Orange: a Bitcoin Layer-2 network with PoW Mechanism

Orange Team
18th March, 2024

I. Overview

Orange lightpaper sheds light on Bitcoin's scalability challenges and introduces the Orange Chain, a Layer-2 solution aimed at enhancing transaction speed and expanding application diversity without compromising security and stability.

Orange represents the first rollup on Bitcoin with PoW mechanism, harnessing rollup technology to enable Turing-complete smart contracts for off-chain transactions. Built upon Op Stack + ZK Fraud Proof technology, Orange Chain ensures compatibility with existing Ethereum tools while maintaining EVM equivalence through Optimistic's Rollup technology. Moreover, it features the Sequence Hub network layer for decentralized ordering and the Oracle DA Hub network layer for decentralized data availability. Through zero-knowledge proof verification commitments and consensus, Orange Chain facilitates the presentation of fraud proofs by any challenger, leveraging Bitcoin's decentralization and consensus mechanisms for enhanced security. Supported by robust underlying service technologies and decentralized ZK computational power, Orange Chain delivers a secure, seamless, user-friendly, cost-effective, and efficient second-layer network solution for Bitcoin.

For increased security and stability, we have implemented a PoW mechanism within Orange. Miners can access and assist with computations permissionlessly. PoW, as the consensus mechanism of the BTC network, plays a critical role in its long-term stable operation. We also aim to enhance Orange's security and stability by incorporating the PoW mechanism, inheriting the traits of security and stability from BTC.

