# THE PARTICULARITIES OF CYBER SECURITY RISK MANAGEMENT IN CRYPTOCURRENCY TRANSACTIONS

**UDC: 005.334:[336.747.5:004.056.55]**
**DOI:** https://doi.org/10.53486/tids2025.12

**LUCHIAN IVAN**
Moldova State University
ivan.luchian@usm.md
**ORCID ID:** 0000-0002-8683-7228

**DONCEV TRAIAN**
Most Organic
tdoncev@gmail.com

**Abstract.** Cryptocurrency is a digital asset based on blockchain technology, enabling decentralized and secure digital transactions. The acquisition, trading and investment in cryptocurrencies are based on the operation of a specialized infrastructure, which includes cryptocurrency exchanges, crypto banks, crypto friendly banks, crypto gateways, platforms and apps. The exponential growth in the number of cryptocurrencies and their integration into financial systems have led to an increased risk of cyber threats, including fraud, theft, and hacking. The article aims to explore the specific cybersecurity vulnerabilities associated with cryptocurrency transactions and reviews the contemporary risk management practices designed to mitigate them. The analysis is based on expert opinions, industry reports, and academic studies. Particular attention is given to the architecture of cyber-attacks and scams in the crypto domain. The research revealed a wide variety of cyber threats to cryptocurrency transactions, which are essentially cyber-attacks and various scam schemes. The objects of criminal activity are the elements of the cryptocurrency market infrastructure and cryptocurrency holdings in digital wallets. All procedures undertaken for to secure cryptocurrency transactions aimed at ensuring protection against fraudulent activities and maintaining the security of digital currency ownership meets the notion of cryptocurrency security. In international practice, complexes of techniques have been developed aimed at ensuring the cyber security of cryptocurrency transactions. The paper examined layered defense strategies that incorporate cryptographic protocols, regulatory frameworks, and artificial intelligence tools. The study emphasizes that effective cybersecurity in cryptocurrency transactions requires a combination of technological, organizational, and legal measures. The findings contribute to a deeper understanding of risk exposure and the practical steps necessary to secure digital assets in an evolving threat landscape.

**Keywords:** cryptocurrency; crypto security; threats; cybercrime; risk management.

**JEL Classification:** B17, F31, L86.

## INTRODUCTION

A cryptocurrency is a digital or virtual currency created by applying encryption algorithms. The use of encryption technologies means that cryptocurrencies function as both a currency and a virtual accounting system. Encryption means the use of algorithms and techniques that protect these inputs, such as elliptic curve encryption, public-private key pairs, and hashing functions. Cryptocurrency is based on a distributed network across a large number of computers, which allows it to operate outside the control of governments and central authorities. The basis of cryptocurrency operation is blockchain technology, which is used to make secure digital payments using tokens. Storage and

transmission of cryptocurrency data between wallets and to public ledgers (Inhope, 2022), (Oswego), (The Investopedia Team, 2024).

According to the information presented by Fabio Duarte (2025), the global number of cryptocurrencies has increased from 50 in the year 2013 to 17134 in April 2025.

Powered by CoinGecko (2025), in the period 01.01.2014-12.05.2025 the level of capitalization of the global cryptocurrency market increased through fluctuations from $10.6 billion to $3450.7 billion.

According to Triple A (2024) in 2024 an estimated 562 million people worldwide (up 34% from 420 million in 2023) owned cryptocurrencies. And for the 2025, the number of people who will use cryptocurrencies was estimated at 861.0 million, which constitutes 11.0% of the world population (Kumar, 2025).

The purpose of this article is to examine the essence of cyber risks of cryptocurrency transactions and their management technologies

## MAIN CONTENT

### 1. Materials and Methods

Cryptocurrencies themselves and the market formed by them remain a relatively little studied field, with advertising information about the attractiveness of investing in them and their use as a payment instrument prevailing in the internet space. At the same time, potential investors remain relatively poorly informed about the associated risks. The research on the topic was based on screening information provided by specialized companies, expert opinions, and academic papers available on the internet. The study examined the essence of cryptocurrencies and provided expert advice on the risks of cryptocurrency transactions, as well as technologies for managing the cybersecurity of these activities. As a result, a summary presentation was developed on the essence of cyber risks of cryptocurrency transactions, followed by a complex vision of their management.

### 2. Results and Discussion

The complex of activities carried out to secure cryptocurrency transactions against criminal activities and to maintain the security of digital currency are collectively known as cryptocurrency security (Arkose Labs).

