Security Concerns and Issues for Bitcoin

Chinmay A. Vyas
Department of Computer Engineering,
Marwadi Education Foundation's Group of Institutions,
Rajkot, Gujarat, India

Munindra Lunagaria
Department of Computer Engineering,
Marwadi Education Foundation's Group of Institutions,
Rajkot, Gujarat, India

ABSTRACT
This paper focuses on the unique characteristics of Bitcoin as a cryptocurrency and the major security issues regarding the mining process and transaction process of Bitcoin. Nowadays, Bitcoin is emerging as the most successful implementation of the concept known as cryptocurrency. The Bitcoin records its transactions in a public log called the blockchain. The distributed protocols that maintain the blockchain are responsible for the security of the Bitcoin. The blockchain is run by participants known as the miners. The Bitcoin technology - the protocol and the cryptography - has a strong security track record, and the Bitcoin network is known as one of the largest distributed computing project in the world. The security aspect of the Bitcoin is the major area of research. This currency may be vulnerable during the transactions or it can be also attacked on its online storage pools or exchanges. The recent researches, mainly focused on the protocol of the Bitcoin, shows that the currency is not fully secure against the colluding groups of users that uses different attacks to fraud the 'Honest' miners of the Bitcoin.

General Terms
Security.

Keywords
Bitcoin; cryptocurrency; security; blockchain; miners;

1. INTRODUCTION
Bitcoin is a cryptocurrency that has recently emerged as a popular medium of exchange, with a rich and extensive ecosystem. Bitcoin is a consensus network that enables a new payment system as completely digital money. It can be considered as the decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen. For a simple user, Bitcoin is something like cash on the internet. Bitcoin is known as a crypto-currency as it relies on 'cryptography' to generate the 'currency' and validate related transactions. There is a global, public log maintained, called the blockchain that records all transactions between Bitcoin clients. The security of the blockchain is established by a chain of cryptographic puzzles. The group or networks of participants solving these puzzles are known as 'miners'. Each miner that successfully solves a cryptopuzzle is allowed to record a set of transactions, and to collect a reward in Bitcoins.

Bitcoin is considered as the first successful implementation of a concept called "crypto-currency", which was first described in 1998 by Wei Dai on the cypherpunks mailing list, suggesting the idea of a virtual money that relies on cryptography for its creation and transactions, rather than a central authority. The concepts of Bitcoin were conceived in the month of January, 2009 by a researcher going by the name 'Satoshi Nakamoto' pseudonymously. The open source project known as Bitcoin was created on the proof-of-work principle that transactions can be securely processed on a decentralized peer to peer network without the need for a central clearinghouse. Bitcoins are controlled by the user of the currency around the world. Bitcoin operates as a p2p file sharing protocol and it is based on SHA-256 algorithm [5]. Bitcoin coin (BTC) is essentially a hashed chain of digital signatures based upon asymmetric or public key cryptography. Each participating Bitcoin address in the P2P network is associated with a matching public key and private key wherein a message signed by private key can be verified by others using the matching public key. A Bitcoin address corresponds to the public key which is a string of 27 to 34 alphanumeric characters. Currently, the Bitcoin market exceeds more than 5 Billion USD.

The blockchain keeps the records of the transactions in units of blocks. Each block includes a unique ID, and the ID of the preceding block. Any miner may add a valid block to the chain by simply publishing it over the network to all other miners that are connected by p2p network [3].

2. PROOF OF WORK
A proof of work [6] is a piece of data which was difficult to produce so as to satisfy certain requirements. The Production of a proof of work is a random process with low probability, so it requires a lot of trial and error on average before a valid proof of work is generated. Bitcoin uses the Hashcash proof of work. Bitcoin's use of a Proof of Work system is one of the defining and unique characteristics it has as a cryptocurrency. Bitcoin uses SHA-256 hash function [3]. The network perform hashing on the block sent by the miner and checks if it still fits the pattern for the next block, by doing this the network can easily prove that the new block found by the miner is legitimate. The difficulty for the calculation of the Proof of Work can be adjusted by the network so that a new block is found at approximately every 10 minutes so it is unpredictable that which worker node in the network will generate the next block.

