

(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 2025/103147 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/CN2024/128764

(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:  
202311537959.4 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 ROLLUP OF LAYER-2 NETWORK, AND LAYER-2 NETWORK

(54) 发明名称: 实现二层网络卷叠的方法及二层网络

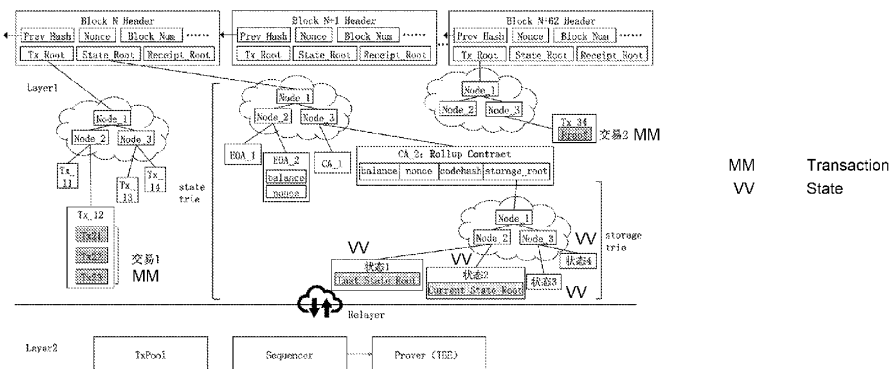


图 5

(57) **Abstract:** A method for implementing the rollup of a layer-2 network. The method comprises: a sequencer of a layer-2 network pulling transactions from a transaction pool, sequencing and packaging the pulled transactions, generating a first transaction root of the packaged transactions, executing the packaged transactions in sequence on the basis of an initial state before the packaged transactions are executed, and generating a first post-state root; the sequencer sending, to a prover of the layer-2 network, the packaged transactions, the first transaction root, the initial state before the packaged transactions are executed, a first pre-state root corresponding to the initial state, and the first post-state root, wherein the prover is implemented by using a trusted execution environment; the prover verifying the first transaction root and the first pre-state root; and after the two roots pass the verification, executing the packaged transactions in sequence on the basis of the initial state, so as to generate a second post-state root, after it is verified that the second post-state root is equal to the first post-state root, signing information of the packaged transactions by using a private key in the trusted execution environment, using the signature as proof, and sending the signature to a blockchain ledger of a main network by means of a second main network transaction.

[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))。

(57) 摘要: 一种实现二层网络卷叠的方法, 包括: 二层网络的排序器从交易池中拉取交易, 对拉取的交易排序并打包, 生成打包交易的第一交易根, 基于打包交易执行前的初始状态按序执行打包的交易并生成第一后状态根; 排序器发送打包的交易、第一交易根、打包交易执行前的初始状态以及初始状态对应的第一前状态根和第一后状态根至二层网络的证明器; 证明器采用可信执行环境实现; 证明器验证第一交易根与第一前状态根; 两个验证通过后, 基于初始状态按序执行打包交易, 生成第二后状态根, 验证第二后状态根与第一后状态根相等后, 采用可信执行环境中的私钥对打包交易的信息签名, 将签名作为证明并通过第二主网交易发送至主网的区块链账本。