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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
03 August 2023 (03.08.2023)

WIPO | PCT

(10) International Publication Number
WO 2023/143880 A1

(51) International Patent Classification:
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)

(21) International Application Number:
PCT/EP2023/050084

(22) International Filing Date:
03 January 2023 (03.01.2023)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2200898.1 25 January 2022 (25.01.2022) GB

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

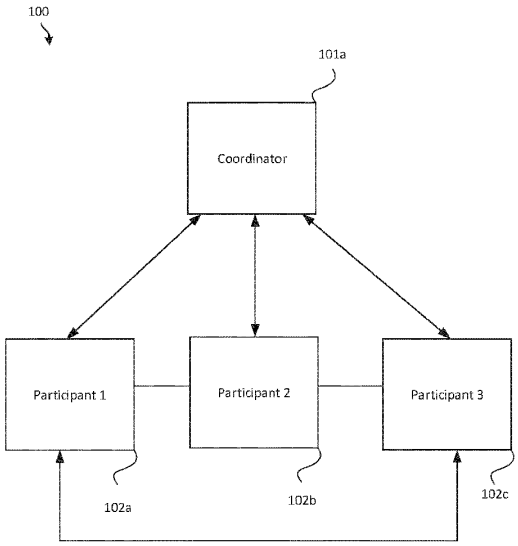
(72) Inventor: **PETTIT, Michaella**; c/o nChain Licensing AG, 30 Market Place, London W1W 8AP (GB).

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

(54) **Title:** GENERATING SHARED PRIVATE KEYS

Figure 1



(57) **Abstract:** A computer-implemented method of generating shares of child private keys, and wherein the method is performed by a first participant of the group and comprises: receiving, from a coordinator, a first share of a master private key, wherein the master private key is generated based on a first portion of a hash of a seed value; receiving, from a coordinator, a master chain code for the master private key, wherein the master chain code is generated based on a second portion of the hash of the seed value; receiving, from a coordinator, a master public key corresponding to the master private key; generating one or more first shares of one or more respective child private keys, wherein each first share of the respective child private key is generated based on the first share of the master private key, and a first portion of a hash of i) the master chain code, ii) the master public key and iii) a respective key index.

WO 2023/143880 A1

[Continued on next page]

(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, 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*