ISBN 978-981-14-4787-7
Proceedings of 2020 the 10th International Workshop on Computer Science and Engineering (WCSE 2020)
Shanghai, 19-21 June, 2020, pp. 501-505
doi: 10.18178/wcse.2020.06.072

Identity Privacy Protection Mechanism Based on Consortium Blockchain

Zongfang Tu [1], Feng Su [2+] and Hui Li [1]

[1] Peking University Shenzhen Graduate School, Shenzhen 518055, China
[2] Guangdong Communications & Networks Institute, Guangzhou 510670, China

Abstract. Aiming at the problem of identity privacy security in blockchain algorithm, an improved identity privacy enhancement (GSPoV) consensus algorithm is proposed based on the PoV for the consortium blockchain. Firstly, a group signature mechanism is introduced in the consensus process, which can verify the validity of the signature, but can't determine the signer, and the identity of the user is anonymous, thus enhancing the privacy protection of the real identity information. Secondly, the random selection algorithm of butler node in PoV consensus mechanism is improved, which reduces the possibility of mischief of butler node and group administrator, and enhances the security of GSPoV consensus algorithm.

Keywords: blockchain, consortium blockchain, group signature, pivacy protection.

1. Introduction

Blockchain is a new decentralized protocol, which constructs a decentralized distributed system by combining digital encryption, consensus algorithm, distributed storage, time stamp and so on [1]. In recent years, many scholars are carrying on the blockchain consensus algorithm research. However, with the development and wide application of blockchain technology, the problem of privacy leakage becomes more and more serious, which must be paid more attention to. The existing blockchain-based digital currency is not completely anonymous [2], with the increase of the number of user transactions, we can trace the source of funds through the transaction law and clustering analysis technology to obtain the transaction information of account number [3]. Reid[4] analyses the public transaction records to get the transaction network topology and the user topology, and found the relationship between the public key address and the user through the traffic analysis and the time analysis of the direct or indirect transaction between the users, the anonymity of the user is compromised. Dorit [5] downloads the complete history of transactions on the blockchain to the local, and then analyse the transaction records to identify the user's address and identity information and their transaction activities. Therefore, blockchain algorithm has the risk of identity privacy leakage.

At present, blockchain can be divided into public chain, consortium blockchain and private chain. As a compromise between private chain and public chain, consortium blockchain adds identity access mechanism, which improves security and is more suitable for realizing "partially decentralized" alliance ecology among some existing commercial organizations, to make alliances more efficient and fair. In 2017, Kejiao Li proposed a novel consensus algorithm PoV [6] for consortium blockchain. The consensus process of separating voting right and executive right of PoV can realize decentralized management in the consortium blockchain, which depends on the credibility of the alliance commissioners and other nodes. Compared with other consensus algorithms, PoV has stronger fault tolerance and better trading performance. Therefore, this paper will carry out the research on enhancing the security of user identity in the blockchain based on PoV.

[+] Corresponding author.
E-mail address: sufeng@gdcni.cn

At the same time, as a special digital signature mechanism, group signature[7][8] is used in the traditional privacy protection scheme, which not only has the security attribute of the traditional digital signature, but also allows group members to sign on behalf of the whole group anonymously, and the group administrator can track the signer if necessary. Therefore, group signature can achieve anonymity and traceability at the same time, it has a strong research and application value.

In this paper, an improved consensus algorithm model (GSPoV) for consortium blockchain is proposed based on group signature technology to solve the problems of PoV consensus algorithm such as identity privacy leakage, random number algorithm still need to be improved.

2. PoV Algorithm Analysis

PoV is a voting-based consensus mechanism for the consortium blockchain, with good collaboration and participation through the design of specific consensus mechanisms, mainly used in the global regions of enterprises or institutions, such as the formation of the alliance jointly maintained the consortium blockchain system. There are four following roles in PoV consensus process: commissioner, butler, butler candidate and ordinary user. Commissioner has the right to recommend, vote and evaluate the butler, and has the obligation to verify the block, vote and forward the transaction data. Butlers are given a limited number of rights by the consortium blockchain to specialize in producing blocks. The appearance of the butler meant the separation of the right to vote from the right to execute. Candidates for butlers are voted by all commissioners to become butlers. Blocks are created in random order during the term of office and are re-elected at the end of the term.

As can be seen from PoV consensus process, the commissioner nodes sign the transaction data separately and collect it in the transaction pool of all the butler nodes, and the signature of the transaction data in the algorithm is the same as other blockchain algorithms, the protection of true identity privacy is not considered, as stated in the introduction, there is a risk that the true identity information of the node will be revealed.

