(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
2022 年 6 月 2 日 (02.06.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/111016 A1

(51) 国际专利分类号:
H04W 12/069 (2021.01) *H04W 12/08* (2021.01)

(21) 国际申请号: PCT/CN2021/120009

(22) 国际申请日: 2021 年 9 月 23 日 (23.09.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202011359296.8 2020年11月27日 (27.11.2020) CN

(71) 申请人: 达闼机器人股份有限公司(**CLOUDMINDS ROBOTICS CO., LTD.**) [CN/CN]; 中国上海市闵行区中青路207号8幢, Shanghai 201111 (CN)。

(72) 发明人: 谢辉(**XIE, Hui**); 中国上海市闵行区昆阳路1508号第2幢二层, Shanghai 201111 (CN)。

(74) 代理人: 北京英创嘉友知识产权代理事务所（普通合伙）(**INNOTRACK INTELLECTUAL PROPERTY LAW FIRM**); 中国北京市朝阳区德胜门外北沙滩1号院31号楼A1108室, Beijing 100083 (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, 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,

(54) **Title:** MOBILE NETWORK ACCESS SYSTEM AND METHOD, AND STORAGE MEDIUM, AND ELECTRONIC DEVICE

(54) 发明名称: 移动网络接入系统、方法、存储介质及电子设备

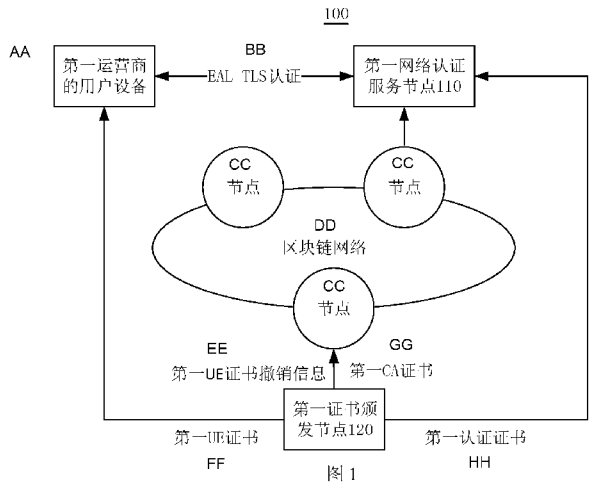


图 1

110 First network authentication service node
120 First certificate issuing node
AA User equipment (UE) of a first operator
BB EAL-TLS authentication
CC Node
DD Blockchain network
EE First UE certificate revocation information
FF First UE certificate
GG First CA certificate
HH First authentication certificate

(57) **Abstract:** The present invention relates to a mobile network access system and method, and a storage medium, and an electronic device. The system comprises: a first network authentication service node and a first certificate issuing node which are in a blockchain network; the first network authentication service node and the first certificate issuing node belong to a first operator; the first certificate issuing node is used for issuing, to the first network authentication service node, a first authentication certificate for indicating the identity of the first network authentication service node, issuing, to a user equipment (UE) of the first operator, a first UE certificate for indicating the identity of the UE, and storing, into a blockchain, first UE certificate revocation information and a first CA certificate indicating the identity of the first certificate issuing node; the first network authentication service node is used for obtaining the first UE certificate revocation information and the first CA certificate from the blockchain, performing mutual identity authentication with the UE when receiving a first access authentication message of the UE, and accessing the UE to a mobile network when authentication is completed.

WO 2022/111016 A1

[见续页]

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：本公开涉及一种移动网络接入系统、方法、存储介质及电子设备，该系统包括：处于区块链网络中的第一网络认证服务节点、第一证书颁发节点，第一网络认证服务节点和第一证书颁发节点属于第一运营商；第一证书颁发节点用于向第一网络认证服务节点颁发用于表明第一网络认证服务节点身份的第一认证证书，向第一运营商的用户设备颁发用于表明该用户设备身份的第一UE证书，将第一UE证书撤销信息和表明第一证书颁发节点身份的第一CA证书存储到区块链中；第一网络认证服务节点用于从区块链中获取第一UE证书撤销信息以及第一CA证书，在接收到用户设备的第一接入认证消息时，与用户设备进行双向身份认证，在认证完成时，接入用户设备到移动网络。

移动网络接入系统、方法、存储介质及电子设备

相关申请的交叉引用

本公开要求在2020年11月27日提交中国专利局、申请号为202011359296.8、名称为“移动网络接入系统、方法、存储介质及电子设备”的中国专利申请的优先权，其全部内容通过引用结合在本公开中。

技术领域

本公开涉及信息技术领域，具体地，涉及一种移动网络接入系统、方法、存储介质及电子设备。

背景技术

在2G/3G/4G移动通信网络中，UE（User Equipment 用户设备）接入移动网络的认证均是基于对称密码机制，即加密（Encryption）与解密（Decryption）使用同样的密钥，移动运营商和用户设备使用同样密钥，导致移动通信安全性得不到保证。此外，用户每次使用对称加密算法进行移动网络接入请求时，需要使用其他人不知道的惟一密钥，使得移动运营商以及用户设备所拥有的密钥的数量呈几何级数增长，增加了移动运营商以及用户设备密钥管理的负担。

因而，在5G移动通信网络中，引入了基于非对称密码机制的接入认证方法，即使用了一对密钥，公钥（Public Key）和私钥（Private Key）。私钥为唯一的密钥，由移动运营商安全保管，不能外泄，公钥发给任何请求接入的用户设备，非对称加密机制使用一对密钥中的进行加密，可以提升移动通信的安全性，并减少密钥管理的负担。但是，非对称虽然使用了一对密钥，但是，若用户设备非法获得了鉴权服务器的公钥，则可以非法接入移动网络，移动网络接入的安全性同样较低。

发明内容

本公开的目的是提供一种移动网络接入系统、方法、存储介质及电子设备，以解决终端设备接入移动网络的安全性较低的问题。

为了实现上述目的，本公开实施例的第一方面，提供一种移动网络接入系统，所述系统包括处于区块链网络中的第一网络认证服务节点、第一证书颁发节点，其中，所述

第一网络认证服务节点以及所述第一证书颁发节点属于第一运营商；

所述第一证书颁发节点用于向所述第一网络认证服务节点颁发用于表明所述第一网络认证服务节点的身份的第一认证证书，以及向所述第一运营商的用户设备颁发用于表明该第一运营商的用户设备的身份的第一 UE 证书，以及将第一 UE 证书撤销信息和表明所述第一证书颁发节点的身份的第一 CA 证书存储到区块链中；

所述第一网络认证服务节点用于从所述区块链中获取所述第一 UE 证书撤销信息以及所述第一 CA 证书，并在接收到所述第一运营商的用户设备的第一接入认证消息的情况下，与该第一运营商的用户设备进行双向身份认证，在所述双向身份认证完成的情况下，接入该第一运营商的用户设备到所述移动网络。

可选地，所述系统还包括处于所述区块链网络中的第二网络认证服务节点以及第二证书颁发节点，所述第二网络认证服务节点以及所述第二证书颁发节点属于第二运营商；

所述第一证书颁发节点还用于，将为所述第二证书颁发节点颁发的第一漫游许可证书写入所述区块链；

所述第二证书颁发节点用于向所述第二网络认证服务节点颁发用于表明所述第二网络认证服务节点的身份的第二认证证书，以及向所述第二运营商的用户设备颁发用于表明该第二运营商的用户设备的身份的第二 UE 证书，以及将第二 UE 证书撤销信息和表明所述第二证书颁发节点的身份的第二 CA 证书存储到区块链中，以及将为所述第一证书颁发节点颁发的第二漫游许可证书写入所述区块链。

可选地，所述第一 CA 证书以及所述第一证书颁发节点向第一运营商的用户设备颁发的所述第一 UE 证书预置在该第一运营商的用户设备的身份识别卡中；

所述第一证书颁发节点向所述第一网络认证服务节点颁发的所述第一认证证书预置在所述第一网络认证服务节点中或者存储在所述区块链中。

本公开实施例的第二方面，提供一种移动网络接入方法，所述方法应用于第一方面所述的系统中的第一网络认证服务节点，所述方法包括：

接收所述第一运营商的用户设备发送的第一接入认证信息，其中，所述第一接入认证信息包括所述第一 UE 证书；

从所述区块链中获取所述第一 UE 证书撤销信息以及所述第一 CA 证书；

根据所述第一 CA 证书中的公钥验证所述第一 UE 证书是否由所述第一证书颁发节点颁发，并根据所述第一 UE 证书撤销信息确定所述第一 UE 证书是否被撤销；

在确定所述第一 UE 证书由所述第一证书颁发节点颁发，且所述第一 UE 证书未被撤销的情况下，向所述第一运营商的用户设备发送第二接入认证消息，所述第二接入认证消息包括所述第一认证证书，所述第一认证证书用于所述第一运营商的用户设备对所述第一网络认证服务节点进行身份认证，并在所述身份认证通过的情况下，接入所述第一运营商的用户设备到所述移动网络。

可选地，所述方法应用于所述移动网络接入系统中的第一网络认证服务节点，所述方法还包括：

接收所述第二运营商的用户设备发送的第三接入认证信息，其中，所述第三接入认证信息包括所述第二 UE 证书；

从所述区块链中获取所述第一 CA 证书、所述第一漫游许可证书、所述第二漫游许可证书；

在获取到所述第一 CA 证书、所述第二 UE 证书、所述第一漫游许可证书以及所述第二漫游许可证书的情况下，根据所述第一 CA 证书中的公钥验证所述第一漫游许可证书是否由所述第一证书颁发节点颁发，根据所述第二漫游许可证书中的所述第二证书颁发节点的公钥验证所述第二 UE 证书是否由所述第二证书颁发节点颁发；

在确定所述第一漫游许可证书由所述第一证书颁发节点颁发，且所述第二 UE 证书由所述第二证书颁发节点颁发的情况下，向所述第二运营商的用户设备发送第四接入认证消息，所述第四接入认证消息包括所述第一认证证书以及所述第一漫游许可证书，所述第一认证证书以及所述第一漫游许可证书用于所述第二运营商的用户设备对所述第一网络认证服务节点进行身份认证，在所述身份认证通过的情况下，接入所述第二运营商的用户设备到所述移动网络。

本公开实施例的第三方面，提供一种移动网络接入方法，所述方法应用于第一运营商的用户设备，所述方法包括：

向第一网络认证服务节点发送第一接入认证信息，其中，所述第一网络认证服务节点为第一方面所述的系统中的所述第一网络认证服务节点，所述第一接入认证信息包括所述第一 UE 证书；

接收所述第一网络认证服务节点发送的第二接入认证消息，所述第二接入认证消息包括所述第一认证证书；

根据预置的所述第一 CA 证书中的公钥验证所述第一认证证书是否由所述第一颁发

节点颁发；

在确定所述第一认证证书由所述第一颁发节点颁发的情况下，接入所述移动网络。

可选地，所述方法还包括：

向第二网络认证服务节点发送第五接入认证信息，其中，所述第二网络认证服务节点为所述移动网络接入系统中的所述第二网络认证服务节点，所述第五接入认证信息包括所述第二 UE 证书；

