Computer Science and Application 计算机科学与应用, 2022, 12(11), 2492-2500
Published Online November 2022 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2022.1211255

Hans汉斯

基于区块链DPoS共识算法的改进

王　昕

佛山科学技术学院机电工程与自动化学院，广东　佛山

收稿日期：2022年10月11日；录用日期：2022年11月9日；发布日期：2022年11月16日

摘　要

本文针对区块链共识算法中授权股权证明DPoS (Delegated Proof of Stake)的工作机制和流程研究发现，该算法明显存在两个安全隐患：一是在该算法中的部分节点上存在投票不积极，二是存在不可避免的腐败节点。针对上述两个问题，本文通过引入激励机制调节区块的生成难度及成本，提升节点生成区块的积极性。通过对节点激励值进行监督来提升腐败节恶意生成区块的成本，进而有效解决上述两个问题，这样就可以使整个区块链的安全性、稳定性得到大大提升。

关键词

区块链，共识算法，DPoS，激励机制

Improvement of DPoS Consensus Algorithm Based on Blockchain

Xin Wang

School of Electrical, Mechanical Engineering and Automation, Foshan University of Science and Technology, Foshan Guangdong

Received: Oct. 11th, 2022; accepted: Nov. 9th, 2022; published: Nov. 16th, 2022

Abstract

This paper focuses on the discovery of a working mechanism and process of Delegated Proof of Stake (DPoS) in the blockchain consensus algorithm and finds that has two obvious security problems in the algorithm: one is that some nodes in the algorithm do not vote actively, the other is that there are inevitable corrupt nodes. In order to solve the above two problems, we introduce an incentive mechanism to adjust the difficulty and cost of block generation and improve the enthusiasm of node block generation. By monitoring the incentive value of nodes to increase the cost of malicious blocks, and then effectively solve the above two problems, the security and stability of the whole blockchain can be greatly enhanced.

文章引用: 王昕. 基于区块链 DPoS 共识算法的改进[J]. 计算机科学与应用, 2022, 12(11): 2492-2500.
DOI: 10.12677/csa.2022.1211255

Keywords

Blockchain, Consensus Algorithm, DPoS, Incentive Mechanism

1. 引言

区块链这一概念是由中本聪于 2009 年在他发表的比特币白皮书中首次提出[1]，区块链的首次亮相和应用就是在比特币领域中，比特币从本质上来说是指，通过运用分布式存储、共识机制[2]、密码学、时间戳等技术将其内部几个互相独立企业互不信任的关键节点“连接起来”，并取得互相信任，从而最终达到交易的目的。

共识机制是区块链的核心机制，其目的是确保与处于分布式网络中的节点的交易信息、目的达成一致或是生产的区块被网络中的大多数节点认可。PoW 作为比特币的底层共识机制[3]，其原理为节点基于自身的算力对区块链给出的基于 SHA-256 哈希函数问题求解，并进行验证，进而争夺记账权，即所谓的“挖矿”。PoW 共识机制有着明显的缺陷：算力浪费，只能通过暴力搜索的方式完成求解；算力集中，节点算力越强，意味着越容易获取记账权。PoS 共识机制基于币龄的理念[4]，是针对 PoW 中节点记账权力归属的改进。该共识机制会根据挑选出的记账节点按币龄顺序排列，依次生产区块，PoS 同样存在着明显的缺点：币龄问题，越早加入的节点，币龄越大，更容易获取记账权，意味着对新加入的节点不友好。实用拜占庭容错算法(PBFT)是由 Miguel Castro 等人[5]在原始拜占庭算法(BFT) [6]上做的进一步优化所得。相较于原始算法而言，新算法的容错性更高。在达到共识的过程中，区块链的各个节点上的用户通过验证受到的数字签名使得信息能够在彼此之间分享，达到了较好的监督作用。但其缺点就是网络不稳定时，很可能会导致信息延迟，因此，它的应用范围较为狭窄。DPoS 共识算法类似于“董事会决定”[7]，它能将 PoS 共识机制中的众多记账者转换成只能由很少一部分代表节点来决定生产区块，这部分代表节点类似于公司中的股东大会，他们在区块链中做出重要决策，这种机制极大地提高了整个系统的吞吐量。如果该记账的节点出现故障或者利用记账权利来作恶，DPoS 中的节点会选取新的记账节点。当出块完成后，根据节点的权益比例分配奖励。DPoS 共识算法的记账节点比较少，所以使得交易效率更高，而且不会出现链分叉攻击，能够确保最终交易一致。

