RESEARCH ARTICLE

Network Dispersity-based Consensus Protocol

Yj1190590*†

Abstract. This article describes a blockchain consensus protocol based on network terminals and transmission latency. The protocol provides a stake-voting mechanism that has low electric power cost and avoids the limitations of the Proof of Stake protocol. The stake-voting mechanism helps build a scalable multi-chain structure that may influence the future direction of cryptocurrencies. In addition, competition relative to the number of terminals and the degree of dispersion involves many developers as potential Miners to maintain or expand the network.

KEY WORDS

1. Proof of Network Dispersity(PoND). 2. Vote. 3. Reward distribution. 4. Self-interest.

1. Introduction

The Proof of Work (PoW) protocol has been criticized due to the amount of electrical energy it consumes. However, regardless of this energy issue, the PoW protocol remains an essential and effective method for the blockchain system. With the logic of "able people should get more pay," PoW is the first consensus protocol that can be used to realize a completely decentralized system. All other protocols, such as the Proof of Activity, Proof of Burn, Proof of Storage, and Proof of Elapsed Time protocols, adopt the same logic. The Proof of Stake (PoS) protocol is the most successful because it does not require external resources and consumes low energy by expanding the main logic from "able people should get more pay" to "rich people should get more pay." This restricts mining competition to static inner states, and there is no need for high power consumption. However, PoS has limitations. For example, the PoS protocol is vulnerable to the "nothing at stake" problem, which can cause a double voting problem, and "stake grinding attacks." In addition, the "rich people should get more pay" logic inevitably causes a problem. Whenever Miners spend the same amount of time, richer Miners earn more; thus, they tend to spend more time working. Thus, rich Miners will gradually become increasingly rich, and this process will continue until only the richest users remain in the system. Some PoS-like protocols offer "interests" to all stakeholders to replace the mining process. It appears that such protocols resolve the wealth concentration problem mentioned above; however, those protocols are vulnerable because they lack incentive to maintain the network.

The purpose of this study is to find a low energy consumption proof of ability to replace the PoS protocol. Here, we consider the following. As a greater number of dispersed online terminals work together, the faster they can acquire randomly distributed information in the network due to network latency. We refer to this type of "ability" as "Network Dispersity." Network Dispersity cannot be improved by enhancing the performance of single machines or by using more electric power. The "stake" property plays an important role as a measurement in the protocol due to its unduplicatable feature. Users can freely choose to participate in the maintenance of the network with their abilities or stakes. The power of mining will be balanced by a dynamic adjustment of the reward distribution to maximize fairness and safety.

†Yj1190590 (3171228@qq.com)

Note that all consensus protocols discussed in this paper relate to fully decentralized systems. Protocols, such as PBFT, DPOS, and Ripple are not considered.

2. Scenario and Characters

The entire network can be considered a type of canvassing scenario that involves three types of characters according to a node's functions.

Voter. Each node that broadcasts a transaction could be a Voter. Voters are primarily responsible for responding to "canvass" requests from Workers and publishing transactions along with their votes. A stake held by a Voter is considered "votes" in this scenario, and the number of "votes" determines mining competition. Note that any user can be a Voter.

Miner. Miners have Workers that canvas for "votes" throughout the network, and Miners use these "votes" to compete in block generation. Any user can be a Miner.

Worker. Workers detect nearby Voters and send a "canvass" request as quickly as possible. Workers primarily run on network terminals by being embedded in client apps or web sources.

The network scheme is shown in Figure 1.

