(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 113541970 B
(45)授权公告日 2021.11.26

(21)申请号 202111090012.4
(22)申请日 2021.09.17
(65)同一申请的已公布的文献号
申请公布号 CN 113541970 A
(43)申请公布日 2021.10.22
(73)专利权人 中国信息通信研究院
地址 100191 北京市海淀区花园北路52号
(72)发明人 李志平 谢家贵 张波 郭健 马旭锋
(74)专利代理机构 北京新知远方知识产权代理事务所(普通合伙) 11397
代理人 马军芳 张艳
(51)Int.Cl.
H04L 9/32(2006.01)
G06Q 20/40(2012.01)
G06Q 20/38(2012.01)

(56)对比文件
CN 113204783 A,2021.08.03
CN 111066020 A,2020.04.24
CN 112702346 A,2021.04.23
CN 112580102 A,2021.03.30
US 2020127828 A1,2020.04.23
CN 111164594 A,2020.05.15
US 2021006410 A1,2021.01.07
CN 111316303 A,2020.06.19
景越等.自主身份理念与关键要素分析.《信息安全与通信保密》.2021,

审查员 李文娟

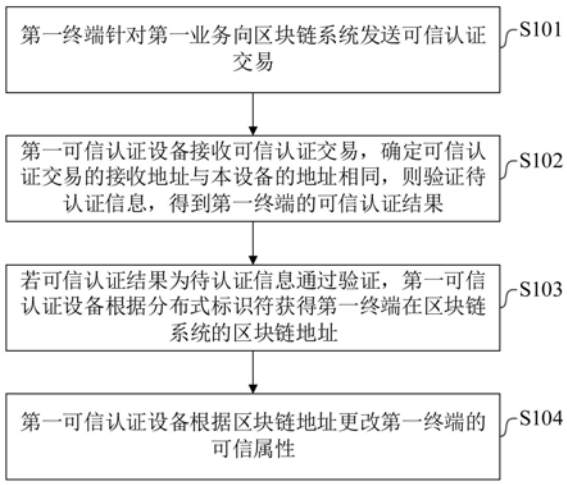
权利要求书3页 说明书10页 附图5页

(54)发明名称

分布式标识符的使用方法和分布式标识符使用系统

(57)摘要

本申请实施例中提供了一种分布式标识符的使用方法和分布式标识符使用系统。通过第一终端针对第一业务向区块链系统发送可信认证交易,可信认证交易携带有分布式标识符、待认证信息和接收地址;第一可信认证设备接收可信认证交易,确定可信认证交易的接收地址与本设备的地址相同,则验证待认证信息,得到第一终端的可信认证结果;若可信认证结果为待认证信息通过验证,第一可信认证设备根据分布式标识符获得第一终端在区块链系统的区块链地址;第一可信认证设备根据区块链地址更改第一终端的可信属性。本申请通过区块链交易而非智能合约的方式,实现分布式标识符的使用逻辑,节约了区块链系统的存储空间,避免了智能合约带来的性能和安全的问题。



CN 113541970 B

1.一种分布式标识符的使用方法,其特征在于,应用于相互通信的第一终端和区块链系统,所述区块链系统包括至少一个可信认证设备,所述至少一个可信认证设备与所述第一终端通信连接,所述方法包括:

所述第一终端针对第一业务向所述区块链系统发送可信认证交易,所述可信认证交易携带有分布式标识符、待认证信息和接收地址,所述接收地址为所述第一业务对应的第一可信认证设备的地址;

所述第一可信认证设备接收所述可信认证交易,确定所述可信认证交易的接收地址与本设备的地址相同,则验证所述待认证信息,得到所述第一终端的可信认证结果;

若所述可信认证结果为所述待认证信息通过验证,所述第一可信认证设备根据所述分布式标识符获得所述第一终端在所述区块链系统的区块链地址;

所述第一可信认证设备根据所述区块链地址更改所述第一终端的可信属性。

2.根据权利要求1所述的方法,其特征在于,所述第一终端针对第一业务向所述区块链系统发送可信认证交易的步骤之前,所述方法还包括:

所述第一终端生成所述分布式标识符。

3.根据权利要求2所述的方法,其特征在于,所述第一终端生成所述分布式标识符的步骤包括:

所述第一终端根据预设的加密算法类型生成公私钥对;

所述第一终端将所述公私钥对中的公钥进行哈希运算,得到输出摘要;

所述第一终端根据预设的编码类型得到要截取的哈希长度信息和编码算法类型;

所述第一终端根据所述哈希长度信息截取所述输出摘要,并根据所述编码算法类型对截取后的输出摘要进行编码生成编码信息;

所述第一终端根据所述编码信息、所述编码类型和所述加密算法类型生成所述分布式标识符。

4.根据权利要求2所述的方法,其特征在于,所述第一终端生成所述分布式标识符的步骤包括:

所述第一终端根据预设的加密算法类型生成公私钥对;

所述第一终端将所述公私钥对中的公钥进行哈希运算,得到输出摘要;

所述第一终端根据预设的编码类型得到要截取的哈希长度信息和编码算法类型;

所述第一终端根据所述哈希长度信息截取所述输出摘要,并根据所述编码算法类型对截取后的输出摘要进行编码生成编码信息;

所述第一终端根据所述编码信息、所述编码类型、所述加密算法类型和预设的子链编号生成所述分布式标识符;其中,所述子链编号用于区分所述区块链系统的子链。

5.根据权利要求1所述的方法,其特征在于,所述区块链系统还包括主链和子链,所述主链上存储有所述分布式标识符的子链编号与子链地址的对应关系;

所述若所述可信认证结果为所述待认证信息通过验证,所述第一可信认证设备根据所述分布式标识符获得所述第一终端在所述区块链系统的区块链地址的步骤包括:

所述第一可信认证设备根据所述分布式标识符的子链编号,从所述主链上获得所述分布式标识符对应的子链地址;

所述第一可信认证设备将所述子链地址作为所述第一终端在所述区块链系统的区块

链地址。

6.根据权利要求5所述的方法,其特征在于,所述第一可信认证设备根据所述区块链地址更改所述第一终端的可信属性的步骤包括:

所述第一可信认证设备根据所述区块链地址向所述区块链系统发送可信属性更改交易;所述可信属性更改交易携带有所述第一终端的可信属性,所述可信属性的可信状态为可信。

7.根据权利要求5所述的方法,其特征在于,所述区块链系统和所述第一终端还与第二终端通信;

所述第一可信认证设备接收所述可信认证交易,确定所述可信认证交易的接收地址与本设备的地址相同,则验证所述待认证信息,得到所述第一终端的可信认证结果的步骤之后,所述方法还包括:

所述第一终端向所述第二终端提供所述分布式标识符;

所述第二终端根据所述分布式标识符的子链编号,从所述主链上获得所述分布式标识符对应的子链地址;

所述第二终端根据所述子链地址,从相应的子链上获得所述第一终端的可信状态和所述接收地址;

所述第二终端根据所述可信状态和所述接收地址验证所述第一终端的可信认证结果是否可信认证通过。

8.根据权利要求7所述的方法,其特征在于,所述第二终端根据所述可信状态和所述接收地址验证所述可信认证结果是否可信认证通过的步骤包括:

所述第二终端在所述可信状态为不可信时,判定所述可信认证结果为可信认证未通过。

9.根据权利要求7所述的方法,其特征在于,所述第二终端根据所述可信状态和所述接收地址验证所述可信认证结果是否可信认证通过的步骤包括:

所述第二终端在所述可信状态为可信时,根据所述接收地址获得所述第一可信认证设备的加密算法类型,根据所述加密算法类型判断所述可信认证结果是否符合安全规范;

若不符合,所述第二终端则判定所述可信认证结果为可信认证未通过;

若符合,所述第二终端通过所述分布式标识符从所述子链上获得交易记录信息;

所述第二终端判断所述交易记录信息是否完整,以及判断所述交易记录信息的状态是否为最新;

若均是,所述第二终端则验证所述接收地址对应的第一可信认证设备是否有可信认证资质;

若有,所述第二终端则判定所述可信认证结果为可信认证通过。

10.一种分布式标识符使用系统,其特征在于,包括相互通信的第一终端和区块链系统,所述区块链系统包括至少一个可信认证设备,所述至少一个可信认证设备与所述第一终端通信连接;

所述第一终端用于针对第一业务向所述区块链系统发送可信认证交易,所述可信认证交易携带有分布式标识符、待认证信息和接收地址,所述接收地址为所述第一业务对应的第一可信认证设备的地址;

所述第一可信认证设备用于接收所述可信认证交易，确定所述可信认证交易的接收地址与本设备的地址相同，则验证所述待认证信息，得到所述第一终端的可信认证结果；

若所述可信认证结果为所述待认证信息通过验证，所述第一可信认证设备还用于根据所述分布式标识符获得所述第一终端在所述区块链系统的区块链地址；

所述第一可信认证设备还用于根据所述区块链地址更改所述第一终端的可信属性。

11.根据权利要求10所述的分布式标识符使用系统，其特征在于，所述第一终端还用于根据预设的加密算法类型生成公私钥对；

所述第一终端还用于将所述公私钥对中的公钥进行哈希运算，得到输出摘要；

所述第一终端还用于根据预设的编码类型得到要截取的哈希长度信息和编码算法类型；

所述第一终端还用于根据所述哈希长度信息截取所述输出摘要，并根据所述编码算法类型对截取后的输出摘要进行编码生成编码信息；

所述第一终端还用于根据所述编码信息、所述编码类型和所述加密算法类型生成所述分布式标识符。

12.根据权利要求10所述的分布式标识符使用系统，其特征在于，所述区块链系统还包括主链和子链，所述主链上存储有所述分布式标识符的子链编号与子链地址的对应关系；

所述第一可信认证设备还用于根据所述分布式标识符的子链编号，从所述主链上获得所述分布式标识符对应的子链地址；

所述第一可信认证设备还用于将所述子链地址作为所述第一终端在所述区块链系统的区块链地址。

13.根据权利要求12所述的分布式标识符使用系统，其特征在于，所述分布式标识符使用系统还包括第二终端，所述区块链系统和所述第一终端还与所述第二终端通信；

所述第一终端还用于向所述第二终端提供所述分布式标识符；

所述第二终端还用于根据所述分布式标识符的子链编号，从所述主链上获得所述分布式标识符对应的子链地址；

所述第二终端还用于根据所述子链地址，从相应的子链上获得所述第一终端的可信状态和所述接收地址；

所述第二终端还用于根据所述可信状态和所述接收地址验证所述第一终端的可信认证结果是否可信认证通过。

分布式标识符的使用方法和分布式标识符使用系统

技术领域

[0001] 本申请涉及区块链技术领域，具体地，涉及一种分布式标识符的使用方法和分布式标识符使用系统。

背景技术

[0002] 目前基于区块链的分布式标识符的使用逻辑，通过Dapp(Decentralized Application，去中心化应用)调用区块链上的智能合约实现的，通过智能合约把分布式标识符与区块链地址或区块链地址的公钥进行绑定。

[0003] 通过智能合约实现分布式标识与区块链地址的绑定的方式性能较差，且存在安全隐患。

发明内容

[0004] 本申请实施例中提供了一种分布式标识符的使用方法和分布式标识符使用系统，未采用智能合约的方式，实现分布式标识符的使用逻辑，以解决现有技术存在的问题。

[0005] 根据本申请实施例的第一个方面，提供了一种分布式标识符的使用方法，应用于相互通信的第一终端和区块链系统，所述区块链系统包括至少一个可信认证设备，所述至少一个可信认证设备与所述第一终端通信连接，所述方法包括：

[0006] 所述第一终端针对第一业务向所述区块链系统发送可信认证交易，所述可信认证交易携带有分布式标识符、待认证信息和接收地址，所述接收地址为所述第一业务对应的第一可信认证设备的地址；

[0007] 所述第一可信认证设备接收所述可信认证交易，确定所述可信认证交易的接收地址与本设备的地址相同，则验证所述待认证信息，得到所述第一终端的可信认证结果；

[0008] 若所述可信认证结果为所述待认证信息通过验证，所述第一可信认证设备根据所述分布式标识符获得所述第一终端在所述区块链系统的区块链地址；

[0009] 所述第一可信认证设备根据所述区块链地址更改所述第一终端的可信属性。

[0010] 根据本申请实施例的第二个方面，提供了一种分布式标识符使用系统，包括相互通信的第一终端和区块链系统，所述区块链系统包括至少一个可信认证设备，所述至少一个可信认证设备与所述第一终端通信连接；

[0011] 所述第一终端用于针对第一业务向所述区块链系统发送可信认证交易，所述可信认证交易携带有分布式标识符、待认证信息和接收地址，所述接收地址为所述第一业务对应的第一可信认证设备的地址；

[0012] 所述第一可信认证设备用于接收所述可信认证交易，确定所述可信认证交易的接收地址与本设备的地址相同，则验证所述待认证信息，得到所述第一终端的可信认证结果；

[0013] 若所述可信认证结果为所述待认证信息通过验证，所述第一可信认证设备还用于根据所述分布式标识符获得所述第一终端在所述区块链系统的区块链地址；

[0014] 所述第一可信认证设备还用于根据所述区块链地址更改所述第一终端的可信属

性。

[0015] 采用本申请实施例中提供的分布式标识符的使用方法和分布式标识符使用系统，应用于相互通信的第一终端和区块链系统，区块链系统包括至少一个可信认证设备，至少一个可信认证设备与第一终端通信连接。第一终端针对第一业务向区块链系统发送可信认证交易，可信认证交易携带有分布式标识符、待认证信息和接收地址，接收地址为第一业务对应的第一可信认证设备的地址；第一可信认证设备接收可信认证交易，确定可信认证交易的接收地址与本设备的地址相同，则验证待认证信息，得到第一终端的可信认证结果；若可信认证结果为待认证信息通过验证，第一可信认证设备根据分布式标识符获得第一终端在区块链系统的区块链地址；第一可信认证设备根据区块链地址更改第一终端的可信属性。本申请的方法直接以交易的形式将分布式标识符的可信认证和可信属性修改存储在区块链系统上，未采用智能合约的方式进行，即节约了区块链系统的存储空间，还可以避免智能合约带来的性能问题和安全问题。

