5-13-2023

An analysis and examination of consensus attacks in blockchain networks

Thomas R. Clark
James Madison University

An Analysis and Examination of Consensus Attacks in Blockchain Networks

An Honors College Project Presented to

the Faculty of the Undergraduate

College of Business

James Madison University

by Thomas Richard Clark

May 2023

Accepted by the faculty of the College of Business, James Madison University, in partial fulfillment of the requirements for the Honors College.

FACULTY COMMITTEE:

Project Advisor: John Guo, Ph. D.

Reader: Thomas Dillon, Ph. D.

HONORS COLLEGE APPROVAL:

Dean, Honors College

PUBLIC PRESENTATION

This work is accepted for presentation, in part or in full, at The Spring 2023 Honors Symposium on Friday, April 21.

Table of Contents

Acknowledgements

I would like to express my sincere gratitude to the following individuals and organizations that have supported me throughout this project and my time while at JMU.

First and foremost, I would like to thank Dr. John Guo who served as my project advisor. His guidance, encouragement, and feedback throughout the project were vital and helped to shape my work and point me in the right direction. Additionally, I would like to thank Dr. Thomas Dillon who served as one of my readers for the project. His willingness to assist and support my work was invaluable.

I am also indebted to the JMU College of Business which has afforded me many opportunities to explore my interests and whose classes were instrumental in shaping my JMU academic experience. In addition, I would also like to thank the JMU Honors College for giving me the chance to discover, research, and present on Blockchain Networks, a topic that I am passionate about. The resources, faculty, and support that I have received were paramount in helping me be successful.

Lastly, I would like to thank my friends and family for their unwavering support and encouragement throughout my academic journey. Their constant presence has been the bedrock of my success and for that I am grateful.

Abstract

This paper examines consensus attacks as they relate to blockchain networks. Consensus attacks are a significant threat to the security and integrity of blockchain networks, and understanding these attacks is crucial for developers and stakeholders. The primary contribution of the paper is to present blockchain and consensus attacks in a clear and accessible manner, with the aim of making these complex concepts easily understandable for a general audience. Using literature review, the paper identifies various methods to prevent consensus attacks, including multi-chain networks, proof-of-work consensus algorithms, and network auditing and monitoring. An analysis revealed that these methods for preventing consensus attacks are not mutually exclusive and can be used in conjunction with each other.

Ultimately, the choice of which methods to implement depends on the specific needs and goals of the network being built. The paper concludes with a discussion of the implications of these findings for blockchain network development and security.

Introduction

We inhabit a digital era where transactions are increasingly conducted online. The significance of safeguarding these transactions is becoming clearer every day. Blockchain technology has emerged as a prominent topic of discussion in response to this need. With the surge of cryptocurrencies and transactions taking place on the deep web, both individuals and business are turning to blockchain to secure data integrity.

In technical terms, a blockchain network is a shared ledger, consisting of a chain of blocks, each containing data and are linked together. To draw a physical analogy, each block can be thought of as a transaction in the ledger.

Each block contains three key components: the hash, the hash of the previous block, and the data. The hash serves as a distinct identifier for each block. Although the computation process lies beyond the scope of this paper, it is worth mentioning that the function responsible for generating this value minimizes the occurrence of duplicate values. So much so, that the uniqueness of the hash has been likened to that of a human fingerprint. For instance, a SHA-1 (Secure Hash Algorithm 1) hash value may appear as 'b03f42af675493b3eb1ee7c4573537de113a00ff'. Each block also contains the hash of the previous block, essentially "linking" them [Figure 1]. Depending on the type of blockchain, each block will have data depending on its usage. For example, transactions, messaging, medical data, etc. In addition to the hash, hash of the previous block, and data, a block might have optional data such as timestamps as well as index values which share its location in the chain.

