

The background is a dark blue gradient. It features several faint, light blue geometric shapes, including triangles and lines, suggesting a network or blockchain structure. Two prominent white line graphs with upward-pointing arrows are visible: one on the left side and one on the bottom right corner. Two Bitcoin logos are also present: one in the upper right and one in the lower right, both rendered in a light blue, semi-transparent style.

DEFI ANOMALY DETECTION

A MULTIPLE BLOCKCHAIN APPROACH

DECENTRALIZED FINANCE

Decentralized finance (DeFi) is an emerging peer-to-peer financial system that uses blockchain and cryptocurrencies to allow people, businesses, or other entities to transact directly with each other. The key principle behind DeFi is to remove third parties like banks from the financial system, thereby reducing costs and transaction times.

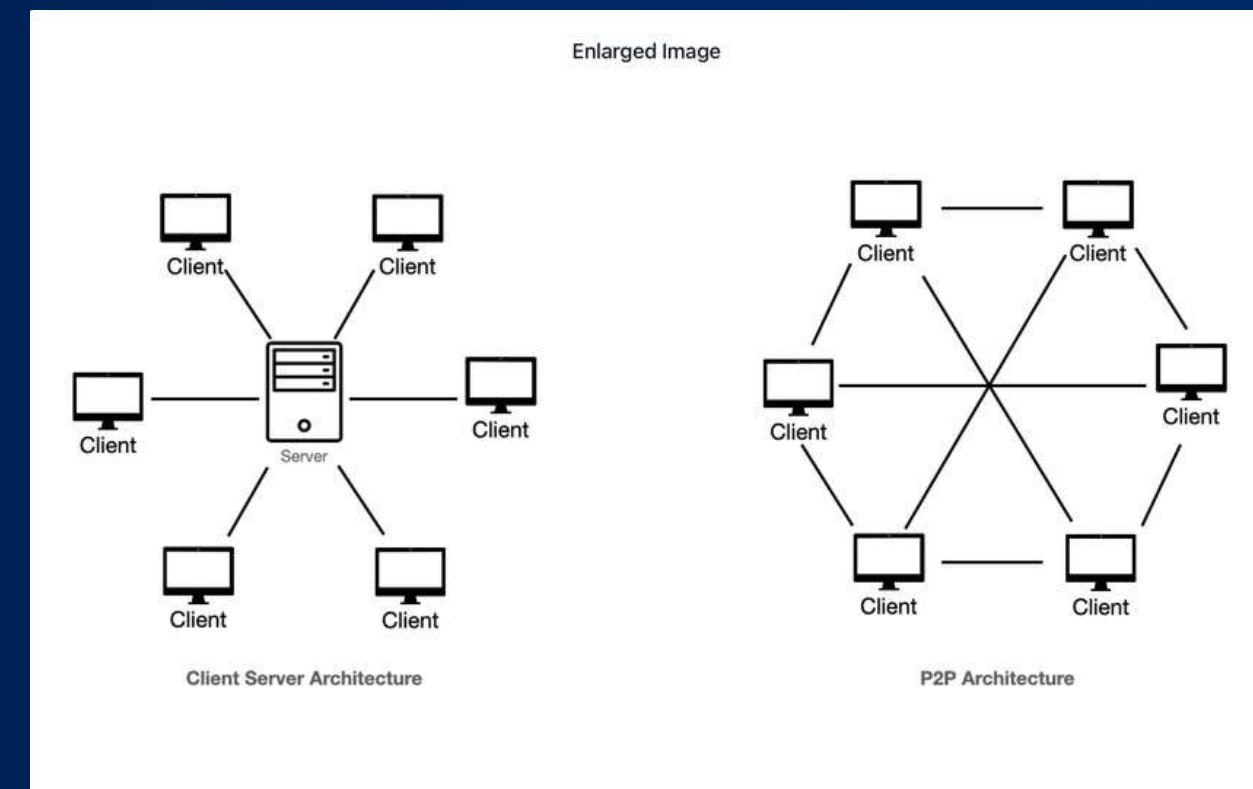


DEFI INTRODUCTION

DeFi (Decentralized Finance) is a financial system built on blockchain technology that enables transactions and services without traditional intermediaries like banks, brokers, or payment processors. Instead, it uses a combination of:

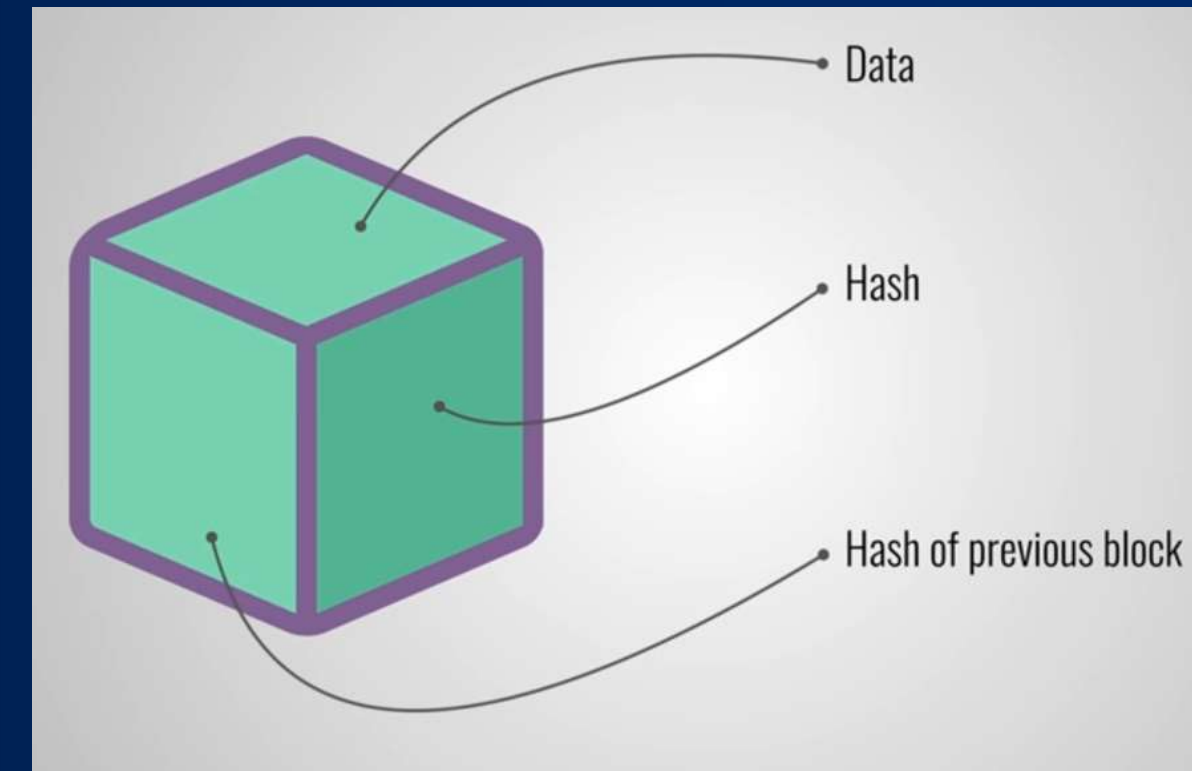
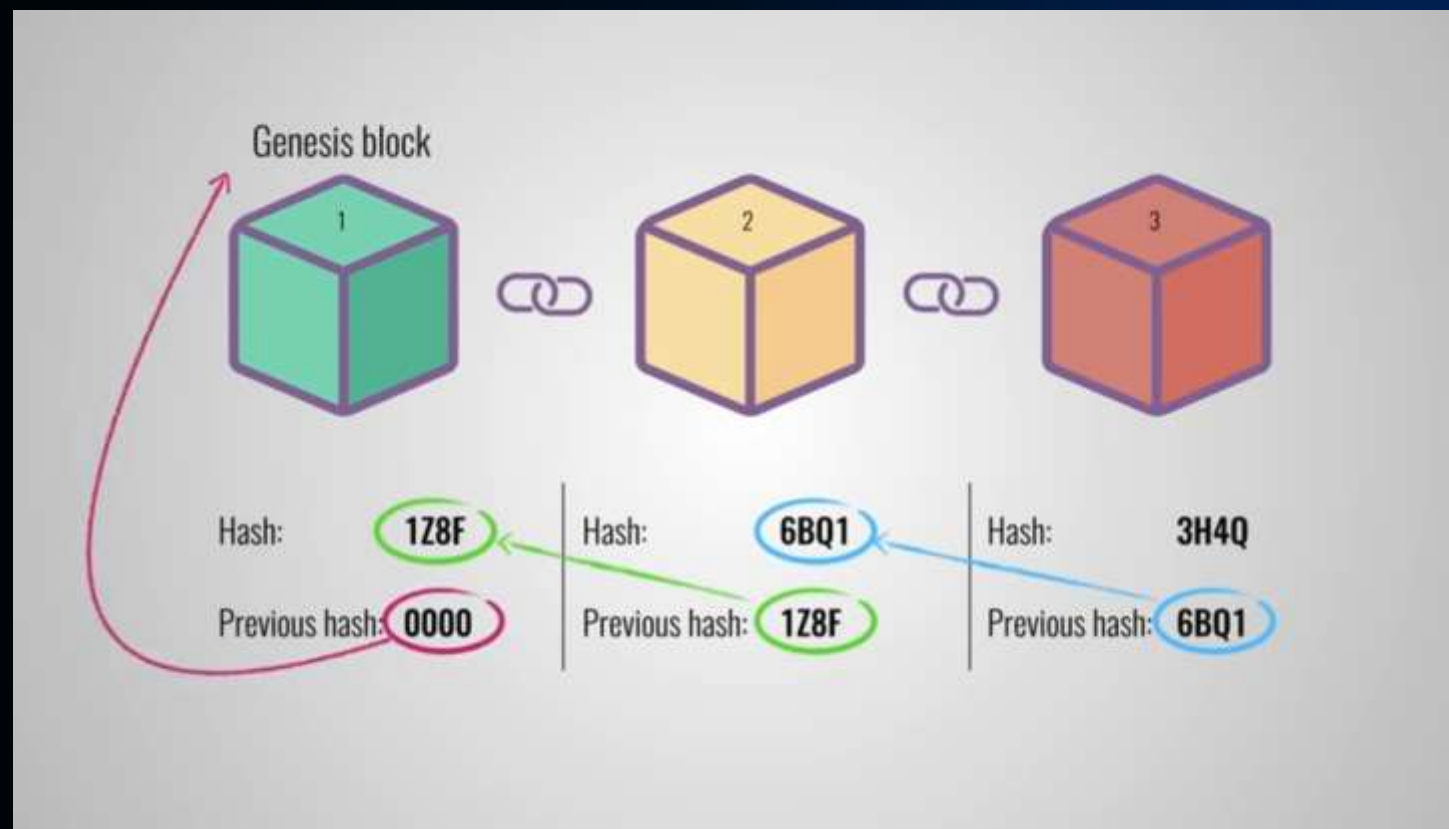
- Peer-to-peer networks
- Smart contracts
- Cryptographic security protocols
- Advanced software and hardware infrastructure

