

CORRECTED VERSION

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
2 February 2017 (02.02.2017)



(10) International Publication Number
WO 2017/019201 A8

- (51) International Patent Classification: Not classified
- (21) International Application Number:
PCT/US2016/038227
- (22) International Filing Date:
17 June 2016 (17.06.2016)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
62/186,266 29 June 2015 (29.06.2015) US
- (71) Applicant: **PEERNOVA, INC.** [US/US]; 100 Century Center Court, Suite 700, San Jose, CA 95112 (US).
- (72) Inventors: **GANESAN, Gangesh, Kumar**; Peernova, Inc., 100 Century Center Court, Suite 700, San Jose, CA 95112 (US). **HUDSON, David, John**; Peernova, Inc., 100 Century Center Court, Suite 700, San Jose, CA 95112 (US). **GEE, Kevin, Michael**; Peernova, Inc., 100 Century Court, Suite 700, San Jose, CA 95112 (US).
- (74) Agents: **PEREZ, Edgar** et al.; FENWICK & WEST LLP, 801 California Street, Mountain View, CA 94041 (US).
- (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,

HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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, 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:

- upon request of the applicant, before the expiration of the time limit referred to in Article 21(2)(a)
- without international search report and to be republished upon receipt of that report (Rule 48.2(g))

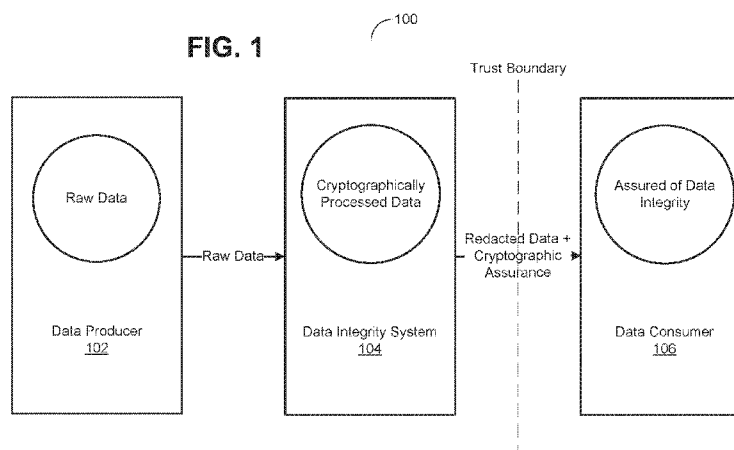
(48) Date of publication of this corrected version:

6 April 2017

(15) Information about Correction:
see Notice of 6 April 2017

(54) Title: CRYPTOGRAPHIC ASSURANCES OF DATA INTEGRITY FOR DATA CROSSING TRUST BOUNDARIES

FIG. 1



(57) Abstract: A data integrity system generates a transaction signature associated with a transaction based on transaction data received from a data producer. The transaction signature is unique to the transaction and is generated by applying a hash function to the transaction data. When the transaction data is to be transmitted to a data consumer, the data integrity system redacts the transaction data based on permission information associated with the data, consumer and transmits the redacted transaction data to the data consumer. To enable the data consumer to verify the integrity of the received data, the data integrity system also transmits a cryptographic assurance that includes at least the transaction signature associated with the transaction. The data consumer verifies the integrity of the received data by independently generating a transaction signature based on the redacted transaction data and matching the independently generated signature with the transaction signature in the cryptographic assurance.