

A Multi-Agent Framework for Auditing Smart Contracts

Thursday 18 September 2025 15:45 (15 minutes)

Smart contracts power a vast array of blockchain applications, securing billions of dollars on decentralized finance, but their immutable nature turns every vulnerability into a permanent and highly exploitable liability. Although automated security tools can efficiently detect many issues, their high false-positive rates and lack of trust still require manual audits, which are costly and introduce deployment delays. In this paper, we present an end-to-end, AI-augmented auditing framework leveraging a multi-agent pipeline for comprehensive vulnerability detection and automated exploit generation.

First, we review existing approaches such as static analysis, fuzzing, symbolic execution, formal verification, and machine-learning methods, highlighting their strengths, limitations, and real-world use.

Building on this survey, we introduce a multi-agent architecture that orchestrates chained AI tools to cross-analyze findings, automatically generate test cases, and produce Proof-of-Concept exploits. The system ingests textual challenge descriptions to outline stepwise attack strategies and synthesizes ready-to-compile Solidity exploit code. Exploits are compiled and validated in a stateless, containerized environment, enabling fully automated verification of attack effectiveness.

To validate our approach, we demonstrate the pipeline on capture-the-flag challenges and discuss how prompt fine-tuning, retrieval-augmented generation, and formal verification integration can further enhance detection accuracy and exploit reliability. Finally, to assess real-world impact, we evaluate the applicability of the framework in online bug bounty platforms and auditing contests, demonstrating its potential to make smart contract security verification more comprehensive, scalable, and cost-effective.

Author: SPATARU, Alexe Luca (Polytechnic University of Bucharest)

Co-author: Mr CARABAS, Costin (Polytechnic University of Bucharest)

Presenter: SPATARU, Alexe Luca (Polytechnic University of Bucharest)

Session Classification: Cloud Computing and Network Virtualisation

Track Classification: Network Security