IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)
e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 12, Issue 5 Ver. II (Sep-Oct. 2017), PP 87-93
www.iosrjournals.org

Bitcoin Approach: Its Challenges and Attacks

Anil Kumar Mishra[1], Rajanikanta sahu[2]
1(Department of Computer Science & Engineering, Gandhi Engineering College ,India)
2(Department of Computer Science & Engineering, Gandhi Institute For Technology ,India)

Abstract: *Bitcoin is the most successful crypto currency that has created a new division in the area of electronic financial transactions. Bitcoin provides a platform to run currency without any central control. It serves as both a peer-to-peer payment system as well as a store of value. Bitcoin records all its transactions in a distributed append-only public ledger called block chain. In this paper, we present a systematic survey that covers the security aspects of Bitcoin. The purpose of this paper is to explore some of these security issues associated with the Bitcoin as well as suggest countermeasures to keep its transactions secure.*

***Key Word**: Bitcoin, Block Chain, Miner, Security Threats.*

I. Introduction

Crypto currencies have made great development in recent years. Earlier forms of electronic currencies such as Digi Cash or Cyber Cash, transfer large amounts of money between parties at fast speeds while offering some level of anonymity. More recent innovations in virtual currency were made by Bitcoin which has taken the next step in characterizing the digital money. Bitcoin was launched soon after the financial crisis of 2007-2008 that had dented people's faith in central banking authorities. This could have been another driving force for Nakamoto to start with the decentralized monetary system. Other than the Bitcoin, there are many other forms of digital currencies called Altcoins, which have emerged in the last few years. Altcoins include LiteCoins, Doge Coin, Ripple, Name coin, Peer coin, DevCoin, Byte Coin and the list goes on. With steady growth in digital currency, a parallel economy is developing and it is time when the government should step in and put regulations into it. Putting regulations may help states to impose taxes and prevent black money to sustain in the system. Japan recognizes Bitcoin as a currency and has a positive viewpoint towards it. The major difference between Bitcoin and other digital currencies is that it is decentralized.

BITCOIN uses peer-to-peer (P2P) technology, and it operates without any trusted third party authority that may appear as a bank, a Chartered Accountant (CA), a notary, or any other centralized service [1].Since its deployment in 2009, Bitcoin has attracted a lot of attention from both academia and industry. With a market capitalization of about 150 billion and more than 150,000 aggregate number of confirmed transactions per day (as of April 2018)

Nakamoto described Bitcoin as providing "a system for electronic transactions without relying on trust" through the use of cryptographic proof [1]. The purpose of Bitcoin is to create a currency through public ledger without the need of the third party and to establish a trust through peer to peer collaboration. Pavel et al. [2] analyzed Bitcoin characteristics to make it a global currency, and identified that it has an insignificant market presence and price volatility that pulls it back when compared to fiat currency. Kleineberg et al. demonstrated how Bitcoin can sustain digital diversity through multidimensional incentive system [3].The open source code of Bitcoin made money transfers without a bank acting as a trusted third party possible for millions of users, and its distributed design gave Bitcoin the properties of permission less network with censorship-resistance. However, Bit-coin's design still struggles to ensure some measure of anonymity, despite the fact that most of its users believe it provides anonymous payments [4].

This paper provides a comprehensive overview of the potential security threats along with their impacts on various entities in Bitcoin and its possible solutions. In section II a brief overview of Bitcoin and its major constituents is given. In section III security challenges associated with its countermeasures are explained in brief. In section IV the challenges of Bitcoin is presented in brief and in the last section V concludes the paper.

II. Overview of Bitcoin Based System

Bitcoin is a decentralized crypto currency providing an open, self-regulating alternative to traditional currencies managed by central authorities such as banks and government. Bitcoin utilizes an innovative technology that permits customers to transfer currency online without relying on centralized trusted parties. The major constituents of a bit coin based system are discussed in brief.