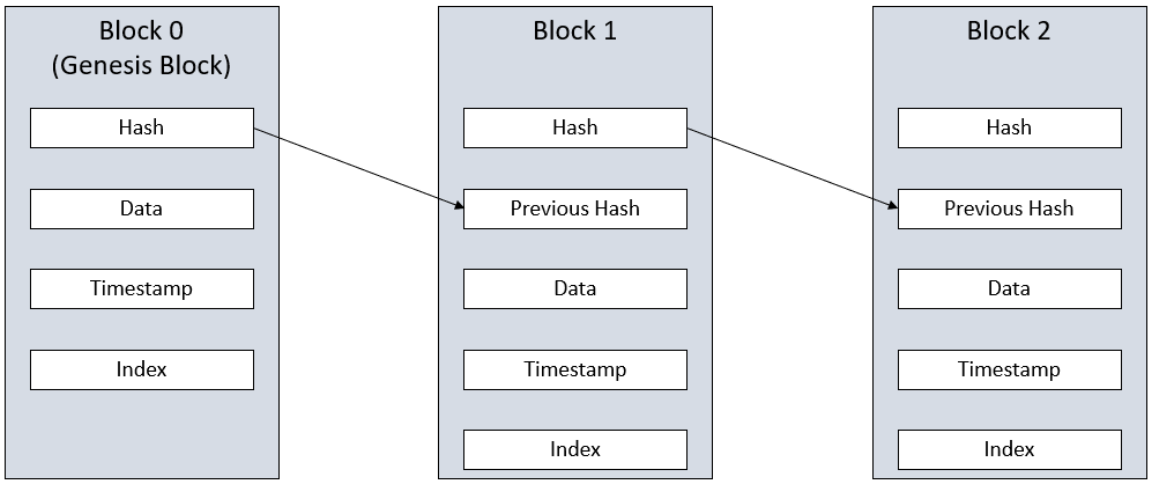

Figure 1: Conceptual Diagram of a Blockchain Network

One unique trait about this technology is that it is distributed and without central authority such as a bank or government. It is distributed in that the ledger is shared among computers in the network and allows the community of computers to record transactions in that shared ledger (Yaga et al., 2018).

As mentioned earlier, data in a blockchain network are stored in unique blocks which are assigned unique digital signatures. These digital signatures are used in order to validate data as well as prove to other computers in that network that the transaction is valid. For example, proving where the transaction came from as well as proof that it was not altered in transit. If information in a block is altered, any subsequent blocks after it are immediately invalidated (Sayeed & Marco-Gisbert, 2019). Additionally, these digital signatures are incredibly difficult to spoof, enhancing their security.

Another characteristic of this technology is that it is immutable. That is to say, data in the network can only be inputted, not removed nor edited. Returning to the physical ledger example, it is the equivalent of writing all transactions in permanent marker. One of the main goals of doing this is to ensure data integrity.

This integrity is achieved by all computers, or, more accurately, the sum of all computing power in the chain, achieving a consensus on whatever transaction is added. That is to say, what a chain "says" happened, will be what a majority of the computers, or processing power in the chain agrees on. For example, if transaction data in one computer is wrong, it will be automatically corrected to follow the *majority*. This supplies a layer of security as well. As long as an attacker does not have a majority of computing power in the network, they won't be able to make fraudulent transactions.

As more individuals and businesses use blockchain networks to facilitate their transactions in the virtual space, both private and public individuals and entities rely on it for these unique security characteristics. Those characteristics being: immutable, anonymous, and consensus-based, among others. Because of these security measures, individuals making transactions that rely on blockchain technologies don't necessarily need to trust the other party, only the technology that they are both using. However, as with most new technologies, new attacks and exploits are developed to cripple even the most sophisticated security measures. One such attack is a consensus attack. The focus of this paper is this threat and how blockchain networks can work to prevent them.

Also known as a "majority" or "51%" attack, this takes advantage of the fact that blockchain technologies are consensus-based. Simply, if an individual were to gain a majority of the

computing power in a chain, they could fraudulently add transactions or data to a ledger that did not actually occur. Because the chain follows the majority of the computing power, all other computers in that chain would be forced to accept those transactions/additions as a truth. The capabilities of these types of attacks get even more interesting as we consider the rise of quantum computing and its ability to generate a large amount of computing power and take over networks.

