DOI: doi.org/10.47363/JAICC/ICAIC2025/2025(4)17

International Conference on
Artificial Intelligence and Cybersecurity (ICAIC 2025)

Conference Proceedings

November 27-28, 2025 (Virtual)

AI-Driven Cybersecurity and Anomaly Detection in Blockchain

Vladimir Gorgadze

Associate Professor, Chair of Blockchain Department at Moscow Institute of Physics and Technology, Russia

Abstract

AI-Driven Cybersecurity and Anomaly Detection in Blockchain While the decentralized and open-source nature of blockchain provides inherent security, vulnerabilities can still exist. AI tools and models can significantly bolster cybersecurity by identifying unusual patterns, detecting threats in real-time, and automating responses to maintain network integrity, prevent fraud, and enhance overall resilience. AI can detect fraud in real-time, predict vulnerabilities, and automate smart contracts for improved efficiency. It strengthens security by identifying unusual patterns that may indicate potential threats or breaches. AI-powered anomaly detection, utilizing techniques such as Long Short-Term Memory networks, can continuously monitor multi-sensor data streams to detect malicious data injection and sensor malfunctions in real-time, recording alerts on a blockchain ledger for incorruptibility and authenticity. Machine learning algorithms can analyze vast amounts of blockchain address and transaction data to identify patterns indicative of malicious activity, such as deviations from typical patterns or known fraud signatures. This includes detecting double-spending, transaction spamming, or unusual transaction volumes. In Decentralized Finance, AI-powered fraud detection systems, employing machine learning and graph-based algorithms, can map complex wallet connections, detect high-risk addresses, and adapt to changing scammer tactics in real-time. This capability is critical for Anti-Money Laundering audits. The ability to freeze accounts, block transfers, or notify users instantly is a key benefit of real-time AI fraud detection in crypto, as transactions are often fast and irreversible. One of the use cases our group implemented was using a modified Smart-LLaMa model to determine the reliability rating of blockchain addresses. We used large language models for detecting vulnerabilities in closed-source Ethereum smart contracts. The model was fine-tuned on a collected dataset of operational codes to adapt to the semantics of compiled smart contracts. The method allows for assessing the reliability of addresses based on the technical content of contracts, eliminating dependence on the source code, which is an excellent tool for enhancing the security of decentralized applications amidst the growing number of attacks on blockchain.