Scalability Of Blockchains: Literature Review

Landyn Moreno
Electrical & Computer Engineering
The University of Texas at Austin
landynmoreno@utexas.edu

December 05, 2023

***Abstract* - This report delves into the critical issue of scalability in blockchain technology. Upon laying a foundational introduction to blockchain technology and its inherent scalability challenges, this report explores various strategies designed to enhance blockchain scalability, including Layer 2 solutions as well as sharding techniques. A portion is dedicated to a case study of Ethereum's transition to Ethereum 2.0, highlighting how this major platform is addressing scalability challenges. The discussion extends to the potential challenges and future trends in blockchain scalability. The report concludes by emphasizing the importance of scalability in the practical implementation and future evolution of blockchain systems.**

I. INTRODUCTION

In today's evolving landscape of digital technology, blockchain stands out as a revolutionary paradigm as it offers a decentralized and secure method of recording transactions and data. Initially popularized by cryptocurrencies, blockchain technology's potential extends far beyond, promising transformative impacts across various industries. However, as the technology matures, scalability has surfaced as a critical bottleneck, posing challenges to its broader adoption and efficiency. Critics of the blockchain often bash the latency and fees in order to transact on the blockchain.

This report analyzes blockchain scalability, presenting a comprehensive exploration of the challenges and examining the spectrum of proposed solutions. It is important to refine and enhance blockchain's scalability in order to strengthen its applicability and efficiency.

II. BACKGROUND

Blockchain scalability refers to the potential for which a blockchain can handle a volume of transactions efficiently and cost-effectively. Historically, as blockchain technology began to gain traction with the rise of cryptocurrencies like Bitcoin and Ethereum, its limitations in handling high transaction volumes became apparent. These limitations are exemplified by increasing transaction fees and longer latency times during periods of network congestion. Scalability issues have historically posed constraints on the broader adoption and practical application of blockchain technology. In the early days, these limitations were less pronounced due to lower transaction volumes. However, as blockchain applications expanded beyond simple financial transactions to complex smart contracts and decentralized applications, the need for greater scalability has become evident.

Today, scalability is more important than ever. The expanding use of blockchain in various industries demands more efficient, faster, and cheaper transaction processing capabilities. The ability of a blockchain to scale effectively directly impacts its practicality for everyday use and its potential for widespread adoption.

III. THE BLOCKCHAIN TRILEMMA

The blockchain trilemma is that there is a delicate balance between three aspects of the blockchain: security, decentralization, and scalability. Scalability is the potential for which a blockchain can handle a volume of transactions. Security is the ability to secure a blockchain from attacks or faulty transactions like double spending. Lastly, decentralization is the transfer of authority to distributed nodes to prevent control from a central entity. At this current point, you cannot improve all three aspects simultaneously. Theoretically, all blockchain technologies face this trilemma and there is no perfect balance yet to deem it 'solved' [1].

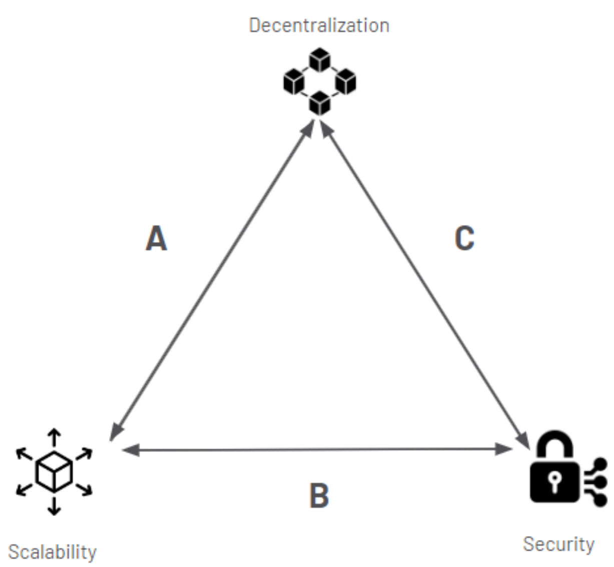

Figure 1: The Blockchain Trilemma Diagram

Visualized as a triangle in *Figure 1*, it is evident that a side must be chosen for which two aspects to improve, A, B, or C. The point that is not present in that chosen side is sacrificed to some extent for the benefits of the other two aspects. For example, choosing side B results in an improvement of scalability and security, but sacrifices decentralization. From a high level, we can imagine in this example that security is enhanced by implementing an advanced algorithm that requires greater validation for each transaction. Scalability is increased by optimizing the network infrastructure. However, due to this, there is an extent to which decentralization is harmed as new participants serving as nodes may have a higher barrier to entry due to the intensive algorithm and specialized network infrastructure. From a high level, this is how the blockchain trilemma works.

As we've seen, the blockchain trilemma presents a persistent challenge, leading innovators to constantly seek a more balanced approach. While a perfect solution that equally addresses all three aspects remains elusive, ongoing efforts in blockchain technology aim to strike a more efficient balance. This continuous evolution has led to the development of various strategies that attempt to enhance scalability, often with minimized impacts on security and decentralization. So, how do we improve scalability while limiting our sacrifices on security and decentralization? The following sections will explore some strategies that have been proposed and implemented to address this very question, shedding light on the ongoing quest to optimize blockchain technology for more efficient applications.

