A Survey of Countermeasures for Well Known Blockchain Mining Attacks

Linir Zamir
Engineering College, FAU
Graduate Research
Boca Raton, FL
lzamir2016@fau.edu

Pouya Pourtahmasbi
Engineering College, FAU
Graduate Research
Boca Raton, FL
ppourtah@fau.edu

Mehrdad Nojoumian
Engineering College, FAU
Assistant Professor
Boca Raton, FL
mnojoumian@fau.edu

***Abstract*——Bitcoin is a cryptocurrency that has gained a substantial popularity since its introduction in 2009. Unlike the traditional fiat currency system that requires an intermediary to keep track of the transactions, Bitcoin provides a decentralized exchange environment which is built upon cryptography and peer-to-peer technologies. The Bitcoin transactions are recorded as ledgers and distributed among all the participants on the network, therefore, all the transactions are public. This public log is known as Blockchain. All peers in the Bitcoin network have full access to the history of transactions and due to the cryptographic relation of each block to its previous block, it would be extremely difficult for an adversary to modify a block once it is broadcasted to the other participants in the network. A new block can be added to the Blockchain in a process called mining. Mining refers to finding a 64 digit hex hash value that must be smaller than a target value. Finding this cryptographic hash value, requires intensive computational work. Once the correct value is found by a miner, it can be easily verified by other miners in the network. This intensive computational process is referred to as proof-of-work. A miner who successfully carried out the proof-of-work obtains bitcoins. Due to it's popularity, mining attacks that aim to harm both the Blockchain network and the miner constantly invented. The peer-to-peer technology makes it so it is almost impossible to point back at the attacker. However, with some measurements it is possible to get *some* information, and in some cases even prevent the attack. The first step, however, is to know what are some of the possible attacks that a miner might see.**

I. Introduction

Cryptocurrencies such as Bitcoin, Etherum and many other have been implemented using the Blockchain protocol, based on Nakamoto [4]. Like other classical state machine protocols, Blockchain allow participants to agree on a state, in this case, the client balance of a certain cryptocurrency. In this agreed state, the data can reach all other nodes on the network, with no risk of having the data tampered in any way. This technology can be used for more than just crypto-transactions. It can also be used to insure intellectual property, creating and using of smart contracts, supply chain track and more. In fact, almost every day there are more and more other industries that manage to implement Blockchain. A new block can be added to the Blockchain in a process called mining. Mining refers to finding a 64 digit hex hash value, namely "nonce", that must be less than or equal to the target hash. Finding this cryptographic hash value can be done in several ways, depending on the Blockchain network. Most common one is the Bitcoin Blockchain that uses Proof-of-Work (PoW) where a miner must solve a challenging mathematical problem in order to acquire the hash value for the next block. This process requires intensive computational work. Once the correct value is found by a miner, it can be easily verified by other miners in the network. A miner who successfully carried out the PoW obtains bitcoins as a reward for his work.

Due to the extremely competitive nature of mining, a miner whose computational power is only a small fraction of the whole network's computational power, has a very low chance to mine a block. Therefore, miners often join mining pools to increase their revenue. Once a mining pool generates a new block, the obtained revenue is distributed among all pool members with the respect to their computational power. The availability of numerous mining pools, brings the opportunity to a miner to switch between pools if he realizes that the new pool can potentially increases his profit. Lewenberg et al. [5] studied the reward sharing mechanism in mining pools by developing game theoretic models. They concluded that specifically when the rate of transactions are high, it can be very difficult or impossible to keep the distribution of the accumulated revenue stable. Therefore, there is always an incentive for some miners to switch between pools. Mining a new block can also be done using the Proof-of-Stake (PoS) method [9]. This is an alternative to the PoW, which requires a huge amount of energy. In this method, instead of using excessive energy to answer the PoW problem, a PoS mine power is based on the percentage of transactions that is reflective of his or her ownership stake.

With how great and useful this technology is, there are many ways to attack its infrastructure and users. These attacks are hard to counter and to find the origin of these attacks, due to the nature of the Blockchain protocol. There are, however, some implementations that can be made to a Blockchain network to make it possible to get some information on the adversary [10].

