(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 107453870 A
(43)申请公布日 2017.12.08

(21)申请号 201710817828.X

(22)申请日 2017.09.12

(71)申请人 京信通信系统(中国)有限公司
地址 510663 广东省广州市科学城神舟路10号
申请人 京信通信系统(广州)有限公司
京信通信技术(广州)有限公司
天津京信通信系统有限公司

(72)发明人 余筱

(74)专利代理机构 北京市立方律师事务所 11330
代理人 刘延喜 王增鑫

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/30(2006.01)
H04L 29/06(2006.01)
G06Q 20/40(2012.01)

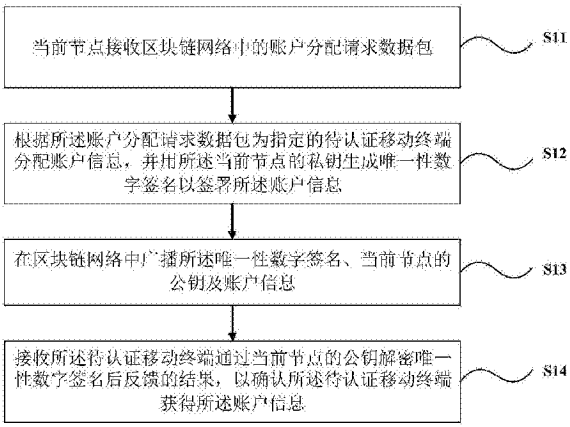
权利要求书4页 说明书18页 附图4页

(54)发明名称

基于区块链的移动终端认证管理方法、装置及相应的移动终端

(57)摘要

本发明提供一种基于区块链的移动终端认证管理方法及装置，所述方法包括如下步骤：当前节点接收区块链网络中的账户分配请求数据包；根据所述账户分配请求数据包为指定的待认证移动终端分配账户信息，并用所述当前节点的私钥生成唯一性多重数字签名以签署所述账户信息；在区块链网络中广播所述唯一性多重数字签名、当前节点的公钥及账户信息；接收所述待认证移动终端通过当前节点的公钥解密唯一性多重数字签名后反馈的结果，以确认所述待认证移动终端获得所述账户信息。该方法能够保证移动终端的认证管理过程中账户信息的有效性，提升整个认证过程的准确性。



CN 107453870 A

1.一种基于区块链的移动终端的认证管理方法，其特征在于，所述方法包括：

当前节点接收区块链网络中的账户分配请求数据包；

根据所述账户分配请求数据包为指定的待认证移动终端分配账户信息，并用所述当前节点的私钥生成唯一性多重数字签名以签署所述账户信息；

在区块链网络中广播所述唯一性多重数字签名、当前节点的公钥及账户信息；

接收所述待认证移动终端通过当前节点的公钥解密唯一性多重数字签名后反馈的结果，以确认所述待认证移动终端获得所述账户信息。

2.根据权利要求1所述的方法，其特征在于，所述账户分配请求数据包包含所述待认证移动终端的身份信息，用于根据所述待认证移动终端的身份信息为指定的待认证移动终端分配账户信息。

3.根据权利要求2所述的方法，其特征在于，所述区块链包括用于存储各节点的私钥的第一区块以及用于存储其他内容的第二区块；所述根据所述账户分配请求数据包为指定的待认证移动终端分配账户信息，并用所述当前节点的私钥生成唯一性多重数字签名以签署所述账户信息的步骤之后，还包括：

将处理所述账户分配请求数据包对应生成的包括所述账户信息、待认证移动终端的身份信息、所述唯一性多重数字签名以及认证节点的公钥的第一交互记录写入所述第二区块中，并在区块链网络中广播所述第一交互记录。

4.根据权利要求1所述的方法，其特征在于，所述用所述当前节点的私钥生成唯一性多重数字签名以签署所述账户信息的步骤具体包括：

对当前节点的公钥、上一节点生成的唯一性多重数字签名进行随机散列运算以生成一个随机散列值；

对所述随机散列值用所述认证节点的私钥进行加密以生成一个当前

节点的唯一性多重数字签名。

5.根据权利要求4所述的方法，其特征在于，所述对当前节点的公钥、上一节点生成的唯一性多重数字签名进行随机散列运算以生成一个随机散列值之前还包括：

对上一节点的唯一性多重数字签名的有效性进行验证，当验证通过后，执行后续步骤。

6.根据权利要求5所述的方法，其特征在于，所述对上一节点的唯一性多重数字签名的有效性进行验证的步骤中具体包括：

用上一节点的公钥对上一节点的唯一性多重数字签名进行解密，若解密后的随机散列值与当前节点的随机散列值一致，依据解密的结果判断该多重数字签名是否有效。

7.根据权利要求1所述的方法，其特征在于，所述身份信息包括验证信息，所述验证信息为所述待认证移动终端的唯一性设备识别码，所述用所述当前节点的私钥生成唯一性多重数字签名以签署所述账户信息的步骤之前还包括：

根据所述验证信息对所述待认证移动终端进行验证。

8.根据权利要求3所述的方法，其特征在于，还包括：

当前节点在区块链获取所述待认证移动终端发送的账户认证请求数据包，并获取所述待认证移动终端的公钥。

9.根据权利要求8所述的方法，其特征在于，所述当前节点在区块链获取所述待认证移动终端发送的账户认证请求数据包之后还包括：

获取所述账户认证请求数据包中包含的所述待认证移动终端发送的密文信息，并用所述待认证移动终端的公钥对所述密文信息进行解密，所述密文信息为所述待认证移动终端用其私钥对所述唯一性多重数字签名进行加密生成。

10.根据权利要求9所述的方法，其特征在于，所述获取所述账户认证请求数据包中包含的所述待认证移动终端发送的密文信息，并用所述待认证移动终端的公钥对所述密文信息进行解密之后还包括：

对比解密后的唯一性多重数字签名若与当前节点为所述待认证移动终端分配账户时签署的唯一性多重数字签名一致，则该待认证移动终端通过本次认证。

11.根据权利要求8所述的方法，其特征在于，所述移动终端发出所述账户认证请求数据包后，将包含所述移动终端的公钥以及处理所述账户认证请求数据包对应生成的所述密文信息的第二交互记录写入所述区块链的第二区块中，并在区块链网络中广播所述第二交互记录。

12.根据权利要求11所述的方法，其特征在于，还包括：

当前节点在区块链获取所述待认证移动终端发起的包含已认证账户信息的撤销账户请求数据包；

依据所述撤销账户请求数据包从所述第二交互记录中找到对应的账户信息；

将该账户信息写入撤销列表，所述撤销列表存储于区块链的所述第二区块中。

13.根据权利要求12所述的方法，其特征在于，所述将所述已认证的账户信息放入撤销列表的步骤之后，还包括：

将包括处理所述撤销账户请求数据包对应生成的撤销列表的第三交互记录写入所述区块链的第二区块中，并在区块链网络中广播所述第三交互记录。

14.根据权利要求11所述的方法，其特征在于，还包括：

将待认证移动终端的认证结果信息写入所述区块链的第二区块中的第二交互记录中并广播，所述认证结果信息包括所述待认证移动终端认证通过及认证失败。

15.根据权利要求3所述的方法，其特征在于，还包括：

接收用户终端发送的账户查询请求，获取所述账户查询请求中包含的账户信息；

根据所述账户信息从所述第二区块中查找所述账户信息对应的交互记录以确定待查询账户信息的交互结果信息；

向所述用户终端发送所述账户信息对应的交互结果信息以便所述用户终端依据该交互结果信息确定所述待查询账户的有效性。

16.根据权利要求15所述的方法，其特征在于，所述向所述用户终端发送所述账户信息对应的交互结果信息以便所述用户终端依据该交互结果信息确定所述待查询账户的有效性，具体包括：

依据第三交互记录判断待查询账户信息对应的账户是否有效。

17.一种基于区块链的账户信息的获取方法，其特征在于，包括：

向区块链网络发送账户分配请求数据包；

接收响应于所述账户分配请求数据包的当前节点发送的账户信息，所述账户信息签署了所述认证节点用其私钥生成的唯一性多重数字签名；

用当前节点的公钥对所述唯一性多重数字签名进行解密以获取所述账户信息。

18.根据权利要求17所述的方法，其特征在于，所述区块链包括用于存储各节点的私钥的第一区块以及用于存储其他内容的第二区块。

19.根据权利要求18所述的方法，其特征在于，当前节点将处理所述账户分配请求数据包对应生成的包括所述账户信息、待认证移动终端的身份信息、所述唯一性多重数字签名以及认证节点的公钥的第一交互记录写入所述第二区块中，并在区块链网络中广播所述第一交互记录。

20.根据权利要求19所述的方法，其特征在于，还包括：

获取与所述账户信息关联性储存于所述第二区块中的待认证移动终端的身份信息；

对比该身份信息与自身的身份信息，若一致，则验证所述账户信息有效。

21.根据权利要求17所述的方法，其特征在于，还包括：

向区块链发起账户认证请求数据包，并向区块链发送所述待认证移动终端用其私钥加密所述唯一性多重数字签名生成的密文信息以供当前节点依据该账户认证请求数据包以及所述密文信息对所述待认证移动终端进行认证。

22.根据权利要求18所述的方法，其特征在于，所述向区块链发出账户认证请求数据包之后还包括：

将包含所述移动终端的公钥以及处理所述账户认证请求数据包对应生成的所述密文信息的第二交互记录写入所述区块链的第二区块中，并在区块链网络中广播所述第二交互记录。

23.根据权利要求20所述的方法，其特征在于，还包括：

将验证后的结果反馈至所述区块链。

24.一种基于区块链的移动终端的认证管理装置，其特征在于，包括：

第一接收模块：当前节点接收区块链网络中的账户分配请求数据包；

分配模块：根据所述账户分配请求数据包为指定的待认证移动终端分配账户信息，并用所述当前节点的私钥生成唯一性多重数字签名以签署所述账户信息；

广播模块：在区块链网络中广播所述唯一性多重数字签名、当前节点的公钥及账户信息；

第二接收模块：接收所述待认证移动终端通过所述公钥解密唯一性多重数字签名后反馈的信息，以确认所述待认证移动终端获得所述账户信息。

25.根据权利要求24所述的装置，其特征在于，还包括：

认证模块：当前节点在区块链获取所述待认证移动终端发送的账户认证请求数据包，并获取所述待认证移动终端的公钥。

26.根据权利要求24所述的装置，其特征在于，还包括：

撤销模块：当前节点在区块链获取所述待认证移动终端发起的包含已认证账户信息的撤销账户请求数据包；依据所述撤销账户请求数据包从所述第二交互记录中找到对应的账户信息；将该账户信息写入撤销列表，所述撤销列表存储于区块链的所述第二区块中。