2.1. Bitcoin and Block chain

The Bitcoin scheme is a digital payment method, i.e. it allows the transfer of values between the two parties. When someone makes a purchase or sale using Bitcoin, Bitcoin miners clumps the transactions together in "blocks" adding them to a public ledger called the "block chain". Block chain is an open database that keeps the record of all transactions made by Bitcoin. It is a new mechanism for data storage, transmission and management. The major advantage that block chain has brought to security is tamper-proofing, disaster recovery and privacy protection [5].

2.2. Bitcoin Transaction

Bitcoin transaction is an authorized transfer of Bitcoin between different accounts on a peer-to-peer basis. Each transaction consists of one or more inputs which represents the debit against a Bitcoin account. The transaction is recorded in a public accounting book, called the lock chain, by network participants. The transaction log is decentralized. There is a reward for registering trans-actions in the block chain and participants compete in the Bitcoin system to make disks. It is important to note that each participant keeps a copy of the master book and the consensus of the incremental changes ensures that these copies are same. BTC and XBT are the symbols used to represent the Bitcoin. The Bitcoin transaction process is quite complex and IT professionals are actively analyzing aspects of their security, privacy, distribution systems, and distributed incentives.

2.3. Mining

It is a process to secure and verify Bitcoin payments on a decentralized network. It is designed intentionally to be resource-intensive and difficult so that the number of blocks found each day by miners remains steady over time, producing a controlled finite monetary supply. The miners in Bitcoin get incentivized with two things: the block reward and the transaction fee. Each block stores a cryptographic hash of the previous block using SHA-256 algorithm. Each block must have a proof of work (PoW) which is verified by other Bitcoin nodes when they receive a block.

2.4. Bitcoin Network

Technology experts often refer Bitcoin network as the Internet of Money. It is a peer-to-peer, decentralized cryptographic network which enables censorship resistant value transfer. It consists of tens of thousands of "nodes" and all transactions are broadcasted to the network, time-stamped and locked into 1 MB - 2 MB data blocks and chained together as an immutable record.

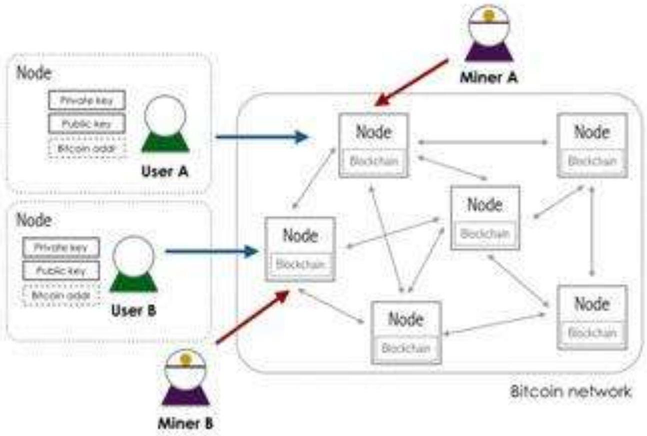

Figure 1: Bitcoin Network

2.5. Bitcoin Wallet

Bit coins are stored in online or offline wallets. Wallets are software that is used to keep a client’s Bit coins secure, and transact or share Bit coins. They come under two categories as full clients and lightweight clients. Wallet is considered as an application for maintaining digital credentials for one’s Bitcoin holding which are allowed to be accessed. Bit coins based transaction processing system uses public key cryptography and a wallet is assumed to store one of the public/private keys for least.

III. Security in BitCoin

Bitcoin is a decentralized models with an uncontrollable environment, hackers and thieves find crypto currency system an easy way to fraud the transactions. Research into the security flaws of Bitcoin itself is still in its infancy due to Bitcoin being a relatively new feature of the digital world. Bradbury [6] talks about the risks Bitcoin faces from cyber-criminals and correctly points out that because it is an entirely online product it will always are at risk one way or another. In this section, a detailed discussion on security threats, potential vulnerabilities that can be found in the Bitcoin protocols as well as in the Bitcoin network is provided. This will be done by taking a close look at the broad attack vector and their impact on the particular components in the Bitcoin system.

