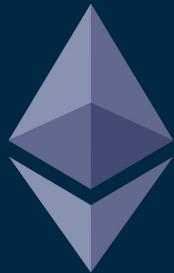


STAYING AHEAD OF FRAUDULENT ETHEREUM WALLETS

Nick Kim



FRAUD IN NUMBERS



PlusToken

\$3 billion Ponzi
Scheme ¹

180k *BTC*, 6.4m *ETH* and more
swindled from +3 million users

Google Chrome Extensions

49 Apps Removed from
Webstore ² around Apr 2020

Browser extensions disguised
leading to a loss of 1.4m *XRP*
before getting removed



Tokensniffer.com

Over 46,000 tokens ³
identified as scam
as of Oct 2021

Pranksy



NFT artwork from the artist Banksy
impersonator sold at \$300k ⁴

¹ [THE 2020 STATE OF CRYPTO CRIME](#); ² [Google Removes 49 Phishing Extensions That Steal Cryptocurrency Data](#); ³ [A whole new world of rug pulls, honeypots and crypto Ponzi schemes](#); ⁴ [Someone paid more than \\$300K for a fake Banksy NFT — and the scammer gave it all back](#)

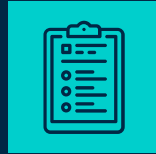
SOLUTION FOR THE ETHEREUM ORGANIZATION

- Build a classification model from known fraud accounts
- Provide functionality to **scan counterparty account address** to check for fraud likelihood



METHODOLOGY

Dataset of
Ethereum accounts



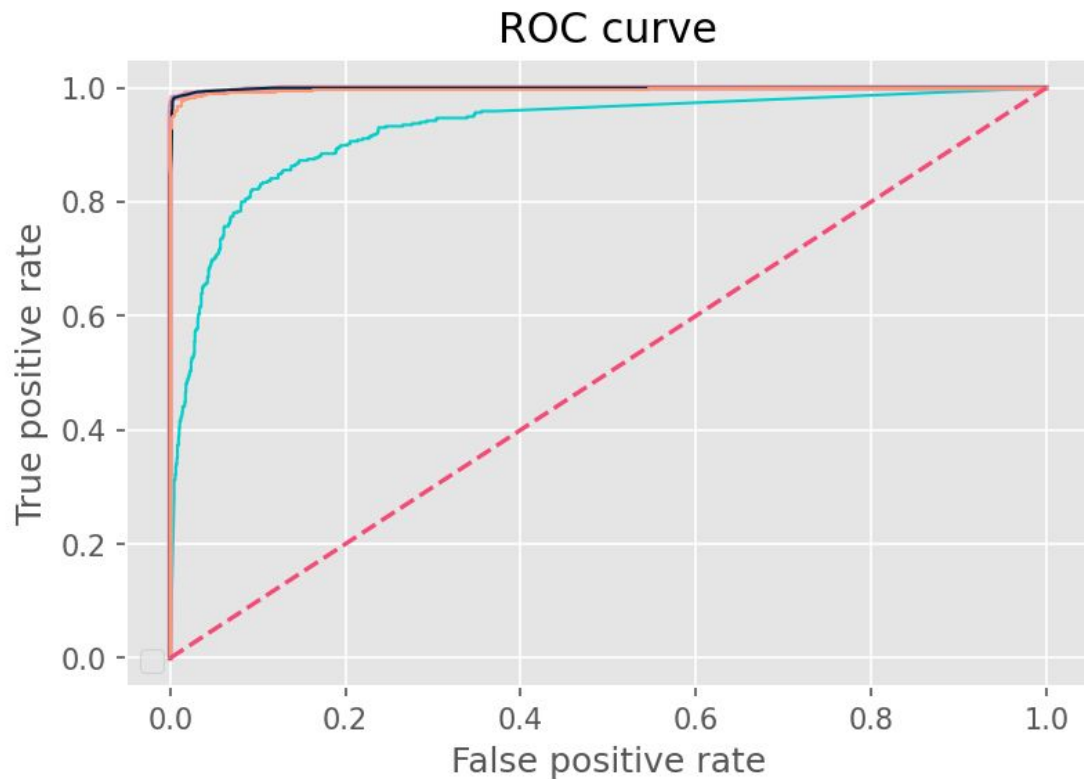
Preprocessing

Classify fraud
accounts



Evaluate
performance

TREE-BASED MODELS



Model	AUC	(Speed)
RandomForest	0.999	(10.5x)
Extra-Trees	0.999	(1.8x)
XGBoost	0.997	(fastest)
kNN	0.926	(78.0x)

WHAT DOES THE MODEL LOOK AT?



