LUISS

Department of Business and Management

Course of Blockchain & Cryptocurrencies

Assessing the Impact of Rollups Scaling Solutions on Ethereum's layer-2 Ecosystem

Prof. Bernaschi Massimo

SUPERVISOR

Alessia Renzoni – 232341

CANDITATE

Academic Year 2022/2023

Acknowledgments

First and foremost, I would like to warmly thank Prof. Bernaschi for patiently supervising my thesis, especially for believing in my journey and supporting me throughout the way.

I would like to dedicate it to my parents, Soada and Marco, for encouraging me to never let go no matter the obstacles I face, for nurturing me into the woman I am today, and for their economic support. To my sister, Valentina, as well, for constantly reassuring me that good times are ahead and for being the muse I always look up to.

A very important dedication to my grandmother, Vanda, who passed away during COVID, whom I miss very much and I am sure would be very proud of the person I have become. A second mother figure, the kindest human soul, who always supported me, and will always be right over me.

A heartfelt thanks to my boyfriend, Matteo, who stood beside me during the highs and lows of my academic career and never made me feel less. A person that works to pay for his studies, with determination and strength that no one has, which I aspire to every day.

To my grandmother, Gerarda, who continuously made me feel like the "Tech-Genius" of the family for resolving simple problems on her phone. Though, she always made me feel that I could achieve great things in life, which were warm mental support that I needed in my low periods.

I want to thank my sister's boyfriend, Davide, for introducing me to the world of blockchain and cryptocurrencies, which ended up being a theme that I am very enthusiastic about.

Thanks to all my family relatives for supporting me. Both to my uncle Stefano and aunt Tania for periodically checking up on me and giving moral supports.

Thanks for the support of my dearest friends, each more unique than the other, for being what friends are supposed to be, being there in times of need. Patricia, who I video call as much as possible as she lives in France, and I have a history with her in China. Andrea and Flavio, are my two childhood friends who always have been there. And, Camilla, for making me believe in adult friends who just show up when you least expect it.

Lastly, a very special thanks to my best friend, my dog, Bart. Who has been there throughout everything, even sacrificing his walks to support me during stressful times.

Table of Contents

Introduction……8

CHAPTER 1

ETHEREUM BLOCKCHAIN AND THE MERGE

1.1 Ethereum Network……9

1.1.1 Introduction to Ethereum……....9

1.1.2 Ethereum Virtual Machine (EVM)……...10

1.1.3 Decentralized Applications (Dapps)……10

1.1.4 Decentralized Finance (DeFi)……...11

1.1.5 Non-fungible-tokens (NFT)…… 11

1.2 Ethereum 1.0 to Ethereum2.0……...12

CHAPTER 2

ETHEREUM'S SCALABILITY

2.1 Scalability Problems……15

2.2 Scalability Factors…… 16

2.2.1 Consensus Model……16

2.2.2 Gas Fees…… 16

2.2.3 Dapps and Smart Contracts……17

2.3 Scaling Solutions…… 18

2.3.1 On-Chain vs. Off-Chain Scaling……18

2.3.2 Sidechains and State Channels……19

2.3.3 Plasma…… 20

2.3.4 Lightning Network…… 20

2.3.5 Rollups……20

CHAPTER 3

ETHEREUM'S LAYER-2 ROLLUPS TECHNICAL SOLUTIONS AND IMPACTS

3.1 Layer-2 Technicalities…… 22
3.2 Optimistic Rollups……23
3.2.1 Optimistic Rollups Description…….. 23
3.2.2 Optimistic Rollups Fraud Proofs……24
3.2.3 Optimistic Rollups Interoperability……25
3.2.4 Optimistic Rollups Scalability……26
3.3 ZK-Rollups…… 27
3.3.1 ZK-Rollups Description…… 27
3.3.2 ZK-Rollups Validity Proofs…… 28
3.3.3 ZK-Rollups Interoperability…… 30
3.3.4 ZK-Rollups Scalability…… 31
3.4 Optimistic Rollups vs. ZK-Rollups……31
3.4.1 Pros and Cons Optimistic Rollups…… 31
3.4.2 Pros and Cons ZK-Rollups……..32
3.4.3 Final Thoughts……32

CHAPTER 4

ETHEREUM'S FUTURE PROSPECTIVE

4.1 Future Scenarios…… 33
4.1 Sharding and Rollups…… 33
4.2 Rollups and More…….. 33

CONCLUSIONS……...35

REFERENCES…….. 36

List of Figures

Figure 1: Ethereum's Upgrade Path……13
Figure 2: Breakdown of how Sharding Works……14
Figure 3: Modular Blockchain Rollups……...23
Figure 4: Layer-2 to Layer-1 Transaction Workflow…… 25
Figure 5: Ethereum vs. Rollup transaction……. 27
Figure 6: Modular Blockchain Rollups Layering……34

ABSTRACT

Solutions for scaling blockchain-based platforms can potentially optimize transaction speed processing through various Off-chain and On-chain methods. However, scalability is a widely recognized weakness for Ethereum as it is not hinting at stopping any time soon, leading to a clogged network and exorbitant gas prices. Trying to fulfill the original Ethereum promise of a secured and decentralized execution platform, developers actively analyze layer-2 scaling methods. A thorough description of the scaling issue will demonstrate the difficulties behind implementing a reliable solution. We will assess the impact on the Blockchain and its economic implications of a layer-2 Rollup scaling solution, which has been catching the attention of Vitalik Buterin together with his team. A clear distinction between two models will be scrutinized, Optimistic Rollups and ZK-Rollups, based on their approaches to fraud proving, operating costs, data availability, and their efficiency at scaling the congested Ethereum network. As ZK-Rollups also incorporate two fraud-proving systems, a deeper evaluation assesses which provides a greater contribution to the security of its users and network as a whole. Equally, we will also understand why several On-chain solutions pose major drawbacks to the principal vision of Ethereum, decentralization. The network's developers need to meticulously calculate the risks and gains of certain scaling solutions for the achievement of decentralized and scalable trust.

INTRODUCTION

In the last few years, blockchains and cryptocurrencies and in particular, Ethereum, have triplicated their active users going from 210 thousand in 2019 to 620 thousand in 2023. Ethereum has come a long way since its launch making throughout the way extremely important decisions which brought successful innovative impacts such as the recent switch to the Proof of State consensus model. Yet, the hype surrounding all blockchains has brought to light a not-yet-solved scalability problem causing the network to clog and slow down. Similar to Bitcoin implementing the Lightning Network solution, Ethereum's developers have constructed a lengthy process to deflect the problem as much as possible while maintaining the principles of decentralization and security. An Off-chain Rollup layer-2 scaling solution is where interests are now directed, the main chain outsources to the Rollup layer the function to validate transactions at increased speed, generate more spaces for blocks, and maintain lower fees. It seems to be an effective solution, at least, on paper.

This paper aims at studying Ethereum's scalability issues focusing on how it turned out to be a problem and analyzing On-Chain and Off-Chain solutions, ultimately assessing the impact of Rollups' scaling solution. We want to verify if a such solution could be the future backbone of Ethereum.

The first chapter gives an overview of Ethereum and the many characteristics involved that differentiates it from other blockchains. Following, is a description of The Merge, a combination of the old Ethereum (consensus layer) and new Ethereum (execution layer) together with the Proof of Stake consensus model, appearing to be the first step for a scaling solution.

The second chapter illustrates the scalability problem of Ethereum before the Merge and how it persists after the merge. An evaluation of On-chain and Off-chain solutions are put in perspective, explicitly layer-2 solutions such as Sidechains, State Channels, Plasma, and Lightning Network.

The third chapter includes a deep analysis of the Rollups layer-2 scaling solution comprising the two most advanced methods, Optimistic Rollups, and ZK-Rollups (zero-knowledge). A thorough comparison of their methods of proving, processing, compressing, and cost resources is made, allowing room for judgment for the most appropriate solution.

Finally, we conclude with personal opinions for future perspectives, based on the evaluation made in the previous chapters, in the evolution of Ethereum and the integration of possible methods that can be adopted for the mitigation of the scalability problem.

CHAPTER 1

Ethereum Blockchain and Merge

1.1 Ethereum Network

1.1.1 Introduction to Ethereum

The book on Ethereum, "The Infinite Machine", written by Camilla Russo, quotes "Vitalik wanted his platform to be the underlying and imperceptible medium for every application, just what medieval scientists thought ether was…plus, it sounded nice.". The word Ethereum originates from the concept of Ether, an invisible material believed to fill up regions of space carrying electromagnetic waves. Such an assumption was debased by Albert Einstein. But in 2013 Vitalik Buterin decided to name Ethereum his decentralized and open-sourced Blockchain.