27.基于区块链的账户信息的获取装置，其特征在于，包括：

发送模块：向区块链网络发送账户分配请求数据包；

接收模块：接收响应于所述账户分配请求数据包的当前节点发送的账户信息，所述账户信息签署了所述认证节点用其私钥生成的唯一性多重数字签名；

解密模块:用当前节点的公钥对所述唯一性多重数字签名进行解密以获取所述账户信息。

28.一种认证管理装置,其特征在于,包括处理器及存储器,所述存储器中存储有计算机程序,其特征在于,所述计算机程序被处理器执行时实现如下步骤:

当前节点接收区块链网络中的账户分配请求数据包;

根据所述账户分配请求数据包为指定的待认证移动终端分配账户信息,并用所述当前节点的私钥生成唯一性多重数字签名以签署所述账户信息;

在区块链网络中广播所述唯一性多重数字签名、当前节点的公钥及账户信息;

接收所述待认证移动终端通过当前节点的公钥解密唯一性多重数字签名后反馈的结果,以确认所述待认证移动终端获得所述账户信息。

29.一种移动终端,其特征在于,包括处理器及存储器,所述存储器中存储有计算机程序,其特征在于,所述计算机程序被处理器执行时实现如下步骤:

向区块链网络发送账户分配请求数据包;

接收响应于所述账户分配请求数据包的当前节点发送的账户信息,所述账户信息签署了所述认证节点用其私钥生成的唯一性多重数字签名;

用当前节点的公钥对所述唯一性多重数字签名进行解密以获取所述账户信息。

基于区块链的移动终端认证管理方法、装置及相应的移动终端

技术领域

[0001] 本发明涉及网络通信技术领域，具体涉及一种基于区块链的移动终端认证管理方法、装置及相应的移动终端。

背景技术

[0002] 随着智能手机、平板电脑等轻薄便携的移动智能终端与人们的生活、工作和学习结合得越来越紧密，随之而来的设备管理也不断挑战传统IT运维管理。传统方式下移动终端普遍都通过USIM卡等用户身份识别模块来统一由运营商等机构认证管理。USIM卡是Universal Subscriber Identity Module的缩写，也称为全球用户识别卡。USIM也称为升级SIM，是在UMTS(Universal Mobile Telecommunication System)网络的一个构件，除能够支持多应用之外，USIM卡还在安全性方面对算法进行了升级，并增加了卡对网络的认证功能。

[0003] 由于USIM卡是一个装有微处理器的芯片卡，也就说这个物理设备可以伪造也可以通过非正规渠道获取从而得到个人私密信息，带来极大的安全隐患；并且USIM卡带来许多生产和运输成本，加大了业务运营、生产成本以及管理费用。

[0004] 由此可见，现有的移动终端认证管理不仅成本高，而且认证准确度不高，存在安全隐患。另外，现有的移动终端认证需要在本地存储移动终端账户，操作繁杂，不利于节约空间并且灵活性不高。

发明内容

[0005] 本发明提供一种基于区块链的移动终端认证管理方法及装置，实现移动终端账户信息的分配及认证管理。

[0006] 第一方面，本发明提供一种基于区块链的移动终端的认证管理方法，所述方法包括：

[0007] 当前节点接收区块链网络中的账户分配请求数据包；

[0008] 根据所述账户分配请求数据包为指定的待认证移动终端分配账户信息，并用所述当前节点的私钥生成唯一性多重数字签名以签署所述账户信息；

[0009] 在区块链网络中广播所述唯一性多重数字签名、当前节点的公钥及账户信息；

[0010] 接收所述待认证移动终端通过当前节点的公钥解密唯一性多重数字签名后反馈的结果，以确认所述待认证移动终端获得所述账户信息。

[0011] 具体的，所述账户分配请求数据包包含所述待认证移动终端的身份信息，用于根据所述待认证移动终端的身份信息为指定的待认证移动终端分配账户信息。

[0012] 优选的，所述区块链包括用于存储各节点的私钥的第一区块以及用于存储其他内容的第二区块；所述根据所述账户分配请求数据包为指定的待认证移动终端分配账户信息，并用所述当前节点的私钥生成唯一性多重数字签名以签署所述账户信息的步骤之后，

还包括：

[0013] 将处理所述账户分配请求数据包对应生成的包括所述账户信息、待认证移动终端的身份信息、所述唯一性多重数字签名以及认证节点的公钥的第一交互记录写入所述第二区块中，并在区块链网络中广播所述第一交互记录。

[0014] 具体的，所述用所述当前节点的私钥生成唯一性多重数字签名以签署所述账户信息的步骤具体包括：

[0015] 对当前节点的公钥、上一节点生成的唯一性多重数字签名进行随机散列运算以生成一个随机散列值；

[0016] 对所述随机散列值用所述认证节点的私钥进行加密以生成一个当前节点的唯一性多重数字签名。

[0017] 具体的，所述对当前节点的公钥、上一节点生成的唯一性多重数字签名进行随机散列运算以生成一个随机散列值之前还包括：

[0018] 对上一节点的唯一性多重数字签名的有效性进行验证，当验证通过后，执行后续步骤。

[0019] 具体的，所述对上一节点的唯一性多重数字签名的有效性进行验证的步骤中具体包括：

[0020] 用上一节点的公钥对上一节点的唯一性多重数字签名进行解密，若解密后的随机散列值与当前节点的随机散列值一致，依据解密的结果判断该多重数字签名是否有效。

[0021] 具体的，所述身份信息包括验证信息，所述验证信息为所述待认证移动终端的唯一性设备识别码，所述用所述当前节点的私钥生成唯一性多重数字签名以签署所述账户信息的步骤之前还包括：

[0022] 根据所述验证信息对所述待认证移动终端进行验证。

[0023] 优选的，还包括：

[0024] 当前节点在区块链获取所述待认证移动终端发送的账户认证请求数据包，并获取所述待认证移动终端的公钥。

[0025] 具体的，所述当前节点在区块链获取所述待认证移动终端发送的账户认证请求数据包之后还包括：

[0026] 获取所述账户认证请求数据包中包含的所述待认证移动终端发送的密文信息，并用所述待认证移动终端的公钥对所述密文信息进行解密，所述密文信息为所述待认证移动终端用其私钥对所述唯一性多重数字签名进行加密生成。

[0027] 具体的，所述获取所述账户认证请求数据包中包含的所述待认证移动终端发送的密文信息，并用所述待认证移动终端的公钥对所述密文信息进行解密之后还包括：

[0028] 对比解密后的唯一性多重数字签名若与当前节点为所述待认证移动终端分配账户时签署的唯一性多重数字签名一致，则该待认证移动终端通过本次认证。

[0029] 具体的，所述移动终端发出所述账户认证请求数据包后，将包含所述移动终端的公钥以及处理所述账户认证请求数据包对应生成的所述密文信息的第二交互记录写入所述区块链的第二区块中，并在区块链网络中广播所述第二交互记录。

[0030] 优选的，还包括：

[0031] 当前节点在区块链获取所述待认证移动终端发起的包含已认证账户信息的撤销

账户请求数据包；

[0032] 依据所述撤销账户请求数据包从所述第二交互记录中找到对应的账户信息；

[0033] 将该账户信息写入撤销列表，所述撤销列表存储于区块链的所述第二区块中。

[0034] 具体的，所述将所述已认证的账户信息放入撤销列表的步骤之后，还包括：

[0035] 将包括处理所述撤销账户请求数据包对应生成的撤销列表的第三交互记录写入所述区块链的第二区块中，并在区块链网络中广播所述第三交互记录。

[0036] 具体的，还包括：

[0037] 将待认证移动终端的认证结果信息写入所述区块链的第二区块中的第二交互记录中并广播，所述认证结果信息包括所述待认证移动终端认证通过及认证失败。

[0038] 优选的，还包括：

[0039] 接收用户终端发送的账户查询请求，获取所述账户查询请求中包含的账户信息；

[0040] 根据所述账户信息从所述第二区块中查找所述账户信息对应的交互记录以确定待查询账户信息的交互结果信息；

[0041] 向所述用户终端发送所述账户信息对应的交互结果信息以便所述用户终端依据该交互结果信息确定所述待查询账户的有效性。

[0042] 具体的，所述向所述用户终端发送所述账户信息对应的交互结果信息以便所述用户终端依据该交互结果信息确定所述待查询账户的有效性，具体包括：

[0043] 依据第三交互记录判断待查询账户信息对应的账户是否有效。

[0044] 第二方面，本发明提供一种基于区块链的账户信息的获取方法，包括：

[0045] 向区块链网络发送账户分配请求数据包；

[0046] 接收响应于所述账户分配请求数据包的当前节点发送的账户信息，所述账户信息签署了所述认证节点用其私钥生成的唯一性多重数字签名；

[0047] 用当前节点的公钥对所述唯一性多重数字签名进行解密以获取所述账户信息。

[0048] 具体的，所述区块链包括用于存储各节点的私钥的第一区块以及用于存储其他内容的第二区块。

[0049] 具体的，当前节点将处理所述账户分配请求数据包对应生成的包括所述账户信息、待认证移动终端的身份信息、所述唯一性多重数字签名以及认证节点的公钥的第一交互记录写入所述第二区块中，并在区块链网络中广播所述第一交互记录。

[0050] 优选的，还包括：

[0051] 获取与所述账户信息关联性储存于所述第二区块中的待认证移动终端的身份信息；

[0052] 对比该身份信息与自身的身份信息，若一致，则验证所述账户信息有效。

[0053] 具体的，还包括：

[0054] 向区块链发起账户认证请求数据包，并向区块链发送所述待认证移动终端用其私钥加密所述唯一性多重数字签名生成的密文信息以供当前节点依据该账户认证请求数据包以及所述密文信息对所述待认证移动终端进行认证。

[0055] 具体的，所述向区块链发出账户认证请求数据包之后还包括：

[0056] 将包含所述移动终端的公钥以及处理所述账户认证请求数据包对应生成的所述密文信息的第二交互记录写入所述区块链的第二区块中，并在区块链网络中广播所述第二

交互记录。

[0057] 优选的，还包括：

[0058] 将验证后的结果反馈至所述区块链。

[0059] 第三方面，本发明提供一种基于区块链的移动终端的认证管理装置，包括：

[0060] 第一接收模块：当前节点接收区块链网络中的账户分配请求数据包；

[0061] 分配模块：根据所述账户分配请求数据包为指定的待认证移动终端分配账户信息，并用所述当前节点的私钥生成唯一性多重数字签名以签署所述账户信息；

[0062] 广播模块：在区块链网络中广播所述唯一性多重数字签名、当前节点的公钥及账户信息；

[0063] 第二接收模块：接收所述待认证移动终端通过所述公钥解密唯一性多重数字签名后反馈的信息，以确认所述待认证移动终端获得所述账户信息。

[0064] 具体的，还包括：

[0065] 认证模块：当前节点在区块链获取所述待认证移动终端发送的账户认证请求数据包，并获取所述待认证移动终端的公钥。

[0066] 具体的，还包括：

[0067] 撤销模块：当前节点在区块链获取所述待认证移动终端发起的包含已认证账户信息的撤销账户请求数据包；依据所述撤销账户请求数据包从所述第二交互记录中找到对应的账户信息；将该账户信息写入撤销列表，所述撤销列表存储于区块链的所述第二区块中。