In this setting, specialists from Darktrace expressed that cybersecurity for cryptocurrency (crypto cybersecurity) is a fundamental thought within the quickly advancing world of digital assets. As more people and businesses grasp cryptocurrencies, the move to digitizing assets presents important vulnerabilities that require security measures. Moreover, as cryptocurrency develops in ubiquity, these digital assets are progressively uncovered to threat actors.

Additionally, cryptocurrency transactions are digital in nature and involve a sophisticated backend process, according to the experts at Arkose Labs. Blockchain, which is basically a distributed database or ledger that is shared among several computer network nodes, is the technology that powers cryptocurrency security. Blockchain uses cybersecurity frameworks and best practices to offer comprehensive risk management against cyber threats. Information and communication are protected by cryptography, which employs codes to make sure that only those with permission may access them.

Cybercrime in the cryptocurrency market refers to criminal activities related to the theft (or otherwise illegal acquisition) of cryptocurrencies and some methods or security vulnerabilities exploited.

In 2021, 0.15% of known cryptocurrency transactions were linked to illicit activities such as cybercrime, money laundering, and terrorist financing, with a total volume of $14 billion (Mengqi Sun, David Smagalla, 2022).

The Immunefi Crypto Losses 2022 Report cites losses from fraud and hacking as a combined total of $3.9 billion for the year and $8 billion for 2021 (Melinek, 2023).

In 2023, the FBI reported on cryptocurrency fraud that cost American investors $4.8 billion (Yaffe-Bellany, 2025).

Two types of cybercrimes are committed in the cryptocurrency market: cyber-attacks and scams.

A cyber-attack is any criminal activity with the intent to steal, expose, modify, disable, or destroy data, applications, or other information assets through unauthorized access to a network, computer system, or digital device (IBM, 2025).

In this field, the main form of illegal activity is hacking aimed at gaining unauthorized access to a computer system or network.

Examples include attacks on cryptocurrency exchanges and digital wallets (Malmqvist, Maartmann-Moe, 2025):

- *Exchange hacking*. Cryptocurrency exchanges are basically digital platforms where individuals can buy, sell, or keep their coins. Because these exchanges often maintain significant amounts of cryptocurrencies, they are attractive targets for cybercriminals. Hackers employ different attack methods, including phishing and social engineering, to take coins that are stored in active wallets on the exchange.
- *Bridge attack*. A bridge attack is a type of cyberattack on cryptocurrency trading services, whereby cybercriminals focus on cryptocurrency while it is being transferred between different blockchains.
- *Wallet hacking*. Digital wallets are designed to hold, oversee, and exchange cryptocurrencies. Cybercriminals can take advantage of software or network vulnerabilities to break into a user's device, gain access to the crypto wallet, and steal the currency stored in it.
- *Phishing attack*. Users are deceived into disclosing their private keys. If an individual loses access to the private key associated with a wallet, the assets become irretrievably lost. A prevalent form of digital attack is executed by criminals who send emails, thereby misleading users into divulging sensitive information or downloading malware, which can enable the hacker to gain access to the crypto wallet and misappropriate their assets.
- *Malware*, or malicious software, is any program or file that's intentionally harmful to a computer, network or server (Kinza Yasar, Ben Lutkevich, 2024). Due to their code-based nature, cryptocurrencies and associated software may have flaws that hackers might take advantage of. Any vulnerability in the crypto architecture allows them to alter the code. For instance, they are able to conduct bridge attacks and hack bitcoin exchanges.
- *Theft of crypto keys*. Users must utilize keys to access their cryptocurrency wallets and exchanges, and if hackers are able to obtain these keys or the passwords that secure them, they can launch attacks on cryptocurrencies.

- *DDoS attacks on cryptocurrency exchanges*. A Distributed Denial-of-Service (DDoS) attack aims to disrupt the operation of a target system by overwhelming it with a massive stream of Internet traffic. When it comes to blockchain networks, DDoS attacks take a unique form due to the decentralized nature of the technology and lead to several negative effects for cryptocurrency users. One of them is the delay in transactions. As spam transactions clog the network, legitimate transactions can experience processing delays or even get stuck in queues waiting for confirmation. The situation can be especially serious for users who need timely completion of transactions for trading or other financial activities. During periods of high congestion caused by DDoS attacks, transaction fees can increase sharply as users compete for limited processing capacity (Trust, 2025).

*A cryptocurrency scam* is a complex of fraudulent activities aimed at deceiving a person or organization into dispossessing them of their digital assets. It can take many forms and is often based on emotions such as fear or greed (Allie Grace Garnett, 2025).

