Tokenomics and Perspectives of Proof of Stake

Maryna Chyzhevska[1], Nataliia Romanovska[2], Vitalii Venger[2], and Volodymyr Sokolov[3]

[1] National University "Yuri Kondratyuk Poltava Polytechnic", 24 Pershotravneva ave., Poltava, 36011, Ukraine
[2] State Institution "Institute for Economics and Forecasting," NAS of Ukraine, 26 Panasa Myrnoho str., Kyiv, 01011, Ukraine
[3] Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudriavska str., Kyiv, 04053, Ukraine

Abstract

Ever since the first block of the Bitcoin network was created, the relevance of research into the assessment of the prospects of the blockchain project is constantly increasing. Ultimately, the economics of a token will have a big impact on how it will be used, how easy it will be to build a network, and whether there will be much interest in the options of its use. The work substantiates that tokenomics allows us to determine which digital assets can be traded or exchanged for other tokens or fiats in the blockchain network. It is noted that the key difference between traditional economics and tokenomics is that the latter is written in code. The authors systematized the elements of tokenomics: supply and demand, the utility of the token, its distribution, the burn of the token, mechanism of token stimulation. The mechanism and working principles of Proof-of-Stake and its differences from Proof of Work, which consists, first of all, of reducing computing costs, are revealed. It is stated in the work that in the coming years, the development of the potential of this algorithm and the growth of the level of popularity of cryptocurrency mining based on it is expected.

Keywords

Blockchain, cryptocurrencies, tokens, tokenomics, Proof of Stake.

1. Introduction

Every day, diving into the news of the information space, we receive information from the crypto world regarding cryptocurrency exchange rates, new technologies, popular trading pairs, etc. Even staunch skeptics no longer deny that cryptocurrency is an important component of the life of modern society and the modern economy [1, 2].

Any country that wants to prosper financially must have sound economic and monetary policies. These policies will become structures for ensuring the normal functioning of the economy [3].

A similar idea exists in cryptocurrencies. To make a project successful, it needs a proper plan for how its tokens will work to keep it afloat. Any project with bad tokenomics will fail. Since the creation of the first cryptocurrency—bitcoin, this field has undergone drastic changes. Currently, the cryptocurrency market is in constant development and new projects appear almost every day. Under these conditions, the promotion of projects becomes more and more difficult and requires the expenditure of large resources [4].

Unlike fiat currencies, cryptocurrencies are not backed by any physical assets. The issue of assets is strictly limited, therefore there are no risks of inflation. Cryptocurrencies do not have a central governing body and function in a network with equal participants. Thanks to this, it is impossible for users to have access to the entire system if the central server fails.

A set of economic rules and models that ensure the functioning of the economy of the project, which is based on tokens, was called tokenomics. It plays a central role in evaluating

DECaT'2024: Digital Economy Concepts and Technologies, April 4, 2024, Kyiv, Ukraine
EMAIL: marfin.poltava@gmail.com (M. Chyzhevska); romnatalina@gmail.com (N. Romanovska); vengerv@ukr.net (V. Venger); v.sokolov@kubg.edu.ua (V. Sokolov)
ORCID: 0000-0003-1637-9564 (M. Chyzhevska); 0000-0002-1377-7551 (N. Romanovska); 0000- 0003-1018-0909 (V. Venger); 0000-0002-9349-7946 (V. Sokolov)

the prospects of the blockchain project. While designing crypto projects, one must carefully work out their tokennomics to ensure sustainable long-term development.

Tokenomics allows you to determine which digital assets in the blockchain network can be traded or exchanged for another token or fiat. In addition, it shows cryptocurrencies that provide incentives and are profitable for their owners and investors.

2. The Essence of Tokenomics

Tokenomics is the fundamental concept of how the law of supply and demand works in cryptocurrency and NFTs. The concept of cryptotokenomics dates back to the 1970s. It covers the main factors that affect the value of a token: issuance, attributes, distribution, supply, demand, and other characteristics. What is important, no single factor provides a perfect key. The assessment should be based on as many factors as possible and analyzed as a whole. The term tokenomics comes from two words: token and economics. A token is a unit of asset in the blockchain. It can exist in the form of a fungible or non-fungible token. Economics studies scarcity, consumer behavior, and the efficient use of resources.

