Hello,

Leo here from Sismo, we are building private attestations on Ethereum.

I’m still fairly new to ZK but have been diving in these past weeks.

After seing this old tweet from Justin Drake I realized I was not the only one hoping for a snark/stark friendly hash function (Pedersen, Poseidon, MiMc, …) for the World State Trie of Ethereum.

I’d be grateful if someone could point me to latest advancement on this topic!

Has someone ever thought about the strategy to modify a fullnode/archive node client so it maintains a second World State Trie, friendly to snarks and update its root regularly onchain?

We could very well imagine a set of nodes maintaining such a State Trie?

Would really appreciate any feedback about this idea or resources on alternatives to get access to the Ethereum state within ZK proofs, thanks!