



(51) International Patent Classification:

G06F 21/62 (2013.01) H04L 9/30 (2006.01)  
G06F 21/60 (2013.01)

(21) International Application Number:

PCT/US2019/055032

(22) International Filing Date:

07 October 2019 (07.10.2019)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

|            |                              |    |
|------------|------------------------------|----|
| 62/744,886 | 12 October 2018 (12.10.2018) | US |
| 62/830,272 | 05 April 2019 (05.04.2019)   | US |
| 62/853,231 | 28 May 2019 (28.05.2019)     | US |

(71) Applicant: **MEDICI VENTURES, INC.** [US/US]; 799  
West Coliseum Way, Midvale, Utah 84047 (US).

(72) Inventors: **CHRISTENSEN, Stephen**; c/o Medici Ven-

tures, Inc., 799 West Coliseum Way, Midvale, Utah 84047 (US). **BECKER, Denny**; c/o Medici Ventures, Inc., 799 West Coliseum Way, Midvale, Utah 84047 (US). **BLACK, Tron**; c/o Medici Ventures, Inc., 799 West Coliseum Way, Midvale, Utah 84047 (US). **CALCANO, Michael**; c/o Medici Ventures, Inc., 799 West Coliseum Way, Midvale, Utah 84047 (US). **PERKINS, Tyler**; c/o Medici Ventures, Inc., 799 West Coliseum Way, Midvale, Utah 84047 (US).

(74) Agent: **BRIGGS, Eric N.**; Fogg & Powers LLC, 4600 W 77th Street, Suite 305, Minneapolis, Minnesota 55435 (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, 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,

(54) Title: DOUBLY-ENCRYPTED SECRET PARTS ALLOWING FOR ASSEMBLY OF A SECRET USING A SUBSET OF THE DOUBLY-ENCRYPTED SECRET PARTS

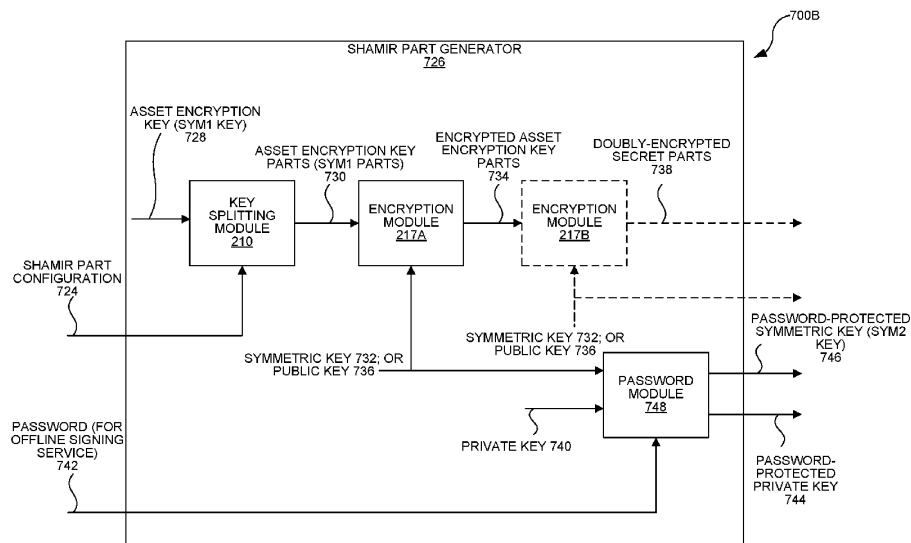


FIG. 7B

(57) Abstract: A system includes at least one processor and at least one memory communicatively coupled to the at least one processor. The at least one processor is configured to encrypt each secret part of at least one set of secret parts into a corresponding singly-encrypted secret part. The at least one processor is also configured to encrypt each corresponding singly-encrypted secret part into a corresponding doubly-encrypted secret part using a corresponding at least one public key, each public key belonging to a corresponding one of at least one public/private keypair. At least a subset of the secret parts of the at least one set of secret parts are used to reconstruct a secret.

[Continued on next page]

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:**

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