3. GSPoV Algorithmic Design

Based on the analysis of PoV algorithm, combined with group signature technology and practical application, this paper proposes the following improvement schemes: In order to protect the identity privacy of member nodes, a group signature scheme is introduced to hide the true identity of member nodes. Changes the transaction processing way, adds the transaction node list, the convenient formation group. The random number generation algorithm is modified to enhance the security of Butler node and GM, and reduce the possibility of malfeasance.

3.1. Random Number Generation Algorithm

The generation of each block corresponds to a random number that points to the number of the next butler to be appointed to ensure that the butlers take turns generating blocks in a random order. In the random number generation algorithm of PoV, the problem is that the malicious node can deliberately delay the sending time and fabricate the timestamp, so that the system uses the fabricated C_time and timestamp to calculate the random number source, and controls the generation law of the number of the on-duty butler to complete the evil. We modify the signature and timestamp of C_time as median mid=$\lfloor C\_time_{max}/2 \rfloor$ to get random source R_source.

$$R\_source=C\_time[mid-1] \oplus C\_sign[mid-1] \quad (1)$$

R_source is more random and prevents malicious falsification of data, reducing the likelihood of malfeasance by butlers and GM.

3.2. Consensus Process

GSPoV retains the node identity setting of PoV and adds the group administrator node GM, which is randomly selected from the steward node to reduce the risk of being hijacked. In a tenure cycle T_w, the butler nodes rotate into blocks in a random order and are subject to re-election upon expiration of their tenure. GM does not change during the term of service, and upon expiration of the term of service, reselects from the list

of butlers for the next period. Add transaction node list $U=\{U_1,U_2,...,U_n\}$, which records the node information needed to generate transactions in each tenure period T_w.

- Step1: System initialization

The commissioner node with the lowest public key hash value is selected as the acting butler to complete the election of the steward node and the identity transformation of each node, and the creation block is published. If a creation block exists in the system, initialization is skipped.

- Step2: Create group

The random number generation algorithm is used to select the group manager GM from the butler list. GM groups the nodes in the transaction node list U into a group. Set the security parameter s to generate the public key G_{pk} and the private key G_{msk} of GM. Then the transaction node U_i negotiates the signature private key U_{ski} with the GM. The U_i generates the transaction data m, and uses the private key U_{ski} to generate an anonymous signature σ_m to the transaction m, and forwards the transaction m to the butler after the signature is completed.

- Step3: Transaction processing

All butler nodes listen for transaction data and put valid transaction data into the transaction pool. The on-duty butler takes some transactions from the transaction pool and wraps them in a pre-block, send it to all commissioners. Commissioners vote on pre-block.

- Step4: Effective Block

When the duty butler receives the consent vote from half the commissioners, it serializes the data into a string, appends the Pre-Header, adds the block generation time and the next duty butler number R, generates the Final-Header, and publishes it to the entire network. If the block does not receive more than half of the votes, the block is not valid, set R=R+1, jump to step 3. Fig. 1 shows a consensus model of tenure cycles.

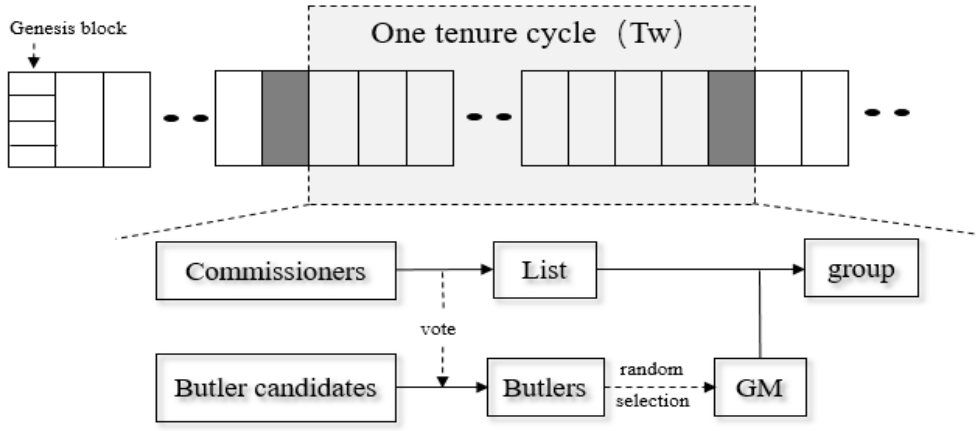

Fig. 1: Consensus model of one tenure cycle.

4. Performance Analysis

4.1. Analysis of Communication Overhead

Let the total number of consensus nodes in the consortium blockchain be N_{all}（N_{all}>3）, the number of commissioner nodes be N_c, the number of butler nodes be N_b.

