ISSN 1975-8359(Print) / ISSN 2287-4364(Online)
The Transactions of the Korean Institute of Electrical Engineers Vol. 67, No. 12, pp. 1685~1689, 2018
http://doi.org/10.5370/KIEE.2018.67.12.1685

블록체인에 있어 다수 공격에 대한 타당성 분석

Feasibility Analysis of Majority Attacks on Blockchains

Il-Hwan Kim*

Abstract - In this research, 51% attack or majority attack is becoming an important security issue for proof of work based blockchains. Due to decentralized nature of blockchains, any attacks that shutdowns the network or which take control over the network is hard to prevent and assess. In this paper, different types of majority attack are summarized and the motivations behind the attacks are explained. To show the feasibility of the majority attack, we build an example mining machines that can take control over two of the public blockchains, Vertcoin and Monero.

Key Words : 51% attack, Blockchain, Proof of work, Majority attack

1. Introduction

Due to increasing interest in blockchain and crypto currency, there have been much interest in security of proof of work (PoW) based blockchains, such as Bitcoin [1] and Ethereum.

PoW is composed of hash calculation and a difficulty adjustment algorithm [1]. The security of the PoW based blockchains is directly dependent on the construction and the consensus that is used to verify the PoW. This is because the underlying assumption is that the party who can produce PoW the fastest, earns the reward for the work.

51% attack or majority attack (MA) is a specific class of attack that is designed against PoW based blockchains [2]. MA is carried out by an attacker who is computationally more powerful than the rest of the network [3]. Under this assumption, the attacker can theoretically produce blocks with more work by themselves at a faster speed than the rest of the network. To put it in another way, the attacker can create blocks by themselves, withhold the blocks. and then release the blocks to the network at a later time, basically undoing all the transactions that were originally included before the withheld blocks are introduced [4].

Although MA is not feasible for popular PoW based blockchains because of the total amount of computational power in the network is too great, this is not true for less popular blockchains.

In this paper, we present an overview of MA on PoW based blockchains and show feasibility analysis of carrying out MA.

* Corresponding Author : Dept. of Electrical and Electronic Engineering, Kangwon National University, Korea.
E-mail:ihkim@kangwon.ac.kr
Received : October 22, 2018; Accepted : November 3, 2018

2. Consensus Using Proof of Work (PoW)

In blockchain, proof of work (PoW) is used to make the consensus between the nodes if there are multiple candidates to build the next block on. PoW requires hash computation with a certain degree of difficulty. This difficulty is set so that a fixed number of blocks are generated in a set time period.

Since block generation is independent and probabilistic, difficulty is adjusted after fixed number of blocks are found; if the blocks are found too quickly, it is assumed that there is more computational power in the network, and the difficulty is raised to reflect that, and vice versa if the blocks are found too slowly.

3. Types of Majority Attack (MA)

There are several types of MA that an attacker can carry out: Private mining, timestamp spoofing, timewarp attacks, selfish mining, cherry picking attack. Following subsection will describe each attacks in details.

3.1 Private mining:

In this MA, the attacker creates blocks without

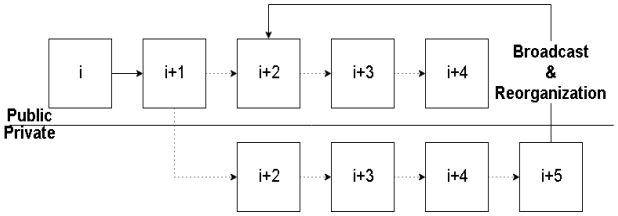

Fig. 1 Example of private mining. The attacker generates blocks without broadcasting them until later

