

(51) International Patent Classification:
H04L 9/32 (2006.01)(21) International Application Number:
PCT/IB2020/054516(22) International Filing Date:
13 May 2020 (13.05.2020)

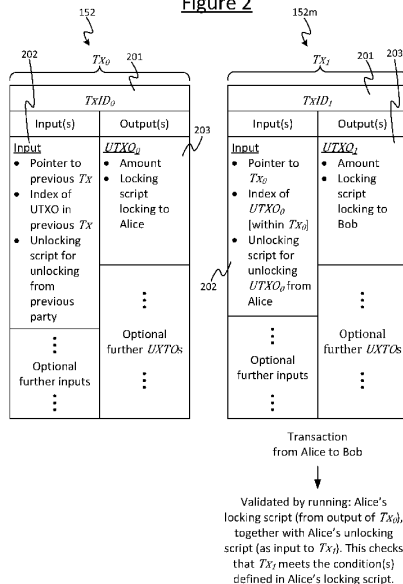
(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1907396.4 24 May 2019 (24.05.2019) GB(71) Applicant: **NCHAIN HOLDINGS LIMITED** [AG/AG];
Fitzgerald House, 44 Church Street, St. John's (AG).(72) Inventors: **WAHAB, Jad**; c/o nChain Holdings Limited,
30 Market Place, London W1W 8AP (GB). **ZHANG, Wei**;
c/o nChain Holdings Limited, 30 Market Place, London W1W 8AP (GB). **DOIRON, Brock**;
c/o nChain Holdings Limited, 30 Market Place, London W1W 8AP (GB). **WRIGHT, Craig**;
c/o nChain Holdings Limited, 30 Market Place, London W1W 8AP (GB).(74) Agent: **WOODHOUSE, Thomas Duncan** et al.; 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, 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).

(54) Title: HASH FUNCTION ATTACKS

Figure 2



(57) Abstract: At least one proof transaction is received at a node of a blockchain network and comprises at least one Elliptic Curve Digital Signature Algorithm (ECDSA) signature and at least one zero-knowledge proof (ZKP) component. The node verifies the ECDSA signature of the at least one proof transaction based on a public key associated with the ECDSA signature and a signed part of the at least one proof transaction, and determined whether the ZKP component is correct for the ECDSA signature and a defined hash value and a defined hash function, in that it proves an ephemeral key counterpart to an r-part of the ECDSA signature to be a preimage of the defined hash value with respect to the defined hash function.

Published:

— *with international search report (Art. 21(3))*