



- (51) **International Patent Classification:**
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
- (21) **International Application Number:**
PCT/EP2020/068420
- (22) **International Filing Date:**
30 June 2020 (30.06.2020)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (71) **Applicant:** **DFINITY STIFTUNG** [CH/CH]; Stockerstrasse 47, 8002 Zürich (CH).
- (72) **Inventors:** **CAMENISCH, Jan**; c/o Dfinity Stiftung, Stockerstrasse 47, 8002 Zürich (CH). **DRIJVERS, Manu**; c/o Dfinity Stiftung, Stockerstrasse 47, 8002 Zürich (CH). **GROTH, Jens**; c/o Dfinity Stiftung, Stockerstrasse 47, 8002 Zürich (CH). **TACKMANN, Björn**; 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,

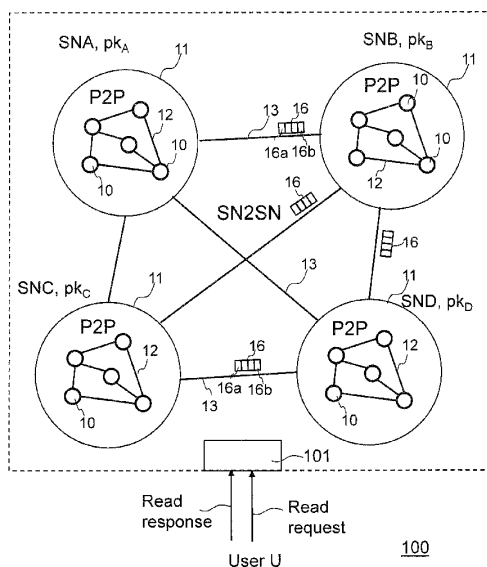
HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, 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:** DISTRIBUTED NETWORKS HAVING A PLURALITY OF SUBNETS



- (57) **Abstract:** According to an embodiment of a first aspect of the invention, there is provided a distributed network comprising a plurality of subnets. Each of the plurality of subnets comprises a changeable set of nodes. The network is configured to generate for each of the plurality of subnets, by a distributed key generation protocol, an individual static verification key of a public-key signature scheme and a first set of corresponding secret key shares for a first set of nodes of the respective subnet. The network is further configured to redistribute, for each of the plurality of subnets, by a secret-redistribution protocol, the secret key shares of the respective first set of secret key shares to a second set of nodes of the respective subnet, thereby creating a second set of secret key shares corresponding to the same static verification key of the respective subnet. Further aspects of the invention relate to a corresponding computer-implemented method, a node, a computer program product and a software architecture.

FIG. 1