Information Technology University

Analysis and Categorization of Smart Contracts on EVM-based Blockchain Networks (Polygon, Binance, Optimism)

Blockchain Project

Phase 1

MSCS22027 – Muhammad Qasim

BSCS21017 – Arham Irshad

Nov 10, 2024

Table of Contents

Introduction

Due to the increasing popularity of EVM-compatible blockchains such as Polygon, Binance Smart Chain (BSC), and Optimism, there is a rapid uptake of DApps and smart contracts. This work explores the taxonomy and application of these smart contracts to identify their distribution by category of token, NFT, and DeFi.

Objective

To perform due diligence on ~10K contracts each from Polygon, Binance, and Optimism networks or broken down, for instance, into token smart contracts, NFTs, wallets, routers, and anything else. The purpose is to track different smart contract platforms and networks as well as provide a comprehensive breakdown of the contract type and quantity within those networks.

Problem Understanding

Description

Given the progressive development of dApps, the blockchain platforms launching smart contracts apply the EVM protocol. However, it should be noted that the types of contracts differ greatly from token contracts and NFTs and extend to DeFi applications and games. Preliminary knowledge about how subnets are spread within the networks, their density or rarity, and their types would provide important information about the ecosystem's growth rate, usage, and potential weaknesses.

Relevance

This analysis helps to reveal patterns of smart contracts in use and assess the appropriateness of the networks for particular uses. Blockchain developers, applicants, and investors can also benefit from it by identifying the most significant smart contracting types and voids to make feasible decisions regarding blockchain development or acquisition of protection against the weaknesses of some specific types.

Expected Outcomes

- **Categorization of Contract Types:** Establishment of the key categories studying tokens, NFTs, DeFi applications, wallets, and others.

- **Deployment Trends:** Comparison of the distribution of each type of contract in various networks.
- **Insights on Contract Usage:** An account of how each network is used, or suggestions for enhancements in either its operations or security measures.

Literature Review

Related Work

- **Blockchain-based Smart Contracts: A Systematic Mapping Study:**

This study is one of the first to categorize academic work About Smart Contracts and initial issues including security, privacy, and performance.

- **Blockchain-based Smart Contracts: A Systematic Mapping Study of Academic Research (2018):**

This paper explores how smart contracts are being implemented and analyzed in academic research and categorizes them into application, security, and scalability.

- **Vulnerabilities and Open Issues of Smart Contracts: A Systematic Mapping:**

A Systematic Mapping: an overview of typical smart contract weaknesses and future research directions of blockchain security that underlines the importance of smart contract categorization and classification.

Technological Foundation

EVM (Ethereum Virtual Machine): EVM is an essential part of Ethereum's compatible networks, such as Binance, Polygon, and Optimism, which enable them to execute smart contracts.

Blockchain Concepts: The core concepts that do have a substantial percentage of influence on the contracts include consensus mechanisms, cryptographic standards, and immutability features.

APIs for Data Collection: Data will be pulled from BscScan, Polygonised, Optimism Etherscan, and MetaMask will enable the acquisition of contact metadata and source codes for analysis.

Research Papers and Articles

- Blockchain-based Smart Contracts: A Systematic Mapping Study

- Blockchain-based Smart Contracts: A Systematic Mapping Study of Academic Research.
- Vulnerabilities and Open Issues of Smart Contracts: A Systematic Mapping.

Project Requirements

Functional Requirements

- **Data Extraction:** Get smart contract details from the Polygonscan website | BscScan website and Optimism etherscan website respectively.
- **Contract Categorization:** Split the contracts into categories which are tokens (ERC-20), Non-Fungible tokens (ERC-721), games, decentralized finance, wallets, and others.
- **Reporting and Visualization:** Produce a report of the outcomes with graphical illustrations of the distribution of the types of contracts.

