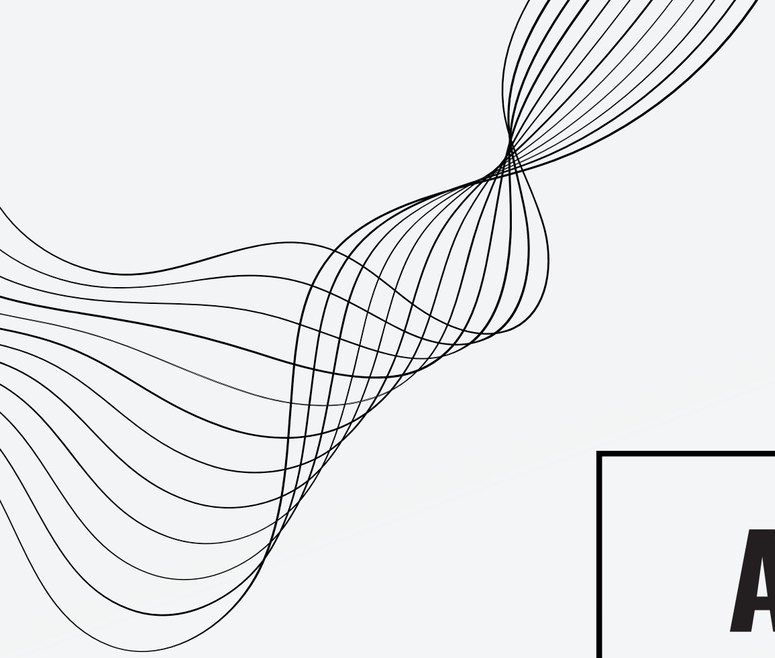
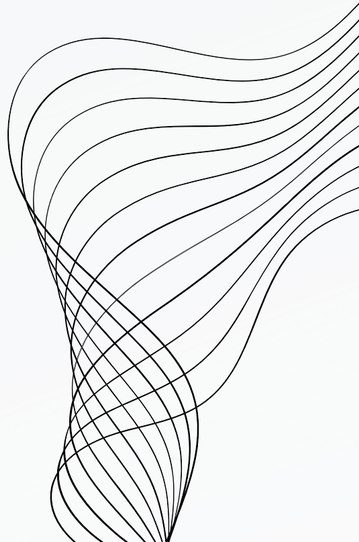


BLOCK3LABS

ADD RANDOMNESS NATIVELY ON STARKNET

PALO ALTO STARKNET HACKATHON 2023

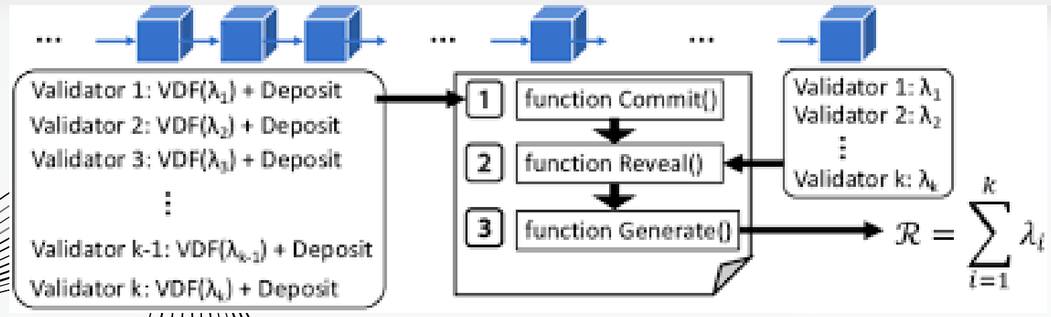


CONTENT

RANDAO

Randao is a random parameter added after the merge and is refreshed at each randao vertex with each new block
Randao is based on the old difficulty block setting

Randao is very secure and unpredictable.
If you want to break the randao randomness it’s equal to break the Ethereum network



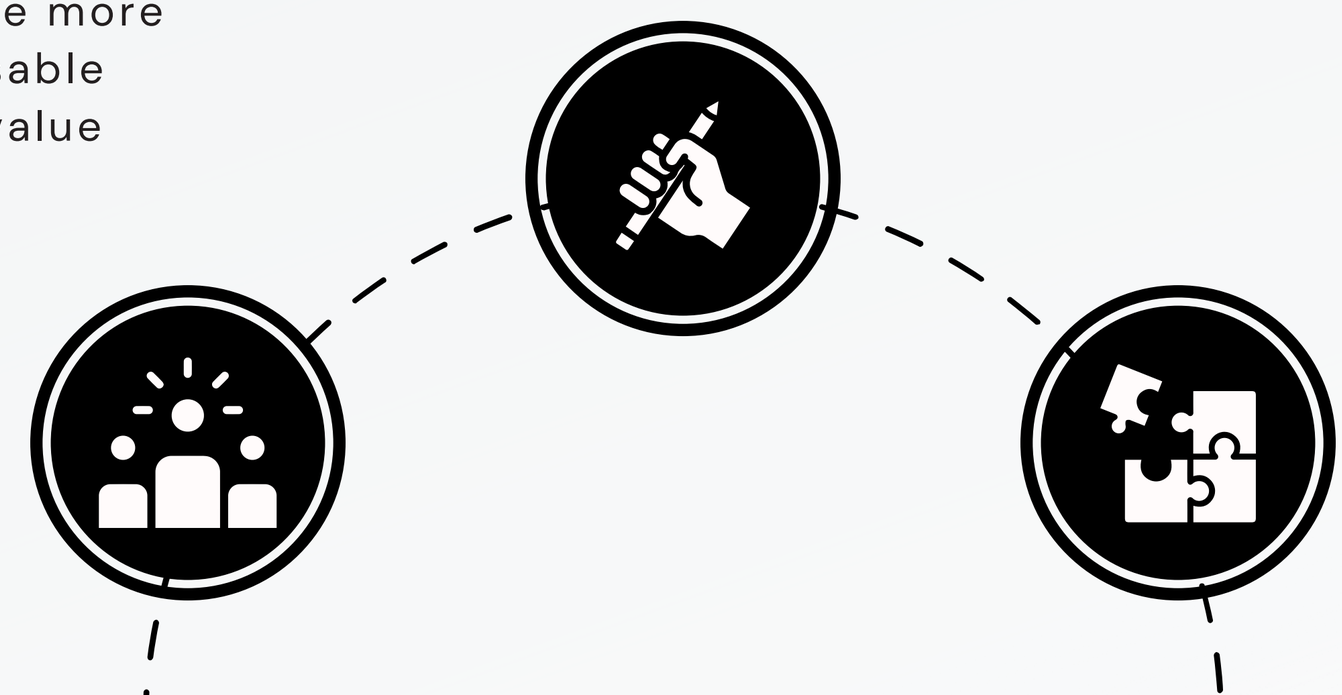
DIFFERENTS STEPS

Step 1

- Get randao from L1
- Use randao as VDF input to generate more secure unbiasable randomness value

Step 2

Generate proof of randao on L1 and verify it



Step 3

Generate proof on Herodotus and retrieve it on L2 such as Starknet

OUR REPO OF ALL OUR RESEARHCH

https://github.com/Hug0x0/randomness-hack

PROBLEMS

Currently with our solution we saw that it took us a lot of time to recover our random number on layer 2

today the storage proof herodotus are free but in the future the costs for this service will be very expensive. we do not think that in the future it will be really effective

THANK'S !

https://github.com/Hug0x0/randomness-hack