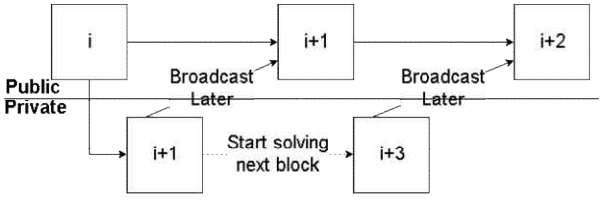

Fig. 2 Example of selfish mining. The attacker gets a head start on solving the next block by broadcasting the solution later

broadcasting them, and then using their computational power, they solve more blocks than the rest of the network [4-6]. After certain amount of time is passed, the attacker broadcasts the privately mined blocks. Figure 1 shows an example of private mining. In this figure, the attacker generates blocks by themselves off the I+1st block, and while the rest of the network generates only 3 additional blocks, the attacker generates 4 blocks. Since the attacker has generated more blocks than the rest of the network, attacker broadcasts his privately mined blocks, which forces reorganization of the blocks, replacing the transactions from the public network that occurred from i+2th block till i+4th block with the transactions from the private network.

3.2 Timestamp spoofing:

In this MA, the attacker takes advantage of the difficulty adjustment period and the fact that the time stamp on the block can be spoofed to a future time[7]. By setting the time stamp way ahead, it tricks the difficulty adjustment algorithm to think that it took very long time to generate the blocks; i.e., the difficulty of the block is too high. This result in reduced difficulty during the next difficulty adjustment period, making the blocks easier to solve.

3.3 Timewarp attack:

Timewarp attack is combination of private mining and timestamp spoofing attack. In this attack, timestamp spoofing is used to lower the difficulties of the block and blocks are privately mined so that only the attacker can benefit from the lowered difficulties [8].

Selfish mining involves an attacker to solve a block before others, but before broadcasting the solution, the attacker starts solving the next block [9]. Since the attacker gets a head start to solve the next block, they are more likely to solve it before the rest of the network does. Figure 2 shows an example of the selfish mining attack. The attacker solves the i+1st block before rest of the network, and then starts working on the i+2nd block. After some time, the attacker broadcasts their solution to the network. Under this scheme, the attacker gets a head start before rest of the network

3.4 Cherry picking attack:

Under this MA, the attacker takes advantage of the difficulty readjustment period by solving the blocks only when the difficulty is low [10]. First, using their computational power, they solve blocks as quickly as possible. Since the blocks are solved very quickly, the difficulty adjustment algorithm will increase the difficulty to reduce the time it will take to solve the blocks. Before the difficulty becomes adjusted and becomes higher, the attacker stops mining and wait for the difficulty adjustment algorithm to decrease the difficulty, and then mine again. This attack is repeated and is coordinated the attack with many different blockchains; the attacker cherry picks between different blockchains. Figure 3 shows an example of cherry picking attack. Each box represents set of blocks that shares the same difficulty. In this example, the attacker first attacks the blockchain 1 until the next difficulty adjustment period, where the difficulty increases for the chain 1, then the attacker attacks the blockchain 2 until the next difficulty adjustment period, and so on. This attack can be combined with other attacks for more effective attacks.

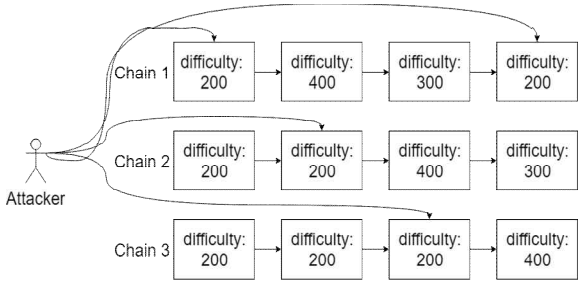

Fig. 3 Example of cherry picking attack between three blockchains

4. Motivation for Majority Attack (MA)

MA achieves following: ownership of coinbase transactions, transaction delay, and overwriting transactions. Following subsections explain possible motivations and description of how they are achieved.

