Journal of Analysis and Computation (JAC)
(An International Peer Reviewed Journal), www.ijaconline.com, ISSN 0973-2861
Volume XVIII, Issue I, Jan-June 2024

EXPLORING THE EFFICACY OF ROLLUPS' A COMPARATIVE STUDY OF OPTIMISTIC AND ZK-ROLLUPS AND THEIR POPULAR IMPLEMENTATIONS

Akshita Jain[1], Yogita Punjabi [2], Ruchi Mathur [3]

[1]*Student, Jaipur Engineering College and Research Centre (JECRC Foundation), Jaipur, India*
[2]*Asst. Professor, Jaipur Engineering College and Research Centre (JECRC Foundation), Jaipur, India*
[3]*Professor, Jaipur Engineering College and Research Centre (JECRC Foundation), Jaipur, India*

ABSTRACT

Scalability is a grave challenge for blockchain technology with consequent repercussions on performance. In recent years, scaling Ethereum has been one of the most deliberated and trending subjects in the crypto and blockchain space. This debate particularly intensifies during periods of high network activity, such as the craze of CryptoKitties in 2017, 2020's DeFi Summer, and 2021's crypto bull market. Lately, network congestion has intensified significantly due to the rising popularity of Decentralized Finance (DeFi), Non-fungible tokens (NFTs) and yield farming. The unparalleled surges in demand during these times, resulted in tremendously high gas fees, making it hard and expensive for commonplace users to pay for their transactions. To overcome these limitations, this paper aims at analysing the available Layer II scalability solutions while highlighting the main differences among the examined frameworks, while focusing on theoretical as well as practical real-world aspects. The first section is an introduction about the scalability issue, the blockchain trilemma and the available layers of solutions. It gives a small overview about Layer1 solutions and the concept of sidechain and then dwells in depth on Layer 2 solutions. Since the Ethereum Layer 2 (L2s) ecosystem has grown tremendously in terms of the number of available systems, system architectures, and their complexity, a deep understanding of these systems is increasingly imperative. So, in the second section, we address the question of what are layer 2 scalability solutions and what do they offer, by doing a comparative study of types of L2s and presenting a tabular summary of the same. Then we analyse the trends and key aspects such as scalability, security, decentralization, privacy, etc. and conclude that rollups are the most effective and adopted solution. With their potential to significantly boost blockchain scalability while preserving transaction privacy and security, they are rightly referred as the Holy Grail of scaling. In the third section of our paper we then answer the questions: What advantages do Rollups offer? And, how have they become the most anticipated and awaited scaling solution of them all? We then present a comparison between Optimistic and Zk Rollup. Through comparative evaluations and discussions of technical challenges and future directions, we elucidate zkRollup's role in shaping the future of decentralized systems and the blockchain technology. In section four, we will do an in-depth breakdown of the implementations of Optimistic and Zk Rollup, by highlighting their potential and analysing the Zero knowledge proofs.

We then conclude this paper by providing insights into Emerging Trends, Potential Enhancements and topics for future research and development on rollups and blockchain technology as a whole.

Keywords: Blockchain, Ethereum, scalability, rollups, optimistic, zk, implementations, zkproofs, Layer-2

[1] INTRODUCTION

Scalability, in context of blockchain technology refers to the blockchain's capacity to provide high transactional throughput and accommodate future growth. This means that as the adoption increases and an increasing volume of transactions occur, the blockchain performance won't suffer, instead it will handle them without compromising on transaction speed or fees. Enhancing scalability is possible, but it comes at the expense of either security or decentralization or both.

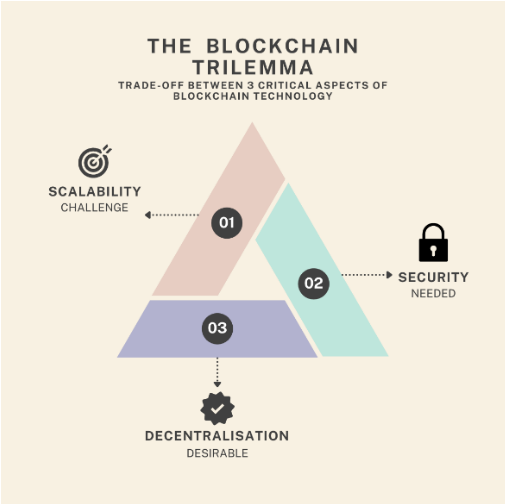
The Scalability Trilemma posits the inherent trade-off in designing blockchain systems between three vital Distributed ledger technology (DLT) properties: decentralization, scalability, and security, where improving one property typically results in compromising another.

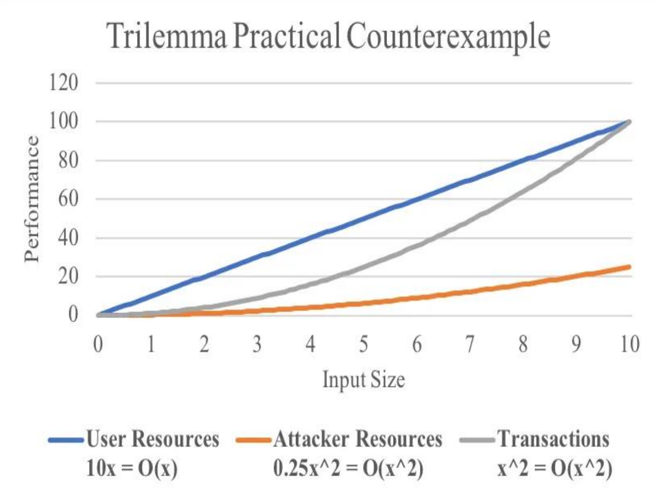
The Trilemma as defined by the Ethereum team is available here.

"**1. Decentralization** (defined as the system being able to run in a scenario where each participant only has access to O(c) resources, i.e. a regular laptop or small VPS)

2. Scalability (defined as being able to process O(n) > O(c) transactions)

3. Security (defined as being secure against attackers with up to O(n) resources)."





Source graph:
https://miro.medium.com/v2/resize:fit:828/format:webp/0*fyQH45n6wCUREEAb

Thus, in a decentralized network, having more participants (nodes) generally enhances security due to increased resilience against attacks, because a greater number of participants (due to its distributed nature) makes it harder for a single entity to gain control of the system. Hence, thwarting potential attacks such as the notorious 51% attack. However, this network growth consequentially makes reaching a consensus more time-consuming, potentially impacting the network's scalability. Additionally, an excessively decentralized network may allow easier pass for malicious actors, possibly compromising security.

Attaining scalability remains the major challenge despite established decentralization and security for today's leading decentralized networks. To tackle this problem, the search for the ultimate scaling solution has been one of the top priorities.

There are 3 chief ways to scale Ethereum or actually, most other blockchains: **Layer 1** scaling (scaling the blockchain itself); **Layer 2** scaling (building on top of layer 1) and **sidechains** (building on the side of layer 1).

