

Development of Passwordless Authentication Based on Blockchain Technologies

Ilyas Mukash

Department of Information Systems, Kazakh-British Technical University, Kazakhstan

Yenlik Begimbayeva

Department of Information Systems, Satbayev University, Kazakhstan

Abstract:

This study presents Zero-Touch Blockchain Authentication (ZTBA), a passwordless framework designed to remove reliance on centrally stored secrets while improving security and usability in high-risk digital services. The architecture integrates decentralized identifiers (DIDs), Ethereum smart contracts, asymmetric challenge-response signatures, and an AI-driven contextual risk module that evaluates device trust, geolocation consistency, and behavioral signals during login and recovery operations. A prototype implementation was tested through controlled attack simulations (replay, man-in-the-middle, phishing-oriented credential stuffing), performance benchmarking, and domain-specific scenarios in FinTech, e-commerce, and healthcare settings. Results show that the proposed model reduced authentication falsification risk by 40% compared with baseline centralized flows, prevented simulated phishing/MITM compromise in all tested sessions, and maintained practical response times (2.8 s in FinTech, 3.1 s in e-commerce, and 4.5 s in healthcare). Under concurrent enterprise-style verification loads, the system sustained throughput above 150 verification transactions per second on an L2 test environment, while remaining interoperable with FIDO2, WebAuthn, and OAuth 2.0 identity ecosystems. The study also evaluated DID-linked recovery pathways, where low-risk scenarios restored account access quickly without reintroducing centralized password-reset weaknesses. The findings indicate that blockchain-anchored passwordless authentication can deliver stronger auditability, resilient trust distribution, and improved user experience, making it a viable foundation for scalable digital identity in Web3 and enterprise infrastructures.

Keywords:

Blockchain, passwordless authentication, decentralized identity, smart contracts, cybersecurity.