Consensus Algorithm Using Transaction History for Cryptocurrency

Yuuki Komi and Takayuki Tatekawa[1]
National Institute of Technology (KOSEN), Kochi college

Abstract

Blockchain consensus algorithms for cryptocurrency consist of the proof of work and proof of stake. However, current algorithms have problems, such as huge power consumption and equality issues. We propose a new consensus algorithm that uses transaction history. This algorithm ensures equality by randomly assigning approval votes based on past transaction records. We also incorporate a mechanism for adjusting issuance volume to measure the stability of the currency's value.

1 Introduction

The P2P electronic money system proposed by Satoshi Nakamoto [1] has been applied in various cryptocurrency systems. A blockchain mechanism was proposed to solve the problem of double spending on online payments without the need for authentication by a trusted third party. Blockchain maintains trust in transactions because it is extremely difficult to destroy or alter data.

Blockchains in Bitcoin and other cryptocurrencies maintain a shared registry of chronologically ordered hash chains to enable continuous proof of work (PoW). The hash chain mechanism is useful for achieving tamper resistance and irreversibility. However, each participant repeats the calculation until a specific hash value appears at each node, and the node that determines the desired hash value can add a new block to the chain. The calculation of this hash value requires an enormous amount of computational work. In addition, because it provides incentives to compute hash values, it is problematic that large computational resources are used for computing hash values, consuming enormous amounts of electric power [2].

As an alternative to PoW, a new algorithm called proof of stake (PoS) has been proposed. In this scheme, for example, Stake is based on the "coin age of" how long a user has held the tokens of a cryptocurrency [3]. Ethereum will transition from PoW to PoS in September 2022, which will reduce energy consumption by approximately 99.95% [4]. However, there is concern that PoS will reduce the flow rate of cryptocurrencies.

In this study, we propose a new consensus algorithm for cryptocurrency that does not require huge computational resources, such as PoW, and does not reduce the circulation volume, as in conventional PoS. Suppose that a user has owned a cryptocurrency in the past but has given it away in some transactions.

[1] e-mail: tatekawa@kochi-ct.ac.jp

This transaction is regarded as contributing to the promotion of cryptocurrency, and the user is granted the right to become a signatory of the block, that is, to add a new block. In other words, instead of calculating the hash value of the PoW, the transaction is an incentive.

In cryptocurrency, users who add blocks are given an incentive to add new blocks, as well as a transaction fee. By appropriately adjusting transaction fees, it can be expected that users will not gain from many self-transactions, and cryptocurrencies can be managed appropriately.

The remainder of this paper is organized as follows. Section 2 presents proposal of a new protocol. Section 3 explains adjustment of issuance with new protocol. Finally, Section 4 summarize our study.

2 Proposal of a new protocol

2.1 Transaction history

To use a cryptocurrency coin for payment, it must be received from someone The fact that the transaction was recorded in the chain proves that someone paid the coin to someone else. Because the value of a cryptographic coin depends only on its liquidity, it is essential to increase the number of participants who can perform transactions.

Transaction history is a record of the transactions a coin has undergone. In a blockchain, transaction information is recorded in blocks. A currency not referenced by any transaction is considered an unspent transaction output (UTXO). When a new transaction occurs, it is formed by finding and clearing the UTXO needed for the transaction.

2.2 Checkpoint system

Our protocol grants the right to choose just one blockchain from a tree of branching blockchains for "having made a transaction". This transaction-based grant of authority is expected to expand the range of cryptocurrency use by participants. This protocol is intended for hybrid use with PoW, in which the PoW system is used for the following purposes.

- Guarantee of blockchain irreversibility
- Verification of previous block
- Some financial risk burden for block generation

PoW can also be substituted by full PoS mining with staking.

The protocol uses a checkpoint system for periodic voting and a discrete logarithm problem on an elliptic curve for voter selection to provide resistance against Sybil attacks. This protocol assumes the application of secp256k1 [5] used in Bitcoin.

