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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 April 2019 (18.04.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/072264 A3

(51) International Patent Classification:
G06Q 20/10 (2012.01)

(21) International Application Number:
PCT/CN2018/114344

(22) International Filing Date:
07 November 2018 (07.11.2018)

(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: **MA, Baoli**; Alibaba Group Legal Department 5/F, Building 3, No.969 West Wen Yi Road, Yuhang District, Hangzhou, Zhejiang 311121 (CN). **ZHANG, Wenbin**; Alibaba Group Legal Department 5/F, Building 3, No.969 West Wen Yi Road, Yuhang 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, 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).

(54) Title: BLOCKCHAIN DATA PROTECTION USING HOMOMORPHIC ENCRYPTION

(57) Abstract: A computer-implemented method, performed by a consensus node of a blockchain network, comprises: receiving, from a first account, a digitally signed copy of a commitment value of a first amount of a transaction amount generated based on a first random number, the first amount of the balance transfer and the first random number encrypted using a public key of the first account, a second amount of the balance transfer and a second random number encrypted using a public key of the second account, and a set of values generated based on one or more selected random numbers. The first account determines if the first amount and the second amount are the same and if the first random number and the second random number are the same based on the set of values, and updates the balance of the first account and a balance of the second account based on the first amount of the balance transfer.

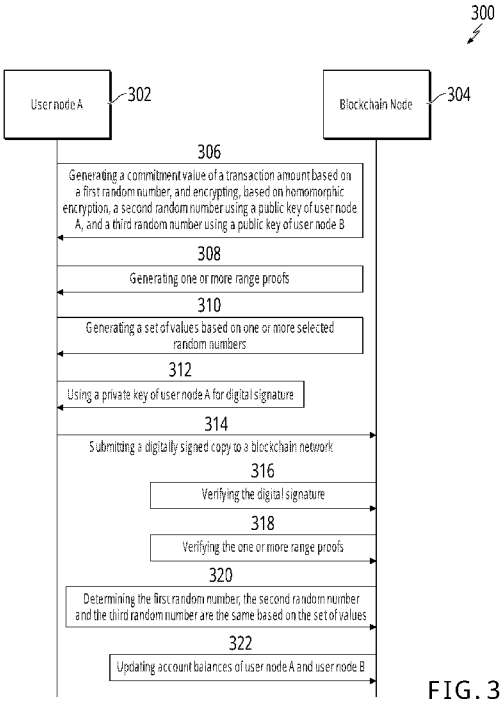

FIG. 3

WO 2019/072264 A3

[Continued on next page]

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:
22 August 2019 (22.08.2019)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/114344

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/10(2012.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, EPODOC, WPI, GOOGLE: block, chain, account, model, consensus, node, verify, commitment, random, value, signature, public, private, key, balance, less, transfer, proof, range

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 108764874 A (SHENZHEN QIANHAI WEBANK CO., LTD.) 06 November 2018 (2018-11-06) abstract, description, paragraphs [0006]-[0021]	1-12
A	CN 108632293 A (UNIV. SHANDONG JIANZHU) 09 October 2018 (2018-10-09) the whole document	1-12
A	CN 107240018 A (CHENGDU LEEREY ENTERPRISE MANAGEMENT LTD.) 10 October 2017 (2017-10-10) the whole document	1-12
A	US 7434726 B2 (PITNEY BOWES INC.) 14 October 2008 (2008-10-14) the whole document	1-12
A	CN 108377189 A (SHENZHEN ONECONNECT INTELLIGENT TECHNOLOGY) 07 August 2018 (2018-08-07) the whole document	1-12
A	CN 106910072 A (GIESECKE&DEVRIENT GMBH CHINA) 30 June 2017 (2017-06-30) the whole document	1-12

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 July 2019	**29 July 2019**

Name and mailing address of the ISA/CN	Authorized officer
National Intellectual Property Administration, PRC **6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing 100088** **China**	**SHU,Qi**
Facsimile No. **(86-10)62019451**	Telephone No. **86-(10)-53961220**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/114344

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 108764874 A	06 November 2018	None	
CN 108632293 A	09 October 2018	None	
CN 107240018 A	10 October 2017	WO 2019019490 A1	31 January 2019
US 7434726 B2	14 October 2008	US 2007262135 A1	15 November 2007
CN 108377189 A	07 August 2018	None	
CN 106910072 A	30 June 2017	None	