Understanding Blockchain Trilemma, Causes and Solutions

Monu Chaudhary, Suman Bhunia
Department of Computer Science and Software Engineering, Miami University, Oxford, Ohio
Email: chaudharymonu45@gmail.com, bhunias@miamioh.edu

***Abstract*—With extensive research and development in blockchain technology, the concern about scalability, security, and decentralization is still evident. Blockchain trilemma describes that it is realistically impossible to simultaneously achieve a high level of decentralization, security, and scalability. However, new developments in the sector of blockchain are making progress in simultaneous achievement of these three aspects. Layer 1 blockchain is the base level of blockchain network architecture. It includes blockchain networks like Bitcoin, Ethereum, etc. However, the Layer 1 blockchain network faces scalability issues. Layer 2 blockchain is a network built on top of Layer 1 blockchain to help eliminate scalability issues. This paper presents a comparative analysis of Layer 1 and Layer 2 blockchain networks and different approaches to solving the blockchain trilemma in Layer 1 and Layer 2 blockchain networks. From the study, we found that Layer 2 blockchain networks are easier and faster to implement.**

***Index Terms*—Blockchain, Blockchain Trilemma, Decentralization, Scalability, Security**

I. Introduction

Blockchain technology has brought revolutionary changes in the digital landscape by introducing immutable, distributed, and decentralized append-only databases. The data in blockchain is stored in the form of blocks after performing some cryptography algorithms. The units of data stored in a blockchain network are called transactions. Each transaction in a blockchain network is verified by either of the two consensus mechanisms: 1) Proof of Work (PoW) [1] or 2) Proof of Stake (PoS) [2].

Proof of Work, commonly associated with the pioneer blockchain, Bitcoin, relies on a computationally intensive process where miners compete to solve complex mathematical puzzles [3]. This process validates transactions and ensures the security and immutability of the blockchain through the expenditure of computational power and energy. PoW has garnered attention for its robustness but has also faced scrutiny due to its energy-intensive nature and scalability challenges.

On the other hand, Proof of Stake offers an alternative consensus mechanism that addresses some of these concerns. PoS relies on validators who are chosen to create new blocks and validate transactions based on the amount of cryptocurrency they 'stake' or lock up as collateral [4]. This approach is more energy efficient and has the potential for scalability, making it a better choice for newer blockchain projects.

However, as blockchain technology evolves, it faces a significant challenge known as the *Blockchain Trilemma*. Blockchain trilemma means that blockchain can only achieve two of three properties - *security, decentralization, and scalability* [5], [6]. Some blockchain projects circumvent the trilemma by compromising on one of the three elements. Often, scalability is compromised to build a highly secure and decentralized system [7]. However, RD on blockchain networks has led to innovative ideas like sharding, side-chains, state channels, etc., to address the trilemma problem [7].

Numerous efforts have been made to address the scalability issues within blockchain networks. Various surveys and literature reviews delve into the intricacies of the blockchain trilemma and its potential solutions. For example, the research paper by [5] provides a detailed discussion of layer 1 and layer 2 solutions. Nevertheless, it fails to provide an analysis of these solutions. On a related note, the survey conducted by [8] is a commendable work, offering a comprehensive explanation of layer 2 solutions in a variety of categories and the associated challenges. However, it is important to emphasize that the scope of this survey excludes layer 1 blockchain solutions. Similarly, the study by [9] conducts a thorough analysis of layer 1 solutions but regrettably neglects to address layer 2 solutions.

The primary objective of our paper is to provide a comprehensive overview of the *blockchain trilemma*, shedding light on the underlying factors contributing to the complexity. In addition, we embark on a thorough exploration of layer 1 and layer 2 solutions designed to tackle the issue along with the advantages and disadvantages inherent in these diverse approaches. Layer 1 solutions emphasize improving the underlying mechanisms of a blockchain network, including consensus algorithm, data structure, network, etc. On the other hand, layer 2 solutions are built on top of layer 1 through off-chain methods, including side-chains, cross-chains, etc.

This paper investigates the main concerns of the blockchain trilemma and highlights some major technological advances to resolve the problem. The main contributions of the paper are:

- Provide a layman's guide to understanding blockchain trilemma, its causes, and solutions.
- Compile different layer 1 and layer 2 solutions and compare them based on different criteria.
- Display how Layer 1 and layer 2 solutions impact transaction rates and blockchain price.

From our analysis, we found that Layer 2 blockchain networks offer notable advantages in terms of ease and speed of implementation. Unlike traditional Layer 1 solutions, which often require significant developmental efforts and time, Layer 2 solutions are more streamlined and can be integrated more swiftly. They are based on the existing Layer 1 blockchain, reducing the need for extensive reconfiguration. In turn, this expedites the deployment of scaling solutions, making Layer 2 an attractive choice for many blockchain projects seeking to enhance their performance and throughput efficiently.

