# A Comparison of Layer 2 Techniques for Scaling Blockchains

Adrià TORRALBA-AGELL
Universitat Oberta de Catalunya and
CYBERCAT,
Center for Cybersecurity Research of Catalonia
atorralbaag@uoc.edu

Cristina PÉREZ-SOLÀ
Universitat Oberta de Catalunya and
CYBERCAT,
Center for Cybersecurity Research of Catalonia
cperezsola@uoc.edu

***Abstract*—Since the creation of Bitcoin, back in 2009, many other cryptocurrencies have appear, and its usage has been growing year after year. With this huge popularity, doubts about the ability of blockchains to become worldwide payment systems (or even universal mediums for general decentralised systems) begin to arise and, with them, solutions started to be explored. In this paper we first explain the blockchain scalability problem and then present a brief review and a comparison among some of the state-of-the-art techniques that are used to scale blockchains on Layer 2 (or *off-chain*), analysing properties related to their Usability, Security and Cost.**

***Index Terms*—zero-knowledge techniques, blockchain, scaling blockchain, payment channels, zkRollups, optimistic rollups.**

## I. Introduction

With the apparition of the Bitcoin white paper in 2009 [1] we have seen a huge rise in popularity over the blockchain technology. The massive adoption and application of this technology has brought several changes to the way we interact with the world. From creating digital, secure and decentralised currencies [1] to implementing fair, secure voting system [2], going through enabling secure and reliable digital identification over the Internet [3].

With this rise in popularity, thousands of different applications; such as dAPPs [4], DeFi [5], NFTs [6] and blockchain games [7]; appeared that had made use of this technology. With it, many blockchains had suffered from heavy congestion resulting in poor performance and/or high transaction fees[1].

With this problem, many proposals have been presented in an aim to make blockchain networks more performant. The adoption of some of these solutions has lead to agitated debates within the community, and some of them even originated hard forks that ended up with the creation of new cryptocurrencies.

In general, there are two primary ways to scale networks: scaling the main network (or Layer 1), or creating networks on top of it (or Layer 2). In this paper, we focus on the later solutions, and provide a comparison of their properties in terms of Usability, Security and Cost. We devote special attention to *zkRollups*, one of the Layer 2 solutions that is currently receiving much thought from both the research and the developing communities. *zkRollups* are based on Zero-Knowledge Proofs, and provide a way to compress a batch of transactions onto a succinct proof, that is easier (and faster) to verify compared to checking and verifying every single transaction in the batch. Yadav et al. [8] have analysed multiple solutions at all different Layers (in particular, they have considered solutions for Layer 0, Layer 1 and Layer 2).

The rest of this paper is organised as follows: in Section II, we present the concrete problem of blockchains with scalability, in Section III we present the actual existing solutions to the aforementioned problem. In Section IV, we present a comparison among the different solutions that implement some kind of scalability technology for blockchains. Finally, in Section V, we present and draw the conclusions for this article, as well as the future work.

## II. Blockchain scalability problem

As we stated in the previous Section, blockchain networks usually suffer from scalability problems. Before exploring the solutions that are currently being studied and deployed to solve this problem, we first review the concept of scalability and explain the impact trivial solutions may have on the security and decentralisation of the networks.

The most common metric for measuring blockchain scalability is **transaction throughput**. All blockchains have a (in some cases variable) block size; which determines the amount of transactions that can be fitted in a block; and a block time; which determines how many units of computation can be processed per block and how fast a new block may be added. These two characteristics determine the *throughput* of a blockchain (as the amount of transactions per second the blockchain is able to confirm). This metric has the benefits of being easy to compute and somehow useful to compare different payment systems (even with traditional non-blockchain based ones). However, it falls short in capturing the diversity of operations a single transaction may convey.

Other popular metrics are **latency** (the time it takes for a transaction to be considered final); **bootstrap time** (the time it takes for a new node to synchronize with the network); **cost per confirmed transaction** (in terms of computation, network and storage resources); or **cost to maintain a full node** (also in terms of computation, networking and storage resources).

