(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108322558 B
(45)授权公告日 2021.01.01

(21)申请号 201711454866.X
(22)申请日 2017.12.28
(65)同一申请的已公布的文献号
申请公布号 CN 108322558 A
(43)申请公布日 2018.07.24
(73)专利权人 北京欧链科技有限公司
地址 100036 北京市海淀区翠微中里14号楼三层B153
(72)发明人 宋承根 谭智勇 赵微
(74)专利代理机构 北京鼎佳达知识产权代理事务所(普通合伙) 11348
代理人 王伟锋 刘铁生
(51)Int.Cl.
H04L 29/12(2006.01)
H04L 9/06(2006.01)
H04L 9/32(2006.01)

(56)对比文件
CN 104392354 A,2015.03.04
CN 104320262 A,2015.01.28
CN 106453407 A,2017.02.22
CN 106357640 A,2017.01.25
CN 107493162 A,2017.12.19
US 2017324711 A1,2017.11.09
CN 106372940 A,2017.02.01
李昊星,等.支持身份认证的数据持有性证明方案.《通信学报》.2016,第37卷(第10期),第2016203-1--2016203-9页.

审查员 王淑婷

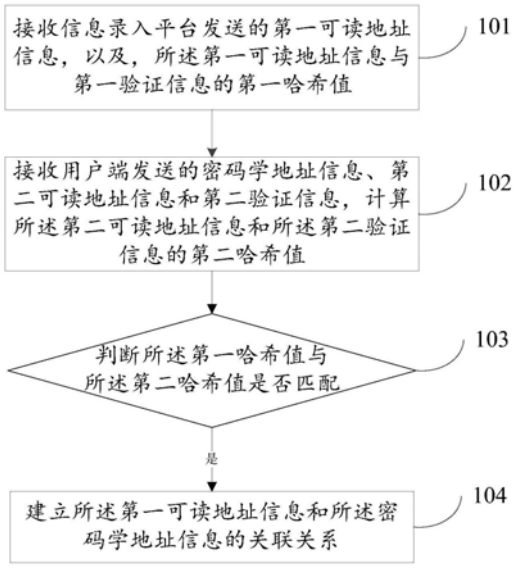
权利要求书2页 说明书9页 附图4页

(54)发明名称

关联地址信息的方法、装置及系统

(57)摘要

本发明公开了一种关联地址信息的方法、装置及系统,其中方法包括:接收信息录入平台发送的第一可读地址信息,以及,所述第一可读地址信息与第一验证信息的第一哈希值;接收用户端发送的密码学地址信息、第二可读地址信息和第二验证信息,计算所述第二可读地址信息和所述第二验证信息的第二哈希值;判断所述第一哈希值与所述第二哈希值是否相同;若所述第一哈希值与所述第二哈希值相同,建立所述第一可读地址信息和所述密码学地址信息的关联关系。通过对用户在区块链上注册的表明身份的地址信息进行验证,由此解决了用户特有地址信息被注册的问题,从而能够实现保证表明用户身份的地址的真实性。



CN 108322558 B

1.一种关联地址信息的方法,应用于区块链,其特征在于,包括:

接收信息录入平台发送的第一可读地址信息,以及,所述第一可读地址信息与第一验证信息的第一哈希值,其中,所述第一可读地址信息包括目标用户的可读地址,所述第一验证信息为所述信息录入平台根据所述第一可读地址信息生成的验证信息,所述目标用户的可读地址包括所述目标用户的邮箱地址或所述目标用户的手机号码;

接收用户端发送的密码学地址信息、第二可读地址信息和第二验证信息;

计算所述第二可读地址信息和所述第二验证信息的第二哈希值;

判断所述第一哈希值与所述第二哈希值是否相同;

若所述第一哈希值与所述第二哈希值相同,建立所述第一可读地址信息和所述密码学地址信息的关联关系。

2.如权利要求1所述的关联地址信息的方法,其特征在于,在所述若所述第一哈希值与所述第二哈希值相同,建立所述第一可读地址信息和所述密码学地址信息的关联关系之后,所述方法还包括:

向用户端发送所述第一可读地址信息和所述密码学地址信息关联成功的信息。

3.如权利要求2所述的关联地址信息的方法,其特征在于,还包括:接收用户端发送的身份标识信息,建立所述身份标识信息与所述第一可读地址信息以及所述密码学地址信息的关联关系,其中,所述身份标识信息包括用于表征用户身份的标识信息。

4.如权利要求2所述的关联地址信息的方法,其特征在于,还包括:

若所述第一哈希值和所述第二哈希值不相同,向用户端发送所述第一可读地址信息和所述密码学地址信息关联失败的信息。

5.一种关联地址信息的装置,应用于区块链,其特征在于,包括:

第一信息接收单元,用于接收信息录入平台发送的第一可读地址信息,以及,所述第一可读地址信息与第一验证信息的第一哈希值,其中,所述第一可读地址信息包括目标用户的可读地址,所述第一验证信息为信息录入平台根据所述第一可读地址信息生成的验证信息;所述目标用户的可读地址包括所述目标用户的邮箱地址或所述目标用户的手机号码;

第二信息接收单元,用于接收用户端发送的密码学地址信息、第二可读地址信息和第二验证信息;

信息计算单元,用于计算所述第二可读地址信息和所述第二验证信息的第二哈希值;

信息验证单元,用于判断所述第一哈希值与所述第二哈希值是否相同;

任务执行单元,用于若所述第一哈希值与所述第二哈希值相同,建立所述第一可读地址信息和所述密码学地址信息的关联关系。

6.如权利要求5所述的关联地址信息的装置,其特征在于,还包括:

信息发送单元,用于在所述任务执行单元在所述第一哈希值与所述第二哈希值相同时,建立所述第一可读地址信息和所述密码学地址信息的关联关系之后,向用户端发送所述第一可读地址信息和所述密码学地址信息关联成功的信息。