WHAT DOES THE MODEL LOOK AT?










Transactions

Erc20 Token Txns

Analytics

Comments

Latest 3 ERC-20 Token Transfer Events

Txn Hash	Age	From	To	Value	Token
 0xe51693a0af1435056...	899 days 20 hrs ago	Binance 3	 Fake_Phishing1269	1.337	 brief.blockw... (brief....)
 0xab5c9c0d067b51223...	1012 days 23 hrs ago	Binance 6	 Fake_Phishing1269	1.337	 Blockwell sa... (NOTSAF...)
 0x26cf7c727cb02e76b8...	1230 days 14 hrs ago	Black Hole: 0x000...000	 Fake_Phishing1269	911	 An Etheal Pr... (HEALP)

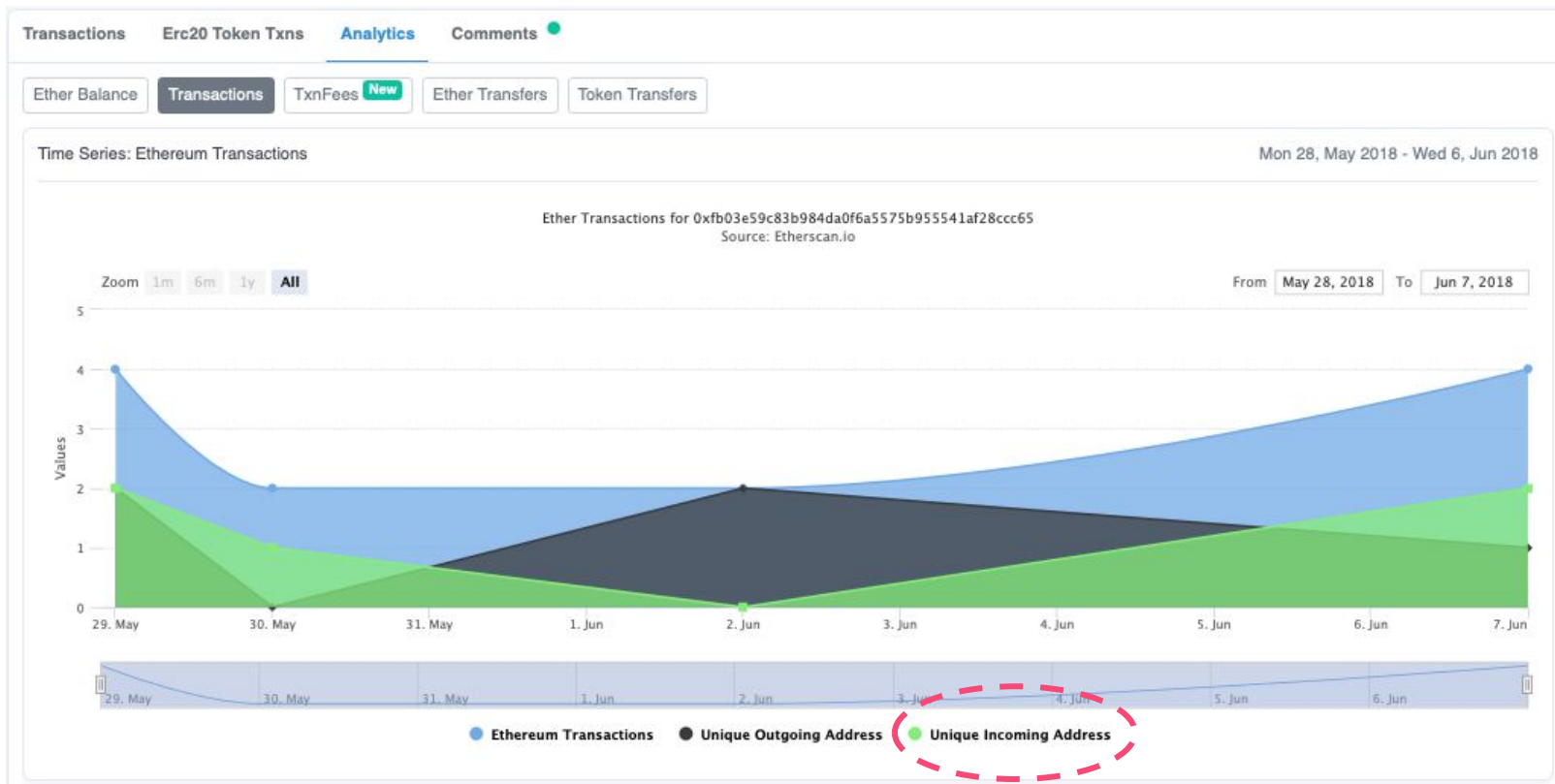
[\[Download CSV Export \]](#)

