Blockchain Attacks and A Model for Double Spending Attack

Submitted By

Abu Hasnat Tareq

142-35-677

&

Mahmuda Sultana

142-35-667

A thesis submitted in partial fulfillment of the requirement for the degree of Bachelor of Science in software engineering

Department of Software Engineering
DAFFODIL INTERNATIONAL UNIVERSITY

Fall – 2018

APPROVAL

This thesis titled on "**Blockchain Attacks and A Model for Double Spending Attack**", submitted by **Abu Hasnat Tareq, ID: 142-35-677 and Mahmuda Sultana, ID: 142-35-667** to the Department of Software Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS

26/12/18

Prof. Dr. Touhid Bhuiyan **Chairman**
Professor and Head
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

K. M. Imtiaz-Ud-Din **Internal Examiner 1**
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Asif Khan Shakir **Internal Examiner 2**
Lecturer
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Dr. Md. Nasim Akhtar **External Examiner**
Professor
Department of Computer Science and Engineering
Faculty of Electrical and Electronic Engineering
Dhaka University of Engineering & Technology, Gazipur

DECLARATION

It hereby declere that this thesis has been done by us under the supervission of **Afsana Begum,Senior Lecturer,** Department of Software Engineering, Daffodil International University. It also declere that neithor this thesis nor any part of this has been submitted elesewhere for award of any degree.

Abu Hasnat Tareq
Student ID:142-35-677
Batch: 14th
Department of Software Engineering
Faculty of Science & Information Technology
Daffodil International University

Mahmuda sultana

Mahmuda Sultana
Student ID:142-35-667
Batch:14th
Department of Software Engineering
Faculty of Science & Information Technology
Daffodil International University

Certified by:

26/12/2018

Afsana Begum
Senior Lecturer
Department of Software Engineering
Faculty of Science & Information Technology
Daffodil International University

ACKNOWLEDGEMENT

We would like to show our gratitude to a number of people whose advice was very valuable in this research. We would like to mention that our supervisor **Afsana Begum**, Senior Lecturer, for her unceasing direction and endurance to accomplish the research uses. We also like to mention **Prof. Dr. Touhid Bhuiyan,** Professor and Head, and **Kausik Sarker**, Assistant Professor & Associate Head Department of Software Engineering, Daffodil International University for sharing their pearls of wisdom to work with us during the course of this research. We also thank all teachers of my department for their valuable advices and suggestions.

TABLES OF CONTENTS

LIST OF TABLE

LIST OF FIGURE

ABSTRACT

Blockcahin is such a technology that helps us to use a shared ledger. Although the ledger is in shared manner, the total system is quiet secure. Bitcoin is a crypto currency which uses blochchain technology. Value of Blockchain is very high than doller or some other expensive currency. This is one of the reasons of encouraging theft attack on the blockchain technology. In this paper, we analyze about the attacks of blockchain, their targeted area, reason and their possible solution. In this paper our main focus was to represent a total review on Blockchain technology. Besides this, Double spending attack is a major attack on blockchain which is occurred twice till now and causes a huge loss of crypto currency. In this paper, we also try to find out the reason of this attack and we have proposed one solution that can prevent Double Spending Attack. Our findings will provide some future direction for initial research and also help the crypto business analysts to predict about present security in the aspects of blockchain network.

Keywords: Blockchain, Bitcoin, Attacks, Double spending Attack, Solution

CHAPTER 1

INTRODUCTION

We have got the first concept about Blockchain and Bitcoin from a published paper of “Sathoshi Nakamoto” named as “A peer to peer electronic cash system”. Blockchain as a secure ledger is the current digital platform and takes attention to it academically and industrially. In 2015 and 2016 Bitcoin was the best performing currency [23], but in 2017 ripple reach to best position [24]. Blockchain is used in transportation and data management system, this transaction allows for decentralized, immediate and dependable, and there is no need third party, such as dealer negotiator, etc. Consensus mechanism is making this network more secure [1]. Though it is a secure system, but for some vulnerability or security loss a huge bitcoin is being stolen from 2010 to 2018. In the first six months of 2018 micro researcher detect more than 787000 [2] of malicious cryptocurrencies mining software. In May and June 2018 Double spending attack occurred which was constructed by “Equihash” algorithm and effect on POW consensus mechanism. By this attack $18.6 million US bitcoin was stolen [3].

1.1 Research Objectives

So we create a review on Bitcoin, their security, their risk, real attack, loss, effect and countermeasure and try to combine them in a single paper. Then our objective was to take any vulnerability for more study and try to propose a solution.

1.2 Motivation of the Research

A workshop was held on a blockchain technology on 2017. We attended there and then we were being eager to know about blockchain, and when we strat studding about this, we found that different types of attack occurred in different times and we could not find these attacks in a single one. So we decided to combine them in a single paper.

1.3 Problem Statement

All of the attacks were not in a single paper, it was hard to find out according one by one. Besides, though countermeasure of double spending attack was given, but this attack occurred still in 2018 so we provide a possible solution for double spending attacks.

1.4 Research Questions

1. Is there a document to gather a complete knowledge about Bitcoin and its attacks?
2. Instead of having countermeasure algorithm why double spending attack is still attacked on the blockchain network?

1.5 Background

Blockchain is a distributed ledger. It is a secure systemic ledger but we can see this network has been under attack in several time and loss its currency because of its vulnerability. As blockchain is a hot topic in this present technological period, so we try to find out about the vulnerabilities and provide possible countermeasures.

1.6 Research Scope

The main contribution of this research is providing a possible solution model for avoiding double spending attack, we also analyze actual attacks of blockchain.

1.7 Thesis Organization

The organization module of our paper is:

a. In chapter 2, we analyze and discuss about blockchian attacks.

b. Our working process or methodology is in chapter 3.

c. Our proposed model is in chapter 4.

d. The results and discussion in chapter 4.

e. Finally, conclusion of our paper is chapter 5.

CHAPTER 2

LITERATURE REVIEW

In this section, we overview the key concept of blockchain, bitcoin, ethureum, concensus mechanism, risk, attacks and possible solution. We found some papers that focus on blockchain attacks within the academic journal and the majority of OI conference, however we also look at the general research confirmation.

2.1 Blockchain

A suite of distributed ledger technology that can be programmed to record and track anything of value it is a technology that powers bitcoin. There are various types of currency based network, these are given in table 2.1.

Table 2.1: Various type of blockchain network[79]

Type	**Description**	**Exmples**	**Transaction medium**
Blockchain 1.0	Currency	Financial transaction	Bitcoin
Blockchain 2.0	Smart Contracts	Facilitation, verification, enforcement	Ethereum
Blockchain 3.0	DApps	Decentralized storage and communication	Ethereum storage
Blockchain 4.0	Making blockchain usable in industry	Making Blockchain technology useable to industry 4.0 demands	

2.2 Block: A size number to specify how much data is coming next. It is composed of a header and a long list of transactions.

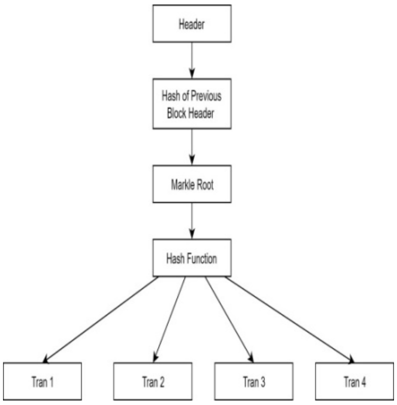

Figure 2.1: Structure of block

2.3 Hash: A converter who converts, input text and numbers into an encrypted output. A one-way function that takes data of any size as an input and produces a fixed length output. Hash computation should be fast and easy while reversing the process should expensive and difficult.

2.4 Hash Function Used to amp data of arbitrary size to data of fixed size. Used in combination with a computer software for rapid data lookup. Hash graph is a distributed ledger technology developed by "lemon baird". The header contains metadata about a block.