The remainder of this paper is structured as follows: Section II introduces various architectural constraints contributing to the scalability issues associated with the blockchain trilemma. In Section III, we elaborate on the components of the blockchain trilemma and provide an overview of its underlying causes. Subsequently, in Sections IV-A and IV-B, we present recent solutions to the scalability issue in blockchain, categorized into layer 1 and layer 2 approaches. In Section V, we examine the outcomes of these scalability solutions, presenting our findings through graphs and tables. Lastly, in Section VI, we offer a summary of our research.

II. Blockchain Architectures that Lead to Trilema

In this section, we discuss the blockchain network architecture that leads to the blockchain trilemma problem.

A. Single Chain Layer 1 Blockchain Network

A single chain layer 1 blockchain network uses a linear chain of blocks to record and validate transactions [10]. Each block contains a set of transactions cryptographically linked to the previous block, forming a chain of blocks that traces back to the network's first block (also known as the Genesis block). This type of blockchain is often called a "first generation" blockchain, as it was the first to be developed.

In a single-chain layer blockchain 1, all transactions are recorded and validated on the same chain, and there is no mechanism to create additional chains or layers to increase scalability [10]. This can make it difficult for a single chain layer 1 blockchain to handle a large volume of transactions, especially compared to more recent blockchain technologies that use multiple chains or layers to improve scalability. Despite this limitation, single-chain layer 1 blockchains are still widely used and are the foundation for many popular cryptocurrencies, such as Bitcoin and Ethereum.

B. Proof of Work (PoW) Consensus Mechanism

Figure 1 shows the proof of work consensus mechanism procedure. PoW is a consensus mechanism some blockchain networks use to validate transactions and add new blocks to the chain. In a PoW system, nodes (also known as miners) compete to solve a complex mathematical problem, and the first node to solve the problem is allowed to add a new block to the chain [1]. This process is known as mining, which requires miners to perform a significant amount of computational work, hence the name 'proof of work.'

PoW consensus mechanism results in scalability issues. In PoW, all the transactions are stored in MemPool – memory, waiting for processing and validating by a miner [10]. The

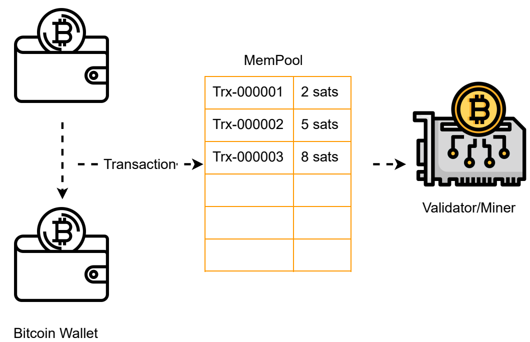

Fig. 1: Proof Of Work [1]: Transactions are stored in a MemPool. Validators pick transactions with high gas prices from MemPool for validation.

process is prolonged since a miner requires much work to validate a transaction. For Bitcoin, it is 7 TPS; Ethereum, it is 20 TPS. However, the rate at which new transactions are added to the MemPool is much higher. Miners only choose to validate transactions with high gas fees to maximize profit. As a result, users begin creating transactions with higher gas fees leading to scaling limitation [10].

III. Background

This section explains the importance of decentralization, security, and scalability for a blockchain network and how decentralization, security, and scalability fail to work together.

A. Decentralization

Decentralization is a core component of the blockchain network [8]. In blockchain, data is distributed across a network of nodes worldwide. Each node has a copy of the entire blockchain, ensuring transparency and reducing data manipulation risk. This network of nodes creates a decentralized system. Decentralization in blockchain allows permissionless access and use without restriction, unlike centralized systems accessible to a select few [11]. Decentralization promotes crowd-sourced consensus where the power to validate and verify transactions is distributed among all the participating miners or stakers [11]. However, it comes with a trade-off of slower speed. The advantages of decentralization in blockchain are twofold: 1) Eliminate central authority [6], and 2) Crowd-source consensus for decision-making

B. Security

Security in Blockchain can be measured in terms of consistency, tamper-resistant, resistance to a Distributed Denial-of-Service (DDoS) attack, pseudonymity, and resistance to double-spending attack [12]. Despite blockchain being considered secure, it is not entirely invulnerable to hacking. If a hacker can gain control of more than half of the nodes (51%) in the network, they can alter the blockchain and manipulate transactions to steal from the network [7]. However, the more nodes a blockchain has, the more secure it is. Despite this, some crypto projects prioritize decentralization and scalability over security, resulting in high-profile hacks of exchanges and

TABLE I: Transaction speed of Visa (centralized network) and blockchain networks to show the contrast in scalability [14]

Networks	Transaction Speed (tps)
Visa	24,000
Ripple	1,500
Paypal	193
Bitcoin Cash	60
LiteCoin	56
Dash	48
Ethereum 1.0	20
BitCoin	7

vulnerabilities in source code being exploited [11]. Advantages of blockchian network in terms of security: 1) Trustless electronic system that uses cryptographic proofs [9] 2) Eliminate double-spending attacks – spending the same asset more than once, caused by network delay [5]

C. Scalability

A critical aspect of blockchain technology is its ability to scale or handle numerous transactions accurately, affordably, efficiently, and promptly [13]. Currently, scalability is a significant limitation for blockchain infrastructure, as it can only handle a limited number of transactions per second (TPS) compared to traditional electronic payment systems. For example, Bitcoin and Ethereum can only process 4.6 and 14.3 TPS, respectively, while Visa can process around $1,736$ TPS and has reached peaks of $47,000$ TPS [9]. This makes it difficult for blockchain to compete with traditional payment systems regarding transaction speed.