The key difference between traditional economics and tokennomics is that the latter is written in code.

Tokenomics can be combined with other fundamental analysis tools to make a reasonable judgment about the prospects of a project and the price of its token.

Eventually, the token economics will have a big impact on how it will be used, how easy it will be to build a network, and whether there will be much interest in its use options.

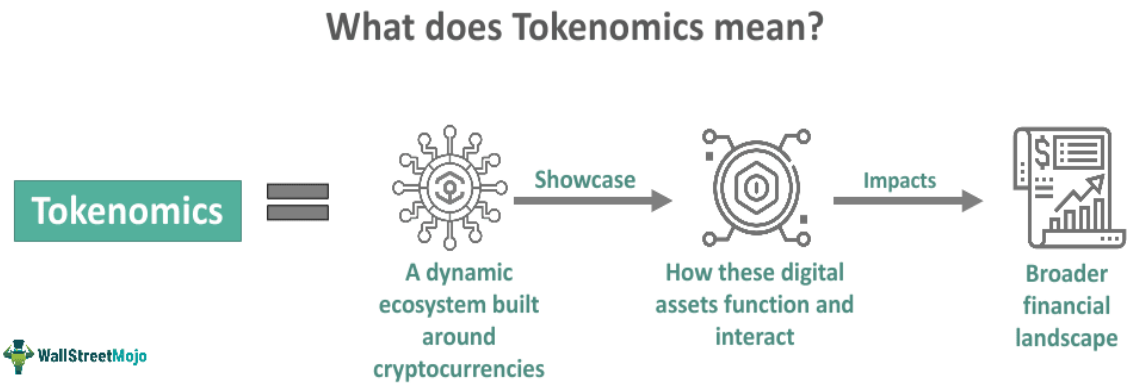

Figure 1: Tokenomics [5]

The tokenomics model has three main pillars: utility, economic security, and value. A successful crypto-token must be useful in its ecosystem, have intrinsic value, and provide economic stability. These factors together affect the usage and value of the token.

3. Elements of Tokenomics

Demand and supply are the main elements and factors that affect the price of any product or service. The same goes for cryptocurrency. Several important indicators measure token offerings.

The first is called the maximum offer. This means that there is a maximum number of tokens encoded for the existence of this cryptocurrency. Bitcoin's maximum supply is 21 million coins. Litecoin has a cap of 84 million coins and BNB has a cap of 200 million [6].

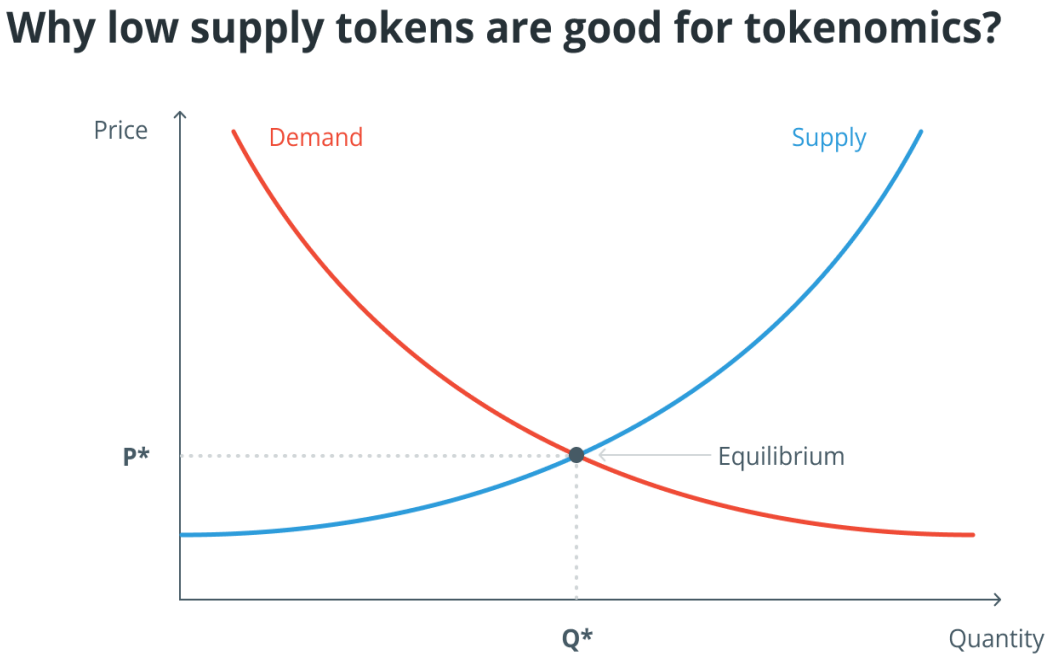

Figure 2: Supply and demand as an element of tokenomics [7]