One of the most notable consensus attacks occurred in January 2019 on the Ethereum Classic blockchain, a form of cryptocurrency. Hackers were able to steal over $1 million worth of ETH over multiple days by reversing transactions after they had already been confirmed. This attack is one example of many that highlights the need for greater blockchain security.

The relevance of this type of attack is particularly significant in the case of cryptocurrencies, especially newer ones that have a limited amount of computing power within the network. One potential impact of this attack is the ability to control the flow of currency within the network. For instance, an attacker could manipulate a transaction between person A and person B, allowing them to fraudulently transfer cryptocurrency from one account to another. To prevent these types of attacks, various security measures can be implemented.

Multi-Chain Networks

The first way networks can prevent these types of attacks is by implementing a multi-chain network. This refers to a network structure in which multiple chains in one network operate in parallel [Figure 2]. To use a real-world comparison, multi-chain networks in blockchain are like a group of students who each have their own specialized skills and are working on a project together. One might be good at writing, another creative design, and other similar things. Each student might be responsible for a specific part of a project, but they all work towards a common goal.

Similarly, multi-chain networks consist of different "chains" that each have their own strengths and responsibilities. For example, one might be good at transaction security, another at transaction speed. These chains work together to make the network stronger.

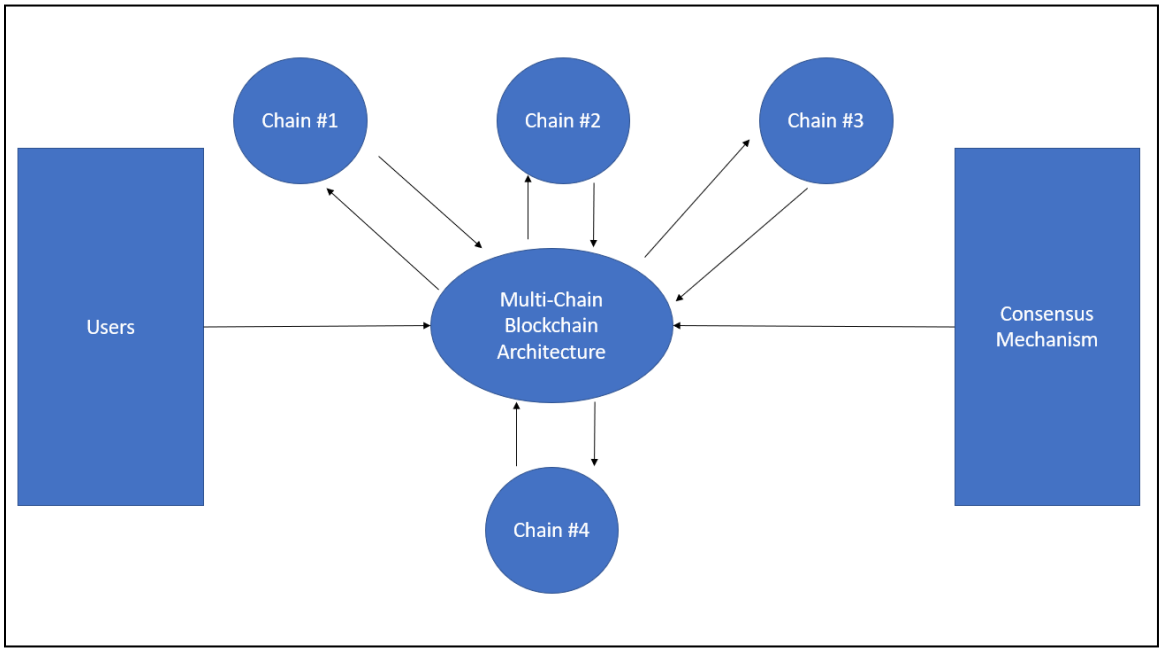

Figure 2: Conceptual Diagram Depicting a Multi-Chain Blockchain Architecture

Returning to its implications in preventing consensus attacks, each chain is responsible for managing a different part of the transaction. This means that any potential attacker would have a much more difficult time gaining a majority of the computing power. This is because they would need to gain control of more than one chain, which is a much harder task than taking over a single chain.