接收所述第二网络认证服务节点发送的第六接入认证消息，所述第六接入认证消息包括所述第二认证证书以及所述第一漫游许可证书；

根据预置的所述第一 CA 证书中的公钥验证所述第一漫游许可证书是否由所述第一证书颁发节点颁发，根据所述第一漫游许可证书中的所述第二证书颁发节点的公钥验证所述第二认证证书是否由所述第二证书颁发节点颁发；

在确定所述第一漫游许可证书由所述第一证书颁发节点颁发，且所述第二认证证书由所述第二证书颁发节点颁发的情况下，接入所述移动网络。

本公开实施例的第四方面，提供一种网络认证服务器存储介质，其上存储有计算机程序，该程序被处理器执行时实现第二方面所述方法的步骤。

本公开实施例的第五方面，提供一种用户设备存储介质，其上存储有计算机程序，该程序被处理器执行时实现第三方面所述方法的步骤。

本公开实施例的第六方面，提供一种网络认证服务器，包括：

存储器，其上存储有计算机程序；

处理器，用于执行所述存储器中的所述计算机程序，以实现第二方面所述方法的步骤。

本公开实施例的第七方面，提供一种用户设备，包括：

存储器，其上存储有计算机程序；

处理器，用于执行所述存储器中的所述计算机程序，以实现第三方面所述方法的步骤。

本公开实施例的第八方面，提供一种计算机程序，包括计算机可读代码，当所述计算机可读代码在计算处理设备上运行时，导致所述计算处理设备执行本公开第二方面或者第三方面实施例所提出的方法。

通过上述技术方案，至少可以达到以下有益效果：

通过第一证书颁发节点向第一网络认证服务节点颁发用于表明第一网络认证服务节点的身份的第一认证证书，以及向第一运营商的用户设备颁发用于表明该第一运营商的用户设备的身份的第一 UE 证书，以及将第一 UE 证书撤销信息和表明所述第一证书颁发节点的身份的第一 CA 证书存储到区块链中；并通过第一网络认证服务节点从区块链中获取第一 UE 证书撤销信息以及第一 CA 证书，并在接收到第一运营商的用户设备的第一接入认证消息的情况下，与该第一运营商的用户设备进行双向身份认证，在双向身份认证完成的情况下，接入该第一运营商的用户设备到移动网络。第一运营商的用户设备可以就近进行移动网络接入认证，并且提高了移动网络接入的安全性。此外，可以在私有或隔离部署的移动网络中实现终端设备的接入，提高了移动网络接入的便捷性。

本公开的其他特征和优点将在随后的具体实施方式部分予以详细说明。

附图说明

附图是用来提供对本公开的进一步理解，并且构成说明书的一部分，与下面的具体实施方式一起用于解释本公开，但并不构成对本公开的限制。在附图中：

图 1 是根据一示例性实施例示出的一种移动网络接入系统的框图。

图 2 是根据一示例性实施例示出的另一种移动网络接入系统的框图。

图 3 是根据一示例性实施例示出的一种移动网络的接入方法的流程图。

图 4 是根据一示例性实施例示出的另一种移动网络的接入方法的流程图。

图 5 是根据一示例性实施例示出的一种移动网络的接入方法的流程图。

图 6 是根据一示例性实施例示出的另一种移动网络的接入方法的流程图。

图 7 是根据一示例性实施例示出的一种电子设备 700 的框图。

图 8 是根据一示例性实施例示出的一种电子设备 1900 的框图。

图 9 为本公开实施例提供了一种计算处理设备的结构示意图。

图10为本公开实施例提供了一种用于便携式或者固定实现根据本公开的方法的程序代码的存储单元的示意图。

具体实施方式

以下结合附图对本公开的具体实施方式进行详细说明。应当理解的是，此处所描述的具体实施方式仅用于说明和解释本公开，并不用于限制本公开。

需要说明的是，在本公开中，说明书和权利要求书以及附图中的术语“第一”、“第二”等是用于区别类似的对象，而不必理解为描述特定的顺序或先后次序。同理，术语“S301”、“S401”等用于区别步骤，而不必理解为按照特定的顺序或先后次序执行方法步骤。

在介绍本公开提供的移动网络接入系统、方法、存储介质及电子设备之前，首先对本公开的应用场景进行介绍。本公开提供的移动网络接入系统可以允许用户设备在通过EAP-TLS 认证协议完成认证后接入运营商的移动网络，其中，用户设备例如可以是智能手机，智能手表，智能手环等具备移动通讯功能的电子设备。

发明人发现，相关技术在接入认证时，虽然采用了非对称密钥，但是，若用户设备非法获得了鉴权服务器的公钥，则可以非法接入移动网络，移动网络接入的安全性同样较低。并且，相关技术中，UE 只能支持对应移动网络的接入，无法在不同的运营商的移动网络之间漫游，因而，在 UE 处于没有对应的运营商的移动网络的情况下，即使 UE 所处地区存在其他运营商的移动网络，UE 也无法接入该移动网络，也会导致 UE 接入移动网络不便捷。

为解决上述技术问题，本公开提供一种移动网络接入系统。图 1 是根据一示例性实施例示出的一种移动网络接入系统的框图，该系统 100 用于执行移动网络接入。如图 1 所示，所述系统 100 包括：处于区块链网络中的第一网络认证服务节点 110、第一证书颁发节点 120，其中，第一网络认证服务节点 110 以及第一证书颁发节点 120 属于第一运营商。

其中，第一证书颁发节点 120 用于向第一网络认证服务节点 110 颁发用于表明第一网络认证服务节点 110 的身份的第一认证证书，以及向第一运营商的用户设备颁发用于表明该用户设备的身份的第一 UE 证书，以及将第一 UE 证书撤销信息和表明所述第一证书颁发节点的身份的第一 CA 证书存储到区块链中；

第一网络认证服务节点 110 用于从区块链中获取第一 UE 证书撤销信息以及第一 CA 证书，并在接收到第一运营商的用户设备的第一接入认证消息的情况下，与该用户设备进行双向身份认证，在双向身份认证完成的情况下，接入该用户设备到所述移动网络。

第一网络认证服务节点 110 可以是 AUSF（(Authentication Server Function，鉴权服务器功能），第一网络认证服务节点 110 与区块链的任一区块链节点通信连接，并可以从区块链获取第一 UE 证书撤销信息以及第一 CA 证书。

可选地，第一网络认证服务节点 110 可以通过 EAP-TLS 的认证协议与第一运营商的用户设备进行双向身份认证。第一运营商的用户设备可以优先与距离最近的第一网络认证服务节点 110 建立通信，进而与其进行双向身份认证。

可选地，第一证书颁发节点 120 还用于颁发第一 UE 证书撤销信息，第一 UE 证书撤销信息用于表征相应的第一 UE 证书失效。

可选地，第一 CA 证书以及第一证书颁发节点 120 向用户设备颁发的第一 UE 证书预置在该用户设备的身份识别卡中。具体地，该身份识别卡可以是 USIM 卡，USIM 卡在出厂时存储由第一证书颁发节点 120 颁发的第一 UE 证书。进一步地，在该 USIM 卡安装到用户设备后，用户设备可以基于该第一 UE 证书生成私钥。该身份识别卡也可以是 eSIM 卡，在用户选择运营商套餐后，用户设备可以基于该第一 UE 证书生成私钥。

可选地，第一网络认证服务节点 110 和第一证书颁发节点 120 可以作为区块链网络的一个节点。

可选地，第一证书颁发节点 120 向第一网络认证服务节点 110 颁发的第一认证证书预置在第一网络认证服务节点 110 中或者存储在所述区块链中。

示例地，第一证书颁发节点 120 将表明自身身份的第一 CA 证书存储到区块链，可选地，也可以将该第一 CA 证书存储到任意第一网络认证服务节点 110。并且，第一证书颁发节点 120 颁发表明第一运营商的用户设备的身份的第一 UE 证书，其中，第一 UE 证书与第一 CA 证书相对应。这样，在第一运营商的用户设备通过 EAP-TLS 的认证协议与第一网络认证服务节点 110 进行接入认证时，可以将第一 UE 证书与第一 CA 证书进行匹配。

进一步地，第一运营商可以通过第一证书颁发节点 120 颁发第一 UE 证书撤销信息，这样，区块链或者第一网络认证服务节点 110 可以基于多个第一 UE 证书撤销信息可以构成撤销列表，在接收到第一运营商的用户设备的第一接入认证信息的情况下，第一网络认证服务节点 110 可以通过撤销列表确定该第一运营商的用户设备是否被取消接入资格。

若第一网络认证服务节点 110 在确定撤销列表中存在该第一运营商的用户设备的第一 UE 证书撤销信息的情况下，生成用户设备撤销信息，并向该用户设备反馈该用户设备撤销信息。这样，便于用户及时了解到该用户设备的第一 UE 证书被撤销。

进一步地，第一网络认证服务节点 110 在确定撤销列表中不存在该第一运营商的用

户设备的第一 UE 证书撤销信息，且第一 UE 证书与第一 CA 证书相互匹配的情况下，接入该用户设备到所述移动网络。

通过第一证书颁发节点向第一网络认证服务节点颁发用于表明第一网络认证服务节点的身份的第一认证证书，以及向第一运营商的用户设备颁发用于表明该用户设备的身份的第一 UE 证书，以及将第一 UE 证书撤销信息和表明所述第一证书颁发节点的身份的第一 CA 证书存储到区块链中；并通过第一网络认证服务节点从区块链中获取第一 UE 证书撤销信息以及第一 CA 证书，并在接收到第一运营商的用户设备的第一接入认证消息的情况下，与该用户设备进行双向身份认证，在双向身份认证完成的情况下，接入该用户设备到所述移动网络。第一运营商的用户设备可以就近进行移动网络接入认证，并且提高了移动网络接入的安全性。此外，可以在私有或隔离部署的移动网络中实现终端设备的接入，提高了移动网络接入的便捷性。

可选地，参考图 2 是所示的另一种移动网络接入系统的框图，如图 2 所示，所述系统 100 还包括处于区块链网络中的第二网络认证服务节点 130 以及第二证书颁发节点 140，第二网络认证服务节点 130 以及第二证书颁发节点 140 属于第二运营商；

第一证书颁发节点 120 还用于，将为第二证书颁发节点 140 颁发的第一漫游许可证书写入区块链；

第二证书颁发节点 140 用于向第二网络认证服务节点 130 颁发用于表明第二网络认证服务节点 130 的身份的第二认证证书，以及向第二运营商的用户设备颁发用于表明该用户设备的身份的第二 UE 证书，以及将第二 UE 证书撤销信息和表明第二证书颁发节点 140 的身份的第二 CA 证书存储到区块链中，以及将为第一证书颁发节点 120 颁发的第二漫游许可证书写入区块链。

可选地，第一网络认证服务节点 110、第一证书颁发节点 120 第二网络认证服务节点 130 和第二证书颁发节点 140 可以作为区块链网络的一个节点。

具体实施时，第一运营商和第二运营商需要达成漫游协议，并且第一运营商通过第一证书颁发节点 120 为第二证书颁发节点 140 颁发的第一漫游许可证书，并且第二运营商通过第二证书颁发节点 140 为第一证书颁发节点 120 颁发的第二漫游许可证书。第一证书颁发节点 120 将第一漫游许可证书上传到区块链存储，第二证书颁发节点 140 将第二漫游许可证书上传到区块链存储。

