

TRAIX

**QUICK SMART CONTRACT
VULNERABILITY SCANNING**



Rug Pull, Squid Game Crypto Developer Mode Takes Away Rp 48 M

By Fahmi Ahmad Burhan
November 4, 2021 14:00



The price of the cryptocurrency Squid Game had shot up 131,800%, suddenly falling to no price or US \$ 0. The fall in price due to the theft of cryptocurrency funds by developers is called a 'rug pull' or carpet pull scheme.

Gizmodo reported that cryptocurrency developer Squid Game brought away investor money worth US \$ 3.36 million or Rp 48.1 billion. The rug pull mode occurred on Monday (1/11) which made the liquidity pool for Squid Game cryptocurrency on the exchange then disappear in an instant.

Traix has a major concern namely that security vulnerabilities in smart contracts or blockchain infrastructure can lead to serious consequences, such as loss of crypto assets, privacy violations, and significant reputational damage.

CNN BUSINESS Markets Tech Media Calculators Videos

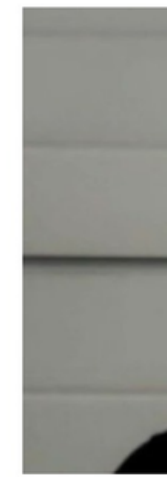
Markets →
 DOW 32,960.26 0.13% ↓
 S&P 500 4,236.62 0.17% ↑
 NASDAQ 13,146.27 0.66% ↑

Fear & Greed Index →
 Extreme Fear is driving the US market

Latest Market News →
 Why you should care about the global
 Trump gets kicked off Forbes 400 list
 Sam Bankman-Fried is about to meet

Hackers steal over \$600 million from video game Axie Infinity's Ronin network

By Jennifer Korn
 Updated 6:35 PM EDT, Tue March 29, 2022



CNBC Indonesia > Tech > Tech News

Turkish Crypto Boss Reportedly Missing, Brings Customer Money Rp 29 T

TECH- Novina Putri Bestari, CNBC Indonesia
 April 23, 2021 12:09 PM



SoIPAD
 @FinanceSolpad · Follow

Luna Yield, the latest IDO on our Launchpad, seems to have some problems. The Luna Yield Team took down their website and all other social media. They also withdraw all liquidity. SoIPAD still can't reach Luna Yield Team to figure out what happened.

6:35 AM · Aug 20, 2021

200 Reply Share this post

Read 103 replies

Decoding Deus DAO \$6.5 Million Exploit | QuillAudits

QuillAudits - Web3 Security · Follow
 4 min read · May 12

45



Decoding Deus DAO's \$6.5 Million Exploit

the Deus DAO Protocol was exploited on the Arbitrum, 1 BNB chains due to a smart contract vulnerability. \$6.5 million was stolen by the hackers in this exploit.

Decoding Ovix Protocol's \$2 Million Exploit | QuillAudits

QuillAudits - Web3 Security · Follow
 5 min read · May 8

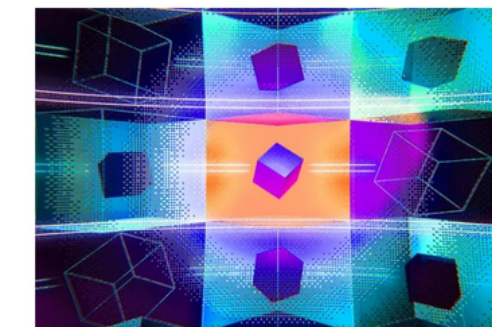
51



Summary:
 On April 28th, the Ovix Protocol on 1 due to a flawed price calculation, w approximately \$2 million from mult

TECH / SECURITY / POLICY

Wormhole cryptocurrency platform hacked for \$325 million after error on GitHub



A security fl seemingly not application be

By Corin Felle
 Feb 4, 2022, 12:43 AM GMT-7

Illustration by Alex Castro / The Verge

On Wednesday, the decentralized finance (DeFi) platform Wormhole became the victim of the largest cryptocurrency theft this year — and among the top five largest crypto hacks of all time — when an attacker exploited a security flaw to make off with close to \$325 million.

The attack seems to have resulted from a recent update to the project's GitHub repository, which revealed a fix to a bug that had not yet been deployed to the project itself.

