

*A. Polchanov, Dr. In Ec., Prof.  
S. Kukharonok, Senior Lecturer  
A. Kostiuchenko, Bachelor Student  
Zhytomyr Polytechnic State University*

## **USING AI TO ANALYSE THE SECURITY OF BLOCKCHAIN PAYMENTS**

The rapid development of technology in recent decades has led to the need for new approaches to data processing and analysis, especially in such dynamic industries as cryptocurrencies and blockchain. With the openness of blockchains, a large number of transactions, and changing market behavior, there is a need for tools that can quickly and accurately interpret complex data. In this context, artificial intelligence (AI) is a powerful tool for analysis and forecasting, capable of identifying patterns that remain inaccessible to traditional methods.

The use of machine learning algorithms, in particular deep neural networks, allows not only to automate the processing of transactional data but also to build predictive models for risk assessment, trend prediction, and detection of anomalous behavior. This opens up new horizons for both research and practical applications in finance, security, and analytics.

As a decentralized data storage technology, blockchain is characterized by a high level of transparency but, at the same time, by complexity in structure and dynamics. Every transaction on the network, every smart contract or token movement leaves a digital trace that can be used for analytics. However, the volume of such data is growing exponentially, making it inefficient to process using traditional statistical methods. In this context, artificial intelligence opens up new opportunities for the structured analysis of blockchain data (online analytics), revealing hidden connections and creating forecasting models [1, p. 46].

Machine learning (ML) methods enable the automation of the blockchain analysis process. One of the most common applications is the classification of wallet types and transaction clustering. For example, the k-means algorithm can be used to group addresses based on their activity, transaction size, frequency of actions, etc. This allows you to separate institutional players from ordinary users, as well as identify potential bots or wallets associated with fraud.

The next step is to build forecasting models based on time series. Algorithms such as LSTM (Long Short-Term Memory) are used to analyze the behavior of the cryptocurrency market in the time dimension. LSTMs are able to take into account both short-term and long-term dependencies between cryptocurrency rate changes, trading volumes, and network activity. Such models demonstrate high accuracy in predicting short-term price changes, especially when combined with technical analysis indicators (e.g., MACD, RSI) [2].

Another promising approach is hybrid models that combine online data with social indicators (content analysis on Twitter, Reddit, etc.). Using natural language processing (NLP), it is possible to detect investor sentiment and predict market growth or decline even before changes become visible in charts. For example, a sharp increase in the number of tweets with the words "bullish", "buy", "ATH" often precedes market growth [3].

In addition, AI systems can be used to detect anomalies in blockchain networks. This is especially relevant for combating money laundering, terrorist financing, and other criminal schemes. Algorithms such as Isolation Forest, AutoEncoder, or DBSCAN can detect atypical transactions that may signal a violation [3].

One example of a commercial application is Chainalysis, which uses blockchain analytics and AI to identify suspicious wallets and build interaction graphs. Glassnode also provides predictive analytics based on online metrics using intelligent models [1, p.59].

Despite the undoubted advantages, it is worth noting the limitations of using AI in the crypto sphere. First of all, it is the high variability of data, its fragmentation (especially in multi-chain systems), and high market volatility. In addition, even the most advanced models can give false signals in the face of market manipulation or force majeure (such as stock market crashes or global regulatory changes) [3].

Thus, the integration of artificial intelligence with blockchain analytics is a promising area of research that combines a high level of innovation with practical value.

It opens up new opportunities for traders, analysts, fintech product developers, and researchers. Further research should focus on improving the accuracy of models, their adaptability to market changes, and creating open platforms for training and testing AI models based on blockchain data.

## REFERENCES

1. Atzori M. Blockchain Technology and Decentralized Governance: Is the State Still Necessary? / M. Atzori // *Journal of Governance and Regulation*. – 2017. – Vol. 6, Issue 1. – C. 45–62. – DOI: 10.22495/jgr\_v6\_i1\_p4.

2. McNally S., Roche J., Caton S. Predicting the price of Bitcoin using Machine Learning / S. McNally, J. Roche, S. Caton // *Proceedings of the 26th European Conference on Information Systems (ECIS)*. – 2018. – C. 1–14. – Режим доступа: [https://aisel.aisnet.org/ecis2018\\_rp/170](https://aisel.aisnet.org/ecis2018_rp/170). – Дата звернення: 08.04.2025.

3. Chen J., Bellavitis C. Blockchain Disruption and Decentralized Finance: The Rise of Decentralized Business Models / J. Chen, C. Bellavitis // *Journal of Business Venturing Insights*. – 2020. – Vol. 13. – Article e00151. – DOI: 10.1016/j.jbvi.2019.e00151.