Our Contribution: Security is one of the most important aspect of every technology, particularly the technologies that are meant to provide an infrastructure for a public service. Blockchain and ryptocurrencies are known to have

security concerns. Different researches have covered various aspects of Blockchain and its associated vulnerabilities. This paper is aimed to focus on mining attacks related to Bitcoin and other cryptocurrencies. We provide an overview to the well known mining attacks that have been the subject of various researches since the introduction of Bitcoin and the Blockchain technology. Many of these attacks such as selfish mining and block withholding have been studied extensively by many researchers while many other attacks such as routing attack and pool hopping have been addressed and discussed more recently. Although the Blockchain technology is not only limited to Bitcoin and more generally cryptocurrencies, the majority of researches in this field are focused on Bitcoin and its infrastructures. In this paper, We briefly describe these mining attacks and then we provide the detection methods and countermeasures for each attack individually. Some of these solutions are solely relied on game theoretic models while many others have been examined in a simulated or a real world situation.

Organization of the Article: This paper is divided into six sections. In Section II, we briefly cover the Blockchain technology, its attributes and related terminologies and concepts. In Section III, we cover individual mining attacks comprehensively followed by the methods of detection and countermeasures. In Section IV, we mention few countermeasures that are not specific to one kind of attack, rather more general consensus adjustment and mechanism that can improve the security and reliability of the Blockchain network. Section V provides technical discussions and finally Section VI includes the concluding remarks.

II. Blockchain Technology

The first time the Blockchain type of data structure was introduced was in 1990 by Stuart Habert and W.Scott Strornetta [11] and was originally intended to timestamp digital documents so that it is not possible to temper with them. However, it was mostly unused until it was adapted by an unknown person goes by the name of Satoshi Nakamoto in 2008 [4] as a core component to support transactions of the digital currency, specifically Bitcoin. These transactions are stored on a constantly growing ledger, as new transactions, or 'blocks', are added to it as seen in Figure.1. Each block includes the cryptographic hash of the prior block (a timestamp and a link), linking the two. The linked blocks form a chain, hence the name 'Blockchain'. The main idea of the Blockchain technology is that users can have access to the shared ledger of the network. This ledger is immutable, which helps establishing trust between users in the unsecured environment.

The basic idea behind the Blockchain Technology is that it allows parties to send and receive digital assets (Usually refers to as digital currency) on the peer-to-peer network that can then store the transactions on "blocks" in a way that is shared across the network. The user who initiated the transaction, the user receiving it and the transaction data are all registered on this "block", or ledger by using public key encryption and digital signatures. The next step is to validate the transaction on the ledger, and this is done using what is called "consensus mechanism". The technology of Blockchain may vary but the basic idea remains the same - some consensus mechanism is running in order to mine a new block in a decentralized fashion, while the block is verified by the peers on the network. This technology, even with all of its security achievements, is still exposed to different types of attacks on different levels of it structure.

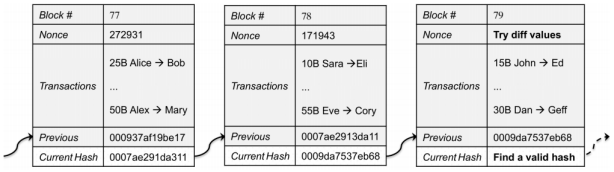

Fig. 1: Example of a Blockchain network blocks [18]

A. Consensus Mechanism

There are many ways to achieve consensus on a Blockchain network. *Proof-of-Work* (PoW) was presented in a 1993 journal [12]. This mechanism is used by Bitcoin [4] and is the most mainstream Blockchain system today. The mining process is based on electing a 'leader' who will decide the content of the next block. Whenever a new block is mined, the first miner to complete the mining process gets to be the leader of the block. The elected leader also responsible for broadcasting the block to the network, so that other users (peers) can verify the validity of its content. Motivation for mining is achieved in the form of currency (currency reward, transaction fees). The most widely used proof-of-work scheme is based on SHA-256 and was introduced as a part of Bitcoin and few other cryptocurrencies. This mechanism, however, have a few problems. A big issue is that the mining process depends on the computational power of the leader [13]. Another issue is that miners started to organize in groups called 'mining pools' where they combine their computational power, and then if they create the next block, they distribute the award evenly across everyone in the pool.

Another very popular consensus mechanism in is *Proof-of-Stake* (PoS) [14], [17]. This method was first introduce in 2012 to address the first problem of PoW, which was the energy inefficiency. In Proof-of-Stake, every miners power is determined by the total amount of currency coins he or she has. In this mechanism, an auction is carried out and whoever wins gets to be the miner. This means that a leader is being selected based on his bid, or how much money he is willing to put 'at stake' in order to win the auction. Unlike PoW, in PoS, whenever a new block is mined, no new coins are being distributed in the system. However, miners are rewarded with transaction fee instead [15].

