Proceedings of the APAN – Research Workshop 2017
ISBN 978-4-9905448-7-4

A Proof of Stake Sharding Protocol for Scalable Blockchains

Y. Gao and H. Nobuhara

***Abstract*— Cryptocurrencies such as Bitcoin has drawn great attention recently. The public ledger blockchain serves as a secure database for cryptocurrencies. However, only 3 to 7 transactions can be processed per second, which means the blockchain does not scale. To address this problem, we propose a new consensus protocol based on sharding and proof of stake. The scalability of our proposed method is expected to increase linearly with the network size. We discuss proposed method from the scalability evaluation, complexity and security view.**

***Index Terms*—Blockchain protocol, Proof of Stake, Scalability, Sharding.**

I. Introduction

SINCE being introduced in 2008, Bitcoin [1] has become a global decentralized cryptocurrency now and led to more than 700 alternative coins [2]. The total venture capital of Bitcoin reached around 330 million USD at the end of 2016 [3]. Bitcoin has attracted great attention in financial, technology as well as academic. The core technology under Bitcoin is the Nakamoto consensus protocol, which plays a key role in maintaining the transaction history of Bitcoin in a public ledger called the blockchain. The blockchain, serving as a distributed database to record Bitcoin transactions chronologically and securely, is considered as the most significant technology of Bitcoin. With high security, immutability and decentralization, blockchain has also been applied on the protection of public/private/semi-public record tools, physical asset keys and intangible assets [4].

Despite these advantages, a major concern of blockchain is the scalability [5, 6, 7]. The Bitcoin blockchain could only deal with at most 7 tps (transactions per second) [8]. On the contrast, centralized payment systems such as PayPal [9] are able to process around 115 tps and in visa's network [10] the capability could reach to a peak rate of 56,000 tps. The processing speed of blockchain is affected by two factors: block size and block interval. Given Bitcoin's 10 minutes average block interval and the 1MB average size for each block, the throughput is limited to 7 tps. The throughput can be improved simply by increasing block size or reducing block interval. However, increased block size results in slower block broadcasting in Bitcoin network and reduced block leads to centralization [5, 6].

This aim of this paper is to propose a scalable protocol for blockchain with sharding and proof of stake (PoS) algorithm. TABLE I gives a simple comparison between Bitcoin protocol and the proposed protocol. The paper has been organized in the following way. Chapter 2 explains three significant concepts related to this research. Chapter 3 presents the design of the proposed sharding proof of stake protocol that can be a possible solution to blockchain's scalability problem. Chapter 4 discusses the evaluation of scalability, complexity and security of the proposed method. The last chapter summarize the proposed methods.

TABLE I
COMPARISON OF BITCOIN PROTOCOL WITH PROPOSED PROTOCOL

	Bitcoin protocol	Proposed protocol
Consensus algorithm	Proof of Work (PoW)	Proof of Stake (PoS)
Sharding	×	✓
Scalable	×	✓

II. Related concepts

This section introduces three important concepts: Proof of Work (PoW), Proof of Stake (PoS) and sharding. Proof of Work is the consensus algorithm of Bitcoin while Proof of Stake is used to make consensus in the proposed method. Sharding is another significant technique used in this research.

A. *Proof of work [1,11,12,13]*

The proof of work is a consensus mechanism used in cryptocurrencies to maintain the security of the blockchain. In the case of Bitcoin, nodes (also known as "miners") compete to solve a difficult math puzzle to including new blocks in the blockchain so that they could receive bitcoins as a reward. The

Submitted on June 24th, 2017

Y. Gao is with the Department of Intelligent Interaction Technologies, University of Tsukuba, Ibaraki, Japan (e-mail: kou@cmu.iit.tsukuba.ac.jp).

H. Nobuhara, is with the Department of Intelligent Interaction Technologies, University of Tsukuba, Ibaraki, Japan. (e-mail: nobuhara@iit.tsukuba.ac.jp).

CPU Power of a node is proportional to the probability to generate a new block, which means the higher the CPU Power is, the more likely the node would receive a reward for creating blocks. The blocks are connected chronologically by one-way hash algorithms such as SHA-256 to form a blockchain. An attacker is required to perform as much proof of work calculation as the other parts of the Bitcoin network do. The attack would not be successful only if the attacker has controlled more than 51% CPU Power of the entire Bitcoin network.

