2017 IEEE 19th International Conference on High Performance Computing and Communications; IEEE 15th International Conference on Smart City; IEEE 3rd International Conference on Data Science and Systems

Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain

Kejiao Li*, Hui Li*, Hanxu Hou†, Kedan Li‡ and Yongle Chen*
Shenzhen Key Lab of Information Theory & Future Network Arch
Future Network PKU Lab of National Major Research Infrastructure
PKU Inst. of Big Data Technology
Huawei & PKU Jointly Engineering Lab of Future Network Based on SDN
*Shenzhen Graduate School, Peking University, Shenzhen, 518055, China
†School of Electrical Engineering & Intelligentization, Dongguan University of Technology, China
‡Dept. of Computer Science, School of Engineering, UIUC, USA
Email: likejiao@pku.edu.cn, *:lih64@pkusz.edu.cn, houhanxu@163.com, kedanli2@illinois.edu, chenyongle@pku.edu.cn

***Abstract*—Bitcoin introduces a revolutionary decentralized consensus mechanism. However, Bitcoin-derived consensus mechanisms applied to public blockchain are inadequate for the deployment scenarios of budding consortium blockchain. We propose a new consensus algorithm, Proof of Vote (POV). The consensus is coordinated by the distributed nodes controlled by consortium partners which will come to a decentralized arbitration by voting. The key idea is to establish different security identity for network participants, so that the submission and verification of the blocks are decided by the agencies' voting in the league without the depending on a third-party intermediary or uncontrollable public awareness. Compared with the fully decentralized consensus–Proof of Work (POW), POV has controllable security, convergence reliability, only one block confirmation to achieve the transaction finality, and low-delay transaction verification time.**

***Index Terms*—blockchain; consortium blockchain; consensus; voting mechanism**

I. Introduction

Blockchain, which is originated from Bitcoin [1], is a comprehensive technology of distributed database, data consistency algorithm, cryptography, peer to peer transmission and so on. Bitcoin maintains a distributed account book in a peer to peer network, where the book is in the form of encrypted data block chain, including all verified digital currency transactions throughout the network. Different from the traditional digital currency system, people can trade bitcoin directly in untrusted networks without relying on third-party intermediary. Bitcoins usage of cryptography makes the entire network data transparent and verifiable, preserves the anonymity of the personal information, and resists the double pay attack based on the whole network consensus based on rivalry of computing power. Hence, as the underlying technology of Bitcoin, blockchain has raised a research boom.

Generally, blockchain can be classified into three types, public, private and consortium blockchain [6]. Blockchain technology is incubated in the public blockchain, but in practical applications, the consortium blockchain can provide solutions to many insolvable financial problems, such as compliance with the rules and regulations, the health insurance portability and accountability act (HIPAA), anti-money laundering (AML) and know-your-customer (KYC) laws. As the fact that the major international financial giants have joined the plan of R3 CEV blockchain [8], financial groups are more favor in consortium blockchain.

Public blockchain is generally considered to be "fully decentralization". Its consensus algorithm relies on public awareness and competition of computing power, and cannot be regulated by rules and regulations. However, when applied to the business community, the consensus mechanism for the public blockchain, such as POW, has been limited by two points: (1) its rivalry of computing power leads to a large amount of energy waste and reduces the efficiency of transaction validation; (2) its transaction verification and the generation of blocks relies on the uncontrollable network-wide autonomous verification, which does not meet the commercial social law and is difficult to meet the rules of business society.

Real business society is the compromise result of freedom and intervention. Even in a financial group, the members of the consortium probably prefer to control the transaction validation. However, they refuse that one individual member to have absolute control over the transaction record. The former can be implemented by a voting mechanism, and the latter can be resolved through decentralized blockchain. Therefore, we design POV, a consensus protocol based on voting mechanism and consortium blockchain.

Take bank as an example of a financial system that relatively closed in management, the inter-bank barriers hinder the sharing of information, resources and account mutual authentication. If several banks are formed to be a consortium using blockchain to share a distributed account book, the customer's

978-1-5386-2588-0/17 $31.00 © 2017 IEEE
DOI 10.1109/HPCC-SmartCity-DSS.2017.61

liquidity information can be quickly shared between different banks. However, as the banks of the consortium would demand for verifying transaction information exclusively, this requirement cannot be satisfied by consensus mechanism of the public blockchain due to its "fully decentralization". In a POV-based consortium blockchain system, the submission and verification of the blocks are decided only by the agencies' voting in the league with rules and regulations on one side. On the other side, the system can achieve decentralization in the common decision-making of banks and meet the requirements of compliance with the rules and regulations. In order to refuse the dominant power and establish the internal control mechanism inside the alliance, POV separates voting rights and execution rights, with the aim of maintaining the independence of execution. The execution role of the block production is assigned to a reliable, leaderless professional team through the campaign, so that the consortium does not have to rely on one of the superpower banking institutions as a third-party trust agent. This team will be recruited from the whole network and accept rotation elections.