Ethereum officially launched in 2015 becoming the second-largest cryptocurrency by market cap right after Bitcoin. Unlike Bitcoin, Ethereum was not only intended to be a digital currency, but Ethereum's founders also established it to become a new large-scale decentralized computing platform leveraging the blockchains' security and providing the foundation for a diverse range of applications. Ethereum blockchain makes it possible for developers to create applications varying from games, and sophisticated databases to intricate decentralized financial tools without the need for any kind of intermediary such as banks. This is all achieved through smart contracts, much like normal contracts yet with one difference lying where smart contracts can automatically execute once the terms are met. Smart contracts convey rapidity and eliminate the concept of trust as they execute without the need for either party to know who they are dealing with as long as the agreements are met and satisfied, thus, no need for any interaction with an intermediary. Ethereum is neither owned nor operated by a single individual, rather, anyone that has access to an internet connection is able to run and interact with the network. Like Bitcoin, ETH is secured by the Ethereum blockchain where the quantity of computing power, contributed from all the computers on the network, evaluates and validates each transaction resulting virtually impossible subvert the system. The Ether currency is used to pay gas, which is an execution fee paid by users for running transactions on Ethereum. However, Ether is necessarily required to build decentralized applications, smart contracts, and peer-to-peer payments. Furthermore, Ethereum has currently welcomed a few popular

Ethereum-based innovations such as *stablecoins*[1], Decentralized finance apps, Decentralized apps, and NFTs. Yet, all the resources mentioned above will be practically impossible to handle and access without the support of a Virtual Machine.

1.1.2 Ethereum Virtual Machine (EVM)

EVM is a runtime compiler fundamental to the execution of Ethereum-based smart contracts. Simply put, EVM is the translator of the smart contract's language, which is written in the Solidity[2] programming language for Ethereum. EVM initially operates in a sandbox environment, it ensures first the well-functioning performance of a smart contract before deploying it on the Ethereum main network. To guarantee security from cyberattacks, smart contracts are compiled into bytecode that is read and executed by the EVM. Suppose a transaction is sent to the EVM through a smart contract, to validate this transaction Ethereum will have to perform a consensus algorithm where nodes on Ethereum validate the transaction in place. During this process, the miner nodes are charged a fee to validate the transaction and earn in turn a reward for the successful completion. All nodes executing the smart contracts have to use their respective EVMs. Therefore, Ethereum has a sole canonical state, and the EVM is what circumscribes the rules for processing a new valid state from block to block.

1.1.3 Decentralized Applications (Dapps)

Dapp is an application based on a decentralized network that takes advantage of a smart contract and a front-end user interface. Dapps are decentralized, deterministic, Turing complete[3] and isolated systems. They are not controlled by anyone, they perform the same action anywhere executed and if they contain a bug it will not hamper the functioning of the blockchain network. Dapps do not require to provide identities to interact with them. No single entity will be able to block users from submitting transactions and interacting with the Decentralized app and no data will also be able to be tampered with as the blockchain is immutable and indisputable due to cryptographic primitives. However, Dapps are harder to maintain and update as it is impossible to modify data and code published on the blockchain. As network congestion increases due to computational resources that the Dapp utilizes and the performance overhead, a true scaling problem occurs when decentralized applications gain a higher user base.

---

[1] Type of cryptocurrency where the value of the digital asset is supposed to be pegged to a reference asset.

[2] Statically-typed curly-braces programming language designed for developing smart contracts that run on the EVM.

[3] Machine that given enough time and memory along with instructions, can solve any computational problem.

1.1.4 Decentralized Finance (DeFi)

DeFi is a term for financial services on a decentralized blockchain like Ethereum. With DeFi, what was done at the bank can be supported by decentralized finance such as borrowing, lending, earning interests, trade assets, and much more. Besides, it is quicker and requires neither a third party nor paperwork. DeFi is a digital alternative that has its main advantage of cutting the unnecessary costs that a bank endures (rent, salaries…) and is free, open with the only requirement of possessing an internet connection to create a wallet. DeFi allows pseudonymous users' information, ensures flexibility in moving assets anywhere at any time while avoiding waiting periods and expensive fees as well as being transparent for everyone involved to observe the full set of transactions. On the other hand, it is suggested to carefully adapt to the environment as investments can experience high volatility and active trading can result in being expensive. Even though Bitcoin could be seen as the first DeFi application, Ethereum, on the contrary, surpasses Bitcoin's characteristics and evolves the DeFi application into digital programmable money, that goes beyond storing and sending value, with the use of smart contracts.

1.1.5 Non-Fungible Tokens (NFTs)

NFTs are tokenized assets having unique identification codes and metadata through smart contracts that separate them from other tokens. They represent ownership of unique items, able to tokenize art, collectibles, and real estate. The ownership of an NFT is secured through the Ethereum blockchain, the record of ownership is immutable and is not interchangeable with other items as they possess unique properties. The purpose of NFTs is to bring back value in properties of tangible items such as scarcity, uniqueness, and proof of ownership. They allow claiming ownership of any unique piece of digital data or non-digital assets as long as it is trackable through the public Ethereum ledger. NFTs can be bought, sold, traded, and pay out royalties to the creators of the assets sold. The NFT world has collided with the gaming world as both gamers and NFT issuers profit from one single game item. Players benefit from the possession of the NFT on the game and in turn, the issuer gains royalties even if the player he sold the NFT item to, is selling it in a secondary exchange market. Additionally, NFTs and DeFi work together interestingly. DeFi applications allow you to borrow money by using collateral, if the user does not possess enough cryptocurrency to cover the cost, DeFi allows you to use NFTs as collateral if in possession. DeFi also enables the possibility for creators to sell their NFTs in fractions like shares, bringing in investors from the DeFi world possibly to a game-related exciting NFT. NFT allows artists, collectors, investors, and many more together, besides it generates economic incentives whether for a loan or for an artist wanting to be

acknowledged, or for a gamer unlocking the greatest vest a game character can have. It is a pool which all types of people can merge into.

1.2 Ethereum 1.0 to Ethereum 2.0

By now, the Ethereum "Merge" has officially happened and before analyzing what it entails, we will first understand what pushed Vitalik Buterin to endeavor this update. The original Ethereum relied on a "Proof of Work" consensus mechanism to verify transactions likewise Bitcoin. Such a method eliminates the risk of double spending and thus achieves a solution to a much like Byzantine General's Problem[4]. Yet the PoW requires a great amount of processing power, which is contributed by "miners" in the network who compete in being the first to resolve a very complex math puzzle subjected to a time frame (miners who solve the problem are compensated with rewards). As this process repeats every 30 seconds and the traffic network increases, Proof of Work is ultimately limited by network congestion, which leads to outraging high fees for the processing of transactions. This was the principal reason for Vitalik Buterin to switch to a staking consensus model also called the "Proof of Stake". This consensus mechanism is expected to contrast the limitations of the proof of work model, providing faster and less resource-demanding output. Instead of a competition, PoS requires a suitable number of network participants to stake their ETH coins to become validators. A participant is selected according to a mechanism that takes into account the staked amount and then validates the latest block of transactions that is also accurately attested by the rest of the validators. All validators receive a reward in proportion to their initial stake, however, if validators wrongfully attest a batch of transactions, their stake will be taken. Therefore, miners are largely more encouraged to migrate towards the PoS chain than PoW as it entails for them lower costs of resourceful computational power.

[4] Game theory problem, which describes the difficulty decentralized parties have in arriving at consensus without relying on a trusted central party.