[0068] 第四方面，本发明提供一种基于区块链的账户信息的获取装置，包括：

[0069] 发送模块：向区块链网络发送账户分配请求数据包；

[0070] 接收模块：接收响应于所述账户分配请求数据包的当前节点发送的账户信息，所述账户信息签署了所述认证节点用其私钥生成的唯一性多重数字签名；

[0071] 解密模块：用当前节点的公钥对所述唯一性多重数字签名进行解密以获取所述账户信息。

[0072] 第五方面，本发明提供一种认证管理装置，包括处理器及存储器，所述存储器中存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现如下步骤：

[0073] 当前节点接收区块链网络中的账户分配请求数据包；

[0074] 根据所述账户分配请求数据包为指定的待认证移动终端分配账户信息，并用所述当前节点的私钥生成唯一性多重数字签名以签署所述账户信息；

[0075] 在区块链网络中广播所述唯一性多重数字签名、当前节点的公钥及账户信息；

[0076] 接收所述待认证移动终端通过当前节点的公钥解密唯一性多重数字签名后反馈的结果，以确认所述待认证移动终端获得所述账户信息。

[0077] 第六方面，本发明提供一种移动终端，包括处理器及存储器，所述存储器中存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现如下步骤：

[0078] 向区块链网络发送账户分配请求数据包；

[0079] 接收响应于所述账户分配请求数据包的当前节点发送的账户信息，所述账户信息签署了所述认证节点用其私钥生成的唯一性多重数字签名；

[0080] 用当前节点的公钥对所述唯一性多重数字签名进行解密以获取所述账户信息。

[0081] 相比现有技术，本发明提供的方案有以下优点：

[0082] 1、本发明提供一种基于区块链的移动终端的认证管理方法，在账户信息分配阶段，表现在认证节点一端，当前节点接收待认证移动终端通过区块链发送的账户信息分配请求数据包，为移动终端分配账户信息，并生成多重数字签名签署该账户信息。相应的，表现在移动终端，移动终端接收所述账户信息，并用当前节点的公钥解密多重数字签名以获取账户信息并验证账户信息的有效性。在账户信息认证阶段，表现在认证节点一端，当前节点接收移动终端通过区块链发送的账户信息认证请求数据包，用移动终端的公钥通过解密变换以验证移动终端的身份。相应的，表现在移动终端，移动终端通过区块链向当前节点发送包含用其私钥加密的多重数字签名的账户信息认证请求，以便当前节点通过对应的解密运算完成账户信息的认证。本发明采用上述双重认证的机制确保了整个认证过程的准确性。另外，本发明将分配账户的交互记录及认证账户的交互记录写入区块链上，结合区块链分布式的特点，所有节点都保存了交互的记录，因此保证了各交互记录的有效性与可靠性。

[0083] 2、具体而言，本发明结合了区块链的开放性与不可篡改性，各节点都可以参与到区块链网络中，每个节点都允许获得一份完整的交互记录的拷贝，单个甚至多个节点对区块链上数据的修改都无法影响其他节点的数据，任一节点失效，其余节点仍然能正常工作，使得认证过程不依赖于单个来源，降低了交互记录被恶意篡改的风险。

[0084] 3、本发明结合了区块链的去中心，去信任，不存在中心化的设备和管理机构，节点之间的数据交互通过唯一性多重数字签名技术进行验证，具体而言，当前节点用其私钥生成的唯一性多重数字签名签署分配的账户信息，一方面能确定该账户信息确实是由当前节点签名并发出的，另一方面，保证了发出的账户信息的完整性，提升了验证过程的准确性。

[0085] 4、本发明通过实时查询当前区块链的第三交互记录来获知账户信息是否被撤销，解决了用户无法及时获知账户信息是否被撤销的问题。

[0086] 综上，本发明所述方法提升了验证过程的准确性，降低了交互记录被恶意篡改的风险，另外，本发明无需通过USIM卡等物理设备对移动终端进行管理，节省了生产和运输成本，最后，移动终端和认证节点可采取任意方式连接到区块链网络中，增大了组网的灵活性。

[0087] 本发明附加的方面和优点将在下面的描述中部分给出，这些将从下面的描述中变得明显，或通过本发明的实践了解到。

附图说明

[0088] 本发明上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中：

[0089] 图1为本发明的一种基于区块链的移动终端认证管理方法实施例一流程框图；

[0090] 图2为本发明的认证节点对账户信息的签名及校验签名方法流程图；

[0091] 图3为本发明的一种基于区块链的移动终端认证管理方法实施例二流程框图；

[0092] 图4为本发明的一种基于区块链的移动终端认证管理装置实施例一流程框图；

[0093] 图5为本发明的一种基于区块链的移动终端认证管理装置实施例二流程框图；

[0094] 图6为本发明的一种基于区块链的账户信息获取方法实施例一流程框图；

[0095] 图7为本发明的一种基于区块链的账户信息获取装置实施例一流程框图；

[0096] 图8为一种移动终端部分结构框图。

具体实施方式

[0097] 下面详细描述本发明的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，仅用于解释本发明，而不能解释为对本发明的限制。

[0098] 请参阅图1，本发明所提供的一种基于区块链的移动终端的认证管理方法，具体的一种实施方式中，具体包括如下步骤：

[0099] S11、当前节点接收区块链网络中的账户分配请求数据包。

[0100] 本发明实施例中，所述待认证移动终端在区块链网络中发送账户分配请求数据包以请求当前节点分配账户信息，所述账户分配请求数据包包含所述待认证移动终端的身份信息，用于根据待认证移动终端的身份信息为指定的待认证移动终端分配账户信息，所述身份信息可以为所述待认证移动终端的设备识别码或设备序列号等可以唯一性表征所述待认证移动终端的身份的信息。

[0101] 所述待认证移动终端发出账户分配请求数据包之后，将该账户分配请求数据包对应生成的交互记录写入区块链中以供其他节点查询或获取数据。

[0102] S12、根据所述账户分配请求数据包为指定的待认证移动终端分配账户信息，并用当前节点的私钥生成唯一性多重数字签名以签署所述账户信息。

[0103] 本发明实施例中，当前节点接收所述账户分配请求数据包后依据其包含的待认证移动终端的身份信息为所述待认证移动终端分配账户信息，并用当前节点的私钥生成的唯一性多重数字签名签署所述账户信息以供待认证移动终端通过验证该唯一性多重数字签名确保该账户信息的准确性以及该账户信息确实是由当前节点所发送。

[0104] 在区块链的分布式网络里，节点之间进行通讯并达成信任，需要依赖多重数字签名技术，它主要实现了身份确认以及信息真实性、完整性验证。多重数字签名是解决网络通信中数据安全的一种有效方法，能够实现对网络中传输数据的辩证和认证，是对传统手写签名的一种模拟。

[0105] 请参考图2，图2示出了一种可能的当前节点用其私钥生成唯一性多重数字签名的流程图，其中，具体步骤如下：

[0106] 对当前节点即图中的节点1的公钥以及上一节点即图中的节点0生成的唯一性多重数字签名进行随机散列运算以生成一个随机散列值；

[0107] 对所述随机散列值用当前节点的私钥进行加密以生成一个当前节点的唯一性多重数字签名。

[0108] 设当前节点的公钥以及上一节点生成的唯一性多重数字签名构成消息明文M，对消息M进行散列运算得到其散列值即消息摘要z＝H(M)，对该散列值用当前节点的私钥加密生成唯一性多重数字签名s＝sig(k,H(M))，其中k为当前节点的私钥，当前节点用该唯一性多重数字签名签署所述账户信息并通过区块链网络发送至待认证移动终端。

[0109] 本发明实施例中，当前节点用生成唯一性多重数字签名并用该唯一性多重数字签名签署所述账户信息的过程总具体涉及用散列函数对消息进行散列转换的算法以及用消息签名算法对消息进行签名。

[0110] 具体而言，散列函数是一种能把不同长度的输入消息转换成固定长度的消息的摘

要的函数。将散列函数运用于多重数字签名中不仅缩短了消息的长度还很大程度上提高了签名的速度。目前，常用的散列函数有Rivest发明的MD系列、NIST(美国国家标准技术研究所)提出的SHA系列。

[0111] 多重数字签名是附加在数据单元上的一些数据，或是对数据单元所做的密码变换。这种数据或变换允许数据单元的接收者用于确认数据单元来源和数据单元的完整性，并保护数据防止被人进行伪造。应用于本发明中，本发明应用多重数字签名算法对当前节点的公钥、上一节点生成的唯一性多重数字签名进行散列运算后生成的摘要用当前节点的私钥进行密码变换生成唯一性多重数字签名，用于签署所述账户信息，并将所述账户以及该唯一性多重数字签名通过区块链网络发送至待认证移动终端，所述待认证移动终端通过区块链获取签署了唯一性多重数字签名的账户信息后进行相应的逆变换得到账户信息。

[0112] 请继续参考图2，图2中当前节点的公钥以及上一节点生成的唯一性多重数字签名进行随机散列运算以生成一个随机散列值之前还包括：

[0113] 对上一节点的唯一性多重数字签名的有效性进行验证，当验证通过后，执行后续步骤。即图中的右侧方框内，用节点1的公钥校验节点1生成的多重数字签名。

[0114] 在多重签名过程中，各个节点在签名之前先验证上一个唯一性多重数字签名签名是否有效(第一个节点签名时不用判断)。如果唯一性多重数字签名有效，则用自己的私钥进行签名，然后把得到的唯一性多重数字签名发送给下一个节点。

[0115] 一种可能的设计中，所述对上一节点的唯一性多重数字签名的有效性进行验证的步骤中具体包括：

[0116] 用上一节点的公钥对上一节点的唯一性多重数字签名进行解密，若解密后的随机散列值与当前节点的随机散列值一致，则判断该多重数字签名有效。

[0117] 本发明实施例结合多重数字签名在消息的传输过程中的两大主要作用：保证消息在传输过程中消息的完整性和提供对消息发送者的身份验证。即发送方在发送消息时附上该消息对应的唯一性多重数字签名，接收方接收到该消息及唯一性多重数字签名，通过解密该唯一性多重数字签名后与接收到的消息的摘要进行对比以完成验签。

[0118] 本发明实施例中，所述身份信息包括验证信息，所述验证信息为所述待认证移动终端的唯一性设备识别码，所述用所述当前节点的私钥生成唯一性多重数字签名以签署所述账户信息的步骤之前还包括：

