ANASTASIA LABS

Midgard

Non-technical Documentation

Contents

1. What is Midgard? 1

2. Understanding Layer 2 Solutions 2
2.1. The Need for Layer 2 2
2.2. How Layer 2 Works 2
2.3. Types of Layer 2 Solutions 2

3. Key Concepts 4

4. How It Works 6
4.1. Transaction Processing 6
4.2. State Commitments 6
4.3. Challenge Period 6
4.4. Dispute Resolution 6

5. Execution Framework 7
5.1. Midgard's Optimistic Rollup Architecture 7
5.2. Fraud Proof System 9
5.3. Types of Fraud Proofs 10
5.4. Seamless Integration with Cardano 11

6. Benefits of Midgard 12
6.1. Scale Up 12
6.2. One Honest Actor 12
6.3. High Security 12
6.4. Efficiency & Lower Transaction Costs 12
6.5. Seamless User Experience 13

7. Why Midgard Matters 14

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 to create compact and secure summaries of all activities, making it easy to keep everything organized.

5.1.1. 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.

5.1.2. 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.

5.1.3. UTxO-Optimized Fraud Proofs

- Leverages Cardano's UTxO (Unspent Transaction Output) model to efficiently detect and prove any dishonest activities without needing to review every single transaction in detail. This makes fraud detection faster and more effective.

5.1.4. Balanced Economic Incentives

- Operators earn rewards for processing transactions correctly, while Watchers earn rewards for successfully identifying and reporting fraud.Encourages honest participation and deters malicious activities.
- These incentives encourage honest participation and deters malicious activities, creating a fair and balanced system where everyone benefits from maintaining the network's integrity.

5.2. Fraud Proof System

A foundational component of Midgard's execution framework is the fraud proof system. This system ensures the integrity and correctness of transactions by allowing participants to challenge any invalid state updates. Here's how it works:

5.2.1. Challenge Period

After a state update is submitted, there is a designated time called the challenge period. During this time, participants (Watchers) can review the update and submit fraud proofs if they find any issues.

5.2.2. Submitting Fraud Proofs

To submit a fraud proof, a challenger provides evidence that a specific transaction or state transition is fraudulent. This involves presenting the original transaction data and secure summaries called Merkle proofs.

5.2.3. Challenge-Response Mechanism

When a Watcher contests the validity of a state update, both the Watcher and the Operator who published the disputed state must actively participate in proving or disproving the claim. If the Watcher's fraud proof is correct, the fraudulent update is canceled, and the Operator faces penalties.

5.3. Types of Fraud Proofs

To maintain the integrity of the system, Watchers can submit various types of fraud proofs. These proofs help ensure that all transactions are valid and that the system remains secure. Here are the different types of fraud proofs:

5.3.1. Value Not Preserved Proofs

Ensures that the total value of inputs and outputs, minus fees, remains consistent. Prevents situations where value is lost or incorrectly calculated during transactions.

5.3.2. Timestamp Misuse Proofs

Validates that transaction and block timestamps are within allowed ranges. Prevents manipulation of transaction times to gain unfair advantages or disrupt the system.

5.3.3. Improper Incentives/Fees Proofs

Ensures that transaction fees are calculated correctly. Prevents Operators from charging incorrect fees, ensuring fairness and transparency.

5.3.4. Double-Spending Proofs

Detects when the same UTXO is used in multiple transactions illegitimately. Prevents the same funds from being spent more than once, maintaining the integrity of transactions.

5.3.5. Invalid Signature Proofs

Proves that a UTXO is included in a transaction without the necessary cryptographic signature. Ensures that all transactions are authorized and secure, preventing unauthorized access.

5.4. Seamless Integration with Cardano

Midgard seamlessly integrates with Cardano's Layer 1 (L1) blockchain, ensuring that all off-chain transactions are secure and verifiable. Here's how it achieves this:

- **Smart Contracts:** Midgard uses smart contracts to manage state transitions, ensuring that every update is properly recorded and verified on the main blockchain.
- **Merkle Roots:** These compact representations are used for efficient proof submissions, making sure that off-chain transactions remain organized and secure.
- **Native Design:** Midgard's design is tailored specifically for Cardano, leveraging its unique features to optimize performance and security.

6. Benefits of Midgard

6.1. Scale Up

- Midgard significantly **increases Cardano's transaction capacity**, enabling the network to handle a much larger number of transactions at once.
- This prevents slowdowns and high costs, making Cardano capable of supporting a wide range of decentralized applications and services without compromising performance.

6.2. One Honest Actor

- Unlike many traditional consensus mechanisms that require multiple honest participants, Midgard requires only one honest, active participant at all times to maintain system integrity.
- This simplifies the security model and reduces the complexity of maintaining the network's trustworthiness.

6.3. High Security

- Midgard combines optimistic rollups, a specialized fraud proof mechanism, and economic incentives to ensure the system remains secure.
- The use of Cardano's UTxO model allows for detailed validation, making it difficult for fraudulent activities to go unnoticed.
- Watchers and Operators work together to maintain the integrity of the protocol.

6.4. Efficiency & Lower Transaction Costs

- By processing transactions off-chain, Midgard reduces the overall cost of transactions.
- The combination of optimistic rollups and efficient state management ensures that the system remains both fast and economical.
- This makes Cardano more accessible and cost-effective for users, encouraging broader adoption.

6.5. Seamless User Experience

- Midgard's complexity is abstracted away, allowing users to interact with Midgard-enabled decentralized applications (dApps) without needing to switch networks or perform manual bridging.

7. Why Midgard Matters

Midgard L2 plays a crucial role in enhancing the capabilities of the Cardano blockchain. Here's why it matters:

- **Speed & Scale:** Allows Cardano to handle a significantly larger number of transactions quickly, supporting more users and applications without slowdowns.
- **Lower Costs:** Reduces transaction fees by handling many processes off the main blockchain, making Cardano more affordable for everyone.
- **High Security:** Maintains strong security standards through a combination of technology and economic incentives, ensuring the system remains safe from fraud and errors.
- **User-Friendly:** Provides a seamless experience for users, eliminating the need for extra steps or complex processes when using Cardano-based applications.