# 클러스터링을 이용한 이더리움 기반 스캠 코인 탐지 연구

배유진, 황유나, 강명석, 이승우, 김성수, 최유남, 김현민, 김경곤
한국정보기술연구원 차세대 보안리더 양성 프로그램(Best Of the Best)
ok2006818@gmail.com, ovo6v6@ewhain.net, kms00129@naver.com, sdds3@naver.com,
korkeep@khu.ac.kr, chldbska4834@gmail.com, hyunmini85@gmail.com, anesra+bob10@gmail.com

# Clustering For Detecting Ethereum-Based Scam Coins

Yujin Bae, Yuna Hwang, Myungseok Kang, Seungwoo Lee, Sungsu Kim, Yunam Choi,
Hyunmin Kim, Kyung-gon Kim
KITRI 차세대 보안리더 양성 프로그램(Best Of the Best)

요 약

최근 스캠 코인에 의한 피해 사례가 증가함에 따라 대부분의 가상자산 거래소가 상장된 가상자산에 대해 자체적 신뢰도 평가를 수행하고 있으나, 관련 법·제도적 체계의 부재로 인해 여전히 위험이 존재한다. 스캠 코인 여부를 판단하는 기존 서비스는 불명확한 스캠 코인 판별 기준으로 인해 충분히 신뢰하기 어려우며, 지도 학습에 필요한 라벨링 된 데이터셋이 충분하지 않아 관련 연구 또한 한계를 가진다. 본 논문은 클러스터링을 통해 스캠 코인 여부를 판단하는 것을 목표로 한다. 스캠 코인과 정상적인 가상자산을 구분하는 과정에서 유의미한 데이터를 수집하여 클러스터링을 수행하고, 스캠 코인 여부가 라벨링 된 테스트셋을 구성하여 클러스터링 결과를 평가한다. 이를 통해 본 논문이 제시하는 이더리움 기반 토큰에 대한 클러스터링 결과를 기반으로 추후 통일된 스캠 코인 판단 기준을 세울 수 있음을 제안한다.

## 1 서론

최근 가상자산에 관한 관심이 높아지며 투자자들에게도 큰 인기를 끌고 있다. 하지만 큰 인기만큼 다양한 부작용도 생겨나고 있으며, 일명 '스캠 코인'에 의한 피해 사례가 증가하고 있다. 스캠 코인은 사실과 다른 내용으로 투자자를 속임으로써 투자금을 유치하기 위해 사용되는 가상자산을 뜻한다.

가상자산 거래소는 자체적으로 가상자산에 대한 신뢰도 평가를 수행하고 이를 기반으로 상장·폐지를 하고 있으나, 이와 관련된 법·제도적 체계의 부재로 인해 거래소별 기준이 달라 투자자들의 피해가 발생하고 있다. 가상자산의 스캠 여부를 판단하는 기존 서비스가 존재하지만, 프로젝트가 완성되지 않은 개발 초기부터 거래되는 가상자산의 특성상 명확한 스캠 코인 판단 기준을 정하기 어려우며, 결과 도출 과정에 대한 설명이 충분하지 않고 판별 가능한 가상자산이 한정되어 있다는 한계를 갖는다.

스캠 코인은 판별 기준이 불명확하므로 명시적으로 라벨링 된 대량의 학습 데이터셋이 충분하지 않다. 스캠 코인을 탐지하기 위한 기존의 많은 연구는 지도 학습에 기반하고 있는데, 지도 학습은 명시적으로 라벨링 된 학습 데이터셋을 필요로 한다는 점에서 한계를 갖는다.

이에 본 연구는 클러스터링을 통해 스캠 코인 여부를 판단하는 것을 목표로 한다. 클러스터링은 주어진 데이터들을 특성을 고려하여 부분 그룹(클러스터)으로 나누는 학습 알고리즘으로, 라벨링 된 학습 데이터셋을 필요로 하지 않는 비지도 학습 방법이다. 본 논문에서는 거래 데이터를 구하기 쉬운 이더리움 기반 토큰에 한정하여 연구를 진행한다.

논문의 구성은 다음과 같다. 2장에서는 배경이 되는 연구 및 서비스에 관하여 기술한다. 3장에서는 학습 데이터셋과 클러스터링 과정 및 결과에 관하여 기술한다. 4장에서는 이더리움 기반 토큰에 대한 클러스터링 결과를 기반으로 추후 통일된 스캠 코인 판단 기준을 세울 수 있음을 제안한다.