进一步地，第二证书颁发节点 140 颁发表明第二证书颁发节点 140 的身份的第二 CA

证书，用户设备的 USIM 卡内预置有第一证书颁发节点 120 颁发的第一 UE 证书以及第二证书颁发节点 140 颁发的第二 UE 证书。

进一步地，第一证书颁发节点 120 将颁发的第一 UE 证书撤销信息写入到区块链网络中，第二证书颁发节点 140 将颁发的第二 UE 证书撤销信息也写入到区块链网络中，进而在区块链网络中根据多个第一UE证书撤销信息和多个第二UE证书撤销信息构建成撤销列表。进而，在任意网络认证服务节点接收到任意用户设备发送的接入认证信息的情况下，相应的网络认证服务节点可以从区块链的撤销列表中确定是否存在相应的 UE 证书撤销信息，从而确定该用户设备的第一 UE 证书或者第二 UE 证书是否被撤销。

值得说明的是，本公开实施例的系统并不局限于第 5 代移动通信网络，在其他采用类似基于证书的认证接入方式的场景，均可采用此系统，以实现单一服务主体或跨服务主体的接入认证。

采用上述系统，可以实现 UE 在不同运营商的移动网络的漫游就近接入，在弥补基于 EAP-TLS 认证方式下不支持 UE 在不同运营商的移动网络漫游的缺陷的同时，也避免了接入认证必须到 UE 归属地进行认证带来的不便以及资源开销，提高了终端设备接入移动网络的便捷性。

基于相同的发明构思，本公开还提供一种移动网络的接入方法，所述方法应用于移动网络接入系统中的第一网络认证服务节点，图 3 是根据一示例性实施例示出的一种移动网络的接入方法的流程图。参照图 3，所述方法包括以下步骤：

在步骤 S301 中，接收第一运营商的用户设备发送的第一接入认证信息。

其中，所述第一接入认证信息包括所述第一 UE 证书；

在步骤 S302 中，从区块链中获取第一 UE 证书撤销信息以及第一 CA 证书。

在步骤 S303 中，根据第一 CA 证书中的公钥验证第一 UE 证书是否由第一证书颁发节点颁发，并根据第一 UE 证书撤销信息确定第一 UE 证书是否被撤销。

在步骤 S304 中，在确定第一 UE 证书由第一证书颁发节点颁发，且第一 UE 证书未被撤销的情况下，向第一运营商的用户设备发送第二接入认证消息。

其中，第二接入认证消息包括第一认证证书，第一认证证书用于第一运营商的用户设备对第一网络认证服务节点进行身份认证，并在身份认证通过的情况下，接入第一运营商的用户设备到移动网络。

具体实施时，第一网络认证服务节点从第一接入认证信息中提取第一 UE 证书，进

而基于第一UE证书查找区块链的撤销列表中是否存在该第一运营商的用户设备的UE证书撤销信息。

可选地，第一网络认证服务节点在确定区块链的撤销列表中存在该第一运营商的用户设备的 UE 证书撤销信息的情况下，确定该第一运营商的用户设备已被撤销，进而生成相应的用户设备撤销信息，并向该用户设备反馈该用户设备撤销信息。这样，便于用户及时了解到该用户设备的第一 UE 证书被撤销，该用户设备无法接入到移动网络。

进一步地，第一网络认证服务节点在确定区块链的撤销列表中不存在该第一运营商的 UE 证书撤销信息的情况下，确定该第一运营商的用户设备未被撤销。

进一步地，第一网络认证服务节点在确定该第一运营商的用户设备未被撤销的情况下，从第一 CA 证书中获取公钥，并根据该公钥验证第一 UE 证书是否由第一证书颁发节点颁发。例如，可以根据该公钥验证第一 UE 证书的私钥，若该公钥与私钥相匹配，则确定第一 UE 证书由第一证书颁发节点颁发。

进一步地，第一网络认证服务节点在确定第一 UE 证书由第一证书颁发节点颁发的情况下，生成第二接入认证消息，并向第一运营商的用户设备发送该第二接入认证消息，以便于第一运营商的用户设备根据第一认证证书的私钥验证第一网络认证服务节点的身份。从而实现第一网络认证服务节点对第一运营商的用户设备的身份认证。这样，可以提高移动网络接入的安全性和便捷性。

可选地，图 4 是根据一示例性实施例示出的另一种移动网络的接入方法的流程图。参照图 4，所述方法还包括以下步骤：

在步骤 S401 中，接收第二运营商的用户设备发送的第三接入认证信息。

其中，所述第三接入认证信息包括所述第二 UE 证书。

在步骤 S402 中，从区块链中获取第一 CA 证书、第一漫游许可证书、以及第二漫游许可证书。

在步骤 S403 中，在获取到第一 CA 证书、第二 UE 证书、第一漫游许可证书以及第二漫游许可证书的情况下，根据第一 CA 证书中的公钥验证第一漫游许可证书是否由第一证书颁发节点颁发，根据第二漫游许可证书中的第二证书颁发节点的公钥验证第二 UE 证书是否由第二证书颁发节点颁发。

在步骤 S404 中，在确定第一漫游许可证书由第一证书颁发节点颁发，且第二 UE 证书由第二证书颁发节点颁发的情况下，向第二运营商的用户设备发送第四接入认证消息。

其中，第四接入认证消息包括第一认证证书以及第一漫游许可证书，第一认证证书以及第一漫游许可证书用于第二运营商的用户设备对第一网络认证服务节点进行身份认证，在身份认证通过的情况下，接入第二运营商的用户设备到移动网络。

具体实施时，在第二运营商的用户设备的身份识别卡预置有第一证书颁发节点颁发的第一 UE 证书以及第二证书颁发节点颁发的第二 UE 证书。示例地，在 USIM 卡安装到第二运营商的用户设备后，第二运营商的用户设备可以基于该第一 UE 证书生成第一私钥，基于该第二 UE 证书生成第二私钥。第二运营商的用户设备基于 EAP-TLS 的认证协议向第一运营商的第一网络认证服务节点发送第三接入认证信息，第一网络认证服务节点在接收到该第三接入认证信息时，从第三接入认证信息中提取第二 UE 证书。

进一步地，在提取到第二 UE 证书的情况下，从区块链中获取第一 CA 证书、第一漫游许可证书、以及第二漫游许可证书，进而根据第一 CA 证书中的公钥验证第一漫游许可证书是否由第一证书颁发节点颁发，根据第二漫游许可证书中的第二证书颁发节点的公钥验证第二 UE 证书是否由第二证书颁发节点颁发。

例如，可以根据第一 CA 证书中的公钥验证第一漫游许可证书的私钥，若该公钥与私钥相匹配，则确定第一漫游许可证书由第一证书颁发节点颁发，并可以根据第二漫游许可证书中的第二证书颁发节点的公钥验证第二 UE 证书的私钥，若该公钥与私钥相匹配，则确定第二 UE 证书由第二证书颁发节点颁发。

进一步地，第一网络认证服务节点生成第四接入认证消息，并将该第四接入认证消息发送到第二运营商的用户设备，以便于第二运营商的用户设备根据第一认证证书的私钥以及第一漫游许可证书的私钥，验证第一网络认证服务节点的身份。

进一步地，在确定第一漫游许可证书不是由第一证书颁发节点颁发的情况下，即第一 CA 证书中的公钥与第一漫游许可证书的私钥不匹配，或者第二 UE 证书不是由第二证书颁发节点颁发的情况下，即第二漫游许可证书中的第二证书颁发节点的公钥与第二 UE 证书的私钥不匹配，第一网络认证服务节点生成非法接入信息，并向第二运营商的用户设备发送该非法接入信息，以便用户及时了解接入认证失败的信息。

值得说明的是，第一运营商的用户设备也可以在身份识别卡预置有第一证书颁发节点颁发的第一 UE 证书以及第二证书颁发节点颁发的第二 UE 证书，进而可以向第二运营商的第二网络认证服务节点发送接入认证消息，进而将第一运营商的用户设备漫游到第二运营商的移动网络中。

采用上述技术方案，可以将第二运营商的用户设备漫游接入第一运营商的移动网络中，从而增加了实现 UE 在不同运营商的移动网络的漫游就近接入，提高了终端设备接入移动网络的便捷性。

基于相同的发明构思，本公开还提供一种移动网络的接入方法，所述方法应用于第一运营商的用户设备，图 5 是根据一示例性实施例示出的一种移动网络的接入方法的流程图。参照图 5，所述方法包括以下步骤：

在步骤 S501 中，向第一网络认证服务节点发送第一接入认证信息。

其中，第一网络认证服务节点为移动网络接入系统 100 中的第一网络认证服务节点 110，第一接入认证信息包括第一 UE 证书。

在步骤 S502 中，接收第一网络认证服务节点发送的第二接入认证消息，第二接入认证消息包括所述第一认证证书。

在步骤 S503 中，根据预置的第一 CA 证书中的公钥验证第一认证证书是否由第一颁发节点颁发。

在步骤 S504 中，在确定第一认证证书由第一颁发节点颁发的情况下，接入移动网络。

示例地，在用户设备装入 USIM 卡后，或者在用户设备在移动网络断开连接后，重新接入移动网络的情况下，第一运营商的用户设备向第一网络认证服务节点发送第一接入认证信息。

进一步地，在接收到第一网络认证服务节点发送的第二接入认证消息的情况下，从第二接入认证消息中提取第一认证证书，并对第一认证证书进行验证。例如，根据预置的第一 CA 证书中的公钥验证第一认证证书的私钥，在第一 CA 证书中的公钥与第一认证证书的私钥相互匹配的情况下，确定第一认证证书由第一颁发节点颁发。进而完成第一运营商的用户设备对第一网络认证服务节点的身份认证。进而将第一运营商的用户设备接入第一运营商的移动网络中。

进一步地，在确定第一认证证书不是由第一颁发节点颁发的情况下，不将第一运营商的用户设备接入第一运营商的移动网络。这样可以提高移动网络接入的安全性和便捷性。

可选地，图 6 是根据一示例性实施例示出的另一种移动网络的接入方法的流程图。参照图 6，所述方法还包括以下步骤：

在步骤 S601 中，向第二网络认证服务节点发送第五接入认证信息。

其中，第二网络认证服务节点为移动网络接入系统 100 中的第二网络认证服务节点 130，第五接入认证信息包括第二 UE 证书。

在步骤 S602 中，接收第二网络认证服务节点发送的第六接入认证消息，第六接入认证消息包括第二认证证书以及第一漫游许可证书。

在步骤 S603 中，根据预置的第一 CA 证书中的公钥验证第一漫游许可证书是否由第一证书颁发节点颁发，根据第一漫游许可证书中的第二证书颁发节点的公钥验证第二认证证书是否由第二证书颁发节点颁发。

在步骤 S604 中，在确定第一漫游许可证书由第一证书颁发节点颁发，且第二认证证书由第二证书颁发节点颁发的情况下，接入移动网络。

具体实施时，第一运营商的用户设备可以在 USIM 卡预置有第一证书颁发节点颁发的第一 UE 证书以及第二证书颁发节点颁发的第二 UE 证书，在确定第一运营商的用户设备需要漫游接入第二运营商的移动网络的情况下，基于第二 UE 证书生成第五接入认证信息，并向第二网络认证服务节点发送第五接入认证信息。

