Study on Bitcoin Mining - Risks and Security Measures

Ms.U.SINTHUJA
M.Sc.,M.Phil, Assistant Professor
Department Of Computer Science
Rathinam College Of Arts And Science

Ms.R.ARTHI
MCA.,M.Phil, Assistant Professor
Department Of Computer Science
Rathinam College Of Arts And Science

***Abstract*—**Bitcoin, the popular digital cryptocurrency that has generated considerable public interest has grown at an enormous rate. In this paper, we look at the fundamental concepts of Bitcoin is called mining. Bitcoin mining is focuses on the process of adding new bitcoin transactions to the blockchain – the public ledger of all bitcoin transactions. This paper lists out the various attacks like 51% attack, Sybil attack, Race attack that affects bitcoin and blockchain. This paper covers the various security measures of bitcoin. We also review the existing vulnerabilities in Bitcoin and its underlying major technologies such as blockchain.

Keywords*—component, formatting, style, styling, insert (key words*

1.Introduction:

1.1 Bitcoin:

Bitcoin is a cryptocurrency, a form of electronic cash. 1 Bitcoin equals 4,60,751.67 Indian Rupee. It is a decentralized digital currency without a central bank or single administrator, and can be sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries.

Transactions are verified by network nodes through cryptography and recorded in a public distributed ledger called a Blockchain. Bitcoins are created as a reward for a process known as mining. They can be exchanged for other currencies, products, and services.

Characteristics of Bitcoin are:

Decentralized :One of Satoshi Nakamoto's main objectives when creating Bitcoin was the network's independence from any governing authorities. It is designed so that every person, business, as well as every machine involved in mining and transaction verification, becomes part of a vast network. Moreover, even if some part of the network goes down, the money will keep moving.

Anonymous :These days banks know virtually everything about their clients: credit history, addresses, phone numbers, spending habits and so on. It is all very different with Bitcoin, as the wallet doesn't have to be linked to any personally identifying information. And while some people just simply don't want their finances to be governed and tracked by any kind of an authority, others might argue that drug trade, terrorism and other illegal and dangerous activities will thrive in this relative anonymity.

Transparent ; The anonymity of Bitcoin is only relative, as every single BTC transaction that ever happened is stored in the Blockchain. In theory, if user's wallet address was publicly used, anyone can tell how much money is in it by carefully studying the Blockchain ledger.

However, tracing a particular Bitcoin address to a person is still nearly impossible.

Fast: The Bitcoin network processes payments almost instantaneously, it normally takes just a few minutes for someone on the other side of the world to receive the money, while normal bank transfers can take several days.

Non-reputable : Once user send their Bitcoins to someone, there is no way of getting them back, unless the recipient would want to send them. This ensures the reception of a payment, meaning that whoever users are trading with can't scam user by claiming that they never got the money.

2. Bitcoin Mining:

Bitcoin mining is making computers do complex math problems to help run the Bitcoin network, and miners are paid with bitcoin for contributing. Bitcoin mining itself is the process of adding new bitcoin transactions to the blockchain – the public ledger of all bitcoin transactions. A new block of bitcoin transactions is added to blockchain every 10 minutes and has been since bitcoin was created in 2009 by Satoshi Nakamoto. Whenever a new block is added to the blockchain, the bitcoin miner who successfully added the block is awarded newly generated bitcoins AND all the mining fees from people who sent a bitcoin transaction during that 10 minutes. Right now a new block rewards 25 new bitcoins, which is a ton of money!

2.2 Mining pool:

It is a way for bitcoin miners to work together for a better chance at finding a bitcoin block. All the miners 'pool' their hash rate together so that they hit new blocks more frequently. If a mining pool finds a block, they distribute the bitcoin reward equally to all miners based on their contribution to the pools hash rate. Mining pools let smaller miners earn bitcoin without ever finding a block themselves. Most mining pools have a small fee of 1-2% for hosting the pool.

2.2 Bitcoins Mining Process:

- Mining Rig Rental
- Hardware Mining
- Cloud Mining

Mining rig rentals is a way to try out bitcoin mining by renting them by the hour from someone else who owns mining hardware.

Hardware mining when user buy user‘s own bitcoin miner and set it up at home or in a warehouse. User have to maintain the hardware, pay for electricity, internet costs, cooling systems, etc. Most users buy a bitcoin miner and join a mining pool.

Cloud mining is a service where an experienced company will maintain all the hardware for you, all user have to do is pay by hash rate. There is a lot of fuss over cloud mining because many bit coiners think it is a scam, which it very well could be.

