Private smart contracts - overview

Secret Contracts are enabled by the “compute” module of the Cosmos SDK, and execute over plaintext while still allowing for encrypted inputs, outputs, and states because of trusted and verifiable computations. Consensus with an encrypted state is reached by using shared secrets amongst the validator nodes of the network.

In this part of the documentation, we highlight the flow of data for interactions on the secret network and dive into the design of Secret Contracts and their differentiations from standard CosmWasm contracts.

Public binary

A Secret Contract’s code isalways deployed publicly on-chain , so users and developers know exactly what code will be executed on submitted data. However, the data that is submitted is encrypted, it cannot be read by a developer, anyone observing the chain, or anyone running a node. If the behavior of the code is trusted (which is possible because it is recorded on chain), a user of Secret Contracts obtains strong privacy guarantees.

Encrypted input, output, state

The encrypted data canonly be accessed from within the “trusted execution environment” , or enclave, that the compute module requires each validator to run. The computation of the Secret Contract is then performed, within this trusted enclave, where the data is decrypted. When the computation is completed, the output is encrypted and recorded on-chain.

Want to learn more about the encryption specification of the contract state? - Read the technical specification on Contract state encryption[here.]

The CosmWasm framework

Secret contracts are an altered version of the CosmWasm Rust based smart contract framework and share many resemblance. The contracts written in Rust compile to a Wasm binary that is than run by the Wasmd module of the cosmos SDK. The version of Secret is altered in such a way that all executions are done inside the secure enclave requiring additional data verification and more.

This also means queries of the contract state or contract execution are permissioned to only the signer of the transaction themselves. Contract state queries requiring opening up the VM in the enclave and are therefore more intensive to run than generic plaintext cosmos-sdk queries.

Want to learn more about the scalability implications of Secret contracts or access control? - Read on in the[Contract fundamentals section.]

Last updated9 months ago On this page *[Public binary] * [Encrypted input, output, state] * [The CosmWasm framework]

Was this helpful? [Edit on GitHub] [Export as PDF]