



PROJECT REPORT
HYBRID FRAUD DETECTION ON ETHEREUM
BLOCKCHAIN USING ML AND SNA

SOUW TIMOTIUS ALVIN FERDINAND

22.K1.0001

Informatics Engineering
Faculty of Computer Science
Soegijapranata Catholic University
2026

ABSTRACT

As Ethereum grows rapidly, blockchain fraud like phishing and illegal fund transfers has surged. Traditional detection relies heavily on transaction statistics, ignoring relational interaction patterns between suspicious wallets. This study proposes a hybrid framework integrating Machine Learning (ML) and Social Network Analysis (SNA) to enhance fraud detection within the Ethereum ecosystem. Transaction data were transformed into a directed graph where wallet addresses represent nodes and transactions represent directed edges. Two feature sets were extracted: transaction-based behavioral features (frequency, value, diversity, burst behavior) and graph-based structural features (Degree, Betweenness, PageRank, Clustering Coefficient). These combined features trained several models, including Random Forest, XGBoost, and Isolation Forest. Experimental results demonstrated that integrating SNA features significantly improves performance over transaction-only approaches. The proposed Hybrid Random Forest + SNA model achieved the best overall performance with an accuracy of 0.9987, F1-score of 0.9956, and ROC-AUC of 0.99998, outperforming the baseline transaction-only model. Graph visualization revealed that suspicious wallets frequently occupy highly connected, influential, and bridge-like positions within the transaction network. These findings indicate that combining ML and SNA provides more robust, interpretable, and context-aware capabilities for identifying structurally suspicious blockchain behavior..

Keyword: anomaly detection, blockchain security, ethereum network, fraud detection, graph topology, machine learning, random forest, social network analysis