Current consensus mechanisms designed for blockchains are slow due to significant time and energy consumed for block producing and safety performance. Different compromises of consensus algorithms are provided as a tradeoff to achieve consistency in distributed systems. One way is to scarify computing power such as the Proof of Work (POW), represented by Bitcoin [1], and Ethereum [2]. Another way is to rely on tokens such as Proof of Stake (POS) represented by Peercoin [5] and Delegate Proof of Stake (DPOS) represented by Bitshare [4]. Besides these inevitable discounts, it remains difficult for the existing solutions to speedup transaction confirmation under security requirement because of the possibility of bifurcation. Arthur et al. [3] analysed the security of POW and found that Litecoin and Dogecoin, Bitcoins most prominent forks, reduce the block generation interval from 10 to 2.5 and 1 minute. However, they still require 28 and 47 block confirmations in order to match the security of Bitcoin, resulting in high-latency transaction validation. Nevertheless, the POV proposed in this paper makes clever use of the characteristics of the consortium blockchain. A unique valid block will finally be generated by voting result, resulting in optimized transaction confirmation time and high throughput of system.

Our goal is to design a consensus algorithm with high performance, to be useful in consortium blockchain. The core nodes of the consortium become the center of the entire network for verification and block production. Within the core nodes, the power is decentralized through the voting mechanism. In order to maintain the independence of implementing the block packing task, the task will be finished by the professional team, elected by the consortium members. This separation of execution and voting rights guarantees the fairness within the consortium, which promotes the development and growth of the consortium.

In this paper, we present the complete consensus process of POV. In the POV, member nodes have the right to vote, and the block with high votes is vaild, making the valid block unique. Some special nodes run for the right of producing blocks in order to transact directly without any third-party intermediary in a consortium blockchain network. We analyse the security, transaction finality and possibility of bifurcation. As show in the paper, POV can obtain excellent performance with ultra-low latency in transaction verification.

II. Threat Model

Nodes can be attacked and become adversaries. We assume that some (less than half) of the union members' machine have been attacked. The system can tolerate less than 50% key nodes being attacked. Adversaries may forge transactions or act like a normal one. Networks may be partitioned. However, the adversary cannot crack and forged the signatures.

The nodes in the alliance use high performance and reliable machines and operating systems, so that the alliance nodes are less likely to be attacked than ordinary nodes. Network Time Protocol (NTP) server is used to synchronize the time of pivotal nodes. When a key node is restarted, it will first adjust its time to synchronize with the NTP server, then participate in consensus process.

III. Proof of Vote

Suppose that several companies have been formed to be a coalition committee to share business data conveniently, and each commissioner on behalf of a company. Blockchain is used to record specific business transactions and operations. However, none of the companies is willing to give out the right of producing blocks to others. As a result, they decide to hire a butler team from the whole world and election is held regularly for butlers. The team is responsible for producing blocks and each block will be submitted to each company for verification and voting, making the power decentralized within the coalition committee. To ensure safety, efficiency and reliability of the team work, these companies have decided that: (a) butlers will be paid high salaries according to the workload; (b) the one who applies to join the butler team must be recommended by the members of the alliance and submit a deposit; (c) the work of a butler will be supervised and graded by the members of the alliance, so that only the most honest will survive.

Therefore, we propose a consensus mechanism, POV, used exclusively for consortium blockchain. The blockchain system are maintained by alliances, consist of enterprises and organizations in different regions of the world. Applications

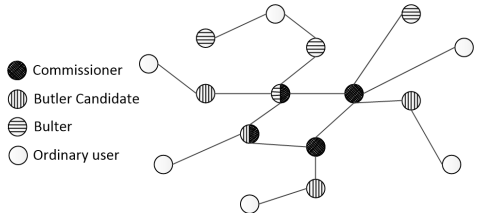


Fig. 1. Four roles in network model.

developed on this consortium chain can serve the terminal users of the global network.

A. Network Model

We establish different security identities for network participants. There are four following roles in POV consensus process: commissioner, butler, butler candidate and ordinary user. As shown in Fig. 1.