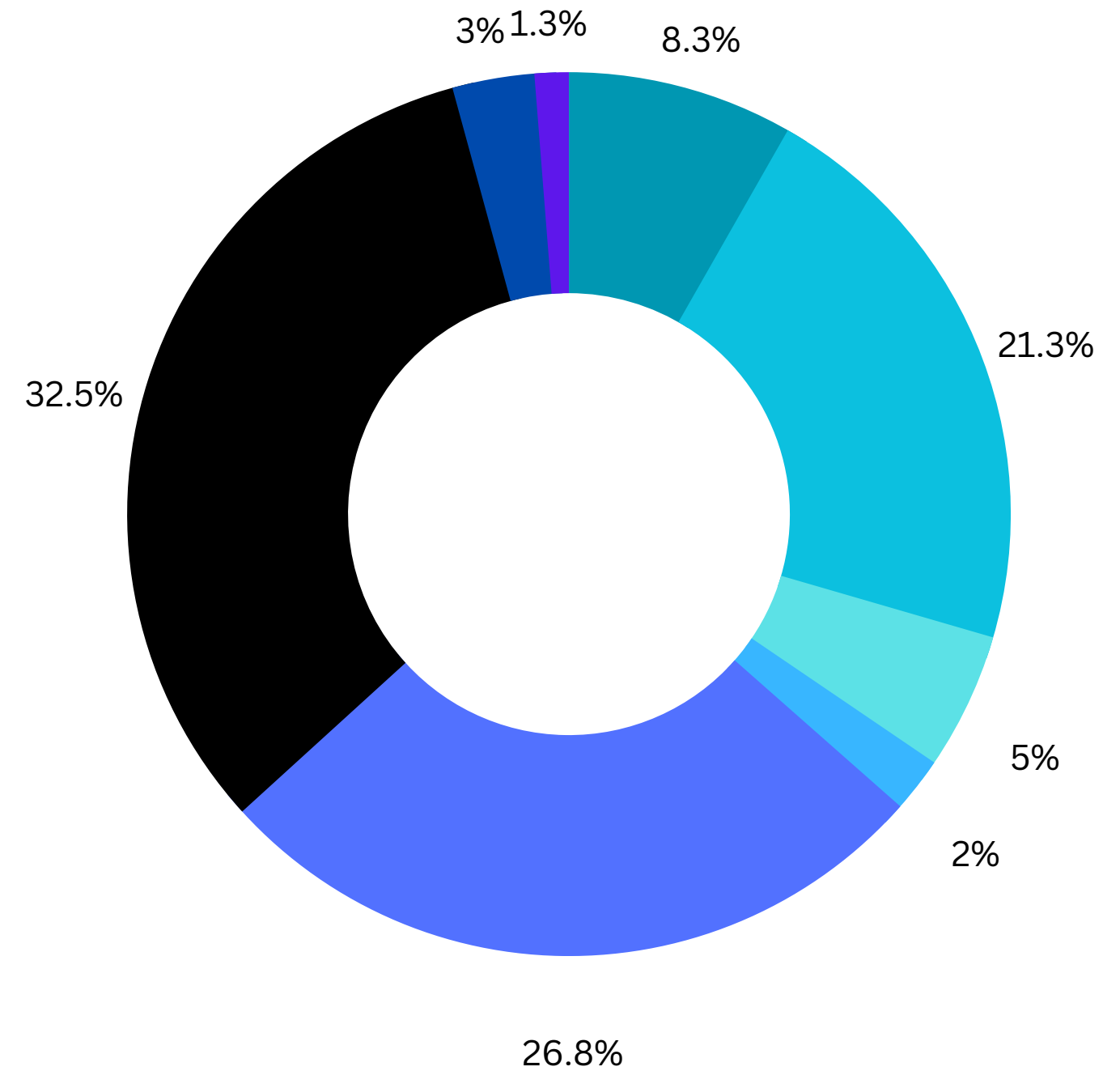
The attack took place on February 2nd and was noticed when a post from the Wormhole Twitter account announced that the network was being taken "down for maintenance" while a potential exploit was investigated. A later post from Wormhole confirmed the hack and the amount stolen.

There are several cases of financial and reputation damage due to unaudited smart contracts

Where a hacker demonstrated it the danger of unaudited smart contracts causing losses of up to