Some tokens do not have a maximum supply. The supply of Ethereum in the network increases every year. Stablecoins such as USDT, USD Coin (USDC), and Binance USD (BUSD) do not have a maximum supply because these coins are issued based on the reserves that back the coins. Theoretically, their number can grow without limits. Dogecoin and Polkadot are two other cryptocurrencies with unlimited supply.

The second indicator is the circulating supply, which refers to the number of tokens in circulation. Tokens can be minted and burned, or blocked in other ways. This also affects the price of the token. Looking at the token supply gives you a good idea of how many tokens there will be in the end.

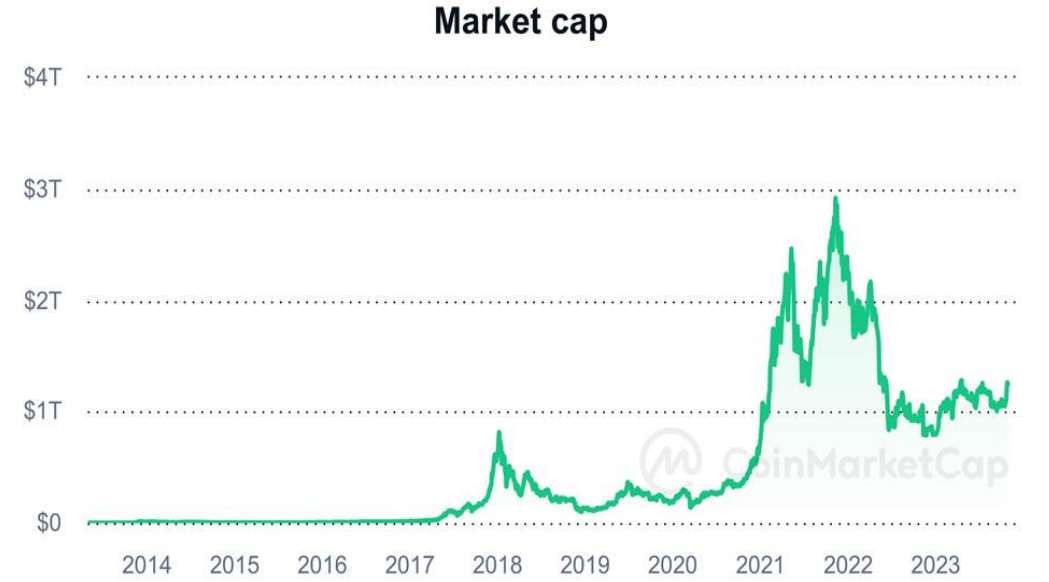

Figure 3: The total market value of all cryptocurrencies, including stablecoins and tokens [8]

The utility of the token refers to the developed options for its use. For example, the utility of BNB is powering the BNB Chain, paying transaction fees and receiving discounts on trading fees on the BNB Chain, and using the utility of the community token in the BNB Chain ecosystem. Users can also stake

BNB in various products within the ecosystem to generate additional income.

There are many other options for using tokens. Management tokens allow the owner to vote for changes in the token protocol. Stablecoins are intended for use as currency. Tokenized securities, on the other hand, are financial assets. For example, a company may issue token shares during the primary offer of coins (ICO), giving the owner property rights and dividends [6].

In addition to supply and demand, it is important to look at how the token is distributed. Large organizations and individual investors behave differently. Knowing what types of organizations own a token provides insight into how they might trade their tokens, which in turn will affect their value.