进一步地，在接收到第六接入认证消息的情况下，从第六接入认证消息中提取第二认证证书以及第一漫游许可证书，并根据预置的第一 CA 证书中的公钥验证第一漫游许可证书的私钥，在确定第一 CA 证书中的公钥与第一漫游许可证书的私钥相互匹配的情况下，确定第一漫游许可证书由第一证书颁发节点颁发。

进一步地，根据第一漫游许可证书中的第二证书颁发节点的公钥验证第二认证证书的私钥，在确定第一漫游许可证书中的第二证书颁发节点的公钥与第二认证证书的私钥相互匹配的情况下，确定第二认证证书由第二证书颁发节点颁发。

进一步地，在确定第一漫游许可证书不是由第一证书颁发节点颁发，或者在确定第二认证证书不是由第二证书颁发节点颁发的情况下，不将第一运营商的用户设备接入第二运营商的移动网络。

值得说明的是，第二运营商的用户设备也可以采用相同的方法漫游接入第一运营商的移动网络中。此处不再赘述。

采用上述技术方案，第一运营商的用户设备可以向第二运营商的第二网络认证服务节点发送接入认证消息，进而将第一运营商的用户设备漫游到第二运营商的移动网络中，提高了接入移动网络的便捷性。

基于相同的发明构思，本公开实施例还提供一种电子设备 700，图 7 是根据一示例性

实施例示出的一种电子设备 700 的框图。可选地，该电子设备 700 可以被提供为一上述的用户设备，如图 7 所示，该电子设备 700 可以包括：处理器 701，存储器 702。该电子设备 700 还可以包括多媒体组件 703，输入/输出（I/O）接口 704，以及通信组件 705 中的一者或多者。

其中，处理器 701 用于控制该电子设备 700 的整体操作，以完成上述的用户设备侧的移动网络的接入方法中的全部或部分步骤。存储器 702 用于存储各种类型的数据以支持在该电子设备 700 的操作，这些数据例如可以包括用于在该电子设备 700 上操作的任何应用程序或方法的指令，以及应用程序相关的数据，例如联系人数据、收发的消息、图片、音频、视频等等。该存储器 702 可以由任何类型的易失性或非易失性存储设备或者它们的组合实现，例如静态随机存取存储器（Static Random Access Memory，简称 SRAM），电可擦除可编程只读存储器（Electrically Erasable Programmable Read-Only Memory，简称 EEPROM），可擦除可编程只读存储器（Erasable Programmable Read-Only Memory，简称 EPROM），可编程只读存储器（Programmable Read-Only Memory，简称 PROM），只读存储器（Read-Only Memory，简称 ROM），磁存储器，快闪存储器，磁盘或光盘。多媒体组件 703 可以包括屏幕和音频组件。其中屏幕例如可以是触摸屏，音频组件用于输出和/或输入音频信号。例如，音频组件可以包括一个麦克风，麦克风用于接收外部音频信号。所接收的音频信号可以被进一步存储在存储器 702 或通过通信组件 705 发送。音频组件还包括至少一个扬声器，用于输出音频信号。I/O 接口 704 为处理器 701 和其他接口模块之间提供接口，上述其他接口模块可以是键盘，鼠标，按钮等。这些按钮可以是虚拟按钮或者实体按钮。通信组件 705 用于该电子设备 700 与其他设备之间进行有线或无线通信。无线通信，例如 Wi-Fi，蓝牙，近场通信（Near Field Communication，简称 NFC），2G、3G、4G、NB-IOT、eMTC、或其他 5G 等等，或它们中的一种或几种的组合，在此不做限定。因此相应的该通信组件 705 可以包括：Wi-Fi 模块，蓝牙模块，NFC 模块等等。

在一示例性实施例中，电子设备 700 可以被一个或多个应用专用集成电路（Application Specific Integrated Circuit，简称 ASIC）、数字信号处理器（Digital Signal Processor，简称 DSP）、数字信号处理设备（Digital Signal Processing Device，简称 DSPD）、可编程逻辑器件（Programmable Logic Device，简称 PLD）、现场可编程门阵列（Field Programmable Gate Array，简称 FPGA）、控制器、微控制器、微处理器或其他电子元件

实现，用于执行上述的用户设备侧的移动网络的接入方法。

在另一示例性实施例中，还提供了一种包括程序指令的计算机可读存储介质，该程序指令被处理器执行时实现上述的用户设备侧的移动网络的接入方法的步骤。例如，该计算机可读存储介质可以为上述包括程序指令的存储器 702，上述程序指令可由电子设备 700 的处理器 701 执行以完成上述的用户设备侧的移动网络的接入方法。

基于相同的发明构思，本公开实施例还提供一种电子设备 1900，图 8 是根据一示例性实施例示出的一种电子设备 1900 的框图。可选地，电子设备 1900 可以被提供为一移动网络接入系统中的第一网络认证服务节点。参照图 8，电子设备 1900 包括处理器 1922，其数量可以为一个或多个，以及存储器 1932，用于存储可由处理器 1922 执行的计算机程序。存储器 1932 中存储的计算机程序可以包括一个或一个以上的每一个对应于一组指令的模块。此外，处理器 1922 可以被配置为执行该计算机程序，以执行上述的第一网络认证服务节点侧的移动网络的接入方法。

另外，电子设备 1900 还可以包括电源组件 1926 和通信组件 1950，该电源组件 1926 可以被配置为执行电子设备 1900 的电源管理，该通信组件 1950 可以被配置为实现电子设备 1900 的通信，例如，有线或无线通信。此外，该电子设备 1900 还可以包括输入/输出（I/O）接口 1958。电子设备 1900 可以操作基于存储在存储器 1932 的操作系统，例如 Windows ServerTM，Mac OS XTM，UnixTM，LinuxTM 等等。

在另一示例性实施例中，还提供了一种包括程序指令的计算机可读存储介质，该程序指令被处理器执行时实现上述的第一网络认证服务节点侧的移动网络的接入方法的步骤。例如，该计算机可读存储介质可以为上述包括程序指令的存储器 1932，上述程序指令可由电子设备 1900 的处理器 1922 执行以完成上述的第一网络认证服务节点侧的移动网络的接入方法。

在另一示例性实施例中，还提供一种计算机程序产品，该计算机程序产品包含能够由可编程的装置执行的计算机程序，该计算机程序具有当由该可编程的装置执行时用于执行上述的第一网络认证服务节点侧的移动网络的接入方法的代码部分。

为了实现上述实施例，本公开还提出了一种计算处理设备，包括：

存储器，其中存储有计算机可读代码；以及

一个或多个处理器，当所述计算机可读代码被所述一个或多个处理器执行时，所述计算处理设备执行前述的移动网络的接入方法。

为了实现上述实施例，本公开还提出了一种计算机程序，包括计算机可读代码，当所述计算机可读代码在计算处理设备上运行时，导致所述计算处理设备执行前述的移动网络的接入方法。

本公开的前述计算机可读存储介质，其中存储了前述的计算机程序。

图 9 为本公开实施例提供了一种计算处理设备的结构示意图。该计算处理设备通常包括处理器 1110 和以存储器 1130 形式的计算机程序产品或者计算机可读介质。存储器 1130 可以是诸如闪存、EEPROM(电可擦除可编程只读存储器)、EPROM、硬盘或者 ROM 之类的电子存储器。存储器 1130 具有用于执行上述方法中的任何方法步骤的程序代码 1151 的存储空间 1150。例如，用于程序代码的存储空间 1150 可以包括分别用于实现上面的方法中的各种步骤的各个程序代码 1151。这些程序代码可以从一个或者多个计算机程序产品中读出或者写入到这一个或者多个计算机程序产品中。这些计算机程序产品包括诸如硬盘，紧致盘(CD)、存储卡或者软盘之类的程序代码载体。这样的计算机程序产品通常为如图 10 所示的便携式或者固定存储单元。该存储单元可以具有与图 9 的计算处理设备中的存储器 1130 类似布置的存储段、存储空间等。程序代码可以例如以适当形式进行压缩。通常，存储单元包括计算机可读代码 1151’，即可以由例如诸如 1110 之类的处理器读取的代码，这些代码当由服务器运行时，导致该服务器执行上面所描述的方法中的各个步骤。

以上结合附图详细描述了本公开的优选实施方式，但是，本公开并不限于上述实施方式中的具体细节，在本公开的技术构思范围内，可以对本公开的技术方案进行多种简单变型，这些简单变型均属于本公开的保护范围。

另外需要说明的是，在上述具体实施方式中所描述的各个具体技术特征，在不矛盾的情况下，可以通过任何合适的方式进行组合，为了避免不必要的重复，本公开对各种可能的组合方式不再另行说明。

此外，本公开的各种不同的实施方式之间也可以进行任意组合，只要其不违背本公开的思想，其同样应当视为本公开所公开的内容。

实施例

1、一种移动网络接入系统，所述系统包括处于区块链网络中的第一网络认证服务节点、第一证书颁发节点，其中，所述第一网络认证服务节点以及所述第一证书颁发节点属于第一运营商；

所述第一证书颁发节点用于向所述第一网络认证服务节点颁发用于表明所述第一网络认证服务节点的身份的第一认证证书，以及向所述第一运营商的用户设备颁发用于表明该用户设备的身份的第一 UE 证书，以及将第一 UE 证书撤销信息和表明所述第一证书颁发节点的身份的第一 CA 证书存储到区块链中；

所述第一网络认证服务节点用于从所述区块链中获取所述第一 UE 证书撤销信息以及所述第一 CA 证书，并在接收到所述第一运营商的用户设备的第一接入认证消息的情况下，与该用户设备进行双向身份认证，在所述双向身份认证完成的情况下，接入该用户设备到所述移动网络。

2、根据实施例 1 所述的系统，其中，所述系统还包括处于所述区块链网络中的第二网络认证服务节点以及第二证书颁发节点，所述第二网络认证服务节点以及所述第二证书颁发节点属于第二运营商；

所述第一证书颁发节点还用于，将为所述第二证书颁发节点颁发的第一漫游许可证书写入所述区块链；

所述第二证书颁发节点用于向所述第二网络认证服务节点颁发用于表明所述第二网络认证服务节点的身份的第二认证证书，以及向所述第二运营商的用户设备颁发用于表明该用户设备的身份的第二 UE 证书，以及将第二 UE 证书撤销信息和表明所述第二证书颁发节点的身份的第二 CA 证书存储到区块链中，以及将为所述第一证书颁发节点颁发的第二漫游许可证书写入所述区块链。

