Systematic literature review of challenges in Blockchain: Scalability and Security

02234 Current Topics in System Security Fall 23

Group 7

Authors

Name	Student ID
Anton Østergaard Schmidt	s163053
Gustav Emil Nobert	s185031
Pooja Shrestha	s230004
Michael Gromiha, Michael Mozim	s232885

December 30, 2023

Abstract

Blockchain technology, a subject of extensive research for numerous years, has garnered significant attention for its transformative potential. Despite widespread research, challenges related to scalability and security persist, impeding its application into various domains. This systematic literature review aims to delve into the landscape of blockchain scalability issues, offering insights into identification and resolution strategies. Furthermore, the review extends its purview to scrutinize the security implications associated with layer 2 solutions. As blockchain continues to evolve, this study also undertakes an examination of contemporary business applications, shedding light on the diverse use cases where layer 2 solutions are actively deployed. Through these multifaceted contributions, this review endeavors to enhance our understanding of the dynamic intersection between blockchain technology, scalability concerns, and security considerations.

Keywords: blockchain, layer-two, scalability, security

1 Introduction

In 2008, Blockchain emerged as a decentralized alternative to traditional centralized banking solutions [1]. This technology functions as a distributed digital ledger, utilizing a Peer-to-Peer network for transaction verification. Its decentralization allows for distinctive features, including immutability, public verifiability, and trustlessness. The security framework of blockchain relies on a consensus mechanism, enabling nodes in the network to agree on the ledger's state. The initial iteration, utilizing Proof-of-Work (PoW), involved miners engaging in computationally challenging puzzles for cryptocurrency rewards. However, PoW's by-design slowness and inefficiency, coupled with substantial energy consumption, led to low transactions per second (TPS), limiting real-world blockchain applications. Subsequent advancements, such as Proof-of-Stake (PoS), Proof-of-Authority (PoA), and Proof-of-History (PoH), aimed to address these issues, yet the consensus mechanism remains crucial for blockchain scalability [2, 3, 4].

The longstanding challenge of blockchain scalability is encapsulated by the blockchain trilemma, an issue present since its introduction. The trilemma, which was first mentioned by Ethereum founder Vitalik Buterin, depicts a triangle with security, decentralization, and scalability at its corners. According to this paradigm, when designing blockchain systems, fulfilling two out of the three attributes becomes a trade-off, emphasizing the inherent complexities in achieving a complete solution [5].

Researchers have addressed scalability issues by dividing the solutions into two categories, layer 1 and layer 2 solutions. The different layers represent *on* and *off-chain* modifications, respectively. Layer 1 focuses on changes to the consensus mechanism or the underlying data structure such as changing the block size, sharding of data, or changing the structure to a different form as seen in Directed Acylic Graphs (DAGs) used in blockchain. Layer 2 solutions are developed off-chain and do not alter the original design of the main blockchain. Layer 2 solutions are utilising that it is not bound by the computational limits of the mainnet and can therefore do more efficient computations to increase scalability. Solutions in this layer include state channels, sidechains, and rollups [6, 7]. When initially

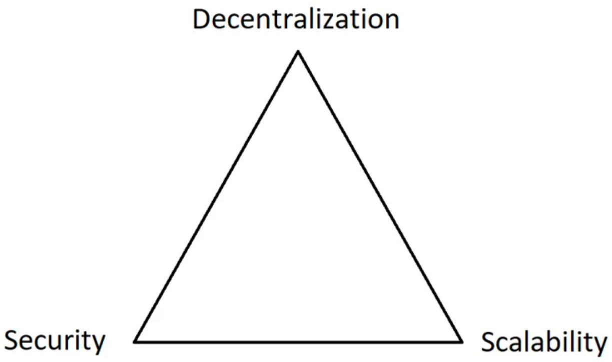

Figure 1: The Blockchain Trilemma

comparing layer 1 and layer 2 solutions, layer 1 has to change the fundamental data structure and will possibly face issues with backward compatibility, since restructuring the underlying consensus and data structure could lead to a relaunch of a blockchain, which is far from practical. Therefore, we have in our review chosen to focus on layer 2 solutions.

1.1 Contribution and Research Questions

This systematic literature review provides an overview of the scalability issues with blockchain technology, along with strategies for identifying and resolving these issues. This paper's primary contribution is a broad overview of these subjects based primarily on peer-reviewed research published during the mentioned year, with an emphasis on scalability issues with blockchain technology. The second contribution consists of an analysis of which security problems arise with layer 2 solutions. The final contribution is to examine the current and recent business applications and use cases that layer 2 solutions are used for.

This study specifically addresses the following research questions:

- RQ1: What layer 2 solutions are proposed in the literature?
- RQ2: What security problems arise with layer 2 solutions, and how does the literature attempt to mitigate them?
- RQ3: What business applications have the recent layer 2 improvements enabled?

1.2 Outline

The paper is laid out as a systematic literature review with a focus on layer 2 solutions in blockchain, what security problems they introduce, and how they can be utilized in the industry. Section 2 covers other literature reviews, as well as the contribution of this paper. Section 3 covers our methodology. Section 4 covers existing solutions and proposed solutions for layer 2. Section 5 is focused on the security problems related to layer 2, while section 6 covers detection and mitigation mechanisms. Lastly, in Section 7 we cover what current business applications and use cases layer 2 can be used to improve. We didn't have time to include all papers retrieved in the search query.

2 Related Works

In this section we will examine other related work in the field of blockchain and scalability, specifically in layer 2. Many great studies have been made that shine light on the problem. Table 1 shows the studies, their main contributions and how this paper differs from them. The authors of [8] focuses on the scalability on the different layers of blockchain. They emphasize that the inherent low TPS of PoW in BitCoin of 7 is no where good enough to compete with e.g. Visa and its 4000 TPS. The paper thoroughly gives on overview of relevant solutions in both layer 0, layer 1, and, layer 2 and references the newest directions at the time of publication, however the paper tends to emphasize layer 1 solutions over the other layers. The authors in [9] have taken a similar approach for the literatture review. They also include most relevant solutions at the time of writing. In addtion, they have added a more extensive pros and cons table, that compared all the different scalability solutions in the different layers. The paper referenced in [10] offers an excellent and in-depth overview of relevant layer 2 solutions to scalability. The paper gives both a technical and a hands-on of the different solutions due to its uses of use cases to illustrate. The paper also emphasizes why layer 2 solutions potentially have higher impact on scalability than layer 1 solutions, stating that current layer 1 solutions alone does not significantly improve TPS in a scalable matter. Written before Ethereum 2, the paper mentions that the transition to PoS can potentially have a massive impact on TPS, when combined with other layer 2 solutions. The authors in [2] focuses on the underlying roots of the problems in scalability in blockchain, and how it impacts implementation in different sectors. They conclude that the large storage requirements needed to replicate the complete ledger in order to run a node, together with the slow TPS are the main factors for the slow adaptation of blockchain. Especially, these factors have a major impact in the IoT industry, where storage is limited and real-time data is crucial to have a high and near instant TPS and data validation time. However, the paper only narrowly addresses the scalability solutions in layer 2. [11] very shortly outlines the most frequent layer 2 solutions and creates good models for understanding their concepts. However, due to the papers short length, it lacks some in-depth analysis of how the different solutions compare. In [12], the authors examine scalability in blockchain based manufacturing. The paper offers a great overview of how scalability impacts the real-world application of blockchain. The paper concludes that layer 1 solutions are better represented in the literature than layer 2, at their moment of writing. The authors of [13] focuses on the taxonomy of layer 2 solutions and gives an overview of the different approaches. Furthermore, the paper gives an extensive look into security and privacy issues on the different protocols.