One example of this type of network is the Cosmos Network which utilizes multiple independent chains (called zones) working together all connected to a central point (hub) (*Cosmos Network - Internet of Blockchains*, n.d.). Aside from the security enhancements that this type of network provides, it also addresses other issues relevant in simple blockchain networks. For example, when dealing with a single chain that has many transactions, there can be issues in efficiency, scalability, and poor performance. These issues are alleviated because transactions are being performed in parallel as opposed to sequentially.

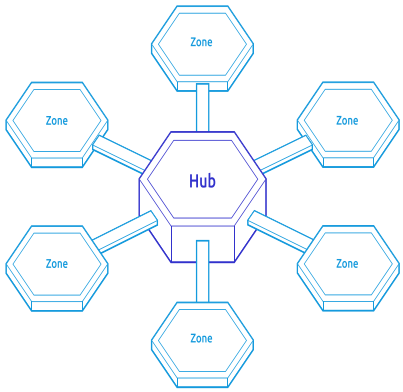

Figure 3: Cosmos Network Diagram

However, as with many solutions, there are drawbacks to using a multi-chain architecture. The most prevalent being the complexity of operating this type of architecture. Using multiple chains can be difficult to manage/coordinate and use together especially if each chain has different rules and protocols. Finally, while the usage of multiple chains might improve the security when it comes to consensus attacks, they can make the network more vulnerable to other types of attacks. This happens as a result of having more chains, and thus, more vulnerable points for an attacker to target, for example, a denial-of-service (DoS) attack.

Lastly, it should be noted that there are other multi-chain frameworks such as Polkadot [Figure 4] which uses a relay chain to connect multiple separate, independent chains (Wood, n.d.). Each framework tries to solve these scalability, efficiency, and security issues using different measures and so the decision usually comes down to application of the system.

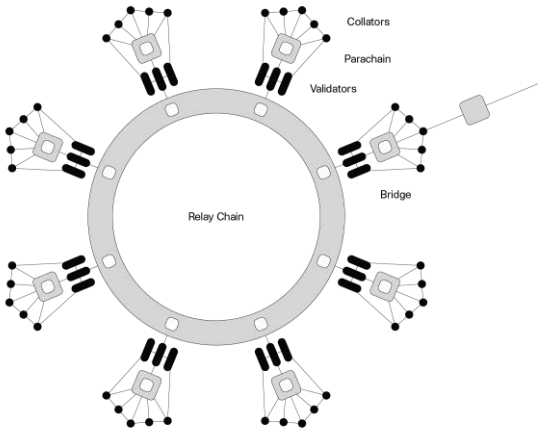

Figure 4: Polka-dot Conceptual Diagram

Proof-of-Work Consensus Algorithms

The second method of preventing consensus attacks is to employ a proof-of-work consensus algorithm within the network. Let's return to the group of students working together on the team project. Each student has a specific role, but their work is interdependent; they must coordinate together to make sure everything fits together properly.

In a proof-of-work consensus algorithm, each computer in the network is like a student working on a task. Instead of physical tasks, though, they are trying to solve complex mathematical problems that verify transactions. Once a computer solves a problem, it shares the solution with the rest of the network to be verified. This is similar to how the students share their completed work with the rest of the team for review and feedback. The first computer to solve the problem gets rewarded with a new cryptocurrency coin or token, which is like how the student who completes their task first might get recognition from the rest of the team.

