(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

(43) 国际公布日
2020 年 5 月 28 日 (28.05.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/103557 A1

(51) 国际专利分类号:
G06F 21/64 (2013.01)

(21) 国际申请号: PCT/CN2019/106890

(22) 国际申请日: 2019 年 9 月 20 日 (20.09.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811385400.3 2018年11月20日 (20.11.2018) 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: 林明树 (**LIN, Mingshu**); 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, 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,

WO 2020/103557 A1

(54) **Title:** TRANSACTION PROCESSING METHOD AND DEVICE

(54) 发明名称: 业务处理的方法和装置

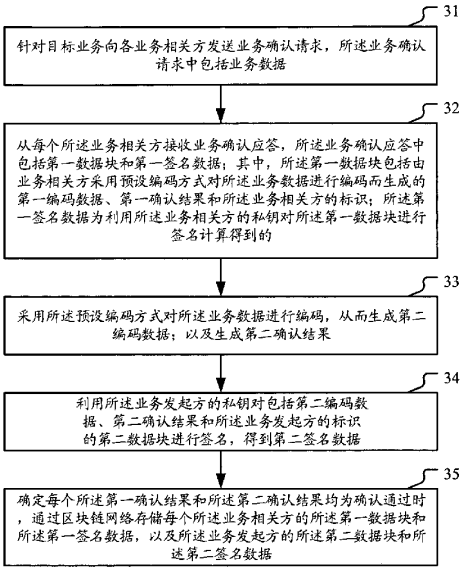

图 3

(57) **Abstract:** A transaction processing method and device. The method performed by a transaction initiator comprises: sending a transaction confirmation request for a target transaction to each transaction-related party, the transaction confirmation request comprising transaction data (31); receiving a transaction confirmation response from each transaction-related party, wherein the transaction confirmation response comprises a first data block and first signature data, the first data block comprises first encoded data, a first confirmation result and an identifier of the transaction-related party, the first encoded data is generated by the transaction-related party

[见续页]

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))。

encoding the transaction data by using a preset encoding scheme, and the first signature data is obtained by performing signature calculation on the first data block by using a private key of the transaction-related party (32); encoding the transaction data by using the preset encoding scheme to generate second encoded data, and generating a second confirmation result (33); performing signing on a second data block by using a private key of the transaction initiator to obtain second signature data, the second data block comprising the second encoded data, the second confirmation result and an identifier of the transaction initiator (34); if confirming that both of the first confirmation result and the second confirmation result are pass confirmations, storing the first data block and the first signature data of each transaction-related party and the second data block and the second signature data of the transaction initiator by means of a blockchain network (35). The method can prevent sensitive data leaks when storing transaction data by using a blockchain network.

(57) 摘要：一种业务处理的方法和装置，业务发起方执行的方法包括：针对目标业务向各业务相关方发送业务确认请求，业务确认请求中包括业务数据（31）；从每个业务相关方接收业务确认应答，业务确认应答中包括第一数据块和第一签名数据；其中，第一数据块包括由业务相关方采用预设编码方式对业务数据进行编码而生成的第一编码数据、第一确认结果和业务相关方的标识；第一签名数据为利用业务相关方的私钥对第一数据块进行签名计算得到的（32）；采用所述预设编码方式对所述业务数据进行编码，从而生成第二编码数据；以及生成第二确认结果（33）；利用所述业务发起方的私钥对包括第二编码数据、第二确认结果和所述业务发起方的标识的第二数据块进行签名，得到第二签名数据（34）；确定每个所述第一确认结果和所述第二确认结果均为确认通过时，通过区块链网络存储每个所述业务相关方的所述第一数据块和所述第一签名数据，以及所述业务发起方的所述第二数据块和所述第二签名数据（35）。该方法能够在利用区块链网络存储业务数据时，不会导致敏感数据的泄露。