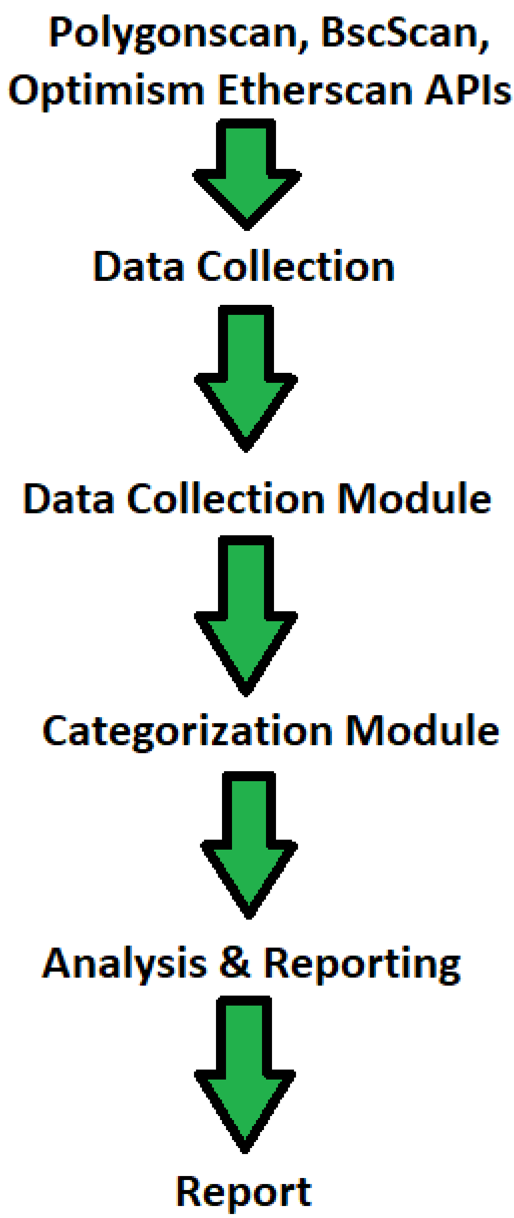
Non-Functional Requirements

- **Performance:** Data extraction and data processing for the management of contracts number more than 10,000 per the given network.
- **Usability:** Gather numerous contracts and organize them systematically, thus there are markers of clear categorizations of contracts for easy analysis.
- **Security:** API data protection, the fact that the API data especially when in transit or storage needs to be protected from access by unauthorized persons, for example, API keys.

Resource Requirements

- **APIs:** Ability to leverage API from Polygonscan, BscScan, and Optimism Etherscan.
- **Development Tools:** For data processing and analysis, Python is majorly used with the help of libraries like the request, to interact with APIs that provide the data, pandas, used for data handling and for getting the visual outputs like bar or line charts we will be using matplotlib or seaborn.
- **Hardware:** Computation capability to accommodate the amount of data storage and processing required to support at least thirty thousand smart contracts.

High-Level Diagram



Conclusion

In this project, we analyzed and categorized smart contracts deployed on three prominent EVM-based blockchain networks: Binance Smart Chain, Polygon, and Optimism. Using the metadata and source code of around {approx 10,000} smart contracts per network fetched from BscScan, Polygonscan, and, Optimism Etherscan APIs. Examining the tokens by their specific features more thoroughly and carefully, we divided them into trends and groups, which were distinguished based on the specifics, tasks, and purposes of tokens: Token contracts, NFTs, DeFi, Games, Wallets, as well as Others.

Further research could elaborate on the performance of contracts in terms of F performance analysis of the specified contracts for blockchains, or vulnerability, and the comparison of functional capabilities of various blockchains. In the same way, while developing blockchain technology and Ether the use of higher-level AI techniques for categorization and automatic identification of new types of contracts emerging within such an environment would expand the picture. The approach described in this project lays down a framework for future continuing smart contract evaluation, which would help build a secure efficient, and user-friendly blockchain environment.

References

Alharby, M., & Van Moorsel, A. (2017). Blockchain-based Smart Contracts: A Systematic Mapping Study. ArXiv. https://doi.org/10.5121/csit.2017.71011

de Sousa Matsumura, G., dos Santos, L.B.R., Conceição, A.F.d., Vijaykumar, N.L. (2021). Vulnerabilities and Open Issues of Smart Contracts: A Systematic Mapping. In: Gervasi, O., et al. Computational Science and Its Applications – ICCSA 2021. ICCSA 2021. Lecture Notes in Computer Science(), vol 12952. Springer, Cham. https://doi.org/10.1007/978-3-030-86973-1_1

M. Alharby, A. Aldweesh and A. v. Moorsel, "Blockchain-based Smart Contracts: A Systematic Mapping Study of Academic Research (2018)," 2018 International Conference on Cloud Computing, Big Data and Blockchain (ICCBB), Fuzhou, China, 2018, pp. 1-6, doi: 10.1109/ICCBB.2018.8756390. keywords: {Smart contracts;Blockchain;Bitcoin;Systematics;Databases;Peer-to-peer computing;Blockchain;Smart contract;Systematic mapping}