Combine DV private key shares

danger Reconstituting Distributed Validator private key shares into a standard validator private key is a security risk, and can potentially cause your validator to be slashed.

Only combine private keys as a last resort and do so with extreme caution. Combine distributed validator private key shares into an Ethereum validator private key.

Pre-requisites

- Ensure you have the.charon
- directories of at least a threshold of the cluster's node operators.
- Ensure you havedocker
- installed.
- Make suredocker
- is running before executing the commands below.

Step 1. Set up the key combination directory tree

Rename each cluster node operator.charon directory in a different way to avoid folder name conflicts.

We suggest naming them clearly and distinctly, to avoid confusion.

At the end of this process, you should have a tree like this:

tree ./cluster

cluster/ ├── node0 | ├── charon-enr-private-key | ├── cluster-lock.json | ├── deposit-data.json | └── validator_keys | ├── keystore-0.json | ├── keystore-0.txt | ├── keystore-1.json | └── keystore-1.txt ├── node1 | ├── charon-enr-private-key | ├── cluster-lock.json | ├── deposit-data.json | └── validator_keys | ├── keystore-0.json | ├── keystore-0.txt | ├── keystore-1.json | └── keystore-1.txt ├── node2 | ├── charon-enr-private-key | ├── cluster-lock.json | ├── deposit-data.json | └── validator_keys | ├── keystore-0.json | ├── keystore-0.txt | ├── keystore-1.json | └── keystore-1.txt .. . └── node* ├── charon-enr-private-key ├── cluster-lock.json ├── deposit-data.json └── validator_keys ├── keystore-0.json ├── keystore-0.txt ├── keystore-1.json └── keystore-1.txt caution Make sure to never mix the various.charon directories with one another.

Doing so can potentially cause the combination process to fail.

Step 2. Combine the key shares

Run the following command:

Combine a clusters private keys

docker run --rm -v "(pwd):/opt/charon" obolnetwork/charon:v0.19.1 combine --cluster-dir /opt/charon/cluster --output-dir /opt/charon/combined This command will store the combined keys in theoutput-dir , in this case a folder namedcombined .

tree combined combined ├── keystore-0.json ├── keystore-0.txt ├── keystore-1.json └── keystore-1.txt We can verify that the directory names are correct by looking at the lock file:

jq .distributed_validators [ ] .distributed_public_key cluster/node0/cluster-lock.json "0x822c5310674f4fc4ec595642d0eab73d01c62b588f467da6f98564f292a975a0ac4c3a10f1b3a00ccc166a28093c2dcd" "0x8929b4c8af2d2eb222d377cac2aa7be950e71d2b247507d19b5fdec838f0fb045ea8910075f191fd468da4be29690106" info The generated private keys are in the standardEIP-2335 format, and can be imported in any Ethereum validator client that supports it.

Ensure your distributed validator cluster is completely shut down before starting a replacement validator or you are likely to be slashed. Edit this page Previous Advanced Docker Configs Next Introduction