

企业级区块链读书报告



题目 公有区块链的共识协议文献综述

作者姓名 肖文翰

作者学号 22151245

学科专业 软件工程

所在学院 软件学院

提交日期 二〇二二 年 一 月

A Systematic Literature Review on Public Blockchain Consenus Algorithms

Major Subject: Software Engineering

By

Xiao Wenhan

Zhejiang University, P.R. China

2021

摘要

区块链是诞生于比特币的一种新兴技术，利用分布式账本的方式解决了传统交易中需要依赖中心化的第三方机构的信任问题。共识算法在区块链的技术体系中扮演了不可获取的角色，它不仅验证了交易系统中每一笔交易的正确性，也帮助系统中所有节点记录的账本能够在有限的步骤中达成一致，即完成系统中所有节点对当前系统交易状态的共识。区块链中的共识算法算法可以分为两大类。第一类是基于证明的共识，它要求记账的节点通过某种方式证明自己拥有记账的资质。第二类是基于投票的共识，它要求节点在记账前通过网络交换关于交易的信息来达成一致，由于这类共识算法需要每个节点了解系统中的网络结构，一般用于联盟链或私有链。在本文中，我们重点关注应用于公有区块链上的第一类共识算法从开始到发展至今研究进展的梳理。

**关键词**：共识算法、区块链

Abstract

Blockchain is an emerging technology born from Bitcoin, which uses distributed ledger to solve the trust problem that traditional transactions need to rely on centralized third-party institutions. Consensus algorithm plays an unattainable role in the technical system of blockchain. It not only verifies the correctness of every transaction in the trading system, but also helps all nodes in the system record ledger to reach agreement in a limited number of steps, that is, to complete the consensus of all nodes in the system on the current system transaction status. Consensus algorithms in blockchain algorithms can be divided into two broad categories. The first type is proof-based consensus, which requires the bookkeeping node to prove in some way that it is qualified to do so. The second type is consensus based on voting, which requires nodes to reach agreement by exchanging information about transactions through the network before accounting. Since this kind of consensus algorithm requires each node to understand the network structure in the system, it is generally used for alliance chain or private chain. In this paper, we focus on the research progress of consensus algorithm of the first type from the beginning to the development up to now .

**Keywords：**consensus algorithm, blockchain

1引言

中本聪在2009年为了解决电子支付问题发明了比特币[1]。区块链作为其中的一项关键技术为比特币在去中心化的分布式环境下构造正确的账本提供了支持。作为一个典型的分布式系统，共识算法在保证各节点账本的一致性上扮演了不可或缺的角色。在传统的分布式系统中，为了通过不断交换节点间的信息完成节点间的共识，整个系统的网络结构必须是已知且可配置的，而这与公有链节点数目众多且加入和退出都自由的特点冲突，因此一些传统的分布式共识算法例如应用在无拜占庭错误下的RAFT算法[2]以及可以拜占庭容错的PBFT算法[3]都不适合应用于公有链。

由于公有链具有的连接自由的特点，将类似人类世界的共识[4]直接应用于公有链的共识是非常困难的。由于节点数量众多且难以监管，节点之间交换协议的通信变得非常复杂，更严重的是，在公有链中节点的行为是不可控的，他们未知的行为很有可能对分布式账本造成破环。因此，比特币以及之后应用于各种公有区块链系统中共识算法都采用了类似的思路，即将修改账本工作的权限控制起来，与一份证明进行绑定，所有想要进行记账的节点都需要完成这个证明，显示出它们比其他节点更有资格完成这项工作，同时其他节点在更新自己账本的时候需要对该证明进行验证，确保进行此更新的节点完成了事先规定的证明。按照此思路设计的共识算法都被称为基于证明的共识。

在这篇综述中，我将重点关注这种基于证明的共识，首先介绍开山鼻祖PoW算法并分析其存在的问题，之后介绍在其基础上进行改进的各种算法。

**2 综述**

2.1PoW算法

在区块链系统中，为了让一笔交易在节点间达成共识，节点将交易广播出去，之后记账节点会将多笔交易打包成一个区块并将区块广播出去，由其他节点验证后修改自己本地的账本。如果广播区块的工作不做控制，所有人都可以进行任意的打包和广播，将会导致账本的混乱。为了解决这一问题，PoW算法要求想要进行打包的节点完成一个可以被其他节点验证的难题来获得打包交易的权力，并且一段时间内只有第一个完成工作的节点才可以得到认可。这个难题在PoW的表现形式为，节点将其已验证的交易进行计算得到Merkel根，之后生成一个随机数，将该随机数、Merkel根以及其他的一些预先规定的信息一起进行SHA-256计算[5]。如果计算结果小于当前系统统一规定的给定难度，则完成工作量证明难题，获得本次的记账权，可以将附有该随机数的区块进行广播并收获一定量的奖励。否则需要调整自己的随机数并再次进行计算直到自己完成工作量证明或得到其他节点完成工作量证明的信息，之后开始下一轮的打包和计算。这一过程是非常困难的，在成千上万的节点共同工作的情况下，大约十分钟才能有一个节点完成一次工作量证明，使链上新增区块的平均速度为每 10 分钟 1 个区块。由于为了争夺一次记账权需要做大量的工作，该算法被成为工作量证明算法。

2.2资源浪费问题

由于挖矿激励的机制，越来越多的节点开始通过升级硬件的手段提高自己的挖矿速度，随之上升的还有挖矿消耗的电量。据估计[6]，现在比特币的年用电量以接近小型国家的年用电量。

为了解决资源浪费问题，一方面，有研究改进了工作量证明需要解决的难题的表现形式，通过让节点计算Cuckoo哈希函数来制造足够多的循环来实现工作量证明[7]。另一方面，有研究希望将算力应用到数学领域来解决现实生活中真正的数学难题，例如寻找最长素数链的难题可以在一定程度上满足要求[8]。通过寻找满足一定要求的数字，不仅可以实现系统中的共识算法，也可以为科学家探索坎安宁链的分布做出贡献，从另一个角度解决了资源浪费问题。

2.3算力中心化问题

在比特币最初提出的时候，由于全网算力还处于较低和分散的级别，原始工作量证明算法结合区块链可以有效抵御双花攻击。随着区块链的发展，越来越多的挖矿节点为了获得稳定的收益开始加入矿池[9]工作。这就使得矿池的算力开始远远超过个人矿工，矿池在收获了更多收益后可以投入更多的资金升级设备并进一步提升自己的算力，在这种正反馈机制下，系统中将会出现算力过于集中的问题，一方面会导致矿池逐渐获得作恶的可能，即接近全网一半的算力，另一方面个人矿工进行挖矿的积极性会下降，使系统逐渐失去活力。

为了应对矿池采矿的问题，Miller等人[10]提出了一种改变机制，将原来的PoW作为新算法的第一阶段，同时设计了需要暴露私钥的第二阶段PoW，由于第二阶段的计算需要结合自己在打包交易时coinbase交易中设置的公钥对应的私钥需要暴露自己的私钥，因此矿池主不能将第二阶段分配给其他矿工进行工作，否则将会导致收益被人非法窃取。

为了应对算力中心化带来的不公正问题，PoS算法被提出了，区别于工作量证明中的证明自己完成了某项工作，PoS证明最初的形式是证明自己拥有某一笔钱，Bentov 等人[11]提出了一种基于拥有的聪来寻找矿工的方法，这个方法被称为 Follow-the-Satoshi算法，其中Satoshi为比特币系统中货币的最小单位，被称为聪。此算法的输入为当前区块链的状态以及一个随机数，输出为一个代表对应Satoshi的数，介于 0 和 Satoshi 总数之间。之后寻找创建此 Satoshi 的块，以及包括这个 Satoshi 在内的所有交易，以确定这个 Satoshi 的最后一个所有者，他将获得下一次的记账权。为了提高系统的记账效率，排除废弃节点和作恶节点的干扰，即选定的 Satoshi 的所有者没有成功创建区块，还有一种额外的惩罚机制，如果选择的 satoshi 在连续 3 次没有成功创建新的区块，它将被列入黑名单，不能再获得记账权。

