TPS and scalability

Max gas per block

As explained in the Gas and fee section Secret computational load is denominated in gas . The amount of gas that can be spend at every block is capped via the max_gas block parameter. This cap is currently set at 6,000,000 (6 million) gas meaning a block will never contain more computational load than what is represented by 6 million gas. The computational load per gas unit is calculated and then denominated in the chain binary.

You can find the Gas settings for Secret Network in the Network code here [SDK/Go message types] , [Wasm messages]

Expected block time

The max_gas parameter is chosen in such a way that validators can ensure they process the full computational load within the target block execution time (~6s). If this computation and expected blocktime don't align the blocks will become longer and longer as they await 66% of voting power to sign the block. When block time increases the TPS of the blockchain drastically decreases only complicating the situation further.

You can read more about this interplay between blocktime, TPS and scalability in this post mortem of the Shade airdrop .

Encryption overhead

One can expect the overhead of all enclave and encryption transactions to be roughly 30% over a vanilla wasm engine. This overhead comes from the decryption and re-encryption done in the enclave and the varying verification's that are required of the message input data. This overhead does not exist for standard SDK messages like "stake", "transfer", "vote" etc.

Additionally Secret leverages an older engine for the wasm VM dubbed "Wasm3". The vanilla engine "Wasmer" is roughly 10-15x more performant. This engine is not yet supported as there is no Enclave compatible version, development effort to support it though is underway as listed in the core roadmap .

Transactions per second

Because of above factors the TPS of Secret is limited in comparison to vanilla Tendermint and Cosmos SDK benchmarks. Based on an average of 100.000 gas for a contract interaction (something like an NFT mint or non-routed DEX swap) Secret can process 60 TXs per block which at ~6s per block 10 WASM transactions per second. SDK interactions take a lot less gas meaning the overall TPS of Secret in practice is ~25.

As explained in the above section this number can still be significantly increased by upgrading the WASM engine but has proven sufficient so far in periods of high demand

Enclave Queries

Important to note is that Queries related to contract state require the API node to access the enclave, these are therefore more resource expensive than SDK queries. Secret API infrastructure needs to be scaled accordingly to fit heavy load user interfaces. One can expect to require more Secret API nodes than standard Cosmos API nodes for a similar application.

As transaction complexity overhead decreases with better engines so does increase the ability for a node to process queries. Verified queries on Secret have already become a hundred times more performant with 1.4-1.6 upgrades, and with the current community API they are in a very stable spot.

Scalability

Short term scalability improvements can come from a WASM engine replacement and increase in Light client verification methods so to lower the enclave load. Also storage access can become more performant with an SGX backend change which is on the short term roadmap.

Long term Secret does not have to worry about blockspace with the plenty opportunities of replicated security and the cosmos sdk. For more on the core development roadmap check out the documentation here .

Last updated 7 days ago On this page * Max gas per block * Expected block time * Encryption overhead * Transactions per second * Enclave Queries * Scalability

Was this helpful? Edit on GitHub Export as PDF