УДК 004.934:004.056 DOI: https://doi.org/10.30837/IYF.IIS.2024.054

ДОСЛІДЖЕННЯ МЕТОДІВ АВТОМАТИЧНОГО РЕЗЮМУВАННЯ ТЕКСТІВ НОВИН

Кітов А. В.
Науковий керівник – проф. Філатов В. О.
Харківський національний університет радіоелектроніки, каф. ШІ,
м. Харків, Україна
e-mail: anton.kitov@nure.ua

Our research is aimed at analyzing and understanding fraudulent activities within the Ethereum network using intelligent analysis. With the increasing adoption of cryptocurrencies and the growing complexity of financial transactions, detecting fraudulent behavior has become a challenging task. The goal of our work is to leverage intelligent analysis techniques to detect, analyze, and prevent fraudulent transactions in real time. We consider various aspects of fraudulent activities, including transaction patterns and network behaviors, to develop a comprehensive approach to their identification and mitigation. Our research aims to develop innovative techniques and tools to help organizations effectively combat fraud within the Ethereum network, safeguarding their financial assets and ensuring the integrity of transactions.

В сучасному світі криптовалютні транзакції стали неодмінною частиною фінансових операцій, зокрема в мережі Ethereum, де кожною секундою відбуваються десятки тисяч операцій. Однак, цей обсяг також збільшує ймовірність шахрайських, що робить важливим завданням виявлення неправомірних дій через аналіз даних за допомогою машинного навчання.

Ми припускаємо, що модель мультислойного персептрона буде ефективною у виявленні шахрайських транзакцій у мережі Ethereum. Ця гіпотеза базується на його високій точності та можливості оптимізованого рішення завдання.

У сучасному світі, де фінансові операції стають все більш цифровими, аналітика виявлення шахрайства стає невід'ємною складовою для організацій. Аналітичні системи виявлення шахрайства грають критичну роль у зменшенні ризику та забезпеченні безпеки фінансових операцій.

Застосування аналітики виявлення шахрайства має декілька важливих переваг. По-перше, вона дозволяє системам закрити потенційні "лазейки" для здійснення шахрайських дій, знижуючи тим самим вероятність їх вчинення. Виявлення шахрайства ще до того, як виникне шкода, підвищує рівень безпеки організації та контролю над фінансовими операціями.

Крім того, аналітика виявлення шахрайства сприяє підвищенню довіри клієнтів до системи організації. Гарантія безпеки та відсутність

проблем з шахрайством сприяють підвищенню лояльності клієнтів, що в свою чергу сприяє росту організації.

Однією з ключових переваг аналітики виявлення шахрайства є здатність аналізувати неструктуровані дані. Багато шахраїв діють у тих випадках, коли дані неструктуровані, і аналітичні системи можуть ефективно аналізувати ці дані для виявлення та запобігання крадіжок.

Також, аналітика виявлення шахрайства допомагає виявляти складні та приховані закономірності, що можуть бути пропущені застарілими методами виявлення шахрайства.

Нарешті, застосування аналітики виявлення шахрайства підвищує ефективність роботи організації, зменшуючи втрати доходів від крадіжок та поліпшуючи процеси фінансових операцій.

У роботі ми проаналізуємо різні методи семплінгу для умов несбалансованих класів, а також вивчимо вплив обробки даних на ефективність моделей. Оптимальні параметри моделі будуть визначені на основі порівняння різних архітектур та метрик їх ефективності.

Отримані результати підтверджують високу точність моделі мультислойного персептрона у виявленні шахрайських транзакцій. Застосування різних методів семплінгу та оптимізація обробки даних значно покращили ефективність моделі. Наша візуалізація через віконний застосунок на мові Python надасть зручний інструмент для аналізу результатів та відображення їх в реальному часі.

Модель мультислойного персептрона виявляється не лише потужним інструментом у виявленні шахрайських транзакцій у мережі Ethereum, але й обіцяним рішенням для комерційного використання. Її висока точність та оптимізоване рішення створюють потенціал для успішного застосування у сфері фінансових операцій з криптовалютами.

Список використаних джерел

1. Ethereum Fraud Detection Dataset. Kaggle: Your Machine Learning and Data Science Community. URL: https://www.kaggle.com/datasets/gescobero/ethereum-fraud-dataset (дата звернення: 13.03.2024).

2. Гороховатський В.О., Творошенко І.С. (2022) Аналіз багатовимірних даних за описом у формі множини компонент: монографія. Харків, ХНУРЕ. 2022. 124 с.

3. Michalski R., Dziubałtowska D., Macek P. Revealing the character of nodes in a blockchain with supervised learning //Ieee Access. 2020. Т. 8. S. 109639-109647.