International Journal of Advanced Smart Convergence Vol.12 No.1 41-52 (2023)
http://dx.doi.org/10.7236/IJASC.2023.12.1.41

IJASC 23-1-5

Comparative analysis of blockchain trilemma

Soonduck Yoo

Professor, Department of Management, Hansei University, Korea

Abstract

The purpose of this study is to review the proposed solutions to the Blockchain trilemma put forward by various research scholars and to draw conclusions by comparing the findings of each study. We found that the models so far developed either compromise scalability, decentralization, or security. The first model compromises decentralization. By partially centralizing the network, transaction processing speed can be improved, but security strength is weakened. Examples of this include Algorand and EOS. Because Algorand randomly selects the node that decides the consensus, the security of Algorand is better than EOS, wherein a designated selector decides. The second model recognizes that scalability causes a delay in speed when transactions are included in a block, reducing the system's efficiency. Compromising scalability makes it possible to increase decentralization. Representative examples include Bitcoin and Ethereum. Bitcoin is more vital than Ethereum in terms of security, but in terms of scalability, Ethereum is superior to Bitcoin. In the third model, information is stored and managed through various procedures at the expense of security. The application case is to weaken security by applying a layer 1 or 2 solution that stores and reroutes information. The expected effect of this study is to provide a new perspective on the trilemma debate and to stimulate interest in continued research into the problem.

Keywords: *Blockchain trilemma; Scalability; Decentralization; Security; Ethereum.*

1. Introduction

As various blockchain-based services continue to emerge, related research is being actively conducted to support and improve blockchain systems[1]. In particular, as a representative smart technology, blockchain has important elements such as security and scalability, which are the basis for securing sustainability. Therefore, blockchain technology is a representative infrastructure technology that contributes to society development.

Proponents of blockchain technology assert that the benefits of decentralization are equal to or greater than those of centralization[2,3,4]. The promise of the blockchain is that it solves security certain problems inherent to cloud-based systems. Therefore, many information systems are being converted from a cloud-based, centralized model to a blockchain-based paradigm[5]. However, blockchain-based systems have their own inherent issues to solve (e.g. information scalability). In fact, despite a substantial volume of re-search and experimentation, all approaches so far have turned out to be trade-offs.

This study intends to discuss the Blockchain Trilemma, a problem related to the balancing of scalability, decentralization, and security - the three most important elements of any information system. The term ‘trilemma’ refers to a widely-held view that decentralized networks can only provide two out of the above

Manuscript Received: December. 17, 2022 / Revised: December. 20, 2022 / Accepted: December. 22, 2022
Corresponding Author: koreasally@gmail.com
Tel:***－****－****   Fax: +82-31-450-9878
Professor, Department of Management, Hansei University, Korea

three benefits (decentralization, scalability and security) at any given time. In this paper, we discuss the obstacles to maximizing all three elements at once, and then review the proposed solutions to the Blockchain trilemma put forward by various research scholars. Finally, we draw conclusions by comparing the findings of each study.

2. Literature Review

2.1. Background of the Blockchain Trilemma

The Blockchain trilemma refers to the concept that the three factors of decentralization, scalability and security cannot be maximized simultaneously. Various studies are being conducted to determine ways for blockchain systems to overcome this limitation[6]. So far, implemented blockchains have been able to optimize only one or two of the three elements, with no chain successfully optimizing all three.

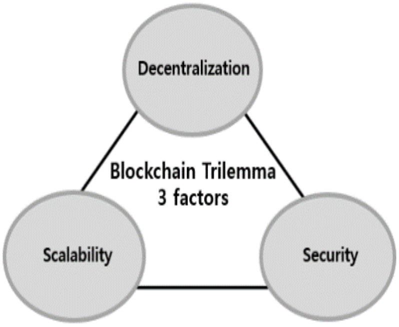


Figure 1. Blockchain trilemma - 3 factors

2.2. Blockchain Trilemma for Sustainability: Fundamentals

“Decentralization” describes a network consisting of autonomous small nodes, rather than a single large centralized server. Decentralization eliminates the role of intermediaries – a core benefit of blockchain technology. A decentralized structure distributes profits and decision power amongst its participants, and proceeds on the basis of their consensus[7,8,9].

“Scalability” determines how quickly a blockchain network can process transactions as the size of the network increases (in terms of users, data throughput, and number of transactions). Maximizing scalability can positively affect security, as well as make the network more centralized as the network expands[10].

“Security” means that data and/or programs are protected from unauthorized or malicious users gaining access. The three elements of the Blockchain trilemma interrelate as follows.

