

**СЕКЦІЯ 8.**  
**ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ. КОМП'ЮТЕРНА**  
**ІНЖЕНЕРІЯ. КІБЕРБЕЗПЕКА. ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ**  
**СИСТЕМИ**

*UDC 004*

**Belous A.O., bachelor`s student**  
**Nakoriakov O.H., PhD student**  
Odesa Polytechnic National University, [belousanna2004@gmail.com](mailto:belousanna2004@gmail.com)

**DEFENSE OF FINANCIAL TRANSACTIONS WITH THE HELP OF BLOCKCHAIN TECHNOLOGY**

The rapid digitalization of financial systems has increased the vulnerability of transactions to cyberattacks, fraud, and unauthorized access. Ensuring the integrity and confidentiality of financial operations is a top priority for modern institutions.

Blockchain technology offers a robust framework for enhancing the security and efficiency of financial transactions. There are lots of security reasons:

- **Immutability:** once transactions are recorded in the blockchain, they cannot be altered or deleted, which guarantees data integrity.
- **Transparency:** all participants in the network have access to the distributed ledger, making it easier to detect and prevent fraudulent activities.
- **Smart contracts:** these are self-executing agreements with predefined rules encoded directly into the blockchain - eliminate the need for third-party intermediaries, thereby reducing costs and enhancing trust.
- **Consensus mechanisms:** protocols such as Proof of Work and Proof of Stake, ensure that transactions are validated through decentralized agreement rather than centralized authorities, maintaining system reliability.
- **Decentralization:** enhances resilience and reduces the risk of single points of failure, contributing to greater security and operational stability in financial systems.

In practice, blockchain is already actively used in various financial applications: ripple (XRP) provides fast and secure international money transfers by using blockchain instead of traditional banking infrastructure; JP Morgan's Onyx is a private blockchain platform designed for real-time interbank payments; decentralized Finance (DeFi) platforms, such as Uniswap and Aave, allow users to exchange and lend digital assets directly, without intermediaries, through smart contracts; Central Bank Digital Currencies (CBDCs) are being developed by governments using blockchain technology to modernize and secure national monetary systems [1].

Despite the numerous advantages that blockchain technology offers - particularly in terms of transparency, immutability, and decentralization - it is not entirely immune to security risks. As the adoption of blockchain in financial applications grows, so too does the importance of understanding the potential vulnerabilities associated with it. Below are some of the most critical threats that persist even in blockchain-based environments:

1. **Vulnerabilities in Smart Contracts:** smart contracts are self-executing programs with the terms of the agreement directly written into code and deployed on the blockchain. While they eliminate the need for intermediaries, they can also introduce significant risks if poorly written or insufficiently audited. Numerous Decentralized Finance (DeFi) platforms have experienced severe breaches resulting from logic flaws or programming errors in smart contracts.

One notable example is the Poly Network hack in 2021, where attackers exploited a vulnerability and stole over \$600 million in assets. Another instance includes the bZx protocol,

which suffered multiple attacks due to design flaws. These cases highlight the need for rigorous code auditing and formal verification before deploying smart contracts in financial systems [2].

2. Loss or Theft of Private Keys: The security of blockchain transactions fundamentally depends on cryptographic private keys. If a user loses access to their private key, the associated assets become permanently inaccessible. Conversely, if a private key is stolen - through malware, phishing, or insecure storage - the attacker gains full control over the assets.

Unlike traditional banking systems, blockchain does not offer password recovery or centralized account restoration mechanisms.

This underscores the importance of secure key management practices, such as hardware wallets, cold storage, or multi-signature schemes.

3. Social Engineering Attacks: even the most secure technological systems are susceptible to human error. Social engineering attacks, such as phishing emails, fraudulent websites, and fake wallet interfaces, target users rather than the blockchain infrastructure itself.

For instance, in recent years, fake MetaMask browser extensions and phishing campaigns have tricked users into revealing their private keys or seed phrases, leading to irreversible financial losses. Security awareness and user education are essential to mitigate such risks.

4. 51% Attacks: a 51% attack occurs when a single entity or group gains control of more than half of the blockchain network's computational power (in Proof-of-Work systems) or staked assets (in Proof-of-Stake systems). This allows the attacker to reverse transactions, double-spend coins, and prevent new transactions from being confirmed. While such attacks are unlikely on major blockchains like Bitcoin or Ethereum due to their scale and decentralization, smaller or newer networks remain vulnerable. This risk highlights the need for strong consensus mechanisms and widespread participation in the network [3].

Looking ahead, blockchain is expected to evolve in several promising directions. The mass adoption of CBDCs will bring blockchain into mainstream finance. Integration of artificial intelligence may automate fraud detection and enhance real-time monitoring. Zero-knowledge proofs will offer greater privacy by verifying transactions without revealing sensitive information. Additionally, interoperability solutions will improve cross-chain communication, enabling broader, more flexible financial ecosystems.

Moreover, ongoing research and education are essential to fully harness blockchain's potential while mitigating its risks. As the technology rapidly evolves, professionals in finance and cybersecurity must stay informed about new vulnerabilities and advancements to implement effective security measures and maintain trust in blockchain-based financial systems [4].

In conclusion, blockchain technology represents a transformative force in securing financial transactions. While challenges remain, continuous development and careful implementation will play a crucial role in shaping a safer, more transparent digital financial future.

### References

1. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. — 2008. — Режим доступу: <https://bitcoin.org/bitcoin.pdf>
2. Buterin V. A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum White Paper. — 2014. — Режим доступу: <https://ethereum.org/en/whitepaper/>
3. Peters G.W., Panayi E. Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money // Banking Beyond Banks and Money. — Springer, 2016. — P. 239-278. — DOI: 10.1007/978-3-319-42448-4\_13
4. Zheng Z., Xie S., Dai H., Chen X., Wang H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends // 2017 IEEE International Congress on Big Data (BigData Congress). — 2017. — P. 557-564. — DOI: 10.1109/BigDataCongress.2017.85