

(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 2020/082898 A1

(43) 国际公布日
2020 年 4 月 30 日 (30.04.2020)

(51) 国际专利分类号:
G06Q 20/40 (2012.01)

(21) 国际申请号: PCT/CN2019/103657

(22) 国际申请日: 2019 年 8 月 30 日 (30.08.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811253448.9 2018 年 10 月 25 日 (25.10.2018) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

(72) 发明人: 王吉元 (WANG, Jiyuan); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼 阿里巴巴集团法务部, Zhejiang 311121 (CN)。 闫雪冰 (YAN, Xuebing); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼 阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京博思佳知识产权代理有限公司 (BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION); 中国北京市海淀区上地三街 9 号嘉华大厦 B 座 409, Beijing 100085 (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, 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,

(54) Title: BLOCKCHAIN-BASED TRANSACTION PROCESSING METHOD AND APPARATUS, AND ELECTRONIC DEVICE

(54) 发明名称: 基于区块链的交易处理方法及装置、电子设备

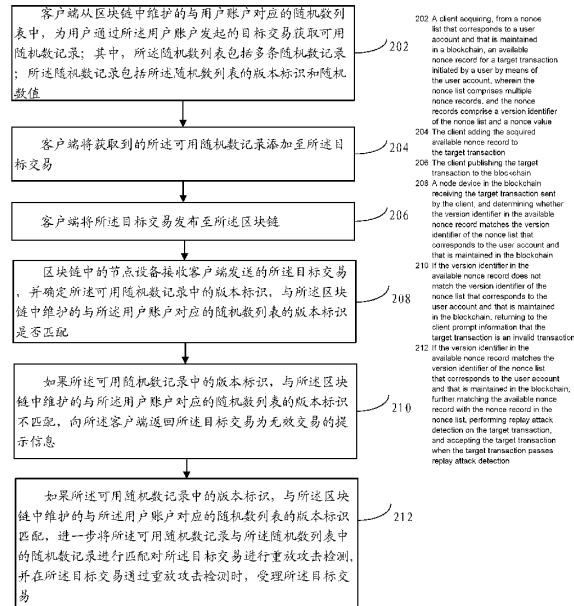


图 2

(57) Abstract: A blockchain-based transaction processing method, comprising: a client acquiring, from a nonce list that corresponds to a user account and that is maintained in a blockchain, an available nonce record for a target transaction initiated by a user by means of the user account, wherein the nonce list comprises multiple nonce records, and the nonce records comprise a version identifier of the nonce list and a nonce value; the client adding the acquired available nonce record to the target transaction, and publishing the target transaction to the blockchain; a node device in the blockchain determining whether the version identifier in the available nonce record

[见续页]

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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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, GH, GM, KE, LR, LS, MW, MZ, NA, RW, 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, 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))。

matches the version identifier of the nonce list that corresponds to the user account and that is maintained in the blockchain; if not, returning to the client prompt information that the target transaction is an invalid transaction; if so, further matching the available nonce record with the nonce record in the nonce list, performing replay attack detection on the target transaction, and accepting the target transaction when the target transaction passes replay attack detection.

(57) 摘要: 一种基于区块链的交易处理方法,包括: 客户端从区块链中维护的与用户账户对应的Nonce列表中, 为用户通过所述用户账户发起的目标交易获取可用Nonce记录; 其中, 所述Nonce列表包括多条Nonce记录; 所述Nonce记录包括所述Nonce列表的版本标识和Nonce值; 客户端将获取到的可用Nonce记录添加至所述目标交易, 并将目标交易发布至所述区块链; 区块链中的节点设备确定可用Nonce记录中的版本标识, 与区块链中维护的与用户账户对应的Nonce列表的版本标识是否匹配; 如果否, 向客户端返回目标交易为无效交易的提示信息; 如果是, 进一步将可用Nonce记录与Nonce列表中的Nonce记录进行匹配对目标交易进行重放攻击检测,并在目标交易通过重放攻击检测时, 受理目标交易。