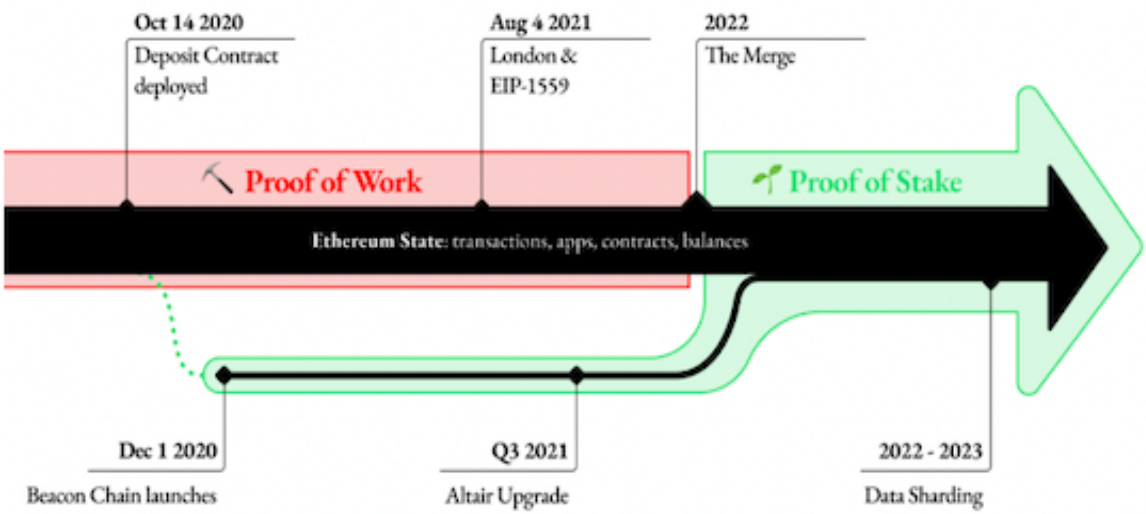

Figure 1- Ethereum's Upgrade Path. Source: "Ethereum Renaming: Ethereum 1.0 and 2.0", Medium (2022)

The first phase of this switch was to implement a Beacon Chain, the new Proof of Stake consensus layer that merges with Ethereum 1.0. The Beacon Chain stores and manages the archive of validators and organizes the shard chains. This chain is the backbone of the Ethereum 2.0 system, the one that continuously scans, validates, collects stakes, and sends out rewards to validators who correctly execute their function, subtract stakes to those not online and slash ETH rewards to malicious users. The Beacon Chain is a coordination system of the newly formed network with the responsibility for generating new blocks and ensuring their validity all while organizing the functions and roles behind validators to keep the network secure. Though, Beacon Chain is not programmed to run smart contracts, which is why shard chains are put in place leading to the next stage of Ethereum 2.0. In addition, the terminologies around Ethereum 1.0 and 2.0 have changed. Ethereum 1.0 is now the execution layer and Ethereum 2.0, is the consensus layer. The combination of the two has formed the new Ethereum and officially represents the switch from the Proof of Work consensus model to the Proof of Stake mechanism.

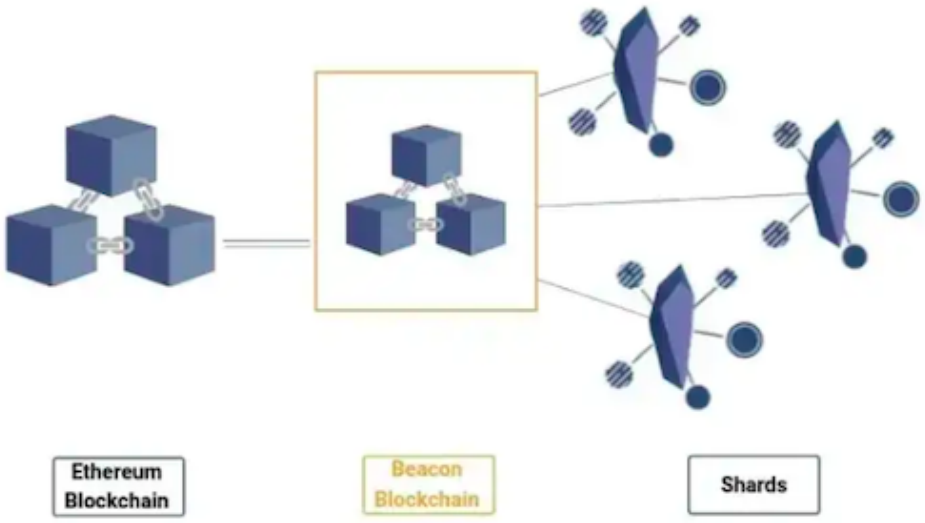

Figure 2 - Breakdown of how sharding works. Source: "Goodbye, Ethereum 1.0 ... Hello, Ethereum 2.0!", Medium (2022)

The second phase surrounds the *sharding* process which will provide increased capacity to store and access data. Since in the Proof of Work blockchains, the majority of nodes in the network contain a copy of the history of the network's transactions, this leads to the huge disadvantage of occupying a great amount of storage. The technique of Sharding partitions and breaks down a large volume of data into smaller and controllable sections (shards) to efficiently scale at large. Shard chains drastically decrease the congestion of the nodes in the network by making one node manage only one shard instead of the entire blockchain. Shards are suitable for parallel processing which resolves the delay of sequential processing executed in single blockchains. Sharding will be an enormous contribution to the scalability of the Ethereum network, yet, it will not be the definitive solution to the network congestion doomed to increment continuously.

Buterin's intended roadmap has not ended here, in reality, it is quite the opposite, it is only the beginning of what the true purpose of Ethereum will turn out to be. Nevertheless, Buterin's priority is to scale the clogged network as the need for speed improvement for better services for its users and increment disk space as running a node is becoming more difficult with the ever-growing network. We will next have a closer look into Ethereum's scalability problem, how Ethereum will be able to face these problems, and finally, shed some light on Ethereum's vision.

CHAPTER 2

Ethereum's Scalability

2.1 Scalability Problem

As previously mentioned, Ethereum is in needs to be more scalable for processing larger numbers of transactions per second without incrementing the size of nodes in the network. Ethereum is a mass, multi-functional decentralized platform hosting numerous decentralized applications of all kinds and would concernedly result in a waste of resources if they are not having the fully efficient capacity to operate. Today, Ethereum can process around 500 000 transactions per day, hence, around 6 transactions per second, a figure that centralized counterparts can easily overcome with their transactional process limit. The main reason for the scalability problem to surge relates to decentralization as its advantage lies in the distribution decision-making process to all the network participants. Unfortunately, decentralization reduces the processing speed of transactions as each node on the network has to validate transactions and transmit their validations as well as blocks of transactions to other participants to keep the network updated. To effectively scale the Ethereum blockchain, many factors in the network have to be addressed. Firstly, the number of transactions in a block and its generation time defines the blockchain's transaction per second rate, thus, the block size is a crucial element in improving the speed of transactions. However, the incrementing block size will affect the blockchain's decentralization as nodes will find it complex to validate larger volumes of data. Secondly, nodes need more disk space since they download each newly formed block and space to hold this kind of data. Furthermore, disk spaces endure higher costs but give access to superior memory capacity and so having larger block sizes. Thirdly, due to network congestion, fees are out of control, and they are bound to increase as nodes can only do so much with the tools and capacity they are given. With the high demand for transactions, users are obliged to pay more fees to skip the queue due to the lack of space in a block. And lastly, the response time given from nodes validating transactions to the transactions settling on the blockchain is in direct correlation to the network's congestion. Both the response time and transaction fees have extremely negative impacts on the user's experience as well as nodes submerged by transactions and developers not satisfying the purpose of their decentralized applications.

2.2 Scalability Factors

2.2.1 Consensus Model

The Scalability issues are inherent to the previous consensus model, Proof of Work. The model consisted in having all the transactions broadcasted to the network for every single block resulting in secured nodes possessing all the data of the blockchain. Contrariwise, it delves into an opposing environment for direct scaling of transactions if not with the increase of block size. As the network receives a higher user influx, miners are flooded by a vast amount of transactions to process and validate to other nodes. This only gives miners the deciding authority to choose which transactions to process and which to leave queued. However, the long-awaited transition to the Proof of Stake consensus mechanism relies in the majority on eliminating malicious actors from reaching consensus. With this system, miners shift to the role of validators nodes that are required to put to stake an amount of their ETH[5] in a smart contract (only nodes who have at least 32 ETH can become validators) and the amount staked will establish the power of a vote a party has on the blockchain. Validators have then the objective to propose block versions to guarantee consensus among all parties on the network. Foremost, the Proof of Stake model is more energy efficient than Proof of Work as it does not require miners to mine Ethereum coins to incentivize miners for validating commitments or to use expensive electrical power for validating them. In addition, transaction throughput could be incremented as validators do not need a copy of the entire chain, but rather only the copy of the state transactions on the blockchain, thus, increasing memory capacity.

2.2.2 Gas Fees

When referring back to miners in the Proof of Work model, there are opposing sentiments toward their work. Miners in the previous consensus model and the highly congested network were the ones prioritizing some transactions over others, yet, without them, there would not be a decentralized network. But this censorship resistance from miners has been an additional factor that impacted the rise of gas fees. Gas fees are an additional mandatory fee with a value from which the user is willing to give without exceeding the limit imposed, and it qualifies for the processing of a transaction given to the miner that uses its resources for validating it. Usually, the more complex the transaction is, the more gas fee is required to spend, if the amount of gas fee exceeds the actual requirements the miner reverts the rest into the user account, however, if the transaction's gas fee is not enough, the system does not process the

[5] Native currency of the Ethereum platform.

transaction and takes the gas fee. The drawback of a clogged network is that miners tend to process first the transactions with higher gas fees while leaving queued the lesser complex transactions backed up in the memory pool to be dealt with later, possibly *much* later. As the network's user popularity keeps on incrementing, the situation only worsens as observed in the case of the "CryptoKitties"[6] Decentralized application, going from 622 000 transaction requests to slightly over one million after only one day. These situations cause gas prices to skyrocket in order to control the number of transactions able to access a block, hence, causing a delay in transaction processing.