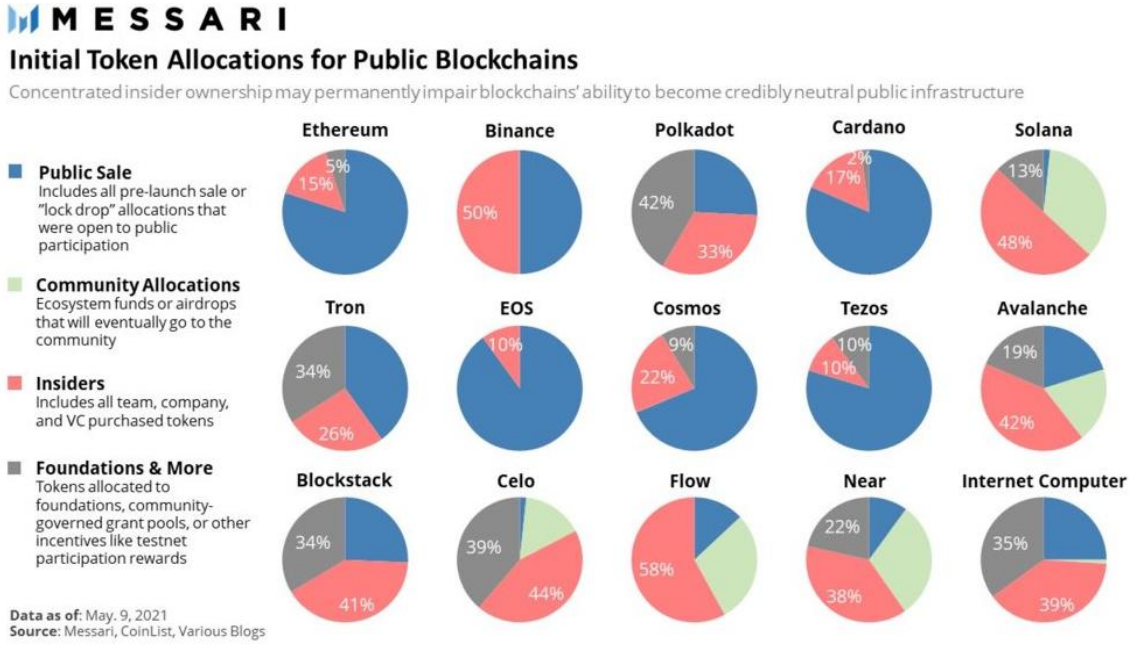

Figure 4: Initial distribution of tokens for public blockchains [9]

There are usually two ways to launch and distribute a token: fair launch and pre-mining launch. A fair launch is when there are no early access or private allocations before a token is minted and distributed to the community. BTC and Dogecoin are examples of this category.

On the other hand, a pre-mining launch allows you to mint a portion of the cryptocurrency and distribute it to a select group before it is offered to the community. Ethereum and BNB are two examples of this type of token distribution.

A scenario where several large organizations own a large portion of the tokens is generally considered more risky. Tokens mostly owned by patient investors and founding teams mean that stakeholders' interests are better aligned for long-term success. It is a good idea to look at the token lock and release schedule to see if a large number of tokens will be released, which will reduce the pressure on their value.