### A. The Blockchain Trilemma

The challenge of scaling blockchains comes from the need to scale without compromising the security and decentralization properties of the network. This problem is usually

[1]For instance, the Ethereum network reached values over 100 USD on transaction fees during peaks of both Ether price and gas transaction fees on December 2017 or August 2020.

referred to as the Blockchain Trilemma[2]. Let us explain each of the three properties and how are they interlinked in the context of blockchains:

**Security** reefers to the fact that every transaction published to the network is immutable and valid. In order to improve the speed of the network, it can be useful to reduce the number of nodes leading to more performant but more centralised and less secure networks. Blockchains like Nano (XNO) and IOTA are known to be networks that are quick and decentralised in exchange of less security.

**Decentralisation** reefers to how the control of the network is split across its participants. Having high decentralisation usually trades-off with the speed of the network, since the more decentralised a network is, the more verifiers you need to have in order to process transactions. Cryptocurrencies like XRP or EOS are known to prioritise speed and security with the cost of decentralisation.

**Scalability** reefers to the capacity of a network to support high transactional throughput and the ability to sustain growth in the future. Scalability usually trades-off with decentralisation and security since, the more decentralised a network is, the longer it takes to process transactions leading to slower performance. Bitcoin (BTC) and Ethereum (ETH) are known to prioritise decentralisation and security in exchange for scalability.

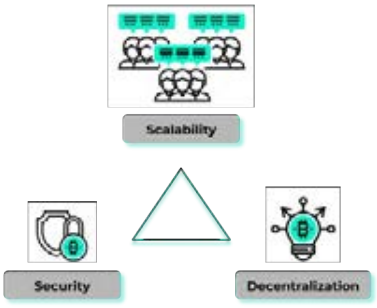


Figure 1. Blockchain Trilemma. Icons from [9]

Taking into account the interactions between scalability and both security and decentralization, the following two constraints are critical to successfully scale blockchains.

**Hardware Requirements** The speed of a blockchain network is determined by the ability of the weakest node in the network to verify transactions and hold its state. Hence, it is desirable to keep the costs to run a node (i.e. the hardware, bandwidth and the storage requirements) as low as possible in order to enable as many participants as possible to the network. Table I summarises the hardware requirements for Bitcoin, Ethereum and Solana blockchains.

**State Growth** State growth refers to how quickly the blockchain grows in the sense that, the more throughput a blockchain allows to happen per unit of time, the quicker the blockchain grows. Since the full nodes of the network store its history –an ever growing ledger– and those nodes should verify all transactions, new nodes can struggle with huge syncing times when joining the network.

[2]Concept coined by Vitalik Buterin, co-founder of the Ethereum Network.

## III. Blockchain scalability solutions

This section summarizes the two main approaches to scale blockchains, and reviews the different techniques that are being discussed and deployed for each one of the approaches (with emphasis on Layer 2 solutions).

### A. Layer 1 scaling (L1)

On the one hand, Layer 1 scalability solutions are focused on the consensus algorithm, the network and the data structure of the blockchain itself. Since the solutions in this layer are performed directly over the chain, these solutions are also commonly named as *on-chain* solutions. One of the main challenges here is to handle block size limit, since its increase directly affects transaction throughput but has consequences on decentralization. Other approaches to Layer 1 go through the implementation of techniques that enable splitting the work of building and verifying blocks across many nodes in the network (sharding).

### B. Layer 2 scaling (L2)

On the other hand, Layer 2 scaling solutions offer to withdraw computation from the main network (Layer 1) and perform this work *off-chain*. This is, instead of performing all the computing-consuming part of the activity onto the blockchain directly, you can perform the bulk and heavy part of the job over the network in the Layer 2.

There are three main approaches that implement Layer 2 scaling.

*1) Payment Channel Networks (PCN):* This system enables the construction of a peer-to-peer network on top of the main blockchain network that allows its participants to perform as many transactions as desired without the main restrictions inherited by the anchored blockchain. However, those payment channels have to overcome several other issues regarding security and reliability. The most well known implementations of PCN are the Lightning Network [10] for the Bitcoin blockchain, and the Raiden Network [11] for the Ethereum blockchain.

*2) Sidechains:* Sidechains build a whole new blockchain in parallel to the main blockchain. The assets can flow freely between both networks, however, the consensus mechanism, the tokens and even their security level are different.

