International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

Proof of Stake with Casper the Friendly Finality Gadget Protocol for Fair Validation Consensus in Ethereum

Akshita Jain *[1], Sherif Arora[1], Yashashwita Shukla[1], Prof. T. B. Patil[1], Prof. S.T. Sawant-Patil[2]
[1]Information Technology, Bharati Vidyapeeth Deemed To Be University, College of Engineering, Pune, Maharashtra, India
[2]Electronics &Telecommunication, Smt. KashibaiNavale College of Engineering, Pune, Maharashtra, India

ABSTRACT

Blockchain technology has expanded from being an unchangeable log of transactions for cryptocurrencies to a programmable collective environment for developing distributed dependable Applications (Ethereum). Nevertheless, blockchain technology has handled various challenges, presumably none of the earlier work focused on using blockchain to develop a secure data transaction system using only proof of stake. Ever since Ethereum first announced its intentions to make a switch from a Proof of Work based system to a Proof of Stake based system, it has had everyone guessing how such a bold move would take place. Ethereum's answer to the question is Casper-the Friendly Finality Gadget protocol, which works as a hybrid of PoW and PoS. Many questions could be raised against the working of Casper and we try to raise a few questions of our own. In this paper, we study about Byzantine's Problem, the Nothing At Stake problem, Proof of Work and Proof of Stake based system. We look into why Ethereum wants to shift from a PoW based blockchain to a PoS based blockchain, how Casper has solved the Nothing At Stake problem through its consensus mechanism and whether or not this consensus mechanism is fair. We study about how the validation in Casper could be exploited and propose a system that could prevent such an exploitation, which may prove to be instrumental in ensuring fair validation.

Keywords: Blockchain, Consensus Mechanism, Proof of Work, Proof of Stake, Casper, Validator Set

I. INTRODUCTION

Blockchains are decentralized public ledgers used to keep track of transactions in the form of blocks. They were initially introduced for peer to peer payments [1]. Crypto currencies are an application of blockchain which are administered publicly by users in the network and have no reliance on any third parties [1]. The blocks, which are part of the blockchain, reflect on the current state and the past states of the system. Thus, there can be no space for error of judgement in the validation of transactions. The process of validation of transactions and creation of blocks is termed as mining. Blocks are mined only when a complex mathematical equation is solved and a consensus is reached with the other nodes on the network over the solution of the equation. In recent times, the applications of blockchain have transcended beyond crypto currencies, paving way for smart contracts, application development in the field of finance, real estate, academia, insurance, healthcare and the public sector.

Since, a large number of applications are based on blockchain, more users make use of it. This gives rise to the frequency of transactions and the blocks to be mined. As the number of blocks increases, mining practices become more competitive. Since there are rewards associated with validating transactions and mining blocks, attackers are attracted towards the technology and use malicious practices, like the 51% attack, to disrupt the consensus of the system. This puts security at stake.

Further, the probability of solving the complex equation is directly proportional to the hardware computational power with the node. This consensus (agreement) mechanism is known as the Proof-of-Work (PoW) algorithm.[2] Most cryptocurrencies use the Proof-of-Work algorithm to mine blocks that contain transaction histories. Since, the high computational power required to solve the complex equations is not easily available. Only a few miners can afford thesehardware and have the power of creating the blocks. By pool mining, hackers or malicious miners can validate invalid(non verified) transactions if they own 51% of the whole mining population - making it centralized, which contradicts the main objective of Blockchain, that is, Decentralization. Another concern is the amount of electricity used to mine crypto currencies. Electricity consumption for crypto currencies, such as bitcoin, last year was more than the yearly usage of 159 countries. Mining for bitcoin this year alone has consumed a staggering 49.19TWh of electricity, as of February 16, 2018(00:53 IST)[3]. This poses a huge threat to the environment.