3、根据实施例 1 或 2 所述的系统，其中，所述第一 CA 证书以及所述第一证书颁发节点向用户设备颁发的所述第一 UE 证书预置在该用户设备的身份识别卡中；

所述第一证书颁发节点向所述第一网络认证服务节点颁发的所述第一认证证书预置在所述第一网络认证服务节点中或者存储在所述区块链中。

4、一种移动网络接入方法，所述方法应用于移动网络接入系统中的第一网络认证服务节点，所述方法包括：

接收所述第一运营商的用户设备发送的第一接入认证信息，其中，所述第一接入认证信息包括所述第一 UE 证书；

从所述区块链中获取所述第一 UE 证书撤销信息以及所述第一 CA 证书；

根据所述第一 CA 证书中的公钥验证所述第一 UE 证书是否由所述第一证书颁发节点颁发，并根据所述第一 UE 证书撤销信息确定所述第一 UE 证书是否被撤销；

在确定所述第一 UE 证书由所述第一证书颁发节点颁发，且所述第一 UE 证书未被撤销的情况下，向所述第一运营商的所述用户设备发送第二接入认证消息，所述第二接入认证消息包括所述第一认证证书，所述第一认证证书用于所述第一运营商的所述用户设备对所述第一网络认证服务节点进行身份认证，并在所述身份认证通过的情况下，接入所述第一运营商的所述用户设备到所述移动网络。

5、根据实施例 4 所述的方法，所述方法应用于实施例 2 中的第一网络认证服务节点，所述方法还包括：

接收所述第二运营商的用户设备发送的第三接入认证信息，其中，所述第三接入认证信息包括所述第二 UE 证书；

从所述区块链中获取所述第一 CA 证书、所述第一漫游许可证书、所述第二漫游许可证书；

在获取到所述第一 CA 证书、所述第二 UE 证书、所述第一漫游许可证书以及所述第二漫游许可证书的情况下，根据所述第一 CA 证书中的公钥验证所述第一漫游许可证书是否由所述第一证书颁发节点颁发，根据所述第二漫游许可证书中的所述第二证书颁发节点的公钥验证所述第二 UE 证书是否由所述第二证书颁发节点颁发；

在确定所述第一漫游许可证书由所述第一证书颁发节点颁发，且所述第二 UE 证书由所述第二证书颁发节点颁发的情况下，向所述第二运营商的所述用户设备发送第四接入认证消息，所述第四接入认证消息包括所述第一认证证书以及所述第一漫游许可证书，所述第一认证证书以及所述第一漫游许可证书用于所述第二运营商的所述用户设备对所述第一网络认证服务节点进行身份认证，在所述身份认证通过的情况下，接入所述第二运营商的所述用户设备到所述移动网络。

6、一种移动网络接入方法，所述方法应用于第一运营商的用户设备，所述方法包括：

向第一网络认证服务节点发送第一接入认证信息，其中，所述第一网络认证服务节点为实施例 1-3 任一项所述的系统中的所述第一网络认证服务节点，所述第一接入认证信息包括所述第一 UE 证书；

接收所述第一网络认证服务节点发送的第二接入认证消息，所述第二接入认证消息包括所述第一认证证书；

根据预置的所述第一 CA 证书中的公钥验证所述第一认证证书是否由所述第一颁发节点颁发；

在确定所述第一认证证书由所述第一颁发节点颁发的情况下，接入所述移动网络。

7、根据实施例 6 所述的方法，所述方法还包括：

向第二网络认证服务节点发送第五接入认证信息，其中，所述第二网络认证服务节点为权利要求 2 所述的系统中的所述第二网络认证服务节点，所述第五接入认证信息包括所述第二 UE 证书；

接收所述第二网络认证服务节点发送的第六接入认证消息，所述第六接入认证消息包括所述第二认证证书以及所述第一漫游许可证书；

根据预置的所述第一 CA 证书中的公钥验证所述第一漫游许可证书是否由所述第一证书颁发节点颁发，根据所述第一漫游许可证书中的所述第二证书颁发节点的公钥验证所述第二认证证书是否由所述第二证书颁发节点颁发；

在确定所述第一漫游许可证书由所述第一证书颁发节点颁发，且所述第二认证证书由所述第二证书颁发节点颁发的情况下，接入所述移动网络。

8、一种网络认证服务器存储介质，其上存储有计算机程序，该程序被处理器执行时实现实施例 4 或 5 中所述移动网络的接入方法的步骤。

9、一种用户设备存储介质，其上存储有计算机程序，该程序被处理器执行时实现实施例 6 或 7 中所述移动网络的接入方法的步骤。

10、一种网络认证服务器，包括：

存储器，其上存储有计算机程序；

处理器，用于执行所述存储器中的所述计算机程序，以实现实施例 4 或 5 中所述移动网络的接入方法的步骤。

11、一种用户设备，包括：

存储器，其上存储有计算机程序；

处理器，用于执行所述存储器中的所述计算机程序，以实现实施例 6 或 7 中所述移动网络的接入方法的步骤。

12、一种计算机程序，包括计算机可读代码，当所述计算机可读代码在计算处理设备上运行时，导致所述计算处理设备执行根据实施例 4 或 5 所述的方法，或者，导致所述计算处理设备执行根据实施例 6 或 7 所述的方法。

权利要求书

1、一种移动网络接入系统，其特征在于，所述系统包括处于区块链网络中的第一网络认证服务节点、第一证书颁发节点，其中，所述第一网络认证服务节点以及所述第一证书颁发节点属于第一运营商；

所述第一证书颁发节点用于向所述第一网络认证服务节点颁发用于表明所述第一网络认证服务节点的身份的第一认证证书，以及向所述第一运营商的用户设备颁发用于表明该第一运营商的用户设备的身份的第一 UE 证书，以及将第一 UE 证书撤销信息和表明所述第一证书颁发节点的身份的第一 CA 证书存储到区块链中；

所述第一网络认证服务节点用于从所述区块链中获取所述第一 UE 证书撤销信息以及所述第一 CA 证书，并在接收到所述第一运营商的用户设备的第一接入认证消息的情况下，与该第一运营商的用户设备进行双向身份认证，在所述双向身份认证完成的情况下，接入该第一运营商的用户设备到所述移动网络。

2、根据权利要求 1 所述的系统，其特征在于，所述系统还包括处于所述区块链网络中的第二网络认证服务节点以及第二证书颁发节点，所述第二网络认证服务节点以及所述第二证书颁发节点属于第二运营商；

所述第一证书颁发节点还用于，将为所述第二证书颁发节点颁发的第一漫游许可证书写入所述区块链；

所述第二证书颁发节点用于向所述第二网络认证服务节点颁发用于表明所述第二网络认证服务节点的身份的第二认证证书，以及向所述第二运营商的用户设备颁发用于表明该第二运营商的用户设备的身份的第二 UE 证书，以及将第二 UE 证书撤销信息和表明所述第二证书颁发节点的身份的第二 CA 证书存储到区块链中，以及将为所述第一证书颁发节点颁发的第二漫游许可证书写入所述区块链。

3、根据权利要求 1 或 2 所述的系统，其特征在于，所述第一 CA 证书以及所述第一证书颁发节点向第一运营商的用户设备颁发的所述第一UE证书预置在该第一运营商的用户设备的身份识别卡中；

所述第一证书颁发节点向所述第一网络认证服务节点颁发的所述第一认证证书预置在所述第一网络认证服务节点中或者存储在所述区块链中。

4、一种移动网络接入方法，其特征在于，所述方法应用于权利要求 1-3 任一项所述的系统中的第一网络认证服务节点，所述方法包括：

接收所述第一运营商的用户设备发送的第一接入认证信息，其中，所述第一接入认证信息包括所述第一 UE 证书；

从所述区块链中获取所述第一 UE 证书撤销信息以及所述第一 CA 证书；

根据所述第一 CA 证书中的公钥验证所述第一 UE 证书是否由所述第一证书颁发节点颁发，并根据所述第一 UE 证书撤销信息确定所述第一 UE 证书是否被撤销；

在确定所述第一 UE 证书由所述第一证书颁发节点颁发，且所述第一 UE 证书未被撤销的情况下，向所述第一运营商的用户设备发送第二接入认证消息，所述第二接入认证消息包括所述第一认证证书，所述第一认证证书用于所述第一运营商的用户设备对所述第一网络认证服务节点进行身份认证，并在所述身份认证通过的情况下，接入所述第一运营商的用户设备到所述移动网络。

5、根据权利要求 4 所述的方法，其特征在于，所述方法应用于权利要求 2 所述的系统中的第一网络认证服务节点，所述方法还包括：

接收所述第二运营商的用户设备发送的第三接入认证信息，其中，所述第三接入认证信息包括所述第二 UE 证书；

从所述区块链中获取所述第一 CA 证书、所述第一漫游许可证书、所述第二漫游许可证书；

在获取到所述第一 CA 证书、所述第二 UE 证书、所述第一漫游许可证书以及所述第二漫游许可证书的情况下，根据所述第一 CA 证书中的公钥验证所述第一漫游许可证书是否由所述第一证书颁发节点颁发，根据所述第二漫游许可证书中的所述第二证书颁发节点的公钥验证所述第二 UE 证书是否由所述第二证书颁发节点颁发；

在确定所述第一漫游许可证书由所述第一证书颁发节点颁发，且所述第二 UE 证书由所述第二证书颁发节点颁发的情况下，向所述第二运营商的用户设备发送第四接入认证消息，所述第四接入认证消息包括所述第一认证证书以及所述第一漫游许可证书，所述第一认证证书以及所述第一漫游许可证书用于所述第二运营商的用户设备对所述第一网络认证服务节点进行身份认证，在所述身份认证通过的情况下，接入所述第二运营商的用户设备到所述移动网络。

6、一种移动网络接入方法，其特征在于，所述方法应用于第一运营商的用户设备，所述方法包括：

向第一网络认证服务节点发送第一接入认证信息，其中，所述第一网络认证服务节

点为权利要求 1-3 任一项所述的系统中的所述第一网络认证服务节点，所述第一接入认证信息包括所述第一 UE 证书；

接收所述第一网络认证服务节点发送的第二接入认证消息，所述第二接入认证消息包括所述第一认证证书；

根据预置的所述第一 CA 证书中的公钥验证所述第一认证证书是否由所述第一颁发节点颁发；

在确定所述第一认证证书由所述第一颁发节点颁发的情况下，接入所述移动网络。

7、根据权利要求 6 所述的方法，其特征在于，所述方法还包括：

向第二网络认证服务节点发送第五接入认证信息，其中，所述第二网络认证服务节点为权利要求 2 所述的系统中的所述第二网络认证服务节点，所述第五接入认证信息包括所述第二 UE 证书；

接收所述第二网络认证服务节点发送的第六接入认证消息，所述第六接入认证消息包括所述第二认证证书以及所述第一漫游许可证书；

根据预置的所述第一 CA 证书中的公钥验证所述第一漫游许可证书是否由所述第一证书颁发节点颁发，根据所述第一漫游许可证书中的所述第二证书颁发节点的公钥验证所述第二认证证书是否由所述第二证书颁发节点颁发；

在确定所述第一漫游许可证书由所述第一证书颁发节点颁发，且所述第二认证证书由所述第二证书颁发节点颁发的情况下，接入所述移动网络。

8、一种网络认证服务器存储介质，其上存储有计算机程序，其特征在于，该程序被处理器执行时实现权利要求 4 或 5 所述方法的步骤。

9、一种用户设备存储介质，其上存储有计算机程序，其特征在于，该程序被处理器执行时实现权利要求 6 或 7 所述方法的步骤。

10、一种网络认证服务器，其特征在于，包括：

存储器，其上存储有计算机程序；

处理器，用于执行所述存储器中的所述计算机程序，以实现权利要求 4 或 5 所述方法的步骤。

11、一种用户设备，其特征在于，包括：

存储器，其上存储有计算机程序；

处理器，用于执行所述存储器中的所述计算机程序，以实现权利要求 6 或 7 所述方

法的步骤。

12、一种计算机程序，包括计算机可读代码，当所述计算机可读代码在计算处理设备上运行时，导致所述计算处理设备执行根据权利要求 4 或 5 所述的方法，或者，导致所述计算处理设备执行根据权利要求 6 或 7 所述的方法。

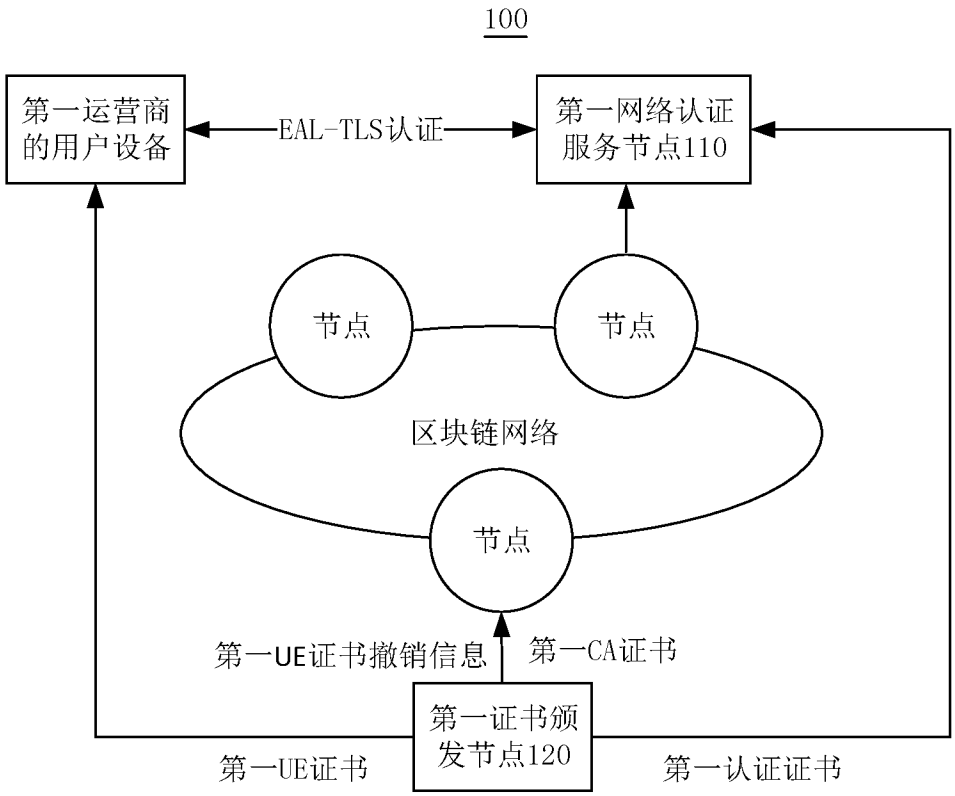

100
第一运营商的用户设备
EAL-TLS认证
第一网络认证服务节点110
节点
节点
区块链网络
节点
第一UE证书撤销信息
第一CA证书
第一证书颁发节点120
第一UE证书
第一认证证书

图 1

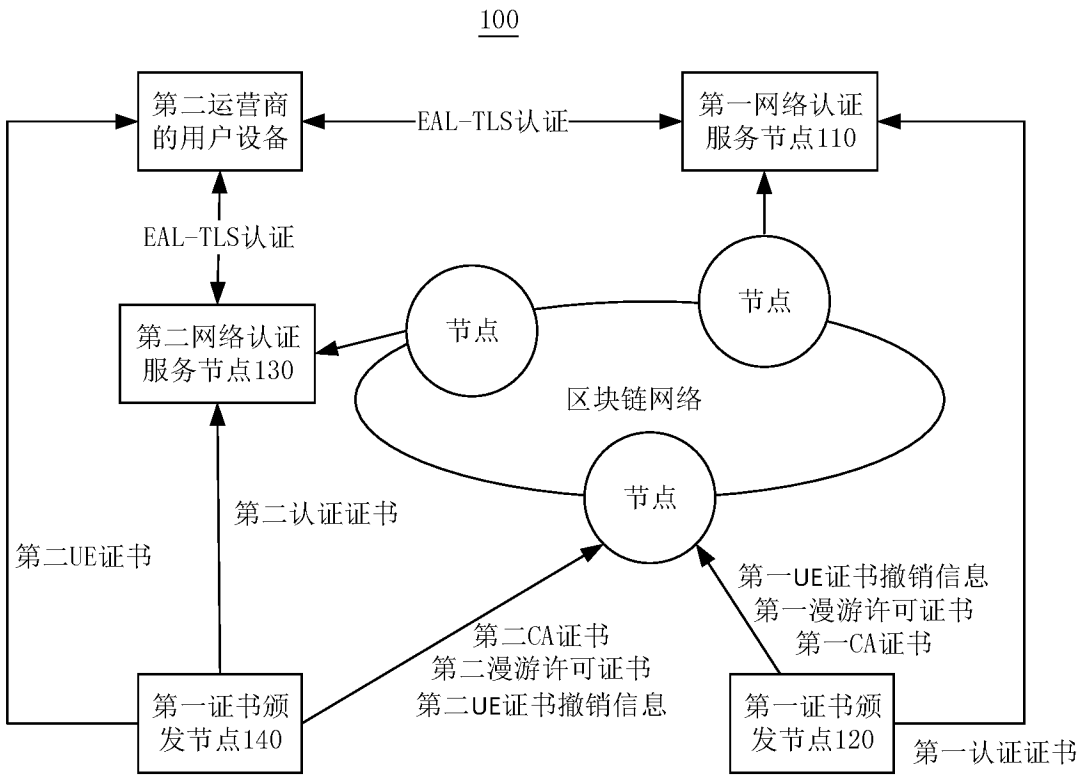

100
第二运营商的用户设备
EAL-TLS认证
第一网络认证服务节点110
EAL-TLS认证
第二网络认证服务节点130
节点
节点
区块链网络
节点
第二认证证书
第二UE证书
第一UE证书撤销信息
第一漫游许可证书
第一CA证书
第二CA证书
第二漫游许可证书
第二UE证书撤销信息
第一证书颁发节点140
第一证书颁发节点120
第一认证证书

图 2

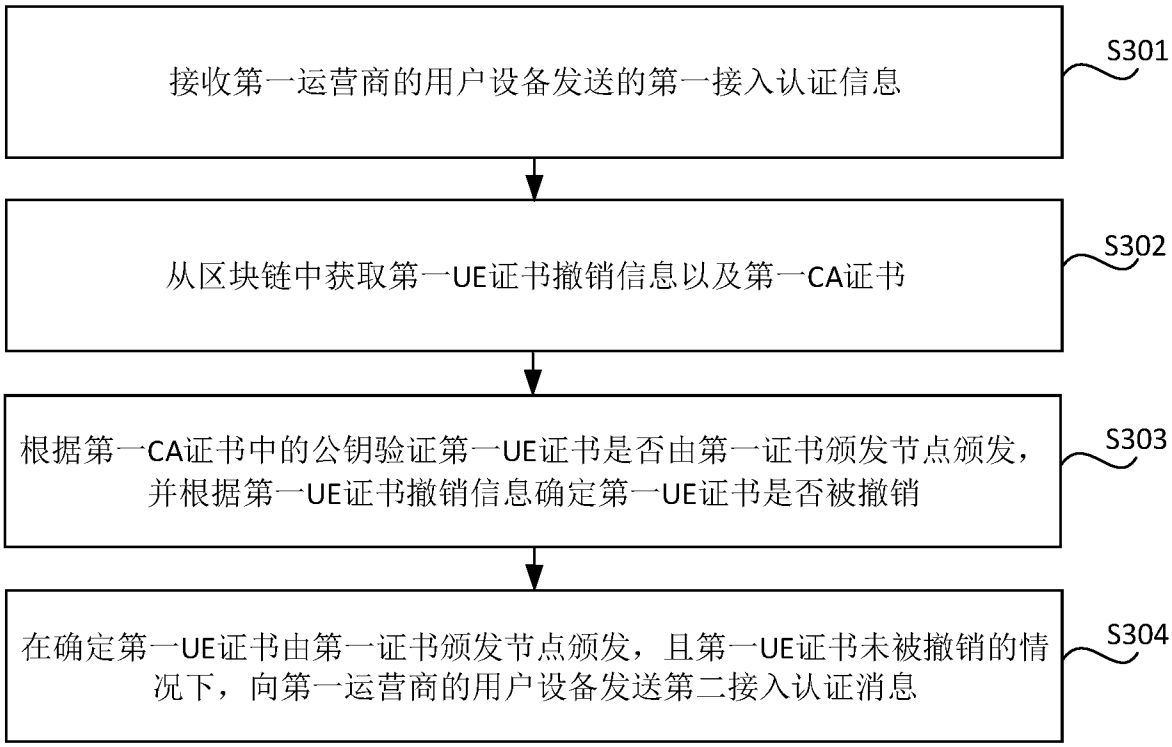

接收第一运营商的用户设备发送的第一接入认证信息
S301
从区块链中获取第一UE证书撤销信息以及第一CA证书
S302
根据第一CA证书中的公钥验证第一UE证书是否由第一证书颁发节点颁发，并根据第一UE证书撤销信息确定第一UE证书是否被撤销
S303
在确定第一UE证书由第一证书颁发节点颁发，且第一UE证书未被撤销的情况下，向第一运营商的用户设备发送第二接入认证消息
S304