When it comes to **layer 1**, Ethereum 2.0 or ETH2 is the preferred solution. It scales blockchain by directly enhancing the underlying protocol to handle more transactions per second (TPS) through a set of interconnected changes and migration to PoS and sharding. It involves integrating the Proof-of-Work (PoW) blockchain into the new Proof-of-Stake (PoS) chain.

Sidechains, in contrast, are usually EVM-compatible and can scale general-purpose applications. They allow for experimentation and scalability improvements without directly impacting the main network. However, they are less secure than layer 2 solutions because they do not rely on the security of Ethereum and instead use their own consensus models. Examples include Polygon (formerly Matic) and Binance Smart Chain.

Outside of layer 1, we have **layer 2** solutions such as channels that are fully secured by Ethereum but work well only for a specific set of applications. Then we also have rollups that aim at achieving the best of all the worlds, by generating a general-purpose scaling solution while fully relying on the security of Ethereum. It allows for deploying all of the existing smart contracts present on Ethereum to a rollup with little or no changes, while not sacrificing security (can be used for any arbitrary contract executions).

2. RELATED WORK

LAYER-2

How does Layer 2 work?

Layer 2 interacts with Ethereum (Layer 1) and takes the transactional burden off of it, it then posts finalized proofs back to the main-chain. By doing so, the base layer becomes less congested, and the ecosystem becomes more scalable. An example of this is how sending a regular Ethereum transaction can run into hundreds of dollars during times of congestion. Layer 2 serves to clear this congestion and keep transaction fees low.

When it comes to genuine Layer 2 scaling solutions there are multiple options available. A comparative table highlighting key differences and similarities among various Layer 2 solutions, including Rollups, Lightning Network, Plasma, and State Channels and Validium is given below:

Feature / Solution	**Rollups**	**Lightning Network**	**Plasma**	**State Channels**	**Validium**
Mechanism	Transactions are aggregated off-chain, summary is posted on-chain.	Uses Off-chain payment channels with bidirectional capabilities.	Uses Child chains with periodic root state commitments to main chain.	Uses Off-chain channels for stateful interactions between parties.	Comparable to Rollups but data is stored off-chain, proofs on-chain.
Security Model	Utilises on-chain data availability and cryptographic proofs.	Security rests on underlying blockchain and participants' honesty.	Relies on fraud proofs, Periodic commitments to main chain.	Security via dispute mechanisms, performs on-chain settlement if disputes arise.	On-chain validity proofs, data availability is off-chain.
Throughput	High; 1000-4000 TPS based on the type (Optimistic/ZK).	Very high; restricted by individual channel capacity.	High; restricted by child chain capacity.	Very high; restricted by the number of participants and channels.	High; alike ZK-Rollups but off-chain data storage.
Latency	Low, however Optimistic Rollups do have challenge periods.	Instant transaction confirmation, no delay.	Low, but finality is subject to main chain checkpoints.	Instant within the channel, no delay.	Low; instantaneous proof verification.
Finality	Immediate for ZK, deferred for Optimistic	Instant within channels; is subject to channel closure for	Is dependent on the root chain’s checkpoi	Instant within the channel; on-chain dispute	Instant upon proof verification.

	(challenge period).	main chain.	nting frequency.	resolution adds interruption.	
Developer Adoption	Moderate to high; rising number of tools and frameworks.	High for Bitcoin; modest for other chains.	Moderate; needs specialized knowledge.	Moderate; needs knowledge of off-chain protocols.	Increasing; needs understanding of ZK proofs.
Security Risk	Reliant on fraud proofs (Optimistic); cryptographic assumptions (ZK).	Participant honesty and right channel management.	Probable centralization and fraud proof vulnerabilities.	Dispute resolution security; participant uprightness.	Cryptographic assumptions; data availability risks.
Integration Challenge	Moderate; rollup-specific integration.	Easy for payment-related use cases; challenging for complex logic.	High; needs integration with child chain and main chain.	Moderate; needs channel establishment and management.	High; complex proof systems and off-chain data handling.
Emerging Trend and Potential Enhancement	Improved fraud proof mechanisms, hybrid rollup models.	Cross-chain compatibility interoperability., improved liquidity management.	More effective fraud proofs, integration with other L2 solutions.	Increased use in gaming and micro-payment solutions; robust dispute resolution mechanisms	Enhanced ZK algorithms, hardware acceleration. More efficient quantum-resistant proof

Regulatory Compliance	Requires compliance with on-chain and off-chain components.	Needs adherence to financial regulations for payments.	Must conform with main chain and child chain regulations.	Compliance related to specific use cases (e.g., gaming, finance).	Requires compliance for off-chain data handling and cryptographic standards.

This table outlines the crucial characteristics and differences among Rollups, Lightning Network, Plasma, State Channels, and Validium**,** across multiple dimensions relevant to blockchain scalability and adoption.

1. ***Rollups***

decentralized; might involve token governance.

- Implication for Scalability Substantial improvement over L1; broad use cases.
- Trade-offs Scalability Bottleneck

a) *Optimistic Rollups:* Incur latency due to potential challenge periods for fraud proof resolution.

b) *ZK Rollups:* Inhibited by the computational intensity and complexity of generating zero-knowledge proofs.

- Notable Projects: Optimism, zkSync, Arbitrum. These are at the forefront of using rollups to scale Ethereum and other blockchains.
- Ecosystem Support: Growing**,** strong support from Ethereum and various DeFi applications. Projects like Optimism and zkSync are gaining noteworthy traction and community support.
- Integration Challenge: Moderate to High Effort; Needs understanding of rollup-specific mechanisms and integration of smart contracts to interact with the rollup.

2. ***Lightning Network***

Decentralized; managed by network participants.

- Implication for Scalability Key improvement for micro-payments and retail transactions.
- Trade-offs Scalability Bottleneck Low Fees; Instant Transactions; Needs active channel management; sufficient liquidity. Scalability is restricted by the need for liquidity in payment channels and the complexity of routing payments through multiple channels.
- Notable Projects: Bitcoin Lightning Network, Lightning Labs. Principally developed for Bitcoin, but also explored for other cryptocurrencies.
- Ecosystem Support: Well-Supported within the Bitcoin community, with growing infrastructure and application support, including wallets and payment processors.
- Integration Challenge: Easier for payment-related use cases rather than complex smart contract interactions, but challenging for more complex logic due to the need for managing payment channels.

3. ***Plasma***

Decentralized; managed by child chain operators.

- Implication for Scalability High scalability for specific applications.

- Trade-offs Scalability Bottleneck Potential centralization risks as child chains might be controlled by fewer entities. Requires periodic interaction with the main chain, introducing delays and costs. Bottlenecked by the need for efficient and secure fraud proof mechanisms and the frequency of main chain checkpoints.
- Notable Projects: OMG Network, Polygon (formerly Matic) use Plasma to enhance scalability.
- Ecosystem Support: Developing Support; Reinforced by specific projects, but overall ecosystem support is more fragmented compared to Rollups.
- Integration Challenge: High Complexity; Involves integration with both the child chain and the main chain, along with managing fraud proofs.