On the other hand, the Proof-of-Stake algorithm is a much greener mechanism which consumes lesser energy in transaction validation and consensus. The probability of creating a block does not depend upon the computational power, instead it depends on your stake in the given cryptocurrency system. It means that if your stake in the given cryptocurrency is at 1%, you can mine upto 1% of the transactions. The process of validating transactions and creating blocks using PoS is known as minting [4]. The nodes that mint blocks are rewarded on the basis of the transaction value and punished for malicious attacks. Their stake in the cryptocurrency is locked up until they perform minting. The problem equations are relatively easier to solve and saves time and resources. If a consensus on the solution is not reached and a malicious attempt is found, the nodes stalked which were locked up are erased from the system. The PoS algorithm also addresses the centralization issue (51% problem) as the attacker or malicious node would have to own 51% of the stake in order to validate invalid transactions. [5] Hoarding 51% of a currency would be very difficult and will only lead to the devaluation of the currency. The attacker would end up hurting himself and make no gain from the malicious attempts.

Cryptocurrencies such as Ethereum have long planned a shift from Proof-of-Work algorithm to Proof-of-Stake algorithm but have so far not been able to do so. However, with the growing popularity of Ethereum, it has also invited a number of attackers to try it's system. As a result, sooner rather than later it must make the switch from the PoW algorithm to the PoS algorithm. Although Casper has been formulated by the owner of Ethereum – VitalikButerin and is nearing implementation, there are still a few things that need to be worked on.

In this paper, we look at the limitations of Proof-of-Stake and Casper and possible solutions to overcome these issues and ensure smoother Proof-of-Stake operation

II. METHODOLOGY

A. Byzantine General's Problem

A Byzantine General's Problem is a consensus problem. It is an extensive problem that all cryptocurrencies have to address.

Assume that various divisions of an army surround an enemy city that they intend to attack. Each division is commanded by its own general and these generals have to communicate with each other to decide on a common plan of action (attack or retreat). This communication takes place through a messenger. The crucial part is that every general must agree on a common decision, as a half-hearted attack would prove to be worse than a coordinated attack or even a coordinated retreat. It may happen that one of the generals is a traitor, who passes two different messages to different generals and disrupts the consensus of the other loyal generals. Thus, an algorithm is required to guarantee that all the generals reach to a consensus and have received common messages from the same general such that no traitor is able to affect the loyal generals from taking a unanimous action. Byzantine Fault Tolerance is a feature of a distributed computer systems that tolerates this class of failure. [6]

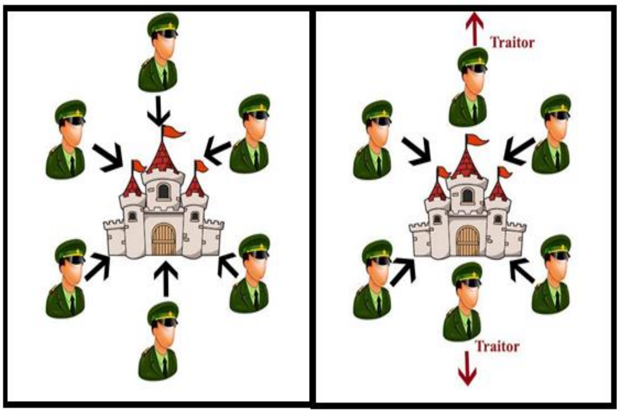

Figure 1. Byzantine General's Problem

B. Consensus Mechanism

It is imperative for the operation of the Blockchain to collectively agree on the contents of the ledger. A shared public ledger like Blockchain which functions on a global scale needs an efficient, functional and secure consensus algorithm. The consensus algorithm has two functions:

1. To ensure that the ledger updates with the same transaction in the same order across the network
2. To prevent attackers from unhinging the system and forking the chain

There are four main types of consensus protocols:[7]

a. Proof of Work
b. Proof of Stake
c. Delegated Proof of Stake
d. Practical Byzantine Fault Tolerance

C. Proof of Work

Proof-of-work was the initial consensus algorithm for the working of Blockchain. This algorithm is used to verify a transaction and add new blocks to the existing chain. In this algorithm, the miners in the network compete against each other in order to complete the transaction and get rewarded. A Proof of work algorithm produces a difficult to solve mathematical equation or puzzle which requires a lot of computational power.

