(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :14/08/2023

(21) Application No.202311054610 A
(43) Publication Date : 08/09/2023

(54) Title of the invention : SYSTEM TO DETECT AND RESPOND TO VIRTUAL CURRENCY THEFT AND METHOD THEREOF

(51) International classification	:G06Q0020400000, G06N0020000000, G06N0003040000, G06N0003080000, G06Q0020060000
(86) International Application No Filing Date	:NA :NA
(87) International Publication No	: NA
(61) Patent of Addition to Application Number Filing Date	:NA :NA
(62) Divisional to Application Number Filing Date	:NA :NA

(71)**Name of Applicant :**
1)Chitkara University
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------
2)Bluest Mettle Solutions Private Limited
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)MISHRA, Rahul
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ---------- ----------
2)PANDEY, Sakshi
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ---------- ----------
3)MANTRI, Archana
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ---------- ----------

(57) Abstract :
The present invention discloses a system (100) and method (200) for detecting and responding to virtual currency theft using machine learning algorithms. The system (100) includes a processor (102) configured to collect transaction data from various sources, including wallets, virtual currency exchanges, and third-party service providers, preprocess the collected transaction data to ensure data quality and eliminate noise, apply one or more techniques, such as machine learning algorithms, neural networks, and decision trees, to identify patterns indicative of fraudulent activity. Upon recognizing one or more fraud patterns, take appropriate actions, including blocking suspicious transactions, suspending accounts associated with fraudulent activities, and notifying relevant entities about the fraudulent activity. The system may further include a feedback mechanism to receive input from entities regarding the identified fraud patterns and actions taken, enhancing the system's accuracy over time.

No. of Pages : 21 No. of Claims : 10