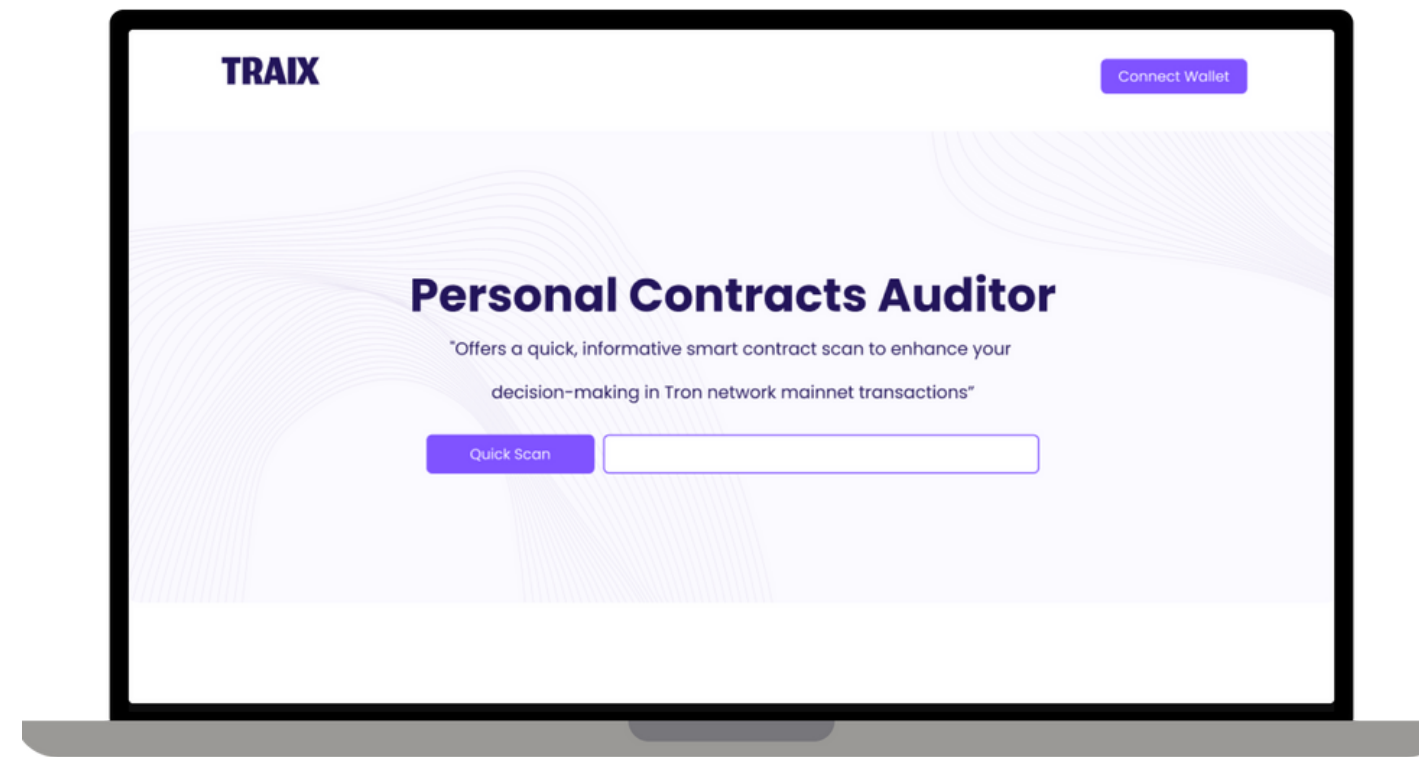
\$9.08B

The total amount of money hacked since 2020!