Key words: *Rollup, Zero-knowledge, PoW mining, BTC Layer-2.*

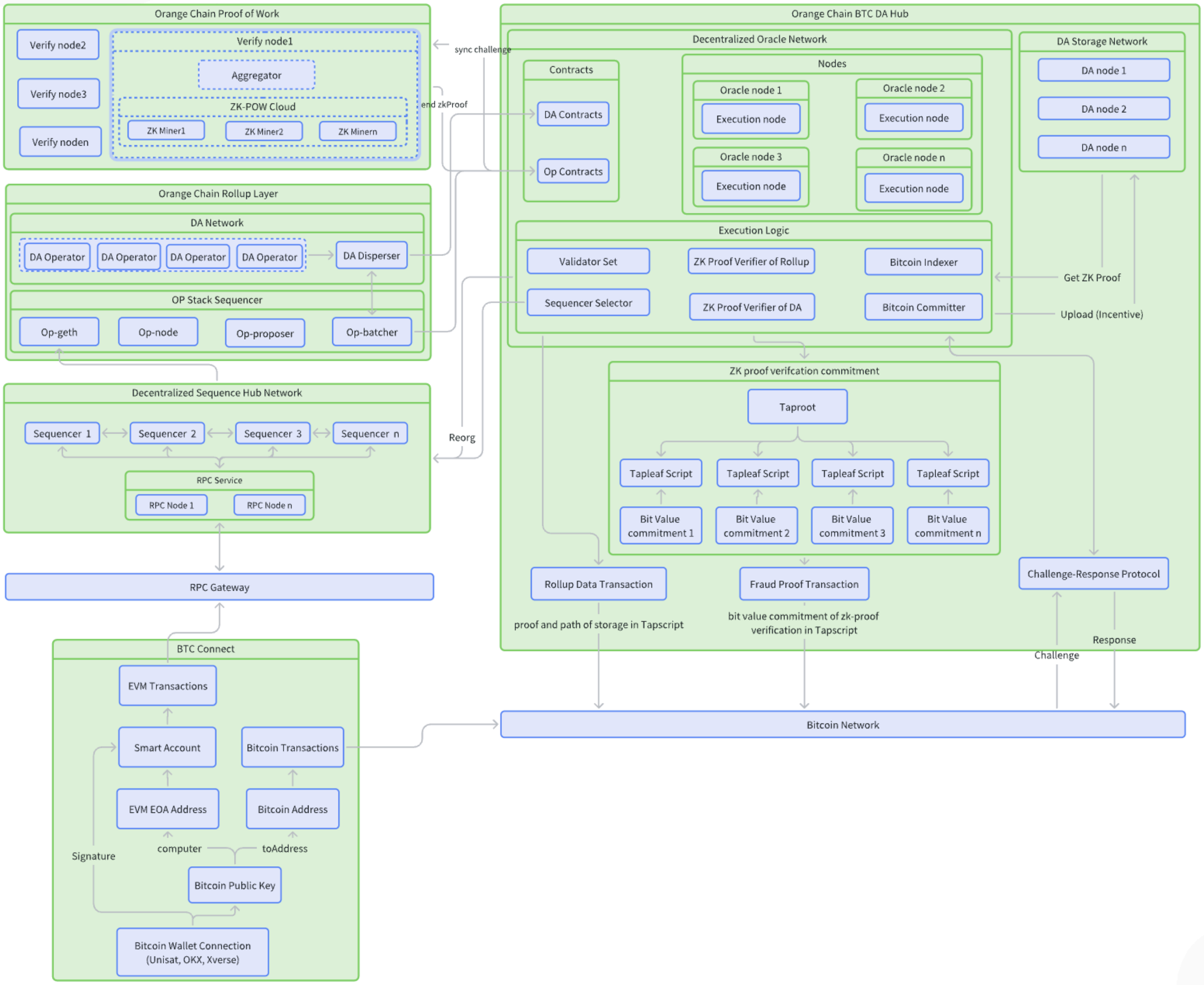
II. Advantages

Orange, as the Bitcoin's Layer-2 scaling network, has the following advantages:

- Security Equivalence: Leveraging zero-knowledge proof verification commitments and consensus mechanisms ensures that the layer-2 network maintains the same level of security as the Bitcoin network.
- EVM Equivalence: Maintains compatibility with existing Ethereum tools while guaranteeing equivalence with the Ethereum Virtual Machine (EVM).
- Cost Efficiency: Utilizes ZK proofs combined with zkSNARK technology to effectively compress data, thereby reducing transaction costs.
- High Performance: Achieves fast network finality through efficient proof of validity, while also utilizing recursive STARK technology for exceptional scalability.
- User-Friendliness: Simplifies the network usage process by directly utilizing BTC as second-layer Gas, enhancing usability.