然而现有的 DPoS 共识算法存在一些不足。首先是节点投票参与度低，积极性不高。在实际生活中，参与投票选举会耗费个人的时间，且无法得到补偿，通常参与投票后的选举结果对其个人来说是关联性不大的。所以投票节点都存在着惰性。其次，节点的账户余额量可影响因素较大。某一节点账户余额量越多，其投票权重越大，这将意味着投票权更容易被少数账户余额量大的节点所掌控，因此，当存在恶意节点的账户余额量多时，更容易被选为代理节点。文献[8]将 DPoS 与 BFT 相结合，提升了生产区块的效率，同时也带来了生成恶意节点概率的增大，存在相应的安全隐患。文献[9]提出了一种基于环的协调器选举算法，降低了生产区块的成本。文献[10]提出了一种带有降级制度的 DPoS 共识算法，将检测到的恶意节点通过降级制度将其剔除出去，提高系统的稳定性。文献[11]提出了一种基于节点行为监控和 Borda 计数投票的改进共识算法，将节点生成块的行为作为节点选举的参考指标，会增加行为不良节点的选举难度，从而选出的节点更安全、更公平。文献[12]将 DPoS 与 PoP 相结合，利用 DPoS 算法的效率弥

补了 PoP 算法在系统效率方面的不足，PoP 算法中基于概率的挖掘行为也显著削弱了 DPoS 算法中超节点进行垄断行为或其他恶意行为的能力。

本文基于现有的 DPoS 共识算法，提出了一种激励机制的 DPoS，其优势在于：1) 可以通过引入激励机制调节区块的生成难度及成本，提升节点生成区块的积极性；2) 通过对节点激励值进行监督来提升腐败节恶意生成区块的成本；3) 通过实验仿真进行验证，激励机制下的 DPoS 共识算法能够有效提升生产区块效率，降低共识时延。

2. 背景知识

2.1. DPoS 共识算法流程

DPoS 共识算法工作流程分为两个阶段[13]。在投票选举阶段中，代币持有节点必须使用代币下注才能参加投票选举。投的代币越多，其票数就越多。在投票期间，已押注的代币被锁定在智能合约中，在选举时，系统将获得票数超过总票数 50%的节点放入候选池，对候选池内的节点进行排序，选出前 N (通常为 101)位节点，将其认证为 bp (区块生产者)，直至选举出足够数量的 bp。投票选举流程如图 1 所示。

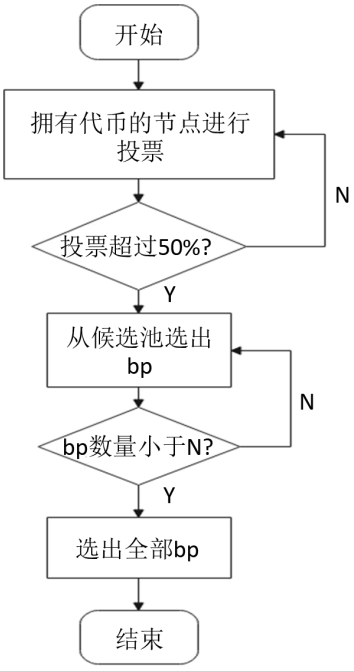

Figure 1. Flow chart of the voting stage
图 1. 投票选举阶段流程图

在共识阶段中，被选举的代表将被定义为区块生产者(bp)，他们验证交易、创建新区块和维护网络，即负责整个网络的运行。共选出 N 个区块生产者(比如 Bitshares 为 101、Asch 为 51、EOS 为 21)。被投票选举出的 N 个区块生产者轮流生成区块，每一位 bp 生产区块时，都将接受其他节点的监督。如果该 bp 在其生产区块环节未生成区块或是恶意生成错误区块，将受到监督节点的举报并且受到相应的惩罚，接着从候选池中重新选择一个节点成为 bp，参与生成区块的过程。当 bp 生产的区块得到(2/3 N + 1)个 bp 验证成功后，该区块才可被定义为正确区块，该 bp 将可获取相应的奖励。直至循环 10 此或达到设定的时间，共识过程结束，再次进行投票选举，重新选举出新的 bp。如图 2 所示。