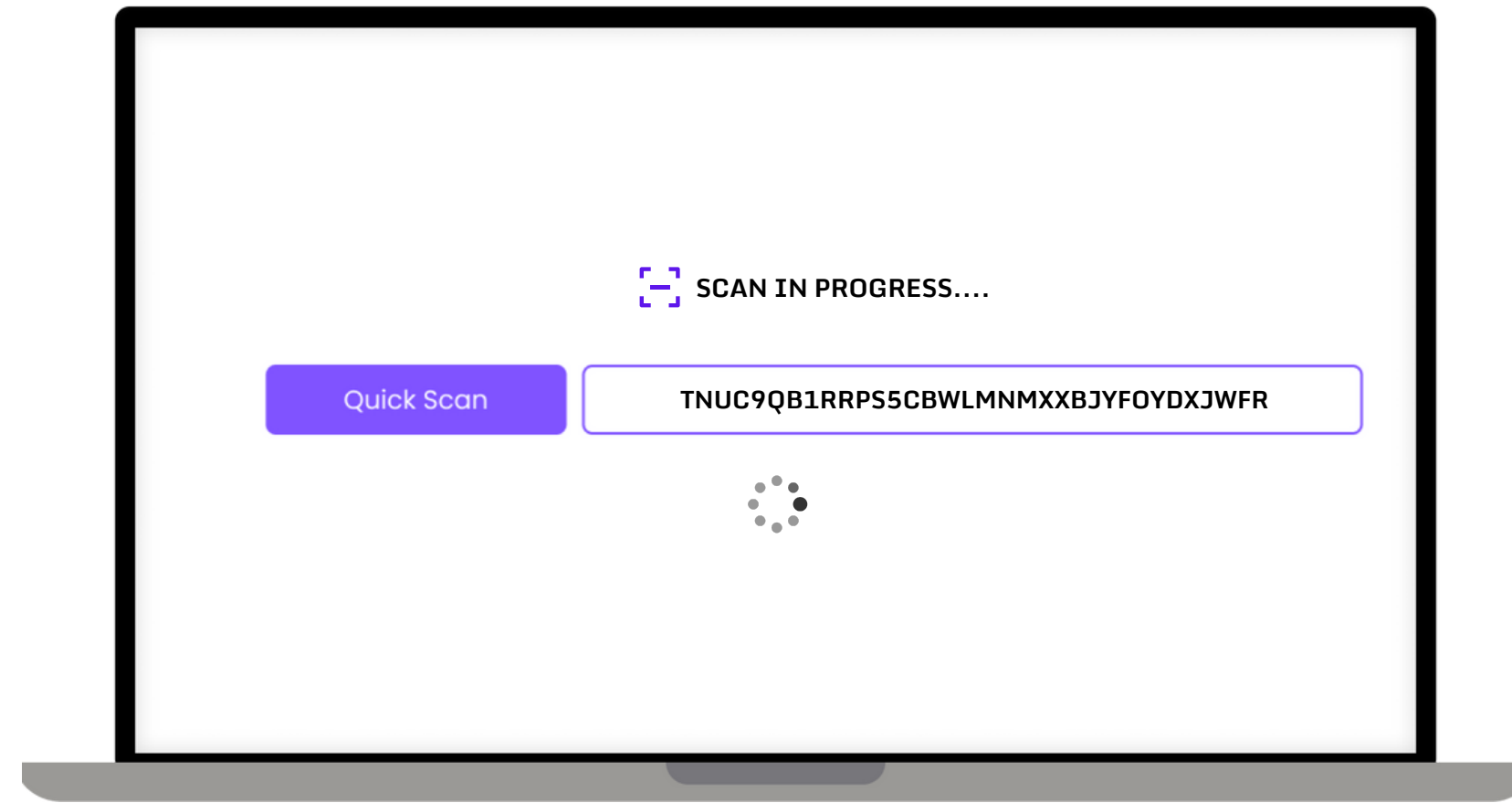
- Off-Chain Attacks
- Flash Loan Attacks
- Smart Contracts Vulnerability
- Price/Oracle Manipulation
- Private Key Compromised
- Social Account Takeover
- Exit Scam
- Other Vulnerabilities

This hack may be intimidating and drive them away from studying for fear of what will happen the loss itself or because they do not understand the reasons hacking.



Traix allows someone to paste the contract of the token they want to invest in there into the text box and get a list of contract-based vulnerabilities discovered through parsing and pattern searching. < >