3.1. Double Spending

Double spending is the most commonly used bit coin exploit. It refers to using the same bit-coin twice effectively doubling the bit coins a person has. A client in the Bitcoin network achieves a double spend (i.e., send two conflicting transactions in rapid succession) if she can simultaneously spend the same set of bit coins in two different transactions [2]. In this section we will discuss the variants of double spending attacks.

3.1.1. Race Attack

Here the attacker does a direct transaction with the merchant and with himself, which in effect leads to the same coin being reversed from the vendor; a vendor can prevent it by stopping a transaction if "0/un-confirmed" is shown on the screen.

3.1.2. Finney Attack

This is another attack when “0/unconfirmed" appears on the screen. The bottom line is that an attacker controls a certain amount of network hashes. It works when an attacker sends a transaction to him-self without broadcasting it, and then uses the coins for a service, it is then broadcasted after the service is confirmed, and the transacted coins are returned to the sender.

Counter Measure

- To avoid the Finney attack, the vendor should wait for multiple confirmations before releasing the product to the client. The waiting for multiple confirmations will only make the double spend for the attacker harder, but the possibilities of the double spend remains.

3.1.3. Brute Force Attack

It is an advancement of the Finney attack. In this attack resourceful attacker has control over n nodes in the network, and these nodes collectively work on a private mining scheme with the motive of double spend.

Counter Measure

- Inserting observers in the network
- Notify the merchant about an ongoing double spend

3.1.4. Vector 76

Vector attack uses the privately mined block to perform a new form of double spending attack on Bitcoin exchange networks Also referred to as a one-confirmation attack, is a combination of the race attack and the Finney attack such that a transaction that even has one confirmation can still be reversed. The primary target of vector76 attack is Bitcoin exchange services. A Bitcoin exchange is a digital marketplace where traders can buy, sell or exchange bit coins for other assets, such as fiat currencies or alt coins.

Counter Measure for multi-confirmations for transactions

3.1.5. Balance Attack

Recently, an author in [3] proposes a new attack against the PoW-based consensus mechanism called the Balance attack. The attack consists of delaying network communications between multiple subgroups of miners with balanced hash power.

3.1.6. >50% Attack or Gold finger Attack

In this attack more than 50% computing resources of the network are under the control of a single miner (or mining pool). The > 50% attack is considered the worst-case scenario in the Bitcoin network because it has the power to destroy the stability of the whole network by introducing the actions such as claim all the block intensives, perform double spending, reject or include transactions as preferred, and play with the Bitcoin exchange rates. The instability in the network once started, it will further strengths the attacker’s position as more and more honest miners will start leaving the network.

Counter Measure

- Inserting observers in the network

- Communicating double spending alerts among peers
- Disincentives large mining pools

From the above discussion on the different type of double spending attacks, we can conclude that It is necessary to set a lower bound on the number of double spend Bit coins, and this number should compensate the risk of unsuccessful attempts of double spend. Additionally, the double spends could be recognized with the careful analysis and traversing of the block chain. Authors in [8] evaluate three techniques that can be used to detect possible double spending in fast payment systems. The three techniques are as follow: listening period, inserting observers, and forwarding double spending attempts.

3.2. Mining Pool Attack

Mining pools are created to increase the computing power which directly affects the verification time of a block. The miners generate partial proofs-of work (PPoWs) and full proofs-of-work (FPoWs), and submit them to the manager in shares. As most of the mining pools allow any miner to join them using a public Internet interface, such pools are susceptible to various security threats.

3.2.1. Selfish Mining/ Block discarding attack

In this attack, a group of colluding group of miners forces an honest group of miners to perform wasted computations on the stale public branch. In other word, the cycles of honest miners are spending on blocks that will not be the part of the block chain. The blocks of the selfish miners are kept private by them and they perform the bifurcation of the block chain secretly. The selfish miners then reveal the block to the public branch and honest miners switch to the recently mines blocks which make the selfish miner earn more revenue. The analysis in [9] shows that using the selfish mining, the pool's reward exceed its share of the network's mining power.