Feature	Traditional Finance	Decentralized Finance (DeFi)
Intermediaries	Banks, brokers, clearinghouses	None (replaced by smart contracts)
Accessibility	Often limited (banking hours, KYC)	24/7, global, more inclusive
Transparency	Opaque systems	Public and auditable on blockchain
Costs	High fees due to middlemen	Lower fees due to automation



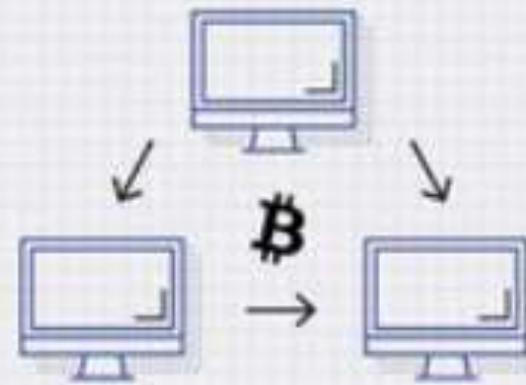
BLOCKCHAIN

A blockchain is a distributed and secured database or ledger. In a blockchain, transactions are recorded in files called blocks and verified through automated processes. If a transaction is verified, the block is closed and encrypted; another block is created with information about the previous block and information about newer transactions.

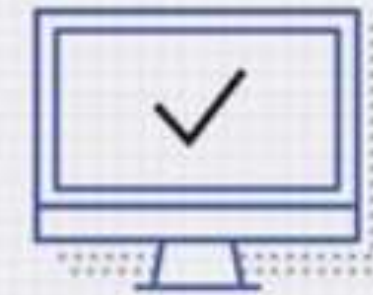




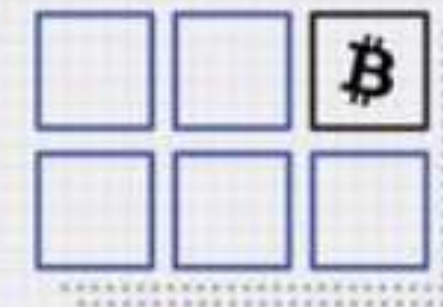
A new transaction is entered.



The transaction is then transmitted to a network of peer-to-peer computers scattered across the world.



This network of computers then solves equations to confirm the validity of the transaction.



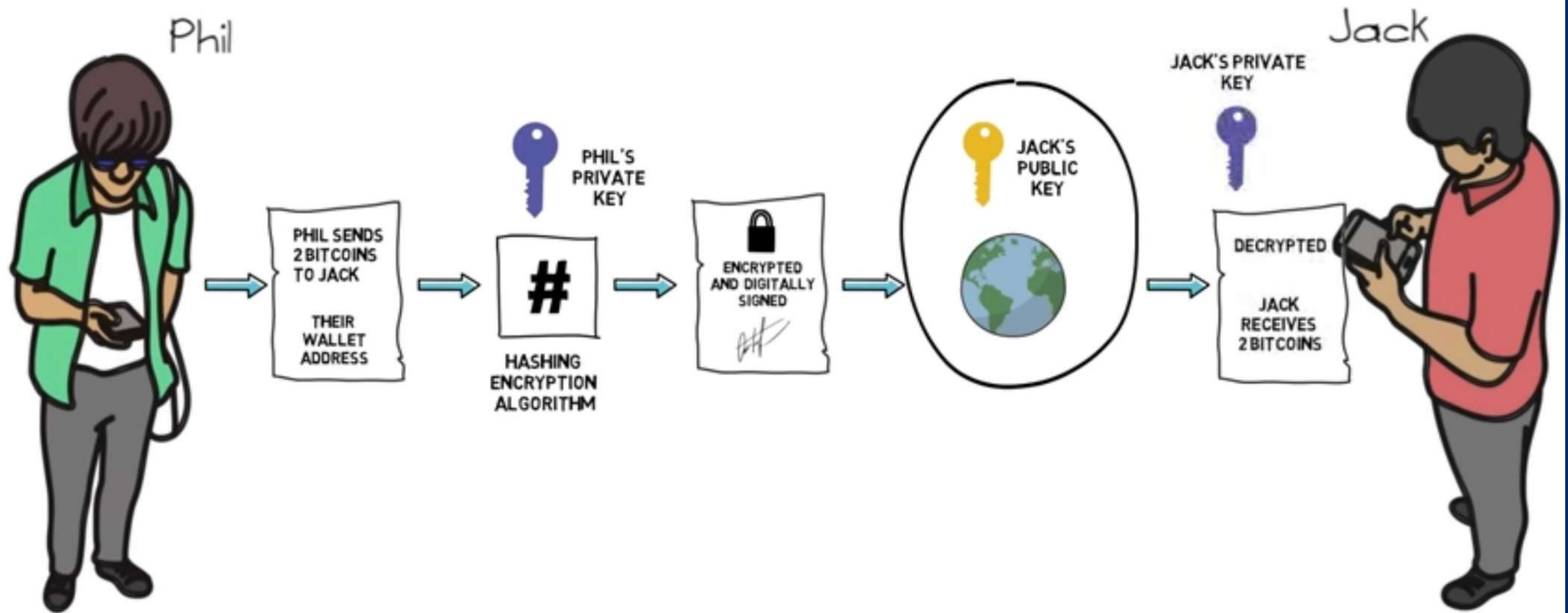
Once confirmed to be legitimate transactions, they are clustered together into blocks.



These blocks are then chained together creating a long history of all transactions that are permanent.



The transaction is complete.

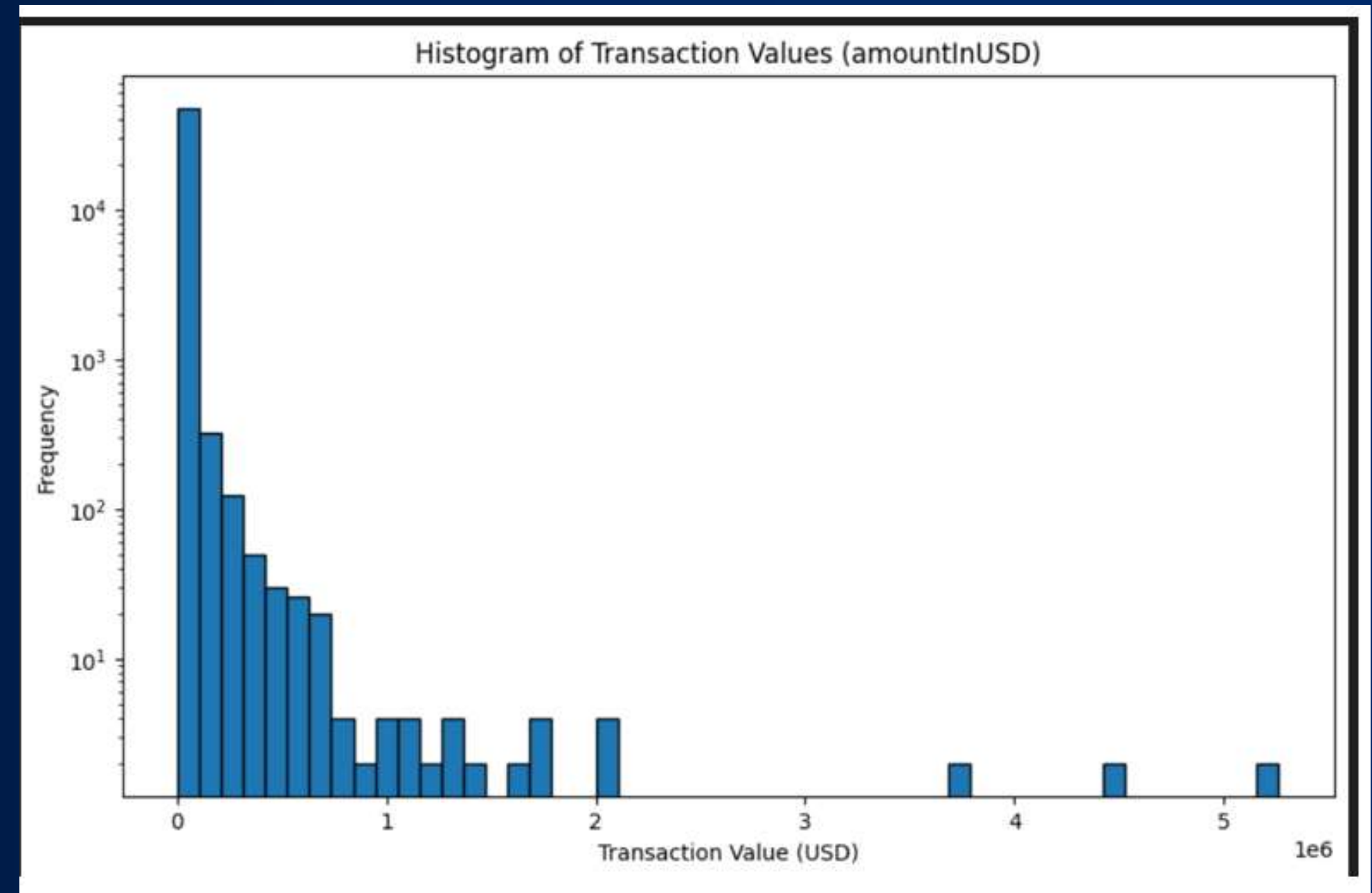
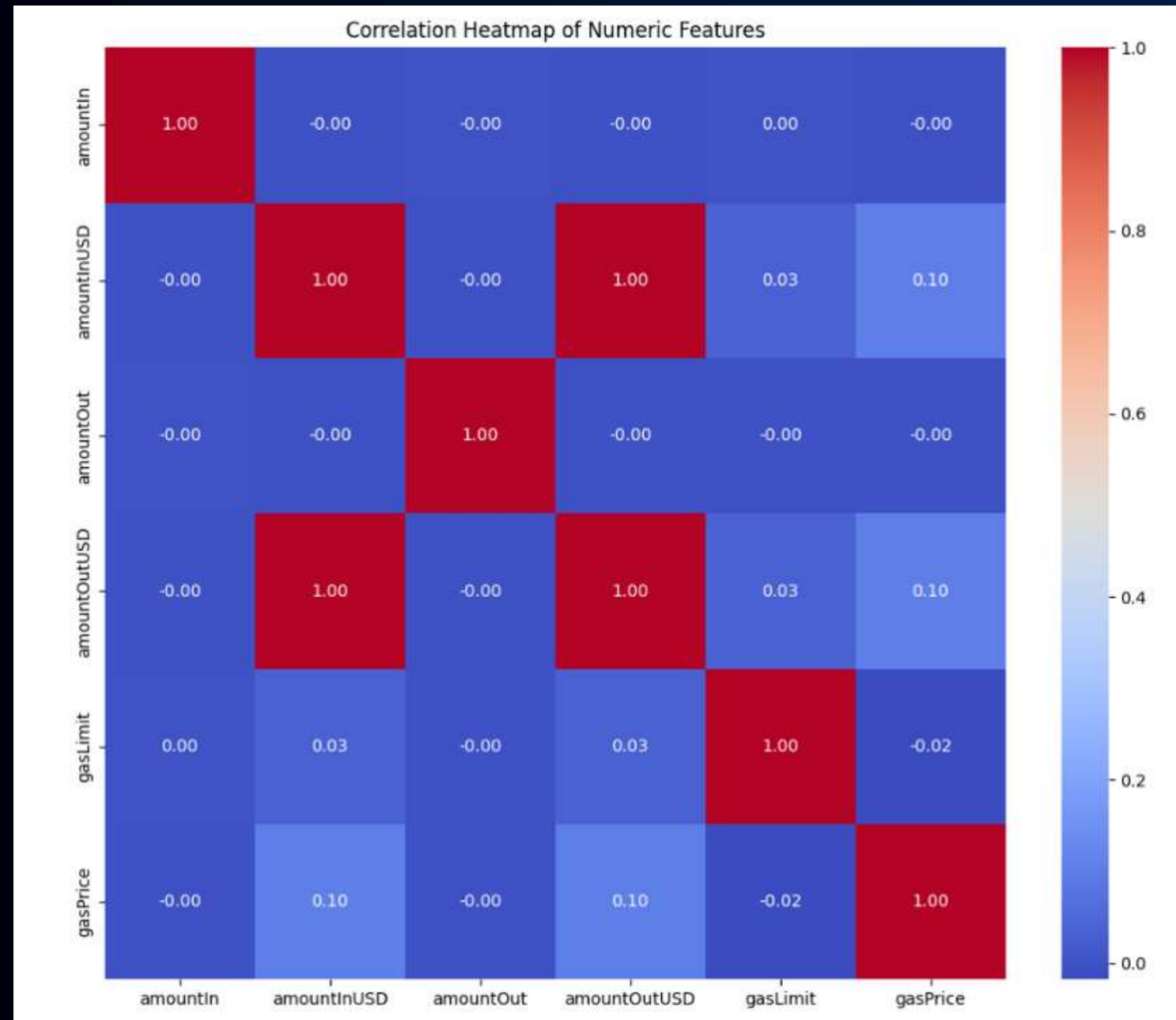