4. *State Channels*

Decentralized; managed by channel participants.

- Implication for Scalability High scalability for private and micro-transactions.
- Trade-offs Scalability Bottleneck: Instant Finality and Low Fees; Limited to predefined participants. Managing the channels and handling disputes can be complex and may require locking significant funds.
- Notable Projects: Raiden Network, Connext. Focus on simplifying off-chain stateful interactions.
- Ecosystem Support: Niche Support; Mainly for applications needing instant micro-transactions or private interactions, such as gaming.
- Integration Challenge: Moderate Effort; Requires setup of channels and mechanisms, fit mainly for applications with frequent interactions between known parties

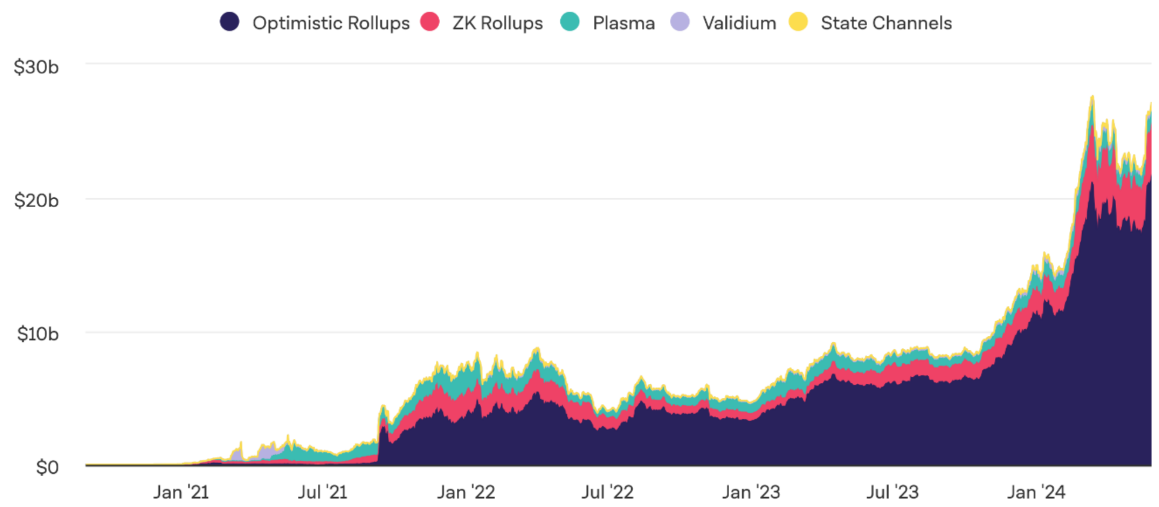
5. *Validium*

Decentralized; might involve token governance.

- Implication for Scalability High scalability with efficient off-chain data handling.
- Trade-offs Scalability Bottleneck: High Throughput and Low Costs; Balances off-chain data availability with the challenge of guaranteeing data integrity and security. Relies on trust in external data availability providers.
- Notable Projects: StarkEx, zkSync. Use Validium to attain high throughput with off-chain data availability.
- Ecosystem Support: Rising Support; Supported by advanced cryptographic projects and institutions, gaining traction in the DeFi space.
- Integration Challenge: High Complexity; Requires handling zero-knowledge proofs and off-chain data availability solutions, offering noteworthy scalability benefits but with integration challenges.

Cost effectiveness					
Feature / Solution	**Rollups**	**Lightning Network**	**Plasma**	**State Channels**	**Validium**
Transaction Fees	Lower than L1	Very low	Lower than L1;	Very low within the channel	Lower than L1

Computational Overhead	moderate on-chain. Lower off-chain.	minimal on-chain. Low; mostly off-chain,	periodic on-chain commitments. Low off-chain	occasional on-chain transactions. Negligeable off-chain	low on-chain. High off-chain
Gas Fees	Reduced	Minimal	Reduced	Very low	Reduced



Source:https://www.theblock.co/data/scaling-solutions/scaling-overview/value-locked-of-ethereum-scaling-solutions
Updated: May 28, 2024

Depicts: The value locked in Ethereum scaling solutions over time. As on May 27th 2024, Optimistic Rollup has a value of $21.86 billion, the highest among all others, followed by Zk rollup which has a value of $3.89 billion. Plasma holds rank 3rd with $1.03billion. Validium has $399.11 million while State channel has $1.55million out of a total of $27.12 billion- which is the sum of values locked in all the represented layer 2 scaling solutions. The graph provides insights into how these metrics have progressed, highlighting trends in adoption, economic activity, security, scalability, ecosystem health, and market dynamics.

3. ROLLUPS

From the graph it is very well evident that Rollups are the preferred Layer 2 solutions for scaling Ethereum. This is so because Rollups bundle hundreds of transactions from L1 off-chain, dispersing transaction fees among all users and then posting transaction data back to L1. By doing so they take advantage of the security of Ethereum and also provide efficient scaling.

Many people believe in this view, and according to [Vitalik](), ETH's main man, Layer 2 scaling and privacy are here to stay.*'ETH2 scaling for data will be available before ETH2 scaling for general computation.'* In his [tweet](), he hinted that rollups would be the dominant scaling paradigm for at least a couple of years. So, here we take a deep dive into the world of Rollup starting with a concise overview of the fundamental differences and similarities between Optimistic Rollups and ZK-Rollups, highlighting their key features, and use cases.

Feature	Optimistic Rollups	ZK Rollups
Mechanism	Posts summary on-chain. Aggregates transactions off-chain	To validate transactions off-chain it uses zero-knowledge proofs
Security Model	Assumes transactions are valid; Uses fraud proofs if challenged.	Transactions are validated with cryptographic proofs (such as ZK-SNARKs, STARKs).
Throughput	around 1000-2000 TPS; Higher than L1	potentially up to 2000-4000 TPS or more; Even higher.
Latency	Higher because of challenge period (up to 7 days).	Lower with immediate proof verification.
Finality	Delayed while waiting for end of challenge period	Instant upon proof verification.
Transaction Fees	Lower than L1; is subject to challenge frequency.	Characteristically, lower than Optimistic Rollups; depends on proof cost.
Computational Overhead	Lower off-chain; possible on-chain costs for fraud proofs.	High off-chain (for proof generation), low on-chain verification.
Gas Fees	Less compared to L1; varies with fraud proof activity.	Lower due to effective proof verification.
Use Case	General-purpose scaling; apt for DApps, DeFi.	High-frequency trading, gaming, payments.
Developer Adoption	Moderate; needs handling challenge mechanisms.	Growing; complex but maturing tools.
Security Risk	Dependent on fraud proofs; risk of unchallenged fraud.	Cryptographic assumptions; risk in proof generation errors.
Governance	Usually decentralized; may involve token-based governance.	Decentralized; may involve complex governance for proof systems.
Regulatory	Needs to ensure compliance with fraud proof mechanisms.	Compliance with cryptographic standards; less regulatory clarity.
Compliance Consideration	Challenge mechanisms must meet legal standards.	ZK proof methods must align with cryptographic regulations.

