Acta Scientific COMPUTER SCIENCES

Volume 4 Issue 8 August 2022

Review Article

Bitcoin Security Risks

Eve Thullen* and Joseph Gorfinkle

Claremont Graduate University, California, USA

***Corresponding Author:** Eve Thullen, Claremont Graduate University, California, USA.

Received: January 08, 2022

Published: July 18, 2022

Abstract

This paper introduces basic fundamentals of bitcoin and how Bitcoin transactions are performed over the Peer to Peer distributed network. Comparisons between the Bitcoin Proof of Transaction system and the traditional banking Trust model are outlined along with the advantages and disadvantages of each. In this paper, we explore several security risks of Bitcoin implementations, such as replay attacks, forking, private key security breaches, along with IP address tracking and linking to deanonymize transactions. Lastly, the paper provides proper security measures and risk management for Bitcoin users with the goal to raise awareness of potential pitfalls as this technology proliferates from an alternative payment system into mainstream business process applications and beyond.

Keywords: IP Address; Bitcoin; Security

Introduction

Bitcoin is a Peer to Peer Electronic cash system that allows payments from one party to another without going through a financial institution [1]. The paper describing this system was released in October 2008 by Satoshi Nakamoto, believed to be a pseudonym. The paper's release was just six weeks after Lehman Brothers was forced into Chapter 11 proceedings, revealing the extent in which Financial Institutions perpetrated a housing bubble which inevitably collapsed, and sent the US into a deep and prolonged recession.

Economists estimated the crisis having the following impact; $7.4 trillion in lost stock market valuations, $3.4 trillion in lost real estate values, $1.2 trillion lost in US GDP through 2010, $5.5M US jobs lost, and a net cost of $72B for the US Gov't to repair the financial system from the crisis with programs such as TARP and QE [2].

The central theme of the Peer to Peer electronic cash system is that it replaces the trust system provided by intermediaries with proof of transaction performed by a decentralized network of participating computers which validate and store the public ledger, while providing tamper evident verification. To provide proof of transaction, a chain of digital signatures is created with public and private keys owned by the transaction sender and receiver parties. Timestamping in conjunction with the distributed network provides consensus of valid transactions blocks in their chronological order.

Participating nodes are incentivized and rewarded for providing CPU power to perform the necessary mathematical computations that validate transactions and broadcast to the public ledger, reinforcing the chain of blocks, and known as the Blockchain. Bitcoin was the 1st application to run atop of the Blockchain protocol and it has been operational since 2009 after Satoshi himself mined the first genesis block [3].

The Bitcoin software was released open- sourced in 2009 and has spawned innovations and new businesses. An estimated 1500 new digital currencies exists along with an array of services from wallets that enable participants to store Bitcoins and initiate transactions, to trading platforms that integrate the currency into portfolio's, along with real time price and volume data, to exchanges that process transactions and blockchain analysis and network tools.

As Bitcoin has evolved, numerous innovations include decreasing transaction processing time, providing new and faster network consensus models, tracking inevitable ledger forks, tailoring platforms to specific industries outside of payment processing, and adding programmability to the ledger itself in a form of smart contracts.

These innovations expect to disrupt many business processes which have costly and time- consuming intermediaries such as in Real Estate transactions, International wire transfers, Records Management systems, Supply Chain Management, Auditing services, and Voting records.

Advantages of Bitcoin

The Bitcoin protocol provides a Peer to Peer electronic cash payment system over a decentralized network of participating nodes and offer advantages over the traditional financial intermediary model including:

- No financial intermediaries
- Lower transaction costs
- Faster cross border transaction times
- An alternative to Fiat currency
- Anti-inflationary
- Microtransaction friendly or low fees
- Protection against account or asset freeze.

Disadvantages of Bitcoin

Although Bitcoin has garnered significant media attention due to its high price and volatility throughout late 2017 and early 2018, it has not replaced or impacted the overall current payment systems. According to an Alliance Bernstein report, less than twenty-five percent of Bitcoin transactions were for goods and services, the majority were speculative transactions [4]. There are many disadvantages of using Bitcoin.

- Cumbersome to setup and use
- Not widely accepted as a payment system
- Volatile price prohibits use
- Irreversible transactions
- No mediation process for transactions
- Slow transaction times, up to one hour
- All transactions are public forever
- Lack of trust in the partner ecosystem
- Unproven distribution partners
- Lack of User understanding
- New tax guidelines and mandates.

