PAPER 1:

TITLE:

Blockchain-enabled fraud discovery through abnormal smart contract detection on Ethereum CITATIONS:

Liu, L., Tsai, W.-T., Bhuiyan, M. Z. A., Peng, H., & Liu, M

WORK DONE:

The research focuses on detecting fraudulent smart contracts on the Ethereum blockchain. They propose a method called Heterogeneous Graph Transformer Networks (S\_HGTNs) to achieve this. This method analyzes features of smart contracts and their relationships with other contracts on the network to identify anomalies indicative of potential fraud.

TOOLS USED:

* S\_HGTNs: This is the core tool a machine learning model specifically designed for the task of anomaly detection on graphs. It leverages heterogeneous graphs which represent smart contracts and their connections.
* Ethereum Blockchain Data: The researchers used real world data from the Ethereum blockchain to train and test their model.

Evaluation Metrics: They employed standard metrics like precision, recall, and F1 score to assess the performance of their model.

ADVANTAGES:

* Improved Fraud Detection: S\_HGTNs outperforms traditional methods in identifying fraudulent smart contracts, potentially offering enhanced security for the Ethereum ecosystem.
* Novel Approach: The use of heterogeneous graphs and specialized transformer networks is a unique approach to anomaly detection in this context.
* Real-world Applicability: The research leverages real-world data and addresses a critical issue in blockchain security.

LIMITATIONS:

* Limited Data: The study used a relatively small dataset, and further research with larger datasets is needed to confirm the generalizability of the findings.
* Black Box Model: S\_HGTNs, like many machine learning models, can be complex and lack interpretability. Understanding the reasons behind their predictions could be challenging.
* Specificity to Ethereum: The research focuses on Ethereum and may not be directly applicable to other blockchains with different structures and functionalities.
* Evolving Fraud Techniques: Fraudsters might adapt their techniques, requiring continuous improvements and updates to the detection methods

PAPER 3:

TITLE:

Fraud Detection System for Identity Crime using Blockchain Technology and Data Mining Algorithms CITATIONS:

Shakadwipi, A. J., Jain, D. C., & Nagini, S

WORK DONE:

* The project aims to develop a fraud detection system for identity crime using blockchain technology and data mining algorithms.
* Blockchain technology is utilized to ensure the security and immutability of data, while data mining techniques are used to analyze vast amounts of data to identify patterns and anomalies associated with fraudulent behavior.
* The system processes the analyzed data to identify suspicious activities and potential instances of fraud, and establishes thresholds and rules to classify transactions as fraudulent or non-fraudulent based on model predictions and predefined criteria.
* The project generates reports, metrics, and visualizations to provide insights into fraud detection performance, patterns, and trends, and continuously refines the system through feedback loops and ongoing monitoring.
* The system architecture includes essential technical elements such as dedicated mobile applications, utilization of the Interplanetary File System (IPFS), and the development of a mathematical model tailored to a specific implementation.

TOOLS USED:

* Blockchain platform: Ethereum, Hyperledger Fabric, or Corda
* Data mining tools: Python, R, Weka, or RapidMiner
* Interplanetary File System (IPFS)
* Mobile application development: Android and iOS platforms
* Mathematical modeling tools: MATLAB, Excel, or R • Smart contract development: Solidity, Vyper, or Chaincode ADVANTAGES:

1.Enhanced Security: Utilizes blockchain technology for secure and transparent identity management.

2.Self-Sovereign Identity: Empowers individuals to independently manage their identities without intermediaries.

3.Privacy Protection: Ensures secure and shielded storage of identity documents, addressing privacy concerns.

Trust and Authenticity: Establishes trust among participants through blockchain-verified identity document authenticity.

Immutable Repository: Provides a secure and immutable repository for identity documents, enhancing data integrity.

PAPER 6:

TITLE:

Tracking Transactions in Crypto Currencies Using the Graph Theory CITATIONS:

Danil A. Subbotin1 , Maria A. Antropova2 , Pavel V. Sukharev3

WORK DONE:

* The particular work done in this paper that stands out is the development of a program in Python that can track transactions in crypto currencies using graph theory. This program can find connections between wallets and visualize them in the form of a graph, which can help identify criminal organizations and illegal traffic related to the sale of goods or services using cryptocurrencies.
* Some key points to consider in a critical analysis of this work are:
* The program is based on publicly available data from the website [www.blockchain.com,](http://www.blockchain.com/) which limits its ability to track transactions on other platforms or those that are not publicly available.
* The program can only track transactions that are related to the sale of illegal goods or services, and may not be effective in identifying other types of criminal activity.
* The program relies on the assumption that wallets with many connections are more likely to be involved in criminal activity, which may not always be accurate.
* The program can be useful for law enforcement agencies and other organizations that are interested in tracking transactions in crypto currencies, but it may also raise privacy concerns for individuals who use cryptocurrencies for legitimate purposes.

