Layer 2 and Rollups

1. Background

1. The main agenda of this presentation is to understand Layer 2 and Rollups
2. As a part of the presentation, I will focus on
    a. What is Layer 2 ? Why Layer 2 ?
    b. Layer 2 types: Rollups, Channels, Sidechains
    c. Deep dive into Rollups (Optimistic and ZK)
    d. Challanges and future tends in Layer 2

2. What is Layer 2 ? Why Layer 2 ?

2.1 Deffination

🚀 Layer 2 refers to a network or technology that operates on top of an underlying blockchain protocol to improve its scalability and efficiency.

🚀 Or Layer 2 is any off-chain network, system or technology built on top of a blockchain to help extend its capabilities.

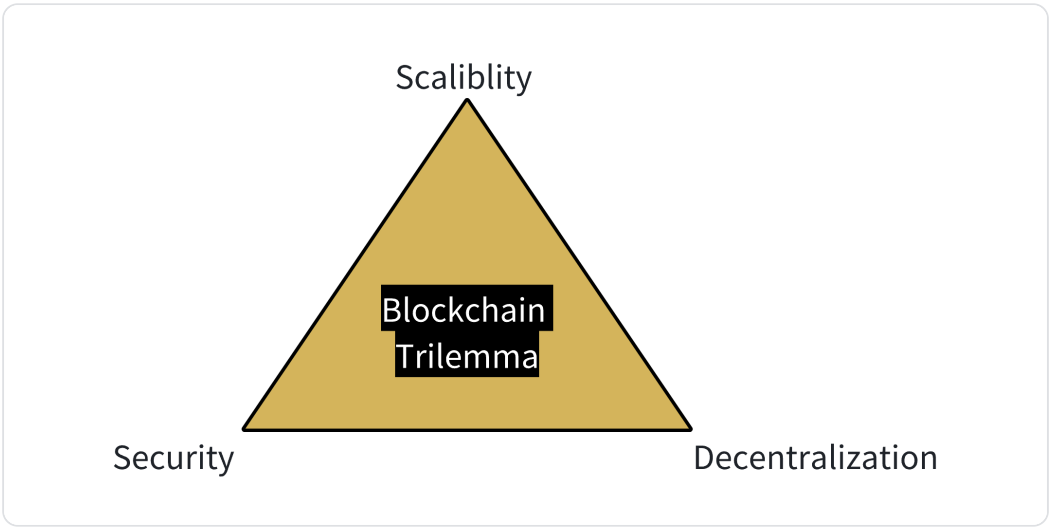
- The core requirements of Layer 2 are
  - It inherits the security of the blockchain it is built on top of.
  - Transaction Data must, in some shape or form, be verified and confirmed by the underlying blockchain network

2.2 Why Layer 2 ?

- Before knowing why Layer 2, we will focus on what the problems that we are trying to solve

2.2.1 Challenges in blockchain

- Blockchain technology is really an amazing deal for the future, but it has some limitations due to its growing demand.
  - Limitations of scalability to match a growing adoption have resulted in high fees and slow execution times
  - diminished ability of blockchain to operate on scale
- Blockchanin mainly holds the responsibility for 3 main features
  - **Scalability** - The number of computations the network can process per second.
  - **Security** - The amount of resources required to corrupt network consensus.
  - **Decentralization** - The number of full nodes participating in the network.
- Today's blockchain can successfully fill 2 out of them simultaneously



2.2.2 How Layer-2 Solves the purpose

🚀 Layer 2 is currently in the early stages and many designs of layer 2 are still unproven and untested

- Potential benefits of Layer 2 are
  - Offloading the transactions from Layer 1
  - Reducing congestion and fees
  - Enabling higher throughput
- Two important parts of Layer 2:
  - **A network** that processes transactions.
  - A **Smart contract** on the underlying blockchain that resolves any disputes and achieves consensus on the state of the layer-2 network by cementing it to an underlying blockchain.
- The **core functions of the smart contract** are always to:
  a. Hold and release funds transferred to layer 2
  b. Receive some kind of proof generated by layer 2, validate it, resolve disputes, and then finalize transactions

3. Layer 2 Types (types of solutions)

3.1 Types

- **Rollups (Optimistic & Zero-Knowledge)** - Bunddle multiple transactions into one proof, reducing data on layer 1
- **State Channels** - Peer to peer transactions where participants can transact off-chain, updating the blockchain when the channel is closed.
- **Side chains** - Independent chains connected to the main chain offering their own consensus mechanism but relying on Layer 1 for security.

