

(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 2020/029660 A1

(43) 国际公布日
2020年2月13日 (13.02.2020)

(51) 国际专利分类号:
G06F 21/60 (2013.01) H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2019/088958

(22) 国际申请日: 2019年5月29日 (29.05.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810911526.3 2018年8月10日 (10.08.2018) 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)。

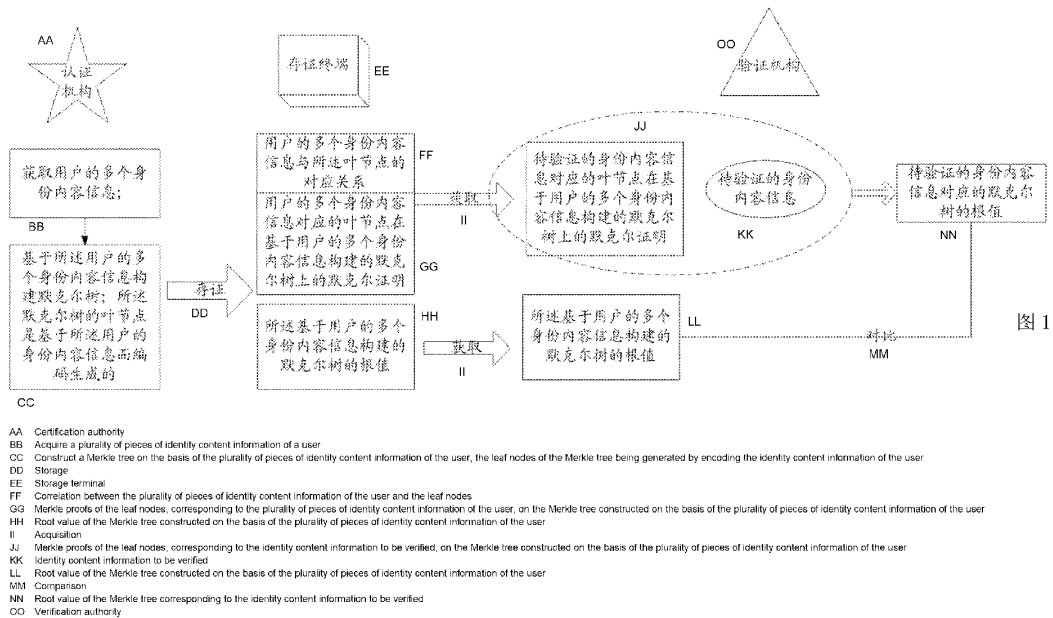
(72) 发明人: 王虎森 (WANG, Husen); 中国浙江省杭州市余杭区文一西路969号3号楼5楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(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,

(54) Title: USER IDENTITY CONTENT INFORMATION AUTHENTICATION AND VERIFICATION METHODS AND DEVICES

(54) 发明名称: 用户的身份内容信息的认证、验证方法和装置



(57) Abstract: One or more embodiments of the present description provide user identity content information authentication and verification methods and devices, said user identity content information authentication method comprising: acquiring a plurality of pieces of identity content information of a user; constructing a Merkle tree on the basis of the plurality of pieces of identity content information of the user, the leaf nodes of the Merkle tree being generated by encoding the identity content information of the user; and sending, to a storage terminal, a correlation between the plurality of pieces of identity content information of the user and the leaf

[见续页]

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))。

nodes, the Merkle proofs of the leaf nodes, corresponding to the plurality of pieces of identity content information of the user, on the Merkle tree constructed on the basis of the plurality of pieces of identity content information of the user, and a root value of the Merkle tree constructed on the basis of the plurality of pieces of identity content information of the user. The storage terminal may comprise one or more of a client of a user, a server of a certification authority, or a distributed database of blockchains.

(57) 摘要: 本说明书的一个或多个实施例提供了用户的身份内容信息的认证、验证方法和装置, 上述用户的身份内容信息的认证方法包括: 获取用户的多个身份内容信息; 基于所述用户的多个身份内容信息构建默克尔树, 所述默克尔树的叶节点是基于所述用户的身份内容信息编码生成的; 向存储终端发送所述用户的多个身份内容信息与所述叶节点的对应关系、所述用户的多个身份内容信息对应的叶节点在基于用户的多个身份内容信息构建的默克尔树上的默克尔证明, 及所述基于用户的多个身份内容信息构建的默克尔树的根值。上述存储终端可以包括用户的客户端、认证机构的服务器或区块链的分布式数据库中的一个或多个。