2.5 Markle Root: Hash of all hashes of all the transactions that are part of a block in a block chain network.

2.6 Consensus mechanism

Table 2.2: Consensus types and their market capitalization of various kind of cryptocurrencies (running time)

Name of Crypto	**Consensus**	**Market cap**
Bitcoin	Pow	$71,890454,161
Ethereum	Pow	$12,092,653,223
Ripple	Ripple protocol	$14,796,628,442
Bitcoin cash	Pow	$3,023,721,859
Steller	Steller consensus	$3,121,437,638
Litecoin	Pow	$1,990,487,368
Cardano	Pos	$1,066,100,559
EOS	Pos	$2,660,752,236

2.7 Bitcoin

Table 2.3: Market value of bitcoin in different time (From starting to running time) [29]

Date	Value of bitcoin in Us $
Jan 2009	**0.00**
July 2010	**0.08**
Feb 2011	**1.00**
July 2011	**31.00**
Dec 2011	**2.00**
Dec 2012	**13.00**
April 2013	**266.00**
June 2013	**100.00**
Jan 2014	**800.00**
April 2014	**440 – 630**
March 2015	**200 – 300**
June 2016	**450 – 750**
Jan 2017	**800 – 1150**
Sept 2017	**5000**
Dec 2017	**17900**
Feb 2018	**6300**
Nov 2018	**3778**

2.8 List of Attacks

We go through at most 60 papers to find out the attacks that may attack the blockchain network or somehow can hamper or hack the network to steal currency. We found 19 different attacks and try to give a short description about all of this attacks.

2.8.1 Spam Attack [4]: A spam attack effects a committed transaction by slowing the network and making the block creation delay. As a result, the reachable peer and network outage appear as less than before [5]. From 2015 to 2017, about 200,000 transactions are unconfirmed for that it halts the network. [6] Koichi Nakayama, Yutaka Moriyama and Chika Oshima propose an algorithm named as "SAGABC algorithm" to prevent spam attack [7]

2.8.2 Double spending Attack [8]: Double spending attack refers to that a different number of transactions occurred where the crypto currencies are same. Suppose an immoral client C1 make a transaction T1 with a bitcoin set B1 to purchase products from vendor V1 at time t1. At the same time/time t2, C1 makes another transaction T2 with the same Bitcoin set B1 where the recipient addresses are not same. If this occurs, then we can say C1 done a successful Double spending attack. Meni Rosenfeld proved an expression that find out the probability of successfulness in Double spending attack (a_z)

$$a_z = min\left(\frac{q}{p}, 1\right)^{\max(z+1,0)}$$

$$= \begin{cases} 1, \ if\ z < 0, q > p \\ \left(\frac{q}{p}\right)^{z+1}, \ if\ z \geq 0, q \leq p \end{cases}$$

Where, a_z = Double spending attack

p = Hash rate of Honest nodes pool

q = Hash rate of Attacker pool

z = Number of blocks

Attacker's hash power and number of blocks mainly define the success of double spending. For a successful attack, attackers hash power should not be less than 50% [8].

To prevent Double spending attack H. Lee, M. Shin, K.S. Kim, Y. Kang, and J. Kim propose a solution ‘’Recipient oriented transaction’’ system [9].

2.8.3 Eclipse Attack [11]: To enlarge and store information about other peer, a node chooses eight peers randomly in a network and eclipse attack invasions on that node to take benefit from peer-to-peer (P2P) network [8]. In this attack Victim peers are changed by an attacker which is separated from public network.

2.8.4 Time jacking Attack [4]: Time jacking attack may divide the network into various parts. In this attack generally network time of a node is changed by an adversary. It is occurred by connecting more peers and telecasting illegal timestamp network [12]. This attack effects on network by developing counterfeit peers, increasing speed of other peers and separating the victim node from the network [13].

2.8.5 Finney Attack [11]: Finney attack occurs if vendor confirms the transaction only once. Suppose, a transaction T1 complete with a bitcoin set B1 for vendor V1 where blockchain fork is BF1. Now an immoral client C1premines a block BL1 having same bitcoin set B1 to make another transaction T2. Here the network is not informed about the mined block. BL1 creates a blockchain fork BF2 of the same length as BF1. BF2 will be extended if a new mined block come and BF2 will be the longest fork in blockchain. As the blockchain ignore shorter fork so BF1 will be ignored and transaction T1 will be invalid. By this process client C1 will get back his currency, but the vendor will lose his product [15].

2.8.6 DAO Attack: The DAO stand for "Decentralized Autonomous organization’’ [16]. A smart contract 'The DAO' took place in Ethersam on 28thmay of 2016. Christoph Jentzsch developed the DAO project source code and released it in GitHub [17]. The DAO contract attacked in Ethereum on 17th may 2016 through this attack, attacker stole US $60 million.

2.8.7 Brute- Force Attack [14]: A brute-force attack is used to collect secret information [18]. Some nodes, which are under control of an adversary in the network, they mine blocks. Suppose, a vendor sends a product after a confirmation, but the immoral client mines the fork number of the block that is used in this transaction and use the block in the network again for another transaction. Thus the new fork length will be the largest and network will ignore the previous fork. Thus the immoral client will get his currency back and the product both [14]. This attack also known as brute force cracking or simply brute force [19]. J. Cho, S. Yeo, S. Kim proposed a hash based protocol that secure against brute force attack named as "RFID system" [20].

2.8.8 Sybil Attack [21]: In Sybil attack, the attacker makes many pseudonymous identities in peer to peer network by hijacking an insecure computer. Here, an attacker presents these identities in distinct node. Thus he makes the user separated from the network and unable the transaction by making an inconsistent level of control over the network. In 2014, Sybil attack occurred against “Tor anonymity network’’ where the adversary was unknown [22].

2.8.9 Targeted DDOS Attack [4]: Targeted DDOS attack relates to overflowing the network with more info in a procedure it develops an insensible exploit. A different mechanism is contained in the modern concept to secure against attacks on elasticity and utility. We may refer to secure consumer inconsistent to the number of signing check, restriction structure of obstructing, minor deal forbidding, inexperience of not usual deal [25].

2.8.10 Nothing at Stake Attack [26]: Debut of proof of stake, a big element of the crypto group was hesitant that is just a liability for sign and plenty of obstacle misconduct manner [23]. Verifiers create a contrasting clog on entire feasible crochs with nothing at stake, so that expand advantages [27]. That is generally referencing by nothing at stake problem. This problem effects on slacks off the concurrency time in the system and decrease capacity of the network [26].

2.8.11 The Long Range Attack [26]: In Long range attack, the history of blockchain is modified by a fork which is already exists in a current block. Suppose, a client doesn’t have any stake in the blockchain network currently but had a huge stake at previous block height. This immoral client can generate a block by creating a fork again by using the previous block’s private key. So the account that has no stake in blockchain is not strongly protected and it can be attacked easily. A possible countermeasure is using checkpoints where it checks the block if it is finalized and would not accept a fork that is changed recently which was not exist in previous 720 blocks [28].

2.8.12 BGP Hijacking Attack [30]: Worldwide internet network able to relate to host. Every internet protocol bears its own identity to communicate each other. A router is able to transfer information to another. In the worldwide stage unique internet protocol address is associated by adjunct. These adjuncts created by an autonomous system and maintain by BGP. BGP stands for Border Gateway Protocol [30]. It is a defector protocol, which maintains the reaching system of IP packet to their target by which attacker interrupt the network. As an effect it makes delay of network messages, crack the network, making slow of block propagates, steal crypto currency. Distribution of mining power (high centralized) controls the successfulness of BGP hijacking. There are two types of attack:

A. Node level attack
B. Network level attack [31].

In 2014, attackers collect US$83000 of crypto currency [32]. The countermeasure only operates the network system like BGP Mon [33]. As it is consisted of modification of configuration which is monitored by a human so it takes a long time to be solved.

2.8.13 Bribery Attack [35]: Bribery attack is an unequivocal attack. In bribery attack, an attacker can get a huge benefit by investing a little constant, thus this attack is undoubtedly profitable. Here, an attacker acquires mining power for a short duration where they are only concern about regulates superiority. Suppose an immoral client make a transaction T1 with bitcoin set BT1 in block B1 where the cost is C1. This client then makes another transaction T2 in block B2 and tariff scope to make B2 as largest block. In the meantime, this immoral client double spends the stock in T1 and makes benefit as same cost as T1. Thus the attacker makes benefit with the abundance of currency.

2.8.14 Block withholding Attack [36]: In generally Block withholding attack formed a block mining by few pool components but they don't express any blocks. This way they reduce the predicting pool benefit. In another way these attacks called 'sabotage' attack and don't acquire pool mining where everything is not for good. But they declare acquire few benefits from attack.