4.1 Ownership of coinbase transactions

Coinbase transactions are the coin reward that is given to the miner who solves the block. During MA, the attacker can use their computational power to produce more blocks than if they mined honestly. In the case of private mining or timewarp attack, only the attacker will gain all the coinbase transactions. In the case of timestamp spoofing and cherry picking, it is not guaranteed that the attacker will receive all the coinbase transactions.

4.2 Transaction delay

Although it is not possible to block a transaction, it is possible to delay it using MA. In this case, the attacker can control when the transaction becomes included in the block or in the case of private mining and timewarp attack, the transactions can be included in the earlier blocks without the rest of the network knowing. This is a problem for time sensitive transactions such as hash time locked transactions, where they have a time limit to submit their proof.

4.3 Double spending

For MA where the blocks are privately mined and broadcasted later, when the privately mined blocks are introduced to the public, it will force reorganization of the existing blocks that are mined by the rest of the network. The attacker can use this chance to overwrite the transactions.

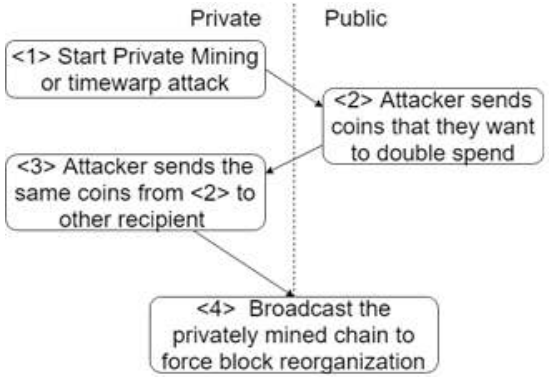

Fig. 4 Double spending

Figure 4 shows how double spending works. First, the attacker starts private mining. Then, the attacker sends coins that they want to double spend in the public network. After that, the attacker sends the same coins that were sent to another recipient (such as themselves) in the private network. Then, the attacker broadcasts the privately mined blocks to the public network. This force block reorganization which will overwrite the transaction that was sent in the public network, effectively double spending the coins.

5. MA Feasibility Analysis

In this section, we collect different data to determine the feasibility of running MA. Several blockchains are considered for testing.

5.1 Machine specification

Following is the list of specification for the miner that was used to simulate the MA.

6 × Hardrive (SSD, hard drive)
24 × Riser
6 × Motherboard (variety)
6 × CPUs (2nd, 3rd, 4th generation cpus)
6 × Power (95%+ conversion efficiency)
6 × RAM (4Gb – 8GB)
24 × GPUs (gtx 1080 ti)
24 × System fans (1 per gpu)
1 × Air conditioner (rated for cooling 6kwh)

The above items were used to assemble 6 miners. In terms of the software, variety of operating systems and mining codes have been tested to reach optimal hashrate.

5.2 List of tested blockchains

Three blockchains, Vertcoin, Monero, and Ethereum are tested to test the feasibility of MA. Description of each blockchain is provided in the following subsubsections.

5.2.1 Vertcoin (VTC)

Vertcoin is a PoW blockchain based on Lyra2rev2 algorithm [11]. It is known to support atomic swap, which is a way to exchange Vertcoin with different PoW based coins. MAs that delays transactions are dangerous for atomic swap, as it uses hash time locked transaction. Because it is

not a very popular blockchain, the difficulty adjustment algorithm is very sensitive to hashrate change, making it an easy target to timestamp spoofing and cherry picking attack.

5.2.2 Monero (XMR)

Monero is PoW blockchain based on Cryptonight algorithm [12]. The difficulty adjustment is done every block with consideration of sudden extreme change in the hashrate. This feature makes Timewarp attacks less effective for Monero blockchain.

5.2.3 Ethereum (ETH)

Ethereum is PoW blockchain based on Ethash algorithm [13]. It is one of the most popular blockchain that supports smart contracts. MAs that delay transactions are especially dangerous for Ethereum, because there many time sensitive smart contracts, such as ICO funding.