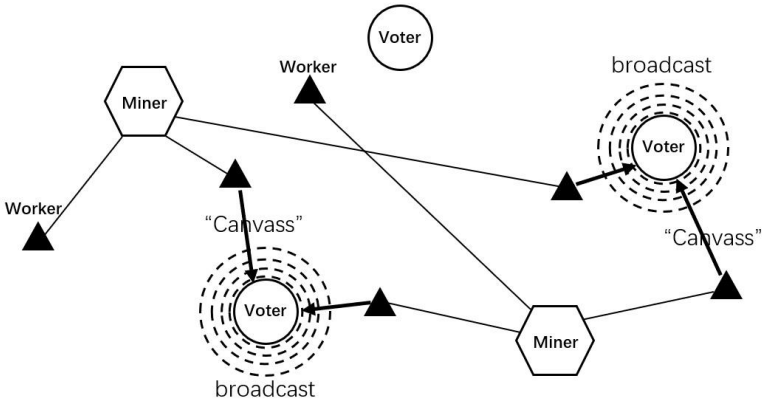

Fig. 1. Network scheme

3. Consensus Process

(1) A Voter broadcasts a signal to preannounce a transaction prior to publishing the transaction. Nearby Workers send "canvass" requests back when they detect this signal.
(2) The Voter packs the main chain's[1] tail-block "b" and the Worker's owner's (i.e., the Miner) account "m" into the transaction structure after receiving the initial request from a Worker and then broadcasts the transaction.
(3) This transaction is validated and packed into a new block by another Miner. Then, the block is published to the network.
(4) When a Miner receives a new block, they begin to validate it. The Miner checks the "b" and "m" fields of each transaction simultaneously and marks transactions with an "x" when the "m" field point to the Miner and with a "y" when the "b" field matches the current chain's tail-block.
(5) Each Voter's stakes are divided equally among all of their transactions in that block.
(6) The stakes of all transactions divided in the previous step are summed and marked with both "x" and "y" block by block until the Miner meets the requirement to generate a block. The result is denoted "X," and the maximum number of accumulated blocks is the voting cycle (*e.g.*, 6000 blocks).[2]

(7) The divided stakes of the transactions marked with "y" in the current block are summed, and the result is denoted "Y".
(8) Miners periodically attempt to meet the target to generate a block using a mathematical operation based on various constants, such as timestamps and private signatures. The operation is expressed as `hashProof()<target*d*X*Y,` where "`d`" is the difficulty adjustment parameter.[3]
(9) The Miner packs all transactions received during the above period into a new block and broadcasts it after meeting the target to generate a block. All referred transactions (coded within 6000 blocks to save space), the profits of all nodes, and the other parameters should also be packed for verification. Note that mining rewards are distributed among the Miner and all participant Voters.[4]

The steps in the consensus process can be summarized as follows. "Every time they publish a transaction, stakeholders vote with their stakes on Miners and on branches. The more stake a Miner or a branch obtains, the higher the chance they win the competition."[5,6]

Figure 2 illustrates mining competition based on network latency.

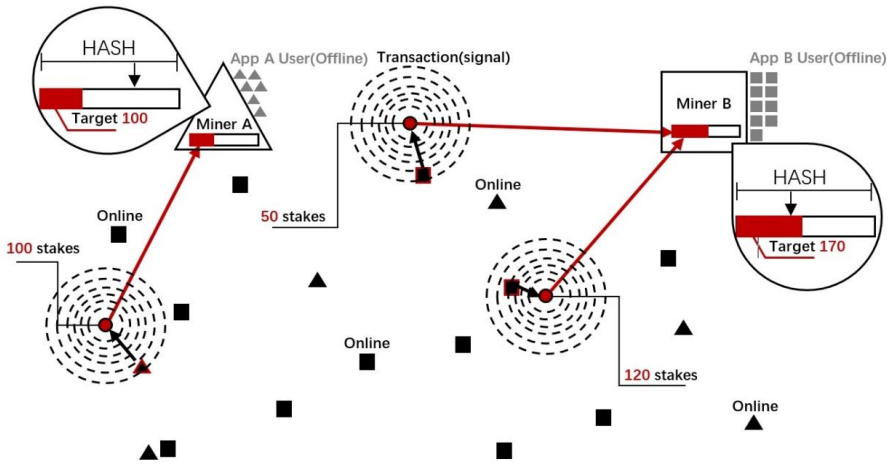

Fig. 2. Mining competition

As shown in Fig. 2, an App with more dispersed online users has a greater likelihood of winning votes (i.e., stakes),[7] which helps Miners win mining competitions later.

Votes are recorded in blocks. Figure 3 and figure 4 show the process of competing for block generation (x-vote) and the main chain (y-vote) respectively.

