Hi, I would like to make some suggestions for ETH, my English is not good and I am not very good at writing the underlying design of ETH, but I would like to make an idea.

I would like to ask if the future of ETH can develop a non-smart contract-like multi-signature wallet, users can upgrade their addresses to this non-smart contract multi-signature wallet, this upgrade can also set the release time, to prevent the multi-signature address control private key is lost, after a period of time can still operate through the original private key, with the development of ETH users can be in any unexpected place will leak their However, with the development of ETH, 0x address has become the address of too many Web3 applications, which may bear too much on one address, such as some future airdrop or binding application account, etc. If the leakage of private key or helper word occurs, it is a very troublesome and difficult thing to change or reduce the loss one by one, and now there are some private key mining tools, although the probability is very small. But in this case, even if the private key is saved, the address may still be lost.

I don't know if I'm wrong or where I read it, but Vitalik once said that he didn't expect ETH to take on so many financial applications, so I think the impact of this problem will be much less if we can support multi-signature addresses for non-smart contracts. vitalik once mentioned social recovery, but I always think this is still a centralized solution, only a compromise solution, not perfect. It is not perfect.

Further, if ETH can add the inheritance function, set a time period if the account is not used for a long time, it can be transferred to a specified address, similar to the change of public key in EOS, but what I hope is similar to the inheritance function, this function will make it easier to distribute the legacy in the traditional sense, and combined with the multi-signature function, it can also have more control over the ownership of the legacy.

The public key generated after the import of the new private key inherits the identity of the previous address, you can use the identity of the previous address to log in to dapp. although this function will definitely be used to steal the number after a quick change of ownership, so the use of this function can limit the time and constrain the wallet for mandatory reminders to carry out specific operations can be released from the inheritance function, when issuing a request to inherit more than how much time the account will be inherited, this time can be set to at least one year, I think this time cost is not what hackers are willing to wait for, even if the private key is leaked, this function will not help hackers to complete the account looting. Although the main task of ETH now is to upgrade, I still hope to see these features on Ether in the future, these features can be the icing on the cake

What I wrote may be conflicting in logic or underlying architecture, if you also agree with my idea then ah, please help me to improve this idea, thank you.