Chapter 4
Detection of Vulnerabilities in Cryptocurrency Smart Contracts Based on Image Processing

Gabbi Evrard Tchoukouegno De Mofo
University of Ngaoundéré, Cameroon

Ali Joan Beri Wacka
University of Buea, Cameroon

Franklin Tchakounte
https://orcid.org/0000-0003-0723-2640
University of Ngaoundéré Cameroon

Jean Marie Kuate Fotso
Ministry of Scientific Research and Innovation, Cameroon & University of Ngaoundéré, Cameroon

ABSTRACT

*The rate of use of cryptocurrencies through smart contracts and decentralized applications remains continually increasing. Ethereum is particularly gaining popularity in the blockchain community. In this work, the authors are interested in retraining vulnerability and timestamping. They propose a detection method based on the transformation of contracts into images and the processing of the latter using Simhash and n-gram techniques to obtain our contracts into images of size 32*32. They combine a technique to preserve the useful characteristics of images for*

DOI: 10.4018/978-1-6684-8127-1.ch004

exploitation. Training carried out with the convolutional neuronal network (CNN) model on a sample of 50 normal contracts, 50 contracts vulnerable to retraining, and 33 vulnerable to timestamping gave an accuracy of 88.98% on the detection of vulnerable contracts. The singular value decomposition (SVD) technique is capable of efficiently extracting from images, the key features that characterize contracts in Ethereum.

1. INTRODUCTION

A cryptocurrency is a digital, decentralized and virtual currency (no need for banknotes, coins, credit cards, checkbooks) which uses cryptographic algorithms and a protocol called blockchain to ensure the reliability and traceability of transactions.

The idea of this currency dates back to the 1980s. But in concrete terms, we will have, in 1983, David Chaum who will introduce the possibility of withdrawing money electronically from a bank and then spending it at merchants accepting this method of payment (Yazid, 2023). In 1998, Wei Dai was the first to propose the creation of virtual currencies through consensus. He did not issue details about the implementation of the consensus method (Sudhani, Divakar, & Girish, 2022). In 2008, Satoshi Nakamoto unveiled Bitcoin (Paul, 2023), considered the first successful project that was implemented on the blockchain. To ensure its operation, the creator unveils the "proof-of-work" consensus method. This allows peers in the network to communicate with each other and agree on the validity of transactions. However, there are so many cryptocurrencies (Figure 1) these days that it can be difficult to tell them apart. We can have in others: coins, the store of value, the means of exchange, the "exchange" of tokens, Decentralized Finance (DEFI), smart contract platforms (ADAM, 2023). Since its creation, the rate of users of cryptocurrencies has continued to grow over the years. At the end of 2019, there were nearly 2,400 cryptocurrencies on the coin-marketcap site (Vitalik). In 2015, the Ethereum cryptocurrency brought a major innovation to the field of blockchains. This platform enabled the development and deployment of applications on blockchains.

2. SMART CONTRACTS AND MINING

2.1 Smart Contract

Smart contracts are scripts stored on the blockchain. They have a unique address (Joonseok, Sumin, & Keunhyuk, 2023).