D. Decentralization, Security, and Scalability

Optimizing for decentralization often comes at the cost of decreased network throughput [6]. This is because decentralized networks rely on a distributed network of nodes to validate and process transactions, which can be slower than centralized systems where one entity handles the transactions. As a result, finding the right balance between decentralization and scalability can be a challenge when designing a blockchain. Table I shows the transaction speed of centralized networks and blockchain networks to show the contrast in scalability.

For an illustrative comparison of this contrast in scalability, Table I presents transaction speed data for centralized and blockchain networks.

Reducing the number or geographical distribution of nodes can also make the network more vulnerable to attacks, as it becomes easier for hackers to gain control of most of the network's nodes. For example, in a proof of work (PoW) network, a hacker can launch a 51% attack [7]. In August 2020, the Ethereum Classic blockchain suffered three 51% attacks that resulted in the loss of millions of dollars. Therefore, it is essential to carefully consider the trade-offs between scalability and security when designing a blockchain network [6].

Decentralization, scalability, and security are essential pillars of a blockchain network. The blockchain trilemma, coined by Vitalik Buterin, refers to the idea that decentralization, scalability, and security constantly strive to co-exist but struggle to live in harmony [7]. Some blockchain networks affected by the blockchain trilemma are shown in the II.

TABLE II: Some of the blockchain networks facing scalability issue

Chosen elements	Give up on	Example networks
Decentralization, Security	Scalability	Bitcoin, Ethereum
Decentralization, Scalability	Security	Email, SMTP
Scalability, Security	Decentralization	Ripple, DASH [15]

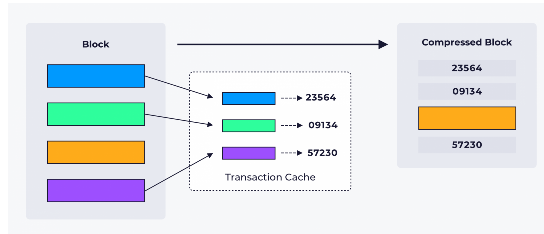

Fig. 2: Block Compression [16]: Data is compressed and stored in a cache. The cache is referenced from a block in the chain.

IV. Strategies for solving Trilema

In the following sections, we will discuss current state-of-the-art solutions focused on improving blockchains' scalability. These solutions can be categorized as Layer 1 and Layer 2 solutions. Layer 1 is the foundational Layer of a blockchain network. In contrast, Layer 2 refers to additional technologies and products that can be built on top of existing blockchain networks to improve scalability. These solutions are designed to address the challenges of increasing the capacity and efficiency of blockchain networks.

A. Layer 1 Solutions

Layer 1 refers to the foundational Layer and the underlying mechanisms of a blockchain network, including the consensus algorithm, network structure, and data structure.

1) Block Data: Block data is a type of data stored on a blockchain network. One Layer 1 scalability solution for blockchains that store large amounts of data is to increase the block size. By increasing the block size, more data can be stored in each block, increasing the number of transactions processed per block. This can help increase the overall throughput of the blockchain network and improve its scalability.

Alternately, another layer 1 scalability solution is to implement a mechanism for compressing the data stored on the blockchain [5] as in Figure 2. This can help reduce the storage space required for each block and improve the network's overall scalability.

Bitcoin Cash Bitcoin Cash, a hard fork [17] from Bitcoin, has a larger block size than Bitcoin to address scalability issues. The block size limit on the Bitcoin Cash is 8 megabytes, compared to 1 megabyte on the original Bitcoin network. This allows for more transactions to be processed in each block, which can help increase the network's overall transaction throughput. Additionally, Bitcoin Cash has implemented other scalability improvements, such as using more efficient transaction signatures and implementing a block size adjustment algorithm that allows the block size to adapt to changing network conditions. These changes have helped to improve the scalability of the Bitcoin Cash network. However, it is worth noting that increasing the block size can also lead to other issues, such as increased centralization and reduced security.

2) Alternative Consensus Algorithm: An alternate consensus mechanism is a method of reaching consensus that is different from the consensus mechanism used by the underlying blockchain protocol. Consensus mechanisms are used to ensure that all participants in a blockchain network agree on the order and validity of transactions, and they play a critical role in the security and reliability of the network. Various consensus mechanisms have been proposed for use in blockchain systems, including proof of work (PoW), proof of stake (PoS), delegated proof of stake, and others. Some of these mechanisms are more energy-intensive or resource-intensive than others, and some are more suited to certain types of networks or use cases. By using an alternate consensus mechanism, it may be possible to improve the scalability and efficiency of a blockchain network. However, it is important to carefully consider the trade-offs and potential impacts of switching to a different mechanism.

