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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
05 December 2019 (05.12.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/228557 A3

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04L 9/00* (2006.01)

(21) International Application Number:
PCT/CN2019/103791

(22) International Filing Date:
30 August 2019 (30.08.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PCT/CN2019/094396
02 July 2019 (02.07.2019) CN
PCT/CN2019/095299
09 July 2019 (09.07.2019) CN

(71) Applicant: **ALIBABA GROUP HOLDING LIMITED** [—/CN]; Fourth Floor, One Capital Place, P.O. BOX 847, George Town, Grand Cayman (KY).

(72) Inventors: **YANG, Renhui**; Alibaba Group Legal Department 5/F, Building 3, No.969 West Wen Yi Road, Yu Hang District, Hangzhou, Zhejiang 311121 (CN). **LIU, Jiawei**; Alibaba Group Legal Department 5/F, Building 3, No.969 West Wen Yi Road, Yu Hang District, Hangzhou, Zhejiang 311121 (CN). **CHEN, Yuan**; Alibaba Group Legal Department 5/F, Building 3, No.969 West Wen Yi Road, Yu Hang District, Hangzhou, Zhejiang 311121 (CN). **LIN, Yuqi**; 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, 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,

(54) Title: SYSTEM AND METHOD FOR DECENTRALIZED-IDENTIFIER AUTHENTICATION

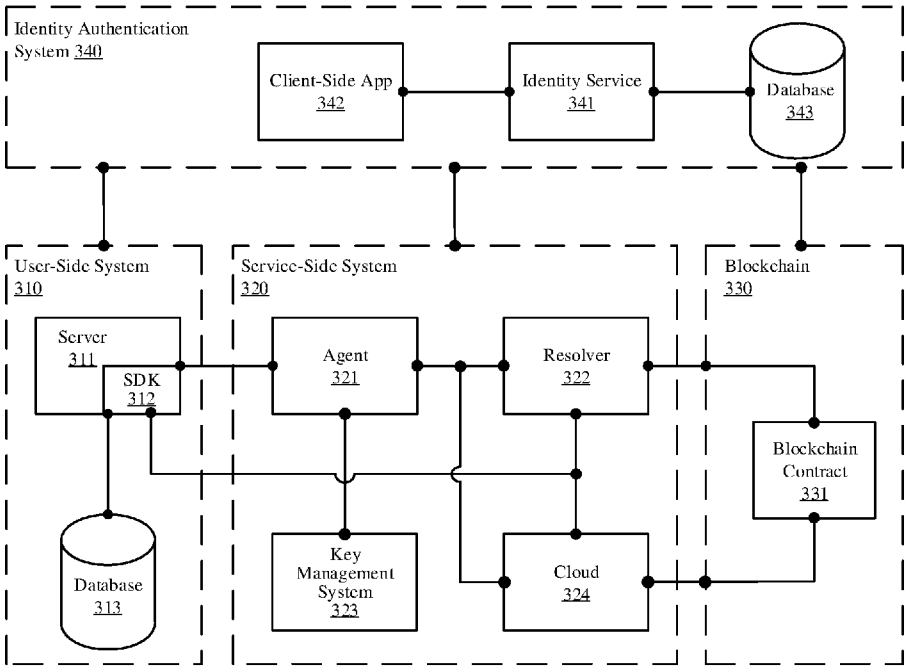

FIG. 3

(57) Abstract: Methods, systems, and apparatus, including computer programs encoded on computer storage media, for blockchain-based decentralized-identifier authentication, are provided. One of the methods includes: obtaining a request for authenticating a decentralized identifier (DID), wherein the request comprises the DID, a plaintext associated with a challenge for authenticating the DID, and a digital signature on the plaintext; obtaining a public key associated with the DID; determining, based on the obtained public key and the plaintext, that the digital signature on the plaintext is created based on a private key corresponding to the DID; and generating, based on the determination, a message confirming authentication of the DID.

WO 2019/228557 A3

[Continued on next page]

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:**
30 April 2020 (30.04.2020)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/103791

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i; H04L 9/00(2006.01)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)

H04L

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, WPI, EPODOC, IEEE: blockchain, request, authentication, DID, decentralized, identifier, digital, signature, plaintext, private, public, verifiable, claims

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	OTHMAN, Asem et al. "The Horcrux Protocol: A Method for Decentralized Biometric-based Self-sovereign Identity" *2018 International Joint Conference on Neural Networks (IJCNN)*, 15 October 2018 (2018-10-15), pages 1-5	1-16
Y	ZHENG, Zibin et al. "Blockchain challenges and opportunities: a survey" *International Journal of Web and Grid Services*, Vol. 14, No. 4, 26 October 2018 (2018-10-26), pages 355-357	1-16
A	AYDAR, Mehmet et al. "Towards a blockchain based digital identity verification, record attestation and record sharing system" *https://arxiv.org/pdf/1906.09791.pdf*, 24 June 2019 (2019-06-24), the whole document	1-16
A	WO 2019104323 A1 (NOK NOK LABS, INC.) 31 May 2019 (2019-05-31) the whole document	1-16
A	CN 109922077 A (BEIJING SYSWIN INTERNET TECHNOLOGY CO., LTD.) 21 June 2019 (2019-06-21) the whole document	1-16

☑ 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
21 March 2020	**01 April 2020**
Name and mailing address of the ISA/CN **National Intellectual Property Administration, PRC** **6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer **BI,Yachao** Telephone No. **86-(10)-53961777**

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/103791

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 109327456 A (BEIJING KNOWNSEC INFORMATION TECHNOLOGY CO., LTD.) 12 February 2019 (2019-02-12) the whole document	1-16

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/103791

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
WO 2019104323 A1	31 May 2019	US 2019164156 A1	30 May 2019
CN 109922077 A	21 June 2019	None	
CN 109327456 A	12 February 2019	None	