7.如权利要求6所述的关联地址信息的装置,其特征在于,

所述信息接收单元还用于接收用户端发送的身份标识信息,其中,所述身份标识信息包括用于表征用户身份的标识信息;

所述任务执行单元还用于,建立所述身份标识信息与所述第一可读地址信息以及所述

密码学地址信息的关联关系。

8.如权利要求6所述的关联地址信息的装置,其特征在于,所述信息发送单元还用于:

若所述第一哈希值和所述第二哈希值不相同,向用户端发送所述第一可读地址信息和所述密码学地址信息关联失败的信息。

9.一种关联地址信息的系统,其特征在于,包括信息录入平台、用户端和区块链,所述信息录入平台、所述用户端和所述区块链通信连接;

所述信息录入平台用于向所述区块链发送第一可读地址信息,以及,所述第一可读地址信息与第一验证信息的第一哈希值,其中,所述第一可读地址信息包括目标用户的可读地址,所述第一验证信息为所述信息录入平台根据所述第一可读地址信息生成的验证信息;所述目标用户的可读地址包括所述目标用户的邮箱地址或所述目标用户的手机号码;

所述用户端用于向所述区块链发送密码学地址信息、第二可读地址信息和第二验证信息;

所述区块链用于接收信息录入平台发送的第一可读地址信息,以及,所述第一可读地址信息与第一验证信息的第一哈希值,接收用户端发送的密码学地址信息、第二可读地址信息和第二验证信息;计算所述第二可读地址信息和所述第二验证信息的第二哈希值;判断所述第一哈希值与所述第二哈希值是否相同;若所述第一哈希值与所述第二哈希值相同,建立所述第一可读地址信息和所述密码学地址信息的关联关系。

关联地址信息的方法、装置及系统

技术领域

[0001] 本发明涉及互联网技术领域，具体涉及一种关联地址信息的方法、装置及系统。

背景技术

[0002] 随着信息技术的不断发展，互联网的应用也越来越普及，例如，用户可以通过互联网进行网上交易、发表言论等行为。通常情况下，用户通过互联网进行这些行为需要一个能够表明用户身份的地址，以保证用户身份的真实性。

[0003] 现有的区块链技术中，表明用户身份的地址是由用户自己决定的，一般是一串不可读的字符串，或者一串可读的字符串和不可读的字符串的结合。这样，用户在注册表明用户身份的地址时可以随机注册，导致部分用户特有的地址被其他人注册，比如用户的手机号、邮箱等，从而影响表明用户身份的地址的真实性。

发明内容

[0004] 鉴于上述问题，提出了本发明提供一种关联地址信息的方法、装置及系统，以便克服现有技术中表明用户身份的地址在区块链中被他人注册，进而影响区块链中表明用户身份的地址的真实性的问题。

[0005] 依据本发明的一个方面，提供了一种关联地址信息的方法，应用于区块链，包括：

[0006] 接收信息录入平台发送的第一可读地址信息，以及，所述第一可读地址信息与第一验证信息的第一哈希值，其中，所述第一可读地址信息包括目标用户的可读地址，所述第一验证信息为所述信息录入平台根据所述第一可读地址信息生成的验证信息；

[0007] 接收用户端发送的密码学地址信息、第二可读地址信息和第二验证信息；

[0008] 计算所述第二可读地址信息和所述第二验证信息的第二哈希值；

[0009] 判断所述第一哈希值与所述第二哈希值是否相同；

[0010] 若所述第一哈希值与所述第二哈希值相同，建立所述第一可读地址信息和所述密码学地址信息的关联关系。

[0011] 可选地，在所述若所述第一哈希值与所述第二哈希值相同，建立所述第一可读地址信息和所述密码学地址信息的关联关系之后，还包括：

[0012] 向用户端发送所述第一可读地址信息和所述密码学地址信息关联成功的信息。

[0013] 可选地，还包括：接收用户端发送的身份标识信息，建立所述身份标识信息与所述第一可读地址信息以及所述密码学地址信息的关联关系，其中，所述身份标识信息包括用于表征用户身份的标识信息。

[0014] 可选地，还包括：若所述第一哈希值和所述第二哈希值不相同，向用户端发送所述第一可读地址信息和所述密码学地址信息关联失败的信息。

[0015] 可选地，所述目标用户的可读地址包括所述目标用户的邮箱地址或所述目标用户的手机号码。

[0016] 依据本发明的另一个方面，提供了一种关联地址信息的装置，应用于区块链，包

括：

[0017] 第一信息接收单元，用于接收信息录入平台发送的第一可读地址信息，以及，所述第一可读地址信息与第一验证信息的第一哈希值，其中，所述第一可读地址信息包括目标用户的可读地址，所述第一验证信息为信息录入平台根据所述第一可读地址信息生成的验证信息；

[0018] 第二信息接收单元，用于接收用户端发送的密码学地址信息、第二可读地址信息和第二验证信息；

[0019] 信息计算单元，用于计算所述第二可读地址信息和所述第二验证信息的第二哈希值；

[0020] 信息验证单元，用于判断所述第一哈希值与所述第二哈希值是否相同；

[0021] 任务执行单元，用于若所述第一哈希值与所述第二哈希值相同，建立所述第一可读地址信息和所述密码学地址信息的关联关系。

[0022] 可选地，还包括：

[0023] 信息发送单元，用于在所述任务执行单元在所述第一哈希值与所述第二哈希值相同时，建立所述第一可读地址信息和所述密码学地址信息的关联关系之后，向用户端发送所述第一可读地址信息和所述密码学地址信息关联成功的信息。

