**Security Mechanism**

Created by Hgminerva

**Introduction**

Xode Parachain implements robust block verification and transaction security mechanisms through cryptographic validation, consensus protocols (AURA & GRANDPA), and relay chain verification. These mechanisms ensure transaction integrity, prevent fraud, and provide economic security within the Kusama ecosystem.

**Security Mechanisms**

**Consensus Mechanisms: Xode Parachain uses a hybrid consensus approach**

* AURA for Block Production: Ensures liveness by providing a round-robin block production method, with validators selected to produce blocks in a defined order.
* GRANDPA (GHOST-based Recursive ANcestor Deriving Prefix Agreement) for Finality: Ensures finality by reaching consensus on a chain of blocks.

**State Proofs and Fraud Prevention**

* Merkle Proofs: Used for efficient and secure storage verification.
* On-Chain Governance and Runtime Upgrades: Prevents unauthorized changes through democratic decision-making.

**Cross-Chain Security (XCMP and HRMP)**

* XCMP (Cross-Chain Message Passing): Ensures secure communication between parachains.
* HRMP (Horizontal Relay-routed Message Passing): A temporary message-passing protocol ensuring message integrity.

**Economic Security**

* Slashing Conditions: Validators and collators can be penalized for misbehavior (e.g., double signing, downtime).
* Transaction Fees and Weight-Based Execution: Prevents spam and DoS attacks.
* Bonding and Staking Requirements: Ensures validators have a financial stake in the network.

**More Information**

**Xode Staking:** <https://wiki.xode.net/app/page/1WwBLI00nnQu8IDGQ8EiPRcVJ0PfXElBzTpyazBc4RtA?p=14_D9JXPSHF8yCRxMoqLaC6ne0PeKgfwX>

**Polkadot Security Protocol:** <https://wiki.polkadot.network/docs/learn-parachains-protocol>