica*, 2018, **44**(11): 2011−2022

共识问题是社会科学和计算机科学等领域的经典问题, 已经有很长的研究历史. 目前有记载的文献至少可以追溯到 1959 年, 兰德公司和布朗大学的埃德蒙 · 艾森伯格 (Edmund Eisenberg) 和大卫 · 盖尔 (David Gale) 发表的 “Consensus of subjective probabilities: the pari-mutuel method”, 主要研究针对某个特定的概率空间, 一组个体各自有其主观的概率分布时, 如何形成一个共识概率分布的问题[1]. 随后, 共识问题逐渐引起了社会学、管理学、经济学、特别是计算机科学等各学科领域的广泛研究兴趣.

计算机科学领域的早期共识研究一般聚焦于分布式一致性, 即如何保证分布式系统集群中所有节点的数据完全相同并且能够对某个提案达成一致的问题, 是分布式计算的根本问题之一. 虽然共识 (Consensus) 和一致性 (Consistency) 在很多文献和应用场景中被认为是近似等价和可互换使用的, 但二者涵义存在着细微的差别: 共识研究侧重于分布式节点达成一致的过程及其算法, 而一致性研究则侧重于节点共识过程最终达成的稳定状态; 此外, 传统分布式一致性研究大多不考虑拜占庭容错问题, 即假设不存在恶意篡改和伪造数据的拜占庭节点, 因此在很长一段时间里, 传统分布式一致性算法的

收稿日期 2018-04-29 录用日期 2018-09-17
Manuscript received April 29, 2018; accepted September 17, 2018
国家自然科学基金 (71472174, 61533019, 71232006, 61233001, 71702182), 青岛智能产业智库基金资助
Supported by National Natural Science Foundation of China (71472174, 61533019, 71232006, 61233001, 71702182), Qingdao Think-Tank Foundation on Intelligent Industries
本文责任编委 刘艳军
Recommended by Associate Editor LIU Yan-Jun
1. 中国科学院自动化研究所复杂系统管理与控制国家重点实验室 北京 100190 2. 青岛智能产业技术研究院平行区块链技术创新中心 青岛 266109 3. 国防科学技术大学军事计算实验与平行系统技术中心 长沙 410073 4. 中国科学院大学中国经济与社会安全研究中心 北京 101408
1. The State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190 2. Innovation Center for Parallel Blockchain, Qingdao Academy of Intelligent Industries, Qingdao 266109 3. Research Center of Military Computational Experiments and Parallel Systems, National University of Defense Technology, Changsha 410073 4. Center of China Economic and Social Security, The University of Chinese Academy of Sciences, Beijing 101408

应用场景大多是节点数量有限且相对可信的分布式数据库环境. 与之相比, 区块链系统的共识算法则必须运行于更为复杂、开放和缺乏信任的互联网环境下, 节点数量更多且可能存在恶意拜占庭节点. 因此, 即使 Viewstamped replication (VR) 和 Paxos 等许多分布式一致性算法早在上世纪 80 年代就已经提出, 但是如何跨越拜占庭容错这道鸿沟、设计简便易行的分布式共识算法, 仍然是分布式计算领域的难题之一.

2008 年 10 月 31 日, 一位化名为 "中本聪" 的研究者在密码学邮件组中发表了比特币的奠基性论文 "Bitcoin: a peer-to-peer electronic cash system"[2],基于区块链 (特别是公有链) 的共识研究自此拉开序幕. 从分布式计算和共识的角度来看, 比特币的根本性贡献在于首次实现和验证了一类实用的、互联网规模的拜占庭容错算法, 从而打开了通往区块链新时代的大门.

一般而言, 区块链系统的节点具有分布式、自治性、开放可自由进出等特性, 因而大多采用对等式网络 (Peer-to-peer network, P2P 网络) 来组织散布全球的参与数据验证和记账的节点. P2P 网络中的每个节点均地位对等且以扁平式拓扑结构相互连通和交互, 不存在任何中心化的特殊节点和层级结构, 每个节点均会承担网络路由、验证区块数据、传播区块数据、发现新节点等功能. 区块链系统采用特定的经济激励机制来保证分布式系统中所有节点均有动机参与数据区块的生成和验证过程, 按照节点实际完成的工作量分配共识过程所产生的数字加密货币, 并通过共识算法来选择特定的节点将新区块添加到区块链. 以比特币为代表的一系列区块链应用的蓬勃发展, 彰显了区块链技术的重要性与应用价值, 区块链系统的共识也成为一个新的研究热点[3−5].

迄今为止, 研究者已经在共识相关领域做了大量研究工作, 不同领域研究者的侧重点也各不相同. 计算机学科通常称为共识算法或者共识协议, 管理和经济学科则通常称为共识机制. 细究之下, 这些提法存在细微的差异: 算法一般是一组顺序敏感的指令集且有明确的输入和输出; 而协议和机制则大多是一组顺序不敏感的规则集. 就区块链领域而言, 本文认为比特币和以太坊等可认为是底层协议或机制, 其详细规定了系统或平台内部的节点交互规则、数据路由和转发规则、区块构造规则、交易验证规则、账本维护规则等集合; 而工作量证明 (Proof-of-work, PoW)、权益证明 (Proof-of-stake, PoS) 等则是建立在特定协议或机制基础上、可灵活切换的算法, 其规定了交易侦听与打包、构造区块、记账人选举、区块传播与验证、主链选择与更新等若干类顺序敏感的指令集合. 因此, 本文后续叙述均采用共识算法的提法.

现有文献研究的共识问题实际上可以分为算法共识和决策共识两个分支, 前者致力于研究在特定的网络模型和故障模型前提下, 如何在缺乏中央控制和协调的分布式网络中确保一致性, 其实质是一种 "机器共识"; 后者则更为广泛地研究无中心的群体决策中, 如何就最优的决策达成一致的问题, 例如关于比特币系统扩容[6] 问题和分叉问题的社区讨论与路线选择, 其实质是 "人的共识". 二者的区别在于: 前者是机器间的确定性共识, 以工程复杂性为主; 而后者则是以 "人在环路中 (Human-in-the-loop)" 的复杂系统为特点的不确定性共识, 以社会复杂性为主. 区块链共识算法研究应属于算法共识分支的子集, 而决策共识则大多见于分布式人工智能、多智能体等研究领域.

拜占庭将军问题是分布式共识的基础, 也是上述两个研究分支的根源. 拜占庭将军问题有两个交互一致性条件, 即一致性和正确性. 由于大多数情况下, 正确性涉及到人的主观价值判断, 很难施加到分布式节点上, 因此算法共识采用的是 "降级的正确性 (Degraded correctness), 即从 "表达的内容是正确的" 降级为 "正确地表达", 这就导致区块链的拜占庭共识实际上是一种机器共识, 其本身等价于分布式一致性 + 正确表达 (不篡改消息). 与之相对的是, 决策共识可以认为是人的共识, 不仅要求一致性, 而且要求所有节点相信 "表达的内容是正确的", 因而决策共识不仅要求内容的客观一致性, 而且还要求其在共识节点间的主观正确性. 由此可见, 算法共识处理的是客观的二值共识, 即对 (唯一正确的账本) 和错 (所有错误的账本), 而决策共识处理的是主观的多值共识, 即意见 1 (及其所属群体)、意见 2 (及其所属群体)、$\cdots$、意见 N (及其所属群体), 各节点最终通过群体间的协调和协作过程收敛到唯一意见 (共识), 而此过程可能失败 (不收敛).