1. *Optimistic Rollups*

- Implication on Scalability and Adoption Noteworthy improvement over L1; diverse use cases.

Feature	Optimism	Arbitrum	Boba Network	Metis	Base
Developed by	Optimism PBC	Offchain Labs	Enya & OMG Foundation	MetisDAO	Coinbase
Fraud Proof Mechanism	Single-round	Multi-round	Single-round	Single-round	Single-round
Transaction Costs	Competitive	Mostly lower than Optimism	Comparable to Optimism	optimized for business use cases. Low	Competitive
Ideal For (Main Use Cases)	General-purpose dApps, DeFi projects where ease of integration and Ethereum compatibility are vital	General-purpose dApps, DeFi, gaming that require lesser transaction costs and robust security mechanisms	General-purpose dApps, DeFi, NFTs, predominantly those needing hybrid compute capabilities and faster withdrawal options.	General-purpose dApps, DeFi, business focused applications that need scalability and decentralized governance.	General-purpose dApps, DeFi, institutional applications looking for solid backing and ease of integration.
Governance	Progressive decentralization	Progressive decentralization	DAO governance	Decentralized governance via MetisDAO	Centralized, transitioning to decentralized
Interoperability	Robust, with other Layer 2s and Ethereum	Robust, with other Layer 2s and Ethereum	Interoperable with Ethereum and other L2 solutions	Focused on Ethereum and business solutions	Robust, with Ethereum ecosystem
Adoption and Ecosystem	Rising, supported by major dApps and DeFi	Rising, widely adopted across DeFi	Emerging ecosystem, focus on DeFi and NFTs	Rising ecosystem with a business focus	Rapid growth, robust support from Coinbase

- Trade-offs Scalability Bottleneck Longer finality time; challenge periods; potential for higher latency.
- Implementations: Optimism, Arbitrum, Boba Network.
- Ecosystem Support: Rising; supported by projects like Optimism, Arbitrum.
- Integration Challenge: Easier to integrate; less computationally intensive.
- Emerging Trend; Potential Enhancement Enhanced fraud proof mechanisms, multi-chain compatibility; Faster challenge resolution, hybrid rollup models.

2. *ZK Rollups*

- Implication on Scalability and Adoption Major enhancement in scalability; potential mass adoption
- Trade-offs Scalability Bottleneck High computational complexity for proof generation; Proof generation time
- Implementations: zkSync, StarkEx, Polygon Hermez.
- Ecosystem Support: Robust; reinforced by projects like zkSync, StarkWare.
- Integration Challenge: Complex integration; requires handling ZK proofs**.**
- Emerging Trend; Potential Enhancement Improved ZK algorithms, hardware acceleration for proof generation. More efficient, quantum-resistant proofs
  While **Optimistic Rollups** provide a good balance of security and performance with an existing developer base but face challenges with latency and finality due to the need for fraud proofs, **ZK Rollups** offer superior throughput and immediate finality at the cost of higher computational overhead and complexity in proof generation, making them ideal for high-frequency applications.

4. ROLLUP IMPLEMENTATIONS

As mentioned earlier, there are many notable projects which are currently utilising rollup technology and trying to minimise the limitations each type offers. A comparative study of some noteworthy projects both for optimistic Rollup implementations and Zk Rollup implementation is discussed below respectively.

IV- I. Optimistic Rollup implementations:

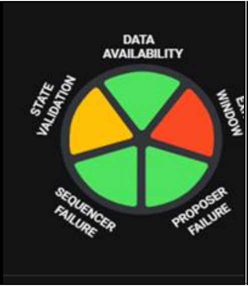
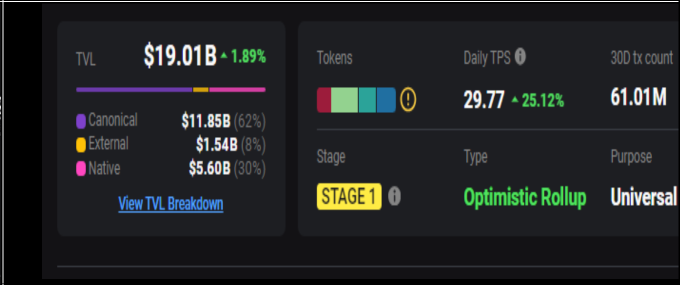
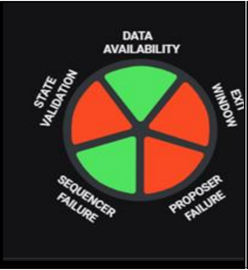
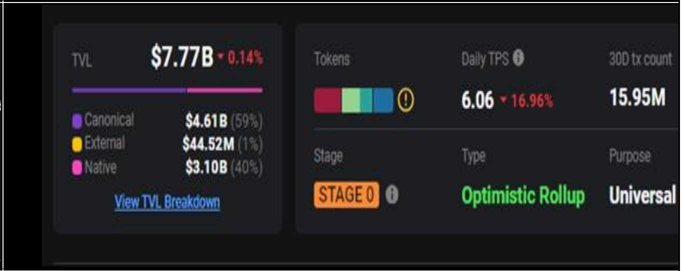
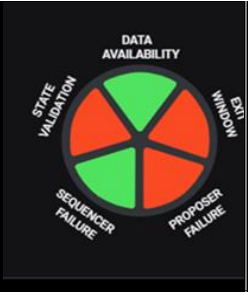
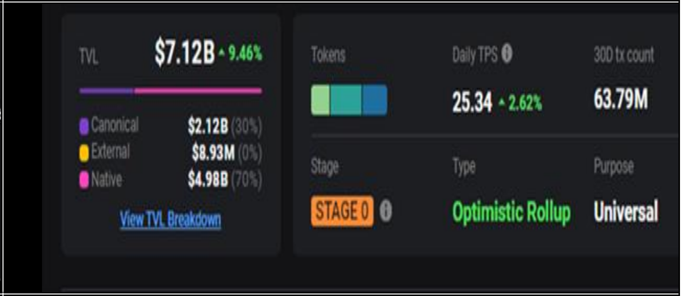
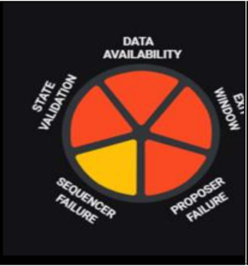
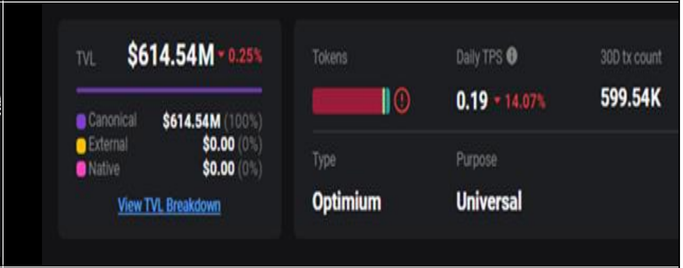
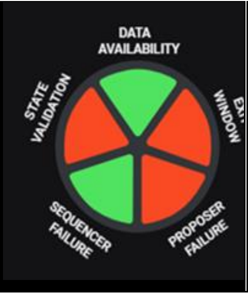
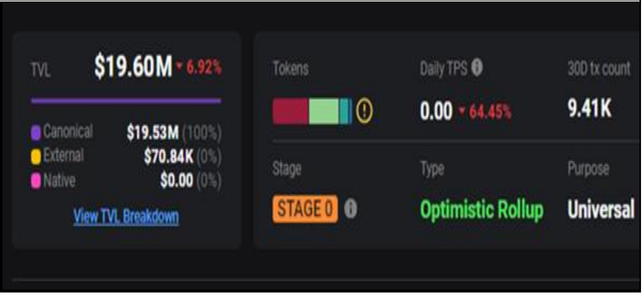
Comparison table summarizing key characteristics of Optimism, Arbitrum, Boba Network, Metis, and Base.

