I have been working on a protocol for tokenizing device security.

Currently there is no in-protocol disincentive for hardware wallet manufacturers to introduce backdoors in the wallet. If the wallet uses Blade protocol, the wallet manufacturer's stake will be slashed in case the wallet's deviation from protocol is proved on-chain.

Also this device can be used as a pseudo Trusted Execution Environment (even though the hardware is not a true TEE). And it allows creation of applications where user is not allowed to cheat (such as payment channels). Since it is not possible for users to cheat, such payment channels don't need settlement periods.

For a short explanation of protocol and how to create instantly settled payment channel, please check my medium article: https://medium.com/@hrishikeshio/blade-protocol-how-to-create-instantly-settled-payment-channels-4d4f5b16ccbc

For more in-depth explanation, please check out my whitepaperhttps://github.com/hrishikeshio/blade (currently in draft stage)