Year	Citations	Paper	Main contributions	This paper
2020	563	[8]	Focuses on layer 1 and 2 solutions to scalability, with an emphasis on layer 1 solutions.	Focuses on security problems related to layer 2 solutions. Also includes more recent papers.
2021	18	[9]	Offers insight into layer 0, 1, and 2 solutions for scalability. Compares the different solutions in TPS and a pros/cons list.	Has more recent papers and also includes use cases from current literature.
2021	73	[10]	Offers a great overview of most solutions on layer 2 and showscases the different solution in different use cases.	Offers more recent papers and focuses more on security
2021	106	[2]	Examines underlying roots of scalability issues. Concludes that high storage requirements and low TPS are the main factors.	More recent papers and more focus on security issues related to layer 2.
2022	0	[11]	Briefly describes layer 2 solutions.	More extensive description of layer 2 solutions. Also includes security risks from current literature.
2022	2	[12]	Examines how blockchain scalability affects manufacturing. Concludes that layer 2 is underrepresented in literature	A more general focus, also more on security and use cases from different sectors.
2023	30	[13]	Gives an overview of layer 2 solutions but also analyses them in a security and privacy context.	More focus on use cases from different sectors.

Table 1: Related papers

3 Methodology

The search and paper selection process used to choose the literature for this paper is explained in this section. The methodology combines parts from [14, 15, 16] which offer guidance on how to draft a systematic literature review and, for paper inclusion, how to apply snowball sampling. Below is a summary of each stage in the paper selection process; a more thorough explanation of each phase will be provided later.

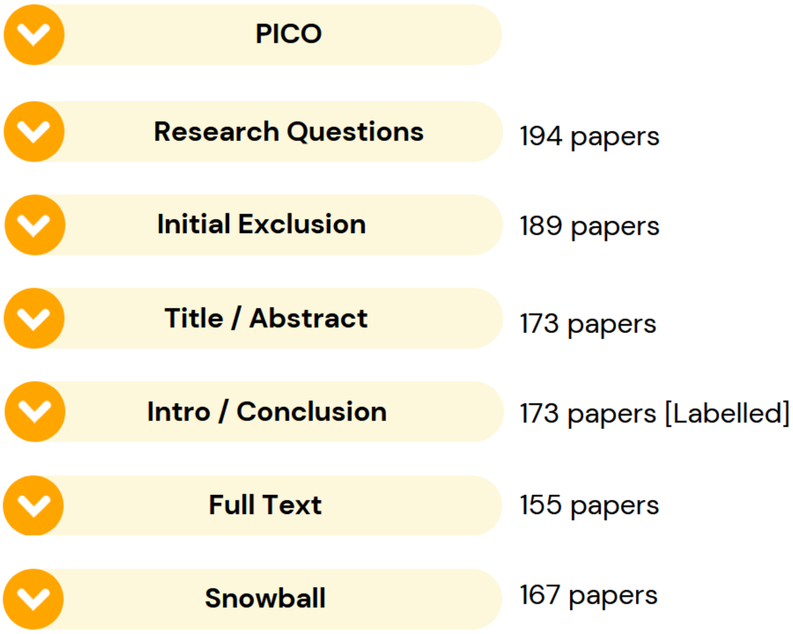

Figure 2: Procedures for selecting papers and the number of papers remaining after each round of exclusion and inclusion.

3.1 Search Strategy

The structure known as **PICO (Population, Intervention, Comparison, Outcome)** is frequently used in the development of strategies for searching for systematic literature reviews.

- *Population*: Information systems and network infrastructures using layer 2 solutions are included in the population of interest. Only papers focusing particularly on security problems on blockchain (with layer 2 solutions) were accepted because blockchain as a generic concept is deemed too broad.
- *Intervention*: The state channels, sidechains, and off-chain computations that are suggested as solutions are represented by the intervention. Every single one of these interventions presents a unique strategy for enhancing the scalability of blockchain technology. For example, sidechains offer parallel chains for higher throughput, state

channels facilitate off-chain transactions, and off-chain computing moves specific computational operations off the main blockchain. The literature attempts to shed light on these interventions' functions, technical aspects, and possible effects on scalability by closely analyzing them.

- *Comparison*: Comparing the various layer 2 solutions to one another and, more importantly, to conventional on-chain transactions is the comparative part. The goal of this review is to draw attention to the relative benefits and drawbacks of each strategy. Researchers examine variables such as transaction speed, financial efficiency, security consequences, and general scalability enhancements. Comprehending the relative advantages of various solutions assists in determining the best methods for particular use cases and enables the well-informed choice of layer 2 solutions in real-world blockchain applications.

- *Outcomes*: When we talk about the outcome, we mean the evaluation of how well layer 2 solutions work to solve scalability problems and reduce security risks. For this, it is necessary to measure how interventions affect the utilization of resources, confirmation times, and transaction throughput. The result also evaluates how well these solutions perform in resolving the security issues that have been identified about layer 2 implementations. A thorough grasp of the potential advantages and practical implications of utilizing different layer 2 solutions in blockchain systems is intended to be provided by the literature through a methodical analysis and presentation of these results.

The important keyword was identified from these criteria, *blockchain AND ("layer 2" OR "layer two").* Since the search query helps to return a set of appropriate research that specifically addresses the integration of blockchain with layer 2 solutions, it has been concluded that this keyword is the most significant. After that, the systematic literature review may assess and investigate these sources to provide a thorough picture of the current status of research in this specific field.

Four sources were used for the initial database searches of Blockchain scalability articles: Google Scholar, DTU FindIt, Scopus, and IEEE Explore. Google Scholar's initial search for "Blockchain AND Scalability" turned over 139000 papers—too much to handle practically. Alternatively, a second query was used to include both the discovered keywords and remove any potentially unrelated papers: *blockchain AND ("layer 2" OR "layer two")*

Using the new query, 11,300 papers were found in Google Scholar, and 194 papers in total were found on DTU FindIt. We agreed to use only DTU FindIt.

3.2 Inclusion / Exclusion Process

To determine which papers to include in this study, several exclusion steps and one inclusion step were carried out.

3.2.1 Initial Exclusion

The following exclusion criteria were used in the first exclusion step to filter out papers; any that didn't match every requirement was removed. A total of 5 papers were excluded

- Papers from 2015 or newer
- English language paper only
- Layer 2 Solution-related papers only
- Peer Reviewed
- Free access through DTU findit.

3.2.2 Title and Abstract Review

We uploaded all the literature in the Rayyan app which is AI AI-powered tool for systematic literature review. After the initial exclusion, we divided 189 papers equally among the 4 of us for a quick title and abstract review. The purpose of this exclusion step was twofold: first to exclude any irrelevant papers and duplicates and second to identify which research questions could be answered by the paper (e.g., other surveys, detection paper, mitigation). If the abstract of a paper did not give any indication of being useful for the research questions, the paper was excluded. 16 papers were excluded in this step, and a total of 173 papers were included in the next step.

3.2.3 Introduction / Conclusion Review

The examination of each paper's title, abstract, introduction, and conclusion constituted the final elimination phase. Since the amount of literature was not very large, we intended to distribute it equally across all the papers. If one reviewer thought a paper was inadequate or unrelated to this work, it was eliminated. Using Rayyan allowed us to see which articles were included, omitted, and maybe, which was incredibly helpful. After that, we utilized this software to filter the literature, classify it according to our needs, and label it—for example, publications that addressed privacy and scalability, related work, and so forth. Instead of removing the papers from this stage, we sorted them using a filter. 9 papers were removed in this step.

3.2.4 Full-Text Review

Lastly, the full-text review was conducted for the categorized papers. To eliminate any repetitive papers, reviewers were given additional tasks of reviewing the papers they had previously evaluated. To enable all reviewers to comprehend the contribution of each paper without having to read it themselves, a brief comment was produced for each included paper. Further 19 papers were removed in this step. There were still 155 papers that could be relied upon to be valuable for this survey of the literature. for each included paper.

3.2.5 Backwards Snowballing Sampling

Our query left out a lot of literature reviews, that were not directly related to layer 2 solutions. By snowballing through the included literature reviews, reviews that focus on scaling in general were added. Through their references scaling solutions used by Ethereum, and Bitcoin were included. The final count of peer-reviewed references included in this publication, after snowballing, was 167.

4 Layer 2 solutions

Recognizing the limitations of traditional layer 1 approaches to scalability, researchers have turned their attention to layer 2 solutions. This section provides an overview of the most important layer 2 solutions.

