

(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)



(10) International Publication Number
WO 2023/144068 A1

- (51) International Patent Classification:
H04L 9/30 (2006.01) *H04L 9/00* (2022.01)
- (21) International Application Number:
PCT/EP2023/051506
- (22) International Filing Date:
23 January 2023 (23.01.2023)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
2200991.4 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; Bedford House John Street, London WC1N 2BF (GB).

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.

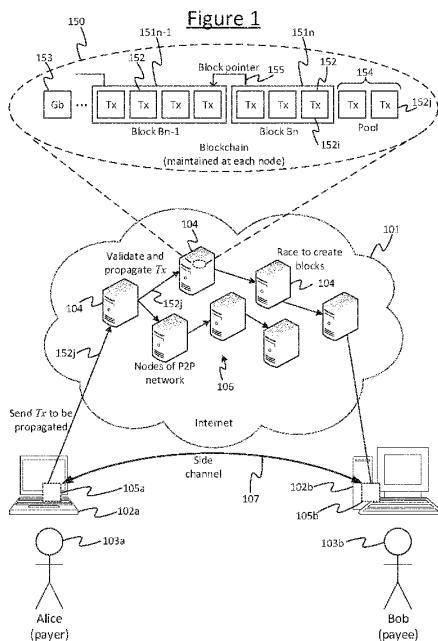
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, 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

- (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,

- (54) Title: ELLIPTIC CURVE ARITHMETIC IN SCRIPT



- (57) Abstract: A computer-implemented method for enabling elliptic curve arithmetic to be performed using blockchain transactions. A first script comprising a modular inversion script is generated. The modular inversion script is configured to obtain a target integer x , a modulus value p , and a pair of indices for a component of an addition chain identifying a pair of previous components which, when summed, equal the component of the addition chain. A modular inverse is generated by computing the exponentiation of x to the reduced modulus $(p-2)$ using the addition chain. For each component of the addition chain for $3 \leq i \leq l$, each multiplier value is calculated by selecting the multiplier values associated with the pair of indices and multiplying the selected multiplier values to generate the respective multiplier value for the component. For $i = 1$, a remainder of the multiplier value with respect to the modulus value is computed.