计算机科学
ISSN: 2790-0622(print)
雙清學術出版社
Contents lists available at www.qingpress.com
Journal homepage: qingpress.com/zh-cn/journals/25

公有区块链共识协议现状及未来发展

李超

北京航空航天大学，经济管理学院，北京市海淀区学院路 37 号，100191

摘要：共识协议(算法)是区块链技术的核心关键，从根本上决定了区块链网络的性能、安全性和可用性。本文简要阐述了目前最主流的两种公有区块链共识协议——PoW(Proof-of-work,工作量证明)和 PoS (Proof-of-stake,权益证明)的起源、设计理念、优势、劣势以及一些知名的改进方案。最后，本文以目前世界上最著名的公有区块链智能合约平台——以太坊为例，总结了以太坊 PoS 方案未来的发展前景和重大战略意义。

关键词：区块链,共识协议, PoW, PoS, 以太坊

Current Status and Future Development of Public Blockchain Consensus Protocols

Chao Li

Abstract: Consensus protocols (algorithms) are the core keys of blockchain technology, fundamentally determining the performance, security, and availability of blockchain networks. This paper briefly describes

作者简介：李超，男，博士，研究方向包括区块链、数字货币、去中心化金融、金融科技、金融市场、投资策略、金融风险管理和能源管理，曾在《Decision Support Systems》《Finance Research Letters》《Conversion and Management》和《Energy》等期刊发表过多篇高水平论文。联系方式：chaoli@buaa.edu.cn.

Article history: Received December 24, 2022 Accepted December 31, 2022 Available online January 3, 2023
To cite this document: 李超 (2023).公有区块链共识协议现状及未来发展.计算机科学, 第 3 卷，第 1 期，1-8 页
Doi: https://doi.org/10.55375/cps.2023.3.1

the origins, design concepts, advantages, disadvantages, and some well-known improvement solutions of the two most mainstream public blockchain consensus protocols-PoW (Proof-of-work) and PoS (Proof-of-stake). Finally, this paper takes the world's most famous public blockchain smart contract platform, Ethereum, as an example and summarizes the future development prospects and significant strategic significance of the Ethereum PoS.

Keywords: Blockchain, Consensus protocol, Proof-of-work, Proof-of-stake, Ethereum

近年来，区块链技术发展如火如荼，已经逐渐融入了包括数字金融、物联网、供应链管理、能源、政务、公益、版权等在内的多个领域。2019 年 10 月 24 日，中共中央总书记习近平在主持中共中央政治局第十八次集体学习时强调，区块链技术的集成应用在新的技术革新和产业变革中起着重要作用，要把区块链作为核心技术自主创新的重要突破口，明确主攻方向，加大投入力度，着力攻克一批关键核心技术，加快推动区块链技术和产业创新发展。

区块链技术之所以被寄予厚望，原因在于其开创了一种在信任缺失的竞争环境中低成本建立信任的新型计算范式和协作模式，凭借其独有的信任建立机制，实现了穿透式监管和信任逐级传递。相比于传统的中心化账本数据库，区块链可以在节点间信任缺乏的环境中，实现基于对等网络(P2P 网络)的去中心化信用交易，推动了实体从事涉及交易或数据共享的商业交易，摆脱了中介，提高了交易效率，降低了交易成本，公开透明、不可篡改且数据安全性较高。区块链技术实质上是解决了人类社会亘古以来的命题：信任问题。比特币便是区块链如何在互不相识的参与者之间实现信任的典型例子。因此，区块链技术被认为是继互联网之后，极具颠覆性的下一代技术创新。

区块链技术本质上是一个由所有参与方共同维护的去中心化的公共账本记录技术，这与现有大多数系统通过中心化机构来确认交易记录有着根本的区别。分布式账本的关键问题在于保证账本的一致性，即保证账本数据的完全相同以及对某个提案达成一致。传统的分布式账本主要应用在节点数量较少且相对节点可信度较高的情境下，基本不考虑拜占庭容错的问题，主要采用 VR 和 Paxos 等算法，此类算法也常用于联盟链和私有链；公有区块链系统运行在开放且信任度较低的复杂环境，系统中节点数量规模较大且往往存在恶意节点，需要考虑拜占庭容错的问题，主要采用 PoW (Proof-of-work，工作量证明)和 PoS (Proof-of-stake，权益证明)等算法。公有链节点间缺乏信任，妨碍了账本信息的协商一致，而且恶意节点可以发起例如女巫攻击这样的恶性事件，伪造两个或多个身份，可能会影响甚至操纵节点间共识的达成过程。因

