



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

(21) International Application Number:
PCT/CN2018/114401

(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 SYSTEM SUPPORTING PUBLIC AND PRIVATE TRANSACTIONS UNDER ACCOUNT MODELS

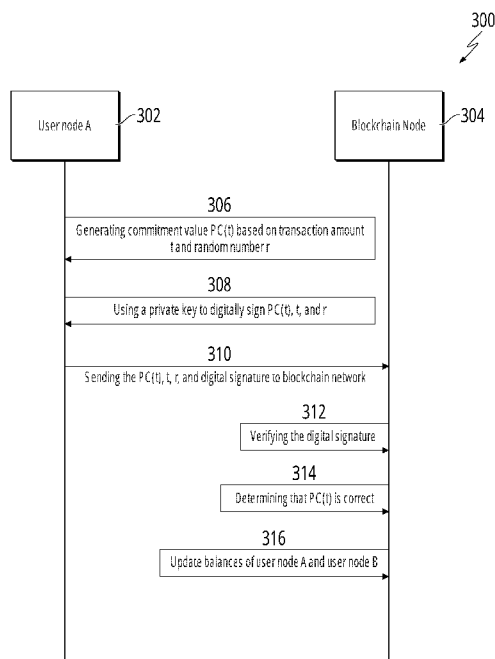


FIG. 3

(57) Abstract: A method includes receiving, by a consensus node of a blockchain, transaction data and a digital signature of the transaction data. The transaction data includes a commitment value, a random number, and a transaction amount to be transferred from one of a public account or a private account of the first user node to one of a public account or a private account of a second user node. The consensus node verifies the digital signature of the transaction data using a public key of the first user node. It then determines that the transaction amount is valid, if the commitment value is correct based on the random number and the commitment scheme, and the transaction amount is less than or equal to a balance of the one of the public account or the private account of the first user node before transfer of the transaction amount.



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/CN2018/114401

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]	1-9
A	CN 106910072 A (GIESECKE & DEVRIENT GMBH CHINA) 30 June 2017 (2017-06-30) the whole document	1-9
A	CN 106911470 A (UNIV. BEIHANG) 30 June 2017 (2017-06-30) the whole document	1-9
A	CN 108389046 A (UNIV. XIAN JIAOTONG) 10 August 2018 (2018-08-10) the whole document	1-9
A	CN 108335103 A (PBOC. DIGITAL CURRENCY RES. INST.) 27 July 2018 (2018-07-27) the whole document	1-9
A	US 7434726 B2 (PITNEY BOWES INC.) 14 October 2008 (2008-10-14) the whole document	1-9
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
<p>* Special categories of cited documents:</p> <p>“A” document defining the general state of the art which is not considered to be of particular relevance</p> <p>“E” earlier application or patent but published on or after the international filing date</p> <p>“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)</p> <p>“O” document referring to an oral disclosure, use, exhibition or other means</p> <p>“P” document published prior to the international filing date but later than the priority date claimed</p> <p>“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</p> <p>“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</p> <p>“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</p> <p>“&” document member of the same patent family</p>		
Date of the actual completion of the international search 01 July 2019		Date of mailing of the international search report 25 July 2019
Name and mailing address of the ISA/CN National Intellectual Property Administration, PRC 6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing 100088 China		Authorized officer JIANG,Lingling
Facsimile No. (86-10)62019451		Telephone No. 86-(10)-53961421

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2018/114401

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 106910072 A	30 June 2017	None	
CN 106911470 A	30 June 2017	None	
CN 108389046 A	10 August 2018	None	
CN 108335103 A	27 July 2018	None	
US 7434726 B2	14 October 2008	None	