For a given level of scalability, decentralization and security are inversely proportional. In other words, when there are many nodes on the system (decentralization), the transaction processing speed is slow.

$$\textbf{Decentralization} \propto \frac{\textbf{1}}{\textbf{Scalability}} \tag{1}$$

For a given level of decentralization, scalability and security are proportional[11].

$$\textbf{Scalability} \ \alpha \ \textbf{Security} \tag{2}$$

When decentralization is lowered, the blockchain formation time becomes faster, and not only security but also scalability increases. As long as the above relationships hold, it is impossible - even in theory – to maximize all three elements at the same time, and they are fundamentally complementary. To strengthen one element, you must compromise at least one of the other two.

3. Methodology

This paper explains the concept and fundamentals and how to approach to solve the Blockchain Trilemma, as well as the research method and data of the article. After analyzing each proposed classification and case, a classification system that can interpret the Blockchain trilemma from a new perspective was suggested.

For this purpose, this study used the case study analysis method. After classifying the cases of the Blockchain trilemma into 1) Limited Validator Solutions, 2) Layer 1 solutions, and 3) Layer 2 solutions, each related case was investigated.

After analyzing each related case, features were extracted and differences were investigated. Through this, considering the characteristics of each classification method, the Blockchain trilemma was reinterpreted by classifying it into 1) Compromising decentralization, 2) Compromising scalability, and 3) Compromising security.

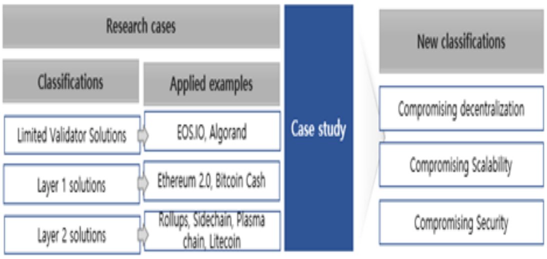


Figure 2. Research method

Although there are various protocols used in blockchain, in this study, for the reader's understanding, only the most representative examples were followed to explain the approach below the classification method. This study supports to interpret the sub problem from a different perspective by reinterpreting the blockchain trilemma.

4. Analysis

4.1. Analysis Outline

Efforts to solve the Blockchain trilemma are continuous, and a review of some of the various methods to solve the Blockchain trilemma follows.

MIT professors Nancy Lynch and Seth Gilbert proposed in 2002 that, CAP Theory proves that it is impossible to provide reliable atomic consistency data when the network is partitioned, while it is feasible to achieve any two of the three properties: consistency, availability, and partition-tolerance[12, 13]. CAP (standing for Consistency, Availability, Partition Tolerance) proposes that it is impossible to achieve the three characteristics of consistency, availability, and partition tolerance in a distributed system simultaneously.

"Consistency" means that all nodes should store the same data for the same item at the same time.

In a blockchain network, Security is a stronger concept than Consistency, as a system in which there is a discrepancy of data between nodes is not only not consistent, but also insecure.

"Availability" means that data should be readable and writable for all users, and even if one node fails, other nodes should not be affected. In addition, scalability typically refers to the ability to perform "read" and "write" operations quickly. In the context of blockchain, scalability refers specifically to the number of transactions that can be processed per second. Since an unavailable blockchain system can nevertheless achieve scalability,

scalability is therefore more important than availability.

“Partition tolerance” means that a system should function well even in a situation where multiple clusters exist and communication between these clusters is impaired due to a failed connection. In a distributed environment, it is impossible to guarantee that no nodes will fail. In other words, decentralization inevitably leads to the emergence of clusters.

According to Paul Dunphy(2022), he made a case study of Hyperledger Indy - an open-source technology designed to facilitate decentralized identity - and conduct two empirical experiments to measure the latency of more than 45,000 transactions in the naturalistic environment of Amazon Web Services.[11] Finally, he suggested that while Hyperledger Indy captures data useful to underpin a decentralized identity scheme, the resulting limitations placed on scalability may place constraints on properties of security and decentralization.

Despite the conclusion that the trilemma is an intractable problem, researchers are nonetheless exploring ways to overcome the challenge.

Limited Validator solutions (EOS, Algorand), as well as Layer 1 and Layer 2 solutions (applied in the form of validator restrictions) have been proposed as potential solutions to the trilemma[14].

Layer 2 solutions use Sidechains, Rollups, Plasma Chains, Channels and are being announced in connection with projects that include Ethereum 2.0, Bitcoin Cash, and Lite-coin. We discuss these developments in detail below. Table 1 sets out the solutions that have appeared so far.