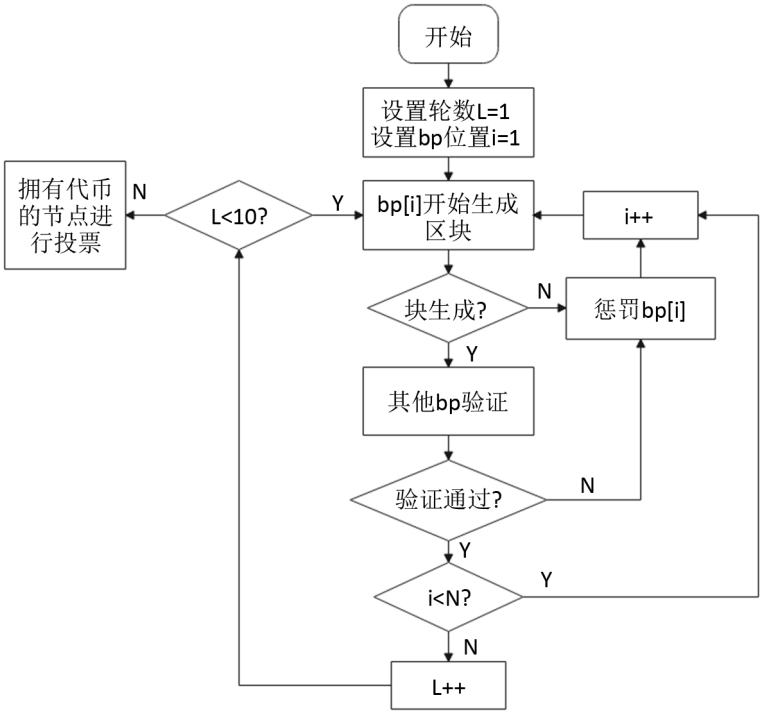

Figure 2. Flow chart of consensus stage
图 2. 共识阶段流程图

2.2. DPoS 共识算法不足点分析

在 DPoS 算法中存在着如下问题：

1) 节点投票参与度低，积极性不高。在实际生活中，参与投票选举会耗费个人的时间，且无法得到补偿，通常参与投票后的选举结果对其个人来说是关联性不大的。所以投票节点都存在着惰性。

2) 节点的账户余额量可影响因素较大。某一节点账户余额量越多，其投票权重越大，这将意味着投票权更容易被少数账户余额量大的节点所掌控，因此，当恶意节点的账户余额量多时，更容易被选为bp。

3) 区块生产者(bp)即使生成区块，被验证通过，所获得的奖励也是极少的，因此，可能出现“消极怠工”行为。

3. 改进方案

3.1. 激励机制 DPoS 共识算法的原理

通过引入激励机制对节点进行测评。根据节点在当前周期内的表现，对节点进行激励。如果节点表现良好，则其激励值会逐渐增大，否则激励值会逐渐减小。激励值是表示节点综合能力的一种方式。在激励机制的 DPoS 中，设定 Incentivizes 值(In)，其数字越大，激励值越高，意味着该节点越值得被信任，更容易的被选举为代理节点，对于激励值过低的节点，将限制被选举为代理节点。对于新添加的节点，其激励初始值为 0.5。激励值范围通常在 0 到 1 之间。对于某一节点，其激励值如下所示：

$$\mathrm{In} = \frac{1}{1+\mathrm{e}^{-(\theta * Sc)}} \tag{1}$$

$$\mathrm{Sc} = \alpha * T + \beta * P_{ij}^{t} \tag{2}$$

$$T = \frac{\lambda * \text{S\_amount} - \mu * \text{E\_amount} - \varphi * \text{F\_amount}}{\text{A\_amount}} \tag{3}$$

$$P_{ij}^{t} = P^{t}\left(P_i, P_j\right) = \frac{\sum_{k=1}^{n} f\left(x\right)}{n} \tag{4}$$