As mentioned in Section 1, layer 2 solutions propose improvements to scalability without changing the underlying data structure of the blockchain. While Layer 1 solutions involve fundamental changes to the blockchain's consensus mechanism, data structure, or block size, layer 2 solutions operate off-chain. This allows for a certain degree of flexibility, enabling developers tackle optimizing scalability without directly altering the main blockchain's foundational design. This effectively means that researchers and developers are building new protocols on top of the core architecture to mitigate the issues. This section will examine specific layer 2 mechanisms, such as state channels, sidechains, and rollups, and how they each contribute to scalability, but also investigate if they introduce new challenges in security or decentralization.

4.1 State channels

State channels represent a layer 2 communication method allowing participants to conduct transactions off-chain. Essentially, a state channel functions as a protocol enabling two parties to engage in numerous transactions between them, utilizing the mainnet blockchain only to verify the initial and final transactions in their interaction. This approach significantly improves transaction speeds by reducing validation time on the mainnet.

Payment system	TPS	Latency	Coin
Lightning network [17, 18]	1,000	387	Bitcoin
Raiden network [19, 20].	unbounded	same as LN	Ethereum
Teechain [21]	1,000,000	350	Bitcoin
Rapido [22]	Same as LN	100	Bitcoin
Speedster [23]	1,000,000	80	Multiple

Table 2: Current solutions and proposed solutions

Payment channels, a specific form of state channels were introduced as Duplex Micropayment channels in [17] and [18], with the latter becoming known as the Lightning Network.

An adaptation was later made for Ethereum with the Raiden network. In these implementations, a channel between two nodes is established, and a private ledger manages transactions. To open a channel, the involved parties must agree on an initial transaction state and transfer funds to a shared wallet or smart contract. Thus, the public blockchain only records the opening and closing transactions, maintaining the privacy of the transactions within the channel.

The use of payment channels enables transactions of any size, facilitating microtransactions without paying transaction fees. The verification process within the private ledger involves the *multisig* protocol, requiring multiple signers to authorize a transaction. In payment channels, both parties must sign with their private keys.

Moreover, payment channels offer heightened privacy, as all transactions between the initial and final states remain visible only on the private ledger accessible to the two parties involved. Additionally, transactions are safeguarded against cheating through the inherent logic of the shared smart contract managing the channel. Both parties can independently withdraw their funds from the current state, and a time lock is implemented to release funds in case of inactivity or intentional transaction halting by one party [19, 20].

More adaptations have been made in payment channels, such as the work done in [24]. In their paper, the authors propose a novel variant of payment channels, Sprites, that reduces the collateral cost of a trading channel, that is, the locked funds being held while a channel is opened. Additionally, the authors added support for partial withdrawals and deposits, where parties keep a connection open after making micro transfers in and out of the channel.

In [21] the authors introduce Teechain which adds asynchronous transactions to the payment channel. Teechain adds treasuries, secured by hardware trusted execution environments (TEEs), to establish off-chain payment channels, ensuring parties cannot engage in misbehavior. These treasuries, equipped with collateral funds, facilitate efficient and secure transaction exchanges without the need for interaction with the underlying blockchain. Furthermore, they introduce committee chains, which replicate states in channels as back-ups, if a communication failure happens. The authors claim to have reached a 33 times higher throughput than state-of-the-art lighting networks at the time of writing.

Another TEE state channel network is Speedster [23]. Speedster is designed to mitigate some of the problems present in other designs, such as e.g: expensive creation and closure of channels, strict synchronization between the main and side chain channels, frozen deposits, and inability to execute multi-party smart contracts. It is an account-based state channel system, that leverages TEE to optimize performance. Speedster functions by creating enclave accounts, and smart contracts to manage the states of the enclaves. Enclaves create certified channels between each other, and because of the TEE the channels are dispute-free, and the channels can keep the main chain state channels up to date. This property allows the channels to close at any time. Speedster achieves a very high TPS and generates far less on-chain data than other solutions, but it is reliant on the Trusted Execution Environment to operate.

To address privacy issues [22] introduces Rapido, an innovative multi-path channel designed to address transfer overloads and privacy leaks. Rapido addresses these issues by splitting and distributing payments across multiple paths. The protocol uses a novel smart contract, D-HTLC, to encode the protocol, providing an effective solution to enhance both scalability and privacy in off-chain transactions. A more recent study referenced in [25] also addresses privacy issues in payment channels. The paper proposes a novel heuristic-based distribution of funds while preserving anonymity for the parties involved. The paper has also improved on the HTLC message exchange protocol, which will not ward off the Flood and Loot attack mentioned in [26].

4.2 Side-chains

Side chains was a concept developed to ease the load on the main network and allow users to transact for a lower fee. Side chains are attached to the root of the main chain. Ethereum proposed their solution in 2018

4.2.1 Pegged side-chain

The pegged-side chain [27] was a novel technology. It invented the side-chain technology that allows assets to be transferred back and forth, between different chains. The technology also allows side chains to interact with each other through the main chain. A chain sends its coins to the main chain, and the other side chain claims them using a simplified payment verification proof (SPV). To synchronize chains there are two waiting periods. During the confirmation period, the child chain locks the coin on the main chain. This period takes a couple of days, to avoid denial of service attacks. The next period is the contest period. In the contest period, another proof can be published with another chain with more aggregate work, not including the block with the desired transaction in it. If this happens, it validates the first block. That is called an aggregation proof. The authors acknowledge weaknesses in their paper, such as the opportunity for malicious attackers to perform e.g. fraudulent transfers. Other risks are the centralizing of mining and a soft-fork.

Plasma

One of the first solutions proposed was Plasma [28]. Plasma was an Ethereum solution proposed to ease the network load on the Ethereum main net. Plasma chains were not as feature-rich as the main chain, as they do not allow smart contracts but only basic token transfers. The goal was to develop a side chain design where transactions can happen off-chain but be enforceable on the main chain. The state would be enforceable by using fraud proofs, and proof-of-stake validators. Plasma utilized the MapReduce framework to conduct transactions and then put the side chain state digest on the main chain. Plasma placed the trust in the chain operator to minimize the amount of work performed by nodes regarding consensus. This introduced massive problems that they could not mitigate. Plasma chains were dropped because of the mass exit problem. The mass exit problem is if the chain operator turns malicious, the operator could make invalid transactions and start draining the users of the chain's wallets. Exiting a chain takes some time, and if all the users try to exit at the same time the Ethereum network would be heavily congested, and the malicious operator could drain many if not all the user's accounts. This drawback made Ethereum ditch the Plasma chains in favor of layer 2 scaling protocols.

Bitcoin rootstock
Rootstock (RSK) [29] is a smart contract platform two-way pegged to Bitcoin. The RSK platform provides smart contracts that are backward compatible with the Ethereum VM, and it is therefore an alternative to Ethereum if users want to utilize Bitcoin security infrastructure. To avoid high fees when trading small transactions RSK supports micropayment channels. It utilizes a novel dynamic hybrid merge-mining federated consensus protocol to ensure consensus security and a low latency network for fast payments. It still uses proof-of-work, as they claim it's the lowest cost consensus system that prevents the re-write of blockchain history. RSK utilizes the DECOR+ block reward system to maximize BTC mining efficiency. The scheme avoids late switching by creating uncles. The network is protected against 51% attack by introducing federated checkpoints for mined blocks. Carefully chosen Federation members and clients can together choose the best chain. If the hashing power is over 66% of the maximum BTC hashing difficulty, they stop using the checkpoints. The federation members are well-known and community-respected members.

4.2.2 Off-chain

In off-chain computations, the most exciting solutions are TRUEBIT and Arbitrum. TRUEBIT, as proposed in [11, 30], outsources computations while maintaining verifiability. The core idea behind off-chain computations is to delegate computational tasks to external entities while ensuring the ability to verify the results. This is achieved by leveraging off-chain solutions for scalability, requiring significantly less computational power.

In the context of TRUEBIT, miners' computational capabilities are enhanced through TRUEBIT smart contracts. A key element is the presence of a verification game known as a subroutine, employed in cases of disputes. On the other hand, Arbitrum differs from Truebit through its focus on enhancing scalability and privacy in smart contracts. It introduces an additional layer to the consensus mechanisms of a blockchain by deviating from the reliance on existing ones.

