ABSTRACT

In this article, we are going to review how current solutions in the public and private blockchain ecosystem look like when it comes to scalability and real-world utility. We are going to discuss the possible and effective transition of blockchain becoming the value layer of the new Internet. In order to achieve the goal which Ethereum community and blockchain technology started with “Becoming a decentralized, scalable and programmable layer of the Internet”, we are going to discuss the problems which needs to be solved and propose some of the probable solutions which might help the community as a whole achieve its goal. of becoming the data and financial layer of the world.

The Beginnings

It all started with Bitcoin, a decentralized peer to peer transfer of value (tokens) over a distributed ledger technology (DLT). Although it was revolutionary at the time, it missed some of the functionalities which could be implemented to put the underlying DLT technology to better use as a wider scope for the world. In order to bring programmability to the DLT termed Blockchain technology, many new research and projects came by. Among all, Ethereum came out to be “THE” programmability layer of the new decentralized Internet that brought the best of blockchain technology in form of immutable “smart contracts”.

But with time and increasing adoption by the day, the community realized it lacked many of the important factors to be considered for adoption by the masses. Over the years, most of the problems have been solved with major upgrades in the Ethereum beacon chain. However, with regards to this thesis, we would be focusing on solving three major problems:

- Hyper-Scalability
- Privacy
- Utility and Composability

Introduction

With limited block size of Ethereum beacon chain, it limits the TPS i.e., number of transactions to be processed on the chain. This restricts Ethereum beacon chain from processing millions of transactions while maintaining its security. Therefore, Ethereum’s Rollup centric roadmap promotes creation of various types of rollups or supporting chains which execute and process their own transactions on their customized blockchains and only pass on proofs of execution and settlement on Layer 1 chain. This creates a separate layer for developers to build their applications with outsourced security of another blockchain and only use Ethereum for finality and data availability of the transactions processed on the rollup.

Join Pioneer Labs’ Discord Community

Follow us on Twitter

Types of Scaling Solutions

Side Chains:

A sidechain is a separate blockchain that runs independent of Ethereum and is connected to Ethereum Mainnet by a two-way bridge. Sidechains can have separate block parameters and consensus algorithms, which are often designed for efficient processing of transactions.

Validiums:

Validium is a scaling solution that enforces integrity of transactions using validity proofs like ZK-rollups, but doesn’t store transaction data on the Ethereum Mainnet.

Optimistic Rollups:

Optimistic rollups are layer 2 (L2) protocols designed to extend the throughput of Ethereum’s base layer. They reduce computation on the main Ethereum chain by processing transactions off-chain, offering significant improvements in processing speeds.

ZK Rollups:

Zero-knowledge rollups (ZK-rollups) are layer 2 scaling solutions that increase throughput on Ethereum Mainnet by moving computation and state-storage off-chain. ZK-rollups can process thousands of transactions in a batch and then only post some minimal summary data to Mainnet. This summary data defines the changes that should be made to the Ethereum state and some cryptographic proof that those changes are correct.

Problems with Current Frameworks

Scalability Trilemma

The scalability trilemma is a concept in blockchain technology that states that it is impossible for a blockchain system to achieve all three of the following properties simultaneously:

- Security
- Decentralization
- Scalability

In the case of Ethereum, this means that the current proof-of-work consensus the algorithm is secure and decentralized, but it cannot scale to meet the needs of a truly global financial system. This is because the more transactions the network processes, the more difficult it becomes to maintain decentralization, as the network requires more and more computational power to process all of the transactions in a timely manner.

[

Scalability Trilemma

771×627 105 KB

](https://ethresear.ch/uploads/default/original/2X/d/d92b30c0ae257bdeb4e5c003c373e99a75981cb9.png)

Scalability Trilemma

In order to solve the scalability trilemma, Ethereum focused towards the Rollup Centric Roadmap, however, the overall motive to achieve scalability has been unsuccessful during events of network clogging. For example, in the meme-coin season of $PEPE, gas fee on Ethereum L1 rose up to $100 and Optimistic L2s up to $8 making it infeasible to use by enterprises and protocols with wider use cases and network requirements

Therefore, in order to make the Ethereum network the utility chain for the Internet which includes business solutions, private enterprise solutions, public solutions, defi, etc. the network needs to achieve hyper-scalability while maintaining a certain level of trust and security of Ethereum Virtual Machine.