[0024] 可选地，所述信息接收单元还用于接收用户端发送的身份标识信息，其中，所述身份标识信息包括用于表征用户身份的标识信息；

[0025] 所述任务执行单元还用于，建立所述身份标识信息与所述第一可读地址信息以及所述密码学地址信息的关联关系。

[0026] 可选地，所述信息发送单元还用于：

[0027] 若所述第一哈希值和所述第二哈希值不相同，向用户端发送所述第一可读地址信息和所述密码学地址信息关联失败的信息。

[0028] 可选地，所述目标用户的地址包括所述目标用户的邮箱地址或所述目标用户的手机号码。

[0029] 依据本发明的再一个方面，提供了一种关联地址信息的系统，包括信息录入平台、用户端和区块链，所述信息录入平台、所述用户端和所述区块链通信连接；

[0030] 所述信息录入平台用于向所述区块链发送第一可读地址信息，以及，所述第一可读地址信息与第一验证信息的第一哈希值，其中，所述第一可读地址信息包括目标用户的可读地址，所述第一验证信息为所述信息录入平台根据所述第一可读地址信息生成的验证信息；

[0031] 所述用户端用于向所述区块链发送密码学地址信息、第二可读地址信息和第二验证信息；

[0032] 所述区块链用于接收信息录入平台发送的第一可读地址信息，以及，所述第一可读地址信息与第一验证信息的第一哈希值，接收用户端发送的密码学地址信息、第二可读地址信息和第二验证信息；计算所述第二可读地址信息和所述第二验证信息的第二哈希值；判断所述第一哈希值与所述第二哈希值是否相同；若所述第一哈希值与所述第二哈希值相同，建立所述第一可读地址信息和所述密码学地址信息的关联关系。

[0033] 根据本发明的关联地址信息的方法、装置及系统，在用户在区块链上注册表明自

己身份的地址时，由区块链接收用户通过信息录入平台发送的第一可读地址信息，以及由第一可读地址信息与第一验证信息计算得到的第一哈希值，同时，接收用户端发送的密码学地址信息、第二可读地址信息和第二验证信息，并通过计算第二可读地址信息和第二验证信息得到第二哈希值，再通过判断第一哈希值与第二哈希值是否相同来验证第一可读地址信息与第二可读地址信息是否相同，当第一可读地址信息与第二可读地址信息相同时，则可以确认通过信息录入平台发送第一可读地址信息的用户与通过用户端发送第二可读地址信息的用户为同一用户，进而建立第一可读地址信息与区块链分配给用户的密码学地址信息的关联关系，使第一可读地址信息与密码学地址信息唯一对应，确保了用户在区块上注册表明自己身份的地址的真实性，进而确保了区块链中表明用户身份的地址的真实性。

[0034] 可以对用户在区块链上注册的表明身份的地址信息进行验证，由此解决了用户特有地址信息被注册的问题，从而能够实现保证表明用户身份的地址的真实性。

[0035] 上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

[0036] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0037] 图1示出了本发明实施例一的关联地址信息的方法的流程图；

[0038] 图2示出了本发明实施例二的关联地址信息的方法的流程图；

[0039] 图3示出了本发明实施例三的关联地址信息的方法的流程图；

[0040] 图4示出了本发明实施例四的关联地址信息的装置的结构图；

[0041] 图5示出了本发明实施例五的关联地址信息的装置的结构图；

[0042] 图6示出了本发明实施例六的关联地址信息的系统的结构图。

具体实施方式

[0043] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0044] 本发明实施例提供一种应用于区块链的关联地址信息的方法，如图1所示，为本发明实施例一的关联地址信息的方法的流程图。从图1中可以看出，本实施例的关联地址信息的方法，包括以下步骤：

[0045] S101：接收信息录入平台发送的第一可读地址信息，以及，所述第一可读地址信息与第一验证信息的第一哈希值，其中，所述第一可读地址信息包括目标用户的可读地址，所述第一验证信息为信息录入平台根据所述第一可读地址信息生成的验证信息。

[0046] 在本实施例中，信息录入平台可以是应用区块链技术的具有交易功能的平台，例

如电子商城，也可以是应用区块链技术的具有支付功能的平台，例如银行，还可以是应用区块链技术的具有通信功能的平台，例如论坛或者社交软件类平台。当用户在所述信息录入平台注册表征用户身份的账号时，所述信息录入平台会要求用户输入第一可读地址信息，所述第一可读地址信息包含有用户特有的地址，以完成对用户身份的合法性的验证，用户特有的地址可以是用户的手机号码或邮箱等。当信息录入平台获取到用户输入的第一可读地址信息后，根据所述第一可读地址信息，随机生成第一验证信息，该第一验证信息与所述第一可读地址信息一一对应。所述第一验证信息可以是包含多个字符的验证码。信息录入平台计算所述第一可读地址信息和对应的第一验证信息的第一哈希值，并将所述第一可读地址信息和所述第一哈希值发送至区块链中，此时，区块链执行如步骤S101所述的步骤。

[0047] 需要说明的是，哈希值是一段数据的唯一且极其紧凑的数值表示形式，信息录入平台计算第一哈希值采用的哈希算法为现有技术中公知的哈希算法，这里不做具体限定和解释。