The most common types of cryptocurrency scams are considered to be the following (Allie Grace Garnett, 2025):

- *Cryptojacking* is the act of using a computer to mine cryptocurrencies, often through websites, against the user's will or while the user is unaware (Caprolu et al., 2021). Cryptojacking can lead to slowdowns and crashes due to the demand on computing resources. Proof-of-work mining for cryptocurrencies such as Bitcoin requires significant computing power and resources. Cryptojackers reap all the benefits of mining cryptocurrencies at no cost, while the device owner consumes electricity and the device malfunctions. Visiting an infected website or downloading compromised software can allow malicious code from a cryptojacker to enter the digital device.
- *Fake ICOs*. Although it lacks the infrastructure and technology necessary to support it, a fake initial coin offering (ICO) has all the characteristics of a real one. In essence, it is the launch of a coin that exists in name only. A fake ICO usually ends with the developers disappearing once the ICO proceeds are collected.
- *Sensitive information theft*. Hackers often target private keys, which are important for accessing digital wallets. Once these keys are compromised, the hacker gains full control over the victim's assets, leading to their loss.
- *Crypto mining*. Crypto mining involves using certain computing resources to validate transactions and secure the blockchain network. Cybercriminals sometimes deploy mining malware, which covertly uses the victim's computer power to mine cryptocurrencies for the attacker. This not only slows down the victim's device, but also increases their electricity costs.
- *Cloud mining scams*. Cloud mining services, often referred to as mining-as-a-service, represent a legitimate business model; however, certain cloud mining companies engage in fraudulent activities. A company might assert that it provides cloud mining services, frequently guaranteeing appealing returns in return for an initial payment. The anticipated returns may never be realized, as the company may not possess the mining equipment.
- *Social engineering schemes* are designed to manipulate individuals into revealing confidential information. Scammers often pose as trustworthy individuals or offer investment opportunities that seem too good to be true.
- *Insider threats* come from individuals within an organization (companies, institutions) who have access to sensitive information and who can abuse their positions to steal digital currency or sabotage security measures.

- *Fake wallets*. A fraudulent (fake) wallet scheme deceives individuals into thinking they are utilizing a genuine digital wallet for asset storage. This counterfeit wallet prompts users to input their private keys, which the scammers subsequently exploit to misappropriate cryptocurrency assets. Fake wallet apps can be found in app stores or promoted through phishing emails.
- *Pump-and-dump schemes*. Scammers use a variety of strategies to artificially raise (or pump) the price of a digital asset in this cybercrime. The scammer sells his tokens on the open market right away when the price is inflated. The rapid increase in the supply of tokens causes their price to plummet, but not before the scammer has made a profit. By making false or misleading claims and purchasing huge amounts of a low-value token all at once, scammers can artificially boost its price.
- *Blockchain-wide attacks***.** Scammers can target entire cryptocurrency networks, and techniques may include the following:
  - *51% attacks*, which involve a single entity obtaining control over more than half of the mining power of a blockchain or cryptocurrency;
  - *Sybil attacks*, or the creation by a single entity of multiple false identities (nodes) to criminally influence network operations;
  - *Routing attacks* involve the participation of a malicious actor that manipulates data routing information to illicitly intercept, alter, or block communication among blockchain nodes;
  - *Time jacking attacks* occur when a malicious actor modifies the timestamps of a network's nodes, creating confusion and enabling the attacker to double-spend cryptocurrencies;
  - *Eclipse attacks* are carried out by hoodlums segregating one or more blockchain hubs with the point of giving wrong data to the isolated node;
  - *Long-range attack* are a hypothetical shape of assault that includes hoodlums making a modern fork of a blockchain from a far-off point within the past, making false exchanges show up genuine;
  - *Selfish mining attacks* happen when mineworkers effectively prepare a modern square but don't transmit this data to the arrange, furtively mining another piece. Such attacks have not however been recognized, but is hypothetically conceivable.