2.4双花攻击与等待时间问题

在区块链系统中，由于分叉机制的存在，攻击者可以通过在主链以外的其他分叉上工作的方式逆转已被某些节点验证的交易，这就是所谓的双花攻击。为了避免双花攻击，区块链系统中的交易一般需要等待六个区块的确认之后才会生效，因为攻击者试图颠覆六个区块的难度相对较大，但是考虑到区块的平均生成时间为十分钟，接近一个小时的等待时间对于小额交易来说是不可接受的，因此有许多研究从提高交易交易速度和提高安全性等方面来解决这一问题。

Bitcoin-NG 共识模型中[12]，将传统区块分为两种不同的类型，称为关键块和微块。当节点完成工作量证明难题后，除了会广播他的区块，这里为关键块，还会将其自身角色转变为领导者，直到另一个矿工找到另一个合适的随机数。 在担任领导者期间，该节点会发布一些包含小额交易的微区块，这些交易能够被快速的验证，大大提高了整个系统对于小额交易的处理速度。

在比特币系统中，挑选主链的方法被称为累计最大工作量,唯一一条具有累计最大工作量的链作为主链，其他分叉被抛弃。而GHOST 协议采用的是一种叫最重链的规则，将分叉区块也作为挑选主链的考量依据[13]。由于最重链代表网络中的大部分算力,GHOST 规则在高吞吐量的情况下也能保证安全性。

参考文献

1. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Decentralized Business Review, 2008: 21260.
2. D. Ongaro and J. K. Ousterhout, “In search of an understandable consensus algorithm,” in Proceedings of 2014 USENIX Annual Technical Conference, Philadelphia, PA, 2014, pp. 305-319.
3. M. Castro and B. Liskov, “Practical Byzantine fault tolerance,” in Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, LA, 1999, pp. 173-186
4. The Public Disputes Program, “A short guide to consensus building,” [Online]. Available: http://web. mit.edu/publicdisputes/practice/cbh\_ch1.html.
5. Bitcoinwiki, “SHA-256,” 2016 [Online]. Available: https://en.bitcoin.it/wiki/SHA-256.
6. De Vries A. Bitcoin’s growing energy problem. Joule, 2018,2(5):801−805. [doi: 10.1016/j.joule.2018.04.016]
7. K. Schwarz, “Cuckoo Hashing,” [Online]. Available: http://web.stanford.edu/class/cs166/lectures/13/ Small13.pdf.
8. S. King, “Primecoin: cryptocurrency with prime number proof-of-work,” 2013 [Online]. Available: http://primecoin.io/bin/primecoin-paper.pdf.
9. CoinDesk Inc., “What are bitcoin mining pools?,” 2014 [Online]. Available: https://www.coindesk. com/information/get-started-mining-pools/.
10. A. Miller, A. Kosba, J. Katz, and E. Shi, “Nonoutsourceable scratch-off puzzles to discourage bitcoin mining coalitions,” in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, New York, NY, 2015, pp. 680-691.
11. I. Bentov, A. Gabizon, and A. Mizrahi, “Cryptocurrencies without proof of work,” in Financial Cryptography and Data Security. Heidelberg: Springer, 2016, pp. 142-157.
12. I. Eyal, A. E. Gencer, E. G. Sirer, and R. V. Renesse, “Bitcoin-NG: a scalable blockchain protocol,” in Proceedings of the 13th Usenix Conference on Networked Systems Design and Implementation, Berkeley, CA, 2016, pp. 45-59.
13. Sompolinsky Y, Zohar A. Secure high-rate transaction processing in Bitcoin. In: Proc. of the Int’l Conf. on Financial Cryptography and Data Security. 2015. 507−527. [doi: 10.1007/978-3-662-47854-7\_32]