The mathematical equation/puzzle can be one of the following:

1. **Hash Function**, i.e., when the output is known and the input is to be found.
2. **Integer factorization**, i.e., a multiplication of two other numbers to be presented as a number.

The solution to the mathematical equation or PoW problem is called *hash*. A lot of trial and error is required before a valid proof of work is generated by the miners as producing a proof of work is a random process with low probability.

The complexity of this equation is adjusted to limit the rate of generating new blocks to one every 10 minutes in the network. As the probability of successful generation is low, it is unpredictable to determine which miner will be able to generate the next block.

In comparison to finding a solution to the mathematical equation, it is relatively easier to verify the solution. Once a hash value has been found by one miner, the rest of the miners in the network are requested to validate this solution and check for the following conditions:

1. Previous block referenced is valid
2. Timestamp of the block is greater than the previous referenced block and is less than 15 minutes into the future
3. Check that the nonce of the block is valid

Once a 51% consensus is reached in the network, the block can be accepted and added to the Blockchain.

The most widely used proof-of-work scheme is based on SHA-256 and was introduced as a part of Bitcoin. Some other hashing algorithms that are used for proof-of-work include CryptoNight, Scrypt, Quark, SHA-3, scrypt-n, and combinations thereof.[8][10] The hashing algorithm used by Ethereum is called Ethash.

D. Proof of Stake

Proof of Stake(PoS) algorithm takes into consideration the number of coins or the stake owned by a person. It requires the users to show ownership of a certain stake in the cryptocurrency, which determines the number of block transactions the user can validate. In this algorithm, the users who validate transactions and create blocks are referred to as forgers and the process is termed forging or minting.

For example, a user who owns 1% of the Crypto currency available can feasibly forge only 1% of the blocks.

When a forger adds a block to the blockchain, he is rewarded with transaction fees rather than crypto currency units. Hence, it means that no new crypto currency is generated. The transaction fee is an interest obtained on the stake of the user.

Proof-of-Stake algorithm have easier puzzles and hence take less time to create a block as compared to the proof of work mechanism. They are also more environment friendly as they require less hardware and electricity cost.

The elementary cryptocurrency to adopt the PoS method was Peercoin. Later it was followed by Nxt, Blackcoin, and ShadowCoin.

Ethereum is in the process of completely switching from a PoW to a PoS system with the help of it'supcoming consensus protocol called Casper.

II. RESULTS AND DISCUSSION

1) The Nothing At Stake Problem:

In the early proof of stake implementations by blockchains, there were only rewards for creating and validating the blocks and no penalties were imposed upon the forgers for any malpractices. In a fork event, which could be accidental or a malicious attempt to rescript the history and reverse a transaction, a validator would attempt to validate blocks on every chain as he would get his reward irrespective of the chain the block is finally added to. This was a major loophole in the implementation of proof of stake as the forgers chased incentives without worrying about their reputation or stake in the cryptocurrency.

Forging was supposed to be done to secure the blockchain and not to make profits. Thus the consensus algorithm was not working as intended.

2) Casper: Ethereum's Proof of Stake

Casper, the Friendly Finality Gadget, is a consensus protocol that implements and monitors Proof of Stake. It builds consensus on the blockchain with the help of the owners who have a stake in Ethereum.

Casper follows Byzantine Fault Tolerant based proof of stake algorithm with some modifications.

The additional features include:

- Accountability: Violation of a rule can easily be detected and the guilty validators are penalized by slashing of their deposit
- Dynamic Validators: Validators can easily join and withdraw from the validator set with some delay
- Defenses: Casper has the ability to defend against long range revision attacks and attacks where > ⅓ validators drop offline.
- Modular overlay: Casper's design is an overlay on the existing Proof of Work chain, which makes it easier to implement

Validators and Votes

Validation is done through voting. An owner of Ether can become a validator by depositing his stake in the cryptocurrency. The deposits increase and decrease depending on the rewards and penalties. The validators are rewarded when a block is finalized on the main chain and penalized when they violate the slashing conditions. This solves the Nothing at Stake problem which was initially faced by cryptocurrencies implementing proof of stake.

