(54) Title of the invention : A SYSTEM AND A METHOD FOR VERIFYING KYC USING DIGITAL LEDGER

(51) International classification	:H04L0009320000, H04L0009060000, G06F0021640000, G06Q0030000000, H04L0067104000
(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)MANTRI, Archana
Address of Applicant :Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala ----------- -----------
  2)MISHRA, Rahul
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ----------- -----------
  3)SINGH, Dhiraj
Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune ----------- -----------

(57) Abstract :
The present disclosure relates to a system (100) and method for verifying know your customer (KYC) using digital ledger comprising one or more blockchain nodes (106) and a processing unit (108). The one or more blockchain nodes (106) form a blockchain network (120). The processing unit (108) is communicatively coupled to the one or more blockchain nodes (106) and a hashing module (112) configured in the node (106). The processing unit (108) has a memory (110) for storing instructions. The processing unit (108) generates one or more hash data using the hashing module (112) when input data is received from one or more administrative users (104). The hashed data is stored in decentralized network (120). One or more third party administrative users (122) access and verify the information in decentralized server. When data is updated, one or more new hash data is generated and broadcasted to the blockchain network (120).

No. of Pages : 19 No. of Claims : 4