## 2 연구 배경 및 관련 연구

### 2.1 이더리움 기반 토큰

가상자산(또는 암호화폐)이란 블록체인 기술을 활용하여 개발된 일종의 디지털 화폐로, 핵심 기술인 블록체인을 통해 탈중앙화된 거래 네트워크를 실현한다. 블록체인의 창시자 사토시 나카모토가 개발한

비트코인[1]이 가장 대표적인 가상자산이다.

이더리움은 스마트 컨트랙트 기능을 기술적으로 구현한 블록체인 플랫폼으로, 알려진 블록체인 플랫폼 중 그 규모가 가장 크다[2]. 이더리움 플랫폼에서 작동하는 탈중앙화 어플리케이션(dApp)은 토큰을 발행할 수 있는데, 해당 토큰은 이더리움 생태계에서 사용 가능하다.

이더리움 기반 토큰은 이더리움 블록체인상에서 동작해 거래 활동에 대한 정보를 얻는 것이 쉬우므로 본 연구는 이더리움 기반 토큰의 거래 데이터 일부를 활용해 클러스터링을 진행하였다.

### 2.2 가상자산 이상 거래 탐지

블록체인 기술의 빠른 발전과 가상자산 거래 시장의 성장에 따라 가상자산 거래와 관련된 사기가 점점 늘어나고 있다[3].

비트코인 트랜잭션 내에서 일어나는 사기행위를 클러스터링을 통해 탐지하는 연구에서 비트코인의 거래 데이터, 네트워크 데이터, 블록체인 노드 데이터와 관련된 총 14개의 feature를 추출하였으며 classical k-means 알고리즘과 이상치를 효과적으로 제거할 수 있는 trimmed k-means기법을 사용하여 결과를 비교하였다. 사기라고 알려진 트랜잭션 데이터를 통해 클러스터링 모델의 성능을 검증하였으며, 5가지 비트코인 사기 사건의 트랜잭션을 성공적으로 구별하였다[4].

이더리움 블록체인의 트랜잭션 네트워크 데이터를 활용하여 스캠 탐지를 위한 프레임워크를 제시하는 연구에서 비지도 학습 알고리즘인 one-class SVM을 사용하였으며, 스캠으로 알려진 트랜잭션 데이터를 활용하여 모델을 검증하였다[5].

본 논문은 특정 가상자산에 한정하지 않고 이더리움 기반 토큰 전체에 대해 스캠 여부를 판단하는 모델 구축을 목표로 한다. 따라서 트랜잭션 데이터뿐만 아니라 가상자산 자체의 데이터를 추가로 활용하여 데이터셋을 구축한다는 차별성을 갖는다.

## 3 클러스터링

### 3.1 데이터셋

데이터셋을 수집하기 위해 CoinMarketCap API[6], Twitter API[7], Ethplorer API[8] 를 사용하였으며, 전처리를 거쳐 총 1,551가지 종류의 가상자산의 규모, 기술, 거래와 관련된 11가지 특성(feature)을 수집하였다.

### 3.2 특성

(1) 규모 관련 데이터: 공식 SNS 계정의 활성화 정도를 확인하기 위해 총 글 수, 팔로워 수를 수집하였다. 또한 소스코드 저장소의 활성화 정도를 확인하기 위해 Github 레포지토리의 총 즐겨찾기(Star) 수를 이용하였다. 공식 웹사이트의 SSL 인증서 유무를 확인하여 1 또는 0으로 점수를 주었으며, Alexa rank를 수집하였다. 비유동 주체(holder)의 수를 활용하였다.

(2) 기술 관련 데이터: 백서의 완성도를 확인하기 위해 수집한 백서간의 유사도를 도출하여 15%이상 유사한 백서가 존재할 시 1로, 아니면 0으로 계산하였다. 또한, Etherscan에 등록된 소스 코드와 실제 컴파일 된 소스 코드의 일치 여부를 확인하여 일치할 시 1, 아니면 0으로 데이터를 주었다.

(3) 거래 관련 데이터: 전체 가상자산 중 개발자가 보유하고 있는 비율을 보았다. 개발자가 5%이상 해당 자산을 가지고 있을 시 1로, 아니면 0으로 계산하였다. 또한, 상위 10개의 비유동 주체의 가상자산 보유 비율을 이용하였다.

