RESEARCH AND ANALYSIS ON SOK: NETWORK-LEVEL ATTACKS ON THE BITCOIN P2P NETWORK

Safio, Abdirahman

Safio Sheik Abubakar Keilie, Department of Computer Engineering, RK University, Gujarat, India

And Abdirahman Abdikadir Nor, Department of Computer Engineering, RK University, Gujarat, India

ABSTRACT

A new generation of blockchain-based innovations has emerged as a result of Bitcoin's influence on the world economy and technology in the past decade. Its protocol has become one of the most important for decentralised systems and digital currencies. In particular, the P2P layer serves as a standard against which all permissionless blockchains can be measured; its solutions are frequently incorporated into the network layer of such systems. Unfortunately, the Bitcoin network protocol does not have a solid security model, which leaves it vulnerable to a variety of dangers. This layer is vulnerable to attacks that can undermine the trustworthiness of the entire system by undermining the consensus layer's reliability. The security of the Bitcoin P2P system must therefore be thoroughly understood and addressed. The primary goal of this study is to educate users and academics on the blockchain peer-to-peer network technology that underpins Bitcoin and to examine the security assaults that threaten this vital financial digital cash network. This research looks into eleven attacks that could compromise the Bitcoin blockchain peer-to-peer network and proposes potential defences against them.

1 INTRODUCTION

In today's technology age, there has been a meteoric rise in fascination in cyberspace. The banking industry has also jumped on this bandwagon by adopting cryptocurrency payments. The blockchain technology laid the groundwork for a new kind of internet by allowing digital crypto currency to be circulated without the possibility of duplication. The first and most popular usage of blockchain technology is the online virtual currency Bitcoin. This solution eliminates the need for intermediary banks by leveraging the decentralised peer-to-peer network and cutting-edge cryptography algorithms to facilitate asset transfers directly between buyers and sellers. Bitcoin's impact on the global economy and the future of the digital marketplace.

While blockchain was primarily developed for the digital currency Bitcoin, its potential applications have now been discovered in many other areas, including healthcare[1], IoT[2], e-voting[3], and supply chain management[4] systems. Satoshi Nakamoto created Bitcoin as a decentralised digital currency and peer-to-peer payment mechanism in[5]. The year 2009 marked the official launch of te money. Bitcoin, the most frequently used virtual currency[6], can be used to purchase goods and services from a growing number of merchants, such as Overstock.com, Expedia, and other online marketplaces[7]. The currency can be exchanged between individual customers as payment for goods and services. The electronic exchanges function similarly to foreign exchange markets, allowing users to trade one kind of currency for another. The currency has far more notable liquidity than other virtual currencies due to its status as the most popular virtual currency money by a wide margin. When trading to more conventional currencies like the Euro or the U.S. dollar, customers can keep a large portion of the cryptocurrency's intrinsic value. However, because to Bitcoin's immense popularity, hackers have begun attacking its networks in hopes of making illegal gains.

Because of its success, the Bitcoin P2P protocol has inspired at least 33 imitators, and 34 of these are direct forks of Bitcoin itself. While other blockchains may have significant differences in the application and consensus layers (35), their underlying network protocol (36) generally has similarities with Bitcoin. Problems

with the Bitcoin P2P system have knock-on effects for other cryptocurrencies. This is especially important when thinking about security threats, which can compromise the guarantees provided by the previous tiers (layers 39 and 40). Because of this, investigating and fixing Bitcoin's P2P protocol's security flaws should be a top priority.

There are already 1560 blockchain platforms available [11], since Bitcoin was first presented in January 2009. For example, businesses can utilise blockchain systems to accept digital payments or bitcoin for specific transactions, such selling a product or service. The use of this digital payment option has helped propel the growth of the digital currency economy on nearly all open blockchain platforms. There are significant privacy and security concerns in the cryptocurrency market due to the prevalence of various network attacks such as Distributed Denial-of-Service (DDoS) assault, Sybil attack, double-spending, transaction malleability, attacks on mining pools, etc. Recent research on Mt. Gox, a popular Bitcoin exchange platform based in Tokyo, revealed that the exchange suffered losses of $4.6 million USD due to a transaction vulnerability hack in Bitcoin in April 2013 [12], and another $470 million USD due to a cyber-attack in 2014. This ultimately led to the demise of the business. Another example is the Hong Kong Bitcoin exchange, which reported hack-related losses of USD$65 million in August of 2015 [12]. Coin check, a major digital crypto currency exchange situated in Japan, was hacked in January 2018, losing XEM worth 534 million USD. Over 73% of Bitcoin platforms using Imperva Incapsula's services were compromised in 2017, according to their research [13].