本文致力于按时间顺序梳理和讨论区块链发展过程中的共识算法, 以期为未来共识算法的创新和区块链技术的发展提供参考. 本文的后续章节安排如下: 首先, 简要介绍了分布式共识领域重要的里程碑式的研究和结论, 包括两军问题、拜占庭问题和 FLP 不可能定理, 并介绍了传统的分布式一致性算法; 然后, 提出了区块链共识算法的一种基础模型和分类方法, 并对当前主流的区块链共识算法进行了分析; 最后, 总结了区块链共识算法的发展和研究趋势.

1 传统分布式一致性算法

1975 年, 纽约州立大学石溪分校的阿克云卢 (Akkoyunlu E. A.)、埃卡纳德汉姆 (Ekanadham

K.) 和胡贝尔 (Huber R. V.) 在论文 “Some constraints and tradeoffs in the design of network communications” 中首次提出了计算机领域的两军问题及其无解性证明[7], 著名的数据库专家吉姆 · 格雷正式将该问题命名为 “两军问题”[8]. 两军问题表明, 在不可靠的通信链路上试图通过通信达成一致共识是不可能的, 这被认为是计算机通信研究中第一个被证明无解的问题. 两军问题对计算机通信研究产生了重要的影响, 互联网时代最重要的 TCP/IP 协议中的 “三次握手” 过程即是为解决两军问题不存在理论解而诞生的简单易行、成本可控的 “工程解”.

分布式计算领域的共识问题于 1980 年由马歇尔 · 皮斯 (Marshall Pease)、罗伯特 · 肖斯塔克 (Robert Shostak) 和莱斯利 · 兰伯特 (Leslie Lamport) 提出[9], 该问题主要研究在一组可能存在故障节点、通过点对点消息通信的独立处理器网络中, 非故障节点如何能够针对特定值达成一致共识. 1982 年, 作者在另一篇文章中正式将该问题命名为 “拜占庭将军问题”[10], 提出了基于口头消息和基于签名消息的两种算法来解决该问题. 拜占庭假设是对现实世界的模型化, 强调的是由于硬件错误、网络拥塞或断开以及遭到恶意攻击, 计算机和网络可能出现的不可预料的行为. 此后, 分布式共识算法可以分为两类, 即拜占庭容错和非拜占庭容错类共识. 早期共识算法一般为非拜占庭容错算法, 例如广泛应用于分布式数据库的 VR 和 Paxos, 目前主要应用于联盟链和私有链; 2008 年末, 比特币等公有链诞生后, 拜占庭容错类共识算法才逐渐获得实际应用. 需要说明的是, 拜占庭将军问题是区块链技术核心思想的根源, 直接影响着区块链系统共识算法的设计和实现, 因而在区块链技术体系中具有重要意义.

1985 年, 迈克尔 · 费舍尔 (Michael Fisher)、南希 · 林奇 (Nancy Lynch) 和迈克尔 · 帕特森 (Michael Paterson) 共同发表了论文 “Impossibility of distributed consensus with one faulty process”[11]. 这篇文章证明: 在含有多个确定性进程的异步系统中, 只要有一个进程可能发生故障, 那么就不存在协议能保证有限时间内使所有进程达成一致. 按照作者姓氏的首字母, 该定理被命名为 FLP 不可能定理, 是分布式系统领域的经典结论之一, 并由此获得了 Dijkstra 奖. FLP 不可能定理同样指出了存在故障进程的异步系统的共识问题不存在有限时间的理论解, 因而必须寻找其可行的 “工程解”. 为此, 研究者们只能通过调整问题模型来规避 FLP 不可能定理, 例如牺牲确定性、增加时间等; 加密货币则是通过设定网络同步性 (或弱同步性) 和时间假设来规避 FLP 不可能性, 例如网络节点可以快速同步, 且矿工在最优链上投入有限时间和资源等.

早期的共识算法一般也称为分布式一致性算法. 与目前主流的区块链共识算法相比, 分布式一致性算法主要面向分布式数据库操作、且大多不考虑拜占庭容错问题, 即假设系统节点只发生宕机和网络故障等非人为问题, 而不考虑恶意节点篡改数据等问题. 1988 年, 麻省理工学院的布莱恩 · 奥奇 (Brian M. Oki) 和芭芭拉 · 里斯科夫 (Barbara H. Liskov, 著名计算机专家、2008 年图灵奖得主) 提出了 VR 一致性算法, 采用主机 – 备份 (Primary-backup) 模式, 规定所有数据操作都必须通过主机进行, 然后复制到各备份机器以保证一致性[12]. 1989 年, 莱斯利 · 兰伯特 (Leslie Lamport) 在工作论文 “The part-time parliament” 中提出 Paxos 算法, 由于文章采用了讲故事的叙事风格且内容过于艰深晦涩, 直到 1998 年才通过评审、发表在 ACM transactions on computer systems 期刊上[13]. Paxos 是基于消息传递的一致性算法, 主要解决分布式系统如何就某个特定值达成一致的问题. 随着分布式共识研究的深入, Paxos 算法获得了学术界和工业界的广泛认可, 并衍生出 Abstract paxos、Classic paxos、Byzantine paxos 和 Disk paxos 等变种算法, 成为解决异步系统共识问题最重要的算法家族[14]. 实际上, Liskove 等提出的 VR 算法本质上也是一类 Paxos 算法. 需要说明的是, VR 和 Paxos 算法均假设系统中不存在拜占庭故障节点, 因而是非拜占庭容错的共识算法. 除以上共识算法外, 获得较多研究关注的早期共识算法还有两阶段提交 (Two-phase commit) 算法、三阶段提交 (Three-phase commit) 算法、Zab、Zyzzyva、Kafka 等, 本文限于篇幅不加详述.

2 主流区块链共识算法

1993 年, 美国计算机科学家、哈佛大学教授辛西娅 · 德沃克 (Cynthia Dwork) 首次提出了工作量证明思想[15], 用来解决垃圾邮件问题. 该机制要求邮件发送者必须算出某个数学难题的答案来证明其确实执行了一定程度的计算工作, 从而提高垃圾邮件发送者的成本. 1997 年, 英国密码学家亚当 · 伯克 (Adam Back) 也独立地提出、并于 2002 年正式发表了用于哈希现金 (Hash cash) 的工作量证明机制[16]. 哈希现金也是致力于解决垃圾邮件问题, 其数学难题是寻找包含邮件接受者地址和当前日期在内的特定数据的 SHA-1 哈希值, 使其至少包含 20 个前导零. 1999 年, 马库斯 · 雅各布松 (Markus Jakobsson) 正式提出了 “工作量证明” 概念[17]. 这些工作为后来中本聪设计比特币的共识机制奠定了基础.

1999 年, Barbara Liskov 等提出了实用拜占庭容错算法 (Practical Byzantine fault tolerance, PBFT)[18], 解决了原始拜占庭容错算法效率不高的问题, 将算法复杂度由指数级降低到多项式级, 使得拜占庭容错算法在实际系统应用中变得可行. PBFT 实际上是 Paxos 算法的变种, 通过改进 Paxos 算法使其可以处理拜占庭错误, 因而也称为 Byzantine paxos 算法, 可以在保证活性 (Liveness) 和安全性 (Safety) 的前提下提供 $(n-1)/3$ 的容错性, 其中 n 为节点总数.