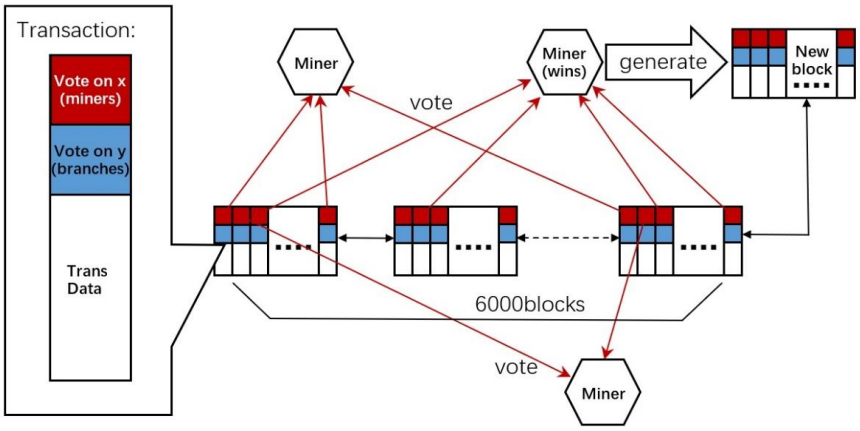

Fig. 3. Process of x-votes taking effect

As shown in Fig. 3, the system counts votes in existing blocks, and the Miner with the maximum number of votes has the greatest chance to win the competition.

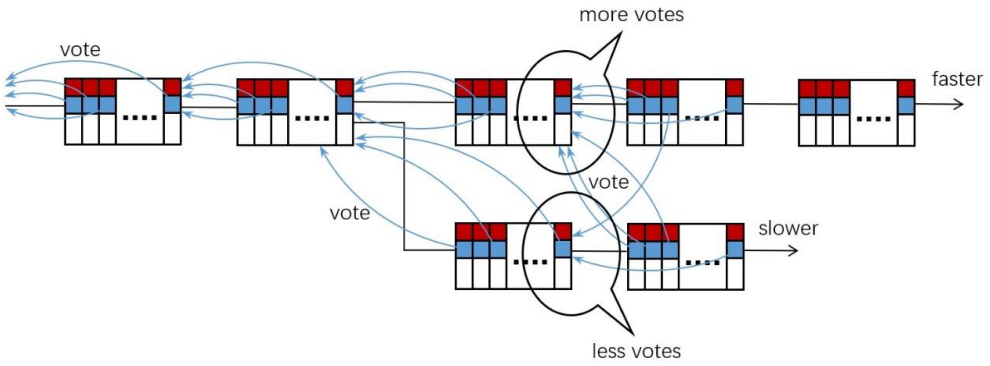

Fig. 4. Process of y-votes taking effect

As shown in the above scheme, when a fork occurs, Voters vote between the branches, and the votes are recorded in the next block. This determines the number of votes (stakes) for both branches in the next block generation (*i.e.*, the block generation difficulty parameter "Y" is determined). Thus, as a single branch receives more votes, the faster the next block can be generated and broadcast, and a branch will receive more votes in the next round. This process increases the speed gap between these two branches and determines the main chain in a short period.

The voting processes for the mainchain and block generation are separated because it could let "stake" decide the main chain individually. Miners only compete for the votes of generating blocks; thus, the mainchain votes have no effect on their incomes. This makes it unnecessary to influence the voting objective. Besides, it is difficult to do that because Voters only need to vote for their desired mainchain according to the blockchain data. Therefore, even if the users are quite centralized, it can also effectively protect the main chain against attacks.

According to the above consensus process, Miners must earn more dispersed Workers to catch up to the randomly distributed signals of the Voters in the network if they want to obtain more advantage in the competition. Thus, competition ability is impossible to simulate on a single computer, and this helps avoid competition by infinitely increasing the performance of mining machines and ensures fairness.

Similar to the PoS protocol, our protocol does not require external resources. The difference is that when votes take effect, they are already sealed in the existing blocks, which resolves the common problems of the PoS protocol, such as the "nothing at stake" and "stake grinding" problems.

Another difference from PoS is that stakeholders can hand over their work to Miners through the voting process. Miners can help complete the competition even though users with low stakes are not so positive to participate. The stakeholders only need to vote once in a voting cycle to ensure their stakes do not miss voting activities, which can essentially avoid the unequal wealth distribution issue.

Meanwhile, the Miner-Workers form can be embedded in App and website development. Hopefully, this will help developers handle the dilemma of only being able to generate income from advertisements. Alternatively, this may contribute to better user experiences with some apps and websites. In addition, a large number of developers could be potential Miners, which would reduce the threshold for starting and improve blockchain sustainability.

