Hello to the Secret community!

Yesterday afternoon (Feb 21, 2022) we started seeing impacted network performance stemming from the launch of the Shade airdrop. Things are already improving, but we want to explain what happened and what users can now expect. In this post, we'll outline:

1. What exactly happened
2. Why these issues arose
3. What fixes are being made now
4. What improvements will be made longer term

Thanks to the SCRT Labs team for their contributions to this post.@Cashmaney @assafmo

What's Happening?

On Feb 21, 2022 at around 11pm UTC the Shade protocol airdrop was launched, drawing a lot of attention to Secret Network.

As a part of their airdrop mechanism, Shade heavily utilized secp256k1 signature verification in their contracts, which is very computationally expensive.

These transactions are causing blocks to slow down due to the time required to compute each block, causing the mempool to fill up which delays the execution of transactions. A further effect of blocks that take a long time to compute is that queries are slowed down as well, as currently a node cannot both compute a block and serve a request.

It's important to realize that these were known issues, and we are already in the process of making improvements on both fronts.

Why Did This Happen?

The reason for the abnormal behavior is mostly due to nodes running an outdated WebAssembly engine, which does not handle long computations very efficiently. Also, gas calculations do not account for this inefficiency, which further compounds the issue.

What's Being Done?

Firstly, we are in the final stages of testing a release which will greatly improve query performance - this will allow nodes to both serve many more requests, and lessen the impact of long block computations. This will help services like Keplr stay available during network-wide events. This will also not require a hard-fork, so node runners will be able to apply it immediately.

Secondly, we are working to improve execution performance. Expensive functions like secp256k1 verification will be exposed to contracts (instead of being executed inside the contract) which will make them much more efficient. We are also replacing our WASM engine with a newer, more performant one.

Lastly, we will also be re-evaluating gas calculation and pricing and try to adjust the gas to more accurately reflect the computational cost of each contract.

What Happens Next?

Short term:

1. Query node upgrade will be released in a few days.
2. Working more closely with airdrops & large projects to make sure things are smooth and efficient given network limitations

Longer term:

1. Network upgrade (hard fork) that will let contracts take advantage of fast, built-in building-blocks for contracts and a better contract execution engine

Discuss!

This is an open thread for discussion by validators, users, and developers on their observations, possible next steps, open questions, and other comments. Please be respectful and constructive - our goal is to get everything working at full capacity ASAP (and to expand that capacity!)