Table 1. Solutions to the Blockchain trilemma proposed so far

Division		Contents
Limited Validator Solutions	Concept	· This configuration is applied based on the validator limit when configuring the blockchain. · When there are many validators, security is strengthened, but scalability (storage speed) decreases, and when the number of validators is small, scalability increases.
	EOS	· EOS.IO is a blockchain architecture designed to facilitate the vertical and horizontal scalability of decentralized applications by creating an operating system-like structure on which applications can be built. · The EOS.IO blockchain uses DPoS (Delegated Proof of Stake), a model that works by limiting validators. · Comparing Ethereum and EOS, we can see that Ethereum is both slower and more secure, while EOS is much faster and more centralized.
	Algorand	· The new Pure Proof of Stake (PPoS) method is built on the Byzantine consensus, and the influence each token holder has depends on the stake they hold. Crucially, the protocol randomly selects users regardless of size of stake.
Layer 1 solutions		- The system is classified into several layers, such as Layer 0, 1, 2, etc., and the relationship between Layer 0 and Layer 1 is explained. A “Layer 1” either L1 solution is a protocol that creates and approves blocks based on the blockchain consensus algorithm. ‘Layer 0’ is a protocol that defines a new incentive model for how to network between blocks or nodes below Layer 1. - Solves by ‘improving the consensus protocol’ (e.g. PoW -> PoS). - A method called ‘sharding’ separates validators into small groups so that each group can process different transactions simultaneously. - Example protocols include Bitcoin Cash, Litecoin, and Ethereum.
Layer 2 solutions	Concept	· A solution developed to scale Layer 1 solutions. · A separate layer designed to solve the scalability problem of (for example) the Ethereum 2.0 main-net. · An L2 aims to execute transactions as quickly and inexpensively as possible instead of relying on the security and data availability of the L1. · As a network technology that works on top of the underlying blockchain protocol to improve scalability and efficiency, it has seen notable growth in recent years. Among them, it is the most efficient way to overcome the scalability problem of PoW networks. · Bitcoin’s Lightning Network is an example of a Layer 2 solution scheme.

Rollups	· Rollups are divided into Zero-Knowledge (ZK) rollups and Optimistic rollups. · ZK-rollups are a Layer 2 scalability solution that allow blockchains to validate transactions faster while also ensuring that gas fees remain minimal. · Optimistic rollups sit in parallel to the main chain on Layer 2. · The difference between ZK-rollups and Optimistic rollups is that the former have the advantage of being significantly faster, as the validation occurs on the mainchain rather than on the sidechain. Because mainchain validation occurs almost instantly, ZK Rollups are both faster and more scalable.
Sidechain	· Blockchain-adjacent transaction chains used for large batch transactions. · Connected to an L1 (e.g. Ethereum) by means of a 2-way peg (2WP). · Use a consensus mechanism independent of the main chain. · Sidechain transactions are publicly recorded on the ledger. · Used as a way to increase speed and scalability without affecting the main chain and other sidechains, even if the sidechain itself is compromised.
Plasma chain	A plasma chain is a separate blockchain that is anchored to the main Ethereum chain, and uses fraud proofs (like Optimistic rollups) to arbitrate disputes.
Channels	A channel is a private communication pathway between two or more members of a Hyperledger Fabric network on Amazon Managed Blockchain.

4.2. Limited Validator Solution

Increasing centralization will increase transaction speed, but security strength may be compromised. Nevertheless, several studies have proposed ways to improve processing speed and scalability.

The consensus algorithm used by the EOS is known as Delegated Proof of Stake (“DPoS”). Those who hold tokens on the platform can select block producers by means of a continuous approval voting system. Anyone can put themselves forward as a block producer, and if they are able to persuade token holders to vote for them, they will be given the opportunity to create blocks.

Another representative example is Algorand, which partially solves the trilemma by adopting a Pure Proof of Stake (“PPoS”) consensus algorithm.

A study by Amani Altarawneh, Tom Herschberg, Sai Medury, Farah Kandah, Anthony Skjellum(2020) argues that, based on this taxonomy of tradeoffs, we are able to discern the types of consensus algorithms that work well within the application area(s) for a given distributed system[15].

They found that a dichotomy of algorithms between leader-based and voting-based consensus algorithms emerges from this taxonomy.

4.2.1. EOS.IO

EOS.IO is a blockchain architecture designed to enable vertical and horizontal scalability of decentralized applications by creating an operating system-like structure on which applications can be built. The software provides accounting, authentication, database, asynchronous communication, and application scheduling capabilities across multiple CPU cores or clusters. The resulting technology is a blockchain architecture that eliminates user fees and allows for quick and easy deployment & maintenance of decentralized applications in the context of a controlled blockchain.