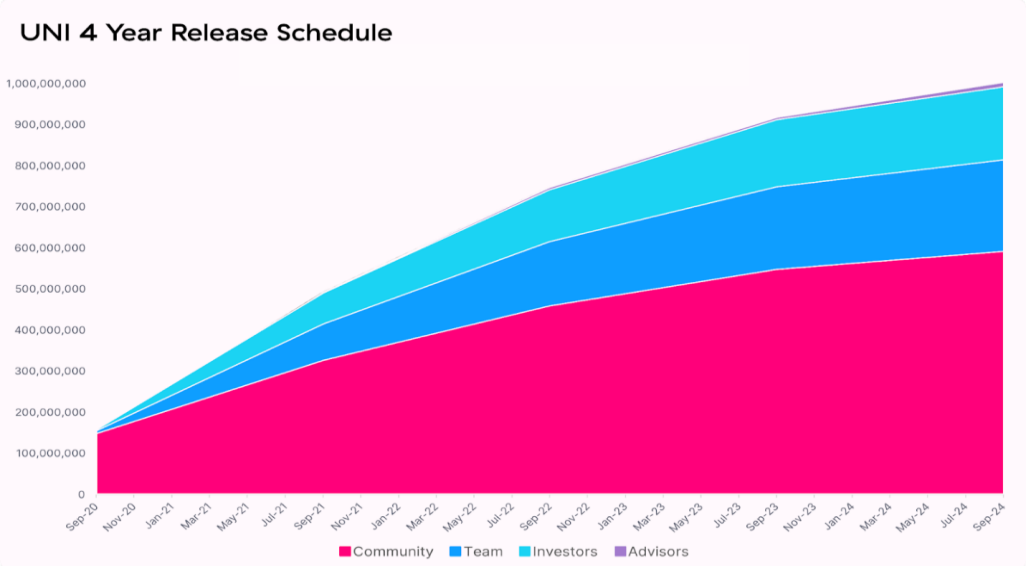

Figure 5: Token release schedule Uniswap (UNI) [10]

Many crypto projects regularly burn tokens, which means the final withdrawal of tokens from circulation.

For example, BNB uses coin burn to remove coins from circulation and reduce the total supply of its tokens. Taking into account the pre-mining of 200 million BNB, the total supply of BNB as of June 2022 was 165,116,760 coins. BNB will burn coins until 50% of the total supply is destroyed, which means the total BNB supply will be reduced to 100 million BNB. Similarly, Ethereum started burning ETH in 2021 to reduce the total supply [6]. When a token's supply decreases, it is considered deflationary. Conversely, when the number of tokens continues to grow, it is considered inflationary.

The incentive mechanism of the token is crucial. The way how a token incentivizes participants to ensure long-term activity is the core of tokennomics. The way Bitcoin develops a block subsidy and transaction fee is a great illustration of an elegant model.

Recently, the Proof-of-Stake mechanism as another verification method is gaining more and more popularity. This development allows participants to lock their tokens to verify transactions. Generally, the more tokens are locked, the higher the chance of being selected as a validator and receiving rewards for validating transactions. It also means that if validators try to harm the network, the value of their assets will be put at risk. These features encourage participants to act honestly and maintain the reliability of the protocol.

4. Proof of Stake Mechanism

Proof of Stake is the most popular consensus algorithm in the blockchain. Many crypto-currencies and blockchain platforms are built on it, including Ethereum, Cardano, Solana, Tezos, and Algorand.

Such popularity is due to the absence of the need to purchase expensive equipment for mining. If earlier bitcoin could be obtained using a home PC, today you need a huge farm with hundreds of video cards and a lot of time to get a small profit. Simple math—a maximum of 900 BTC is generated per day, and the number of miners chasing BTC exceeds several million.

Proof of Stake, compared to another popular Proof of Work algorithm, has low energy consumption for block generation and blockchain security.

The inventor of Bitcoin, Satoshi Nakamoto, proposed the Proof of Work mechanism in October 2008. According to Proof of Work, NOD operators of the decentralized network (miners) in the mode of free competition solve resource-intensive mathematical problems—finding the hash of a block by the matching method. If successful, the winning miner or pool gets the opportunity to add the block they found, and in return receives a reward of new bitcoins.

Literally in a couple of years after the launch of bitcoin, it became clear that the Proof of Work principle leads to a constant increase in mining power and, therefore, electricity costs.

In addition, due to the need to use powerful equipment, the availability of mining decreased, and already in 2011, on July 11, at the then-popular cryptocurrency forum Bitcointalk, the idea of an alternative consensus mechanism for Bitcoin was proposed, which was called Proof of Stake (proof of ownership share).

It was proposed that the right to vote in the decentralized network should be given to all its participants by the share of the total number of coins they own.

Already in August 2012, this new consensus mechanism received its first practical implementation in the PPCoin cryptocurrency. New coins were distributed through mining, and transactions could be processed by any NOD that stored the PPC cryptocurrency. The same hybrid consensus scheme was used in other early PoS projects, such as Gridcoin and Blackcoin. The first "pure" PoS cryptocurrency without mining was the NXT blockchain, launched on November 24, 2013.

The Proof of Stake consensus mechanism turned out to be so successful and flexible that in the following years, it was implemented in hundreds of cryptocurrencies in various variants and modifications.