A vote is created (in the form of a message), signed by validators and is broadcasted to different validators. The vote message attributes are:

Table1. attributes for a vote message

Notation	Description
s	hash of a justified checkpoint (the source)
t	hash of the target checkpoint we want to justify
h(s)	height of the source checkpoint
h(t)	height of the target checkpoint
S	Signature of the whole message with the validator's private key

Hashes are unique identifiers of the corresponding checkpoints. h(s) and h(t) confirms that whether the vote is following the rules of the protocol or not.

For any two distinct votes casted by a validator V,

such as:

(V, s1, t1, h(s1), h(t1)) and (V, s2, t2, h(s2), h(t2))

The two Slashing conditions are violated if either of the following conditions holds true:

1. $h(t1) = h(t2)$:

   i.e. heights of both target checkpoint are same

2. $h(s1) < h(s2) < h(t2) < h(t1)$:

   i.e. a vote is casted within the span of another vote

On violation of either of the two Casper Commandments, the validator will lose his deposit.

An evidence of the violation can be included as a transaction into the blockchain, which would lead to the validator losing his entire deposit. The deposit is burned and a small "finder's fee" is awarded to the whistle-blower who submitted the evidence.

For efficiency purposes, validators cast their votes on checkpoints instead of individual blocks. These checkpoints are a multiple of epoch (set of 100 blocks for Ethereum). [9]

A checkpoint or block is confirmed only when ⅔ of the validation is received for it. When we talk about consensus by ⅔ validation, it does not mean ⅔ of the number of validators who have casted their votes for the checkpoint. Instead, we measure validation in terms of the deposited stake. So if ⅔ of the weighted deposit reach consensus, a checkpoint will be validated.

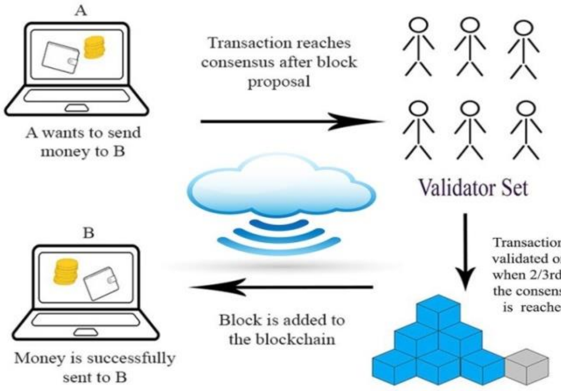
A
A wants to send money to B
Transaction reaches consensus after block proposal
Validator Set
Transaction is validated only when 2/3rd of the consensus is reached
B
Block is added to the blockchain
Money is successfully sent to B

Figure 2. Working of Proof of Stake Using Casper Protocol

Validators, then earn rewards for finalizing checkpoints collectively which in turn helps the entire network. [5]

Accountable Safety

The main duty of Casper is to finalize a checkpoint by selecting a specific chain that represents the canonical transactions of the ledger. Casper guards against finalizing two conflicting checkpoints.

It is quite evident that if two checkpoints are finalized, it would mean that both the checkpoints have received ⅔ of the votes, which implies that ⅓ of the validations were repeated, which is a violation of the Slashing conditions. It results in the slashing of ⅓ of the validators that were acting maliciously by voting on two blocks.

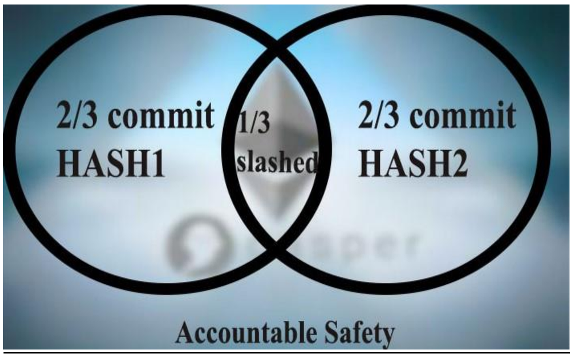

Figure 3. Accountable Safety

Plausible Liveness

In spite of any previous events which may have lead to slashing, delay of blocks or censorship attacks, it is always possible to finalize a checkpoint if ⅔ of the validator set does not violate any of the slashing conditions and follows the protocol. This property of Casper is called Plausible Liveness.