To uncover criminal activities in the cryptocurrency market, experts recommend using the ten red flags system (Merkle Science, 2025):

1. *Smurfing* involves splitting large transactions into smaller transactions to avoid compliance alerts;

2. *Peel chains*. To distribute stolen money, criminals frequently practice transferring money between several wallets. This idea is carried out by a peel chain, which transfers progressively smaller sums to more wallets;

3. *Rapid movement of funds*. Predictable patterns, like keeping a current balance or holding coins for a long time, are indicative of legitimate wallet activity. Within minutes of receiving the money, a criminal wallet can be completely depleted, indicating a brief halt end route to its ultimate destination;

4. *Incongruous trading volume*. Users are required to reveal their sources of pay and assessed exchange sums as portion of the Know Your Client (KYC) handle. A major red flag is when exchange volume distant surpasses these declarations;

5. *Involvement with high-risk jurisdictions*. Blacklisted nations are often regarded as high-risk. Additionally, there is a grey list of countries that are being enhanced monitored for strategic flaws in their counterterrorism finance and anti-money laundering regulations;

6. *Association with dark net marketplaces*. By buying products and reselling them for clean fiat money, criminals can use dark net markets to launder cryptocurrency. They also facilitate and enable the illicit trade of commodities and services. Sometimes, these products might end up in the hands of terrorist or criminal groups;

7. *Use of coin mixers or tumblers*. Coin mixers, sometimes referred to as tumblers, combine money from several users, severing the connections between transactions. When a user deposits cryptocurrencies into a mixer, for instance, they receive an equivalent amount from other funds that have been pooled;

8. *Sending funds to clustered wallets*. Multiple crypto addresses can be created by an individual. Clustering algorithms are used in blockchain analytics to find wallets that are probably under the control of the same person. Transferring money to many wallets may be a sign of wash trading, which is used to conceal illegal transactions or increase currency trade volumes;

9. *Chain hopping*

10. *Use of privacy coins*. Privacy coins prioritize user anonymity. Criminals can use them to hide their transactions from regulatory scrutiny.

International cyber practice has developed a set of recommended measures for managing risks related to cryptocurrency transactions (Arkose Labs):

- *Risk assessment*. It is essential to carry out a thorough risk evaluation to pinpoint possible weaknesses, dangers, and risks related to cryptocurrency operations, in addition to prioritizing efforts for mitigation;
- *Private key protection*. Cryptocurrency transactions involve the use of cryptographic keys, particularly private keys, to access and control ownership of these digital assets. It is essential to safeguard private keys through methods like encryption, secure storage solutions, and hardware wallets;
- *Wallet security*. It is necessary to use strong passwords, multi-factor authentication, and regular updates of wallet software to improve wallet security;
- *Two factor authentication*. It is advised to enable two-factor authentication (2FA) to add an extra level of protection to cryptocurrency accounts;
- *Secure transactions*. It is necessary to use extra security features like transaction signing and encryption to confirm the recipient's wallet address;
- *Network security*. Network monitoring and cryptographic algorithms are necessary to defend blockchain infrastructure against bot-generated attacks like DDoS attacks. Strong encryption, virtual private networks, firewalls, intrusion detection and prevention systems, and frequent network device application and updates are also necessary;
- *The security of cryptocurrency exchanges* encompasses strategies to safeguard user accounts and ensure secure storage of assets, two-factor authentication, anti-money laundering and know-your-customer procedures, regular security audits, and compliance with regulatory standards. Additional security features like IP restrictions or withdrawal whitelists must be enabled, and careful consideration must be given when choosing trading partners;

- *Data encryption*. It is imperative to implement encryption measures for sensitive data, both during transmission and while stored, employing a variety of encryption methodologies available to safeguard information against unauthorized access or interception;
- *Smart contract and token security*. The adoption of secure coding methodologies is imperative, and comprehensive testing protocols must be executed prior to deployment;
- *Strong password practices*. Strong password creation advice is required, as are suggestions for using password managers to safely store and handle login information;
- *Access control and user privileges*. Strict user privileges and access controls are advised in order to limit access to sensitive information and systems;
- *Software and firmware updates*. Periodically updating hardware wallet firmware, software clients, and cryptocurrency wallets is necessary since these processes may include security fixes and enhancements for better defense against known threats;
- *Backup and recovery*. Regularly backing up bitcoin wallets and keeping backups safe are essential;
- *Continuous monitoring*. Cryptocurrency security networks and systems must be continuously monitored in order to identify and address any suspicious activity or any security breaches. This will involve the use of monitoring tools, security information and event management systems, intrusion detection systems, and threat intelligence feeds to detect and mitigate security incidents;
- *Incident response and recovery*. Developing an incident response plan, which contains procedures for reporting and analyzing incidents, limiting and mitigating damage, recovering lost funds, and strengthening the security system in order to avoid incidents in the future;
- *User education and awareness*. This is a comprehensive attempt to inform cryptocurrency users about common attack vectors, security best practices, and potential hazards, including social engineering and phishing attempts, as well as the significance of upholding personal security hygiene, which includes creating strong passwords, updating software frequently, and refraining from disclosing sensitive information;
- *Partnering with a security vendor*. After evaluating the security system in terms of data management, access controls and incident response capabilities, it is necessary to select a reliable security provider;
- *Security audits and assessments.* The periodic conduct of audits and assessments is required by the need to assess the efficiency of the security system and detect any vulnerabilities.

