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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
07 April 2022 (07.04.2022)

WIPO | PCT

(10) International Publication Number
WO 2022/069133 A1

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

(21) International Application Number:
PCT/EP2021/073964

(22) International Filing Date:
31 August 2021 (31.08.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2015541.2 30 September 2020 (30.09.2020) GB

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

(72) Inventors: **DAVIES, Jack, Owen**; c/o nChain Licensing AG 30 Market Place, London W1W 8AP (GB). **WRIGHT, Craig, Steven**; c/o nChain Licensing AG 30 Market Place, London W1W 8AP (GB).

(74) Agent: **TOWNSEND, Martyn, James** et al.; Page White & Farrer, Bedford House John Street, London WC1N 2BF (GB).

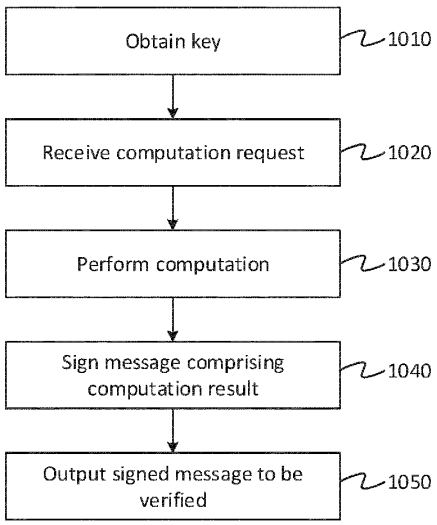
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, 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))*

(54) Title: AUTHENTICATION SYSTEM AND METHOD

FIGURE 10



(57) Abstract: A comprising, by target computer equipment of a target party: obtaining a cryptographic key derived from a response generated by PUF module comprising a physically unclonable function, PUF, the response having been generated by the PUF module based on the PUF in response to a corresponding challenge input to the PUF module, wherein key information comprising the cryptographic key or a corresponding public key is also made available to a verifying party; from an issuing party, receiving a computation request specifying the computation to be performed; in response to the computation request, performing the computation in order to generate a computation result; signing a message comprising the computation result with the cryptographic key; and making the signed message available to the verifying party by sending the signed message to be recorded on a blockchain.

WO 2022/069133 A1