Research on Consensus Mechanism for Anti - mining Concentration

Kailing Sui, Chaozhi Yang, and Zhihuai Li

Information college, Dalian Maritime University,116000 Dalian, China
{suikailing,qhlee}@dlmu.edu.cn

Abstract. Based on the analysis of the existing blockchain consensus mechanism, Proof of Work Based on Adjusted Stake, or POWS, a workload proof mechanism based on equity adjustment is proposed. In the POW consensus mechanism, the concept of coinage is introduced to adjust the mining difficulty of different nodes. The POWS adjusts the mining difficulty through two factors: calculation force and coinage. The POWS is compared with the POW and the POS in two aspectsthe basic performance and the ability to resist the mining pool. The experimental results show that the POWS can meet the performance requirements of normal blockchain system, at the same time it can better diminish the impact of calculation force and coinage on block generate efficiency, narrow the efficiency gap between the mining pool nodes and the non-mineral pool nodes, and reduce the interest of the mining pool to non-mineral pool nodes.

Keywords: blockchain; consensus mechanism; mining pool; POW; POS; POWS

1 Introduction

Blockchain technology is a decentralized recording technology [1], it can also be called a distributed general ledger technology based on P2P network [2]. Blockchain technology is originally applied to decentralized bitcoin electronic cash transaction system [3], whose main features are decentralization and detrustment. The most harmful and significant technical defect of bitcoin is that the consensus mechanism itself can easily cause the man-made centralization of mining pools [4]. That has violated the original intention of blockchain technology, becoming the main problem of the development of blockchain technology.

One of the core technologies of blockchain technology is consensus mechanism technology [5]. The consensus mechanism solves the problem of credible communication in peer-to-peer networks, named the Byzantine failures [6]. There are two main types of consensus mechanism in the employment of public chain, one is the POW consensus mechanism [7], and the other is the POS consensus mechanism [8]. The POW consensus mechanism will artificially generate the mining pool with the concentration of calculation force, while the POS consensus mechanism will produce the pool with the concentration of coinage. Therefore, to

improve the consensus mechanism is the primary method of solving the problem of concentration of mining pools.

Based on the analysis of the existing consensus mechanism, this paper proposes a hybrid consensus mechanism of POW+POS called Proof of Work Based on Adjusted Stake, or POWS. The POWS consensus mechanism is designed to prevent the concentration of the mining pool, increase the operation cost of the mining pool effectively, and reduce the interest drive of the mining pool to the common miners node.

Experiments to compare the basic performance and the ability to resist the mining pool of the POWS consensus mechanism, the POW consensus mechanism and the POS consensus mechanism were conducted in laboratory environment. The experimental results show that the POWS consensus mechanism can meet the performance requirements of normal blockchain system, well reduce the impact of the calculation force or coinage on the block generate efficiency, and weaken the interest drive of mining pool on common nodes.

2 Design of POWS consensus mechanism

The consensus on the whole network is one of the core challenges in distribution systems [9]. With the idea of a hybrid consensus mechanism of POW+POS, this paper introduces the concept of equity (coinage) in the POS consensus mechanism to adjust the mining mode of the POW consensus mechanism, and designs a workload proof mechanism based on equity adjustment called the POWS [10].

2.1 Overall structure and node design of POWS

Overall structure design of the POWS consensus mechanism The POWS consensus mechanism system designed in this paper consists of four parts: application layer, extension layer, network layer and storage layer. The function of the application layer is to provide users with specific block links and to meet the specific needs of users. The most representative applications include wallet client, trading platform, communication software and so on;The function of the extension layer is to introduce the side chain applications such as intelligent contract and lightning network. The function of the storage layer is to store complete blockchain data; And the network layer realizes the consistency of the local blockchain data of all nodes through the consensus mechanism. The consensus mechanism adopted in the network layer is the POWS consensus mechanism.

Synchronization of node communication and block When a connection is established between nodes, the node sending the request first sends its system version information to the corresponding node. The corresponding node will also send its system version information to the newly added node after receiving the information. The tow nodes which have established communication connection will both confirm each others timestamp. If their timestamps are

corresponded, they will send back the confirmation and establish the communication connection successfully, otherwise the communication connection will not be established. When the newly-added node in the system maintains the communication connection with other nodes, the block information can be synchronized.The blockchain system will provide all nodes with the function of searching the mining node in the current P2P network, so as to record the IP address of corresponding node and conduct block information synchronization and mining.In the system, only full nodes can participate in mining and maintaining blockchain system. Light nodes are only using the blockchain system, rather than participating in maintaining the blockchain system.