2000 年, 加利福尼亚大学的埃里克 · 布鲁尔 (Eric Brewer) 教授在 ACM Symposium on Principles of Distributed Computing 研讨会的特邀报告中提出了一个猜想: 分布式系统无法同时满足一致性 (Consistency)、可用性 (Availability) 和分区容错性 (Partition tolerance), 最多只能同时满足其中两个. 其中, 一致性是指分布式系统中的所有数据备份在同一时刻保持同样的值; 可用性是指集群中部分节点出现故障时, 集群整体是否还能处理客户端的更新请求; 分区容忍性则是指是否允许数据分区, 不同分区的集群节点之间无法互相通信. 2002 年, 塞斯 · 吉尔伯特 (Seth Gilbert) 和南希 · 林奇 (Nancy Lynch) 在异步网络模型中证明了这个猜想, 使其成为 CAP (Consistency, availability, partition tolerance) 定理或布鲁尔定理[19]. 该定理使得分布式网络研究者不再追求同时满足三个特性的完美设计, 而是不得不在其中做出取舍, 这也为后来的区块链体系结构设计带来了影响和限制.

2008 年 10 月, 中本聪发表的比特币创世论文催生了基于区块链的共识算法研究. 前文所提到的传统分布式一致性算法大多应用于相对可信的联盟链和私有链, 而面向比特币、以太坊等公有链环境则诞生了 PoW、PoS 等一系列新的拜占庭容错类共识算法.

比特币采用了 PoW 共识算法来保证比特币网络分布式记账的一致性, 这也是最早和迄今为止最安全可靠的公有链共识算法. PoW 的核心思想是通过分布式节点的算力竞争来保证数据的一致性和共识的安全性. 比特币系统的各节点 (即矿工) 基于各自的计算机算力相互竞争来共同解决一个求解复杂但是验证容易的 SHA256 数学难题 (即挖矿), 最快解决该难题的节点将获得下一区块的记账权和系统自动生成的比特币奖励. PoW 共识在比特币中的应用具有重要意义, 其近乎完美地整合了比特币系统的货币发行、流通和市场交换等功能, 并保障了系统的安全性和去中心性. 然而, PoW 共识同时存在着显著的缺陷, 其强大算力造成的资源浪费 (主要是电力消耗) 历来为人们所诟病, 而且长达 10 分钟的交易确认时间使其相对不适合小额交易的商业应用[3].

2011 年 7 月, 一位名为 Quantum Mechanic 的数字货币爱好者在比特币论坛 (www.bitcointalk.org) 首次提出了权益证明 PoS 共识算法[20]. 随后, Sunny King 在 2012 年 8 月发布的点点币 (Peercoin, PPC) 中首次实现. PoS 由系统中具有最高权益而非最高算力的节点获得记账权, 其中权益体现为节点对特定数量货币的所有权, 称为币龄或币天数 (Coin days). PPC 将 PoW 和 PoS 两种共识算法结合起来, 初期采用 PoW 挖矿方式以使得 Token 相对公平地分配给矿工, 后期随着挖矿难度增加, 系统将主要由 PoS 共识算法维护. PoS 一定程度上解决了 PoW 算力浪费的问题, 并能够缩短达成共识的时间, 因而比特币之后的许多竞争币都采用 PoS 共识算法.

2013 年 2 月, 以太坊创始人 Vitalik Buterin 在比特币杂志网站详细地介绍了 Ripple (瑞波币) 及其共识过程的思路. Ripple 项目实际上早于比特币, 2004 年就由瑞安 · 福格尔 (Ryan Fugger) 实现, 其初衷是创造一种能够有效支持个人和社区发行自己货币的去中心化货币系统; 2014 年, 大卫 · 施瓦尔茨 (David Schwartz) 等提出了瑞波协议共识算法 (Ripple Protocol Consensus Algorithm, RPCA)[21], 该共识算法解决了异步网络节点通讯时的高延迟问题, 通过使用集体信任的子网络 (Collectively-trusted subnetworks), 在只需最小化信任和最小连通性的网络环境中实现了低延迟、高鲁棒性的拜占庭容错共识算法. 目前, Ripple 已经发展为基于区块链技术的全球金融结算网络.

2013 年 8 月, 比特股 (Bitshares) 项目提出了一种新的共识算法, 即授权股份证明算法 (Delegated proof-of-stake, DPoS)[22]. DPoS 共识的基本思路类似于 "董事会决策", 即系统中每个节点可以将其持有的股份权益作为选票授予一个代表, 获得票数最多且愿意成为代表的前 N 个节点将进入 "董事会", 按照既定的时间表轮流对交易进行打包结算、并且签署 (即生产) 新区块[3]. 如果说 PoW 和 PoS 共识分别是 "算力为王" 和 "权益为王" 的记账方式的话, DPoS 则可以认为是 "民主集中式" 的记账方式, 其不仅能够很好地解决 PoW 浪费能源和联合挖矿对系统的去中心化构成威胁的问题, 也能够弥补 PoS 中拥有记账权益的参与者未必希望参与记账的缺点, 其设计者认为 DPoS 是当时最快速、最高效、最去中心化和最灵活的共识算法.

2013 年, 斯坦福大学的迭戈 · 翁伽罗 (Diego Ongaro) 和约翰 · 奥斯特豪特 (John Ousterhout) 提出了 Raft 共识算法. 正如其论文标题 "In search of an understandable consensus algorithm"[23] 所

述, Raft 的初衷是为设计一种比 Paxos 更易于理解和实现的共识算法. 要知道, 由于 Paxos 论文极少有人理解, Lamport 于 2001 年曾专门写过一篇文章 “Paxos made simple”[24], 试图简化描述 Paxos 算法但效果不好, 这也直接导致了 Raft 的提出. 目前, Raft 已经在多个主流的开源语言中得以实现.

3　共识算法的模型与分类

随着比特币的普及和区块链技术的发展, 越来越多的新共识算法被提出. 为使读者更为深刻地理解不同的共识算法, 本节给出区块链共识过程的一个主流模型. 需要说明的是, 该模型并非通用模型, 可能无法涵盖所有种类的共识过程, 但是可以体现大多数主流共识算法的核心思想.

区块链系统建立在 P2P 网络之上, 其全体节点的集合可记为 P, 一般分为生产数据或者交易的普通节点, 以及负责对普通节点生成的数据或者交易进行验证、打包、更新上链等挖矿操作的 “矿工” 节点集合 (记为 M), 两类节点可能会有交集; 矿工节点通常情况下会全体参与共识竞争过程, 在特定算法中也会选举特定的代表节点、代替它们参加共识过程并竞争记账权, 这些代表节点的集合记为 D; 通过共识过程选定的记账节点记为 A. 共识过程按照轮次重复执行, 每一轮共识过程一般重新选择该轮的记账节点.

共识过程的核心是 “选主” 和 “记账” 两部分, 在具体操作过程中每一轮可以分为选主 (Leader election)、造块 (Block generation)、验证 (Data validation) 和上链 (Chain updation, 即记账) 4 个阶段. 如图 1 所示, 共识过程的输入是数据节点生成和验证后的交易或数据, 输出则是封装好的数据区块以及更新后的区块链. 4 个阶段循环往复执行, 每执行一轮将会生成一个新区块.

第 1 阶段: 选主. 选主是共识过程的核心, 即从全体矿工节点集 M 中选出记账节点 A 的过程: 我们可以使用公式 $f(M) \to A$ 来表示选主过程, 其中函数 f 代表共识算法的具体实现方式. 一般来说, $|A| = 1$, 即最终选择唯一的矿工节点来记账.

第 2 阶段: 造块. 第一阶段选出的记账节点根据特定的策略将当前时间段内全体节点 P 生成的交易或者数据打包到一个区块中, 并将生成的新区块广播给全体矿工节点 M 或其代表节点 D. 这些交易或者数据通常根据区块容量、交易费用、交易等待时间等多种因素综合排序后, 依序打包进新区块. 造块策略是区块链系统性能的关键因素, 也是贪婪交易打包、自私挖矿等矿工策略性行为的集中体现.