EOS.IO operates as both a base layer blockchain and a smart contract platform. The protocol works like a decentralized operating system and enables the deployment of industrial-scale applications through a decentralized autonomous enterprise model. The consensus algorithm is based on DPoS, which means that those who hold tokens on the platform can choose block producers via a continuous approval voting system, and the block-producing role is open to anyone who can secure the required votes. Cryptocurrencies are scalable in line with the speed of the transaction process. EOS is much more centralized than Bitcoin or Ethereum[16].

The EOS.IO consensus algorithm respects Byzantine Fault Tolerance (BFT) by allowing any block to be

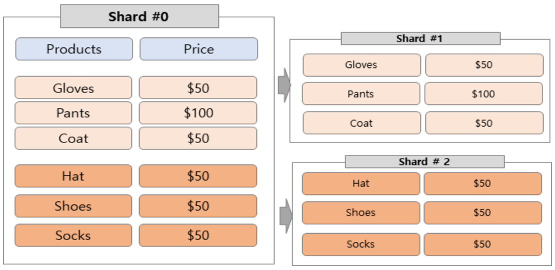
signed unless another producer signs a block with the same timestamp or the same block height.
When 15 producers sign a block, it is considered irreversible. If we compare Ethereum and EOS, we can see that Ethereum is much slower and more secure, while EOS is much faster and more centralized[17].

4.2.2. Algorand

The Algorand algorithm randomly selects a validator from all token holders to perform validation. The network uses an algorithm that automatically selects the next group of nodes to add blocks to, and this approach allows all users to be selected by the system, thus maintaining decentralization. The fact that no one knows who the next validator will be keeps the system secure.
A persistent question in validation based consensus systems is whether a system or entity can be trusted to guarantee random selection. Algorand offers a partial solution to the Blockchain trilemma by adopting a new Pure Proof of Stake ("PPoS") consensus algorithm.
Algorand selects randomly from all token holders. The network relies on an algorithm that automatically picks the next group of nodes that are eligible to add blocks.
PPoS is built on the Byzantine consensus model, and the influence each token holder has depends on the stake they hold.
The fact that any online user can (in theory) be selected offers a number of advantages for decentralized networks, by increasing the level of decentralization of the blockchain and ensuring system stability.
According to Mauro Conti, Ankit Gangwal and Michele Todero in their paper "Blockchain trilemma Solver Algorand has Dilemma Over Undecidable Messages", it is possible to slow down the message validation process on honest nodes, which eventually forces them to select default values on the consensus, leaving the targeted nodes behind in the chain as compared to the non-attacked nodes[18]. Ultimately, Algorand has not succeeded in solving the blockchain trilemma, but it has succeeded in designing a more advanced approach to the problem.

4.3. Layer 1 Solutions

One of the optimal solutions to the blockchain scalability problem is the development of a Layer 1 solution. Layer 1 solutions add utility to a native blockchain to optimize its performance. In other words, they improve the underlying protocol to make the entire system more scalable by design.
An example of a Layer 1 solution is an approach known as 'Sharding'. Sharding means splitting the L1 blockchain into multiple chains or shards. Nodes only need to verify and store the transactions in the shards to which they belong, resulting in reduced network burden and increased efficiency[19]. Transactions are sent to different shard groups according to various rules as shown in the figure below. Figure 4 describes the shard structure.



Shard #0

Products	Price
Gloves	$50
Pants	$100
Coat	$50
Hat	$50
Shoes	$50
Socks	$50

Shard #1

Gloves	$50
Pants	$100
Coat	$50

Shard # 2

Hat	$50
Shoes	$50
Socks	$50

Figure 3. Shard Structure

Example protocols that use Layer 1 solutions are Ethereum 2.0, Bitcoin Cash, and the case studies discussed as follows.

4.3.1. Ethereum 2.0

Ethereum 2.0 is a generic term for a series of upgrades currently in process to make the Ethereum blockchain more scalable and sustainable. The creator of Ethereum, Vitalik Buterin, has argued that in Ethereum 2.0 it will be possible for a blockchain to secure scalability and decentralization at the same time. This is because, if the Ethereum 2.0 structure is rebuilt based on a Proof of Stake consensus approach and sharding technology, transactions can be processed in real time.

