Anomaly detection

Comparison between Classical and Quantum Variational Autoencoders

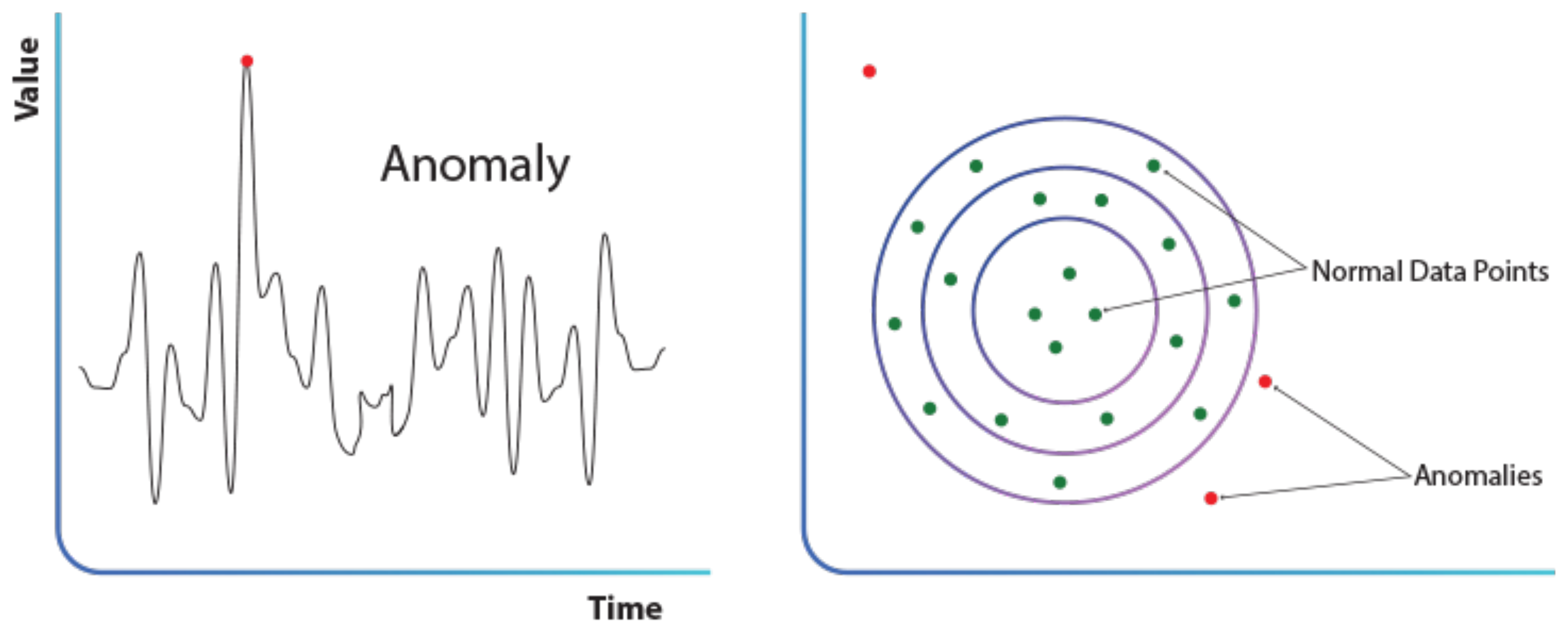
Edoardo Zappia

PML exam 11th July

Anomaly detection
Problem definition

In data analysis, anomaly detection is generally understood to be the identification of rare items, events or observations which deviate significantly from the majority of the data and do not conform to a well defined notion of normal behavior.

