

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
28 September 2023 (28.09.2023)



(10) International Publication Number
WO 2023/180000 A1

(51) International Patent Classification:
H04L 9/00 (2022.01) *H04L 9/32* (2006.01)
H04L 9/30 (2006.01)

(72) Inventors: **BURNS, Alec**; c/o nChain Licensing AG, 30 Market Place, London W1W 8AP (GB). **WRIGHT, Craig Steven**; c/o nChain Licensing AG, 30 Market Place, London W1W 8AP (GB).

(21) International Application Number:
PCT/EP2023/054369

(74) Agent: **MAHON, Thomas James**; Page White & Farrer, Bedford House, 21 John Street, London WC1N 2BF (GB).

(22) International Filing Date:
22 February 2023 (22.02.2023)

(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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, 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, ST, SV, SY, TH,

(25) Filing Language: English

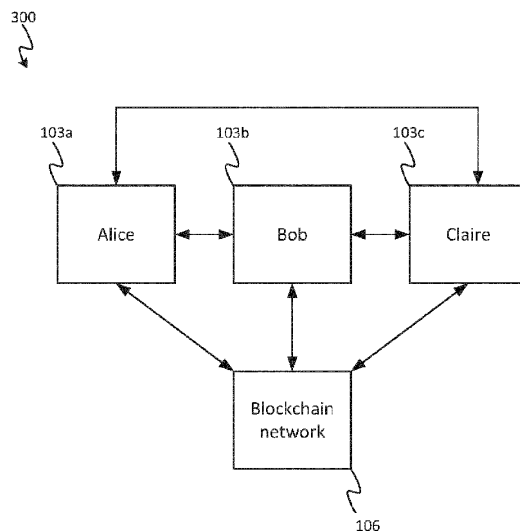
(26) Publication Language: English

(30) Priority Data:
2203988.7 22 March 2022 (22.03.2022) GB

(71) Applicant: **NCHAIN LICENSING AG** [CH/CH]; Grafenauweg 6, 6300 Zug (CH).

(54) Title: SET SHUFFLING

Figure 3



(57) Abstract: A computer-implemented method of shuffling an ordered set of data items, comprising: generating an ordered set of shuffle keys, each shuffle key being an elliptic curve point, and said generating comprising, for each data item: either deriving the shuffle key based on a respective private key, or generating the shuffle key and deriving the respective private key based on the shuffle key, deriving, based on the respective private key, a public key, and mapping the public key to the respective data item; encrypting each shuffle key with a first scalar to obtain a respective first encrypted shuffle key; placing each first encrypted shuffle keys in an ordered set, wherein the order of the first encrypted shuffle keys is shuffled compared with the order of the shuffle keys in the ordered set of shuffle keys; and sharing the ordered set of first encrypted shuffle keys with at least a second party.

[Continued on next page]

TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS,
ZA, ZM, ZW.

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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))
- in black and white; the international application as filed contained color or greyscale and is available for download from PATENTSCOPE