IV. STRATEGIES FOR IMPROVING SCALABILITY

As blockchain technology evolves, several strategies have been developed to tackle the scalability challenge. Among these, Layer 2 solutions and sharding are prominent approaches, each offering unique methods to enhance transaction processing capabilities without compromising the foundational principles of blockchain technology.

A. *Layer 2 Solutions*

Layer 2 solutions are techniques designed to improve scalability by handling transactions off the main blockchain (Layer 1). By doing so, they reduce the load and congestion on the main blockchain, resulting in faster transactions and lower fees. These solutions are built on top of the existing blockchain prioritizing scalability, while maintaining the security and decentralization aspects of the underlying network. Within the realm of Layer 2 solutions, two innovative approaches stand out: Rollups and Sidechains. Each of these techniques addresses scalability in distinct ways, offering unique advantages and considerations. Let's delve deeper into these solutions to understand how they contribute to resolving the scalability challenge in blockchain technology.

A.1 *Rollups*

Rollups are a type of Layer 2 solution that play a crucial role in scaling blockchain networks. They work by rolling up or bundling multiple transactions into a single transaction. This bundle is then processed off-chain, significantly reducing the strain on the main blockchain [7]. This benefits the blockchain since it reduces the traffic of multiple transactions that can simply be rolled up. It also benefits the user as they would not have to pay so many transaction fees for each individual transaction and would only need to pay one transaction fee in order to publish the final settlement to the blockchain.

The question may arise: Wouldn't it be easy to publish faulty transactions then through rollups that are processed off chain? Well, there are two main types of rollups that help handle this: Optimistic Rollups and Zero-Knowledge Rollups. Optimistic Rollups assume transactions are valid by default and only run computations in case of a dispute, whereas Zero-Knowledge Rollups validate transactions using cryptographic proofs, ensuring both speed and security.

A.2 *Sidechains*

Another Layer 2 approach is the use of sidechains. Sidechains are separate blockchains that are connected to the main blockchain and run in parallel. They allow for transactions and processes to be conducted independently of the main chain, which can significantly increase the overall capacity of the network and reduce congestion on the main blockchain. Once the transactions are completed on a sidechain or a threshold target is reached, they are then compressed and pushed to the main blockchain, ensuring continuity and security [8]. An operating example of this is with Polygon (POL) acting as a layer 2 sidechain on the Ethereum (ETH) layer 1 base chain.

B. *Sharding*

As said by the co-founder of Ethereum, Vitalik Buterin, "Scalability is this idea of coming up with a blockchain that can scale much larger than existing chains essentially by processing transactions in parallel. And moving away from this paradigm where every single node on the network has to process every single transaction." This is essentially a definition of sharding.

There's two common ways to scale when sharding, vertically, and horizontally. Vertical scaling calls for a network infrastructure improvement by requiring better hardware, resulting in fewer nodes. This hardware improvement initially improves transaction throughput, however, that improvement is limited by Moore's law due to its hardware dependency. On the other hand, horizontal scaling focuses on adding more nodes to the network. In horizontal scaling, performance is improved in proportion to traffic as nodes are strategically used.

Sharding is a different approach to scalability that involves dividing the blockchain into smaller, more manageable parts called 'shards' [2]. Each shard contains its own independent piece of state and transaction history. By distributing the data across multiple shards, the network can process transactions in parallel, greatly increasing the throughput. By doing this, each node does not have to process all of the data of the entire blockchain anymore, it only must process its shards data. This method not only speeds up transaction processing times but also reduces the load on individual nodes, making it easier to participate in the network and maintain decentralization.

However, just like a traditional blockchains traffic hinders its scalability, what happens when a shard becomes too congested? Accounts and contracts are assigned to shards and these usages are not always equal all of the time. There's a process called resharding that helps to prevent one shard from being loaded too heavily or becoming too slow. Basically, resharding is the process of periodically rebalancing these shards and/or creating new shards if a traffic threshold is crossed.

Stated earlier, improving scalability and maintaining decentralization is prevalent with the sharding strategy. However, to relate back to the trilemma, sharding theoretically threatens the security aspect to some degree. For example, by the '51% attack' definition, it would take 51% or more of nodes to maliciously participate in consensus in order to corrupt the blockchain. When that blockchain is sharded into 10 (arbitrary) shards, it now only takes 5.1% of the original malicious actors to win the majority of the nodes and corrupt a shard. That being said, sharding is still an optimal strategy for scalability as protections such as random assignments to shards and frequent rotations of assignments are practiced.

V. ETHEREUM'S TRANSITION TO 2.0

Ethereum is the second largest blockchain by market capitalization and possesses smart contract functionalities. As it is increasingly adopted, Ethereum's transition to 2.0 is a significant step in its evolution, driven by the need to address key challenges and improve the network's overall functionality [4]. The primary goals of this transition include tackling scalability issues and adopting a more efficient and sustainable consensus mechanism to be the foundation of scalability improvements. Let's explore how these changes are being implemented through the roadmap laid out by Ethereum's co-founder, Vitalik Buterin [5].