5.3 Experimental results

In this subsection, we collected average estimated network hashrates of the three blockchains and compare it with the hashrates of our 6 mining machines.

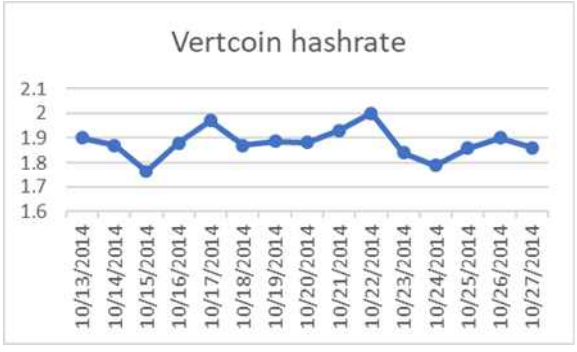

Fig. 5 Vertcoin hashrate

Fig. 6 Monero hashrate

Following table shows the network hashrate of our setup and whether MA is feasible.

Figures 5 and 6 are a small compilation of the estimated network hashrate of the Vertcoin and Monero blockchains, where our setup can successfully launch MA. Unfortunately, our machine cannot launch MA for Ethereum, as the estimated network hashrate is far greater than 1.32 Ghash.

Table 1 Hashrate of our setup

Blockchain Name	Hashrate	MA feasibility
Vertcoin	1.92 Ghash	yes
Monero	24 Khash	yes
Ethereum	1.32 Ghash	no

6. Conclusion

In this paper, overview of 51% attack, also known as majority attack, in a proof of work based blockchain is shown. Several attacks are detailed and the motivation behind the attacks are also shown. Finally, feasibility analysis also show that our machine could have launched majority attacks for Vertcoin and Monero using the hashrate of 1.92 and 2.4 Ghash respectively. As the technology improves, we expect more sophisticated attacks to surface, and blockchains which are less susceptible to these attacks will be required.

References

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system”, URL http://bitcoin.org, 2008.

[2] J. Yli-Huumo, D. Ko, S. Choi, S. S. Park, and K. Smolander, “Where is current research on blockchain technology? — A systematic review”, *PLOS ONE*, vol. 11, no. 10, 2016.

[3] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, “A survey on the security of blockchain systems”, *Future Generation Computer Systems*, 2017.

[4] A. Gervais, “On the security, Performance and Privacy of Proof of Work Blockchains”, *Doctoral Thesis, ETH Zurich*, 2016.

[5] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, “Optimal selfish mining strategies in bitcoin”, *In International Conference on Financial Cryptography and Data Security*, pp. 515-532, 2016.

[6] I. Eyal and E. G. Sirer, “Majority is not enough: Bitcoin mining is vulnerable”, *Communications of the*

ACM, vol. 61, no. 7, pp. 95-102, 2018.
[7] http://en.bitcoin.it/wiki/Block_timestamp
[8] http://litecoin.info/index.php/Time_warp_attack
[9] M. Conoscenti, A. Vetro and J. C. De Martin, "Block-chain for the Internet of Things: A systematic literature review", *In Computer Systems and Applications International Conference*, pp. 1-6, 2016.
[10] D. Meshkov, A. Chepurnoy and M. Jansen, "Short Paper: Revisiting Difficulty Control for Blockchain Systems. In Data Privacy Management, Cryptocurrencies and Blockchain Technology", *Springer*, pp. 429-436, 2017.
[11] http://vertcoin.org
[12] http://getmonero.org
[13] http://www.ethdocs.org/en/latest/

저 자 소 개

Il-Hwan Kim

He received B.S. and M.S. degree in the dept. of control and instrumentation engineering from Seoul National University in 1982 and 1985 respectively and Ph.D. at the Tohoku University in 1993. In 1995, he joined the dept. of electrical and electronic engineering at the Kangwon National University and is currently a professor.