

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
02 April 2020 (02.04.2020)



(10) International Publication Number
WO 2020/065633 A1

(51) International Patent Classification:

H04L 9/08 (2006.01) G06F 21/60 (2013.01)
H04L 29/06 (2006.01) H04L 9/32 (2006.01)

(21) International Application Number:

PCT/IB2019/058292

(22) International Filing Date:

30 September 2019 (30.09.2019)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

201811161190.X 30 September 2018 (30.09.2018) CN

(71) Applicant: **VECHAIN GLOBAL TECHNOLOGY S.A.R.L** [LU/LU]; 16 Rue des Primeveres, 2351 Luxembourg (LU).

(72) Inventors: **ZHANG, Lei**; Room 501, No. 17, Lane 349, Huqiu Road, Baoshan District, Shanghai 20044 (CN). **MA, Bangya**; Room 303, Branch 2, No. 1028, Xiuyan Road,

Pudong Xin District, Shanghai 201315 (CN). **GU, Jianliang**; Room 2301, Block C, Lane 555, Hailun Road, Hongkou District, Shanghai 200080 (CN).

(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.

(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,

(54) Title: METHOD, USER DEVICE, MANAGEMENT DEVICE, STORAGE MEDIUM AND COMPUTER PROGRAM PRODUCT FOR KEY MANAGEMENT

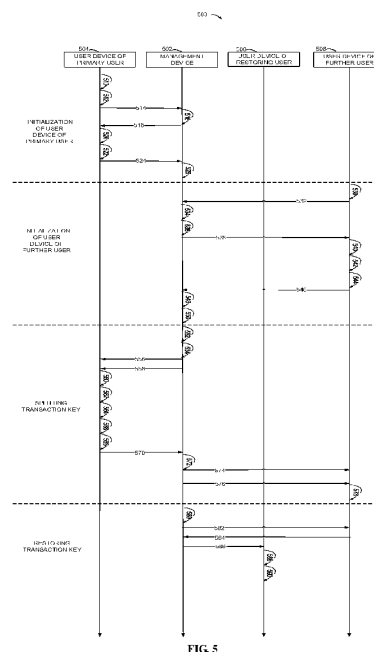


FIG. 5

(57) Abstract: The present disclosure provides methods and devices for key management. In one example, a method of key management comprises: obtaining, at a user device, a number of users in a group of users and a minimum number of users for restoring a transaction key; randomly generating the transaction key; splitting the transaction key into a plurality of sub-keys, the number of sub-keys being the same as the number of users; and sending the plurality of sub-keys to a management device, each of the plurality of sub-keys being encrypted with a public key of a user corresponding to a sub-key.

[Continued on next page]

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))*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*
- *in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE*