Methodology forchoosing a consensus algorithm forblockchain technology

УДК 004.65:004.75

Tetiana Bazhan[1], Viktoriia Zhebka[2], Serhii Zhebka[3]

State University of Information and Communication Technologies,
tetiana.olexandrivna@gmail.com[1], digitaldut2022@gmail.com[2],
szhebka@hotmail.com[3]

Blockchains are decentralised, meaning that data can be distributed across multiple host servers, which distinguishes them from conventional databases. Decentralisation is the main feature of blockchain.

Since control over data or resources is shared among several nodes simultaneously, it makes it very difficult for an attacker to delete or use resources.

Consensus maintenance is very important because without it, copies of data on different nodes may conflict with each other, leading to inefficient and inconsistent data storage.

A successful consensus algorithm should help a blockchain application achieve its goal. The purpose of the blockchain is to provide a tool for decentralised decision-making. The complex nature of blockchain consensus stems from its original goal of making decisions without a central authority. Therefore, the level of decentralisation of the consensus algorithm is included in the evaluation criteria. A consensus algorithm with a higher level of decentralisation is considered good.

The following energy consumption criteria for choosing a consensus algorithm in blockchain technology should be considered:

1. Proof of Work (PoW): computational complexity (the more difficult the task is for miners, the more energy is consumed); algorithm efficiency (some PoW algorithms may be more energy efficient than others).
2. Proof of Stake (PoS): selective efficiency (the less currency a participant has, the less energy he uses); methods for controlling misuse (it is important to have mechanisms to prevent concentration of power that may affect the effectiveness of PoS)
3. Delegated Proof of Stake (DPoS): chosen legitimacy (some participants may spend more energy to obtain delegate status); flexibility of the voting policy (if the voting system is not efficient, it can lead to an incorrect distribution of power and energy costs).
4. Proof of Burn and other alternatives: spending strategies (determining exactly how currency is spent in the consensus process and how this affects energy costs; innovative approaches (alternative methods such as Proof of Space (PoSpace) or Proof of Time (PoT) may offer lower energy costs).

However, the energy consumption criteria must be balanced with other important aspects, such as security, decentralisation and bandwidth, when choosing a consensus algorithm for blockchain technology.

Here is a comparative description of consensus algorithms for different types of cryptocurrencies (Table 1)

Table 1

Characteristics of consensus algorithms

Crypto-currency	Type	Security	Decentralisation	Energy consumption	Bandwidth
Dash	Hibrid	Medium	Medium	Medium	OK
Peercoin	Hibrid	Medium	Medium	Low	Not So Fast
Verus coin	Hibrid	Medium	Medium	Low	OK
Decred	Hibrid	Hight	Hight	Medium	OK
Stratis	Hibrid	Medium	Medium	Medium	Fast
Bitcoin	PoW	Hight	Hight	Hight	Not So Fast
Conflux	PoW	Hight	Medium	Low	Very Fast
Ethereum Classic	PoW	Medium	Medium	Medium	Fast
Monero	PoW	Hight	Hight	Medium	OK
Dogecoin Litecoin	PoW	Medium	Medium	Medium	OK
Ethereum	PoS	Medium	Hight	Low	Fast
Polygon	PoS	Hight	Medium	Low	Fast
TON coin	PoS	Medium	Medium	Low	Fast
Solana	PoS	Hight	Medium	Hight	Very Fast
Cardano	PoS	Hight	Medium	Low	Fast

For any future work, it would be interesting to have a study on the selection of a consensus algorithm and it is possible to choose a wider list of criteria or reduce it to a minimum. In addition, the blockchain application industry is developing rapidly and new algorithms are being created that can quickly replace the old ones on the market. There is always a need for future research, so it is a necessity to keep up to date with the latest developments in consensus algorithms and blockchain technology.

1. F. Kipchuk, et al., Assessing Approaches of IT Infrastructure Audit, in: IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (2021). doi: 10.1109/ picst54195.2021.9772181.
2. Center for Combating Disinformation, How Ukraine Survived Russia's Winter Terror (2023). URL: https://cpd.gov.ua/ articles/yak-ukrayina-perezhyla-zymovyj-teror-rosiyi/
3. V. Perun, The Russian Federation Launched more than 1,200 Missiles and Drones at Key Energy Facilities of Ukraine, Ukrenergo (2023). URL: https://lb.ua/society/2023/04/08/551391_rf_vipustila_klyuchovih.html
4. UKRAINE. Rapid Damage and Needs Assessment. February 2022 – February 2023; Anne Himmelfarb (Ed.). The World Bank, the Government of Ukraine, the European Union, the United Nations.