Despite the security merits, producing a proof of work data is costly. The costs including electricity and hardware are estimated over one million per day [15]. Six hundred trillion SHA256 computations are conducted by Bitcoin network every second, however, these calculations turn out to be useless in practice [14].

B. Proof of stake [12]

The proof of stake is one of the alternative consensus mechanisms of PoW. As shown in TABLE II, the probability of generating a new block is proportional to the stake status rather than the CPU power. In Peercoin, the stake status is known as coin age, which is defined as coin amount times holding period [14]. A user holding large amount of coin for a longer time (i.e. user owns larger coin age) has higher probability to create a new block. Without the need of large quantities of hash calculation, PoS is much more cost effective compared to PoW, Additionally, penalties can be set to make 51% attacks much more expensive in PoS than in PoW [16].

TABLE II
DIFFERENCES BETWEEN POW AND POS CONSENSUS ALGORITHM

	Proof of Work (PoW)	Proof of Stake (PoS)
Based on	CPU power	Coin age
Cost	High	Low
Security concern	Potential 51% attack	Lower probability of 51% attack

C. Sharding [17]

In current blockchains, the nodes are distributed around the world, processing all of the transactions and storing the whole transaction history. This contributes to high security but limits the scalability. In the case of Bitcoin, only 3~7 transactions can be processed per second. Several sharding protocols have been proposed to solve the scalability problem. Luu et al. (2016) proposed ELASTICO for open blockchains. This sharding protocol divides the mining network into small groups where the transactions shards are processed in parallel.

III. PROPOSED METHOD

In this chapter, we introduce our proposed method as a possible solution of the blockchain scalability problem. Assume there are *nc* nodes in the network forming *c* groups, therefore each group contains *n* nodes. Two types of blocks are generated in proposed method. The middle blocks are generated by regular node groups and sent to final validation node group. The final blocks are generated by final validation group and broadcast to the network. In order to distinguish, the middle blocks are represented by lower-case “block” and the final blocks are represented by upper-case “BLOCK”.

A. Overview of the proposed method

The proposed method is mainly based on a sharding protocol and PoS consensus scheme. Assume the initial number of nodes in the network is *cn*. The *cn* nodes form *c* groups, which means each group contains *n* nodes. One of the *c* node groups works as validation node group and the other *c-1* node groups are regular groups. The regular node groups created middle blocks from the transaction shards assigned to them. The middle blocks are then processed in validation node group to produce final blocks which are recorded in the blockchain. To distinguish the two types of blocks created in the processes, the lower case “block” represents the middle block in Step 2 and the upper case “BLOCK” represents the final block in Step 3. Fig. 1. shows the main steps of the proposed method.

Each epoch contains 4 steps:

Step 1: Form node groups. Each node belongs to a group. After a node group is formed, a leader node is chosen randomly and all of the nodes’ identities in this group are sent to it. After the group leader gathering all the nodes information in its group, an identity list is generated and broadcasted to other group leaders. This process reduces the communication complexity between nodes from $O(n^2)$ to $O(cn)$.

Step 2: Run internal group consensus. A transaction shard is assigned to a node group randomly. An internal PoS consensus is run in each node group. The node with large coin age (coin amount times holding time) has higher probability to be chosen to generate a new middle block.

Step 3: Generate final BLOCK. The final validation group collects and combines the middle blocks. A PoS consensus is run to generate a final BLOCK which is broadcasted to the whole network.

