Today, we believe mining pools in Casper are hard.

If people join a mining pool, they take the risk of losing the money.

However, what if people can securely

join a mining pool in Casper (proof-of-stake)?

Background:

In Casper, people mine according to their deposits, people with bigger deposit have a higher possibility of being selected.

If people join a mining pool, they need to deposit their money to a third-party. It is possible that the third-party takes the money away and does not give the deposit back.

Opportunity:

Intel SGX is a new hardware technology that provides secure execution with confidentiality and integrity. And it can prove such security to any third party.

We can verify a piece of the code be securely run by a machine. The operating system in this machine cannot steal or tamper the information in this execution.

Issue:

It seems possible to build a secure mining pool by Intel SGX, where people will not lose their money. With such a security guarantee, it is possible that people can securely join a mining pool, and will do so.

Why mining pool?:

I guess many people have coins, yet not being online to mine. If they can delegate this to a mining pool, they do not need to be a full node, and they do not need to be always online.

And another benefit for any pool: even if one’s deposit is small, it is still possible to earn some share – you are consistently making a profit.

Possible security problem:

I am not sure whether a mining pool in Casper can cause problems – have a preference for selecting the next miner?

Existing Casper mining pool:

https://www.rocketpool.net/ But they have not yet considered SGX.

please give more ideas, comments!