SMART INDIA HACKATHON 2024

TITLE PAGE

- **Problem Statement ID -** SIH1675
- **Problem Statement Title -** Software solution to identify the end receiver of a cryptocurrency transaction
- **Theme -** Blockchain & Cybersecurity
- **PS Category -** Software
- **Team ID -**
- **Team Name (Registered on portal)**

Callisto Labs

IDEA APPROACH/DETAILS

SMART INDIA HACKATHON 2024

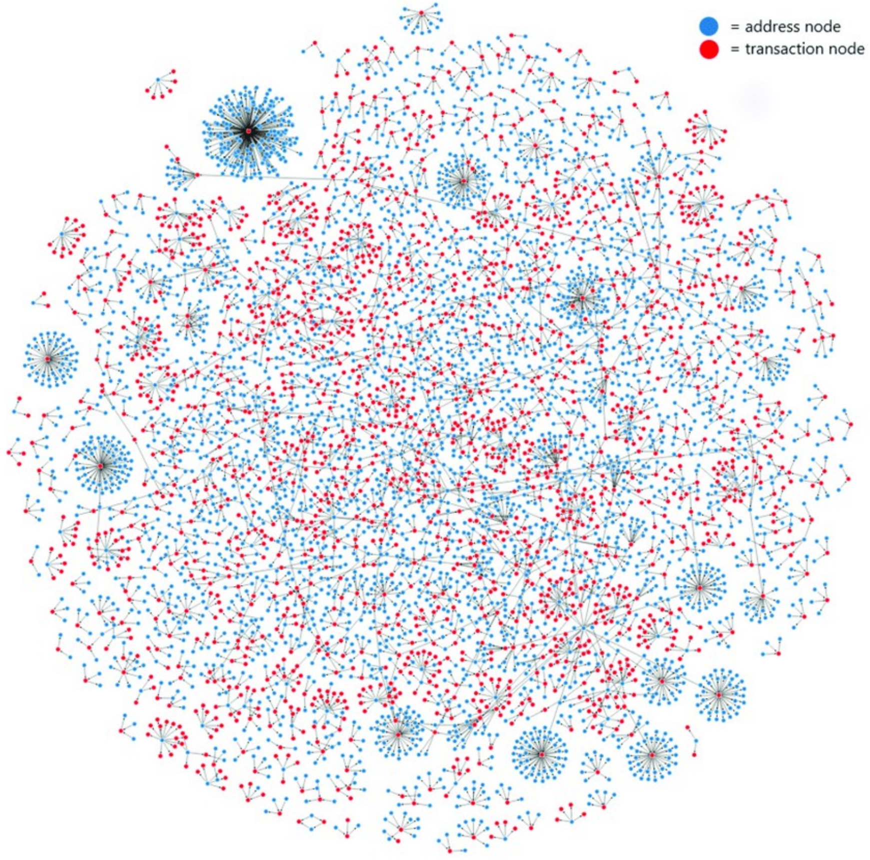
❖ Using Graph Neural Networks to trace cryptocurrency transactions

- Crypto networks merely function as a distributed ledger, hence the transactions between various addresses can be represented as a graph, with addresses as nodes and transactions as edges

- Using Graph Neural Networks, we can gain insightful information from these graphs to identify fraudulent/suspicious transactions

- Many threat actors also use services such as coin mixers to further hide their activities. We can experiment with novel approaches to de-anonymize these mixers using techniques such as timestamp analysis, merkle root changes (for zkSNARK mixers such as Tornado.cash) and heuristic based clustering to tackle traditional mixers