2.2.3 DApps and Smart Contracts

Smart contracts are on-chain elements of a decentralized application (Dapp) executing transactions with met conditions and connecting them back to the blockchain. Unlike Bitcoin, Ethereum was purposely created for running and executing smart contracts where they allow to transfer of values between parties or held in escrow inside the smart contract. Ethereum provides a virtual machine where developers can build applications incorporating plenty of smart contracts, without which are unable to function and connect back to the main network. Developers are free to program their smart contract, define the instructions of their code and submit it to the EVM for execution. On top of the resources spent to validate transactions on the main chain, executing smart contract transactions takes an additional computational power to validate across the network which also requires an amount of gas fee to be paid. Smart contracts' gas fees are correlated to the complexity of the smart contract itself and the computation required to process the transaction, theoretically incentivizing developers to program simple and efficient smart contracts. Developers are also allowed to build decentralized applications taking benefits of the smart contract technology, hence, Ethereum is home to plenty and unimaginable types of applications. However, Ethereum's scalability issues are only aggravated by the fact that there are and will continue to be many applications on top of the blockchain due to smart contracts and transactions too being processed across all nodes in the network. As the demand for Dapps continues to increase, transaction times and fees will continue to augment due to the restricted space in a block and expensive computational power for miners to validate transactions. In addition, smart contracts are serialized, meaning that miners are not able to move on to another smart contract until they complete the current one, and, smart contracts are immutable, thus, if any errors are present in the code it is almost impossible to update the pre-defined conditions. As the codes are created by anyone qualified enough to be a developer, errors and flaws are to be considered and if changes can be

[6] Blockchain game developed by Canadian studio Dapper Labs, it allows to buy, sell, and create NFTs through Ethereum.

implemented, they have to be added as a new transaction which not only conflicts with the existing one but requires further costs and computations to validate.

2.3 Scaling Solutions

2.3.1 On-Chain vs. Off-Chain Scaling

There are three possible approaches that Ethereum can advance on for improving the network's scalability; internal scaling, node splitting, and external scaling. Internal scaling consists in improving the internal structure of the nodes and the consensus protocol for it to optimize resources as much as possible. Whereas, node splitting considers splitting full nodes into sub-nodes generating each sub-node a specific role to accomplish governed by specific parties, subsequently lowering the cost of fees for users as the workload of nodes is reduced. Yet, both of these solutions entail bringing the blockchain towards a more centralized ledger, which is against Buterin's and his team's vision. Consequently, they reside for the third solution being external scaling, an Off-chain scaling method. This method entails adding layer-2 chains on top of the main network chain referred to as layer-1, which will then be considered to be modular scaling. Off-chain scaling can also be seen from the latest Bitcoin's Lightning Network, involved in processing light-speed transactional payments on Bitcoin's layer-2 chain.

With the Merge successfully put in place, Ethereum's scaling approaches will be a part of the new Ethereum's future upgrades. Ethereum's transition to Proof of Stake was initially intended to be accompanied by the upgrade of Sharding, which increased transaction throughput and decreased fees. Yet, Sharding was then postponed after the Merge and to sometime around 2023, nevertheless, interest was shifted towards layer-2 systems. Concerning layer-2 scaling systems, two distinct paths can be considered, On-chain scaling and Off-chain scaling. On-chain scaling refers back to approaches mentioned above like internal scaling and node splitting which also covers the possibility of reverting to a centralized system. On the other side, Off-chain scaling consists of this second layer on top of the main one that could manage transactions without using the main network. The principal concept of Off-chain models is viewing the main blockchain as a trust and arbitration layer. The Ethereum community and Buterin himself largely prefer walking down the road of the layer-2 approach to preserve the decentralization of the network, since it incorporates the ideology behind Ethereum. Off-chain scaling is now mostly called layer-2 scaling because it entails moving transactions up from the base layer-1, and it could on paper be extended to a third and fourth layer in future upgrades. Layer-2 scaling requires more complex software and hardware to be built and is a process that takes time. Even though On-chain scaling is not an optimal solution

for Ethereum, Sharding is a much anticipated on-chain scaling key that helps internally optimize the main blockchain, however, the only drawback is the technical complication in changing the core protocol. Transferring a fundamental role from the main blockchain layer to the second layer offers the most rapid track to scalable applications. As an example, by March 2021 approximately 365 000 (ERC-20)[7] smart contracts operating on the network and around 60% of the contracts have never been dealt with since the system is only limited to processing one transaction per hour for each project.

2.3.2 Sidechains and State Channels

Examining the second-layer scaling solutions, Sidechains were one of the first proposals for obtaining a scaling blockchain while keeping intact privacy and decentralization of the base layer protocol. Sidechains are created and maintained once developed as they enable users to lock coins on the main chain in exchange for coins in this parallel chain that obeys its own rules, consensus, and flexibility concerning governed protocols. With Sidechains, there is no need to create separate chains for every new participant like State Channels and they also allow interaction with other cryptocurrencies. Unlike State Channels, Sidechains require enough miners to secure the network and keep it running, additionally, a Federation layer[8] is needed instead of a smart contract which can result in a security weakness. State Channels are an analogous concept to sidechains, they re-instate the idea of trustless consensus between two parties, instead of global consensus they make use of local consensus, strengthening privacy properties by only publicly broadcasting opening and closing transactions. A payment channel must be created with a node connecting to the main network while locking tokens on the base chain ensuring security and honest conduct as they are kept for collateral. On the other hand, State Channels necessitate 100% availability of all the participants and if anyone goes unavailable, it can risk security and/or higher validation costs. The number of participants is limited to the Judge contract that is in possession of the participants' addresses and participant changes are enabled only by contract updates, unlike Sidechains which do not contain a limit on the movement of participants. The central downside of sidechain approaches, they contain some degree of decentralization, as the gateway that enables transfers of coins is generally controlled by a party that can be exposed to malicious attacks.

[7] Standard token used for creating and issuing smart contracts on the Ethereum Blockchain.

[8] Pre-selected, equally privileged participants. Single party or group that determines the rules.

2.3.3 Plasma

Moreover, Plasma is similar to a sidechain that leverages smart contracts and Merkle trees anchored to the main Ethereum chain, which uses fraud proofs to arbitrate disputes. Plasma's framework operates as a blockchain tree arranged in a way where smaller chains (Plasma Chains) can be created on top of the main ones. Each Plasma chain entails a smart contract serving different purposes independently operating and coexisting with other chains. Therefore, child chains are specifically designed in a way that can ease the workload of the main chain. Unlike sidechains, Plasma chains benefit from Ethereum's main network's security. Each child chain has its own implemented fraud-proof validation blocks and can be operating on top of different consensus models. Plasma also benefits from MapReduce, which allows simplified data verification within the tree of chains, making the network more efficient. One concern involved with Plasma is where users mass exits the network, creating congestion and triggering malicious activities in child chains.

2.3.4 Lightning Network

Furthermore, Lightning Network is a very well-known payment network built for Bitcoin-like blockchains. Lightning Network evolves the concept of payment channels by providing bi-directional transfers with instantaneous speed, zero risk of counterparty dishonest behavior, and low fees. It uses channels amongst participants allowing multiple transactions to happen without waiting for the main network to confirm these exchanges. Once the channel is opened, parties can exchange funds as much as they prefer until they decide to close it after which the transactions are sent to the main network for validation. This layer-2 solution entails a 2-of-2 multi-sig, meaning that both sides are required to sign each other's transactions to complete the execution of the transaction, protecting both parties' funds. Lightning Network exchanges can take from milliseconds to seconds and millions of transactions per second can be obtained. However, concerns delve around malicious attacks causing network congestion and so making the network freeze and steal funds, closed channel frauds where one user in the channel after the exchange goes offline (closes the channel) and the other user does not. This fraudulent act enables the user that did not close the channel to manipulate the state of the exchange and get away with a free exchange. In this case, a third party is needed to oversee the Lightning Network channel exchange to prevent fraudulent acts.