Arbitrum operates by executing smart contracts within a virtual machine where contract rules are predefined. This approach contributes to scalability by substantially reducing the cost associated with contracts. The exploration of off-chain computations is not exclusive to this context; [9] also delves into this subject. Within this paper, TRUEBIT and Arbitrum, previously mentioned in [11], are further discussed.

4.2.3 Cross chain

The platforms used by blockchain applications are struggling to operate together, when they are on different systems. Third-party entities often bridge communication gaps between these systems. The problem arises when applications need to transmit information across the chain, a requirement that hinders widespread adoption of the technology. The need for robust cross-communication and scalability is one of the things blocking the widespread adoption of blockchain. Two noteworthy heterogeneous cross-chain techniques, namely Polkadot and Cosmos, address these challenges.

Polkadot distinguishes itself through a unique design that avoids awkward functionalities. It supports dynamically robust data structures capable of global existence, facilitated by Relay chains. Polkadot achieves scalability by utilizing para chains, that have high capabilities bound in the security of Polkadot's relaychain.

In contrast, Cosmos presents an innovative blockchain network comprised of independent chains known as zones, supported by the Byzantine Fault Tolerance (BFT) consensus protocol, exemplified by Tendermint. As discussed in [9], the paper emphasizes interoperability among independent and heterogeneous blockchains, presenting two distinct methods: Polkadot [11] and Cosmos, exclusively covered in the referenced paper. Cosmos is powered by Tendermint BFT. This consensus algorithm ensures high performance, consistency, strict accountability, and control over the behavior of malicious actors.

4.3 Roll ups

Roll ups is a hybrid solution, in between the full of-chain solutions and on-chain solution. The solutions differ regarding when information is posted on the main chain. With off-chain solutions such as e.g Plasma or the Lightning Network, transactions are posted in bulk on the main chain. In rollups, some information from every transaction is recorded on the main chain. It is that every time a transaction is made on a side chain, it's posted on the main chain. There are two types of roll-ups, optimistic roll-ups and zero-knowledge rollups.

In [31] they define a system of rollups for the Metaverse. They forecast blockchain to be one of the driving forces in the Metaverse and propose a solution using optimistic roll-ups and sidechain protocols to reduce the delay time in account settlements. They introduce the concept of layer-2-sphere (L2S) where a business organization deploys a consortium blockchain. The contact between those is facilitated by smart contracts. The authors chose a consortium chain, to hide business logic from competitors.

Zero-knowledge roll-ups is a topic of interest for many researchers. [32, 33, 34, 35] all research zero-knowledge roll ups. [32] evaluates blockchain techniques for scaling solutions and concludes the most promising one for tackling the Internet of Everything (IOE's) problems is zero-knowledge roll-ups. They argue zero-knowledge proofs no trust architecture is superior to that of optimistic roll-ups, since it does not trust users to not behave maliciously. They argue the need for a role-based roll-up structure if only some actors can submit changes. [34] proposes and evaluates a layer 2 solution for Ethereum with zk-roll up. They mitigate the "Token Transaction Problem", and formulate two functions, one to validate the Merkle root and one for updating the Merkle root. In the end, they showcase results stating that the gas cost is down 85% with a batch size of 50tps or above. To explore some of the privacy-enhancing abilities [33] formulate a concept of modular zk roll-ups. The article states problems regarding zk roll-ups being deployed as multiple smart contracts, and therefore being quite expensive. Another problem they want to mitigate is the high expertise required to develop and audit zero-knowledge circuits. They formulate an idea where the smart contracts take additional information and allow smart contracts to support multiple roll-ups at the same time. They claim this design would reduce the cost of setting up a zk roll-up by 99%.

[35] argues the Ethereum fee model is not the most suitable model for layer 2 fees. The article states that the solution can be used for other use cases than currency exchange or business. They then evaluate models used in channel access, to see if they are applicable to the zk-rollup model. They evaluate the Fixed Window Common Flow Control, Fixed Window Variable Flow Control, Sliding Window Flow Control, and lastly Leaky Bucket Flow Control. All of the models have a slightly higher cost, but they argue they could be implemented to allow for new fee models.

To increase the efficiency of rollups Ethereum proposed the EIP-1559. It proposes to change the fee structure of Ethereum and has been adapted by some rollups. It introduces a scheme that reduces prices paid by users, and makes its cryptocurrency a deflationary currency by burning some of it during operations. In [36] they study the negative consequences the proposal has on rollups such as Polygon and arbitrum. The study concludes that the EIP-1559 structure is only fitting for a PoW blockchain, as it makes miners lose incentives.

4.4 Proposed layer 2 blockchains

W3Chain [37] is a layer 2 blockchain that has measured increased performance compared to the current solutions. The chain introduces novel solutions in the reconfiguration of committees, query APIs, and how to handle cross-shared APIs. Furthermore, they achieve their biggest performance gain by decoupling the correctness of the blockchain into two parts. They divide it into two parts, chain consistency, and block correctness. Partitioning the correctness of the shard, allows the chain to delegate the answer consistency to the main chain. Therefore a chain does not need to store the full data and can reconfigurate faster. The main chain is called the "Time Beacon Chain". It is connected to W3Chain with smart contracts, and W3Chain calls the contract with basic information about blocks when they are built. Testing shows that W3Chain is secure against the most common attacks, and can achieve a TPS close to 10.000.

Another proposal is L2Chain[38]. L2Chain also saves the state digest of the layer 2 chain on the main chain and performs transactions on the side chain. L2Chain reaches an improved TPS and secure transactions by having the layer 2 chain as a Trusted Execution Environment (TEE). L2Chain utilizes an RSA accumulator for the permissioned setup. The RSA accumulator introduces overhead costs that lead to a higher latency than other solutions. They try to mitigate this problem by building a witness cache, but it's costly since the witness state updates every time a block is published. The author's solution is splitting up the cache into multiple groups based on frequency, achieving bounded storage and update costs.

When compared with other papers, L2chain achieves increased throughput.

4.4.1 Offline payments

Current offline payment systems are limited in their capabilities, but blockchain could provide an improved solution. [39] builds on the advancements in layer 2 solutions, to formulate Xipcoin for offline payments. Xipcoin uses trusted platform computing (TPM) to ensure the integrity of the devices and utilizes the TPM to hold the coins. Customers and merchants sign up by generating a private key, and their wallets can then either be topped up by other members offline, or by using an online service. When a transaction is performed between a customer and a merchant they validate each other's certificates and store the transaction. When either is online again, they submit the transaction to the chain.

Another paper enabling offline payment with blockchain is [40]. The paper formulates an approach to creating mesh networks for offline usage, where payments can still be made over the lightning network. The paper contains an analysis of how to construct the mesh network topology, and channel assignment for the users, and evaluates the results. They achieve a success rate of 95% of payments, and the last 5% fails because of capacity problems on the channels.

4.4.2 Other solutions

[41] formulates a scalable approach to atomic cross-chain calls without modifying the code of the blockchain platform. To reach cross blockchain consensus the paper proposes to sign block headers when needed. They use an example setup where multiple companies want to keep information secret but share a blockchain.

Bitcoin has adapted various layer 2 solutions, but there is still room for improvement. [42] proposes two improvements to Easypaysy. The first is deniable authenticated payments, that is unlinkable, deniable authentication, and non-repudatable. The authors achieve this by producing addresses akin to the stealth addresses utilized by other cryptographic currencies. The other contribution is Hierarchical Accounts. The accounts allow accounts higher up in the hierarchy to spend funds from the lower-ranked accounts. This protocol also has the property of unlinkability and non-reputability.

To incentivize users in the bandwidth reward use case [43] propose a new off-chain micro payment pool. The bandwidth use case is when a user requests some content, and users chime in and help form a network where multiple parties each transmit part of the content to the user. In [43] the user creates a pool, with a deposit, collateral, and a timelock. The user then performs handshakes with peers, and the peers verify from the user's Merkel root that the pool has the required deposits. After receiving, the user sends service settlements from the pool off-chain, which can then be redeemed by the receiver on-chain. To avoid double spending the smart contract checks the remaining amount in the pool, and slashes the deposit if it deems the user is double-spending.

