

Security

PoS

The Quasar blockchain is built with and secured by the Tendermint consensus engine. Tendermint is a proof-of-stake (PoS) consensus algorithm designed with Byzantine Fault Tolerance (BFT), meaning that it is able to operate reliably even if up to $\frac{1}{3}$ of its nodes fail or act maliciously. Validators can participate in committing blocks to the blockchain by staking a required sum in QSR.

Tendermint consensus works by offering the opportunity to commit a block to a randomly selected validator at regular intervals. Validators can increase their chances of being selected by staking more QSR. Upon successfully generating a new block, the validator receives a portion of transaction fees from the network as a reward. If a selected validator is unavailable or acts maliciously, they are penalized (referred to as slashing) and lose a portion of their stake.

Non-validator QSR holders can delegate their QSR to validators to share in a portion of rewards for successful block generation (and slashing penalties when a selected node fails). These incentives promote security by encouraging greater decentralization of the liquidity powering the consensus layer, making it significantly more difficult for a validator or group of colluding validators to disrupt the network.

Vaults

To create a new vault, creators are required to delegate a minimum amount of QSR to a network validator. Importantly, this requirement incentivizes vault creators to align with validators on the objective of a healthy and secure Quasar chain. This prevents coordinated attacks to devalue QSR and compromise consensus-level security.

You can read more about how requiring QSR for vault creation contributes to chain-level security in the QSR section of our documentation.

Cosmos SDK and CosmWasm

The languages used by Cosmos SDK and CosmWasm, Golang and Rust, are general-purpose, type-safe, and widely audited. CosmWasm was designed to preclude reentrancy attacks, a major class of exploits to which Ethereum smart contracts are vulnerable. This is discussed in greater detail under the actor model section of Quasar's documentation. The Cosmos SDK also utilizes an object-capability model which confines code implementations to their intended use cases by preventing unnecessary rights from being included with shared objects by default.

Security Audits

We are regularly audited by Halborn, an award-winning blockchain cybersecurity firm. They evaluate our blockchain and smart contracts to identify and eliminate any vulnerabilities, bugs, or possible exploits. They deliver detailed reports of their work which we generally make publicly available. Additional testing is also being provided by Lightshift Capital. Quasar has also partnered with the cybersecurity firm Groom Lake for additional monitoring and security for our off-chain processes.

[Previous Ecosystem](#) [Next FAQ](#) * [PoS](#) * [Vaults](#) * [Cosmos SDK and CosmWasm](#) * [Security Audits](#)