Sidechains can interact in many different ways with the main blockchain. Usually, the main use case for them are exchanging assets between blockchains, for instance, implementing exchanges that allow to swap Bitcoin for Ether. However, other use cases are considered when implementing them, such as scalability.

*3) Rollups:* Rollups are a technique that allow to "roll-up" a batch of transactions and put them on the blockchain all together with a proof that the transactions included in the batch are correctly processed.

In all these three variants, there is only a Smart Contract on-chain which has two main tasks: (1) to process deposits and

| Network | Hard drive space | Number of CPU Cores | Amount of RAM | Internet bandwidth | Number of Nodes |
|---|---|---|---|---|---|
| **Bitcoin** | 350GB HDD | 1 | 1GB | 5Mbps | $\approx 10.000$ |
| **Ethereum** | >500GB SSD | 2-4 | 4-8GB | 25Mbps | $\approx 6.000$ |
| **Solana** | >1.5TB SSD | >12 | 128GB | 300Mbps | $\approx 1.200$ |

Table I
COMPARISON OF BITCOIN, ETHEREUM AND SOLANA NETWORK IN TERMS OF HARD DRIVE, CPU CORES, RAM MEMORY AND BANDWIDTH REQUIREMENTS. DATA OBTAINED FROM [12].

| | | Usability | | | |
|---|---|---|---|---|---|
| **Scalability solution type** | **Technology name** | **General-purpose script / Turing Complete Machine** | **Separate client or software** | **Supported tokens** | **Native proprietary token** |
| **Payment Channels** | **Lightning Network** | No | Yes | Bitcoin (BTC) | No |
| | **Raiden Network** | Yes, native | Yes | ERC20 tokens | Yes, Raiden Network Token (RDN) |
| **Zero-Knowledge Rollups** | **zkSync** | Yes, in Zinc [18] | Yes | Ether (ETH), ERC20 tokens | No |
| | **Loopring 3.8** | No | Yes | Ether (ETH), ERC20 tokens | Yes, Loopring (LRC) |
| | **Starknet** | Yes, implemented using Cairo [19] | Yes | Ether (ETH), some ERC20, ERC721 tokens | No |
| **Optimistic Rollups** | **Arbitrum** | Yes, through ArbOS [20] (EVM compatible) | Yes | ERC20, ERC721 tokens | No |
| | **Optimism** | Yes, supports Solidity and Vyper [21] | Yes | ERC20, ERC721 tokens | Yes, Optimism (OP) |

Table II
TABLE COMPARING USABILITY

withdrawals and (2) verify *proofs* that everything happening off-chain is following the predefined set of rules.

For rollups, the way these proofs are generated and validated give rise to two different kinds of rollups: Optimistic rollups –which are backed by *fraud proofs*– and zkRollups –which are backed by *validity proofs*–.

There are many differences between fraud proofs and validity proofs. In short, fraud proofs present an evidence that a state transition was *incorrect*, while validity proofs present an evidence that a state transition was *correct*. Therefore, fraud proofs present an *optimistic* point of view, whereas validity proofs present a more pessimistic approach.

Due to the optimistic nature of the fraud proofs, they are not needed for every state transition, they are only required in a possible fraudulent scenario. For this reason, the main advantage is the fact that they require fewer computational resources since proofs are only needed in case a party is trying to cheat the rest of the participants. However, they come with a cost: interactivity and long withdrawal time. There is the need to provide a *challenge period* in which any party in the system can submit a fraud proof invalidating the batch of transactions. The implementation of this challenge period implies interactivity –which forces the node to be *live*– and long withdrawal times –since the challenge period should be long enough for it to be reliable (around 7 days)–.

Validity proofs, on the other hand, represent off-chain computation sent to the main network. The main advantages for this kind of proofs are the fact that the main network always have a correct Layer 2 state, and that this new state can be relied and trusted immediately (unlike fraud proofs). However, they come with the cost that every state transition needs for a proof (which should be both generated and verified), possibly impacting scalability.