2.2 POWS decentralized consensus process

The consensus mechanism designed by Dorian S. Nakamotoi is a mechanism which operates spontaneously under decentralized conditions [11]. The characteristic of the mechanisms operating spontaneously is embodied in the accomplishment of asynchronous consensus when explicit election has not been done or the consensus cannot be reached, that is to say, each individual node in blockchain system under the rule of established program interacts asynchronous and form consensus spontaneously. The process of the POWS consensus mechanism in this paper is as shown in figure 1.

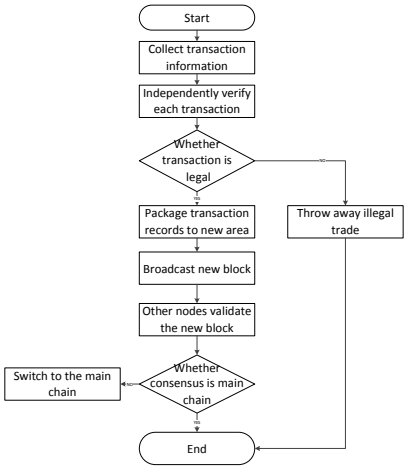

Fig. 1. POWS consensus process

2.3 POWS transaction

Independent verification of POWS transaction Blockchain wallet will construct transaction information through a series of operations including collecting

transaction input UTXO application system, providing the correct UTXO unlock script, and creating UTXO output used by those who output in the transaction to receive information. Then the wallet sends the transaction log to the other nodes in the blockchain application system, allowing the transaction to circulate in the blockchain network and to be added to the miner node's transaction pool.

Each miner node needs to independently verify the transaction after receiving the blockchain transaction record. After receiving the transaction record, the miner node will inspect the transaction information independently according to a certain standard. After successful inspection, the miner node will continue to broadcast the transaction record to the whole network, and add the transactions which have been independently verified to the transaction pool in the order that they are received.

Independent packaging of POWS transactions The miner node saves all transaction records that are verified in the local transaction pool. When the miner node packages the transaction records in the transaction pool to the candidate block, the priority order is decided by the currency coinage of UTXO. The calculation formula of the coinage of a single UTXO is as shown in formula 1.

$$Coinage = Value * InputAge \tag{1}$$

The transaction priority is acquired when the total UTXO coinage divides the total length of the transaction. The formula is as shown in formula 2.

$$\text{Priority} = \sum \text{CoinAge}/\text{TransactionSize} \tag{2}$$

Where TransactionSize represents the total length of the transaction. The unit of UTXO that trades in is cong; the unit of age is the block number; the unit of coinage is the byte; and the unit of transaction record is the byte.

POWS coinbase transaction Miner nodes must create a coinbase transaction to package into the candidate block before packaging the transaction records in the transaction pool into candidate blocks. The POWS designed in this paper improve the function of coinbase transaction, increaseing the function of clearing coinage which is the sum of all UTXO's coinage in the blockchain address of the miner node. The calculation formula of total coinage is as shown in formula 3.

$$\text{SumCoinAge} = \sum_{\text{i}}^{\text{n}} (\text{Value} * \text{InputAge}) \tag{3}$$

The UTXO value of the coinbase transaction output is the sum of the UTXO values entered, the total transaction costs of all other transactions in the block, and the sum of three awards of the block miners entered, The temporary bonus of the POWS is 1. The coinbase transaction of POWS has three roles: the total coinage using to participate in mining is cleared; Transaction fees in the block are paid to miner nodes; The reward for generating the block is paid to the miner node.

The generation and mining algorithm of POWS block The block is mainly divided into the block head and the block body. And the main record of the block body is transaction record. The block head of the miner node needs to package the segmentation field, the length of the block, equities record, transaction counter, transaction log details and so on, generating the candidate block. In order to generate candidate block, the miner nodes need to try to calculate different random number Nonce to find the appropriate random number Nonce, makeing the calculated block hash values conform to the rules, which means that the hash value of the block is less than the target difficulty. The POWS consensus mechanism generates blocks for hash calculation to find the specific process of the conditional block hash value as shown in algorithm 1.