$$f\left(k\right) = f_k = \eta^{n-k}, 0 < \eta < 1, 1 < k < n \tag{5}$$

In 为最终的激励值，Sc 是节点的综合评分，θ 为可调节的激励系数，T 为节点自身的行为评分，P_{ij}^{t} 为节点 i 对节点 j 在 t 时段内 n 次行为的评分，α、β 为行为评分与评价评分的权重系数，S_amount 代表节点良好行为次数(选举投票或是成为 bp 后生产区块并被验证通过)，E_amount 代表节点无效行为的的次数(成为 bp 后没有及时生成区块)，F_amount 代表恶意行为的次数(成为 bp 后生成错误区块)，A_amount 代表节点行为的总次数；λ、μ、φ 是节点进行良好、无效、恶意行为的权重系数。P_i 代表节点 node_i，P_j 代表节点 node_j。$f(x)$是一个衰减函数，为节点在第 k 个时段内进行的行为相较于第 n 个时段内(当前时段)行为评价的变换幅度，f_k 为衰减因子，意味着节点 i 对节点 j 的评价机制并不是线性改变，例如在计算节点在第一次行为时，其 $f_1 = \eta^{n-1}$；计算在第 n 个时段内其衰减因子为 $f_n = 1$，也就是未经衰减。

由上述可得知，节点在近期行为的影响将会更大，意味着节点需要在每一次的行为中都需要表现良好才可稳定提升激励值。

基于激励机制的 DPoS 共识算法流程如图 3 所示。

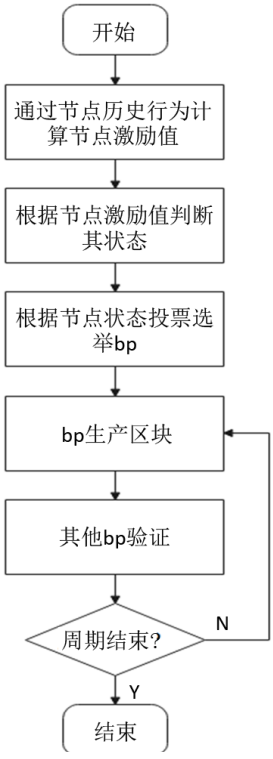

Figure 3. Flow chart of DPoS consensus algorithm based on incentive mechanism
图 3. 基于激励机制的 DPoS 共识算法流程图

3.2. 节点的状态变更

通过行为的判定评估，对某个节点激励值做出计算得到结果，判定该节点是否值得被信任，激励值

越高越值得被信任，反正将不被信任，本文将其信任状态分为三种：

Good：节点的激励值 $\mathrm{In}\subset(b,1]$；

Normal：节点的激励值 $\mathrm{In}\subset[a,b)$；

Bad：节点的激励值 $\mathrm{In}\subset[0,a)$。

其中，$a\subset[0,0.5)$；$b\subset[0.5,1)$。节点的状态关系如图 4 所示。

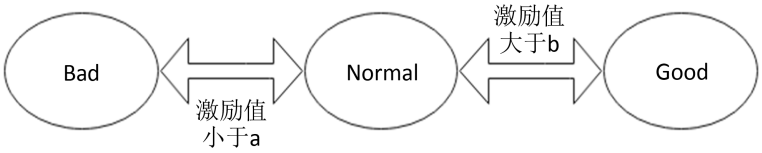

Figure 4. Node state diagram
图 4. 节点状态关系图

当节点第一次加入时，将他的初始状态设定为 Normal，将其激励值赋予初始值 0.5；在后续投票或是生成区块时，当节点做出良好行为，其激励值会增加，直到激励值触碰到上限阈值 b，节点状态就会由 Normal 转为 Good，也就是说这一节点更值得信任；如果节点处于惰性或者腐败状态时，激励值也会随之降低，当其降低到 a 以下时，节点状态会变成 Bad，该节点将不被信任。

4. 实验与结果分析

本章详细叙述仿真实验的细节及相关结果分析，在一台操作系统为 Windows10；CPU：Intel(R)Core(TM)i5-8250U；内存：16 G；GPU：NVIDIA GeForce GTX 960 的服务器上进行。

4.1. 节点激励值变更

本节首先模拟了三个激励系数不同的节点进行验证。节点 1 (激励系数为 0.8，对应状态为 Good)、节点 2 (激励系数为 0.5，对应状态为 Normal)、节点 3 (激励系数为 0.1，对应状态为 Bad)。下面，先对处于不同状态的节点在多轮次(50、100、150、200、250、300)的投票、共识且其行为全部良好时，激励值的变化情况进行仿真。如图 5 所示。