AIMS / OBJECTIVES

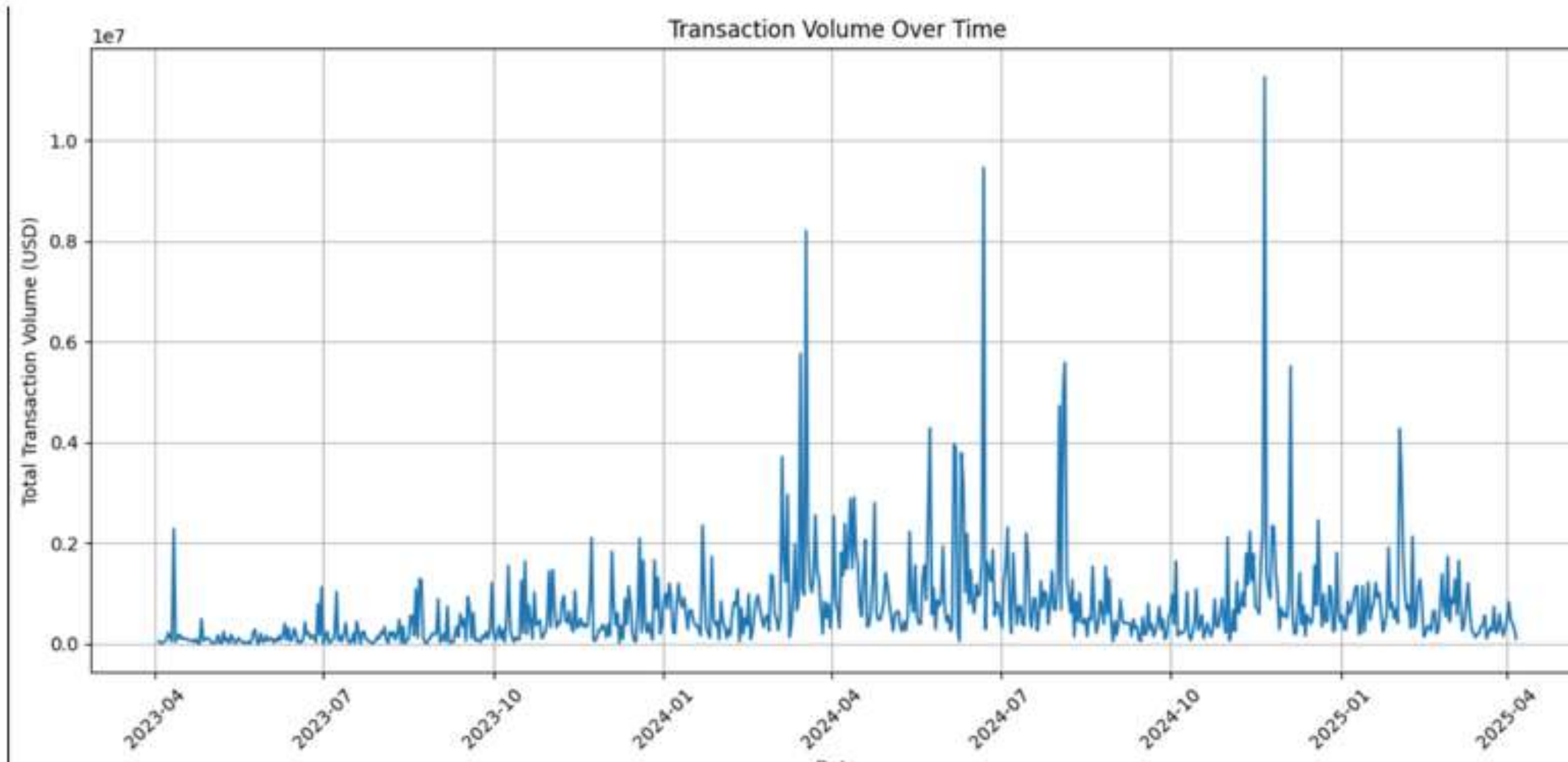
- “To develop a robust anomaly and fraud detection pipeline for DeFi transactions by combining rule-based heuristics and machine learning models (e.g., Isolation Forest, LOF).”
- The goal is to identify high-risk and potentially fraudulent activities by analyzing transaction patterns, token behavior, and temporal anomalies, enabling proactive detection and better risk mitigation in decentralized finance ecosystems.”



BASIC VISUALISATION



BASIC VISUALISATION



DETECTION TYPES

ANOMALY

- An anomaly in DeFi refers to any unusual or unexpected activity that deviates from normal patterns—like sudden spikes in trading volume or irregular transaction flows.
- Find Outliers
- Further Investigation is needed

FRAUD

- Fraud is deliberate deception for financial gain, such as hacking smart contracts, creating fake projects (rug pulls), or manipulating prices
- Prove Malicious intent
- Take action

MODEL USED

S

ISOLATION FOREST

It is an unsupervised machine learning algorithm that identifies anomalies or outliers in data by isolating them through a process of random partitioning within a collection of decision trees

LOCAL OUTLIER FACTOR

It is an unsupervised anomaly detection method that identifies outliers based on how much a data point's local density deviates from its neighbors

DBSCAN

DBSCAN (Density-Based Spatial Clustering of Applications with Noise) is a clustering algorithm that groups data points based on density, identifying clusters as densely packed regions and outliers as noise.

MODEL USED

S

AUTOENCODER

It is generative machine learning model that learns a probabilistic representation of data, allowing it to generate new samples similar to the training data

VAE

A Variational Autoencoder (VAE) is a type of deep generative model that learns to represent input data in a compressed latent space and then reconstructs it as closely as possible to the original