Lightpay [44] is a payment channel network aiming to solve the problem of long payment confirmation time and limited throughput in Bitcoin. When the network congestion is high, the lightning network has the split the payment into multiple smaller payments for them to be processed. This results in delays and higher processing fees. Lightpay secures them by performing the payments atomically off-chain. Lightpay utilizes an adapter scheme to reduce the fee required for the payment process. Compared to other solutions in the domain, Lightpay has the same security guarantees, but a lower overhead, and a higher success rate.

5 Security issues arise with Layer 2 solutions

In the field of blockchain technology, the introduction of Layer 2 solutions has presented several security problems that need to be carefully considered, even though they promise improved scalability and transaction throughput. Careful evaluation is necessary due to the unique complications and potential vulnerabilities introduced by Layer 2 solutions, including those seen in the Bitcoin Lightning Network and other off-chain scaling techniques, So in this paper, we discuss different security issues and ways to mitigate them.

5.1 Flood and Loot Attack

“Flood and Loot” refers to a systematic attack on the Lightning Network, a second-layer scaling solution for Bitcoin. In this attack, an adversary triggers the simultaneous closure of multiple Lightning channels, causing a flood of transactions on the Bitcoin blockchain. The high transaction volume overwhelms the blockchain’s capacity to settle debts properly, creating an opportunity for the attacker to steal funds potentially. This issue is also addressed in the literature review [26] and mentions the primary concern is a systemic attack on the protocol where an attacker triggers the simultaneous closure of numerous Lightning channels which results in a high volume of transactions on the Bitcoin blockchain, making it challenging to settle all debts properly and allowing the attacker to steal funds potentially.

5.1.1 Mass exit

This paper [45] delves into the tricky balance between privacy and scalability in blockchain-based cryptocurrencies. It points out that the current big players like Bitcoin and Ethereum have their struggles, being too public and not keeping up with transaction demands. Even privacy-focused alternatives like Zcash and Monero face their challenges, especially when it comes to scalability. This paper also introduces us to various scalability solutions like Plasma [4.2.1] and ZK-Rollup [4.3], but it doesn’t shy away from mentioning their issues, such as mass exits and the need for trust.

Facilitating off-chain calculations and interactions is a recurring theme in these technologies. With this method, a sizable number of transactions can be handled off-chain by a middleman or operator. Periodically, a brief overview of these off-chain transactions is posted on the main blockchain to ensure transparency. When faced with a mass exit situation, a major drawback appears in several of these systems. A ”mass exit” occurs when the designated operator, who is in charge of supervising off-chain transactions, is malicious or untrustworthy. In this case, users are forced to demonstrate that they are the rightful owners of their assets on the main blockchain to securely leave the system. Regrettably, the surge in ownership proofs that occurs during a mass exit event causes congestion on the main chain, which could prevent users from quickly leaving the system and result in delays. In addition to the problem of mass exits, some of the current solutions include transaction integrity flaws. Robust measures to guarantee the integrity and authenticity of transactions are absent from certain implementations. Moreover, even though some solutions use zero-knowledge proofs to improve the integrity of off-chain and blockchain systems, the transaction information in these systems is still available to the general public. Therefore, privacy issues in the blockchain realm continue to exist.

5.2 Smart Contract Attacks

The literature [46] has addressed attacks using smart contracts that provide different risks in Layer 2 solutions. Through the use of code execution order, reentrancy attacks can call a function repeatedly, allowing for unauthorized fund withdrawals. Attacks that manipulate arithmetic operations have the potential to compromise the status of the contract along with Front-running attacks that make use of advanced knowledge by focusing on off-chain transactions. Denial-of-service (DoS) overloads networks or contracts, leading to delays and congestion. Unprotected personal information could result in privacy violations, and improper random number generation could jeopardize results that depend on chance. To reduce these dangers, attention to secure coding techniques, thorough testing, and awareness are crucial.

5.3 Data Availability Problem

Three general approaches to data availability in the L2 system are described in [47]. The literature discusses the challenges related to data availability in layer 2 systems of blockchain, with a focus on Data Availability Committees (DAC). It encounters significant security challenges. The primary concern is the vulnerability of compromised DACs, where malicious control over a substantial number of members can lead to data manipulation, jeopardizing the integrity and availability of critical information. This manipulation extends to the rollup state [4.6], potentially hindering users from executing transactions and exposing them to financial risks. Liveness issues further exacerbate the problem, impeding the system's ability to process transactions seamlessly. The fundamental reliance on trust in DAC members raises the specter of trust dependency, posing a threat to the overall security of the blockchain system. Attempts to introduce financial incentives for proper behavior face challenges, with potential misalignment between incentives and actual node conduct, along with the risk of bribery influencing rational behavior. Addressing these multifaceted security issues is imperative to fortify the reliability and trustworthiness of DACs in blockchain ecosystems.

6 Detection and Mitigation

This section describes the security issues mitigation and detection strategies proposed within the research.

6.1 Detection Mechanism

This section covers all papers, that are related to detection approaches and compares several techniques for each category.

In Table 3 papers are describing the detection and mitigation of security issues of blockchain. Each row describes the year, model or protocol, main contribution, and related papers

Year	Model	Main Contribution	Papers
2023	Rebalancing Model	The approach seeks to improve the security and effectiveness of rebalancing procedures addressing privacy issues and fostering the enhancement of the Layer-2 ecosystem as a whole.	[25]
2023	CryptoMaze	Detects security issues associated with high-valued payments in Payment Channel Networks	[48]
2023	Data Availability Committees (DACs)	By detecting and dealing with adversarial behavior in DAC nodes, the protocol seeks to maintain the security and dependability of the L2 system without making unwarranted assumptions about trust.	[47]
2020	Arwen Trading Protocol	Emphasizes preventing traders from giving up custody of their coins to address issues with safe cryptocurrency trading on centralized exchanges.	[49]
2021	Adaptive Dispute Cutoffs (ADCs)	Allow to handle a larger number of disputes and prevent fraud effectively	[46]

Table 3: Detection mechanisms

As a countermeasure, the literature [25] on the rebalancing model has included an overview of current plans and the reasons behind their methodological shortcomings. An imbalance affects the network's overall efficiency when nodes have trouble forwarding transactions because there are more one-way transactions [48]. Rebalancing requires providing details about the current condition of the channel, including the entities and amount being transferred. When users disclose private information, it might also expose individual channel balances, which is a privacy breach. A few of the current strategies, including Revive, Hide and Seek, Imbalance measure and proactive channel, Hubs, rebalancing, and Rebal, are also mentioned in the study. By filling in current research gaps, the suggested solution seeks to improve the general security and effectiveness of rebalancing processes. To guarantee a strong and secure Layer-2 ecosystem, it is also important to improve privacy preservation, address smart contract weaknesses, and promote interoperability among various Layer-2 solutions. To increase the throughput of the blockchain and combine transactions outside of it, other detection techniques, such as the one suggested by [50], also employ comparable techniques. Supernodes and supernode-based pooling are introduced in Reference [51] to overcome the difficulty. Pooling helps small nodes with their liquidity problems by redistributing funds within a pool to its supernode's external channels, hence fostering balanced fund distribution.

The literature [48] explains how Payment Channel Networks (PCNs) facilitate off-chain payments to address blockchain scalability challenges. The CryptoMaze protocol aims to address security issues associated with valuable payments being divided and sent via several routes. In contrast to current multi-path payment methods, CryptoMaze protects against the possibility of a wormhole attack and guarantees atomicity. It accomplishes this by guaranteeing unlinkability between partial payments and preventing the formation of several off-chain contracts on shared edges. In addition to practical implementations on Lightning Network instances demonstrating efficient routing with minimal computational and communication costs, exceeding existing state-of-the-art payment protocols, the protocol's formal design in the Universal Composability framework proves its security. CryptoMaze offers a safe and private way to manage off-chain payments in second-layer blockchains.

The subject of a different study [47] is roll-up systems, which keep all transaction data on a layer 1 parent chain, like Ethereum. To guarantee that the data is constantly accessible, these systems rely on the L1 nodes' security. They go on to discuss alternative strategies, like off-chain data that is periodically sampled using data availability and off-chain data that is kept by a data availability committer (DAC).