It means that no matter what, a block will be finalized as long as the block has a child in the checkpoint tree.

III. PROPOSED SYSTEM

We've learned that in Casper Protocol, the consensus is reached not when ⅔ of the validators vote for a checkpoint but when the validators whose deposits constitute ⅔ of the total deposits of the validator set agree on checkpoint. We take an example to explain how this could act as a limitation:

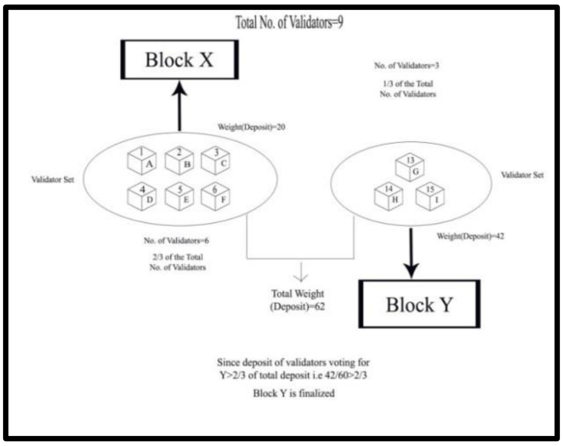

Figure 4. Current Problem in Finalization of a Block(Internal Process of Validation)

In the above example, we have considered a set of 9 validators and the deposit of each of these validators is specified. Now for instance, the members G, H and I vote for block X to be the next block in the chain. On the other hand members A, B, C, D, E and F vote for block Y to be the next block in the chain. Even though ⅔ of the validators(A-F) vote for block Y, it is not considered to be finalized. Instead, the block X gets the consensus as the weight of the deposits of G, H and I is 42, which is more than ⅔ of the total deposit, i.e. 62. Since, the six members had a deposit of only 20 and thus did not make ⅔ of the total deposit; their vote is of no value. This is a game of unfair advantage to those who have more stake in the deposit.

It's fair to say that the validators who have more stake in the currency should exercise more power through their votes, but they could also exploit this power to their advantage. This could mean that the powerful validators may form a pool and have all the voting power, which would ultimately lead to centralization.

To avoid such a circumstance, we propose the following solution:

The voting power of the validators, which is calculated in terms of their deposit should persist, i.e. validation should be done when validators having ⅔ of the weighted deposit vote. But we should also take into consideration the number of validators who have voted for the block. If the number of validators, who have reached consensus, is less than ½ of the total validators of the validator set, neither of the block gets finalized and voting continues. Ultimately, a consensus should always be reached for a checkpoint. When we get ⅔ validation and at least ½ of the number of votes, we can consider that the validation was fair and a just block will be finalized. This would also discourage the powerful validators from forming a pool as it would mean that they would have to persuade ½ of the validator community to join them.

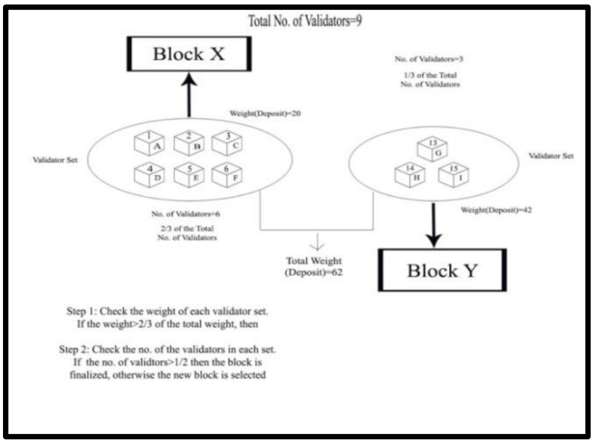
Total No. of Validators=9
Block X
No. of Validators=3
1/3 of the Total No. of Validators
Weight(Deposit)=20
Validator Set
1 A
2 B
3 C
4 D
5 E
6 F
13 G
14 H
15 I
Validator Set
No. of Validators=6
2/3 of the Total No. of Validators
Weight(Deposit)=42
Total Weight (Deposit)=62
Block Y
Step 1: Check the weight of each validator set. If the weight>2/3 of the total weight, then
Step 2: Check the no. of the validators in each set. If the no. of validtors>1/2 then the block is finalized, otherwise the new block is selected