Fragmentation vs Adoption

With many new types and forms of rollups being developed, the blockchain community is getting more and more fragmented, developers must learn new tech stack, understand new concepts and build new architectures to make their applications compatible with each new type of chains. This not only hinders the goal for simplicity and improvement of User experience but also complicates the developer experience on the new chains.

[

937×529 94.2 KB

](https://ethresear.ch/uploads/default/original/2X/6/65c5c10864b4b0c8c9cb1a6e68805f2f06bc340b.png)

With each new rollup framework, the community keeps on getting fragmented with no single form of framework being adopted across the market. With the creation of each new rollup, the team must bootstrap the entire community and create real value for the developers and businesses to build on their blockchain. This creates additional costs for adoption not only by developers but by enterprise. This creates very limited utilities for enterprises to adopt public blockchains for building their internal or external solutions for their businesses.

Siloed Ecosystem vs Interoperability

With sidechains, plasma chains, Layer 2 Rollups, ZK Rollups each having separate execution environments, settlement layers, sequencers, proof generations, etc. This creates the major issue of cross- chain trustless messaging creating security issues for users for transferring assets from one chain to another through third parties such as bridges. Each blockchain and rollup have their siloed ecosystem and technical architecture creating it very difficult for developers to adapt to each architecture and develop their application compatible with all architectures.

If multiple Layer 3 chains as well as app-chains are developed using the similar EVM equivalent framework without having to transition to other technologies or going through multiple developer education programs, it will make the development and deployment of trustless solutions not only faster but cheaper. This would allow multiple publics, private as well as enterprise chains to share security as well as arbitrary message passing creating trustless interoperability among rollups.

Proposed Solution

For our research purposes, we'll only be focusing on ZK-rollups for now i.e., we'll be exploring solutions particularly on zk-

EVMs and avoiding other frameworks for mainly two reasons:

1. L3s cannot be effectively deployed on Optimistic rollups due to the 7-day fraud proof period. For deploying a Layer 3 chain, the execution of the chains from middleware to Layer 2 VM will become very complicated in terms of generating proofs. Not only the solution becomes complicated but not many optimistic rollups support the framework for fractal scaling.
2. We'll not be focusing on using an EVM sidechain or an EVM-compatible Layer 1 Chain for our thesis due to the adoption and security dilemma. Due to pre-existing community adoption of Ethereum by hundreds of millions and Ethereum beacon chain secured by tens of billions of dollars, it becomes difficult for any network to get the level of security and finality as Ethereum beacon chain.

Our solution will focus on building the tech stack allowing developers and enterprises to create their own Layer 3 scaling solution(rollups) on Type 2.5 and/or Type 3 zk-EVMs using Ethereum equivalent Virtual Machine with ZK-SNARKS (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge).

Why Zk-SNARKS?

The solution would be built with ZK-Rollups since the time involved with fraud proof generation and the 7 day challenge period would make proof generation and validation of L3 rollups very complicated and the security with transaction finality would be weak to order-flow hacks. Why we chose ZK-SNARKS over STARKS is due to:

- Efficiency and Scalability:

ZK-SNARKs provide more efficient proofs compared to ZK-STARKs. They generate smaller proof sizes, which reduces the computational and storage requirements for validating transactions and executing smart contracts. This efficiency is particularly crucial in the context of fractal scaling, where aggregating multiple transactions into a single proof is essential for achieving scalability.

- Ecosystem Maturity:

The ecosystem around ZK-SNARKs is more mature and has seen wider adoption compared to ZK-STARKs. This maturity translates into more available tools, libraries, and expertise for implementing and utilizing ZK- SNARKs. The larger developer community and existing infrastructure make it easier to integrate ZK-SNARKs into Layer 3 rollups on the Ethereum blockchain.

Why Type 3 ZK-EVMs should be preferred for Layer 3s

Type 2.5 or Type 3 ZK-EVMs are more preferred than Type 4 ZK-EVMs for fractal scaling solutions:

- Efficiency and Proof Size:

Type 3 ZK-EVMs typically offer more efficient proofs compared to Type 4ZK-EVMs. Fractal scaling heavily relies on aggregating multiple transactions into a single proof, and smaller proof sizes are desirable for improved efficiency. Type 3 ZK-EVMs are generally designed with succinct proof generation in mind, optimizing the proof size and reducing computational and storage overhead.

