

(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 2022/166556 A1

(43) 国际公布日
2022 年 8 月 11 日 (11.08.2022)

(51) 国际专利分类号:
H04L 9/14 (2006.01)

(21) 国际申请号: PCT/CN2022/071800

(22) 国际申请日: 2022 年 1 月 13 日 (13.01.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202110152304.X 2021年2月3日 (03.02.2021) CN

(71) 申请人: 支付宝 (杭州) 信息技术有限公司 (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) [CN/CN]; 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。蚂蚁区块链科技 (上海) 有限公司 (ANT BLOCKCHAIN

TECHNOLOGY (SHANGHAI) CO., LTD.) [CN/CN]; 中国上海市黄浦区外马路 618 号 8 层 803 室, Shanghai 200010 (CN)。

(72) 发明人: 曾柯 (ZENG, Ke); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。曾超 (ZENG, Chao); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。孔令涛 (KONG, Lingtao); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (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)。

(54) Title: METHOD AND APPARATUS FOR REALIZING SECURE MULTICAST IN BLOCKCHAIN NETWORK

(54) 发明名称: 在区块链网络中实现安全组播的方法及装置

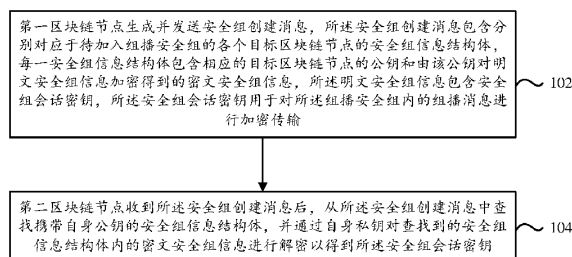


图 1

- 102 A first blockchain node generates and sends a security group creation message, wherein the security group creation message comprises security group information structures respectively corresponding to various target blockchain nodes of a multicast security group to be added, each of the security group information structures comprises a public key of a corresponding target blockchain node and ciphertext security group information which is obtained by encrypting plaintext security group information by means of the public key, the plaintext security group information comprises a security group session key, and the security group session key is used for encrypted transmission of multicast messages in said multicast security group
- 104 Upon receipt of the security group creation message, a second blockchain node searches the security group creation message for a security group information structure carrying its own public key, and decrypts ciphertext security group information in the found security group information structure by means of a private key of the found security group information structure, so as to obtain the security group session key

(57) Abstract: One or more embodiments of the description provide a method and an apparatus for realizing secure multicast in a blockchain network. Said method comprises: a first blockchain node generating and sending a security group creation message, wherein the security group creation message comprises security group information structures respectively corresponding to various target blockchain nodes of a multicast security group to be added, each of the security group information structures comprises a public key of a corresponding target blockchain node and ciphertext security group information which is obtained by encrypting plaintext

[见续页]

WO 2022/166556 A1

(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, 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))。

security group information by means of the public key, the plaintext security group information comprises a security group session key, and the security group session key is used for encrypted transmission of multicast messages in said multicast security group; and upon receipt of the security group creation message, a second blockchain node searching the security group creation message for a security group information structure carrying its own public key, and decrypting ciphertext security group information in the found security group information structure by means of its own private key of the found security group information structure, so as to obtain the security group session key.

(57) 摘要: 本说明书一个或多个实施例提供一种在区块链网络中实现安全组播的方法及装置, 包括: 第一区块链节点生成并发送安全组创建消息, 所述安全组创建消息包含分别对应于待加入组播安全组的各个目标区块链节点的安全组信息结构体, 每一安全组信息结构体包含相应的目标区块链节点的公钥和由该公钥对明文安全组信息加密得到的密文安全组信息, 所述明文安全组信息包含安全组会话密钥, 所述安全组会话密钥用于对所述组播安全组内的组播消息进行加密传输; 第二区块链节点收到所述安全组创建消息后, 从所述安全组创建消息中查找携带自身公钥的安全组信息结构体, 并通过自身私钥对查找到的安全组信息结构体内的密文安全组信息进行解密以得到所述安全组会话密钥。