图 3

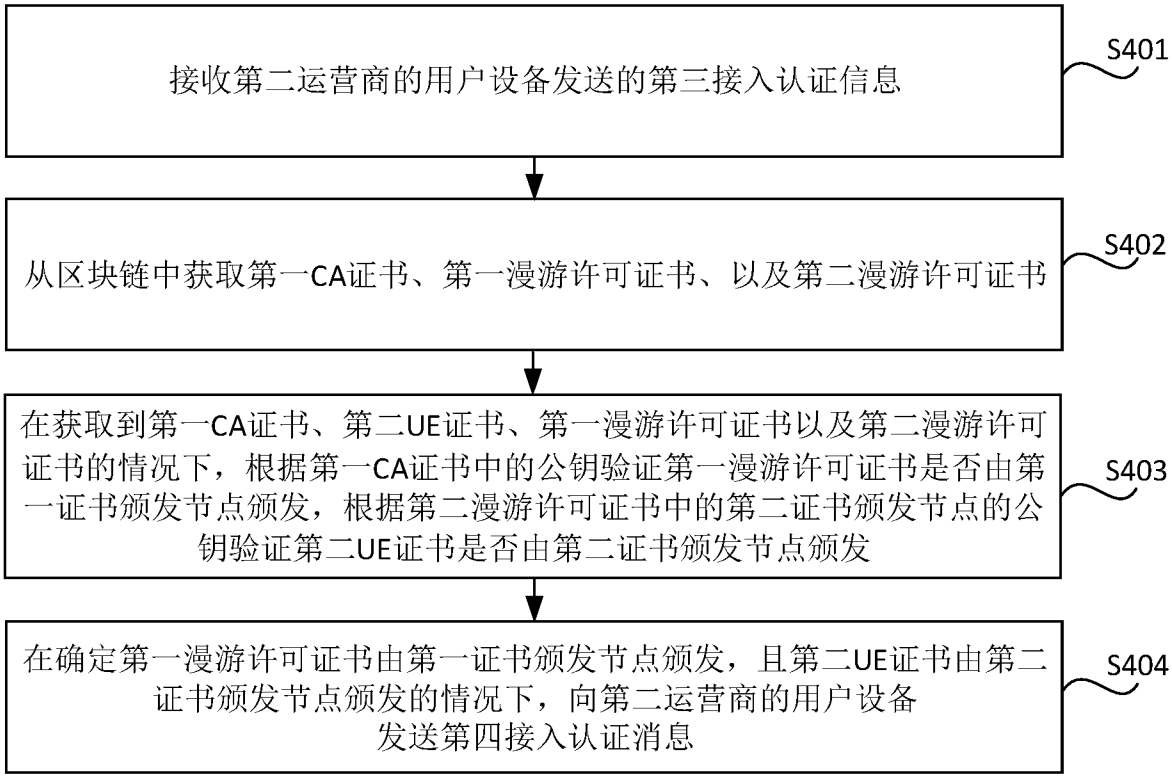

接收第二运营商的用户设备发送的第三接入认证信息
S401
从区块链中获取第一CA证书、第一漫游许可证书、以及第二漫游许可证书
S402
在获取到第一CA证书、第二UE证书、第一漫游许可证书以及第二漫游许可证书的情况下，根据第一CA证书中的公钥验证第一漫游许可证书是否由第一证书颁发节点颁发，根据第二漫游许可证书中的第二证书颁发节点的公钥验证第二UE证书是否由第二证书颁发节点颁发
S403
在确定第一漫游许可证书由第一证书颁发节点颁发，且第二UE证书由第二证书颁发节点颁发的情况下，向第二运营商的用户设备发送第四接入认证消息
S404

图 4

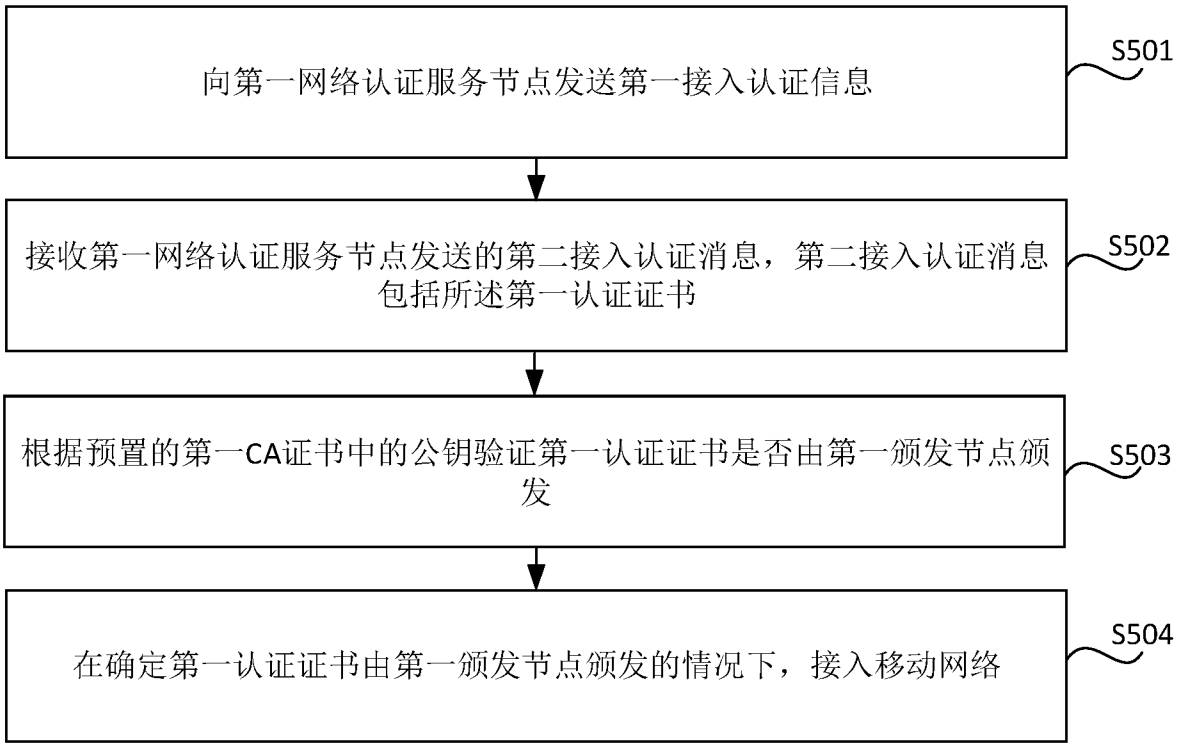

向第一网络认证服务节点发送第一接入认证信息
S501
接收第一网络认证服务节点发送的第二接入认证消息，第二接入认证消息包括所述第一认证证书
S502
根据预置的第一CA证书中的公钥验证第一认证证书是否由第一颁发节点颁发
S503
在确定第一认证证书由第一颁发节点颁发的情况下，接入移动网络
S504

图 5

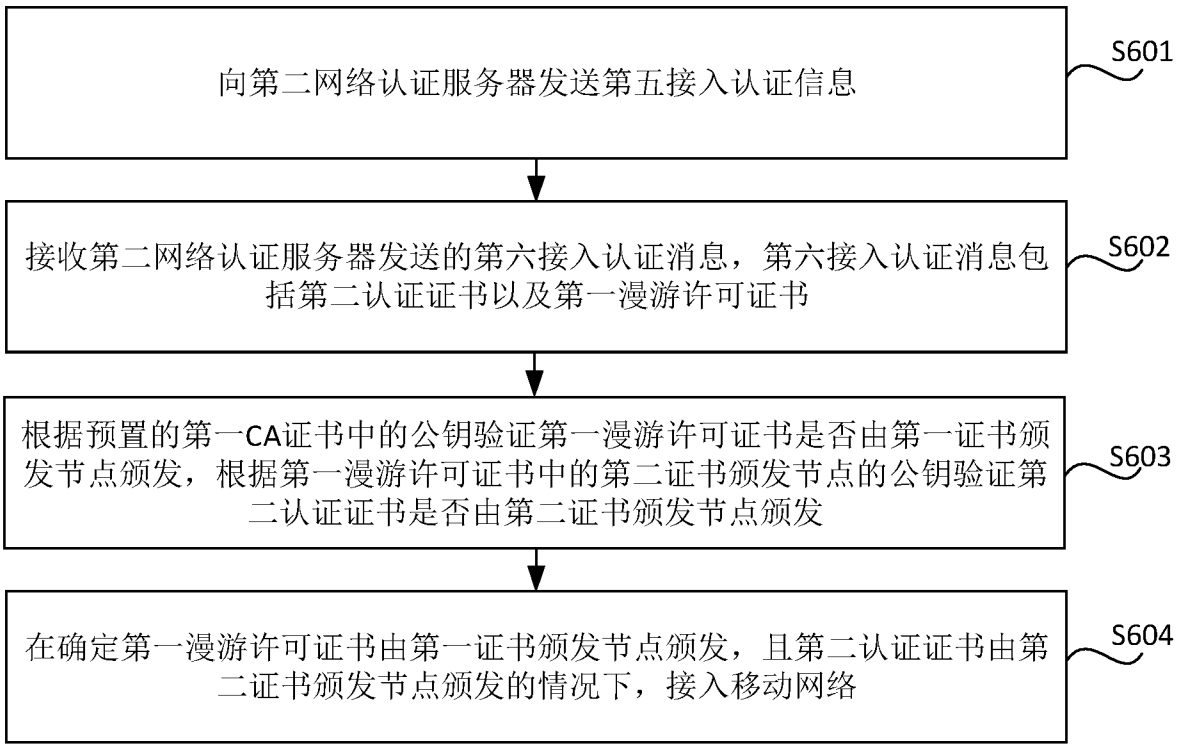

向第二网络认证服务器发送第五接入认证信息
S601
接收第二网络认证服务器发送的第六接入认证消息，第六接入认证消息包括第二认证证书以及第一漫游许可证书
S602
根据预置的第一CA证书中的公钥验证第一漫游许可证书是否由第一证书颁发节点颁发，根据第一漫游许可证书中的第二证书颁发节点的公钥验证第二认证证书是否由第二证书颁发节点颁发
S603
在确定第一漫游许可证书由第一证书颁发节点颁发，且第二认证证书由第二证书颁发节点颁发的情况下，接入移动网络
S604