第 3 阶段: 验证. 矿工节点 M 或者代表节点 D 收到广播的新区块后, 将各自验证区块内封装的交易或者数据的正确性和合理性. 如果新区块获得大多数验证/代表节点的认可, 则该区块将作为下一区块更新到区块链.

第 4 阶段: 上链. 记账节点将新区块添加到主链, 形成一条从创世区块到最新区块的完整的、更长的链条. 如果主链存在多个分叉链, 则需根据共识算法规定的主链判别标准, 来选择其中一条恰当的分支作为主链.

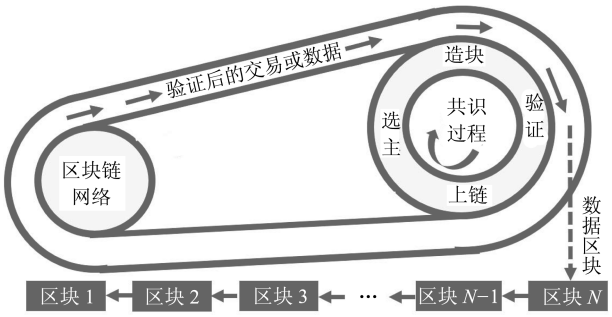

图 1　区块链共识过程的基础模型

Fig. 1　A basic model of blockchain consensus processes

区块链共识算法可以根据其容错类型、部署方式和一致性程度等多个维度加以分类. 例如, 根据容错类型, 可以将区块链共识算法分为拜占庭容错和非拜占庭容错两类; 根据部署方式, 可以将区块链共识算法分为公有链共识、联盟链共识和私有链共识三类; 根据一致性程度, 还可以将区块链共识算法分为强一致性共识和弱 (最终) 一致性共识等. 本文提出一种按照共识过程的选主策略的新分类方法, 其优点在于便于刻画共识算法的核心机理. 具体来说, 可根据选主策略 (即函数 f 的具体实现方式) 将区块链共识算法分为选举类、证明类、随机类、联盟类和混合类共 5 种类型:

选举类共识: 即矿工节点在每一轮共识过程中通过 “投票选举” 的方式选出当前轮次的记账节点, 首先获得半数以上选票的矿工节点将会获得记账权; 多见于传统分布式一致性算法, 例如 Paxos 和 Raft 等.

证明类共识: 也可称为 “Proof of X” 类共识, 即矿工节点在每一轮共识过程中必须证明自己具有某种特定的能力, 证明方式通常是竞争性地完成某项难以解决但易于验证的任务, 在竞争中胜出的矿工节点将获得记账权; 例如 PoW 和 PoS 等共识算法是基于矿工的算力或者权益来完成随机数搜索任务, 以此竞争记账权.

随机类共识: 即矿工节点根据某种随机方式直接确定每一轮的记账节点, 例如下文将要提到的 Algorand 和 PoET 共识算法等.

联盟类共识: 即矿工节点基于某种特定方式首

先选举出一组代表节点, 而后由代表节点以轮流或者选举的方式依次取得记账权. 这是一种以 “代议制” 为特点的共识算法, 例如 DPoS 等.

混合类共识: 即矿工节点采取多种共识算法的混合体来选择记账节点, 例如 PoW + PoS 混合共识、DPoS+BFT 共识等.

4 区块链共识算法的新进展

自 2014 年起, 随着比特币和区块链技术快速进入公众视野, 许多学者开始关注并研究区块链技术, 共识算法也因此进入快速发展、百花齐放的时期. 许多新共识算法在这段时间被提出. 它们或者是原有算法的简单变种, 或者是为改进某一方面性能而做出的微创新, 或者是为适应新场景和新需求而做出重大改进的新算法. 需要说明的是, 这些共识算法由于提出时间晚, 目前大多尚未获得令人信服的实践验证, 有些甚至只是科研设想; 但这些算法均具有明显的创新之处, 具有一定的大规模应用的前景, 因此我们写出来以飨读者, 并期待能够启发后续的创新研究.

4.1 主线 1: PoW 与 PoS 算法的有机结合

研究者基于 PoW 和 PoS 算法的有机结合, 相继提出了权益–速度证明 (Proof of stake velocity, PoSV)[25]、燃烧证明 (Proof of burn, PoB)[26]、行动证明 (Proof of activity, PoA)[27] 和二跳 (2-hop)[28] 共识算法, 致力于取长补短、解决 PoW 与 PoS 存在的能源消耗与安全风险问题. 2014 年 4 月, 拉里·雷恩 (Larry Ren) 在蜗牛币 Reddcoin 白皮书中提出了 PoSV 共识算法, 针对 PoS 中币龄是时间的线性函数这一问题进行改进, 致力于消除持币人的屯币现象. PoSV 算法前期使用 PoW 实现代币分配, 后期使用 PoSV 维护网络长期安全. PoSV 将 PoS 中币龄和时间的线性函数修改为指数式衰减函数, 即币龄的增长率随时间减少最后趋于零. 因此新币的币龄比老币增长地更快, 直到达到上限阈值, 这在一定程度上缓和了持币者的屯币现象. 2014 年 5 月发行的 Slimcoin 借鉴了比特币和点点币的设计, 基于 PoW 和 PoS 首创提出了 PoB 共识算法. 其中, PoW 共识被用来产生初始的代币供应, 随着时间增长, 区块链网络累积了足够的代币时, 系统将依赖 PoB 和 PoS 共识来共同维护. PoB 共识的特色是矿工通过将其持有的 Slimcoin 发送至特定的无法找回的地址 (燃烧) 来竞争新区块的记账权, 燃烧的币越多则挖到新区块的概率越高. 2014 年 12 月提出的 PoA 共识也是基于 PoW 和 PoS, 其中采用 PoW 挖出的部分代币以抽奖的方式分发给所有活跃节点, 而节点拥有的权益与抽奖券的数量即抽中概率成正比. 二跳共识于 2017 年 4 月提出, 其设计初衷是为解决 PoW 潜在的 51 % 算力攻击问题, 解决思路是在 PoW 算力的基础上引入 PoS 权益, 使得区块链安全建立在诚实节点占有大多数联合资源 (算力 + 权益) 的基础上. 换句话说, 拜占庭节点必须同时控制 51 % 以上的算力和 51 % 以上的权益, 才能成功实施 51 % 攻击, 这无疑极大地提高了区块链的安全性.

4.2 主线 2: 原生 PoS 算法的改进

原生 PoS 共识算法的改进目标主要是解决其固有的 “无利害关系 (Nothing at stake)” 问题, 形成了 Tendermint[29] 以及由其衍生出的 Casper[30]、Ouroboros[31]、Tezos[32] 和 Honeybadger[33] 等新共识算法. 原生 PoS 共识一般假设系统中的对等节点都是静态和长期稳定的, 这在区块链环境中并不现实. 2014 年提出的 Tendermint 的重大突破是使用区块、哈希链接、动态验证器集合和循环的领导者选举, 实现了第一个基于 PBFT 的 PoS 共识算法. 为解决无利害关系问题, Tendermint 节点需要缴纳保证金, 如果作恶则保证金就会被没收. Tendermint 是一种拜占庭容错的共识算法, 具有抵御双花攻击的鲁棒性, 并且可以抵御网络中至多三分之一的破坏者的攻击.