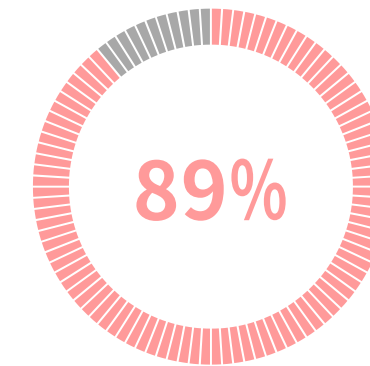
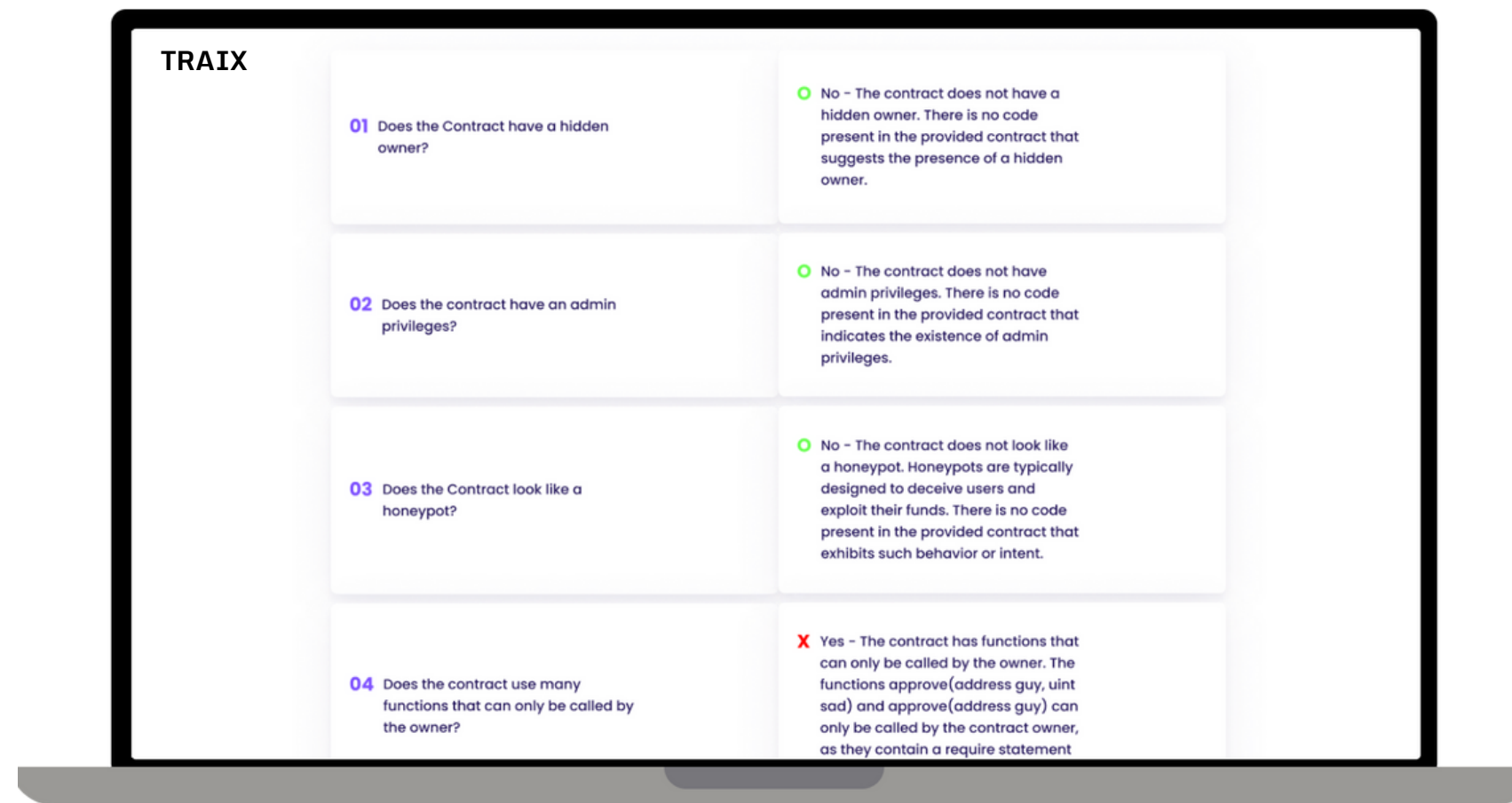


Provides users with fast and simple interface was the rationale behind the motivation.

Traix will be a tool used as the first barrier for scanning vulnerable smart contract code.

TRAIK

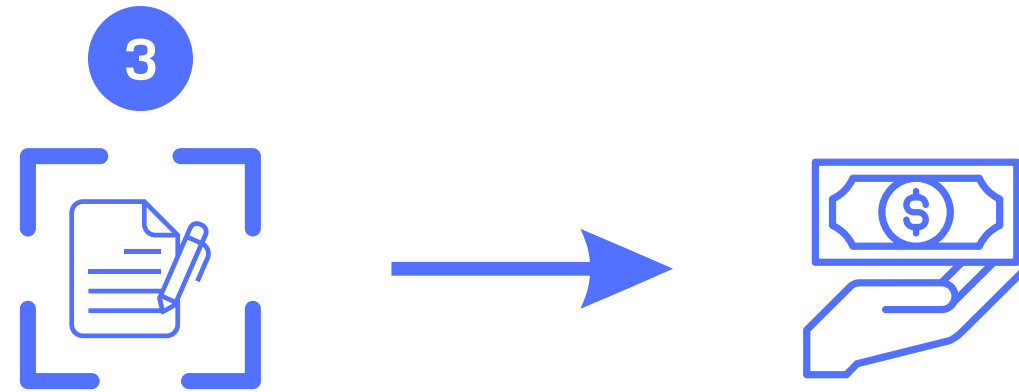
After Traix performs a thorough scan of the smart contract, it provides comprehensive results that have been analyzed through machine learning and artificial intelligence (AI) methodologies. This advanced approach ensures comprehensive vulnerabilities and provides actionable insights to improve the security of scanned smart contracts.



Smartcontract
Possible
High Risk

Business Model

We implement a freemium business model, where users can access our platform for free with a scan limit of up to three smart contracts.




Additionally, as our product progresses through further milestones, we will introduce pricing for each feature, catering to the needs of crypto enthusiasts, junior researchers, and senior researchers. This tiered pricing approach will provide users with the flexibility to choose the features and capabilities that best suit their requirements as they engage with our platform.