A. Communication Overhead on PoV

The consensus process can be analysed to calculate the number of times a full set of PoV consensus needs to be communicated. The calculation scope includes four main stages: The initiation of the transaction, the butler's handling of the transaction, the voting of the commissioners, and the generation of the effective block. At the same time, assuming the probability of invalid block is p, the highest total communication times of the four stages are obtained from the analysis of PoV consensus process.

$$W1 = N_c(5 + N_b)(1 + p) + N_{all} \quad (2)$$

B. Communication Overhead on GSPoV

According to the analysis of GSPoV consensus process, the number of network communication is N_c in the stage of transaction node list creation. The number of network communication is 2 N_c+N_{all} in the group establishment stage, and the consumption is the same as PoV in the other stages. Therefore, the number of network traffic of GSPoV can be obtained.

$$W2 = 3N_c + N_c(5 + N_b)(1 + p) + 2N_{all} = 3N_c + N_{all} + W1 \quad (3)$$

Let K be the ratio of the communication overhead of the two algorithms.

$$K = \frac{N_c(5 + N_b)(1 + p) + 2N_{all}}{N(5 + N_b)(1 + P) + 3N_c + 2N_{all}} \quad (4)$$

Because the number of commissioners is close to the total number of nodes in the active consortium blockchain system ($N_c \approx N_c$). Because of the high trustworthiness of the nodes in the consortium blockchain, the probability of invalid blocks is small when the consensus system works stably, let P be minimal.

$$K \approx \frac{6 + N_b}{10 + N_b} \quad (5)$$

It can be seen that K is strongly related to the number of butter nodes N_b. when N_b is larger, the cost of both is closer. In a large group usage scenario that is actually active, as the number of nodes increases, so does the number of butler nodes, the cost of the two algorithms is closer. Therefore, GSPoV algorithm does not significantly increase the communication overhead of the consensus process in the case of large groups.

4.2. Security Analysis

The entry of nodes in the consortium blockchain system has undergone a corresponding authentication mechanism, such as third-party-based identity authentication, pure distributed identity authentication and other combination of cryptography technology, therefore, its use scenario has a high degree of credibility. It has been demonstrated in the literature that PoV can effectively prevent Double Spend Attack, Selfish Mining, and Sybil Attack. After adding group signature mechanism, the GSPoV algorithm in this paper not only retains the security properties of PoV, but also adds the following features:

- Anonymity: The group signature mechanism is added to verify the validity of the signature transaction, but the signer can't be determined. The user's identity information is anonymous.
- Traceability: In the event of a dispute, the GM can "open" the disputed signature, locate the true signer, and track it down.

Due to objective reasons, it is impossible to use the experimental resources in the laboratory of the school in the near stage, build the experimental network to test the throughput and delay of consensus algorithm, and complete the performance comparison between GSPoV and PoV. At present, only the feasibility of GSPoV is verified by simulation. This part of work will be one of the follow-up work of this paper, and will be implemented when conditions permit.

5. Conclusion

In this paper, an improved algorithm model GSPoV based on PoV is proposed, in the usage scenario of "partial decentralization" of the alliance chain, the group signature mechanism is added to verify the validity of the signature transaction, but the signer cannot be determined. The users' identity information is anonymous, which enhances the protection of the real identity privacy in the system. At the same time, the random number generation algorithm of PoV is improved to reduce the possibility of malicious nodes to do evil, further ensure the credibility of butler nodes and ensure the security of the consensus process. Future work will continue to optimize the algorithm details, further reduce network traffic consumption, and build a test platform in the actual network environment to complete the throughput and delay performance verification and further optimization.

6. References

[1] Nakamoto S, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[2] Henry R, Herzberg A, Kate A. Blockchain access privacy: challenges and directions[J].IEEE Security & Privacy, 2018, 16(4): 38-45.

[3] Wang Q, Qin B, Hu J, et al. Preserving transaction privacy in bitcoin[J]. Future Generation Computer Systems, 2017, 29(2):38-47.

[4] Reid F, Harrigan M. An analysis of anonymity in the bitcoin system[M]. Security and privacy in social networks. Springer, 2013: 197-223.

[5] Ron D, Shamir A. Quantitative analysis of the full bitcoin transaction graph[C]. International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2013:6-24.

[6] Kejiao Li, Hui Li, Hanxu Hou, Kedan Li, and Yongle Chen. 2017. Proof of vote: A high-performance consensus proto-col based on vote mechanism & consortium blockchain. In IEEE 19th International Conference on High Performance Computing and Communications (HPCC). 466–473.

[7] CHAUM D, HEYST E V. Group signatures[C]. Theory and Application of Cryptographic Techniques. Brighton:Springer, 1991, 547: 257-265.

[8] BOOTLE J, CERULLI A, CHAIDOS P, et al. Foundations of fully dynamic group signatures[C]. Applied Cryptography and Network Security. Guildford: Springer, 2016: 117-136.