Proof of Work Based on Adjusted Stake (POWS)

```
max_nonce = 2 ^ 32
//The upper limit of the random number is about 4 billion.
def proof_of_work_based_on_adjusted_stake (header,SumCoinAge):
        target=coefficient*2^(8*(exponent-3))*(SumCoinAge)^(1/2)
        //POWS consensus mechanism difficulty value calculation formula
        for nonce in xrange(max_nonce):
            hash_result=hashlib.sha256(str(header)+
            str(nonce)).hexdigest()
             //Calculate the candidate block hash value.
            if long(hash_result,16)<target:
            return(hash_result,nonce)
        return nonce
if __name__=__main__:
    nonce=o
    hash_result=
    start_time=time.time()
    //Verification time stamp
    new_block=test block with transactions+hash_result
    (hash_result,nonce)=proof_of_work_based_on_adjusted
    _stake(new_block,SumCoinAge)
    //Find the random number nonce in the new block.
    end_time=time.time()
     //End time
    Eta=end_time-start_time
     //Calculate the time to create blocks
    if eta>0
        hash_power=float(long(nonce)/eta)
        //Calculate the hash rate.
```

The POWS consensus mechanism introduces the concept of the total coinage and the concept of miners node to adjust the target in the calculation formula. The calculation of target value target is shown in formula 4.

$$\text{Target} = \sqrt{\text{SumCoinAge}} * \text{cofficient} * 2 \wedge (8 * (\text{exponent} - 3)) \tag{4}$$

The parameter SumCoinAge in formula 4 is the sum of all UTXO's coinage in the address of the miner node, which is used to adjust the mining difficulty; Parameter Exponent and parameter Coefficient indicate the difficulty of mining.

3 Experimental result

The experiment is constructed by constructing the P2P network and simulating blockchain network in the laboratory server. The version information of the major softwaresused in the experiment are as follows:Bitcoin Core version is v14.02; PeerCoin version is v0.6.1; Qt Creator version is 3.1.0; The Berkeley DB version is 6.4.9. The data set used in the load test was the transaction data of the bitcoin system. The experiment selected all transaction data of the bitcoin system from the creation block to the 495000 block. And the transaction data is slightly normalized to accommodate the transaction structure of the other two blockchain consensus mechanisms.

3.1 Average block time

The average block time of the three consensus mechanisms is as shown in figure 2. The average length of the POW consensus mechanism is the longest. The average time of the POWS consensus mechanism is in the middle level; The average time of the POS consensus mechanism is the shortest. The average block time of the three blockchain is relatively stable.

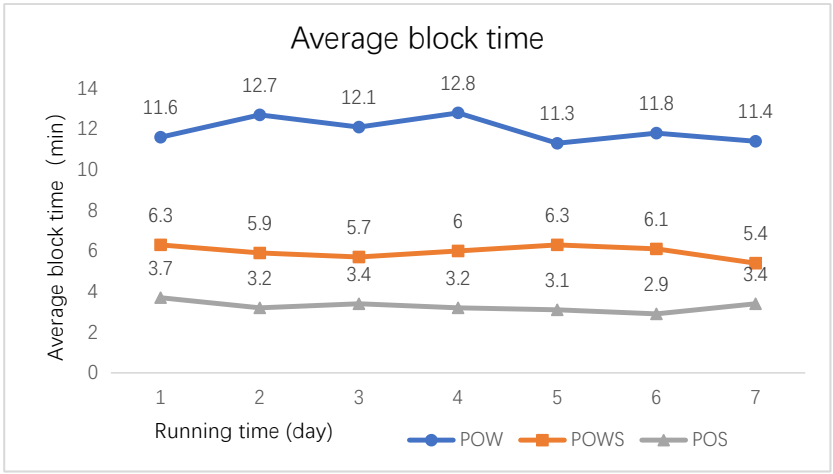

Fig. 2. average time of make block

3.2 Anti-load comparison experiment

As shown in figure 3, under the condition of heavy concurrency, the block size limit of the POW consensus mechanism is 1M, POWS consensus mechanism changes the size limit to 4M, so the POWS consensus mechanism of block has stronger ability to deal with transaction. The transaction handling capacity of the three blockchain consensus mechanisms decreases with the increase of transaction concurrency.