Buterin has planned to transition from PoW to PoS from the very beginning of the project's launch in order to ensure continued competitiveness[20]. Ultimately, Ethereum will be reborn as a modular blockchain; that is to say, a blockchain composed of multiple layers, with each layer handling execution, security, and data availability tasks respectively to streamline data processing efficiency and maximize productivity and hence scalability. Figure 5 shows Ethereum 2.0 Architecture

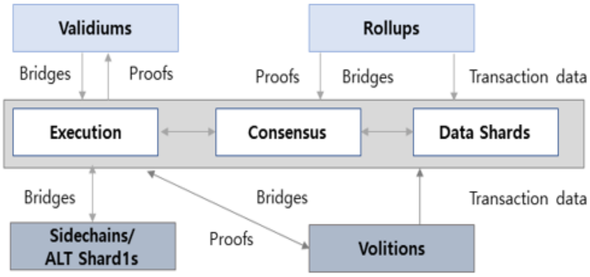


Figure 4. Ethereum 2.0 Architecture

4.3.2. Bitcoin Cash

Altcoins also provide examples of ways to solve the blockchain trilemma. Bitcoin Cash was conceived out of the view that transaction speeds on the Bitcoin blockchain were constrained by the limitations on "the size of the block and the number of transactions it can contain". The solution was to increase the size of the block by 2 - 8 times compared with the status quo.

Due to limited scalability, however, there is a danger that if the existing structure remains more or less unchanged, and the number of transactions and nodes increases in the future, the PoW algorithm will be unable to distribute mining power owing to the concentration of capital arising from the centralization of resources.

4.4. Layer 2 Solutions

A Layer 2 is an independent framework or additional layer, which processes data outside the main blockchain to increase its scalability.

The goal of a Layer 2 solution (also known as an "off-chain" solution) is to directly address the transaction speed and scalability issues of major cryptocurrency networks. It is thus possible to compensate for the scalability problems of Layer 1, such as high gas costs and slow transmission speeds. Layer 2s have essentially solved the problem of vertical scalability by essentially relocating large numbers of transactions off-chain.

4.4.1. Rollups

Layer 2 solutions can be classified into Rollups, Sidechains, Plasma chain and Channels. Rollups are divided into ZK-rollups and Optimistic rollups. Zero-Knowledge rollups or ZK-rollups are a Layer 2 scalability solution that allow blockchains to validate transactions faster while also ensuring that gas fees remain minimal. Optimistic rollups sit in parallel to the main chain on Layer 2.

4.4.2. Sidechain

A “Sidechain” is a separate blockchain that is connected to the Layer 1 blockchain, used for processing large-batch transactions. The asset movement is recorded and processed on the sidechain, and only the result is uploaded to the Layer 1 blockchain. This increases the rate of transactions per second (TPS) and facilitates the exchange of cryptographic assets.

“Off-chain computation” runs the code for Layer 1’s smart contract operation in an off-chain locale called the computation network, and sends only the resulting value of the code’s execution to the Layer 1 blockchain. It is therefore another method of improving TPS.

4.4.3. Plasma Chain

A plasma chain is a separate blockchain that is anchored to the main Ethereum chain, and uses fraud proofs (like Optimistic rollups) to arbitrate disputes. A channel is a private communication pathway between two or more members of a Hyperledger Fabric network on Amazon Managed Blockchain. Examples of this include Bitcoin and Ethereum.

4.4.4. Litecoin

Litecoin is based on the concept that Bitcoin's transaction speed is slow because of the need to store large amounts of transaction data. The Lightning Network is used to register all transaction details off-chain, synthesizing transaction details and uploading only the final result to the main-net. Trust is secured using multi-key and time-locking contracts. Because no transactions are made on the blockchain, waiting time for approval is eliminated, and costs are lower because miners do not have to pay fees. However, the Lightning Network technology applied to Litecoin has an important limitation in that it cannot solve the decentralization problem, as it requires the participation of a third party.

5. Results and Discussion: Comparative Analysis and Implications

5.1. Comparison between Layer 1 and Layer 2 Solutions

Previously, Layer 1 and Layer 2 cases were discussed. Through this, the difference between Layer 1 and Layer 2 in this study will be discussed as follows.

Layer 2 solutions can be classified into Rollups, Sidechains, Plasma chains and Channels. Among L2 solutions, the ZKrollups are the most popular technical solution. A Layer 2 solution is quite literally a separate layer designed to solve the scalability problem of the main-net, making it possible to execute transactions as quickly and inexpensively as possible.

The purpose of a Layer 1 is to expand the independent ecosystem, including dApps and Layer 2 solutions, by improving processing speed and reducing fees. Figure 3 shows the difference between Layer 1 and Layer 2. Therefore, comparing Layer 1 and Layer 2, we see that L2 solutions weaken security in comparison to L1 based approaches.

Table 2. Comparison between Layer 1 and Layer 2 solutions

Division	Layer 1 solution	Layer 2 solution
Concept	Independently operated blockchain	A separate network connected to the existing blockchain
Goal	Make it possible to expand the independent ecosystem (e.g. dApps)	Improved processing speed, lower fees

Features	Block generation, proof, transaction processing, etc.	Only handles transaction processing (with the rest handled by L1).