[0048] S102：接收用户端发送的密码学地址信息、第二可读地址信息和第二验证信息，计算所述第二可读地址信息和所述第二验证信息的第二哈希值。

[0049] 在本实施例中，用户端可以是手机、笔记本、平板电脑或者车载电脑，当用户通过用户端在应用区块链技术的信息录入平台注册表征用户身份的账号时，用户可以将密码学地址信息、第二可读地址信息和第二验证信息发送至区块链中，其中，密码学地址信息为用户在区块链中的特有的地址信息，该密码学地址信息具有识别用户身份的唯一标识，不同用户在区块链中的密码学地址信息不同。通常，密码学地址信息为一串不可读的字符串，在正常语言环境下没有特定含义，用其表示用户的身份不容易被识别，因此，用户通常需要一个在区块链中能够表明自己身份且容易被识别的可读地址信息，并建立该可读地址信息和用户的密码学地址信息之间的关联关系，即建立可读地址信息和用户的密码学地址信息之间的对应的关系。第二可读地址信息包含有用户特有的地址，以完成对用户身份的合法性的验证，用户特有的地址可以是用户的手机号码或邮箱等。第二验证信息也可以是包含多个字符的验证码。因此，当用户在所述信息录入平台注册表征用户身份的账号时，还会向区块链发送密码学地址信息、第二可读地址信息和第二验证信息，以完成对用户身份的认证。

[0050] 通常情况下，所述第二可读地址信息与用户通过用户端向信息录入平台发送的第一可读地址信息相同，第二验证信息与信息录入平台根据所述第一可读地址信息生成的验证信息相同。此时在信息录入平台注册表征用户身份的账号的用户与向区块链发送上述密码学地址信息、第二可读地址信息和第二验证信息的用户可以被认定为同一用户。

[0051] 区块链在接收到的用户端发送的密码学地址信息、第二可读地址信息和第二验证信息后，计算所述第二可读地址信息和所述第二验证信息的第二哈希值。第二哈希值的算法与第一哈希值的算法可以相同，当然根据实际需要，第二哈希值的算法与第一哈希值的算法也可以不相同。

[0052] S103：判断所述第一哈希值与所述第二哈希值是否相同。

[0053] 在计算得到所述第二可读地址信息和所述第二验证信息的第二哈希值后，区块链将第一哈希值与第二哈希值比较，并判断第一哈希值与第二哈希值是否相同。

[0054] S104：若所述第一哈希值与所述第二哈希值相同，建立所述第一可读地址信息和所述密码学地址信息的关联关系。

[0055] 在本实施例中，当区块链判断并得出第一哈希值与所述第二哈希值相同后，即所述第二可读地址信息与用户通过用户端向信息录入平台发送的第一可读地址信息相同，第二验证信息与信息录入平台根据所述第一可读地址信息生成的验证信息相同，则建立所述第一可读地址信息和所述密码学地址信息的关联关系，即将所述第一可读地址信息和所述密码学地址信息绑定。绑定的方式可以为将所述第一可读地址信息和所述密码学地址信息单向对应，也可以说将所述第一可读地址信息和所述密码学地址信息双向对应，即所述密码学地址信息能且仅能与一个第一可读地址信息对应。

[0056] 由于所述密码学地址信息为用户在区块链中的特有的地址信息，将所述第一可读地址信息和所述密码学地址信息绑定后，所述第一可读地址信息也为用户在区块链中的特有的地址信息，因此，所述第一可读地址信息中的用户特有的地址不可再被注册。这样，实现了保证表明用户身份的地址的真实性，即第一可读地址信息与用户身份相对应。

[0057] 本实施例中关联地址信息的方法，在用户在区块链上注册表明自己身份的地址时，由区块链接收用户通过信息录入平台发送的第一可读地址信息，以及由第一可读地址信息与第一验证信息计算得到的第一哈希值，同时，接收用户端发送的密码学地址信息、第二可读地址信息和第二验证信息，并通过计算第二可读地址信息和第二验证信息得到第二哈希值，再通过判断第一哈希值与第二哈希值是否相同来验证第一可读地址信息与第二可读地址信息是否相同，当第一可读地址信息与第二可读地址信息相同时，则可以确认通过信息录入平台发送第一可读地址信息的用户与通过用户端发送第二可读地址信息的用户为同一用户，进而建立第一可读地址信息与区块链分配给用户的密码学地址信息的关联关系，使第一可读地址信息与密码学地址信息唯一对应，确保了用户在区块上注册表明自己身份的地址的真实性，进而确保了区块链中表明用户身份的地址的真实性。

[0058] 如图2所示，示出了本发明实施例二的关联地址信息的方法的流程图，作为本发明的一个可选实施例，在上述实施例中的步骤S104之后，所述关联地址信息的方法还可以包括：

[0059] S205：向用户端发送所述第一可读地址信息和所述密码学地址信息关联成功的信息。

[0060] 这样，可以将所述第一可读地址信息和所述密码学地址信息关联成功的信息告知用户。

[0061] 此外还可以包括：

[0062] S206：接收用户端发送的身份标识信息，建立所述身份标识信息与所述第一可读地址信息以及所述密码学地址信息的关联关系，其中，所述身份标识信息包括用于表征用户身份的标识信息。

[0063] 在本实施例中，当建立所述第一可读地址信息和所述密码学地址信息的关联关系后，还可以进一步的建立身份标识信息与所述第一可读地址信息以及所述密码学地址信息的关联关系。其中，所述身份标识信息包括用于表征用户身份的标识信息，所述标识信息可以为用户的名称、昵称或笔名等，其可以作为用户身份的另一种表示。

[0064] 此外，在上述实施例中的步骤S104之后，所述关联地址信息的方法还可以包括：

[0065] S207：若所述第一哈希值和所述第二哈希值不相同，向用户端发送所述第一可读地址信息和所述密码学地址信息关联失败的信息。

[0066] 这样，当所述第一可读地址信息和所述密码学地址信息关联失败时，可以及时通知用户，用户可以及时采取相应的措施，例如，重新注册。

[0067] 本实施例中关联地址信息的方法，在用户在区块链上注册表明自己身份的地址时，由区块链接收用户通过信息录入平台发送的第一可读地址信息，以及由第一可读地址信息与第一验证信息计算得到的第一哈希值，同时，接收用户端发送的密码学地址信息、第二可读地址信息和第二验证信息，并通过计算第二可读地址信息和第二验证信息得到第二哈希值，再通过判断第一哈希值与第二哈希值是否相同来验证第一可读地址信息与第二可读地址信息是否相同，当第一可读地址信息与第二可读地址信息相同时，则可以确认通过信息录入平台发送第一可读地址信息的用户与通过用户端发送第二可读地址信息的用户为同一用户，进而建立第一可读地址信息与区块链分配给用户的密码学地址信息的关联关系，使第一可读地址信息与密码学地址信息唯一对应，确保了用户在区块上注册表明自己身份的地址的真实性，进而确保了区块链中表明用户身份的地址的真实性。

