Hi!

I’m part of the AZTEC protocol team, and I thought I’d share our working proof of concept zero knowledge circuit on mainnet, which was created by Dr Zac Williamson. It uses range proofs and homomorphic encryption to validate notes and transactions.

The main advancement compared to similar past effort is it’s efficiency, currently sitting at around 800’000 gas per validated proof on main net.

GitHub

AztecProtocol/AZTEC

Public repository for the AZTEC protocol. Contribute to AztecProtocol/AZTEC development by creating an account on GitHub.

To demo, we’ve deployed a contract which creates confidential DAI.

Looking forward to questions and comments!