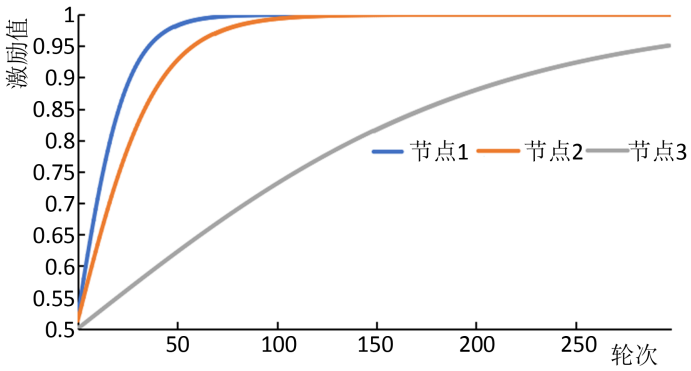

Figure 5. The graph of transformation of excitation values of nodes in good performance
图 5. 节点在表现良好情况下激励值变换曲线图

通过仿真结果可以看出三个节点在表现均为良好的情况下，其激励值都在稳步增加，节点激励值的增长速度会逐渐减慢，同时可以看出，初始激励系数高的节点激励值增长速度最快，但最终都趋近于上限值 1，经过多轮次的行为评估，各个几点的激励值都将维持在相对恒定的水准。

在运行过程中，存在部分节点不参与投票选举，或是在被选举为 bp 时，不生成区块或是生成错误区块，该节点的激励值将会下降。接下将对于上述三个节点在进行多轮次恶意行为时的激励值变化情况进行仿真。如图 6 所示。

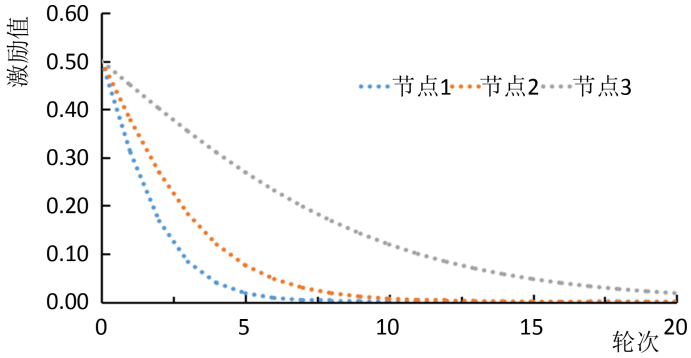

Figure 6. The graph of transformation of excitation values of nodes under abnormal performance
图 6. 节点在表现异常情况下激励值变换曲线图

通过上图可看出，当节点在多轮次的投票、共识过程中存在异常行为时，节点的激励值将会迅速下降，本身激励系数越高的节点其激励值下降速度越快，例如激励系数为 0.8 的节点 1，在被检测到有 7 次异常表现时，其激励值就会降低至 0，将被禁止参与投票以及失去被选为 bp 的资格。

4.2. 恶意节点激励值变更

模拟 500 个代理节点对激励机制 DPoS 共识算法进行验证，该 500 个节点均为初始状态，即 500 个代理节点的初始激励值和为 250。在这 500 个节点中，分别挑选 150、250、350 个节点作为恶性节点，分析其经过 10 轮共识过程后恶性节点激励值的变换情况。

从图 7 中可看出，在所有节点均为初始状态下，恶性节点的数量越多，在激励机制 DPoS 共识算法下，其激励值下降速度越快。且恶性节点的激励值最终都将趋于 0。从图 8 中可以看出，当 500 节点中含有 150 恶性节点时，所有节点的激励值在多轮次的共识后，其激励值缓慢增长，但是，当恶性节点的数目达到 350 个时，所有节点的激励值和将逐渐下降，且恶意节点越多，激励值下降速度越快。这也意味着改算法可容纳少数恶性节点，但是当恶性节点的数目超多一定限度，其激励值下降速度将增快，激励值降为 0 时将被禁止参与投票以及失去被选为代理节点的资格，从而增加恶性节点生成区块的成本。