There are more consensus mechanisms that are being used for different Blockchain networks such as *Delegated-Proof-of-Stake* (DPoS), *Proof-of-Capacity* (PoC), *Proof-of-Elapsed-*

Block	transaction records that includes a timestamp, transaction data and the hash value of the previous record.
Blockchain	A digital ledger of all transactions that are saved chronologically as individual blocks. The blocks are linked together through a cryptographic signature and cannot be modified. The blockchain is distributed to all the nodes on the network therefore, it's decentralized.
Mining	The computationally intensive process of generating a new block by finding a matched hash value through trial and error.
Proof-of-Work (POW)	The hash value for the new transaction can be found only through mining process but can be verified easily by other nodes in the network.
Mining Pools	number of miners combine their computational power to increase their mining performance. The rewards are spited proportionately between the miners based on their individual mining power.
Mining Power (Hash Power)	The amount of computational power each miner or mining pool allocates to the mining process
Fork	When two or more branches are created from a single block. Forks are usually resolved by blockchain consensus and therefore short-lived.

Time (PoET), but in this paper we will cover attacks on the two mostly used algorithms.

B. Fork

The Blockchain fork can be seen as a collectively agreed upon update of the Blockchain. In this case, the Blockchain splits into two distinct branches. It usually happened as a result of a change in the consensus mechanism, but sometimes it can be unintentionally initialized by mistake as a part of protocol malfunction or issues in the software updates. Looking at Bitcoin, there has been many forks that can be seen as updates to the Blockchain. A very famous one is the Bitcoin Cash fork. Bitcoin original block size is 1MB, which was fine during the first few years, but as Bitcoin gained popularity more and more transactions were initiated and the size stated to became an issue. This is when the Bitcoin Cash developed by a group of Bitcoin developers which was a new Bitcoin client with a new block size of 8MB. However, this new Blockchain was not accepted by the majority of users on the Bitcoin Blockchain, and this was why they created this as a fork on the Bitcoin Blockchain.

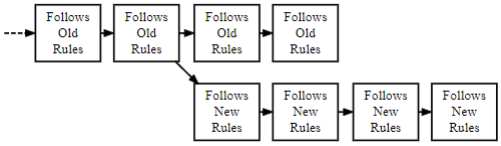

Fig. 2: A Blockchain fork [100]

Intentional forks can be either soft or hard. A *hard fork* is a *permanent* divergence from the previous version of the Blockchain, blocks of the old version will not be accepted by the newest version. A hard fork is a big change to the protocol that makes previously valid blocks or transactions invalid. Any transaction on the newer fork will not be valid on the older chain. All nodes and miners will have to upgrade to the latest version of the protocol software if they wish to be on the new forked chain.

A *soft fork* can happen in similar situation, however it is common when there is a change in the software protocol, in such a way that it is required to keep the previous transactions, or block, valid to the new rule. It means that the new forked chain will have new rules but it will still work with the old rules (An example will be a change of the consensus mechanism). This type of fork doesn't require everybody in the network to upgrade in order for the new rule to apply, it is possible to have only the majority of nodes in the network. Hard fork, on the other hand, requires (almost) all to upgrade and agree on the new version.

When it comes to resolving forks on a Blockchain network, *soft forks* are relatively easy to fix. Verifying the fork can be done by achieving consensus with all of the peers on the network. This way, the state of the Blockchain can be resumed to its correct state. *Hard forks*, however, are slightly more difficult to resolve because of the need to trace back all the way back to the initial fork. A famous example of resolving hard fork was made in Spring of 2016 where a Distributed Autonomous Organization (DAO) [21] was created on Ethereum [20]. The basic idea of it was to encourage people to invest and pay Ethers (The currency of Ethereum) to DAO so that they can get the opportunity to vote on and become investors in different projects proposed by Ethereum-based startups. The DAO experiment failed after a hacker managed to steal over $50M USD worth of Ethers. After that, the community of Ethereum voted to return (fork) to the state before the hack.

C. Stale and Orphaned Blocks

During the mining process, many users attempt to be the leaders of the next block. In a case that a more than one miner successfully finds a valid next block at the same time, both proposed blocks are *valid*, but only one can be appended to the Blockchain. At this point, the block that will be verified faster will be the block to be appended. The other block is called *stale block* and will be left on the Blockchain until deleted. There are mining attacks that lead to creation of stale blocks on the network, which makes it so the miner of the block will not be rewarded. Another similar form is the *orphaned block*. As the name suggests orphan is a child with no parent. In Bitcoin an orphaned block is a block that is not part of the big chain. Similar to stale blocks, it usually happens when two or more miners solve a block at a similar time. However, orphan blocks are legitimate, verified, and were originally accepted by the network at one point of time. Since they are no longer active