# SMART INDIA HACKATHON 2024

SMART INDIA HACKATHON 2024

- **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-** 14289
- **Team Name –** TrackWallet.in

# Proposed Solution

**1. Wallet Address Tracking:** Input the suspicious wallet address into an **analysis portal** (react website) that provides insights into its **activity across all blockchains**, including **transactions and linked wallets**.

**2. Linked Wallet Detection:** Identify all wallet addresses that have transacted with the **suspicious wallet,** across any blockchain, for deeper investigation. From a **single wallet**, we can identify **N wallets to track**.

**3. ENS Domain and Nickname Search:** Check for any ENS domains or **nicknames associated** with **these linked wallets** to find potential identities. **(ens, web3 domains, debank, CivicID, BlockID, etc)**

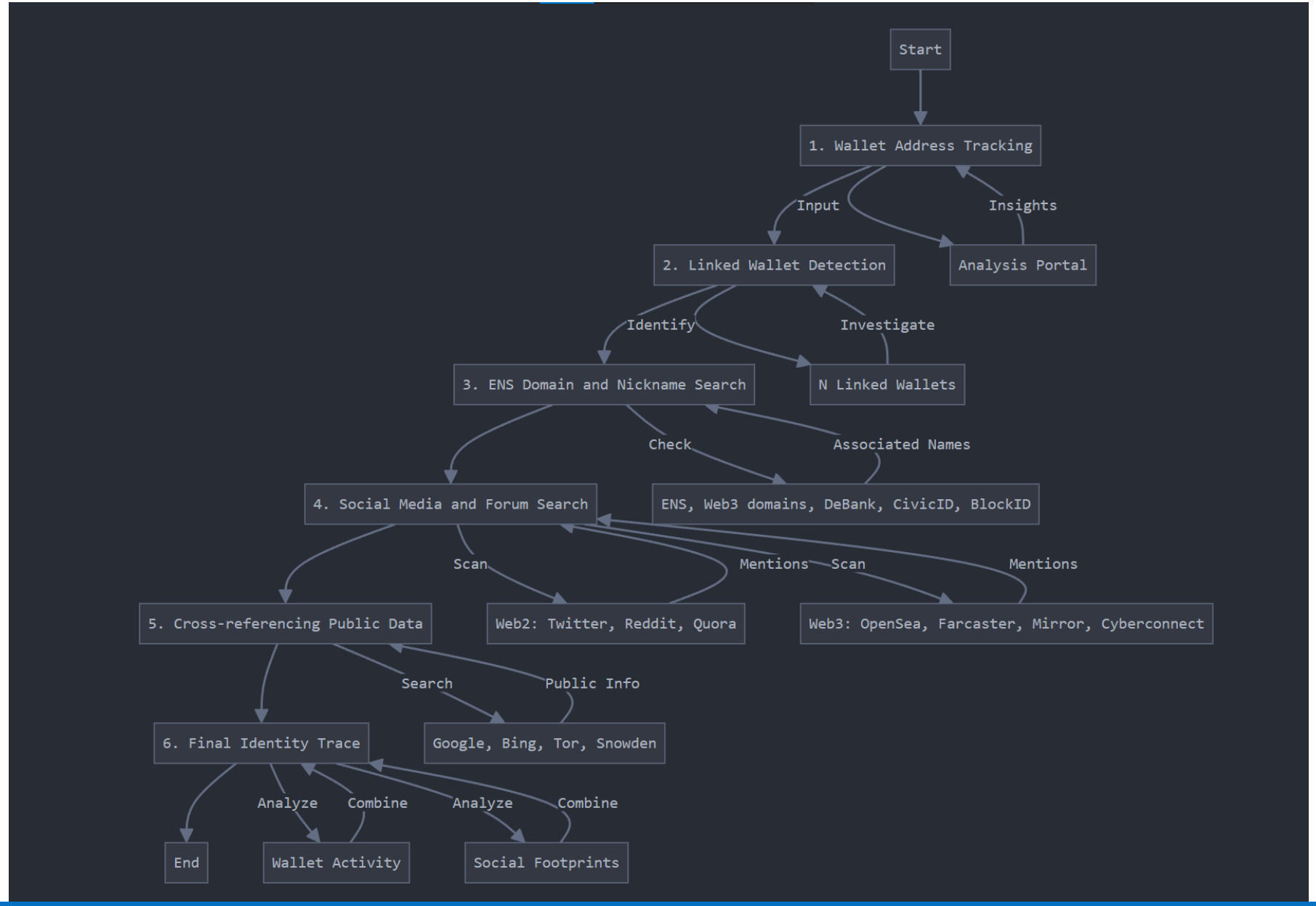
**4. Social Media and Forum Search:** Use a **tracker portal** (python web scrapper) to scan **Web2 (e.g., Twitter, Reddit, Quora)** and **Web3 (e.g., OpenSea, Farcaster, Mirror, Cyberconnect)** platforms, as well as **forums and blog posts, comment section, bio**, etc for **any mentions** of the wallet address or nickname.

