IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

A Survey on Consensus Mechanism for Blockchain

Hyeon-Ju Yoon

Associate Professor, Department of Computer Engineering, Kumoh National Institute of Technology, Gumi-City, Republic of Korea

Abstract: Blockchain is introduced as the basic technology of cryptocurrency, with characteristics of decentralization, stability, security, and immutability. Because there is no authority on the peer-to-peer network, the consensus mechanism is essential to make distributed peers reach an agreement on some data value. Including Proof-of-Work mechanism of first implementation of blockchain cryptocurrency, Bitcoin, several consensus mechanisms are introduced to meet the requirements of several kinds of applications. In this paper, we study some representative blockchain consensus mechanisms, analyse their characteristics, and consider matching between applications and consensus mechanisms.

Keywords: Blockchain, Consensus, Permissionless, Permissioned, Requirements of Applications.

I. INTRODUCTION

Blockchain started from Bitcoin[1] of Satoshi Nakamoto as a method to serve timestamp for transactions by cascading the hash value of blocks of which each records a transaction. It can track ownerships of digital assets within a distributed ledger, while users can share the contents of blocks but the record cannot be changed. First application area was cryptocurrency, but there are lots of industrial areas to try to use this technology. The centre of this distributed ledger system is a consensus mechanism because there is no centralized authority agency or decision maker. Bitcoin uses PoW (Proof of Work)[1] mechanism which introduces concept of mining competition which decides who can add a new block of transaction. It allows fully decentralized control, high scalability, unlimited and unrestricted peer participation, but suffers from high energy consumption to solving the puzzle and very low transaction speed. Most of cryptocurrencies use PoW mechanism, but other mechanisms are being developed to overcome the demerits or to apply for applications not requiring incentive or token. In PoS(Proof of Stake)[2], the amount of stake is main factor of choosing block generator. It does not require complicated computation, so has faster transaction processing rate and lower energy consumption. But it's more vulnerable to whom has enough money to destruct the system by investing money and there is "the rich get richer" problem. DPoS(Delegated Proof of Stake)[3] is a modification of PoS. The participants do not take part in the consensus, but vote for the validators. PoET (Proof of Elapsed Time)[4] uses a random leader election model supported by the Intel SGX(Software Guard Extensions) instruction set. PBFT(Practical Byzantine Fault Tolerance)[5] uses message exchanges to reach consensus, as adopted from the classical distributed system problem, Byzantine General Problem[6]. PoA(Proof of Authority)[7] uses the validator's identity as a stake. Besides them, there are many consensus mechanisms and several implementations of each mechanism [8, 9, 10, 11, 12]. On the other hand, many distributed applications which want security and fault tolerance in fast stable way. One type of blockchain cannot support all kinds of applications because they have a variety of characteristics and requirements. In this paper, we study some representative blockchain consensus mechanisms and analyse their characteristics to find the appropriate mechanism our future application. Before that, we introduce the category of blockchain and requirements of various applications.

II. REQUIREMENTSOF APPLICATIONS

A. Types of Blockchain

Blockchains can be largely classified into 2 categories, permissionless and permissioned according to the existence of authority.

In permissionless blockchain, anyone who wants to participate can get an access to blockchain and read/write from/to distributed ledger, audit the ongoing activities on the network, which helps a public blockchain maintain its self-governed nature. Participants are unknown to each other and trust comes from game-theoretical incentives. Because the more participants join, the more stable network is guaranteed, public blockchain mechanism usually offer an incentivizing scheme such as virtual currency. While the permissionless blockchain offer particularly valuable solution from the point of view of truly decentralized, democratized and authority-free operation, it sometimescosts high energy consumption to achieve the incentive or does not guarantee secrecy of transactions.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

