

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
28 October 2021 (28.10.2021)



(10) International Publication Number
WO 2021/213959 A1

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

(21) International Application Number:
PCT/EP2021/060032

(22) International Filing Date:
19 April 2021 (19.04.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2005953.1 23 April 2020 (23.04.2020) GB

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

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

(74) Agent: TOWNSEND, Martyn James; Page White & Farrow, Bedford House, John Street, London Greater 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, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN,

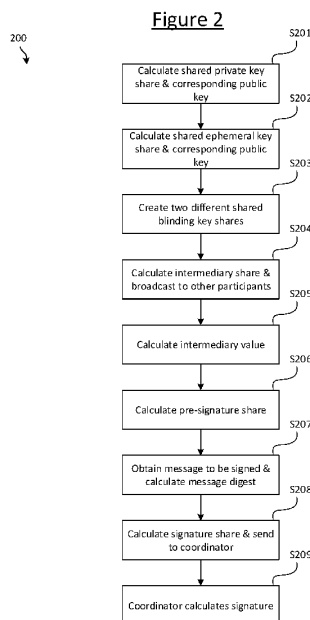
KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, 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, 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))
- before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

(54) Title: (EC)DSA THRESHOLD SIGNATURE WITH SECRET SHARING



(57) Abstract: A computer-implemented method of generating a share of a digital signature of a message, wherein a threshold number of different signature shares from respective participants of a group of participants are required to generate the digital signature, wherein each participant has a respective private key share, the method being performed by a first one of the participants and comprising: generating a first message-independent component and a first message-dependent component, wherein the message-independent component is generated based on a first private key share and wherein the message-dependent component is generated based on the message; causing the first message-independent component to be made available to a coordinator; and causing a first signature share to be made available to the coordinator for generating the signature based on at least the threshold number of signature shares, wherein the first signature share comprises at least the message-dependent component.

WO 2021/213959 A1