[0068] 在本实施例中，信息录入平台发送至区块链的第一可读地址信息可以是由用户端发送至信息录入平台中的，第一可读地址信息包括目标用户的地址，信息录入平台在接收到所述第一可读地址信息后，根据所接收到的第一可读地址信息生成对应的第一验证信息，并将所生成的第一验证信息发送至对应目标用户的地址的用户端。另一方面，信息录入平台计算第一可读地址信息与第一验证信息的第一哈希值，并将第一可读地址信息和第一哈希值发送至区块链中。

[0069] 用户端在接收到的信息录入平台发送的第一验证信息后，可以将该第一验证信息作为第二验证信息发送至区块链中，并将第一可读地址信息作为第二地址信息发送至区块链中，同时将密码学地址信息发送至区块链中。需要说明的是，这里的“第一”和“第二”是相对与区块链而言的。在本实施例中，第一可读地址信息与第二地址信息相同，第一验证信息也与第二验证信息相同。

[0070] 本实施例的方法，可以保证在信息录入平台注册表征用户身份的账号的用户与向区块链发送密码学地址信息、第二可读地址信息和第二验证信息的用户的身份的一致性，即可以对用户在区块链上注册的表明身份的地址信息进行验证，由此解决了用户特有地址信息被注册的问题，从而能够实现保证表明用户身份的地址的真实性。

[0071] 此外，还可以在区块链中预设接收信息录入平台发送的第一可读地址信息，以及，所述第一可读地址信息与第一验证信息的第一哈希值相对与接收用户端发送的密码学地址信息、第二可读地址信息和第二验证信息的时间间隔。当两次接收信息的时间间隔大于预设的时间间隔时，则不再判断所述第一哈希值与所述第二哈希值是否相同，都不再建立所述第一可读地址信息和所述密码学地址信息的关联关系。可选的，还可以将包含接收用户端发送的密码学地址信息、第二可读地址信息和第二验证信息的时间相对应与接收第一可读地址信息，以及，所述第一可读地址信息与第一验证信息的第一哈希值的时间间隔超多预设时间间隔的信息方式至用户端，以通知用户重新验证。

[0072] 如图3所示，示出了本发明实施例三的关联地址信息的方法的流程图。

[0073] 在本实施例中，第一验证信息是信息录入平台根据用户端发送的第一可读地址信息生成的，信息录入平台对第一可读地址信息和第一验证信息进行哈希运算，生成第一哈希值，并将第一可读地址信息和第一哈希值发送至区块链。用户端向区块链发送第二可读

地址信息、第二验证信息和密码学地址信息，其中所述密码学地址信息为用户在区块链中的特有的地址信息。区块链接收所述第二可读地址信息、第二验证信息和密码学地址信息后，对第二可读地址信息和第二验证信息进行哈希运算，生成第二哈希值，并判断所述第一哈希值与所述第二哈希值是否相同。判断规则可以是第一哈希值与第二哈希值是否相同。并且当所述第一哈希值与所述第二哈希值相同时，建立密码学地址信息与第一可读地址信息的关联关系，即将密码学地址信息与第一可读地址信息绑定，并写入区块链中的一个区块(如图所示的区块n)中，并通过点对点网络同步到其它信息录入平台中。这样，避免了其它用户将自己的密码学地址信息与上用户提供的第一可读地址信息绑定的情形，从而解决了用户特有地址信息被注册的问题，能够实现保证表明用户身份的地址的真实性。

[0074] 如图4所示，示出了本发明实施例四的关联地址信息的装置的结构图。在本实施例中，应用于区块链的关联地址信息的装置，包括：

[0075] 信息接收单元301，用于接收信息录入平台发送的第一可读地址信息，以及，所述第一可读地址信息与第一验证信息的第一哈希值，其中，所述第一验证信息为信息录入平台根据所述第一可读地址信息生成的验证信息；接收用户端发送的密码学地址信息、第二可读地址信息和第二验证信息，计算所述第二可读地址信息和所述第二验证信息的第二哈希值；

[0076] 信息验证单元302，用于判断所述第一哈希值与所述第二哈希值是否相同；

[0077] 任务执行单元303，用于若所述第一哈希值与所述第二哈希值相同，建立所述第一可读地址信息和所述密码学地址信息的关联关系。

[0078] 如图5所示，示出了本发明实施例四的关联地址信息的装置的结构图。作为本发明的一个可选实施例，在上述实施例中的关联地址信息的装置中，还包括：信息发送单元304，用于向用户端发送所述第一可读地址信息和所述密码学地址信息关联成功的信息。

[0079] 作为本发明的一个可选实施例，所述信息接收单元301还用于接收用户端发送的身份标识信息，当所述信息接收单元301接收到用户端发送的身份标识信息后，所述任务执行单元303还用于建立所述身份标识信息与所述第一可读地址信息以及所述密码学地址信息的关联关系。