[0119] 根据所述验证信息对所述待认证移动终端进行验证。

[0120] S13、在区块链网络中广播所述唯一性多重数字签名、当前节点的公钥及账户信息。

[0121] 本发明实施例中，所述区块链包括用于存储各节点的私钥的第一区块以及用于存储其他内容的第二区块。优选的，本步骤之前还包括：将处理所述账户分配请求数据包对应生成的包括所述账户信息、待认证移动终端的身份信息、所述唯一性多重数字签名以及认证节点的公钥的第一交互记录写入第二区块中，并在区块链网络中广播所述第一交互记录。

[0122] 具体而言，当前节点为所述待认证移动终端分配账户信息后，将签署了所述唯一性多重数字签名的账户信息、待认证移动终端的身份信息以及当前节点的公钥作为第一交互记录写入第二区块中，区块链上的每一个区块都有一个数据库用于储存该区块上的交互

记录，它相当于一个“账本”，当前节点将签署了所述唯一性多重数字签名的账户信息、待认证移动终端的身份信息以及当前节点的公钥写入并储存于所述第二区块中的具体形式可以是以一种一一映射的对应关系存储于所述第二区块的数据库中以便后续查询。

[0123] 本发明所述基于区块链的移动终端认证管理方法结合了区块链网络的交易透明性及不可篡改性的特点，将账户信息的分配及认证作为交互的一部分写入区块链，将每一个交互的记录都实时记录在对应的区块中，构成一种几乎不可能被更改的分布式数据库，提升了账户信息的有效性。

[0124] 具体而言，正是由于本发明所述方法中，当前节点在区块链网络中广播所述唯一性多重数字签名、当前节点的公钥及账户信息，使得每一个节点都能接收到广播，每一个节点都允许获得完整的当前节点的交互记录对应的数据库的拷贝，每一次的交互记录对所有的节点都是可见的，因此，用户可以连接到任意节点去进行认证，使得认证过程不依赖于单个来源，降低了记录被恶意篡改的风险。这里的“分布式”不仅仅体现为数据的分布式存储，也体现为数据的分布式记录(即由系统参与者共同维护)。另外，节点与节点之间的数据交互通过多重数字签名进行验证，无需相互信任，节点之间基于一套共识机制，共同维护整个区块链的数据，任意一节点失效，其他节点仍能正常工作，提升数据交互的效率与可靠性。

[0125] S14、接收所述待认证移动终端通过当前节点的公钥解密唯一性多重数字签名后反馈的结果，以确认所述待认证移动终端获得所述账户信息。

[0126] 本发明实施例中，当前节点为所述待认证移动终端分配账户信息后，将签署了所述唯一性多重数字签名的账户信息、待认证移动终端的身份信息以及当前节点的公钥作为第一交互记录写入第二区块中，其可以是以一种一一映射的对应关系存储于所述第二区块的数据库中并广播该次的交互记录，当待认证移动终端收到广播后向区块链获取该次交互记录的相关数据。

[0127] 具体而言，待认证移动终端首先获取签署了所述唯一性多重数字签名的账户信息并用当前节点的公钥解密出所述账户信息。待认证移动终端再获取与该账户信息关联性储存于数据库中的待认证移动终端的身份信息，通过对比获取的待认证移动终端的身份信息与自身的身份信息，若匹配，则验证了解密出的账户信息为与自身身份信息相匹配的账户信息，并将验证结果通过区块链网络反馈至当前节点，当前节点接收到反馈的结果后以此来确认所述待认证移动终端获取到其分配的账户信息。

[0128] 请参考图3，本发明的另一个实施例中还包括一个步骤S15，用于当前节点在区块链获取所述待认证移动终端发送的账户认证请求数据包，并获取所述待认证移动终端的公钥。

[0129] 本发明实施例中，待认证移动终端获取当前节点分配的签署了唯一性多重数字签名的账户信息后向区块链发出账户认证请求数据包，并发送用自己的私钥对获取的唯一性多重数字签名加密后的密文信息。所述待认证移动终端发出账户认证请求数据包后将该账户认证请求数据包以及所述密文信息作为第二交互记录写入所述第二区块中并广播所述第二交互记录以实时记录最新的交互记录形成一个永久的、可靠的“账本”。

[0130] 所述待认证移动终端广播所述第二交互记录之后，当前节点向区块链获取所述待认证移动终端发送的账户认证请求数据包，并获取所述待认证移动终端的公钥。具体而言，当前节点获取所述账户认证请求数据包中包含的所述待认证移动终端发送的密文信息，并

用所述待认证移动终端的公钥对所述密文信息进行解密，对比解密后的唯一性多重数字签名与当前节点为所述待认证移动终端分配账户时签署的唯一性多重数字签名是否一致，若一致，则该待认证移动终端通过本次认证。

[0131] 优选的，当前节点认证完所述待认证移动终端后将待认证移动终端的认证结果信息写入所述区块链的第二区块中的第二交互记录中并广播，所述认证结果信息包括所述待认证移动终端认证通过及认证失败。

[0132] 请继续参考图3，本发明的另一个实施例中还包括一个步骤S16用于当前节点在区块链获取所述待认证移动终端发起的包含已认证账户信息的撤销账户请求数据包；依据所述撤销账户请求数据包从所述第二交互记录中找到对应的账户信息；将该账户信息写入撤销列表，所述撤销列表存储于区块链的所述第二区块中。

[0133] 本发明实施例中，当前节点认证完所述待认证移动终端的账户信息后可以将分配的账户信息进行撤销。其中该撤销的操作可以是由待认证移动终端发起的撤销请求而触发撤销。

[0134] 所述待认证移动终端向区块链网络中发送包含已认证账户信息的撤销账户请求数据包，当前节点向区块链网络获取该撤销账户请求数据包并依据其中携带的账户信息从所述第二交互记录中找到对应的第二交互记录，依据该第二交互记录将该账户信息写入撤销列表，具体而言，查看第二交互记录中该账户信息是否已经完成认证，若是，则执行撤销操作，否则不执行。

[0135] 在一种可能的设计中，当前节点也可以通过实时查询所述第二交互记录判断是否有有账户待撤销，若有，则自动触发撤销操作。

[0136] 具体而言，当前节点从区块链上查找待认证移动终端发起交易的交易记录，找到最新的交易并取出其中包含的已分配或者已认证的账户信息。其中，若能从最新的交易中取出已认证的账户信息，则说明有可撤销的账户信息，否则没有，直接返回。如果有可撤销的账户，则当前节点将对应的账户信息写入撤销列表，并将包括处理所述撤销账户请求数据包对应生成的撤销列表的第三交互记录写入所述区块链的第二区块中，并在区块链网络中广播所述第三交互记录。

[0137] 一种可能的设计中，当前节点对所述账户信息进行撤销时的撤销操作可以是在待认证移动终端发起撤销请求下触发，也可以是在当前节点发起的撤销请求下触发，其具体的触发机制在此不做限定。

[0138] 优选的，本发明实施例还包括接收用户终端发送的账户查询请求，获取所述账户查询请求中包含的账户信息；根据所述账户信息从所述第二区块中查找所述账户信息对应的交互记录以确定待查询账户信息的交互结果信息；向所述用户终端发送所述账户信息对应的交互结果信息以便所述用户终端依据该交互结果信息确定所述待查询账户的有效性。

[0139] 优选的，查询账户信息的有效性也可以依据第三交互记录判断待查询账户信息对应的账户是否有效，具体的，只需要通过查询区块链上第三交互记录获知。

[0140] 参考图4所示，本发明还提供一种基于区块链的移动终端认证管理装置，一种实施例中，包括第一接收模块11、分配模块12、广播模块13以及第二接收模块14。请参考图5，另一个实施例中还包括认证模块15以及撤销模块16其中，

[0141] 第一接收模块11：当前节点接收区块链网络中的账户分配请求数据包；

[0142] 本发明实施例中，所述待认证移动终端在区块链网络中发送账户分配请求数据包以请求当前节点分配账户信息，所述账户分配请求数据包包含所述待认证移动终端的身份信息，用于根据待认证移动终端的身份信息为指定的待认证移动终端分配账户信息，所述身份信息可以为所述待认证移动终端的设备识别码或设备序列号等可以唯一性表征所述待认证移动终端的身份的信息。

[0143] 所述待认证移动终端发出账户分配请求数据包之后，将该账户分配请求数据包对应生成的交互记录写入区块链中以供其他节点查询或获取数据。

[0144] 分配模块12：根据所述账户分配请求数据包为指定的待认证移动终端分配账户信息，并用所述当前节点的私钥生成唯一性多重数字签名以签署所述账户信息；

[0145] 本发明实施例中，当前节点接收所述账户分配请求数据包后依据其包含的待认证移动终端的身份信息为所述待认证移动终端分配账户信息，并用当前节点的私钥生成的唯一性多重数字签名签署所述账户信息以供待认证移动终端通过验证该唯一性多重数字签名确保该账户信息的准确性以及该账户信息确实是由当前节点所发送。

[0146] 在区块链的分布式网络里，节点之间进行通讯并达成信任，需要依赖多重数字签名技术，它主要实现了身份确认以及信息真实性、完整性验证。多重数字签名是解决网络通信中数据安全的一种有效方法，能够实现对网络中传输数据的辩证和认证，是对传统手写签名的一种模拟。

[0147] 一种可能的设计中，本发明用当前节点的私钥生成的唯一性多重数字签名的具体步骤如下：

[0148] 对当前节点的公钥以及上一节点生成的唯一性多重数字签名进行随机散列运算以生成一个随机散列值；

[0149] 对所述随机散列值用所述认证节点的私钥进行加密以生成一个当前节点的唯一性多重数字签名。

[0150] 设当前节点的公钥以及上一节点生成的唯一性多重数字签名构成消息明文M，对消息M进行散列运算得到其散列值即消息摘要z＝H(M)，对该散列值用当前节点的私钥加密生成唯一性多重数字签名s＝sig(k,H(M))，其中k为当前节点的私钥，当前节点用该唯一性多重数字签名签署所述账户信息并通过区块链网络发送至待认证移动终端。

[0151] 本发明实施例中，当前节点用生成唯一性多重数字签名并用该唯一性多重数字签名签署所述账户信息的过程总具体涉及用散列函数对消息进行散列转换的算法以及用消息签名算法对消息进行签名。

[0152] 具体而言，散列函数是一种能把不同长度的输入消息转换成固定长度的消息的摘要的函数。将散列函数运用于多重数字签名中不仅缩短了消息的长度还很大程度上提高了签名的速度。目前，常用的散列函数有Rivest发明的MD系列、NIST(美国国家标准技术研究所)提出的SHA系列。

[0153] 多重数字签名是附加在数据单元上的一些数据，或是对数据单元所做的密码变换。这种数据或变换允许数据单元的接收者用于确认数据单元来源和数据单元的完整性，并保护数据防止被人进行伪造。应用于本发明中，本发明应用多重数字签名算法对当前节点的公钥、上一节点生成的唯一性多重数字签名进行散列运算后生成的摘要用当前节点的私钥进行密码变换生成唯一性多重数字签名，用于签署所述账户信息，并将所述账户以及