2.3.5 Rollups

Finally, Rollups are second-layer scaling systems that execute transactions outside the base layer. Rollups implicate rolling up Off-chain batches of transactions, compressing them

into a final rolled-up transaction before submitting them to the main blockchain as one single transaction. The cost of the batched and compressed transactions together with the Ethereum transaction is spread amongst users. Rollups process transaction at a higher speed than the Ethereum main chain and facilitates them by publishing single transaction rather than many. Next, we will examine in detail how Rollups function as Vitalik Buterin trusts that they ought to play a fundamental role in Ethereum 2.0.

CHAPTER 3

Ethereum's Layer-2 Rollups Technical Solutions and Impacts

3.1 Layer-2 Technicalities

As the need for scaling solutions is becoming vitally stronger, imminent, and at the moment options have piqued interest in tackling Ethereum's most defiant enemy, exponential growth. To fully immerse ourselves into studying the characteristics and impacts of the Rollups scaling solutions, we initially need to comprehend how layer-2's technicalities work. Layer-2 is a designed solution assuming the role of helping to scale applications by managing the congestion of transactions taking place on Ethereum's main network[9], which is based on layer-1, all while replicating its unfaultable decentralized security model. For the purpose to ease the highly active network, increasing user experience, and reduce gas prices, layer-2 implements a cluster of servers represented by either validators, operators, or nodes. Various layer-2 implementations differ from each other, however, for the majority, the transactions are grouped by prior in anchoring to layer-1, which is in turn secured and with the unfeasibility to be modified. Such a technique has proved to be efficient in reducing part of the main network's workload as well as applications specific to layer-2 networks, yet it seems to not achieve effectively the purpose of its goal and consequently, the scaling problem keeps on persisting.

[9] https://ethereum.org/en/developers/docs/scaling/

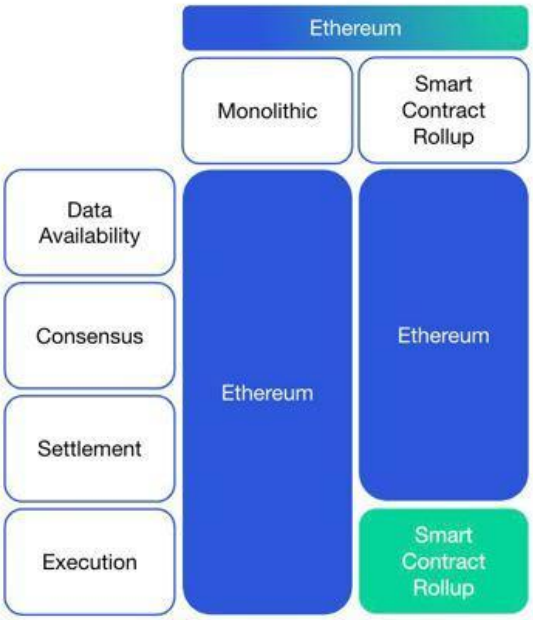

Figure 3- Modular Blockchain Rollups. Source: "The Complete Guide to Rollups", DelphiDigital Medium (2022)

Second-layer solutions do not alter Ethereum's Blockchain core instead they take advantage of the use of the platform's transactional protocol, the smart contract, which allows operations to be made outside the main Blockchain network. This is where Rollups are based, each Rollup has precise contracts adopted on Ethereum's main network. Rollups possess the technicalities to "rolling up" transactions into a batch and compress such data. By doing so the space quantity in a block needed is substantially lower than validating these transactions individually on the main network providing a superior rate, diminished transactional costs, and an upper quality of output. Rollups play a major role in being the forthcoming solution to the scalability problem, nevertheless, is there certainty on the validity of each data transaction forwarded by rollups onto the base layer? Developer teams have engineered what are, at the moment, the two main types of rollups consisting of different security models: Optimistic Rollups and ZK (zero knowledge) Rollups.

3.2 Optimistic Rollups

3.2.1 Optimistic Rollups Description

Optimistic Rollups have similar functions as layer-2, its ideology is to assume transactions are valid and uniquely implement control computation through fraud proofs exclusively when a challenge has been requested. An Optimistic Rollups is composed of two fundamental parts, On-chain contracts, and an Off-chain virtual machine. On-Chain contracts are the Rollup's operations managed by smart contracts running on Ethereum, which is utilized

as layer-1 for Optimistic Rollups. The off-chain virtual machine is independent of the Ethereum Virtual Machine (EVM) and is where the rollup protocol executes computation and state storage, which is instead utilized as layer-2 for Optimistic Rollups. Subsequently, Off-chain virtual machines integrate largely the EVM's design facets, therefore, Optimistic Rollups limits itself to running EVM-compatible programs. In addition, they rely on Ethereum's security for supervising the rollup's off-chain computation and data availability providing Optimistic Rollups security benefits concerning pure Off-chain protocols that do not base on Ethereum's security. Optimistic Rollups publish data back to Ethereum as *calldata*,[10] used for the compression of data transactions, becoming information available to anyone to execute and verify the rollup's state transition. Without such availability, challengers are not able to fraud-proof the incorrect operations, instead, with Ethereum providing this data availability the probability of malicious acts is quite diminished.

3.2.2 Optimistic Rollups Fraud Proofs

As previously mentioned, anyone is allowed to submit blocks without the need to effectively prove the validity of the transactions, but to maintain the chain's safety when a state transition is being disputed or challenged, a specific time window is applied usually lasting no more than a week. When an invalid assertion is in place Optimistic rollup employs crypto-economic incentives to guarantee the existence of honest nodes meaning that both the challenger and the operator have their ETH staked. Once the rollup protocol re-executes the asserted transaction back on the base layer, a verified contract is requested to determine the validity of the false transaction. Whether the challenger or the operator has won the dispute, the other party will be faced with the loss of their staked ETH. Despite the fraud-proof system being a reasonable incentive based on the proof-of-stake consensus model, its efficacy is reduced when the proving scheme is a single-round interaction. Single-round fraud-proof interaction entails publishing state commitments for each transaction separately resulting in important gas costs, hence the significance of a switch to multi-interaction fraud proofs systems. Multi-round interactive proving is where essentially both the challenger and the asserter have a back-and-forth communication supervised by a layer-1 verifier. Once the challenge has been activated the asserter will then equally divide the assertion's computation into two halves, called a *bisection protocol*, where the challenger will indicate from which of the two halves it wants to dispute. From there the two parties will eventually come to a single step of execution where they firmly disagree. The layer-1 verifier contract that has been overseeing the dispute will take control of verifying this single step of execution, resolving the dispute, and penalizing the party

[10] Non-modifiable, non-persistent area where function arguments are stored.

at fault. This type of fraud-proof has the advantage to optimize the work of layer-1 in dispute arbitration, consequently, it reduces as well the quantity of data published on the Ethereum main network and minimizes gas costs for the layer-1 chain when re-executing the disputed step.

3.2.3 Optimistic Rollups Interoperability

Optimistic Rollups exist due to its program design enabling communication with Ethereum's main network. This feature facilitates users and fraud proofs to interact with layer-1 and layer-2 as well as *dapps*[11] previously existing in layer-1 since Optimistic Rollups are EVM compatible. Many benefits can surge from being EVM compatible, one of the most important is transferring existing smart contracts on Ethereum to Optimistic rollups together with the rich infrastructure that Ethereum possesses such as testing tools, code libraries, and programming languages. These benefits are not superficial, instead, they provide developers with the same tools and environment they have been used to initially, therefore, saving developers team time that can be allocated for improving scalability.

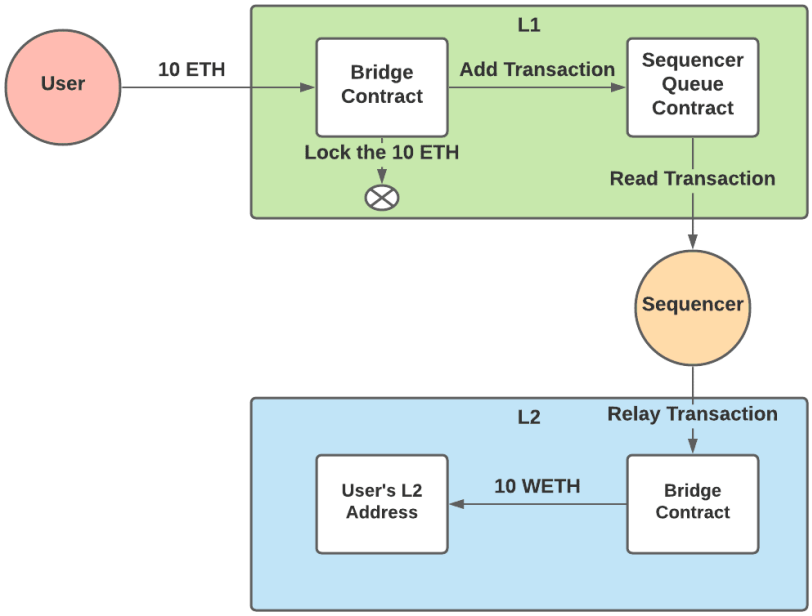

Figure 4 - L2 to L1 Transaction Workflow. Source: "Introduction to Optimism's Optimistic Rollup", Medium (2021)