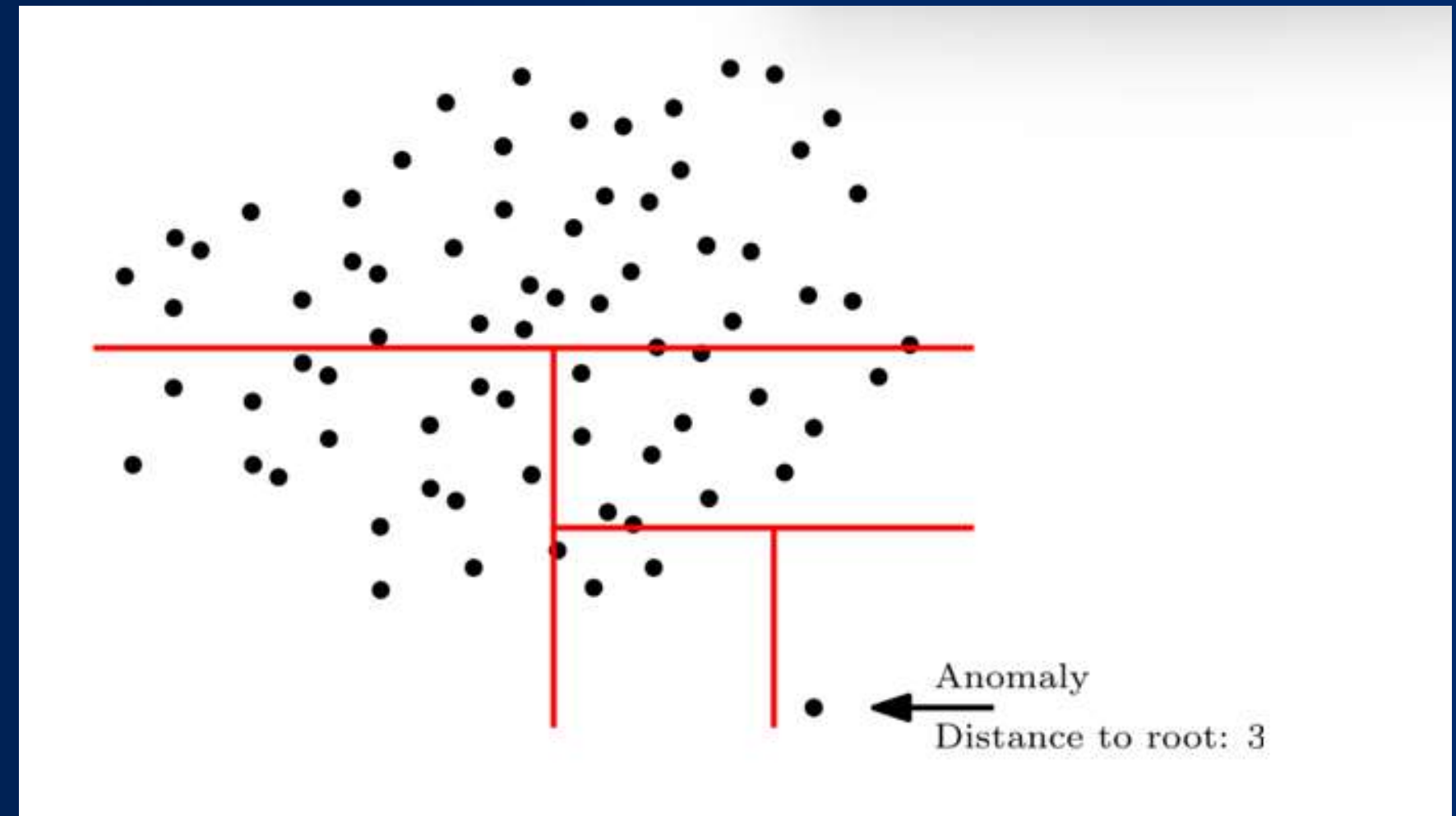
ISOLATION FOREST

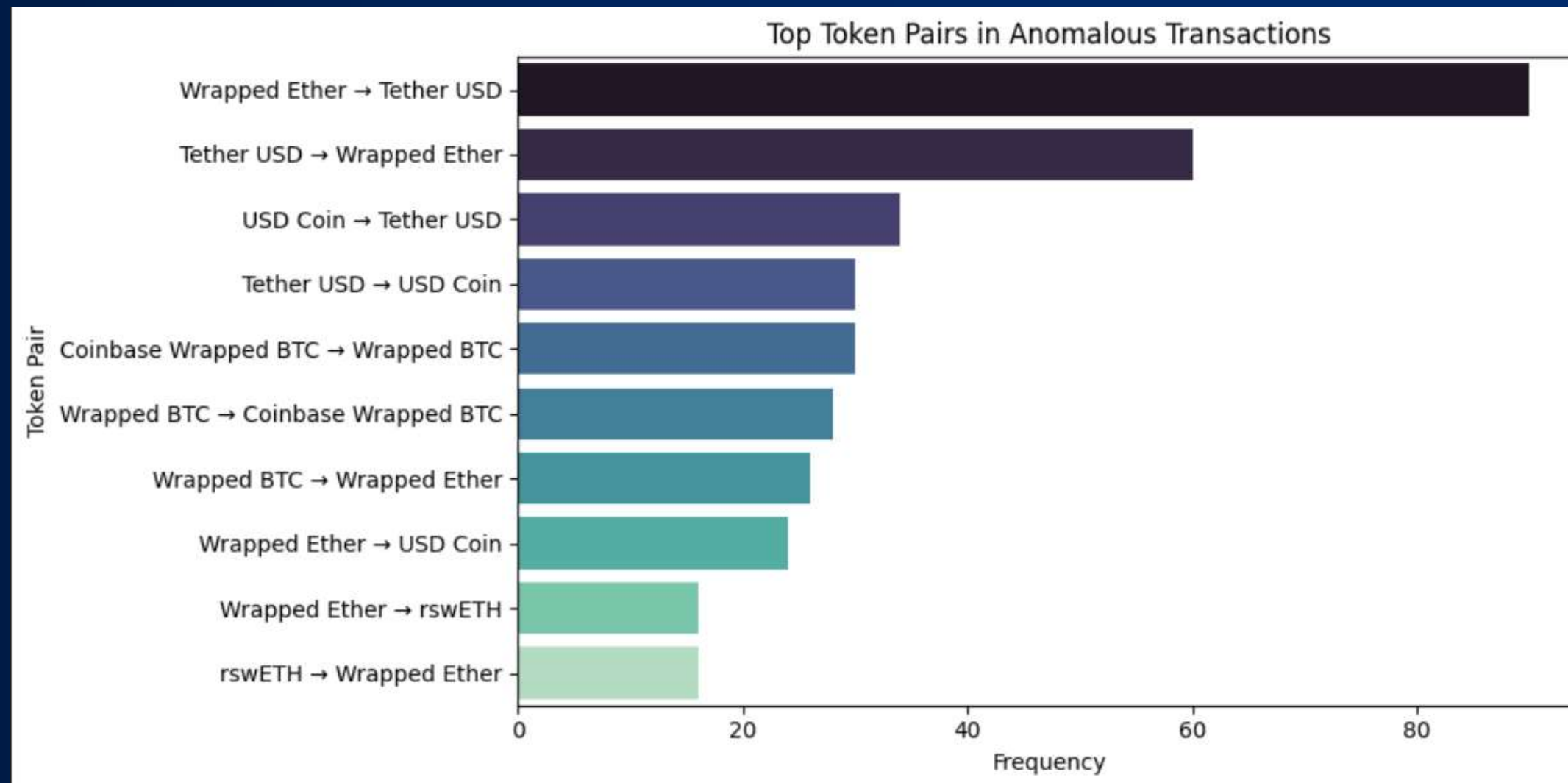
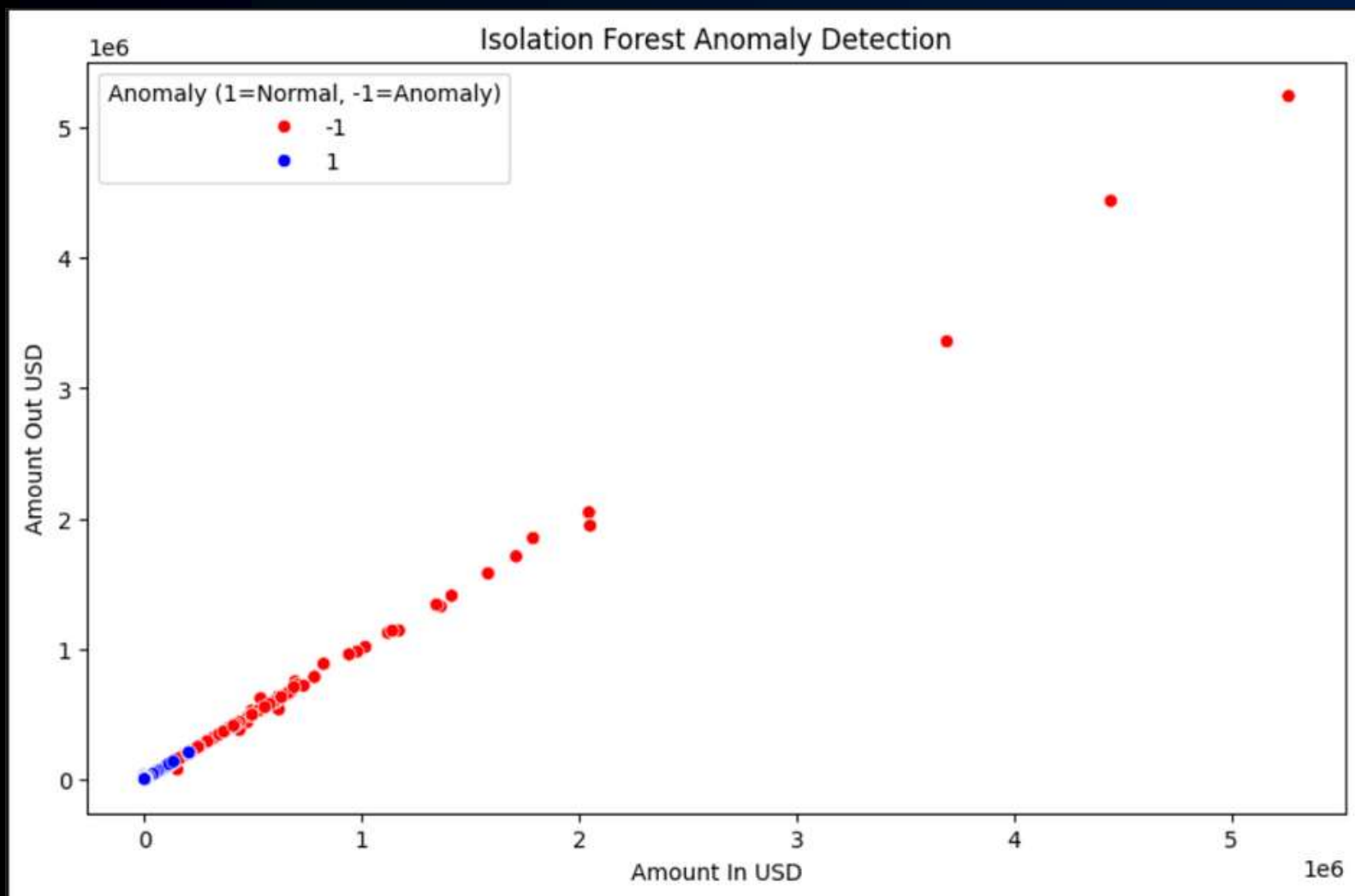
Workflow

- Randomly sub-sample dataset.
- Build isolation trees via random splits.
- Compute average path length for each point.
- Shorter paths → higher anomaly scores.
- Apply threshold to detect outliers.

Assumptions

- Anomalies are rare and easier to isolate.
- Random splits isolate anomalies faster than normal points.
- Feature independence (loosely assumed).





