



- (51) **International Patent Classification:**  
*H04L 9/08* (2006.01) *H04L 9/32* (2006.01)
- (21) **International Application Number:**  
PCT/EP2021/062209
- (22) **International Filing Date:**  
07 May 2021 (07.05.2021)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (71) **Applicant:** **DFINITY STIFTUNG** [CH/CH]; Stockerstrasse 47, 8002 Zürich (CH).
- (72) **Inventors:** **BREITNER, Joachim**; c/o Dfinity Stiftung Stockerstrasse 47, 8002 Zürich (CH). **CAMENISCH, Jan**; c/o Dfinity Stiftung Stockerstrasse 47, 8002 Zürich (CH). **CERULLI, Andrea**; c/o Dfinity Stiftung Stockerstrasse 47, 8002 Zürich (CH). **DERLER, David**; c/o Dfinity Stiftung Stockerstrasse 47, 8002 Zürich (CH). **KASHITSYN, Roman**; c/o Dfinity Stiftung Stockerstrasse 47, 8002 Zürich (CH). **NEVEN, Gregory**; c/o Dfinity Stiftung Stockerstrasse 47, 8002 Zürich (CH). **WARINSCHI, Bogdan**; c/o Dfinity Stiftung Stockerstrasse 47, 8002 Zürich (CH).
- (74) **Agent:** **E. BLUM & CO. AG**; Vorderberg 11, 8044 Zürich (CH).

(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.

(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))

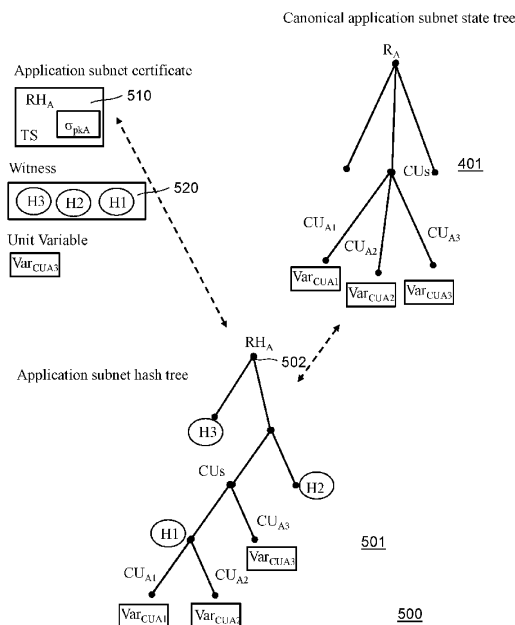
(54) **Title:** DATA AUTHENTICATION IN DISTRIBUTED NETWORKS

FIG. 5

(57) **Abstract:** Embodiments of the invention relate to a computer-implemented method for authenticating data in a distributed network. The distributed network comprises at least one application subnet. The application subnet comprises a plurality of nodes and each of the plurality of nodes is configured to run one or more computational units. The computational units are configured to execute computations in a deterministic and replicated manner across the application subnet. The method comprises steps of regularly computing, by the plurality of nodes of the application subnet, a digest of an application subnet accumulator. The application subnet accumulator comprises for each of the computational units of a respective application subnet an assigned accumulator element as unit variable. The method comprises further steps of regularly executing, by the nodes of the application subnet, a joint signature on the digest of the application subnet accumulator, thereby producing an application subnet certificate. Further aspects relate to a distributed network, a node of a distributed network and a corresponding computer program products.