2 LITERATURE REVIEW

Kiayias et al. demonstrate how the architecture of the network has a direct impact on the efficiency with which information is spread throughout the network. The amount of connections that nodes have can also have a significant impact on the time it takes for information to propagate. In addition, it is well knowledge that unstructured P2P networks, such as blockchain ones, are plagued by a problem known as "topology mismatch," which refers to the incoherence that exists between logical and physical linkages and is the root cause of inefficiency in the transmission of data. Blockchain networks are not immune to this issue.

Concerning matters pertaining to safety, it has been demonstrated that the topology of the Bitcoin network is not, as was originally intended, that of a random graph. Instead, it demonstrates high levels of centralization through the presence of node communities and a supernode. Having knowledge of the topology of the network could assist identify these kinds of problems and promote decentralisation. It's also possible that an open topology might speed up the propagation of transactions and blocks, which, in turn, would make it more difficult to carry out double-spending attacks and mining for one's own benefit.

All of these concerns might be handled in real time if nodes had access to information about the topology of the network. In addition, the availability of such information might be able to assist in minimising the disparities that exist between formal models and the actual network.

Hiding the topology prevents network analysis and measurement, as mentioned by Delgado et al., which further complicates the process of finding a solution to the problems that are already present. In a similar vein, Miller et al. [11] note that having an understanding of the topology makes it possible to locate structural defects in the network, which may prevent broadcast optimisation from occurring. Because of this, they are in favour of the premise that monitoring the network can assist in assisting in the rapid detection and reaction to assaults as well as mistakes. In addition, the authors of assert that acquiring knowledge of topology is essential if one wishes to accurately manage the network, maximise its capabilities, and guarantee that it operates in an effective manner.

An open Bitcoin topology may enable the introduction of techniques for avoiding centralization and improving communication among nodes, as well as the detection of weak places that may be used to do network-level attacks. This may also make it possible to find weak spots that may be exploited to perform network-level assaults. As a result of this work, one of our goals is to make the initial move in the desired direction. To do this, we will first demonstrate that an open topology should not be regarded a security risk, and then we will provide a workable protocol that can reliably monitor the condition of the network.

3 THE BITCOIN P2P NETWORK

Clients exchange transactions and come to a consensus on the data contained in the blockchain using the Bitcoin P2P network, which serves as the primary infrastructure for the cryptocurrency. When new nodes are added to the network, they do so via establishing connections with well-known nodes or by contacting a reliable DNS server. Once the initial connections have been made, nodes will begin to discover new peers when they begin to receive ADDR messages from their existing neighbours. These messages inform users of other nodes in the network that are already known and to which it is possible to connect.

Each node establishes connections with a subset of its peers and, to the extent that it is able, accepts connections offered by other nodes. If a connection is initiated by a node other than itself, it is said to be outbound relative to that node; otherwise, it is said to be incoming. Nodes that are running the Bitcoin Core reference client, which is the client that is used the most in the network [10], are required to constantly keep 8 outbound connections and are allowed to accept inbound connections from a maximum of 125 peers. Despite this restriction, the protocol does not actively enforce it, which means that nodes are allowed to establish any number of connections they choose.

