# Research On Ethereum Blockchain

# Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Alterations | Author | Date |
| 0.1 | Document design | Fabian ifionu | 2-22-2022 |
|  |  |  |  |
|  |  |  |  |

## Abstract

Ever since the inception of Ethereum, scalability has been in the forefront of developer’s minds. From the very beginning, it was understood that 15 transactions per second would be insufficient to support a large ecosystem of thousands of applications with billions of dollars of values changing hands every day. As early as 2017, a mere two years after the lunch of Ethereum, Vitalik Buterin and Joseph Poon were already researching layer two scaling solutions in their paper [Plasma: Scalable Autonomous Smart Contracts](https://plasma.io/plasma.pdf). Since then, developers have been working on numerous other approaches to scale Ethereum. On this research, I aim at characterizing different layer two scalable solutions to answer my research question – How to clone Ethereum Defi protocol with the hope of reducing high transaction fees and increasing the 15 transactions per second which is a very big problem with Ethereum products. I conducted a library research strategy to identify available Ethereum Defi protocols, to find out if they have implemented the suggested layer two scalable solutions. Based on my findings which is explained below, the few who have implemented the layer two scalable solutions have better scalability.

## Acknowledgement

This work is done at Fontys Open Learning Eindhoven. I am very grateful to

**Lara Rojas John, Vorst Rens Van Der and Ruissen Martijn** My project coaches for giving me this opportunity to work on this project. My ver special gratitude goes to **Lemmen Dirk**, **Simons Jovi**, **Staykov Martin** and **Wilde Sem** highly talented team working on the Fintech Revolution project with me.

Contents

[Research On Ethereum Blockchain 1](#_Toc96499033)

[Document History 1](#_Toc96499034)

[Abstract 1](#_Toc96499035)

[Acknowledgement 2](#_Toc96499036)

[Introduction 3](#_Toc96499037)

[Layer Two Solution 3](#_Toc96499038)

[Sidechains 3](#_Toc96499039)

[Rollups 4](#_Toc96499040)

[Optimistic Rollups 5](#_Toc96499041)

[ZK Rollups 5](#_Toc96499042)

[Comparing Layer Two Solutions 5](#_Toc96499043)

[The Fork 7](#_Toc96499044)

[Conclusion 7](#_Toc96499045)

[References 9](#_Toc96499046)

## Introduction

### What is an Ethereum node or client?

Ethereum nodes are computers participating in Ethereum blockchain network. These nodes are actual computers running software that verifies, stores and sometimes creates blocks. The actual software is called “client”, and it allows us to interact with the blockchain using the JSON-RPC API, parse and verify the blockchain, and read or write to smart-contracts.

Ethereum is reaching far more developers than ever, with this growth adoption of Ethereum, there has been a flow of multiple Ethereum clients in the industry with the likes of Nethermind, Aleth, Geth and Trinity being the official library written and maintained by Ethereum foundation. Geth is the most popular Ethereum client today. It is aimed to be the fastest, lightest, and most secure Ethereum client. To clone Ethereum and have a private blockchain, one must clone Geth which I am going to explain later.

Looking into Ethereum Defi like uniswap, shushiswap, they are the most used Defi finance in Ethereum, but they are very slow with high transaction fees to be compared to the likes of polygon which implemented the layer two scalable solution.

## Layer Two Solution

I will go through the three types of layers two scaling solutions that have emerged as clear winner in the quest for scalability – sidechains, optimistic rollups, and ZK rollups.

### Key Takeaways

* Although they are not a true layer two solution, sidechains are the simplest scaling solution. A sidechain is a separate, more scalable blockchain that operates alongside the main chain. Although they achieve scalability, they do not benefit from the security of the main chain.
* Rollups are true layer two scaling solutions that operate on the back of the main blockchain. They achieve scalability by batching multiple transactions, while applying compression techniques to stop out non-essential data to save block space. Computations for transactions are also moved off-chain, leaving only essential data to be stored on the main chain
* There are two main types of rollups: optimistic rollups and zero-knowledge rollups (ZK rollups), which differ in how they deal with invalid and fraudulent transactions.
* All these solutions can achieve transactions per second in the range of 2,000 to 7,000+, more than 100x faster than Ethereum’s current 15 TPS.
* Sidechain and optimistic rollups have significant disadvantages, in contrast to ZK rollups that achieve scalability without sacrificing much.

## Sidechains

Examples: Polygon (MATIC), xDai (XDAI)

The simpliest layer two scaling solution are sidechains. As the name implies, a sidechain is a separate, more scalable blockchain that operates alongside the main chain, which in this case is the Ethereum network. The diagram below shows the general principle of the sidechains work.

A picture containing icon

Description automatically generated

Transactions occurring on the sidechain don’t take up any space on the main chain, and at the end of it all, users can use bridges to move their assets back unto the main chain.

Although sidechains built on proof-of-stake or other consensus algorithms can improve scalability, it comes with tradeoffs. Since sidechains are essentially a separate blockchain, they don’t really benefit from the security of main chain, which usually has a more diverse set of validators, and a proven consensus mechanism. Furthermore, bridges can be slow and inefficient, leading to long delay time when moving assets between the main chain and sidechain.