Rami Khalil and Naranker Dulay [46] propose that restricted transaction processing capability is addressed by the adaptive dispute cutoffs (ADCs) technique. The risk of fraud is reduced since it makes sure that users may still report fraudulent activity even when the blockchain is congested. Compared to their non-adaptive counterparts, second-layer protocols that use the ADC mechanism are more efficient at handling a higher volume of disputes and preventing fraud because they dynamically modify dispute period lengths in response to the volume of disputes.

7 Use cases

Layer 2 solutions mitigates some of the problems that blocks a broader adaptation of blockchain technology in various applications. Vital for this are the increased TPS, and lower latency, which enable more distributed applications in blockchain. In this section we will dive deeper into the current and most recent business applications and use cases developed using the layer 2 of blockchain.

Year	Paper	Use Case area	Main contribution
2023	[52]	Voting	Review of current e-voting trends. Conclude that scalability is the biggest issue to major adoptation.
2022	[53]	Voting	Computer Vision system for couting mailed in ballots. Uses layer 2 to train their model.
2023	[54]	Legal and Governance	Decentralised digital evidence using Polygon.
2023	[55]	Legal and Governance	Investigates how the Indonesian government can adopt blockchain by comparing different layered models.
2021	[56]	Legal and Governance	Preventing rumour spreading created by social bots. They create a decentralised social based on state channels to communicate between two parties.
2022	[12]	Manufacturing and Supply Chain	Survey of current manufacturing using blockchain. Concludes that layer 2 solutions and under-represented in the literature.
2023	[30]	Manufacturing and Supply Chain	Examines shared manufacturing to increase decentralization and trustlessness between manufacturer and consumer. They utilise rollups to scale horizontally.
2023	[57]	Manufacturing and Supply Chain	Reducing food waste by optimizing ineffecient supply chains. They utilise state channels to improve efficiency.
2022	[58]	IoT	Improves Crowdsensing but improving scalability to enabling real-time data collection using off-chain computations.
2023	[59]	IoT	Compares different layer 2 solutions in the field of UAVs.
2023	[60]	Computer Science	Improves blockchain based RT by reducing costs by combining on-chain and off-chain techniques.
2020	[61]	Computer Science	Decentralized identity management by moving verification processes off-chain.
2021	[62]	Computer Science	Graph data storage using blockchain. Leverages on layer 2 techniques to improve scalability.
2023	[63]	Gaming	DeFi platform for gaming. The improve scalability by reducing transaction costs by using state channels.

Table 4: Use Cases

7.1 Voting

One of the most studied cases is using the blockchain to implement a voting system. [52] performs a literature review of studies related to e-voting. They conclude most of them ensure voter anonymity and verifiability, but can't meet the scalability demands of a country. The reviewed articles use different techniques and rely on different cryptographic primitives, but the author finds none of the solutions to be sufficient. They believe it will be possible in the future when layer 2 solutions mature more.

Another solution for using blockchain in voting is proposed in [53]. The paper proposes a computer vision system that counts mailed in ballots, but the computation and training is decentralized on a layer 2 blockchain. The paper argues this would increase trust in the system, after the US presidential election had claims of election fraud in 2016 and 2020. The solution performs training and verification on Ethereum, and would be quite expensive and non-practical to execute.

7.2 Legal and Governance

Another area that has been represented in our research has been legal and governance. Researchers have here tried to utilise in particular the data immobility, that blockchain inherently has. The authors of [54] proposes a decentralized system built in Polygon to enhance the security and integrity of digital evidence, critical in modern legal proceedings. With a focus on overcoming issues such as data alteration and unauthorized access, their approach leverages smart contracts and blockchain technology to ensure data integrity. Furthermore, they emphasize the importance of evidence protected in a decentralised manner, so that the public or the legal system does not have to rely on a single central authority to trust their valuable evidence with. However two factors where affecting their results in a negative manner; scalability and security. With digital evidence having many different forms and sizes, storage becomes an issue the more widely the system is used. In their future works, the authors claim that storage and storage retrieval methods needs to be optimised for their solution to be scalable. Furthermore, they claim that the privacy of the actual evidence needs to be better protected with cutting-edge cryptography like zero-knowledge proofs or homomorphic encryption.

Another interesting study comes from the authors of [55]. Here the authors investigate the opportunities in applying blockchain architecture tailored specifically to meet the needs of the Indonesian government—IDNat-Blockchain. Having a country with a large population and a diverse and growing digital economy, the authors compares 4 different solutions, that combines techniques from different blockchain layers, that could help digitizing the country more in governmental affairs. The compare them in areas such as, speed, security, transparency, and cost. The study does not emphasize which combination would suit the governmental institutions best, and lets it be up for the reader and specific use case to decide.

To counter the negative effects caused by social, political, and economic disturbances through the spreading of rumors, the authors of [56] present a decentralized approach to mitigate the influence of social bots. In their solution, users collectively establish a secure and privacy-preserving decentralized social network. Users choose trustworthy neighbors within this network, and content is accepted only if it comes from a neighboring node in the decentralized social network. By enabling users to select their trusted neighbors, the solution impedes social bots from persuading users to accept and propagate rumors. To counter scalability and privacy-perserving issues, the authors utilise the layer 2 solution of state channels to communicate securely between two parties.

7.3 Manufacturing and Supply Chain

As mentioned in the related works section, the authors of [12] surveyed how blockchain scalability solutions are applied in manufacturing. They conclude that the potential of blockchain comes with limitations, most notably the inherent trade-off among scalability, decentralization, and network security. Different scalability solutions in blockchain aim to address this trade-off, offering diverse settings for these core properties or mitigating scalability issues. The study concludes that layer 2 solutions are underrepresented in general smart manufacturing system. More paramount, the study concludes that absence of industry implementations of proposed concepts raises questions about the practical uses of blockchain systems in manufacturing.

In [30] the authors are more hopeful, when exploring the potential of blockchain technology in revolutionizing the manufacturing industry, specifically through the innovative concept of shared manufacturing. The concept resolves around having a decentralized and trustless platform that facilitates collaborations between manufacturers and consumers, cutting the middleman out of the equation. The concept offers new solutions to conventional manufacturing and supply chain management, but faces new issues in regards to privacy, trust, and scalability. Some of the novel contribution that the authors make are utilising horizontal scaling through the layer 2 solution roll-ups. Additionally, the integration of social graphs, Non-Fungible Tokens (NFTs), and Self-Sovereign Identity is suggested for effective trust and reputation management.

To counter food waster due to inefficient supply chains, the study in [57] tries to mitigate the issue by creating a decentralised and dynamic distribution plan. They claim that by incorporating real-time quality information about perishable goods, their algorithm can facilitate the creation of distribution plans, allowing products to be strategically sold before reaching the end of their shelf life. The author utilise payment channels as the layer 2 solution to claim enhanced efficiency and preservation of privacy throughout the distribution process.

7.4 IoT

IoT has been identified as an area where blockchain technology could improve the security and trustless in a system with many distributed components. However, due to scalability issues, this is yet to happen in a broader adaptation of the technology. The authors of [58] propose a novel solution to improve crowdsensing, which is a method for collecting extensive data sets through people and their mobile devices. The challenges of privacy and trust within centralized crowdsensing systems are being addressed through the promising integration of blockchain technology. However, the scalability limitations of current blockchain systems make it challenging for crowdsensing applications to efficiently collect real-time or large-scale data. Their proposed scheme operates as a layer 2 solution, facilitating off-chain data evaluations within TEE (Trusted Execution Environments - an off-chain tamper-resistant processing unit) enclaves. This approach eliminates the need to propagate sensing data over the blockchain network, addressing scalability concerns.

Another interesting study examines how layer 2 solutions can be applied in order to improve security, privacy and trust in UAVs (unmanned aerial vehicles) [59]. The authors investigate different layer 2 solutions, such as roll ups, state channels and plasma chains to deliver efficient and privacy-preserving UAV services. They demonstrate the work through an interesting use case simulating aerial surveillance, where they highlight the potential advancements in credibility and effectiveness.