## IV. COMPARISON OF LAYER 2 SOLUTIONS

In this section, we present three different tables comparing existing scalability solutions for blockchains in terms of Usability, Security and Cost. Our comparison considers examples of Payment Channel Networks, Zero-Knowledge Rollups, and Optimistic Rollups. In particular, we have chosen the most popular solutions of each kind, except for zkRollups where we have also considered representativity of the different Zero-Knowledge techniques as selection criterion. Our analysis thus includes the Lightning Network (LN) [10] and the Raiden Network [11] as Payment Channel Networks; zkSync [13], Loopring 3.8 [14] and Starknet [15] as Zero-Knowledge Rollups; and Arbitrum [16] and Optimism [17] as Optimistic Rollups.

It is important to note that the Lightning Network aims to scale the Bitcoin blockchain, while all the other solutions are implemented in order to scale the Ethereum network.

### A. Usability

Table II shows the comparison in terms of Usability. This category is intended to illustrate the versatility of the different scalability solutions. For this reason, we have considered

| | | Security | | | | | |
|---|---|---|---|---|---|---|---|
| **Scalability solution type** | **Technology name** | **Security model** | **Cryptographic primitives** | **ZK technique** | **Quantum resistant** | **Separate network** | **Type of network** |
| **Payment Channels** | **Lightning Network** | Inherited from L1 + node always online + censorship-resistant within time $t$ | Hash functions, digital signature | Not applicable | No | Yes | P2P |
| | **Raiden Network** | Inherited from L1 + node always online + censorship-resistant within time $t$ | Hash functions, digital signature | Not applicable | No | Yes | P2P |
| **Zero-Knowledge Rollups** | **zkSync** | Inherited from L1 + CRS always hidden + censorship-resistant within time $t$ | Pairings, KoE, minimal trusted setup | PLONK [22] | No | Yes | Centralised |
| | **Loopring 3.8** | Inherited from L1 + CRS always hidden + censorship-resistant within time $t$ | Pairings and trusted setup | zkSNARK | No | Yes | Centralised |
| | **Starknet** | Inherited from L1 + censorship-resistant within time $t$ | Hash Functions | zkSTARK [23] | Yes | Yes | Centralised |
| **Optimistic Rollups** | **Arbitrum** | Inherited from L1 + based on Game Theory + censorship-resistant within time $t$ | Fraud Proofs (Merkle Trees or SNARK/STARK) | Not applicable | No | Yes | Centralised |
| | **Optimism** | Inherited from L1 + based on Game Theory + censorship-resistant within time $t$ | Fraud Proofs (Merkle Trees or SNARK/STARK) | Not applicable | No | Yes | Centralised |

Table III
TABLE COMPARING SECURITY

if they provide some kind of **general-purpose scripting** (Turing Complete Machine), we have studied if they need an **additional** –separated– **client** or software, which are the **tokens** those solutions can handle and, finally, if they run a **native** –proprietary– **token** in order to interact with the solution.

Let us start with the scripting capabilities. We have found that almost all of the considered solutions present some kind of mechanism that enables the user to implement general-purpose Smart Contracts. However, the Lighting Network does not support this kind of scripting due to the limitations imposed by the Bitcoin Script.

Moreover, all those solutions need a separated –dedicated– client or software. In this sense, none of them are "built-in" or directly integrated into the L1 network.

Regarding the supported tokens, we have found that the LN only supports Bitcoin (BTC), while the rest of solutions implemented on top of the Ethereum Network, in general, support ERC20 tokens and, some of them, also support Ether (ETH) and/or ERC721 tokens. It is worth mentioning that Starknet is currently in an alpha stage and only supports Ether (ETH), some ERC20 and ERC721 tokens, but in the future they plan to support WBTC, USDC, USDT and DAI as well.

Finally, in this topic, some of these off-chain solutions have a native –proprietary– token in order to interact with the auxiliary network. In our listed technologies, the Raiden Network, Loopring and Optimism are the ones that have a native token, while the rest of the solutions inherit the token from the parent network, namely, Bitcoin for the LN and Ether for the rest of solutions.

### *B. Security*

Table III shows the comparison in terms of Security. In this table we present the different security-related features that these solutions have. In particular, we have considered the **security model**, the **cryptographic primitives**, the kind of specific **Zero-Knowledge technique** they implement in each zkRollup, whether they feature **quantum resistance** (i.e. the cryptographic primitive will be still secure once quantum computing is well stablished). Finally, we have studied the needed for independent and **separated network**, as well as, the **type of network** they implement.