TOOLS USED:

* The particular tools used in this paper that stand out are the Python programming language and specific libraries for graph visualization, such as NetworkX and Pyvis. These tools enable the creation of a program that can track transactions in crypto currencies and visualize them in a graph format.
* Python is a versatile and widely-used programming language that allows for efficient data processing and analysis, making it a suitable choice for developing this type of program.
* The NetworkX library provides functionalities for creating and manipulating complex networks and graphs, which is essential for visualizing the connections between wallets in the crypto currency transactions.
* The Pyvis library offers interactive visualization capabilities, enhancing the user experience and making it easier to explore and analyze the graph data.
* While these tools are effective for the specific task of tracking transactions in crypto currencies, they may have limitations in handling large datasets or complex network structures, which could impact the scalability of the program.

ADVANTAGES:

1.Visualization of Complex Networks: The program allows for the visualization of complex networks of crypto currency transactions, providing a clear and understandable representation of the connections between wallets.

2.Identification of Criminal Activity: By tracking transactions and visualizing the connections between wallets, the program can aid in identifying criminal organizations and illegal traffic related to the sale of prohibited goods or services using cryptocurrencies.

3.Database Expansion: The program adds all discovered wallets to a database, which can significantly expand over time, providing a valuable resource for analyzing and understanding crypto currency transactions.

4.Proportional Display: The use of proportional display of wallet size and transfer amounts in the graph visualization allows for an accurate representation of the real form of transfer networks for any Bitcoin wallet entered at the input.

5.Practical Application: The program's ability to determine the tasks performed by wallet owners and identify their involvement in illegal activities can have practical implications for law enforcement and investigative purposes.

PAPER 7:

TITLE:

Oversampling Techniques for Detecting Bitcoin Illegal Transactions

CITATIONS:

Jungsu Han1, Jongsoo Woo2, and Jame Won-Ki Hong1

WORK DONE:

1.Integration of Conditional GAN (CGAN) and Wasserstein GAN (WGAN) for detecting illegal Bitcoin transactions, addressing the issue of mode collapse and improving the classification performance 2.

2.Utilization of Principal Component Analysis (PCA) to mitigate the problem of high-dimensional data and overfitting when training a classification model.

3.Comparison of SMOTE and well-designed GAN models for generating synthetic data, demonstrating improved classification performance on average.

4.Exploration of the use of Extreme Gradient Boosting (XGBoost) algorithm to evaluate the distribution of synthetic and actual data, providing insights into the impact of input features on classification 3.

5. Experimentation with DRAGAN and resampled training sets to address training difficulty and low performance of basic GAN/WGAN architecture, resulting in improved stability and classification performance 4.

* These contributions collectively advance the understanding and application of oversampling techniques and GAN models in detecting illegal activities in cryptocurrency transactions.

TOOLS USED:

* This paper utilizes the following tools that stand out for their specific contributions:

1.SMOTE: Synthetic Minority Over-sampling Technique, a popular oversampling technique used to generate synthetic data for the minority class.

2.GAN: Generative Adversarial Networks, a deep learning architecture consisting of a generator and a discriminator that compete to generate realistic synthetic data .

3.PCA: Principal Component Analysis, a data preprocessing method used to reduce the dimensionality of highdimensional data and mitigate the problem of overfitting.

4.XGBoost: Extreme Gradient Boosting, a machine learning algorithm used to evaluate the distribution of synthetic and actual data and determine the importance of input features for classification.

5.DRAGAN: Deep Regret Analytic GAN, a GAN variant used to address training difficulty and improve stability and classification performance.

* These tools collectively contribute to the development and implementation of effective oversampling techniques and GAN models for detecting illegal activities in cryptocurrency transactions.

ADVANTAGES:

Improved Classification Performance: The integration of SMOTE and GAN techniques leads to enhanced classification performance in detecting illegal Bitcoin transactions, addressing the challenge of imbalanced datasets.

Data Diversity Representation: The use of GAN models allows for the generation of diverse and realistic synthetic data, overcoming the limitations of SMOTE in fully representing the diversity of the data .

Feature Importance Analysis: The application of XGBoost algorithm enables the evaluation of the importance of input features, providing insights into the impact of different features on the classification of fraudulent activities .

Training Stability and Performance Improvement: The utilization of DRAGAN helps in achieving faster training, improved stability, and better modeling performance compared to basic GAN/WGAN architectures, leading to enhanced classification results LIMITATIONS:

Mode Collapse: The issue of mode collapse is observed in the GAN models, particularly in the vanilla GAN and CGAN architectures, which can lead to suboptimal sample distribution and affect the overall performance .

Dataset Quality: The dataset composed solely of on-chain data may lack key information such as market prices and trading locations, potentially limiting the representation of real-world transaction patterns .

Dependency on Off-chain Data: To address the limitations of on-chain data, the paper suggests the need for off-chain data such as exchange information, which may introduce additional complexities and dependencies in the analysis .

Recall Value Improvement: While SMOTE shows better performance than GAN-based frameworks in dealing with imbalanced data, there is room for further improvement in enhancing the recall value for detecting illegal transactions