Hello,

I'd like to discuss a way to increase the security of Ethers stored for Casper POS.

A large number of Ethers will be necessary to run a Casper node. As a result, security is a very important issue.

The problem with the proposed implementation is that Ethers will be locked in a smart-contract, which will have the power to inflict penalties.

It means the smart contract will be able to withdraw Ethers from the account.

If something happens, such like a mistake, hacking, virus, middle man attack, spectre attack or anything you can imagine, Ethers might be stolen or lost.

At the same time, there is a very safe and reliable way to improve the security of Ethers stored for POS.

There are currently dozens of successful POS Masternode cryptocurrencies, which also require the deposit of large amount of coins, but in a safe way called "cold storage wallets".

Masternode coins become more and more popular, with several dedicated websites https://mntop.co.in , https://masternodes.pro , …

To run a masternode, you have to deposit the required amount of coins (for example 1000 coins), on an account.

It is very safe because you never have to disclose the private key of this account, nor have to sign anything with the private key.

In my opinion, the private key of the account on which huge amounts of coins are stored should never be disclosed until you decide to sell the coins. The private key should be kept safe, on a computer disconnected from the internet, or on a paper wallet. This is cold storage, which is the safest option possible.

As regards the way to implement cold storage security in Casper, just copy the masternode implementation. In order to run a Casper Node, just ask a large amount of Ethers to be deposited on an Ethereum account, without signing any smart contract with the private key.

In order to solve the "nothing at stake" problem, just implement an additional contract : for example, if the ethereum deposit is 1 000 Ethers to run a masternode, just pass a smart-contract on another account on which a small amount of Ethers would be locked (for example 10 Ethers).

The penalties would be applied on these 10 Ethers, without endangering the large deposit of 1 000 Ethers, which would benefit from cold storage security, the private key having never been disclosed in any way.

This implementation has many other advantages, besides from security :

- the large amount of Ethers could be withdrawed at any time, since it wouldn't be locked in any smart-contract. The node would just be disconnected from the network.
- reach enough decentralization : if Casper is implemented without maximum security of deposits, I fear only the very core of early holders will run a Casper node, that's to say those who have so many ethers that they can afford to lose 1 000 ethers in case something went wrong. Many secondary investors would feel unsafe to put at stake such large amounts of Ethers, without cold storage. So the system would be very centralized.
- reliability : masternode coins are well established, it's always a good thing to benefit from proven solutions.
- boost in Ether price : cold storage masternodes are very popular, so implementing this solution in Casper would give an additional boost to the price of Ethers.