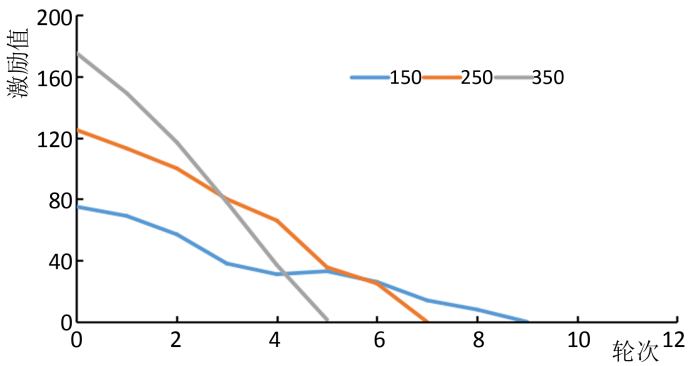

Figure 7. The graph of transformation of excitation values of different numbers of malignant nodes
图 7. 不同数目的恶性节点激励值变换曲线图

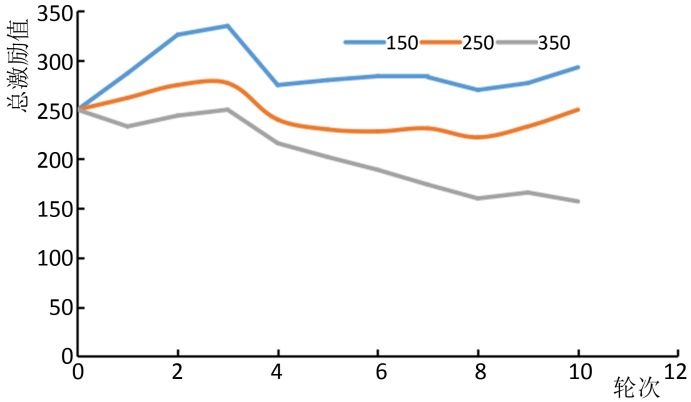

Figure 8. The graph of transformation of excitation values of malignant nodes to the total nodes
图 8. 恶性节点对总体节点激励值变化曲线图

4.3. 吞吐量测试

对激励机制 DPoS 共识算法吞吐量(TPS)做出测试。分别与传统的 PoW、PoS、DPoS 共识算法做出比较。

$$\mathrm{TPS}=\frac{\mathrm{Transactions}}{\Delta t} \tag{6}$$

其中，Transactions 表示的是确认交易的数量， Δt 为单位周期。

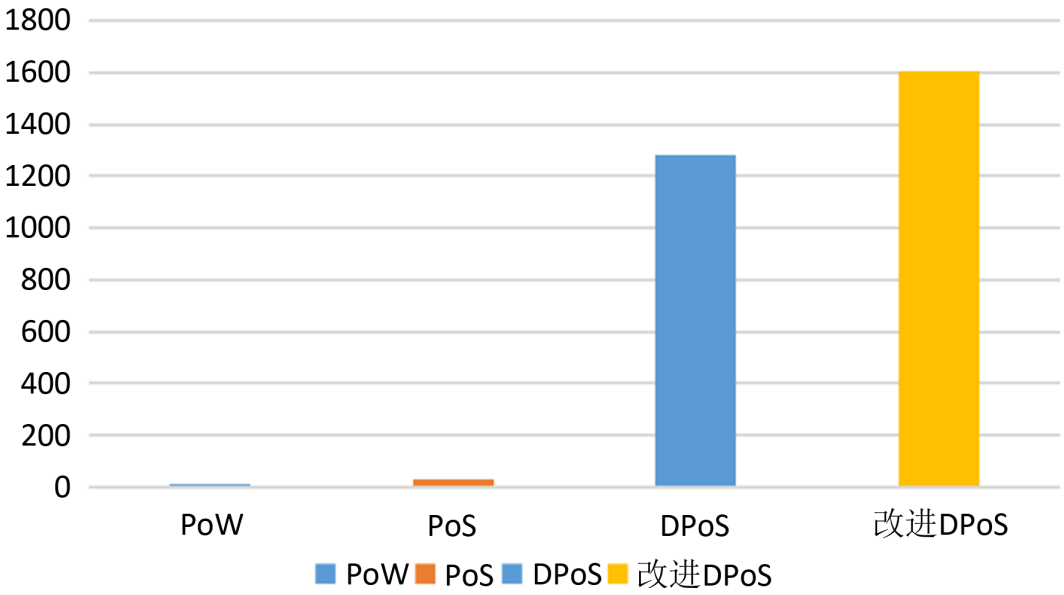

Figure 9. Comparison of throughput data of different consensus algorithms
图 9. 不同共识算法吞吐量数据比较

