



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

(21) International Application Number:
PCT/EP2023/055444

(22) International Filing Date:
03 March 2023 (03.03.2023)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2203994.5 22 March 2022 (22.03.2022) GB

(71) Applicant: NCHAIN LICENSING AG [CH/CH]; Grafe-
nauweg 6, 6300 Zug (CH).

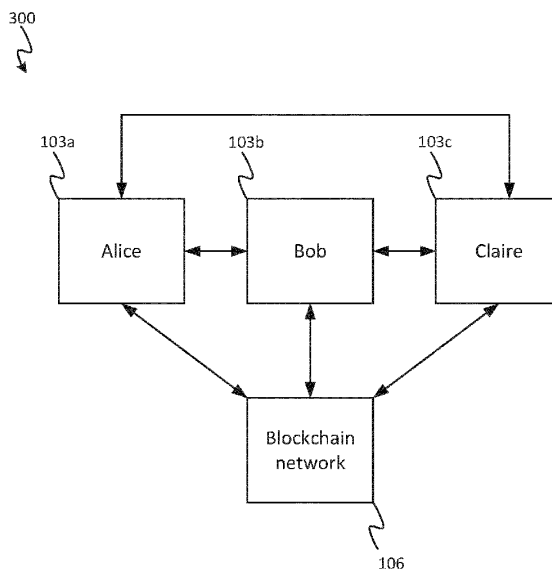
(72) Inventors: **BURNS, Alec**; c/o nChain Licensing AG, 30
Market Place, London W1W 8AP (GB). **WRIGHT, Criag
Steven**; c/o nChain Licensing AG, 30 Market Place, Lon-
don W1W 8AP (GB).

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

(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,

(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 first party shuffle keys; for each data item, deriving a first party public key, and mapping the first party public key to the data item; obtaining, from each party, a party public key mapped to each data item, wherein a combined public key is generated based on each party public key mapped to that data item, and an ordered set of party encrypted shuffle keys; for each data item, generating a sequence of elements; encrypting each sequence with a first scalar to generate a first encrypted sequence; generating a first ordered set of first encrypted sequences, wherein the order of the first encrypted sequences of elements differs compared to the initial ordered set of sequences of elements; sending the first ordered set of first encrypted sequences of elements to the 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