LCPoA

LCPoA (Limited Confidence Proof of Activity is a hybrid blockchain consensus algorithm consisting of two technical elements:

1. Proof of Activity - a principle based on solving a problem similar to the problem of the principle of Proof of Work, but with a significantly reduced complexity, thanks to which the solution of the problem takes from fractions of a second to several minutes
2. Limited Confidence - system of automatic creation of "control points" in the blockchain network

Currently, the algorithm is used only in the IZZZIO network, and has a number of advantages and disadvantages.

Limited Confidence (LC)

Limited Confidence - is a mechanism for creating control points in the network, limiting the possibility of rewriting blocks within the blockchain network beyond the specified limit from the last block. For example:

Situation 1

- In the network settings of the example, the **LC** number is set to 10
- **Client1** - contains a chain of blocks from 0 to block 30
- **Client2** - contains a chain of blocks from 0 to 34, while for the current client, block 29 differs from a similar block of the **Client1**

In such a situation, **Client1** downloads a piece of the **Client2** chain from block 29 to block 34, i.e. block 29 will be replaced, and the chains of both clients will be the same.

Situation 2

- In the network settings of the example, the **LC** number is set to 10
- **Client** - contains a chain of blocks from 0 to block 30
- **Attacker** - re-created a chain of blocks from 1 to 31, replacing all transactions on the network

In this situation, the **Attacker** will offer to
synchronize the chain from 1 to 31 blocks, but the minimum block from which you can synchronize: **31 - 10 = 21**
Synchronization with the chain of the attacker in this case will not be performed.

A smaller number of LC reduces the chance of overwriting the chain, a larger number reduces the chance of non-synchronized (dead-end) chains appearing.

Proof of Activity

As the algorithm for generating blocks, a modification of Proof of Work with reduced complexity is used. The peculiarity consists in using as a nonce-Unix timestamp, as well as in additional checks and limitations:

- GTM + 0 is used as the general time
- In the block, it is necessary to record information about the start time of the block generation
- In the block timestamp, a nonce block is written

Parameters are checked:

- Matching a hash block with a filtered hash filter
- The start time of the block generation is not greater than the current network time, and no more than the timestamp of the block
- The timestamp is no longer than the current network time, and no less than the beginning of the block generation time
- timestamp and the start time of the block generation is not less than the timestamp of the previous block

At the same time it is allowed to be tested for no more than 60 seconds.

It is also possible to use classic PoW or other algorithms in conjunction with the LC mechanism.

Advantages

- Average speed of work on devices of different classes - 1 unit in 5 seconds
- Limiting the maximum speed of block selection for all devices is 1000 hashes per second, which makes the use of miners meaningless
- Generation of a unit can easily be performed by a device of any power
- A completely decentralized algorithm, to generate a new block, only information about the last block of the network is needed
- Does not require the existence of tokens and remuneration in the network for work

Disadvantages

- With very low network activity, it is possible to attack an excessive number of **LCs**. An alternative protection option is to change the operation of the Limited

Confidence mechanism to check not the number of blocks, but the time elapsed since the addition of the block
- When working with a small **LC** threshold, there is a chance of a large number of dead-end chains
- Limitation of generation in 1000 blocks per second
- The need for synchronization with world time

Security

Attack 51%

Basically, without using protection from the mechanism of Limited Confidence, the described variant of Proof of Activity in itself is highly vulnerable to an attack of 51%. With the use of the confidence limit, an attack of 51% is possible only on a very small number of blocks, which makes it meaningless in most cases.

Free entry into the chain of blocks

To protect the network from spam blocks, **it needs to use additional security methods, for example**:

- Increase the complexity of generating a block by the PoA algorithm
- Commission for recording a block (transaction)
- Limiting the recording of a large number of blocks from one participant