附图说明

[0016] 此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

[0017] 图1为现有技术的一种主子链架构的结构示意图；

[0018] 图2为现有技术的一种分布式标识符的使用场景示意图；

[0019] 图3为本申请实施例提供的一种分布式标识符使用系统的结构示意图；

[0020] 图4为本申请实施例提供的一种分布式标识符的使用方法的流程示意图；

[0021] 图5为本申请实施例提供的另一种分布式标识符的使用方法的流程示意图；

[0022] 图6为本申请实施例提供的又一种分布式标识符的使用方法的流程示意图。

[0023] 图标：10-分布式标识符使用系统；100 -第一终端；200-区块链系统；300-可信认证设备；400-可信认证联盟；500-第二终端；600-第三终端。

具体实施方式

[0024] 现对本申请涉及的部分名词进行解释说明：

[0025] 区块链技术：区块链是分布式存储、点对点传输、共识机制、加密算法和智能合约等计算机技术在互联网时代的创新应用模式。区块链是一种利用加密算法和点对点传输技术构建的分布式网络数据存储技术，其特点是去中心化、防篡改和可溯源。数据不再储存于一个中心化的硬件或管理机构，而是由权利和义务对等的节点来共同维护；数据被记录在区块链技术构建的系统的多个节点上，能够实现在任意时间查看任何节点保存在本地区块链中的数据；一旦数据经过验证并添加到区块链，就会被永久地存储起来，利用共识算法和哈希链式数据存储技术能够实现数据的不可篡改，保证数据的安全性和真实性。

[0026] 主子链架构：2020年8月，在工信部的支持下，国家级链网协同基础设施“星火·链网”正式启动建设，“星火·链网”采用许可公有链技术，通过工业互联网标识和区块链技术融合，构建了新型区块链标识基础设施。如图1所示，“星火·链网”采用主子链构建的两层架构，国家主链加行业/地域链双层，系统参与方角色分为国家主链超级节点、行业/地域骨干节点和业务节点三类。

[0027] MPT树(Merkle Patricia Tree):一种经过改良的、融合了默克尔树和前缀树两种树结构优点的数据结构,以太坊等区块链中,MPT是一个非常重要的数据结构,在以太坊中,帐户的交易信息、状态以及相应的状态变更,还有相关的交易信息等都使用MPT来进行管理,其是整个数据存储的重要一环。交易树,收据树,状态树都是采用的MPT结构。

[0028] DID(Decentralized Identifier,分布式标识符):用于可验证的“自我主权”数字身份的新型标识符。DID独立于任何集中注册表,身份提供者或证书颁发机构,具有全球唯一性、可解析性高、可加密和能够加密验证的特点。DID通常与加密内容相关联,例如公钥和服务第一终端,用于建立安全的通信信道。DID受益于自分配,对于可加密验证的标识符(例如个人标识符,组织标识符和物联网方案标识符)的任何应用程序都很有用。表面上看,DID只是一种新型的全球性的唯一标识符,但在更深层次上,DID是互联网的一种全新的分布式数字身份,同时,它也是公钥基础设施(PKI)层的核心组成部分。这种分布式的公钥基础设施(DPKI)可能对全球网络安全和隐私与加密网络流量(现在是世界上最大的PKI)的SSL / TLS协议具有同等重要的影响力。

[0029] 门限签名:是一种分布式多方签名协议,包含有分布式密钥生成,签名和验签算法。主要原理:基于分布式通信网络,各参与方通过自己的私钥份额 ski 完成对消息 m 的分布式协作签署并输出最终的可验证签名 Sig(sk, m),这个签名跟单独用 sk 私钥签出的一模一样,可以用基于基础签名机制里的验证函数进行本地验证,无需走通信交互验证,通常利用门限签名的访问结构设计不同权重和不同组合的授权方式。

[0030] 在实现本申请的过程中,发明人发现,如图2所示,目前基于区块链的分布式标识符的使用逻辑,通过Dapp调用区块链上的智能合约实现的,通过智能合约把分布式标识符与区块链地址或区块链地址的公钥进行绑定。通过智能合约实现分布式标识与区块链地址的绑定的方式存在以下问题:

[0031] 1、多了一层分布式标识符和链地址的绑定关系,造成了链上存储资源的浪费;

[0032] 2、分布式标识符的使用逻辑通过智能合约实现,而链上的智能合约很容易出现代码漏洞,可能会有安全隐患;

[0033] 3、区块链系统执行智能合约是在虚拟机上执行,性能不高,如果同时有大量对分布式标识符的操作,会造成区块链系统上的交易拥堵。

[0034] 针对上述问题,本申请实施例中提供了一种分布式标识符的使用方法和分布式标识符使用系统,应用于相互通信的第一终端和区块链系统,区块链系统包括至少一个可信认证设备,至少一个可信认证设备与第一终端通信连接。第一终端针对第一业务向区块链系统发送可信认证交易,可信认证交易携带有分布式标识符、待认证信息和接收地址,接收地址为第一业务对应的第一可信认证设备的地址;第一可信认证设备接收可信认证交易,确定可信认证交易的接收地址与本设备的地址相同,则验证待认证信息,得到第一终端的可信认证结果;若可信认证结果为待认证信息通过验证,第一可信认证设备根据分布式标识符获得第一终端在区块链系统的区块链地址;第一可信认证设备根据区块链地址更改第一终端的可信属性。本申请的方法直接以交易的形式将分布式标识符的可信认证和可信属性修改存储在区块链系统上,未采用智能合约的方式进行,即节约了区块链系统的存储空间,还可以避免智能合约带来的性能问题和安全问题。

[0035] 为了使本申请实施例中的技术方案及优点更加清楚明白,以下结合附图对本申请

的示例性实施例进行进一步详细的说明，显然，所描述的实施例仅是本申请的一部分实施例，而不是所有实施例的穷举。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

[0036] 请参照图3，为本申请实施例提供的一种分布式标识符使用系统10的结构示意图，分布式标识符使用系统10包括相互通信的第一终端100 和区块链系统200，区块链系统200包括至少一个可信认证设备300，至少一个可信认证设备300与第一终端100 通信连接。

[0037] 区块链系统200可以采用主子链架构，若区块链系统200为主子链架构，区块链系统200包括主链和子链。

[0038] 第一终端100 可以理解为分布式标识符使用系统中的普通用户，在分布式标识符使用系统中有唯一的分布式标识符作为区块链系统200上的账户地址，可以申请可信认证，还可以申请成为可信认证设备300。

[0039] 可信认证设备300可以理解为可信认证中心，在分布式标识符使用系统中有唯一的分布式标识符作为区块链系统200上的账户地址。是可信认证联盟400成员，有给普通用户颁发可信认证的资质。

[0040] 可信认证联盟400为可信认证中心组成的联盟，在区块链系统200初始化时，指定至少四个普通用户作为可信认证联盟400的初始成员。初始成员需要写入主链的创世区块，由整条主链的共识机制作为背书。

[0041] 在本实施例中，利用MPT树作为账户树，将分布式标识符以MPT树形式作为区块链系统200的原生账户地址。MPT树的叶子节点上的账户状态内嵌可信属性，实现基于区块链的分布式标识符的内生可信。

[0042] 分布式标识符使用系统还包括第二终端500和第三终端600，区块链系统200和第一终端100 还与第二终端500通信，第三终端600与区块链系统200通信。