The security model in which those technologies rely is very different among the three different scalability solution types.

| | | Cost | | |
|---|---|---|---|---|
| **Scalability solution type** | **Technology name** | **Fees** | **Processing time** | **Withdrawal time** |
| **Payment Channels** | **Lightning Network** | Fees for the funding transaction (+ possible hops) + closing transaction | Near instant | From 1 hour to several days |
| | **Raiden Network** | Similar to Lightning Network fee system | Near instant | Up to 3 hours |
| **Zero-Knowledge Rollups** | **zkSync** | $\approx$ 1/100th of mainnet costs for ERC20 tokens and $\approx$ 1/30th for Ether (ETH) transfers | Near instant | From 10 minutes to 7 hours |
| | **Loopring 3.8** | From 1/30th up to 1/100th of the mainnet costs for ETH and ERC20 tokens | Near instant | From 6 minutes to 2 hours |
| | **Starknet** | Fees only to post to L1, in the future fees also for L2 | Near instant | Not specified |
| **Optimistic Rollups** | **Arbitrum** | Up to 1/10th of the mainnet cost | Near instant | Around 7 days |
| | **Optimism** | L2 execution fee + L1 security fee | Near instant | Around 7 days |

Table IV
TABLE COMPARING COST

In the case of the Payment Channels, the security is granted with the guarantees that L1 provides in addition to the assumptions that the node is always online, and that the network is censorship-resistant[3] within time $t$. Both solutions on this category make use of hash functions and digital signatures as cryptographic primitives.

Regarding the Zero-Knowledge Rollups, they rely on the security inherited from L1 –just like the Payment Channels– but, in this case, they also rely on the validity proofs obtained from the Zero-Knowledge techniques in order to verify that the computation made off-chain is properly done. In particular, for the zkSync, they use PLONK as the zkSNARK that relies on Pairings, Knowledge of Exponent, and a Universal Trusted Setup as cryptographic primitives. The reader can find more information about the security and the cryptographic assumptions that zkSync makes on [24] and [25].

We were not able to find much information about the technical specifications of Loopring but they are using some zkSNARK [26], so we assume that they need Pairings and some kind of trusted setup as cryptographic primitives.

Starknet relies on zkSTARK, which has the constrain requirement of hash functions, presenting the minimum cryptographic requirements among all the Zero-Knowledge solutions studied here. Moreover, given that Starknet *only* relies on Hash functions, it is the only technology –in our list– that is assumed to be Quantum resistant.

Optimistic solutions present a totally different security approach. While they inherit the security from L1, both Arbitrum and Optimism rely on Game Theory when securing their algorithm, and they provide incentives for nodes that detect frauds to uncover them. A single party executing and validating transactions is thus enough to detect a fraud.

Finally, when looking at the actual implementation of the different solutions, we found that all the studied solutions implement a separated network. To be precise, both the Lightning Network and the Raiden Network use a Peer-to-peer (P2P) network, while the rest of solutions have a centralised approach. Nonetheless, zkSync, Starknet and Arbitrum have plans for decentralising their network [27], [28], [29].

[3]This is, there exists a high enough fee threshold such that the transaction will be mined onto L1 in a block within a specific amount of time.

### C. Cost

Table IV shows the comparison in terms of Cost. In this Table, we have considered two different approaches for the transaction cost: **fees** and **time**. We have considered these two approaches since we find that they are the main concerns regarding cost for the scalability solutions.

The fees systems used in those solutions vary in a wide range. The Lightning Network uses a fee system composed by some on-chain fees to pay for the funding and closing transactions; and some off-chain fees nodes may charge to use their channels for multi-hop payments. The Raiden Network fee system is similar to the Lightning Network model.

For the zkRollup approaches and for Optimism the table summarizes the claims the projects make in their official websites [30], [14], [28], [31] (zkSync, Loopring, Starknet and Optimism, respectively); for Arbitrum, we include an estimation based on external resources [32].