TransactionsErc20 Token TxnsAnalyticsComments

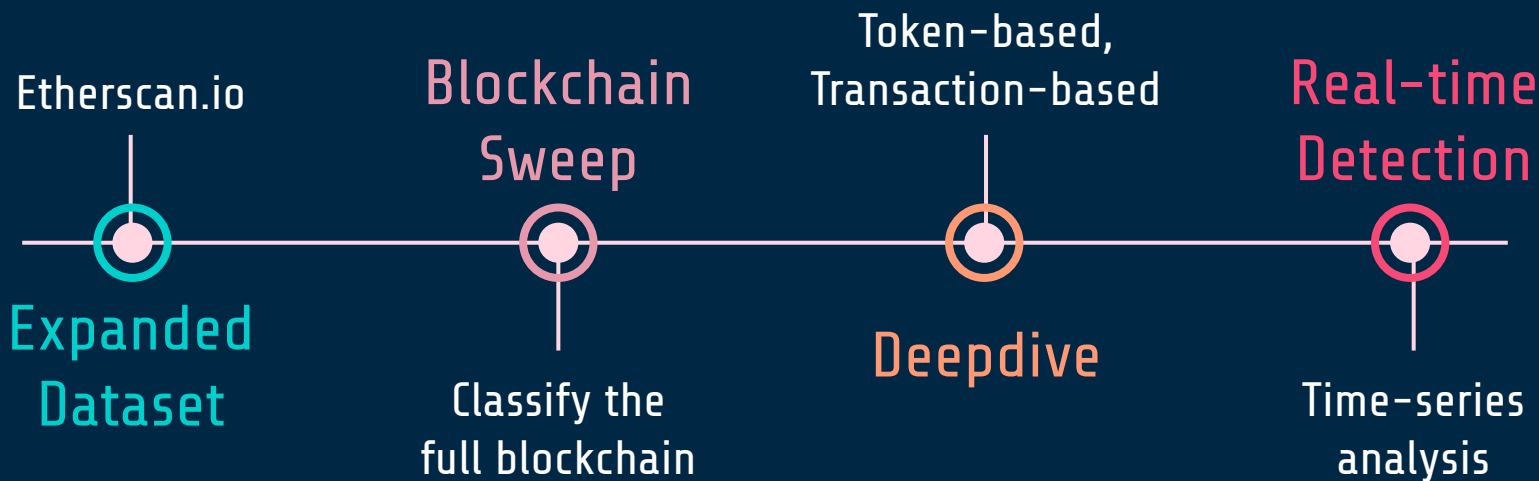
Latest 12 from a total of 12 transactions

Txn Hash	Method	Block	Age	From	To	Value
0x2ef50656ffc0c96015...	Transfer	5744849	1240 days 3 hrs ago	Fake_Phishing1269	OUT 0x685e0d0796ce8ad08...	2.0091
0xc27c87bcc765d84d6...	Transfer	5744819	1240 days 3 hrs ago	0x680abdfce950f4401e...	IN Fake_Phishing1269	2.0091

WHAT DOES THE MODEL LOOK AT?



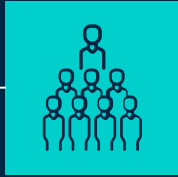
FUTURE WORK



Q&A

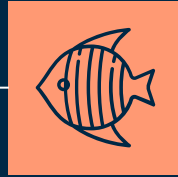
The background is a dark blue gradient. It features an abstract pattern of thin white vertical lines and small squares in various colors (pink, orange, teal, and light blue). The squares are scattered across the page, some solid and some outlined, creating a modern, minimalist aesthetic.