### 3.3 클러스터링 알고리즘

클러스터링 모델을 위한 알고리즘으로, 거리 기반 클러스터링 알고리즘인 K-Means와 이상치 탐색에 뛰어난 성능을 보이는 밀도 기반 클러스터링 알고리즘인 DBSCAN을 사용했다.

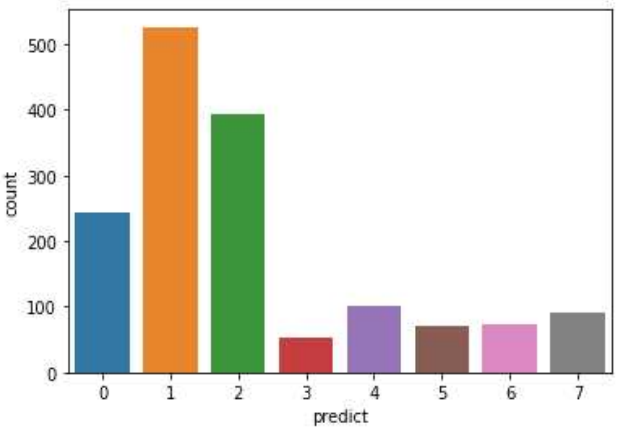
K-Means의 입력 모수인 클러스터 수를 결정하기 위해 silhouette 기법을 활용했으며, silhouette 계수 계산 결과 클러스터 개수를 8로 설정하였다. DBSCAN의 입력 모수인 Eps, MinPts를 결정하기 위해 Eps는 Elbow 기법을 활용한 결과 0.3으로, MinPts는 데이터셋 크기에 자연로그를 취한 결과 7로 설정하였다.

### 3.4 클러스터링 결과

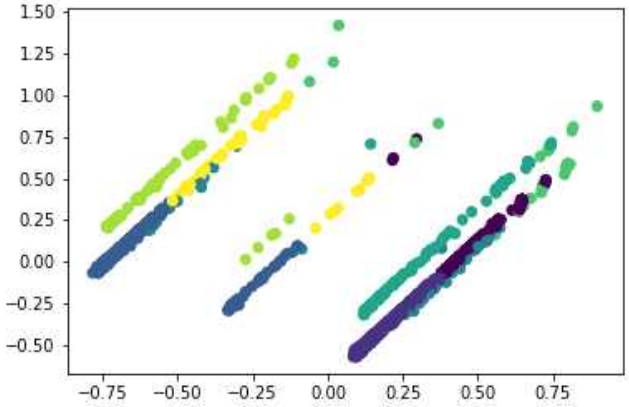
클러스터링 결과를 2차원으로 시각화하기 위해 Standard Scaler를 사용해 PCA 분석을 수행했으며, 분석 결과 variance가 가장 큰 두 개의 특성을 주 차원으로 사용해 클러스터링 결과를 시각화했다. 다음은 각각의 모델의 클러스터링 결과이다.

#### (1) K-Means

각 8개 클러스터의 데이터 분포와 K-Means 클러스터링을 시각화한 결과는 그림 1, 그림 2와 같다.




(그림 1) K-Means 클러스터에 대한 데이터 분포



(그림 2) K-Means 클러스터링 결과

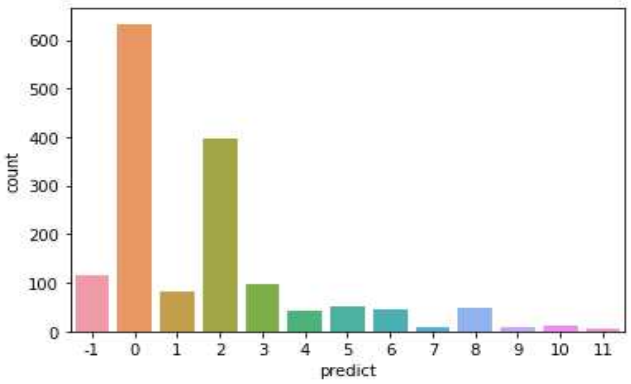
각 8개의 클러스터 중 스캠 코인 클러스터를 특정화하기 위해, 각 클러스터의 센트로이드의 주요 특성에 대한 값을 추출했다. 표 1은 주요 특성에 대한 각 클러스터 센트로이드의 값을 소수점 첫째 자리에서 반올림한 값을 나타낸다.