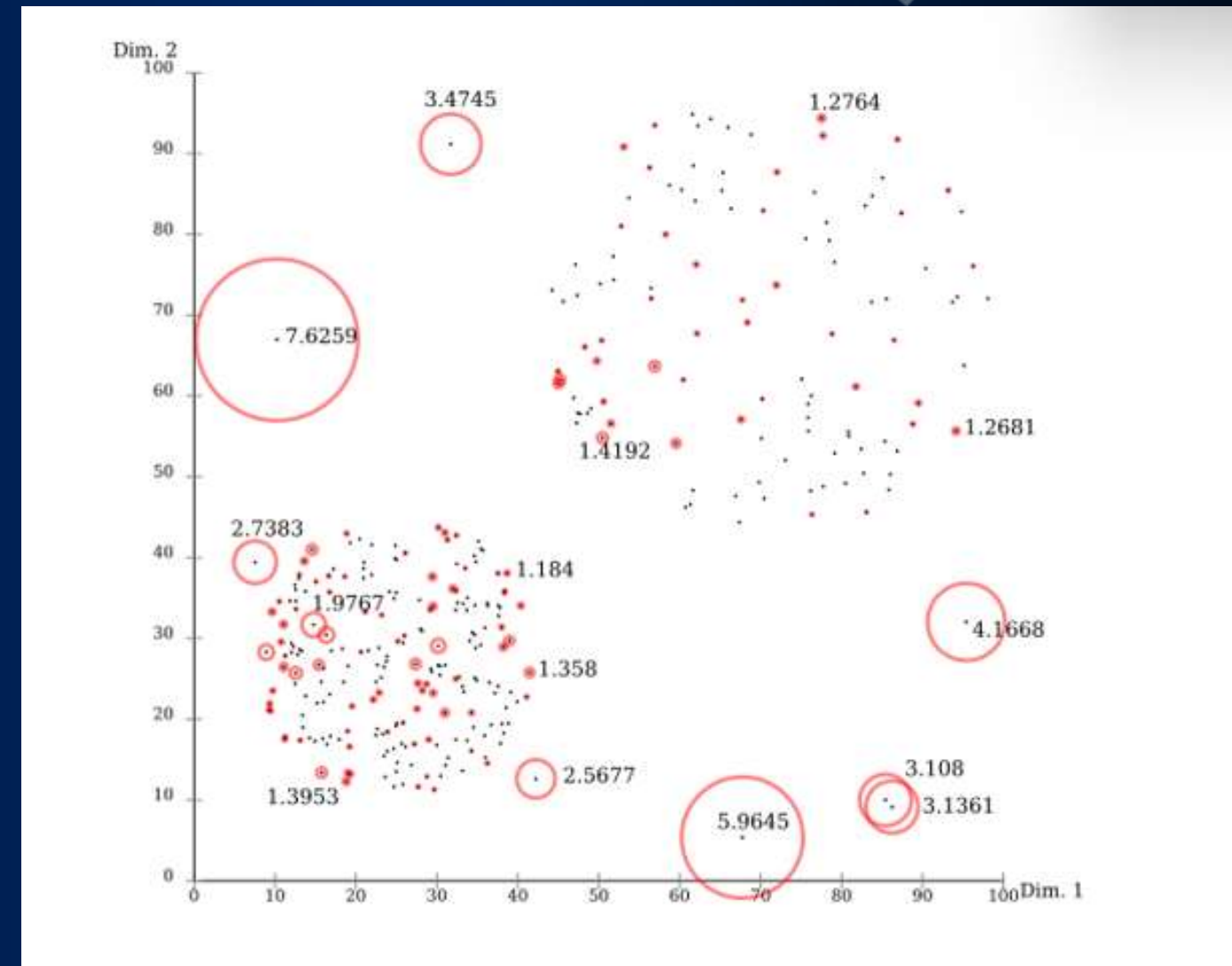
LOF

Workflow

- Scale data, choose k.
- Compute k-nearest neighbors.
- Estimate local reachability density (LRD).
- Compute LOF score for each point.
- High LOF score → potential anomaly.

Assumptions

- Normal points have similar local densities.
- Outliers have lower density than neighbors.
- Requires a good choice of k (neighbors).

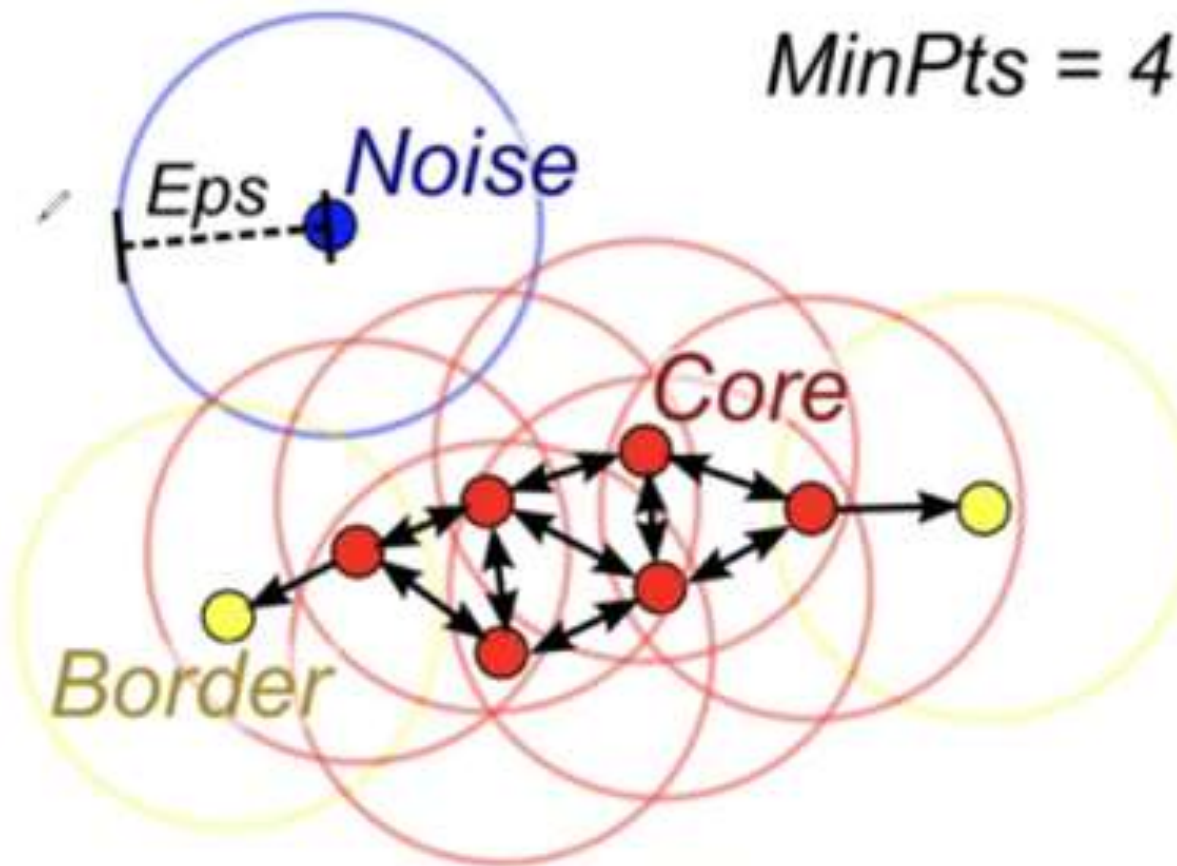


```
# Compare anomalies detected by both
common = set(df[df["anomaly_iso"] == -1]["hash"]) & set(df1[df1["anomaly_lof"] == -1]["hash"])
print("Common anomaly transactions:", len(common))
```

```
Common anomaly transactions: 53
```

DBSCAN

Density-Based Spatial Clustering of Applications with Noise (DBSCAN)



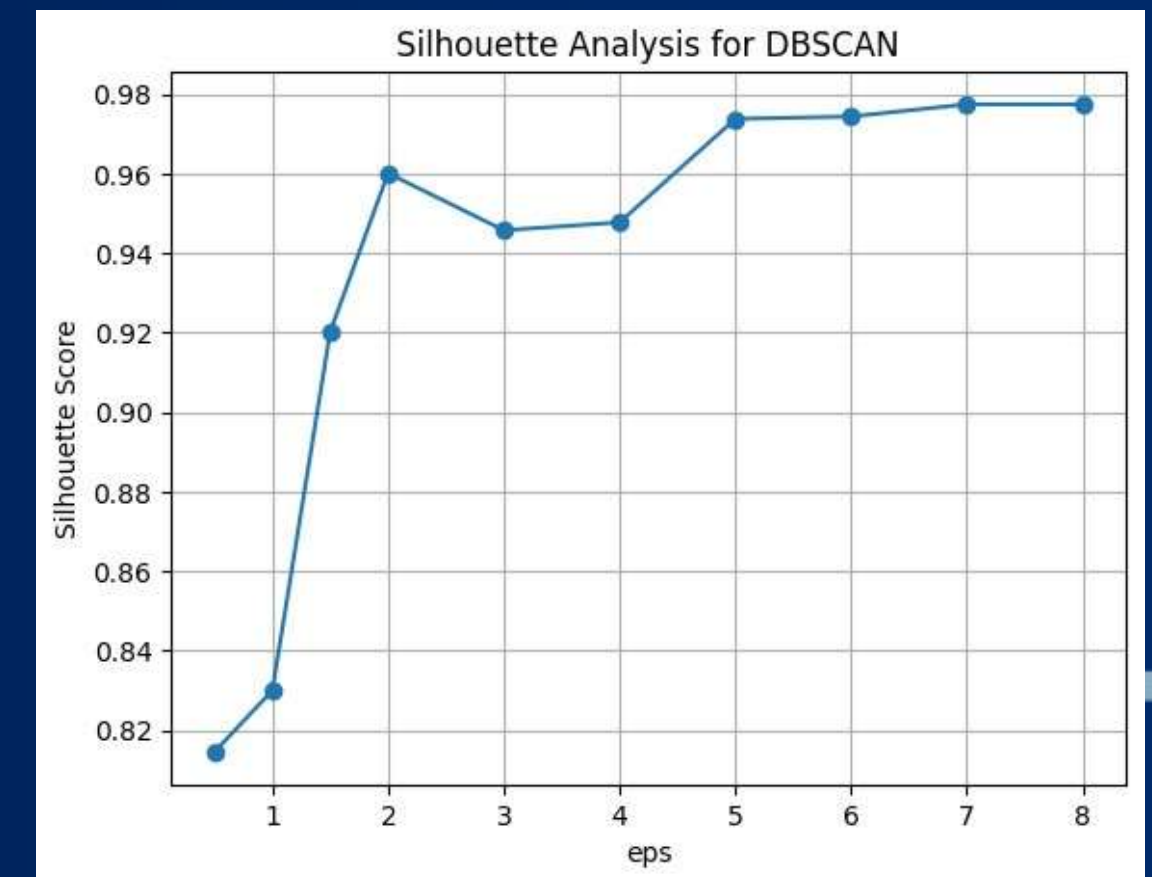
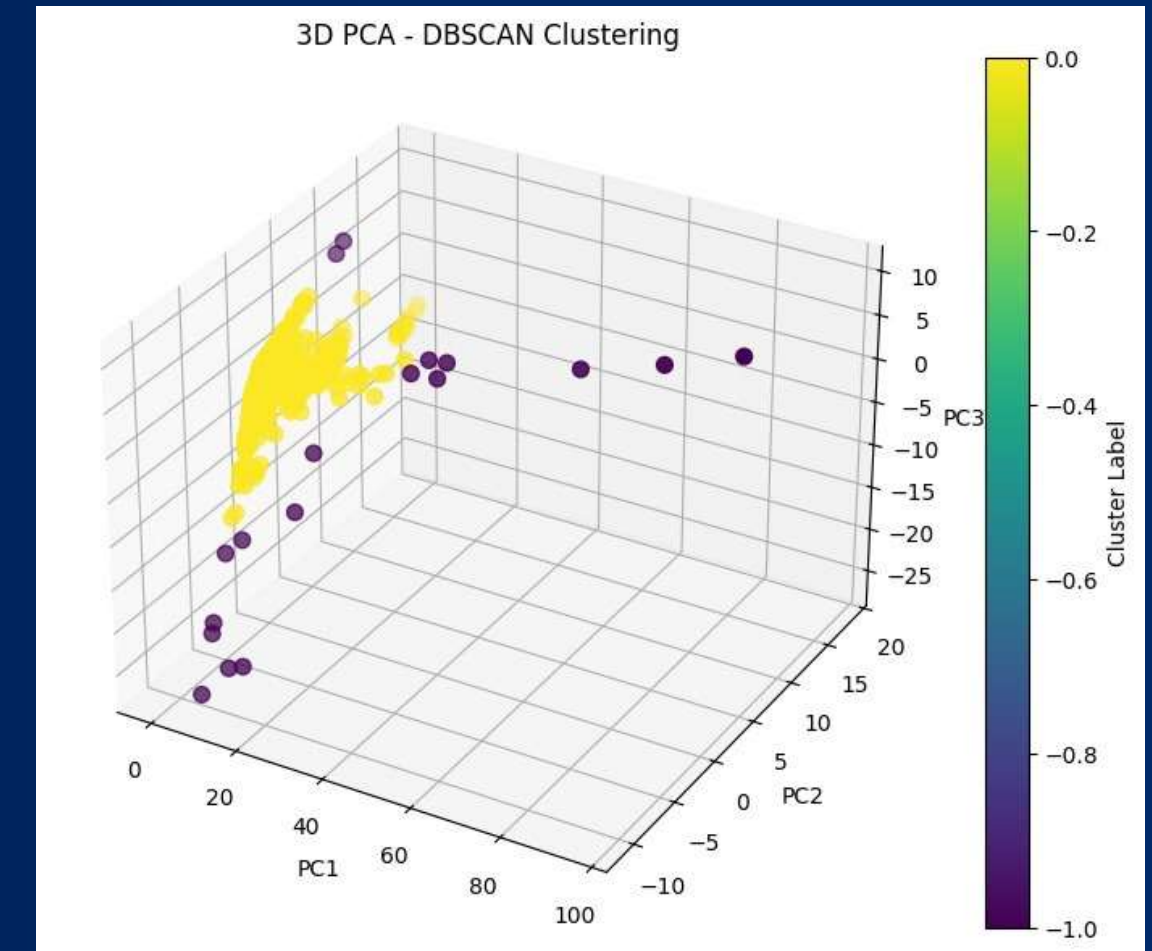
Red: Core Points