[0043] 第二终端500可以理解为验证者，即业务上存在的第三方机构。在分布式标识符使用系统中可以没有唯一的分布式标识符作为区块链系统200上的账户地址。

[0044] 第三终端600可以理解为预备可信认证设备，即申请加入可信认证联盟400之前的可信认证中心。

[0045] 其中，第一终端100 、第二终端500、第三终端600和可信认证设备300可以是，但不限于手机、平板电脑和可穿戴设备等。

[0046] 在本实施例中，第一终端100 用于针对第一业务向区块链系统200发送可信认证交易，可信认证交易携带有分布式标识符、待认证信息和接收地址，接收地址为所述第一业务对应的第一可信认证设备的地址；第一可信认证设备用于接收可信认证交易，确定可信认证交易的接收地址与本设备的地址相同，则验证待认证信息，得到第一终端100 的可信认证结果；若可信认证结果为待认证信息通过验证，第一可信认证设备还用于根据分布式标识符获得第一终端100 在所述区块链系统200的区块链地址；第一可信认证设备还用于根据区块链地址更改第一终端100 的可信属性。

[0047] 由于第一终端100 的分布式标识符为第一终端100 在区块链系统200的账户地址，第一可信认证设备的地址(即接收地址)为第一可信认证设备的分布式标识符。所以可以实现以交易的形式将分布式标识符的可信认证和可信属性修改存储在区块链系统200上，未采用智能合约的方式进行，即节约了区块链系统200的存储空间，还可以避免智能合

约带来的性能问题和安全问题。

[0048] 在本实施例中，第一终端100 可以包括多个分布式标识符，不同的分布式标识符对应不同的业务。第一终端100 的分布式标识符可以采用国密算法生成，也可以采用国际密码学算法生成，用户可以根据具体的业务需求，选择国密算法或国际密码学算法生成的标识符作为被认证的分布式标识符。

[0049] 例如，第一业务可以为商业密码业务，对应的分布式标识符则使用SM国密算法生成；第一业务还可以为区块链或智能设备业务，对应的分布式标识符则使用椭圆曲线加密算法。

[0050] 在本实施例中，待认证信息可以理解为可信认证材料，第一终端100 将可信认证材料打包成区块链系统200的交易结构，用私钥签名后发送到区块链系统200上。第一可信认证设备监听区块链系统200上发给自己的可信认证交易，确定可信认证交易的接收地址与该可信认证交易的地址是否相同，若相同，则验证该待认证信息，得到第一终端100 的可信认证结果。

[0051] 其中，根据第一业务的类型确定待认证信息，如第一业务为需证明用户已经拿到驾照，用户通过第一终端100 上传的待认证信息为该用户的驾照编码和身份证号加密后的信息。

[0052] 接收地址为第一可信认证设备的分布式标识符，第一终端100 针对第一业务选择对应的第一可信认证设备，并获得第一可信认证设备的地址。如第一业务为需证明用户已经拿到驾照，则对应的第一可信认证设备为车管所。

[0053] 第一终端100 获得接收地址的方式为，第一终端100 调用可信认证联盟400的查询接口，查询可信认证联盟400中存储的所有的可信认证设备300的认证中心列表，该认证中心列表上记录有可信认证联盟400中所有可信认证设备300的地址。第一终端100 根据第一业务选择对应的第一可信认证设备，并从认证中心列表获得第一可信认证设备的地址(即接收地址)。

[0054] 在本实施例中，第一终端100 在发送可信认证交易之前，需先生成分布式标识符。分布式标识符根据区块链系统200的主链和子链，可以有两种生成方式。

[0055] 针对主链，分布式标识符的生成方式为：第一终端100 根据预设的加密算法类型生成公私钥对；第一终端100 将公私钥对中的公钥进行哈希运算，得到输出摘要；第一终端100 根据预设的编码类型得到要截取的哈希长度信息和编码算法类型；第一终端100 根据哈希长度信息截取输出摘要，并根据编码算法类型对截取后的输出摘要进行编码生成编码信息；第一终端100 根据编码信息、编码类型和加密算法类型生成分布式标识符。

[0056] 应理解，为兼容不同的认证业务场景，第一终端100 生成公私钥对时，可以选择不同的加密算法类型。该加密算法类型可以为传统的CA(Certificate Authority，证书颁发机构)认证体系使用的RSA算法、商业密码业务场景使用的SM系类算法以及区块链或者智能设备业务场景下使用的椭圆曲线加密算法。同时，为方便用户记忆，除了支持随机生成私钥以外，还支持利用密码作为生成私钥的种子生成私钥，第一终端100 根据相应的算法可以随时用密码生成私钥。

[0057] 第一终端100 对公私钥对中的公钥进行哈希运算，可以得到一个固定长度的输出摘要，如256-bit/32-Byte固定长度的输出摘要。因为不同的加密算法生成的公钥长度是不

同的，故需要一个定长的输出摘要生成区块链系统200的账户地址，因此利用哈希算法对公钥进行运算，得到具有定长特性的输出摘要。

[0058] 不同的业务对分布式标识符的长度或大小写要求是不同的，为兼容不同业务场景，在分布式标识符中加入了编码类型。第一终端100 根据编码类型得到要截取的哈希长度信息和编码算法类型，根据哈希长度信息截取输出摘要，并根据编码算法类型对截取后的输出摘要进行编码生成编码信息。

[0059] 不同的编码算法类型可以生成不同长度或者大小写规范的分布式标识符，例如，在需要人工识别和输入的业务场景中，若分布式标识符中存在着看起来会产生歧义的字符(如:0(零)、O(大写字母O)、I(大写的字母i)以及l(小写的字母L))，则可能会发生错误，这时则需要选择base58编码算法，避免产生歧义的情况出现。在不需要区分字母大小写的业务场景，则可以选择bech32编码算法。在对分布式标识符的性能要求特别高的业务场景，则可以选择base64编码算法。

[0060] 针对子链，分布式标识符的生成方式为:第一终端100 根据预设的加密算法类型生成公私钥对;第一终端100 将公私钥对中的公钥进行哈希运算，得到输出摘要;第一终端100 根据预设的编码类型得到要截取的哈希长度信息和编码算法类型;第一终端100 根据所述哈希长度信息截取输出摘要，并根据编码算法类型对截取后的输出摘要进行编码生成编码信息;第一终端100 根据编码信息、编码类型、加密算法类型和预设的子链编号生成分布式标识符;其中，子链编号用于区分区块链系统200的子链。

[0061] 应理解，子链和主链的分布式标识符的区别在于子链编号，子链的分布式标识符具有子链编号，主链的分布式标识符无子链编号。

[0062] 其中，主链上的可信认证联盟400合约中存储有子链编号与子链地址的对应关系。不同子链上的分布式标识符的子链编号是不同的，但编码信息、编码类型和加密算法类型均相同，用户可以使用同一私钥控制不同子链上除子链编号外的其它内容。

[0063] 在本实施例中，主链和子链的分布式标识符均还包括前缀。主链的分布式标识符可以按照前缀、加密算法类型、编码类型和编码信息依次排布的方式组成，子链的分布式标识符可以按照前缀、子链编号、加密算法类型、编码类型和编码信息依次排布的方式组成。