3) Proof of Stake (PoS): Proof of stake (PoS) [18] is a consensus mechanism that some blockchain networks use to achieve distributed consensus. In a proof of stake system, the creator of a new block is chosen in a deterministic way, depending on their stake in the network. Stake refers to the number of coins or tokens a user holds in the network, and the probability of a user being chosen to create a new block is proportional to their stake.

PoS systems are more energy-efficient and resource-efficient than PoW systems, as they do not require users to perform resource-intensive computations to create new blocks [19]. However, PoS systems may be more vulnerable to certain types of attacks, such as the "nothing at stake" problem, and they may also be less decentralized than PoW systems, as the distribution of stakes in the network can be more concentrated.

4) Ethereum 2.0*:* Ethereum 2.0 [20] is the next major upgrade to the Ethereum blockchain, a decentralized platform to run smart contracts. Ethereum 2.0 intends to address several scalability and security issues in the current version of Ethereum and introduce new features and capabilities to the platform.

One of the main changes in Ethereum 2.0 is the adoption of a PoS consensus mechanism [18]. Figure 3 shows the trend of daily transactions for the Ethereum network.

5) Sharding: Sharding [22] is a technique to improve the scalability of a blockchain by dividing the network into smaller pieces, or shards, and allowing each shard to process transactions in parallel. By distributing the workload across multiple shards, it is possible to increase the overall transaction throughput of the network and reduce the time it takes to confirm transactions. Figure 4 shows the sharding technique. Sharding is often used with other scalability solutions, such as increased block sizes or off-chain transactions, further to improve the capacity and efficiency of the network.

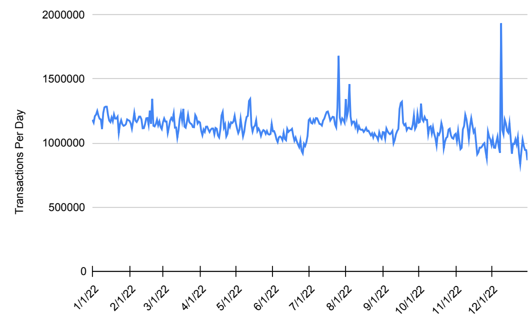

Fig. 3: Ethereum daily transactions chart for 2022. The data for this graph is taken from Etherscan [21].

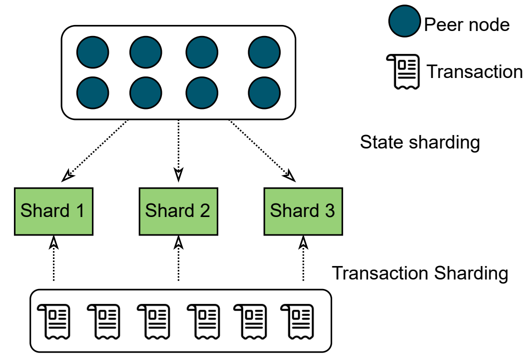

Fig. 4: Sharding [5]: Peer nodes are assigned to different shards. Transactions are distributed to different shards to run in parallel.

Sharding also comes with a security trade-off where 51% attack becomes 31% attack [10] and can introduce additional complexity to the network. Cross-shard communication [5], the interaction between two shards, is also a concern.

6) Directed Acyclic Graph (DAG): DAG [23] is a data structure used in some distributed systems, including some blockchain protocols. In a DAG, nodes represent data or events, and edges represent relationships or dependencies between the nodes, as shown in figure 5. A DAG is called directed because the edges have a direction, and acyclic because it does not contain any cycles (that is, there are no paths that start and end at the same node) [23].

Some blockchain protocols, such as IOTA [24] and Hashgraph [25], use DAGs as their underlying data structure to store and organize transactions on the network. DAG-based blockchain protocols are designed with scalability in mind and

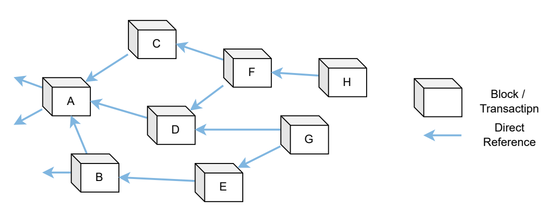

Fig. 5: Overview of DAG. Each cube represents a block/-transaction. Multiple blocks can be concurrently generated and linked to the previous block(s) in DAG. i.e., blocks B, C, and D can be concurrently generated which point to A.

