(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :16/08/2023

(21) Application No.202311054943 A
(43) Publication Date : 15/09/2023

(54) Title of the invention : SYSTEM OF DISTRIBUTED KEY GENERATION WITH SMART CONTRACTS AND METHOD THEREOF

(51) International classification	:H04L0009080000, H04L0009320000, H04L0009060000, H04L0009300000, 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 describes a system (100) and method (200) for distributed key generation (DKG) that use zero-knowledge succinct non-interactive argument of knowledge (zk-SNARKs) to produce and distribute one or more cryptographic keys using smart contracts. The proposed system (100) leverages blockchain-based smart contracts to facilitate a trustless and decentralized the one or more cryptographic key generation process. Multiple participants collaboratively contribute to the generation of a public-private key pair. One or more parties (112) contribution remains private, preserving user privacy and confidentiality during the one or more cryptographic key generation process. To ensure the integrity and verifiability of the one or more cryptographic key generation, the system (100) employs zk-SNARKs. The use of zk-SNARKs allows parties (112) to prove the correctness of the contributions without revealing the actual input data. he contributions without revealing the actual input data.

No. of Pages : 21 No. of Claims : 7