Recently, there's been a lot of excitement around TEEs as a means to bolster security for applications in the "crypto"/blockchain space. TEEs in their current form can already add a lot of value to use cases by providing some guarantees where there were none before or adding collusion resistance to committee-based approaches.

However, current TEE's were not designed with web3 use cases in mind and consequently leave much room for improvement. A group of researchers within Flashbots has set out to realise a TEE which more thoroughly enables the decentralised ethos and goals of the crypto industry. More specifically, such a new design would satisfy:

- decentralised security model:

current TEE security models completely fail if a single party (like the manufacturer) does not behave according to the specified protocol. There are no ways of verifying that current TEEs were constructed correctly and that key material is indeed private. Any manufacturer of sufficient sophistication should be able to produce the hardware (requiring open source designs) and the security of the TEE should not be vulnerable to the whims of any individual party. Essentially, we aim for a decentralised root of trust.

- physical tamper resistance:

TEE designs have seen a cat-and-mouse game over the last few years as vulnerabilities are found and patched. While this process represents progress, no suitable TEE (to the best of our knowledge) is resistant to the presence of a physical attacker. In order to remove trust in cloud providers, TEEs must provide guarantees against even physical attackers.

Note: these requirements are hard enough as they are. To make this easier we are willing to target more narrow use-cases like running the EVM.

We are certainly unable to complete this mission on our own and plan to rely heavily on security communities broadly. In order to do so, we are progressively moving the work in this direction into the open. Our first goal is to produce a position paper to communicate the problem and its importance to the broader hardware research community.

Please, let us know if you'd like to contribute in one way or another

Relevant Pages

First and foremost, I highly recommend, Sylvain Bellemare from IC3's[living draft] giving a more elaborate explanation of this line of thinking.

Other pages:

- [Taxonomy of TEE attacks]
- [Project T-TEE reading list]
- [Destructive Hardware Trojan Detection Protocol Brainstorming]