MAIN TYPES OF FRAUDS



Ponzi

Like pyramid scheme
Existing investors are paid
by later-joining investors



Phishing

Electronic identity theft
Deceptive technique to
extract sensitive data (2FA,
password) from victims

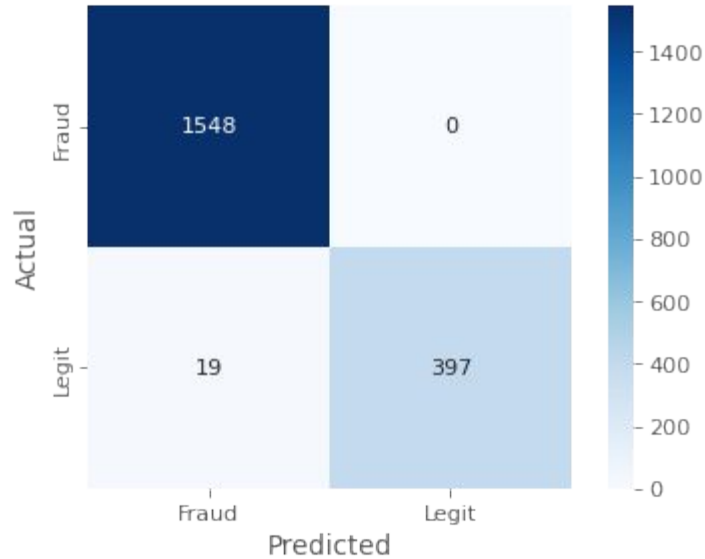


Honeypot

A trap in disguise
Smart contracts which
accept deposits but do
not withdraw

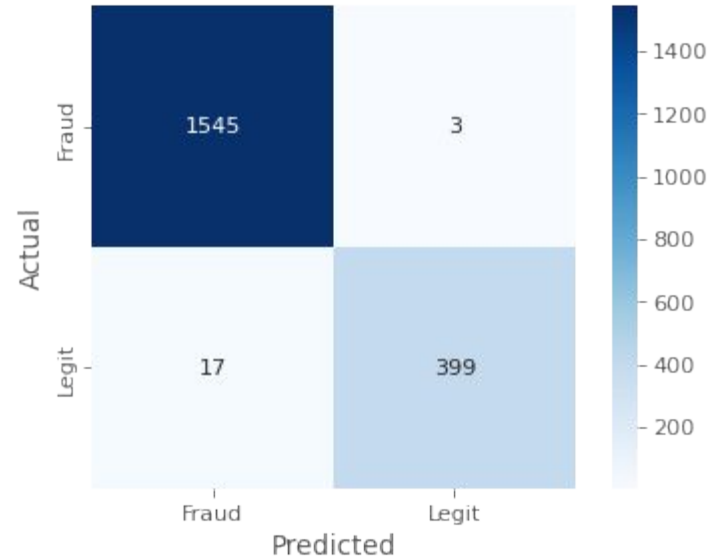