3.Attacks that effects Bitcoin and Blockchain:

3.1. 51% Attack:

A 51% attack is a potential attack on the bitcoin network whereby an organization is somehow able to control the majority of the network mining power (hashrate). Bitcoin is secured by having all miners (computers processing the networks transactions) agree on a shared ledger called the Blockchain. Bitcoin nodes look to each other to verify what they're working on is the valid Blockchain. If the majority of miners are controlled by a single entity, they would have the power to (at least attempt to) decide which transactions get approved or not. This would allow them to prevent other transactions, and allow their own coins to be spent multiple times - a process called double spending.

3.2. 34% Attack:

The tangle, a distributed ledger that is fundamentally distinct from a Blockchain but designed to accomplish similar goals, could theoretically succumb to an attacker deploying over a third of the network's hashrate, referred to as a 34% attack.

3.3. Sybil attack:

If an attacker attempts to fill the network with clients that they control, user would then be very likely to connect only to attacker nodes. Although Bitcoin never uses a count of nodes for anything, completely isolating a node from the honest network can be helpful in the execution of other attacks.

Low-latency encryption/anonymization of Bitcoin's transmissions can be defeated relatively easily with a timing attack if user connected to several of the attacker's nodes and the attacker is watching user’s transmissions at user ISP. Bitcoin makes these attacks more difficult by only making an outbound connection to one IP address per /16 (x.y.0.0).

3.4. Race attack:

Traders and merchants who accept a payment immediately on seeing "0/unconfirmed" are exposed to the transaction being reversed. An attempt at fraud could work that the fraudster sends a transaction paying the merchant directly to the merchant, and sends a conflicting transaction spending the coin to himself to the rest of the network. It is likely that the second conflicting transaction will be mined into a block and accepted by bitcoin nodes as genuine.

Merchants can take precautions to lessen the risk of a race attack but the risk cannot be eliminated. Therefore, the cost/benefit of the risk needs to be considered when accepting payment on 0/unconfirmed when there is no recourse against the attacker.

3.5. Finney attack:

The Finney attack is a fraudulent double-spend that requires the participation of a miner once a block has been mined. The risk of a Finney attack cannot be eliminated regardless of the precautions taken by the merchant, but some miner hash power is required and a specific sequence of events must occur. Just like with the race attack, a trader or merchant should consider the cost / benefit when accepting payment on just one confirmation when there is no recourse against the attacker.

4.Security Measures of Bitcoin:

4.1 KeepKey – Hardware Wallet

The coolest looking tech gadget to show off to user’s friends. Made by a relatively new company, KeepKey offers a hardware wallet of a polished design. KeepKey is said to be a port of Trezor’s code and firmware, so their main difference is the material. KeepKey feels like a ‘premium’ wallet but might be a little on the heavy side and hence more susceptible to drops. It comes with a standard, simple to use client UI.

4.2 Nano Ledger S – Hardware Wallet

Nano Ledger S is just as secure as the other two hardware wallets. It is popular because of its relatively low price of $65 compared to its competitors. Being smaller than KeepKey, it is more portable and easier to carry around. It is a hardware wallet that comes at a very competitive price.

4.3 Trezor – Hardware Wallet

Trezor is one of the first movers in the hardware wallet industry and sets the gold standard for crypto security. Trezor has a reputation for providing top-notch security, protecting against both virtual and physical theft. What Trezor lacks in style, it more than makes up in the security department. Even if user’s is compromised with malware, user’s private keys will still be safe with Trezor. In this sense, Trezor is more of a vault than a wallet.

4.4 Coinbase – Hot Wallet

Coinbase is an online web-based wallet and is the beginner-friendly version of GDAX. As a hot wallet, user can easily transfer to the GDAX exchange instantly, and for free. In the

same interface, user can make quick purchases with fiat. What's more, 100% of user's crypto holdings on Coinbase is insured. User can activate 2-Step Verification and Google Authenticator for more protection, and Coinbase even has a vault available if user wish to trade convenience for an added layer of security. The only drawback is that Coinbase only offers Bitcoin and Ethereum wallets.

4.5 MyEtherWallet – Paper Wallet

Paper wallets are for those who wish to have their own private wallets without forking out cash for hardware wallets. The money saved could be invested in their coins. Simply generate user's wallet online at myetherwallet.com and note user's private keys. The website does not store or transmit any of user'sprivate information. If user don't trust the online version, user can even download it from GitHub and run it offline. Paper wallets are free but require an in-depth knowledge to set it up properly. In short, this type of wallets generally take a lot of hassle and are not advised for novices.

