

hi

is it possible to have an Aztec contract that stores a secret value that will be made public only after a requirement is met?

requirement can be an ETH L1 block.header with timestamp > the year 2024.

Would it be safe to assume that only the owner(s) of the contract source code would be able to “cheat” to get the value out? or not even with that if the secret value is initialized on another contract?

Is this still “cheatable” in any other way? (i.e. by the “sequencer”)