CIPHERTRACE

CRYPTOCURRENCY FRAUD DETECTION

GROUP # 06:

ASHISH KUMAR

HASHIR HABIB

SAMEEN SHAHID

SAMIA FATIMA

SUKAINA ALI

UME ABEEHA

ABOUT COMPANY

CipherTrace is a cryptocurrency intelligence company acquired by Mastercard in 2021. It provides tools and services for analyzing crypto transactions, identifying scams and illicit activity, and helping organizations comply with cryptocurrency regulations.

KEY CHALLENGE

CipherTrace faced evolving **Fraud challenges** due to the dynamic, decentralized crypto landscape such as:

- **Crypto Anonymity:** Use of privacy coins and mixers to hide transactions.
- **Evolving Scams:** New fraud types like rug pulls, DeFi hacks, and phishing.
- **Cross-Chain Activity:** Criminals moving funds across multiple blockchains.
- **Lack of Standardization:** Varying blockchain structures require custom solutions.
- **Constant Updates Needed:** Tools and algorithms had to evolve rapidly.

ABOUT THE DATASET

CIPHERTRACE

DATASET OVERVIEW

- Contains **9,841** Ethereum transactions
- **51 features** capturing detailed transaction activity
- **Goal:** Identify suspicious wallets

IMPORTANT FEATURES

- **Total** Ether sent, received, and balance
- **Avg/min/max** values of Ether sent/rec
- Unique sent/received addresses
- Time difference between first and last transaction

PROJECT OBJECTIVES

Use transaction data to classify wallets as:

- **0 = Legitimate**
- **1 = Flagged/Suspicious**

DATA PREPROCESSING

- Drops Unnamed: 0, Index columns.
- Fills missing categorical values with 'Unknown', numerics with 0.
- Converts object columns to category.
- Scales numeric columns to [0, 1].
- Computes total transactions if missing.

COMPARING ALGORITHMS

	Accuracy	f1-score	recall	precision
LightGBM	0.998984	0.997712	1.000	0.995434
XGBoost	0.995429	0.989619	0.983945	0.99536
KNN	0.91	0.79	0.78	0.81
Random Forest	0.995259	0.989410	1.000	0.979042
Logistic Regression	0.793769	0.611359	0.732416	0.524644
Linear SVM	0.751101	0.562239	0.721713	0.460488

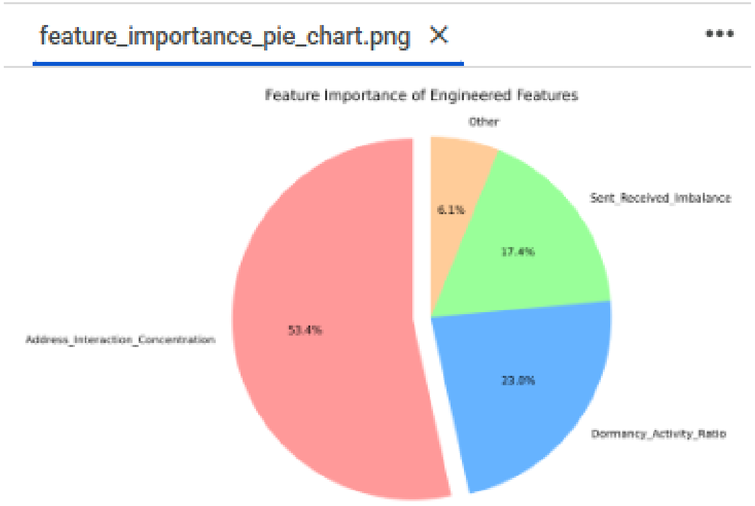
OBSERVATIONS AT THIS STAGE

- SIGNS OF OVERFITTING
- SIGNS OF DATA LEAKAGE
- ABNORMALLY HIGH RESULTS
- XGBOOST & LIGHTGBM HAVE GIVEN THE BEST RESULTS
- FURTHER RESEARCH SHOWS PAYPAL HAS SUCCESSFULLY USED XGBOOST TO CREATE A FRAUD DETECTION ML

Engineering Features For Enhanced Fraud Detection

Correlation of the Target Variable and Engineered features

```
Correlation with FLAG:
Num_Bursts                          NaN
Burst_Intensity                     NaN
Night_Ratio                   -0.442870
Dormancy_Activity_Ratio       -0.018096
Address_Interaction_Concentration   -0.053055
ERC20_Token_Diversity               NaN
Value_Anomaly_Ratio           -0.037649
Sent_Received_Imbalance        0.051980
```



- **Num_Bursts :** Counts transaction bursts, detecting sudden spikes signaling potential fraud.
- **Burst_Intensity**: Measures transaction density in bursts, highlighting rapid, suspicious activity
- **Night_Ratio:** Estimates night-time transaction fraction, flagging off-hour activity
- **Dormancy_Activity_Ratio:** Captures dormant-then-active transaction spikes typical of fraud.
- **Address_Interaction_Concentration:** Measures transactions per unique address, signaling fund funneling.
- **ERC20_Token_Diversity:** Gauges unique ERC20 tokens per transaction, flagging scam token focus.
- **Value_Anomaly_Ratio**: Identifies large transaction outliers relative to average values.
- **Sent_Received_Imbalance**: Quantifies sent vs. received transaction asymmetry in fraud schemes.