4.6 Jaxx — Software Wallet

Carrying user's crypto around safely and conveniently is no longer a distant dream. Behold Jaxx, the world's first mobile wallet solution. Versions for iOS, Android, desktop and browser are now available. Jaxx uses a mnemonic seed to back up user's wallet or transfer it to a different device. Jaxx allows user to receive user's funds, scan QR code, view user's crypto holdings, all in one intuitive app. Advanced features such as shape shift integration and multiple platforms wallet linkage makes this the preferred wallet for the tech savvy. The only drawback with this wallet is that it might have a steep learning curve, and features might not be stable with all the new integrations. With time, this will prove to be a promising solution.

4.7Electru– Software Wallet

Electrum is a fast, lightweight wallet for desktop and mobile users. It has a long list of supported features to make it the most flexible wallet today. It offers cold storage solutions, integration with hardware wallets (KeepKey, Nano Ledger S, Trezor) and able to achieve anonymity (with Tor). On the security side, Electrum enables multi-sig support, and it is not tied to a centralized server, so server downtime will not be an issue. Overall, Electrum is the established software wallet solution out there that warrants a try-out.

5. Impact Analysis

The vulnerabilities are discovered pose a serious threat to the Bitcoin network and its users. A miner communicating via Stratum presents a series of possible scenarios in which a user is at risk. These include:

- An attacker can sniff the clear text credentials in the mining. Authorize message. These credentials may be used elsewhere across the internet and may lead to account compromise.

- An attacker in the middle of a connection can replace the Bitcoin address in the username field of a mining. Authorize message with their own to steal the users' payouts from the pool.

- An attacker can spoof a "client. Reconnect" message from the pool to redirect the miner to a private pool. This reconnection would not be initially obvious to the users and the pool would not need to payout any shares of the Block rewards.

- An attacker can spoof a message from a pool containing a malicious payload related to one of the discovered CVE's to initiate a client DOS. If this is done en mass, this can reduce mining competition from the attacker's pool, or increase their relative share of the network hashrate and make it easier to execute a successful double spend.

- An attacker or malicious pool can send a message containing a malicious payload that remotely executes code on a victim's machine. This can be used to install malware such as rootkits and key loggers. If the mining system is also used as a desktop, this can lead to various compromises including stolen passwords, credit card numbers, and banking information. The vulnerabilities mentioned above also increase the likelihood of a 51% attack from a party with little stake in the mining equipment. An attacker who can compromise mining software and redirect hashes to their own pool may not have invested any capitol into using these exploited devices and may have little concern over the attack's effect on the currency. For this reason, trust in stake holders is a dangerous assumption to make when securing the Bitcoin network

6. Conclusion:

In this paper, we have described aspects of Bitcoin relevant to Bitcoin mining and the Block chain technology that runs the bitcoin cryptocurrency. The goal of Blockchain is to provide the anonymity, security, privacy and transparency to all its users. Together with security, the distributed nature of Bitcoin blockchain has lead glitches in the privacy and anonymity requirements of the users. In summary, this paper attempts towards highlighting the security and privacy issues in Bitcoin.

7.References:

[1] I. Bentov, A. Gabizon, and A. Mizrahi, "Cryp-tocurrencies without proof of work," CoRR,vol. abs/1406.5694, 2014.

[2] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A.Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in IEEE Symposium on Security and Privacy , pp. 104–121, May 2015.

[3] N. T. Courtois and L. Bahack, "On subversive miner strategies and block withholding attack in bitcoin digital currency,"CoRR , vol. abs/1402.1718, 2014.

[4] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," CoRR , vol. abs/1311.0243, 2013.

[5] J. Garay, A. Kiayias, and N. Leonardos, The Bit- coin Backbone Protocol: Analysis and Applications , pp. 281–310, Springer Berlin Heidelberg, Berlin, Hei- delberg, 2015.

[6] A. Gervais, G. O. Karame, V. Capkun, and S. Cap- kun, "Is bitcoin a decentralized currency?," IEEE Security Privacy , vol. 12, pp. 54–60, May 2014.

[7] A. Gervais, G. O. Karame, K. W¨ust, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in Proceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS'16), pp. 3–16, New York, NY, USA, 2016.

[8] A. Gervais, H. Ritzdorf, G. O. Karame, and S. Cap kun, "Tampering with the delivery of blocks and transactions in bitcoin," in Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security (CCS'15) , pp. 692–705, New York, NY, USA, 2015.

[9] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on bitcoin's peer-to-peer network," in 24th USENIX Security Symposium , pp. 129–144, Washington, D.C., 2015.

[10] G. Karame, "On the security and scalability of bitcoin's blockchain," in Proceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS'16) , pp. 1861–1862, New York, NY, USA, 2016.

[11] G. O. Karame, "Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin," in Proceedings of Conference on Computer and Communication Security, pp. 1–17, 2012

[12]Mick Ayzenberg et al. A Security Analysis of the Bitcoin Mining Ecosystem.