A checkpoint tree applied in this protocol is a method used in Casper FFG [6], a type of PoS method proposed by the Ethereum Foundation. The checkpoint tree streamlines the legitimacy of the chain such that the entire block tree is not handled. Checkpoints are established at regular heights such that only the legitimate chain can be determined from the forked chains.

As shown in Figure 1, the checkpoints are all blocks whose height (or block number) in the block tree is a multiple of 100, or a genesis block with a height of 0. The "checkpoint height" of a block whose block number is $100k$ is k. The height $h(c)$ of checkpoint c is given by the number of elements in the checkpoint chain, extending from checkpoint c to the root along the parent link.

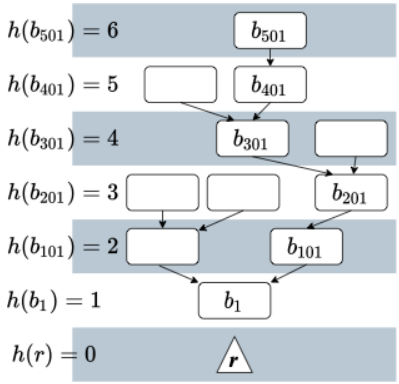

Figure 1: Checkpoint Tree and Height

If the blocks at checkpoints of height n are agreed upon, a legitimate chain up to this point is established. Because FFG is a PoS protocol, in the case of Ethereum, voting is performed by a validator who takes the economic risk of charging one ETH for each vote at each checkpoint. The vote is cast by a validator who carries an economic risk. A checkpoint of height $n$is justified if it receives more than 2/3 of the votes of the valid validators. The block of checkpoints of height $n + 1$ is then justified, and the block of height n is determined (Figure 2). When the tree extends from checkpoint a to checkpoint b, it is denoted as$a \rightarrow b$.

This mechanism must not deny the transactions made in the past by having the property that the established checkpoints are not overturned.

2.3 Selection of verifiers

The selection of verifiers is conducted by the factors shown in Table 1.

All of these elements can be uniquely computed from checkpoint a. To prevent a reference to a block between $a \rightarrow b$ that has not yet been justified in transaction t, 100 is added to the index of the block. To prevent duplicate verifiers, duplicate i is avoided through addition and logical operations. The verifier is determined by t.

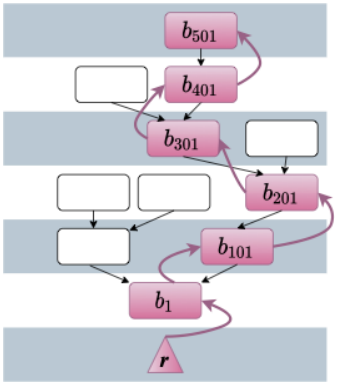

Figure 2: Number of checkpoint blocks and checkpoint height. Downward arrows indicate 99 blocks between checkpoints. Up arrows indicate the order of justification.

Table 1: Factors used in the selection of verifiers

Notation	Description
hash(a)	Hash value of block B_{n-100} at checkpoint a
P	hash(a) multiplied by a scalar with the private key e
S	Set of values P divided by 16 bits
i	Each element in set S
t	Transaction recorded in block $B_{n-(i+100)}$

Thus, the verifier cannot be selected arbitrarily. The output at t must be unused to introduce a punitive mechanism to disable the corresponding UTXO in the case of fraud in checkpoint voting.

2.4 Verifier's Strategy

To ensure that the verifiers selected at a given checkpoint perform verification legitimately, we consider providing them with incentives to perform verification. Subsequently, the verifiers are prevented from cheating. The following rules can be used to ensure that verifiers perform legitimate verifications. The chain extends $c \rightarrow c' \rightarrow c''$.