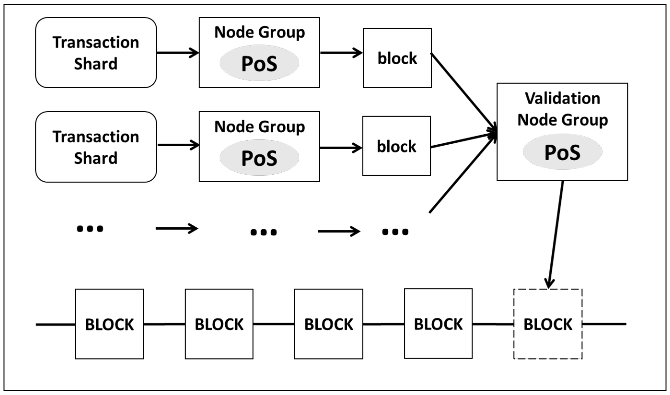

Fig. 1. Step 2 and 3 of the proposed method

Step 4: Reshuffle the nodes. After *t* epochs, all of the nodes are reshuffled to form new node groups.

B. Form node groups

First, node groups are formed. Assume a group contains *n* nodes. The identities of the nodes are supposed to be known by others. A simple way is that each node broadcasts its identity to all other nodes. However, this results in *$O(n^2)$* message complexity. The strategy to reduce the complexity is presented in Section IV.

C. *Run internal group consensus*

After the node groups are formed, transaction shards are randomly assigned to groups. An internal group consensus is run in each group to generate middle blocks. We choose the PoS consensus mechanism. The node owes the highest coin age are more likely to be chosen to generate a middle block. The middle block is sent to the final validation node group.

D. *Generate final block*

The final validation node group collects the middle blocks and generates the final BLOCK. A PoS consensus is run to select a node to generate the final BLOCK. A final BLOCK mainly includes two parts: the previous BLOCK hash and new middle blocks.

E. *Reshuffle the nodes*

Nodes are reshuffled to form new groups every *t* epochs for higher security. Reshuffling could help to reduce the risk of centralization. After new node groups are formed, a new epoch starts from step 1.

IV. EVALUATION AND ANALYSIS

This section discusses the possible evaluation and analysis the complexity and security of the proposed method.

A. *Evaluation*

In our proposed method, the network is separated into node groups where the transaction shards are processed in parallel. Therefore, the throughput of the network is expected to be *c* times higher than the non-sharding consensus protocols. Experiments will be conducted to evaluate the scalability of the proposed method. An emulated network will be built on Amazon EC2 and the nodes in the network ranges from 100 to 1000. According to the steps introduced in section III, node groups is formed firstly. Then transaction shards are assigned to node groups randomly to be processed. The process time is recorded. Finally, the relationship between the network size and the process time will be analyzed.

Although the experiments are still being performed, the proposed method is expected to have a linear scalability. The reason is that transactions are processed in parallel by *c* node groups, which means the processing speed is *c* times of the non-sharding protocols.

B. *Complexity analysis*

Assume the network contains *cn* nodes. If each node broadcasts its identity to all other nodes in the network, the message complexity will be *$O(n^2)$*. To reduce the complexity, we propose to form node groups. Assume each group contains *n* nodes, then *c* node groups are formed in total. When a node group is formed, a leader node is randomly selected and all other *n-1* nodes in the group send their identities to the leader node. The leader node generates an identity list base on the collected information and broadcast this list to the whole network. At the same time, the leader node also receive identity list from other node groups. To reduce the number of messages, a non-leader node only receive the identity list of its own group. In this way, each node knows the identities of other nodes in the same group and the leader node in every group has a view of the nodes in the whole network. The complexity is reduced to *O(cn)*.

C. *Security analysis*

One of the security problems related to the blockchain is known as 51% attack. If one or more nodes take control of over 51% CPU power, they may successfully perform malicious attacks [18]. According to Larimer D. (2013), a 51% attack is much more costly and difficult in a PoS network rather than in the PoW one [19]. In a PoW network, a 51% attack can be executed with enough cost and hard ware. However, in a PoS network, a 51% attack requires not only cost (over 51% possession of stake) but also holding time. In our proposed method, we set limitations on coin age. The coin age is defined as the amount of coins times the holding time. The coin age is valid only if the holding time is between *t* and $t+\alpha$. This limitation could help to reduce the risk of 51% attack.

Another effect related to 51% attack is the incentive. Assume a 51% attack is succeeded in a PoW network to create a false blockchain fork, with enough CPU power, the attacker is able to keep the false fork to receive more profits. This is one possible incentive. However, in a PoS network, even if a 51% attack is succeed to create a false blockchain fork, what the attacker could receive is 1% award of its stake. Since the coinage returns to zero after the attack, the attacker could not keep the false fork to keep making profits. Therefore, the incentive to make a 51% attack is lower in PoS than in PoW network.