APPENDIX

RandomForest confusion matrix



Threshold	0.64
Precision	1.00
Recall	0.95
F-Beta	0.97

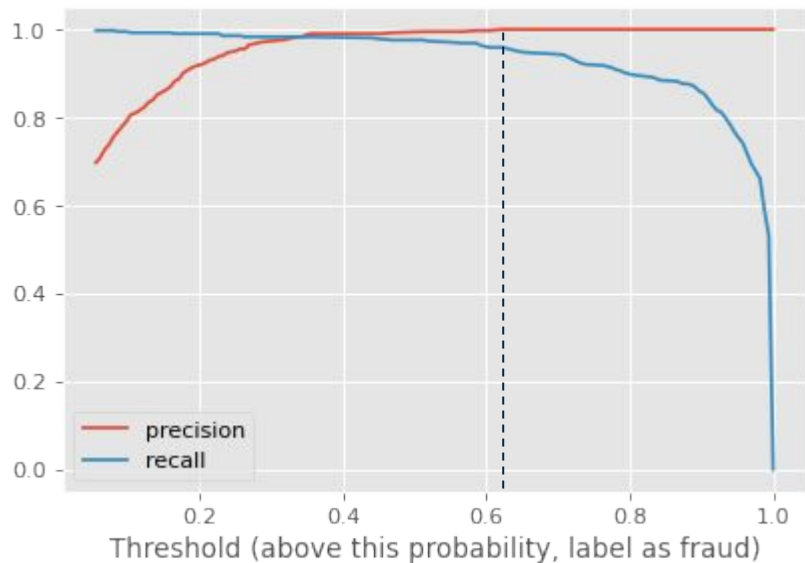
Extra Tree confusion matrix



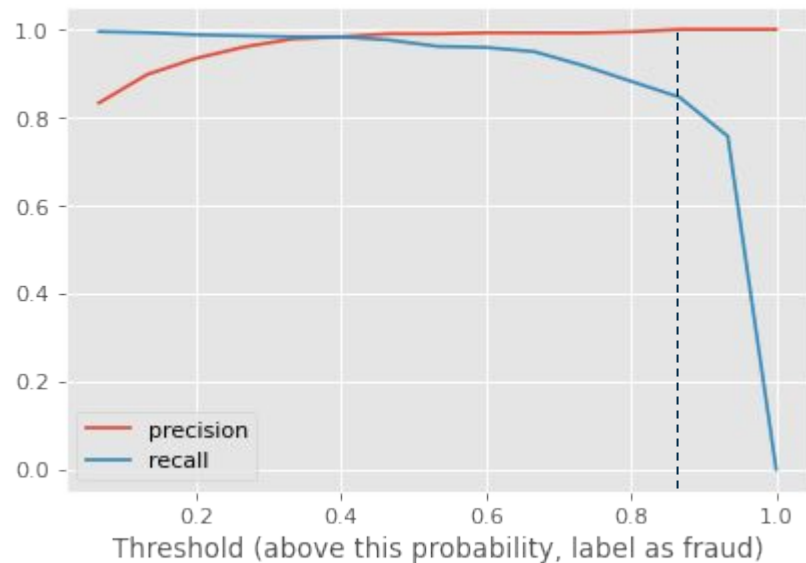
Threshold	0.64
Precision	0.99
Recall	0.96
F-Beta	0.97

APPENDIX

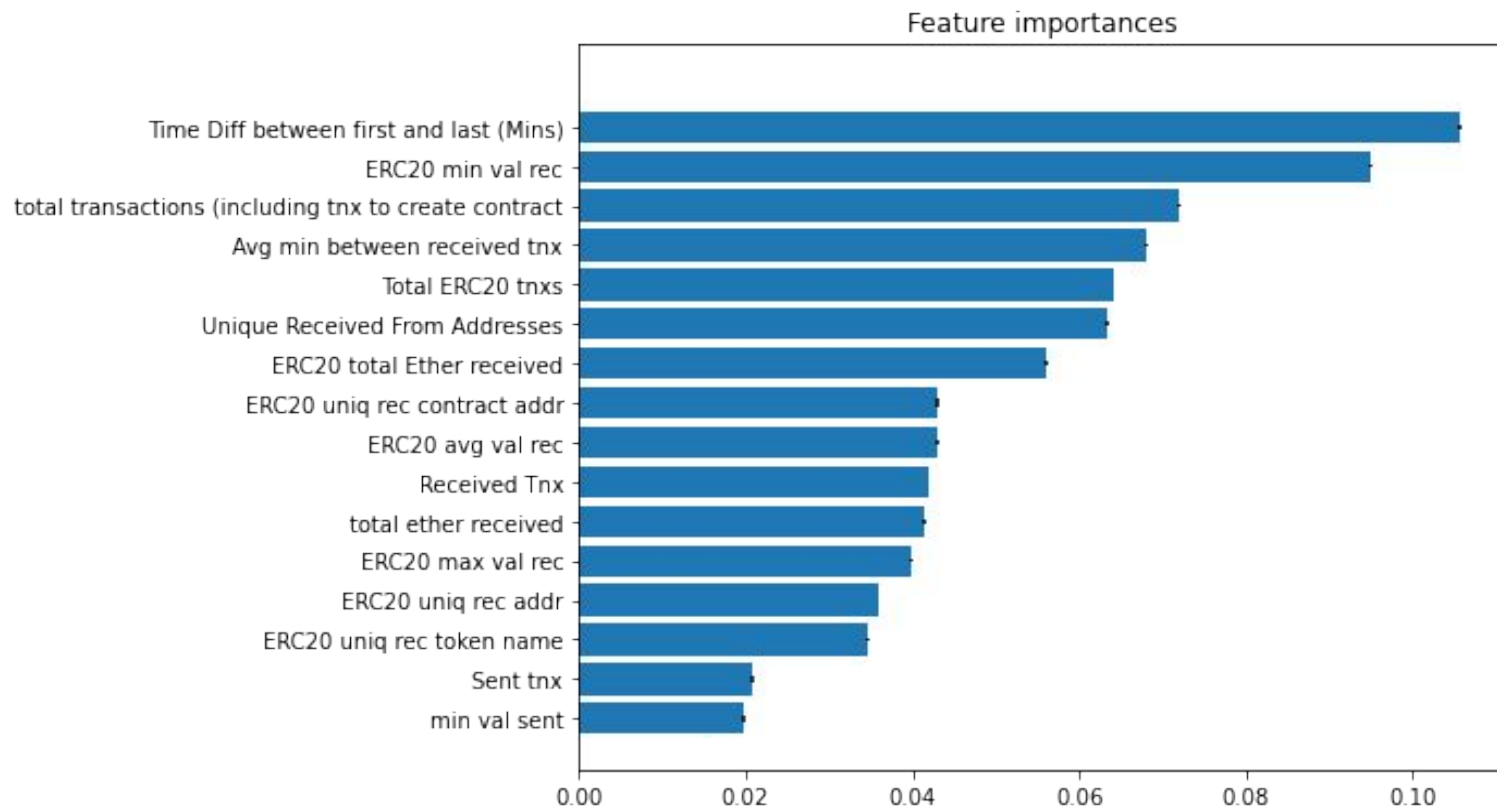
Precision and Recall Curves for RandomForest