2.8.15 Selfish Mining Attack [14]: There are two types of miner [37]:

(a) The immoral group who follows selfish mining strategy
(b) The honest group who follows pure mining strategy

By selfish mining, the attacker gets more revenue as he would get for his spending mining power, where he hides information by keeping mined blocks private while honest miners keep their block public. The selfish miners use their mining strategy for two types of motive [14]:

(a) Getting illegal reward
(b) Get honest miner to waste their capital

Suppose, in the network an immoral miner's fork is F1 in block and honest miner's fork is F2. If F1 lead for a long time, the selfish miner would get a reward and if F2 achieve the length as same as F1, the selfish miner publishes their mined block again. As a result, this immoral miner achieves a rivaling advantage and honest miners would lose their capital from the chain which is maintained by a selfish miner.

A possible countermeasure would be propagated branches as long as a miner gets information about competing block [38]. He would choose a block randomly and if he gets two block of same length, he would divide the nodes on two of them. This will reduce the control of selfish miners group.

2.8.16 Balance Attack [39]: The Balance attack proves that proof-of-work system is constant. In Balance attack, it defines which miners are in the same groups who have same mining strength. It is not concerned about its own block, but it makes slow the other block, delay sending information and rattle the communication. The adversary distinguishes the subgroup and makes the transaction. The transaction is devoted but the attacker can edit the block which is in a current transaction and the do this by altering the subtree which was holding that transaction. Once the vendor trucked the product, the adversary starts to delay message. In the meantime, the attacker makes another transaction to buy new products from another vendor as long as the previous vendor figure out the transaction is altered by another subtree. Balance attack rattles the consistency of network and lets the attacker do a double spend.

2.8.17 Malleability Attack [38]: Malleability is the mostly resource of the normal cryptographic system. It alters information, suppose a bank uses a cipher text monetary data. One client sent an encrypted message "Transfer $200. 00 to account #201'' if any attacker alters the message on the network and estimate the encrypted data type, then he will be capable to convert the amount or the account number of the transaction, e.g. '' $20000.00 to account #222''. This attack does not define the attacker's capability of data encryption [40]. Bitcoin system use digital signatures to demonstrate the possessor ship of bitcoin. But this signatures are not collateral as long as they are not a transaction for this vulnerability, an attacker gets a chance to make malleability attack by rattling the transaction, alter the digital signature and transmit the transaction again. By this attack the client will get the information like his transaction has been canceled. Here, two transactions are occurred, at first, one transaction is conducted to purchase the product and the second one is to get back the currency to him. It will be successful if both transactions are proved. Possible countermeasures for this attack is time stamping [38] and confirm only one transaction that comes first.

2.8.18 DDOS Attack [14]: DDOS attack is a criminal undertaking interrupt freight in an indicate server. It's a dauntless indicate by the network or that is a contiguous structure with lots of internet freight. This attack acquires capability exploit more accommodate in computing system from authority of attack freight. Mostly DDOS attack as like a defender who block striker in the game, counter the defender and reach at its target. The researcher provides a game theory for research DDOS attack. The game estimates that pool contest between each other the main reason is the biggest pool weightier than little pools [60]. Game lie in the pools and they struggle to raise their competition charge from others, and that's the way they established DDOS attack on the other pools. That's the way to draw a geometric situation between the gamer and finish that bigger pools incitement little pools.

Chapter 3

Methodology

We have collected our data regarding blockchain, its attacks, vulnerability and try to find their solution. To collect information about blockchain attacks we reads total 58 journal and conference papers that have been published from 2010 to 2018. From these 58 papers we use 41 papers as a reference. Besides this, we went through different blogs, online website to gather information about attack date, losses due to that attacks.

When we have finished our data collection in our survey period, we found that, there is a possible solution for double spending attack. Though that countermeasure is being implemented but still double spending attack occurred in 2018. So, we give a possible solution model according to the double spending attack mechanism. There are five stage that represents how a double spends occur.

Stage 3.1: Block adding process

At first user sign off and request for transaction through their user wallet. This unconfirmed transaction take place in a pool of unconfirmed transaction from where the miner picks transactions and solve complicated mathematical problem through Pow consensus to get hash output as unique one and broadcast them to add the block to blockchain. If other miners verify this hashes only then the block being added [80].

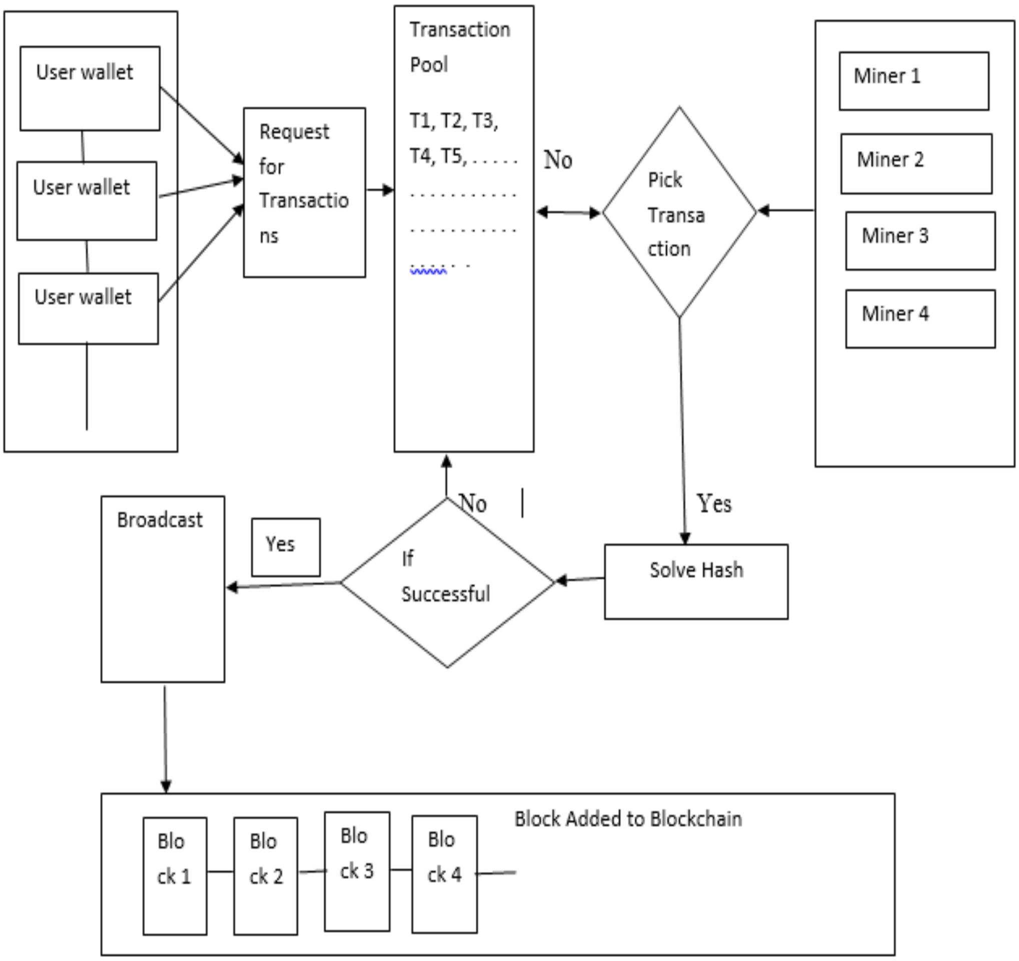

Figure 3.1: Process of mining and adding block to blockchain

Stage 3.2: As long as the good miners verify the block and the block is being added to the real blockchain, on that time the corrupted miner starts his own chain with the verified block. This time corrupted miner spends all his currency and sends this information to the real blockchain but not to his own isolated chain [81].