Nodes in a network are often classified as either reachable or unreachable. This is because some clients, due to the presence of NAT or firewall, are unable to accept incoming connections. According to the findings of study, there are around ten times as many unreachable nodes as there are reachable nodes, making up almost 90 percent of the entire network. Despite this, the majority of study concentrates solely on the part of the network that can be reached [. This is because it is simpler to investigate and is thought to be more significant for the dissemination of messages because it is the section of the network that maintains the great majority of connections. In a similar vein, we shall limit our attention in this work to nodes that can be reached

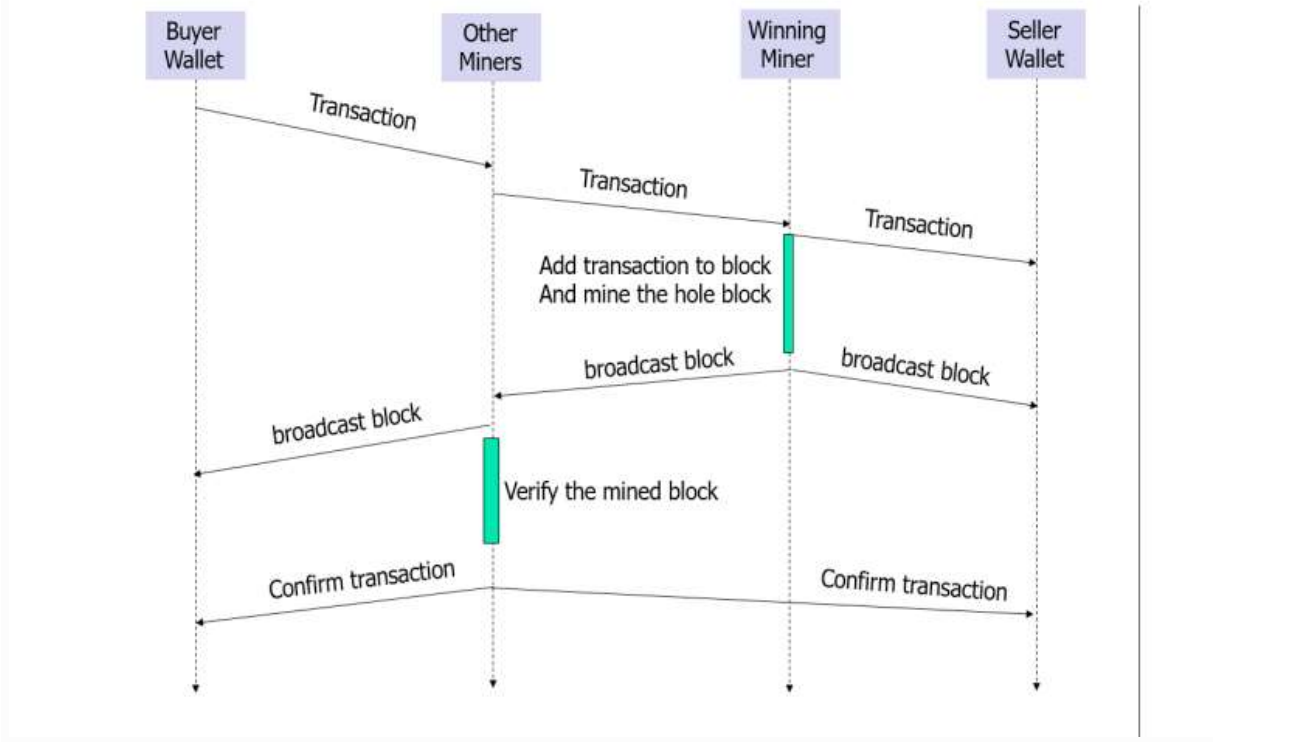

FIGURE 3.1. Bitcoin transaction processing

As shown in Figure 3.1, the process that takes place when one holder of bitcoins (the buyer) wants to transfer some money to another holder of bitcoins (the seller) in order to pay for goods or services. The amount of Bitcoin that is going to be transferred must be included in the transaction, as well as the public key of the seller, which identifies the seller's Bitcoin wallet as the recipient of the transferred amount. This transaction must be created by him. To further demonstrate that he is the rightful owner of these Bitcoins, the sender is required to

sign the transaction using his own private key. After that, he will send the transaction to the seller and then broadcast it to all of the nodes in the network [5]. Some of the nodes in the network take on the role of miners; it is their responsibility to validate the transaction, determine who owns it, and ensure that it has not been spent twice in order to avoid double spending. A miner will compile all of the valid transactions into a block before beginning mining on that block. In order to "mine" a block, miners must first attempt to solve a difficult cryptographic challenge that is easy to verify but difficult to compute. The first miner who is successful in decoding the secret message is declared the winner. Instantaneously, he sent out a broadcast to other nodes in the network, sharing the newly mined block.

