Gem Chain Overview

dl@gemchain.org

`https://gemchain.org`

Introduction

Gem Chain is a high-performance, decentralized blockchain designed to provide fast, secure, and cost-effective transactions. Utilizing Delegated Proof of Stake (DPoS) consensus, Gem Chain ensures rapid block finality within 5 seconds, supporting a wide range of transactions including simple transfers, swaps, and limit order creations. The network's staking and fee coin, $GEM, plays a central role in its ecosystem, incentivizing validators and facilitating seamless transactions.

In addition to its core functionalities, Gem Chain offers sophisticated trading capabilities with support for marginal trading and perpetual futures. The blockchain's unique timestamping mechanism mitigates Miner Extractable Value (MEV) exploitation, ensuring a fair and transparent order execution process. Gem Chain is committed to providing a user-friendly experience, offering features like fee grants and simplified top-up processes to enhance accessibility and usability.

The following sections provide a detailed overview of Gem Chain's technical specifications, performance metrics, supported assets, and network architecture.

Parameters

- **Framework:** Cosmos SDK

- **Consensus Type:** Delegated Proof of Stake (DPoS)

- **Staking and Fee Coin:** $GEM

- **Address Format:** bech32 with "g" prefix

- **Block Time:** 5 seconds with instant finality

- **Transaction Throughput:**

    - Simple Transactions (e.g., Send): 100-200 per second
    - Swaps: Up to 100 per second
    - Limit Order Creation: Up to 1000 per second

- **Price per Send:** A few US cents

- **Price per Swap:** A few US cents

- **Limit Order Creation Price:** Zero

- **Limit Order Cancellation Price:** A few cents

- **Cross Chain Transfers:** Supported Assets: any TON blockchain jettons, Ethereum ERC-20 tokens and Solana Assets

- **Staking and Rewards:** Stake $GEM coins to validators to get rewards

Fee Grants

- Allows one account to delegate transaction fee payments to another account.

- Useful for users lacking tokens to cover fees or for organizations sponsoring user fees.

- Grants have specific limits, such as maximum fee allowances or expiration dates, recorded transparently on the blockchain.

Advanced Trading Features

- **Gem Chain v2:**
  - Marginal Trading (up to 50x)
  - Perpetual Futures

- **Order Types:**
  - Deposit and withdraw funds from TON and EVM compatible networks
  - Make orders in decentralized order book
    * Short-Term Orders: For programmatic, low-latency traders with shorter expirations
    * Stateful Orders: For retail traders with longer expirations, exist on chain
  - Timestamp-Proven Orders: To mitigate MEV
  - Support of Marginal Trading

User-Friendly Features

Gem Chain aims to enhance user experience by providing features that simplify interactions with the blockchain. One such feature is the use of deposit addresses associated with each user to streamline the top-up process.

- **Personalized Deposit Addresses:** Each user is assigned a unique deposit address, making it easy to add funds to their account. This eliminates the need for users to generate a new address for each transaction, simplifying the process of managing their assets.

- **Streamlined Top-Up Process:** Users can quickly and easily deposit funds to their account by sending assets to their personalized address. This reduces the complexity and potential errors associated with copying and pasting addresses for each transaction.

- **Enhanced Security:** By using a consistent deposit address, users reduce the risk of errors in address entry, which can lead to loss of funds. It also helps in avoiding phishing attacks where malicious actors provide incorrect deposit addresses.

- **Convenient Fund Management:** Users can manage their deposits more efficiently, tracking their transactions and balances with greater ease. This feature is particularly beneficial for frequent traders and those who regularly interact with the blockchain.

Lifecycle of an Order

1. User places a trade on a decentralized front-end or via API.

2. The order is routed to a validator, which gossips the transaction to other validators and full nodes.

3. The consensus process selects a validator to propose the next block.

4. The proposer matches the order and adds it to the proposed block.

5. The block proceeds through the consensus process:

   - If 66%+1 of validators approve, the block is committed and added to the blockchain.

- If the block is rejected, the process restarts.

6. Committed blocks update on-chain and off-chain data, which is streamed to Indexers and made available via API and Websockets.

Trades Ordering

- Validators timestamp orders to prevent MEV exploitation, maintaining an unchangeable order of transactions.

- Timestamping is power-weighted by stake, ensuring reliable validators have significant influence.

Enabled Cosmos SDK Modules

- Auth - Authentication of accounts and transactions for Cosmos SDK applications.

- Authz - Authorization for accounts to perform actions on behalf of other accounts.

- Bank - Token transfer functionalities.

- Crisis - Halting the blockchain under certain circumstances.

- Distribution - Fee distribution and staking token provision distribution.

- Evidence - Evidence handling for double signing, misbehaviour, etc.

- Feegrant - Grant fee allowances for executing transactions.

- Governance - On-chain proposals and voting.

- Mint - Creation of new units of staking token.

- Params - Globally available parameter store.

- Protocolpool - Functionalities handling community pool funds.

- Slashing - Validator punishment mechanisms.

- Staking - Proof-of-Stake layer for public blockchains.

- Upgrade - Software upgrades handling and coordination.

- Consensus - Consensus module for modifying CometBFT's ABCI consensus params.

Network Nodes

- **Validators:** Responsible for storing orders in an in-memory orderbook, gossiping transactions, and producing new blocks. Validators propose blocks and achieve consensus with at least 66%+1 approval by stake weight.

- **Full Nodes:** Do not participate in consensus but maintain a complete view of the blockchain, processing each new committed block and participating in transaction gossiping.