

(12) PATENT APPLICATION PUBLICATION

(21) Application No.202211048864 A

(19) INDIA

(22) Date of filing of Application :26/08/2022

(43) Publication Date : 04/11/2022

(54) Title of the invention : SYSTEM AND METHOD FOR BLOCKCHAIN BASED DOCUMENT VERIFICATION

(51) International classification :H04L0009320000, G06Q0020380000, H04L0029060000, H04L0009060000, G06Q0020060000

(86) International Application No :NA  
Filing Date :NA

(87) International Publication No : NA

(61) Patent of Addition to Application Number :NA  
Filing Date :NA

(62) Divisional to Application Number :NA  
Filing Date :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)SINGH, Dhiraj**

Address of Applicant :ODC-4, Panchshil Tech Park, inside Courtyard by Marriott premises, Hinjewadi Phase - 1, Pune - 411057, Maharashtra, India. Pune -----

**3)AHUJA, Sachin**

Address of Applicant :Director - Research, Chitkara University, Chandigarh-Patiala National Highway, Village Jhansla, Rajpura, Punjab - 140401, India. Patiala -----

(57) Abstract :

The present disclosure relates to a system, and method (100) for blockchain based document verification. The system (100) has one or more block chain nodes (102) configured with a certificate hashing module (106) where the blockchain nodes (102) are communicatively coupled through the blockchain network (104). Additionally, the block chains nodes are configured with one or more processing units (108) which generate a tree through the certificate hashing module (106). The processing unit (108) hashes input data to create hashed data, signs the hashed data with a key assigned to a user. Moreover, it also encrypts the signed hashed data, and stores the encrypted signed hashed data with timestamps in a decentralized server (110). The processing unit (108) also enables a third party user to use the user's keys to form signature data, and provide a validity response to access the information from the decentralized server (110).

No. of Pages : 21 No. of Claims : 8