Rollup users adopt the layer-1 blockchain and layer-2 chain interaction by depositing funds into one of the chain's smart contracts, called the *bridge contract*, which will later result in an unlocked amount on the user's rollup address. Often layer-1 to layer-2 deposits are queued until the sequencer, a third party responsible for validating the deposit, re-submits the

[11] Decentralized applications that operate autonomously with the use of smart contracts providing utility to its users.

transactions to the rollup. The sequencer employs a quite important function while submitting a batch of compressed transactions to the rollup contract since it necessitates the demonstration of a pre-state root and a post-state root. This mechanism allows the contract to verify if the two states match and if they indeed match, the contract proceeds to drop the old state root and store the new one. On the other hand, exiting the rollup or withdrawing funds from an optimistic rollup to the base layer inquires the user to attend the challenge period, which roughly lasts seven days. The user is obligated to provide *Merkle* proof [12]to prove the user's transaction residing in the rollup's state root. However, constructing a *Merkle* proof compels us to fully entrust the sequencer as it is the only one that can provide the initial transaction data that is compulsory for the submission to the rollup contract. Assuming that the sequencer is offline or more maliciously denies access to the data proving the ownership of the funds, the optimistic rollups decentralization and security are put at risk. To deflect this possible and probable malicious attempt, Optimistic rollups impose sequencers to publish the full transaction data onto the main execution layer. By doing so, another sequencer can resume the work left by the offline sequencer by reconstructing the rollup's state from the transaction data and the user can then download the data to create its *Merkle* proof. Nevertheless, if users are against waiting a week and feel more secure to proceed on a path of trustless finality, they can employ a liquidity provider [13](LP). The liquidity provider takes ownership of the funds to be withdrawn and directly compensates the user on the Ethereum main network in exchange for a fee. The LP can allow this to happen as they can check the validity of the user's exiting state request by executing the chain itself and can be assured that the transaction will ultimately be complete.

3.2.4 Optimistic Rollups Scalability

As previously mentioned, Optimistic Rollups augments data availability in blocks by creating a batch of compressed transactions. This process helps to scale the congestion on Ethereum by outsourcing the execution layer to Rollups. The main layer of Ethereum imposes a gas limit per transaction and subsequently the number of gas units a block can handle. Optimistic Rollups improve the transaction per second rates (TPS) by achieving the compression of transaction data.

[12] Confirms specific transactions represented by a leaf or branch hash within a Merkle hash root.

[13] Service that allows user to withdraw funds immediately without waiting the 7-days period time.

Parameter	Ethereum	Rollup
Nonce	~3	0
Gasprice	~8	0-0.5
Gas	3	0-0.5
To	21	4
Value	~9	~3
Signature	~68 (2 + 33 + 33)	~0.5
From	0 (recovered from sig)	4
Total	~112	~12

Figure 5: Ethereum vs. Rollup transaction. Source: "An incomplete guide to Rollups", Medium

We can observe from the table above that a single and simple Ethereum transaction takes about 112 bytes, whereas an ETH rollup transfer takes as little as 12 bytes. To understand how can an optimistic rollup extensively gain scalability compared to Ethereum we will look at some calculations with values taken from the figure above. If a block on Ethereum consists of 15 million gas and verifying one byte of data costs 16 gas, then 15 million divided by 16 will result in 937,500 bytes of data an average block can hold. Yet, a rollup transaction can cost 12 bytes, therefore, 937,500 divided by 12 will mean that a rollup can process 78,125 rollup transactions. Dividing that number by 15 seconds, which is when a new block on Ethereum is produced, means that the rollup's TPS equals around 5,208 transactions. This estimate demonstrates how much scalable a rollup can be compared to the 2,000 TPS of Ethereum on the main network.

3.3 Zero-Knowledge Rollups

3.3.1 ZK Rollups Description

A ZK-rollup operates on Ethereum's layer-2 like Optimistic Rollups, but unlike this last one, ZK-rollup does not implement any sort of dispute resolution mechanisms. It utilizes cryptography Zero-Knowledge proof evaluated by a contract and updated only through validity proof. ZK-rollup is composed of two essential elements, On-chain contracts, and an Off-chain virtual machine. On-chain contracts are ZK-rollup protocols supervised by Ethereum's smart contracts including the contract that is occupied with storing rollup blocks, tracking deposits, and observing state updates. A verifier contract is also an on-chain contract that evaluates zero-knowledge proofs published by block producers. The off-chain virtual machine is where transaction execution and state storage are based, which is a virtual machine independent from the EVM one. This off-chain virtual machine is where transactions of ZK-rollup are executed

which serves as a layer-2 for the ZK-rollup protocol. Verifiers on the Ethereum base layer secure the validity of state transitions in the off-chain virtual machine. Furthermore, ZK-rollups can be considered a hybrid scaling solution in off-chain protocols since it operates outside the Ethereum main network yet simultaneously derives its security from Ethereum, which in turn implements the validity of ZK-rollup's state updates and secures the availability of data behind each of them. ZK-rollups are safer than *sidechains*[14] in terms of security properties and safer than *validiums*[15] in terms of validity proofs as they make use of the same process, however, *validiums* store transaction data in a completely different place. Compared to Optimistic Rollups, ZK-rollups submit state data for each transaction performed off-chain, called *calldata*, back to Ethereum. The *calldata* is available to anyone for it to be reproduced in the rollup's state and subsequently validated. Even though ZK-rollups do not submit transaction data on-chain due to the validity proofs process (that already authenticates the state), it is still crucial to store on-chain data as it consents verifications of the layer-2 chain's state averting malicious users from wrongly operating the chain.

3.3.2 ZK Rollups Validity Proofs

Much like Optimistic Rollups, Ethereum converts into a settlement layer where ZK rollups' transactions are processed if and only if the Ethereum contract admits the validity proof. When a ZK rollup operator publishes an updated rollup's state to the layer-1 contract, it must prove the new Merkle root contains correct and verified updates of the rollup's state. The operator can do so by a validity proof, which is fundamental for the layer-1 contract to accept the proposed state commitment. This proof mechanism derives from a succinct cryptographic commitment having the function of accurately controlling the validity of batched transactions. It is also named zero-knowledge proof for the reason that it allows one to prove the validity of a statement without revealing its content. ZK-rollups utilize validity proofs in order not to re-execute statements on the main network when confirming their correctness in an off-chain state. Hence, proofs can come in two forms, ZK-SNARK and ZK-STARK, each supporting in confirming the reliability of off-chain computations with distinctive features.

Zero-Knowledge Succinct Non-Interactive Argument (ZK-SNARK) necessitates a Common Reference String[16] (CRS) that provides public parameters in asserting validity proofs, which is where the security of the system relies on. If under any circumstance a malicious user

[14] Separate blockchain that runs independent from Ethereum and is connected to the Main net by a two-way bridge.

[15] Scaling solutions use off-chain data availability and computations to improve the processing transaction speed off Ethereum.

[16] Captures the assumption that a trusted setup which all parties involved get access to the same string taken from a distribution exists.

can gain possession of public parameters, they will certainly succeed in generating false validity proofs. ZK-rollups have implemented a technique to counter-interact this potential attack by using a multi-party computation ceremony [17](MPC), where trusted users generate public parameters while contributing randomness for building the CRS which is subsequently destroyed. Trusted setups are put in place for improved security since at least one honest participant that destroys their input is sufficient to safeguard the ZK-SNARK system. Although this procedure still entails trusting involved participants, ZK-SNARKs brings an incredible opportunity for Ethereum to verify rapidly and cheaply proofs through layer-2. Zero-Knowledge Scalable Transparent Argument of Knowledge (ZK-STARK) explores the equivalent concept of ZK-SNARK, however, they improve in scalability and transparency features. They result in being transparent as, unlike ZK-SNARK, they do not rely on CRS, thus they do not rely on a trusted individual's setup. Additionally, they are more scalable as the time required to prove and process validity proofs increase *quasilinearly* relative to the computation's complexity leading to a higher speed of proving computations than ZK-SNARK, which has a linear time scale. The upside of ZK-STARK is that is not susceptible to quantum computers[18] unlike ZK-SNARK and the downside is that it could be more expensive to evaluate its proofs on Ethereum as they usually handle larger sizes.

