

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

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
19 December 2024 (19.12.2024)



(10) International Publication Number
WO 2024/258665 A3

(51) International Patent Classification:

H04L 9/32 (2006.01) H04L 9/06 (2006.01)
H04L 9/08 (2006.01) H04L 9/40 (2022.01)

(21) International Application Number:

PCT/US2024/032267

(22) International Filing Date:

03 June 2024 (03.06.2024)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

63/472,482 12 June 2023 (12.06.2023) US
18/583,378 21 February 2024 (21.02.2024) US

(71) Applicant: **PROVABLE INC.** [US/US]; 5470 Kietzke Lane, Ste 300, Reno, NV 89511 (US).

(72) Inventors: **MISHRA, Pratyush**; 5470 Kietzke Lane, Ste 300, Reno, NV 89511 (US). **WU, Howard**; 5470 Kietzke Lane, Ste 300, Reno, NV 89511 (US).

(74) Agent: **QU, Jia-ning**; Van Pelt, Yi & James, LLP, 1 1st St, Ste 12, Los Altos, CA 94022 (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, 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, 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).

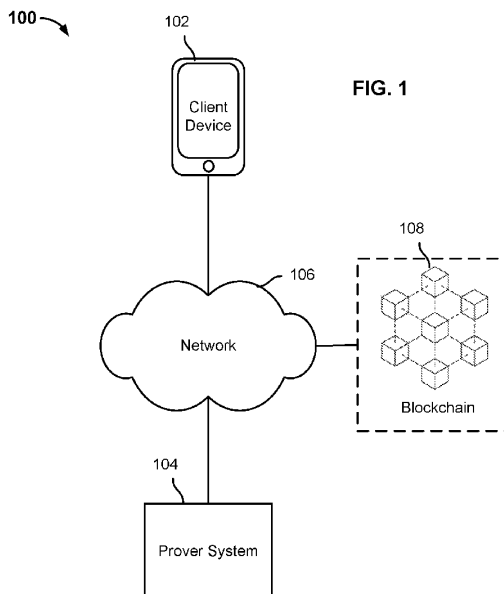
Published:

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

(88) Date of publication of the international search report:

23 January 2025 (23.01.2025)

(54) Title: DELEGATION OF PROOF COMPUTATION



(57) Abstract: Delegation of proof computation is disclosed, including: receiving, at a first processor, a private input data and a public input data to generate a computationally intensive proof associated with a transaction to be posted to a blockchain; and executing, at the first processor, a first proof computation based at least in part on the private input data and the public input data to generate an intermediate proof state; sending, from the first processor, the intermediate proof state to a second processor, wherein the second processor is configured to execute a second proof computation based at least in part on the intermediate proof state to generate the computationally intensive proof associated with the transaction, wherein it is computationally infeasible for the second processor to derive the private input data from the intermediate proof state.

WO 2024/258665 A3