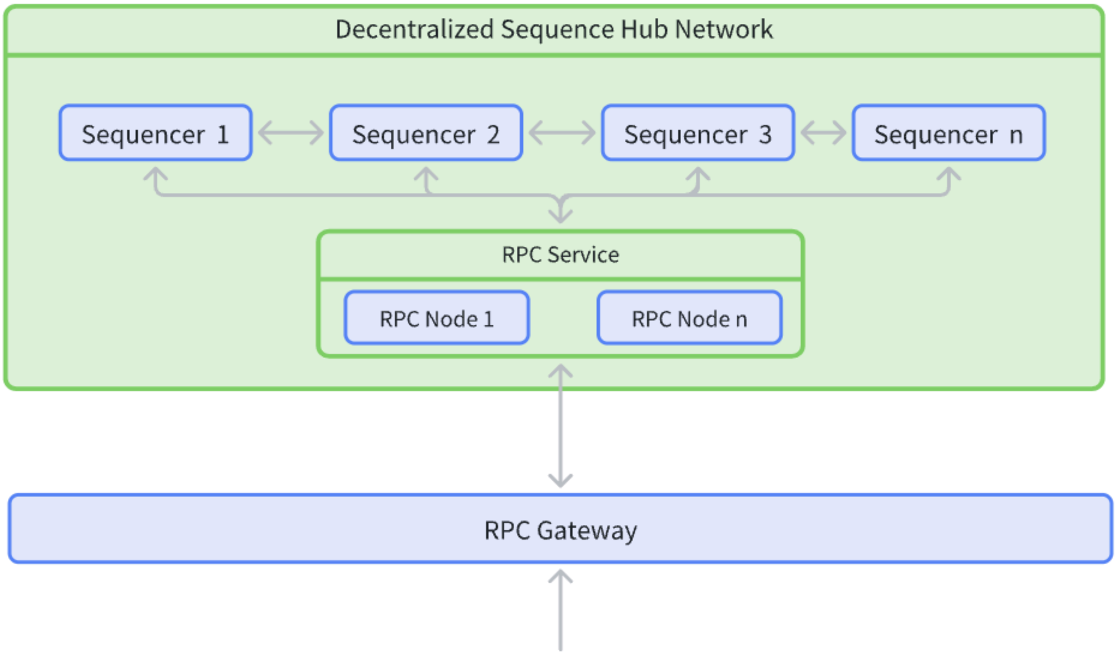
III. Technical Architecture

The overall technical architecture of the Orange Chain is as illustrated in the diagram below. The network primarily consists of five key layers: decentralized sorting layer, aggregation layer, modular computing layer, data availability layer, and Hub interaction layer. Utilizing efficient and secure technology solutions, it has redefined the implementation approach of the Bitcoin layer-2 network.



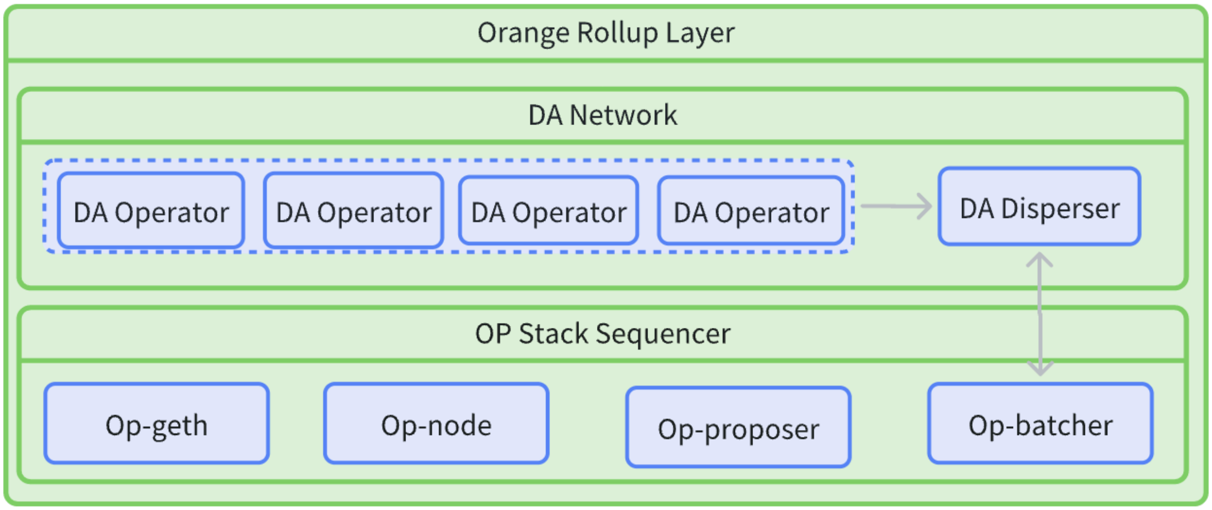
A. Decentralized Sorting Layer

The main process of sorting is as follows:



1. Transactions are received through the RPC aggregation gateway service (RPC Gateway).
2. The RPC Gateway forwards transactions to the Decentralized Sequence Hub Network (DSHN) for consensus ordering.
3. DSHN packages the ordered transactions into blocks and forwards the validated transactions to the Rollup Layer for execution via subnet gateways.
4. DSHN simultaneously issues succinct commitments for the blocks. Contract verification and sorting proofs are validated, then block commitments are stored.
5. The Rollup Layer publishes the updated state to the Decentralized Oracle Network.