2015 年提出的 Casper 是以太坊计划在其路线图中称为宁静 (Serenity) 的第 4 阶段采用的共识算法, 尚在设计、讨论和完善阶段. 目前 Casper 总共有两个版本, 即由 Vlad Zamjir 领导的 Casper the friendly ghost (CTFG)[34] 和由 Vitalik Buterin 带领实现的 Casper friendly finality gadget (CFFG)[35]. 前者是明确的 PoS 共识, 而后者则是 PoW 和 PoS 共识的有机结合. 同时, PoS 共识的两个主要原理分别是基于链的 PoS 和基于拜占庭容错的 PoS. Tendermint 是基于拜占庭容错的 PoS 设计. 相比之下, CTFG 是基于链的 PoS 设计, 而 CFFG 则是两者的结合.

2016 年提出的 HoneyBadger 共识是首个实用的异步拜占庭容错共识协议, 可以在没有任何网络时间假设的前提下保证区块链系统的活性 (Liveness). 该共识基于一种可实现渐近有效性的原子广播协议, 能够在广域网的上百个节点上处理每秒上万笔交易. 2017 年 8 月提出的 Ouroboros 共识是首个基于 PoS 并且具有严格安全性保障的区块链协议, 其特色是提出了一种新的奖励机制来驱动 PoS 共识过程, 使得诚实节点的行为构成一个近似纳什均衡, 可以有效地抵御区块截留和自私挖矿等由于矿工的策略性行为而导致的安全攻击.

4.3 主线 3: 原生 PoW 共识算法的改进

原生 PoW 共识算法的改进目标主要是实现比特币扩容或者降低其能耗. 2016 年 3 月, 康奈尔大学的 Eyal 等提出一种新的共识算法 Bitcoin-NG[36], 将时间切分为不同的时间段. 在每一个时间段上由一个领导者负责生成区块、打包交易. 该协议引入了两种不同的区块: 用于选举领导者的关键区块和包含交易数据的微区块. 关键区块采用比特币 PoW 共识算法生成, 然后领导者被允许小于预设阈值的速率 (例如 10 秒) 来生成微区块. Bitcoin-NG 可在不改变区块容量的基础上通过选举领导者生成更多的区块, 从而可辅助解决比特币的扩容问题. 同年 8 月提出的 ByzCoin[37] 共识算法借鉴了 Bitcoin-NG 这种领导者选举和交易验证相互独立的设计思想, 是一种新型的可扩展拜占庭容错算法, 可使得区块链系统在保持强一致性的同时, 达到超出 Paypal 吞吐量的高性能和低确认延迟. 2016 年提出的 Elastico[38] 共识机制通过分片技术来增强区块链的扩展性, 其思路是将挖矿网络以可证明安全的方式隔离为多个分片 (Shard), 这些分片并行地处理互不相交的交易集合. Elastico 是第一个拜占庭容错的安全分片协议. 2017 年, OmniLedger[39] 进一步借鉴 ByzCoin 和 Elastico 共识, 设计并提出名为 ByzCoinX 的拜占庭容错协议. OmniLedger 通过并行跨分片交易处理优化区块链性能, 是第一种能够提供水平扩展性而不必牺牲长期安全性和去中心性的分布式账本架构.

为改进 PoW 共识算法的效率 (能耗) 和公平性, 研究者相继提出了消逝时间证明 (Proof of elapsed time, PoET)[40] 和运气证明 (Proof of luck, PoL)[41]. PoET 和 PoL 均是基于特定的可信执行环境 (Trusted execution environments, TEE, 例如基于 Intel SGX 技术的 CPU) 的随机共识算法. PoET 是超级账本 HyperLedger 的锯齿湖 Sawtooth 项目采用的共识算法, 其基本思路是每个区块链节点都根据预定义的概率分布生成一个随机数, 来决定其距离下一次获得记账权的等待时间. 每当一个新区块提交到区块链系统后, SGX 即可帮助节点创建区块、生成该等待时间的证明, 而这种证明易于被其他 SGX 节点验证. PoET 共识的意义在于使得区块链系统不必消耗昂贵算力来挖矿、从而提高了效率, 同时也真正实现了 “一 CPU 一票” 的公平性. 类似地, PoL 共识也采用 TEE 平台的随机数生成器来选择每一轮共识的领导者 (记账人), 从而可降低交易验证延迟时间和交易确认时间、实现可忽略的能源消耗和真正公平的分布式挖矿.

2014 年提出的空间证明 (Proof of space, PoSp)[42] 和 2017 年提出的有益工作证明 (Proof of useful work, PoUW)[43] 也是为解决 PoW 的能耗问题而提出的共识算法. PoSp 共识要求矿工必须出具一定数量的磁盘空间 (而非算力) 来挖矿, 而 PoUW 则将 PoW 共识中毫无意义的 SHA256 哈希运算转变为实际场景中既困难又有价值的运算, 例如计算正交向量问题、3SUM 问题、最短路径问题等.

4.4 主线 4: 传统分布式一致性算法的改进及其他

传统分布式一致性算法大多是非拜占庭容错的, 因而难以应用于区块链场景 (特别是公有链). 为此, 克里斯托弗 · 科普兰 (Christopher Copeland) 等结合 Raft 和 PBFT 算法的优势, 于 2014 年提出拜占庭容错的 Tangaroa 算法[44]. Tangaroa 继承了 Raft 简洁和容易理解的优势, 同时在拜占庭错误环境下也能够维持安全性、容错性和活性. 受 Tangaroa 共识启发, 2016 年 Github 平台的 Juno 项目提出一种拜占庭容错的 Raft 算法, 此后该算法演变为一种称为 ScalableBFT[45] 的专用拜占庭容错协议, 能够实现比 Tangaroa 和 Juno 更好的性能.

2015 年, Stellar.org 首席科学官 David Mazieres 教授提出了恒星共识协议 (Stellar consensus protocol, SCP)[46]. SCP 在联邦拜占庭协议和 Ripple 协议的基础上演化而来的, 是第一个可证明安全的共识机制, 具有分散控制、低延迟、灵活信任和渐近安全 4 个关键属性. 同年, 超级账本的锯齿湖项目将 Ripple 和 SCP 共识相结合, 提出了法定人数投票 (Quorum voting) 共识算法, 以应对那些需要即时交易最终性的应用场景. 2016 年, 中国区块链社区 NEO (原名小蚁) 提出一种改进的拜占庭容错算法 dBFT, 该算法在 PBFT 的基础上借鉴了 PoS 设计思路, 首先按照节点的权益来选出记账人, 然后记账人之间通过拜占庭容错算法来达成共识. 该算法改进了 PoW 和 PoS 缺乏最终一致性的问题, 使得区块链能够适用于金融场景.

2016 年, 图灵奖得主、MIT 教授 Sivio Micali 提出了一种称为 AlgoRand[47] 的快速拜占庭容错共识算法. 该算法利用密码抽签技术选择共识过程的验证者和领导者, 并通过其设计的 BA* 拜占庭容错协议对新区块达成共识. AlgoRand 只需极小计算量且极少分叉, 被认为是真正民主和高效的分布式账本共识技术.

2017 年, 康奈尔大学提出了一种称为 Sleepy Consensus (休眠共识) 的新算法[48]. 这种共识针对的是互联网环境下大规模的共识节点中可能多数都处于离线状态, 仅有少数节点在线参与共识过程的实际情况. 该研究证明, 传统共识算法无法在这种环

境下保证共识的安全性. 而采用休眠共识算法, 只要在线诚实节点的数量超过故障节点的数量, 即可保证安全性和鲁棒性.

综上所述, 区块链共识算法的演进历史如图 2 所示, 表 1 则给出了每一种共识算法的提出时间、拜占庭容错性能、基础算法以及具有代表性的应用系统或平台.