[0080] 作为本发明的一个可选实施例，所述信息发送304单元还用于：

[0081] 若所述第一哈希值和所述第二哈希值不相同，向用户端发送所述第一可读地址信息和所述密码学地址信息关联失败的信息。

[0082] 作为本发明的一个可选实施例，所述第一可读地址信息包括目标用户的地址。

[0083] 作为本发明的一个可选实施例，所述目标用户的地址包括所述目标用户的邮箱地址或所述目标用户的手机号码。

[0084] 作为本发明的一个可选实施例，所述第二验证信息与所述第一验证信息相同。

[0085] 本发明实施例中的关联地址信息的装置能够确定与本发明上述实施例中的关联地址信息的方法相同的技术效果，这里不再赘述。

[0086] 如图6所示，示出了本发明实施例六的关联地址信息的系统的结构图。在本实施例中，关联地址信息的系统包括：信息录入平台601、用户端602和区块链603，所述信息录入平台601、所述用户端602和所述区块链603通信连接。

[0087] 所述信息录入平台601用于向所述区块链603发送第一可读地址信息，以及，所述

第一可读地址信息与第一验证信息的第一哈希值，其中，所述第一可读地址信息包括目标用户的可读地址，所述第一验证信息为所述信息录入平台601根据所述第一可读地址信息生成的验证信息；

[0088] 此外，所述信息录入平台601还可以用于将所述第一验证信息发送至用户端602。

[0089] 所述用户端602用于向所述区块链603发送密码学地址信息、第二可读地址信息和第二验证信息，还可以用于接收信息录入平台601发送的第一验证信息。用户端602用于向所述区块链603发送的第二验证信息可以为接收到的信息录入平台601发送的第一验证信息。

[0090] 所述区块链603用于接收信息录入平台601发送的第一可读地址信息，以及，所述第一可读地址信息与第一验证信息的第一哈希值，并接收用户端602发送的密码学地址信息、第二可读地址信息和第二验证信息。计算所述第二可读地址信息和所述第二验证信息的第二哈希值；判断所述第一哈希值与所述第二哈希值是否相同；若所述第一哈希值与所述第二哈希值相同，建立所述第一可读地址信息和所述密码学地址信息的关联关系。

[0091] 本实施例中的关联地址信息的系统，能够取得与上述方法和装置实施例相同的技术效果，这里不再赘述。

[0092] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

[0093] 可以理解的是，上述方法及装置中的相关特征可以相互参考。另外，上述实施例中的“第一”、“第二”等是用于区分各实施例，而并不代表各实施例的优劣。

[0094] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统，装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0095] 在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

[0096] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0097] 类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0098] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或

子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书(包括伴随的权利要求、摘要和附图)中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书(包括伴随的权利要求、摘要和附图)中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0099] 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0100] 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器(DSP)来实现根据本发明实施例的区块链交易信息正确性的校验方法、装置及系统中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序(例如，计算机程序和计算机程序产品)。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

[0101] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

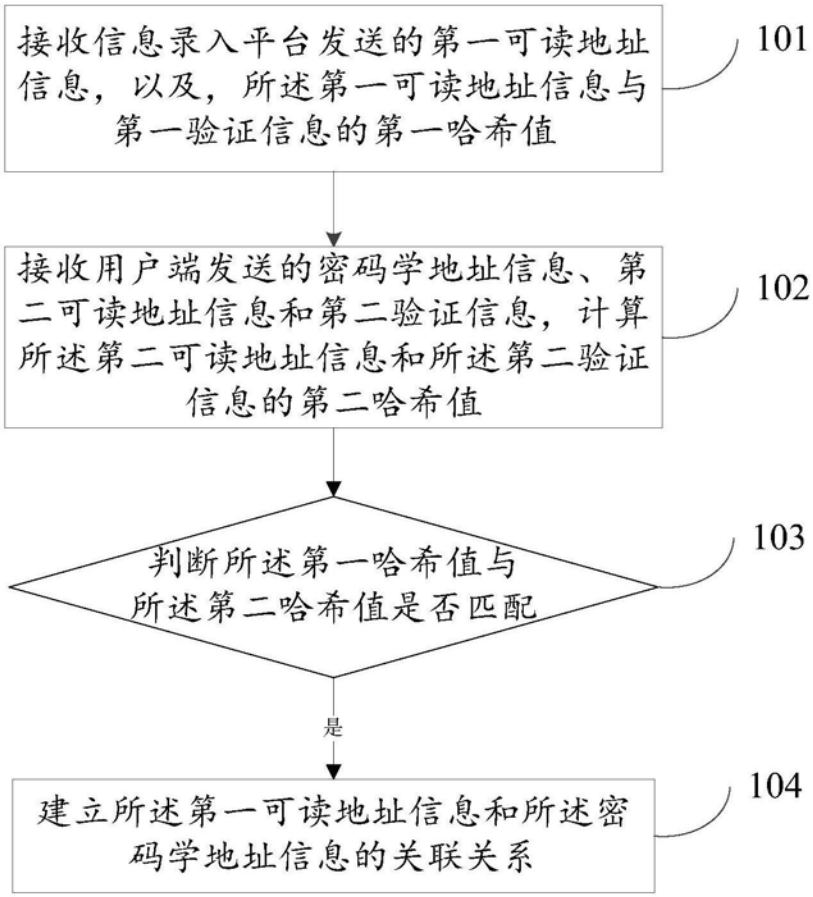

接收信息录入平台发送的第一可读地址信息，以及，所述第一可读地址信息与第一验证信息的第一哈希值
101
接收用户端发送的密码学地址信息、第二可读地址信息和第二验证信息，计算所述第二可读地址信息和所述第二验证信息的第二哈希值
102
判断所述第一哈希值与所述第二哈希值是否匹配
103
是
建立所述第一可读地址信息和所述密码学地址信息的关联关系
104