In the future, it is expected that most transactions will be executed on Layer 2, and the Ethereum main-net will operate only on the consensus and data availability layers. Accordingly, it is predicted that most blockchains, including Ethereum, will follow a modular blockchain structure with groups of tasks are distributed by layer.

5.2. Findings: Three Models for Compromise

Already we mentioned that blockchain cannot fulfill the three factors of scalability, decentralization, and security, as at least one must be compromised. Table 3 explains instances where scalability, decentralization or security are compromised

Table 3. Compromised scalability, decentralization, or security

Division			Contents
Examples of compromises on decentralization	Features		- By accepting a certain measure of centralization, the transaction processing speed is improved, but the strength of security may be weakened. - (Algorithm) Apply Validator Limit solution.
	Cases	Algorand	- Adopting a new Pure Proof of Stake (“PPoS”) consensus algorithm partially solves the trilemma.
		EOS	- Delegated Proof of Stake (DPoS) consensus algorithm solves the problem of decentralization and scalability (a method of electing 21 block producers and trusting them to operate the blockchain). - Democratic decision-making system (21 nodes capable of fast computation). - As authority increases, it is possible to move away from decentralization.
Cases of Compromising Scalability	Features		- Developed with a focus on decentralization and security. - Delay in speed when transactions are connected in blocks (resource allocation time according to the structure of the blockchain platform, such as block generation cycle and data size). - The problem of delay in the speed required for the consensus process between consensus nodes (a problem inherent to the network itself owing to the consensus algorithm and network scalability requirements). - (Algorithm) Layer 1, Layer 2 solutions.
	Cases	Bitcoin	- High decentralization and security but low scalability. - Low processing speed with 7 Transactions Per Second. - Transaction abandonment and scalability are the biggest disadvantages of Bitcoin.
		Ethereum	- Only about 20 dApp transactions on the ETH (Ethereum) platform can be processed per second. - Used not only as a means of payment, but also in a wider field (dApp).

Cases of Compromising Security	Features		- Focus on decentralized and improved scalability rather than security. - (Algorithm) Layer 1, Layer 2 solutions.
	Cases	Ethereum 2.0	- Ethereum 2.0 applies Layer 2, and in this environment the security aspect is weakened.

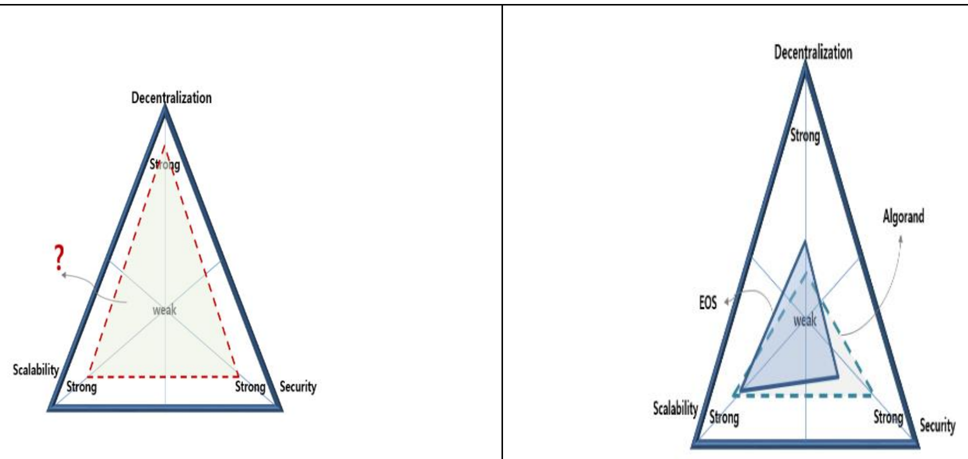
The first model compromises decentralization. By partially centralizing the network, transaction processing speed can be improved, but security strength is thereby weakened. Examples of this include Algorand and EOS.

The second model recognizes that inc reased scalability causes a delay in speed when transactions are included in a block, reducing the efficiency of the system. Reducing the burden of scalability makes it possible to enhance decentralization. The reasons why Ethereum has better scalability than Bitcoin are presented in the table below(Table 2).

