

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局



(10) 国际公布号
WO 2025/103146 A1

(43) 国际公布日
2025年5月22日 (22.05.2025)

(51) 国际专利分类号:
H04L 9/00 (2022.01)

(21) 国际申请号: PCT/CN2024/128762

(22) 国际申请日: 2024年10月31日 (31.10.2024)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202311538590.9 2023年11月16日 (16.11.2023) CN

(71) 申请人: 蚂蚁区块链科技(上海)有限公司
(**ANT BLOCKCHAIN TECHNOLOGY (SHANGHAI) CO., LTD.**) [CN/CN]; 中国上海市黄浦区外马路618号8层803室 200010 (CN)。

(72) 发明人: 胡文博(**HU, Wenbo**); 中国上海市黄浦区外马路618号8层803室 200010 (CN)。 周晨辉

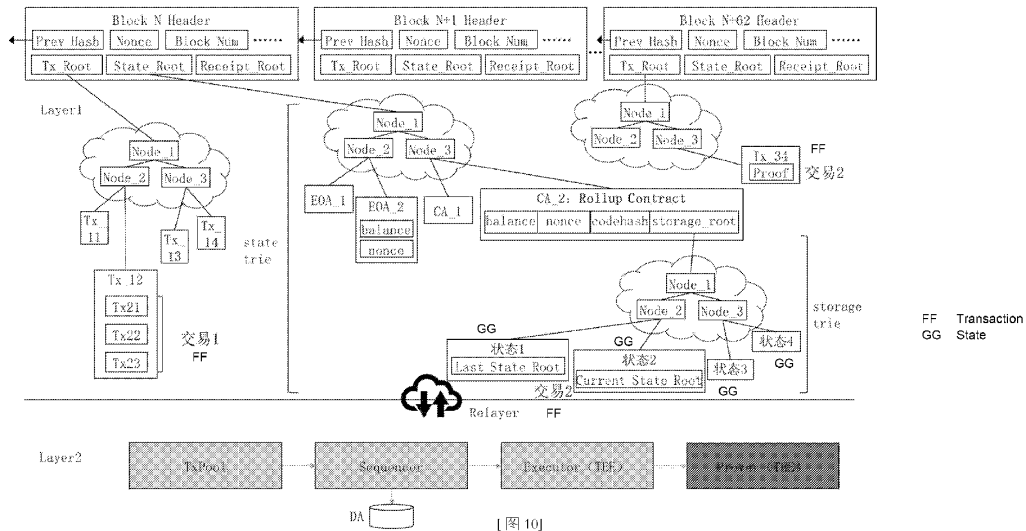
(**ZHOU, Chenhui**); 中国上海市黄浦区外马路618号8层803室 200010 (CN)。 李育文(**LI, Yuwen**); 中国上海市黄浦区外马路618号8层803室 200010 (CN)。 卓海振(**ZHUO, Haizhen**); 中国上海市黄浦区外马路618号8层803室 200010 (CN)。 魏长征(**WEI, Changzheng**); 中国上海市黄浦区外马路618号8层803室 200010 (CN)。 闫莺(**YAN, Ying**); 中国上海市黄浦区外马路618号8层803室 200010 (CN)。 蒋国飞(**JIANG, Guofei**); 中国上海市黄浦区外马路618号8层803室 200010 (CN)。

(74) 代理人: 北京亿腾知识产权代理事务所(普通合伙) (**E-TONE INTELLECTUAL PROPERTY FIRM (GENERAL PARTNERSHIP)**); 中国北京市海淀区中关村紫金数码园3号楼707 100190 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG,

(54) **Title:** METHOD FOR IMPLEMENTING LAYER 2 NETWORK ROLLUP, LAYER 2 NETWORK, AND PROVER

(54) 发明名称: 实现二层网络卷叠的方法、二层网络和证明器



(57) **Abstract:** A method for implementing layer 2 network rollup. An executor and prover of a layer 2 network are implemented by adopting a trusted execution environment. The method comprises: a sequencer of a layer 2 network pulls transactions from a transaction pool, sequences and packages the transactions, reads to the prover an SPV proof of an initial state/read set before execution of a packaged transaction, and sends the initial state/read set and the packaged transaction to an executor; on the basis of the initial state/read set, the executor executes the packaged transaction, adopts a private key of the executor to generate a first signature for a generated write set, and sends the write set and the first signature to a prover; after the prover verifies that the first signature passes, on the basis of the SPV of the initial state/read set, the prover constructs a Merkle tree and uses a tree root as a pre-state root, updates the write set to a

[见续页]

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) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (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)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

leaf node of the Merkle tree, and updates a Merkle root and uses the Merkle root as a post-state root; and the prover adopts a private key of the prover to generate a second signature for the pre-state root and the post-state root, uses the second signature as a proof, and sends the second signature along with the pre-state root and the post-state root to a rollup contract on the mainnet by means of a second mainnet transaction.

(57) 摘要: 一种实现二层网络卷叠的方法, 二层网络的执行器和证明器采用可信执行环境实现, 包括: 二层网络的排序器从交易池拉取交易并对其排序和打包, 读取打包交易执行前的初始状态/读集的SPV证明至证明器, 发送初始状态/读集和打包交易至执行器; 执行器基于初始状态/读集执行打包交易, 采用自身私钥对产生的写集生成第一签名, 将写集及第一签名发送至证明器; 证明器验证第一签名通过后, 根据初始状态/读集的SPV构建Merkle树并将树根作为前状态根, 将写集更新至Merkle树的叶子节点, 更新Merkle根并将其作为后状态根; 证明器采用自身私钥对前状态根和后状态根生成第二签名, 将第二签名作为证明并与前状态根和后状态根一并通过第二主网交易发送至主网上的卷叠合约。