The validity proofs work involves the operator employing specific step-by-step operations. When evaluating transactions, the operator is in charge to overview that the parties of the transactions are indeed part of the state tree and that the sender parties have adequate funds to cover the cost of the transactions requested. In addition, the operator must also confirm the correct senders' public keys on the rollup as well as their nonces[19]. Once the ZK-rollup node contains a sufficient amount of transactions, it can then compress them into a batch ready to be submitted for the succinct ZK-proof section. Both of the succinct ZK-proofs include a Merkle tree with all the batched transactions, Merkle proofs for transactions in the batch, Merkle proofs for each sender-receiver pair that are effectively part of the rollup's state tree, and finally a set of intermediate state roots for each transaction state updates. From now on the proving circuit will prove and validate the transactions by looping over each commitment and verifying all the checks previously computed by the operator. The proving circuit will then assert the existence of the sender's account in the state root through the Merkle proof, decrease its account balance, increase its nonce, hash the new account data, and produce a new Merkle root. The only changes

[17] Protocols which allow multiple independent parties to collaboratively construct the parameters.

[18] Technology that harnesses the laws of quantum mechanics to solve problems too complex for classical computers.

[19] Number of transactions sent from a given address.

in the ZK-rollup's state are the sender's balance and nonce, which will be reflected by the Merkle root. The proving circuit will subsequently perform the identical procedure on the receiver's account. Finally, after the ZK-proving circuit loops over the entire batch of transactions, it will result in a final state root. The last Merkle root generated will convert into the new state root of the ZK-rollup. The layer-2 operator is now ready to submit the final validity proof to the verifier contract on layer-1, which evaluates the proof's correctness and checks its public inputs. The contracts' verification circuit verifies the pre-state root (ZK-rollup's old state root), the post-state root (ZK-rollup's new state root), the batch root (Merkle root of the batch), and the transaction inputs. If the proof is valid, it will entail that the pre-state root and the post-state root are correctly connected by a sequence of valid transactions. Therefore, the rollup contract considers the post-state root and updates the state tree to match the rollup's updated state.

3.3.3 ZK Rollups Interoperability

Users can enter the ZK rollup with allocated tokens to the rollup's contract from the layer-1 chain. Solely operators are in charge to submit transactions to the rollup contract, which ultimately can lead to queued transactions. After the user's funds are present in the rollup, users can now submit operations to the operator for process completion. If the users intend to withdraw funds from ZK rollup to the main network, it first needs to make an exit transaction by moving their assets to a specified burn account. If this transaction will be included in the batch, then the user can request a withdrawal to the on-chain contract, which contains a Merkle proof of the transaction to the burn account in the batch, the transaction data, the batch root and the on-chain address of the users. Eventually, the rollup contract verifies the validity of the withdrawal request and completes the exit transaction to the user's account.

Unlike Optimistic Rollups, ZK rollups are not EVM compatible. Yet, developers are shifting their attention to generating a zero-knowledge EVM (zkEVM) that simulates existing EVM operation codes for in-circuit proofs also allowing the execution of smart contracts. In contrast to EVM, zkEVM generates zero-knowledge proofs to attain the correctness of each step in the program's execution, meaning that validity proofs can verify both the operations in the Virtual Machine's state and the computations. If zkEVMs are implemented, they can procure the opportunity to leverage scalability and security through the adoption of zero-knowledge virtual machine proofs.

3.3.4 ZK Rollups Scalability

As transaction fees are dependent on gas fees, ZK rollup fees are cost-efficient compared to the Ethereum main network since they handle data differently. State write costs are reduced in layer-2 as ZK rollups batch transactions and so allows to secure fixed costs through users. Other costs are also influenced by data publication, the layer-2 operator fee, and the cost for the ZK rollup operator to produce validity proofs. Predominantly, compressing transaction data is where ZK rollups can efficiently scale Ethereum and reduce costs. ZK rollups can compress data transactions more effectively than Optimistic Rollups as they only need to submit sufficient data to reconstruct the latest root state on the rollup. Furthermore, ZK rollups contain a feature, recursive proofs[20], that can efficiently optimize the work output of the chain. Recursive proofs are proofs that verify other proofs, presently, ZK rollups verify and generate validity proofs for single blocks which highly limits the potential ZK rollups can achieve. With the use of recursive proofs, ZK rollups have the possibility to conclude multiple blocks at once with one validity proof as the proving circuit recursively combines many block proofs to create one final proof. If this final recursive proof, which is submitted from layer-2, is accepted by the contract, all the related blocks are instantly completed. Implementing this ZK rollup advantage will result in a higher and more efficient transaction speed process on Ethereum.

3.4 Optimistic Rollups vs. ZK-Rollups

3.4.1 Pros and Cons of Optimistic Rollups

The benefits of Optimistic Rollups are essential to improve scalability without compromising Ethereum's security. In order to maintain the same level of security, Optimistic rollups rely on crypto-economic incentives allowing honest participants to guarantee the chain when fraud-proving transactions, which can be verified by layer-2 nodes. Optimistic Rollups' compatibility with EVM and Solidity holds the gain of transferring existing Ethereum smart contracts onto the rollups as well as environments for the creation of new *dapps*. On the other hand, Optimistic Rollups delay the completion of transactions as the need to verify potential fraud challenges requires a time window which is also implemented when a user request funds withdrawal. As the proving scheme does not prove each transaction like ZK-rollups, a potential malicious operator has the power to submit invalid blocks and state commitments if there are no honest nodes. At least one honest node is required to stop this malicious attack threatening the security and decentralization of Ethereum but if this last one is compromised there is no

[20] https://ethereum.org/en/developers/docs/scaling/zk-rollups/#recursive-proofs

reverting. Time is a lacking factor of Optimistic Rollups, yet, also the cost is not optimized as rollups post all transaction data on-chain, unlike ZK-rollups.

3.4.2 Pros and Cons of ZK-Rollups

ZK-rollups gain and ensure security through the adaption of validity proofs, which indeed are costly and increase fees for rollup users, but in contrast, prevent malicious operators to submit invalid transactions. ZK- rollups deploy faster transaction finality through approved state updates and unlike Optimistic rollups, they rely on cryptographic mechanisms instead of incentivized honest participants. In addition, users benefit from withdrawing funds from layer-2 without delays and do not have to validate the chain to protect their funds. Since ZK-rollups compress data more efficiently than Optimistic Rollups, the cost of publishing *calldata* on Ethereum is reduced as well as rollup fees for users. Then again, ZK-rollups necessitate specialized hardware to produce validity proofs that may lead to centralized control by some parties. Conversely, ZK-SNARK proving system involves a trusted setup and if all dishonest nodes are handing the CRS it could certainly destabilize the rollup's security system.

3.4.3 Final Thoughts

At this moment in time, the on-chain speed process is the most important factor for the Ethereum scalable solution, and the speed that ZK-rollups are able to accomplish overcompensates the speed that Optimistic Rollups can achieve. The Optimistic Rollups' waiting period and transaction's legitimacy can be reasonably questioned compared to the full-proof systems of ZK-rollups even though this last one utilizes a great amount of hash power to compute the correctness of the transactions. Nonetheless, Optimistic Rollups solutions can be implemented and may be more adequate for projects with less on-chain activity and EVM compatibility. However, zero-knowledge rollups with EVM compatibility can quite literally become a game changer and drastically improve layer-2 scaling solutions, yet the difficulty in building them is extremely challenging due to the zero-knowledge complexity which will demand time. Layer-2 rollups are the future solutions to Ethereum's scalability obstacle where both ZK-rollups and Optimistic Rollups are valid options.

CHAPTER 4

Ethereum's Future Prospective

4.1 Future Scenarios

4.1.1 Sharding and Rollups

In light of the Merge and urgent need for Ethereum to scale, there are various possible scenarios that the network can take on and we will analyze a few of them. The first scenario, the one that most theoretically imitates Vitalik Buterin's vision entails a fusion per se of an On-chain and Off-chain scaling solution. This collaboration consists in having Rollups, whether Optimistic Rollups or ZK Rollups, built on top of Sharding with the assumption that Sharding's technical complex can be overcome. If and when Sharding will ensure security and communication between shards, meaning that shards will not risk taking over other shards resulting in the corruption of shards and loss of data, then Sharding can mitigate the internal main chain congestion and facilitate the work for Rollups. As demand increases, the cost of gas fees will keep reducing in Rollups settings since they are split amongst users. Since the network's data is split across shards, the role of validators is minimized since they do not require to store the entire history of the blockchain but rather are only required to continue to confirm data integrity. Thus, making Rollups more efficient as they report their state more efficiently in the sharded network. Sharding and Rollups will then have shared security and shared data availability optimizing efficiency and speed while maintaining the blockchain decentralized. However, in the event of one of the aforementioned obstacles of data Sharding being that one shard is corrupted, hence, having the possibility to collide and corrupt other shards it could put at risk the whole system of Ethereum by hacking funds, data and blocking the network. That is what is stopping the Beacon Chain to be implemented because the risk of having only one rotten shard could lead to the downfall of Ethereum. Therefore, Vitalik Buterin and his team are more focused on Rollups solutions alone as they can function without having to first resort to Sharding and can still offer a 100 times increase in throughput.