此，区块链需要一种新的可靠的共识协议来解决上述问题。

总的来讲，作为区块链技术的核心，共识协议从根本上决定了整个区块链系统的性能、安全性和可用性。因此，本文的主要内容便是对代表区块链技术前沿的公有区块链共识协议进行简要分析。

一、 公有区块链共识协议现状

目前最著名且最常用的公有链共识协议主要有 PoW (Proof-of-work, 工作量证明)和 PoS (Proof-of-stake, 权益证明)。

(一) PoW (Proof-of-work, 工作量证明)

工作量证明的思想最早源于美国计算机科学家、哈佛大学教授辛西娅·德沃克 (Cynthia Dwork)，该证明要求邮件发送者必须解答出某个数学问题的答案，以证明其确实付出了一定的成本代价，从而增加垃圾邮件发送者的作恶成本，因此可以很大程度上解决垃圾邮件的问题。

2008 年 11 月 1 日，在金融危机爆发后不久，一个作者名为中本聪的人(Nakamoto, 2008)发布了比特币白皮书《比特币：一种点对点的电子现金系统》，阐述了基于对等网络(P2P)技术和加密技术的电子现金系统的构架理念，即比特币系统的基本框架。2009 年 1 月 3 日，比特币系统开始运行，标志着比特币的正式诞生。区块链是比特币运行的核心底层技术，而比特币则是区块链技术第一个成功的应用。比特币采用的共识协议是 PoW (Proof-of-work, 工作量证明)，是第一个区块链共识协议，也是目前采用最广泛的区块链共识协议。

PoW 的机制设计极为巧妙。PoW 要求节点(矿工)进行运算去解决一个求解复杂但验证容易的 SHA256 计算问题(即挖矿)，也就是找到一个随机数 Nouce，使得区块头的哈希值小于或等于难度目标的设定值。难度设定值越小，挖矿的难度就越大。为了适应矿工算力的变化，难度值会定期进行调整，以保证区块的平均生成时间基本不变。解答出该问题的概率与节点的算力大小成正比，率先求解出该问题的节点将获得记账权(即挖出一个新区块)，并得到相应数量的加密数字货币作为奖励。这样，PoW 通过提高参与记账的门槛以及提供记账的奖励，保证了系统的安全可靠运转。

PoW 共识协议的基本步骤如下：第一，广播。新交易发生后，所有交易被广播到全网的节点。第二，计算。每个节点根据前一区块生成以来的所有交易，得到区块头的 Merkle 根，并寻找随机数 Nouce，使得区块头的哈希值小于或等于难度目标的设定值。第三，选主。若某节点率先找到了正确的 Nouce，便可以将交易信息打包进新的区块，向全网广播，并得到相应的区块奖励。第四，上链。其余节点收到新区块后，验证交易信息和随机数 Nouce，如果没有问题，则新区块将链接到主链，并如此往复。

PoW 的核心思想是通过分布式节点的计算能力竞争来确保数据的一致性和共识的安全性，这使其成为一种安全可靠的公有链共识算法。在 PoW 中，如果攻击者想要篡改或伪造区块链上已经记录的数据，需要替换掉从该数据所在区块开始之后的所有区块，也就是要找到前述所有区块头的随机数 Nouce，且区块生成速度还要超过原有的主链。这就需要攻击者掌握全网至少 51%以上的算力，才能把握攻击成功的确定性，而获得全网 51%以上的算力需要极高的成本和难度，因此 PoW 区块链的安全性较高。

但是，PoW 的问题也很明显，第一，它需要消耗巨量的计算资源(验证比特币交易所需的能源甚至比挪威等整个国家的能源消耗量还多)，进而造成环境污染和能源成本上升。第二，PoW 实际上是牺牲了一部分可扩展性来换取系统的安全性和去中心化，因而 PoW 区块链性能普遍较低。第三，PoW 中交易发生后往往需要较长时间来等待确认，比如比特币需要等待 6 个区块，大约 60min，因此结算周期较长，不适合时间敏感型交易和大规模的商业应用。

