Study on Bitcoin and Ethereum Distributed System and Finding Solution to Their Related Problems

Mushfique Nasir Probor, Sahrika Bintey Kabir, Md. Muhtasim Fuad,
Md. Mustakin Alam,Md Humaion Kabir Mehedi,Annajiat Alim Rasel
Department of Computer Science and Engineering
BRAC University
66 Mohakhali, Dhaka-1212, Bangladesh
mushfique.nasir.probor@g.bracu.ac.bd,sharika.bintey.kabir@g.bracu.ac.bd,
md.muhtasim.fuad@g.bracu.ac.bd, md.mustakin.alam@g.bracu.ac.bd,
humaion.kabir.mehedi@g.bracu.ac.bd, annajiat@gmail.com

***Abstract*—In this paper we will be talking about the misconception there is regarding the concept of Bitcoin and Ethereun as a distributed system and find an alternative solution to these problems. Most of the works and research done on the fiend of cryptography based on Ethereum and Bitcoin are somewhat ignorant of the problems that comes with these distributed system. In order to have a solution that takes on the positive side of Bitcoin and Ethereum should also look upon the problems that comes with it. According to our work we will be putting forward the shortcomings of the two stated solutions and discuss about the solution that could eradicate or minimize the existing problems.**

***Index Terms*—Bitcoin, Ethereum, Ring-signature, Sawtooth, Fabric.**

I. Introduction

From the beginning of distributed systems, finding the correct solution to have a decentralized system with proper security has been the goal for many. With the initiation if Bitcoin, it was first seemed to be possible. But for many lack of knowledge on distributed systems like Bitcoin and Ethereum, lead them to a dead-end. Although the good sides of Ethereum and Bitcoin is quite handy, but every solution which used Ethereum and Bitcoin as secured decentralized became faulty due to the innate problems that lies within them. The power consumption problem of Bitcoin and the collaborative approach in Ethereum meant that, any system built on top of Bitcoin was not power efficient, again any system built on Ethereum was not fully anonymous. We introduce smart contract as a way to resolve the power consumption problem, again ring signature mechanism to solve the annonymity problem in Ethereum.

II. Literature Review

A. Energy Consumption of Bitcoin Mining

This paper describes how energy consumption is at a rise exponentially with the increase of the Bitcoin network. This paper concentrates only on the power that is wasted during the PoW mechanism. This gives us an idea of why Bitcoin cannot be used in third world countries which cannot produce such huge amount of electricity and waste it. The loss here is much greater than the gain [1].

B. Exploring Ethereum's Blockchain Anonymity Using Smart Contract Code Attribution

This paper finds the pseudo anonymity in ethereum blockchain and discuss how it is hard to track back the public key without any prior knowledge to information exterior to the network. But it also discuss how the publicly available knowledge on related subgroups can hurt the anonymity [2]

C. Three Attacks on Proof-of-Stake Ethereum

This paper introduces to three attacks that can happen on the PoS mechanism of Ethereum. One attack can stall the consensus to be stalled indefinitely, another can maximize the the profit of the miners who own stakes. The third attack is a combination of both [3].

III. Bitcoin

Bitcoin is a decentralised cryptocurrency which acts as a replacement of physical currency and has no third party involvement during transactions. Bitcoin

A. Transaction

The transactions of Bitcoins are stored in Blockchain Technology. When a miner adds a block, the block contains all the transactions and the hash of the previous block along with miners signature and receivers public key. The hash function then computes a hash of all data i.e Block hash. Hash function takes a string of arbitrary length and generates a unique id of fixed length. If any transaction is modified, the hash will change. Now, the problem with this is the receiver cannot verify whether the miner has double spend their currency [4].

B. Double Spending

While electronic cash system is distributed, decentralised and is a potential mechanism to avoid data corruption. It is difficult to keep tabs on users since blockchain maintains the anonymity of cash owners. This could be the potential chance for miners to double spend their currency i.e using the same currency in more than one case.

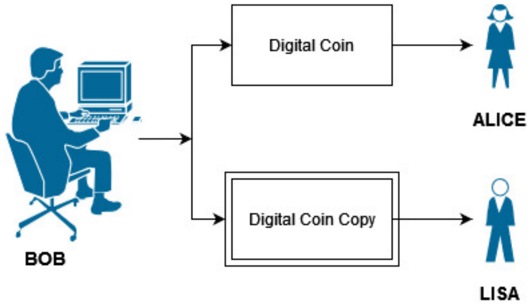


Fig. 1. Double Spending

To solve this problem, the easier way would be checking if the miner has spent their amount in some other place too. If yes, the receiver will reject the currency. But it is not feasible to check if the transaction is high with suppose 1000's of nodes. Thus, a single chain of transactions has to be maintained to ensure everyone agrees who owns what note. This single chain of transactions can be maintained through the Proof of Work(PoW) mechanism.

