

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

(19) World Intellectual Property  
Organization  
International Bureau

(43) International Publication Date  
26 January 2023 (26.01.2023)



(10) International Publication Number  
**WO 2023/001461 A1**

(51) International Patent Classification:

H04L 9/00 (2022.01) H04L 9/32 (2006.01)  
H04L 9/30 (2006.01) G06Q 20/06 (2012.01)

(21) International Application Number:

PCT/EP2022/066649

(22) International Filing Date:

20 June 2022 (20.06.2022)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

2110348.6 19 July 2021 (19.07.2021) GB

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

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

(74) Agent: MAHON, Thomas James et al.; Page White & Far-  
rer, 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, IQ, IR, IS, IT, JM, 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: ENFORCING CONDITIONS ON BLOCKCHAIN TRANSACTIONS

Figure 6

| TxID <sub>0</sub>     |                                             |              |             |                                                                                                                                                                                                           |
|-----------------------|---------------------------------------------|--------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version               | 1                                           | Locktime     | 0           |                                                                                                                                                                                                           |
| In-count              | 1                                           | Out-count    | 1           |                                                                                                                                                                                                           |
| Input list            |                                             |              | Output list |                                                                                                                                                                                                           |
| Outpoint              | Unlocking script                            | nSeq         | Value       | Locking script                                                                                                                                                                                            |
| Outpoint <sub>A</sub> | < Sig <sub>A</sub> ><br>< PK <sub>A</sub> > | FFFFFF<br>FF | 1000        | [outputsRequest] [sign]<br>OP_CHECKSIGVERIFY OP_SWAP<br><0x68> OP_SPLIT OP_NIP OP_8<br>OP_SPLIT OP_SWAP OP_CAT<br>OP_EQUALVERIFY OP_DUP<br>OP_HASH160 <H(PK <sub>B</sub> )><br>OP_EQUALVERIFY OP_CHECKSIG |

(57) Abstract: A computer-implemented method of enforcing conditions on a second blockchain transaction using a first blockchain transaction, wherein a first one of the conditions is that, when a first unlocking script of the second transaction is executed alongside a first locking script of the first transaction, a representation of the second transaction is output to memory, wherein the representation is based on a plurality of fields of the second transaction and a first output of the first transaction, and wherein the method comprises: generating the first transaction, wherein the first transaction comprises a first output, wherein the first output comprises the first locking script, and wherein the first locking script comprises: a message sub-script; a signature sub-script; a public key corresponding to a private key; and a verification sub-script.

[Continued on next page]

**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