图1

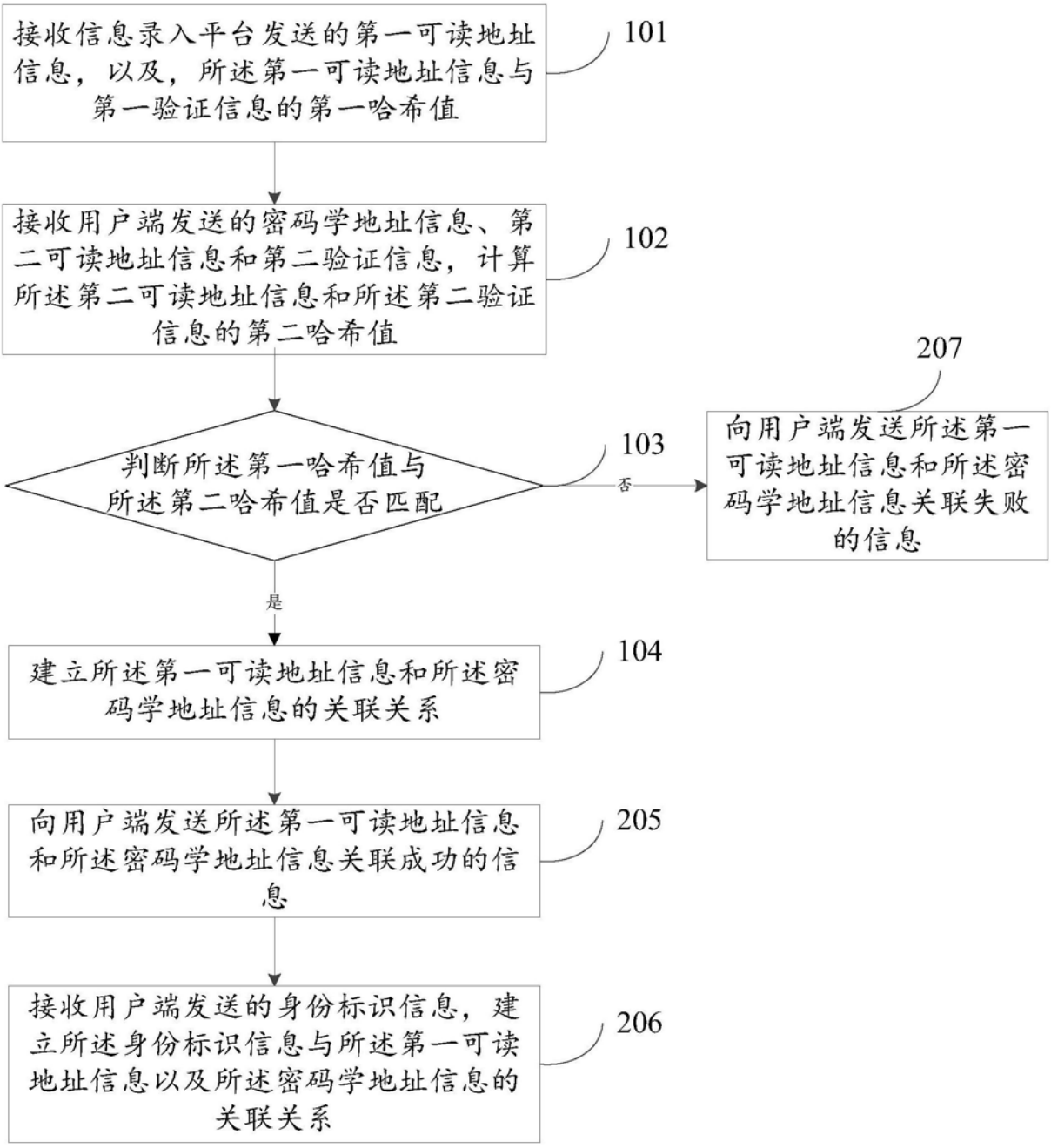

接收信息录入平台发送的第一可读地址信息，以及，所述第一可读地址信息与第一验证信息的第一哈希值
101
接收用户端发送的密码学地址信息、第二可读地址信息和第二验证信息，计算所述第二可读地址信息和所述第二验证信息的第二哈希值
102
判断所述第一哈希值与所述第二哈希值是否匹配
103
否
207
向用户端发送所述第一可读地址信息和所述密码学地址信息关联失败的信息
是
建立所述第一可读地址信息和所述密码学地址信息的关联关系
104
向用户端发送所述第一可读地址信息和所述密码学地址信息关联成功的信息
205
接收用户端发送的身份标识信息，建立所述身份标识信息与所述第一可读地址信息以及所述密码学地址信息的关联关系
206

