

I've been waiting for eth 2 to integrate the randao into my casino project.

My project is built in solidity and i'd like to know:

Will solidity be supporting randao requests?

(Currently prylabs has a 'randao reveal' but it's in GO)

How will the requests work?

Cost estimations?

And general purpose use cases...

I'm also wondering how it can be manipulated by users skipping their turn if they do/don't like a number to persuade a result...

For example:

If a fruit machine has a 100x potential reward...

There were 50,000 validators

Say attacker has 100 validators...

And wants to produce a number between 99-100 to receive 100x gains...

Could a user increase his chance of winning by 500 to 1 adding a 0.2% chance of winning?

By turning off their nodes at the right time if the user doesn't support the given number?

Any clarity about randaos is much appreciated...

The website hasn't been updated for 2 years

Love you all!

Sources:

(randao website: <https://www.randao.org>)

(randao reveal: <https://beacon.etherscan.io/slot/324063>)