Every Optimistic rollup implementation has a finality time of (7 days default), with high scalability and security and provides unique strengths tailored to different needs within the Ethereum ecosystem.

Unique Features

- **Optimism:** High EVM compatibility (close to native), simple fraud-proof system, robust security, and competitive transaction costs. easy to integrate
- **Arbitrum:** Multi-round fraud-proof system for potentially lower costs, high EVM compatibility (close to native), robust security, and wide adoption.
- **Boba Network:** Offers added features like hybrid compute, fast withdrawals, and DeFi incentives, with high security and EVM compatibility.
- **Metis:** Focused on scalability and usability for business and DeFi applications with decentralized governance, providing high security and EVM compatibility.
- **Base:** Supported by Coinbase, designed for easy integration, strong security, and interoperability within the Ethereum ecosystem
  The choice between these implementations rests on the specific requirements of the project, such as cost sensitivity, desired ease of integration, governance preferences, and target use cases.

Below are the images showing the total value locked, displayed together with percentage change compared to 7 days ago, associated risks, stage based on its feature and maturity, purpose, transactions per second averaged over the past day displayed together with percentage change compared to 7 days ago of the various optimistic Rollup implementations discussed above.

Implementation	Associated Risks	Information
Arbitrum		TVL $19.01B ▲1.89% Canonical $11.85B (62%) External $1.54B (8%) Native $5.60B (30%) View TVL Breakdown Tokens Daily TPS 29.77 ▲25.12% 30D tx count 61.01M Stage STAGE 1 Type Optimistic Rollup Purpose Universal
OP Mainnet		TVL $7.77B ▼0.14% Canonical $4.61B (59%) External $44.52M (1%) Native $3.10B (40%) View TVL Breakdown Tokens Daily TPS 6.06 ▼16.96% 30D tx count 15.95M Stage STAGE 0 Type Optimistic Rollup Purpose Universal
Base		TVL $7.12B ▲9.46% Canonical $2.12B (30%) External $8.93M (0%) Native $4.98B (70%) View TVL Breakdown Tokens Daily TPS 25.34 ▲2.62% 30D tx count 63.79M Stage STAGE 0 Type Optimistic Rollup Purpose Universal
Metis		TVL $614.54M ▼0.25% Canonical $614.54M (100%) External $0.00 (0%) Native $0.00 (0%) View TVL Breakdown Tokens Daily TPS 0.19 ▼14.07% 30D tx count 599.54K Type Optimium Purpose Universal
Boba		TVL $19.60M ▼6.92% Canonical $19.53M (100%) External $70.84K (0%) Native $0.00 (0%) View TVL Breakdown Tokens Daily TPS 0.00 ▼64.45% 30D tx count 9.41K Stage STAGE 0 Type Optimistic Rollup Purpose Universal

Source:https://l2beat.com/scaling/projects/arbitrum,https://l2beat.com/scaling/projects/optimismhttps://l2beat.com/scaling/projects/base,https://l2beat.com/scaling/projects/metis, https://l2beat.com/scaling/projects/bobanetwork

IV- II. Zk-Rollup implementations:

Before we do a comparative study of the various implementations it is necessary to understand the zk proofs which are of 2 types-

Feature	**zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge)**	**zk-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge)**
Proof Size	Small	Larger
Verification Time	Fast	comparatively slower
Setup	Requires a trusted setup	No trusted setup required
Security (Cryptographic Primitives)	Depends on on elliptic curve cryptography and pairings	Based on hash functions and information-theoretic security
Quantum Resistance	Not quantum-resistant	Quantum-resistant
Scalability	Efficient for small to moderately large proofs	Highly scalable, efficient for large data sets
Transparency	Requires trust in the initial setup phase	Fully transparent
Performance	Efficient for small to moderately large proofs with low computational costs	Highly scalable, though with potentially higher computational costs
Adoption	Widely adopted in various projects, e.g., Zcash, zkSync	Increasing adoption in high-throughput applications, e.g., StarkNet

zk-SNARKs:

- Advantages*:* Smaller proof sizes, fast verification times, and efficient for many applications.
- Disadvantages*:* Requires a trusted setup, which can be a security concern.
- Ideal Use Cases*:* Applications where small proof sizes and fast verification are critical, such as privacy-focused cryptocurrencies and certain Layer 2 scaling solutions.

zk-STARKs:

- Advantages: No trusted setup required, quantum-resistant, and highly scalable for large data sets.
- Disadvantages: Larger proof sizes and potentially more computationally intensive verification.
- Ideal Use Cases: Applications needing high throughput and security without a trusted setup, such as high-throughput blockchain applications and data-intensive environments.

Each type of zero-knowledge proof has its own set of strengths and trade-offs, making them suitable for different kinds of applications within the blockchain ecosystem. The choice between zk-SNARKs and zk-STARKs will depend on the specific requirements and priorities of the project, such as security, scalability, performance, and the need for transparency.

Comparison of various zk-Rollup implementations: zkSync, StarkNet, Polygon zkEVM, Loopring, and Manta Pacific.

