International Journal of
Advanced Science and Convergence

ISSN : 2619-8150
Volume 1, Number 2, June 2019
https://doi.org/10.22662/IJASC.2019.1.2.027

One way to solve the problem of presales of Ethereum: how to use public key cryptography.

Chan-Young Song[1] and Sunghyuck Hong[2]

[1] Student, Division of ICT, Baekseok University, KOREA

[2] Professor, Division of ICT, Baekseok University, KOREA

Abstract

Background/Objectives: Ethereum is a next-generation blockchain developed in 2014 by Vitalik Buterin, a cryptocurrency that can implement various smart contracts. **Methods/Statistical analysis:** When making any contract on a blockchain, the miner is given the corresponding compensation, the block, which is obtained earlier than the hash of the set size by applying a random nonce value and hash algorithm according to the prop-off-work method. In the case of Ethereum, the ETH will be given to the miner who uses more gas in addition to the work proof method. **Findings:** In this case, if the malicious miner increases the amount of gas first, obtains the priority for block generation, intercepts the value derived by the general miner and sends it to the miner, the miner will give the block to the malicious miner. As such, miner, a problem that arises due to the nature of blockchain, analyzes the problem of relying on transaction order that gives the miner a block option to the miner who uses more gas and proposes a solution. **Improvements/Applications:** we described how to solve the problem of pre-sales in the blockchain with public key cryptography using confidentiality. It is hoped that this approach will be fairer and safer.

Index Terms

Ethereum, POW(Proof-of-work), transaction order dependency, Gas, Front-Running

Corresponding author : Sunghyuck Hong
shong@bu.ac.kr

• Manuscript received May 7, 2019.
• Revised May 28, 2019 ; Accepted June 20, 2019.
• Date of publication June 30, 2019.

I. INTRODUCTION

Ethereum, a decentralized computing platform developed by Vitalik Buterin, is implemented with blockchain technology and Ethereum enables smart contracts when compared to Bitcoin using the same technology. The platform on which decentralized applications (dApps) can be used is the Ethereum platform. Although Bitcoin aims to replace the monetary function, Ethereum executes various applications such as SNS, healthcare, finance and insurance through smart contracts. Blockchain takes up a lot of weight in the 4th Industrial Revolution, and smart contract is the most suitable in the Industrial Revolution. However, blockchain still has many vulnerabilities and may not be complete, but there are many problems with transactions and contracts. There are many issues such as double payment, replay attack and 51% attack, but we will deal with the problem of transaction order dependence that the miner who finds the value when creating the block has less gas than other miner, so he can't mine. To find a solution.

II. RELATED TECHNOLOGY

A. Ethereum

Bitcoin can be likened to an application that performs the role of money, and Ethereum is a smartphone that provides an ecosystem to produce various applications. In addition to providing applications using smart contracts, it also has value as a currency itself. In the case of mining to produce blocks using POW (Proof-Of-Work) algorithm, the first block to give miners motivation and profit When creating a token, a cryptocurrency called ETH is paid. When trading, the transaction is stored in this block, so miners are indispensable. Commonly used languages are Solidity (Java script) and Serpent (Python). This language enables smart contracts and builds distributed applications. To maintain a smart contract, a gas fee is required [1].

Table 1. Bitcoin VERSUS ETHEREUM

	Bitcoin	**Ethereum**
role	currency	platform
proof method	POW	POW
mining speed	slow	fast
program language	script	Solidity, Python

