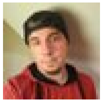
BUZZ CHRONICLES > CRYPTO
Saved by @Shubham51ngh
See On Twitter

Twitter Thread by Oliver Jumpertz



Oliver Jumpertz
@oliverjumpertz

"Blockchain technology is energy-intensive..." => No, it doesn't have to be.

Let's look at Proof-Of-Stake, an alternative to the energy-intensive Proof-Of-Work algorithm.

■■

1■■ A Quick Recap On Proof-Of-Work

A Proof-Of-Work algorithm requires miners to do a certain amount of work that is compute-intensive to gain access to a service or the right to do something. This algorithm, by design, also requires that the work done shall not ...

... be reusable for anything else than what it was performed for. This lies at the core of the security concept of a blockchain. To gain the right to append a new block to a chain and to get some currency as a reward, there is work to be done, and this work must be verifyable.

That work is a race between different miners. Many miners try to compete and to be the first to find the answer to a problem presented to them. This implies that a lot of energy is wasted as only the first correct solution is accepted.

You can find a more detailed thread on Proof-Of-Work here:

https://t.co/VGzmmbMisE

> Proof-Of-Work is the name of a cryptographic algorithm that is used for some blockchains when new blocks are to be appended to the chain.
>
> Let's take a higher-level look at how this one works, shall we?
>
> \U0001f9f5\U0001f53d
>
> — Oliver Jumpertz (@oliverjumpertz) April 3, 2021

2■■ Enter Proof-Of-Stake

Proof-Of-Stake is another algorithm, designed to create distributed consensus on a blockchain while being less energy-intensive and more scalable than Proof-Of-Work.

The first mention (I know of) of Proof-Of-Stake dates back to 2011 when it was discussed on the Bitcointalk forums.

While having the same goal as Proof-Of-Work, distributed consensus, the process is completely different.

3■■ How It Works

A Blockchain that uses Proof-Of-Stake chooses a node to create and append the next block randomly. This process of appending a new block to the chain is usually called "forging" and not "mining".

To be eligible to be chosen, nodes must stake some of the chain's cryptocurrency. This means that a certain amount of coins is locked away and can't be accessed for as long as the node wants to act as a forger.

If a new block is to be appended to the chain, the network randomly chooses between all nodes that have staked at least the minimum amount of coins required. This draft is usually weighted which could mean that the node with the largest amount staked has the ...

... highest chance to be chosen. To compensate this, blockchains usually take other factors into account like the age of the node's stake.

Whenever a node is chosen to forge a new block, the stake's age is reset to zero to distribute forging among all nodes ...

... a little more equal.

There are many other factors that can be taken into account and they are usually as individual as the blockchain using Proof-Of-Stake. Taking a look at the specific blockchain's whitepaper usually helps you to decide whether the chain is legit ...

... and it is worth setting up a forging node for it or if it's not working in everyone else's favor.

When chosen, a forging node checks whether all transactions for the next block are valid. It then signs the block and appends it to the chain.

The stake of a forging node is always at risk. If a node harmfully tries to insert manipulated blocks into the chain and the network notices, it loses its stake and is banned from ever participating in the forging process again.

This is to ensure that all parties involved in the forging process play by the rules as there is a lot of money at risk when they commit a fraud.

A forging node that wants to exit the forging process usually needs to wait for some time until its stake is released. This time is used to recheck all the blocks it ever forged. This is the last time a potential fraud can be detected.

Only after the check completed successfully, the stake is released and can be transferred again.

4■■ That's It

Well, we are at the end of this thread, and I hope you now understand Proof-Of-Stake, the alternative to the energy-intensive Proof-Of-Work a little better.

If you enjoy threads like this one, drop a like, comment with you feedback, and follow me if you want more content like this. Your support is highly appreciated!

5■■ A Small Addition

Forging nodes are also often called validators. The process is still called forging but validators validate transactions which is where this name comes from.