B. Rollup Layer

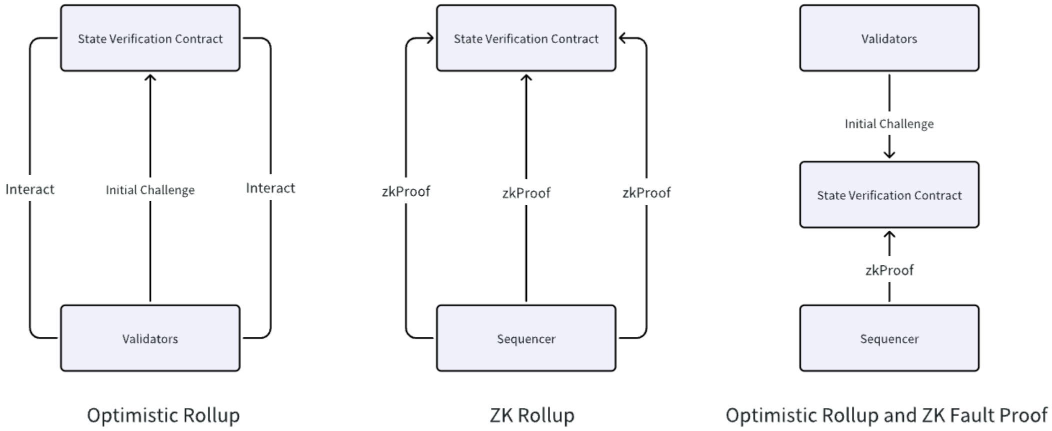


Orange Chain utilizes Optimistic Rollup to implement the Rollup Layer, responsible for executing user transactions and generating related proofs within the second-layer network. Users submit their transactions to the Rollup Layer for processing, and their states are stored in this layer as well. Batches and generated zero-knowledge proofs are transmitted to the data availability layer provided by the Decentralized Oracle Network for storage and verification purposes.

C. Decentralized Oracle Network DA (DONA)

The Decentralized Oracle Network ensures the integrity of state transitions using validity proofs, but it doesn't store transaction data on the BTC network. For the DA service itself, it issues scatter requests to dispersers, who encode the Blob using Reed-Solomon coding, compute KZG commitments for the encoded Blob, and generate KZG proofs for each block. The dispersers then send the blocks, KZG commitments, and KZG proofs to operators, who return signatures. The dispersers aggregate these signatures and upload them to L1 in the form of calldata for the DA contract.

D. Op Stack + ZK Fraud Proof



Optimistic Rollup

ZK Rollup

Optimistic Rollup and ZK Fault Proof

The Op Stack + ZK Fraud Proof architecture is a novel design integrating validity proofs based on zero-knowledge proofs into Optimistic Rollup technology. When challengers point out that the sequencer has submitted incorrect data, they submit a challenge to Layer 1. The sequencer must generate the corresponding ZK Proof within a limited challenge time and submit it to the Layer 1 contract for verification. If the verification result indicates that the data is valid, the challenge fails; otherwise, the challenge succeeds.