Commissioner: Several enterprises or institutions from different regions of the world that are formed to be a league committee, maintain a consortium blockchain together. The commissioner is one of the members of the league committee. In the league committee, a new commissioner must be accepted by the alliance law (beyond the scope of this article) and represented by a machine working in the consortium blockchain network. Commissioners have the right to recommend, vote and evaluate the butlers. They also have the obligation to verify and forward blocks and transactions. Each commissioner has the same rights and obligations and is equal in status. A block generated in blockchain network will be sent to all commissioners for verification. When a block has received at least 51% of the votes, the block will be marked as valid and be added to the blockchain. The result of the voting can represent the will of all the commissioners.

Butler: Butler specializes in producing blocks. The number of butler nodes is limited. The design of the identity of butler means the separation of voting right and executive right. Commissioners are in charge of voting and butlers are responsible for producing blocks. Butlers are like the miners in the Bitcoin, but they have no need to waste computing power in order to snatch the right of producing block, and they will randomly be appointed to produce a block. A butler will gather transaction information from network and pack them into a block, and sign the block. Becoming a butler takes two steps:

- Becoming a butler candidate.
- Win an election for butler.

The Commissioners vote for butler candidates to elect butlers. The butlers take turns to generate blocks in a random order during a tenure cycle and accept re-election after the expiration of their term of office. A node can be a commissioner and a butler at the same time.

Butler candidate: As the number of butlers is limited, a butler must be elected from butler candidates, and candidates will be voted by all commissioners. If they lose in the election, they can stay online, and wait for the next election. There are three steps to apply for butler candidate:

- Register a user account in the consortium blockchain-based system and submit an application for butler candidate.
- Submit a recommendation letter signed (by secret key encryption) by at least one commissioner. The recommendation letter is similar with the invitation code, generated by the commissioner via calling a function using asymmetric encryption. Private key is used to encrypt recommended letter content so that the recommendation letter cannot be forged.
- Submit deposit to become a butler candidate.

Commissioners can retain dual roles as commissioner and butler candidate so that they can recommend themselves to become butler candidates.

Ordinary user: All of the four roles use cryptography to authenticate their identities. They need to sign the messages they send, and their actions can be verified. Ordinary users can join or exit the network anytime without being authorized and their behavior can be arbitrary. Without the permission to participate in the process of block generation, they can only take part in the process of block distribution and message forwarding. They can see the whole consensus process, while using the service of the system.

The conversion of each role is shown in Fig. 2.

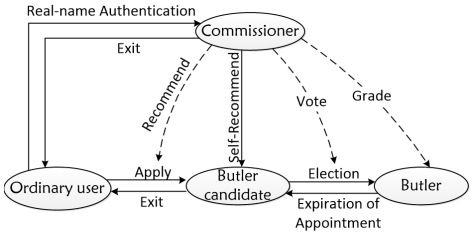


Fig. 2. Relationship conversion between four roles.

B. Consensus process

Our algorithm assumes that the number of commissioners is N_c, the number of butlers is N_b, the number of butler candidates is N_{bc}, and the number of ordinary users is N_o. Since a node can have dual identities, the total number of all roles is N_{all}, and satisfies $N_{all} \leq N_c + N_b + N_{bc}$, where N_b is quantify. In each tenure cycle, we assign a number to each butler, starting at 0, and the last number is $N_b - 1$. We set the period of butler's tenure to T_w, and, in each term, there are $B_w + 1$ blocks generated. The last block is a special block including election results and related records, as well as server information of the new elected butler nodes. Butler is required to generate a block within the allotted time, which is the packing cycle of the block T_b. Fig. 3 shows a consensus model of tenure cycles.

Each time a valid block is generated and signed, we call it a round of consensus. At the end of each round of consensus, the butler call a function to generate a random number R, $0 \leq R < Nb$. If a butler's number is equal to R, this butler is the appointed one to generate the next block. A block must have at least $N_c/2 + 1$ signatures that are sent from different commissioners to become a valid block. If no valid block is generated in the T_b time, the butler whose number is $R+1$ will re-generate the block and let $R = R + 1$. When $R + 1 > N_b$, then R begin to increase from 0. The network can finally reach a consensus, if at least one butler works normally. Because only one block can received at least $N_c/2+1$ signatures in one packing cycle, each valid block has finality, and blockchain will not bifurcate.

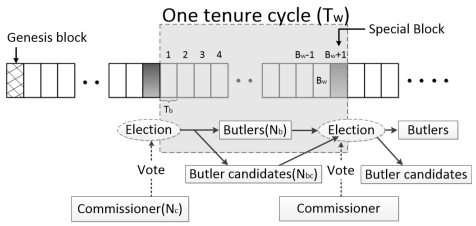


Fig. 3. Consensus model of one tenure cycle.