In permissioned blockchain system, it is regarded that all or some of the participants are known and can be trusted to behave honestly. With the additional authentication and authorization, it is possible to facilitate the interactions among participants without giving out guarantees on control and performance. Some people distinguish the permissioned blockchain from the private blockchain, and call the permissioned blockchain as consortium blockchain as in [13]. In consortium blockchain, anyone to join the network may acquire permission through a suitable verification of their identity or only a part of participants can participate in some activities.In this kind of classification, a private blockchain is a special permissioned blockchain operated by one entity, that is, a single trust domain. On the other hand, the UK Government Office for Science provides 3 categories of blockchain – unpermissioned, permissioned public, and permissioned private based on existence of permission for read and maintenance functions [9]. The similar classification is introduced in [14]. [14] also proposed 2 criteria matters, level of anonymity of validators and level of trust in validators. Some people criticize that the permissioned (or private) blockchain systems do not conform the basic philosophy of decentralization and strong protection nature against the malicious acts of participants, so the private blockchain is mere cumbersome databases [15].

B. Requirements of Applications

Real world applications of blockchain platforms are very strict and various requirements. They include low latencies, high performance, good scalability, immediate transaction finality, immutability, anonymity, security, and so on. Cryptocurrencies such as Bitcoin should be public so that anyone who wants to use the currency can enter the network and its activities. Blockchain technology can be used to create immutable and censorship-resistant distributed records of any content. One very useful way to apply such a technology is for records of ownership. Financial services or real estate area, this kind of ownership maintenance can be used. The clients can benefit increasing security, more privacy and better control over their personal financial assets. To businesses, blockchain technology enables lower payment processing fees, accepting payments from anywhere in the world, and reduced or eradicated risk of chargeback fraud.
In logistics or supply chain area, the record and proof of products are easily kept track of the legitimacy of complex supplier or logistics networks. Blockchain technology has the potential of large improvement to both providing companies and consumers with access into detailed and immutable records. IoT (Internet of Things) systems consist of lots of products involved with lots of companies. Usually companies do not like to submit into operating within technical frameworks that are controlled by other companies, while the components of IoT should be inter-operable. Blockchain could provide a way to overcome this problem by offering a neutral region where all participants can operate on a shared platform, on completely equal position. Digital or electronic online voting systems require to ensure a fair election, anonymous yet auditable, tamper-proof. Blockchain'sanonymity and public architecture can be adapted to voting system to verify the voting outcome maintaining ballot secrecy. But qualification process of voter should be integrated into the blockchain system.

TABLE 1
REQUIREMENTS OF APPLICATIONS

Area	Requirements					
	Permissioned	**Incentive**	**Finality**	**Performance**	**Scalability**	**Security**
Cryptocurrency	×	○	○	○	○	○
Financial Service	○	△	○	○	○	○
Logistics	△	×	○	○	△	○
Internet of Things	×	△	×	○	○	○
Voting	○	△	○	○	×	○
Real Estate	○	×	○	△	△	○

III.CONSENSUS MECHANISM

A blockchain system can be regarded as a kind of classical distributed system with shared data on globally distributed different kind of networks. The consensus is a fundamental problem of distributed computing, and

A. Proof of Work (PoW)

POW is the first and most well-known consensus mechanism and invented by Bitcoin's founder, Satoshi Nakamoto. In POW, a miner who finds the hash first will be allowed to add a new block of the transaction to the blockchain. The process of mining is extremely computation-intensive, so having a high hashrate is the key for miners to calculate the hash, thus getting the rewards. The main benefits are the anti-DoS attacks defence and low impact of stake on mining

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

possibilities. PoW imposes some limits on actions in the network. They need a lot of efforts to be executed. Efficient attack requires a lot of computational power and a lot of time to do the calculations. Therefore, the attack is possible but kind of useless since the costs are too high. It doesn't matter how much money you have in your wallet. What matters is to have large computational power to solve the puzzles and form new blocks. Thus, the holders of huge amounts of money are not in charge of making decisions for the entire network. The main disadvantages are huge expenditures, "uselessness" of computations and 51 percent attack. Mining requires highly specialized computer hardware to run the complicated algorithms. The costs are unmanageable Mining is becoming available only for special mining pools. These specialized machines consume large amounts of power to run that increase costs. Large costs threaten centralization of the system since it benefits. Miners do a lot of work to generate blocks and consume a lot of power. However, their calculations are not applicable anywhere else. They guarantee the security of the network but cannot be applied to business, science or any other field. Another problem with PoW is 51% attack. A 51 percent attack, or majority attack, is a case when a user or a group of users control the majority of mining power. The attackers get enough power to control most events in the network. They can monopolize generating new blocks and receive rewards since they're able to prevent other miners from completing blocks. They can reverse transactions.