- The verifier must prove in the message indicating that the UTXO entitled to vote is theirs.
- A UTXO included in a message indicating a vote is considered used and removed from the UTXO set.
- If an irregularity is discovered at a node and the branch on which the irregularity occurs has been voted on, the discoverer of the irregularity

will receive the UTXO that was voted on. An irregularity can be verified by anyone other than the verifier.

- Moreover, those who discover fraud have the right to create a transaction using the voter's UTXO as input. In other words, the mechanism allows anyone to issue a transaction with the voter's UTXO as input. A transaction cannot be used for any purpose other than to prove fraud.
- Because the method described in the previous section would result in a loss to the voter, it is possible to issue a transaction that allows UTXO to input c as it is toward itself after c is fixed, and before some checkpoints are fixed.
- The verifier that casts the correct vote is rewarded with a special signature that earns half of the transaction fee in the block from c' to c''.
- The checkpoint with the highest number of votes is justified.

If the verifier commits fraud, it must have the largest number of transactions in the set of transactions from which it selects verifiers.

2.5 Resistance to Sybil attacks

Sybil attacks are attacks in which an attacker attempts to dominate a network system using multiple nodes, accounts, and computers. The proposed algorithm addresses Sybil attacks in the following manner.

First, PoW was used to generate blocks, ensuring that the creation of a block was not a significant burden for the participant. This prevents attacks that can create many blocks. Second, voters are chosen by participants based on values that cannot be manipulated, and voters cannot assume any interest in others, thus preventing organized voting. Many transactions must be issued to increase the likelihood of being selected as a voter. However, because transactions require a fee, issuing many transactions requires a large fee. This prevents transactions from being issued to become voters artificially.

The following is a quantitative explanation of the difficulty of a Sybil attack: A person who performs a transaction has the potential to become a verifier until $2^{16}(= 65536)$ blocks have been mined after the block containing the transaction is finalized. If the average target time for a block to be mined is 15 s, the verifier will not be confirmed by the block in which the transaction occurred until approximately 273 h later. A total of 655 checkpoints occurred during that time and the possibility of voting at 653 checkpoints, excluding the two starting and ending checkpoints. If a Sybil attack is to be launched, the attacker must generate most transactions in approximately 273 h between the time a transaction is made and when the verifier is determined. Therefore, Sybil attacks are challenging.

3 Adjustment of issuance volume

For cryptocurrency to be accepted for real transactions, the exchange rate between cryptocurrency and legal tender must be stable. Stablecoin, which allows cryptocurrency to be backed by a legal tender to minimize fluctuations in the exchange rate with the legal tender, is being considered. In this proposal, we consider a mechanism to reduce the fluctuation of the exchange rate with legal tenders without backing.

In PoW, miners approve and trust the transactions performed by miners who perform massive computations. Even if the value of cryptocurrency is recognized and the number of miners increases, the amount of cryptocurrency that miners can obtain will decrease. To maintain the number of miners, the value per unit of cryptocurrency increases without a limit. Furthermore, PoW cannot reduce assets and does not act as an adjustment to the money supply.

In economics, the relationship between transactions and the quantity of money is expressed by the following equation, named "Equation of exchange"[7].

$$MV = PT\,, \tag{1}$$

where $M$is the average total money supply in circulation in an economy, V is the velocity of the money transaction circulation, P is the price level. T is the transaction volume of goods and services in a period. Previous studies have applied the laws of economics, including this equation, to the exchange rate between Bitcoin and the US dollar, and it has been shown that exchange rate fluctuations fit the laws well [8].

The difficulty of PoW is determined by the time it takes to add the block and the amount of computation required for the previous block. If a large amount of computation is performed in the previous block, the difficulty of the PoW increases.

However, it is difficult to measure the exact volume of cryptocurrency transactions. Although all transactions are recorded in the blockchain and can be viewed by anyone, if the same person owns multiple accounts and repeatedly trades for themselves, it may appear that far more transactions have been made than have occurred.

