

(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 2020/165669 A1

- (51) **International Patent Classification:**
G06F 7/58 (2006.01) *H04L 9/32* (2006.01)
- (21) **International Application Number:**
PCT/IB2020/050599
- (22) **International Filing Date:**
27 January 2020 (27.01.2020)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
1901893.6 11 February 2019 (11.02.2019) GB
- (71) **Applicant:** NCHAIN HOLDINGS LIMITED [AG/AG];
Fitzgerald House, 44 Church Street, St. John's (AG).
- (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).
- (74) **Agent:** VINSOME, Rex Martin; 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, 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))

(54) **Title:** COMPUTER IMPLEMENTED METHOD AND SYSTEM FOR PSEUDO-RANDOM DATA GENERATION

Figure 1

Table 1: Script to generate random number $\langle R_N \rangle$		
Stack	Script	Description
Empty	$\langle s'_1 \rangle \langle s'_2 \rangle \dots \langle s'_N \rangle \text{ OP_ADD OP_ADD } \dots \text{ OP_ADD OP_HASH256 } \langle N \rangle \text{ OP_MOD}$	
$\langle s'_1 \rangle \langle s'_2 \rangle \dots \langle s'_N \rangle$	$\text{ OP_ADD OP_ADD } \dots \text{ OP_ADD OP_HASH256 } \langle N \rangle \text{ OP_MOD}$	Constants are added to the stack
$\langle s'_1 \rangle \langle s'_2 \rangle \dots \langle s'_{N-1} + s'_N \rangle$	$\text{ OP_ADD } \dots \text{ OP_ADD OP_HASH256 } \langle N \rangle \text{ OP_MOD}$	Top two values on stack added
$\langle s'_1 \rangle \langle s'_2 \rangle \dots \langle s'_{N-2} + s'_{N-1} + s'_N \rangle$	$\dots \text{ OP_ADD OP_HASH256 } \langle N \rangle \text{ OP_MOD}$	Top two values on stack added
$\langle \sum_i s'_i \rangle$	$\text{ OP_HASH256 } \langle N \rangle \text{ OP_MOD}$	Repeated addition of top two values
$\langle H(\sum_i s'_i) \rangle$	$\langle N \rangle \text{ OP_MOD}$	Top value hashed twice with SHA-256
$\langle H(\sum_i s'_i) \rangle \langle N \rangle$	 OP_MOD	Constants are added to the stack
$\langle R_N \rangle$	Empty	Remainder of 2^{64} value divided by 1^{st} value computed; a random number

(57) **Abstract:** A method of pseudo-randomly generating data is disclosed. The method comprises receiving first data items ($s'_1 s'_2 \dots s'_N$) from a plurality of first participants and combining the first data items to generate second data ($\sum_i s'_i$). A one-way function is applied to the second data to generate third data ($\sum_i s'_i$), wherein the one-way function is adapted to receive input data and generate output data based on the input data, wherein the input data is not deducible from the output data and the one-way function.

WO 2020/165669 A1