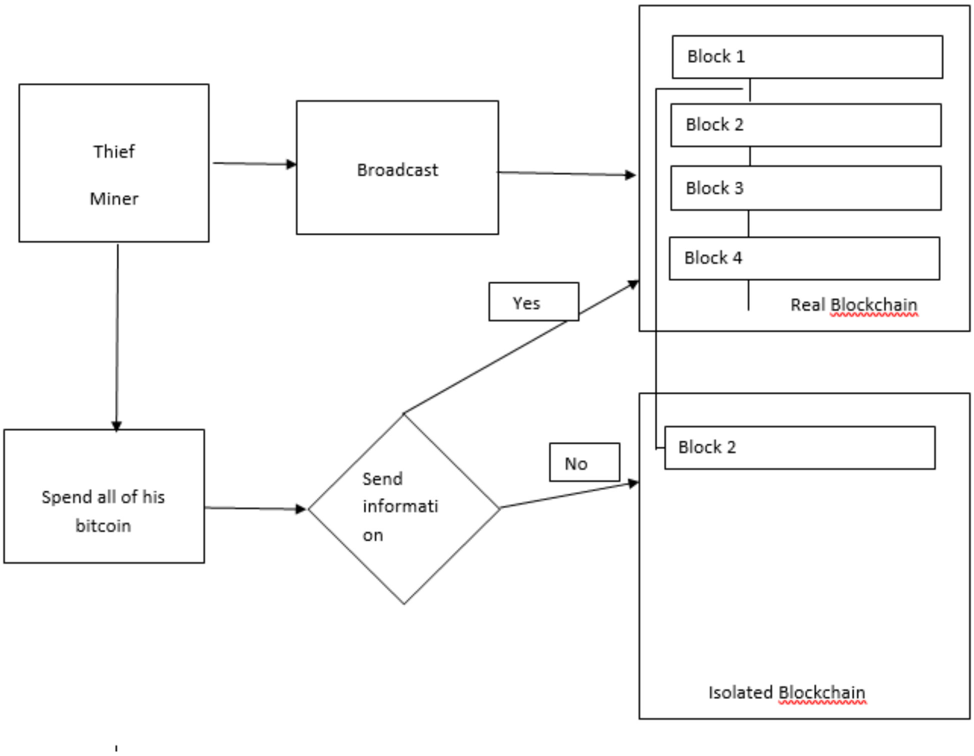

Figure 3.2: Corrupted miner own his personal chain and sends all his currency without informing to his isolated chain

Stage 3.3: In this stage the corrupted miner picks transactions and add block to his isolated chain by verifying them by himself with strong computational power faster than the good miners add block to the real blockchain [81].

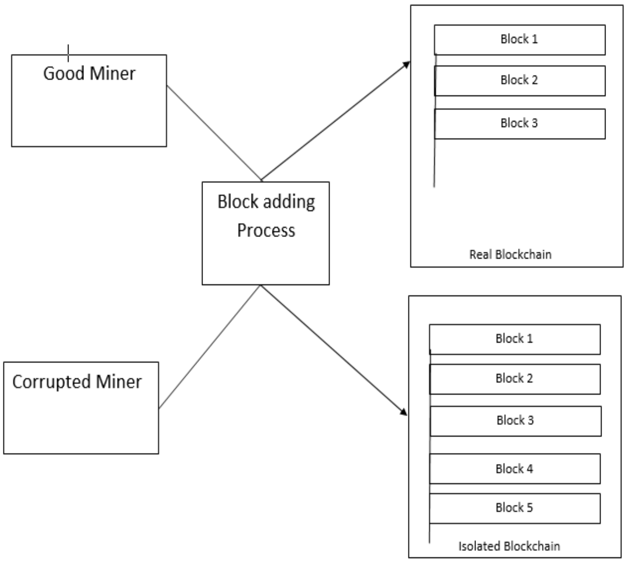

Figure 3.3: Corrupted miner adds blocks to his own chain

Stage 3.4: The corrupted miner broadcast isolated blockchain's transaction to the real blockchain when isolated chain is larger than the real one and the miner of real chain try to add their block to the isolated one [81].

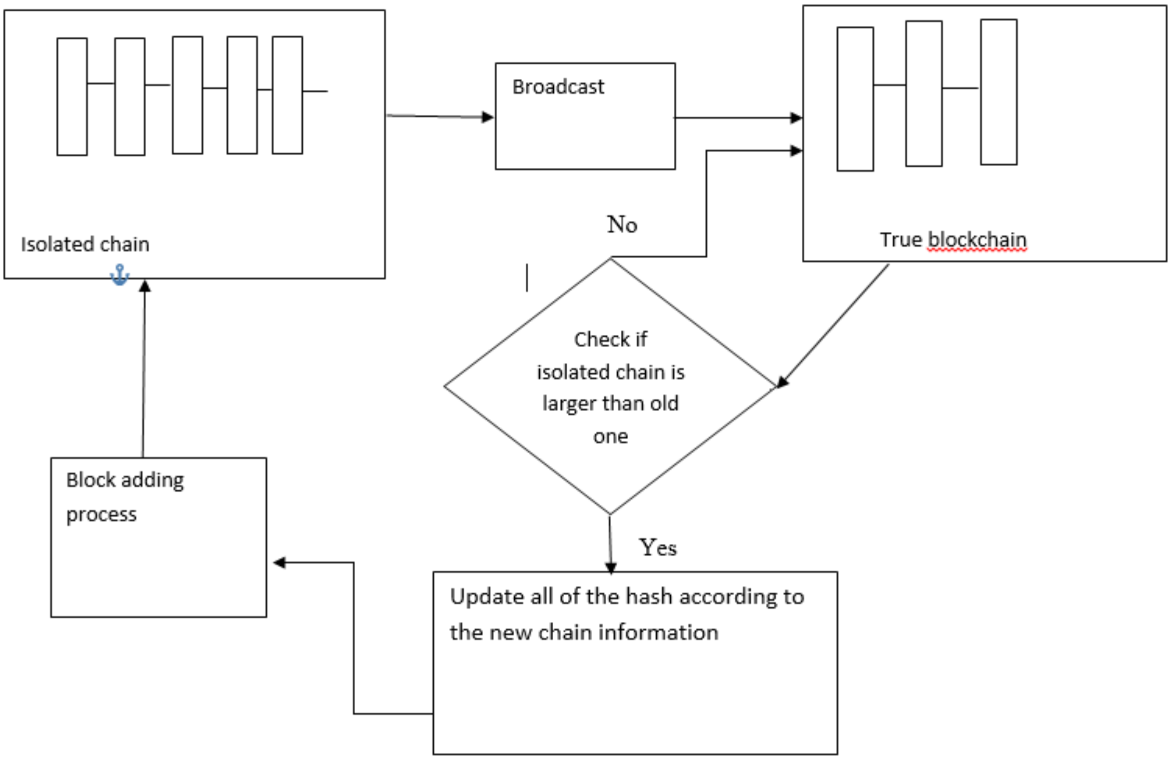
Isolated chain
Broadcast
True blockchain
No
Check if isolated chain is larger than old one
Yes
Block adding process
Update all of the hash according to the new chain information

Figure 3.4: Good miners add their block to the isolated chain

Stage 3.5: The democratic governace rule states that the blocks will add to the larger one by reemoving the previous records that they have. As the real blockchain's block had the information about thetransaction where the corrupted miner spent his currency but the isolated one don't know about the transaction. So, when the blocks try to add the isolated chain then they would remove the previous transaction informatin. So, in the new isolated chain, the corrupted miner would be able to spend all of the currencies that he had spent once in the real blockchain [81].

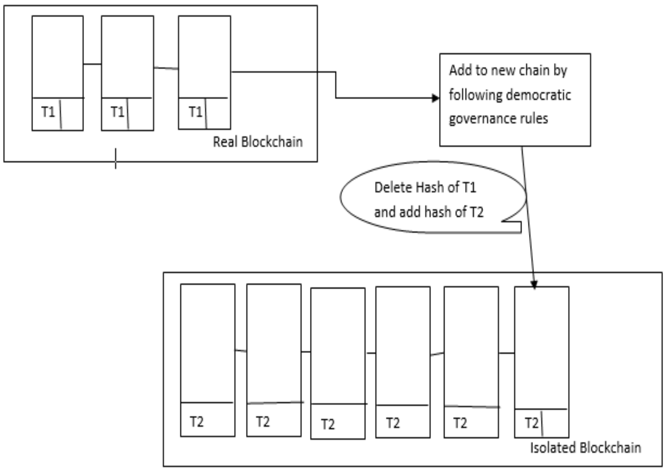
T1
T1
T1
Real Blockchain
Add to new chain by following democratic governance rules
Delete Hash of T1 and add hash of T2
T2
T2
T2
T2
T2
T2
Isolated Blockchain

Figure 3.5: How data is being changed by following the democratic governance protocol

Chapter 4

Result and Discussion

We have found 15 different attacks during this survey from where 4 attacks are "POW consensus based". These 4 attacks are double spending attack, finney attack, brute force attack and block withholding attack. Five attacks of these attacks targets on network, three are on blocking protocol and the others are on computing power as well as database. We also listed down their effects and possible countermeasures that we found on different papers.