Feature	**zkSync**	**StarkNet**	**Polygon zkEVM**	**Loopring**	**Manta Pacific**
Developed by	Matter Labs	StarkWare	Polygon, formerly Matic Network	Loopring Foundation	Manta Network
Proof Type	zk-SNARKs	zk-STARKs	zk-SNARKs	zk-SNARKs	zk-SNARKs
Scalability	High, effective for moderate data sets	Very high, effective for large data sets	High, effective for moderate data sets	High, optimized for DEXs	High, focused on privacy and DeFi
Proof Size	Small	Larger	Small	Small	Small
Verification Time	Fast	Moderate	Fast	Fast	Fast
Trusted Setup	Yes	No	Yes	Yes	Yes
Quantum Resistance	No	Yes	No	No	No
EVM Compatibility	High, zkSync 2.0 a for full EVM compatibility.	Evolving in the direction of full compatibility	Full EVM compatibility	Limited, focuses on specific use cases	Evolving towards EVM compatibility
Adoption	Rising, used by various DeFi projects	Rising, used in high-throughput apps	Rapid adoption within Polygon ecosystem	Widely adopted in DEX space	Evolving, focusing on privacy and DeFi
Ideal for (Main Use Cases)	DeFi projects needing fast and safe transactions, general-purpose dApps	High-throughput applications, DeFi, gaming, dApps and data-intensive projects demanding scalability and security.	General-purpose DeFi and dApps inside Polygon	Decentralized exchanges (DEXs) DEX platforms, Loopring Exchange, trading platforms requiring high performance and reduced costs.	Privacy-focused DeFi applications projects requiring secure and private transactions
Development Tools	Wide-ranging tools and documentation	Strong tools and documentation	Comprehensive tools and documentation	Specific tools for DEX development	Comprehensive tools focusing on privacy

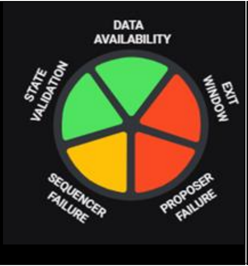
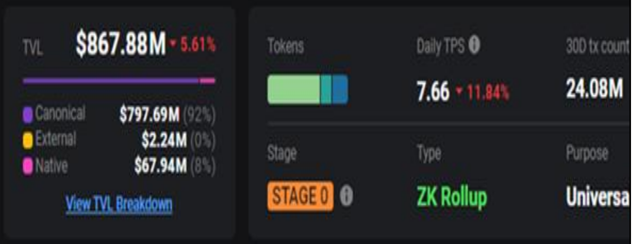
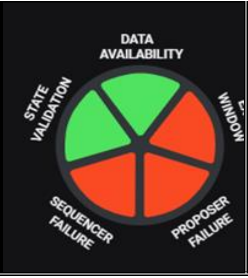
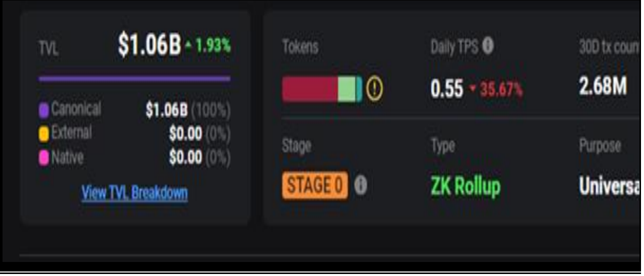
Each zk-Rollup implementation has its unique strengths, making them suitable for different types of applications within the Ethereum ecosystem:

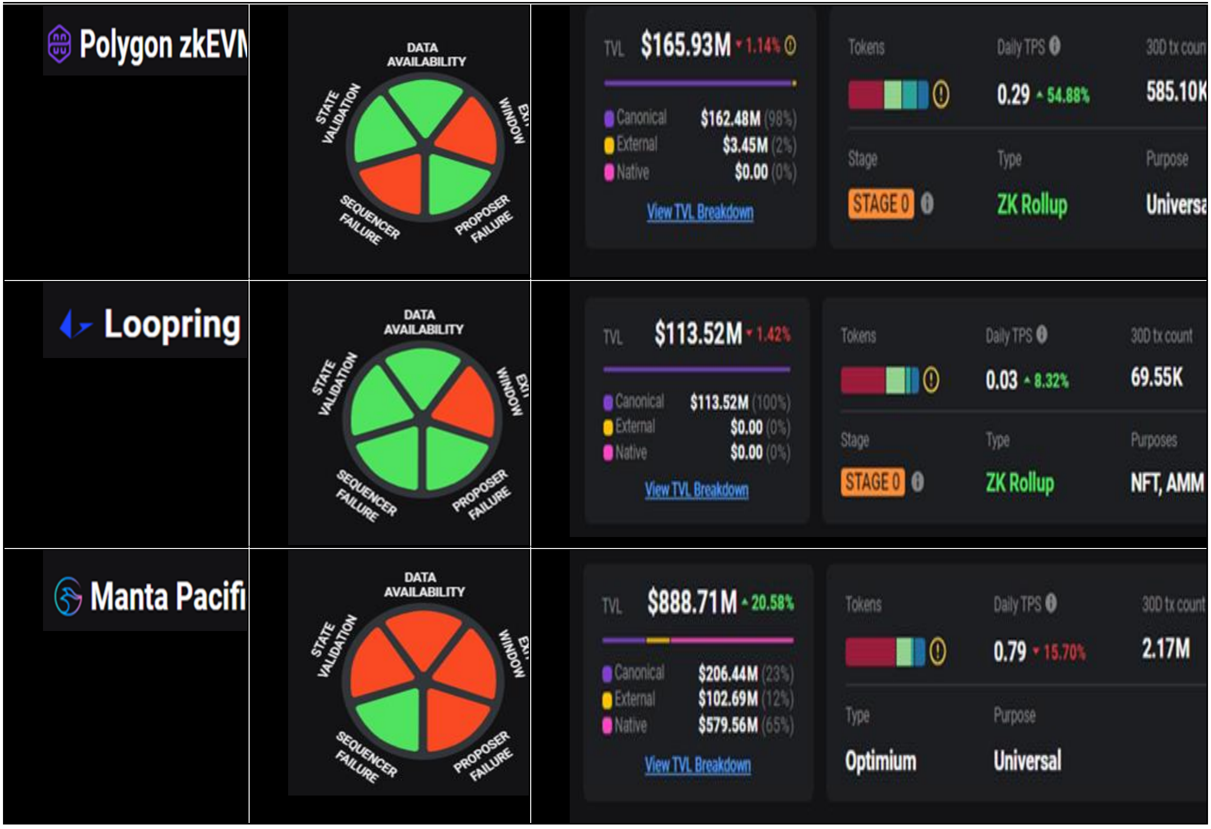
Unique Features

- **zkSync:** Ideal for projects requiring fast and secure transactions with high compatibility with Ethereum. Small proof size, fast verification, high security with zk-SNARKs, aiming for full EVM compatibility with zkSync 2.0.
- **StarkNet:** Best for high-throughput and data-intensive applications needing scalability and security without a trusted setup. Highly scalable with zk-STARKs, no trusted setup, quantum-resistant, robust security.
- **Polygon zkEVM:** Suitable for projects within the Polygon ecosystem that need seamless integration and full EVM compatibility. Full EVM compatibility, seamless integration with the Polygon ecosystem, small proof size, fast verification.
- **Loopring:** Optimized for decentralized exchanges and trading platforms that need high performance and low costs. Optimized for decentralized exchanges (DEXs), small proof size, fast verification, high throughput.
- **Manta Pacific:** Focused on privacy, ideal for DeFi applications that require secure and private transactions. Focused on privacy, high throughput, low costs, built-in privacy features.