Counter Measure

- Zero Block technique
- Timestamp based techniques such as freshness preferred
- DECOR+ protocol

3.2.2. BWH – Block Withholding

This attack is much similar to the selfish mining that could be performed on a mining pool. In BWM attack, a pool member never publishes a mined block to sabotage the pool revenue, however, submit a share consists of PPoWs, but not FPoWs.

Counter Measure

- To include only known and trusted miners in pool, dissolve and close a pool when revenue drops from expected

- Cryptographic commitment schemes

3.2.3. FAW-Fork after Withholding

Authors in [10] propose a novel attack called a fork after withholding (FAW) attack. Authors show that the BWH attackers reward is the lower bound of the FAW attackers, and it is usable up to four times more often per pool than in BWH attack. Moreover, the extra reward for a FAW attack when operating on multiple mining pools is around 56% higher than BWH attack. More importantly, unlike selfish mining, a FAW attack is more practical to execute while using intentional forks.

Counter Measure

- No practical defense reported so far.

3.2.4. Pool Hopping

It uses the information about the number of submitted shares in the mining pool to perform the selfish mining. In this attack, the adversary performs continuous analysis of the number of shares submitted by fellow miners to the pool manager to discover a new block. The idea is that if already a large number of shares have been sent and no new block has been found so far, the adversary will be getting a tiny share from the reward because it will be distributed based on the shares submitted. Therefore, at some point in time, it might be more profitable for the adversary to switch to another pool or mine independently.

3.2.5. Bribery Attack

In this, an attacker might obtain the majority of computing resources for a short duration via bribery. There are 3 ways three ways to introduce bribery in the network: (i)Out-of-Band Payment, in which the adversary pays directly to the owner of the computing resources and these owners then mine blocks assigned by the adversary, (ii) Negative-Fee Mining Pool, in which the attacker forms a pool by paying higher return, and (iii) In-Band Payment via Forking, in which the attacker attempts to bribe through Bitcoin itself by creating a fork containing bribe money freely available to any miner adopting the fork.

Counter Measure

•To increase the rewards for honest miners, make aware the miners to the long-term losses of bribery.

3.2.6. Punitive and Feather Forking

The objective of punitive forking is to censor the Bitcoin addresses owned by certain people and prevent them from spending any of their Bit coins. The strategy is to perform the blacklist dishonest miners' transactions of specific address. Punitive forking doesn't work unless we have > 50% of hash rate. However, another strategy to achieve the blacklisting called feather forking.

Counter Measure

•It still remains an open challenge.

3.3. Wallet Thefts

It is performed using mechanisms that include system hacking, installation of buggy software, and incorrect usage of the wallet. A wallet attack is more easily done on an online wallet. The most common wallet software attack is a DDOS attack where the user is unable to access their bit coins and in turn may not be able to complete transactions. Inputs.io is an example of wallet attack. This attack was carried out on October 2013. It led to a loss of 4, 100 bit coins which at that time was estimated to be around $1.2 Million. This was a social engineering attack where the attacker was able reset the site's password.

Counter Measure

•The best way to prevent such an attack from taking place is having a wallet which is DDOS secure.

3.4. Bitcoin Network Attack

3.4.1. DDOS

It is the most common networking attack called Distributed Denial-of-Service (DDoS) which targets Bitcoin currency exchanges, mining pools, e Wallets, and other financial services in Bitcoin. Majority of DDoS attack targets the exchange services and large mining pools because a successful attack on these will earn massive revenue for the adversary as compared to attacking an individual or small mining pools.

Counter Measure

•Continuous monitoring of network traffic by using browsers like Tor or any user-defined web service.
•Configure the network in a way that malicious packets and requests from additional ports will be prohibited

3.4.2. Malleability Attack

Malleability attack also facilitates the DDoS attacks in Bitcoin. For instance, by using a Malleability attack an adversary clogs the transaction queue. This queue consists of all the pending transactions which are about to be serviced in the network. This attack wastes time and resources of the miners and the network.