One phase of Ethereum's transition to 2.0 is "The Merge," a critical update transitioning the network from the energy-intensive Proof of Work (PoW) to the more efficient Proof of Stake (PoS) consensus mechanism. This shift brings several advantages:

- Reduced Computational Intensity: PoS is far less computationally demanding compared to PoW, which means lower energy consumption and increased sustainability.
- Validator Selection: In PoS, validators are chosen based on the number of tokens they hold and are willing to stake as collateral. This system encourages validators to act honestly, as they risk losing their staked tokens if they attempt to cheat the system.

Upon the completion of "The Merge," a key component of Ethereum 2.0 is "The Surge," which focuses on enhancing scalability through sharding, a topic discussed earlier in this report. Sharding is obviously expected to significantly increase Ethereum's transaction processing capacity and that is the purpose of implementing such a strategy.

Additionally, there will be a phase called "The Verge" that is geared towards streamlining block verification. By making the process of verifying blocks simpler and more efficient, Ethereum aims to further improve its performance and scalability.

Overall, the implementation of Ethereum 2.0, with its focus on PoS, sharding, and efficient block verification, marks a major leap in the network's capabilities. Originally designed to handle around 15 transactions per second, these updates and a completion of the roadmap provided by Mr. Vitalik Buterin is expected to propel Ethereum's capacity to an optimistic 100,000+ transactions per second [9]. This dramatic increase in scalability not only demonstrates Ethereum's commitment to evolving in response to the growing demands of its users, but also highlights the impact of scalability strategies as they are used in everyday innovations such as sharding.

VI. CHALLENGES AND FUTURE TRENDS

As blockchain evolves, addressing scalability comes with its own set of challenges, and the industry continues to look toward future trends to find solutions. As networks become more scalable, maintaining high security levels becomes challenging. The more a blockchain scales, the harder it may be to keep it secure against attacks. Ensuring that blockchain remains decentralized as it scales is another challenge. As the technology becomes more complex, it may become harder for average users to participate as nodes, potentially leading to more 'centralization.'

Future trends include developing ways for different blockchains to interact seamlessly. This interoperability can lead to more efficient systems and improved scalability. Additionally, the development of more advanced consensus mechanisms beyond PoW and PoS is on the horizon. These new mechanisms aim to balance scalability, security, and decentralization more effectively.

VII. CONCLUSION

This report has explored the pivotal issue of scalability in blockchain technology, showcasing various strategies and innovations aimed at addressing this challenge. From the detailed examination of Layer 2 solutions like rollups and sidechains to the comprehensive analysis of sharding, it's clear that the blockchain community is actively seeking solutions to enhance scalability while balancing security and decentralization. Ethereum's ambitious transition to 2.0, with its focus on the Merge, Surge, and Verge within its roadmap, exemplifies the proactive steps being taken by leading blockchain platforms to tackle scalability [6]. The path to resolving blockchain scalability is lined with challenges, but the future is undeniably promising. Continuous innovations and advancements in blockchain technology are expected to overcome these hurdles, leading to more efficient, secure, and user-friendly networks. As blockchain technology continues to evolve, it will undoubtedly open new avenues for development and application, further solidifying its position as a cornerstone of modern digital technology.

In conclusion, while blockchain scalability remains an ongoing challenge, the progress made thus far points to a future where these limitations are significantly mitigated, enabling wider adoption and more innovative applications of blockchain technology. As adopters, we are in good hands.

VIII. ACKNOWLEDGEMENT

Thank you to The University of Texas at Austin, professor Sriram, the teaching assistants, and student participants for a wonderful and learning-filled semester.

IX. REFERENCES

[1]: YVES LONGCHAMP, SAURABH DESHPANDE, UJJWAL MEHRA (2020). The Blockchain Trilemma. The Bridge

[2]: TEAM NEAR PROTOCOL (2019). The NEAR White Paper. NEAR Protocol

[3]: KEVIN SEKNIQI, DANIEL LAINE, STEPHEN BUTTOLPH, AND EMIN GUN SIRER (2020). Avalanche Platform. AVA Labs

[4]: VITALIK BUTERIN, TEAM ETHEREUM (2023). Ethereum Whitepaper. Team ETH

[5]: KENDRICK LAU (2020). Ethereum 2.0 An Introduction. Crypto.com

[6]: TEAM ETHEREUM (2023). Ethereum Roadmap. Team ETH

[7]: JOSEPH POON, THADDEUS DRYJA (2016). The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. Poon & Dryja

[8]: MIHAILO BJELIC, SANDEEP NAILWAL, AMIT CHAUDHARY, WENXUAN DENG (2021). POL: One token for all Polygon chains. POL Team

[9]: VITALIK BUTERIN (2022). Updated roadmap diagram!. @VitalikButerin, X.

[10]: DIANA AMBOLIS (2023). Emerging Trends In Blockchain Scalability: A Glimpse Into The Future. Blockchain Magazine.