ANASTASIA LABS

Midgard

Non-technical Documentation

Contents

1. What is Midgard?

Midgard is an innovative layer 2 scaling solution built on top of the Cardano blockchain to make it faster, cheaper, and easier to use.

If Cardano was a busy city with a main highway (Layer 1), where all the traffic (transactions) flows, as the city grows, the main highway can get crowded, causing traffic jams and and higher costs for drivers.

Midgard acts like an additional set of express lanes alongside this main highway. These express lanes handle a large volume of traffic efficiently without overwhelming the main highway, ensuring the city runs smoother, faster, and cheaper for everyone.

2. Understanding Layer 2 Solutions

2.1. The Need for Layer 2

As blockchain networks like Cardano become more popular, they face challenges in handling a high number of transactions.

High transaction volumes can lead to network congestion, causing slower transaction times and higher fees.

Layer 2 solutions aim to solve these issues by enabling **faster**, **cheaper**, and **more scalable** transactions.

2.2. How Layer 2 Works

Layer 2 solutions operate on top of the main blockchain **(Layer 1)** but execute transactions **off-chain**.

This means the primary blockchain remains secure and decentralized, while the transaction processing happens separately.

This setup increases the number of transactions that can be handled at once and reduces costs.

2.3. Types of Layer 2 Solutions

1. **Optimistic Rollups**
   - Assume transactions are valid by default.
   - Only verify transactions if a fraud proof is submitted.
   - Midgard L2 utilizes optimistic rollups to effectively scale the Cardano blockchain.
2. **State Channels**
   - Allow participants to conduct transactions off-chain.
   - Only the final state is recorded on the main blockchain.
3. **Sidechains**
   - Separate blockchains connected to the main chain.

- Handle specific types of transactions independently.

4. **Plasma**

- Creates smaller chains linked to the main blockchain.

- Ensures scalability by offloading processing.

3. Key Concepts

1. **Layer 2 (Extra Lanes for Traffic)**

   - **Midgard L2** operates on top of **Cardano's** main blockchain **(Layer 1)** to help handle more transactions at once.

   - It uses a special technology called **optimistic rollups** to manage transactions efficiently.

2. **Operators**

   - Operators are like traffic controllers who manage the flow of transactions in the express lanes.

   - They handle transactions off the main highway and then periodically report back to the main blockchain with updates to keep traffic flowing smoothly.

   - To ensure they do their job honestly, Operators must deposit **ADA** (Cardano's native currency) as a bond. If they cheat, they lose this bond, ensuring they act in the system's best interest.

3. **Watchers**

   - Watchers are like undercover inspectors who keep an eye on the Operators to ensure no one is cheating.

   - If they spot any suspicious activity, they raise a red flag (submit a "**fraud proof**") to challenge the Operator's actions.

   - If the fraud proof is valid, the bad update is canceled, and the Operator may face penalties.

4. **Fraud Proofs**

   - A fraud proof is basically evidence that something went wrong with the transactions.

   - During a designated challenge period, Watchers can submit fraud proofs to contest invalid state commitments.

   - If a fraud proof is validated, the fraudulent update is undone and penalizes the dishonest Operator and they may lose their bond.

5. **State Management – Keeping Track**

- Midgard uses a smart system to keep track of all transactions and states (like the current traffic conditions).

- Instead of storing every single transaction in detail, Midgard creates a secure and concise summary using **Merkle roots**. This ensures everything stays organized and secure without handling every tiny detail.

6. **Optimistic Rollup**

- Optimistic rollups assume that all transactions are valid by default, speeding up the process.

- Only if a Watcher raises a concern (a fraud proof) does the system take a closer look to verify the transaction.

- This approach significantly increases transaction throughput and efficiency..

7. **Tokenless Design**

- Midgard uses **ADA**, Cardano's native currency, for all transactions and incentives.

- There's no need for an additional token, simplifying the system and maintaining focus on ADA.

4. How It Works

4.1. Transaction Processing

· Transactions are first handled off the main blockchain (off-chain) by Operators.
· Operators bundle these transactions and prepare a summary (similar to a progress report) to send back to the main blockchain.

4.2. State Commitments

· Operators regularly send summaries (state commitments) to Cardano's main blockchain.
· These summaries include the current state, new transactions, and what the state will be next, all represented in a compact form using Merkle roots.

4.3. Challenge Period

· After an update is submitted, there's a waiting period called the challenge period.
· During this time, Watchers can check for any mistakes or fraudulent activities in the update.

4.4. Dispute Resolution

· If a Watcher submits a fraud proof during the challenge period, the system verifies it.
· If the fraud proof is correct, the bad update is undone, and the responsible Operator may be penalized.
· If no one raises a concern, the update is finalized and becomes part of the main blockchain.

5. Execution Framework

5.1. Midgard's Optimistic Rollup Architecture

At the heart of Midgard's functionality is its **optimistic rollup** architecture, designed to scale Cardano while maintaining its security.

This system combines several elements:

- **Validator Network:** Ensures transactions are processed correctly.
- **Efficient State Management:** Uses Merkle roots for concise and secure state tracking.
- **UTxO-Optimized Fraud Proofs:** Leverages Cardano's UTxO (Unspent Transaction Output) model for detailed and efficient fraud detection.
- **Balanced Economic Incentives:** Encourages honest participation and deters malicious activities.

5.2. Operator Network

- **Midgard implements an on-chain linked list of Operators** who manage the Layer 2 state and submit state transitions to Cardano's Layer 1.
- **Operators must deposit ADA into a bond contract** on Layer 1 to secure their role.
- The system uses a **rotating schedule** for Operators, giving each an exclusive turn to process Layer 2 events and commit their block of events.
- **Operators verify transactions**, **update the state**, **prepare state commitments**, and **submit** these updates to the Layer 1 State Validator smart contract.

5.3. State Management

- Midgard's state management revolves around a **State Validator smart contract** on Cardano's Layer 1, optimized for the eUTxO model.
- The system maintains three key components:
  1. **Current State:** Represents valid Layer 2 transactions and balances.
  2. **Incoming Transactions:** Transactions waiting to be processed.

3. **Next State:** The outcome after processing incoming transactions.

- These components are represented as **Merkle roots**, allowing for efficient state transitions and verification.