The last round of consensus in a tenure cycle will produce block $B_w + 1$, which is the special block. The incumbent butlers and butler candidates run for new butlers of the next round of tenure in this consensus. Each commissioner will give a vote list, and eventually the top N_b candidates will win the election. Election results and related records will be written into this special block. After this special consensus, the current butlers officially retired, and the new butlers will start working at the new round of tenure. There are totally $B_w + 1$ rounds of consensus in each round of tenure, with $B_w + 1$ blocks generated.

C. The Generation of an Ordinary Valid Block

The generation of a valid block is called a round of consensus. A round of consensus may take M packing cycles (T_b), and if the butler i fails to generate a valid block within T_b time, the permissions of this block production will be handed over to the butler $i+1$. The total time for a round of consensus is $T_c = M * T_b$ ($1 \leq M \leq N_b$). The number M means that there are $M - 1$ invalid blocks have been abandoned in this consensus. When $M \leq N_b$, generating a valid block contains the following steps:

- S1 All nodes can generate transaction data with their signature attached. At the same time, they receive transaction data, verify whether the received transaction data is valid, they forwards the transaction data to commissioners and butlers if it is valid;
- S2 All Butlers monitor transaction data and store legal transaction data into the transaction pool respectively;
- S3 $M = 1$, $R = GetPreviousBlockRandomNum()$. If this is the first block of this tenure, then the previous block is the last valid special block of the pre round of tenure. If this consensus is to produce the genesis block (the first block of the blockchain), then R defaults to zero;
- S4 Butler i ($i = R$) takes out some transactions from the transaction pool, packs them into a block, and sends the block to all the commissioners. The cutoff time of this block is $T_{cut} = GetPreviousBlockComfirmTime()+ m * T_b$;
- S5 After receiving a block, the commissioners verify the data in the block, and if they agree on this production, sign the block header and send signature back to the butler;
- S6 After receiving at least $N_c/2+1$ signatures, the butler obtains timestamp information signed by the NTP server. If the time is before T_{cut}, the butler can calculate the R value, write it to the block and sign the block to prove that the producer is the bulter itself. Then the bulter publish the complete valid block to the whole network. Jump to step 8;
- S7 If the time has exceeded T_{cut}, then this block will become an invalid block. Let $R = R+1$, M increments, jump to step 4;
- S8 After receiving the valid block, all the butlers will delete illegal transactions from the transaction pool, obtain the random number R of the valid block and begin the next round of consensus.

Specially, If $M > N_b$, let $M = 1$ again, this means none of butlers can generate a valid block. This may happen in situations of network partitions, discussed in Section 4. Under this circumstances, the generation of the block will fall into a dead circle until network is restored.

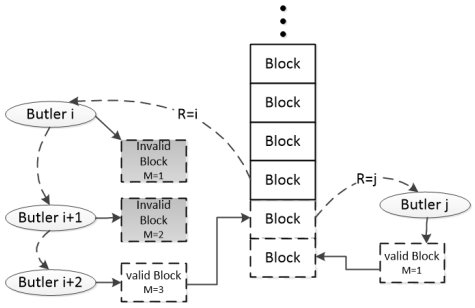


Fig. 4. The generation of valid blocks.

D. The Generation of an Special Valid Block

A special block is the last block in a tenure cycle, with the aim of completing an election for new butlers. The generation of a special block is similar with that of an ordinary block:

- S1 Prior to the emergence of the special block, all commissioners will generate a sequence from the list of the current butler and butler candidates to form a voting list;
- S2 All commissioners and the current butlers will receive voting information from all commissioners and put it into their memory pool (transaction pool).
- S3-S7 Similar with S3-S7 of the generation of an ordinary valid block, special blocks also need to fetch commissioners' signature for authentication and finally reaching a consensus. The difference with ordinary block is that the special block contains voting information, but not transactions. After calculation, the top N_b nodes will win the election and become new butlers of the next tenure.
- S8 After the production of this special block, the butlers of the current tenure will be relieved of their office and delete the relevant voting information in the memory pool.

E. One Tenure Cycle

Normally, the number of butler candidate (N_{bc}) is larger than the number of butlers (N_b). Before the production of

genesis block of the consortium blockchain, butler candidates appear by means of self-recommendation or recommendation. When the condition $N_{bc} \geq N_b$ is satisfied, the first batch of butler will be voted by commissioners, and one of the commissioners will write the initial information into genesis block. Then start a normal tenure cycle. One tenure cycle involves the following steps:

- S1 At the beginning of each round of term, $R = GetPreviousBlockRandomNum()$;
- S2 Complete the B_w round consensus and generate B_w ordinary valid blocks;
- S3 In the $(B_w + 1)^{th}$ consensus, which is the last round of consensus, commissioners update grade of their list of butler candidate, and vote for election. A special block will be generated, containing the voting information.
- S4 This tenure is over. Execute step 1-4 cyclically.

If $N_{bc} < N_b$, commissioners will supplement the number of candidates through self-recommendation in the absence of candidates.

F. Voting Process

There are two main voting procedures. The first is the voting for block production, and the second is the voting for the butler candidate. The commissioners vote by returning their signatures.

Voting for block production. Butler i generates a block and sends it to all commissioners. If a commissioner agrees to produce this block, he will encrypt the block header and returns the signature to butler i. If butler i receives at least $N_c/2 + 1$ signatures within the predefined time, the block is valid. Otherwise, the block is invalid, and will be reproduced by the butler $i + 1$.

Voting for the butler candidate. Butler j sends requests to all commissioners for voting. After collecting and counting the ballot tickets, butler j generates a special block with election results and related records. Then butler j will send this block to all commissioners for validation.

The commissioner's voting information is a combination of two kinds of tickets:

- Score tickets: every commissioner maintains a list to record butler candidates' score, commissioner selects a candidate sequence with a high score.
- Designated tickets: commissioner sets a specific collection of candidates with consideration of human factors, or sets a random candidate collection, which increases the butler's mobility.

G. Time Synchronization Strategy

NTP server is a trusted, entity that provides and signs timestamps for the transactions. Butlers need to fetch time information from the NTP server, and the NTP server will sign the timestamp to ensure that the time information are not falsified. For instance:

- S1 A Butler sends block to all commissioners;
- S2 If a commissioner agrees to this block, sign the block header and return signature;
- S3 When butler receives at least the $N_c/2+1$ signatures, these signatures will be appended after the block header in sequence, and the new block header will be sent to the NTP server;
- S4 After receiving the block header, NTP server provides the current timestamp, encrypts the new block header and timestamp, generates the signature, and returns the timestamp and signature to the butler.
- S5 Butler receives message from NTP server, verifies the message, extracts timestamp information, then gets the timestamp to be the block's confirmed time, attaches signature to the end of the new block header, consummates block with timestamp and butler's own signature, then releases the block.
- S6 Nodes in the network can verify the time information of the block. According to $T_{cut} = GetPreviousBlockComfirmTime() + m * T_b$, if the confirmed time of this block is less than T_{cut}, the block is finally valid.

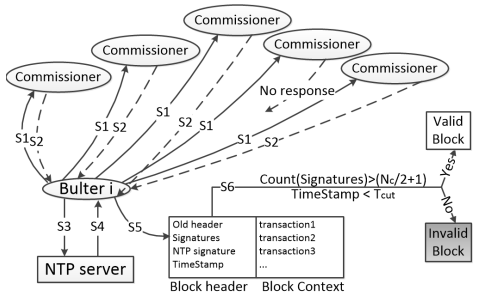


Fig. 5. The process of obtaining a timestamp to generate a block.

H. Generation of Random Number R

Each block generates a random number that determines who will be the next butler, which ensures that butlers generate blocks in a random order. The random number generation algorithm is as follows:

Suppose the butler has received signatures from K commissioners, represented by $Signature[i](0 \leq i \leq K, N_c/2 < K \leq N_c - 1)$. The time it is received from the NTP server is $TimeStramp$. Get R_{source}:

$$R_{source} = (\bigoplus_{i=0}^{K-1} Signature[i]) \oplus TimeStramp \quad (1)$$

Suppose the function of taking the last 32 bits of the string is $SubStringEnd32(string)$, so R is:

$$R = StrToInt(SubStringEnd32(Hash(R_{source})))modN_b \quad (2)$$

Since the value of each block header is unpredictable, we can obtain an unpredictable R_{source} and a random number R, preventing the possibility that butlers may unite to get more income by making R values appear in a certain pattern.

I. Alliance Fund

After the establishment of the alliance, an account will be set up for storing the deposit submitted by the butler candidate and the salary of the butler. Butlers are rewarded for their efficiency, basically the number of successfully validated blocks. Each commissioner has the obligation to supplement the alliance fund regularly.

J. Excitation Mechanism

Butler candidate can give up his identity at any time. When it exits, it retrieves its own deposit if it does not have any bad record. And butler cannot retrieve his deposit if he applies for exit from the network during the tenure, for this is a bad behavior.