图2

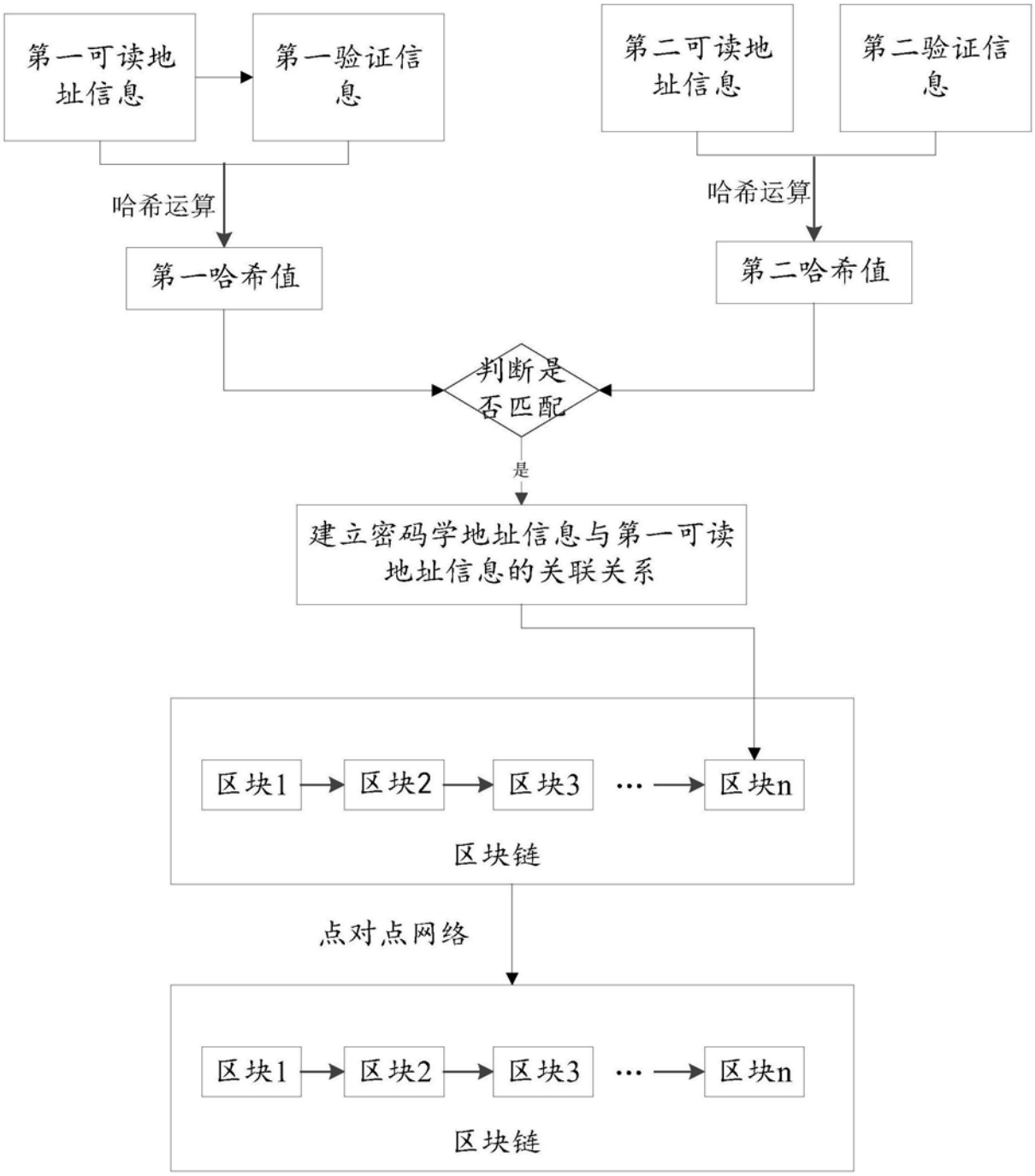

第一可读地址信息
第一验证信息
第二可读地址信息
第二验证信息
哈希运算
哈希运算
第一哈希值
第二哈希值
判断是否匹配
是
建立密码学地址信息与第一可读地址信息的关联关系
区块1
区块2
区块3
…
区块n
区块链
点对点网络
区块1
区块2
区块3
…
区块n
区块链

图3

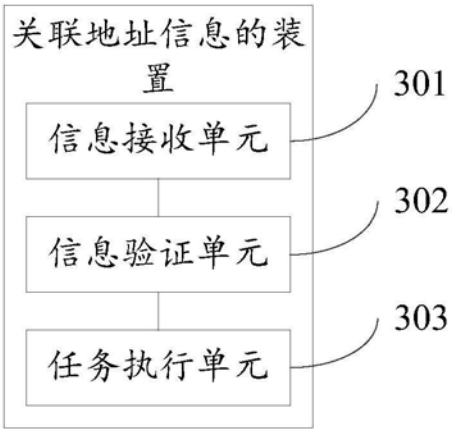

关联地址信息的装置
信息接收单元
信息验证单元
任务执行单元
301
302
303

图4

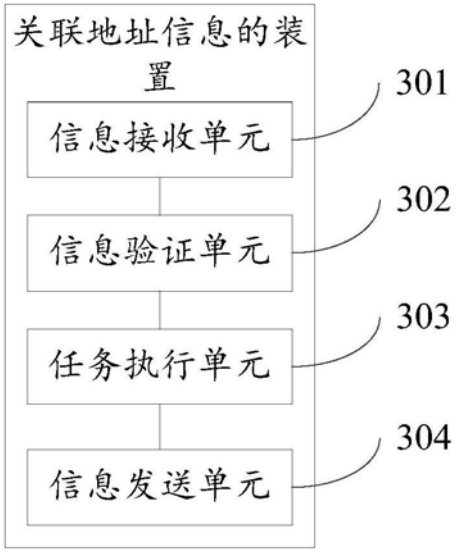

关联地址信息的装置
信息接收单元
信息验证单元
任务执行单元
信息发送单元
301
302
303
304

图5

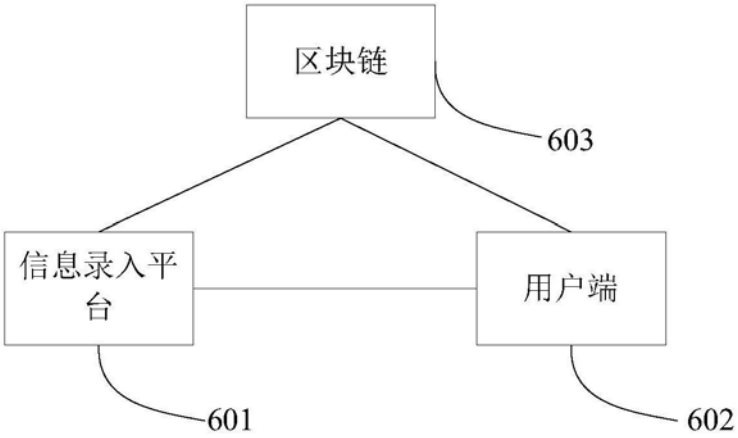

区块链
603
信息录入平台
用户端
601
602

图6