C. Proof of Work

Proof of Work is a decentralised consensus mechanism, which asks the miners to solve a puzzle as a prerequisite before adding their block to the chain. In any system, there must be a motivation for participants in the system. PoW works as that motivation and controls how blocks are produced. All the miners are given a random puzzle to solve, whoever is able to solve first can mine their block. The other participant blocks get dropped. When the block is created along with the set of transactions, the hash of the block is the proof that the miner has solved the puzzle. Like this, no two blocks can be mined together, thus a single chain of transaction can be maintained, which will avoid the double spending problem. Now the question arrives: what happens when two miners are able to solve a puzzle at the same time. This will create a Fork.

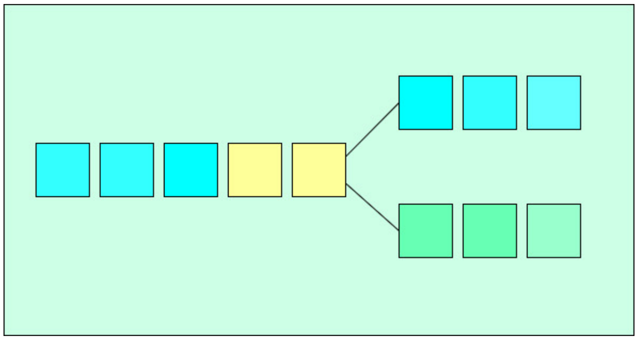


Fig. 2. Fork

Here, two different chains of miners get added like unregistered blocks. In such a situation, the longer chain will be accepted and the other will get dropped. If the length of chains are the same, that chain that maximises the profit will get mined [5].

D. Power Consumption

While PoW does solve the problem of fork and double spending and has an ease of implementation over other consensus mechanisms. There are limitations and one of the biggest drawbacks of PoW is the huge power consumption. In the Proof of Work mechanism, the miners solving the puzzle need huge computing power and since many miners are trying to solve the puzzle there is a massive consumption of power and energy. Since only one miner is able to solve the puzzle at a given time, the energy of other miners just goes to waste. The whole mechanism also needs expensive hardware and machinery which eventually spreads environmental hazards. There is also a risk of hackers attacking the system.

IV. Ethereum

Ethereum is a decentralized blockchain - based platform that creates a peer-to-peer network to safely run and verify program code, often known as smart contracts. Using smart contracts anyone can create their own set of rules for ownership or the formats of transactions. Because of its scalability, big organizations are picking Ethereum as their preferred blockchain. While Bitcoin is "digital gold," Ethereum may be thought of as "digital oil." Ethereum is going to be the more valuable cryptocurrency in the long term since it has more real - world applications.

A. Smart contracts

Nick Szabo first put forth the idea of smart contracts in 1994. Szabo, a cryptographer and legal scholar, is credited with creating the foundation for digital currency. cryptographer and legal expert. Simple to understand, smart contracts are essentially algorithms that run on blockchains and are triggered by the satisfaction of particular conditions. They are frequently used to speed the execution of an agreement so that all parties are informed of the outcome immediately, eliminating the need for a middleman or extra delay. Smart contracts are digital agreements that are executed according to predetermined expressions stored in a distributed ledger. When the prerequisites are satisfied and validated, a network of computers will carry out the activities. Transferring payments, registering a car, notifying relevant parties, and issuing tickets are all examples of such activities. When the deal closes, the blockchain is automatically updated. That means the transaction can't be altered, and only those who have access can view the final outcomes.

B. Benefits of smart contracts

- Independence and cost-cutting: In order to ratify the agreement, smart contracts do not rely on brokers or any other third parties, which removes the possibility of manipulation by these parties. To add, smart contracts save money since there is no middleman involved.
- Efficiency, Speed and Accuracy: When a precondition is satisfied, the agreement is automatically put into effect.

Due to the digital and automated nature of smart contracts, there is no need for cumbersome paperwork or the time-consuming process of reconciling the inevitable human mistakes that arise while filling out forms.

- Security: Due to their encrypted nature, blockchain transaction data are indeed very secure. The interconnected nature of a distributed ledger's data makes it very difficult for hackers to modify a single record without affecting the rest of the chain as well.

C. *Ethereum Transactions*

A transaction must be sent in order to make any change to the Ethereum blockchain. According to the rules of consensus the transaction will only be included in a block when the network agrees that the transaction is valid. Transactions must be authenticated in a block and cost a charge.