4 RESULTS AND STUDY

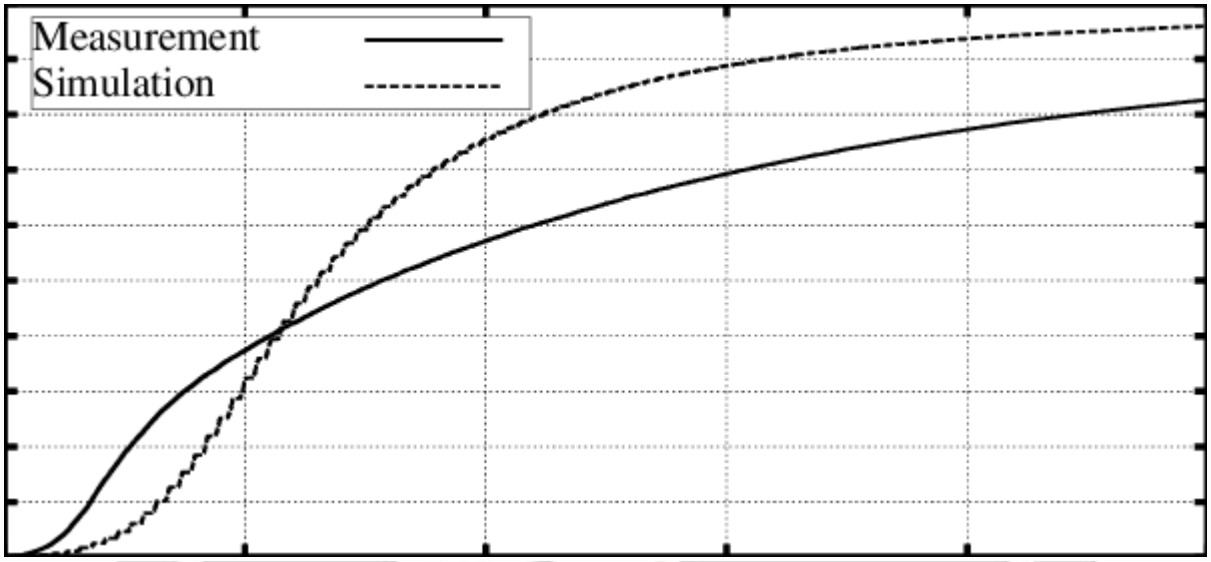

Fig 4.1 - Comparison of the distribution of Δt h,i as measured in the Bitcoin network with simulation results.

