

(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 4 月 2 日 (02.04.2020)



(10) 国际公布号  
**WO 2020/063186 A1**

(51) 国际专利分类号:  
**G06Q 20/38** (2012.01) **G06F 21/62** (2013.01)

(21) 国际申请号: PCT/CN2019/101104

(22) 国际申请日: 2019 年 8 月 16 日 (16.08.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:  
201811160480.2 2018 年 9 月 30 日 (30.09.2018) 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: 张文彬 (ZHANG, Wenbin); 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)。 马

宝利 (MA, Baoli); 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, 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,

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

(54) 发明名称: 基于区块链的交易方法、装置和汇出方设备

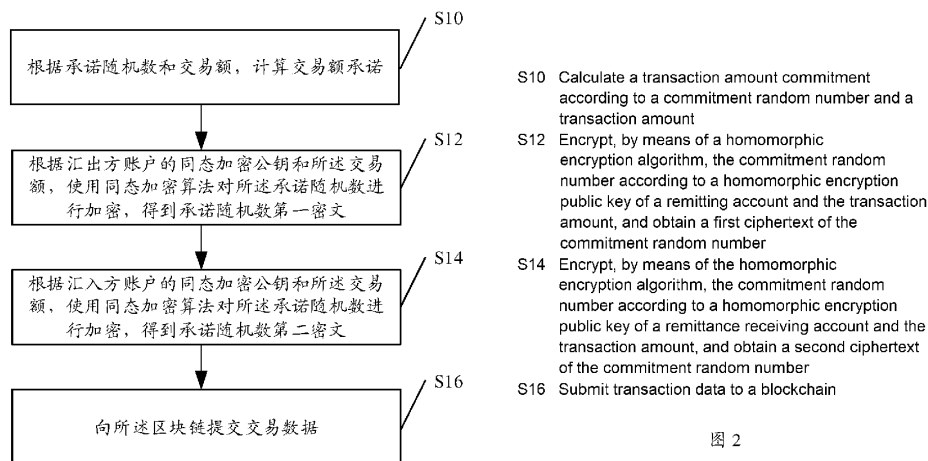


图 2

(57) Abstract: Embodiments of the present disclosure provide a blockchain-based transaction method, a device, and a remitting apparatus. The method comprises: calculating a transaction amount commitment, a first ciphertext of a commitment random number, and a second ciphertext of the commitment random number; and submitting transaction data to a blockchain, the transaction data comprising the transaction amount commitment, the first ciphertext of the commitment random number, and the second ciphertext of the commitment random number, such that the transaction amount commitment and the first ciphertext of the commitment random number are debited from a remitting account, and the transaction amount commitment and the second ciphertext of the commitment random number are credited to a remittance receiving account.

[见续页]

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))。

(57) 摘要: 本说明书实施例提供一种基于区块链的交易方法、装置和汇出方设备。所述方法包括: 计算交易额承诺、承诺随机数第一密文和承诺随机数第二密文; 向所述区块链提交交易数据; 所述交易数据包括所述交易额承诺、所述承诺随机数第一密文和所述承诺随机数第二密文; 以便于将所述交易额承诺和所述承诺随机数第一密文记入所述汇出方账户, 以及将所述交易额承诺和所述承诺随机数第二密文记入所述汇入方账户。