(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 108009825 A
(43)申请公布日 2018.05.08

(21)申请号 201711228362.6

(22)申请日 2017.11.29

(71)申请人 江苏安凰领御科技有限公司
地址 214000 江苏省无锡市新吴区震泽路18-3无锡软件园二期射手座A218室

(72)发明人 申子熹

(74)专利代理机构 无锡华源专利商标事务所（普通合伙）32228
代理人 聂启新

(51)Int.Cl.
G06Q 20/38(2012.01)
H04L 9/32(2006.01)

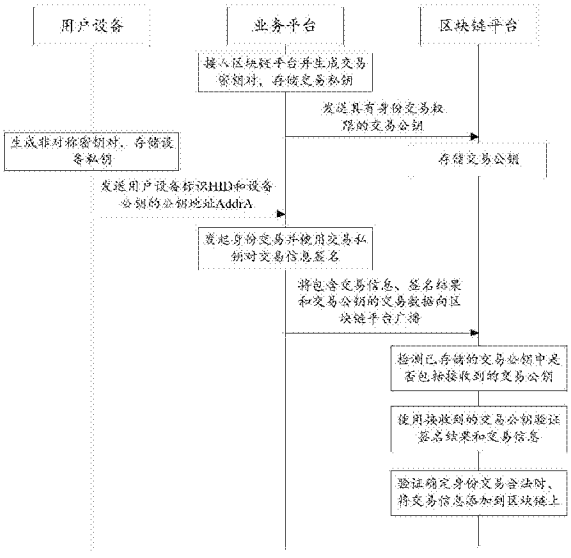
权利要求书1页 说明书4页 附图2页

(54)发明名称

一种基于区块链技术的身份管理系统及方法

(57)摘要

本发明公开了一种基于区块链技术的身份管理系统及方法，涉及区块链技术领域，该系统包括：区块链平台、业务平台和用户设备，用户设备连接业务平台，业务平台连接区块链平台中的一个节点；业务平台可以发起身份交易并对身份交易签名，将身份交易的交易数据向区块链平台广播，区块链平台验证身份交易合法后会将身份交易添加到区块链上，由于区块链技术具有去中心化、防篡改以及共享等特点，因此其他的业务平台只需要接入区块链平台中的节点，即可从区块链上读取到与用户有关的所有业务及各个业务内的相关信息，实现了信息共享，同时信息安全性较高。



CN 108009825 A

1.一种基于区块链技术的身份管理系统，其特征在于，所述系统包括：区块链平台、业务平台和用户设备，所述区块链平台中包括至少三个节点，所述至少三个节点互相建立通讯连接，所述业务平台是为所述用户设备提供服务的业务平台，所述用户设备连接所述业务平台，所述业务平台连接所述区块链平台中的一个节点。

2.一种基于区块链技术的身份管理方法，所述方法用于如权利要求1所述的身份管理系统中，其特征在于，所述方法包括：

所述用户设备向所述业务平台发送认证请求；

所述业务平台接收所述认证请求并根据所述认证请求发起身份交易；

所述业务平台使用存储的交易私钥对所述身份交易的交易信息进行签名得到签名结果；

所述业务平台将所述身份交易的交易数据向所述区块链平台广播，所述交易数据包括所述交易信息、所述签名结果以及交易公钥，所述交易公钥与所述交易私钥为一对密钥；

所述区块链平台中的各个节点根据所述交易数据验证所述身份交易是否合法；

在所述身份交易合法时，所述区块链平台中的各个节点将所述身份交易的交易信息添加到区块链上。

3.根据权利要求2所述的方法，其特征在于，所述区块链平台中的各个节点根据所述交易数据验证所述身份交易是否合法，包括：

所述区块链平台中的各个节点检测所述交易数据中包括的所述交易公钥是否具有身份交易权限；

所述区块链平台中的各个节点通过所述交易数据中包括的所述交易公钥验证所述签名结果和所述交易信息是否有效；

当所述区块链平台中的各个节点检测到所述交易公钥具有身份交易权限且所述签名结果和所述交易信息有效时，确定所述身份交易合法。

4.根据权利要求2或3所述的方法，其特征在于，所述身份交易的交易信息包括所述身份交易的目的地址、交易类型标识、业务平台标识、用户设备标识、账户标识以及用户设备状态标识，所述交易类型标识用于标识发起的是身份交易，所述业务平台标识用于标识所述业务平台，所述用户设备标识用于标识所述用户设备，所述账户标识用于标识用户在所述业务平台内的身份，所述用户状态标识用于标识所述用户设备处于使用状态或者处于注销状态。

