

no particular order/coherence, just liveblogging:

Leor Fishman, [8/9/2022 7:09 AM]

@guyzys

disagree that zk complexity is high with stuff like aleo

Leor Fishman, [8/9/2022 7:09 AM]

actually ima just liveblog my thoughts here

Leor Fishman, [8/9/2022 7:09 AM]

computational cost for generic MPC is not

low-medium lmao

Leor Fishman, [8/9/2022 7:10 AM]

you need to recompile your circuits into either addition/multiplication or yao's, it's a mess

Leor Fishman, [8/9/2022 7:10 AM]

it's at least as high as ZK compute cost

yep, well put point about blockchains doing trustless correctness and needing zk/MPC/FHE to do trustless privacy

ah, and that's it, ok