Hi!

We’re pretty close to finalizing our encryption protocol:

github.com

enigmampc/EnigmaBlockchain/blob/master/docs/encryption-specs.md

Implementing the Secret in Contracts

:warning: This is a very advanced WIP.

This file has been truncated. show original

This^ document includes:

1. Bootstrapping the network
2. Registration of new nodes
3. Contracts state encryption
4. Contracts inputs and outputs encryption

Still not finished:

1. How network upgrades can occur without losing state and tx input/output history.
2. How to generate contract_id

in a trusted way, to prevent two contracts having the same encryption key (this section).

We’d love to get your feedback on this!

So please ask us hard questions, including about all of the “TODO reasoning” and about attack vectors.

List of previous discussions: https://github.com/enigmampc/EnigmaBlockchain#implementation-discussions