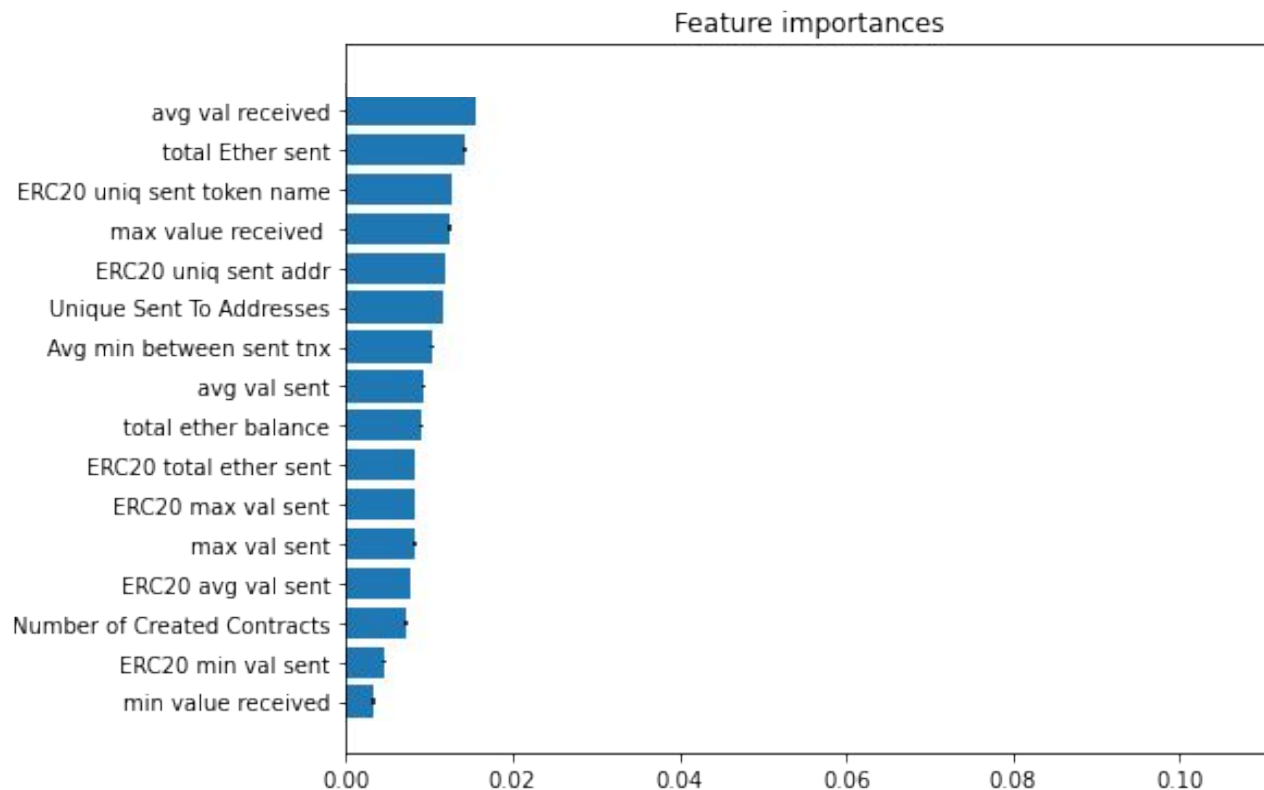
Precision and Recall Curves for Extra Trees



