

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
14 July 2022 (14.07.2022)



(10) International Publication Number
WO 2022/150617 A1

- (51) International Patent Classification:
G06Q 20/06 (2012.01) *G06Q 20/34* (2012.01)
G06Q 20/32 (2012.01) *G06Q 20/38* (2012.01)
- (21) International Application Number:
PCT/US2022/011660
- (22) International Filing Date:
07 January 2022 (07.01.2022)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
63/135,157 08 January 2021 (08.01.2021) US
63/271,545 25 October 2021 (25.10.2021) US
- (71) Applicant: **ARCULUS HOLDINGS, LLC** [US/US]; 500
Memorial Drive, Somerset, NJ 08873 (US).
- (72) Inventor: **LOWE, Adam**; 2092 Amwell Road, Somerset,
NJ 08873 (US).
- (74) Agent: **DONNELLY, Rex, A.**; RatnerPrestia, 2200 Re-
naissance Boulevard, Suite 350, King of Prussia, PA 19406
(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, IT, 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.

(54) Title: DEVICES, SYSTEMS, AND METHODS FOR PUBLIC/PRIVATE KEY AUTHENTICATION

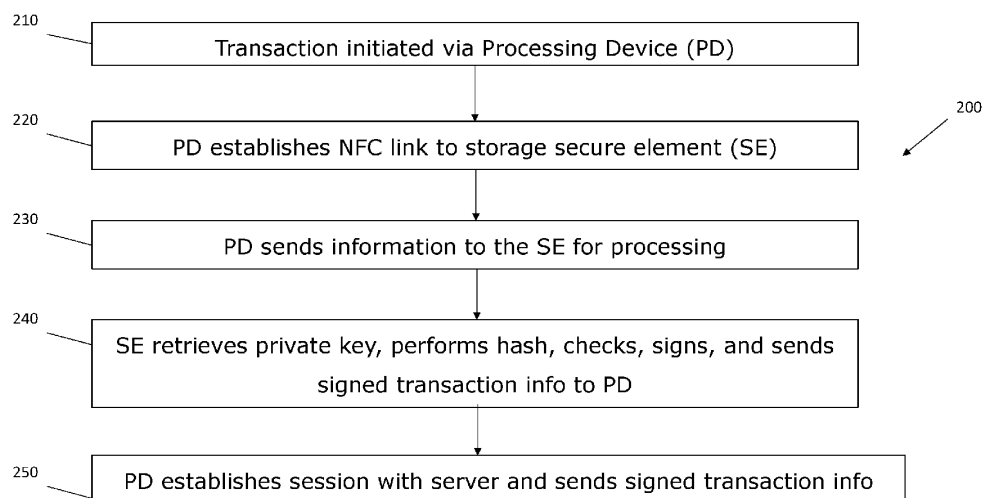


FIG. 2

(57) Abstract: A system for conducting authentication transactions, such as cryptocurrency transactions, includes a storage device with a secure element (SE) that digitally stores encrypted public and private keys, generates a public key using the private key, and performs sign and hash operations. A processing device (PD) is configured to establish a connection over NFC with the SE. The PD receives initiation of a transaction via a user interface, establishes an NFC link with the SE, and sends the SE information for processing via NFC. The secure element retrieves the private key, performs hash operations using the private key to generate a signature, confirms the signature conforms to a public key that could only have been generated using the private key, signs the transaction, and sends signed transaction information to the processing device. The processing device accesses a network and sends signed transaction information operative to complete the transaction.

[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:

- *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
- *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

- *with international search report (Art. 21(3))*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*