4. Compete for Voters

Miners will attempt to win as many Voters as possible to achieve faster block generation. Some Miners may reach agreement with some Voters to mine cooperatively rather than using more Workers as canvassers. In this case, the protocol provides alternatives for Voters relative to Miners in the transaction structure: type *A*: accept vote canvassing from Workers in the broadcast-request form; type *B*: designate one Miner and make him win the voting; type *C*: designate themselves and work on mining individually. Regular Miners will compete with Miners with cooperating Voters and the individual Voters acting as Miners. There is competition relative to the ability to gather users between Miners of types *A* and *B*, and there is competition relative to stakes between type *C* and types *A* and *B*. Essentially, the three types of Miners compete using the stakes gathered with three different abilities. Dynamic adjustment mechanisms are introduced through the reward distribution process to balance the mining power of the three different abilities. The risk that attackers will come to control the network by dominating one type of ability will be reduced effectively by this dynamic balance.

4.1 Wallet application

Wallet applications can guide or even control Voters to choose a transaction type and voting targets due to a special user group. However, considering their benefit, wallet applications would attempt to make Voters vote for Miners that belong to their suppliers, which would eliminate the chances for other ordinary Miners to participate in the competition. Therefore, a mechanism to encourage wallet applications to select type *A* is required to provide a fair competition environment. In this case, the "wallet account" field is added to type *A* transactions and some of the profits are distributed to the suppliers of wallet applications; however, types *B* and *C* do not have this kind of reward. Any behavior that influences the fairness of the competition in type *A* should be considered malicious because wallet applications have legitimate income. There is extra benefit if the wallet suppliers profit from the system, and this encourages developers to make better wallet applications, or, more importantly, it provides incentive to build sidechain projects that may help build an extendable open system with multi-chains.

4.2 PoS variant

We can also derive a variant for this protocol when there only type *C* mining is present. Here, each Miner mines with his own stake, and this becomes pure PoS consensus. This variant system can also ensure fairness without introducing the common problems of the traditional PoS protocol, with the exception of the wealth distribution issue.

5. Reward distribution

Users may engage different selections of mining types, and this will affect the network structure if the distribution strategy of mining rewards is different. The distribution strategy is only for the profits from type A mining because type *B* profits are distributed by Miners and there is no distribution requirement for type *C* mining. Consider the following statements.

(1) Miners should achieve rewards according to a fixed proportion of the total amount to avoid Miners dividing themselves to obtain more benefit.

(2) The weight of the stake while distributing influences Voter choice, and absolute fair distribution may not be sufficient to attract more ordinary Voters if we follow the stake proportion exactly. However, we would lose too many high-stake Voters if the stake weight is too low.

(3) It is necessary to implement a transaction fee as a reference to avoid Voters dividing their stakes to obtain more rewards after reducing the stake weight, and this can also provide Voters with more strategies.

Therefore, the best solution for the distribution plan of type *A* mining is to be affected by both the stake and transaction fee parameters, *e.g.*, the Miner shares 20% of the total rewards, and the rest is divided into two parts, i.e., 1/3 of which is distributed according to the proportion of the transaction fee, and the other 2/3 are distributed according to the proportion of the stake. Here, 25% of the rewards from Voters (*i.e.*, 20% of the total amount) is distributed to the wallet account.

However, the distribution plan of type *B* mining is determined by the Miner according to the agreement between the Miner and cooperating Voters. The plan is relatively freer; however, there are also some restrictions, i.e., B-type Miners' rewards must be restricted under the wallet income out of type *A* mining to ensure the benefit of the wallet applications of type *A*, which is always greater than that of type *B*, which is less than 20% in this case.

The reward proportion of type *A* Miners should be adjusted dynamically according to the sum of the stakes of each type of transaction to balance mining power, i.e., the proportion should be reduced if the sum of stakes of type *A* is too high to reduce the number of type A Miners; otherwise, the proportion should be increased to attract more type *A* Miners.

The default transaction fee of different voting plans could be adjusted dynamically according to the average number of Miners of type *A* or *B*. If there are more Miners, the transaction fee can be reduced to attract more Voters to match the number of Miners. Actually, even if there is no such adjustment, the economic principle would help people create such a balance; however, this would occur at a somewhat slower rate.

6. Frauds and attacks

(1) Filtered transaction. Miners only pack transactions that are beneficial.

Miners may want to gain more advantage by selecting transactions because the transactions included in each block could influence the competition environment.