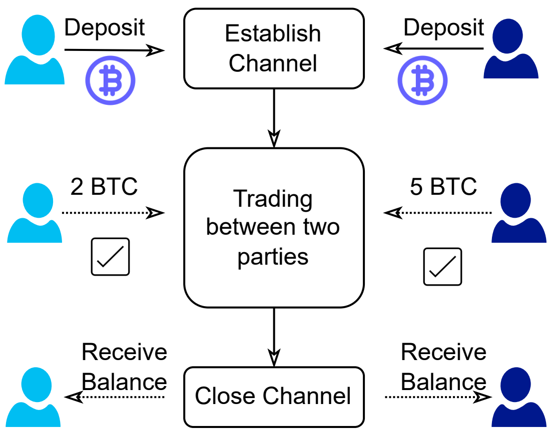

Fig. 6: Working of Lightning Network [5]

can potentially offer higher transaction throughput and lower fees than traditional blockchain protocols.

B. Layer 2 Solutions

Layer 2 solutions are techniques and protocols that operate on top of an underlying blockchain layer to improve its scalability and efficiency. Layer 2 solutions address the Blockchain Trilemma by offloading a significant portion of the transaction processing onto secondary layers. This allows the primary blockchain (Layer 1) to focus on security and decentralization while accommodating an increased transaction load and providing a better user experience regarding speed and cost in Layer 2. Some Layer 2 solutions are off-chain channels, side-chains, and cross-chain protocols.

1) Channels: Channels [26], also known as payment channels or off-chain transactions, are a technique that can be used to improve the scalability of a blockchain by allowing some transactions to be conducted off the main blockchain [26]. This can help to reduce the burden on the main blockchain, as only the opening and closing of the channel need to be recorded on the chain, rather than every individual transaction [26].

Channels are often used with other scalability solutions, such as increased block sizes or sharding, to improve the network's capacity and efficiency further. They can be particularly useful for applications that require a high volume of small or frequent transactions, as they can help reduce the overhead and fees associated with sending each transaction on the main blockchain.

2) Lightning Network: The Lightning Network [27] is a layer 2 payment protocol that operates on the Bitcoin blockchain. It enables fast, low-cost, and private off-chain transactions between participating parties. Figure 6 shows procedures involved in the lightening network. It uses a network of payment channels to allow users to conduct transactions directly with each other instead of broadcasting every transaction to the entire network. This helps to reduce the burden on the main blockchain and improve the scalability of the network.

3) Side Chains: Side chains [28] is a technique that can be used to improve the scalability of a blockchain by allowing some transactions to be conducted on a separate chain that is

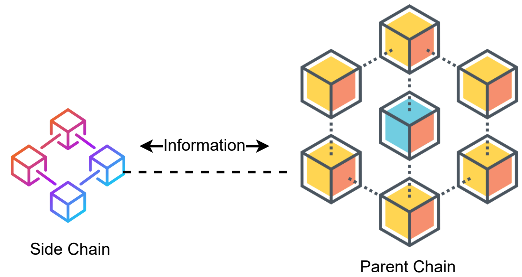

Fig. 7: Side Chain: Information flows two ways between the side and parent chains. This allows the parent chain to delegate tasks to the side chain.

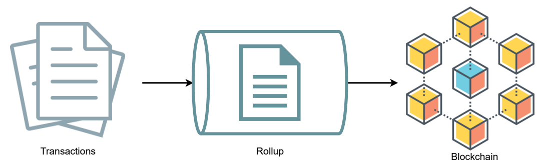

Fig. 8: Rollup: Aggregates multiple transactions as one and stores the final result on the blockchain.

"pegged" [29] to the main chain. Side chains are connected to the main chain through a two-way peg, transferring assets back and forth between the two chains [29] [30]. This can help reduce the main chain's burden and improve its efficiency by allowing some transactions on the side chain rather than the main chain. Figure 7 shows an illustration of the side chain.

Side chains depend on the main chain as a "backstop" to ensure the security and integrity of the system. They are often used with other scalability solutions, such as off-chain transactions or sharding, to improve the network's capacity and efficiency.

Blockchain networks running side chains are Polygon, xDai, Binance Smart Chain, Liquid Network, and SKALE.

4) Rollup: Rollup is a technique that can be used to improve the scalability of a blockchain by reducing the amount of data that needs to be stored on the chain [31]. Rollup works by aggregating multiple transactions into a single "super transaction" and storing the result on the blockchain rather than storing each transaction separately. This can help reduce the storage overhead and increase the network's overall transaction throughput. Figure 8 gives a general overview of how rollup works.

5) Cross Chains: Cross-chain [34] projects are a popular approach to improving the scalability of blockchain systems by connecting different blockchains and enabling interoperability between them. One technique for achieving this is the use of a relay chain [32] [33], which serves as a router and connects multiple independent blockchains within a cross-chain system [34]. Figure 9 is a synopsis of how the relay chain works. The relay chain is responsible for processing cross-chain transactions and ensuring consistency between the blockchains. In addition to the relay chain, pegged chains can bridge existing blockchains with the cross-chain system. These pegged chains, such as Peg Zone in Cosmos or Parachain bridge in Polkadot [33], allow existing blockchains to join

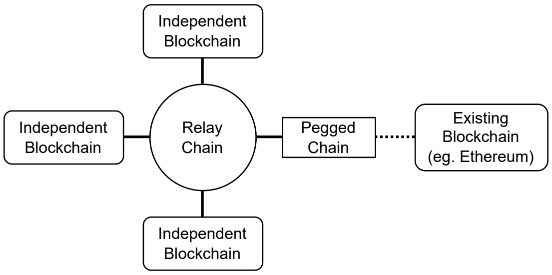

Fig. 9: Relay Chains [32] [33]: Multiple independent blockchains are connected via relay chains. Relay chain facilitates cross-chain transactions. The pegged chain connects the relay chain with the existing blockchain .