B. Smart Contract

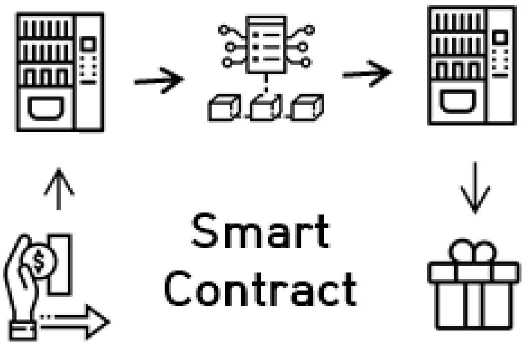

Fig. 1. Smart contract model

It is a technology that can conclude and modify contracts easily and conveniently with P2P without an intermediary in Fig. 1, and it is the same way as the vending machine. Select a drink you want to drink, put the amount according to the price of the drink, and the vending machine automatically gives the change if the drink and change are present. However, the vending machine has received money and you can receive the goods without putting money in unrecognized or fraudulent ways. In order to prevent this, there are auxiliary devices for periodic management and problem solving. Likewise, blockchains require several auxiliary devices to maintain reliability, and additional costs are required to maintain them [2].

C. Gas

Anyone can be a node in the blockchain, but a special group called miners works hardest. Miners protect the network from attacks and prioritize computations. Without these miners, Ethereum cannot exist, so compensation is needed to keep them away.

Before rewarding miners for prioritizing work, they must quantify what Ethereum does and measure it is the gas unit. Every node, or computer, can only handle gas prices for a given amount of time. Thus, miners need to be able to handle the large number of transaction requests that are sent to Ethereum. Adjusting speed can prevent overloading from heavy use or a large number of malicious transactions. Miners rely on gas prices and gas limits to know what is done first.

Gas units are not monetary values, but values of the work to be done. In order to pay the miner, the price of gas is given, and the unit is a small value of Ethereum called Gwei.

You can use this value to pay more for a transaction when many people use Ethereum, so that your transaction can execute first. If the gas price is set to zero, the priority may be pushed back by a value higher than zero, resulting in a late performance.

This lower limit increases the likelihood that the task will fail and the amount of used ether will be lost. So it's very difficult to guess the amount of work you're requesting, so you only have to pay within the range the Wallet app measures the gas limit and tells you. Even if the work is done before the limit, the unused ether is returned because there is no problem [3].

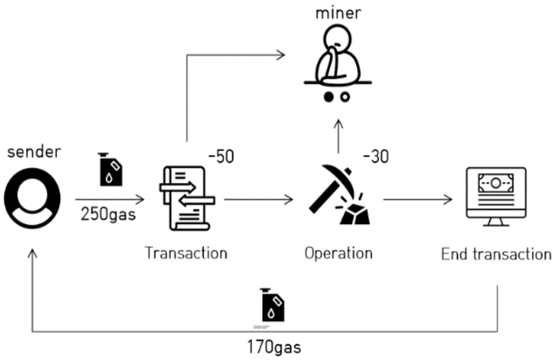

Fig. 2. Gas-Based Transaction

In Ethereum, a fee called gas is used for smart contracts and all transactions. [Fig. 2] is a visualization of the transaction process using gas. When you send money to someone, you enter the gas quantity and the maximum gas quantity and send it to the transaction. This time, it is only on the transaction and not on the block. When you put 250 gas into a transaction as shown in the figure, Ether is deducted from your account and gas is consumed as the transaction is executed. For example, 50 and 30 are subtracted. After the last transaction, the remaining 170 gas is returned back to the user. And gas cost consumed is sent to miner as fee.

D. POW(Proof-Of-Work)

To trade on Ethereum, you need a white book called a block, and you need a miner to make these blocks. The miner who creates the block rewards and motivates the cryptocurrency ETH. Blocks are created using block hashes and the difficulty level is adjusted by difficulty. Blocks are generated when data conditions are satisfied by continuously assigning random nonce values that match the difficulty-adjusted block hash, which consumes computing resources and receives cryptocurrency as a reward. However, there is a problem that the proof-of-work algorithm is not environmentally friendly due to the disadvantage that the block is generated slowly and the wasted energy is serious [4].