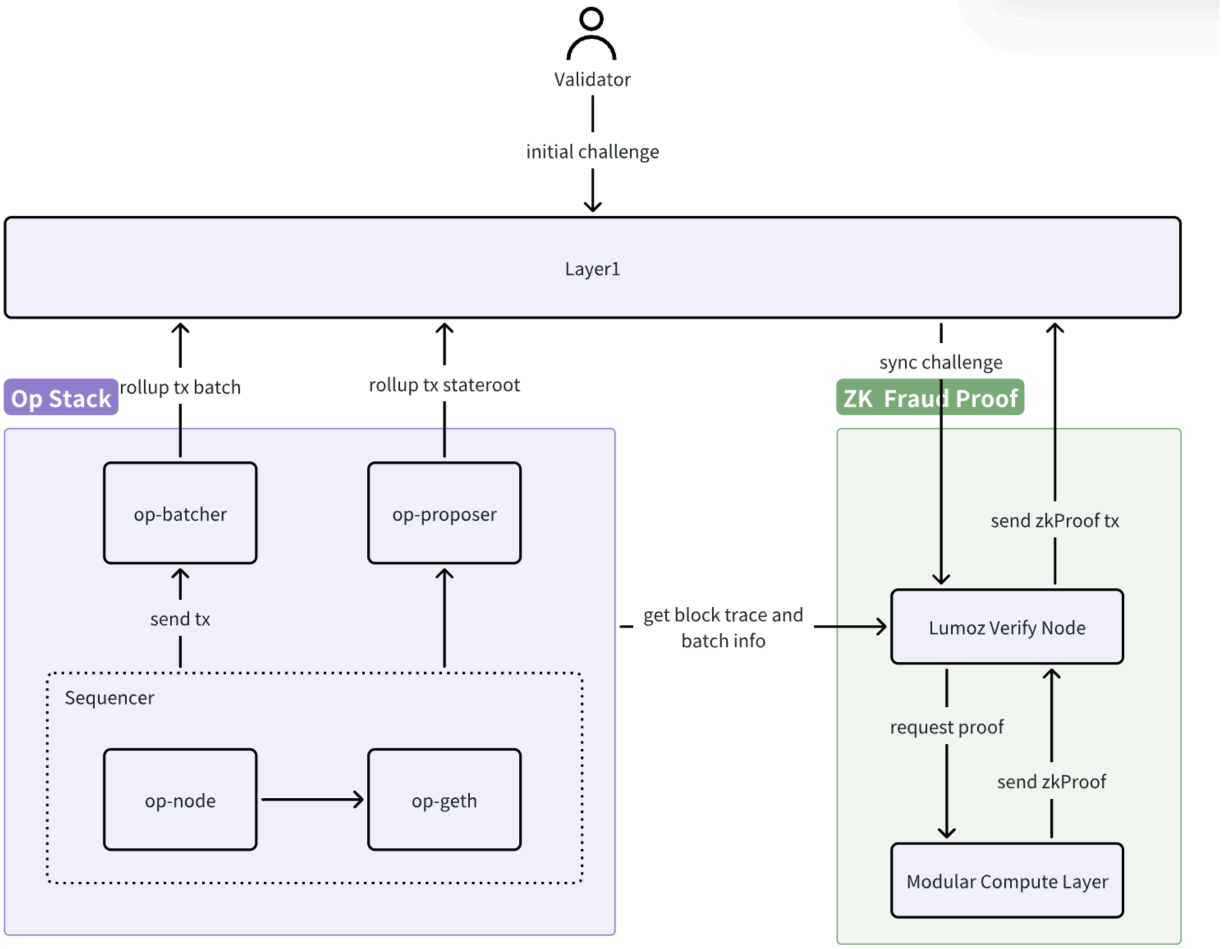
The diagram illustrates the specific process of handling fraud proofs in Layer 2 technology under the Op Stack and ZK Fraud Proof architecture. In this architecture, the Op Stack module performs the core functions of Layer 2, including handling basic blockchain functions and submitting batches to Layer 1. Meanwhile, the ZK Fraud Proof module focuses on handling challenges of fraud proofs.

The process details are as follows:

1. Challenge initiation: Validators initiate challenges of fraud proofs.
2. Information synchronization: Lumoz verification nodes synchronize challenge information to prepare for the next verification step.
3. Obtain zero-knowledge proof inputs: Verification nodes retrieve necessary zero-knowledge proof input data from the Op Stack module, including block traces and batch information.
4. Generate zero-knowledge proofs: Lumoz subsequently requests the modular computing layer to generate the required zero-knowledge proofs.
5. Proof submission: Once the zero-knowledge proofs are generated, Lumoz verification nodes submit the proofs to Layer 1 for verification.

