

(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
2019 年 5 月 31 日 (31.05.2019)



(10) 国际公布号
WO 2019/100864 A1

(51) 国际专利分类号:
G06Q 20/10 (2012.01)

海淀区上地三街 9 号嘉华大厦 B 座 409,
Beijing 100085 (CN)。

(21) 国际申请号: PCT/CN2018/109984

(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。

(22) 国际申请日: 2018 年 10 月 12 日 (12.10.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201711185796.2 2017 年 11 月 23 日 (23.11.2017) 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)。

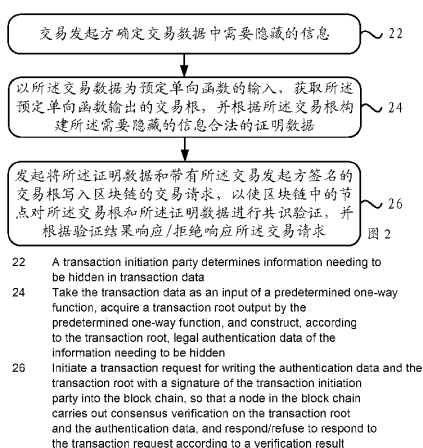
(84) 指定国(除另有指明, 要求每一种可提供的地区
保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM,
AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG,
CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU,
IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,
RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI,
CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

(72) 发明人: 王虎森 (WANG, Husein); 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

(54) Title: DATA PROCESSING METHOD AND APPARATUS

(54) 发明名称: 一种数据处理方法和装置



(57) Abstract: Provided are a data processing method and apparatus. The method comprises: a transaction initiation node in a block chain firstly determining transaction data of a transaction and information needing to be hidden therein (22); then, taking the transaction data as an input of a predetermined one-way function, acquiring a transaction root of the transaction, and constructing, based on the transaction root, authentication data corresponding to the information needing to be hidden (24); and finally, after the transaction root is signed, initiating a transaction request for writing the transaction root and the authentication data into the block chain, carrying out consensus verification on the transaction root and the authentication data by means of a node in the block chain, and responding/refusing to respond to the transaction request based on a verification result (26).

(57) 摘要: 一种数据处理方法和装置。方法包括: 区块链中的交易发起节点首先确定交易的交易数据, 以及其中的需要隐藏的信息 (22); 然后, 将交易数据作为预定单向函数的输入, 获取交易的交易根, 并基于交易根构建需要隐藏的信息对应的证明数据 (24); 最后, 在对交易根进行签名后, 发起将交易根和证明数据写入区块链的交易请求, 由区块链中的节点对交易根和证明数据进行共识验证, 并基于验证结果响应/拒绝响应该交易请求 (26)。

[见续页]

WO 2019/100864 A1

本国际公布：

— 包括国际检索报告(条约第21条(3))。