E. Front-Running

If a trader or investment broker receives or is likely to receive a buy or sell order that could have a significant impact on the price of a financial investment instrument, he or she may buy or sell, or sell to a third party, at his or her account before entering into the order. It is an act to recommend buying or selling.

Pre-marketing on decentralized exchanges uses a trading bot to pay high fees in advance to secure order priorities, and to gain visibility by trading users in advance [5].

III. Risk Case

A. Decentralized Exchange Pre-Sale Problem

Cornell Tech's team published a report describing the size and nature of cryptocurrency market manipulation through trading bots. Six decentralized exchanges were selected to track transactions and analyze their records in real time, confirming a variety of problematic trades found in the general stock market, including front-running. Over 500 bots with $ 20,000 worth of transactions per day were captured.

Pre-marketing on decentralized exchanges involves paying high commissions through trading bots to secure order priorities and gaining profits by understanding the transactions of ordinary users in advance. Ether Delta and Bancor are mentioned as decentralized exchanges for which this type of transaction has been identified. Banco explained that it is preventing attempts to secure transaction priorities by setting a maximum commission price [6].

IV. Main Subject

In the securities market, pre-sales cause damage to customers, and decentralized exchanges suffer pre-sale by using transaction fees. This is a problem because we can see that the fee problem on the exchange is the same as the gas problem on Ethereum.

Ethereum knows all transactions before entering a block. Since there is no algorithm for the order in which transactions go into the block, this is possible with Miner's choice. Usually, ETH is paid through the factorization factor. If the blockchain contract presents the problem of finding two large prime numbers p and q, we assume that we pay ETH to the first solver.

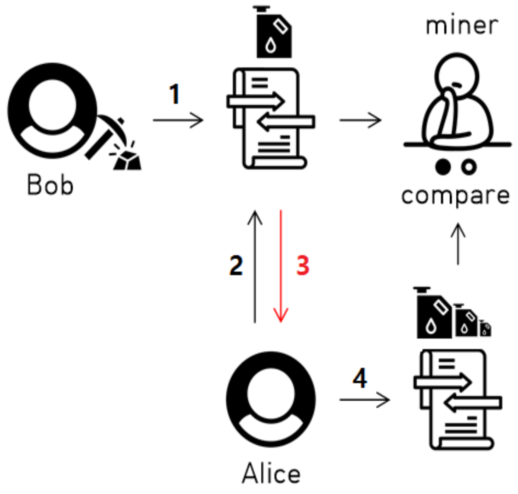

Fig. 3. Ethereum front-running problem

Fig. 3. When there is Bob and Alice as in [3]

Bob gets p and q and puts p and q in a transaction to get ETH. At this time, it is not yet on the blockchain, but the transaction is open to everyone, so anyone can check it.

2. Alice checks Bob's transaction. N is the product of p and q, so we can multiply two numbers to verify that N is correct.

3. If the answer is correct, bring the rice p and q and the amount of gas.

4. Put more gas costs in my transaction than Bob's gas limit.

5. Finally, miner chooses Alice, who costs more gas when Bob and Alice are compared.

The problem is not the one who solves the problem, but the malicious user who steals the problem. These vulnerabilities can block attempts to gain transaction priority by setting the maximum fee price described above. By adopting the maximum fee method, Bob can be compensated with the maximum amount of gas. However, if the amount of gas is too high, it becomes inefficient in terms of cost, and if the maximum gas amount is set low, the amount of gas that the hacker can afford when attacked by the hacker has a disadvantage. Also, if Alice uses the same gas as Bob in a transaction, the miner may have a problem with whom to give ETH, or an unexpected error may cause the block to fail in the worst case.

V. Countermeasures

Ethereum has no algorithm for the order in which transactions go up to the block, and miner pays only for the correct answer and the gas limit.