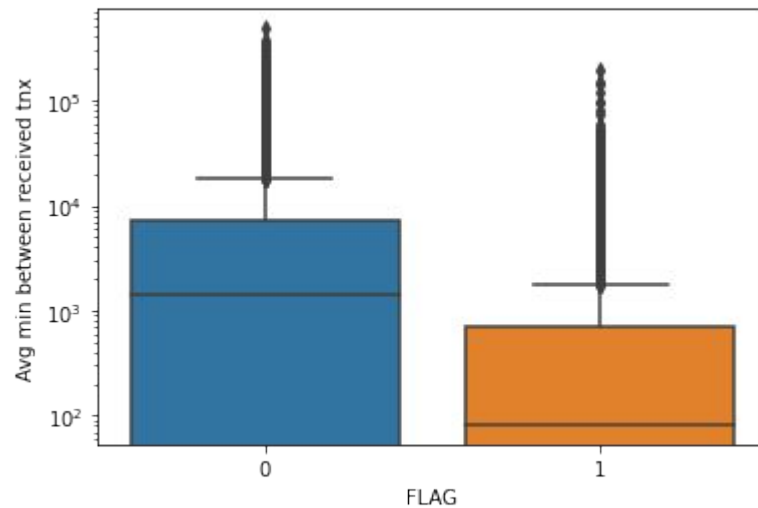
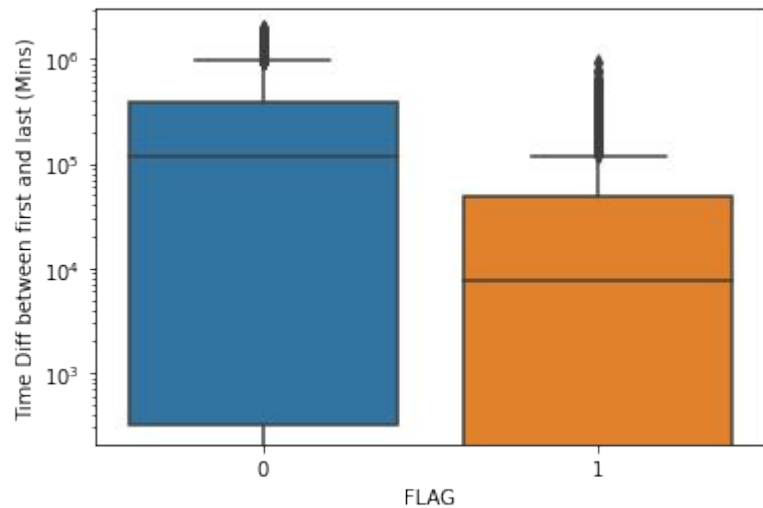
APPENDIX