3.4.3. Refund Attack

Refund attack performed by a malicious user due to the vulnerabilities that exist in the refund policies of the current Bitcoin payment protocol. There are two types of refund attacks called Silk Road Trader attack which highlights authentication vulnerability in the BIP70 payment protocol, and Marketplace Trader attack which exploits the refund policies of existing payment processors.

3.4.4. Time Jacking Attack

Time jacking is a dreaded attack that might split the network into multiple parts. Hence it can isolate the victim node.

Counter Measure
•Use of the system time instead of network time to determine the upper limit of block timestamps
•Tighten the acceptable time ranges
•Use only trusted peers

3.5. Eclipse Attack

In this attack, an adversary manipulates a victim peer, and it force network partition between the public network and a specific miner (victim). The IP addresses to which the victim user connects are blocked or diverted towards an adversary. Besides, an attacker can hold multiple IP addresses to spoof the victims from the network.

Counter Measure
- Users can have unique intrusion detection system to check the misbehaving nodes in the network

IV. Challenges in Bitcoin

Bit coin's popularity has made usable and secure key management important to a large new group of users. Unlike many other applications of cryptography, users will suffer immediate and irrevocable monetary losses if keys are lost or compromised. A Bitcoin wallet give a good assistance to manage and preserve all private keys belong to its owner. However, saving complete private keys on local storage meets a big challenge in case of theft. Efficient methods to enhance Bitcoin wallet security are to be developed. The key technical challenge of any decentralized e-cash is distributed consensus [11]. Another misconstrued problem is block chain's slow performance in transaction clearance rates that has led some business to give up on bit coin or switch to alternative crypto assets. Bit coin's network requires an average of 10 minutes to create a block, and it's estimated that it can only manage seven transactions per second (TPS). Lack of privacy on public block chain is a major challenge faced by Bitcoin because bit coin transactions are hashes and not encrypted which is considered as a major privacy concern associated with it. For better growth, it is very important that Bitcoin is able to overcome this challenge to become a mainstream method of payment.

Table 1 Bitcoin Statistics over last year

NO	Year	Bit coins in	Market Price	Block	Total Number of	of Loss
1	Dec '17	16774500	14165.575	21506448	287815664	Dec '17
2	Nov '18	17389037.5	4548.7975	30887305	358973915	Nov '18

The above statistics analysis is made to show the growth of bit coin in which the numbers of users and their transaction using bit coin has increased drastically in recent year.