(二) PoS (Proof-of-stake，权益证明)

为了解决 PoW 的诸多问题，PoS (Proof-of-stake，权益证明)应运而生。不同于 PoW 的“算力为王”，PoS 主张“权益为王”。PoS 首次出现在 2011 年的 bitcointalk 论坛(www. bitcointalk. org)上，由 King 和 Nadal 于 2012 年在 Peercoin 首次实现。在接下来的几年中，Ethereum(以太坊)和 Tezos 等大型区块链项目陆续提出了自己的 PoS 设计方案。PoS 通常根据节点(验证者)质押的权益(如质押代币的数量、质押代币的币龄等)的多少来选择下一个区块的生成者，权益越多的节点生成新区块的概率越大。PoS 近年来逐渐被业界广泛采用。MIT 在《麻省理工科技评论》中，将 PoS 纳入 2022 年“全球十大突破性技术”。世界上最著名的区块链智能合约平台——以太坊已经于 2022 年 9 月 15 日正式完成了“The merge”升级，将主网的共识协议从 PoW 转为 PoS，标志着 PoS 的发展进入到了一个新的阶段。

与 PoW 相比，PoS 具有诸多优势：

第一，节能环保，不依赖昂贵的特定挖矿设备。PoS 依据节点质押权益的多少来选取区块生成者，能耗大幅降低。

第二，区块生成时间短、吞吐量大，达成共识的速度更快。

第三，节点参与度更高，从而去中心化程度和安全性更高。通常，PoS 区块链中验证者可以从质押代币中获得相对较高的回报。但如果他们只是被动地持有 PoS 代币，而不进行质押，他们将支付所谓的铸币税(由于 PoS 代币通常会通货膨胀)，这并不符合他们的利益。因此，这会推动 PoS 代币的持有者积极地参与质押，节点数量的增多可降低系统被攻击从而瘫痪的概率，这进一步提高了 PoS 区块链网络的去中心化

和安全性。此外，PoW 中的矿工挖矿具有规模经济效果，使得主流大矿池占据越来越多的算力份额，而 PoS 在相当程度上减轻了这种份额向头部集聚的趋势。

第四，安全性更高。如果 PoS 中的攻击者想要发动“51%攻击”，持有超过 51%数量的代币的难度远超 PoW 中拥有 51%的算力(因为代币数量有限，而算力可视为无限)，因此系统的安全性大大提高。

第五，不同于 PoW 通常存在的通货紧缩，PoS 往往通过新发代币或者支付质押的利息收益来奖励验证者，因而可以保持代币数量的合理增长。

由此可见，由于 PoS 仅需要验证者参与质押，且参与难度和成本更低，更多的验证者可以参与到达成共识的过程中，这意味着它可以提供更高级别的能源效率、可扩展性、去中心化水平和安全性。

尽管在早期围绕 PoS 的一些问题存在不小的争议，但根据学界和业界的研究实践来看，相应的解决方案已经出现。不少学者在早年间就认为 PoS 存在“Nothing at stake”(无利害关系)问题，但是通过保证金对验证者进行惩罚可以有效解决这一问题。也有部分学者认为 PoS 将加剧代币的集聚，从而使得富人变得更富裕。然而 Roşu 和 Saleh(2021)以及 Saleh(2021)证明了这些直觉是错误的，PoS 并不会导致财富积累和富人更富，反而会带来稳定的持有份额。此外，PoS 一个容易被忽略的缺点在于质押机制会促进代币的囤积而不是被用于流通消费，不过对验证者的奖励会增加 PoS 代币的供给，可在一定程度上缓解代币囤积的问题。

总的来讲，PoW 当前被采用比例较高，发展较为成熟，在算力较高的情况下安全性较高，与此同时也存在着可扩展性较差、能源消耗较多以及随着挖矿专业化竞赛而来的节点中心化的问题。PoS 可扩展性较好，能源消耗量较少，但可能机制设计较为复杂且运行不够成熟、未经过长时间检验的问题，目前仍在迅猛发展之中。