How this works to enhance the security of the network is that it requires a computer to complete a certain amount of work before they are allowed to add to the consensus of the chain (Gupta & Mahajan, 2020). As highlighted earlier, this work is usually a computational puzzle that the miner must solve before adding to the chain. The amount of work that must be done prevents attacks since potential attackers will not be able to easily generate a large number of malicious solutions. Thus, it is much more expensive for an attacker to gain a majority of the computing power.

An additional feature of proof-of-work algorithms is that often times they are able to adjust the difficulty of the puzzles required to add to the chain. This has multiple uses. Firstly,

chains with less value are able to have easier algorithms to quickly add to the chain, and vice versa. Secondly, if there are issues with the network being too slow/fast in adding new proofs, the algorithm can adjust. For example, if it is noticed that the network is slowing down in creating proofs, the algorithm can make the puzzle easier to solve to increase the rate at which they are added. This is important as this proof defines the overall capacity for the system. Like lines or pages to write transactions on a ledger. If an attacker attempts to add new proofs too quickly, the algorithm can respond by increasing the difficulty of these proofs, thereby slowing down the attacker.

Of course, there are drawbacks to proof-of-work algorithms. Firstly, they are slow and resource intensive. Miners must invest a not insignificant number of resources into solving these puzzles and thus, the computing power required can be expensive. Additionally, because of the difficulty of the puzzles, they can be time consuming as well. For reference, a new block on the bitcoin network is solved about every 10-15 minutes. Although this doesn't seem too long, relative to computer processing power and considering that there are only about 2 million bitcoins left to mine, it is anticipated that it will take until about 2140 before all bitcoins are mined (*How Many Bitcoins Are There and How Many Are Left to Mine*, 2022).

Preventing Consensus Attacks: The Role of Network Auditing and Monitoring

Another suggested method towards protecting blockchain architectures against fraudulent activities involves using specialized software or third-party auditors to monitor the network. One of the major challenges of auditing and monitoring blockchain networks is that transactions are anonymous and the nature of the technology is decentralized. This makes it difficult to go to a central authority to ensure no illicit activities are taking place. While the technology to monitor these networks is still being developed, one solution has been proposed that utilizes collecting, storing, and analyzing data from a blockchain network (Bang & Choi, 2019).

The proposed solution is like a security system that is designed to detect illegal actions and potential attempts to gain control of the system. It does this by using advanced technologies like Apache Kafka and Apache Storm, which help process and organize data in real-time.

Imagine a busy store with lots of customers. Each customer has a shopping cart and is buying items at a very fast rate, more than a thousand transactions per second. The proposed system would be like a team of employees who are constantly watching the transactions to make sure there are no illegal actions or attempts to take over the store. To keep up with the high volume of transactions, the employees use advanced tools and strategies to process and collect data quickly and efficiently. One of the main challenges the system solves is reducing bottlenecks, which means that it helps prevent delays that might happen when too many transactions happen at once. The system is designed to process and collect data in parallel, meaning that it can handle lots of transactions at the same time without slowing down or causing problems.

Something to note with this technology, however, is that it fundamentally changes blockchain technology. That is, it takes it one step closer to being centralized. The monitoring system introduces an authority that oversees transactions and monitors them. While the computing power itself is still decentralized, the introduction of this system might raise concerns, especially for those who don't want their transactions stored in a database.

Another tool, or service, rather, that blockchain networks have to utilize are third-party entities monitoring the network. Companies like BlocWatch have formed in order to provide private monitoring of blockchain networks. Such companies provide analytics and reporting in order to ensure that networks are kept secure. Utilizing these SaaS technologies can prove beneficial for companies especially if they do not already have the existing infrastructure/investment/expertise to monitor their networks.

Unfortunately utilizing third-party oversight can suffer from similar issues surrounding the implementation of monitoring software on blockchain networks. The most prevalent being, again, adding a certain level of centrality to an otherwise decentralized network. In smaller networks, such as those used for a private company recording internal or fewer transactions, may not prove to be a major issue. However, in much larger networks, such as those used for cryptocurrencies, it may be a sore area. Additionally, although extremely rare, failures or any oversight in the monitoring company may prove catastrophic e.g., unauthorized users, data leaks, etc. Regardless, both methodologies can prove incredibly useful in the monitoring and prevention of consensus attacks, among others, in blockchain networks.

