



- (51) **International Patent Classification:**
H04L 9/40 (2022.01) *G06F 21/57* (2013.01)
- (21) **International Application Number:**
PCT/IB2024/051398
- (22) **International Filing Date:**
14 February 2024 (14.02.2024)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
63/487,304 28 February 2023 (28.02.2023) US
18/463,716 08 September 2023 (08.09.2023) US
- (71) **Applicant: BLOCKAID LTD** [IL/IL]; Tashah 2, Tel Aviv (IL).
- (72) **Inventors: BENNATAN, Ido;** c/o Blockaid LTD, Tashah 2, Tel Aviv (IL). **NIV, Raz Abraham Eliahou;** c/o Blockaid LTD, Tashah 2, Tel Aviv (IL).

KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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, ME, 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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG,

- (54) **Title:** TECHNIQUES FOR DECENTRALIZED APPLICATION DISCOVERY AND SCANNING

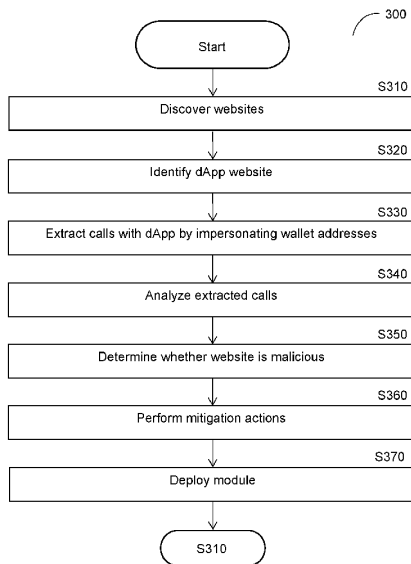


FIG. 3

(57) **Abstract:** Systems and methods for decentralized application (dApp) discovery and scanning. A method for scanning includes performing tests by extracting calls from dApps and analyzing the extracted calls for potentially malicious behavior. To this end, calls made by a dApp are extracted by impersonating wallet addresses. More specifically, transactions are generated based on sample transactions from one or more known wallet addresses, and the generated transactions are broadcast to websites. Calls such as remote procedure calls (RPCs) are extracted from responses to those transactions. The extracted calls are analyzed in order to determine whether the behavior represented in those extracted calls is anomalous. Calls requesting anomalous transactions may be determined to be malicious or potentially malicious, and websites which requested anomalous transactions may be flagged as malicious or potentially malicious. The scanning may be performed on websites found during a discovery process that efficiently analyzes site-indicating data to discover websites.