Government regulations are of paramount importance in improving the security of cryptocurrency transactions. The Financial Action Task Force's recommendations require cryptocurrency exchanges to implement know-your-customer and anti-money laundering policies to prevent illicit activities. In the United States, the Securities and Exchange Commission enforces compliance regulations for Initial Coin Offerings and other financial activities related to cryptocurrencies (Anifowose et. al., 2022). The Markets in Crypto-Assets Regulation establishes legal rules across the European Union for the issuance and trading of crypto-assets, including transparency, disclosure, authorization and supervision of transactions and the activities of crypto-asset service providers (Abramova, Andreeva, 2025).

In all of these regulatory measures, challenges persist in enforcing global compliance due to the decentralized nature of cryptocurrencies. Regulatory arbitrage, where entities operate in jurisdictions

with lax regulations, undermines the effectiveness of security measures. International collaboration between regulatory agencies is needed to address this issue (Anifowose et. al., 2022).

The emphasis on privacy and anonymity in the cryptocurrency market makes it difficult to identify criminals. However, there are certain tools that law enforcement agencies operate to identify criminal users. They work closely with cryptocurrency companies to track transactions on the blockchain and conduct on-chain investigations. Given that the technology is developing at a rapid pace, collaboration between law enforcement and the crypto financial market is vital to ensure that government institutions are informed about the latest technologies (Inhope, 2022).

Artificial intelligence (AI) has become a tool for detecting and preventing cyber threats in cryptocurrency transactions. AI-based fraud detection systems examine transaction behaviors and identify suspicious activity in real time. Machine learning models are trained on historical fraud data to increase detection accuracy. For example, AI algorithms can flag transactions related to money laundering, such as rapid movement between multiple wallets. These solutions provide an additional layer of security, supplementing cybersecurity measures. At the same time, AI-based systems also face challenges, including adversarial attacks in which hackers manipulate AI models to avoid detection (Anifowose et. al., 2022).

An important aspect of ensuring the security of cryptocurrency companies and platforms is conducting audits, which include code reviews, penetration tests, and risk assessments to detect potential vulnerabilities before fraudsters take advantage of them. A crypto audit also provides a comprehensive review of a company's operations, systems, and processes to ensure compliance with external and internal security standards (Malmqvist, Maartmann-Moe, 2025).

## CONCLUSIONS

The dynamic expansion of the cryptocurrency market has made it a prime target for increasingly sophisticated cyberattacks. Although blockchain technology provides inherent security features such as decentralization and cryptographic validation, these alone are insufficient to ensure comprehensive protection. Cyber threats-including hacking, phishing, insider threats, and advanced scam schemes-highlight the urgent need for robust cybersecurity strategies.

This study has shown that an effective defense against cryptocurrency-related cyber risks must include a multi-layered approach that combines: technical safeguards (e.g., key encryption, secure wallets, AI-based monitoring); regulatory compliance (e.g., KYC/AML frameworks, international standards); and user education to build awareness of potential vulnerabilities.

The role of artificial intelligence in real-time fraud detection is growing, though it must be supplemented by continuous audits and adaptive risk management practices. Furthermore, international cooperation among regulators, cybersecurity firms, and crypto platforms is essential to close jurisdictional gaps and ensure effective enforcement.

Future research should explore quantum-resistant cryptographic protocols and the integration of decentralized AI in securing blockchain infrastructures. Only through a holistic and proactive approach can the long-term security and trustworthiness of cryptocurrency ecosystems be maintained.