该唯一性多重数字签名通过区块链网络发送至待认证移动终端，所述待认证移动终端通过区块链获取签署了唯一性多重数字签名的账户信息后进行相应的逆变换得到账户信息。

[0154] 本发明实施例中，当前节点的公钥以及上一节点生成的唯一性多重数字签名进行随机散列运算以生成一个随机散列值之前还包括：

[0155] 对上一节点的唯一性多重数字签名的有效性进行验证，当验证通过后，执行后续步骤。

[0156] 在多重签名过程中，各个节点在签名之前先验证上一个唯一性多重数字签名签名是否有效(第一个节点签名时不用判断)。如果唯一性多重数字签名有效，则用自己的私钥进行签名，然后把得到的唯一性多重数字签名发送给下一个节点。

[0157] 一种可能的设计中，所述对上一节点的唯一性多重数字签名的有效性进行验证的步骤中具体包括：

[0158] 用上一节点的公钥对上一节点的唯一性多重数字签名进行解密，若解密后的随机散列值与当前节点的随机散列值一致，则判断该多重数字签名有效。

[0159] 本发明实施例结合多重数字签名在消息的传输过程中的两大主要作用：保证消息在传输过程中消息的完整性和提供对消息发送者的身份验证。即发送方在发送消息时附上该消息对应的唯一性多重数字签名，接收方接收到该消息及唯一性多重数字签名，通过解密该唯一性多重数字签名后与接收到的消息的摘要进行对比以完成验签。

[0160] 本发明实施例中，所述身份信息包括验证信息，所述验证信息为所述待认证移动终端的唯一性设备识别码，所述用所述当前节点的私钥生成唯一性多重数字签名以签署所述账户信息的步骤之前还包括：

[0161] 根据所述验证信息对所述待认证移动终端进行验证。

[0162] 广播模块13：在区块链网络中广播所述唯一性多重数字签名、当前节点的公钥及账户信息；

[0163] 本发明实施例中，所述区块链包括用于存储各节点的私钥的第一区块以及用于存储其他内容的第二区块。优选的，本步骤之前还包括：将处理所述账户分配请求数据包对应生成的包括所述账户信息、待认证移动终端的身份信息、所述唯一性多重数字签名以及认证节点的公钥的第一交互记录写入第二区块中，并在区块链网络中广播所述第一交互记录。

[0164] 具体而言，当前节点为所述待认证移动终端分配账户信息后，将签署了所述唯一性多重数字签名的账户信息、待认证移动终端的身份信息以及当前节点的公钥作为第一交互记录写入第二区块中，区块链上的每一个区块都有一个数据库用于储存该区块上的交互记录，它相当于一个“账本”，当前节点将签署了所述唯一性多重数字签名的账户信息、待认证移动终端的身份信息以及当前节点的公钥写入并储存于所述第二区块中的具体形式可以是以一种一一映射的对应关系存储于所述第二区块的数据库中以便后续查询。

[0165] 本发明所述基于区块链的移动终端认证管理方法结合了区块链网络的交易透明性及不可篡改性的特点，将账户信息的分配及认证作为交互的一部分写入区块链，将每一个交互的记录都实时记录在对应的区块中，构成一种几乎不可能被更改的分布式数据库，提升了账户信息的有效性。

[0166] 具体而言，正是由于本发明所述方法中，当前节点在区块链网络中广播所述唯一

性多重数字签名、当前节点的公钥及账户信息，使得每一个节点都能接收到广播，每一个节点都允许获得完整的当前节点的交互记录对应的数据库的拷贝，每一次的交互记录对所有的节点都是可见的，因此，用户可以连接到任意节点去进行认证，使得认证过程不依赖于单个来源，降低了记录被恶意篡改的风险。这里的“分布式”不仅仅体现为数据的分布式存储，也体现为数据的分布式记录(即由系统参与者共同维护)。另外，节点与节点之间的数据交互通过多重数字签名进行验证，无需相互信任，节点之间基于一套共识机制，共同维护整个区块链的数据，任意一节点失效，其他节点仍能正常工作，提升数据交互的效率与可靠性。

[0167] 第二接收模块14：接收所述待认证移动终端通过所述公钥解密唯一性多重数字签名后反馈的信息，以确认所述待认证移动终端获得所述账户信息。

[0168] 本发明实施例中，当前节点为所述待认证移动终端分配账户信息后，将签署了所述唯一性多重数字签名的账户信息、待认证移动终端的身份信息以及当前节点的公钥作为第一交互记录写入第二区块中，其可以是以一种一一映射的对应关系存储于所述第二区块的数据库中并广播该次的交互记录，当待认证移动终端收到广播后向区块链获取该次交互记录的相关数据。

[0169] 具体而言，待认证移动终端首先获取签署了所述唯一性多重数字签名的账户信息并用当前节点的公钥解密出所述账户信息。待认证移动终端再获取与该账户信息关联性储存于数据库中的待认证移动终端的身份信息，通过对比获取的待认证移动终端的身份信息与自身的身份信息，若匹配，则验证了解密出的账户信息为与自身身份信息相匹配的账户信息，并将验证结果通过区块链网络反馈至当前节点，当前节点接收到反馈的结果后以此来确认所述待认证移动终端获取到其分配的账户信息。

[0170] 请参考图5，本发明的另一个实施例中还包括认证模块15用于当前节点在区块链获取所述待认证移动终端发送的账户认证请求数据包，并获取所述待认证移动终端的公钥。

[0171] 本发明实施例中，待认证移动终端获取当前节点分配的签署了唯一性多重数字签名的账户信息后向区块链发出账户认证请求数据包，并发送用自己的私钥对获取的唯一性多重数字签名加密后的密文信息。所述待认证移动终端发出账户认证请求数据包后将该账户认证请求数据包以及所述密文信息作为第二交互记录写入所述第二区块中并广播所述第二交互记录以实时记录最新的交互记录形成一个永久的、可靠的“账本”。

[0172] 所述待认证移动终端广播所述第二交互记录之后，当前节点向区块链获取所述待认证移动终端发送的账户认证请求数据包，并获取所述待认证移动终端的公钥。具体而言，当前节点获取所述账户认证请求数据包中包含的所述待认证移动终端发送的密文信息，并用所述待认证移动终端的公钥对所述密文信息进行解密，对比解密后的唯一性多重数字签名与当前节点为所述待认证移动终端分配账户时签署的唯一性多重数字签名是否一致，若一致，则该待认证移动终端通过本次认证。

[0173] 优选的，当前节点认证完所述待认证移动终端后将待认证移动终端的认证结果信息写入所述区块链的第二区块中的第二交互记录中并广播，所述认证结果信息包括所述待认证移动终端认证通过及认证失败。

[0174] 请继续参考图5，本发明的另一个实施例中还包括撤销模块16用于当前节点在区块链获取所述待认证移动终端发起的包含已认证账户信息的撤销账户请求数据包；依据所

述撤销账户请求数据包从所述第二交互记录中找到对应的账户信息;将该账户信息写入撤销列表,所述撤销列表存储于区块链的所述第二区块中。

[0175] 本发明实施例中,当前节点认证完所述待认证移动终端的账户信息后可以将分配的账户信息进行撤销。其中该撤销的操作可以是由待认证移动终端发起的撤销请求而触发撤销。

[0176] 所述待认证移动终端向区块链网络中发送包含已认证账户信息的撤销账户请求数据包,当前记节点向区块链网络获取该撤销账户请求数据包并依据其中携带的账户信息从所述第二交互记录中找到对应的第二交互记录,依据该第二交互记录将该账户信息写入撤销列表,具体而言,查看第二交互记录中该账户信息是否已经完成认证,若是,则执行撤销操作,否则不执行。

[0177] 在一种可能的设计中,当前节点也可以通过实时查询所述第二交互记录判断是否有有账户待撤销,若有,则自动触发撤销操作。

[0178] 具体而言,当前节点从区块链上查找待认证移动终端发起交易的交易记录,找到最新的交易并取出其中包含的已分配或者已认证的账户信息。其中,若能从最新的交易中取出已认证的账户信息,则说明有可撤销的账户信息,否则没有,直接返回。如果有可撤销的账户,则当前节点将对应的账户信息写入撤销列表,并将包括处理所述撤销账户请求数据包对应生成的撤销列表的第三交互记录写入所述区块链的第二区块中,并在区块链网络中广播所述第三交互记录。

[0179] 一种可能的设计中,当前节点对所述账户信息进行撤销时的撤销操作可以是在待认证移动终端发起撤销请求下触发,也可以是在当前节点发起的撤销请求下触发,其具体的触发机制在此不做限定。

[0180] 优选的,本发明实施例还包括接收用户终端发送的账户查询请求,获取所述账户查询请求中包含的账户信息;根据所述账户信息从所述第二区块中查找所述账户信息对应的交互记录以确定待查询账户信息的交互结果信息;向所述用户终端发送所述账户信息对应的交互结果信息以便所述用户终端依据该交互结果信息确定所述待查询账户的有效性。

[0181] 优选的,查询账户信息的有效性也可以依据第三交互记录判断待查询账户信息对应的账户是否有效,具体的,只需要通过查询区块链上第三交互记录获知。

[0182] 综合上述实施例可知,本发明最大的有益效果在于本发明将移动终端的账户分配以及账户认证作为一种交易写入区块链,运用区块链的通过去中心、去信任、交易透明的方式集体维护一个可靠的数据库的技术方案,使得移动终端的账户分配以及账户认证的数据交互过程得到可靠的保证。

[0183] 具体的,表现在账户分配方面,本发明通过当前节点接收待认证移动终端发起的账户分配的请求数据包,为待认证移动终端分配账户信息,并用当前节点的私钥生成的多重数字签名签署该账户信息后将其通过区块链网络发送至待认证移动终端。待认证移动终端获取该账户信息以及多重数字签名后验证该账户信息的有效性。

[0184] 表现在账户认证方面,本发明通过当前节点接收待认证移动终端通过区块链发送的账户信息认证请求数据包,获取该账户信息认证请求数据包中的包含的加密信息,用待认证移动终端的公钥解密该加密信息后得到多重数字签名,对比解密后的多重数字签名是否与当前节点分配账户信息时签署的多重数字签名一致,若一致,则表示该移动终端的认

证通过，并将认证通过的结果写入区块链的对应的交互记录中并广播，完成认证。

[0185] 因此，本发明无需使用USIM卡等物理设备来对移动终端进行认证管理，节省了生产和运输成本。在账户信息的分配过程中采用多重数字签名技术以完成对发送方身份的验证以及发送的账户信息的有效性验证；在账户信息的认证过程中采用私钥加解密技术以完成对移动终端身份的验证，两者结合，构成双重认证机制，提升交互过程的安全性，交互数据的有效性与完整性。另外，结合区块链分布式的特点，所有节点都保存了交互的记录，因此用户可以连接到任意节点去进行认证。使得认证过程不依赖于单个来源，降低了记录被恶意篡改的风险。