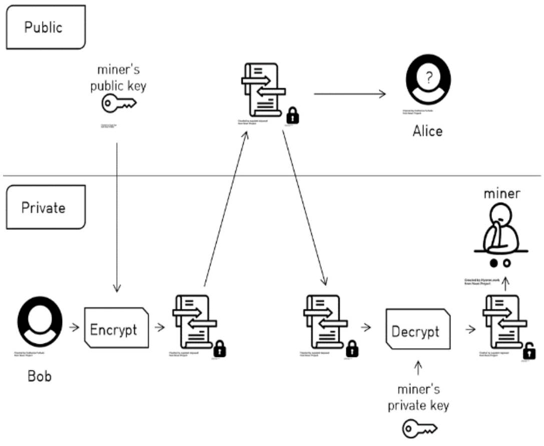

Fig. 4. public key encryption

To solve this problem, [Fig. 4] is used to group p and q together with p and q together with Bob's signature value, and then encode them with miner's signature value, and then put them on the transaction. Insert the message verification algorithm between the steps in which the miner checks the transaction. Miner validates the message using a private key. You can confirm that Bob solved the problem because it contains the signature price while checking the correct answer. The point here is that there is no algorithm for the sequence in which transactions are uploaded to the block as before. But Ellis checks Bob's transaction to find out p, q. It is very difficult to detect p and q encoded by the public disclosure key, and p and q can solve the problem of pre-selling because only miner can check them using private key. p, q, but to be exact, it is to find a nonce value. As Bob encrypts the nonce value using Miner's public key, Alice needs Miner's private key to check Bob's encrypted nonce. Still, the company could be exposed to the danger of hacking due to an enterprise-wide attack, but already miner will give Bob an ETH through verification during the enterprise-wide attack.

VI. Conclusion

The issue of pre-sales has been prevalent in the financial markets even before the blockchain was created. This is also a problem due to the inevitable centralization, which is a way of taking advantage of the information only one gains from evil. Blockchain has tried many connections with the financial sector because it solves everything on the computer and because it cannot be manipulated, but there are many trials and errors until it is officially serviced. . One of them, we described how to solve the problem of pre-sales in the blockchain with public key cryptography using confidentiality. It is hoped that this approach will be fairer and safer.

REFERENCES

[1] Min, Y. & Min, B. (2019). A study on the development of a block chain ethereum technology for digital contents transaction. In *Proceedings of the Korean Society of Computer Information Conference* (pp. 413-414). Korean Society of Computer Information.

[2] Kim, E. Y., Kim, J. W., Jang, H. J. & Shin, J. H. (2018). Implementing a blockchain-based survey platform using Etherium smart contracts. *Academic presentation paper of the Korea Information Society, 2,* 182-184.

[3] Song, J. H, Kim, S. H. & Park, S. Y. (2018). Experiment and Analysis of Ethereum Smart Contract Performance Decline The actual paper of Information Science Society Computing, *24(7)*, 381-384.

[4] Park, S. J. & Hwang, K R. (2018). A Study of fair consensus in blockchain, 36(5), 34-38.

[5] Ko, D. W. & Kwon, T. Y. (2017). Legislative Tasks for Enacting a New Trust Business Law Separated from the Capital Market Act in Korea. *Enterprise Law Research, 31(3),* 33-66.

[6] Cornell, research. (2019.04.16). ″The bot (bot) in exchange for a central spread trading″ ...the delta, Banco were cited.... *TokenPost.*. p, 1. https://www.tokenpost.kr/article-8001

[7] Hong, S. W., Shin, J. C. & Lee, S. J. (2018). Technology Trends for Enhancing Ethereum Blockchain Performance. *Proceedings of the Korean Information Science Society, (19),* -1944.

[8] Kim, M. S. & Lim, E. J. (2018). Ethereum Smart Contract Vulnerability Checker. Paper presented at the Korean Institute of Information Scientists and Engineers, (9403).

[9] Kim, K. H. & Yeom, H. Y. (2017). File Exchange Model Using Ethereum. *Paper presented at the Korean Institute of Communication Sciences,* 1498-1499.

[10] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.