Bitcoin setup and use

The following are steps necessary for anyone to transact using Bitcoin with basics that will enhance the user understanding of how Bitcoin transactions take place and risk management techniques to put in place.

- Create a wallet
- Fund your wallet
- Purchase and pay
- Receive change
- Store wallet offline.

Creating a Bitcoin wallet necessitates choosing which device type one will use to make transactions. Your wallet can be stored on either a Desktop, Mobile phone, Hardware device, or Web based wallet. Each option requires choices; if you choose Desktop you then must choose the Operating System you run and download the full node Bitcoin Core which is 145 GB in size. The full node allows processing of transactions but also validating other's transactions which you can charge a fee for. The full node provides complete control for five key items: a) over the money in your wallet, b) provides variable validation parameters, c) is very secure d) provides variable fee and e) variable privacy control [5].

The non-Desktop options generally provide less control over these five key items. There are plenty of tradeoffs to consider. If you choose a Hardware wallet you will also need Software from the device manufacturer which they provide, and as with all software is subject to hacker's and breaches. Hardware wallets are viewed as being the most secure form of wallet [6]. User's must insure the Hardware wallet chosen is supported by the Bitcoin exchange you will use to process transactions. User's should think through how, when, where, and with what frequency they will be performing transactions, before making this important choice. They should also consider user maintenance and backup.

It is important to understand that the wallet provides access to single or multiple accounts each of which hold key pairs; Public and Private, which are necessary for every Bitcoin transaction. Regardless of which type of wallet chosen, this key pair is crucial, your actual Bitcoin or the value in your account is associated to your Public key. When receiving Bitcoin, you provide a public- address key to the sender. When you transfer Bitcoin to another party, you do so by the act of digitally signing with your Private key, which is related to your Public key, and sent to the receiver's public key. Your key pair needs to be secure, protected by passphrases, PIN's, and other methods depending upon the Wallet chosen. A copy of this important information is crucial, storing it in a safe place, and being able to retrieve it when needed.

You can fund your wallet either from a Bitcoin exchange, a Bitcoin ATM, or directly from another Bitcoin user. www.coinatmradar.com provides locations of nearby ATM's, the fees charged, and currencies supported.

There are many Bitcoin exchanges worldwide which tailor services to individuals, corporations, financial institutions, and currency traders. In general, they all require creating an account and purchasing the Bitcoin with a Debit/Credit card, which will be transferred into your wallet. One advantage of using the Exchange Web wallets is that you create a single account which you transact from, while also having the ability to transfer to other accounts housed at the same Exchange.

The downside of using Exchanged based wallets is the high number of security breaches and lost funds. According to the Bitcoin Exchange Guide, 78% of stolen cryptocurrency funds have occurred at exchanges [7]. It is far safer to transfer funds from the exchange account to your Desktop, Mobile, or Hardware wallet, albeit with the responsibility of keeping it secure and backed up.

Bitcoin transactions are initiated from your wallet which now have valid funds in a Block that was validated by the Bitcoin network when the Waller was funded, tied to your Public key. To make a payment the buyer/sender inputs a payment address from the seller/recipient, which is the soon to be owner's Public key [8]. The Public key is often embedded in a QR code which can be easily scanned with your mobile device at a retail outlet or online provided by the seller. The act of confirming the transaction in the Wallet application digitally signs the block with the buyer's Private key and add an all-important digital timestamp.

The Wallet application broadcasts the transaction block to the decentralized public ledger where upon confirmation a new block will be created and chained via the digital signature to the block just broadcasted. In the network full nodes begin a validation process to confirm and process the transaction.

First, the validation insures that buyer/sender indeed owns the Bitcoin associated with the Block and that it has not already been spent. The ledger is public and holds all transactions, so this is simply a matter of traversing the ledger history of that Public key and checking its' timestamps to insure the chronological order.

Second, the full nodes compete in a race to complete a Proof of Work which requires a high amount of computational power. The idea behind this is to incentivize full nodes to participate in this race as these nodes are crucial to the existence of the decentralized ledger system. The node that completes the Proof of Work receives a small amount of newly minted Bitcoin.

The actual Proof of Work is to find a value that when concatenated and hashed using SHA- 256 with the "nonce" that exists in the block to be validated will result in a 32-bit prefix of zeros. The most effective way to produce this Proof of Work for the prefix is through brute force computational power as it could require 4.3 billion tries to achieve. The difficulty factor for finding the Proof of Work is directly proportional to the number of leading zeros, and is adjusted by the network, after every 2016 blocks based on the average computed time [9].

