

Related to Decent – We are running on an unpermissioned chain, want to not rely on centralized storage and want to run a proprietary claim analysis algorithm in a fully decentralized setting that I don't want to make public.

I assume that I have to sign any code (algorithm) going into the TEE, is that correct?

Assuming that there is some Diffie Hellman scheme in place, I'd like to encrypt the code (algorithm) and pass it to the TEE, making it such that I only trust the TEE and myself to know what my code is. I feel like you have all of the building blocks for that.

FYI, I'm not near ready to build this. But it is an important high level use case that I plan on addressing in our WP.