Finally, regarding the processing time cost on L2, we found that all the solutions have a near instant processing time, only limited by the hardware that actually performs the operation on the L2 and communication delays. However, when considering the withdrawal time[4], we can see a wide variety of time ranges. In the case of the Lightning Network, the withdrawal time window is up to 1 hour in case of cooperative closing (6 block confirmations in the Bitcoin blockchain), and may vary from 1 hour to several days in case of fraudulent closing. A similar approach applies for the Raiden Network, however, in this case, the time windows is shrinked to up to 3 hours in the worst case [33].

zkRollups are considered to be fastest in terms of withdrawal time, with an average withdrawal time between 6 and

[4]The time required to take the funds from L2 back to L1.

10 minutes and with a maximum time window of 7 hours.

Optimistic Rollups have bad withdrawal times since they rely on fraud proofs that take a considerable amount of time (around 7 days) due to the challenge window.

## V. Conclusions and Future Work

In this paper, we have presented some of the state-of-the-art existing solutions implemented as scalability techniques for blockchain. These solutions can be categorised in two different categories: Payment Channel Networks and Rollups.

We have first introduced the scalability problem in blockchains. Then, we have presented a brief introduction to the different types of scalability techniques considered in this review and we have compared them among different dimensions (Usability, Security, and Cost). Several insights can be drawn from the result of this review.

Firstly, from a usability standpoint, we can see that both rollup approaches excel at providing a wide variety of compatible tokens, as well as Smart Contract support in most cases.

Secondly, from a security point of view, we can see that generally Layer 2 solutions inherit their security model from the underlying Layer 1, and tend to add additional security assumptions. Moreover, most zkRollups require the usage of complex cryptographic primitives (pairings), whereas the other approaches are based only on signatures and hash functions.

Thirdly, considering the costs of using those solutions, we can see that, theoretically, zkRollups are the best ones in terms of both fees and time constraints, in the sense that they are the ones that present less fees when transacting and interacting between Layers, and they provide a reasonable amount of withdrawal time. However, since they are centralized, they may be prone to censorship, less privacy preserving than PCN (where L2 transactions are only seen by the sender and the receiver), and susceptible to classic single point of failure attacks.

As future work for this paper, we plan to extend this article by deploying the actual considered solutions and performing experiments on those in order to benchmark the capabilities of them. To be precise, we want to review and classify the actual capabilities for the general-purpose scripting those solution offer, we want to detail better the Zero-Knowledge techniques zkRollups are using and, finally, perform experiments regarding the fee cost and the processing time these solutions offer.

## Acknowledgements

This work is partially supported by the Spanish Government under grants RTI2018-095094-B-C22 “CONSENT” and PID2021-125962OB-C31 “SECURING”.

## References

[1] NAKAMOTO, Satoshi. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 2008, p. 21260.

[2] KHAN, Kashif Mehboob; ARSHAD, Junaid; KHAN, Muhammad Mubashir. Secure digital voting system based on blockchain technology. *International Journal of Electronic Government Research (IJEGR)*, 2018, vol. 14, no 1, p. 53-62.

[3] SULLIVAN, Clare; BURGER, Eric. Blockchain, digital identity, e-government. *En Business Transformation through Blockchain*. Palgrave Macmillan, Cham, 2019. p. 233-258.

[4] Decentralized applications (DAPPS). *ethereum.org [online]*. [Accessed 23 May 2022]. Available from: https://ethereum.org/en/dapps/

[5] Decentralized finance (DEFI). *ethereum.org [online]*. [Accessed 23 May 2022]. Available from: https://ethereum.org/en/defi/

[6] Non-fungible tokens (NFT). *ethereum.org [online]*. [Accessed 23 May 2022]. Available from: https://ethereum.org/en/nft/

[7] Top blockchain games. *DappRadar [online]*. [Accessed 23 May 2022]. Available from: https://dappradar.com/rankings/category/games

[8] Yadav, Jyoti & Shevkar, Ranjana. (2021). Performance-Based Analysis of Blockchain Scalability Metric. *Tehnički glasnik*. 15. 133-142. 10.31803/tg-20210205103310.