Each commissioner will maintain a list of butler candidates and rate their behaviors. The scoring rules include:

- Each time the commissioner passes and signs a block, it will give the butler extra points, otherwise the score will go down.
- When the butler node is offline and have missed the block production, the score will be cleared, which means that when the butler is online, he needs to start scoring again.

A butler may have different score recorded by different commissioners. The score represent the degree of trust from a commissioner, and also becoming one of the grounds for voting.

After a specified period of time, butlers and butler candidates will receive reward from the alliance fund based on the number of valid blocks they have generated so that they can be motivated to take the job, work honestly, and stay online for long periods of time.

IV. Performance Analysis

A complete consensus model is proposed in this paper based on voting mechanism and consortium blockchain. Due to the importance of security and availability, the current consensus mechanism sacrifices performance in order to guarantee security. Our model can ensure the high performance of block chain and low delay of transaction recognition, under the circumstance of safety assurance. In this chapter, we will analyze the reliability of POV, which can be controlled by two parameters, voting mechanism and incentive mechanism. Finally, we compare the performance of POV and existing POW-based block chains, and show that POV can achieve higher performance in terms of low transaction latency.

A. Security

Lemma 4.1: Suppose the number of commissioners is N_c. As long as more than $N_c/2+1$ commissioners are working effectively, blocks are safe and legitimate.

Proof: Assume that illegal blocks can be effectively validated. Because a butler must fetch more than $N_c/2+1$ signatures to produce a valid block, under the circumstances that the number of effectively commissioners is greater than $N_c/2+1$, the effective commissioners will not sign illegal block. So the number of signatures of illegal block is at most $N_c-(N_c/2+1)=N_c/2-1$. Therefore, the assumption is failed and the original proposition is correct.

B. Reliability

In order to be rewarded after winning the election, butlers must maintain the maximum time online, honest work, fulfill the responsibility of producing block within the allotted time.

Lemma 4.2: The butler team is getting more reliable.

Proof: If block production did not consistent with the system rules, the block cannot pass the commissioners' verification, and the butler's scores will go down. As a result, its probability of getting a vote will be lowered in the election. Defeat in the election makes the butler lose opportunity of producing blocks as well as getting profit. It can be proved that it is difficult for the butler who attempts to create illegal blocks to succeed in the election or gain any profit. Reliable butlers are more likely to win in election, and the system will become more reliable.

The reliability of the butler is controllable, and we can adjust the reliability of the butlers' work with two parameters: the number of votes cast K and the butler's income B.

First of all, we analyze the number of votes cast by each commissioner. According to the rules of voting, in each round of elections,N_b butlers will be selected from N_{bc} butler candidates by N_c commissioners, $N_{bc}>N_b$. By establishing a mathematical model, we study the minimum number of votes K that each jury is casting, which is the simplest, time-saving, fair and reasonable voting rule.

Without the consideration of the impact of the scoring mechanism, we assume that the votes are random without any abandonment, and each commissioner cast a K tickets, then the probability of each candidate to get a vote is the same, K/N_{bc}. The voting activity subject to binomial distribution in principle:

The probability that a butler candidate gets X votes is $P(X)$:

$$P(X)=\frac{N_c!}{X!(N_c-X)!}(\frac{K}{N_{bc}})^X(1-\frac{K}{N_{bc}})^{N_c-X} \tag{3}$$

In order to make the results of the voting more impartial, we hope that the number of votes that a butler can receive exceeds $N_c/2$. So we can figure out the probability $P1$ that a candidate's votes can exceed $N_c/2$.

$$P1=\sum_{i=N_c/2}^{N_c}\frac{N_c!}{i!(N_c-i)!}(\frac{K}{N_{bc}})^i(1-\frac{K}{N_{bc}})^{N_c-i} \tag{4}$$

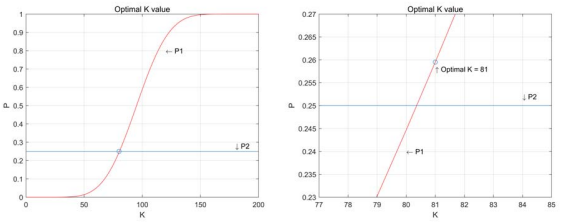
For the purpose to select N_b butlers among N_{bc} candidates, the probability of a candidate's success in the election is $P2$.

$$P2=\frac{N_b}{N_{bc}} \tag{5}$$

According to (4) (5), the minimum K value satisfying (6) is the optimal number of votes.

$$P1 > P2 \tag{6}$$

For example, we set the parameters $N_c = 20$, $N_b = 50$, $N_{bc} = 200$, and draw the image of $P1$ and $P2$, as shown in Fig. 6. The abscissa is K, the ordinate is the probability value. We can get the optimal value K from the curve intersection of $P1$ and $P2$.



