ZK Bootcamp: Day 6 Problem Set

Brian Justin Stout*

August 4, 2023

Problem 1. *Discuss in your teams the need for confidential tokens.*

I think there is more need for private computation than private tokens or private transfers of value.

Problem 2. *Have you/ do you want to use Zcash or other confidential tokens?*

I have sort of used ZCash. I've gotten free drips from some faucets, but I've never purchased it or mined it. I think it is cool and would be interested in mining it just for the fact that I'm interested in the idea of construct ZKPs in return for tokens. I am less interested in pure payment applications, though.

Problem 3. *Discuss the future for Axtec and private transactions on Ethereum in light of what has happened to Tornado Cash.*

I think of Tornado Cash as being more of an obfuscation tool than a privacy tool. I think peer to peer privacy and private computation are less at risk than a tool like Tornado Cash. I think it is clear that Aztec was concerned, because they made a major product shift. I'm not sure if that was in response to direct communication, though.

*email: bjstout@proton.me