

(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 2019/179277 A1

(43) 国际公布日
2019年9月26日 (26.09.2019)

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2019/075719

(22) 国际申请日: 2019年2月21日 (21.02.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810224356.1 2018年3月19日 (19.03.2018) CN

(71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 胡瑞丰 (HU, Ruifeng); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 蒋飞虎 (JIANG, Feihu); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 阮子瀚 (YUEN, Tsz Hon); 中国广东省深圳市龙岗区坂田华为总部办

楼, Guangdong 518129 (CN)。 姜耀国 (JIANG, Yaoguo); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 周皓隼 (ZHOU, Haojun); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (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。

(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,

(54) Title: DATA ACCESS RIGHTS CONTROL METHOD AND DEVICE

(54) 发明名称: 一种数据访问权限的控制方法和装置

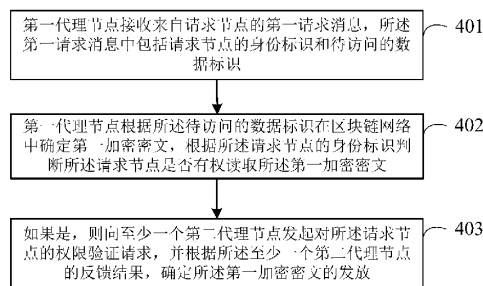


图 4b

(57) Abstract: Disclosed are a data access rights control method and device. The method comprises: a first proxy node receiving a first request message from a requesting node, the first request message comprising therein the identity identifier of the requesting node and a data identifier to be accessed; determining a first encrypted ciphertext in a block chain network according to said data identifier, and determining, according to the identity identifier of the requesting node, whether the requesting node has the rights to read the first encrypted ciphertext; if so, initiating to at least one second proxy node a rights verification request on the requesting node, and according to the feedback result of the at least one second proxy node, determining the issuing of the first encrypted ciphertext. By adding the proxy nodes in the block chain network, the method realizes that a data source node can also freely grant or revoke the rights of the requesting node without modifying the ciphertext, thereby ensuring information security in the network.

[见续页]

WO 2019/179277 A1

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：公开了一种数据访问权限的控制方法和装置，所述方法包括：第一代理节点接收来自请求节点的第一请求消息，所述第一请求消息中包括请求节点的身份标识和待访问的数据标识；根据所述待访问的数据标识在区块链网络中确定第一加密密文，根据所述请求节点的身份标识判断所述请求节点是否有权读取所述第一加密密文；如果是，则向至少一个第二代理节点发起对所述请求节点的权限验证请求，并根据所述至少一个第二代理节点的反馈结果，确定所述第一加密密文的发放。本方法通过在区块链网络中加入代理节点，实现了数据源节点在不修改密文的情况下也能够自由地授予或撤销请求节点的权限，从而保证了网络中信息的安全。