- Interoperability:

Type 3 ZK-EVMs typically maintain a high level of interoperability and byte-code compatibility with existing Ethereum infrastructure. They are designed to be compatible with Ethereum's EVM (Ethereum Virtual Machine), enabling seamless integration with smart contracts and existing decentralized applications (dApps). This interoperability is crucial for frictionless adoption and leveraging the robust ecosystem of Ethereum. Type 3 ZK-EVMs have byte-code level compatibility with EVM making the transitioning and network shifting much easier for developers and applications unlike Type 4 ZK-EVMs like CairoVM or VyperVM which use high level language ZK-Proofs which cannot be computed by Type 1 ZK-EVM.

Why Layer 3s?

This would be most effective on Layer solutions due to hyper scalability and middleware. With the existence of Layer 2 middleware between app-chains and Ethereum beacon chains. When it comes to scaling solutions, privacy and customized scaling, Layer 3 rollups have significant benefits over sovereign app-chains and Layer 2 app specific rollups.

- Interoperability and Network Effects:

Layer 3 rollups are designed to be fully compatible with the Ethereum network. They inherit Ethereum's smart contract functionality and benefit from the existing ecosystem of decentralized applications (dApps), wallets, and tools. This interoperability allows for seamless integration with existing Ethereum applications and maximizes network effects. Sovereign app-chains, being separate chains, may lack the same level of interoperability and may require building a new ecosystem from scratch, potentially hindering adoption.

- Security and Finality:

Layer 3 rollups provide strong security guarantees through the finality of transactions. Once a transaction is included in a Layer 3 rollup, it is considered final and cannot be reversed or tampered with. Sovereign app-chains may have different security models, and the finality of transactions may depend on their specific consensus mechanism. The security and finality guarantee of Layer 3 roll ups provide users and developers with a higher degree of confidence.

- Recursive Composition:

Fractal scaling leverages recursive composition, enabling the aggregation of transactions at multiple levels. This recursive approach allows for more efficient proofs, as transactions can be grouped hierarchically and processed collectively. It provides a higher level of scalability compared to Layer 2 ZK-rollups, which typically focus on aggregating transactions within a single layer.

- Flexibility and Granularity:

Fractal scaling offers greater flexibility and granularity in scaling solutions. It allows for different layers of aggregation and enables selective inclusion or exclusion of transactions based on specific criteria or requirements. This flexibility allows developers to optimize the scaling solution based on their application's needs. In contrast, Layer 2 ZK-rollups may have predefined structures and aggregation mechanisms, limiting the level of customization and fine-tuning.

- Layer Composition:

Fractal scaling supports the composition of multiple layers, each providing its own level of scalability. This hierarchical composition allows for a more modular and flexible approach to scaling, where different layers can be added or removed depending on network demands. Layer 2 ZK-rollups, while providing scalability within a specific layer, may not offer the same seamless composition of multiple layers.

Background

App-Chain Thesis

The app chain thesis proposes that every application should have its own rollup over Ethereum. This would create a separate layer for developers to build their applications with outsourced security of another blockchain and only use Ethereum for finality and data availability of the transactions processed on the rollup. The idea behind this thesis is to solve the problem of fragmentation in the blockchain community.

With many new types and forms of rollups being developed, developers have to learn new tech stacks, understand new concepts, and build new architectures to make their applications compatible with each new type of chain. By creating a separate rollup for each application, developers can build their applications on customized blockchains, allowing for greater flexibility and innovation while maintaining the security and finality of the Ethereum network.

With Layer 3 scaling solutions, Ethereum can be aligned with the app-chain thesis. As mentioned above, it would be more beneficial for applications and enterprises to launch their app-chains with interoperability and shared security. With shared execution environments and shared settlement layers, thousands of app-chains would be able to operate in a shared environment and focus on developing their business logic instead of bootstrapping security or community as compared to other chains.

MEV Capture

MEV, or miner extractable value, refers to the value that miners can capture by reordering or censoring transactions on a blockchain. App-chains and Layer 3 rollups can capture their own MEV by creating their own customized blockchains that enable them to process and settle transactions off-chain. This allows them to capture the full value of the transactions they process, rather than letting other blockchains capture the MEV of their users. By building customized blockchains, app-chains and Layer 3 rollups can also achieve greater scalability and efficiency, enabling them to process more transactions at a lower cost than other blockchains.