5 总结与展望

共识算法是区块链系统的关键要素之一, 已成为当前信息领域的一个新的研究热点. 本文对目前已经提出的 32 种主流区块链共识算法进行了系统性的梳理与分析. 需要说明的是, 由于近年来共识算法研究发展较快, 本文讨论的共识算法可能仅为实际共识算法的一个子集, 尚存在若干新兴或者小众的共识算法未加以讨论, 同时一些较新的共识算法仍在不断试错和优化阶段. 本文工作可望为后续的研究与应用提供有益的启发与借鉴.

以目前的研究现状而言[49−50], 区块链共识算法的未来研究趋势将主要侧重于区块链共识算法性能评估、共识算法−激励机制的适配优化以及新型区块链结构下的共识创新三个方面.

首先, 区块链共识算法在经历过一段百花齐放式的探索和创新之后, 势必会趋向于收敛到新共识算法的性能评估和标准化方面的研究. 目前, 共识算法的评价指标各异, 但一般均侧重于社会学角度的公平性和去中心化程度, 经济学角度的能耗、成本与参与者的激励相容性以及计算机科学角度的可扩展性 (交易吞吐量、节点可扩展等)、容错性和安全性等. 如何结合具体需求和应用场景[51−52], 自适应地实现针对特定性能评价目标的共识机制设计与算法优化, 将是未来研究的热点之一.

其次, 区块链的共识算法与激励机制是紧密耦合、不可分割的整体, 同时二者互有侧重点: 共识算法规定了矿工为维护区块链账本安全性、一致性和活性而必须遵守的行为规范和行动次序; 激励机制则规定了在共识过程中为鼓励矿工忠实、高效地验证区块链账本数据而发行的经济权益, 通常包括代币发行机制、代币分配机制、交易费定价机制[53] 等. 从研究角度来看, 如果将区块链系统运作过程建模

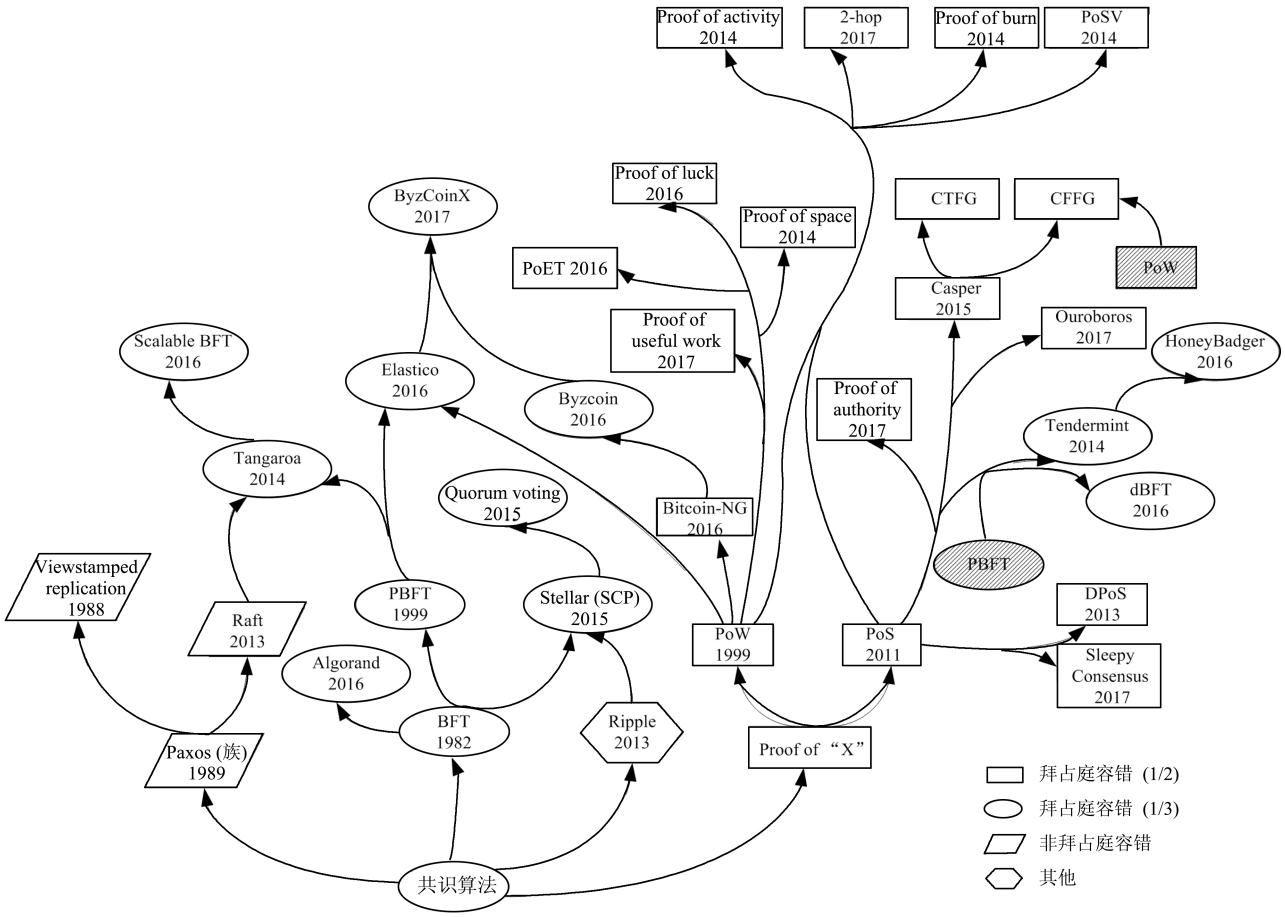

图 2 区块链共识算法的历史演进

Fig. 2 The evolutionary tree of blockchain consensus algoirthms

表 1 区块链共识算法汇总表

Table 1 Summary of blockchain consensus algorithms

名称	提出年份	拜占庭容错	基础算法	代表性应用
Viewstamped replication	1988	否	无	BDB-HA
Paxos (族)	1989	否	无	Chubby
PBFT	1999	是 (<1/3)	BFT	Hyperledger v0.6.0
PoW	1999	是 (<1/2)	无	Bitcoin
PoS	2011	是 (<1/2)	无	Peercoin, Nxt
DPoS	2013	是 (<1/2)	PoS	EOS, Bitshares
Raft	2013	否	无	etcd, braft
Ripple	2013	是 (<1/5)	无	Ripple
Tendermint	2014	是 (<1/3)	PoS+PBFT	Monax
Tangaroa (BFTRaft)	2014	是 (<1/3)	Raft+PBFT	—
Proof of activity	2014	是 (<1/2)	PoW+PoS	Decred
Proof of burn	2014	是 (<1/2)	PoW+PoS	Slimcoin
Proof of space	2014	是 (<1/2)	PoW	Burstcoin
Proof of stake velocity (PoSV)	2014	是 (<1/2)	PoW+PoS	ReddCoin
Casper	2015	是 (<1/2)	PoW+PoS	Ethereum
Quorum voting	2015	是 (<1/3)	Ripple+Stellar	Sawtooth Lake
Stellar (SCP)	2015	是 (<1/3)	Ripple+BFT	Stellar
Algorand	2016	是 (<1/3)	PoS+BFT	ArcBlock
Bitcoin-NG	2016	是 (<1/2)	PoW	—
Byzcoin	2016	是 (<1/3)	BTC-NG	—
dBFT	2016	是 (<1/3)	PoS+pBFT	NEO
Elastico	2016	是 (<1/3)	PBFT+PoW	—
HoneyBadger	2016	是 (<1/3)	Tendermint	—
PoET	2016	是 (<1/2)	PoW	Sawtooth Lake
Proof of luck	2016	是 (<1/2)	PoW	Luckychain
Scalable BFT	2016	是 (<1/3)	Tangaroa	Kadena
2-hop	2017	是 (<1/2)	PoW+PoS	—
ByzCoinX	2017	是 (<1/3)	ByzCoin+Elastico	OmniLedger
Proof of authority	2017	是 (<1/2)	PoS	Parity
Proof of useful work	2017	是 (<1/2)	PoW	—
Ouroboros	2017	是 (<1/2)	PoS	Cardano
Sleepy consensus	2017	是 (<1/2)	PoS	—

为矿工和矿池的大群体博弈过程[54] 的话, 那么共识算法将决定其博弈树的结构和形状、激励机制将决定矿工和矿池在博弈树中每个叶子结点的收益. 因此, 区块链共识算法和激励机制不仅各自存在独立优化的必要性, 更为重要地是共识–激励二元耦合机制的联合优化、实现共识与激励的 “适配”, 这是解决区块链系统中不断涌现出的扣块攻击、自私挖矿等策略性行为、保障区块链系统健康稳定运行的关键问题, 迫切需要未来研究的跟进.

