

(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 2020/098365 A1

(43) 国际公布日
2020 年 5 月 22 日 (22.05.2020)

(51) 国际专利分类号:
H04L 9/08 (2006.01)

区文一西路 969 号 3 号楼 5 楼 阿里巴巴集团
法务部, Zhejiang 311121 (CN)。

(21) 国际申请号: PCT/CN2019/106017

(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)。

(22) 国际申请日: 2019 年 9 月 16 日 (16.09.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811338344.8 2018 年 11 月 12 日 (12.11.2018) 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,
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。

(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, KY (KY)。

(72) 发明人: 李书博 (LI, Shubo); 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)。 张翼
翔 (ZHANG, Yixiang); 中国浙江省杭州市余杭

(54) Title: BLOCKCHAIN-BASED SERVICE DATA ENCRYPTION METHOD AND APPARATUS

(54) 发明名称: 基于区块链的业务数据加密方法及装置

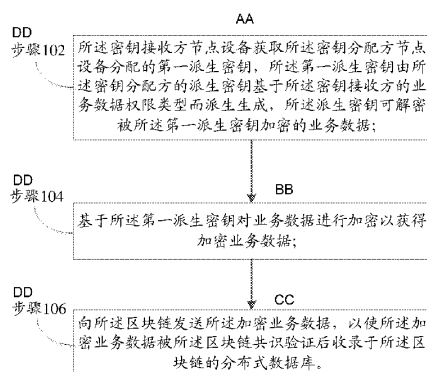


图 1

(57) Abstract: Disclosed are a blockchain-based service data encryption method and apparatus, being applied to a blockchain comprising a key distributor node device and a key receiver node device. The method comprises: a key receiver node device acquiring a first derived key distributed by a key distributor node device, wherein the first derived key is derived and generated from a derived key of a key distributor based on a service data permission type of a key receiver, and the derived key can decrypt service data encrypted by the first derived key (102); encrypting the service data based on the first derived key to obtain encrypted service data (104); and sending the encrypted service data to a blockchain, so that the encrypted service data is consented to and verified by the blockchain and is then recorded in a distributed database of the blockchain (106).

[见续页]

WO 2020/098365 A1

(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))。

(57) 摘要: 一种基于区块链的业务数据加密方法及装置, 应用于包括密钥分配方节点设备和密钥接收方节点设备的区块链, 该方法包括: 所述密钥接收方节点设备获取所述密钥分配方节点设备分配的第一派生密钥, 所述第一派生密钥由所述密钥分配方的派生密钥基于所述密钥接收方的业务数据权限类型而派生生成, 所述派生密钥可解密被所述第一派生密钥加密的业务数据 (102); 基于所述第一派生密钥对业务数据进行加密以获得加密业务数据 (104); 向所述区块链发送所述加密业务数据, 以使所述加密业务数据被所述区块链共识验证后收录于所述区块链的分布式数据库 (106)。