Blockchain Security and Cryptographic Approaches

Abstract: This research examines security mechanisms in blockchain systems, focusing on consensus algorithms, smart contract vulnerabilities, and cryptographic primitives. We analyze common attack vectors including 51%% attacks and double-spending.

Introduction

Blockchain technology has revolutionized distributed systems through its decentralized and immutable ledger. However, security remains a critical concern as blockchain applications handle increasingly valuable assets.

Smart Contract Security

Analysis of Ethereum smart contracts reveals common vulnerabilities including reentrancy, integer overflow, and access control issues. We propose automated verification tools and best practices for secure development.