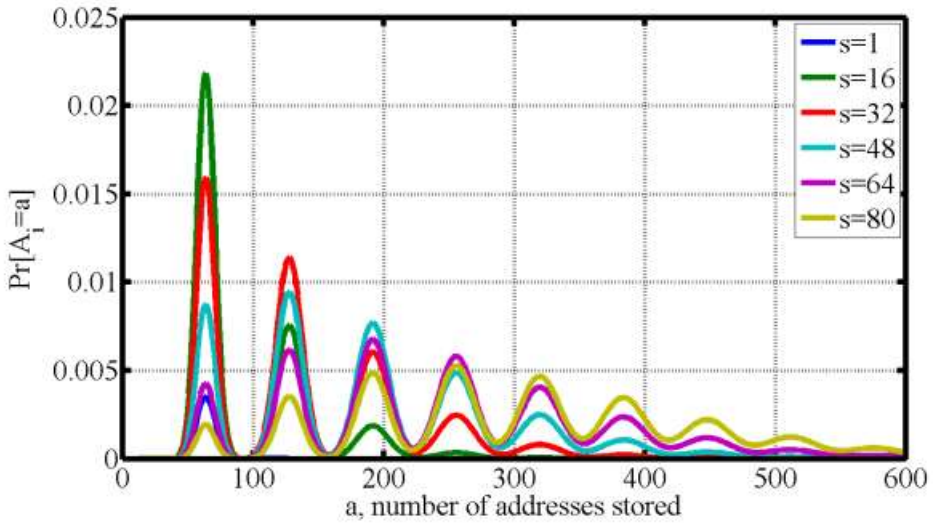

Figure 4.2: Distribution of Ai , for different choices of s (the number of groups) and with t = 256 (addresses per group), per equation (15).

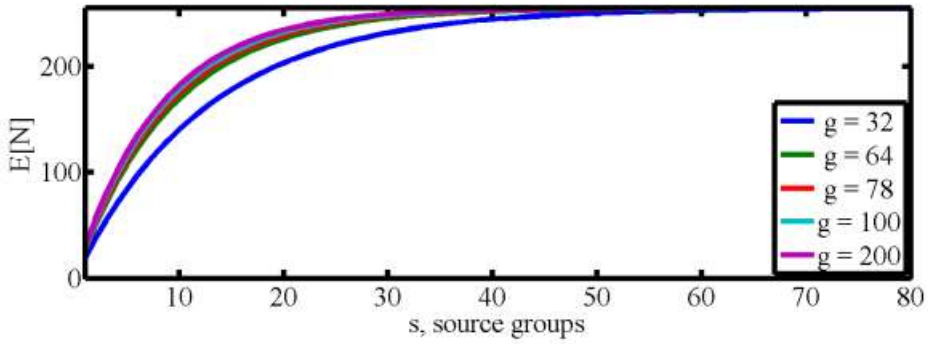

Figure 4.3: E[N] vs s (the number of source groups) for different choices of g (number of groups per source group).

Delay Routing Network Attack

The Bitcoin nodes are designed to only request a block from a single peer in order to prevent the network from becoming overburdened by an excessive number of block broadcasts. If the initial request for the block does not receive a response after a predetermined amount of time—say, twenty minutes—an additional peer will make the request again. Because of this design decision, massive network attacks are now possible, in which anyone who disrupts Bitcoin transmission can delay the block's propagation on the connections that correspond to it. During this phase of the assault, the attacker will attempt to make certain fundamental alterations to the content of Bitcoin messages known as inv, obtain data, and tx.

Distributed Denial-of-Service Attack

The DDoS attack is distinct from the DoS attack in several key respects, including the fact that in the DDoS attack, multiple malicious machines are coordinated to concentrate their attention on a single resource. It is more likely that the DDoS attack will be successful in interrupting the objective than it is that the DoS attack coming from a single source will be successful. As a result of the fact that the attacks come from a variety of locations, this tactic is favoured by a great number of malicious actors as it is progressively more difficult to track down where the attacks originated. DDoS assaults have been used to target the internet servers of huge organisations, such as banks, online commerce shops, and even key public and government services, in the vast majority of cases. However, it is crucial to keep in mind that any network, server, or device associated with the internet could potentially be a target for the kinds of assaults that are being discussed here.

5 CONCLUSION AND FUTURE DIRECTIONS

The Blockchain technology has undergone significant progress over the course of the past few years. There are numerous other blockchain technologies that are beginning to make a name for themselves in the market in addition to Bitcoin. However, the peer-to-peer networks that Bitcoin use have a significant number of security flaws. This article offered a detailed analysis of a variety of security concerns that are associated with Bitcoin peer-to-peer networks. Additionally, this article presented proper solutions for these issues. However, there are other problems that haven't been fully solved yet, and researchers need to look at those so they may come up with more creative answers. In this section, some avenues for further research are outlined. The Proof-of-Work (PoW) consensus protocol makes blockchain more resistant to various assaults, such as double spending and the Sybil attack. However, the time-wasting nature of the PoW consensus protocol has a dramatic impact on the amount of time it takes for Bitcoin transactions to be processed. When compared to other digital cash systems, such as the VISA card, it is extremely sluggish. In addition, the high rate of power consumption that Proof of Work causes poses a risk to the long-term viability of Bitcoin. Due to these factors, researchers are compelled to develop alternative consensus protocols such as Proof of Authority (PoA), Proof-of-Stake (PoS), Proof of Storage, Federated Byzantine Fault Tolerance (FBFT), Practical Byzantine Fault Tolerance (PBFT), and Proof of Elapsed Time (PoET). However, each of these protocols suffers from a unique set of drawbacks. It is

necessary to have more recommendations that blend desirable qualities and avoid problematic aspects of earlier ones.