Once the Proof of Work is found by a full node it is broadcasted to its peer network where all nodes check the results and vote on its validity with the consensus determining the outcome. If the outcome from the vote is valid, the network attaches a confirmation "one" to the pending block status and this notification is fed back to the Wallet application. The full nodes continue to work on subsequent blocks and as each new block is validated the confirmation is increased by one. At a confirmation of three, a bitcoin transaction is deemed very secure although for high value transactions, a confirmation of six is required [10]. Block confirmation times are running at roughly ten minutes per block thus it can take thirty minutes to execute a secure transaction, and this is dependent upon many network loading factors.

Compared to cash or debit card transactions which occur in seconds, this is a huge disadvantage for Bitcoin and seemingly limits its acceptance as a replacement payment system for retail transaction processing.

A nuance of the Bitcoin cash transaction system is the way in which change is handled. If the value of your Bitcoin in the wallet is 10.00 BTC, and your purchase value is for 2.00 your wallet will put the change of 8.00 BTC into a separate change addresses also stored in your wallet. It is not advisable to spend the funds in change accounts until the confirmation occurs from the public ledger although not prohibited. This time delay is unlike either a cash transaction or debit card transaction, whereby it is common to spend the entire available balance quickly across multiple transactions.

The distinct change addresses provide additional preservation of anonymity especially if one has multiple change addresses. However, since the public ledger shows all transactions, spent amounts as one address, and unspent amounts as change addresses, it is possible to relate one or more change addresses to its primary spending address.

Once a Bitcoin transaction has been confirmed by the consensus network, the wallet provides a notification of confirmation to you. At this point it is a good practice to disconnect from an active network and move remaining Bitcoins into an offline account, called cold storage in a secure place.

Bitcoin anonymity

Bitcoin transactions take place between public key addresses, more precisely, hashes of public key addresses. This prohibits transactions from being linked to IP addresses, yet there have been many instances whereby thieves have determined Bitcoin owner's personal identities and held them captive at gunpoint until their Bitcoin accounts were transferred to accounts under control by the thieves [11].

In 2014, researchers at the University of Luxembourg, simulated the deanonymization of Bitcoin clients and were able to determine their IP addresses in eleven percent of transactions without false positives, thirty-five percent allowing one false positive, and sixty percent if the Anti-DoS features built into Bitcoin was able to prohibit Tor VPN servers from participating in the Bitcoin transactions [12].

Although details of exactly how thieves were able to link transactions to IP addresses and to specific individuals have not been divulged, the cross referencing or data mining of information across multiple sources are believed to be the methods used [13]. User's should be aware of the potential risks of using this new cash payment system and realize without proper risk management precautions, they can effectively be broadcasting their Bitcoin account balances to the public, and yet most users would agree that publishing the balances of their Bank account would not be a good idea.

Bitcoin decentralization and vulnerability

One of Bitcoin's most important features is its decentralized structure. Comparing to traditional bank, Bitcoin has no central repository of information, no central management. All the transaction processes rely on miners in the net. The users have the right and possibility not to hand your money to any third parties. However, this situation also creates tension and certainly risks.

First, the user need to broadcasting transaction request message in the net each time. All Bitcoin transactions are stored publicly and permanently on the network, which means anyone can see the balance and transactions of any Bitcoin address. If any hackers in the net are monitoring and watching the transaction message, which can start potential Forking, Replay Attack, etc.

Second, Bitcoin works by implementing two pieces of data, or keys - one public, and the other private. The public key or Bitcoin address is what other users are provided with when they would like to make a payment. The private key is specific to each individual wallet, serving as a signature on the transaction and verification that the funds have been sent from the owner of that wallet. When users use either Bitcoin Wallet, exchange platforms, or any cryptocurrencies software, such as Bitbase, BitGo, etc., to generate those private keys, it has the risk that those private keys can be stolen by the hackers, due to weaknesses in exchanges security systems.

The other vulnerability of Bitcoin is related to transaction verification party. As Bitcoins are mined and transactions are verified via peer-to- peer cryptographic proof of-work they also called miners, which are not reliable enough and has possible security problems called Selfish Mining.