PRICING SIMULATION


BEGINNER


Junior Developer or
Associate Security
Researcher or NFT
Enthusiast

\$ 149.99
/
MONTHLY


No of Scans
 20 Scans

Vulnerability Detectors coverage
 All Detectors

Private Github
 Private Github

Github Actions
 Github Actions


Generate and Publish report
 Publish Reports


Private API Access
 API Access


INTERMEDIATE


Senior Developer or Senior
Security Research or
Experienced NFT Buyer/
Trader or Small Teams

\$ 249.99
/
MONTHLY

No of Scans
 40 Scans

Vulnerability Detectors coverage
 All Detectors

Private Github
 Private Github

Github Actions
 Github Actions


Generate and Publish report
 Publish Reports

Private API Access
 API Access


PRO


Development SME or
Security Research SME
or NFT SME or Medium
Size Teams

\$ 299.99
/
MONTHLY


No of Scans
 80 Scans

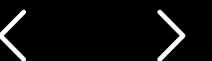
Vulnerability Detectors coverage
 All Detectors

Private Github
 Private Github

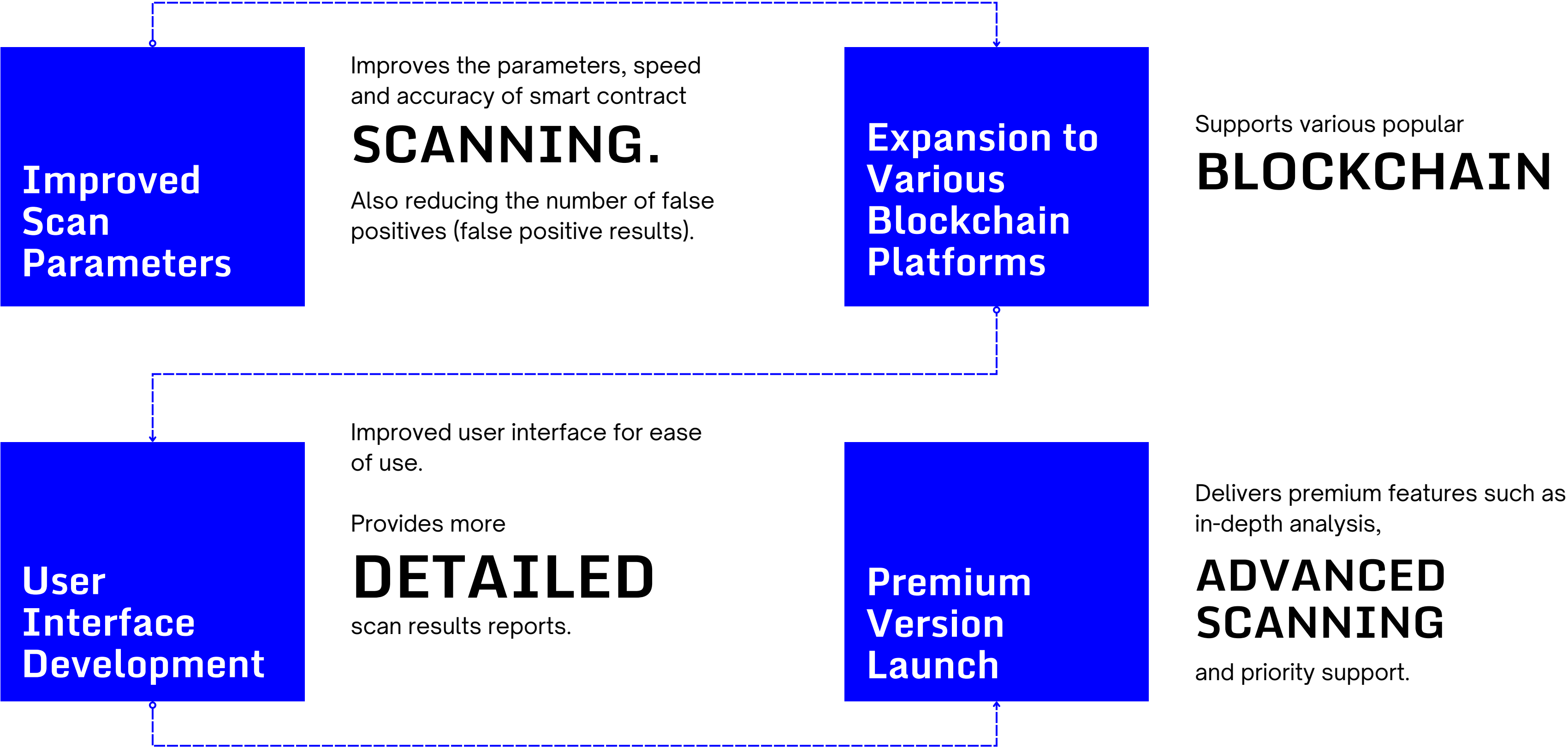
Github Actions
 Github Actions

Generate and Publish report
 Publish Reports

Private API Access
 API Access

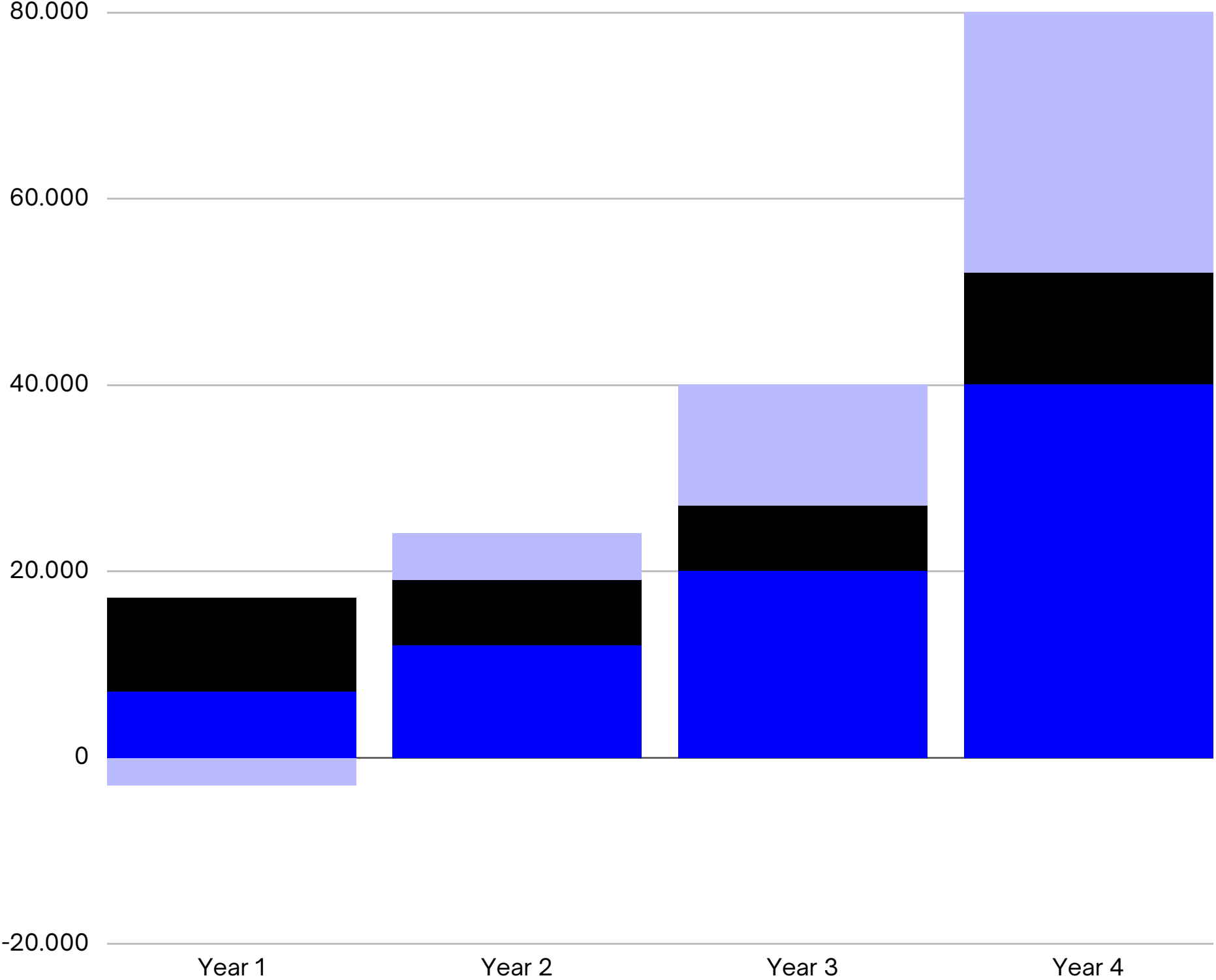
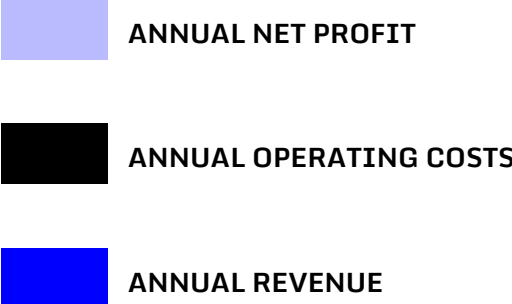