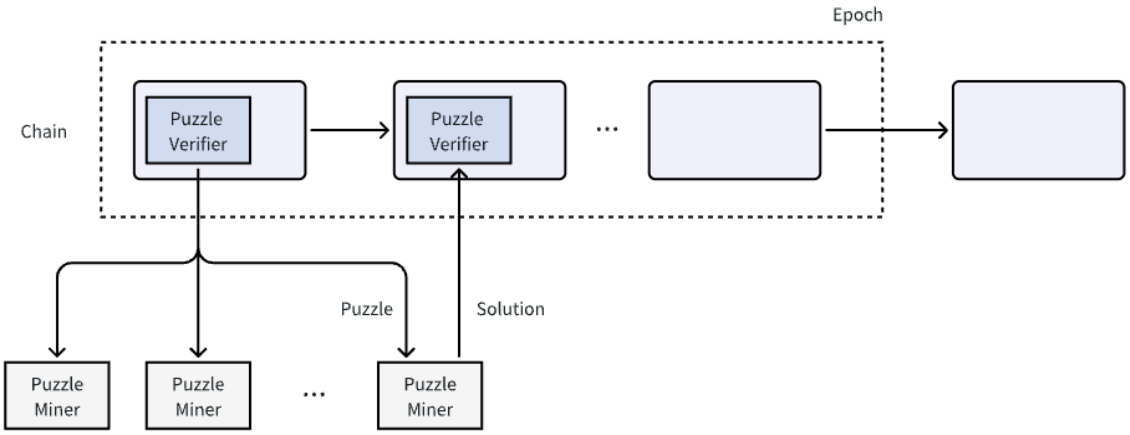
Through the above process, the challenge and verification process of ZK Fraud Proof is completed.

As is well known, Optimistic Rollup has lower costs but longer withdrawal wait times, while ZK Rollup requires almost no waiting time for withdrawals but has higher costs. This solution combines the strengths and weaknesses of Optimistic Rollup and ZK Rollup, maintaining the characteristics of low cost while effectively reducing waiting times.



E. Proof of Work

The introduction of PoW ensures the security of the Orange Chain, as the entire chain is supported by continuously accumulating computational power. Additionally, it enables fair distribution of governance tokens based on the computational power provided by miners, enhancing the decentralization of governance. The success of PoW has been well demonstrated in the Bitcoin network, and thus, we designed a PoW mechanism tailored to the characteristics of the Orange Chain.



Orange Puzzle

The Orange Puzzle is a proof-of-work puzzle designed to incentivize miners to generate ZK (Zero-Knowledge) proofs as solutions for the network. Unlike traditional PoW algorithms, the Orange Puzzle possesses the following three characteristics:

1. ZK Prover as a Miner: Unlike traditional PoW algorithms where hash computations such as SHA256 are performed, Orange Chain utilizes ZKP calculations. Miners are incentivized to generate ZK proofs to meet the corresponding difficulty. These ZK proofs provide verifiable computational power to the chain and can be utilized in future applications such as ZK co-processors and ZKML.
2. Smart Contract as a Verifier: Unlike the traditional PoW where solutions are verified in the consensus layer, Orange Chain employs smart contracts to verify ZK proofs and distribute rewards. This approach enhances the flexibility of PoW algorithm upgrades and tuning, reduces its impact on block production, and mitigates risks of forks and 51% attacks to the chain.
3. Proof Validated, Prover Incentivized: All valid proofs are rewarded, contrasting with many PoW systems where only one valid solution per height or epoch is rewarded. As long as the proof is valid and meets the difficulty requirements, miners receive rewards.