Bitcoin security issues

The danger behind most exchanges' mechanism

As the availability and adoption of cryptocurrencies increases, Bitcoin exchanges are an integral part of the virtual currency world and its ecosystem. There are over 140 exchanges over the world and some most popular cryptocurrency exchanges, such as Bitstamp, Bitfinex, Coinbase, etc., stored not only a massive amount of valuable Personally identifiable information (PII), also a lot of cash or coin deposits and withdrawals. However, few of them implemented deeper security controls and protections. The 10 biggest crypto exchanges have an average grade of 3.8 out of a maximum of 10 and a median of 4.5 [14]. Those exchange platforms are becoming new targets of the hackers! Examples of successful hacks of exchanges are countless.

The most famous is probably the Mt. Gox hack, worth $450 million been stolen, left thousands of users without a penny. MT. Gox was the world's' largest BTC exchange headquartered in Tokyo, Japan. On 6/11/2011, $460M of BTC was stolen by Hackers and another $26M of cash was lifted in the hack. Those 850,000 BTC would worth $2.1B today. In February 2014 MT. Gox filed for bankruptcy due to lawsuits and investigations by FINCEN and US Homeland Security [15].

One of the other famous one is the successful US$65 million-dollar hacking attack launched on the Bitfinex trading platform. The major factor that caused the Bitfinex trading platform vulnerability was its improper implementation of the multi-signature technology and of the BitGo software [16].

Some other exchanges faced similar outcomes: Coincheck got breached over $500M, Youbit got breached $70M and bankruptcy, Nicehash had a $68M breach [17].

Bitcoin replay attack

A "replay attack" is an exploit that can occur when two forked crypto-currencies allow transactions to be valid across both chains [18]. There are two identical blockchains, and both function in the same way, and they have the same history. If you make a Bitcoin transaction and there are two chains, it could get broadcast to both. You might think you just sent one amount of BTC, but twice.

Here is a good example of how Replay Attack works:

"You create a transaction, send 3 coins from my wallet to address Y. You sign it, and you broadcast it to the BT2 network. The transaction circulates the BT2 network and is eventually confirmed, transferring 3 BT2 coins to address Y".

"But somewhere along the line, such as a hacker, sees your transaction data, copies it, and re-uploads it to the BT1 network. This can happen by accident as well, If a transaction is accidentally rebroadcast by insight servers like blockchain.info or Bitpay, you sent out your money twice" [18].

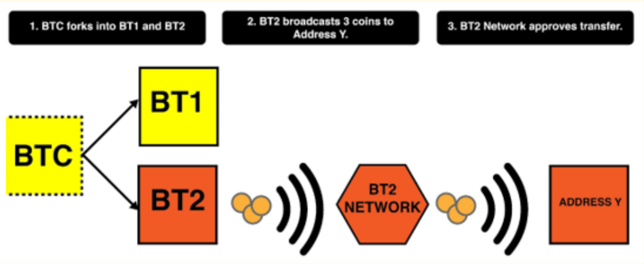
1. BTC forks into BT1 and BT2
2. BT2 broadcasts 3 coins to Address Y.
3. BT2 Network approves transfer.
BTC
BT1
BT2
BT2 NETWORK
ADDRESS Y

Figure 1: Bitcoin Replay Attack [18].

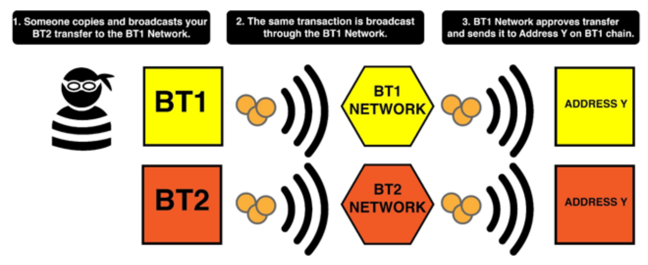
1. Someone copies and broadcasts your BT2 transfer to the BT1 Network.
2. The same transaction is broadcast through the BT1 Network.
3. BT1 Network approves transfer and sends it to Address Y on BT1 chain.
BT1
BT1 NETWORK
ADDRESS Y
BT2
BT2 NETWORK
ADDRESS Y

Figure 2: Bitcoin Replay Attack [18].

Citation: Eve Thullen and Joseph Gorfinkle. "Bitcoin Security Risks". *Acta Scientific Computer Sciences* 4.8 (2022): 68-74.

Bitcoin selfish mining

Selfish mining also called block withholding. During the Bitcoin transaction process, multiple miners join hands to form a mining pool to sum up their computing power and solve the proof of work that could be associated with one Bitcoin block [19].