[0186] 请参考图6，本发明还提供一种基于区块链的账户信息获取方法，具体的一种实施方式中，具体包括如下步骤：

[0187] S100、向区块链网络发送账户分配请求数据包。

[0188] 本发明实施例中，所述待认证移动终端在区块链网络中发送账户分配请求数据包以请求当前节点分配账户信息，所述账户分配请求数据包包含所述待认证移动终端的身份信息，用于根据待认证移动终端的身份信息为指定的待认证移动终端分配账户信息，所述身份信息可以为所述待认证移动终端的设备识别码或设备序列号等可以唯一性表征所述待认证移动终端的身份的信息。

[0189] 所述待认证移动终端发出账户分配请求数据包之后，将该账户分配请求数据包对应生成的交互记录写入区块链中的第二区块以供其他节点查询或获取数据。

[0190] S101、接收响应于所述账户分配请求数据包的当前节点发送的账户信息，所述账户信息签署了所述认证节点用其私钥生成的唯一性多重数字签名；

[0191] 当前节点向区块链获取所述账户分配请求数据包后，响应于该账户分配请求数据包为所述待认证移动终端分配账户信息。

[0192] 一种可能的设计中，当前节点具体依据如下方案为待认证移动终端分配账户信息：

[0193] 一、当前节点获取所述账户分配请求数据包中的所述待认证移动终端的身份信息，并依据该身份信息为所述待认证移动终端分配账户信息。

[0194] 二、当前节点依据所述身份信息中包括的验证信息，对所述待认证移动终端进行验证，当验证通过后，当前节点用其私钥对上一次交易生成的多重数字签名以及本身的公钥进行散列运算户生成的摘要加密生成当前节点的唯一性多重数字签名，并用该唯一性多重数字签名签署所述账户信息。

[0195] 三、将签署了所述唯一性多重数字签名的账户信息通过区块链网络发送至待认证移动终端。待认证移动终端接收该账户信息并用当前节点的公钥验证该唯一性多重数字签名以验证该账户信息与自身的身份信息相匹配并且该账户信息确实是由当前节点所发送的。

[0196] S102、用当前节点的公钥对所述唯一性多重数字签名进行解密以获取所述账户信息。

[0197] 当前节点为所述待认证移动终端分配账户信息后，将签署了所述唯一性多重数字签名的账户信息、待认证移动终端的身份信息以及当前节点的公钥作为第一交互记录写入第二区块中，其可以是以一种一一映射的对应关系存储于所述第二区块的数据库中并广播

该次的交互记录，当待认证移动终端收到广播后向区块链获取该次交互记录的相关数据。

[0198] 具体而言，待认证移动终端首先获取签署了所述唯一性多重数字签名的账户信息并用当前节点的公钥解密出所述账户信息。待认证移动终端再获取与该账户信息关联性储存于数据库中的待认证移动终端的身份信息，通过对比获取的待认证移动终端的身份信息与自身的身份信息，若匹配，则验证了解密出的账户信息为与自身身份信息相匹配的账户信息。

[0199] 优选的，本发明实施例中，所述待认证移动终端解密出与之身身份信息相匹配的账户信息之后，向区块链发起账户认证请求数据包。与此同时，所述待认证移动终端用自身的私钥对获取的唯一性多重数字签名进行加密生成对应的密文信息，并向区块链发送该密文信息并将所述账户认证请求数据包以及该密文信息作为第二交互记录写入第二区块中并广播。当前节点收到广播后获取所述账户认证请求数据包以及该密文信息以及该认证移动终端的公钥，并用待认证移动终端的公钥解密所述密文信息得到唯一性多重数字签名，当前节点对比解密出的唯一性多重数字签名与其为所述待认证移动终端签署账户信息时签署的唯一性多重数字签名，若二者一致，则验证了待认证移动终端的身份。优选的，当前节点验证完待认证移动终端的身份信息之后将验证结果作为第二交互记录写入所述第二区块中以备查询。本次验证与待认证移动终端验证当前节点的身份够成双重认证机制，提升本方案的可靠性。

[0200] 参考图7所示，本发明还提供一种基于区块链的账户信息获取装置，一种实施例中，包括发送模块100、接收模块101以及解密模块102。其中，

[0201] 发送模块100：向区块链网络发送账户分配请求数据包。

[0202] 本发明实施例中，所述待认证移动终端在区块链网络中发送账户分配请求数据包以请求当前节点分配账户信息，所述账户分配请求数据包包含所述待认证移动终端的身份信息，用于根据待认证移动终端的身份信息为指定的待认证移动终端分配账户信息，所述身份信息可以为所述待认证移动终端的设备识别码或设备序列号等可以唯一性表征所述待认证移动终端的身份的信息。

[0203] 所述待认证移动终端发出账户分配请求数据包之后，将该账户分配请求数据包对应生成的交互记录写入区块链中的第二区块以供其他节点查询或获取数据。

[0204] 接收模块101：接收响应于所述账户分配请求数据包的当前节点发送的账户信息，所述账户信息签署了所述认证节点用其私钥生成的唯一性多重数字签名；

[0205] 当前节点向区块链获取所述账户分配请求数据包后，响应于该账户分配请求数据包为所述待认证移动终端分配账户信息。

[0206] 一种可能的设计中，当前节点具体依据如下方案为待认证移动终端分配账户信息：

[0207] 一、当前节点获取所述账户分配请求数据包中的所述待认证移动终端的身份信息，并依据该身份信息为所述待认证移动终端分配账户信息。

[0208] 二、当前节点依据所述身份信息中包括的验证信息，对所述待认证移动终端进行验证，当验证通过后，当前节点用其私钥对上一次交易生成的多重数字签名以及本身的公钥进行散列运算户生成的摘要加密生成当前节点的唯一性多重数字签名，并用该唯一性多重数字签名签署所述账户信息。

[0209] 三、将签署了所述唯一性多重数字签名的账户信息通过区块链网络发送至待认证移动终端。待认证移动终端接收该账户信息并用当前节点的公钥验证该唯一性多重数字签名以验证该账户信息与自身的身份信息相匹配并且该账户信息确实是由当前节点所发送的。

[0210] 解密模块102：用当前节点的公钥对所述唯一性多重数字签名进行解密以获取所述账户信息。

[0211] 当前节点为所述待认证移动终端分配账户信息后，将签署了所述唯一性多重数字签名的账户信息、待认证移动终端的身份信息以及当前节点的公钥作为第一交互记录写入第二区块中，其可以是以一种一一映射的对应关系存储于所述第二区块的数据库中并广播该次的交互记录，当待认证移动终端收到广播后向区块链获取该次交互记录的相关数据。

[0212] 具体而言，待认证移动终端首先获取签署了所述唯一性多重数字签名的账户信息并用当前节点的公钥解密出所述账户信息。待认证移动终端再获取与该账户信息关联性储存于数据库中的待认证移动终端的身份信息，通过对比获取的待认证移动终端的身份信息与自身的身份信息，若匹配，则验证了解密出的账户信息为与自身身份信息相匹配的账户信息。

[0213] 优选的，本发明实施例中，所述待认证移动终端解密出与之身身份信息相匹配的账户信息之后，向区块链发起账户认证请求数据包。与此同时，所述待认证移动终端用自身的私钥对获取的唯一性多重数字签名进行加密生成对应的密文信息，并向区块链发送该密文信息并将所述账户认证请求数据包以及该密文信息作为第二交互记录写入第二区块中并广播。当前节点收到广播后获取所述账户认证请求数据包以及该密文信息以及该认证移动终端的公钥，并用待认证移动终端的公钥解密所述密文信息得到唯一性多重数字签名，当前节点对比解密出的唯一性多重数字签名与其为所述待认证移动终端签署账户信息时签署的唯一性多重数字签名，若二者一致，则验证了待认证移动终端的身份。优选的，当前节点验证完待认证移动终端的身份信息之后将验证结果作为第二交互记录写入所述第二区块中以备查询。本次验证与待认证移动终端验证当前节点的身份够成双重认证机制，提升本方案的可靠性。

[0214] 结合上述的实施例可知，本发明最大的有益效果在于，本发明通过移动终端配合认证节点完成账户信息的分配与认证过程。

[0215] 具体的，待认证移动终端通过区块链向当前节点发起账户信息的分配请求数据包并将对应的交互记录写入区块链中，当前节点依据该账户信息分配请求为待认证移动终端分配账户信息并将对应的交互记录写入区块链中完成账户信息的分配。

[0216] 待认证移动终端通过区块链向当前节点发送账户信息认证请求数据包，并将对应的交互记录写入区块链中，当前节点依据账户信息认证请求数据包为待认证移动终端认证账户信息并将对应的交互记录写入区块链中，完成账户信息的认证。

[0217] 因此，表现在移动终端，其配合认证节点完成账户信息的分配、认证以及撤销、查询各个交互过程，保证各交互过程的数据传输的准确性与可靠性，配合认证节点完成双重认证机制。

[0218] 本发明实施例还提供一种了一种移动终端，如图8所示，为了便于说明，仅示出了与本发明实施例相关的部分，具体技术细节未揭示的，请参照本发明实施例方法部分。该终

端可以为包括手机、平板电脑、PDA(Personal Digital Assistant,个人数字助理)、POS(Point of Sales,销售终端)、车载电脑等任意终端设备,以终端为手机为例:

[0219] 图8示出的是与本发明实施例提供的终端相关的手机的部分结构的框图。参考图8,手机包括:触敏显示器0813、处理器0811、存储器0814等部件。本领域技术人员可以理解,图8中示出的手机结构并不构成对手机的限定,可以包括比图示更多或更少的部件,或者组合某些部件,或者不同的部件布置。

[0220] 下面结合图8对手机的各个构成部件进行具体的介绍:

[0221] 存储器0814可用于存储软件程序以及模块,处理器0811通过运行存储在存储器0814的软件程序以及模块,从而执行手机的各种功能应用以及数据处理。存储器0814可主要包括存储程序区和存储数据区,其中,存储程序区可存储操作系统、至少一个功能所需的应用程序(比如声音播放功能、图像播放功能等)等;存储数据区可存储根据手机的使用所创建的数据(比如音频数据、电话本等)等。此外,存储器0814可以包括高速随机存取存储器,还可以包括非易失性存储器,例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。

[0222] 触敏显示器0813可包括触摸检测装置和触摸控制器两个部分。其中,触摸检测装置检测用户的触摸方位,并检测触摸操作带来的信号,将信号传送给触摸控制器;触摸控制器从触摸检测装置上接收触摸信息,并将它转换成触点坐标,再送给处理器,并能接收处理器发来的命令并加以执行。此外,可以采用电阻式、电容式、红外线以及表面声波等多种类型实现触敏显示器。