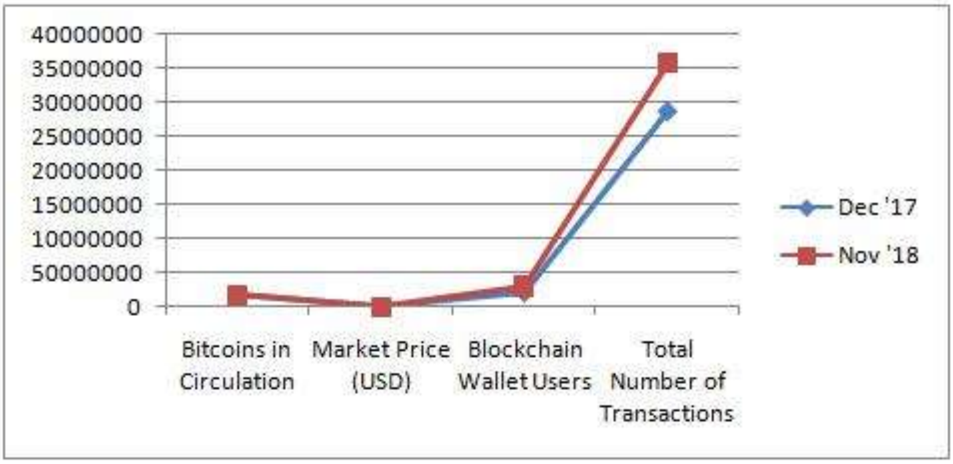

Figure 2 Statistics about bit coin obtained with different heuristics

V. Conclusion

The development of Bitcoin has not only led to advancement in crypto currency but also in different fields such as computer security, distributed system, hardware design and economics. While Bitcoin is a very popular and easy way to transfer money, it is important to note that one of biggest security concerns is not with how secure the bit coin method itself is but rather who is using it. Because of its anonymous nature, bit coin has become a popular mode of payment for criminal activity. Therefore it is important to build as more people begin to use bit coin newer and more innovative attacks are bound to come out. Therefore, it is important to keep these attacks in mind preventing them from taking place again. This paper conducts a comprehensive research on bit coin and analyses its security breaches which have been the greatest factor contributing to the drop in value of Bitcoin. In future works, more efforts will be done in addressing and exploring better solutions for the security problems in bit coin.

References

[1]. S. Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System,” available at https://bitcoin.org/bitcoin.pdf, 2008.

[2]. P. Ciaian, M. Rajcaniova and d. Kancs, "The digital agenda of virtual currencies: Can Bit Coin become a global currency?", Information Systems and e-Business Management, vol. 14, no. 4, pp. 883-919, 2016.

[3]. K. Kleineberg and D. Helbing, "A “Social Bitcoin” could sustain a democratic digital world", 2016.

[4]. Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. A fistful of bit coins: characterizing payments among men with no names. In Proceedings of the 2013 conference on Internet measurement conference, pages 127–140. ACM, 2013.

[5]. Fang Dai, Yue Shi, Nan Meng, Liang Wei, Zhiguo Ye, "From Bitcoin to Cyber security: a Comparative Study of Block chain Application and Security Issues", 4th International Conference on Systems and Informatics, 2017.

[6]. D. Bradbury, “The Problem with Bitcoin,” Computer Fraud and Security, vol. 2013, no. 11, pp. 5-8, 2013.foundation.Diabetes Care. 2008;31(4):811–822

[7]. C. Natoli and V. Gramoli, “The balance attack against proof-of work block chains: The R3 tested as an example,” CoRR, vol. abs/1612.09426, 2016.

[8]. G. O. Karame, E. Androulaki, and S. Capkun, “Double-spending fast payments in bit coin,” in Proceedings of the 2012 ACM Conference on Computer and Communications Security, ser. CCS ’12. New York, NY, USA: ACM, 2012, pp. 906–917.

[9]. I. Eyal and E. G. Sirer, “Majority is not enough: Bitcoin mining is vulnerable,” inFinancial Cryptography and Data Security: 18th International Conference. Springer Berlin Heidelberg, 2014, pp. 436– 454.

[10]. Y. Kwon, D. Kim, Y. Son, E. Vasserman, and Y. Kim, “Be selfish and avoid dilemmas: Fork after withholding (faw) attacks on bit coin,” in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, ser. CCS ’17. ACM, 2017, pp. 195–209.

[11]. T. Bamert, C. Decker, L. Elsen, R. Wattenhofer, and S. Welten, “Have a snack, pay with bit coins,” in IEEE P2P 2013 Proceedings, Sept 2013, pp. 1–5.

[12]. Arvind Narayanan, Joseph Bonneau, Edward Selten, Andrew Miller, Steven Goldfeder, ”Bitcoin and Crypto currency Technology”.

[13]. John Gregor Fraser and Ahmed Bouridane, “Have the Security Flaws Surrounding BITCOIN

[14]. L. Bahack, “Theoretical bit coin attacks with less than half of the computational power (draft),” CoRR, vol. abs/1312.7013, 2013.

[15]. Mauro Conti, Sandeep Kumar E, Chhagan Lal, Sushmita Ruj, “A Survey on Security and Privacy Issues of Bitcoin”, DOI 10.1109/COMST.2018.2842460, IEEE Communications Surveys & Tutorials

[16]. S. Bag, S. Ruj, And K. Sakurai, “Bitcoin Block Withholding Attack : Analysis And Mitigation,” Ieee Transactions On Information Forensics And Security, Vol. Pp, No. 99, Pp. 1–12, 2016.