Modular Architecture and Hyper-Scalability

Rollups would be built withmodular architecture with customized data availability solutions. Unlike monolithic blockchain architecture where Ethereum blockchain is used for data availability instead of acting as a layer just for proof generation and transaction finality. This creates unnecessary data storage of Ethereum chain resulting in clogging of data and high gas fee for users of beacon chain as well as rollups. In order to achieve hyper-scalability, rollups need to adopt modular architecture where they use off-chain data availability solutions such as validiums, data availability committees, honest DAC minority, etc. Modular architecture will not only reduce gas costs and allow more transactions into a single batch but also help all Layer 3 rollups achieve customized privacy and scaling.

Existing ZK-Rollup Framework

ZK Rollups are a layer 2 scaling solution that uses cryptographic validity proofs to scale computation: each batch of transactions comes with a cryptographic proof (SNARK) that is verified by an Ethereum smart contract. This way every single transaction is fully verified by all Ethereum full nodes before a block is finalized. Zero-knowledge rollups (ZK-rollups) are layer 2 scaling solutions that move computation and state storage off-chain to increase throughput on Ethereum Mainnet. ZK-rollups can process thousands of transactions in a batch and then only post some minimal summary data to Mainnet. This summary data defines the changes that should be made to the Ethereum state and some cryptographic proof that those changes are correct.

ZK-rollups use zero-knowledge proofs to verify the validity of transactions and state transitions without revealing any of the transaction details, thereby maintaining privacy. These proofs are verified by a smart contract on Ethereum Mainnet, allowing the network to confirm the validity of the rollup’s state transitions without having to verify each transaction individually. This reduces the computational load on Ethereum Mainnet, allowing it to process significantly more transactions per second.

Utilities of a Fractal Scaling Solution

L2 is for Scaling, L3s are for customized Scaling:

Layer 3 rollups offer significant benefits for customized scaling on the Ethereum blockchain. Their customizability, specialized features, enhanced scalability, independent governance, ecosystem integration, security, and reliability make them a compelling choice for developers seeking tailored scaling solutions that align closely with their application’s requirements and objectives. L3s can be used for application specific rollups where developers can build their custom solutions with their business logic on their customized Layer 3 rollup.

Privacy in blockchains:

Layer 3 rollups can improve privacy in blockchain networks through various mechanisms and techniques.

- Zero-Knowledge Proofs: Layer 3 rollups can utilize zero-knowledge proofs (ZKPs) to provide privacy guarantees. ZKPs allow for the verification of certain properties or computations without revealing the underlying data. This enables users to prove the validity of their transactions or the correctness of certain operations without disclosing sensitive information.
- Trusted/Private Data Availability: Developers and Enterprises who want to utilize the security of Ethereum in a trusted environment while keeping their data private in a trusted environment can create their custom validium data availability models for their Layer 3 rollups.

Utilities for Enterprises:

Enterprises can utilize Layer 3 rollups for their custom use cases to build their solutions by utilizing the security and ecosystem of Ethereum in their trusted environment. Layer 3 customized enterprise specific rollups can be utilized best for these solutions:

- High Volume Transaction Systems
- Tokenization of Real-World Assets
- Customized Financial Solutions
- Privacy-Focused Applications
- Supply Chain and Logistics Solutions
- Gaming and NFT Utility Applications

Conclusion

In conclusion, the integration of a fractal scaling solution over Type 3 ZK-EVM using Halo2 presents a significant advancement in the scalability and privacy of blockchain networks. By combining the power of fractal scaling, which enables recursive composition of computation, and the privacy-preserving properties of the ZK-EVM protocol, this solution offers a promising path forward for addressing the limitations of existing blockchain systems.

Fractal scaling allows for the efficient aggregation of multiple transactions into a single proof, reducing the computational and storage overhead associated with processing and validating transactions. This recursive composition enables a higher throughput of transactions, thereby significantly improving the scalability of blockchain networks. By leveraging this approach, the Type 3 ZK-EVM protocol can benefit from enhanced scalability while preserving the security guarantees and decentralized nature of the underlying blockchain.

The utilization of the Halo2 protocol further enhances the privacy aspects of the system. Halo2 leverages zero-knowledge proofs to enable secure computation and verification without revealing any sensitive information. By employing this protocol within the fractal scaling solution, users can conduct transactions with confidentiality, ensuring that their personal and financial information remains private while still benefiting from the scalability improvements. With this integration, blockchain systems can handle a significantly higher transaction volume while maintaining the security, decentralization, and privacy that users expect. As this technology continues to mature, it has the potential to unlock new possibilities and drive widespread adoption of blockchain technology across various industries and use cases.