An RLP-encoded array that contains the transaction's specifics is the message that makes up the transaction. The values listed below are encoded:

- Recipient: The address where the transaction will transfer value if it is an externally owned account. If a contract account, the contract code will be executed during the transaction.
- Nonce - A ”nonce” is a sequence number. The sequence number is unique to each sender and should exactly match the following available sequence number.
- Signature- This is produced when the transaction is signed with the sender's private key, demonstrating that the sender has given permission for this transaction.
- Value- How much ether should be sent from the sender to the recipient.
- Data- element that is optional and can include any data.
- Gas limit- The most gas that can be used for the transaction is known as the gas limit.
- Gas price- the most gas that you're willing to pay for this transaction.

D. *Alternative of Proof of Work*

In a PoW system, miners must first solve a problem and then send the solution to the network in order for the current block to be mined. The first participant to figure out the puzzle will have access to mine the block. It causes multiple issues, such as energy and time waste. The puzzle-solving component must be removed in order to remove PoW, and in doing so, we must also incorporate collaboration because we are doing away with competitiveness. In general, maintaining anonymity when working together is impossible, however Ethereum's POS (Proof of Stake) feature does so to some extent. There is a sub-protocol for choosing a limited number of entities to propose a block that is part of the voting protocol. When enough people vote in favor of the set of proposals, the block is considered to be finalized.

E. *Proof of Stake*

In case of voting if anyone votes twice then it becomes impossible to choose one group of miners to get the block mined. That is where POS comes to help. The computing effort required to validate blocks and transactions is greatly reduced by proof-of-stake. Blockchain was protected by its use of proof-of-work. With proof-of-stake, blocks are validated by the computers of currency holders rather than a central authority, reducing the need for extensive computing efforts. In order to stake, or compete for the right to validate blocks, currency owners put up their coins as collateral. A coin holder must ”stake” (or put at risk) a certain number of coins in order to join the network of validators. To become a validator on Ethereum, for instance, one must first deposit 32 ETH. To ensure the integrity of the blockchain, many validators check each block before it is closed. If any participant tries to double vote then they will be given a penalty from their deposit amount.

F. *Positives of Proof-of-Stake Mechanism*

The Proof of Stake mechanism has the benefit of using less energy to process transactions and verify blocks. In terms of reducing the effects of global warming, this is obviously very beneficial. When validating blocks, PoS validators don't require a lot of processing power, therefore there's no need for them to keep upgrading their hardware.Due to the significantly reduced time required to choose a validator, PoS blockchains have the potential to be far more effective than PoW ones.

G. *Problems with Proof of Stake and anonymity*

In contrast to the Proof of Work methodology, the Proof of Stake method has not been subjected to extensive testing, therefore it is possible that it could be susceptible to security weaknesses. Additionally, in order to buy stakes, participants are required to make an initial deposit, and as a result, their personal information is already available on the network. And when they try to double vote to the same group of miners, they will be penalized for it, which makes it obvious that they can be tracked within the network; hence, this undoubtedly makes it more difficult for participants to remain anonymous. Also, validators who have big holdings may have an excessive amount of influence over the verification of transactions.

V. Relative solution

Here we will discuss the solution to some of the problems related to Ethereum and Bitcoin.

A. *Power consumption problem of bitcoin and its solution*

The puzzle solving part to mine any block in the blockchain for a miner requires high computational power. Even though it is a distributed system, here each miner works as a node doing the same computation trying to solve the same puzzle or problem. The very concept of a distributed system is to divide the task among different systems so that computation is easier. But as the miners try to solve the same problem here we see a large amount of power consumption being wasted. Once a miner solves the puzzle all the computation by the other miners to solve the problem is nullified or goes to waste. To solve this PoV (proof of voting) is used. In this solution the miners will vote among themselves to choose a single miner to mine the block. By this the power consumption is decreased to a great extent.

B. Solving the trust on third party problem

Smart contract is a public transparent piece of agreement between different parties which ensures that there is no third party involved in any transaction. In some kind of agreement or transaction a third party is involved in real life to mitigate any kind of anomaly or breach of contract between parties. Which in return demands a comprehensive and blind trust on the third party. But through smart contracts no such third party is required as the agreed upon contract comes in a form of code and the code is made public so that there is transparency. And once the contract is deployed there is no chance for any party to alter the contract as a result there is no question of breach of contract.

C. Solution to the anonymity problem of the miners in Ethereum suing ring signature and homomorphic encryption

1) Ring signature: Ring signature is a mechanism to hide the identity of the user of a system. In ring signature a single signature is made through the combination of public and private keys of different users together. By using that signature it is possible to do the relative task without disclosing the true identity of the user.