V. CONCLUSION

In this paper, we present the design of a proof of stake sharding protocol which is considered to be a possible solution to blockchain's scalability problem. To the best of our knowledge, this is the first blockchain protocol combining sharding protocol and proof of stake consensus algorithm. To our expectation, the proposed method could increase the blockchain's scalability linearly with the network size. Experiments will be conducted in an emulate network to evaluate the proposed method.

REFERENCES

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] Crypto Currency Market Capitalizations. [Online]. Available: https://coinmarketcap.com/currencies/views/all/

[3] COINFOX. (2016). Bitcoin venture capital in 2016: slowing growth rate. [Online]. Available: http://www.coinfox.info/news/reviews/6496-bitcoin-venture-capital-in-2016-slowing-growth-rate

[4] Swan, M. (2015). “Blockchain 2.0: Contracts,” in *Blockchain: Blueprint for a new economy*. "O'Reilly Media, Inc.", p. 10.

[5] Eyal, I., Gencer, A. E., Sirer, E. G., & Van Renesse, R. (2016, March). Bitcoin-ng: A scalable blockchain protocol. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)* (pp. 45-59). USENIX Association..

[6] Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A.. & Song, D. (2016, February). On Scaling Decentralized Blockchains. In *International Conference on Financial Cryptography and Data Security* (pp. 106-125). Springer Berlin Heidelberg.

[7] Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. (2016, October). A secure sharding protocol for open blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 17-30). ACM.

[8] Scalability. Bitcoin wiki. [Online]. Available: https://en.bitcoin.it/wiki/Scalability.

[9] PayPal. [Online]. Available: https://web.archive.org/web/20141226073503/https://www.paypal-media.com/about .

[10] VISA. [Online]. Available: https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf

[11] Proof of work. bitcoinwiki. [Online]. Available: https://en.bitcoin.it/wiki/Proof_of_work

[12] Proof of Stake versus Proof of Work. [Online]. Available: http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf

[13] What Proof of Stake Is And Why It Matters. [Online]. Available: https://bitcoinmagazine.com/articles/what-proof-of-stake-is-and-why-it-matters-1377531463/

[14] PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. [Online]. Available: https://peercoin.net/whitepaper .

[15] Proof of Stake FAQ. [Online]. Available: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ

[16] A Proof of Stake Design Philosophy. [Online]. Available: https://medium.com/@VitalikButerin/a-proof-of-stake-design-philosophy-506585978d51

[17] On sharding blockchains. [Online]. Available: https://github.com/ethereum/wiki/wiki/Sharding-FAQ

[18] Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. (2016, October). A secure sharding protocol for open blockchains. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (pp. 17-30). ACM

[19] Bradbury, D. (2013). The problem with Bitcoin. Computer Fraud & Security, 2013(11), 5-8.

[20] Larimer, D. (2013). Transactions as Proof-of-Stake. [Online]. Available: https://bravenewcoin.com/assets/Uploads/TransactionsAsProofOfStake10.pdf

Yuefei Gao was born in Guizhou Province, China in 1992. She received the B.S. degree in Engineering from China Beijing Science and Techonology University in 2013 and the M.S. degree from University of Tsukuba in 2016. She is currently pursuing the Ph.D. degree at the same university.

She has been engaged in research of Decentralized Trusted Timestamp. Her research interests include decentralized system, cryptocurrencies and the blockchain technology.

Ms. Gao was a recipient of the Outstanding Master Thesis Award.

Hajime Nobuhara received the Ph.D. degree from Tokyo Institute of Technology, Japan in 2002. He worked as a post doctoral fellow in University of Alberta, Canada from April to September in 2002. From 2002 to 2006, he has been affiliated with Tokyo Institute of Technology, Japan. From 2006 until now, he has been affiliated with University of Tsukuba, Japan. IEEE, Japan Society for Fuzzy Theory and Intelligent Informatics, the Institute of Electronics, Information and Communication Engineers member.