Table 4.1: Attack name, their targeted area of attack, effect for the attack and possible countermeasures that we collected from different paper during our survey

NO.	ATTACK NAME	TARGETTED AREA	EFFECT FOR ATTACK	POSSIBLE COUNTERMEASURES
1.	Eclipse Attack	Network[41]	inconsistent view of the network and blockchain [41]	Use whitelists, disabling incoming connections[42]
2.	Spam Attack	Network[4]	Slow transaction, network and computing Power[4]	permanent nominal transaction fee [61]
3.	DDOS Attack	Network[4]	Generates huge unnecessary responses about transaction[4]	Proof-of-Activity (PoA) protocol[41]
4.	Time Hijacking Attack	Network[46]	Fake peers[46]	constraint tolerance ranges, network time protocol (NTP) or time sampling on the values received from trusted peers [47]
5.	Sybil Attack	Network[48]	Pseudonymous identities, threatens user privacy[44]	Xim (a two-party mixing protocol)[49]
6.	Nothing at Stake Attack	Block[26]	Slow consensus time[26]	Slasher Protocol [78]
7.	Pool Mining Attack	Block, Computing Power[50]	Slow verification time, fake transaction[50]	Not Found
8.	Selfish Mining	Block, Computing	Increase personal share on	Address bitcoin protocol and raise threshold,

	Attack	power[30]	transaction [30]	computing branches are same length and propagate all of them, Zero Block technique[37]
9.	DAO Attack	Computing Power[16]	Fake transaction[16]	Hard fork proposal, Soft fork proposal [45]
10.	Brute Force Attack	Computing Power, Pow Consensus [51]	Data encryption [52]	inserting observers in the network, notify the merchant about an ongoing double spend[53]
11.	Long Range Attack	Database[26]	Alter transaction history[26]	Nodes trust identity provider, implementation of trusted hardware[26]
12.	BGP Hijacking	Database, Protocol[30]	Fake transaction[30]	Human driven process consisting of altering configuration or disconnecting the attacker.[26]
13.	Refund Attack	Payment protocol[54]	Lose money, reputation[30]	publicly verifiable evidence[54]
14.	Wallet Attack	Private key[55]	Lose of bitcoin[55]	threshold signature based two-factor security, hardware wallets [56], Password-Protected Secret Sharing (PPSS)[57]
15.	Double Spending Attack	Bitcoin transaction, Pow Consensus [10]	lose products, create forks[10]	Recipient oriented transaction[10]

From these above 15 attacks, we found only seven attacks that occurred in several time. We listed down these attack name, their occurring date and the losses of the companies due to these attack. We also give a visual represent in figure 4.1 that shows that in which year the network being attacked frequently and from the chart we can get an easy overview of the attacks being occurred.

Table 4.2: Attack date and their losses during the according attack

No	Attack Name	Attack Date	Currency loss due to attack
1.	Wallet Attack	2013[59], 2016[62]	US $70 million [62]
2.	Double Spending Attack	March 2013 [63], 2018[3]	Rapidly drop off bitcoin prices[63], US $175 million [64]
3.	BGP Hijacking	2014[65]	US $83000 [65]
4.	Spam Attack	2015 [66] to 2017 [67], 2018 [68]	Effect on 80000 transactions [66]
5.	Dao Attack	28th may 2016[16]	US $60 million
6.	DDOS Attack	16 times in 2016 [69] 2017 [70]	Staminus network down for 20 hours, peaking at over 650 Gbps [69] US $123000[70]
7.	Selfish Mining Attack	May 2018 [58]	US $90,000 [58]

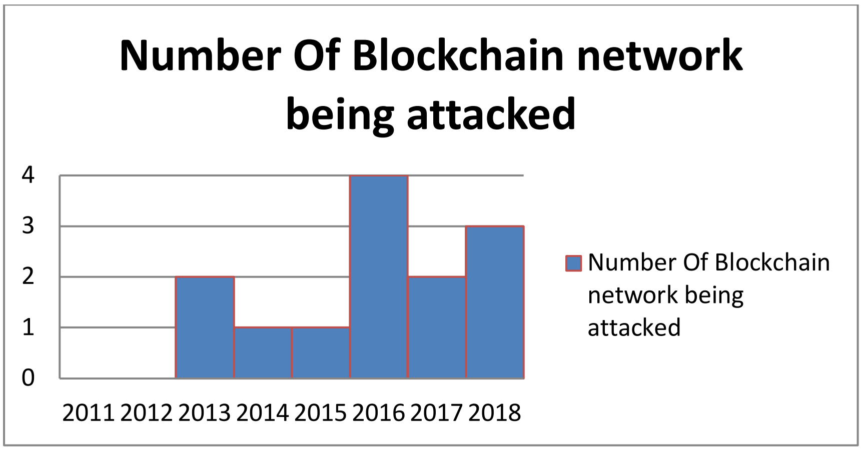

Figure 4.1: Number of blockchain network being attacked yearly from 2011 to 2018

Instead of the attacks that occurred in several time, the bitcoin currency based blockchain network had being hacked and bitcoin being stolen in various time. We also try to find out and listed down these stolen amount, and the network that was being hacked by the hacker with a wish of steal bitcoin. The entries total up to 818,485.77 stolen Bitcoins, presently worth some $502,081,166.11. [76]

Table 4.3: Attacker hacked the network and stole bitcoin in various time in blockchain history. This table represent the stolen amount with date and hacked network name.

Date	**Stolen amount**	**Blockchain network**
June 2011	16,120 bitcoins worth $500,000	Allinvain[71]
August 2011	Wallet service was disappeared	Mybitcoin[71]
March 2012	46,703 bitcoin	Linode user[71]
May 2012	18,000 bitcoin	Bitcoinica[71]
September 2012	24,000 bitcoin	Bitfloor[71]
2013	1000 bitcoins worth $100,000	WIRED [72]
February 2014	850,000 bitcoins	collapse of Mt. Gox[71]
March 2014	100,000 bitcoins	Poloniex [73]
January 2015	19,000 bitcoins	Bitstamp[71]
August 2016	102,666 bitcoins worth $77 million	Bitfinex[71]
2017	240,000 bitcoins worth $1.2 billion [75]	
First half of 2018	174,603 bitcoins worth $1.1 billion [74]	
September 2018	5966 bitcoins	Japan based cryptocurrency exchange [77]

We make two visual representations according to table 4.3 where figure 4.2 gives an overview of the stolen amount of bitcoin that is hacked by the adviser and figure 4.3 presents the overview of bitcoin currency based blockchain had being attacked with an aim to steal bitcoin.

