

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
28 October 2021 (28.10.2021)



(10) International Publication Number
WO 2021/213922 A1

- (51) **International Patent Classification:**
H04L 9/32 (2006.01) *H04L 29/06* (2006.01)
- (21) **International Application Number:**
PCT/EP2021/059937
- (22) **International Filing Date:**
16 April 2021 (16.04.2021)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
2005822.8 21 April 2020 (21.04.2020) GB
- (71) **Applicant:** NCHAIN LICENSING AG [CH/CH]; Grafenauweg 6, 6300 Zug (CH).
- (72) **Inventor:** COUGHLAN, Steven, Patrick; c/o nChain Licensing AG 30 Market Place, London W1W 8AP (GB).
- (74) **Agent:** TOWNSEND, Martyn, James; Bedford House John Street, London WC1N 2BF (GB).

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))

- (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, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD,

- (54) **Title:** BLOCK PROPAGATION WITH POISONED TRANSACTIONS IN A BLOCKCHAIN NETWORK

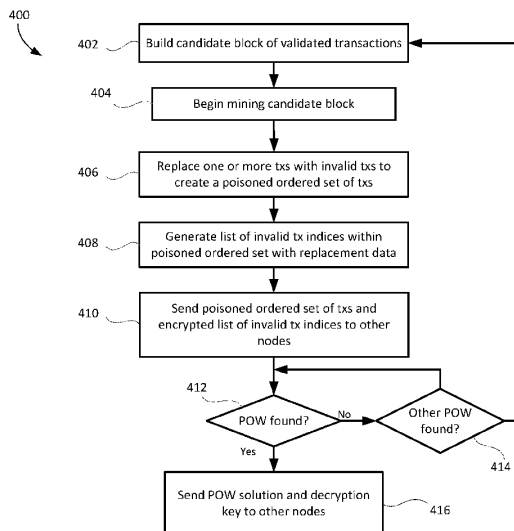


FIG. 4

(57) **Abstract:** Methods and devices for propagating blocks in a blockchain network. At a first mining node, while hashing a first block header of a first candidate block, the first mining node sends, to other mining nodes, a first message specifying transactions and their order in a first ordered set of transactions contained in the first candidate block. To prevent the other nodes from relying on the first mining node having validated the transactions in the candidate block, the first mining node seeds the first ordered set with one or more invalid transactions to create a poisoned ordered set, and provides an encrypted list identifying the invalid transactions. Once a proof-of-work is found for the candidate block, the first mining node provides a decryption key to decrypt the encrypted list and identify the invalid transactions. It may further provide replacement transactions for the invalid transactions.

WO 2021/213922 A1