(三) PoW 和 PoS 的改进协议

如果说 PoW 和 PoS 都有各自的优缺点，那么将两者结合起来会有好的效果吗？Bentov 等(2014)引入了一种基于 PoW 和 PoS 结合的共识算法，PoA(Proof of Activity，活动证明)。PoA 通过 PoW 的挖矿机制来产生新区块，同时根据 PoS 中节点质押权益的多少来选出验证者，对交易进行验证。该算法是一种更高安全级别的算法，只有当预定数量的验证者认为该区块有效时，其才能被永久附加到区块链中；PoA 受到 51%攻击的概率几乎为零，因为这种攻击需要攻击者同时拥有 51%的挖矿能力和 51%的所有代币，所以相对于 PoW 和 PoS，PoA 更加安全。另一方面，PoA 利用了 PoW 的挖矿机制，因此仍然无法摆脱需要消耗大量能源和计算能力的缺陷。

DPoS(Delegated proof of stake，委托权益证明)，由 Daniel Larimer 在 2013 年 8 月提出，并成功应用于比特股(BitShares)项目。该方法是对 PoS 的改进，节点通过投票来选择少数代表(验证者)，来生成并验证新的区块。相比于 PoS 依赖验证者的权益多少，DPoS 更看重验证者的信誉，信誉不佳的验证者不会得到较多的选票。如果选定的代表在提交信息时出现延迟或错误，网络的节点可以投票决定其替换，这约束着验证者按照规则行事。在成功生成新区块后，验证者将分配给投票者相应的区块奖励。DPoS 中验证者的数量较少，因此整个网络的工作变得高效。简单来讲，DPoS 的主要优势是可扩展性强、高效和成本低。但其缺点也较为明显，由于验证者的数量较少且收益较多，可能会催生多个验证者或其与节点的共谋获利，以及对某个验证者的声誉攻击。此外，尽管一些知名区块链项目如 EOS 和 TRON 使用了 DPoS，但其仍是一种半中心化的共识协议，更适合用于联盟链和私有链。

DAG(有向无环图)是一种数据结构形式，简单来讲就是多条支链与主链并存，这些链的大方向一致且不存在环路，其不是传统意义上的区块链网络，但已经被广泛使用。DAG 区块链最初的雏形是 2013 年以色列希伯来大学学者在 bitcointalk 论坛上提出的 GHOST 协议，即比特币的扩容技术方案。目前，IOTA、Byteball、NANO 和 Conflux 是最成功的 DAG 区块链。在传统的区块链网络中，交易存储在一个区块链中，但在 DAG 中，交易以拓扑的方式存储在一个“图”中。DAG 由于其无区块结构，被认为是没有区块的区块链。在区块链中，需要设置一段时间，即区块时间，节点利用这一时间来验证链的哪个分支是正确的，只允许存在一条主链。而在 DAG 中，网状拓扑可以并发写入，允许多线程存在，可以解决传统区块链的高并发问题。因此，DAG 网络上没有挖矿过程，不依赖于特殊的硬件，因此功耗非常低。此外，交易的验证几乎立即发生，交易费用可以非常低。因此，DAG 网络对小微交易支付十分友好。例如，物联网链每秒可以处理超过 10，000 笔交易。DAG 网络的这些特性，以及防御 51%攻击的能力，使其成为物联网和机器间通信的较完美方案。DAG 的主要缺陷在于，其本身是异步操作，可能会导致节点间的存储的数据出现偏差，交易确认时间会更长；多链结果很容易产生“双花”问题。

总的来讲，以上区块链共识机制都有各自的优势和劣势，或多或少存在一些问题，如果倾向于同时满足去中心化程度较高、能源消耗较低、一致性强以及可以大规模应用等条件时，PoS(权益证明)不失为一种理想的选择，而这也正是被目前业界和学界寄予厚望的发展方向。

二、公有区块链共识协议未来的发展趋势——以以太坊(Ethereum)为例

作为目前世界上最活跃、开发者规模最大的公有区块链智能合约平台，以太坊的一举一动都吸引着区块链爱好者的关注，并在某种程度上代表了区块链行业的最新进展。这里以以太坊 PoS 为例，简要阐述主