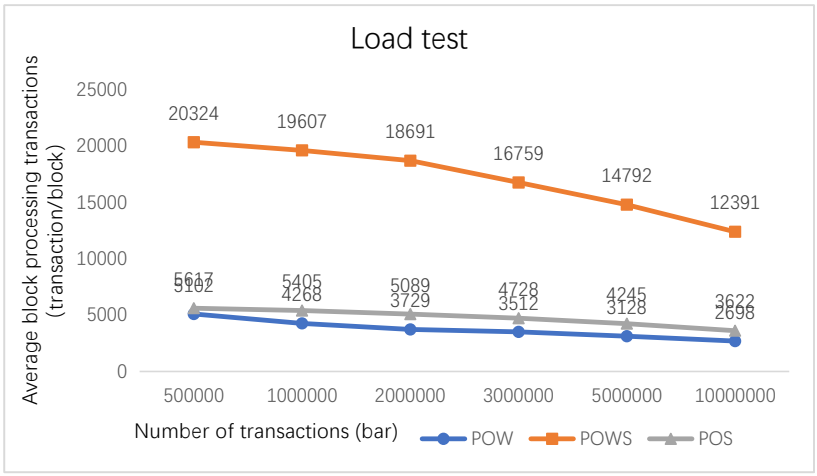

Fig. 3. load experiment

3.3 Comparison experiment of average block efficiency with the change of calculation force

As shown in figure 4, the effect of the proposed POWS consensus mechanism is less than that of the POW consensus mechanism. The reason for this phenomenon is that the POWS consensus mechanism limits more in coinage compared with the POW consensus mechanism.

3.4 Comparison experiment of average block efficiency with the change of coinage

As shown in figure 5, the effect of the proposed POWS consensus mechanism is less than that of the POS consensus mechanism. The reason for this phenomenon is that the POWS consensus mechanism is more powerful in calculation force compared with the POS consensus mechanism.