4.1.2 Rollups and More

The second scenario is indeed directed towards Rollups only. Both ZK Rollups and Optimistic Rollups are promising scaling solutions for the improvement of scalability in the Ethereum context. It is difficult to assert which one is better than the other as they both have distinctive good and bad features, it eventually depends on the necessities Ethereum's

developers ought to be more suitable. Surely, there is one fact that we can be certain of and that Ethereum needs to be scaled very soon, ZK Rollups do have higher levels of scalability as they process larger numbers of transactions and compresses data more efficiently than Optimistic Rollups. More specifically, ZK-STARK seems to be the most compelling solution as they process transactions in a more secure way than ZK-SNARK. On the other hand, ZK-STARK does deal with a higher cost of processing transactions since they handle larger sizes, but, if one official update has to be made and knowing that an Ethereum upgrade can be lengthy and complex, ZK-STARK would be a more than valid option. Even though the technology is not completely up to speed with what this model requires, it would be a great foundation for when it does. From here on, there are further solutions that can be applied in the sense that possible layers 3 solutions are to be considered for additional improvements. An on-ward envision considers to be a Rollup that has a precise function of settling and recording transactions to the blockchain. The idea of having layers on top of layers that each has different functions yet coexist and are coherent with one another is only the definition of decentralization viewed from a bigger picture.

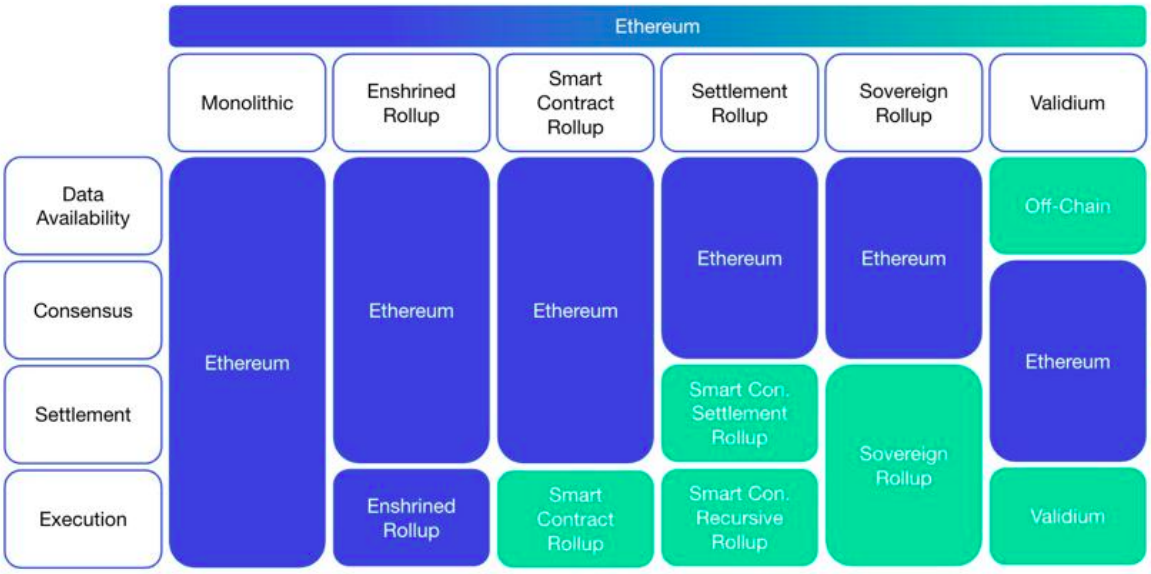

Figure 6 - Modular Blockchain Rollups. Source: "The Complete Guide to Rollups", DelphiDigital Medium (2022)

CONCLUSIONS

Ethereum has been facing the not-yet-solved scaling problem, which undoubtedly will continue to persist. Even if they succeed in scaling current transactions that are in place with the number of users involved, one day that number will just increment, and the demand for processing transactions will persist even more. So, the question is, will the technology implemented be enough? There is one important piece of knowledge we haven't quite touched base on, technology progress. We want security, want scalability and we want decentralization as there is no intention of involving a centralized authority that would resolve all problems except one, data control. Thus, implementing a solution that is beyond our current technological capabilities such as ZK-STARK is perfectly fine. Yes, approving transactions might be costly but it is better than what we deal with at this moment. In addition, data availability will become higher as well as processing speed will be more efficient. Though, Ethereum's main focus is to deal with the present time for the sake of its users and applications regardless of what tomorrow might look like. If so, the future of Ethereum will entail plenty of upgrades, both mitigating the faults of the previous upgrades and improving for the next. Yet, let us assume that one day shortly with advanced technology there is the plausibility to deal with the costs behind ZK-STARK computational power, also caused by zero-knowledge proofs, and more so the possibility to make ZK Rollups EVM compatible. This optimistic perspective could be a real breakthrough for an effective solution to the menacing scaling problem since it enables the fraud proofs processing of not too many transactions but many blocks. A possibility like this happening could potentially solve the famous Blockchain Trilemma introduced by Vitalik Buterin itself, where a blockchain can perfectly balance the three major aspects of a blockchain; decentralization, security, and scalability.

References

[1] Thomas Lavaur et al. “Enabling Blockchain Services for IoE with Zk-Rollups”, University of Toulouse, August 2022.

[2] Thomas Chen et al. “A Review of zk-SNARKs”, May 2022.

[3] Eli Ben-Sasson et al. “Scalable, Transparent, and Post-quantum Secure Computational Integrity”, March 2018.

[4] Aditya Asgaonkar. “Scaling Blockchains and the Case for Ethereum”, November 2022.

[5] Pleksandr Marushnenko et al. “The Overview of Decentralized Systems Scaling Methods”, Kharkiv National University of Radio Electronics, Ukraine, May 2021.

[6] Corwin Smith, “Scaling”, GitHub, https://ethereum.org/en/developers/docs/scaling/, January 2023.

[7] Tech Deep Dive “What is Arbitrum: Optimistic Rollups to solve Scaling without compromise”, Bybit Learn, https://learn.bybit.com/deep-dive/what-is-arbitrum-optimistic-rollups/, February 2022.

[8] Yoav Weiss “Cross-rollup-bridge”, GitHub, https://github.com/yoavw/cross-rollup-bridge, May 2021.

[9] Mesquita Oliveira “Zero-Knowledge Rollups”, Ethereum.org, https://ethereum.org/en/developers/docs/scaling/zk-rollups/#validity-proofs, January 2023.

[10] Christine Kim “zkEVMs: The Future of Ethereum Scalability”, galaxy.com, https://www.galaxy.com/research/whitepapers/zkevms-the-future-of-ethereum-scalability/, November 2022.

[11] Sahil Sen “Introduction to Ethereum Rollups”, QuickNode, https://www.quicknode.com/guides/infrastructure/introduction-to-ethereum-rollups, September 2022.

[12] Stepan Gershuni “Second Layer Blockchain Scaling: Off-chain solutions”, mastercrypto, https://masterthecrypto.com/second-layer-blockchain-scaling-off-chain-solutions/, 2022.

[13] Paul Wackerow “Introduction to Dapps”, Ethereum.org, https://ethereum.org/en/developers/docs/dapps/, September 2022.

[14] Ethereum “The Merge”, Ethereum.org, https://ethereum.org/en/upgrades/merge/, February 2023.

[15] Emily Shin “ZK-Rollups vs. Optimistic Rollups”, Data Wallet, https://www.datawallet.com/crypto/zk-rollups-vs-optimistic-rollups, January 2023.

[16] Guram Kasmadze “Modular Blockchain Architecture – Rollups, Sharding, ‘DankSharding’”, Medium, https://medium.com/web3chronicles/modular-blockchain-architecture-rollups-sharding-danksharding-db8e84e22e64, June 2022.

[17] Vitalik “An Incomplete Guide to Rollups”, Blog, https://vitalik.ca/general/2021/01/05/rollup.html, January 2021.

[18] Chris Buckland “Fraud Proofs and Virtual Machines”, Medium, https://medium.com/@cpbuckland88/fraud-proofs-and-virtual-machines-2826a3412099, October 2021.