MILESTONES



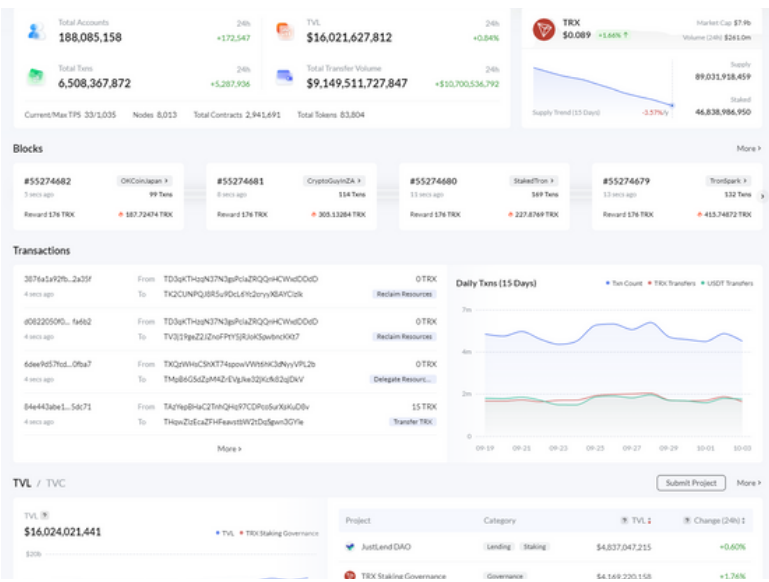
FINANCIAL PROJECTIONS

ANNUAL REPORT



Report figures are in \$

TECHNICAL PARAMETERS



MACHINE LEARNING AND ARTIFICIAL INTELLIGENCE

PARAMETERS

Address, Reputation on Tron scan, Average minimum between sent transactions, average times, and various transaction statistics such as sent transactions, received transactions, created contract transactions, and unique addresses involved. Additionally, it covers Trx value metrics like minimum, maximum, and average values. The data also includes insights into TRC20 token transactions, such as the total number and value received, sent, and sent to contracts. Other details encompass unique addresses involved in TRC20 token transactions, average time intervals and value statistics. Lastly, it provides insights into the most frequently transferred and the predominant token types.

Begin by gathering transaction data, encompassing the mentioned parameters such as addresses, transaction times, values involved, and TRC20 token types.

Preprocess the data, including handling missing values, converting transaction times into a usable format, and potentially computing additional statistics like averages and maximum values.

Normalize the data to bring all parameters to a consistent scale. This step aids KNN in calculating distances more effectively.

Not all of the mentioned parameters may be necessary. Choose the most relevant parameters for detecting suspicious or fraudulent transactions.

Divide the data into two segments, training data (for model training) and testing data (for model evaluation). take a small portion of the data as testing data and use the rest for training.

Train a KNN model using the training data. The model will learn to identify patterns within the training data.

Employ the testing data to evaluate the KNN model. The model will compute distances between the testing data and the previously learned training data. Subsequently, it will classify whether transactions are fraudulent or not.

Assess the model's performance using metrics like accuracy, precision, recall, or F1-score to ensure its accuracy.

If the model's performance falls short of expectations, experiment with different K values in KNN or adjust other parameters to enhance results.

Once the model is deemed adequate, deploy it in production to scan and automatically detect suspicious transactions.

Furthermore, you can establish an automated workflow to periodically scan transactions or as needed. This will efficiently aid in identifying suspicious transactions within the blockchain ecosystem.

PROVIDE ANSWERS BY QUICK SCAN

Traix also uses the ChatGPT API to get answers from smart contract values to check the following parameters:

1. Does the Contract have a hidden owner?
2. Does the contract have an admin privileges?
3. Does the Contract look like a honeypot?
4. Does the Contract Owner can change the balance token?
5. Does the contract is proxy contract?
6. Does the Contract have a whitelist?
7. Does the Contract have a blacklist?
8. Does the slippage can be modified on contract?
9. Does the contract can take back ownership?
10. Does the contract have a trading-cool-down mechanism?
11. Does the contract can mint new tokens?
12. Does the contract can burn the tokens?
13. Does the contract upgradeable?
14. Does the contract can be paused?
15. Does the contract have a cooldown feature?
16. Does the contract can establish or update Fees?
17. Does the contract was hardcoding addresses?
18. Does the contract use many functions that can only be called by the owner?