RMIT UNIVERSITY

School of Science, Engineering & Technology

BY BTECH X SSET

PUMP.FUN

SCAN ME

AUTHORS:

Nguyen Phat Dat - s3894433
Nguyen Hoang Phuong - s3924593
Phan Vinh Loc - s3938497
Le Phuc Thinh - s3893964
Nguyen Tien Dung - s3999561

OBJECTIVE

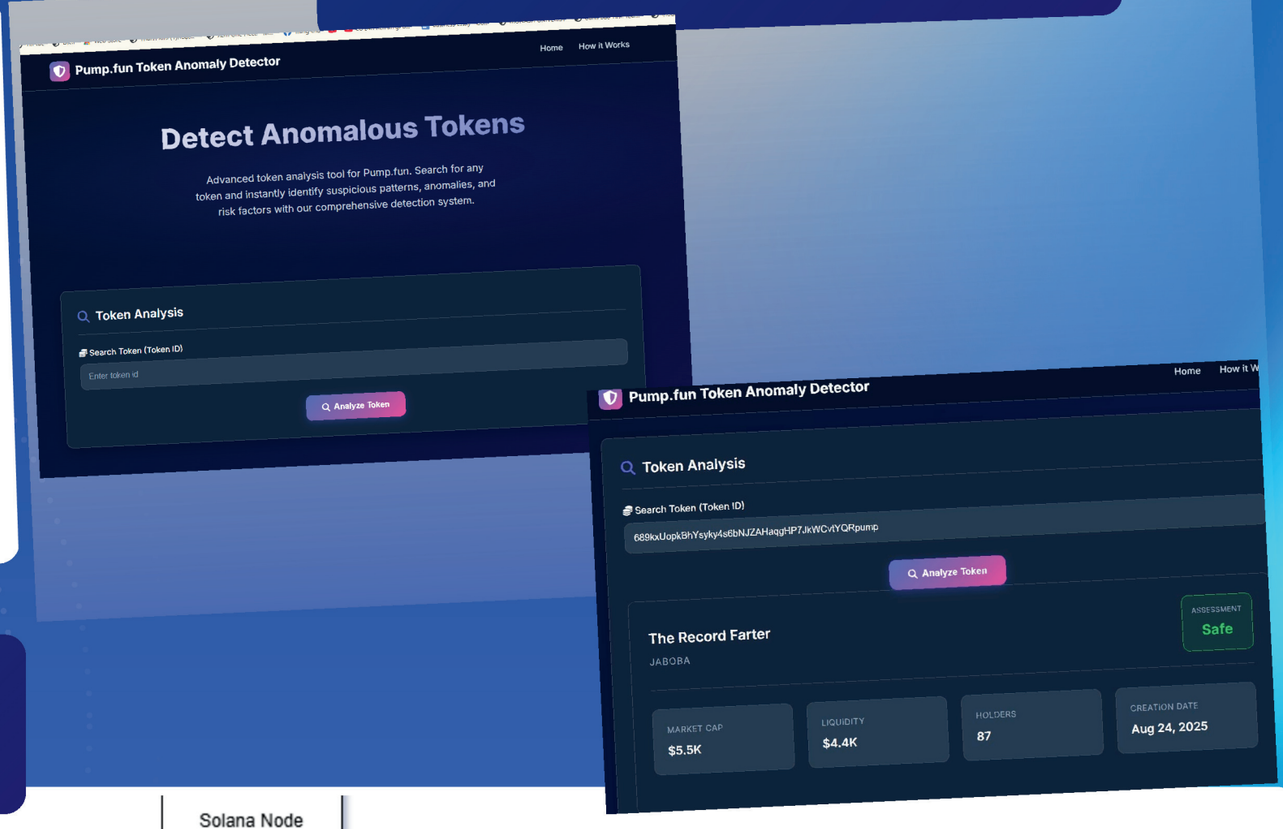
Our objective is to develop a scalable fraud detection system for the Solana blockchain that uses machine learning to classify transactions with over 85% accuracy, ensure data integrity above 90%, and improve anomaly detection. The system will include a user-friendly web interface for near real-time monitoring, enhancing security and trust on platforms like Pump.fun while supporting future cross-blockchain applications.