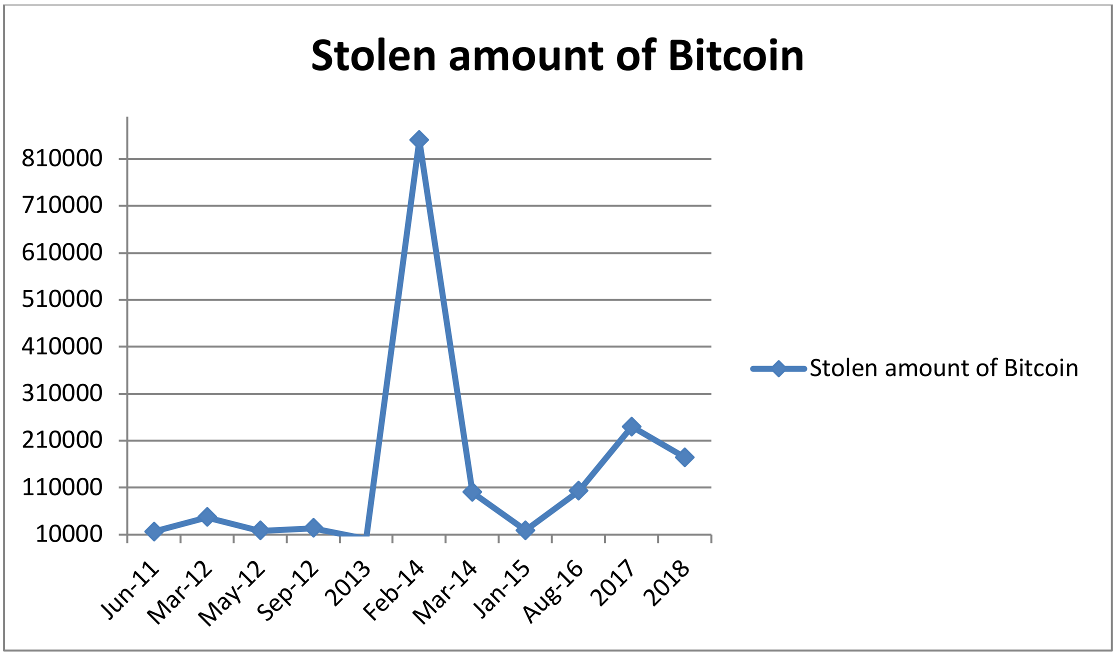

Figure 4.2: visual representation of stolen amount of bitcoin in various time

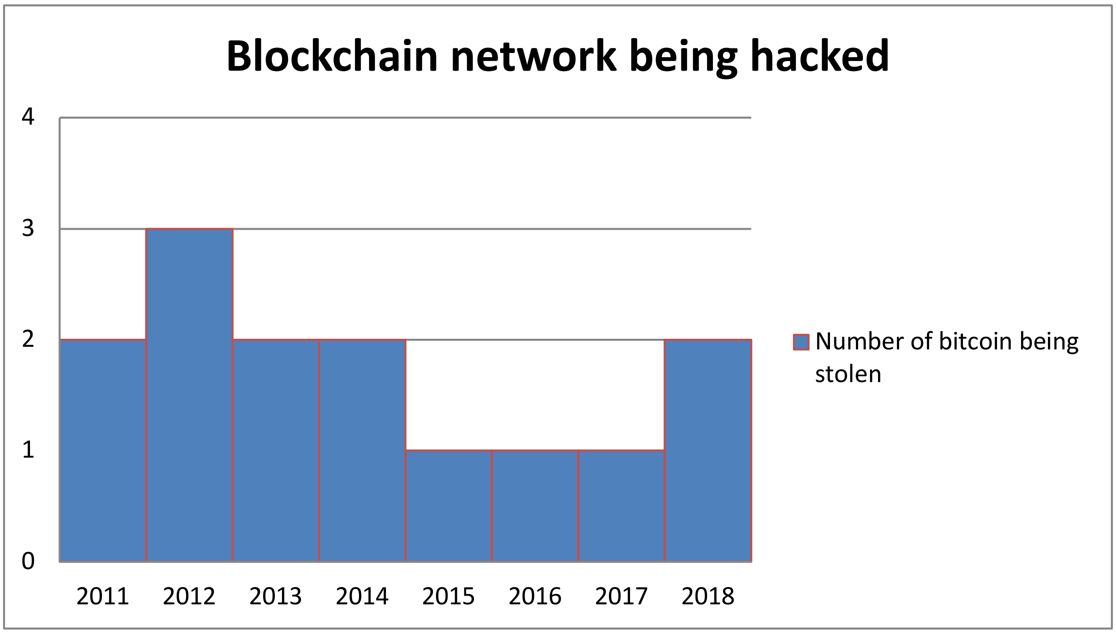

Fig 4.3: Number of blockchain network being hacked to steal bitcoins from 2011 to 2018

Our Proposed Model

As we state before, double spending problem starts in stage (3.2), when the corrupted miner starts his own chain with the verified block and the starts to make his chain larger than the real blockchain with his strong computational power.

Suppose, corrupted miner M1 spends all his bitcoins B1 to purchase a product from vendor V1. This corrupted miner adds this transaction to his block and spread the information to the real blockchain and other miners of the real blockchain verified this transaction, but this corrupted miner does not add the transaction T1 to his own isolated chain. As a result, the owner of the block in isolated chain do not know about the transaction T1.

When the corrupted miner would be able to make his chain larger than to the real chain, on that time he would spread information about a transaction to the real blockchain that is existat in the isolated one. When the miner would going to verify the transaction, then miner found that the isolated chain is larger.

As democratic governance protocol rules the larger chain will be define as real and miner from the smallest one would like to add in the larger one by removing their previous record and update the information according to the new chain.

That means, as the block in isolated chain do not have the information about transaction T1, but real blockchain blocks have, so when the old block add to the new chain, that time they would remove the information about transaction T1. That how, the corrupted miner would be able to spend the bitcoin B1 that has already been spent [82]. But in the new chain no one has that information.

To solve the problem we give a solution which states that when the block tries to add the new chain, on that time it will not remove its previous memory, it will update its information with keeping the previous one.

By following our proposed rule, whenever a block from smaller chain would add to the isolated chain, who has the hash of transaction T1, it will update its transaction information with keeping previous one. That means if isolated one has the transaction information T2, T3, when block A would add to isolated chain who has the information T1, after being added it would have the information about T1, T2 and T3 and beside it will also spread the information of T1 to the new chain. Thus, if one transaction that have ever been occurred, will be recorded permanently and all of the blocks of chain would have the information about all transaction.

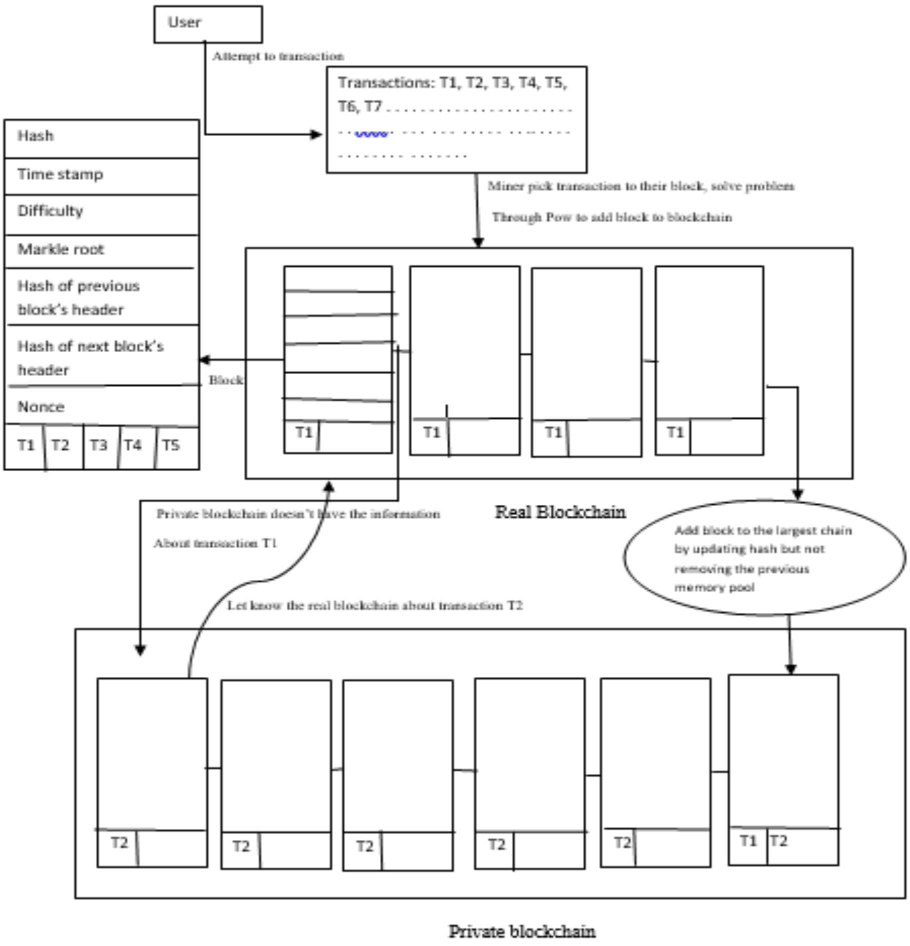
User
Attempt to transaction
Transactions: T1, T2, T3, T4, T5, T6, T7
Hash
Time stamp
Difficulty
Markle root
Hash of previous block's header
Hash of next block's header
Nonce
T1
T2
T3
T4
T5
Block
Miner pick transaction to their block, solve problem
Through Pow to add block to blockchain
T1
T1
T1
T1
Private blockchain doesn't have the information
About transaction T1
Real Blockchain
Add block to the largest chain by updating hash but not removing the previous memory pool
Let know the real blockchain about transaction T2
T2
T2
T2
T2
T2
T1
T2
Private blockchain

Figure 4.4: Proposed model to overcome the double spending problem

After recording all the transaction in any new chain come, we also proposing that all the vendor should have a broadcast history of transactions which would never be altered. So, whenever a user takes an attempt to make a transaction from any vendor, he will generate a onetime public key by using vendor public key. When the vendor will receive the transaction attempt, he will be in a waiting time period where vendor will check the broadcast history and decrypt user's public key. If the decrypted public key is as the same of the user's key and the transaction data is not included in broadcast history, only then the vendor would send the product.

