Zephyria Network

What is Zephyria Network?

Zephyria Network can be Described as a Network Layer Somewhere in between Layer 1 and Layer 2, We must say more bent towards Layer 2 in Order to leverage on Ethereum.

What is it Exactly doing?

Zephyria Network is aimed to become an Ultra Scalable Network. But how exactly, Zephyria Network aims to use Recursive SNARK's to Generate Succinct Proofs of the Transaction. But Only Transaction? I don't think so, Even We also do the same.

There are lot of CDK Based zkEVM arriving every month or day, Zephyria doesn't wants to be one of them. What Zephyria wants is to Rule Over them.

But Exactly How: Let's understand the **Blockchain Trilemma**, it is **Scalability**, **Decentralization** and **Security**.

But What we think is Scalability is everything, If a Blockchain is highly scalable it can be very easily decentralized by common public with their existing devices, and If the Network is decentralized then the Network by default is Secure to very high extent as there's no risk of centralization of the network (like the example with Bitcoin).

So, What difference will Zephyria do

The Answer is Global State Proof (GSP not your 30% GST), now what is that it is like a snapshot of the Whole Blockchain represented in just few Kilobytes or Megabytes.

This GSP can then be used by new nodes and start syncing and validating the network without any need of holding the Whole Blockchain. Now this means that If implemented on devices like android or ios they can also participate in the network as the On-Chain Data or the Whole Blockchain (GSP) is just few KBs/MBs in size.

Definitely Heard of Something like this before, **Mina Protocol**.

We can say that Our Idea is Derived from there, but the implementation and execution is on complete different level.

Zephyria will be a SDK for building Layer 2 Solutions which are highly scalable.

- The Succinctness of Zephyria will help in achieving High Scalability even after millions or billions of transactions, It's the Future Proof solution we aim for.
- Secondly, The Small size will help in running full nodes anywhere and nearly on any device in the world making it Highly Decentralized Network.
- Third, Security ZKProof's are a Security themselves and Leveraging Ethereum's Security drastically make the network Strong and Secure.

Now Comes **The Technical Part of How Zephyria will be Designed to Solve these problems**.

Stating the Problems faced by ZK Layer 2's as per our observation:

1. EVM Compatibility: Very Less ZK Solutions are compatible with Ethereum, Only PolygonzkEVM, Scroll, zksync, Linea are some compatible solutions.
2. Transaction Speeds: Transactions Speeds are comparatively slow on ZK Chains currently running.
3. Low Throughput: Lesser Number of Transactions being processed.
4. Gas Fees: There's not a huge difference between the gas prices as compared to Ethereum.

How Zephyria Will solve These:

On-Chain

Researching on Polygon's CDK, We have an idea of twisting the Kit to Wrap Zephyria around.

- First, The Transactions Will be Sent to Node via RPC by End User → Which will be Propagated to all the Nodes as msg (All Nodes having same set of Transactions)

- **Sequencer** Module in ZkNode which is used as Transaction Receiver and Executes L2 Transaction, Then Creates a Batch of Transactions of L2 and Sends to L1

Using This Module: Our Modification Idea- converting sequencer so as the Sequencer will batch multiple Batches of Transactions (After validating transactions) as per Chronological order (mimicking Blocks) → Propagating The Batches to Aggregator Protocol

Next Step Will Involve **Aggregator** Module

- Aggregator is used to Fetch Batches from L1, Interaction with Prover (send and receive proofs) and lastly updating proofs to the L1
- Our Idea: Using The Aggregator to Send Batch to Prover → Receive Proof of State Transition → Update the Network of New Proof and State → Update State Contract on L1

Prover

- The Prover will create a Global Proof of State Transition After Applying the Transaction to the Previous state (S0), using them to create a New Proof Validating the State Transition S1 is Valid After Applying the Transaction (T1).

Global State Proof

Can be Described as result of Recursively Proofing the State (Proof of State Change before and after applying any transaction which leads to state transition of the Whole Blockchain)

That Means We can Use that Proof to Verify that the Current Global State of the Blockchain is valid after applying Transaction to the Previous State of the Blockchain and any New Node can Sync further without gathering any ancient history of the network.

Off-Chain

The Transactions and All Other Data is Propagated to all the nodes and is stored Off-chain.

Nodes will validate the Integrity/Validity of Transactions as done by Sequencer in PolyZkEVM

The Transaction is applied to the State and State is Updated with State Transition Recorded.

Which is then used to Create zk Global State Proof with Previous State.

The Data’s integrity is maintained with Zero Knowledge GS Proof whether the current state is valid or not.