First, transactions in each block only take up a small percentage of the total amount; thus, there will be little influence on statistical results if some changes are made in a single block. To better address this kind of problem, we must count the sum of the stakes of all Voters in the given transaction, which will affect the next block generation interval. As the stake increases, the calculation period will be reduced, *e.g.*,

if we make the calculation period 0.9-1.1 s, this would directly affect the generation speed of the next block. In this case, it would be better to pack as many transactions as possible, which could disincentive Miner fraud. This parameter should be adjusted per the average value every once in a while.

(2) It is also a filtered transaction; however, the purpose is to influence branch growth speed.

Transactions included in each block also determine the speed of the next block generation in the same branch by influencing parameter "Y," and attackers can reduce the transactions deliberately in a certain branch to affect the determination of the mainchain.

Solution. In step 4 of the consensus process, when checking transaction field "b," other than marking transactions when they match the tail of the current chain as "y," we must also mark the transaction that points to the current chain's countdown second, third (quantity adjustable) blocks as "y1." Note that marks "y" and "y1" are counted when calculating the value of "Y." In this case, this count will compensate deliberate missing transactions if the latter Miners are honest, even though the attacker reduces the speed of a certain block generation. In addition, all "b" fields of missing transactions will point to the countdown second block and backward.

(3) 51% attack.

The system will be vulnerable to this attack if anyone controls more than 50% of the stakes in the network, which is the same as the PoS protocol. However, the PoS system cannot maintain a high participation rate because users must run full nodes and keep them online to join the competition. Therefore, a lower online stake proportion reduces the level of security. In the PoND system, stakeholders can join network maintenance with only a single vote during a voting cycle. With a lower participation requirement, we can maintain a higher online proportion of the stake, which improves the system's security.

(4) Simulate Workers. Creating a large number of Worker nodes by simulation and adding those virtual nodes to the P2P network will increase the success probability of canvassing.

To deal with this situation, we can control the process of creating P2P links, *e.g.*, each node only needs to build connections with a certain number of nodes with the fastest response speeds.

7. Conclusion

Compared to the PoW and PoS protocols, our model has the following benefits:

(1) No hashpower competition and no high-energy-consumption;
(2) No "nothing at stake" and "stake grinding" attacks;
(3) Provides sufficient incentive to maintain the network without the wealth concentration problem;
(4) Provides incentive to develop extended projects, which ensures the sustainability and extendibility of the system;
(5) The new mining competition method helps change App or website development environments and improve their user experiences.

Conflict of Interest

Patent NO. : CN2018102289423.

Notes

[1] The main chain is selected as the “heaviest” branch according to the GHOST protocol.

[2] The “x” mark means the vote of generating blocks; however, the “y” mark must also be checked. By doing so, nobody will obtain any reward if they select an incorrect branch, which motivates users to be more careful relative to branch selection.

[3] If there are any blocks from the competitive branches received during the mining process, they should be parallel processed. Miners should not stop working on the competitive branches if the weight of the main chain is less than the competitive chain’s weight plus eight in order to not weaken the main chain. In addition, it actually follows their own benefit (possibility to become the main chain).

[4] In terms of the extra storage space for validation parameters and reward distribution, only an addition 4 bytes in the ID and 4 bytes in the profit of each transaction would be required at maximum, which is entirely acceptable. The additional block validation work would proceed through the last 6000 blocks, and this will not cause a bottleneck with a proper design.

[5] It is necessary to count the block interval between the last transaction and the current block in each account in a unit of certain granularity, e.g., 10 blocks, as the adjustment coefficient of the stake to control voting frequency. From zero, the coefficient increases proportionally every unit time, and only after a voting cycle, such as 6000 blocks (approximately 100 hours), can the coefficient be restored to the maximum value. In addition, the same adjustment coefficient will be added to each UTXO, and the transaction frequency can adjust the number of stakes with the same approach and parameters as the former.

[6] We could add transactions with pure voting, and users should be able to decide whether they want to vote with the current transaction to improve efficiency.

[7] Theoretically, the probability of wining is proportional to the number of online terminals.

References

[1] Yj1190590 (/yj1190590). “PoND(Proof of Network Dispersity) BlockChain Project.” Github (accessed 29 April 2018) https://github.com/yj1190590/PoND/blob/master/README_eng.md