最后, 随着区块链技术的发展、特别是数据层的技术和底层拓扑结构的不断创新, 目前已经涌现出若干新兴的区块 “链” 数据结构, 例如有向无环图 (Directed acyclic graph) 和哈希图 (HashGraph) 等. 这些新数据结构将以单一链条为基础的区块链技术的范畴拓展为基于图结构的区块 “链” 或分布式账本. 例如适用于物联网支付场景的数字货币 IOTA 即采用称为 “Tangle (缠结)” 的 DAG 拓扑结构, 其共识过程以交易 (而非区块) 为粒度, 每个交易都引证其他两个交易的合法性、形成 DAG 网络, 因而可以实现无区块 (Blockless) 共识; HashGraph 共识则更进一步, 基于 Gossip of gossip 协议和虚拟投票等技术, 以交易为粒度, 在特定的 DAG 结构上

实现公平和快速的拜占庭容错共识. 这些新型区块拓扑结构及其共识算法是未来发展趋势之一, 建立在这些新型数据结构之上的共识算法也值得深入研究.

References

1 Eisenberg E, Gale D. Consensus of subjective probabilities: the pari-mutuel method. *The Annals of Mathematical Statistics*, 1959, **30**(1): 165−168

2 Nakamoto S. Bitcoin: a peer-to-peer electronic cash system [Online], available: http://bitcoins.info/bitcoin.pdf, April 10, 2018.

3 Yuan Yong, Wang Fei-Yue. Blockchain: the state of the art and future trends. *Acta Automatica Sinica*, 2016, **42**(4): 481−494
(袁勇, 王飞跃. 区块链技术发展现状与展望. 自动化学报, 2016, **42**(4): 481−494)

4 Yuan Yong, Zhou Tao, Zhou Ao-Ying, Duan Yong-Chao, Wang Fei-Yue. Blockchain technology: from data intelligence to knowledge automation. *Acta Automatica Sinica*, 2017, **43**(9): 1485−1490
(袁勇, 周涛, 周傲英, 段永朝, 王飞跃. 区块链技术: 从数据智能到知识自动化. 自动化学报, 2017, **43**(9): 1485−1490)

5 Yuan Yong, Wang Fei-Yue. Parallel blockchain: concept, methods and issues. *Acta Automatica Sinica*, 2017, **43**(10): 1703−1712
(袁勇, 王飞跃. 平行区块链: 概念、方法与内涵解析. 自动化学报, 2017, **43**(10): 1703−1712)

6 Zeng Shuai, Yuan Yong, Ni Xiao-Chun, Wang Fei-Yue. Scaling blockchain towards bitcoin: key technologies, constraints and related issues. *Acta Automatica Sinica*, DOI: 10.16383/j.aas.c180100
(曾帅, 袁勇, 倪晓春, 王飞跃. 面向比特币的区块链扩容: 关键技术, 制约因素与衍生问题. 自动化学报, DOI: 10.16383/j.aas.c180100)

7 Akkoyunlu E A, Ekanadham K, Huber R V. Some constraints and tradeoffs in the design of network communications. In: Proceedings of the 5th ACM Symposium on Operating Systems Principles. Austin, Texas, USA: ACM, 1975. 67−74

8 Gray J N. Notes on data base operating systems. *Operating Systems: An Advanced Course*. Berlin: Springer-Verlag, 1978. 393−481

9 Pease M, Shostak R, Lamport L. Reaching agreement in the presence of faults. *Journal of the ACM*, 1980, **27**(2): 228−234

10 Lamport L, Shostak R, Pease M. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 1982, **4**(3): 382−401

11 Fischer M J, Lynch N A, Paterson M S. Impossibility of distributed consensus with one faulty process. *Journal of the ACM*, 1985, **32**(2): 374−382

12 Oki B M, Liskov B H. Viewstamped replication: a new primary copy method to support highly-available distributed systems. In: Proceedings of the 7th Annual ACM Symposium on Principles of Distributed Computing. Toronto, Ontario, Canada: ACM, 1988. 8−17

13 Lamport L. The part-time parliament. *ACM Transactions on Computer Systems*, 1998, **16**(2): 133−169

14 Wattenhofer R. *The Science of the Blockchain*. USA: CreateSpace Independent Publishing Platform, 2016.

15 Dwork C, Naor M. Pricing via processing or combatting junk mail. In: Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology. Santa Barbara, California, USA: Springer-Verlag, 1992. 139−147

16 Back A. Hashcash — a denial of service counter-measure [Online], available: http://www.hashcash.org/papers/hashcash.pdf, April 10, 2018.

17 Jakobsson M, Juels A. Proofs of work and bread pudding protocols (extended abstract). *Secure Information Networks*. Boston, MA, Germany: Springer, 1999. 258−272

18 Castro M, Liskov B. Practical Byzantine fault tolerance. In: Proceedings of the 3rd Symposium on Operating Systems Design and Implementation. New Orleans, USA: USENIX Association, 1999. 173−186

19 Gilbert S, Lynch N. Brewers conjecture and the feasibility of consistent, available, partition-tolerant web services. *ACM SIGACT News*, 2002, **33**(2): 51−59

20 Proof of stake [Online], available: https://en.bitcoin.it/wiki/Proof_of_Stake, April 11, 2018.

21 Schwartz D, Youngs N, Britto A. The Ripple protocol consensus algorithm [Online], available: https://ripple.com/files/ripple_consensus_whitepaper.pdf, April 10, 2018.

22 BitShares. Delegated proof of stake [Online], available: http://docs.bitshares.org/bitshares/dpos.html, April 10, 2018.

23 Ongaro D, Ousterhout J. In search of an understandable consensus algorithm. In: Proceedings of the USENIX Annual Technical Conference. Philadelphia, PA, USA: USENIX ATC, 2014. 305−319

24 Lamport L. Paxos made simple. *ACM SIGACT News*, 2001, **32**(4): 51−58

25 Ren L. Proof of stake velocity: building the social currency of the digital age [Online], available: https://assets.coss.io/documents/white-papers/reddcoin.pdf, April 10, 2018.

26 Proof of burn [Online], available: https://en.bitcoin.it/wiki/Proof of burn, April 10, 2018.

27 Bentov I, Lee C, Mizrahi A, Rosenfeld M. Proof of activity: extending Bitcoins proof of work via proof of stake [Online], available: http://eprint.iacr.org/2014/452, April 10, 2018.

28 Duong T, Fan L, Zhou H S. 2-hop blockchain: combining proof-of-work and proof-of-stake securely [Online], available: https://eprint.iacr.org/2016/716, April 10, 2018.

29 Kwon J. Tendermint: consensus without mining [Online], available: https://tendermint.com/static/docs/tendermint.pdf, April 10, 2018.