If a fee is charged for the transaction, it will prevent many self-transactions, and as described in Section 2.5, it takes about 273 h from the time the transaction is generated to the time the verifier is determined. Coins of cryptocurrency that have already been used to identify verifiers can be considered "correct coins". By examining the "correct coins", we can express the number of transactions that have been verified.

Given the difficulty of PoW, the "Equation of Exchange" is expected to be modified according to the historical circulation rate V_O, transaction value P_O, and number of transactions T_O as follows.

$$MV_O = P_O T_O D\,. \tag{2}$$

Here D denotes the current PoW difficulty. V_O can be determined by referring to transaction records in the blockchain.. P_O and T_O can be determined

from the previous block; therefore, there is no need to refer to all blocks. It is necessary to implement a mechanism to ensure that the value of a variable is uniquely determined in the blockchain, and to detect incorrect values.

The total amount of cryptocurrency can be obtained from the past blocks.

$$M = \frac{P_O T_O D}{V_0} \,. \tag{3}$$

This Mvalue was obtained for each checkpoint. If $M_n > M_{n-1}$ when the n-th block is added, the difference is an additional PoW fee; otherwise, no additional fee is paid. If no additional reward is generated at many checkpoints in a row, a transaction is generated to send 1/2 of the fee paid to the verifier to an address from which no one can withdraw. Because the miner and verifier are rarely the same in this protocol, it is expected that this action is unlikely to reduce the number of miners.

4 Summary

In this study, we propose a new consensus algorithm for cryptocurrency as an alternative to PoW and PoS. The proposed algorithm does not require a large amount of computational work, does not have the problem of decreasing the volume of circulation, and is expected to adjust the issuance volume of cryptocurrencies.

The parameters used in the example of the proposed algorithm mechanism are provisional values that may not be optimal. Further verification is needed to ensure that consensus is properly reached and that cryptocurrency can be operated by many anonymous users without any fraud.

As with other algorithms for cryptocurrencies, software development based on this algorithm is expected to take years of time and effort, and testing will require a large number of collaborators. Software development and testing based on this algorithm will be the subject of future work.

A game-theoretic analysis is needed to determine whether it is in the participants' best interest not to cheat. In a previous study, it was proved that the algorithm for cryptocurrencies that provide disk space instead of PoW is stable and consensus-building using game theory [9], and that this algorithm needs to be verified in detail using game theory as well.

Acknowledgment

This paper is based on YK's graduation thesis and has been reorganized with the addition of new findings. The authors would like to thank Ryuji Enomoto for reviewing the thesis, and Kouki Hamada, Kazuha Hasegawa, and Akimoto Nakayama, and for their useful comments. We would like to thank Editage (www.editage.com) for English language editing.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system" https://bitcoin.org/bitcoin.pdf

[2] Bitcoin energy consumption index (Digiconomist). https://digiconomist.net/bitcoin-energy-consumption

[3] P. Tasca and C. J. Tessone, 2019, "A Taxonomy of Blockchain Technologies: Principles of Identification and Classification", Ledger, 4. https://doi.org/10.5195/ledger.2019.140

[4] Ethereum: The Merge https://ethereum.org/en/upgrades/merge/

[5] Brown, D. R. L., Jan. 2010, "Recommended Elliptic Curve Domain Parameters", Tech. rep. Certicom Research.

[6] Buterin, V. and Griffith, V., 2017, "Casper the Friendly Finality Gadget", arXiv:1710.09437.

[7] Fisher, I., 1911, "The Equation of Exchange 1896-1910", American Economic Review 1, 296-305.

[8] Kristoufek, L., 2019, "Is the Bitcoin price dynamics economically reasonable? Evidence from fundamental laws", Physica A, 536, 120873.

[9] Park, S. *et al.*, 2015, "SpaceMint: A Cryptocurrency Based on Proofs of Space", Cryptology ePrint Archive, Report 2015/528, https://eprint.iacr.org/2015/528