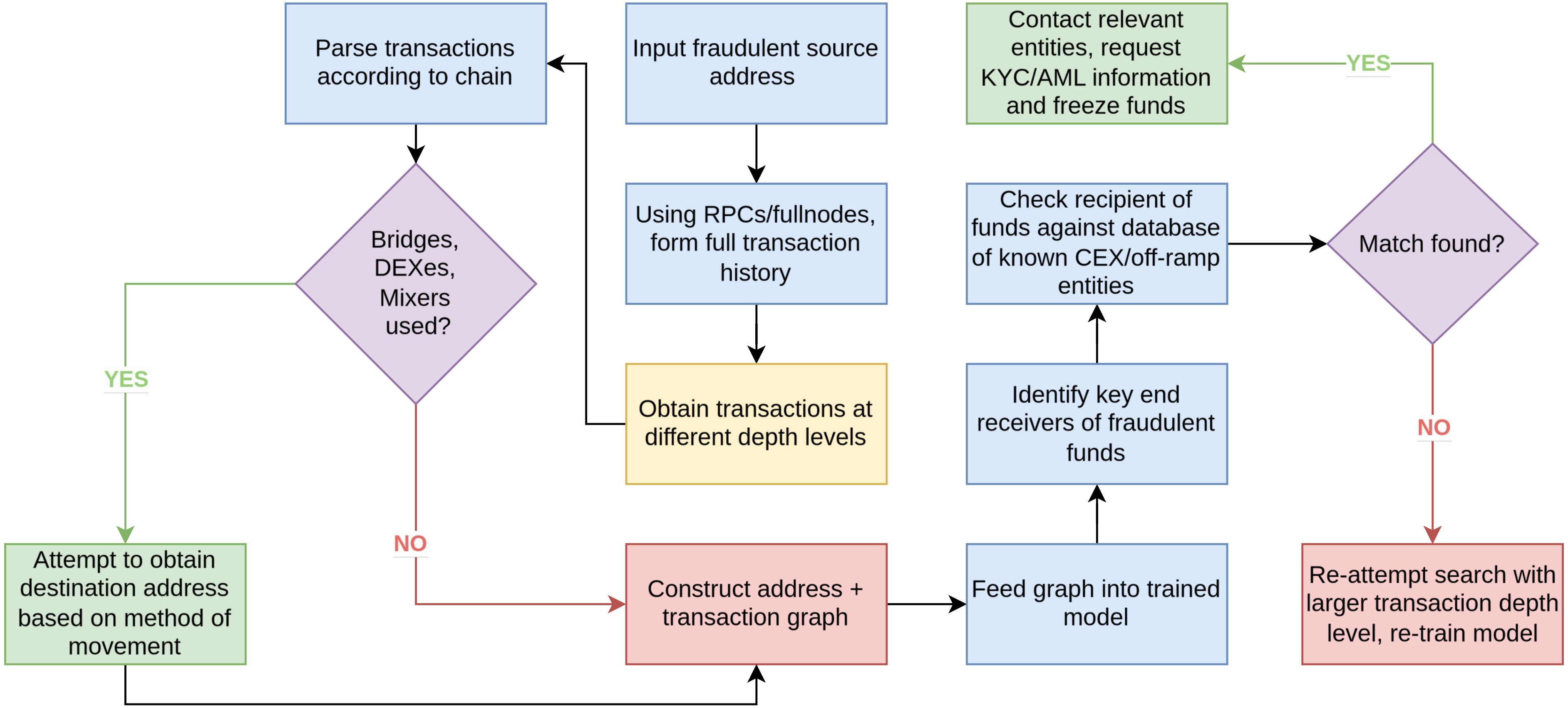
- The innovation and uniqueness comes from the fact that this is the first time multi-chain analysis has been done using graph neural networks, especially targetting services designed to circumvent tracking such as mixers, exchanges and bridges



Example of an address graph

TECHNICAL APPROACH

- **Languages/frameworks required (MVP):** Typescript, Python, Pytorch, Solidity (for EVM chains), NodeJS, RPC/full nodes for implemented networks



Parse transactions according to chain
Input fraudulent source address
Contact relevant entities, request KYC/AML information and freeze funds
YES
Bridges, DEXes, Mixers used?
Using RPCs/fullnodes, form full transaction history
Check recipient of funds against database of known CEX/off-ramp entities
Match found?
YES
Obtain transactions at different depth levels
Identify key end receivers of fraudulent funds
NO
NO
Attempt to obtain destination address based on method of movement
Construct address + transaction graph
Feed graph into trained model
Re-attempt search with larger transaction depth level, re-train model

FEASIBILITY AND VIABILITY

- **Feasibility:** The idea is feasible for public blockchains. It may be applied to addresses which are known to be associated to fraud (DeFi hacks, scams etc.) to find the true perpetrator

- **Challenges/Risks:** Requires compliance from CEX and large off-ramp entities. Great care needs to be taken to avoid false-positive detections

- **Overcoming risks:** Model will be trained with data of both innocent and suspicious addresses to ensure accurate detection. There needs to be proper compliance from central entities

Callisto Labs

IMPACT AND BENEFITS

SMART INDIA HACKATHON 2024

- Allows for de-anonymization of cryptonetworks, and better regulation of digital assets
- Reduces the likelihood of scams, hacks and other malicious activities and disincentivises threat actors.
- Creates a safer environment for DeFi projects and cryptocurrency innovations to thrive

RESEARCH AND REFERENCES

- Li, Zhiyuan & He, Enhan. (2023). Graph Neural Network-Based Bitcoin Transaction Tracking Model. IEEE Access
- Tan, Runnan, et al. "Graph neural network for ethereum fraud detection." 2021 IEEE international conference on big knowledge (ICBK). IEEE, 2021.
- Y. Zhang, J. Wang and J. Luo, "Heuristic-Based Address Clustering in Bitcoin," in IEEE Access, vol. 8, pp. 210582-210591, 2020
- A. A. Maksutov, M. S. Alexeev, N. O. Fedorova and D. A. Andreev, "Detection of Blockchain Transactions Used in Blockchain Mixer of Coin Join Type," 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Saint Petersburg and Moscow, Russia, 2019, pp. 274-277