[0064] 例如，did:bid: byo1:zf2LL97siENHaNYpEHpTHW1MA5RBbpM为子链的分布式标识符的一种可实施方式。子链的分布式标识符的前缀由固定字符串值"did:bid:"表示，子链的分布式标识符的子链编号由编号“byo1”+“:”表示，子链的分布式标识符的加密算法类型可以由字符“z”表示，子链的分布式标识符的编码类型可以由字符“f”表示，子链的分布式标识符的编码信息由“2LL97siENHaNYpEHpTHW1MA5RBbpM”表示。

[0065] 同理，可信认证设备300和第三终端600生成分布式标识符的原理与第一终端100的生成原理相同，可以参照第一终端100 生成分布式标识符的流程，在此不再累述。

[0066] 在分布式标识符生成后，在区块链系统200上创建可信认证设备300。创建原理为:在区块链系统200初始化时，指定至少四个普通用户的账户地址作为主链的创世账户地址。并在主链的创世区块部署可信认证联盟400合约，完成可信认证联盟400合作的初始化。在部署可信认证联盟400合约是需要指定创世账户地址对应的普通用户作为可信认证联盟400的默认成员，同时指定投票的超时时间。

[0067] 预备可信认证设备申请成为可信认证设备300的原理为，预备可信认证设备调用

可信认证联盟400合约的申请接口，调用时传入的参数包括其账户地址、有效证件、认证资质和认证的行业等。可信认证联盟400的成员审核预备可信认证设备的身份和认证资质，然后发起投票。投票的超时时间结束后，统计投票结果。若超过三分之二的成员审核通过，该预备可信认证设备正式成为可信认证设备300。

[0068] 第一可信认证设备根据分布式标识符获得第一终端100 在区块链系统200的区块链地址的原理为：第一可信认证设备根据分布式标识符的子链编号，从主链上获得分布式标识符对应的子链地址；第一可信认证设备将子链地址作为第一终端100 在区块链系统200的区块链地址。

[0069] 第一可信认证设备根据区块链地址更改第一终端100 的可信属性的原理为：第一可信认证设备根据区块链地址向区块链系统200发送可信属性更改交易；可信属性更改交易携带有第一终端100 的可信属性，可信属性的可信状态为可信。

[0070] 应理解，第一可信认证设备用其私钥签名发起可信属性更改交易，以便将第一终端100 的可信属性的可信状态更改为可信。其中，第一终端100 在区块链系统200上创建账户地址时，第一终端100 的可信属性也写入在区块链系统200上。若第一终端100 在子链上创建的账户地址，第一终端100 的可信属性写入在对应的子链上。

[0071] 由于区块链系统200的签名算法支持门限签名，将第一终端100 的账户属性设置门限，账户属性包括可信属性和其它属性，其它属性可以为账户积分余额。因此，第一终端100 采用其签名只可以修改可信属性的可信认证设备300，也就是说第一终端100 可以修改指定的第一可信认证设备；而被第一终端100 指定的第一可信认证设备有权限修改第一终端100 的可信属性的可信状态，即被指定的第一可信认证设备通过其私钥签名可以发起可信属性更改交易。

[0072] 当第一可信认证设备需要撤销第一终端100 的可信认证时，第一可信认证设备通过其私钥签名可以发起可信属性更改交易，该可信属性更改交易携带有第一终端100 的可信属性，该可信属性的可信状态为非可信。

[0073] 第一可信认证设备对第一终端100 进行可信认证后，虽然能够得到可信认证结果，但为了进一步地保证改可信认证结果的可信性，还可以通过第二终端500进行第三方的验证。

[0074] 第二终端500的验证原理为：第一终端100 向第二终端500提供分布式标识符；第二终端500根据分布式标识符的子链编号，从主链上获得分布式标识符对应的子链地址；第二终端500根据子链地址，从相应的子链上获得第一终端100 的可信状态和接收地址；第二终端500根据可信状态和接收地址验证第一终端100 的可信认证结果是否可信认证通过。

[0075] 应理解，第一终端100 向第二终端500提供第一终端100 的分布式标识符，第二终端500根据第一终端100 的分布式标识符的子链编号，到主链的可信认证联盟400合约中查询子链编号对应的子链地址，即根据可信认证联盟400合约中子链编号与子链地址的对应关系查找对应的子链地址。该子链地址对应的子链上存储有第一终端100 的可信状态和接收地址。第二终端500根据子链地址从对应的子链上获取第一终端100 的可信状态和接收地址。该可信状态为第一终端100 的可信属性的可信状态，接收地址为第一终端100 指定的第一可信认证设备的地址。

[0076] 第二终端500获取可信状态后，判断可信状态是否可信，若为不可信，第二终端500

则判定第一可信认证结果为可信认证未通过;若为可信,第二终端500根据接收地址获得第一可信认证设备的加密算法类型,根据加密算法类型判断可信认证结果是否符合安全规范;若不符合,第二终端500则判定可信认证结果为可信认证未通过;若符合,第二终端500通过分布式标识符从子链上获得交易记录信息;第二终端500判断交易记录信息是否完整,以及判断交易记录信息的状态是否为最新;若均是,第二终端500则验证接收地址对应的第一可信认证设备是否有可信认证资质;若有,第二终端500则判定可信认证结果为可信认证通过。

[0077] 应理解,因为第一可信认证设备的分布式标识符为其账户地址,故接收地址即为第一可信认证设备的分布式标识符,根据接收地址的加密算法类型判断可信认证结果是否符合安全规范。如,金融领域相关的认证需要使用国密算法,若第一业务为金融业务,而第一可信认证设备的分布式标识符未采用国密算法,则不符合安全规范,第一终端100 的可信认证结果为可信认证未通过。

[0078] 第二终端500获得交易记录信息后,通过检测交易记录信息是否完整,以及判断该交易记录的状态是否为最新,来确定可信属性有没有被篡改。若该交易记录信息完整且为最新状态,则说明可信属性没有被篡改;若该交易记录信息不完整和/或不为最新,则说明可信属性有被篡改。

[0079] 第二终端500验证接收地址对应的第一可信认证设备是否有可信认证资质的原理可以为,第二终端500在可信认证联盟400合约中查询是否存储有接收地址,若有,则说明该第一可信认证设备具有可信认证资质,第一终端100 的可信认证结果为可信认证通过;若没有,则说明该第一可信认证设备不具备可信认证资质,第一终端100 的可信认证结果为可信认证不通过。

[0080] 下面在图3示出的分布式标识符使用系统的基础上,本申请实施例提供一种分布式标识符的使用方法,请参见图4,图4为本申请实施例提供的一种分布式标识符的使用方法,该分布式标识符的使用方法可以包括以下步骤:

[0081] S101,第一终端针对第一业务向区块链系统发送可信认证交易。

[0082] S102,第一可信认证设备接收可信认证交易,确定可信认证交易的接收地址与本设备的地址相同,则验证待认证信息,得到第一终端的可信认证结果。

[0083] S103,若可信认证结果为待认证信息通过验证,第一可信认证设备根据分布式标识符获得第一终端在区块链系统的区块链地址。

[0084] S104,第一可信认证设备根据区块链地址更改第一终端的可信属性。

[0085] 请参见图5,图5为本申请实施例提供的另一种分布式标识符的使用方法,该分布式标识符的使用方法可以还可以包括以下步骤:

[0086] S201,第一终端生成分布式标识符。

[0087] 第一终端100 根据预设的加密算法类型生成公私钥对;第一终端100 将公私钥对中的公钥进行哈希运算,得到输出摘要;第一终端100 根据预设的编码类型得到要截取的哈希长度信息和编码算法类型;第一终端100 根据哈希长度信息截取输出摘要,并根据编码算法类型对截取后的输出摘要进行编码生成编码信息;第一终端100 根据编码信息、编码类型和加密算法类型生成分布式标识符。

[0088] 第一终端100 还根据编码信息、编码类型、加密算法类型和预设的子链编号生成

分布式标识符;其中,子链编号用于区分区块链系统200的子链。

[0089] 请参见图6,图6为本申请实施例提供的又一种分布式标识符的使用方法,该分布式标识符的使用方法可以还可以包括以下步骤:

[0090] S301,第一终端向第二终端提供分布式标识符。

[0091] S302,第二终端根据分布式标识符的子链编号,从主链上获得分布式标识符对应的子链地址。

[0092] S303,第二终端根据子链地址,从相应的子链上获得第一终端的可信状态和接收地址。

[0093] S304,第二终端根据可信状态和接收地址验证第一终端的可信认证结果是否可信认证通过。

[0094] 应理解,S101-S104、S201和S301-S304的具体实现原理,可以参照上述第一终端100 、第二终端500、区块链系统200和第一可信认证设备的描述内容。

[0095] 综上,本申请提供了一种分布式标识符的使用方法和分布式标识符使用系统,应用于相互通信的第一终端和区块链系统,区块链系统包括至少一个可信认证设备,至少一个可信认证设备与第一终端通信连接。第一终端针对第一业务向区块链系统发送可信认证交易,可信认证交易携带有分布式标识符、待认证信息和接收地址,接收地址为第一业务对应的第一可信认证设备的地址;第一可信认证设备接收可信认证交易,确定可信认证交易的接收地址与本设备的地址相同,则验证待认证信息,得到第一终端的可信认证结果;若可信认证结果为待认证信息通过验证,第一可信认证设备根据分布式标识符获得第一终端在区块链系统的区块链地址;第一可信认证设备根据区块链地址更改第一终端的可信属性。本申请的方法直接以交易的形式将分布式标识符的可信认证和可信属性修改存储在区块链系统上,未采用智能合约的方式进行,即节约了区块链系统的存储空间,还可以避免智能合约带来的性能问题和安全问题。

[0096] 本领域内的技术人员应明白,本申请的实施例可提供为方法、系统、或计算机程序产品。因此,本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且,本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0097] 本申请是参照根据本申请实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器,使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0098] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品,该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0099] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上,使得在计

算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0100] 尽管已描述了本申请的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本申请范围的所有变更和修改。

[0101] 显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

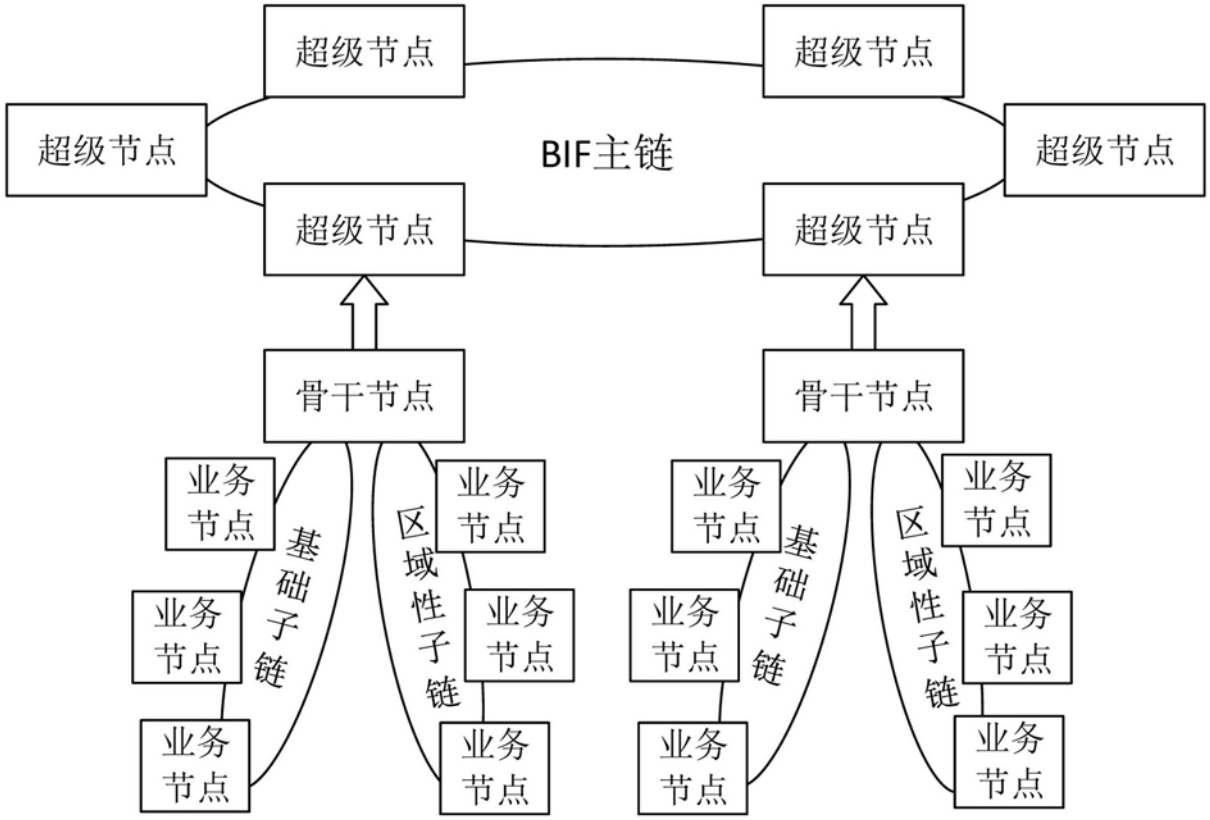

超级节点
超级节点
超级节点
BIF主链
超级节点
超级节点
超级节点
骨干节点
骨干节点
业务节点
业务节点
业务节点
基础子链
区域性子链
业务节点
业务节点
业务节点
业务节点
业务节点
业务节点
业务节点
业务节点
业务节点

