Hello everyone,

There is one particular topic that cannot go out of my mind, hopefully some of you have good solutions.

The topic is about users interacting with Dapps. If you quickly think about the layers that lie between the user and the smart contract, you have the frontend (through react, angular etc…) a bridge provider and the wallet.

The problem that I see, is that we are not focusing enough on the frontend's security. Most of the security's efforts goes to the smart contracts (this is completely fine) but leaving off guard the user's main contact interaction.

There has been multiple hacks because of this issue, we saw the sushi-swap:SushiSwap's token launchpad, MISO, hacked for $3M and there are multiple web-site clones that imitate the exact look & feel of the original one.

There a couple of assumptions that we need to take in consideration to understand the gravity of this problem:

1. The majority of the users will not check the details of the transaction.

2. Front end code is likely to be vulnerable.

3. The source of truth for the users is what they see on the frontend.

Users today trust the brands more than the protocol, they do not audit the contracts, they care about good "brands" like uni swap, aave etc…

The problem with all of this, is that if you have access to the frontend code, it becomes extremely easy to trick the user to deposit funds to another address.

There must be a way to guarantee that what you are signing is what you are "seeing", most likely, this would be a job that the wallets would need to be a part of.

Anyway, if any of you are working in something related to this, I would be very interesting to fund it and cooperate.