References

1. Nakamoto S (2008) Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

2. CoinMarketCap (2020) Bitcoin price, charts, market cap and other metrics. Last accessed: 2020-01-16. https://coinmarketcap.com/currencies/bitcoin/

3. Conti M, et al. (2018) A survey on security and privacy issues of bitcoin. In: IEEE communications surveys tutorials 20(4)(Fourthquarter). issn: 2373-745X. https://doi.org/10.1109/COMST.2018.2842460, pp 3416–3452

4. Tapsell J, Akram RN, Markantonakis K (2018) An evaluation of the security of the bitcoin peer-to- peer network. In: arXiv:1805.10259

5. Reid F, Harrigan M (2013) An analysis of anonymity in the bitcoin system. In: Security and privacy in social networks. isbn: 978-1-4614-4139-7. https://doi.org/10.1007/978-1-4614-4139-7n_10. Springer, New York, pp 197–223

6. Neudecker T, Andelfinger P, Hartenstein H (2015) A simulation model for analysis of attacks on the Bitcoin peer-to-peer network. In: 2015 IFIP/IEEE international symposium on integrated network management (IM). https://doi.org/10.1109/INM.2015.7140490, pp 1327–1332

7. Heilman E, et al. (2015) Eclipse attacks on bitcoin's peer-to-peer network. In: 24th USENIX Security Symposium (USENIX Security 15). Washington, D.C.: USENIX Association. isbn: 978-1-931971-232, pp 129–144

8. Biryukov A, Khovratovich D, Pustogarov I (2014) Deanonymisation of clients in bitcoin P2P network. In: Proceedings of the 2014 ACM SIGSAC conference on computer and communications security. CCS '14. Scottsdale, Arizona, USA. isbn: 978-1-4503-2957-6, https://doi.org/10.1145/2660267.2660379. ACM, pp 15–29

9. Koshy P, Koshy D, McDaniel P (2014) An analysis of anonymity in bitcoin using P2P network traffic. In: Financial cryptography and data security. isbn: 978-3-662-45472-5. Springer, Berlin, pp 469–485

10.Yeow A (2020) Bitnodes - global bitcoin nodes distribution. Last accessed: 2020-01-16. https://bitnodes.earn.com/

11. Miller A, et al. (2015) Discovering bitcoin's public topology and in uential nodes

12. Neudecker T, Andelfinger P, Hartenstein H (2016) Timing analysis for inferring the topology of the bitcoin peer-to-peer network. In: 2016 Intl IEEE conferences on ubiquitous intelligence computing, advanced and trusted computing, scalable computing and communications, cloud and big data computing, internet of people, and smart world congress. https://doi.org/10.1109/UIC-ATCScalCom-CBDCom-IoP-SmartWorld.2016.0070, pp 358–367

13. Delgado-Segura S, et al. (2019) TxProbe: Discovering Bitcoin's Network Topology Using Orphan Transactions. In: Financial cryptography and data security. isbn: 978-3-030-32101-7. Springer International Publishing, Cham, pp 550–566

14. Neudecker T (2019) Characterization of the bitcoin peer-to-peer network (2015-2018). Tech. rep. 1, Karlsruher Institut für Technologie (KIT). https://doi.org/10.5445/IR/1000091933

15. Bitcoin Core Last accessed: 2020-07-02. https://bitcoincore.org/

16. Bitcoin Wiki (2019) Protocol Documentation. Last accessed: 2019-12-03. https://en.bitcoin.it/wiki/Protocoldocumentation.