流区块链协议未来的发展方向。

以太坊诞生之初采用的共识协议是 PoW，今年以太坊进行了计划已久的共识协议转换升级“The merge”，该升级是以太坊有史以来最重大的一次技术升级。根据以太坊官方社区的公告(https://ethereum.org/en/)，“The merge”升级已经于 2022 年 9 月 15 日成功执行。“The merge”是将以太坊的原始执行层(自创立以来就存在的主网)与新的权益证明共识层——信标链(Beacon Chain)结合起来。它使网络能够用以太坊代币 ETH 进行质押，从而取代能源密集型挖矿，实现了以太坊从 PoW 向 PoS 的过渡，并降低了约 99.95%的能耗。这是实现以太坊愿景的极为重要的一步——更多的可扩展性、安全性和可持续性。

以太坊 PoS 为分片奠定了基础。区块链的三个理想属性是去中心化、安全和可扩展。区块链不可能三角指出，简单的区块链架构只能实现三个理想属性的三分之二。一个安全且去中心化的区块链可能需要牺牲可扩展性。分片是一种重要的提高以太坊可扩展性的协议改进方案，它根据用户地址将区块链拆分成许多独立的分片(并发区块链)，每个分片内均运行一条独立的子链。在分片实施后，PoW 不再适合以太坊，因为每个分片内的算力会大幅下降，系统的安全性也会随之降低，此时 PoS 是更加适合的选择。

以太坊 PoS 提高了系统的安全性。以太坊开发者认为，由于网络的验证者必须将大量的 ETH 质押到协议中，如果他们试图攻击网络，该协议会自动销毁他们的 ETH。此外，在代币发行方面，“The merge”升级将使每年的 ETH 发行量从目前的净 3.5% 减少到大约净 0%，大幅降低了 ETH 的通货膨胀，甚至导致了通货紧缩，这将有利于 ETH 的保值增值。

但以太坊 PoS 也并非完美无瑕。以太坊社区认为“The merge”将会使以太坊更为安全，原因在于更多的节点将参与到以太坊的质押过程中来，帮助系统进行交易确认。如果情况恰恰相反，验证者的数量过少，攻击者便可以较容易地操纵 PoS 区块链，系统将存在较大的风险。值得注意的是，采用共识协议的区块链的重要意义在于避免必须依赖中心化的中介机构来验证交易，如果缺乏有意义的去中心化，以太坊本身存在的价值将受到严重挑战。具体情况如何，如前文所述，笔者认为 PoS 可能仍需经历较长时间的考验。以太坊区块链作为世界上使用最广泛的区块链之一，是 Web3、NFT 和去中心化金融等前沿金融创新和科技创新的主要平台，在笔者看来，“The merge”升级可被视为全球区块链开发者和爱好者进行的一次伟大探索和试验，是对 PoS 协议的一次全方位综合检验，对区块链技术的发展以及未来大规模应用落地意义重大。

参考文献：

[1] 刘懿中，刘建伟，张宗洋，徐同阁，喻辉．区块链共识机制研究综述[J]．密码学报，2019，6(04)：395-432

[2] 邵奇峰，金澈清，张召，钱卫宁，周傲英．区块链技术：架构及进展[J]．计算机学报，2018，41(05)：969-988.

[3] 王劲松，杨唯正，赵泽宁，魏佳佳．基于有向无环图的区块链技术综述[J]．计算机工程，2022，48(06)：11-23.

[4] 夏清，窦文生，郭凯文，梁赓，左春，张凤军．区块链共识协议综述[J]．软件学报，2021，32(02)：277-299.

[5] 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.

[6] Chiu J, Koeppl T V. Blockchain-based settlement for asset trading[J]. The Review of Financial Studies, 2019, 32(5): 1716-1753.

[7] Li C, Wang L, Yang H. The optimal blockchain asset trading settlement based on PoS protocol[J]. Decision Support Systems, 2022: 113909.

[8] Li C, Yang H. Will memecoins' surge trigger a crypto crash? Evidence from the connectedness between leading cryptocurrencies and memecoins[J]. Finance Research Letters, 2022, 50: 103191.

[9] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Decentralized Business Review, 2008: 21260.

[10] Roşu I, Saleh F. Evolution of shares in a proof-of-stake cryptocurrency[J]. Management Science, 2021, 67(2): 661-672.

[11] Saleh F. Blockchain without waste: Proof-of-stake[J]. The Review of financial studies, 2021, 34(3): 1156-1190.