7.5 Computer Science

The study in [60] proposes a novel framework, that improves that already existing and popular framework RT (Role-based Trust Management). The proposed system, termed Layer 2 DecentrAlized Role-based Trust Management (L2DART), implements the RT framework on a public blockchain. It is strategically designed as a layer-2 technology, seamlessly integrating both on-chain and off-chain functionalities. This dual-layer approach is crafted to mitigate blockchain costs while preserving critical attributes such as immutability and transparency.

In the context of decentralized applications built on blockchains, achieving decentralized IdM (Identity Management) is essential. Certain applications demand a robust assurance that a given endpoint genuinely belongs to a specific subject. Presently, this verification is either conducted by the requesting party, which is impractical in blockchain applications, or through a centralized authority—contrary to the decentralization of blockchain. The study in [61] examines how layer-two blockchain-based protocols can be designed to establish the association between a subject and an endpoint in a decentralized manner.

The authors of [62] proposes a novel concept of a distributed graph data storage system tailored for the Ethereum ecosystem called GraphChain. By leveraging the GraphChain architecture together with Ethereum-based layer 2 architectures, they propose a 3rd generation Blockchain system specifically designed for the storage and processing of data, named Ontospace. Their paper contributes to improve the capabilities of blockchain systems regarding scalability in terms of efficient storage of data.

7.6 Gaming

This paper in [63] addresses the challenges posed by high transactions costs in decentralized finance (DeFi) and blockchain-based gaming platforms, hindering their widespread adoption. The authors introduce a novel DeFi gaming platform that utilises the advantages of layer 2 solutions to reduce transaction costs. The novel platform utilises the layer 2 solution of state channels to enable player interactions off-chain. The architecture and smart contracts of the platform prioritizes security and transparency. Through various test scenarios, the authors demonstrate the feasibility and effectiveness of the platform. They conclude that leveraging a layer 2 solution significantly reduces transactions costs, making DeFi gaming more accessible to a broader audience.

8 Conclusion

This systematic literature review aimed to address three key research questions about Layer 2 solutions in the field of blockchain scalability. The present discourse on blockchain scalability is enriched by this thorough examination of Layer 2 solutions and associated recommendations. This review offers important insights into the condition of Layer 2 technologies today, as well as their advantages and potential disadvantages, by combining the results of numerous research publications. The comparative study adds to a more comprehensive knowledge of the changing situation, and each option has advantages and potential drawbacks.

Numerous Layer 2 solutions are identified by the literature review, such as rollups, state channels, sidechains, Plasma, and zero-knowledge proofs. By lowering transaction costs, increasing scalability, and increasing efficiency, these methods seek to improve blockchain systems. The literature offers a variety of methods, including DACs, ADCs, CryptoMaze, Arwen Trading, and rebalancing models. These detection methods support a safe and scalable blockchain environment by improving security while also boosting Layer 2 Solutions' general resilience and efficiency. The incorporation of advanced detection and mitigation techniques is important in light of the ongoing evolution of blockchain technology to effectively handle new threats and maintain the steady expansion of decentralized systems.

Decentralized solutions are emerging to improve the security and integrity of digital evidence, which is another focus area in legal and governance. This literature addresses issues related to security and scalability, highlighting the necessity of sophisticated cryptographic methods and optimal storage. The study concludes with the gaming sector, where layer 2 solution integration is essential to lowering transaction costs for gaming platforms that support decentralized financing. Using state channels off-chain, the proposed DeFi gaming platform is a concrete example of how layer 2 solutions can promote accessibility and acceptance.

Overall, by addressing security issues and examining the revolutionary potential across industries, this literature analysis adds to an in-depth comprehension of the various uses of layer 2 solutions. The results highlight how blockchain technology is still developing and how layer 2 solutions are crucial enablers of innovation, security, and scalability in the digital world.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized business review*, 2008.

[2] D. Khan, L. T. Jung, and M. A. Hashmani, "Systematic literature review of challenges in blockchain scalability," *Applied Sciences*, vol. 11, no. 20, p. 9372, 2021.

[3] A. Chauhan, O. P. Malviya, M. Verma, and T. S. Mor, "Blockchain and scalability," in *2018 IEEE international conference on software quality, reliability and security companion (QRS-C)*, pp. 122–128, IEEE, 2018.

[4] A. I. Sanka and R. C. Cheung, "A systematic review of blockchain scalability: Issues, solutions, analysis and future research," *Journal of Network and Computer Applications*, vol. 195, p. 103232, 2021.

[5] "Layer 2 — ethereum.org." `https://ethereum.org/en/layer-2/`. (Accessed on 12/19/2023).

[6] D. Yang, C. Long, H. Xu, and S. Peng, "A review on scalability of blockchain," in *Proceedings of the 2020 the 2nd International Conference on Blockchain Technology*, pp. 1–6, 2020.

[7] A. Hafid, A. S. Hafid, and M. Samih, "Scaling blockchains: A comprehensive survey," *IEEE access*, vol. 8, pp. 125244–125262, 2020.

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

[9] J. Yadav and R. Shevkar, "Performance-based analysis of blockchain scalability metric," *Technical Journal / Tehnicki Glasnik*, 2021.

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

[11] S. Shirodkar, K. Kulkarni, R. Khanjode, S. Kohle, P. Deshmukh, and P. Patil, "Layer 2 solutions to improve the scalability of blockchain," *5th Ieee International Conference on Advances in Science and Technology, Icast 2022*, pp. 54–57, 2022.

[12] N. Rožman, M. Corn, G. Škulj, J. Diaci, and P. Podržaj, "Scalability solutions in blockchain-supported manufacturing: A survey," *Strojniski Vestnik/journal of Mechanical Engineering*, vol. 68, no. 10, pp. 585–609, 2022.

[13] 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.

[14] K. Petersen, S. Vakkalanka, and L. Kuzniarz, “Guidelines for conducting systematic mapping studies in software engineering: An update,” *Information and Software Technology*, vol. 64, pp. 1–18, 2015.

[15] P. V. Torres-Carrión, C. S. González-González, S. Aciar, and G. Rodríguez-Morales, “Methodology for systematic literature review applied to engineering and education,” in *2018 IEEE Global Engineering Education Conference (EDUCON)*, pp. 1364–1373, 2018.

[16] C. Wohlin, “Guidelines for snowballing in systematic literature studies and a replication in software engineering,” in *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering*, EASE ’14, (New York, NY, USA), Association for Computing Machinery, 2014.

[17] C. Decker and R. Wattenhofer, “A fast and scalable payment network with bitcoin duplex micropayment channels,” in *Stabilization, Safety, and Security of Distributed Systems: 17th International Symposium, SSS 2015, Edmonton, AB, Canada, August 18-21, 2015, Proceedings 17*, pp. 3–18, Springer, 2015.

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

[19] “Lightning-network copy.” `https://lightning.network/lightning-network-summary.pdf`. (Accessed on 12/19/2023).

[20] “State channels — ethereum.org.” `https://ethereum.org/en/developers/docs/scaling/state-channels/`. (Accessed on 12/19/2023).

[21] J. Lind, O. Naor, I. Eyal, F. Kelbert, E. G. Sirer, and P. Pietzuch, “Teechain: A secure payment network with asynchronous blockchain access,” *Sosp 2019 - Proceedings of the 27th Acm Symposium on Operating Systems Principles*, pp. 63–79, 2019.

[22] C. Lin, N. Ma, X. Wang, and J. Chen, “Rapido: Scaling blockchain with multi-path payment channels,” *Neurocomputing*, vol. 406, pp. 322–332, 2020.

[23] J. Liao, F. Zhang, W. Sun, and W. Shi, “Speedster: A tee-assisted state channel system,” 2021.

[24] A. Miller, I. Bentov, S. Bakshi, R. Kumaresan, and P. McCorry, “Sprites and state channels: Payment networks that go faster than lightning,” in *International conference on financial cryptography and data security*, pp. 508–526, Springer, 2019.

[25] S. S. Sahoo, M. M. Hosmane, and V. K. Chaurasiya, “A secure payment channel rebalancing model for layer-2 blockchain,” *Internet of Things (netherlands)*, vol. 22, p. 100822, 2023.

[26] J. Harris and A. Zohar, "Flood & loot: A systemic attack on the lightning network," in *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, pp. 202–213, 2020.

[27] 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.