TABLE III: Layer 2 blockchain networks speed [10]

Blockchian Network	**Transaction (tps)**
Solana	3,000
Ripple (XRP)	1,500
Ethereum 2.0	100,000 (theoretical)
Algorand (ALGO)	3,000
Fantom (FTM)	25,000
Avalanche (AVAX)	4,500
Cardano (ADA)	250
Polygon (MATIC)	7,000
Bitgert (BRISE)	100,000

the cross-chain system and benefit from its scalability and interoperability features.

In general, cross-chain projects aim to build an extensive network of interconnected blockchains that can exchange value and information with each other efficiently and securely.

V. Discussion

This section discusses and performs a comparative analysis of Layer 1 and Layer 2 solutions.

Table III shows the transaction speed of different blockchain networks implementing some of the abovementioned solutions. However, the theoretical speed has not yet been achieved.

Figures 10 and 12 show the Bitcoin and Ethereum prices over 2022. Figures 11 and 13 show the change in the transaction speed for Bitcoin and Ethereum blockchain over 2022. The transactions per second (TPS) for Bitcoin and Ethereum have reached the highest of all time. This increase in transaction speed could be attributed to increased usage and network throughput. However, the speed is insufficient for the blockchain network to scale worldwide.

Figures 14 and 15 show the price of Layer 2 blockchain networks. When comparing the price with the Layer 1 blockchain networks shown in Figures 10 and 12, Layer 2 networks have significantly lower prices in 2022.

A. Advantages and disadvantages of Layer 1 and Layer 2 scaling solutions

The advantages of Layer 1 scaling solutions are listed below.

- Layer 1 scaling on the blockchain allows the network to scale without additional trust in third-party entities. This is because the scaling solutions are built into the protocol,

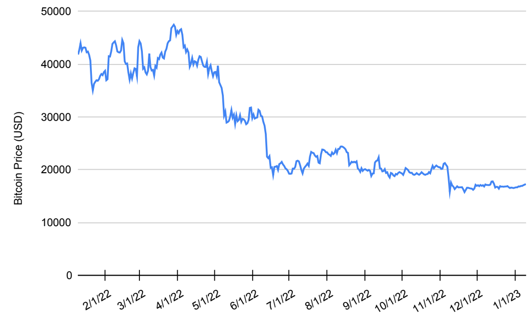

Fig. 10: Bitcoin Price in 2022 [35].

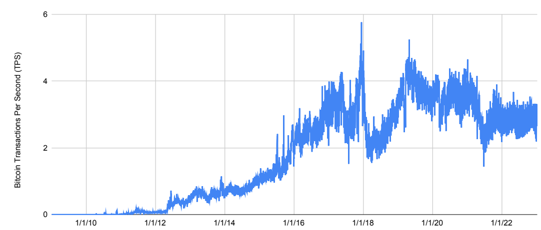

Fig. 11: Transactions per second (TPS) for Bitcoin since 2009. The maximum TPS for Bitcoin is 6 [35].

Fig. 12: Ethereum Price in 2022 [35].

Fig. 13: Transactions per second (TPS) for Ethereum since 2016. The maximum TPS for Ethereum is less than 25 [35].

Fig. 14: Price of Bitcoin Cash (bch) and Avalanche (avax) in USD in 2022 [35].

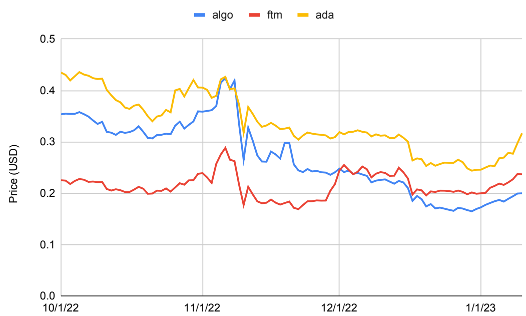

Fig. 15: Price of Algorand (algo), Fantom (ftm), and Cardano (ada) in USD in 2022 [35].

meaning that all nodes in the network can take advantage of them.

- Layer 1 scaling solutions can improve the underlying structure and capabilities of the blockchain network by incorporating new technology and features directly into the protocol. This can promote the growth and development of the blockchain ecosystem as a whole [36].