B. Practical Byzantine Fault Tolerance (PBFT)

Practical Byzantine Fault Tolerance (PBFT) was introduced by Miguel Castro and Barbara Liskov at the MIT Laboratory for Computer Science in 1999[5]. PBFT is one of the potential solutions to theByzantine Generals' Problem, one of the classical distributed system issues[6]. With PBFT, the goal is to decide whether to accept a piece of information submitted to the blockchain or not.

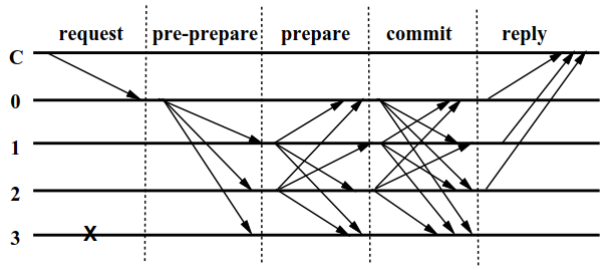

Fig.1 Normal Case Operation of PBFT [Castro]

Each party ("general") maintains an internal state. When a party receives a message, they use the message with their internal state to run a computation. This computation will lead to this party's decision about the message. Then, the party will share the decision with all other parties in the network. The final decision is determined based on the total decisions from all parties. As in classical Byzantine Generals' Problem, PBFT can tolerate betrayal of 1/3 nodes. A high hashrate is not required in this process because PBFT relies on the number of nodes to confirm trust. Once enough responses are reached, the transaction is verified to be a valid transaction. PBFT is a representative consensus mechanism in permissioned blockchain. But it should accept danger of centralization and relatively low scalability due to a number of message exchanges.

C. Proof of Stake (PoS)

POW requires extensive energy consumption. Unlike POW, POS is based on the participants' coin stake [16]. The more coins the stakeholder has, the more likely the stakeholder will add a new block of the transaction to the blockchain. There's no block reward in POS. Because of lower energy consumption compared to POW, POS system is suited for platforms with static coin supply.Under the PoS mechanism, tokens are issued to the validating nodes in the network from the very beginning of the network's existence, which means that tokens are not concurrently minted as new blocks are added to the ledger. A specific node is then selected to commit the new block every few seconds or minutes. But if a node holds more coins, it retains greater power over what is considered to be the truth on the ledger. As such, the selection is strongly influenced by those that have the most coins. Another influencing factor is the time period that coins have been held by users, which indicates whether they are invested for the long-term. Usually PoSrequires considerably less computational work, so the cost of executing PoS is substantially lower. One of the most cited problems with PoS is known as the "nothing-at-stake" problem. On the PoWblockchains, there is an incentive to keep on mining the longest chain on the ledger, as this chain will be considered the primary version of the truth. So the miners are clearly incentivized to mine that one single chain. But with PoS, there is little to prevent a miner from mining on numerous PoS chains and the cost of mining is very low. Therefore a PoS miner operating on various chains can make it difficult for the network to reach consensus, while a bad actor try to change the history.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

There are some variations of PoS to overcome the disadvantages of PoS. In chain-based PoS, the algorithm pseudo-randomly selects a validator during each time slot, for example every 10 seconds, and assigns that validator the right to create a single block, and this block must point to some previous block, usually the block at the end of the previously longest chain, and so over time most blocks converge into a single constantly growing chain. In BFT-style PoS, validators are randomly assigned the right to propose blocks, but agreement to select a block is done through a multi-round process where every validator sends a "vote" for some specific block during each round. At the end of the process all validators permanently agree on whether or not any given block is part of the chain. The consensus on a block does not depend on the length or size of chain.