3.2 What are Rollups ?

- **Rollups** are a Layer 2 scaling solution for blockchains, designed to increase throughput and reduce transaction costs while maintaining security.

- They work by **bundling multiple transactions** into a single batch and posting minimal data back to the Layer 1 blockchain (e.g., Ethereum).
- This allows transactions to be processed off-chain, reducing the load on the main chain while still benefiting from its security.
- Types of Rollups
  - Optimistic rollups
  - Zero-knowledge rollups

4. Deep dive into Rollups

> 🚀 Optimistic and zero-knowledge rollups offer higher throughput and lower costs by executing smart contract state changes off-chain and proving them on-chain.

4.1 Optimistic Rollups

- **Definition:**
  - Rollups that assume transactions are valid by default, with fraud proofs as a fallback in case of disputes.
- **How They Work:**
  a. Off-chain transactions bundled into a rollup.
  b. Optimistic assumption: No fraud unless proven otherwise.
  c. Validators post data to Layer 1; challenge period allows users to contest incorrect transactions.
- **Key Examples:**
  - Arbitrum
  - Optimism

4.2 Zero-Knowledge Rollups

- **Definition:**
  - Rollups that use cryptographic proofs to instantly verify the correctness of transactions off-chain before batching them onto Layer 1.
- **How They Work:**

a. Transactions are computed off-chain.
b. ZK-Proof (SNARK or STARK) is generated.
c. The proof is posted on-chain and is verified by Layer 1 without needing the transaction data.

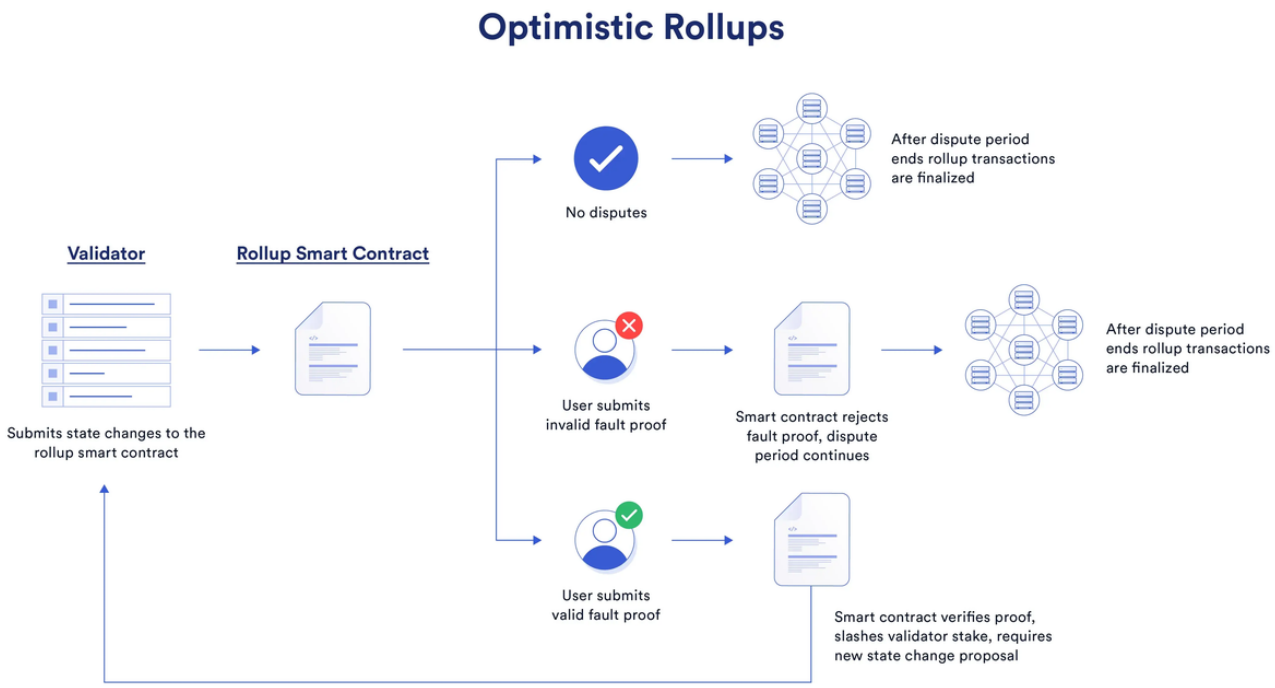
- **Key Examples:**
  - zkSync
  - StarkWare