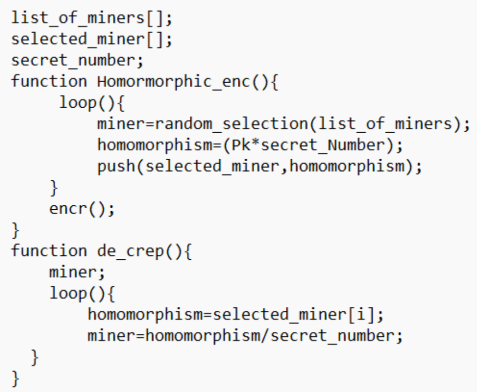
TABLE I
RING SIGNATURE ELEMENTS

Tnx ID	Nonce	Pk	Sk

Ring Signature Elements

2) Homomorphic Encryption: It is a form of encryption where the encrypted data can be processed without decrypting it. For example: Let's say A has 10 bdt and B has 20 bdt. We want C to compute the sum of our money but we do not want C to know the amount of money that we have. Now an encryption function can be f(x)=10*x. This encryption is not known to C but known to A and B. Now A and B send their encrypted information on possessed data. Thus C receives 100 from A and 200 from B. Now thus the addition of the two amounts and returns the result 300 to both A and B. A and B uses the decryption function of f(x)=x/10, and finds that the total amount between them is 30. This is how through encrypting a data, data processing is done with the encrypted data, but still get the right result.

3) Solution: From the previous discussion we found that during the PoS mechanism, the identity of the miners could get disclosed and an attack on the group of selected miners could result in the transaction being compromised. Here through homomorphic encryption we could make the list of selected voters hidden and through ring signature we could make the votes of the voters anonymous. For example: Let A,B,C,D,E and F are the stakeholders in ethereum. Now let 4 of them be randomly selected. Now through homomorphic encryption we will make the list of selected miners hidden. We take the public key of the miners and make a list. Now let's create an encryption method which will shuffle the selected miner's public keys and X-OR them by adding a secret number to each public key. Now the list cannot be disclosed by anyone except the selected miners using their public key and the secret number.



```
list_of_miners[];
selected_miner[];
secret_number;
function Homormorphic_enc(){
     loop(){
         miner=random_selection(list_of_miners);
         homomorphism=(Pk*secret_Number);
         push(selected_miner,homomorphism);
    }
    encr();
}
function de_crep(){
    miner;
    loop(){
        homomorphism=selected_miner[i];
        miner=homomorphism/secret_number;
  }
}
```

Fig. 3. Pseudo code for Homomorphic encryption

Now while voting each of the miners will endorse creating a ring signature. Where the vote will be hashed. Then a random value u will be produced. We encrypt u to produce v. Now for each non signers an e will be created by where e=pi to the power si; where pi is the public key and si is the generated fake secret key for each non-signer. Each e will be X-OR ed with the produced v. For the actual signer, the created v will be X-ORed with u and raised to the power d; where d is the actual private key of the signer. This will make the voting list and the voter anonymous in the PoS methodology of Ethereum.

$$E_K = \text{Hash(Vote)}$$
$$v = E_K(\text{u})$$
$$v = E_K(S_1^{P_1} \oplus v)$$
$$v = E_K(S_2^{P_2} \oplus v)$$
$$v = E_K(S_4^{P_4} \oplus v)$$
$$\text{for voter:}$$
$$v = E_K(u \oplus v)^d$$

REFERENCES

[1] K. Sinan, O. Ozkuran, ”Energy consumption of bitcoin mining”, University of Cambridge, 2019.

[2] L. Shlomi, S. StakhanovaNatalia, M. MatyukhinaAlina, “Exploring ethereum’s blockchain anonymity using smart contract code attribution,” IEEE. Halifax, NS, Canada, 2019 [International Conference on Network and Service Management (CNSM), 2019].

[3] S. Caspar, N. Joachim, M. Barnabé, A. Asgaonkar, T. Ertem and T. David “Three attacks on proof-of-Stake ethereum,” LNCS(Lecture Notes in Computer Science book series),volume 13411. FC 2022: Financial Cryptography and Data Security pp 560–576.

[4] N. Shatoshi, “Bitcoin: A peer-to-peer electronic cash system,” Research Gate, 2009.

[5] G. Gusti, S. Riri, “Evaluation of proof of work (POW) blockchains security network on selfish mining,” 2018 [IEEE Internasional Seminar on Research of Information Technology Intelligent Systems (ISRITI), 2018].