Each zk-Rollup implementation addresses different needs within the Ethereum ecosystem, providing various advantages in terms of scalability, security, compatibility, and performance. The choice between these implementations will depend on the specific requirements of the project, including the need for EVM compatibility, trusted setup considerations, and the target use case.

Below are the images showing the total value locked, displayed together with percentage change compared to 7 days ago, associated risks, stage based on its feature and maturity, purpose, transactions per second averaged over the past day displayed together with percentage change compared to 7 days ago of the various Zk- Rollup implementations discussed above.

Implementation	Associated Risks	Information
zkSync Era	 DATA AVAILABILITY STATE VALIDATION EXIT WINDOW SEQUENCER FAILURE PROPOSER FAILURE	 TVL $867.88M ▾ 5.61% Canonical $797.69M (92%) External $2.24M (0%) Native $67.94M (8%) View TVL Breakdown Tokens Daily TPS 7.66 ▾ 11.84% 30D tx count 24.08M Stage STAGE 0 Type ZK Rollup Purpose Universa
Starknet	 DATA AVAILABILITY STATE VALIDATION E... WINDOW SEQUENCER FAILURE PROPOSER FAILURE	 TVL $1.06B ▴ 1.93% Canonical $1.06B (100%) External $0.00 (0%) Native $0.00 (0%) View TVL Breakdown Tokens Daily TPS 0.55 ▾ 35.67% 30D tx coun 2.68M Stage STAGE 0 Type ZK Rollup Purpose Universa



Polygon zkEV		TVL $165.93M ▾1.14% Canonical $162.48M (98%) External $3.45M (2%) Native $0.00 (0%) View TVL Breakdown Tokens Daily TPS 0.29 ▴54.88% 30D tx coun 585.10K Stage STAGE 0 Type ZK Rollup Purpose Universa
Loopring		TVL $113.52M ▾1.42% Canonical $113.52M (100%) External $0.00 (0%) Native $0.00 (0%) View TVL Breakdown Tokens Daily TPS 0.03 ▴8.32% 30D tx count 69.55K Stage STAGE 0 Type ZK Rollup Purposes NFT, AMM
Manta Pacifi		TVL $888.71M ▴20.58% Canonical $206.44M (23%) External $102.69M (12%) Native $579.56M (65%) View TVL Breakdown Tokens Daily TPS 0.79 ▾15.70% 30D tx count 2.17M Type Optimium Purpose Universal

Source:https://l2beat.com/scaling/projects/zksync-era
https://l2beat.com/scaling/projects/starknet
https://l2beat.com/scaling/projects/polygonzkevm
https://l2beat.com/scaling/projects/loopring
https://l2beat.com/scaling/projects/mantapacific

[5] SUMMARY

Rollup technologies represent a pivotal advancement in the pursuit to scale blockchain networks without compromising on security or decentralization. The comparative analysis of the various rollup solutions' that we have done through this paper highlights the diverse styles of achieving scalability, security, and efficiency in blockchain technology and dealing with the blockchain trilemma. Each implementation brings exceptional advantages tailored to specific use cases, from general-purpose dApps and DeFi to privacy-focused applications and high-performance trading platforms.

As the ecosystem continues to evolve, the ongoing innovation and adoption of zk-Rollups and Optimistic Rollups will play a crucial role in grasping the full potential of decentralized systems, paving the way for broader mainstream adoption and the development of a more efficient, secure, and scalable blockchain infrastructure.

For what regards Ethereum, instead, the reasoning is a bit more complex, because the community, in addition to Layer 2 proposals, is heavily pushing on Eth2 development as main scaling solution. The apprehension, now, is to understand whether Eth2 will cause uselessness of all Ethereum L2 solutions presented in this work. Here, it is important to point out that Layer 2 technologies can integrate on top of Ethereum 2.0, as well as adapted implementations of Rollups are likely to be the most important scaling solutions for some time. As stated by Vitalik Buterin "the scalability gains from the Layer 1 improvements and

Layer 2 improvements do ultimately multiply with each other”. Therefore, it is conceivable to consider sharding and existing L2 solutions as complementary. The Layer-3 scaling Solutions built on top of Layer-2 provide further scalability improvements and additional features, are rapidly evolving, and it’s exciting to witness how these innovative solutions will further develop and transform blockchain technology in the years to come. With their diverse approaches and use cases, Layer-3 solutions have the power to shape the future of blockchain technology and enable pioneering applications across various industries.

In conclusion, Layer 2 solutions certainly represent the best presently available solution for solving blockchain scalability problem, without renouncing to a secure and decentralized architecture. Even so, ZK rollups are considerably quicker and more scalable than Optimistic rollups, the former combines the efficiency of Rollup technology with the security and privacy guarantees of zero-knowledge proofs (ZKPs).There are currently a lot of projects working on zkEVMs to make zk compatible EVM to further advance rollup technology : zkEVM (a project funded by the Ethereum Foundation), Polygon zkEVM , Scroll , ZKSync (ZkSync Era is an EVM-compatible ZK Rollup built by Matter Labs, powered by its own zkEVM.), Starknet , Morph (a hybrid rollup scaling solution that utilizes zk-proof to address the Layer 2 state challenge issue).

Almost all present-day L2s are equipped with some form of upgrade mechanism, whether a code implementation upgrade or system parameters update. Given these systems are in their relative infancy and continue to evolve, it's reasonable to expect that these upgrade mechanisms will remain an essential aspect of L2s for the foreseeable future. Some of the future research areas that will further advance rollup technologies and ensure they meet the demands for scalability, security, and efficiency in blockchain applications include Optimization of zk-STARKs - by Reduced proof size, verification time and enhanced integrability. For wider adoption, creating trustless zk-SNARKs, quantum resistant cryptographic primitives and standard protocols for Cross-Rollup interoperability are some vital areas for research.