The Solution: A Hybrid Approach Combining Multiple Methods

Because of the many options available for preventing consensus attacks on blockchain networks, there is some debate as to what the best method of prevention is. Fortunately, many of these methods are not mutually exclusive. Therefore, the best method of prevention is a combination of the three methods mentioned earlier, along with any other options that might be available. By leveraging multi-chain architectures, proof-of-work algorithms, as well as monitoring and auditing systems, it is possible to create a robust and secure blockchain network. As an added benefit, many of these prevention methods also work to prevent other types of attacks such as denial-of-service (DOS) attacks, routing attacks, etc.

When considering different approaches to security in a blockchain network, it is also important to consider scalability and the ability to adapt to the future of the network. Everyday attacks on networks become more sophisticated and so network administrators must take the necessary steps to stay secure. The trend towards cheaper and more efficient computing power, as well as the impending emergence of quantum computing, which can solve blockchain proofs millions of times faster than current miners, makes adaptability crucial.

Ultimately, whoever is designing and implementing the network must decide what is right for their needs and implement those measures from the beginning. It is much easier to build a network with security measures in place rather than change it as it has already grown. Lastly, while blockchain networks are decentralized in nature, decisions still need to be made regarding how the network will be managed and secured. This responsibility falls on the group of individuals or entities that participate in the network. It's crucial that these groups work together to design and implement a secure network that serves the needs of all participants. By doing so,

the network can operate efficiently and securely, maintaining its decentralized architecture while still ensuring that decisions are made in the best interests of all stakeholders. Blockchain architectures do not form by themselves and do not exist in a vacuum, so the importance of designing a network with security in mind for both the users and network itself is crucial.

References

Bang, J., & Choi, M.-J. (2019). Design and Implementation of Storage System for Real-time Blockchain Network Monitoring System. *2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, 1–4. https://doi.org/10.23919/APNOMS.2019.8892967

BlocWatch—Crunchbase Company Profile & Funding. (n.d.). Crunchbase. Retrieved January 8, 2023, from https://www.crunchbase.com/organization/blocwatch-inc

Cosmos Network—Internet of Blockchains. (n.d.). Cosmos Network. Retrieved December 27, 2022, from https://cosmos.network

Debnath, S., Chattopadhyay, A., & Dutta, S. (2017). Brief review on journey of secured hash algorithms. *2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix)*, 1–5. https://doi.org/10.1109/OPTRONIX.2017.8349971

Gupta, C., & Mahajan, A. (2020). Evaluation of Proof-of-Work Consensus Algorithm for Blockchain Networks. *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 1–7. https://doi.org/10.1109/ICCCNT49239.2020.9225676

How many bitcoins are there and how many are left to mine? -. (2022, February 8). https://www.blockchain-council.org/cryptocurrency/how-many-bitcoins-are-left/

Lin, I.-C., & Liao, T.-C. (n.d.). *A Survey of Blockchain Security Issues and Challenges*. 7.

Sayeed, S., & Marco-Gisbert, H. (2019). Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. *Applied Sciences*, *9*(9), 1788. https://doi.org/10.3390/app9091788

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K.-K. R. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, *6*(2), 147–156. https://doi.org/10.1016/j.dcan.2019.01.005

THE IMPORTANCE OF BLOCKCHAIN MONITORING. (n.d.).

Wood, D. G. (n.d.). *POLKADOT: VISION FOR A HETEROGENEOUS MULTI-CHAIN FRAMEWORK*.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain technology overview* (NIST IR 8202; p. NIST IR 8202). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8202

Zhang, R., Xue, R., & Liu, L. (2020). Security and Privacy on Blockchain. *ACM Computing Surveys*, *52*(3), 1–34. https://doi.org/10.1145/3316481