5.根据权利要求4所述的方法，其特征在于，所述用户设备向所述业务平台发送认证请求，包括：

所述用户设备生成与所述业务平台对应的一对密钥，所述一对密钥包括设备私钥和设备公钥，所述用户设备存储所述设备私钥；

所述用户设备将所述用户设备标识和所述设备公钥的公钥地址发送给所述业务平台；

则所述方法还包括：所述业务平台确定所述公钥地址为所述身份交易的目的地址。

6.根据权利要求2或3所述的方法，其特征在于，所述方法还包括：

所述业务平台在通过所述区块链平台中的节点接入所述区块链平台时，生成交易密钥对，所述交易密钥包括所述交易公钥和所述交易私钥，所述交易密钥对是具有身份交易权限的密钥对。

一种基于区块链技术的身份管理系统及方法

技术领域

[0001] 本发明涉及区块链技术领域，尤其是一种基于区块链技术的身份管理系统及方法。

背景技术

[0002] 互联网虚拟世界正不断与现实世界相交融，用户接受的网络服务也越来越多，用户使用的不同的智能硬件通常由不同的业务平台来提供服务。比如用户拥有一个智能手环、一块智能手表和一张蓝牙卡，这三个智能设备分别属于不同的硬件厂商，则很可能需要分别在每个智能设备各自对应的业务平台上进行认证。而这些业务平台都分别由各自所属的企业进行管理，业务平台之间相互独立、数据不一致、信息共享程度不高，用户的认证和身份管理较为麻烦。

发明内容

[0003] 本发明人针对上述问题及技术需求，提出了一种基于区块链技术的身份管理系统及方法，该系统及方法可以将用户的相关信息脱敏之后放在区块链上，任何一个业务平台需要时，只需要接入区块链平台并从区块链上读取即可，较为便捷且安全性较高。

[0004] 本发明的技术方案如下：

[0005] 一种基于区块链技术的身份管理系统，该系统包括：区块链平台、业务平台和用户设备，区块链平台中包括至少三个节点，至少三个节点互相建立通讯连接，业务平台是为用户设备提供服务的业务平台，用户设备连接业务平台，业务平台连接区块链平台中的一个节点。

[0006] 一种基于区块链技术的身份管理方法，该方法用于上述身份管理系统中，该方法包括：

[0007] 用户设备向业务平台发送认证请求；

[0008] 业务平台接收认证请求并根据认证请求发起身份交易；

[0009] 业务平台使用存储的交易私钥对身份交易的交易信息进行签名得到签名结果；

[0010] 业务平台将身份交易的交易数据向区块链平台广播，交易数据包括交易信息、签名结果以及交易公钥，交易公钥与交易私钥为一对密钥；

[0011] 区块链平台中的各个节点根据交易数据验证身份交易是否合法；

[0012] 在身份交易合法时，区块链平台中的各个节点将身份交易的交易信息添加到区块链上。

[0013] 其进一步的技术方案为，区块链平台中的各个节点根据交易数据验证身份交易是否合法，包括：

[0014] 区块链平台中的各个节点检测交易数据中包括的交易公钥是否具有身份交易权限；

[0015] 区块链平台中的各个节点通过交易数据中包括的交易公钥验证签名结果和交易

信息是否有效；

[0016] 当区块链平台中的各个节点检测到交易公钥具有身份交易权限且签名结果和交易信息有效时，确定身份交易合法。

[0017] 其进一步的技术方案为，身份交易的交易信息包括身份交易的目的地址、交易类型标识、业务平台标识、用户设备标识、账户标识以及用户设备状态标识，交易类型标识用于标识发起的是身份交易，业务平台标识用于标识业务平台，用户设备标识用于标识用户设备，账户标识用于标识用户在业务平台内的身份，用户状态标识用于标识用户设备处于使用状态或者处于注销状态。

[0018] 其进一步的技术方案为，用户设备向业务平台发送认证请求，包括：

[0019] 用户设备生成与业务平台对应的一对密钥，一对密钥包括设备私钥和设备公钥，用户设备存储设备私钥；

[0020] 用户设备将用户设备标识和设备公钥的公钥地址发送给业务平台；

[0021] 则方法还包括：业务平台确定公钥地址为身份交易的目的地址。

[0022] 其进一步的技术方案为，该方法还包括：

[0023] 业务平台在通过区块链平台中的节点接入区块链平台时，生成交易密钥对，交易密钥包括交易公钥和交易私钥，交易密钥对是具有身份交易权限的密钥对。

[0024] 本发明的有益技术效果是：

[0025] 结合区块链技术的去中心化、防篡改、共享等特点，本申请中业务平台接入区块链平台后将用户及用户设备相关的认证信息脱敏之后添加到区块链上，其他的业务平台只需要接入区块链平台中的节点，即可从区块链上读取到与用户有关的所有业务及各个业务内的相关信息，实现了各业务平台之间的信息共享，使得各业务平台之间可以更好的贴心的为用户提供服务。同时由于区块链中的记录都不可被篡改，身份交易也无法抵赖和破坏，因此在信息共享的同时可以保证信息的隐私和安全。