REFERENCES

[1]. Cosimo Sguanci, Roberto Spatafora, Andrea Mario Vergani. "Layer 2 Blockchain Scaling: a Survey" June 2021, URL: https://arxiv.org/pdf/2107.10881

[2]. Louis Tremblay Thibault, Tom Sarry, And Abdelhakim Senhaji Hafid. "Blockchain Scaling using Rollups: A Comprehensive Survey" August 2022, IEEE Access , DOI:10.1109/ACCESS.2022.3200051

[3]. Ankit Gangwal, Haripriya Ravali Gangavalli , Apoorva Thirupathi . "A survey of Layer-two blockchain protocols" Volume 209, January 2023 , URL: https://doi.org/10.1016/j.jnca.2022.103539 , https://www.sciencedirect.com/science/article/abs/pii/S1084804522001801

[4]. Sijia Zhao, Donal O'Mahony. "Applying Blockchain Layer2 Technology to Mass E-Commerce" URL: https://eprint.iacr.org/2020/502.pdf

[5]. Chengpeng Huang, Rui Song, Shang Gao, Yu Guo, Bin Xiao. "Data Availability and Decentralization: New Techniques for zk-Rollups in Layer 2 Blockchain Networks" Mar 2024, URL: https://doi.org/10.48550/arXiv.2403.10828

[6]. Maxim Jourenko, Mario Larangeira, Kanta Kurazumi, Keisuke Tanaka. "SoK: A Taxonomy for Layer-2 Scalability Related Protocols for Cryptocurrencies" 2019, URL: https://eprint.iacr.org/2019/352.pdf

[7]. Houshyar Honar Pajooh, Mohammad Rashid, Fakhrul Alam, Fakhrul Alam, Serge Demidenko. "Multi-Layer Blockchain-Based Security Architecture for Internet of Things" 2021, MDPI, URL: https://doi.org/10.3390/s21030772

[8]. He Bai, Geming Xia, Shaojing Fu. "A Two-Layer-Consensus Based Blockchain Architecture for IoT" 2019, IEEE, DOI: 10.1109/ICEIEC.2019.8784458

[9]. Gabriel Antonio F. Rebello, Gustavo F. Camilo, Lucas Airam C. de Souza, Maria Potop-Butucaru, Marcelo Dias de Amorim, Miguel Elias M. Campista, Luís Henrique M. K. Costa. "A Survey on Blockchain Scalability: From Hardware to Layer-Two Protocols" 2024, IEEE, DOI: 10.1109/COMST.2024.3376252

[10]. Lewis Gudgeon, Pedro Moreno-Sanchez, Stefanie Roos, Patrick McCorry & Arthur Gervais. "SoK: Layer-Two Blockchain Protocols" https://link.springer.com/chapter/10.1007/978-3-030-51280-4_12

[11]. Zihuan Xu, Lei Chen. "L2chain: Towards High-performance, Confidential and Secure Layer-2 Blockchain Solution for Decentralized Applications", 2022, URL: https://dl.acm.org/doi/abs/10.14778/3574245.3574278

[12]. Leonardo Maria De Rossi, Michel Avital, Rob Gleasure, Rebecca Solcia. "The Impact of Layer 2 Technologies on the Adoption and Security of Blockchain" URL: https://iris.unibocconi.it/bitstream/11565/4055398/1/ICIS2022_The%20impact%20of%20Layer2%20Technologies%20on%20Blockchain_vsubmission.pdf

[13]. Tobias Schaffner. "Scaling Public Blockchains A comprehensive analysis of optimistic and zero-knowledge rollups"2021, URL: https://wwz.unibas.ch/fileadmin/user_upload/wwz/00_Professuren/Schaer_DLTFintech/Lehre/Tobias_Schaffner_Masterthesis.pdf

[14]. "Upgradeability of Ethereum L2s", Report, July 2023, URL: https://drive.google.com/file/d/182ycEW8C2wk5tGd3X1tG8oQfUy9WmSJk/view

[15]. zkSync FAQ. zkSync Mainnet Explorer URL: https://zksync.io/faq/,URL: https://zkscan.io/.

[16]. Introduction to zkSync for Developers. URL: https://zksync.io/dev/#overview.

[17]. Lightning Network Daemon. URL: https://github.com/lightningnetwork/lnd.

[18]. "What Is Ethereum 2.0 And Why Does It Matter?" In: Binance Academy(2021). URL: https://academy.binance.com/en/articles/what-is-ethereum-2-0-and-why-does-it-matter

[19]. "The Eth2 upgrades. The path to more scalability, security and sustainability for Ethereum".URL: https://ethereum.org/en/eth2/

[20]. Scaling URL: https://l2beat.com/scaling/summary

[21]. “Interactive reference of the Ethereum rollup ecosystem - A comprehensive tool for developers to compare and do in-depth analysis of the expanding Ethereum ecosystem”. URL: https://www.rollup.codes/
[22]. Arbitrum One documentation URL: https://docs.arbitrum.io/welcome/get-started
[23]. Optimism documentation URL: https://docs.optimism.io/
[24]. “Ethereum for everyone - Scaling Ethereum for mass adoption”. URL: https://ethereum.org/en/layer-2/
[25]. Introduction to smart contracts. URL:https://ethereum.org/en/smart-contracts/
[26]. Learn about Ethereum - educational guide to the world of Ethereum; includes technical and non-technical articles, guides, and resources.URL: https://ethereum.org/en/learn/#what-is-crypto-ethereum
[27]. Introduction to Web3, URL:https://ethereum.org/en/web3/
[28]. “Everything You Know about the Scalability Trilemma is Probably Wrong” URL: https://medium.com/logos-network/everything-you-know-about-the-scalability-trilemma-is-probably-wrong-bc4f4b7a7ef
[29]. An Incomplete Guide to Rollups https://vitalik.eth.limo/general/2021/01/05/rollup.html
[30]. “Scaling Solutions”, Overview, URL: https://www.theblock.co/data/scaling-solutions/scaling-overview
[31]. “Zero-Knowledge Rollups”,2024, URL:https://ethereum.org/en/developers/docs/scaling/zk-rollups/
[32]. Vitalik Buterin. “Ethereum in 30 minutes”, URL: https://archive.devcon.org/archive/
[33]. Base documentation, URL: https://docs.base.org/docs/
[34]. Metis Developer Documentation, URL: https://docs.metis.io/dev
[35]. Manta Network docs, Introduction, URL: https://docs.manta.network/docs/Introduction
[36]. What is Starknet? URL: https://www.starknet.io/what-is-starknet/
[37]. Boba Developer Docs, URL: https://docs.boba.network/
[38]. Introduction to zkSync Lite for Developers- Overview, URL: https://docs.lite.zksync.io/dev/ [24]. Polygon zkEVM https://docs.polygon.technology/zkEVM/overview/
[38]Looprings,URL:https://github.com/Loopring/protocols/blob/master/packages/loopring_v3/DESIGN.md
[39]. Joel Agbo, Optimistic vs. Zero Knowledge Rollups: Which Layer 2 is Better? 2024, URL: https://www.coingecko.com/learn/optimistic-vs-zero-knowledge-rollups
[40]. Optimistic vs. ZK Rollup: Deep Dive. URL: https://blog.matter-labs.io/optimistic-vs-zk-rollup-deep-dive-ea141e71e075
[41]. Blockchain Scalability and Privacy: The Rollup Ecosystem, 2023, URL: https://www.gemini.com/cryptopedia/layer-2-scaling-zk-rollup-optimistic-rollup-ethereum#section-examples-of-top-optimistic-rollup-projects