



(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/CN2019/089486

(22) International Filing Date:
31 May 2019 (31.05.2019)

(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: **YANG, Dayi**; Alibaba Group Legal Department
5/F, Building 3, No.969 West Wen Yi Road, Yu Hang Dis-
trict, Hangzhou, Zhejiang 311121 (CN). **XIA, Ning**; Al-

ibaba Group Legal Department 5/F, Building 3, No.969
West Wen Yi Road, Yu Hang District, Hangzhou, Zhejiang
311121 (CN). **LI, Kang**; Alibaba Group Legal Department
5/F, Building 3, No.969 West Wen Yi Road, Yu Hang Dis-
trict, Hangzhou, Zhejiang 311121 (CN).

(74) Agent: **BEIJING BESTIPR INTELLECTUAL PROP-
ERTY 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,
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,

(54) Title: SYSTEM AND METHOD FOR PROVIDING PRIVACY AND SECURITY PROTECTION IN BLOCKCHAIN-BASED
PRIVATE TRANSACTIONS

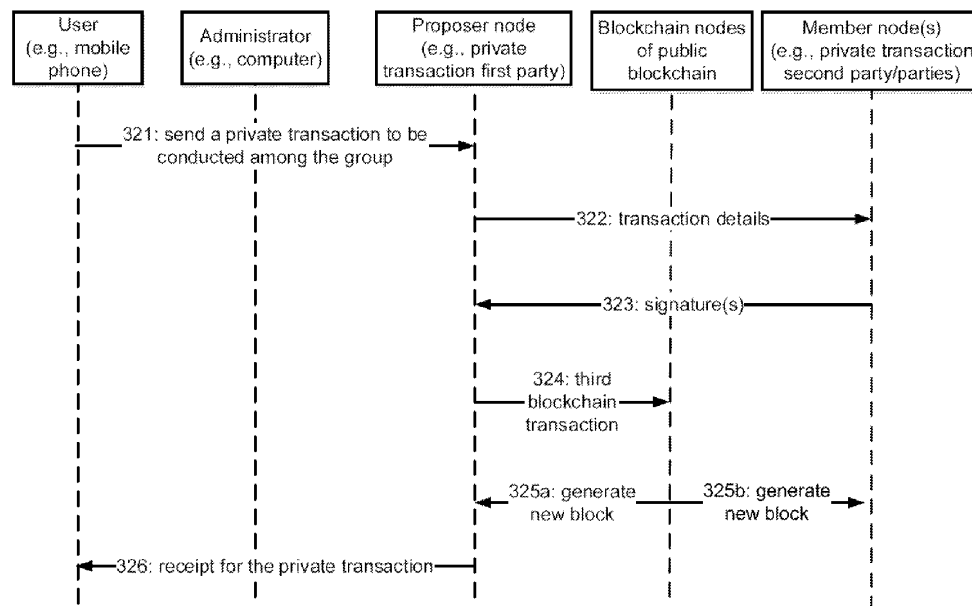


FIG. 4

(57) Abstract: Methods, systems, and apparatus, including computer programs encoded on computer storage media, for implementing blockchain-based private transactions are provided. One of the methods is performed by a first blockchain node to a private transaction, the method including: determining one or more second blockchain nodes to the private transaction according to a blockchain contract in a public blockchain; transmitting transaction information to the one or more second blockchain nodes, the transaction information comprising one or more senders of the private transaction, one or more recipients of the private transaction, and one or more transaction amounts of the private transaction; obtaining a signature from each of a number of the one or more second blockchain nodes certifying receipt of the transaction information; and in response to obtaining the number of the signatures over a threshold, storing at least a representation of the private transaction and the signatures in the public blockchain.

[Continued on next page]

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:

02 April 2020 (02.04.2020)