(a) original map (b) magnified map

Fig. 6. Distribution map of $P1$ and $P2$. The optimal K value can be obtained at the curve intersection. We can see the detail from the magnified map on the right. When $K \geq 81$, $P1 > P2$, when $K < 81$, $P1 < P2$, so the optimal value of K=81.

As shown in Fig. 6, when K = 81, each commissioner can submit 81 votes to support 81 butler candidates. The number of votes that received by the butler who win the election is probably exceed $N_c/2$ (half the number of commissioners), which means that the elected butlers can get more than half of the commissioners' recognition. In this way, the results of the vote will be more scientific and impartial, so that the results can be recognized by the majority of commissioners. When POV is applied to different systems, K can be figured out by changing the values of N_c, N_b, N_{bc}.

By introducing a scoring mechanism, a butler who has worked reliably will get a higher score. So an honest butler is more likely to receive score tickets during the election, and each commissioner could grade each butler independently (Section 3.F). We can rewrite the formula (4) as:

$$P3 = \sum_{i=N_c/2}^{N_c} \frac{N_c!}{i!(N_c-i)!}(\frac{K}{N_{bc}} + \alpha)^i (1 - \frac{K}{N_{bc}} - \alpha)^{N_c - i} \tag{7}$$

$$-\frac{K}{N_{bc}} < \alpha < 1 - \frac{K}{N_{bc}}$$

If $\alpha > 0$, it means that the candidate has a higher probability to be voted by commissioners on account of a higher score. While $\alpha < 0$ represents the candidate has a lower chance of getting votes than average.

By setting up $\alpha = -0.3, -0.2, -0.1, 0, 0.1, 0.2, 0.3$, we can compare the probability distributions of different situations. The results are shown in Fig. 7.

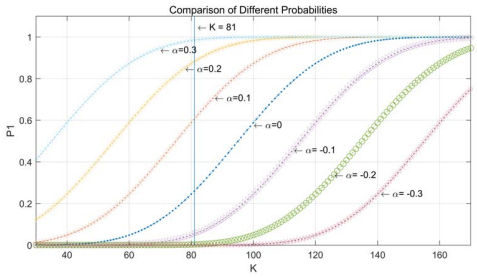


Fig. 7. Comparison of Different Probabilities..

As shown in Fig. 7, when K is a fixed value, the more reliable the butler works, the higher the score the butler can get during the tenure. Therefore, the butler has a higher probability of getting the votes as a candidate, and is more likely it is to win the election.

The second parameter is the butler's benefit. In one tenure cycle, a candidate i has the probability of N_b/N_{bc} being elected to be a butler. After becoming a butler, the butler has the probability of $1/N_b$ to pack a block at each packing cycle. Assuming that a reward for a block is B, we define the average energy cost of a single packing cycle as e_i. After n cycles, the total cost is $e_i * n$. We can define an event as below that the butler candidate i successfully win the election and producing a valid block k($k = 1, 2, \cdots n$). We indicate p_i as the probability of packing a valid block.

$$p_i = \frac{N_b}{N_{bc}} * \frac{1}{N_b}$$

$$E_{ik} = \begin{cases} 1 & p_i \\ 0 & 1 - p_i \end{cases} (k = 1, 2, \cdots n)$$

We take the process E_{ik} as an identical independent distribution (iid). Then the total reward that butler i can receive after n packing cycle is:

$$R_i = \sum_{k=0}^{n} E_{ik} * B - e_i * n$$

Ri follows a binomial distribution with the mean indicated as:

$$\mu(R_i) = n * p_i * B - e_i * n$$

A butler candidate will survive only if $\mu(R_i)$ exceeds 0, i.e.,

$$B > N_{bc} * e_i \tag{8}$$

We can conclude it as follow. Considering the scoring mechanism and voting mechanism, butlers trying to ruin the system will fail to emit blocks and thus receive negative grade. Therefore, the probability that the butler or the candidate can win the election is below the average. If the system has a larger number of candidates than the expected number, unreliable candidates will quit the network because their meager rewards

are unable to compensate for their energy cost. The condition (6) (8) can be a criterion for quality and quantity control of candidates.

C. Transaction Finality

Lemma 4.3: A block can eventually be generated and it is unique.

Proof: According to step 7 of the generation process of an ordinary valid block in Section 3, a butler that fails to generate a valid block within the allotted time will lose the opportunity to generate the block and leave the executive rights to the next node. As long as at least one of the butler nodes is honest, a valid block will finally be generated in a round of consensus. Each valid block is unique by verifying the $TimeStamp$ and T_{cut}.

D. Blockchains do not "Fork"

Lemma 4.4: Blockchains will never bifurcate.

Proof: Considering that network partitions may cause the blockchain to bifurcate, we assume that the network environment is divided into two completely isolated parts, A and B, $A \cap B = \emptyset$. As long as one of the partition commissioners amount $|A| \geq \lfloor N_c/2 \rfloor + 1$. In A region, blocks can still be generated and validated. But in B region, transactions cannot continue to be confirmed, and blocks cannot be validated and generated, for none of the butlers can receive at least $\lfloor N_c/2 \rfloor + 1$ signatures in region B. So POV allows up to two network partitions, and cannot tolerate commissioners to be separated equally in two regions.

E. Low-latency Transaction Validation

The POV consensus mechanism is designed to speed up block producing. It can provide lower latency transaction validation and high throughput (number of transactions per second). Based on an evaluation of information in the Bitcoin network [7], propagation speed of a block in the Bitcoin network is about 6.5s. In the ideal case of POV, the limited time of the block generation is T_b (can be set about 15s), so that the valid block can be propagated to the whole network within 15s.

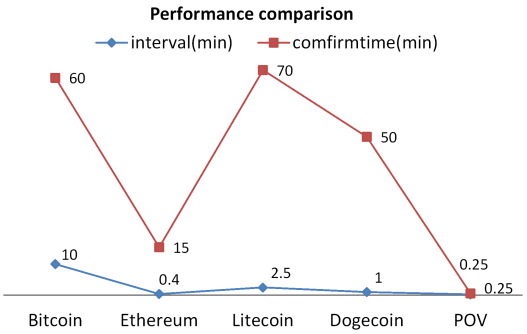


Fig. 8. Performance Comparison of Transaction Validation Time.

As Gervais studied [3], a block is generated within about 10min by POW, and the transaction in an effective block takes about 1 hour (6 blocks generated) to be confirmed [1]. Ethereum requires at least 37 confirmations to match bitcoin' s security with an average 25s block interval, and the transaction verification latency is about 15min. Litecoin (block interval = 2.5 minutes, requires 28 confirmation) and Dogecoin (block interval = 1 minutes, requires 47 confirmation) require 70 min and 47 min transaction delay time [3]. The comparison chart with POV-based blockchain and some POW-based blockchains is shown in Fig. 9. Theoretically, POV shows the optimal performance in comparison with these POW-based blockchains.

In addition, POV shows outstanding performance in terms of low power consumption. On the basis of excellent collaborative mechanisms, POV does not need to waste a large amount of computing power to reach a consensus in consortium blockchain.

V. Conclusion

In this paper, we propose a new consensus mechanism (POV) used exclusively for the consortium blockchain. We design four identities for network participants based on the key idea of voting campaign and voting mechanism. The former guarantees the separation of voting right and executive right, which enhance the independence of bulter's role, so does the internal control system within the consortium. As for the latter, under the circumstance that at least $N_c/2 + 1$ commissioners are working effectively, our analysis shows that POV can guarantee the security, transaction finality, low power consumption and make sure that the blockchain will never bifurcate. We further analyze the reliability of POV through parameter tuning and demonstrate its strong performance in terms of low transaction latency.

Acknowledgment

This work is supported by the National Keystone R&D Program of China (No. 2017YFB0803204, 2016YFB0800101), Natural Science Foundation of China (NSFC) (No. 61671001, No.61521003), GuangDong Key Program (GD2016B030305005), Shenzhen Research Programs (ZDSYS201603311739428, JCYJ20170306092030521, JCYJ20150331100723974).

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[2] Ethereum Foundation. "Ethereum's white paper," https://github.com/ethereum/wiki/wiki/White-Paper, 2014.
[3] A. Gervais, G. O. Karame, K. Wüst, et al. "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, March 2016.
[4] D. Larime, "Delegated Proof-of-Stake (DPOS)," Bitshare whitepaper, 2014.
[5] S. King, S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," self-published paper, August, 2012.
[6] V. Buterin, "On public and private blockchains," Ethereum Blog, 2015.
[7] C. Decker, R. Wattenhofer, "Information propagation in the bitcoin network," in *Peer-to-Peer Computing (P2P), 2013 IEEE International Conference on*. IEEE, 2013, pp. 110.
[8] R3, http://www.r3cev.com/, 2016.
[9] I. Eyal, A. E. Gencer, E. G. Sirer, et al. "Bitcoin-ng: A scalable blockchain protocol," *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*. USENIX Association, March 2016, pp. 45-59.