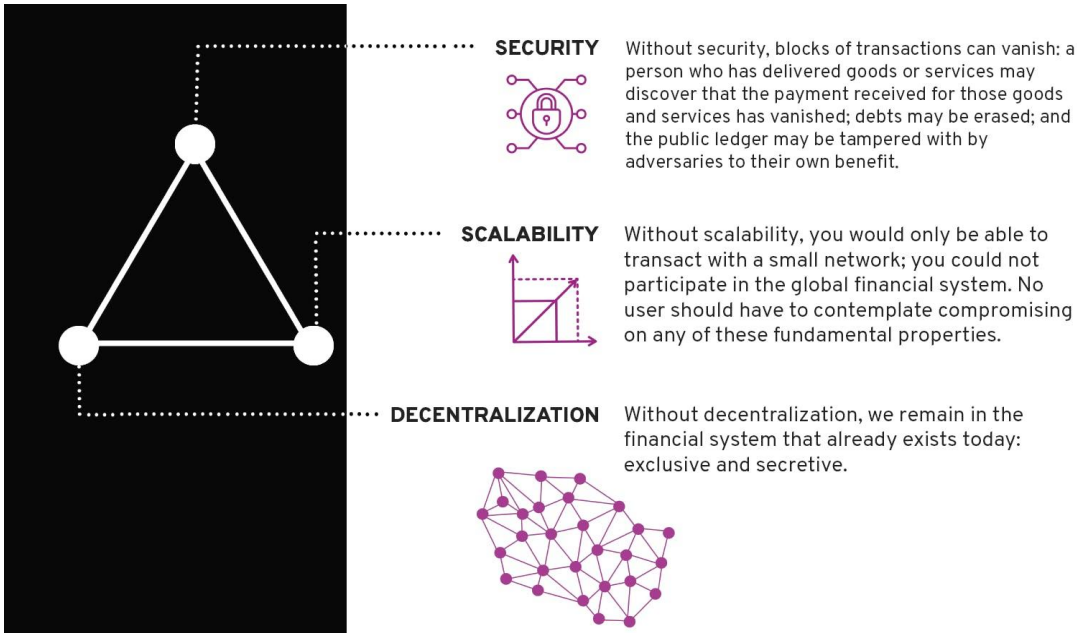

Figure 6: Proof of Stake Mechanism [11]

5. The Working Principle of Proof of Stake

As stated above, the concept of Proof of Stake provides the right to manage the blockchain to all participants by the share of coins they own.

For example, in a cryptocurrency with its "canonical" PoS mechanism, all users who have at least 1002 NXT during the last 1440 blocks in the official NXT Client wallet, have a chance to form the next block. At the same time, each wallet is a full node (NOD) and stores its copy of the blockchain. Such a wallet can be launched both on a high-performance server and on a laptop, a Raspberry Pi micro-computer, and even in a cloud service.

The more coins in the NXT wallet, the more likely it is to get the right to form a new block, and then the user will get all the transaction fees that went into the block. Ideally, a wallet that has 1% of coins will generate 1% of all new blocks.

The process of creating blocks in NXT and other early PoS cryptocurrencies was called "forging", but this term is not commonly used at this time.

The process of holding cryptocurrency in a wallet to receive rewards for participating in network security is called staking. Today, in many PoS cryptocurrencies, sending coins to staking involves locking them in a special smart contract with no possibility of movement for a certain period (from several hours to several weeks).

The use of the Proof-of-Stake mechanism, when almost any cryptocurrency owner can be a block producer, allows for a high level of blockchain decentralization and security.

However, according to the blockchain trilemma, this comes at the cost of performance. The mentioned NXT cryptocurrency network has a throughput of only 4 transactions per second, which is noticeably lower than many cryptocurrencies that use PoW consensus. For example, Dogecoin processes 33 transactions per second.

To find a compromise between decentralization and performance, the concept of delegation was proposed, where coins from multiple wallets together with the right to vote can be transferred to a few computing NODs.

In 2013, Daniel Larimer, an American programmer, and crypto-entrepreneur, used this concept to create the Delegated Proof-of-Stake (DPoS) mechanism, which was first implemented on the BitShares blockchain platform, and then used in various versions in the most famous crypto projects EOS, Cardano, Tezos etc. Today, the delegation function has become an industry standard and is used in almost all PoS implementations.