D. Delegated Proof of Stake (DPoS)

DPoS [3] is a variation of PoS. With DPoS, coin holders can use their balance to elect a list of nodes to be possibly allowed to add new blocks of transactions to the blockchain. Coin holders can also vote on changing the network parameter. PoS is more like winning a lottery, while DPoS gives all coin holders more influence and ownership in the network.Those who have more coins or tokens will have a greater impact on the network that those with fewer.In DPoS, token holders don't vote on the validity of the blocks themselves, but vote to elect delegates to do the validation on their behalf.The delegates are shuffled periodically and given an order to deliver their blocks in. Having few delegates allows them to organize themselves efficiently and create designated time slots for each delegate to publish their block. If delegates continually miss their blocks or publish invalid transactions, the stakers vote them out and replace them with a better delegate.In DPoS, miners can collaborate to make blocks instead of competing like in PoW and PoS. By partially centralizing the creation of blocks, DPoS is able to run orders of magnitude faster than most other consensus algorithms.

E. Proof of Elapsed Time (PoET)

PoET is supported by HyperledgerSawtooth[4], a modular blockchain platform originally developed by Intel. It's applicable to permissioned and public platforms. It lets users on a permissioned blockchain reach consensus, even when the parties don't know each other, while other usual permissioned blockchains require that users know and trust each other.PoET is similar to PoW but without the high resource consumption. Simply put, it leverages trusted computing to enforce random waiting times for block construction. Each participant in the blockchain network waits a random amount of time. The first participant to finish waiting gets to be leader for the new block. In order for this to work, two requirements must be verified. The lottery winner should actually choose a random wait time, not to choose a short time intentionally. Next, the lottery winner should actually finish waiting the specified amount of time. PoET comes from Inter, and it relies on a special CPU instruction set called Intel Software Guard Extensions(SGX). SGX allows applications to run trusted code in a protected environment. For PoET, the trusted code is what ensures that the two requirements are satisfied in order to keep the lottery fair.

F. Proof of Authority (PoA)

PoA[7] is a consensus algorithm where transactions are validated by approved accounts, kind of like the "admins" of the system.PoA is a modified form of PoS where instead of stake with the monetary value, a validator's identity performs the role of stake.In PoA-based networks, transactions and blocks are validated by approved accounts, known as validators. Validators run software allowing them to put transactions in blocks. The process is automated and does not require validators to be constantly monitoring their computers. But it does require maintaining the computer uncompromised. With PoA individuals earn the right to become validators, so there is an incentive to retain the position that they have gained. By attaching a reputation to identity, validators are incentivized to uphold the transaction process, as they do not wish to have their identities attached to a negative reputation. This is considered more robust than PoS, because the incentives in PoS can be unbalanced

G. Comparison of Mechanisms

We compared the consensus mechanisms by borrowing the framework of [8]. Permission means that the network requires explicit membership allowance protocol. Finality indicates whether the transaction once added to a block in the blockchain is considered as final and immutable. In the PoW-like mechanisms, clients have to wait some time to end the competition for the next block. It is not determined, so considered as probabilistic. The performance is higher with platforms that can confirm transactions immediately and reach consensus fast. A cryptographic token is inherent requirement of specific mechanism, such as PoW and PoS. This can be used as anti-spam anti-DDoS measure. Cost means the external resource to participate in the network. In PoW and PoS, the participants should pay for computing power or cryptocurrency. Scalability is the ability to reach consensus when the number of participants are constantly increasing. Most mechanisms are highly scalable, but PBFT needs a number of message exchanges so the scalability is

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 6, June 2018

not so high. Requirement for trust explains that participating peer in the consensus have to be known or trusted. In PoW, PoS and PoET, untrusted peer can participate in the consensus and reach consensus. Last, adversary tolerance is the fraction of the network that can be compromised without the consensus being affected.