图 6

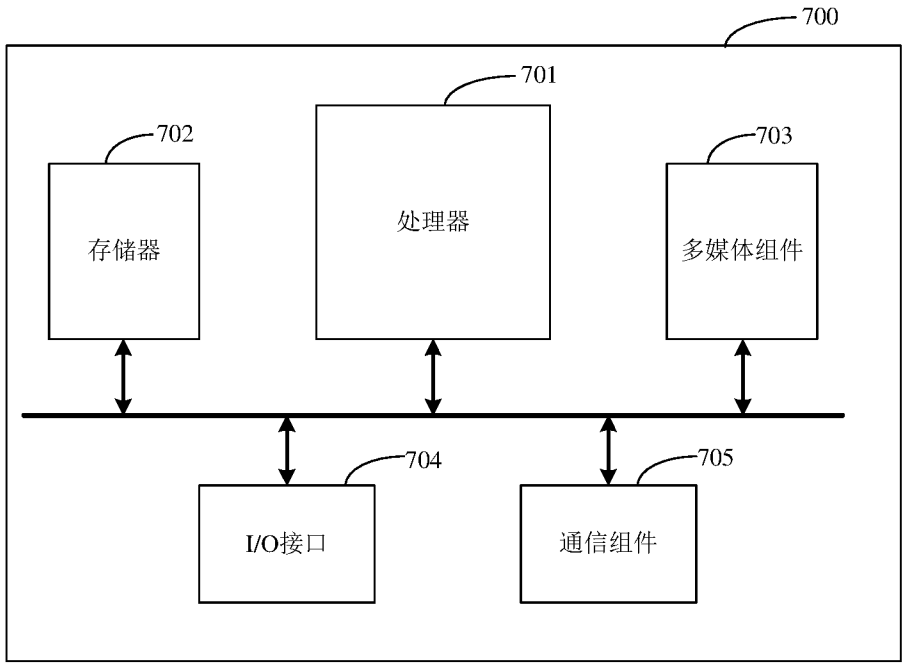

700
701
702
703
处理器
存储器
多媒体组件
704
705
I/O接口
通信组件

图 7

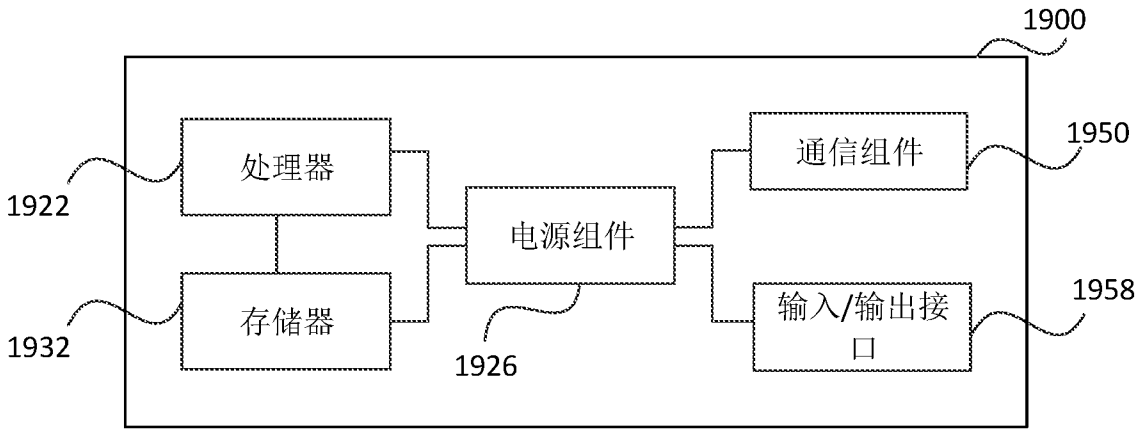

1900
处理器
1922
通信组件
1950
电源组件
存储器
1932
1926
输入/输出接口
1958

图 8

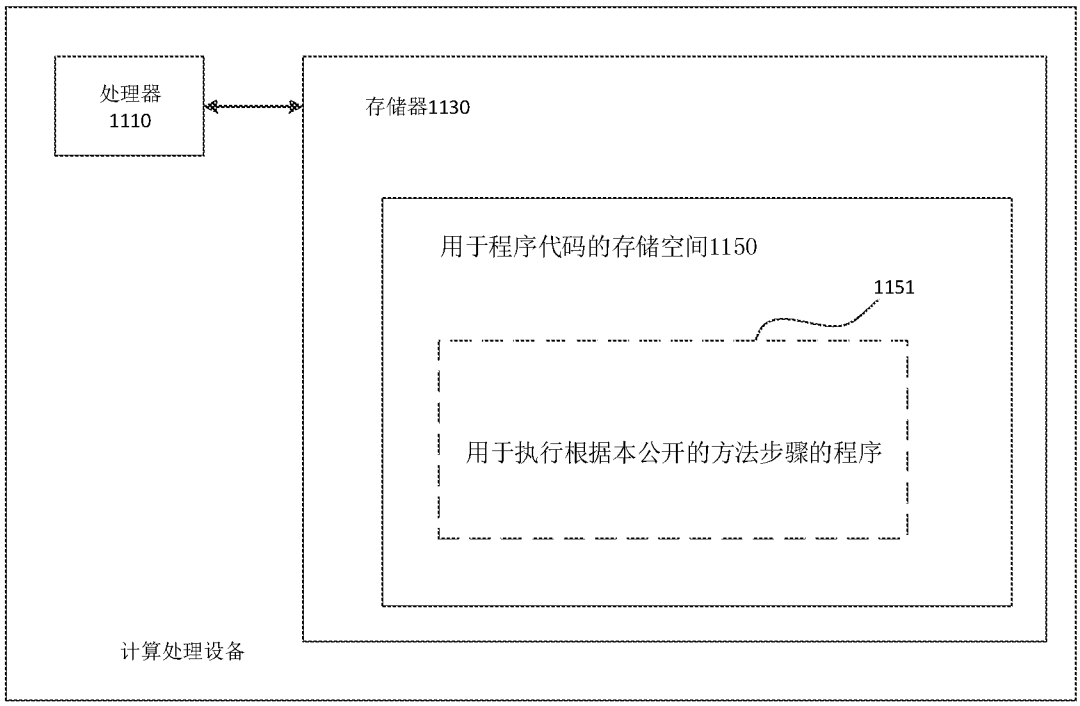

处理器
1110
存储器1130
用于程序代码的存储空间1150
1151
用于执行根据本公开的方法步骤的程序
计算处理设备

图 9

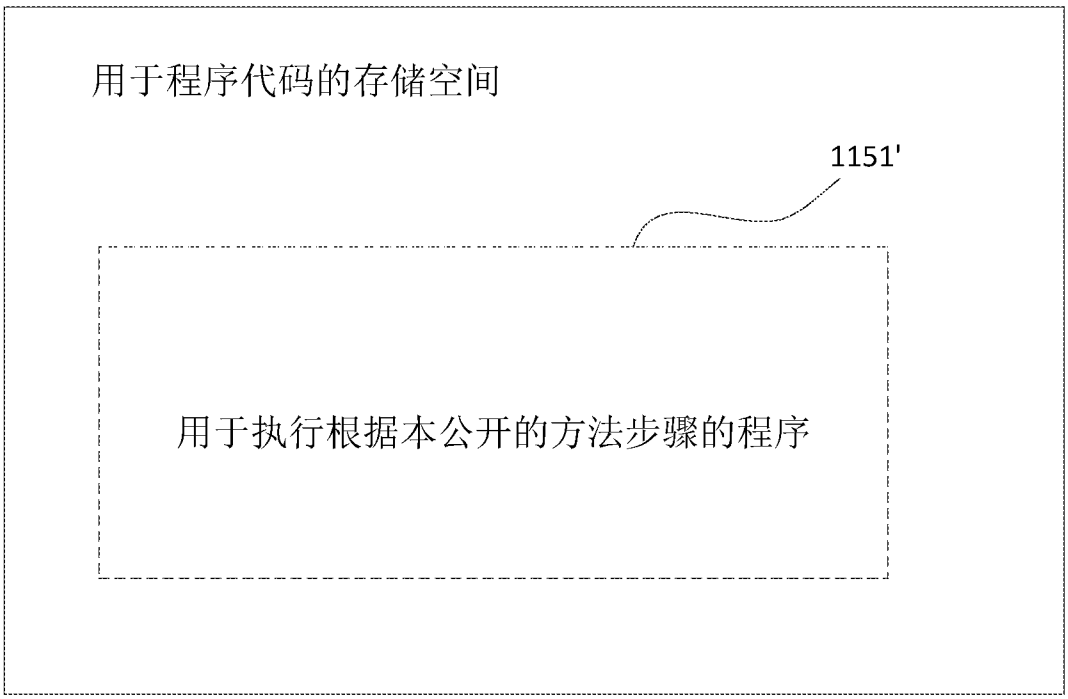

用于程序代码的存储空间
1151'
用于执行根据本公开的方法步骤的程序

图 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/120009

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/069(2021.01)i; H04W 12/08(2021.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W,H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CNPAT, WPI, EPODOC, 3GPP: 接入, 认证, 证书, 许可, 区块链, 双向, 身份, 撤销, 运营商, 漫游, 权威, 公钥, 私钥, access, authenticate, certificate, credential, block chain, bidirection, identity, revocation, operator, roaming, authority, CA, public key, private key, EAP-TLS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 112512048 A (CLOUDMINDS ROBOT CO., LTD.) 16 March 2021 (2021-03-16) claims 1-11, description paragraphs 29-32	1-12
Y	CN 108702622 A (CLOUDMINDS (SHENZHEN) ROBOTICS SYSTEMS CO., LTD.) 23 October 2018 (2018-10-23) description paragraphs 47-114	1, 3, 4, 6, 8-12
Y	CN 107079007 A (QUALCOMM INC.) 18 August 2017 (2017-08-18) description paragraphs 102-155	1, 3, 4, 6, 8-12
A	CN 110572824 A (PLA STRATEGIC SUPPORT FORCE INFORMATION ENGINEERING UNIVERSITY) 13 December 2019 (2019-12-13) entire document	1-12
A	CABLELABS. "Error correction and clarification of Annex O" *3GPP TSG-SA3 Meeting #101e S3-203507,* 20 November 2020 (2020-11-20), entire document	1-12
A	CN 109417709 A (SAMSUNG ELECTRONICS CO., LTD.) 01 March 2019 (2019-03-01) entire document	1-12

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
08 December 2021	**28 December 2021**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/120009

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2020223319 A1 (NIX, John, A.) 05 November 2020 (2020-11-05) entire document	1-12

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2021/120009

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	112512048	A	16 March 2021	None			
CN	108702622	A	23 October 2018	WO	2019104690	A1	06 June 2019
CN	107079007	A	18 August 2017	WO	2016048774	A1	31 March 2016
				US	2016087972	A1	24 March 2016
				EP	3198827	A1	02 August 2017
				JP	2017535989	A	30 November 2017
CN	110572824	A	13 December 2019	None			
CN	109417709	A	01 March 2019	WO	2018008983	A1	11 January 2018
				EP	3466135	A1	10 April 2019
				US	2019261178	A1	22 August 2019
				KR	20190016540	A	18 February 2019
WO	2020223319	A1	05 November 2020	None			

国际检索报告

国际申请号
PCT/CN2021/120009

A. 主题的分类

H04W 12/069(2021.01)i; H04W 12/08(2021.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04W,H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNKI,CNPAT,WPI,EPODOC,3GPP:接入,认证,证书,许可,区块链,双向,身份,撤销,运营商,漫游,权威，公钥，私钥，access，authenticate，certificate，credential，block chain，bidirection，identity，revocation，operator，roaming，authority，CA，public key，private key，EAP-TLS

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 112512048 A (达闼机器人有限公司) 2021年3月16日 (2021-03-16) 权利要求1-11，说明书第29-32段	1-12
Y	CN 108702622 A (深圳前海达闼云端智能科技有限公司) 2018年10月23日 (2018-10-23) 说明书第47-114段	1，3，4，6，8-12
Y	CN 107079007 A (高通股份有限公司) 2017年8月18日 (2017-08-18) 说明书第102-155段	1，3，4，6，8-12
A	CN 110572824 A (中国人民解放军战略支援部队信息工程大学) 2019年12月13日 (2019-12-13) 全文	1-12
A	CABLELABS. "Error correction and clarification of Annex O" 3GPP TSG-SA3 Meeting #101e S3-203507, 2020年11月20日 (2020-11-20), 全文	1-12
A	CN 109417709 A (三星电子株式会社) 2019年3月1日 (2019-03-01) 全文	1-12

☑ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2021年12月8日	2021年12月28日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 董振兴 电话号码 01053961757

国际检索报告

国际申请号
PCT/CN2021/120009

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	WO 2020223319 A1 (NIX, John, A.) 2020年11月5日 (2020-11-05) 全文	1-12

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2021/120009

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	112512048	A	2021年3月16日	无			
CN	108702622	A	2018年10月23日	WO	2019104690	A1	2019年6月6日
CN	107079007	A	2017年8月18日	WO	2016048774	A1	2016年3月31日
				US	2016087972	A1	2016年3月24日
				EP	3198827	A1	2017年8月2日
				JP	2017535989	A	2017年11月30日
CN	110572824	A	2019年12月13日	无			
CN	109417709	A	2019年3月1日	WO	2018008983	A1	2018年1月11日
				EP	3466135	A1	2019年4月10日
				US	2019261178	A1	2019年8月22日
				KR	20190016540	A	2019年2月18日
WO	2020223319	A1	2020年11月5日	无			