图1

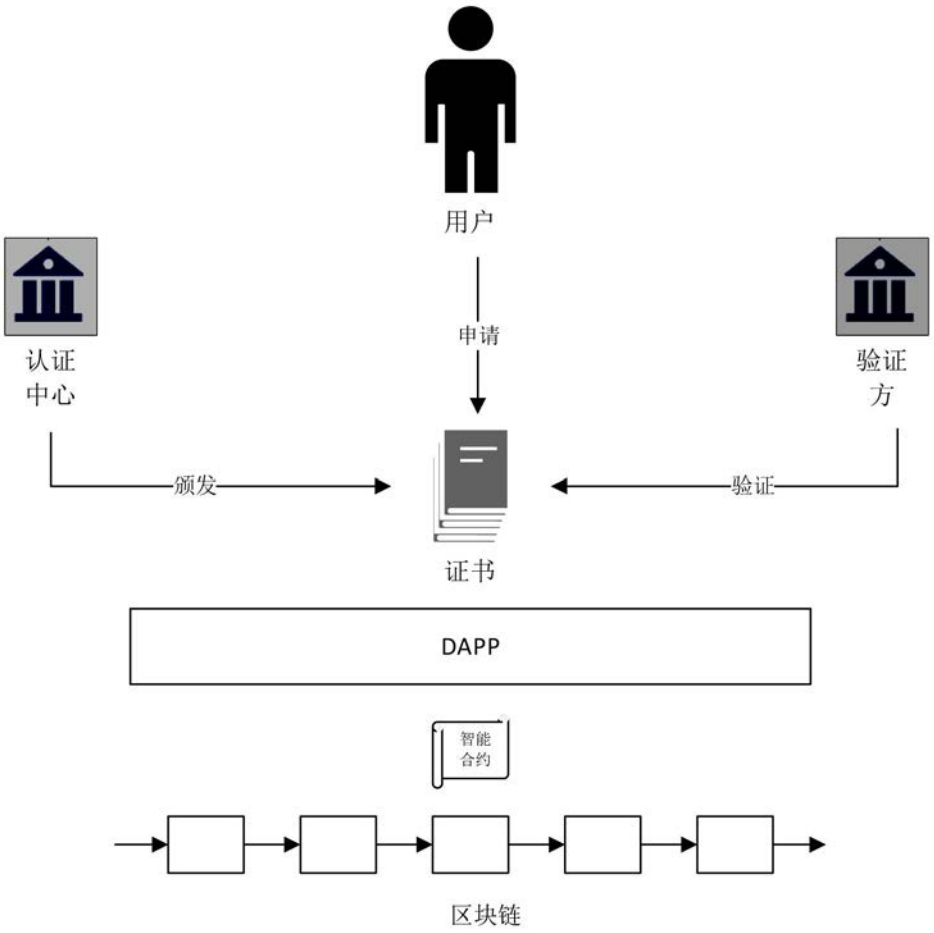


图2

10

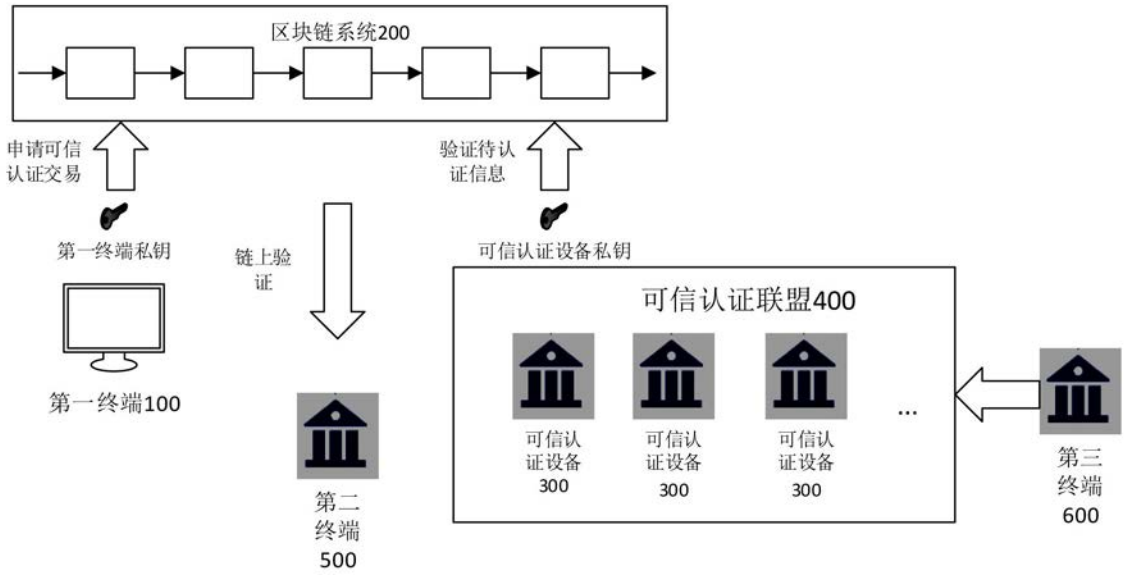

区块链系统200
申请可信认证交易
验证待认证信息
第一终端私钥
链上验证
可信认证设备私钥
可信认证联盟400
第一终端100
可信认证设备300
可信认证设备300
可信认证设备300
...
第三终端600
第二终端500

图3

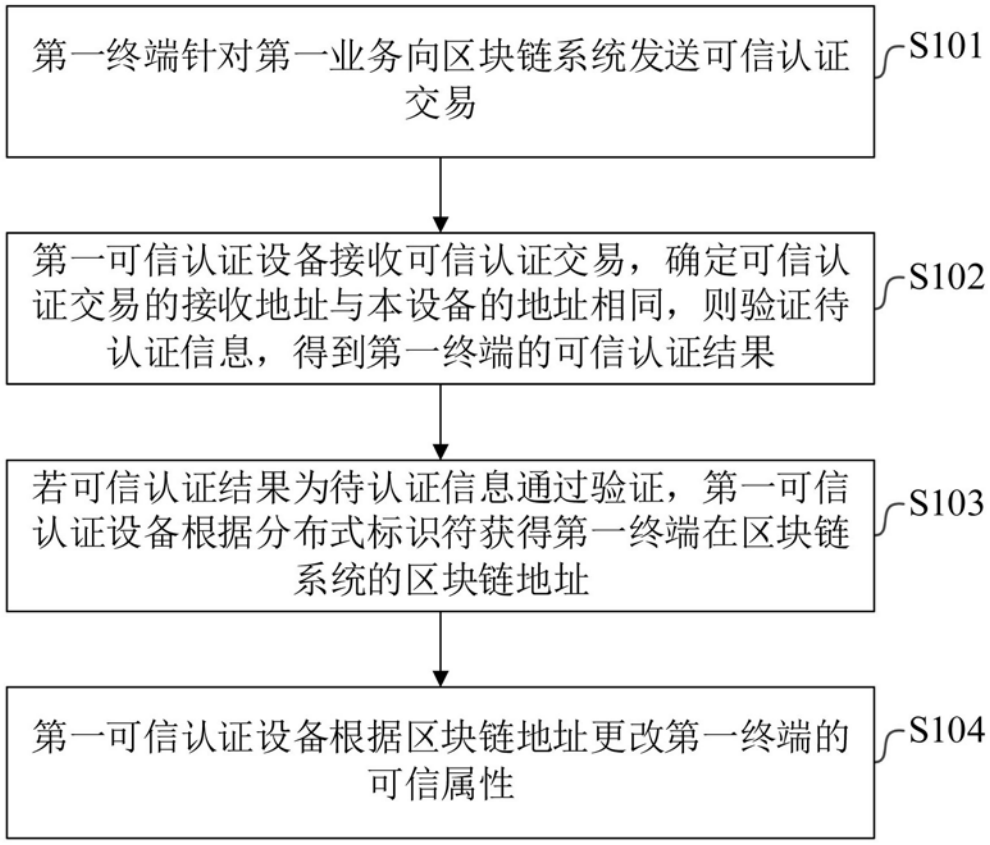

第一终端针对第一业务向区块链系统发送可信认证交易
S101
第一可信认证设备接收可信认证交易，确定可信认证交易的接收地址与本设备的地址相同，则验证待认证信息，得到第一终端的可信认证结果
S102
若可信认证结果为待认证信息通过验证，第一可信认证设备根据分布式标识符获得第一终端在区块链系统的区块链地址
S103
第一可信认证设备根据区块链地址更改第一终端的可信属性
S104