从图 9 中可得知，在相同周期内，DPoS 以及激励机制的 DPoS 吞吐量远高于 PoW、PoS 共识算法，其原因是 DPoS 共识在生成区块之前，就会投票选举出多个可信任的代理节点，并由这些代理节点轮流生成区块交由全体节点验证，因而其单位周期内确认较交易的数量要远高于 PoW 及 PoS 共识算法。激励机制下的 DPoS 与 DPoS 相比，由于引入激励激励，被选举出的可信任代理节点生成确认交易的区块数量

较高，即表现为共识效率较高、对交易的处理能力良好。

5. 总结

本章对 DPoS 共识算法进行了详细说明，对其投票选举阶段、共识阶段存在的问题进行了分析。针对 DPoS 共识算法存在惰性节点、腐败节点的现象进行改进，提出了激励机制的 DPoS 共识算法，并介绍了该算法的原理和流程；最后，通过实验仿真分析，验证基于激励机制的 DPoS 共识算法提升节点生成区块效率及防止腐败节点的有效性，并且通过将激励机制的 DPoS 共识算法与传统的 PoW、PoS、DPoS 共识算法生成区块效率做比较，验证了该算法的高效性。

参考文献

[1] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. Working Paper. https://www.bitcoinpaper.info/bitcoinpaper-html/

[2] 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.

[3] Wustrow, E. and VanderSloot, B. (2016) DDoSCoin: Cryptocurrency with a Malicious Proof-of-Work. *WOOT*'16: *Proceedings of the* 10*th USENIX Conference on Offensive Technologies*, Austin, TX, August 2016, 168-177.

[4] King, S. and Nadal, S. (2012) PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. Report.

[5] Castro, M. and Liskov, B. (1999) Practical Byzantine Fault Tolerance. *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, New Orleans, February 1999, 1-14.

[6] Saltini, R. (2021) BigFooT: A Robust Optimal-Latency BFT Blockchain Consensus Protocol with Dynamic Validator Membership. *Computer Networks*, **204**, Article ID: 108632. https://doi.org/10.1016/j.comnet.2021.108632

[7] Pan, J., Song, Z. and Hao, W. (2021) Development in Consensus Protocols: From PoW to PoS to DPoS. 2021 2*nd International Conference on Computer Communication and Network Security* (*CCNS*), Xining, 30 July 2021-1 August 2021, 59-64. https://doi.org/10.1109/CCNS53852.2021.00020

[8] Liu, J.L., Zheng, W.L., Lu, D.Y., Wu, J.J. and Zheng, Z.B. (2022) Understanding the Decentralization of DPoS: Perspectives from Data-Driven Analysis on EOSIO. *ArXiv*, 2201.06187v1

[9] Luo, Y., Chen, Y., Chen, Q. and Liang, Q. (2018) A New Election Algorithm for DPos Consensus Mechanism in Blockchain. 2018 7*th International Conference on Digital Home* (*ICDH*), Guilin, 30 November-1 December 2018, 116-120. https://doi.org/10.1109/ICDH.2018.00029

[10] Yang, F., Zhou, W., Wu, Q., *et al*. (2019) Delegated Proof of Stake with Downgrade: A Secure and Effient Blockchain Consensus Algorithm with Downgrade Mechanism. *IEEE Access*, **7**, 118541-118555. https://doi.org/10.1109/ACCESS.2019.2935149

[11] Tan, C. and Xiong, L. (2020) DPoSB: Delegated Proof of Stake with Node's Behavior and Borda Count. 2020 *IEEE* 5*th Infonnation Technology and Mechatronics Engineering Conference* (*ITOEC*), Chongqing, 12-14 June 2020, 1429-1434. https://doi.org/10.1109/ITOEC49072.2020.9141744

[12] Wang, B.C., Li, Z.T. and Li, H.B. (2020) Hybrid Consensus Algorithm Based on Modified Proof-of-Probability and DPoS. *Future Internet*, **12**, Article 122. https://doi.org/10.3390/fi12080122

[13] Luo, Y., Chen, Y., Chen, Q. and Liang, Q. (2018) A New Election Algorithm for DPos Consensus Mechanism in Blockchain. 2018 7*th International Conference on Digital Home* (ICDH), Guilin, 30 November-1 December 2018, 116-120. https://doi.org/10.1109/ICDH.2018.00029