In DPoS, cryptocurrency owners may not participate in the operation of the network themselves, but transfer their coins to validators—professional participants who manage blockchain NODs. In return, they undertake to reward coin owners, often for a small fee.

In different blockchains, depending on their architecture, the number of validators involved in the production of blocks differs significantly: Polkadot-up to 16; BNB Chain and EOS-21; Near-100; Cardano—about 3200; Avalanche-about 1200; Solana-more than 3400; Ethereum-more than 400 thousand.

As a rule, to run a validator, you need special equipment with constant access to the Internet, as well as a significant amount of native coins of the network. For example, a validator on the Ethereum network must have at least 32 ETH and a Tezos validator must have at least 8000 XTZ.

To compensate for the costs of computing nodes for verifying transactions and generating new blocks, most PoS blockchains provide a reward that is paid in the native coins of this network. As a rule, the size for each block is fixed, but it can change depending on the current network parameters.

The profitability of staking for validators and coin owners is determined by two factors: the emission rate, which is determined by the fixed value of coins issued for each new block, and by the share of coins in circulation that are blocked in staking (Staking Ratio). For example, if 1 million coins are issued through staking in a year with a total supply of 100 million coins, then the profitability of staking with 50% of blocked coins will be 2% per year. If 25% of the offer is blocked in staking, the profitability doubles to 4% per annum.

6. Proof of Stake Types

Many consensus mechanisms have been developed based on the principles of PoS and delegation, which differ in several nuances, for example, the distribution of roles between participants of the decentralized network. In particular:

- **Leased Proof of Stake.** It presents several distinct features that make it an attractive choice for cryptocurrency users and participants in blockchain ecosystems. The goal of LPoS is to enhance decentralization, accessibility, and fairness while maintaining network security and efficiency.
- **Nominated Proof of Stake** is emerging as a noteworthy development of traditional Proof of Stake (PoS) mechanisms. While both mechanisms share the fundamental concept of using tokens to participate in network consensus, NPoS represents a new level of community engagement and decentralization. In NPoS, participants are not just token holders, but also active participants in the validator selection process. NPoS is based on the principles of decentralization and fairness. Unlike traditional PoS, where validators are chosen mainly based on the number of tokens staked, NPoS offers a democratic approach. Token holders become nominees, playing a critical role in appointing the validators they trust to protect the network. This change ensures that the authority to verify transactions is distributed among different people rather than concentrated in the hands of a few individuals.
- **Pure Proof of Stake (PPoS)** is used in the Algorand network, where the

validators of the next block are secretly and randomly selected from among all wallets with a balance greater than 1 ALGO.

- **Effective Proof of Stake (EPoS)** is used in the Harmony blockchain platform. It has a special reward distribution mechanism that encourages the launch of many small validators instead of a small number of large ones, which encourages decentralization.
- **Proof of Authority (PoA)** is a hybrid algorithm that combines proof of stake and reputation of validators, each of which must be approved by developers. In PoA, the validator must undergo an identity verification procedure similar to KYC. This algorithm uses the BNB Chain.

7. Advantages of Proof of Stake

After the successful transition of the Ethereum network to Proof-of-Stake consensus on September 15, 2022, the network's energy consumption has decreased by almost 2000 times or 99.95%. In connection with this, the discussion of the transition of popular PoW cryptocurrencies to PoS has developed with renewed vigor.

Also, the transition to a new consensus algorithm completely changes the tokenonomics of ETH. While previously the mining reward was 2 ETH for each block, now these coins will not be created and the reward will be received by Ethereum stakes. This, according to experts, will reduce the rate of ETH emission by about 90%. Along with the burning mechanism, ETH can become a deflationary asset.

Cryptocurrencies on the PoS algorithm are built on the principle of complete decentralization. These networks do not provide for the presence of a single control center for decision-making regarding further development of the system and making adjustments to its operation. Proof of Stake is extremely inconvenient for fraudsters and hackers.

They will not be able to access information about the real version of the Blockchain database. Accordingly, committing illegal actions becomes impossible. In addition, the probability of hacking cryptocurrency is minimized, because attackers need expensive computing power, which makes the attack unprofitable. Hackers have a serious supply of crypto, attacks will not be profitable for them, because they will break the stability of the network and, accordingly, assets will depreciate.

