

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
13 September 2018 (13.09.2018)



(10) International Publication Number
WO 2018/163031 A1

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

(21) International Application Number:
PCT/IB2018/051336

(22) International Filing Date:
02 March 2018 (02.03.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
1703562.7 06 March 2017 (06.03.2017) GB

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

(72) Inventor: **JOSEPH, Daniel**; C/o 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,
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, SM, ST, SV, SY, TH, TJ, TM, TN,
TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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,

(54) Title: **COMPUTER-IMPLEMENTED SYSTEM AND METHOD**

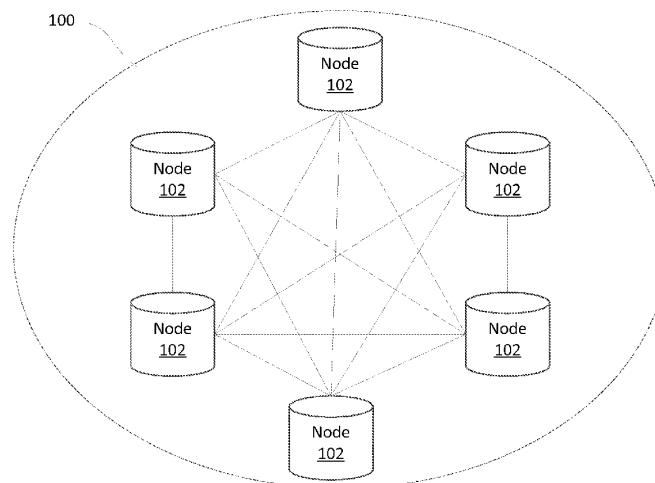


FIG. 1

(57) **Abstract:** The invention provides cryptographic techniques for ensuring and controlling security in respect of blockchain transactions which transfer digital assets or entities from one resource to another. The blockchain may be the Bitcoin blockchain or an alternative protocol. An embodiment of the invention provides a computer-implemented method for improving the security, anonymity and/or control of a value-mixing blockchain transaction having a plurality of participating nodes, each node having a respective output address to which the transaction is to allocate value. The method includes, each participating node, in a first sequence, encrypting its output address using that node's public key, adding the encrypted output address to a set of output addresses for the transaction, and if there is more than one encrypted output address in the set, shuffling the order of the encrypted output addresses in the set. Each participating node, in a second sequence, identifies its encrypted output address in the set, and replaces its encrypted output address

[Continued on next page]

WO 2018/163031 A1

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))