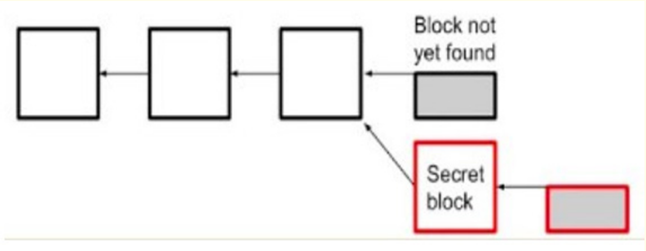

Figure 3: Selfish Mining [20].

However, with some mining pools becoming powerful enough to command significant mining ratios, some selfish miners try to increase their incentive by reducing the winning probability of other miners. The selfish miners use their computational power to mine a block, instead of broadcasting the new block to the network, they hide it and keep it secret from other miners. Then, the selfish miner attempts to find the second block while the other racers still looking for blocks. If this selfish miner can find a new block before the other miners, then broadcasting the two blocks makes the forked chain the longest. This selfish miner will always be ahead of the other miners, getting all the rewards.

Such pool attach can be combined with the Sybil attack to cause considerable harm to bitcoin mining, because selfish miners can use their power to disturb even invalided the transactions on the network.

Risk Management and Conclusion

Before beginning to use Bitcoins as user should be aware that although the Bitcoin network has been operating for eight years, it is still considered "experimental" [21]. A user should consider the following security measures to insure the safety of their Bitcoin assets.

- Preserve anonymity by performing the transaction behind a NAT or Firewall, over an encrypted log-less VPN, or through an anonymity service.
- Use multi-factor authentication when transacting; including PIN's, strong passphrases, USB keys, or Smart-Cards.
- Remove the wallet from an active network after making a transaction.
- Move funds within a wallet to another wallet used for storage only, similar to a savings account, and store this wallet in a safe place.
- Make subsequent transactions from another account in the wallet as it will use a different public address yet still be associated with your private key. Some wallets do this automatically.
- Do not link your public key to personal identification, such as in the Bitcoin Address Tag, which is a label to name transactions.
- Refrain from social media posts or blogs about Bitcoin transactions and if seeking donations or optional payments, insure this is a separate account from your main transaction account.
- Be wary of buying items with Bitcoin that have a shipment address, it is safer to send to a Post Office or PO Box.
- Avoid using a Thin Client or Hosted Wallet service for transactions as the service provider can determine your IP address and potentially social engineer your identity.
- Be aware of Bitcoin ledger fork timetables and understand if and how it affects your wallet account.

Bibliography

1. S Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System", October 31, (2008): 1.
2. P Swagel. "The Cost of the Financial Crisis: The Impact of the September 2008 Economic Collapse". Financial Reform Project, Pew Economic Policy Group, March (2010): 1-19.
3. https://en.wikipedia.org/wiki/Bitcoin
4. "Will Blockchain Change Everything?". Alliance Bernstein, LLP, New York, April 10, (2018):4.
5. https://bitcoin.org/en/getting-started
6. https://en.bitcoin.it/wiki/Hardware_wallet

7. https://bitcoinexchangeguide.com/top-cryptocurrency-theft-hacks

8. https://www.coindesk.com/information/how-do-bitcoin-transactions-work/

9. https://en.wikipedia.org/wiki/Bitcoin_network

10. https://bitcoin.org/en/developer-guide#transactions

11. https://www.nytimes.com/2018/02/18/technology/virtual-currency-extortion.html

12. Biryukov Alex., *et al*. "Deanonymisation of clients in Bitcoin P2P network". ACM Conference on Computer and Communications Security (2014).

13. https://en.wikipedia.org/wiki/Bitcoin_network#Deanonymisation_of_clients

14. Paul SECURITY. "Security analysis of the most popular cryptocurrency exchanges" (2018).

15. Chuck Russell. "Blockchain 101". Jul 12, (2017).

16. Joseph Young. "How is Bitcoin Actually Stolen? Theft Prevention". Aug 16, (2016).

17. Fan Yu and Epoch Times. "Coinbase Charge Confusion Highlights Growing Pains of Digital Currency Industry". February 24, (2018).

18. EXODUS. "What is a replay attack?". March 10, (2018).

19. Anandhu KK. "Bitcoin block withholding attack". Jan 21, (2018).

20. Blockchain at Berkeley. "Game Theory and Network Attacks: How to Destroy Bitcoin". Nov 1, (2016).

21. https://bitcoin.org/en/you-need-to-know