

(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 2022/089518 A1

(43) 国际公布日  
2022 年 5 月 5 日 (05.05.2022)

(51) 国际专利分类号:  
H04L 9/00 (2006.01)

(21) 国际申请号: PCT/CN2021/126962

(22) 国际申请日: 2021 年 10 月 28 日 (28.10.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:  
202011196897.1 2020 年 10 月 31 日 (31.10.2020) 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: 康鑫 (KANG, Xin); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129

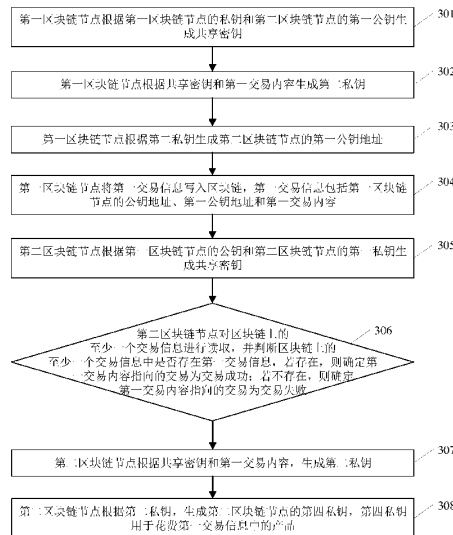
(CN)。 杨艳江 (YANG, Yanjiang); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 王海光 (WANG, Haiguang); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 深圳市深佳知识产权代理事务所 (普通合伙) (SHENPAT INTELLECTUAL PROPERTY AGENCY); 中国广东省深圳市罗湖区南湖街道春风路庐山大厦 B 座 18C2、18D、18E、18E2, Guangdong 518001 (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, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK,

(54) Title: ADDRESS GENERATION METHOD, BLOCKCHAIN INFORMATION PROCESSING METHOD, AND RELATED DEVICE

(54) 发明名称: 地址的生成方法、区块链信息的处理方法以及相关设备



301 A FIRST BLOCKCHAIN NODE GENERATES A SHARED KEY ACCORDING TO A PRIVATE KEY OF THE FIRST BLOCKCHAIN NODE AND A FIRST PUBLIC KEY OF A SECOND BLOCKCHAIN NODE  
302 THE FIRST BLOCKCHAIN NODE GENERATES A SECOND PRIVATE KEY ACCORDING TO THE SHARED KEY AND A FIRST TRANSACTION CONTENT  
303 THE FIRST BLOCKCHAIN NODE GENERATES A FIRST PUBLIC KEY ADDRESS OF THE SECOND BLOCKCHAIN NODE ACCORDING TO THE SECOND PRIVATE KEY  
304 THE FIRST BLOCKCHAIN NODE WRITES FIRST TRANSACTION INFORMATION INTO A BLOCKCHAIN, THE FIRST TRANSACTION INFORMATION COMPRISING THE PUBLIC KEY ADDRESS OF THE FIRST BLOCKCHAIN NODE, THE FIRST PUBLIC KEY ADDRESS, AND THE FIRST TRANSACTION CONTENT  
305 THE SECOND BLOCKCHAIN NODE GENERATES A SHARED KEY ACCORDING TO A PUBLIC KEY OF THE FIRST BLOCKCHAIN NODE AND A FIRST PRIVATE KEY OF THE SECOND BLOCKCHAIN NODE  
306 THE SECOND BLOCKCHAIN NODE READS AT LEAST ONE TRANSACTION INFORMATION ON THE BLOCKCHAIN, AND DETERMINES WHETHER THE FIRST TRANSACTION INFORMATION EXISTS IN AT LEAST ONE TRANSACTION INFORMATION ON THE BLOCKCHAIN, IF YES, A TRANSACTION TO WHICH THE FIRST TRANSACTION CONTENT POINTS IS DETERMINED TO BE SUCCESSFUL, AND IF NOT, THE TRANSACTION TO WHICH THE FIRST TRANSACTION CONTENT POINTS IS DETERMINED TO FAIL  
307 THE SECOND BLOCKCHAIN NODE GENERATES A SECOND PRIVATE KEY ACCORDING TO THE SHARED KEY AND THE FIRST TRANSACTION CONTENT  
308 THE SECOND BLOCKCHAIN NODE GENERATES A FOURTH PRIVATE KEY OF THE SECOND BLOCKCHAIN NODE ACCORDING TO THE SECOND PRIVATE KEY, THE FOURTH PRIVATE KEY BEING USED TO SPEND A PRODUCT IN THE FIRST TRANSACTION INFORMATION

图 3

(57) Abstract: Disclosed in embodiments of the present application are an address generation method, a blockchain information processing method, and a related device, capable of being used in the field of blockchains. The address generation method comprises: a first blockchain node generates a shared key according to a private key of the first blockchain node and a first public key of a second blockchain node, generates a temporary first public key address of the second blockchain node according to the shared key and a first transaction content, and writes first transaction information into a blockchain, the first transaction information comprising the public key address of the first blockchain node, the first public key address, and the first transaction content between the first blockchain node and the second blockchain node. The first public key address needs to be verified using the shared key; a receiving party can also

[见续页]

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,  
ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US,  
UZ, VC, VN, WS, 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))。

generate the shared key by means of a public key of the first blockchain node and a first private key of the second blockchain node  
so as to verify the transaction information; and the receiving party does not need to store and manage a plurality of public-private key  
pairs, thereby reducing the management difficulty.

(57) 摘要: 本申请实施例公开一种地址的生成方法、区块链信息的处理方法以及相关设备, 可用于区块链领域中。方法包括: 第一区块链节点根据第一区块链节点的私钥和第二区块链节点的第一公钥生成共享密钥, 根据共享密钥和第一交易内容生成第二区块链节点的临时的第一公钥地址, 将第一交易信息写入区块链, 第一交易信息包括第一区块链节点的公钥地址、第一公钥地址和第一区块链节点和第二区块链节点之间的第一交易内容; 第一公钥地址需要利用共享密钥进行验证, 接收方也可以通过第一区块链节点的公钥和第二区块链节点的第一私钥生成共享密钥, 以对交易信息进行验证, 接收方无需存储并管理多个公私钥对, 降低了管理难度。