Table 2. The reason Ethereum has better scalability than Bitcoin

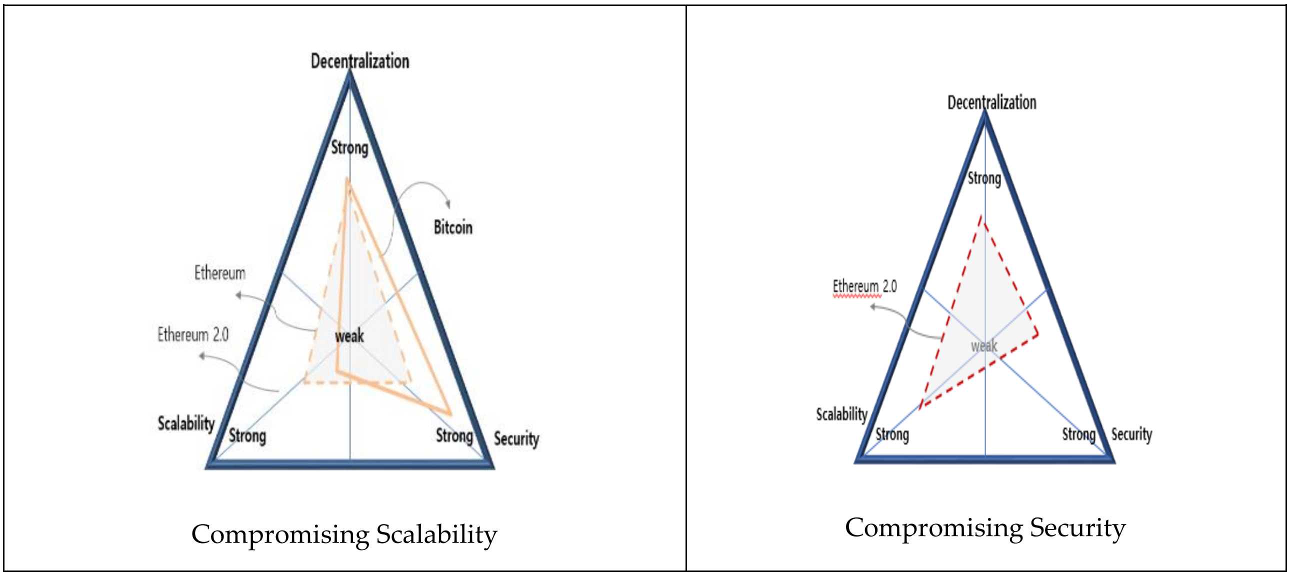
Division	Contents
Higher transaction processing capacity	Ethereum has a higher transaction processing capacity than Bitcoin. While Bitcoin can process only about 7 transactions per second, Ethereum can process about 15 transactions per second.
Higher flexibility	Ethereum supports smart contracts, which provide higher flexibility. Smart contracts are self-executing contracts that automatically execute when certain conditions are met. Ethereum's smart contracts can be used to run various applications on the blockchain.
Faster block creation	Ethereum creates blocks every 15 seconds, while Bitcoin creates blocks every 10 minutes. The faster block creation speed of Ethereum allows for faster transaction processing and quicker response times.

The third model is to deploy a Layer 1 or 2 solution, whereby information is stored and managed through various procedures that weaken security. The following figure describes the application cases for each related solution in terms of three elements, decentralization, scalability and security.



The blockchain trilemma solution what we want

Compromising decentralization



Compromising Scalability

Compromising Security

Figure 5. Comparing Cases of Compromise

In the figure above, the upper left represents the desired solution to the blockchain trilemma, which enhances decentralization, scalability, and security simultaneously. As shown in the upper right figure, Algorand's security is superior to EOS because Algorand randomly selects the node that determines consensus, while EOS relies on a designated selector. In the lower left figure, Bitcoin is stronger than Ethereum in terms of security, but Ethereum surpasses Bitcoin in scalability.The lower right figure shows that Ethereum 2.0 can be considered a compromise between security and scalability.

6. Conclusions and further recommendation

This study examines the cases and potential solutions for the blockchain trilemma and finds that the existing models compromise either scalability, decentralization, or security.

The first model compromises decentralization by partially centralizing the network to improve transaction processing speed, but this weakens security. Examples of this model include Algorand and EOS.

The second model recognizes that scalability causes a delay in transaction processing speed when transactions are included in a block, reducing the efficiency of the system. Reducing the burden of scalability can enhance decentralization.

The third model is to apply a Layer 1 or 2 solution whereby information is stored and re-routed, which weakens security. An L2 solution is a separate layer designed to solve the scalability problem of the main-net, making it possible to execute transactions quickly and inexpensively. In the future, it is expected that most transactions will be executed on Layer 2, and the Ethereum main-net will only operate on the consensus and data availability layers. Consequently, most blockchains, including Ethereum, will likely have a modular blockchain structure whereby groups of tasks are distributed by layer.

The expected impact of this study is to stimulate interest in further research and provide a structured view of the current state of the trilemma debate.

