Hey everyone,

We at Panther published our SNARK paper earlier this year (https://eprint.iacr.org/2023/1255.pdf), as well as a follow-up paper (https://eprint.iacr.org/2023/1264.pdf). This scheme circumvents the overhead of non-native field arithmetic arising from Ed25519 signatures.

Right now we survey some approaches to IBC light clients via Snarks. The implementation uses a 570-bit outer curve to Ed25519 constructed via the Cocks-Pinch algorithm.

The prover time for a million gate circuit on a 64 vCPU AWS machine's 32 seconds for the version optimized for the proof size and verification time, and 20 seconds for the version optimized for the Prover time.

I am wondering if 100 blocks within ~ 90 seconds / 1 minute is efficient enough for the Snark to be useful within the given context outlined above, and if someone here has a use for this work.

We are currently working on a piece describing an IBC scheme related to our earlier work.