



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

(21) International Application Number:
PCT/EP2023/050089

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

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2200993.0 26 January 2022 (26.01.2022) GB

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

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

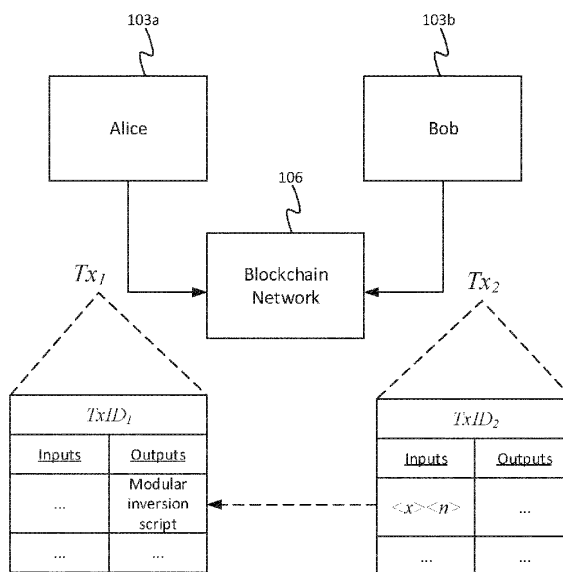
(74) Agent: COLLERTON, Catriona Louise; Page White & Farrer, Bedford House, John Street, London WC1N 2BF (GB).

(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.

(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,

(54) Title: ELLIPTIC CURVE ARITHMETIC IN SCRIPT

Figure 4



(57) Abstract: A computer-implemented method for enabling elliptic curve arithmetic to be performed using blockchain transactions, wherein the method is performed by a script generator. A first script of a first blockchain transaction is generated, wherein the first script comprises a modular inversion script configured to obtain a target integer and a modulus value and output a modular inverse of the target integer. The target integer and the modulus value are co-prime. The modular inverse is generated by iteratively computing a first sequence of the extended Euclidean algorithm with the target integer and modulus value as inputs, and using the first sequence to compute a Bezout co-efficient of the target integer, wherein the Bezout co-efficient of the target integer is output as the modular inverse. The first script is outputted for inclusion in the first blockchain transaction.

[Continued on next page]

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*