Acknowledgments

The authors would like to express their heartfelt gratitude to Mathew Jackson for advising

Funding

This research received no external funding.

Author Contributions

All author contributed equally all of the work. The author has read and agreed to the published version of the manuscript.

Institutional Review Board Statement: Not applicable.
Informed Consent Statement: Not applicable
Data Availability Statement: Not applicable.
Conflict of Interest: The author declares no conflict of interest.

References

1. Yoo Seong-min, A Study on the Consensus Algorithm Design Process. Journal of the Korean Telecommunications Society (Information and Communication) 37, no. 3, 13-20, 2020.
2. Yaga, Dylan, Peter Mell, Nik Roby, and Karen Scarfone, Blockchain technology overview. arXiv preprint arXiv:1906.11078 (2019).
3. Monte, Gianmaria Del, Diego Pennino, and Maurizio Pizzonia, Scaling blockchains without giving up decentralization and security: A solution to the blockchain scalability trilemma. In Proceedings of the 3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems, pp. 71-76. 2020.
4. Jongdae Park, Blockchain Internet Technology, Journal of the Korean Association for Tele-communications (Information and Communication) 36, no. 1, 17-22, 2018.
5. Liu, Xuanzhe, Sam Xun Sun, and Gang Huang, Decentralized services computing paradigm for blockchain-based data gov-ernance: Programmability, interoperability, and intelligence. IEEE Transactions on Services Computing 13, no. 2, 343-355, 2019.
6. Soonduck, Yoo. Blockchain-based Consensus Algorithm Study. Journal of the Korean Internet and Broadcasting Associa-tion 19, no. 3, 25-32, 2019.
7. Soondcuck Yoo, and Ki-Heung Kim, A study on improvement measures for the spread of blockchain-based services, Journal of the Korean Society for Internet and Broadcasting Communication 18, no. 1, 185-194, 2018.
8. Soondcuck, Yoo, A study on consensus algorithm based on Blockchain. The Journal of the Institute of Internet, Broadcasting and Communication 19, no. 3, 25-32, 2019.
9. Aiyar, Kamalani, Malka N. Halgamuge, and Azeem Mohammad, Probability distribution model to ana-lyze the trade-off between scalability and security of sharding-based blockchain networks. In 2021 IEEE 18th Annual Consumer Communi-cations & Networking Conference (CCNC), pp. 1-6. IEEE, 2021.
10. Cohen, Lewis Rinaudo, Lee Samuelson, and Hali Katz, How securitization can benefit from blockchain technology. The Journal of Structured Finance 23, no. 2, 51-54, 2017.
11. Gilbert, Seth, and Nancy Lynch. "Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web ser-vices." Acm Sigact News 33, no. 2, 51-59, 2002
12. Gilbert, Seth, and Nancy Lynch, Perspectives on the CAP Theorem. Computer 45, no. 2 (2012): 30-36.
13. Dunphy, Paul, A Note on the Blockchain trilemma for Decentralized Identity: Learning from Experi-ments with Hyperledger Indy. arXiv preprint arXiv:2204.05784, 2022.
14. Gilad, Yossi, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich, Algorand: Scaling byzantine agree-ments for cryptocurrencies. In Proceedings of the 26th symposium on operating systems principles, pp. 51-68. 2017.
15. Altarawneh, Amani, Tom Herschberg, Sai Medury, Farah Kandah, and Anthony Skjellum, Buterin's scalability trilemma viewed through a state-change-based classification for common consensus algorithms. In 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0727-0736. IEEE, 2020.
16. Dernayka, Iman, and Ali Chehab. Blockchain development platforms: Performance comparison. In 2021 11th IFIP Interna-tional Conference on New Technologies, Mobility and Security (NTMS), pp. 1-6. IEEE, 2021.
17. https://finance.yahoo.com/news/eos-vs-ethereum-blockchain-comparison-150018067.html?
18. Conti, Mauro, Ankit Gangwal, and Michele Todero, Blockchain trilemma solver algorand has dilemma over undecidable messages. In Proceedings of the 14th International Conference on Availability, Reliability and Security, pp. 1-8. 2019.
19. Zhou, Qiheng, Huawei Huang, Zibin Zheng, and Jing Bian., Solutions to scalability of blockchain: A survey. Ieee Access 8,16440-16455, 2020.
20. Lee, Eun-Young, Nam-Ryeong Kim, Chae-Rim Han, and Il-Gu Lee. Evaluation and Comparative Analysis of Scalability and Fault Tolerance for Practical Byzantine Fault Tolerant based Blockchain. Journal of the Korea Institute of Information and Communication Engineering 26, no. 2, 271-277, 2022.