Yellow: Border points. Still part of the cluster because it's within epsilon of a core point, but not does not meet the min_points criteria

Blue: Noise point. Not assigned to a cluster

Assumption

- Clusters exist as dense regions.
- Noise lies in low-density regions.
- Distance metric accurately reflects structure.



AUTOENCODER

What is an Autoencoder?

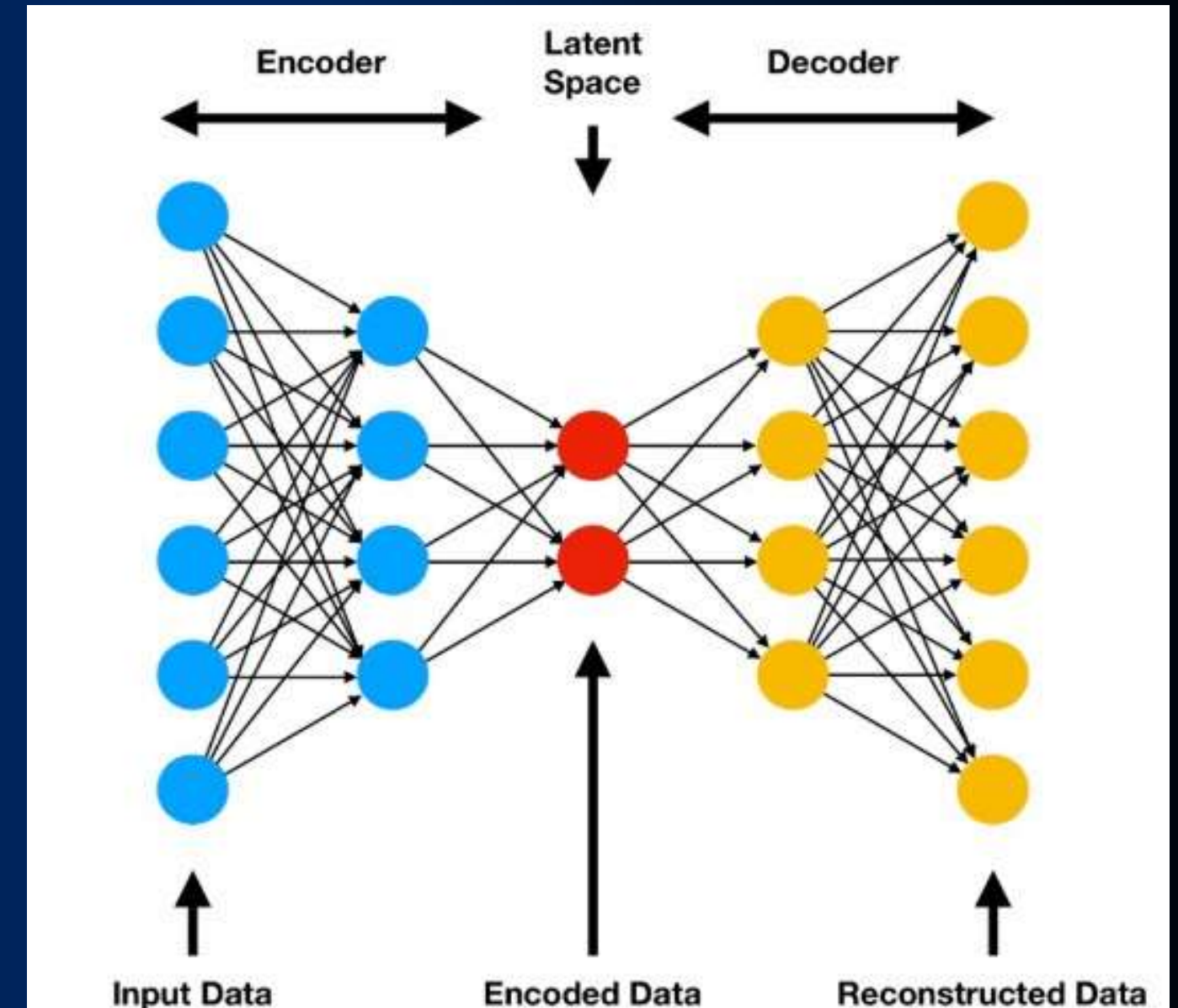
- An unsupervised neural network architecture trained to reconstruct its input.