[28] J. Poon and V. Buterin, "Plasma: Scalable autonomous smart contracts," *White paper*, pp. 1–47, 2017.

[29] S. D. Lerner, "Rsk," *RootStock Core Team, White Paper*, 2015.

[30] J. B. Burgos and M. Pustisek, "Tackling trust and scalability of the blockchain-based shared manufacturing concept," *17th International Conference on Telecommunications, Contel 2023*, pp. 1–7, 2023.

[31] M. S. Chishti and A. Banerjee, "Instantaneous account settlement in roll-up based layer-2 blockchain framework for metaverse applications," *Proceedings - 2023 Ieee International Conference on Metaverse Computing, Networking and Applications, Metacom 2023*, pp. 78–85, 2023.

[32] T. Lavaur, J. Lacan, and C. P. Chanel, "Enabling blockchain services for ioe with zk-rollups," *Sensors*, vol. 22, no. 17, p. 6493, 2022.

[33] T. Lavaur, J. Detchart, J. Lacan, and C. P. Chanel, "Modular zk-rollup on-demand," *Journal of Network and Computer Applications*, vol. 217, p. 103678, 2023.

[34] A. C. Tran, V. V. Thanh, N. C. Tran, and H. T. Nguyen, "An implementation and evaluation of layer 2 for ethereum with zk-rollup," *Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 13831, pp. 107–115, 2023.

[35] S. Martinez, T. Lavaur, J. Lacan, and C. P. C. Chanel, "Proven transaction flow control for zk-rollups," *2023 5th Conference on Blockchain Research and Applications for Innovative Networks and Services (brains)*, pp. 1–4, 2023.

[36] S. Gontara, A. Boufaied, and O. Korbaa, "Impact of eip-1559 on transactions in the ethereum blockchain and its rollups," *Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 13857, pp. 114–126, 2023.

[37] M. Xu, Q. Wang, H. Sun, J. Lin, and H. Huang, "W3chain: A layer2 blockchain defeating the scalability trilemma," *2023 Ieee International Conference on Blockchain and Cryptocurrency, Icbc 2023*, pp. 1–9, 2023.

[38] Z. Xu and L. Chen, "L2chain: Towards high-performance, confidential and secure layer-2 blockchain solution for decentralized applications," *Proceedings of the Vldb Endowment*, vol. 16, no. 4, pp. 986–999, 2022.

[39] A. Tanksali, "Xipcoin: A proposal for decentralized offline payments using ethereum," *2021 Ieee 2nd International Conference on Technology, Engineering, Management for Societal Impact Using Marketing, Entrepreneurship and Talent, Temsmet 2021*, p. 6 pp., 2021.

[40] A. Kurt, A. Sahin, R. Harrilal-Parchment, and K. Akkaya, "Lnmesh: Who said you need internet to send bitcoin? offline lightning network payments using community wireless mesh networks," *Proceedings - 2023 Ieee 24th International Symposium on a World of Wireless, Mobile and Multimedia Networks, Wowmom 2023*, pp. 261–270, 2023.

[41] P. Robinson and R. Ramesh, "Layer 2 atomic cross-blockchain function calls," p. 12, 2020.

[42] E. Ebadi, H. Yajam, and M. A. Akhaee, "Improvements on easypaysy: The bitcoin's layer-2 accounts protocol," *Proceedings of 17th International Isc Conference on Information Security and Cryptology, Iscisc 2020*, pp. 54–59, 2020.

[43] J. Long and R. Wei, "Off-chain micropayment pool for high-throughput bandwidth sharing rewards," *Ieee International Conference on Blockchain and Cryptocurrency, Icbc 2021*, p. 3 pp., 2021.

[44] Y. Liu, W. Liang, K. Xie, S. Xie, K. Li, and W. Meng, "Lightpay: A lightweight and secure off-chain multi-path payment scheme based on adapter signatures," *Ieee Transactions on Services Computing*, vol. PP, no. 99, pp. 1–14, 2023.

[45] K. Gjøsteen, M. Raikwar, and S. Wu, "Pribank: Confidential blockchain scaling using short commit-and-proof nizk argument," *Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 13161, pp. 589–619, 2022.

[46] R. Khalil and N. Dulay, "Adaptive layer-two dispute cutoffs in smart-contract blockchains," *2021 3rd Conference on Blockchain Research and Applications for Innovative Networks and Services, Brains 2021*, pp. 129–136, 2021.

[47] E. N. Tas and D. Boneh, "Cryptoeconomic security for data availability committees," 2023.

[48] S. Mazumdar and S. Ruj, "Cryptomaze: Privacy-preserving splitting of off-chain payments," *Ieee Transactions on Dependable and Secure Computing*, vol. 20, no. 2, pp. 1060–1073, 2023.

[49] E. Heilman, S. Lipmann, and S. Goldberg, "The arwen trading protocols," *Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12059, pp. 156–173, 2020.

[50] T. Takahashi, T. Higuchi, and A. Otsuka, “Velocash: Anonymous decentralized probabilistic micropayments with transferability,” *Ieee Access*, vol. 10, pp. 1–1, 2022.

[51] J. Wu and S. Jiang, “On increasing scalability and liquidation of lightning networks for blockchains,” *Ieee Transactions on Network Science and Engineering*, vol. 9, no. 4, pp. 2589–2600, 2022.

[52] A. De Castro and C. Coutinho, “Electronic voting through blockchain: A survey,” *Hora 2023 - 2023 5th International Congress on Human-computer Interaction, Optimization and Robotic Applications, Proceedings*, pp. 1–6, 2023.

[53] P. Xie, Z. Zheng, X. Zhang, and S. Chen, “Decentralized verifiable mail-in ballot counting for postal voting,” 2022.

[54] S. K. Rana, A. K. Rana, S. K. Rana, V. Sharma, U. K. Lilhore, O. I. Khalaf, and A. Galletta, “Decentralized model to protect digital evidence via smart contracts using layer 2 polygon blockchain,” *Ieee Access*, vol. 11, pp. 83289–83300, 2023.

[55] D. S. K. Putra and A. Amiruddin, “A proposed architecture for the indonesia’s national blockchain,” *Proceedings - 2023 Ieee International Conference on Cryptography, Informatics, and Cybersecurity: Cryptography and Cybersecurity: Roles, Prospects, and Challenges, Icocics 2023*, pp. 230–235, 2023.

[56] S. Thakur and J. G. Breslin, “Rumour prevention in social networks with layer 2 blockchains,” *Social Network Analysis and Mining*, vol. 11, no. 1, p. 104, 2021.

[57] S. Thakur and J. Breslin, “A model of decentralised distribution line using layer 2 blockchains,” *Lecture Notes in Networks and Systems*, vol. 595, pp. 23–36, 2023.

[58] Y. Liang, Y. Li, and B. S. Shin, “Private decentralized crowdsensing with asynchronous blockchain access,” *Computer Networks*, vol. 213, p. 109088, 2022.

[59] B. Buzcu, M. Ozgun, O. Gurcan, and R. Aydogan, “Fully autonomous trustworthy unmanned aerial vehicle teamwork: A research guideline using level 2 blockchain,” *Ieee Robotics and Automation Magazine*, pp. 2–12, 2023.

[60] A. De Salve, L. Franceschi, A. Lisi, P. Mori, and L. Ricci, “L2dart: A trust management system integrating blockchain and off-chain computation,” *Acm Transactions on Internet Technology*, vol. 23, no. 1, p. 3561386, 2023.

[61] D. Pennino, M. Pizzonia, A. Vitaletti, and M. Zecchini, “Binding of endpoints to identifiers by on-chain proofs,” *Proceedings - Ieee Symposium on Computers and Communications*, vol. 2020-, p. 9219594, 2020.

[62] D. Tomaszuk, D. Kuziński, M. Sopek, and B. Swiecicki, “A distributed graph data storage in ethereum ecosystem,” *Lecture Notes in Computer Science (including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 13072, pp. 223–231, 2021.

[63] T. Rafaj, L. Mastilak, K. Kostal, and I. Kotuliak, “Defi gaming platform using the layer 2 benefits,” *Conference of Open Innovation Association, Fruct*, vol. 2023-, pp. 236–242, 2023.