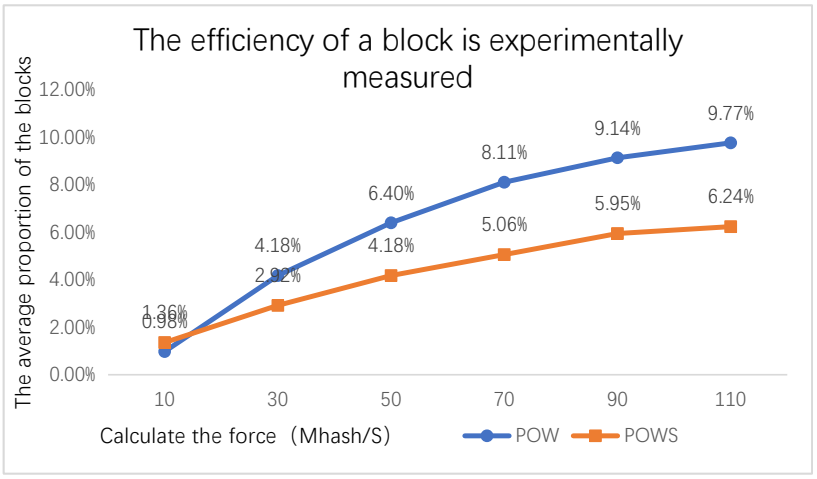

Fig. 4. block efficiency and calculation of power experiment

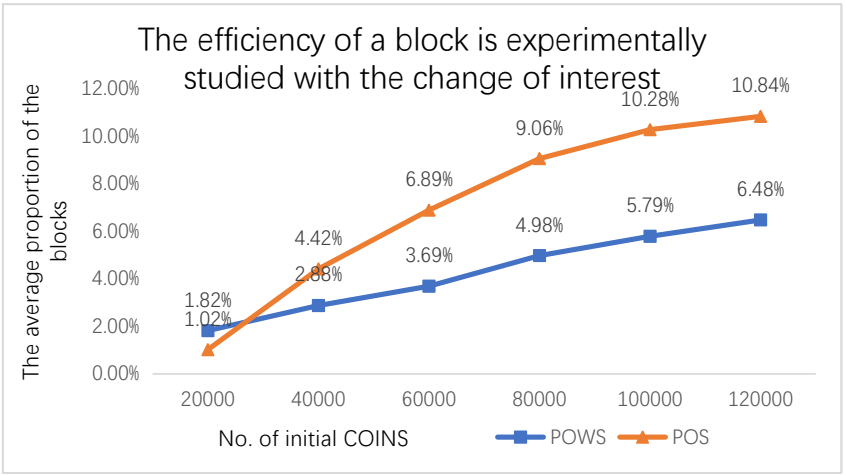

Fig. 5. block efficiency and stake experiment

3.5 The comparison experiment on the profit driving of non - mineral pool nodes

As shown in figure 6, in this paper, in the designed POWS consensus mechanism in this paper, the average efficiency ratio of non-mineral pool nodes and miner nodes is highest. The average efficiency ratio of the non-mineral node and miner node in the POW consensus mechanism and the POS consensus mechanism decreases with the increase of the mining pool calculation force or the coinage.

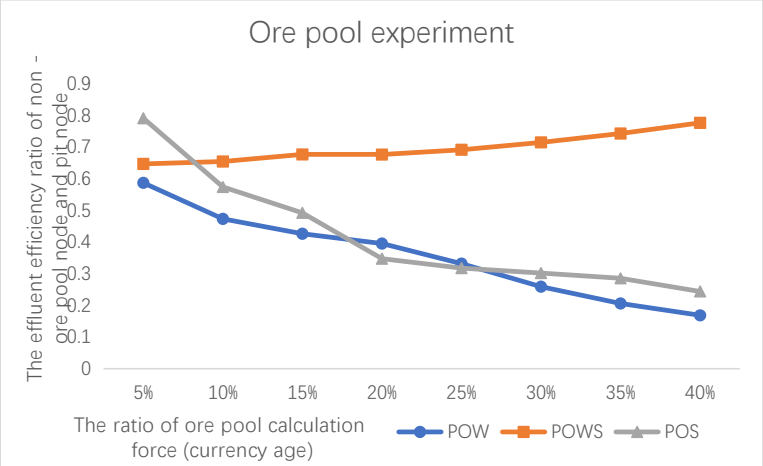

Fig. 6. POWS mining pool experiment

4 Conclusion

Based on the proposed POWS consensus mechanism, this paper carried out an experiment from two aspects: the basic performance and the ability to resist the mining pool, and reached the following conclusions:

(1) Compared with the POW consensus mechanism and the POS consensus mechanism, the POWS consensus mechanism has higher average efficiency ratio of non-mineral pool nodes and mining pool nodes, and the mining pool has less interest drive to the non-mineral pool nodes.

(2) The average block efficiency of the POWS consensus mechanism is slowing down with the growth of the calculation force or the age of the currency.

The above conclusion proves that the POWS consensus mechanism proposed in this paper is reasonable and feasible, and the mechanism can achieve the goal of effective inhibition of the concentration of the mining pool.

5 The References Section

References

1. George Hurlburt.Might the Blockchain Outlive Bitcoin?. 18(2).IT Professional,:12-16(2016)
2. Janusz J. Blockchain technology in the chemical industry: Machine-to-machine electricity market. Applied Energy,195: 234-246(2017)
3. Xu X, Pautasso C, Zhu L, et al. The Blockchain as a Software Connector. Software Architecture. IEEE:182-191(2016)
4. Schrijvers O, Bonneau J, Dan B, et al. Incentive Compatibility of Bitcoin Mining Pool Reward Functions.(2016)
5. Xia Q, Zhang F J, Zuo C. Review for Consensus Mechanism of Cryptocurrency System. Computer Systems Applications(2017)
6. Leslie Lamport, Robert Shostak, and Marshall Pease. The Byzantine Generals Problem. ACM Transactions on Programming Languages and Systems (TOPLAS), 4(3):382C401
7. Aste T. The Fair Cost of Bitcoin Proof of Work. Social Science Electronic Publishing(2016)
8. Spasovski J, Eklund P. Proof of Stake Blockchain: Performance and Scalability for Groupware Communications. The, International Conference on Management of Digital Ecosystems(2017)
9. Kosba A, Miller A. Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. 2016 IEEE SymPOSium on Security and Privacy, San Jose, California, USA(2016)
10. Bitcoin Wiki. Proof of Stake [EB/OL]. `https://en.bitcoin.it/wiki/Proof_of_Stake,2015.`
11. J. G?bel, A.E. Krzesinski, H.P. Keeler, et al. Bitcoin Blockchaindynamics: The selfish-mine strategy in the presence of propagation delay[J]. Performance Evaluation, 104(1): 23-41(2015)