

(51) International Patent Classification:
G06F 21/64 (2013.01)

(21) International Application Number:

PCT/EP2019/075505

(22) International Filing Date:

23 September 2019 (23.09.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

16/138,082 21 September 2018 (21.09.2018) US

(71) Applicant: **BLOCKCHAIN CERTIFIED DATA**
[FR/FR]; 104 Avenue Albert 1er, 92500 RUEIL-MAL-
MAISON (FR).(72) Inventors: **JARRY-LACOMBE, Luc**; 84 Avenue Al-
bert 1er, 92500 RUEIL-MALMAISON (FR). **LANGARD,**
Vincent; 15 rue du Chasselas, 34990 JUVIGNAC (FR).(74) Agent: **TOUROUDE, Magali**; 2 Bis rue Alfred Nobel,
77420 MARNE LA VALLEE (FR).(81) Designated States (*unless otherwise indicated, for every
kind of national protection available*): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ,
CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN,
HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP,
KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME,
MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ,
OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,
SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(54) Title: SYSTEMS AND COMPUTER-BASED METHODS OF DOCUMENT CERTIFICATION AND PUBLICATION

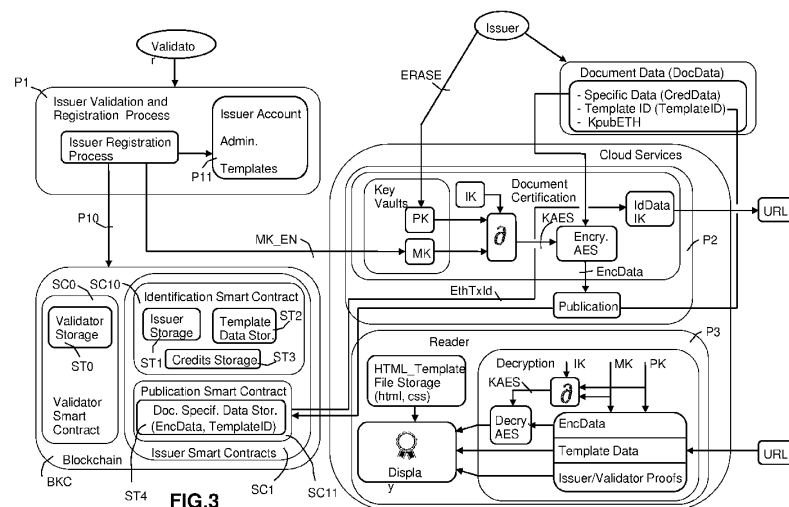


FIG. 3

(57) **Abstract:** The method is implemented in a computer system deployed through the internet and interacts with a blockchain (BKC). Document issuers and validators are connected to the system. The method comprises generating a master key (MK) assigned to an issuer, certifying a document (DocData) through a first process (P2) including generating a document persistence key (PK), encrypting document data (CredData) with an encryption algorithm (AES) and an encryption key (KAES) derived (∂) from the master key, the document persistence key and an intermediate key (IK), registering encrypted document data (EncData) in the blockchain, and generating a web address (URL) carrying recovery information of the certified document; reading the document through a second process (P3) accessible to the web address, the second process including recovering the encrypted data in the blockchain and an access to the three keys, decrypting the encrypted data using the encryption key derived from the three keys, and displaying the document; and upon

[Continued on next page]

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))