

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
11 June 2020 (11.06.2020)



(10) International Publication Number
WO 2020/115748 A1

(51) International Patent Classification:
G06F 15/16 (2006.01)

(21) International Application Number:
PCT/IL2019/051330

(22) International Filing Date:
05 December 2019 (05.12.2019)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/775,942 06 December 2018 (06.12.2018) US

(71) Applicant: **GK8 LTD.** [IL/IL]; 3 Israel Bak Street, 4th floor, 6701908 Tel Aviv (IL).

(72) Inventors: **SHAMAI, Shahr**; 6B Sokolov Street, 7644508 Rehovot (IL). **LAMESH, Lior**; 13 Heil HaShiry-on Street, 7570243 Rishon-LeZion (IL).

(74) Agent: **EHRlich, Gal** et al.; G.E. Ehrlich (1995) LTD., 11 Menachem Begin Road, 5268104 Ramat-Gan (IL).

(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.

(54) Title: SECURE CONSENSUS OVER A LIMITED CONNECTION

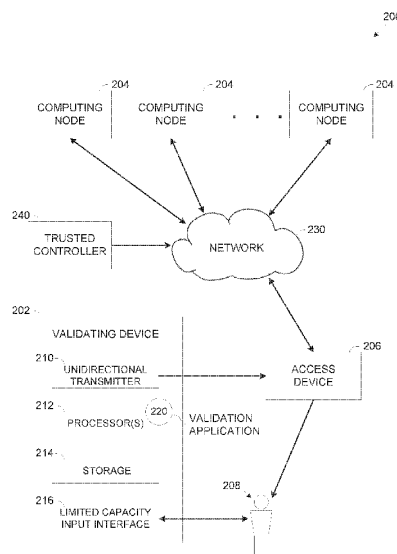


FIG. 2

(57) Abstract: A method of validating a multi-party consensus over a limited connection comprising a validating device configured to transmit a query having a finite number of possible valid answers to a plurality of computing nodes via a unidirectional secure communication channel, receive a limited length string computed based on an aggregated response aggregating a plurality of responses each computed for a multi-party consensus answer to the query by each of at least some of the plurality of computing nodes using a respective secret component, compute a plurality of locally computed strings each computed based on a respective one of the finite number of possible valid answers using an aggregated secret aggregating the plurality of secret components, validate the multi-party consensus answer by comparing the received limited length string to each of the plurality of locally computed strings and initiating one or more operations according to an outcome of the validation.

[Continued on next page]

(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).

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

Published:

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