(12) International Application Status Report

Received at International Bureau: 09 December 2019 (09.12.2019)
Information valid as of: 25 May 2020 (25.05.2020)
Report generated on: 29 September 2020 (29.09.2020)

(10) Publication number:
WO2020/115748

(43) Publication date:
11 June 2020 (11.06.2020)

(26) Publication language:
English (EN)

(21) Application Number:
PCT/IL2019/051330

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

(25) Filing language:
English (EN)

(31) Priority number(s):
62/775,942 (US)

(31) Priority date(s):
06 December 2018 (06.12.2018)

(31) Priority status:
Priority document received (in compliance with PCT Rule 17.1)

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

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

(72) Inventor(s):
SHAMAI, Shahar; 6B Sokolov Street 7644508 Rehovot (IL)
LAMESH, Lior; 13 Heil HaShiryon Street 7570243 Rishon-LeZion (IL)

(74) Agent(s):
EHRLICH, Gal; G.E. Ehrlich (1995) LTD. 11 Menachem Begin Road 5268104 Ramat-Gan (IL)

(54) Title (EN): SECURE CONSENSUS OVER A LIMITED CONNECTION

(54) Title (FR): CONSENSUS SÉCURISÉ SUR CONNEXION LIMITÉE

(57) Abstract:

(EN): 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.

(FR): La présente invention concerne un procédé de validation d'un consensus multi-partie sur une connexion limitée. Ladite invention comprend un dispositif de validation configuré pour transmettre une interrogation qui a un nombre fini de réponses valides possibles à une pluralité de nœuds informatiques par l'intermédiaire d'un canal de communication sécurisé unidirectionnel, recevoir une chaîne de longueur limitée calculée sur la base d'une réponse agrégée qui rassemble une pluralité de réponses chacune calculée pour une réponse de consensus multi-partie à l'interrogation par chacun d'au moins certains de la pluralité de nœuds de calcul en utilisant un composant secret respectif, calculer une pluralité de chaînes calculées localement, chacune étant calculée sur la base d'une respective du nombre fini de réponses valides possibles en utilisant un secret agrégé qui rassemble la pluralité de composants secrets, valider la réponse de consensus multi-partie en comparant la chaîne de longueur limitée reçue à chacune de la pluralité de chaînes calculées localement et initiant une ou plusieurs opérations selon un résultat de la validation.

International search report:
Received at International Bureau: 27 March 2020 (27.03.2020) [US]

International Report on Patentability (IPRP) Chapter II of the PCT:
Not available

(81) Designated States:

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

European Patent Office (EPO) : 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

African Intellectual Property Organization (OAPI) : BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG

African Regional Intellectual Property Organization (ARIPO) : BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW

Eurasian Patent Organization (EAPO) : AM, AZ, BY, KG, KZ, RU, TJ, TM

Declarations:

Declaration of inventorship (Rules 4.17(iv) and 51bis.1(a)(iv)) for the purposes of the designation of the United States of America