TABLE 2
COMPARISON OF CONSENSUS MECHANISMS

	PoW	PoS	DPoS	PBFT	PoET	PoA
Permission	×	both	×	○	both	○
Finality	probabilistic	probabilistic	probabilistic	immediate	probabilistic	immediate
Performance	low	high	high	high	medium	high
Token	○	○	○	×	×	○
Cost	○	○	×	×	×	×
Scalability	high	high	high	low	high	medium
Trust	×	×	×	△	×	○
Adversary Tolerance	<=25%	depends on algorithms	depends on algorithms	<=33%	unknown	<=33%

IV. CONCLUSION

There are lots of consensus algorithms and platforms realizing blockchain system. Different types of applications need different consensus mechanisms which vary in terms of decentralization, performance, scalability, security, consistency, immutability, fault tolerance, incentive, anonymity, finality, and so on. Typical permissionless blockchains should achieve robust consensus among very high number of untrusted participants using computational or memory capacity while sacrificing transaction finality and performance. The permissioned blockchains are not fully decentralized but show much higher throughput that ensures faster transaction finality. When introducing a blockchain-based transaction system to a business or social problems, we should consider the scale of the intended network, the relationships between peers, and both functional and non-functional aspects such as performance and confidentiality before determining the platform and consensus algorithm. It is not easy to say which consensus mechanism is suitable for a certain application because the characteristics of the application requirements are not completely matched with features of consensus mechanism and there may exist several algorithms and implementations for one mechanism. As next step, we will implement an electronic voting system as a blockchain application, search or design appropriate consensus algorithm to support the secrecy of voting. From our survey result, we selected a PoA mechanism as a first candidate, because the voting requires identity of participants, anyone who has the right to vote should be able to participate without any extra cost and the size of network can be predefined.

ACKNOWLEDGMENT

This paper was supported by research year program of Kumoh National Institute of Technology.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://bitcoin.org/bitcoin.pdf, 2008.
[2] S. King and S. Nadal, “PPCoin: Peer-to-Per Crypto-Currency with Proof-of-Stake,”https://peercoin.net/assets/paper/peercoin-paper.pdf, 2012.
[3] M. Snider, K. Samani, and T. Jain, “Delegated Proof of Stake: Features & Tradeoffs,”Multicoin Capital, https://multicoin.capital/wp-content/uploads/2018/03/DPoS_-Features-and-Tradeoffs.pdf, 2018.
[4] HyperledgerSawtooth, https://www.hyperledger.org/projects/sawtooth
[5] M. Castro and B. Liskov, “Practical Byzantine Fault Tolerance,” In the Proceedings of the Third Symposium on Operating Systems Design and Implementation, pp.173-186, 1999.
[6] L. Lamport, R. Shostak and M. Pease, “The Byzantine General Problem,” ACM Transactions on Programming Language and Systems, Vol.4, No.3, pp.382-401, 1982.
[7] Proof of Authority, https://github.com/paritytech/parity/wiki/Proof-of-Authority-Chains.
[8] A. Baliga, “Understanding Blockchain Consensus Models,” White Paper, Persistent, April 2017.
[9] UK Government Chief Scientific Adviser, “Distributed Ledger Technology: beyond Block Chain,” https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf, 2016.
[10] C. Cachin and M. Vukolic, “Blockchain Consensus Protocols in the Wild,”https://arxiv.org/abs/1707.01873v2, 2017.

[11] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso and P. Rimba, "A Taxonomy of Blockchain-Based Systems for Architecture Design," In Proceedings of 2017 IEEE International Conference on Software Architecture (ICSA), pp.243-252, April 2017.
[12] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blokchain", Italian Conference on Cyber Security, pp. 1-11, 2018.
[13] S. Seth, "Public, Private, Permissioned Blockchains Compared", http://www.investopedia.com/news/public-private-permissioned-blockchains-compared/, April 2018.
[14] P. Kravchenko, "Ok, I need a blockchain, but which one?", https://medium.com/@pavelkravchenko/ok-i-need-a-blockchain-but-which-one-ca75c1e2100, Sept. 2016.
[15] N. Hampton, "Understanding the blockchain hype: Why much of it is nothing more than snake oil and spin," Computerworld (online), https://www.computerworld.com.au/article/606253/understanding-blockchain-hype-why-much-it-nothing-more-than-snake-oil-spin/, 2016.
[16] J. Ray, "Proof of Stake FAQ", https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ, 2018.
[17] V. Buterin, "On Public and Private Blockchains," https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/, August 2015.