In this earlier post we discuss how to allow private functions to read historic or constant public state. Would it be possible to let private functions read current

public state

as well? This would be useful, for example, whenquerying the current implementation of an upgradeable contract

The main issue with this is that public state can change over time, so the private function would need to “nail down” the values it depends on. Any changes to those public values would render the tx invalid, so a private tx would need to include a list of the public slots with their expected value for the sequencer to check before it accepts it. Note that checking the public state tree root would not work, since it changes too often, and checking any node lower in the tree already leaks information.

However, by publicly announcing what public values a private tx depends on, we’re leaking a lot of information. Is there a cryptographic magic we could use here to express this dependency, in a way that it’s easy to check by the sequencer, but without revealing info on what fields are actually being checked? Could something like OMR help here?