Some of the disadvantages of Layer 1 scaling solutions are:

- Layer 1 blockchain scaling solutions can require a hard fork, a change to the protocol that is not backward-compatible. Hard forks can be controversial and lead to a split in the network, creating multiple versions of the blockchain with different rules. This could lead to decreased security and a lack of interoperability between different versions of the blockchain.
- Layer 1 scaling solutions can also be limited by current technology and infrastructure, requiring new and expensive hardware to be implemented to improve the scalability of the network.

The advantages of layer 2 scaling solutions are as follows.

- Layer 2 scaling solutions can be implemented without a hard fork. This means there is no need to create a new blockchain version, and nodes not updating their software can continue to participate in the network. This can help to avoid the controversies and network splits that can occur with a hard fork.
- Layer 2 scaling solutions can be implemented more quickly than Layer 1 solutions. Layer 2 solutions are also often more flexible, as they can be adjusted and upgraded over time as the needs of the network change.
- Layer 2 scaling solutions can be less expensive to implement as they do not require the purchase of additional hardware. It does not place additional stress on the underlying infrastructure, making it a more cost-effective solution for scaling.

Some of the disadvantages of the Layer 2 scaling solutions are as follows.

- Layer 2 scaling solutions can introduce additional complexity to the blockchain ecosystem. Since they are built on top of the base protocol, they may have their own rules and requirements, making them difficult for users to understand and use. Additionally, Layer 2 solutions often depend on a separate set of nodes or validators to function, which can create additional points of failure in the network.
- They may require additional trust in third-party entities. For example, off-chain scaling solutions like Plasma and state channels rely on smart contracts and payment channels managed by a separate set of nodes or validators. This can significantly make the network more centralized and less secure if these third-party entities are compromised.
- Layer 2 scaling solutions can also have limited interoperability with other blockchain networks, meaning they may not readily communicate or exchange data with other networks. This can limit the ability of users to move assets between different blockchains.

B. *Layer 1 vs Layer 2 Scaling Solutions*

The table IV compares Layer 1 and Layer 2 scaling solutions.

C. *Solving Trilemma*

Multiple studies in the blockchain trilemma have led to the development of different Layer 1 and Layer 2 solutions. In addition, some researchers have also studied concepts such as zero-knowledge proof [38] and off-chain storage protocol [39]. In [38], only scalability and security constraints of blockchain are addressed, leaving decentralization unknown. Similarly, the solution proposed in [39] is limited to the proof-of-work consensus mechanism.

Despite the development of multiple solutions, there is still a massive gap in achieving decentralization, security, and scalability in blockchain [38].

VI. Conclusion

Blockchain technology has become increasingly popular in recent years and has been applied to various applications in different fields. As the number of users of blockchain technology has grown, the issue of network congestion has become more pressing. Several solutions have been proposed to address this scalability problem. These solutions can be classified into several layers, including Layer 1 solutions

TABLE IV: Layer 1 vs Layer 2 scaling solutions [37]

Criteria	Layer 1	Layer 2
Definition	Layer 1 scaling solutions involve modifications in the base protocol of the blockchain network to achieve improved scalability	Layer 2 scaling solutions involve the use of off-chain services or networks to improve the scalability of the underlying blockchain network.
Method of Scaling	Scaling method focuses on modifying the core protocol	Operate independently of the primary blockchain protocol
Type of Solutions	Consensus protocol enhancement and sharding	SideChains, Channels, etc. Virtually no restriction on the solutions
Speed	Slower as it requires a shift from the currently adopted technique	Faster as layer 2 solutions can be adjusted and upgraded over time as needed
Hard Fork	Requires hard fork which may make the older versions incompatible	Does not require hard fork
Cost	May be expensive to implement as it requires new hardware	Less expensive as no additional hardware required
Complexity	Does not add much to the complexity of the existing protocol	Introduces additional complexity to the blockchain ecosystem
Centralization	No risk of centralization	Dependence on third-party entity may result in centralization

that address the base layer of the blockchain and Layer 2 solutions that build on top of the base layer. Among the popular solutions proposed to improve blockchains' scalability are sharding, sidechains, and cross-chain transactions.

Regardless of the different off-chain and on-chain solutions to the blockchain trilemma of scaling the network, a perfect solution is not easy. Before blockchain becomes widespread, the practical harmony between decentralization, scalability, and security must be achieved.

References

[1] https://wiki.bitcoinsv.io/index.php/Proof_of_Work.

[2] P. Gaži, A. Kiayias, and D. Zindros, "Proof-of-stake sidechains," in *2019 IEEE Symposium on Security and Privacy (SP)*, pp. 139–156, 2019.

[3] T. Darwish, K. Abu Bakar, G. Matsuda, A. Aliyu, A. H. Abdullah, A. S. Ismail, A. F. Yusof, M. M. Mohamad, M. Y. Idris, Z. Ismail, *et al.*, "Comparative analysis of blockchain consensus algorithms from shariah perspective," *Journal of Contempory Islamic Studies*, vol. 6, no. 1, pp. 1–21, 2020.

