

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
20 August 2020 (20.08.2020)



(10) International Publication Number
WO 2020/165680 A1

(51) International Patent Classification:

G06Q 20/20 (2012.01) G06Q 20/36 (2012.01)
G06Q 20/22 (2012.01) G06Q 20/38 (2012.01)
G06Q 20/30 (2012.01) G06Q 20/40 (2012.01)

1902092.4 15 February 2019 (15.02.2019) GB

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

(21) International Application Number:

PCT/IB2020/050740

(72) Inventors: WRIGHT, Craig Steven; c/o Urquhart-Dykes & Lord LLP, 7th Floor Churchill House, Churchill Way, Cardiff CF10 2HH (GB). DAVIES, Jack Owen; c/o Urquhart-Dykes & Lord LLP, 7th Floor Churchill House, Churchill Way, Cardiff CF10 2HH (GB). MACKAY, Alexander Tennyson; c/o Urquhart-Dykes & Lord LLP, 7th Floor Churchill House, Churchill Way, Cardiff CF10 2HH (GB).

(22) International Filing Date:

30 January 2020 (30.01.2020)

(25) Filing Language:

English

(26) Publication Language:

English

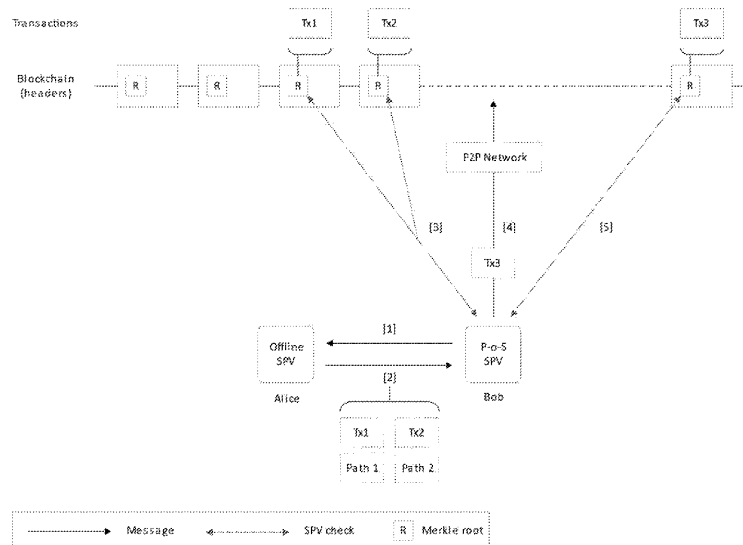
(30) Priority Data:

1902086.6 15 February 2019 (15.02.2019) GB
1902088.2 15 February 2019 (15.02.2019) GB
1902090.8 15 February 2019 (15.02.2019) GB
1902089.0 15 February 2019 (15.02.2019) GB

(74) Agent: JONES, Cerian Elizabeth; Urquhart-Dykes & Lord LLP, 7th Floor Churchill House, Churchill Way, Cardiff CF10 2HH (GB).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

(54) Title: COMPUTER-IMPLEMENTED SYSTEMS AND METHODS FOR IMPLEMENTING TRANSFERS OVER A BLOCKCHAIN NETWORK



An illustrative embodiment of the invention

Figure 10

(57) Abstract: The invention provides improved verification solutions for blockchain-implemented transfers. It is suited for, but not limited to, implementation in an SPV wallet. In accordance with one embodiment, a method, system or resource is provided in which Bob verifies a Merkle proof for a first transaction and, upon successful verification, submits a second transaction to the blockchain. The second transaction has an input that spends an output (UTXO) from the first transaction. Generally, the invention provides an arrangement in which Bob sends Alice a payment transaction template (template Tx3) and requests: the full transaction data for all input transactions (Tx1, Tx2) comprising at least one output that Alice wants to spend as inputs to a transfer (Tx3); the Merkle path for all input transactions (Tx1, Tx2) linking them to their respective Merkle roots associated with their respective block headers; the completed transfer transaction (Tx3). Alice provides this information plus her signature and optionally a change address. Bob can then perform

[Continued on next page]

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).

Published:

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

local SPV checks on the input transactions $Tx1$, $Tx2$ using transactions $Tx1$ and $Tx2$, their corresponding Merkle paths $Path\ 1$, $Path\ 2$, and Bob's local list of block headers. Bob broadcasts the transfer transaction ($Tx3$) to the P2P network.