Background & Motivation

The rise of DeFi on the Solana blockchain has enabled fast, low-cost transactions and token creation on platforms like Pump.fun, but also exposed users to risks such as rug pulls and pump-and-dump scams. Existing detection methods lack the scalability and accuracy to address these challenges, leading to financial losses and reduced trust. This motivates our project to develop a machine learning–based fraud detection system that enhances transparency, protects users, and strengthens confidence in DeFi platforms.

Pump.fun

Website LayOut

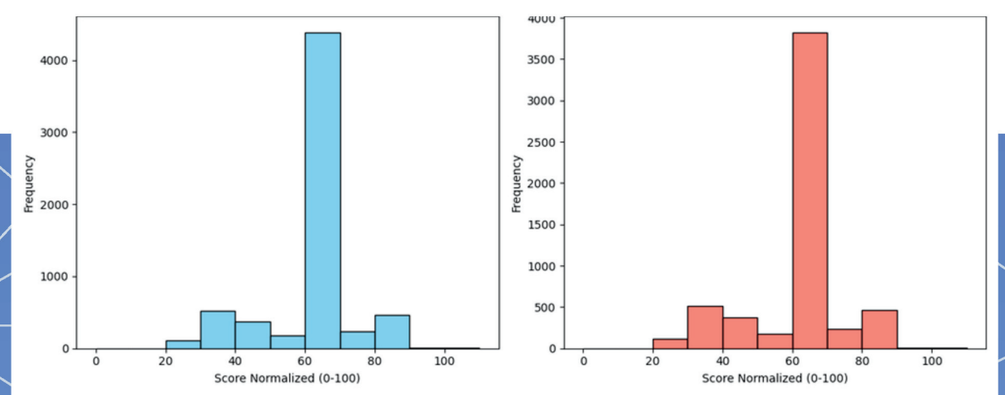


Methodology

The methodology of our project began with collecting transaction data from the Solana blockchain through an ingestion service, ensuring consistent retrieval and organization. The raw data was then cleaned and validated to achieve over 90% integrity, removing duplicates and malformed records. Next, feature engineering was applied to extract meaningful attributes such as token transfer frequencies, graph metrics, and temporal patterns for fraud detection. Using these features, we trained a Random Forest classifier along with baseline anomaly detection models, tuning parameters to achieve at least 85% accuracy and a 2% improvement over existing methods. Once evaluated, successful models were deployed via a Flask server, which communicates predictions to a user-friendly web interface displaying fraud classifications and key metrics. The iterative workflow allows for retraining whenever performance drops, ensuring reliability and scalability. Future improvements will focus on refining anomaly detection techniques and expanding compatibility with other blockchain platforms.

Findings

- No public labeled dataset are available on Solana
- We have to create custom labeled data set through scraping and label them with Rugcheck for scores.
- Analyzing the inclusive dataset reveal most fraudulent token have around 62 score.
- We created a data pipeline to fetch token attributes
- Developed frontend and backend for fraud analysis.



Results & Conclusion

RESULTS:

- After analyzing datasets, we conclude on a fraudulent threshold
- Distribution graphs show most data hover around 60ish scores.
- A => 62 cutoff score to determined fraudulent tokens
- Random Forest model achieved target F1 score (~45%)
- Prototype system provides fraud analysis with good response time.

CONCLUSIONS:

- Demonstrated that fraud detection on Pump.fun is feasible with AI + labeled datasets.
- Self labeling data with Rugcheck verification enabled a reliable fraud threshold (62+ = fraud).
- Random Forest classifier + pipeline achieved required accuracy and efficiency.
- Created a frontend web application for fraudulent token detection