## Rollups

I have gone through some of the benefits and disadvantages of sidechains, which sacrifice security and usability for scalability. The goal of layer two scaling, however, is to maintain the security and capability of Ethereum which being fast and inexpensive. This is where rollups come in.

Rollups combine multiple transactions and fit them into a single block, allowing each block to effectively process more transactions. This reduces cost and latency greatly- Vikalik Buterin has stated that transaction speeds could increase by a factor of 100 with rollups.

### How does Rollups Work?

Rollups move on-chain storage and computation off-chain but keep just the essential data on-chain. This is achieved by combining multiple transactions, while using superior encoding and data compression to limit the amount of memory that a transaction takes up within each block. The following diagram is a simplified generalized demonstration of how rollup works.

Diagram

Description automatically generated

## Optimistic Rollups

Optimistic rollups use fraud proofs to prevent malicious actors from publishing fraudulent batches. The rollup keeps track of the entire history of state roots, which allows transactions to be reverted if anyone discovers an invalid transaction inside of any batch and publishes a fraud proof. If fraudulent batches are found, the operator responsible will have their staked assets slashed while the party finding the proof is reward with a portion of these confiscated assets. This mechanism is where optimistic rollups derive their name – it assumes that batches are valid unless proven otherwise. In this way, optimistic rollups can achieve significant scalability for the main chain 200 – 2,000 per second verses Ethereum’s 15.

There are significant drawbacks, however. Due to its reliance on fraud proofs, withdrawals from optimistic rollups must be subject to a significant delay in order to prevent assets from being withdrawn due to invalid or fraudulent transactions. As long as there is a delay, there will be time to revert transactions in the optimistic rollups.

## ZK Rollups

Zk Rollups, or zero-knowledge proof rollup, take a more conservative route in making sure transactions are valid. It does this by requiring cryptographic proof called ZK-SNARK to be submitted along with each batch. These proofs can be quickly verified by observers on-chain leading to greater and low withdrawer delays since it is virtually impossible for batched to contain invalid transactions.

## Comparing Layer Two Solutions

In this section, I summarize the layer two solutions, examining the benefits and drawbacks against one another.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Shape  Description automatically generated with medium confidence |  | Shape  Description automatically generated with medium confidence |
| Shape  Description automatically generated with medium confidence | Shape  Description automatically generated with medium confidence | Shape  Description automatically generated with medium confidence | Shape  Description automatically generated with medium confidence |
|  | Shape  Description automatically generated with medium confidence | Shape  Description automatically generated with medium confidence | Shape  Description automatically generated with medium confidence |
| Shape  Description automatically generated with medium confidence | Shape  Description automatically generated with medium confidence |  |  |
| Shape  Description automatically generated with medium confidence |  |  |  |

As you can see, all these solutions offer much higher throughput than the other Ethereum Defi like uniswap and sushiswap. Although sidechains and optimistic rollups have significant disadvantages that could potentially make them cumbersome to use, they are easy to roll out and operate.

ZK rollups seems to have limited disadvantages -however, the cryptographic proofs that ZK rollups rely on are technologically complex and are very new.

## The Fork

In order to answer my research question, I investigated two possible ways to fork Ethereum. Either We fork Geth and create a sidechain using this [tutorial](https://arctouch.com/blog/how-to-set-up-ethereum-blockchain/) or we fork a decentralized exchange like uniswap and deploy it on another blockchain like Solana which is the fastest blockchain with a very cheap transaction fees. To answer my research question I found a solution, yes, a good solution. The answer is Solang.

Solang is a solidity compiler, it can compile smart contracts written in Solidity for Solana blockchain. Yes, you heard me right, for Solana blockchain – this means we will be able to deploy to the fastest blockchain without compromising the security of the system. The process of installing Solang, compiling and deploying smart contracts on Solana blockchain can be found [here](https://soliditydeveloper.com/solana)

## Conclusion

Using the layer two scalable solutions will without a doubt improve the transaction per second but it also comes with some tradeoffs as stated above. Deploying on Solana comes with great benefit, it is known to have developed a highly scalable and user-oriented applications. This blockchain network is particularly the fastest blockchain right now and offers one of the most efficient ecosystem. It will be nice to look at the [comparison](https://101blockchains.com/solana-vs-polygon-vs-ethereum/) between Solana vs Polygon vs Ethereum

Chart, treemap chart

Description automatically generated

## References

Buterin, V. (2021). An Incomplete Guide to Rollups. Retrieved from https://vitalik.ca/general/2021/01/05/rollup.html

Ivan on Tech. (2021). Comparing Layer-2 Ethereum Scaling Solutions. Retrieved from https://academy.ivanontech.com/blog/comparing-layer-2-ethereum-scalingsolutions

Konstantopoulos, G. (2021). How does Optimism's Rollup really work? Retrieved from https://research.paradigm.xyz/optimism

Matter Labs. (n.d.). zkSync. Retrieved from https://zksync.io/

Optimism. (n.d.). Retrieved from https://optimism.io/ Polygon. (n.d.). Retrieved from https://polygon.technology/ xDai. (n.d.). Retrieved from https://www.xdaichain.com/