Puzzle Verifier

The Puzzle Verifier implements the core logic of PoW through smart contracts, including difficulty adjustments, puzzle iterations, reward adjustments and distribution, and management of different ZK circuits. The specific mechanisms are as follows:

1. Epoch-based Puzzle: Puzzle Verifier divides time into fixed epochs. During each epoch, miners compute ZK proofs based on the same puzzle and difficulty.
2. Difficulty Adjustment: At the end of each epoch, Puzzle Verifier adjusts the difficulty based on the submission status of solutions from the previous epoch, ensuring a roughly equal number of solutions per epoch and uniform reward distribution over time. Additionally, a new puzzle is randomly chosen for the next epoch.
3. Reward Distribution: Puzzle Verifier periodically adjusts the reward distribution based on tokenomics to ensure that the distribution of governance tokens aligns with a reasonable inflation rate.
4. Flexibility in ZK Circuits: Puzzle Verifier allows for the replacement of ZK verification circuits and algorithms. For instance, early support might resemble ZK algorithms used in Aleo mining, while future iterations may lean towards useful ZK calculations like ZK co-processors and ZKML.The design of the algorithm will take into account both high-end hardware (like GPU) and mobile hardware.

Puzzle Miner

Puzzle Miners compute ZK proofs off-chain that adhere to the current epoch's difficulty and puzzle, then submit them to Puzzle Verifier on-chain to receive rewards. The steps involved are as follows:

1. Puzzle Retrieval: Puzzle Miners obtain the current epoch's difficulty and puzzle settings from Puzzle Verifier's contract. They use these parameters along with their miner address and nonce values for ZK circuit input, generating a ZK proof.
2. Verification: Puzzle Miners check the hash of the generated ZK proof. If it does not meet the current epoch's difficulty, they discard it and iterate nonce values to generate a new ZK proof.
3. Submission and Verification: If the ZK proof meets the difficulty, Puzzle Miners immediately submit the nonce and ZK proof as a solution to Puzzle Verifier for verification.

Puzzle Verifier conducts the following checks:

1. Verification of the ZK proof hash against the current epoch's difficulty.
2. Confirmation that the solution does not repeat within the current epoch.
3. Validation of the ZK proof, ensuring that inputs comply with circuit constraints.

Upon successful verification, Puzzle Verifier rewards the miner.

F. Hub Interaction Layer

User transactions are all submitted and processed at the Rollup layer, with their states also stored in this layer. The network generates relevant zero-knowledge proofs, packages them, and sends them to the DONA layer for storage and verification. The DONA layer encompasses decentralized storage, Orange Chain nodes, and the BTC network, used to verify the zero-knowledge proofs of Rollup and permanently store data copies from the Rollup layer. Ultimately, data is imprinted into the BTC network in plaintext.

The DSHN sequencer packs user transaction data, which is then saved through DONA distributed storage to avoid single points of failure and enhance reliability. To ensure data availability, Orange Chain writes Tapscript scripts to the Bitcoin network within each block, achieving continuous data availability.

In the Ethereum network, Rollup passes Layer 2 network data to the mainnet contract for verification and storage via calldata. However, the Bitcoin network does not support automatic verification of smart contracts. ZK-Rollup only writes zero-knowledge proofs and aggregated Rollup data to the Bitcoin network via Taproot, ensuring the anchoring of ZK-Rollup data in Bitcoin and preventing tampering.

However, this does not guarantee the validity and correctness of transactions within ZK-Rollup, nor does it utilize Bitcoin's powerful consensus to ensure the security of Layer 2 ZK-Rollup. Therefore, the approach adopted by Orange Chain is to write commitments of zero-knowledge proofs to the mainnet, allowing challengers to verify the commitments within a specified period. If a challenge succeeds, Rollup will roll back, and the challenger will receive assets locked by nodes. If no one challenges or the challenge fails within the challenge period, Rollup will receive final confirmation on the BTC network.

Technical Features of Orange Chain

Security and Decentralization

1. Decentralized Oracle Network DA: Based on data on Bitcoin, all transactions on Orange Chain can be recovered on the Rollup Layer, while the decentralization and consensus of the BTC network reinforce the security of Orange Chain data.
2. Bitcoin Transaction Confirmation: Through zk-proof commitments and allowing challenges, the Orange Chain network achieves secure bidirectional confirmation of Bitcoin transactions, rather than just one-way data writing to Bitcoin.
3. Decentralized Sequence Hub Network: Achieves decentralized consensus sorting, reducing the possibility of malicious behavior.