Today a validator must remain connected and secured against hacking: a hacker could disconnect a node from the network or lead the validator to sign invalid blocks, making it slashable. Remaining connected can be problematic for some countries. Iran recently cut its Internet connection for 5 days. It's generally accepted that China could cut its Internet network from the rest of the world as well. Russia is also aiming at this. A possibility for these users is to join a staking pool. The staking pool will take of the connectivity and security. However, it is not a trustless solution: the staker has to trust the staking pool. While it is possible to ensure that the staking pool cannot unlock the funds, the staking pool can still lose all the funds because of the slashing & leaking mechanisms: the staking pool can have bugs or can be hacked. Moreover the staking pool must remain up and cannot cut its services for 2 weeks like an exchange can when something goes wrong. We can also imagine a staking pool threatening its users to be voluntary slashed if they don't pay a fee.

In other words, it would be great if a user could stake its funds without having to trust the staking pool, regardless of what happens. The staking pool would take the risks (i.e. slashing/leaking/hacking) for the user against a cut on the rewards.

This can be implemented with a protocol change which adds 3 mechanisms:

1. The staker's funds are locked, but the staking pool does not have access to these funds. Only the staker can unlock these funds (with a long delay as today).
2. The funds slashed/leaked are not the funds locked but funds owned by the staking pools.
3. There is ratio between locked funds and slashable funds. That corresponds to a leverage effect. 1% seems economically reasonable. If there are more locked funds than leveraged slashable funds only the first locked funds are used for slashing.

To illustrate, we can imagine a scenario like this one:

Locked funds

Slashable funds

Initial start: 1000 users

32000 (32 *1000)

320 (32*1000* 0.01)

Event: 1 validator in the pool is slashed with many others from other pools, hence get slashed by 32 ETH.

32000

288 (320-32)

Now the mining pool has only 900 validator slots (288 / .32)

Event: the staking pool transfers 112 ethers to the slashable funds wallet.

32000

400

Now the mining pool has 1000 validator slots again.

Event: The mining pool stops participating for 1 day.

32000

398 (400-0.002 * 1000)

Event: The mining pool is hacked and use its validating power to create slashable conditions.

32000

0 (max (0, 398-1000*32)

There are two impacts:

- The number of validators can vary a lot because of the leverage.
- The cost of acting badly is divided by 100 for a mining pool. Has it really an impact? That's doubtful.

We can compare this to today's mining pools: one can buy a set of GPUs and participate in a mining pool:

GPU Mining

This staking

Investment

A set of GPUs

32 ETH

Infrastructure

Network / Site

No infra

Daily cost

Electricity

0

Financial risk if the pool misbehaves

Electricity + Amortization of the GPUs

0

Daily to leave the pool (for example if the pool misbehaves)

No delay

Months

Of course, anything that helps staking pools could be suspected of pushing for centralization. But with this mechanism anyone can create a staking pool, as the participants are not taking any risk by joining a staking pool without an established reputation.