[0223] 触敏显示器0813可用于显示由用户输入的信息或提供给用户的信息以及手机的各种菜单,如信息编辑界面等。触敏显示器0813可包括显示面板,可选的,可以采用液晶显示器(Liquid Crystal Display,LCD)、有机发光二极管(Organic Light-Emitting Diode,OLED)等形式来配置触敏显示器。进一步的,当触敏显示器0813检测到在其上或附近的触摸操作后,传送给处理器以确定触摸事件的类型,随后处理器根据触摸事件的类型在触敏显示器上提供相应的视觉输出。

[0224] 手机还可包括至少一种传感器0812,比如光传感器、运动传感器以及其他传感器。具体地,光传感器可包括环境光传感器及接近传感器,其中,环境光传感器可根据环境光线的明暗来调节显示面板的亮度,接近传感器可在手机移动到耳边时,关闭显示面板和/或背光。作为运动传感器的一种,加速计传感器可检测各个方向上(一般为三轴)加速度的大小,静止时可检测出重力的大小及方向,可用于识别手机姿态的应用(比如横竖屏切换、相关游戏、磁力计姿态校准)、振动识别相关功能(比如计步器、敲击)等;至于手机还可配置的陀螺仪、气压计、湿度计、温度计、红外线传感器等其他传感器,在此不再赘述。

[0225] 处理器0811是手机的控制中心,利用各种接口和线路连接整个手机的各个部分,通过运行或执行存储在存储器0814内的软件程序和/或模块,以及调用存储在存储器0814内的数据,执行手机的各种功能和处理数据,从而对手机进行整体监控。可选的,处理器0811可包括一个或多个处理单元;优选的,处理器0811可集成应用处理器和调制解调处理器,其中,应用处理器主要处理操作系统、用户界面和应用程序等,调制解调处理器主要处理无线通信。可以理解的是,上述调制解调处理器也可以不集成到处理器0811中。

[0226] 手机还包括给各个部件供电的电源(比如电池),优选的,电源可以通过电源管理

系统与处理器0811逻辑相连，从而通过电源管理系统实现管理充电、放电、以及功耗管理等功能。

[0227] 尽管未示出，手机还可以包括摄像头、蓝牙模块等，在此不再赘述。

[0228] 在本发明实施例中，该终端所包括的处理器0811还具有以下功能：

[0229] 向区块链网络发送账户分配请求数据包；

[0230] 接收响应于所述账户分配请求数据包的当前节点发送的账户信息，所述账户信息签署了所述认证节点用其私钥生成的唯一性多重数字签名；

[0231] 用当前节点的公钥对所述唯一性多重数字签名进行解密以获取所述账户信息。

[0232] 所述区块链包括用于存储各节点的私钥的第一区块以及用于存储其他内容的第二区块，当前节点将处理所述账户分配请求数据包对应生成的包括所述账户信息、待认证移动终端的身份信息、所述唯一性多重数字签名以及认证节点的公钥的第一交互记录写入所述第二区块中，并在区块链网络中广播所述第一交互记录。

[0233] 获取与所述账户信息关联性储存于所述第二区块中的待认证移动终端的身份信息；

[0234] 对比该身份信息与自身的身份信息，若一致，则验证所述账户信息有效。

[0235] 向区块链发起账户认证请求数据包，并向区块链发送所述待认证移动终端用其私钥加密所述唯一性多重数字签名生成的密文信息以供当前节点依据该账户认证请求数据包以及所述密文信息对所述待认证移动终端进行认证。

[0236] 将包含所述移动终端的公钥以及处理所述账户认证请求数据包对应生成的所述密文信息的第二交互记录写入所述区块链的第二区块中，并在区块链网络中广播所述第二交互记录。

[0237] 将验证后的结果反馈至所述区块链。

[0238] 本领域普通技术人员可以理解上述实施例的全部或部分步骤是可以通过程序来指令相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：只读存储器(ROM,Read Only Memory)、随机存取存储器(RAM,Random Access Memory)、磁盘或光盘等。

[0239] 本领域普通技术人员可以理解实现上述实施例的全部或部分步骤是可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0240] 以上对本发明所提供的一种移动终端进行了详细介绍，对于本领域的一般技术人员，依据本发明实施例的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

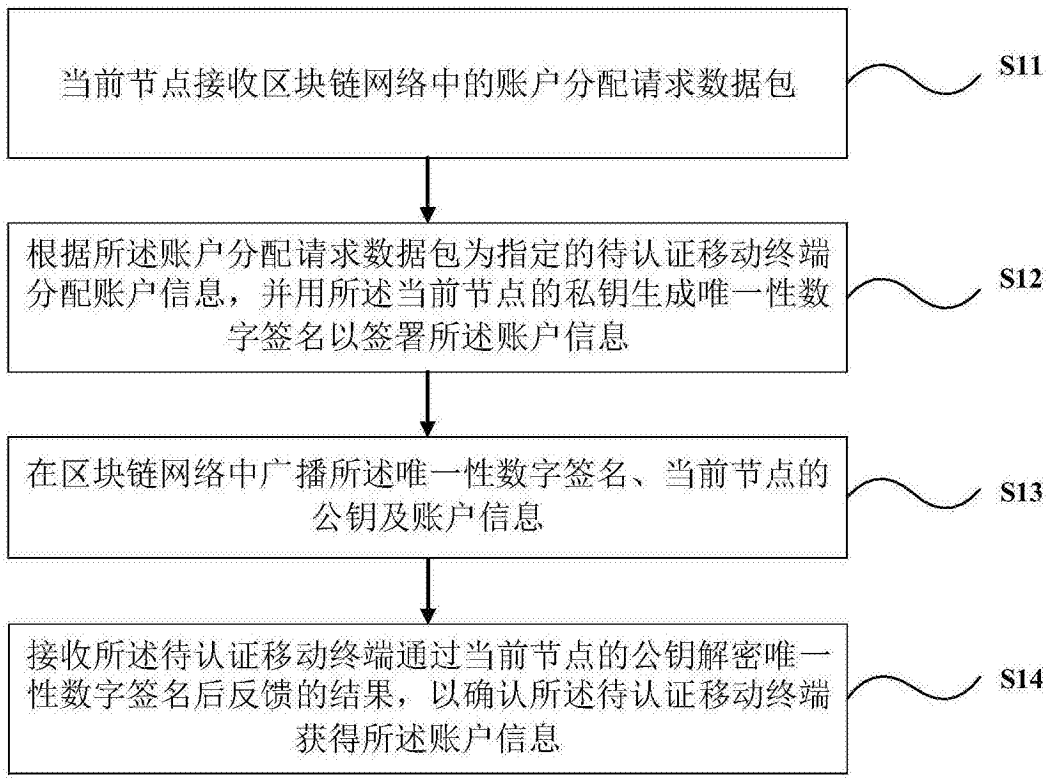

当前节点接收区块链网络中的账户分配请求数据包
S11
根据所述账户分配请求数据包为指定的待认证移动终端分配账户信息，并用所述当前节点的私钥生成唯一性数字签名以签署所述账户信息
S12
在区块链网络中广播所述唯一性数字签名、当前节点的公钥及账户信息
S13
接收所述待认证移动终端通过当前节点的公钥解密唯一性数字签名后反馈的结果，以确认所述待认证移动终端获得所述账户信息
S14

图1

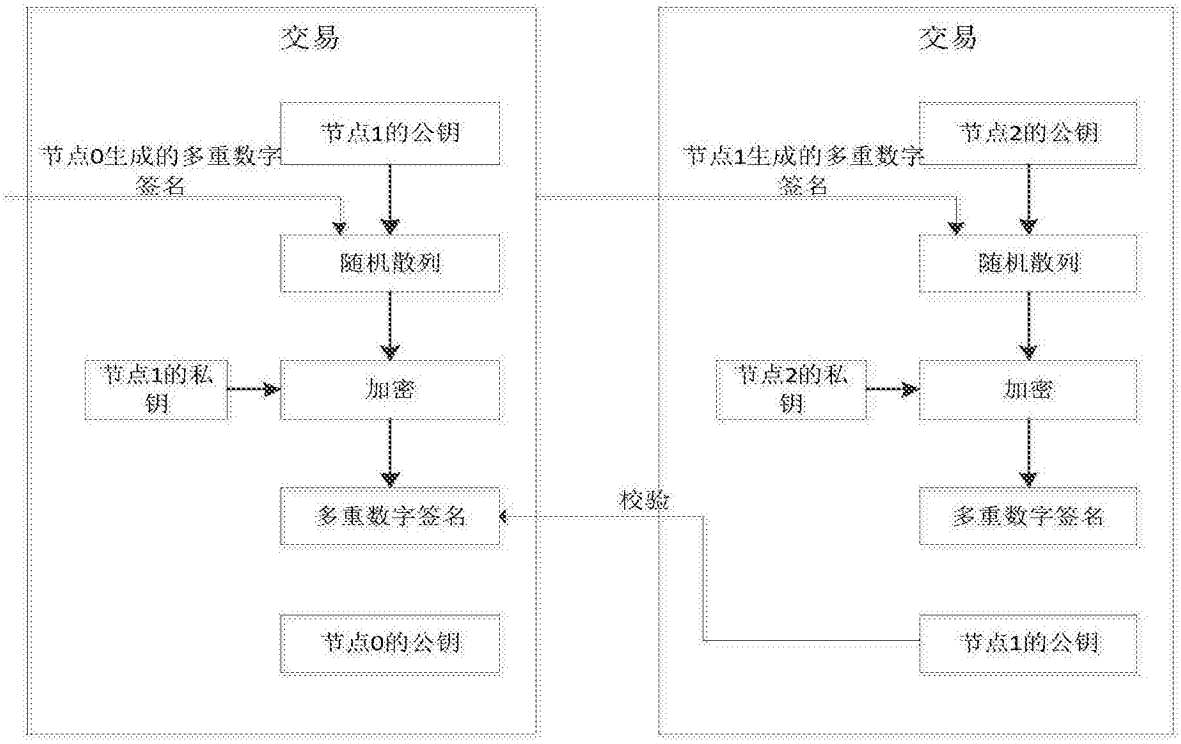

交易
节点1的公钥
节点0生成的多重数字签名
随机散列
节点1的私钥
加密
多重数字签名
节点0的公钥
交易
节点2的公钥
节点1生成的多重数字签名
随机散列
节点2的私钥
加密
多重数字签名
节点1的公钥
校验