4.3 How do Rollups work

- **Off-Chain Execution:** A key feature of rollups is that they perform off-chain execution of transactions. This means that layer-2 networks handle the processing of transactions, whether with another user or with a smart contract, on behalf of the base blockchain
- **Batching Transactions:** Rollups group multiple off-chain transactions into a single batch and submit a "rolled-up" transaction to Layer 1. This minimizes the data that needs to be posted on the main chain, thus lowering gas fees.
- **Security Guarantees:** Rollups inherit security from the base blockchain (Layer 1), either by relying on cryptographic proofs (ZK-Rollups) or fraud-proof mechanisms (Optimistic Rollups).

4.4 ZK-Rollups Validity Proof

4.5 Optimistic Rollups



4.6 Difference between Optimistic and ZK Rollups

- **Transaction Validation**
  - **ZK-Rollups**: Transactions must be verified before being sent to the mainnet using **Zero Knowledge Proofs (ZKPs)**. ZKPs prove the validity of transactions without revealing additional information.
  - **Optimistic Rollups**: Transactions are assumed to be valid by default. No proof is submitted when data is sent to the mainnet. Validity is challenged only if fraud is suspected, using a **fraud proof mechanism**.
- **Proof Mechanism**
  - **ZK-Rollups**: Use **Zero Knowledge Proofs**, a mathematical method that proves correctness without revealing sensitive information.
  - **Optimistic Rollups**: Rely on a **fraud proof mechanism**, where any participant can challenge the correctness of transactions if they suspect fraud.
- **Transaction Finality Time**
  - **ZK-Rollups**: Transactions and asset transfers are finalized almost instantly, often within seconds, as the proof of validity is already included.
  - **Optimistic Rollups**: Asset transfers are delayed, often by 1 week, to allow time for potential challenges or fraud detection.
- **Data Compression**

- **ZK-Rollups**: Compress large amounts of transaction data into small pieces before sending them to the mainnet, reducing space usage on-chain.
- **Optimistic Rollups**: Do not have the same level of data compression as ZK-Rollups.

- **Complexity and Implementation**
  - **ZK-Rollups**: More complex and technologically advanced due to the use of zero knowledge proofs, making them harder to develop.
  - **Optimistic Rollups**: Simpler to implement, making them easier to adopt by developers.
- **Ethereum Virtual Machine (EVM) Compatibility**
  - **ZK-Rollups**: Currently, most ZK-Rollups cannot run **EVM**-based smart contracts, though projects like **zkSync** are working towards EVM compatibility.
  - **Optimistic Rollups**: Fully compatible with the Ethereum Virtual Machine, allowing DeFi protocols like Uniswap and Compound to migrate more easily.
- **Confidentiality**
  - **ZK-Rollups**: Offer better confidentiality because of the zero knowledge proof system, which hides transaction details.
  - **Optimistic Rollups**: Do not offer the same level of confidentiality, as transactions are openly posted on-chain unless proven fraudulent.
- **Security Approach**
  - **ZK-Rollups**: Security is derived from the cryptographic strength of zero knowledge proofs, ensuring correctness upfront.
  - **Optimistic Rollups**: Security relies on the challenge-response mechanism, where fraud can be disputed after the fact.

5. Challanges and Future tends in Layer 2

- **Challenges:**
  - **Optimistic Rollups:** Long withdrawal times; reliance on honest validators.
  - **ZK-Rollups:** High development complexity, proving systems not yet widely adopted.
- **Future Trends:**
  - **Interoperability:** Solutions enabling cross-rollup and cross-chain interactions.
  - **Layer 3:** Innovations beyond Layer 2 for further scalability.
  - **Hybrid Solutions:** Combining the best of optimistic and ZK approaches.

❓ Question and Answers