**5. Cross-referencing Public Data:** Search engines **(Google, Bing, Tor, Showden etc.)** are utilized to find public information **linked to the wallet or nickname**, tracing back to potential **real-world users.**

**6. Final Identity Trace:** By **analyzing wallet activity** and associated users' **social footprints**, identify the **real person** behind the suspicious **cryptocurrency transactions**.

# TECHNICAL APPROACH






**Analysis Portal:**
**Framework:** React.js
**Language:** Typescript
**Modules:** Axios

**Tracker Portal:**
**Framework:** Flask
**Language:** Python
**Module:** BeatifulSoup4

# FEASIBILITY AND VIABILITY



**Feasibility Analysis:**

- The idea is technically feasible with the **integration** of blockchain **analysis tools** and Web2/Web3 data scraping platforms. It relies on existing technologies like **ENS, social media tracking**, and public data search engines.

- Wallet addresses **may not always link to identifiable usernames**, and **false positives** could occur in linking real-world identities to blockchain addresses.

- Tracking and identifying users through their **social activity raises privacy** and ethical considerations, especially in regions with strict data protection laws.

- **Handling large volumes** of blockchain transactions and social media data efficiently could be resource-intensive, **requiring robust infrastructure**.

**Overcoming Challenges:**

- Improve **data filtering** methods to **minimize false positives**.
- Focus on **publicly available information** to avoid privacy violations.
- Build **scalable solutions** using **cloud-based infrastructure**.

# IMPACT AND BENEFITS



**1. Enhanced Security:** The solution can help law enforcement and compliance teams **identify illicit activities**, improving the **overall security of the cryptocurrency ecosystem** and deterring fraudulent behavior.

**2. Informed Decision-Making:** By providing insights into wallet activities and **potential user identities**, businesses and individuals can make **better-informed** decisions **regarding partnerships and transactions.**

**3. Improved Compliance: Financial institutions and crypto exchanges** can enhance their compliance with regulations, **reducing the risk of penalties** and fostering a safer environment for legitimate users.

**4. Increased Accountability:** Linking wallet addresses to **real identities promotes** accountability within the cryptocurrency space, encouraging **responsible use and discouraging bad actors**.

**5. Economic Growth:** By fostering trust in cryptocurrency transactions, the solution can stimulate **economic activities within the blockchain ecosystem,** leading **to increased adoption** and investment in innovative projects.

# RESEARCH AND REFERENCES



**1. Chainalysis Reports**
Chainalysis. (n.d.). Blockchain analysis, investigations, and compliance solutions. Retrieved from Chainalysis

**2. Elliptic Research**
Elliptic. (n.d.). Blockchain analytics for crypto compliance and investigations. Retrieved from Elliptic

**3. Tracing Bitcoin Transactions**
Meiklejohn, S., Pomarole, M., Lefranc, A., & Savage, S. (2013). Tracing Bitcoin Transactions. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (pp. 255-266). ACM. Retrieved from arXiv

**4. The Use of Blockchain Technology in the Fight Against Money Laundering**
Zohar, A. (2019). The Use of Blockchain Technology in the Fight Against Money Laundering. Retrieved from ResearchGate