Overview of the Final Code

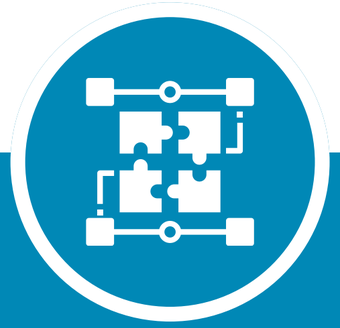
The code builds an advanced fraud detection system using XGBoost with optuna on transaction dataset

Handling Class Imbalance

- applied SMOTE on training data to handle class imbalance

Handling Missing Values

- we filled missing values with “unknown” for text-based and “0” for numeric values
- we had 2 models; baseline and enhanced model
- baseline model worked without the addition of new features



Normalizing

- we converted labels to categories and scaled all numbers between 0 and 1.
- this helped the model learn more efficiently as all features were at the same scale

Enhanced Model

- it used both old and new features
- this has a higher and better performance making it better at catching fraud

Optuna

- we used “optuna” to find the best settings for our ML model to get the best result
- It tried 100 different options of XGBoost settings and chose the best combination (no. of trees, depth, learning rate)

Correlation Analysis

- we did correlation analysis to find out which feature strongly effects fraud

Improved Results of the Enhanced Model

Enhanced Fraud Detection

- Boosted recall by 0.68% (87.61%), identifying more true positive
- Improved F1-score (+0.08%) and ROC-AUC (+0.05%) for fraud class.
- Captured nuanced patterns like network and value anomalies.

Point: Improved True Positives and True Negatives

- Engineered features increased true positives to 382 (19.40%), detecting ~3 more fraudulent accounts.
- Maintained high true negatives at 1479 (75.11%), ensuring accurate non-fraud identification.
- Address_Interaction_Concentration (19.82% importance) drove fraud detection by flagging suspicious network patterns.

	Predicted: Non-Fraud (0)	**Predicted: Fraud (1)**
Actual: Non-Fraud (0)	1479 (✅ True Negatives)	54 (❌ False Positives)
Actual: Fraud (1)	54 (❌ False Negatives)	382 (✅ True Positives)

```
Confusion Matrix (Enhanced Model):
          Predicted 0    Predicted 1
Actual 0         1479             54
Actual 1           54            382
```

```
Model Performance:
                    Model  Accuracy  Precision    Recall  F1 Score   ROC AUC

1  Enhanced (All Features)   0.94515   0.876147  0.876147  0.876147  0.982803

Prediction Breakdown (Enhanced Model):
✅ True Positives (Fraud correctly detected): 382 (19.40%)
✅ True Negatives (Non-fraud correctly detected): 1479 (75.11%)
❌ False Positives (Non-fraud wrongly flagged as fraud): 54 (2.74%)
❌ False Negatives (Fraud missed): 54 (2.74%)

Per-Class Accuracy (Enhanced Model):
Class 0 (Non-Fraud) Accuracy: 96.48%
Class 1 (Fraud) Accuracy: 87.61%

Cross-Validated F1 Score (Enhanced): 0.8680 ± 0.0096
```

Solutions: Addressing CipherTrace's Fraud Detection Challenges with Enhanced Features

CipherTrace's Limitation: Reliance on Static Rules and Known Labels

- Static rules & blacklists
- Misses new evasive wallets
- Undetected emerging fraud

What CipherTrace Could Do Better — And What We Did Differently

- Replaced static rules with behavioral features
- Moved beyond blacklists using XGBoost model
- Optimized performance with Optuna tuning

Dataset Constraints: Why We Couldn't Fully Implement All Suggestions

- Limited to on-chain data only
- Missing external sources (e.g., exchange logs, metadata)
- Still achieved strong results with available data

Impact of Using Additional Features: Enhanced Fraud Detection

- Improved recall, F1 score, and ROC-AUC
- Detected 3 more fraudulent accounts
- Top feature: Address_Interaction_Concentration (19.8% importance)

Why This Solution is Relevant for CipherTrace's Future

Behavior-based ML outperforms static rules
Reduces false negatives with richer signals & tuning
Provides a data-driven upgrade path for CipherTrace