ABSTRAK

Perkembangan teknologi blockchain pada platform Ethereum mendorong meningkatnya penggunaan token berbasis ERC20 dalam berbagai aktivitas digital, seperti *decentralized finance* dan perdagangan aset kripto. Seiring dengan tingginya volume transaksi tersebut, muncul berbagai aktivitas anomali dan penipuan, antara lain *Ice Phishing*, *NFT Scam*, dan *Reward Scam*, yang menyebabkan kerugian finansial serta menurunkan kepercayaan terhadap ekosistem blockchain. Permasalahan utama dalam mendeteksi anomali pada transaksi ERC20 terletak pada kompleksitas struktur jaringan transaksi dan ketidakseimbangan data yang ekstrem antara transaksi normal dan anomali. Penelitian sebelumnya umumnya menggunakan pendekatan berbasis data tabular dan hanya berfokus pada satu jenis anomali, sehingga belum mampu menangkap pola hubungan antar alamat dompet secara menyeluruh. Oleh karena itu, diperlukan pendekatan deteksi anomali yang mampu memodelkan struktur jaringan transaksi serta mendeteksi berbagai jenis anomali secara simultan.

Penelitian ini menggunakan metode kuantitatif dengan pendekatan pengembangan sistem berbasis *prototyping*. Dataset transaksi token ERC20 diperoleh dari Etherscan dan diproses melalui tahapan pembersihan data, rekayasa fitur, serta transformasi ke dalam bentuk graf. Alamat dompet dimodelkan sebagai node dan transaksi sebagai *directed edge*, dengan penambahan metrik struktural seperti *in-degree*, *out-degree*, dan *PageRank* sebagai fitur node. Dataset dibagi menjadi data pelatihan, validasi, dan pengujian menggunakan strategi *stratified split*. Model yang digunakan adalah Graph Neural Network dengan arsitektur GraphSAGE, sedangkan ketidakseimbangan kelas ditangani menggunakan *class weighting*. Evaluasi kinerja model dilakukan menggunakan metrik *accuracy* dan *F1-score*, serta didukung oleh visualisasi embedding node menggunakan t-SNE.

Hasil penelitian menunjukkan bahwa model GraphSAGE mampu mendeteksi anomali pada jaringan transaksi token ERC20 secara efektif. Berdasarkan lima kali pengujian independen, model memperoleh rata-rata *accuracy* sebesar 95,92% dan *F1-score macro* sebesar 82,62%, dengan performa terbaik mencapai *accuracy* 97,42% dan *F1-score macro* 88,69%. Evaluasi per kelas menunjukkan bahwa model mampu mengklasifikasikan transaksi normal dan seluruh jenis anomali dengan *F1-score* di atas 76%, meskipun data bersifat sangat tidak seimbang. Visualisasi t-SNE memperlihatkan pemisahan yang jelas antara node normal dan anomali. Dengan demikian, penelitian ini membuktikan bahwa pendekatan Graph Neural Network berbasis GraphSAGE efektif untuk deteksi anomali multikelas pada transaksi ERC20. Kontribusi penelitian ini adalah penerapan deteksi anomali berbasis graf pada transaksi token ERC20 serta pengembangan sistem pendukung untuk mitigasi penipuan pada blockchain Ethereum.

Kata Kunci: *Blockchain*, ERC20, Deteksi Anomali, *Graph Neural Network*, *GraphSAGE*.

ABSTRACT

The rapid development of blockchain technology on the Ethereum platform has led to the widespread adoption of ERC20 tokens in various digital applications, including decentralized finance and crypto asset trading. Along with the increasing transaction volume, various anomalous and fraudulent activities have emerged, such as Ice Phishing, NFT Scams, and Reward Scams, which cause significant financial losses and reduce user trust in the blockchain ecosystem. The main challenge in detecting anomalies in ERC20 transactions lies in the complexity of transaction network structures and the extreme imbalance between normal and anomalous data. Previous studies have mostly relied on tabular-based approaches and focused on a single type of anomaly, which limits their ability to capture relational patterns among wallet addresses. Therefore, an anomaly detection approach that can effectively model transaction network structures and detect multiple types of anomalies simultaneously is required.

This study employs a quantitative research method with a prototyping-based system development approach. The ERC20 transaction dataset was collected from Etherscan and underwent preprocessing steps including data cleaning, feature engineering, and transformation into a graph representation. Wallet addresses were modeled as nodes and transactions as directed edges, with additional structural features such as in-degree, out-degree, and PageRank. The dataset was divided into training, validation, and testing sets using a stratified split strategy. A Graph Neural Network with the GraphSAGE architecture was employed as the anomaly detection model due to its ability to handle large-scale graphs and perform inductive learning. Class imbalance was addressed using class weighting in the loss function. Model performance was evaluated using accuracy and F1-score metrics and supported by node embedding visualization using t-SNE.

The results demonstrate that the proposed GraphSAGE-based model effectively detects anomalies in ERC20 transaction networks. Based on five independent experiments, the model achieved an average accuracy of 95.92% and a macro F1-score of 82.62%, with the best performance reaching 97.42% accuracy and 88.69% macro F1-score. Class-wise evaluation shows that the model successfully classifies normal transactions and all anomaly types with F1-scores above 76%, despite severe class imbalance. The t-SNE visualization reveals a clear separation between normal and anomalous nodes, indicating that the model successfully learns structural transaction patterns. This study confirms that Graph Neural Networks, particularly GraphSAGE, are effective for multi-class anomaly detection in ERC20 transaction networks. The main contribution of this research lies in applying graph-based anomaly detection to ERC20 transactions and developing a supporting system that can be utilized to enhance fraud mitigation and security in the Ethereum blockchain ecosystem.

Keywords: *Blockchain, ERC20, Anomaly Detection , Graph Neural Network, GraphSAGE.*