Anomaly detection finds application in many domains including robotics, cybersecurity, medicine, machine vision, statistics, neuroscience, law enforcement and financial fraud



Global Market Size for Fraud Detection and Prevention 2022

Grand View Research:
$25.67 billion
Compound Annual Growth Rate (CAGR): 17.6% from 2023 to 2030 [1]

Global Market Insights:
$30 billion
Estimated growth:
25% from 2023 to 2032 [2]

[1] Grand View Research GVG:

https://www.grandviewresearch.com/industry-analysis/fraud-detection-prevention-market#:~:text=The%20global%20fraud%20detection%20%26%20prevention,USD%2028.98%20billion%20in%202023.

[2] Global Market Insights:

https://www.gminsights.com/industry-analysis/fraud-detection-and-prevention-market

Variational Autoencoder

Possible solution using classical computation

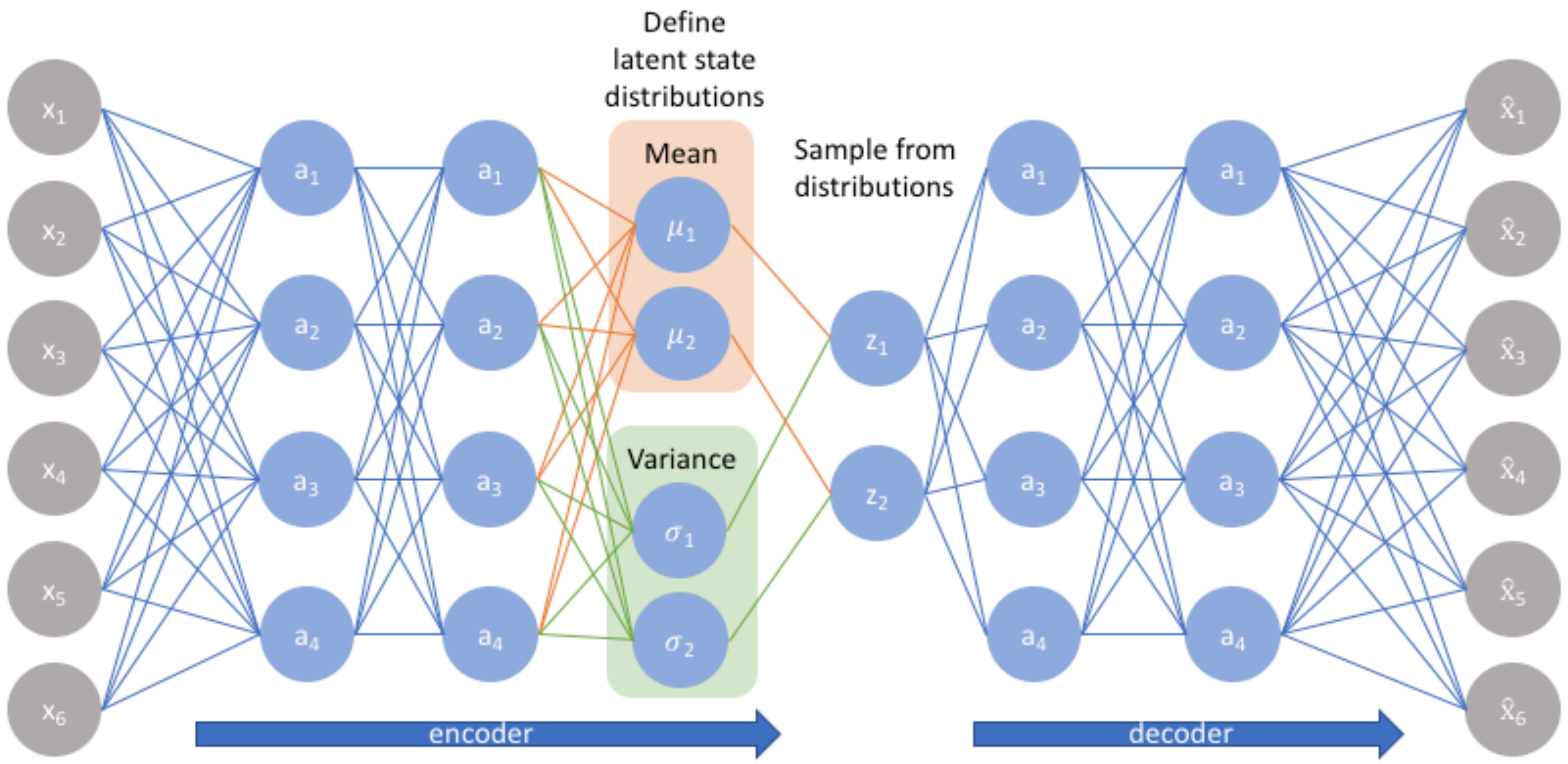
Goal: estimate the distribution $p(x)$