[4] https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-proof-of-stake, Jan 2023.

[5] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to scalability of blockchain: A survey," *Ieee Access*, vol. 8, pp. 16440–16455, 2020.

[6] "Blockchain trilemma: Scaling and security issues." https://www.gemini.com/cryptopedia/blockchain-trilemma-decentralization-scalability-definition.

[7] M. Musharraf, "What is the blockchain trilemma?." https://www.ledger.com/academy/what-is-the-blockchain-trilemma, Oct 2022.

[8] A. Gangwal, H. R. Gangavalli, and A. Thirupathi, "A survey of layer-two blockchain protocols," *Journal of Network and Computer Applications*, vol. 209, p. 103539, 2023.

[9] C. Sguanci, R. Spatafora, and A. M. Vergani, "Layer 2 blockchain scaling: A survey," *arXiv preprint arXiv:2107.10881*, 2021.

[10] RyanRMatta, "What is the blockchain trilemma ?," Sep 2022.

[11] CertiK, "The blockchain trilemma: Decentralized, scalable, and secure?," Oct 2019.

[12] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Computing Surveys (CSUR)*, vol. 52, no. 3, pp. 1–34, 2019.

[13] OpenSea, "The Blockchain Trilemma." https://opensea.io/learn/blockchain/the-blockchain-trilemma, 2024. Accessed: 2024-06-23.

[14] "A deep dive into blockchain scalability." https://crypto.com/university/blockchain-scalability#:~:text=While\%20Visa\%20can\%20process\%20up,capability\%20to\%20achieve\%20mass\%20adoption.

[15] SoFi, "5 most private cryptocurrencies." https://www.sofi.com/learn/content/most-private-cryptocurrency/, Jan 2023.

[16] "Block compression." https://docs.bloxroute.com/bdn-architecture/performance-techniques/block-compression.

[17] J. Redman, "Fork watch: Block 478558 initiates 'bitcoin cash' split – first blocks now mined – blockchain bitcoin news." https://news.bitcoin.com/fork-watch-first-bitcoin-cash-block-mined/, Aug 2017.

[18] A. Nandwani, M. Gupta, and N. Thakur, "Proof-of-participation: Implementation of proof-of-stake through proof-of-work," in *International Conference on Innovative Computing and Communications*, pp. 17–24, Springer, 2019.

[19] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[20] "The merge." https://ethereum.org/en/upgrades/merge/.

[21] "Ether daily price (usd) chart — etherscan."

[22] "Shard (database architecture)," Jan 2023.

[23] "Directed acyclic graph." https://en.wikipedia.org/wiki/Directed_acyclic_graph, Oct 2022.

[24] "Home." https://www.iota.org/.

[25] L. Baird, M. Harmon, and P. Madsen, "Hedera: A governing council & public hashgraph network," *The trust layer of the internet, whitepaper*, vol. 1, pp. 1–97, 2018.

[26] J. Lind, O. Naor, I. Eyal, F. Kelbert, P. Pietzuch, and E. G. Sirer, "Teechain: Reducing storage costs on the blockchain with offline payment channels," in *Proceedings of the 11th ACM International Systems and Storage Conference*, pp. 125–125, 2018.

[27] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," 2016.

[28] M. Mohan *et al.*, "Sidechain: A scalable blockchain," in *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, pp. 1337–1342, IEEE, 2022.

[29] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille, "Enabling blockchain innovations with pegged sidechains," *URL: http://www.opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains*, vol. 72, pp. 201–224, 2014.

[30] L. Besançon, C. F. Da Silva, P. Ghodous, and J.-P. Gelas, "A blockchain ontology for dapps development," *IEEE Access*, vol. 10, pp. 49905–49933, 2022.

[31] L. T. Thibault, T. Sarry, and A. S. Hafid, "Blockchain scaling using rollups: A comprehensive survey," *IEEE Access*, 2022.

[32] "Internet of blockchains." https://cosmos.network/whitepaper.

[33] G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework," *White Paper*, vol. 21, pp. 2327–4662, 2016.

[34] H. Wang, Y. Cen, and X. Li, "Blockchain router: a cross-chain communication protocol," in *Proceedings of the 6th international conference on informatics, environment, energy and applications*, pp. 94–97, 2017.

[35] "Data file downloads." https://coinmetrics.io/community-network-data/, Jan 2022.

[36] "Layer 1 vs. layer 2: What is the difference?." https://beincrypto.com/learn/layer-1-vs-layer-2/, Dec 2022.

[37] "layer 1 vs layer 2: what is the difference? - beincrypto." https://beincrypto.com/learn/layer-1-vs-layer-2/.

[38] M. Principato, M. Babel, T. Guggenberger, J. Kropp, and S. Mertel, "Towards solving the blockchain trilemma: An exploration of zero-knowledge proofs," 12 2023.

[39] S. Reno and M. Haque, "Solving blockchain trilemma using off-chain storage protocol," *IET Information Security*, vol. 17, pp. n/a–n/a, 07 2023.