Figure 5. Proposed System

IV. CONCLUSION

The Casper update will change the way the Ethereum network is run. In this paper, we have delineated how Casper-the Friendly Finalty Gadget Protocol is run to reach the consensus using Proof of Stake. Our proposed system mainly focuses on addressing the problem of validation, which is solely based on the weighted deposit as it gives exploitatory benefits to the validators who have a higher stake over the ones who have a lower stake in the cryptocurrency. Although in a system where thousands of validators are present, this problem may not occur so easily, but it still could be an opportunity to exploit the power of stakes. the help of our proposed system, we try to bring a higher sense of fairness to the consensus mechanism of Casper.

Since Casper has not been implemented till now, some ambiguity exists in understanding how the proposed system would be implemented. A clear picture could be painted once the implementation begins, so we can unravel other features of the system as well.

A few other features like the burning of the slashed deposit and prohibiting validators from joining the validator set again after they have exited from it could also be questioned and solutions could be proposed once there's more clarity on those subjects by Ethereum in the near future.

V. REFERENCES

[1]. Iuon-Chang Lin and Tzu-Chun Liao "A Survey of Blockchain Security Issues and Challenges" International Journal of Network Security, Vol.19, No.5, PP.653-659, Sept. 2017 , Page number 653

[2]. Ali Dorri, Salil S. Kanhere, Raja Jurdak, and Praveen Gauravaram "LSB: A Lightweight Scalable BlockChain for IoT Security and Privacy" arXiv: 1712.02969v1 cs.CR] , 8 Dec 2017, Page number 2

[3]. Digiconomisit,"Bitcoin Energy Consumption" , 2018, Online] Available: https://digiconomist.net/bitcoin-energy-consumption Accessed: February 15,2018 00:52 IST]

[4]. Blockgeeks,"Proof of Work vs. Proof of Stake", 2017, Online] Available: https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stakeAccessed: February 16, 2018 00:53 IST]

[5]. VitalikButerin and Virgil Griffith Ethereum Foundation "Casper the Friendly Finality Gadget" , Cornell University Library,arXiv:1710.09437 cs.CR], Page number 1-5, Last Updated: Wed, 15 Nov 2017 01:18:09 GMT]

[6]. Medium, "The Byzantine Generals Problem", 2016, Online] Available: https://medium.com/all-things-ledger/the-byzantine-generals-problem-168553f31480 Accessed: February 16,2018 1:00 IST]

[7]. Medium, "Consensus In Blockchain Systems", 2016, Online] Available: https://medium.com/@chrshmmmr/consensus-in-blockchain-systems-in-short-691fc7d1fefe Accessed: February 16,2018 1:14 IST]

[8]. Bitcoin, "Proof of Work", 2016, Online] Available: https://en.bitcoin.it/wiki/Proof_of_workAccessed: February 16,2018 1:17 IST]

[9]. Olivier Moindrot ,Charles Bournhonesque ICME "Proof of Stake Made Simple with Casper", Page number 1-4, CS244b: Distributed Systems, Autumn 2017 ,Stanford University

[10]. Satoshi Nakamoto "Bitcoin: A Peer-to-Peer Electronic Cash System" Available: https://bitcoin.org/bitcoin.pdfAccessed: February 16,2018 1:17 IST]