

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
26 August 2021 (26.08.2021)



(10) International Publication Number
WO 2021/165755 A1

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

(21) International Application Number:
PCT/IB2021/050364

(22) International Filing Date:
19 January 2021 (19.01.2021)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2002311.5 19 February 2020 (19.02.2020) GB

(71) Applicant: **NCHAIN HOLDINGS LIMITED** [AG/AG];
Fitzgerald House, 44 Church Street, St. John's (AG).

(72) Inventors: **WRIGHT, Craig Steven**; c/o nChain Holdings Limited, 30 Market Place, London W1W 8AP (GB).

VAUGHAN, Owen; c/o nChain Holdings Limited, 30 Market Place, London W1W 8AP (GB). **DAVIES, Jack Owen**; c/o nChain Holdings Limited, 30 Market Place, London W1W 8AP (GB).

(74) Agent: **TOWNSEND, Martyn James**; PAGE WHITE & FARRER, 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,

(54) Title: ATTESTATION SERVICE FOR USE WITH A BLOCKCHAIN NETWORK

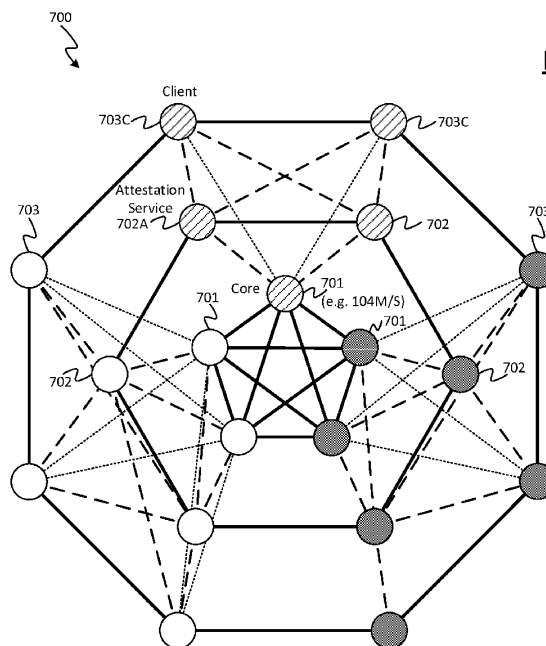


Figure 7

(57) Abstract: A method comprising, at an attesting node of a network: receiving a sequence of data items from one or more client nodes of the network, determining an order of the sequence of data items, and attesting to the order by: including an indication of a respective set of one or more of the data items in each of a series of blockchain transactions. Each successive transaction comprises a respective input pointing to an output of the respective preceding transaction, wherein the output of the respective preceding transaction comprises a locking script, and the input of the respective successive transaction includes an unlocking script comprising a respective signature based on a respective key in a series of keys. The respective signature in each successive transaction signs a portion of the respective successive transaction including at least the indication of the respective set of data items.

[Continued on next page]

WO 2021/165755 A1

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))