图2

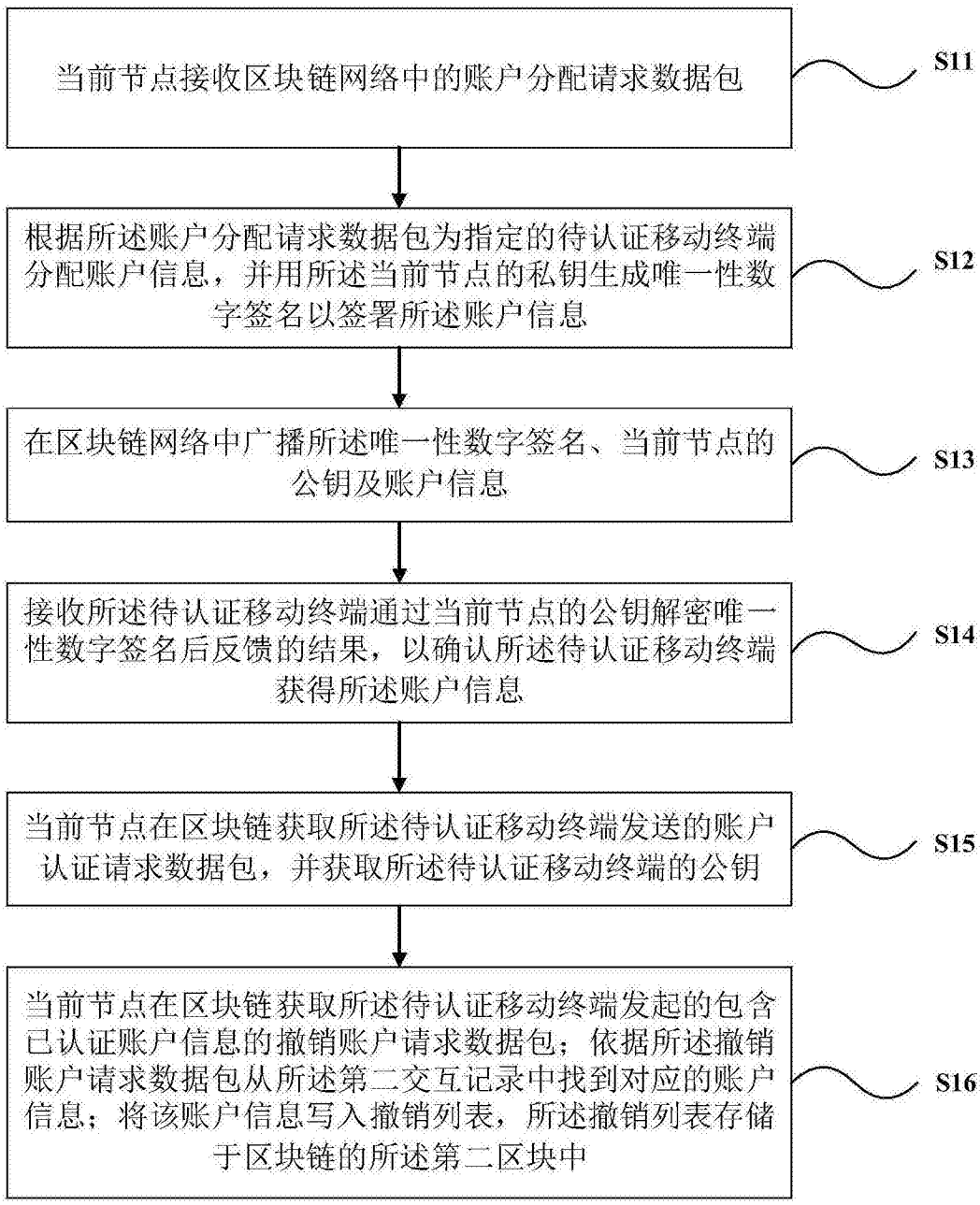

当前节点接收区块链网络中的账户分配请求数据包
S11
根据所述账户分配请求数据包为指定的待认证移动终端分配账户信息，并用所述当前节点的私钥生成唯一性数字签名以签署所述账户信息
S12
在区块链网络中广播所述唯一性数字签名、当前节点的公钥及账户信息
S13
接收所述待认证移动终端通过当前节点的公钥解密唯一性数字签名后反馈的结果，以确认所述待认证移动终端获得所述账户信息
S14
当前节点在区块链获取所述待认证移动终端发送的账户认证请求数据包，并获取所述待认证移动终端的公钥
S15
当前节点在区块链获取所述待认证移动终端发起的包含已认证账户信息的撤销账户请求数据包；依据所述撤销账户请求数据包从所述第二交互记录中找到对应的账户信息；将该账户信息写入撤销列表，所述撤销列表存储于区块链的所述第二区块中
S16

图3

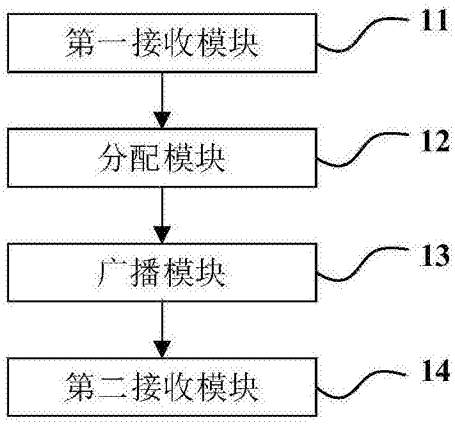

第一接收模块
11
分配模块
12
广播模块
13
第二接收模块
14

图4

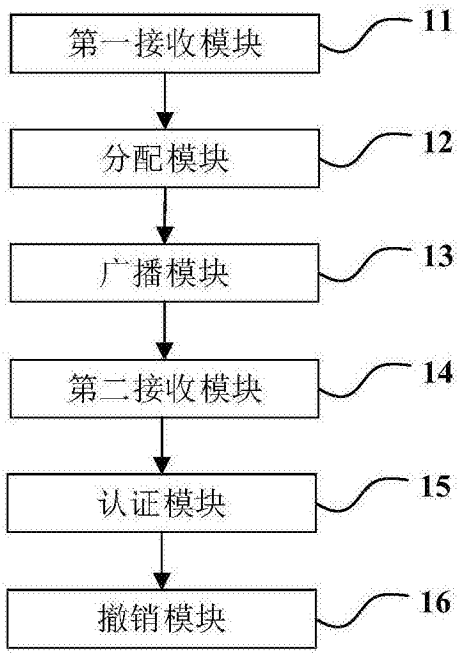

第一接收模块
11
分配模块
12
广播模块
13
第二接收模块
14
认证模块
15
撤销模块
16

图5

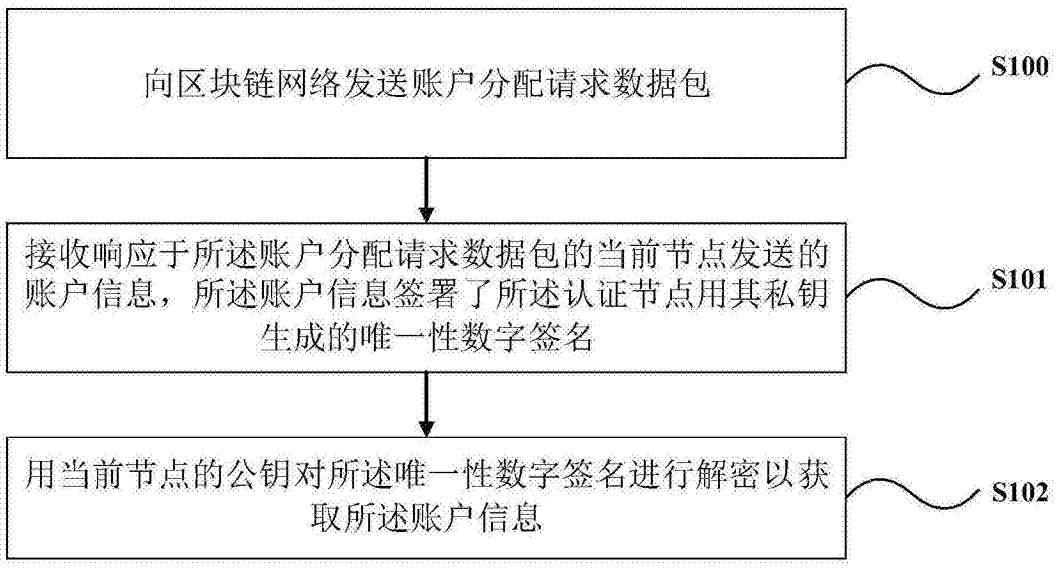

向区块链网络发送账户分配请求数据包
S100
接收响应于所述账户分配请求数据包的当前节点发送的账户信息，所述账户信息签署了所述认证节点用其私钥生成的唯一性数字签名
S101
用当前节点的公钥对所述唯一性数字签名进行解密以获取所述账户信息
S102

图6

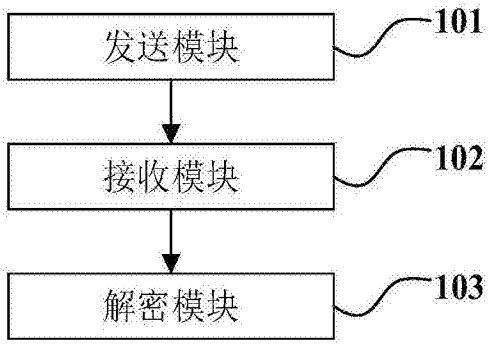

发送模块
101
接收模块
102
解密模块
103

图7

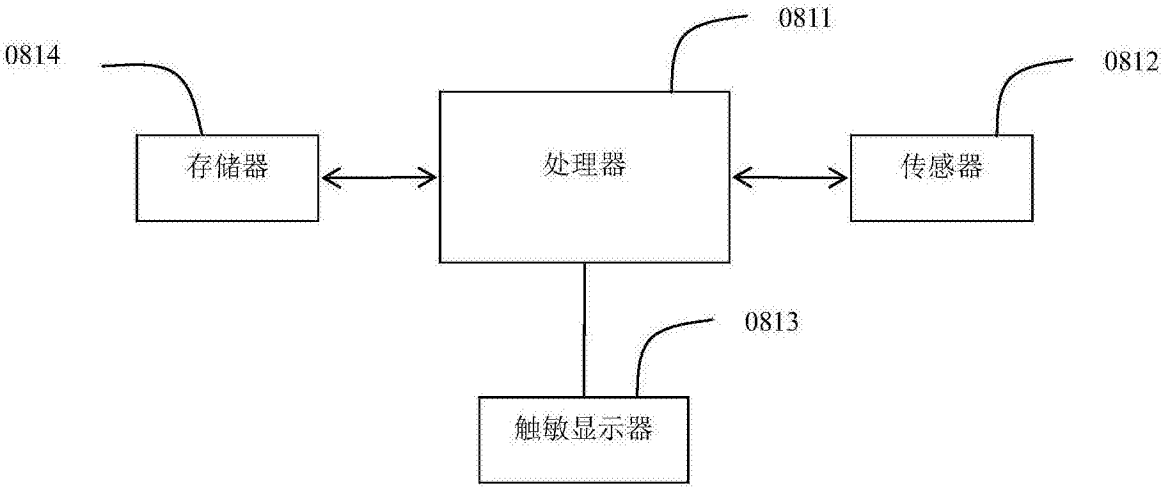

0811
0814
0812
存储器
处理器
传感器
0813
触敏显示器

图8