3. TRANSACTION PROCESS
The electronic payments by the Bitcoin are performed by generating Transactions that transfers the Bitcoin between the two peers of the network. The peers are referred by the unique virtual Bitcoin Address that is actually an alphanumeric value of 27-34 characters. The interesting point is that each peer can have more than one address that are stored and managed by the 'wallet' that is a client side application to manage Bitcoin Transactions. Peers transfer coins to each other by issuing a Transaction. A transaction is formed by digitally signing a

hash of the previous transaction where this coin was last spent along with the public key of the future owner of the coin [1]. This signature is incorporated in the coin. The authenticity of the coin is maintained by checking the chain of the signature

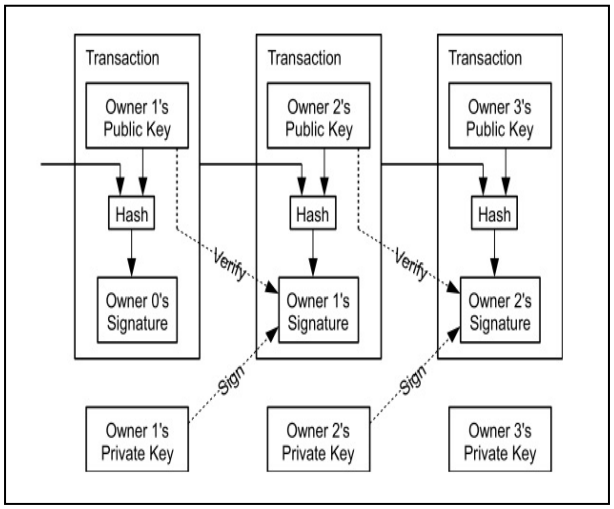

Fig 1: Transaction Process of Bitcoin (Source : [1])

There are two major types of payments supported by Bitcoin network i.e. 'slow payments' and 'fast payments'. Slow payments means that the Transaction is confirmed by the receiving node before making actual payment or service while in the case of later, the payment or service is made available on the reception of the transaction. Generally Fast payments are carried out with vary small amount of Bitcoins.

4. SECURITY ISSUES

The Bitcoin is the purely digital currency that has no physical existence. The issues related to the security of the currency are the center of the discussion from the beginning. The efforts are made to make the currency as well as its transaction and mining secure but there are still some threats exist in front of this virtual currency. The mining process as well as transaction is not fully secure and colluding users can take the advantage of the flaws in the process. There are some services that provide the facility of online digital wallet for the clients and thus can be the target of hacking attacks. Even the exchange services can also be the target for the attackers. Some of the major harmful attacks or threats on this cryptocurrency are discussed here.

4.1 Attacks on the Wallet Softwares

The client-side applications known as 'wallets' are basically used to manage the Bitcoins owned by the client as well as the transaction of the Bitcoins from/to the client. The client can either go for the online wallet services or he can choose to have wallet application downloaded in his node. Generally, the online wallets are more vulnerable to the attacks and thus need to be encrypted and backed off-line. Existing backup facilities allows the user to retrieve old wallet files and contents. The coin history is traceable that leads to link the user identity with the Bitcoin address. Distributed denials of service (DDoS) attacks are potential threats for the online wallet application.

4.2 Timejacking Attacks

Sometimes, the attacker announces the inaccurate timestamp while connecting to a node for a transaction. The network time counter of node is altered by the attacker and the deceived node may accept an alternate block chain. The serious consequences of this are double-spending and wastage of computational resources during mining process.

4.3 '>50%' Attack

This can be one of the major threats for the Bitcoin network that targets the mining process. This is when any colluding user or group of user acquires more than 50% of the computing power in mining process. This user or group can then be able to exclude, modify, and self-reverse transactions and prevent some or all 'mining' of valid blocks for their benefit. Recent researches have shown that even with about 40% of computational resources, the attackers can overcome to 6-deep confirmed transaction and that to with the 50% success probability [3]. One possible solution to reduce the harmful effect is to establish checkpoints so that the blocks before checkpoints cannot be altered. However, if this attack is successful, the attacker can launch other attacks as well. The chaos created in network by such an attack is difficult to handle and some changes done by the attacker might become permanent. The recent research at Cornell University shows that '>50%' [3] attack is feasible since single mining pools in network sometimes control 25%-33% of mining power.

4.4 Double-spending

The double spending attack [4] is a serious threat for the Bitcoin transaction in which the attacker successfully makes more than one transaction using single coin resulting into invalidating the 'honest' transaction. This attack is most likely to occur with 'Fast payment' mode. In this attack, an attacker with coin A makes a transaction to the receiver and at the same time the transaction with the same coin is made to another address that might be in the control of attacker or it may be another receiving node. By varying the timestamp, the fraud transaction can be made as a real one. Since Bitcoin peers will not accept multiple transactions with same input, they will validate the transaction that reaches them first and will invalidate all other transactions. Thus the original receiver will not be able to confirm its transaction. One possible solution for this attack is to insert the 'observers' in the network.

4.5 Selfish Mining

One of the newly researched characteristic of Bitcoin mining that makes the Bitcoin vulnerable is known as **'Selfish Mining'** [2] that allows a pool of sufficient size to obtain revenue larger than its ratio of mining power. In this attack, the colluding group of miners will force the honest miners into performing wasted computations on the stale public branch. In other words, the honest miners spend their cycles on blocks that eventually will not be part of the blockchain and they are forced by selfish miners to do so. The selfish mining group will keep their mined blocks private and will secretly perform bifurcation the blockchain while the 'honest' miners continue to waste their computational power to public branch. The selfish miners will then reveal the blocks to public branch and the 'honest' miners will switch to the recently mined blocks which will make the selfish miner group earn more revenue. In simple word, selfish miner will work to invalidate the 'honest' miners' work.

The solution provided by Ittay Eyal and Emin Gün Srer of Cornell University [2] shows that some fixation are needed in the Bitcoin protocols to reduce the success probability of selfish mining.

5. CONCLUSION

The Bitcoin is the first known successful implementation of a concept known as cryptocurrency but it is still in immature state and the developers are continuously putting their efforts to reduce the vulnerability of the Bitcoin. The main threats for Bitcoin are its vulnerability in the mining process and transactions and lack of security during the storage of the coins on the online pools. The recent research efforts are going on to reduce the threats that come forward during the mining process. The mining process of the Bitcoin is potentially vulnerable under attacks like '>50%' attacks and 'Selfish-mining' attacks. To provide security against the attack on mining process, the framework of Bitcoin protocols needs to be changed and since the Bitcoin is indeed a decentralized cryptocurrency, the protocols are accepted by the all the users and to change the protocol set of Bitcoin, the agreement of majority of the users(approximately 80%) is needed. Thus, the implementations of advanced the Bitcoin protocol security seems somewhat complex. The Advantage and Disadvantage of Bitcoin as a currency are given in below table-1. The major attacks on Bitcoin cryptocurrency are summarized in table-2.

Table 1. PROS AND CONS OF BITCOIN

Advantage	**Disadvantage**
Payment Freedom	Degree of acceptance
Fewer risks for merchants	Volatility
Very low transaction fees	Ongoing Development
Security and Control	Flaws in Mining and Transaction
Transparent and Neutral	Flaws in protocols
Decentralized Nature	
Active involvement of users	

Table 2. MAJOR ATTACK/THREATS AND THEIR TARGETS

Attack	**Target**
Attacks on Wallet File	Coins of users stored in the online wallets
DDOS Attack	Online Cloud-based exchanges and wallet services for Bitcoin
Timejacking	Transaction process, Mining process
>50%	Mining process
Double-spending	Transaction process
Selfish Mining	Mining process

6. ACKNOWLEDGMENTS

We are thankful to Nitul Dutta for his continuous support, appreciation and help for writing this manuscript.

7. REFERENCES

[1] Satoshi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system" (2008).

[2] Ittay Eyal and Emin Gün Sirer, "Majority is not Enough: Bitcoin Mining is Vulnerable," unpublished.

[3] Yogesh Malhotra, "Bitcoin Protocol: Model of 'Cryptographic Proof' Based Global Crypto-Currency & Electronic Payments System", December 4, 2013.

[4] Ghassan O. Karame, Elli Androulaki and Srdjan Capkun, "Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin," In Proceedings of the ACM Conference on Computer and Communications Security (**CCS**), Chicago, IL, USA, pp. 1-17, 2012.

[5] M. Babaioff, S. Dobzinski, S. Oren, and A. Zohar, "On Bitcoin and Red Balloons," in ACM Conference on Electronic Commerce (EC'12), ACM,. pp. 1-18, June 2012.

[6] Proof of work (online available at: https://en.bitcoin.it/wiki/ Proof _of _stake).