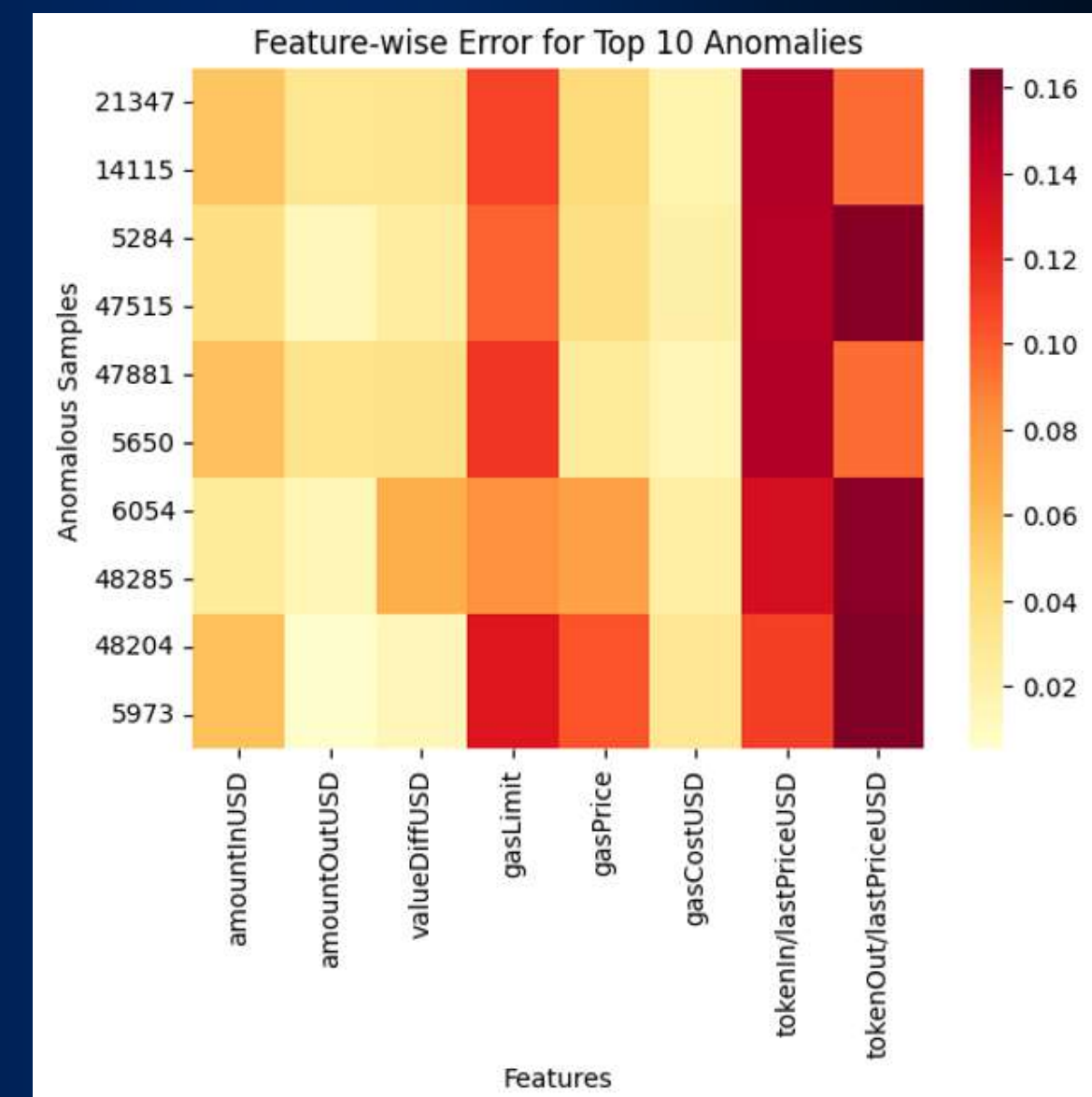
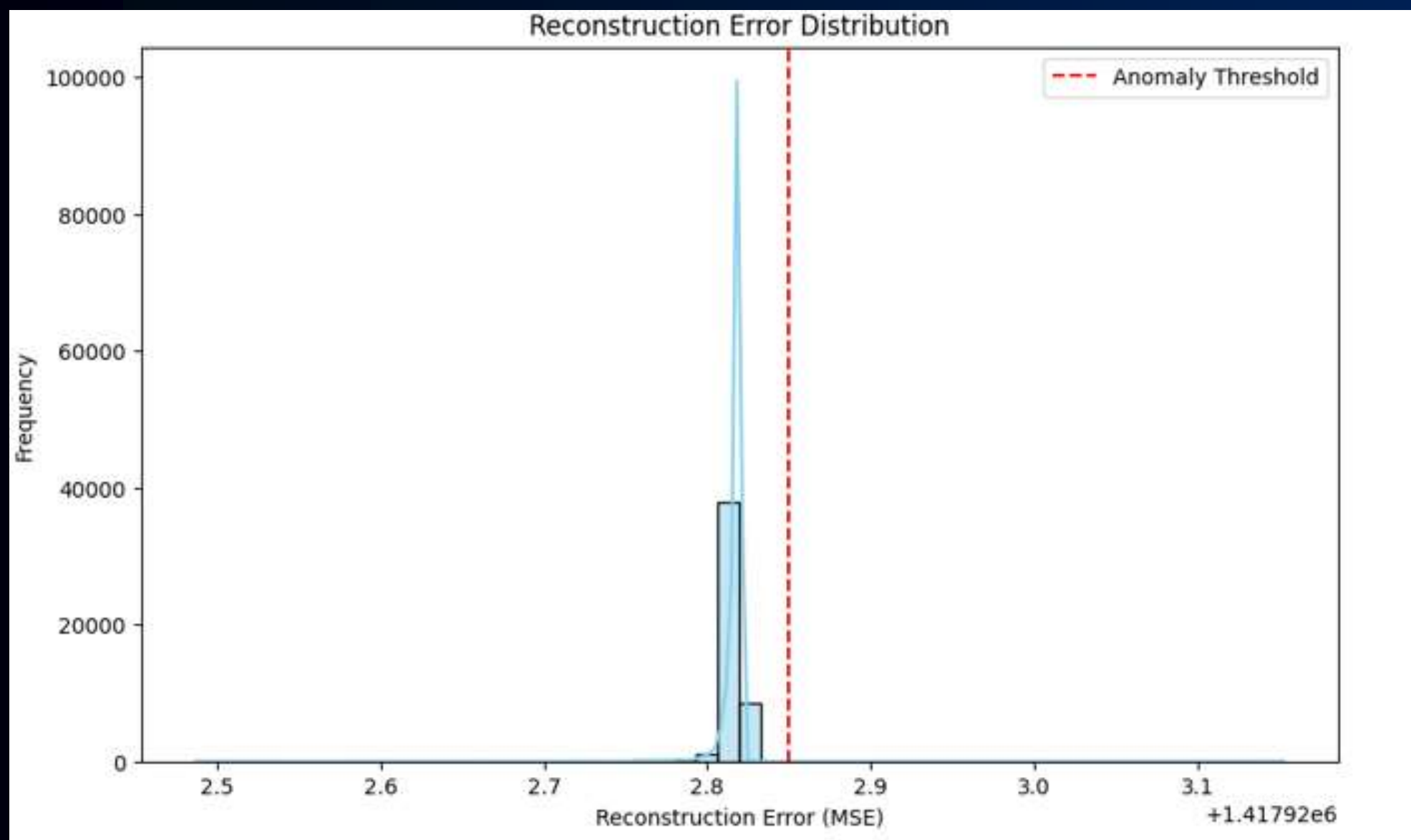
Composed of two parts:

- Encoder: Compresses the input data into a lower-dimensional latent representation.
- Latent Space (Code): This is the compressed version — like a summary of the original data.
- Decoder: Reconstructs the original data from this representation.

Why use Autoencoders for Anomaly Detection?

- Trained on normal (non-anomalous) data, the autoencoder learns to reconstruct only typical patterns.
- Anomalies are poorly reconstructed → leading to higher reconstruction errors.

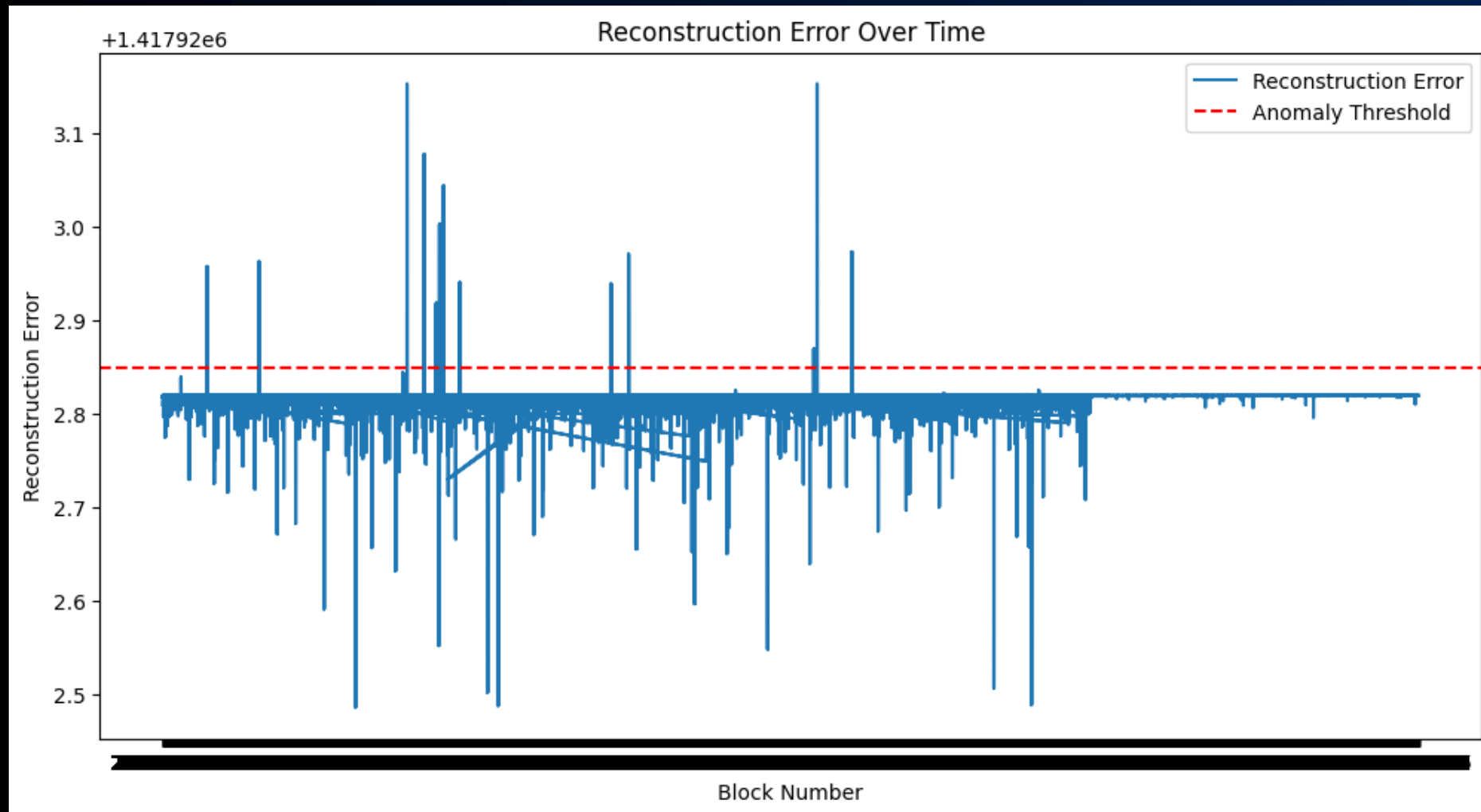




How anomalies were detected:

- Computed Mean Squared Error (MSE) between original input and reconstructed output.
- Set an anomaly threshold based on reconstruction error distribution.
- Points with error above the threshold were flagged as anomalies.

```
Top contributing features to anomaly detection:
tokenIn/lastPriceUSD    0.137370
tokenOut/lastPriceUSD   0.135592
gasLimit                 0.106509
gasPrice                 0.056751
amountInUSD              0.046799
valueDiffUSD             0.035128
gasCostUSD               0.021848
amountOutUSD             0.020246
dtype: float64
```



- MODEL ANALYZED 55,696 BLOCKCHAIN TRANSACTIONS USING RECONSTRUCTION ERROR FROM AN AUTOENCODER.
- ANOMALY THRESHOLD WAS SET BASED ON RECONSTRUCTION ERROR DISTRIBUTION, ENSURING A DATA-DRIVEN AND STATISTICALLY SOUND APPROACH.
- 2,405 TRANSACTIONS (~4.3%) WERE FLAGGED AS ANOMALIES, INDICATING A RARE BUT MEANINGFUL PATTERN OF DEVIATIONS.
- FEATURE-WISE HEATMAP REVEALED KEY ANOMALY CONTRIBUTORS, ESPECIALLY:
 - TOKENIN/LASTPRICEUSD
 - TOKENOUT/LASTPRICEUSD
 - GASLIMIT

[illegible]

VAE

A Variational Autoencoder (VAE) is a type of deep generative model that learns to represent input data in a compressed latent space and then reconstructs it as closely as possible to the original. Unlike traditional autoencoders, VAEs model the latent space probabilistically, allowing them to capture the underlying distribution of the data.

