



- (51) **International Patent Classification:**
G06F 17/30 (2006.01) *G06Q 30/02* (2012.01)
- (21) **International Application Number:**
PCT/US2021/030022
- (22) **International Filing Date:**
29 April 2021 (29.04.2021)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
63/017,604 29 April 2020 (29.04.2020) US
- (71) **Applicant: BRAVE SOFTWARE, INC.** [US/US]; 512
Second Street, Floor 2, San Francisco, California 94107
(US).
- (72) **Inventors: PESTANA, Gonalo**; Water Gardens, Dove-
cote House 264, London Surrey SE16 6RG (GB).
LIVSHITS, Benjamin; 9 Appold Street, London Middle-
sex EC2A 2AP (GB).
- (74) **Agent: SANDERSON, Scott**; 665 Milwaukee Street, Den-
ver, Colorado 80206 (US).

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.

- (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))*

- (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,

-
- (54) Title:** DECENTRALIZED PRIVACY-PRESERVING REWARDS WITH CRYPTOGRAPHIC BLACK BOX ACCUMULATORS

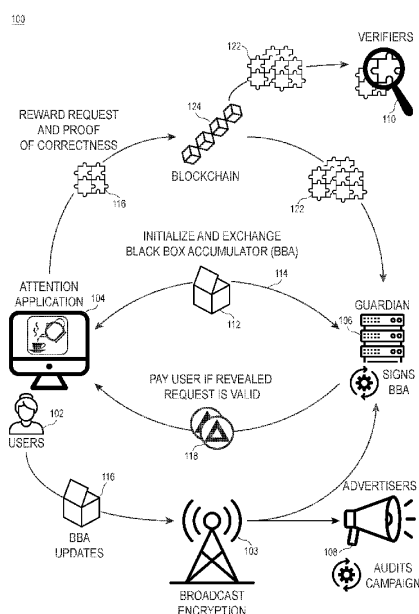


FIG. 1

(57) Abstract: A decentralized and trust-minimizing computer architecture for computing rewards for users of an advertising system includes cryptographic black box accumulators (BBA), which is a cryptographic counter that only the issuer can update. An attention application requests initialization of a BBA from a guardian and subsequently requests updates to the BBA to track interactions between a user of the attention application and ads on the attention application. The guardian signs updates to the BBA to reach agreement on the state of ad interactions. The attention application may randomize the BBA and submit requests via an anonymous channel such that no participant can link two encounters with the BBA to each other or link the BBA to a specific attention application, thus improving user privacy. Reward redemption requests can be made based on a known policy and committed to a public blockchain for verification by observers that the protocol is operating correctly.