Tool: latent variables z, $p(x, z \mid \theta) = p(x \mid z, \theta)p(z)$

Constraint: posterior distribution $p(z \mid x)$ intractable

Object of optimization:

$$\mathscr{L}(\theta, \phi) = \mathbb{E}_{q(\mathbf{z}|\mathbf{x},\phi)}\left[\log p(\mathbf{x} \mid \mathbf{z}, \theta)\right] - \mathrm{KL}\left[q(\mathbf{z} \mid \mathbf{x}, \phi) \parallel p(\mathbf{z})\right]$$



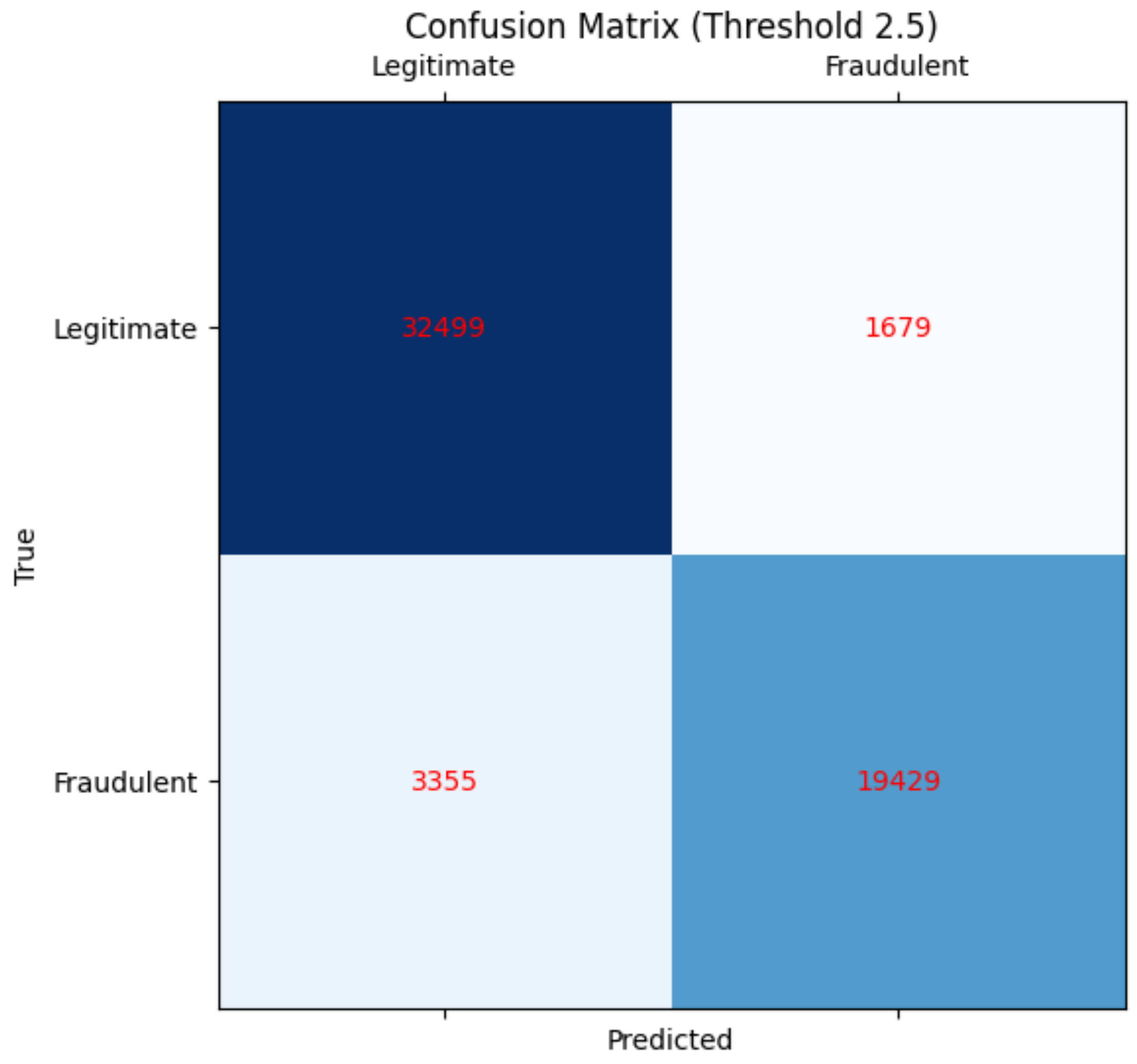
Technical Details:

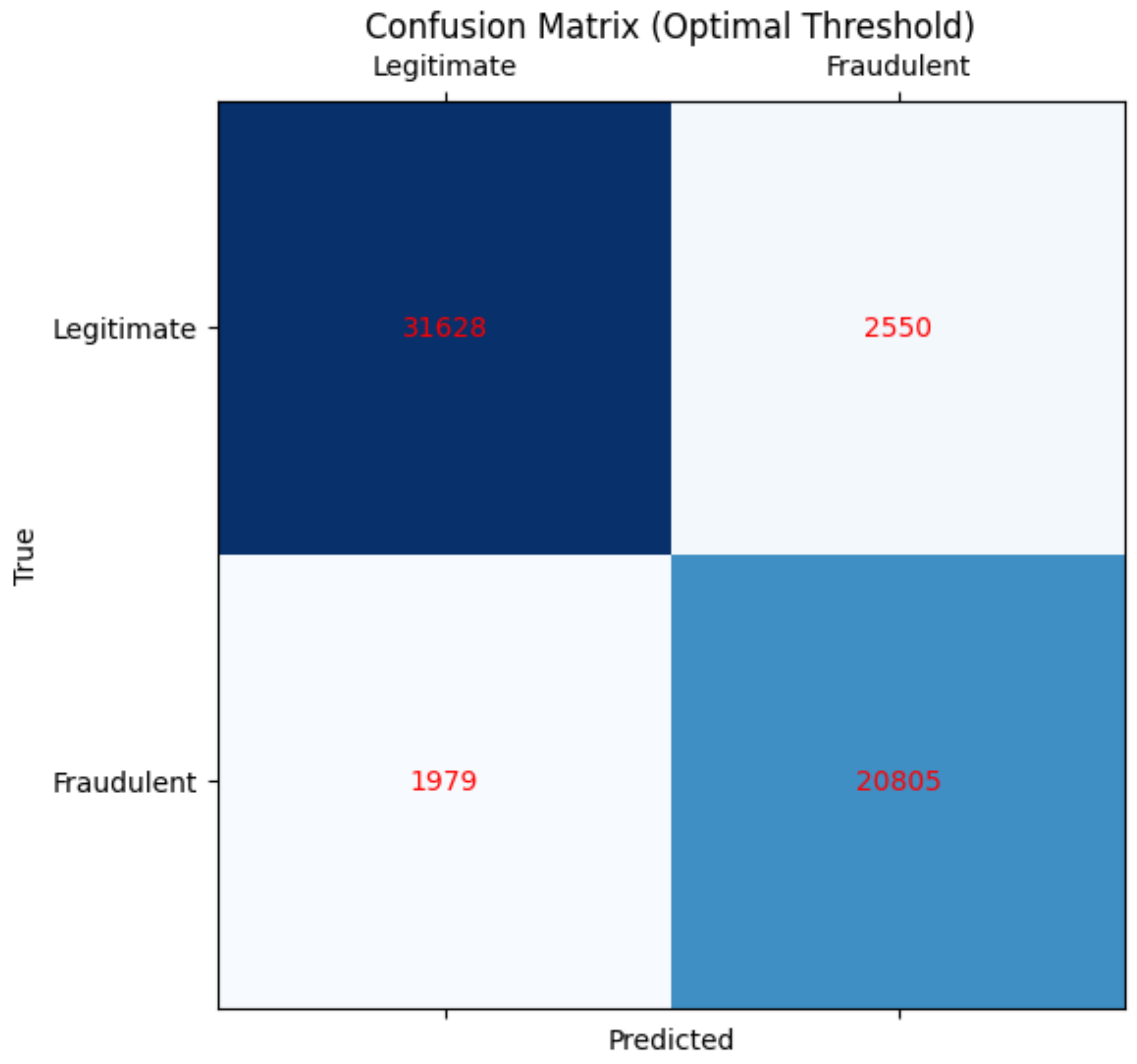
- Encoder: input layer, 3 dense layers with 20, 10, and 8 neurons, computes mean and std of z
- Latent space: latent dimension of 2
- Decoder: 3 dense layers with 8, 10, and 20 neurons, and an output layer with sigmoid activation.

