



- (51) **International Patent Classification:**
G06F 21/64 (2013.01) *G06Q 20/40* (2012.01)
- (21) **International Application Number:**
PCT/CN2019/084523
- (22) **International Filing Date:**
26 April 2019 (26.04.2019)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (71) **Applicant: ALIBABA GROUP HOLDING LIMITED**
[—/CN]; Fourth Floor, One Capital Place, P.O. BOX 847,
George Town, Grand Cayman (KY).
- (72) **Inventors: WEI, Changzheng;** Alibaba Group Legal Department 5/F, Building 3, No.969 West Wen Yi Road, Yu Hang District, Hangzhou, Zhejiang 311121 (CN). **YAN,**

Ying; Alibaba Group Legal Department 5/F, Building 3, No.969 West Wen Yi Road, Yu Hang District, Hangzhou, Zhejiang 311121 (CN). **ZHAO, Boran;** Alibaba Group Legal Department 5/F, Building 3, No.969 West Wen Yi Road, Yu Hang District, Hangzhou, Zhejiang 311121 (CN). **SONG, Xuyang;** Alibaba Group Legal Department 5/F, Building 3, No.969 West Wen Yi Road, Yu Hang District, Hangzhou, Zhejiang 311121 (CN). **DU, Huabing;** Alibaba Group Legal Department 5/F, Building 3, No.969 West Wen Yi Road, Yu Hang District, Hangzhou, Zhejiang 311121 (CN).

- (74) **Agent: BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION;** Room 409, Tower B, Ka Wah Building, No. 9 Shangdi 3rd Street, Haidian District, Beijing 100085 (CN).

- (81) **Designated States** (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM,

- (54) **Title: SECURELY EXECUTING SMART CONTRACT OPERATIONS IN A TRUSTED EXECUTION ENVIRONMENT**

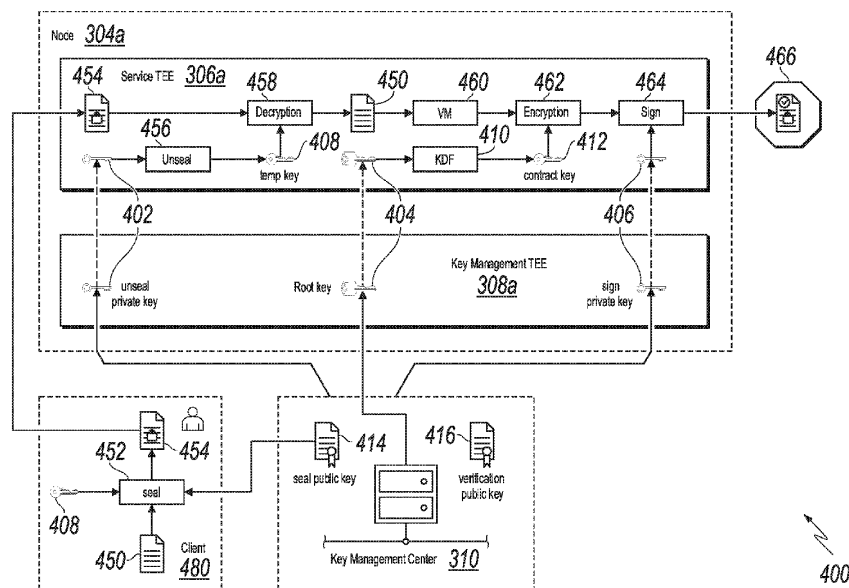


FIG. 4

- (57) **Abstract:** Disclosed herein are methods, systems, and apparatus, including computer programs encoded on computer storage media, for securely executing smart contract operations in a trusted execution environment (TEE). One of the methods includes receiving, by a blockchain node participating in a blockchain network, a request to execute one or more software instructions in a service TEE hosted by the blockchain node, wherein the request is encrypted by a public key associated with the service TEE; decrypting the request with a first private key associated with the service TEE, wherein the first private key is paired with the public key; in response to decrypting the request, executing the one or more software instructions to produce an execution result; encrypting the execution result with a client encryption key associated with the service TEE to produce an encrypted result; and signing the encrypted result using a second private key associated with the TEE to produce a signed encrypted result.

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, 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))
- upon request of the applicant, before the expiration of the time limit referred to in Article 21(2)(a)

(88) Date of publication of the international search report:

12 March 2020 (12.03.2020)