<표 1> 주요 특성에 대한 K-Means 클러스터 센트로이드의 값

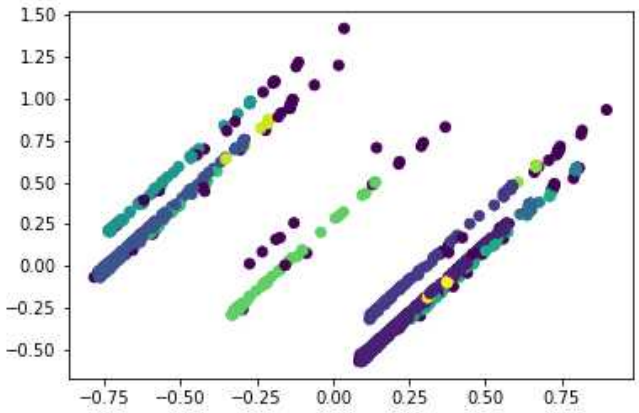
| 라벨 | twt_tweets | twt_followers | alexa_rank | top_holders_rate |
|---|---|---|---|---|
| 0 | 139 | 224 | 42 | 88 |
| 1 | 223 | 356 | 13 | 78 |
| 2 | 270 | 509 | 9 | 79 |
| 3 | 0 | 0 | 97 | 85 |
| 4 | 124 | 90 | 93 | 81 |
| 5 | 109 | 126 | 47 | 77 |
| 6 | 155 | 62 | 89 | 81 |
| 7 | 0 | 0 | 34 | 74 |

공식 SNS 계정이 활성화 되어 있고, 공식 웹사이트의 완성 정도가 높으며, 비유동 주체의 수가 높은 등의 기타 경향을 띠는 클러스터 0, 1, 2를 정상적인 가상자산 클러스터로 구분했다. 스캠 코인으로 이미 알려진 가상자산이 속하며, 공식 SNS 계정의 활성화 정도가 낮고, 공식 웹사이트의 완성 정도가 낮으며, 비유동 주체의 수가 낮은 등 기타 경향을 띠는 클러스터 3, 4, 5, 6, 7를 스캠 위험성이 있는 가상자산 클러스터로 구분했다.

### (2) DBSCAN




(그림 3) DBSCAN 각 클러스터에 대한 데이터 분포



(그림 4) DBSCAN 클러스터링 결과

클러스터링 결과 이상치를 제외한 12개의 클러스터가 만들어졌으며, 각 12개 클러스터에 대한 데이터 분포와 2차원 시각화를 통한 DBSCAN 클러스터링 결과는 각각 그림 3, 그림 4와 같다. 12개의 클러스터 중 스캠 코인 클러스터를 특정화하기 위해, 각 클러스터의 주요 특성에 대한 중간값을 추출했다.

공식 SNS 계정이 활성화 되어 있고, 공식 웹사이트의 완성 정도가 높으며, 비유동 주체의 수가 높은 등 기타 경향을 띠는 클러스터 0, 2를 정상적인 가상자산 클러스터로 구분했다. 이미 스캠으로 알려진 가상자산이 속하며, 공식 SNS 계정의 활성화 정도가 낮고, 공식 웹사이트의 완성 정도가 낮으며, 비유동 주체의 수가 낮은 등 기타 경향을 띠는 클러스터 1, 3, 4, 5, 6, 7, 8, 9, 10, 11 및 이상치를 스캠 위험성이 있는 가상자산 클러스터로 구분했다.

### 3.5 실험 및 평가

실험을 수행하기 위해 가상자산의 신뢰도를 산정하는 주요 서비스 'coinmarketcap', 'Coincodex[9]', 'CryptoCompare[10]', 'coingecko[11]'의 결과를 종합하여 가상자산의 스캠 여부가 라벨링 된 실험 데이터셋을 구성했다.

스캠 코인으로 라벨링 된 실험 데이터셋은 위 4개 서비스의 랭킹에 등록되지 않았고, 일주일 이상 활동이 없으며, 30일 동안 트랜잭션 데이터가 존재하지 않는 가상자산 55종으로 구성되어 있다. 정상적인 가상자산으로 라벨링 된 실험 데이터셋은 위 4개 서비스의 랭킹 등수 평균이 100등 이내이고, 활동이 30일동안 매일 존재하며, 30일 동안의 트랜잭션 데이터가 10,000개 이상 존재하는 가상자산 36종으로 구성되어 있다.

실험 데이터셋은 스캠 코인으로 라벨링 된 55개의 데이터와 정상적인 가상자산으로 라벨링 된 36개의 데이터로 이루어져 있다. 각 모델을 평가하기 위해, 1) 스캠 코인으로 라벨링 된 실험 데이터셋을 스캠 위험성이 있는 가상자산 클러스터로 구분한 비율과 2) 정상적인 가상자산으로 라벨링 된 실험 데이터셋을 정상적인 가상자산 클러스터로 구분한 비율을 계산해 소수점 둘째 자리에서 반올림했다. 실험 데이터셋에 대한 실험 결과는 표 2와 같다.

<표 2> 실험 데이터셋에 대한 실험 결과

| | 비율 1 | 비율 2 |
|---|---|---|
| K-Means | 74.6% (41/55) | 94.4% (34/36) |
| DBSCAN | 69.1% (38/55) | 77.8% (28/36) |

실험 결과, K-Means는 스캠 코인으로 라벨링 된 55개의 데이터 중 41개의 데이터를 스캠 위험성이 있는 가상자산으로 분류했으며, 정상적인 가상자산으로 라벨링 된 36개의 데이터 중 34개의 데이터를 정상적인 가상자산 클러스터로 구분하였으며, DBSCAN보다 더 좋은 성능을 보였다. DBSCAN은 스캠 코인으로 라벨링 된 55개의 데이터 중 38개의 데이터를 스캠 위험성이 있는 가상자산으로 분류했으며, 정상적인 가상자산으로 라벨링 된 36개의 데이터 중 28개의 데이터를 정상적인 가상자산 클러스터로 구분하였다.

## 4 결론

스캠 코인에 의한 피해 사례의 증가와 함께 가상자산 거래소의 자체적 신뢰도 평가나 스캠 코인 탐지를 위한 서비스 및 연구가 수행되고 있으나 불명확한 스캠 코인 판별 기준으로 인해 한계를 갖는 상황이다.

이에 본 연구는 클러스터링을 통해 이더리움 기반 가상자산의 스캠 코인 여부를 판단했다. 이더리움 기반 가상자산은 이더리움 블록체인상에서 동작하여 거래 활동 정보를 얻는 것이 쉬워 본 연구의 범위를 이더리움 플랫폼 기반으로 특정했으며, 추후 연구를 통해 모든 플랫폼 기반으로 확장할 수 있을 것이다.

이더리움 기반의 가상자산 1,551종류에 대하여 14개의 특성을 수집하고, K-Means 및 DBSCAN 알고리즘을 기반으로 클러스터링을 수행했다. 스캠 코인 여부를 판단하는 기존의 서비스 및 연구를 바탕으로 스캠 코인 여부가 라벨링 된 테스트셋을 만들어 각 모델의 클러스터링 결과를 평가 및 비교했다.

본 연구에서 제시하고 있는 스캠 코인의 특성은 추후 스캠 코인 판별 기준을 세우기 위한 기반 자료가 될 수 있으며, 연구를 발전시켜 최종적으로 통일된 스캠 코인 판단 기준을 세우는 데 기여할 수 있을 것이다.

## 참고문헌

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic cash System", Decentralized Business Review, 2008
[2] S. Wang, L. Ouyang, et al. "Blockchain-enabled smart contracts: Architecture, applications, and future trends," IEEE, 2019
[3] A. Holub, J. O'Connor, "CoinHoarder: Tracking a ukrainian bitcoin phishing ring DNS style", IEEE, 2018
[4] Wu, Jiajing, et al. "Who are the phishers? Phishing Scam Detection on Ethereum via Network Embedding", IEEE, 2020
[5] P. Monamo, V. Marivate, and B. Twala, "Unsupervised learning for robust bitcoin fraud detection,", IEEE, 2016
[6] https://coinmarketcap.com/api/
[7] https://developer.twitter.com/en/docs/twitter-api
[8] http://github.com/EverexIO/Ethplorer/
[9] https://coincodex.com/
[10] https://www.cryptocompare.com/
[11] https://www.coingecko.com/ko