Variational Autoencoder

Results

Anomaly detection: The idea is to train the VAE exclusively with legitimate transactions. This way, when a fraudulent transaction is presented, the reconstruction error will exceed a predetermined threshold (either arbitrarily set or optimized according to chosen metrics)





Arbitrary Threshold: 2.5

AUC: 0.9114

Accuracy: 0.9114

Precision: 0.9198

Recall: 0.8527

F1-score: 0.8850

Optimal Threshold: 1.9515

AUC: 0.9519

Accuracy: 0.9205

Precision: 0.8908

Recall: 0.9131

F1-score: 0.9018

Quantum Autoencoder

Possible solution using quantum computation

Amplitude encoding: Ansatz composed of CNOT and RY gates that encodes classical data into the probability amplitudes of the quantum state

Qubit: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \alpha, \beta \in \mathbb{C}$

Encoder: Variational quantum circuit (QNN)
Maps the input $|\psi_x\rangle$ into the latent spate $|\psi_z\rangle$

Swap test (training): Utilizes an ancilla qubit to measure the similarity between the input and latent quantum states (probability amplitudes)

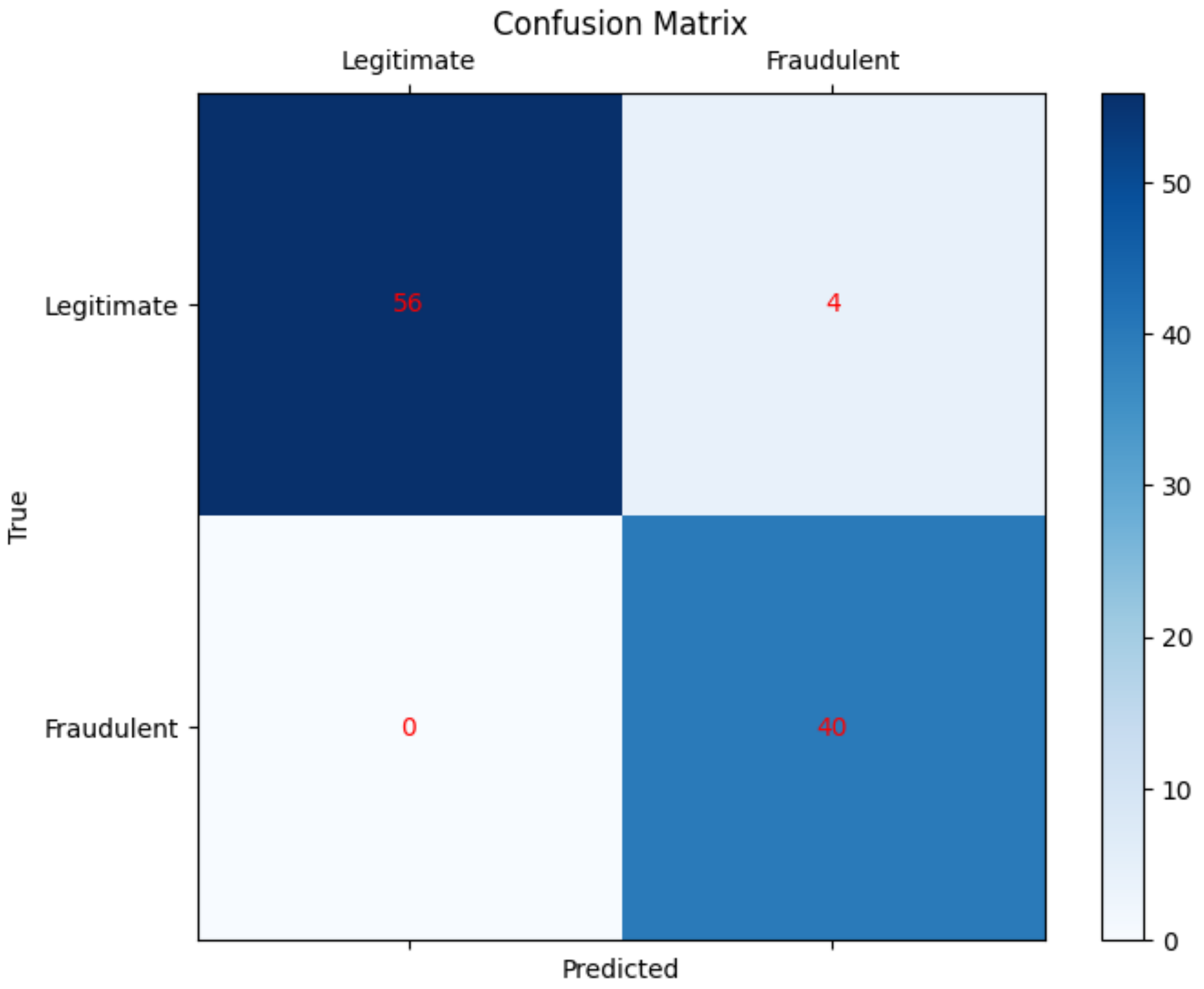
Reset to zero: Reset the state of some qubits to $|0\rangle$

