

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
28 June 2018 (28.06.2018)

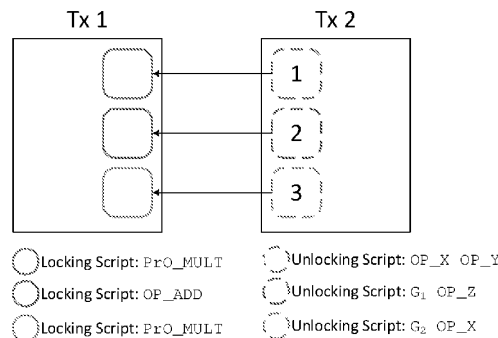


(10) International Publication Number
WO 2018/116105 A1

- (51) International Patent Classification:
H04L 9/32 (2006.01)
- (21) International Application Number:
PCT/IB2017/058008
- (22) International Filing Date:
15 December 2017 (15.12.2017)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
1621831.5 21 December 2016 (21.12.2016) GB
1621830.7 21 December 2016 (21.12.2016) GB
1621827.3 21 December 2016 (21.12.2016) GB
- (71) Applicant: NCHAIN HOLDINGS LIMITED [AG/AG];
Fitzgerald House, 44 Church Street, St. John's (AG).
- (72) Inventor: VINCENT, Stephane; 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 Systems and Methods To Enable Complex Functionality On A Blockchain While Preserving Security-Based Restrictions On Script Size and Opcode Limits

Figure 1: Chain of transaction for Embodiment 1 example



(57) Abstract: The invention relates to blockchain technologies such as the Bitcoin blockchain. The invention uses a novel technique to decompose the functionality of a blockchain transaction script into several chunks or functional parts, and to use the output of a chunk as the input of the next chunk. Advantageously, this allows the blockchain to be used for ever complex tasks and computations while minimising script size, and also provides a novel architecture for the distributed execution of computational processes. The invention comprises a method of using a plurality of blockchain transactions to execute a computer- implemented task, comprising the steps: using an unlocking script (ULS1) associated with a first input (In1) in a blockchain transaction (Tx2) to present at least one data item to a first locking script (LS1) of another transaction (Tx1) so as to provide a result on a stack; generating a further unlocking script (ULS2) associated with a second input (In2) and comprising the result from the stack; wherein the second input (In2) is provided in a further blockchain transaction (Tx3); and presenting the further unlocking script (ULS2) to a further locking script (LS2) such that the

[Continued on next page]

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))

result from the stack is provided as input to the further locking script. Preferably, the locking script (LS1) and further locking script (LS2) are associated with outputs in different blockchain transactions.