Architecture:

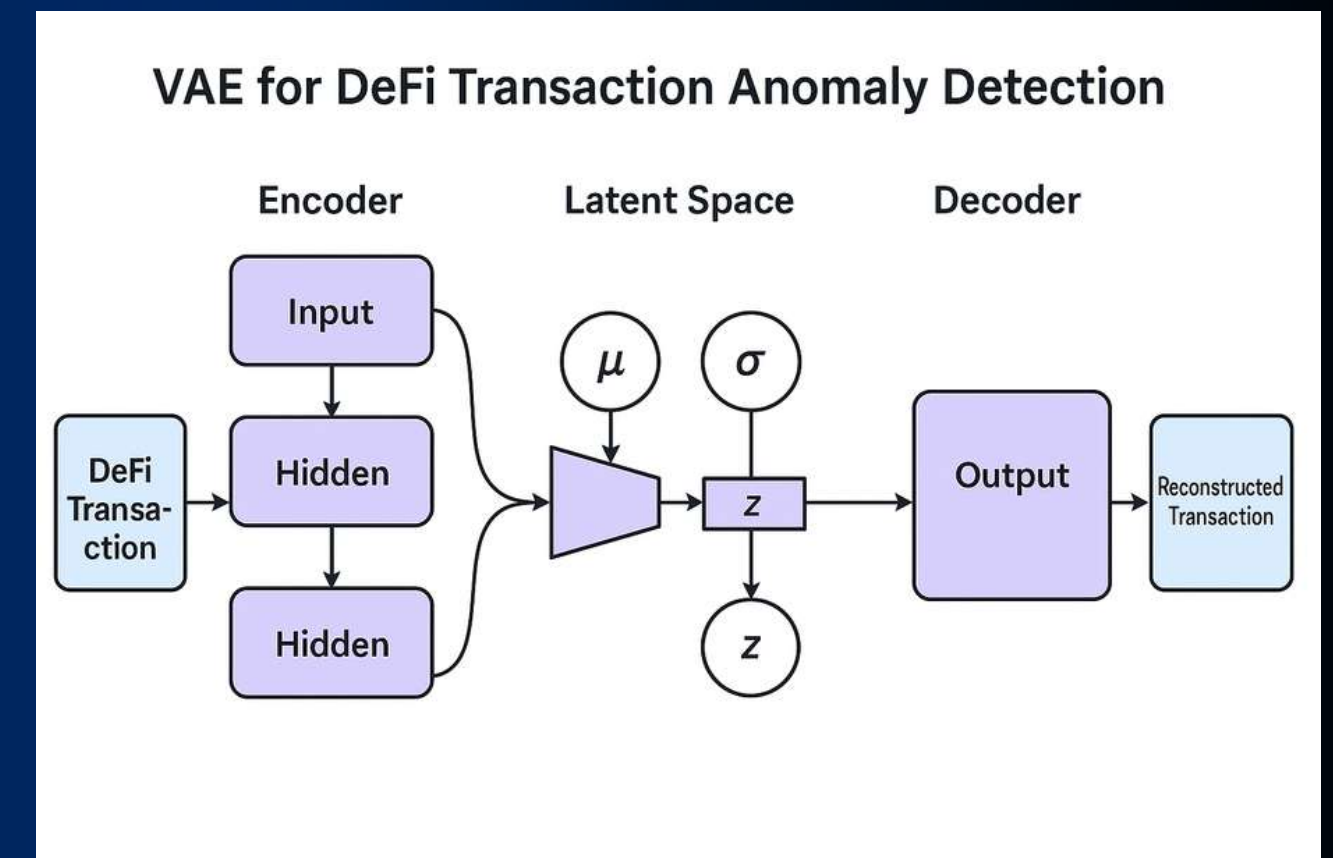
- Encoder: Maps input data to a latent distribution (mean & variance).
- Latent Space: A probabilistic space where samples are drawn using the learned distribution.
- Decoder: Reconstructs data from sampled latent vectors.

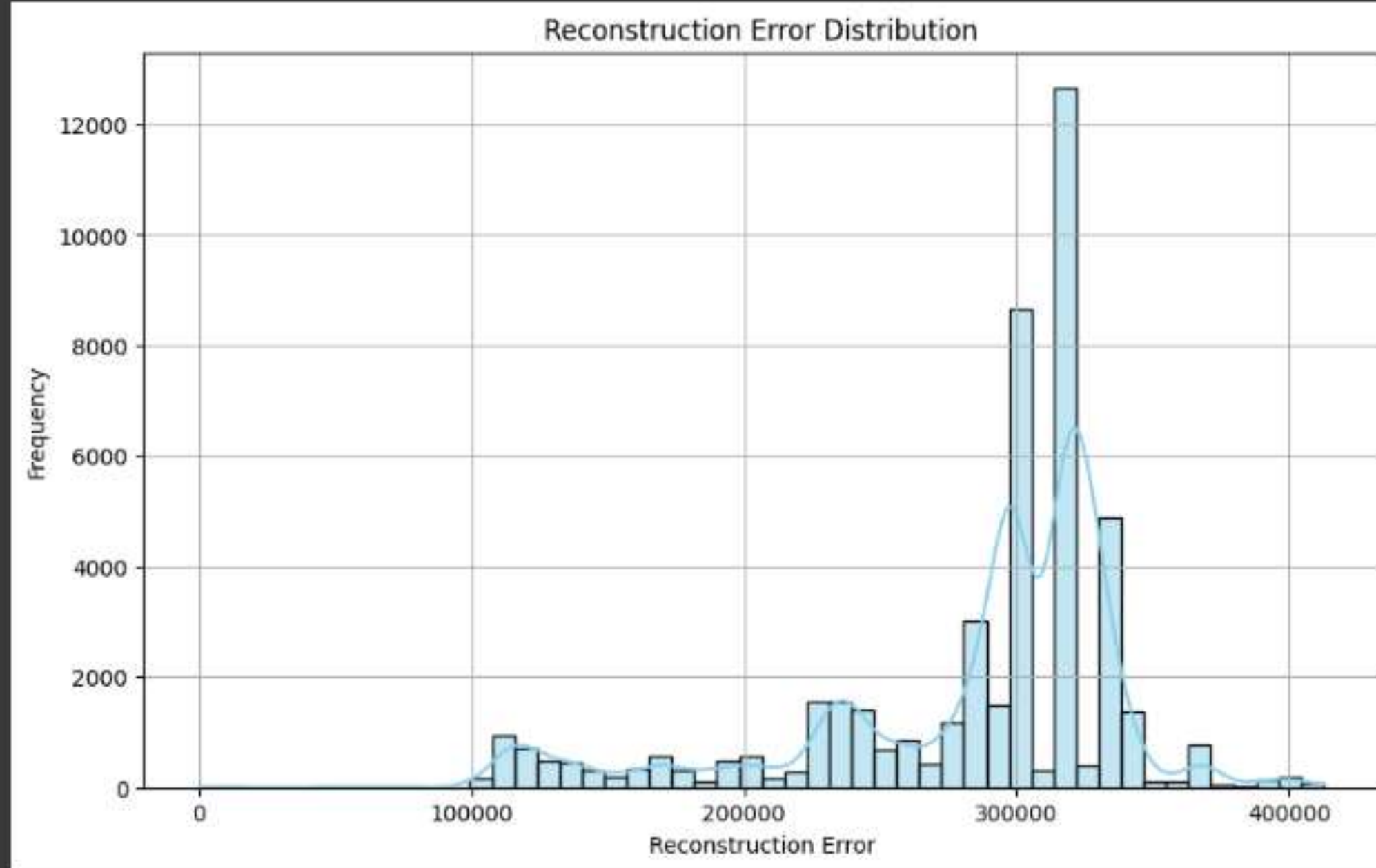
how does the model learn?

The VAE uses a loss function with two terms:

The first is the Reconstruction Loss – which measures how well the output matches the input.

The second term is the KL Divergence Loss, which measures how close our learned latent distribution is to a standard normal distribution, $N(0, I)$. This acts as a regularizer and keeps the latent space well-behaved, smooth, and continuous.





- Most transactions have reconstruction error between 270k–320k.
- Transactions with errors beyond ~350k may indicate anomalies.
- This distribution confirms the VAE has effectively learned the structure of typical transactions.
- Useful for flagging unusual or risky transactions.

CONCLUSION



- We used a Variational Autoencoder (VAE) to analyze over 55,000 blockchain transactions and detect unusual activity. The model works by trying to reconstruct normal transactions, and if it makes a big error, it means the transaction is likely anomalous.
- Established a statistically grounded threshold from the error distribution, ensuring a robust, data-driven approach to anomaly detection without relying on arbitrary cutoffs..
- The model flagged around 2,400 transactions as anomalies, which is close to the 5% flagged by the Isolation Forest model, showing our results are consistent and accurate.
- Most normal transactions had low reconstruction errors (around 270k–320k), while anomalies had much higher errors, usually over 350k. This means the VAE clearly learned what a typical transaction looks like.
- Overall, this method shows strong potential to automatically catch risky or suspicious blockchain activity, helping make DeFi systems more secure.

LIMITATIONS

- API issue of Paid and Free
- Data issue a lot of the rows or columns were in in comprehensible
- Interpretability and Trust



FUTURE TRENDS



1. Integration with Real-Time Monitoring Systems

Future DeFi anomaly detection systems can be integrated with real-time monitoring tools to instantly identify and respond to threats like flash loan attacks or rug pulls as they happen.

2. Self-Learning and Adaptive Models

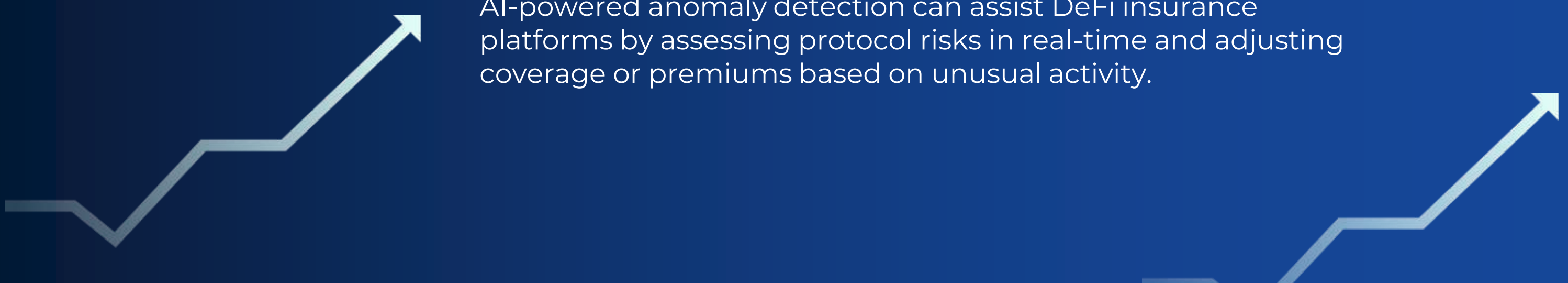
Detection models can evolve into self-learning systems that automatically adapt to new fraud patterns and protocol updates without needing full retraining.

3. Collaboration with Regulators and Auditors

Anomaly detection tools can support emerging DeFi regulations by helping auditors and regulators automatically identify risky transactions and ensure protocol compliance.

4. AI-Driven DeFi Insurance Risk Assessment

AI-powered anomaly detection can assist DeFi insurance platforms by assessing protocol risks in real-time and adjusting coverage or premiums based on unusual activity.





THANK YOU!