30 Ethereum′s Casper protocol explained in simple terms [Online], available: https://www.finder.com/ethereum-casper, April 10, 2018.

31 David B, Gaži P, Kiayias A, Russell A. Ouroboros Praos: an adaptively-secure, semi-synchronous proof-of-stake protocol [Online], available: http://eprint.iacr.org/2017/573, April 10, 2018.

32 Goodman L M. Tezos-a self-amending crypto-ledger position paper [Online], available: https://www.tezos.com/static/papers/position_paper.pdf, April 10, 2018.

33 Miller A, Xia Y, Croman K, Shi E, Song D. The honey badger of BFT protocols. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria: ACM, 2016. 31−42

34 Zamfir V. Introducing Casper "the Friendly Ghost" [Online], available: https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/, April 10, 2018.

35 Buterin V, Griffith V. Casper the friendly finality gadget [Online], available: https://arxiv.org/pdf/1710.09437.pdf, April 10, 2018.

36 Eyal I, Gencer A E, Sirer E G, van Renesse R. Bitcoin-NG: a scalable blockchain protocol. In: Proceedings of the 13th USENIX Conference on Networked Systems Design and Implementation. Santa Clara, USA: USENIX Association, 2016. 45−59

37 Kogias E K, Jovanovic P, Gailly N, Khoffi I, Gasser L, Ford B. Enhancing bitcoin security and performance with strong consistency via collective signing. In: Proceedings of the 25th USENIX Security Symposium. Austin, TX, USA: USENIX Association, 2016. 279−296

38 Luu L, Narayanan V, Zheng C D, Baweja K, Gilbert S, Saxena P. A secure sharding protocol for open blockchains. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria: ACM, 2016. 17−30

39 Kokoris-Kogias E, Jovanovic P, Gasser L, Gailly N, Syta E, Ford B. OmniLedger: A secure, scale-out, decentralized ledger via sharding [Online], available: http://eprint.iacr.org/2017/406, April 10, 2018.

40 Buntinx J P. What is proof of elapsed time? [Online], available: https://themerkle.com/what-is-proof-of-elapsed-time/, April 10, 2018.

41 Milutinovic M, He W, Wu H, Kanwal M. Proof of luck: an efficient blockchain consensus protocol [Online], available: https://eprint.iacr.org/2017/249.pdf, April 10, 2018.

42 Ateniese G, Bonacina I, Faonio A, Galesi A. Proofs of space: when space is of the essence. In: Proceedings of the 9th International Conference on Security and Cryptography for Networks. Amalfi, Italy: Springer, 2014. 538−557

43 Ball M, Rosen A, Sabin M, Vasudevan P V. Proofs of useful work [Online], available: https://allquantor.at/blockchainbib/pdf/ball2017proofs.pdf, April 10, 2018.

44 Copeland C, Zhong H X. Tangaroa: a byzantine fault tolerant raft [Online], available: http://www.scs.stanford.edu/14au-cs244b/labs/projects/copeland_zhong.pdf, April 10, 2018.

45 Martino W. Kadena: the first scalable, high performance private blockchain [Online], available: http://kadena.io/docs/Kadena-ConsensusWhitePaper-Aug2016.pdf, April 10, 2018.

46 Mazières D. The stellar consensus protocol: a federated model for internet-level consensus [Online], available: https://www.stellar.org/papers/stellar-consensus-protocol.pdf, April 10, 2018.

47 Gilad Y, Hemo R, Micali S, Vlachos G, Zeldovich N. Algorand: scaling byzantine agreements for cryptocurrencies [Online], available: http://eprint.iacr.org/2017/454, April 10, 2018.

48 Pass R, Shi E. The sleepy model of consensus [Online], available: https://eprint.iacr.org/2016/918.pdf, August 16, 2018.

49 Yuan Y, Wang F Y. Blockchain and cryptocurrencies: model, techniques, and applications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2018, **48**(9): 1421−1428

50 Zeng S, Ni X C, Yuan Y, Wang F Y. A bibliometric analysis of blockchain research. In: Proceedings of the 29th IEEE Intelligent Vehicles Symposium (IV′18). Changshu, China: IEEE, 2018. 102−107

51 Ni X C, Zeng S, Han X, Yuan Y, Wang F Y. Organizational management using software-defined robots based on smart contracts. In: Proceedings of the 29th IEEE Intelligent Vehicles Symposium (IV′18). Changshu, China: IEEE, 2018. 274−279

52 Wang S, Yuan Y, Wang X, Li J J, Qin R, Wang F Y. An overview of smart contract: architecture, applications, and future trends. In: Proceedings of the 29th IEEE Intelligent Vehicles Symposium (IV′18). Changshu, China: IEEE, 2018. 108−113

53 Li J J, Yuan Y, Wang S, Wang F Y. Transaction queue game in bitcoin blockchain. In: Proceedings of the 29th IEEE Intelligent Vehicles Symposium (IV′18). Changshu, China: IEEE, 2018. 114−119

54 Qin R, Yuan Y, Wang S, Wang F Y. Economic issues in bitcoin minning and blockchain research. In: Proceedings of the 29th IEEE Intelligent Vehicles Symposium (IV′18). Changshu, China: IEEE, 2018. 268−273

袁 勇 中国科学院自动化研究所复杂系统管理与控制国家重点实验室副研究员. 青岛智能产业技术研究院副院长. 2008 年获得山东科技大学计算机软件与理论专业博士学位. 主要研究方向为社会计算, 计算广告学, 区块链技术. 本文通信作者. E-mail: yong.yuan@ia.ac.cn

(**YUAN Yong** Associate professor at the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences. He is also the vice president of Qingdao Academy of Intelligent Industries. He received his Ph. D. degree of computer software and theory from Shandong University of Science and Technology in 2008. His research interest covers social computing, computational advertising, and blockchain. Corresponding author of this paper.)

倪晓春 中国科学院自动化研究所复杂系统管理与控制国家重点实验室工程师. 2008 年于大连海事大学获得管理科学与工程专业硕士学位. 主要研究方向为社会计算与区块链.
E-mail: xiaochun.ni@ia.ac.cn
(**NI Xiao-Chun** Engineer at the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences. He received his master degree in management science and engineering from Dalian Maritime University in 2008. His research interest covers social computing and blockchain.)

曾 帅 中国科学院自动化研究所复杂系统管理与控制国家重点实验室助理研究员. 2011 年于北京邮电大学获得信号与信息处理专业博士学位. 主要研究方向为社会计算, 策略优化, 区块链.
E-mail: shuai.zeng@ia.ac.cn
(**ZENG Shuai** Assistant professor at the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences. She received her Ph. D. degree in signal and information processing from Beijing University of Post & Telecommunication in 2011. Her research interest covers social computing, strategy optimaization, and blockchain.)

王飞跃 中国科学院自动化研究所复杂系统管理与控制国家重点实验室主任, 国防科技大学军事计算实验与平行系统技术研究中心主任, 中国科学院大学中国经济与社会安全研究中心主任, 青岛智能产业技术研究院院长. 主要研究方向为平行系统的方法与应用, 社会计算, 平行智能以及知识自动化.
E-mail: feiyue.wang@ia.ac.cn
(**WANG Fei-Yue** State specially appointed expert and director of the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences. Professor of the Research Center for Computational Experiments and Parallel Systems Technology, National University of Defense Technology. Director of China Economic and Social Security Research Center in University of Chinese Academy of Sciences. Dean of Qingdao Academy of Intelligent Industries. His research interest covers methods and applications for parallel systems, social computing, parallel intelligence, and knowledge automation.)