Time: 15:00-18:30

- 15:00-16:20 Open Source Hardware - Why, what, how
- 16:30-16:55 ETH++: A roadmap to (real) decentralization in a world of centralized power (DevCon Mainstage Talk - Phil Daian)
- 17:00-18:30 Open source hardware role in bringing network states on-chain

Location:

DevCon Venue

t/acc Contributors: Quintus Kilbourn (Flashbots), Mateusz (Flashbots, Nethermind), Michael Gao (Fabric Cryptography)

Every piece of software runs on a physical substrate. Software has eaten the world on the foundation of hardware which now underpins our societies. Every time we step in a car, use a hardware wallet, a password manager, validator or even a pacemaker - we trust with our digital identities, data and lives. We want to make hardware trustless to remove this unspoken profound reliance on a few hardware companies which also constitute nation state attack vectors. We also want trustless hardware because TEEs and other primitives that leverage remote attestation promise to greatly enhance our cryptographic toolkit for decentralisation.

To arrive at hardware, the use of which does not demand strong trust assumptions, we need to solve 2 problems

1. improved imaging technology which can make the physical chips legible to us
2. arriving at a trustworthy public reference (“blueprint”) against which we can compare our chip images and which can be traced back to auditable chip logic

To achieve the same for remote attestation, we need to solve 2 more problems

3) attaching keys to hardware without giving even the manufacturer access to these keys

4) developing remote attestation protocols so that users who have never been in physical contact with a machine can be assured of the trustworthiness of the hardware

Today we want to focus on problem 2, which is in large part a question of open source technology, but could also benefit from some clever cryptographic tricks.