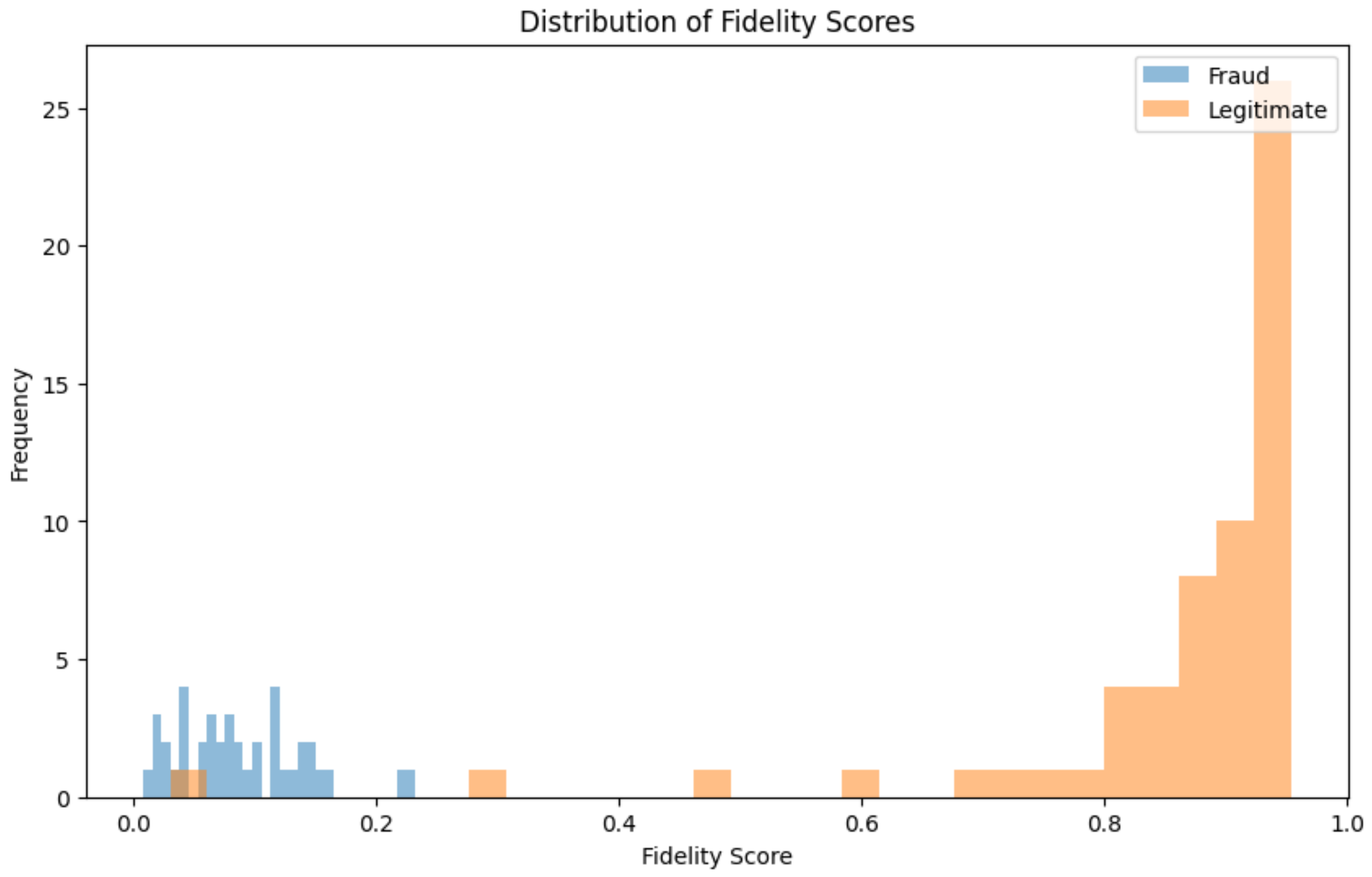
Decoder: Hermitian conjugate of the encoder
Reconstructs the original state $|\psi_{\hat{x}}\rangle$ from the latent state $|\psi_z\rangle$

Quantum Autoencoder

Results

Anomaly detection: The model is trained exclusively on legitimate transactions and subsequently tested on a dataset of unseen legitimate transactions. The threshold is set as the mean fidelity minus one standard deviation. When a fraudulent transaction is presented to the model, the fidelity will fall below this threshold





Dataset:

Train: 100 legitimate

Validation: 100 legitimate

Test: 60 legitimate 40 fraudulent

AUC: 0.9667

Accuracy: 0.96

Precision: 0.9090909090909091

Recall: 1.0

F1-score: 0.9523809523809

Comparison

Classical vs Quantum

Classical VAE

- A lot of samples required
- Fast training
- Good performance
- Easier to trace operations
- Easier debug

Quantum AE

- Few samples
- Encoding of classical data may effect performance
- Few resources
- Slow training with simulators
- Good performance
- More difficult to trace operations
- More difficult to debug