[9] Vecteezym.com, Bitcoin elements thin line and pixel perfect icons [online]. [Accessed 4 June 2022]. Available from: https://www.vecteezy.com/vector-art/681001-bitcoin-elements-thin-line-and-pixel-perfect-icons

[10] Lightning network. Lightning Network [online]. [Accessed 30 May 2022]. Available from: https://lightning.network/

[11] Fast, cheap, Scalable token transfers for Ethereum. Raiden Network [online]. [Accessed 30 May 2022]. Available from: https://raiden.network/

[12] STARKWARE. Redefining scalability. Medium [online]. 1 December 2021. [Accessed 4 June 2022]. Available from: https://medium.com/starkware/redefining-scalability-5aa11ffc5880

[13] ZkSync - rely on math, not validators [online]. [Accessed 4 June 2022]. Available from: https://zksync.io/

[14] Loopring [online]. [Accessed 4 June 2022]. Available from: https://loopring.io/#/

[15] StarkNet [online]. [Accessed 4 June 2022]. Available from: https://starknet.io/

[16] Arbitrum One Portal [online]. [Accessed 4 June 2022]. Available from: http://arbitrum.support/

[17] Optimism [online]. [Accessed 4 June 2022]. Available from: https://www.optimism.io/

[18] LABS, Matter. ZKEVM FAQ. zkSync Documentation [online]. [Accessed 4 June 2022]. Available from: https://docs.zksync.io/zkevm/#general

[19] Hello, cairo. Hello, Cairo - StarkNet documentation [online]. [Accessed 4 June 2022]. Available from: https://starknet.io/docs/hello_cairo/index.html#hello-cairo

[20] Arbos: The Arbitrum Operating System · Offchain Labs Dev Center. · Offchain Labs Dev Center [online]. [Accessed 4 June 2022]. Available from: https://developer.arbitrum.io/docs/arbos

[21] Developing smart contracts on optimism. Optimism Docs [online]. [Accessed 4 June 2022]. Available from: https://community.optimism.io/docs/guides/smart-contract-devs/#

[22] GABIZON, Ariel; WILLIAMSON, Zachary J.; CIOBOTARU, Oana. Plonk: Permutations over lagrange-bases for oecumenical noninteractive arguments of knowledge. *Cryptology ePrint Archive*, 2019.

[23] BEN-SASSON, Eli, et al. Scalable, transparent, and post-quantum secure computational integrity. *Cryptology ePrint Archive*, 2018.

[24] LABS, Matter. Security. zkSync Documentation [online]. [Accessed 4 June 2022]. Available from: https://docs.zksync.io/userdocs/security/#cryptography-used

[25] MATTER-LABS. Zksync/protocol.md at master Matter-Labs/zksync. GitHub [online]. [Accessed 4 June 2022]. Available from: https://github.com/matter-labs/zksync/blob/master/docs/protocol.md#assumptions

[26] Loopring open sources its ZKSNARK Circuit code. [online]. 29 October 2019. [Accessed 4 June 2022]. Available from: https://blogs.loopring.org/loopring-open-sources-its-zksnark-circuit-code/

[27] LABS, Matter. Decentralization. zkSync Documentation [online]. [Accessed 4 June 2022]. Available from: https://docs.zksync.io/userdocs/decentralization/

[28] StarkNet terms of use. StarkNet [online]. 6 December 2021. [Accessed 4 June 2022]. Available from: https://starknet.io/starknet-terms-of-use/

[29] Inside arbitrum · Offchain Labs Dev Center. · Offchain Labs Dev Center [online]. [Accessed 4 June 2022]. Available from: https://developer.offchainlabs.com/docs/inside_arbitrum

[30] LABS, Matter. Overview. zkSync Documentation [online]. [Accessed 4 June 2022]. Available from: https://docs.zksync.io/userdocs/intro/#introduction

[31] Transaction fees – optimism. [online]. [Accessed 4 June 2022]. Available from: https://help.optimism.io/hc/en-us/articles/4411895794715-Transaction-fees

[32] L2fees.info. L2Fees.info [online]. [Accessed 4 June 2022]. Available from: https://l2fees.info/

[33] NETWORK, Raiden. How do I withdraw tokens to my on-chain account? Medium [online]. 5 October 2021. [Accessed 4 June 2022]. Available from: https://medium.com/raiden-network/how-do-i-withdraw-tokens-to-my-on-chain-account-dfb27771829e