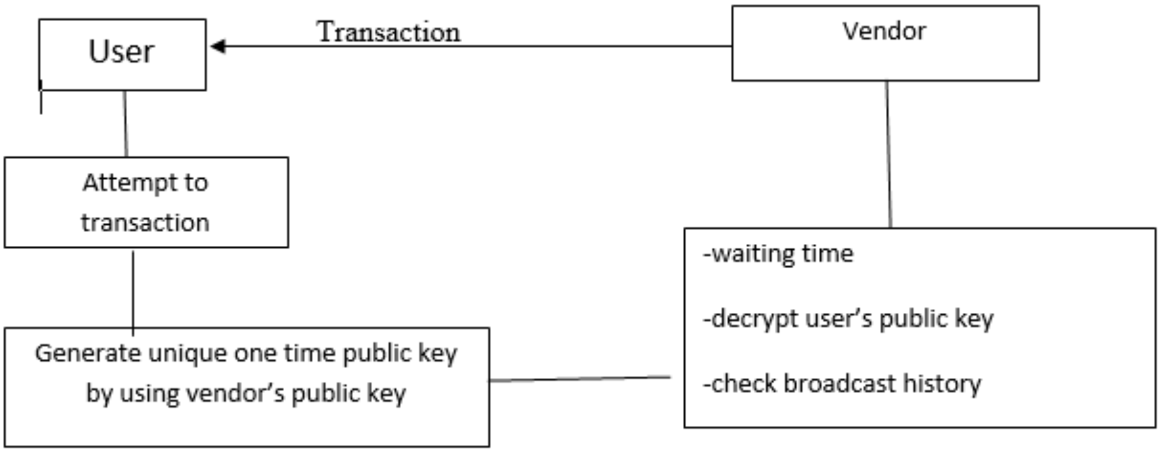
User
Transaction
Vendor
Attempt to transaction
-waiting time
-decrypt user's public key
-check broadcast history
Generate unique one time public key by using vendor's public key

Figure 4.5: Proposed model to overcome the vendor loss product due to double spending problem

Discussion

We interpret & discus about blockchain, bitcoin and ethereum attacks. Our main findings are given as follows:

(1) We found many attacks in several papers, online site, but they are distributed. We listed down the attacks, reasons and their solution in our paper as much as possible where 33% attacks target on network protocol, 26% on computing power mechanism and 20% on block history.

(2) We found total 18 attacks on which 21% attacks are targeted on POW based consensus, but the attacks occurred still now, 85% on them are on POW based consensus.

(3) Bitcoin stole rate was high at the first period of blockchain history (in year 2011-2014) and protocol targeted attack happened frequently in the recent year (2016 – 2018), even in 2016- 4 different type attacks happened and only DDOS attack hit 16 times on blockchain network.

(4) We give a proposed model where we show how double spending attack may be prevented with a simple changing in governance protocol.

CHAPTER 5

CONCLUTIONS AND RECOMENDATIONS

5.1 Conclusion

We make an exhaustive survey on blockchain, its attacks, their solutions and compile them future described before. We mainly concentrated on attacks, their effects and countermeasure. We analyze about the attack affected area and conducted area, also we analyze double spending attack and try to find out their limitation and provide a possible solution that may prevent double spending attack. We make a pattern of real attacks on blockchain. Finally, we set a finding that will motivate beginner researcher in this area.

5.2 Limitation and Future works

In this paper, according to our data set (Table 4.1) we found many blockchain attacks, but could not find a solution for all of the attacks like pool mining attack. We will further work with the mechanism of this attack in future to find out an algorithm that prevents such kind of crisis. Besides we proposed a solution model of double spending prevention, but we did not give any mathematical prove of this model. We will further work with this model.

REFERENCES

[1] D. K. Tosh, S. Shetty, X. Liang, C. Kamhoua, L. Njilla (2017). *Consensus Protocols for Blockchain-based Data Provenance: Challenges and Opportunities*. In: IEEE

[2] https://www.coindesk.com/ accessed on:10-09-2018

[3] https://en.wikipedia.org/wiki/2018_double-spend_attacks_on_Equihash-based_cryptocurrencies accesed on:11-09-2018

[4] J. Moubarak, E. Filiol, M. Chamoun(2018). *On Blockchain Security and Relevant Attacks.* In: IEEE.

[5] L. Parker (2017).*Bitcoin spam attack stressed network for at least 18 months, claims software developer.*

[6] https://steemit.com/cryptocurrency/@superfreek/btc-spam-attack-200-000-unconfirmed-transactions-halts-bitcoin. accessed on :12-09-2018

[7] K. Nakayama, Y. Moriyama, C. Oshima (2018). *An Algorithm that Prevents SPAM Attacks using Blockchain.* In:IJACSA.

[8] Deepak K. Toshi, S. Shetty, X. Liang, Charles A. Khamhua, Kevin A. Kwiat, L. Njilla(2016). *Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack*

[9] M. Rosenfeld (2012). *Analysis of hashrate-based double-spending.*

[10] H. Lee, M. shin, Kyeong S. Kim, Y. Kang, J. Kim (2018). *Recipient-Oriented Transaction for Preventing Double Spending Attacks in Private Blockchain.* In: IEEE.

[11] Y. Marcus, E. Heilman, S. Goldberg (2018). *Low-Resource Eclipse Attacks on Bitcoin's Peer-to-Peer Network*. In: IEEE.

[12] corbixgwelt,"Timejacking and bitcoin," Available: http://culubas. blogspot.de/ 2011/ 05/timejacking-bitcoin 802.html, Mar. 2011.

[13] M. Apostolaki, A. Zohar, L. Vanbever(2017).*Hijacking bitcoin: routing attack on bitcoin.* In:IEEEXplore.

[14] M. Conti, S. Kumar, C. Lal, S. Ruj (2018). *A Survey on Security and Privacy Issues of Bitcoin.* In: IEEE.

[15] H. Finney, "Best practice for fast transaction acceptancehow high is the risk?" Available:https://bitcointalk.org/index.php?topic=3441.msg48384\#msg48384, 2011.

[16] X. Zhao, Z. Chen, X, Chen, Y. Wang, C. Tang(2017). *The DAO Attack Paradoxes in Propositional Logic.* In: ICSAI.

[17] "Slock.it," https://slock.it/accesed on : 01-11-2018

[18] https://medium.com/@UnibrightIO/blockchain-evolution-from-1-0-to-4-0-3fbdbccfc666 Accessed on 13-10-2018

[19] https://www.techopedia.com/definition/18091/brute-force-attack Accessed on: 02-11-2018

[20] J. Cho, S. Yeo, Sung K. Kim (2011). *Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value.* In:ELSEVIER.

[21] G. Bissias, A. Pinar Ozisik, Brian N. Levine, M. Liberatore(2014). *Sybil-Resistant Mixing for Bitcoin*. In: ACM.

[22] https://blog.torproject.org/tor-security-advisory-relay-early-traffic confirmation-attack accesed on: 14-10-2018

[23] https://medium.com/@BambouClub/best-and-worst-performing-currencies-in-2015d1e62088bc29?fbclid=IwAR0IR7KZWvdk7QeLIFzt7W_1tynjAqUaoOQ5zHJdxSoahjs3RNrJ-thqg accesed on : 14-10-2018

[24] https://qz.com/1169000/ripple-was-the-best-performing-cryptocurrency-of-2017-beatingbitcoin/?fbclid=IwAR1fLy9zKDL3XUtCC8H4fGLyjOUb3c1D0vi__zFqzsOuudY5n796zTAMbLY accesed on : 14-10-2018

[25] R. R. O'Leary, "Bitcoin gold website down following ddos attack," https://www.coindesk.com/ bitcoin-gold-website-following-massive-ddos-attack/, 2017.