The Proof of Stake algorithm makes the process of cryptocurrency mining profitable because for effective mining it is not necessary to invest unheard-of sums for the purchase of computer equipment.

The level of popularity of cryptocurrency mining using the Proof of Stake algorithm is growing every year. Developers create and launch new networks, and coins that have appeared before are gradually becoming more expensive. Users are primarily interested in mining without significant investment in the acquisition of computing power.

Proof of Stake technology offers a slightly different approach. To effectively mine tokens, you need to invest in the purchase of coins. In the future, they can be sold or converted into another cryptocurrency. Proof of Stake mining is a guarantee of equal and fair distribution of rewards, i.e. new tokens [12, 13].

However, the Proof of Stake algorithm cannot be considered solely in the context of cryptocurrency mining. This technology also became a guarantee of security of the money invested in the purchase of coins. All participants in the process have a direct interest in the correct operation of the project.

8. Conclusion

So, crypto is not as difficult as it seems at first glance. But this issue is worth understanding because cryptocurrency has great potential. We established that tokenomics refers to the economic system that governs the functioning of cryptocurrencies on the market. Each cryptocurrency has its own unique set of tokenomics. Several critical elements of tokenomics include token mining, staking, utility, burn, governance, and distribution. Important factors affecting this model include supply and demand, price stability, market capitalization, and safety and regulatory compliance issues.

Tokenomics is often created to attract investors and is tailored to the interests of the majority. The strongest model of tokenomics that has stood the test of time remains the Bitcoin model. Tokenomics is essential for every player in the cryptocurrency and blockchain ecosystem. Before the public launch and release of the blockchain protocol, the tokenomics will be documented to outline what the digital asset will do, the idea behind its launch, and the underlying technology. Blockchain is at an early stage of its development, so investors' profits in the long run may turn out to be even more significant than the growth of Bitcoin in recent years.

The most popular blockchain consensus algorithm today is Proof of Stake. Many cryptocurrencies and blockchain platforms are built on it. This is the first algorithm whose reliability has been proven mathematically. The level of popularity of cryptocurrency mining using the Proof of Stake algorithm is growing every year. Specialists are constantly creating and launching new networks.

References

[1] S. Obushnyi, et al., Ensuring Data Security in the Peer-to-Peer Economic System of the DAO, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3187 (2021) 284–292.

[2] S. Obushnyi, et al., Autonomy of Economic Agents in Peer-to-Peer Systems, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 125–133.

[3] B. Bebeshko, et al., Application of Game Theory, Fuzzy Logic and Neural Networks for Assessing Risks and Forecasting Rates of Digital Currency, Journal of Theoretical and Applied Information Technology 100(24) (2022) 7390–7404.

[4] D. Virovets, et al., Ways of Interaction of Autonomous Economic Agents in Decentralized Autonomous Organizations, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 182–190.

[5] D. Vaidya. Tokenomics. URL: https://www.wallstreetmojo.com/tokenomics/

[6] What is Tokenomics and Why is it Important? URL: https://academy.binance.com/uk/articles/what-is-tokenomics-and-why-does-it-matter

[7] J. Fáwọlé, O. Malanii, Tokenomics: Supply & Demand of Crypto. URL: https://hacken.io/author/john-fawole/

[8] CoinMarketCap, Global Live Cryptocurrency Charts & Market Data (2024). https://coinmarketcap.com/charts/

[9] Messari, Overview (2024). URL: https://messari.io/dashboard

[10] Uniswap Labs, DeFi (2024). URL: https://app.uniswap.org

[11] Overcoming Poverty and the Root Causes of inequality. URL: https://www.un.org/en/desa/highlights-report-2021-2022

[12] M. Chyzhevska, et al., Dual Impact of Crypto Industry Technologies on the Energy Poverty, in: Cybersecurity Providing in Information and Telecommunication Systems vol. 3421 (2023) 293–299.

[13] Proof of Work, Proof of Stake & Pure Proof of Stake: An Evolution in Distributed Consensus. URL: https://algorand.com/resources/blog/proof-of-stake-vs-pure-proof-of-stake-consensus