图4

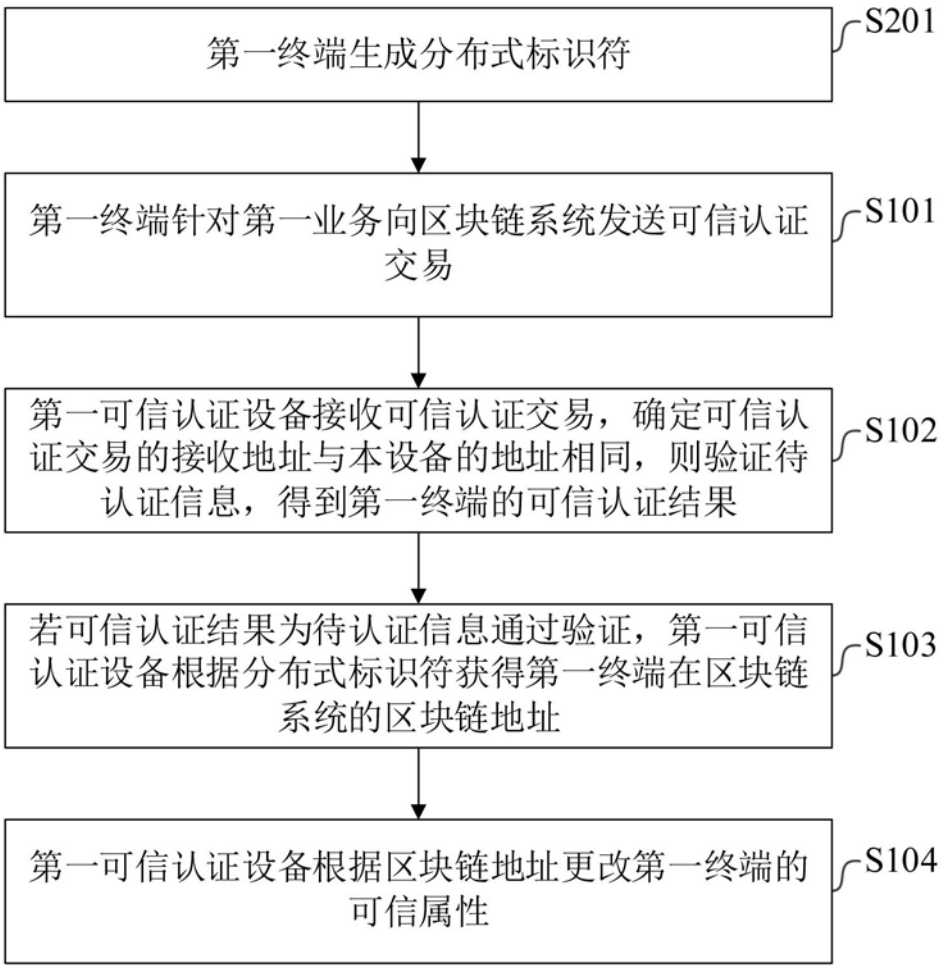

第一终端生成分布式标识符
S201
第一终端针对第一业务向区块链系统发送可信认证交易
S101
第一可信认证设备接收可信认证交易，确定可信认证交易的接收地址与本设备的地址相同，则验证待认证信息，得到第一终端的可信认证结果
S102
若可信认证结果为待认证信息通过验证，第一可信认证设备根据分布式标识符获得第一终端在区块链系统的区块链地址
S103
第一可信认证设备根据区块链地址更改第一终端的可信属性
S104

图5

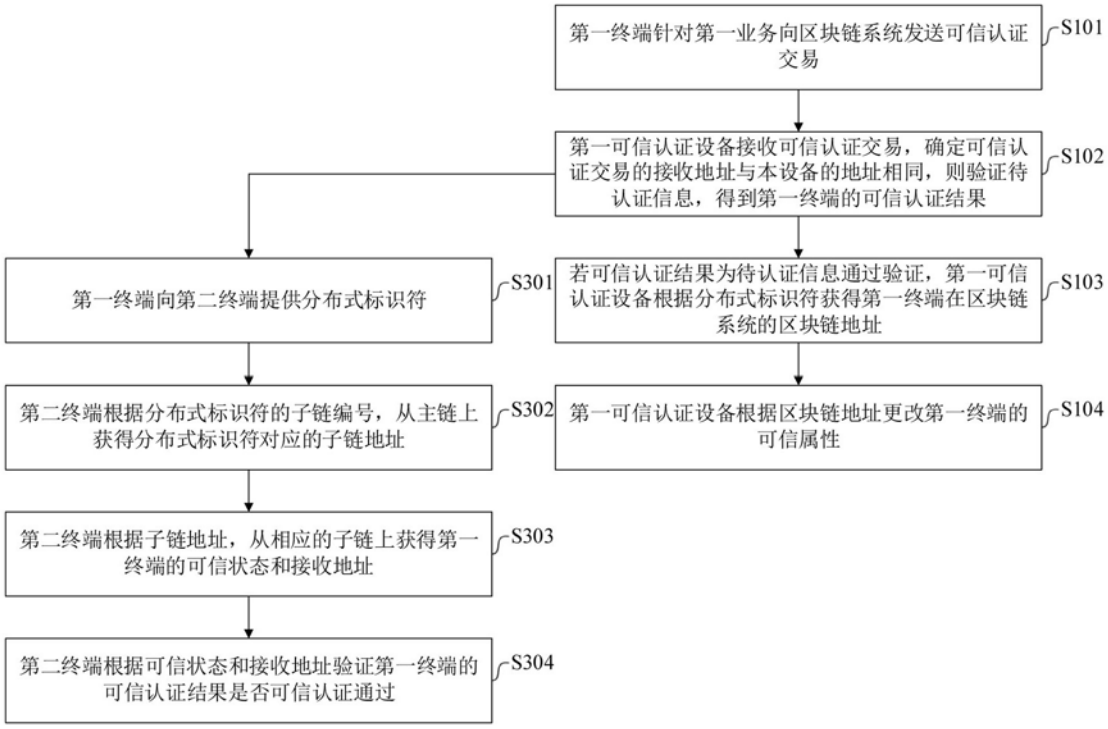

第一终端针对第一业务向区块链系统发送可信认证交易
S101
第一可信认证设备接收可信认证交易，确定可信认证交易的接收地址与本设备的地址相同，则验证待认证信息，得到第一终端的可信认证结果
S102
第一终端向第二终端提供分布式标识符
S301
若可信认证结果为待认证信息通过验证，第一可信认证设备根据分布式标识符获得第一终端在区块链系统的区块链地址
S103
第二终端根据分布式标识符的子链编号，从主链上获得分布式标识符对应的子链地址
S302
第一可信认证设备根据区块链地址更改第一终端的可信属性
S104
第二终端根据子链地址，从相应的子链上获得第一终端的可信状态和接收地址
S303
第二终端根据可信状态和接收地址验证第一终端的可信认证结果是否可信认证通过
S304

图6