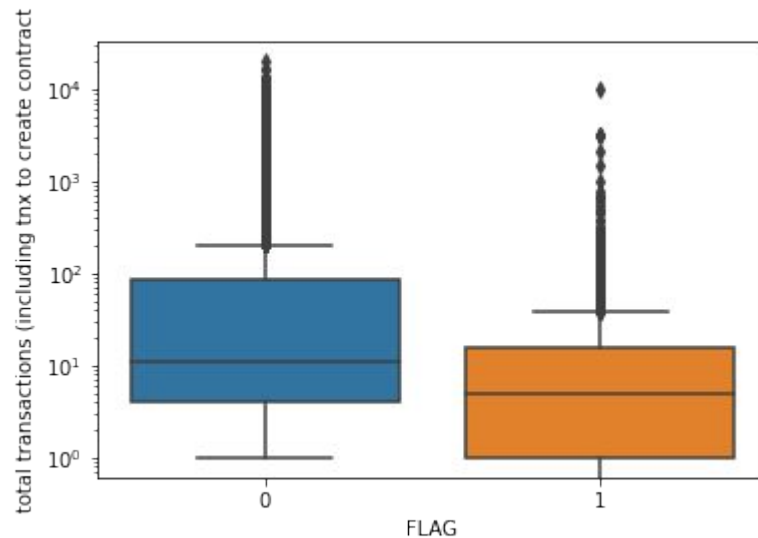
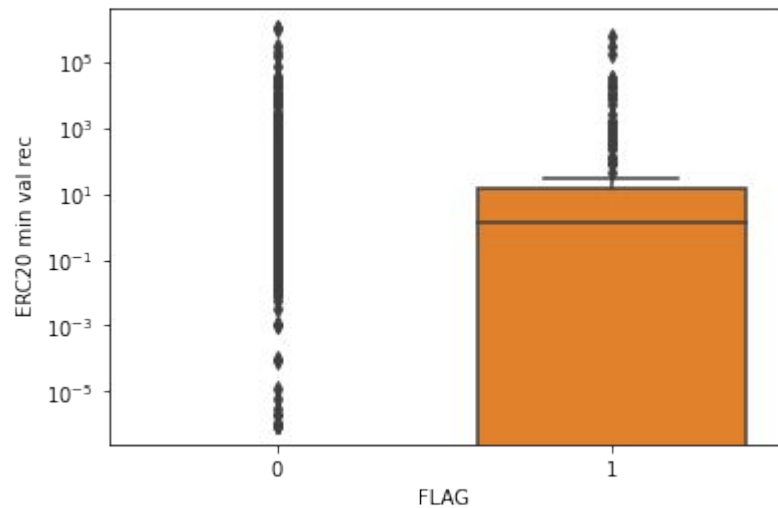
APPENDIX



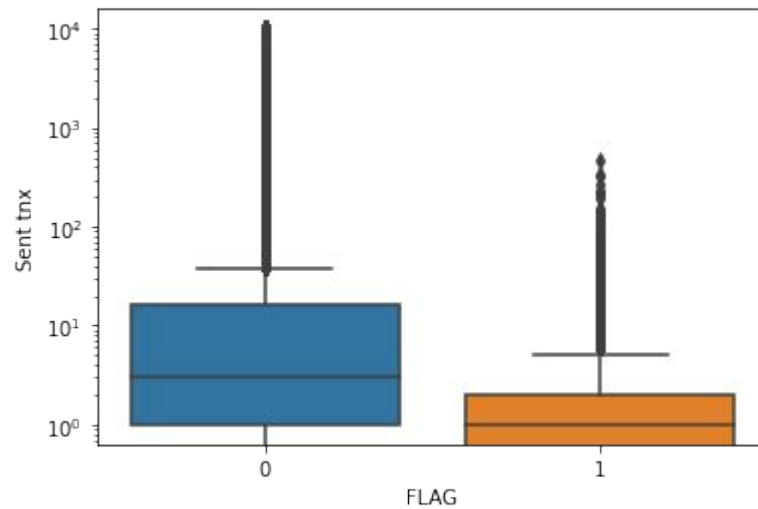
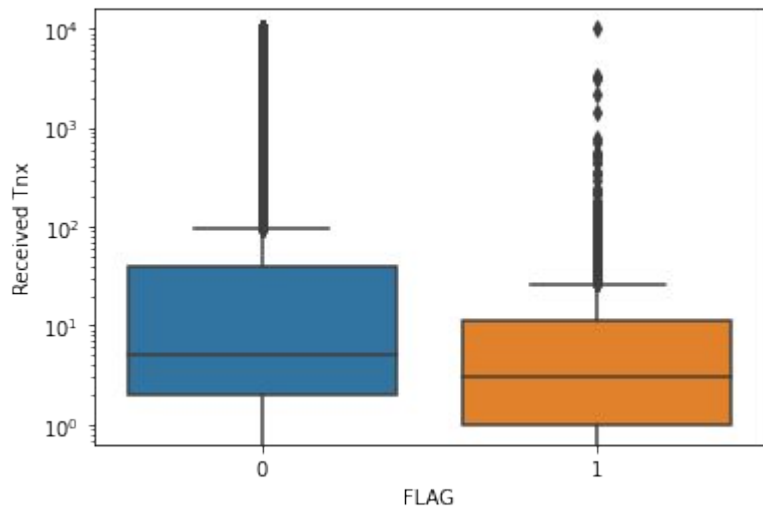
APPENDIX



APPENDIX



APPENDIX



APPENDIX

