

A Multi-Network Blockchain Framework for Rapid Fund Protection and Transaction Data Analysis in Compromised Cryptocurrency Wallets

M.M.H.M. Jayakodi, M.P.S.K.N. Thilakarathna, and G.F. Nufla

Department of ICT, Faculty of Technological Studies, University of Vavuniya, Sri Lanka

Abstract

Cryptocurrency wallet security is vital, with private key compromises causing \$2.2 billion in losses in 2024 (Chainalysis, 2024). This research introduces a multi-network blockchain framework to safeguard funds in compromised wallets. The primary objective is to develop a bot that, upon manual activation after a private key leak (e.g., phishing), scans all EVM-compatible networks (Ethereum, Arbitrum, Base, Optimism, BNB Chain) for any tokens (native or ERC-20) exceeding \$1 in value, prioritizes transfers high to low, and handles gas shortages via automated cross-chain swaps. Methods include a literature review on wallet vulnerabilities (Li et al., 2020) and blockchain analytics (Bogner et al., 2019), bot implementation using Python with web3.py for EIP-1559-optimized transfers, and HTTP RPC (Infura endpoints) for monitoring. Enhancements utilize free APIs: Moralis for comprehensive asset scanning (listing network, token contract address, amount, USDT value), CoinGecko for real-time pricing and sorting, Etherscan for gas estimation (with a 5x buffer for safety), and 1inch for cross-chain swaps (e.g., swapping ARB ETH to OPETH if gas is insufficient). The framework's dashboard requires only the hacked wallets private key and a safe address, enabling quick (few seconds) scanning and transfers. Testing on Sepolia and Arbitrum Goerli simulated 100–1,000 transfers, validating 10-second speed and over 95% success rate, with Telegram notifications for transfers (e.g., “Transferred \$10 USDT at 14:30”). Major findings reveal Arbitrum gas fees of 0.0001 ETH compared to Ethereum’s 0.01 ETH, with K-means clustering (scikit-learn) detecting anomalies (95th percentile fees) as hacker indicators. The framework achieves 98% fund protection, but limitations include manual activation and HTTP latency (1–2s). The proposed research concludes that the bot minimizes losses by prioritizing high-value assets and enabling swaps, advancing blockchain security. Future implications involve automated hack detection (e.g., 2+ transactions in 10s) and DeFi integration.

Keywords: Blockchain Security, Wallet Protection, Cross-Chain Swaps, Asset Prioritization, Transaction Analytics.