## REFERENCES

1. Abramova Alisa, Andreeva Julia, 2025. *EU Crypto Regulations 2025*. Available at: https://sumsub.com/blog/eu-crypto-regulations/. [Accessed 14.05.2025]

2. Anifowose Victor, Mei Song, Nicole Reed (2022) *Cybersecurity Frameworks for Crypto Transactions*. Available at: https://www.researchgate.net/publication/389079078_Cybersecurity_Frameworks_for_Crypto_Transactions. [Accessed 28.04.2025]
3. Arkose Labs. *Guide to cryptocurrency security*. Available at: https://www.arkoselabs.com/explained/guide-to-cryptocurrency-security/. [Accessed 28.04.2025]
4. Caprolu Maurantonio, Raponi Simone, Oligeri Gabriele, Di Pietro Roberto, 2021. *Cryptomining makes noise: Detecting cryptojacking via Machine Learning*. Available at: https://www.sciencedirect.com/science/article/pii/S0140366421000797?via%3Dihub. [Accessed 10.05.2025]
5. CoinGecko, 2025. Available at: https://www.coingecko.com/en/global-charts#:~:text=The%20global%20cryptocurrency%20market%20cap,a%20Bitcoin%20dominance%20of%2061.03%25. [Accessed 12.05.2025]
6. Darktrace. *What is crypto cyberseucity?*. https://www.darktrace.com/cyber-ai-glossary/crypto-cybersecurity#:~:text=Cybersecurity%20for%20Crypto%20is%20an,vulnerabilities%20that%20require%20security%20measures. [Accessed 07.05.2025]
7. Duarte Fabio, 2025. How Many Cryptocurrencies are There In 2025?. Available at: https://explodingtopics.com/blog/number-of-cryptocurrencies. [Accessed 07.05.2025]
8. Garnett Allie Grace, 2025. *Cryptocurrency scams: 8 crypto cons to avoid*. Available at: https://www.britannica.com/money/cryptocurrency-scams. [Accessed 01.06.2025]
9. IBM, 2025. *What is a cyberattack?*. Available at: https://www.ibm.com/think/topics/cyber-attack. [Accessed 06.05.2025]
10. Inhope, 2022. *What is Cryptocurrency?*. Available at: https://www.inhope.org/EN/articles/what-is-crypto. [Accessed 08.05.2025]
11. Kumar Naveen, 2025. How Many Cryptocurrencies Are There in 2025?. Available at: https://www.demandsage.com/number-of-cryptocurrencies/#:~:text=The%20Future%20Of%20Cryptocurrencies&text=The%20number%20of%20cryptocurrency%20users,by%20the%20end%20of%202025. [Accessed 12.05.2025]
12. Malmqvist Ritva, Maartmann-Moe Carsten, 2025. *Summary of Cryptocurrency and Blockchain Risks, Protections, and the Importance of Audits*. Available at: https://advisense.com/2025/03/13/cryptocurrency-and-blockchain-risks/. [Accessed 07.05.2025]
13. Melinek Jacquelyn, 2023. *Crypto losses in 2022 dropped 51% year on year to $4B*. Available at: https://techcrunch.com/2023/01/05/crypto-losses-in-2022-dropped-51-year-on-year-to-4b/. [Accessed 07.05.2025]
14. Merkle Science, 2025. *Top 10 Red Flags to Watch for in Crypto Transactions*. Available at: https://www.merklescience.com/blog/top-10-red-flags-to-watch-for-in-crypto-transactions. [Accessed 19.05.2025]
15. Oswego. *The Basics about Cryptocurrency*. Available at: https://www.oswego.edu/cts/basics-about-cryptocurrency. [Accessed 07.05.2025]
16. Sun Mengqi Smagalla David, 2022. *Cryptocurrency-Based Crime Hit a Record $14 Billion in 2021*. Available at: https://www.wsj.com/articles/cryptocurrency-based-crime-hit-a-record-14-billion-in-2021-11641500073. [Accessed 07.05.2025]
17. The Investopedia Team, 2024. *Cryptocurrency Explained With Pros and Cons for Investment*. Available at: https://www.investopedia.com/terms/c/cryptocurrency.asp. [Accessed 08.05.2025]
18. Triple A, 2024. *Global Crypto Ownership Reaches 562 Million People in 2024: New Report*. Available at: https://www.triple-a.io/blog/crypto-ownership-report. [Accessed 19.05.2025]

19. Trust, 2025. *DDoS attacks in blockchain networks, explained*. Available at: https://trustwallet.com/blog/security/ddos-attacks-in-blockchain-networks-explained. [Accessed 19.05.2025]
20. Yaffe-Bellany David, 2025. *The Cryptocurrency Scam That Turned a Small Town Against Itself*. Available at: https://www.nytimes.com/2025/02/19/magazine/cryptocurrency-scam-kansas-heartland-bank.html. [Accessed 06.05.2025]
21. Yasar Kinza, Lutkevich Ben, 2024. *What is malware? Prevention, detection and how attacks work*. Available at: https://www.techtarget.com/searchsecurity/definition/malware. [Accessed 06.05.2025]