الجمهورية الشعبية الديمقراطية الجزائرية
People's Democratic Republic of Algeria
وزارة التعليم العالي و البحث العلمي
Ministry of Higher Education and Scientific Research
المدرسة العليا للإعلام الآلي 8 ماي 1945 - سيدي بلعباس
Higher School of Computer Science
8 Mai 1945 - Sidi Bel Abbes

[Graduation/Master's] Thesis

To obtain the diploma of [**Engineering/Master's**] **Degree**

Field of Study: **Computer Science**

Specialization: [**ISI**]

Theme

[Vulnerability Detection In Smart Contracts Using Deep Learning]

Presented by
[**Gaouaoui Kamel**]
Supervised by: [**Alaa Eddine Belfedhal, Oussama Serhane**]

Defended on: [**September , 2025**]
In front of the jury composed of

Dr. [**Dr. ANANI Djihed**]	President of the Jury
Dr. [**Serhane Oussama**]	Thesis Supervisor
Mr. [**Dr. NEGGAZ Imene**]	Examiner

Academic Year: 20XX/20XX

Abstract

Abstract

Smart contracts are integral to blockchain technology, enabling decentralized, trustless, and automated transactions without intermediaries. Their widespread adoption—particularly in finance, supply chains, and governance—has made them attractive targets for attacks due to their immutable and publicly accessible nature. As decentralized applications (DApps) and Decentralized Finance (DeFi) systems increasingly depend on smart contracts, identifying and preventing code vulnerabilities has become a pressing challenge.

Traditional vulnerability detection methods, such as static and dynamic analysis, face limitations in scalability, accuracy, and handling complex behaviors. With the growing number of deployed contracts, manual audits and heuristic tools are no longer sufficient, necessitating advanced and scalable approaches.

This thesis investigates the application of deep learning—known for its success in fields like NLP, image recognition, and cybersecurity—to the detection of smart contract vulnerabilities. We first introduce the core concepts of blockchain, smart contracts (with a focus on Ethereum and Solidity), and the Ethereum Virtual Machine (EVM). We then explore major vulnerability types, including reentrancy, arithmetic bugs, denial-of-service, and access control flaws.

This thesis provides a state-of-the-art review on the application of deep learning techniques for detecting vulnerabilities in smart contracts. It explores and analyzes the use of various deep learning models—such as RNNs and Transformers—in this context. Additionally, it examines key aspects like dataset quality, feature extraction, model interpretability, and evaluation metrics. By synthesizing current research, this work aims to highlight the potential of deep learning in enhancing smart contract security and to identify promising directions for future developments at the intersection of blockchain and artificial intelligence.

By leveraging deep learning, this research contributes to the development of accurate, scalable, and automated tools for smart contract security—offering promising directions for future research at the intersection of blockchain and artificial intelligence.

Keywords— Blockchain, Smart Contracts, Deep Learning, Vulnerability detection