[26] W. Li, S. Andreina, J. Bohli,G.Karame (2017). *Securing Proof-of-Stake Blockchain Protocols.* In: Springer

[27] https://medium.com/coinmonks/understanding-proof-of-stake-the-nothing-at-stake-theory-1f0d71bc027 accessed on: 15-09-2018

[28] https://blog.positive.com/rewriting-history-a-brief-introduction-to-long-range-attacks-54e473acdba9 accessed on: 15-09-2018

[29] https://arstechnica.com/tech-policy/2017/12/a-brief-history-of-bitcoin-hacks-andfrauds/?fbclid=IwAR0ATqnYcz53teqz8V8ljv4lJaGfVeD7mfHRvFvec8aI5eVlCp6LJP5de8w Accessed on: 14-08-2018

[30] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen(2017). *A survey on the security of blockchain systems.* In: ELSEVIER

[31] https://en.wikipedia.org/wiki/BGP_hijacking Accessed on: 17-09-2018

[32] M. Apostolaki, A. Zohar, L. Vanbever(2017) *Hijacking bitcoin: Routing attacks on cryptocurrencies*. In: IEEE

[33] D. SecureWorks(2014) BGP hijacking for cryptocurrency profit. URL: https://www.secureworks.com/research/bgp-hijacking-for-cryptocurrency-profit

[34] H. Yan, R. Oliveira, K. Burnett, D. Matthews, L. Zhang, D. Massey (2009). BGPmon: A real-time, scalable, extensible monitoring system, in: Cybersecurity Applications Technology Conference for Homeland Security.

[35] J. Bonnaeau (2016). *Why buy when you can rent? Bribery attacks on Bitcoin-style consensus*. In: Springer verlag

[36] Deepak K Toshi, S. Shetty, X. Liang, Charles A. Kamhoua, Kevin A. Kwiat, L. Njilla(2016). *Security Implications of Blockchain Cloud with Analysis of Block Withholding Attack.*

[37] I. Eyal, Emin G. Sirer(2018). *Majority is not enough:Bitcoin mining is vulnerable.* In: ACM.

[38] R. Kaushal(2016). *Bitcoin: Vulnerabilities and Attacks*. In: UIR.

[39] C. Natoli,V. Gramoli(2017). *The Balance Attack or Why ForkableBlockchains Are Ill-Suited for Consortium*. In: IEEE.

[40] https://en.wikipedia.org/wiki/Malleability_(cryptography) accessed on: 20-09-2018

[41] E. Heilman, AKendler, A. Zohar, S. Goldberg (2015). *Eclipse Attacks on Bitcoin's Peer-to-Peer Network*. In: USENIX

[42] Y. Marcus, E. Heilman, S. Goldberg (2018). *Low Resource Eclips Attacks on Ethereum Peer-to-Peer Network*. URL: https://eprint.iacr.org/2018/236.pdf

[43] https://bravenewcoin.com/insights/bitcoin, Accesed on: 25-09-2018

[44] https://coincentral.com/sybil-attack-blockchain Accessed on: 25-09-2018

[45] https://coincentral.com/sybil-attack-blockchain/ accessed on: 27-09-2018

[46] M. Apostolaki, A. Zohar, L. Vanbever- *Hijacking Bitcoin: Routing Attacks on Cryptocurrencies*

[47] D. Mills, J.Martin, J. Burbank and W. kasch(2010), *Network time protocol version 4: protocol and algorithms specification.* In: IETF

[48] en.m.wikipedia.org/wiki/Sybil_attack. Accesed on: 26-09-2018

[49] G. Bissias, A. P. Ozisik, B. N. Levine, M. Liberatore (2014). *Sybilresistant mixing for bitcoin,*. In: ACM

[50] Y.Velner, J. Teutsch, L. Luu (2017). *Smart Contracts Make Bitcoin Mining pools Vulnerable.* In: IFCA

[51] www.cloudways.com/blog/ accessed on: 28-09-2018

[52] J. S. Cho, S.S. Yeo , S. Kim (2011). *Securing against brute-force attack: A hash-based RFID mutual authentication protocol using a secret value.* In: ELSEVIER

[53] T. Bamert, C. Decker, L. Elsen, R. Wattenhofer,S.Welten (2013). *Have a snack, pay with bitcoins*. In: IEEE

[54] P. McCorry, S. F. Shahandashti, F. Hao(2017). *Refund Attacks on Bitcoin's Payment Protocol*. In: IFCA

[55] R.Latifa , K. Ahmed, G. Mohammad. *Blockchain: Bitcoin wallet cryptography security, challenges and countermeasures.*

[56] T. Bamert, C. Decker, R. Wattenhofer,S.Welten (2014). *Bluewallet: The secure bitcoin wallet.* In: STM

[57] S. Jarecki, A. Kiayias, H. Krawczyk, J. Xu (2016*). Highly-efficient and composable password-protected secret sharing*. In: IEEE

[58] https://www.ccn.com/japanese-cryptocurrency-monacoin-hit-by-selfish-mining-attack/ Accessed on: 04-11-2018

[59] A. Gkaniatsou, M. Arapinis, A. Kiayias(2017). *Low-Level Attacks in Bitcoin Wallets*. In: Springer

[60] https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/accesed on : 05-10-2018

[61] https://en.bitcoin.it/wiki/July_2015_flood_attack accessed on: 03-10-2018

[62] K. Karagiannis(2017). *Hacking Blockchain*. In: RSA.

[63] https://blogs.cornell.edu/info4220/2013/03/29/bitcoin-and-the-double-spending-problem/ Accessed on: 05-11-2018.

[64] G.O.Karame, E. Androulaki, S. Capkun(2012).*Double-spending fast payments in bitcoin*. In: ACM

[65] https://bgpmon.net/bgp-routing-incidents-in-2014-malicious-or-not/ accessed on : 12-07-2018

[66] https://en.bitcoin.it/wiki/July_2015_flood_attack accessed on : 12-07-2018

[67] https://bravenewcoin.com/insights/bitcoin-spam-attack-stressed-network-for-at-least-18-months-claims-software-developer accessed on : 12-07-2018

[68] https://neonewstoday.com/general/neo-blockchain-experiences-transaction-spam-attack/ Accessed on: 12-07-2018

[69] https://www.linkedin.com/pulse/notorious-ddos-2016-highlights-12-months-16-massive-ashkenazi-1?fbclid=IwAR341LHDpu0moPV4FIfcq_31wb9qxHh3Pe-SmjxznYM_fhUBwiDtgA9qWmk accessed on: 13-07-2018

[70] https://lab.getapp.com/how-to-prevent-a-ddos-attack/ accessed on: 13-07-2018

[71] https://arstechnica.com/tech-policy/2017/12/a-brief-history-of-bitcoin-hacks-and-frauds/?fbclid=IwAR0ATqnYcz53teqz8V8ljv4lJaGfVeD7mfHRvFvec8aI5eVlCp6LJP5de8w accessed on: 14-11-2018

[72] https://www.wired.com/story/wired-lost-bitcoin/?fbclid=IwAR2RxU5jadm9yhawa_LVcoJEYz0F_BAD9It6G1ImrQC6dz68MpmNy-BZ-fA
Accessed on: 15-11-2018

[73] https://hacked.com/biggest-bitcoin-hacks-thefts-time/ accessed on: 14-11-2018

[74] https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html accessed on: 15-11-2018

[75] https://www.reuters.com/article/us-crypto-currency-crime-idUSKCN1IP2LU accessed on: 15-11-2018

[76] https://www.businessinsider.com.au/how-many-bitcoins-have-been-stolen-2014-3 accessed on: 15-11-2018

[77] https://www.coindesk.com/crypto-exchange-zaif-hacked-in-60-million-6000-bitcoin-theft accessed on: 16-11-2018

[78] https://hackernoon.com/protocol-evolution-and-the-future-of-blockchain-governance-24ffd53c052b accessed on: 20-11-2018

[79] J. Lluais De La Rosa, V. Torres-padrosa, D. Gibona, O. Hornyak(2017). *A Survey of blockchain technologies for open innovation*. In: Research Gate publication.

[80] https://medium.com/coinmonks/how-a-miner-adds-transactions-to-the-blockchain-in-seven-steps-856053271476?fbclid=IwAR1kTZJFLhreEBD4MBxszrQ1VgkevPYqAmHRdyDM5dKgP5ffBqc80qWbSxM accessed on: 21-11-2018

[81] https://medium.com/coinmonks/what-is-a-51-attack-or-double-spend-attack-aa108db63474 accessed on: 21-11-2018

[82] G. karame, E. Androulaki, S.capkun (2012). *Double spending fast payment in bitcoin.* In: ACM