附图说明

[0026] 图1是本申请公开的基于区块链技术的身份管理系统的系统结构图。

[0027] 图2是本申请公开的基于区块链技术的身份管理方法的流程示意图。

具体实施方式

[0028] 下面结合附图对本发明的具体实施方式做进一步说明。

[0029] 本申请公开了一种基于区块链技术的身份管理系统，请参考图1，该系统包括：区块链平台10、业务平台20和用户设备30。区块链平台10中包括至少三个节点，该至少三个节点两两之间互相建立通讯连接，这里的节点可以是计算机、服务器、工作站和打印机等各种设备，如图1以区块链平台10中包括第一节点11、第二节点12以及第三节点13为例。业务平台20连接区块链平台10中的一个节点，该系统中通常包括若干个业务平台，每个业务平台分别连接区块链平台10中的一个节点，可以是不同的节点也可以是同一个节点，如图1示出了该系统中包括业务平台A和业务平台B，业务平台A连接第一节点11，业务平台B连接第二节点12。业务平台20连接用户设备30并为用户设备30提供服务，用户设备30是诸如计算机、智能手机、智能手环、智能手表以及蓝牙卡之类的智能硬件设备，每个业务平台还可以连接

并为多个用户设备提供服务，图1中仅以业务平台A连接用户设备A，业务平台B连接用户设备B为例。

[0030] 在本申请中，业务平台20在通过区块链平台中的节点接入区块链平台10时会生成交易密钥对，交易密钥包括交易公钥和交易私钥，区块链平台10会赋予此交易密钥对发起身份交易的权限，交易私钥存储在业务平台20中无法导出，交易公钥可以导出至区块链平台10，同时区块链平台10上会保存所有具有身份交易权限的交易公钥的信息。

[0031] 基于图1示出的身份管理系统，本申请还公开了一种基于区块链技术的身份管理方法，该方法主要包括三个部分，请参考如图2所示的流程图：

[0032] 第一部分，绑定部分，包括如下几个步骤：

[0033] 步骤1：用户使用手机软件或其他方式连接用户设备发起绑定操作。

[0034] 步骤2：用户设备生成与业务平台对应的一对非对称密钥，用户设备生成的该密钥对包括设备私钥和设备公钥，用户设备存储设备私钥并导出设备公钥的公钥地址，设备私钥无法导出。

[0035] 步骤3：用户设备读取自身的用户设备标识，用户设备标识用于标识用户设备并与用户设备一一对应，可以是用户设备40的IMEI(International Mobile Equipment Identity，国际移动设备身份码)号或MAC地址(Media Access Control，物理地址)等，用户设备将用户设备标识和设备公钥的公钥地址携带在认证请求中发送给业务平台。

[0036] 绑定部分可以在业务平台接入区块链平台之前或之后，图2以绑定部分在业务平台接入区块链平台之后为例。

[0037] 第二部分，广播部分，包括如下几个步骤：

[0038] 步骤1：业务平台接收认证请求并根据认证请求发起身份交易，该身份交易的交易信息包括身份交易的目的地址、交易类型标识、业务平台标识、用户设备标识、账户标识以及用户设备状态标识。该身份交易的目的地址即为用户设备的设备公钥的公钥地址；交易类型标识用于标识发起的是身份交易；业务平台标识用于标识业务平台，该标识与业务平台一一对应；账户标识用于标识用户在业务平台内的身份，该账户标识由业务平台根据预设的规则生成；用户状态标识用于标识用户设备处于使用状态或者处于注销状态。

[0039] 步骤2：业务平台使用存储的交易私钥对身份交易的交易信息进行签名得到签名结果。

[0040] 步骤3：业务平台将身份交易的交易数据向区块链平台广播，交易数据包括交易信息、签名结果以及交易公钥，交易公钥与交易私钥为一对密钥。

[0041] 第三部分，记录部分，包括如下几个步骤：

[0042] 步骤1：区块链平台中的各个节点根据交易数据验证身份交易是否合法:，该步骤具体过程如下：

[0043] (1)、区块链平台中的各个节点检测交易数据中包括的交易公钥是否具有身份交易权限，如上所述，业务平台在接入区块链平台时会生成具有身份交易权限的交易密钥对并将其中的交易公钥发送给区块链平台，而区块链平台中的各个节点会保存所有具有身份交易权限的交易公钥的信息，因此区块链平台中的各个节点会在已保存的交易公钥中查询是否包括接收到的交易公钥，若包括则表示该接收到的交易公钥具有身份交易权限；否则该接收到的交易公钥不具备身份交易权限，可能是伪造的。

[0044] (2)、区块链平台中的各个节点通过交易数据中包括的交易公钥验证签名结果和交易信息是否有效。

[0045] (3)、当区块链平台中的各个节点检测到交易公钥具有身份交易权限且签名结果和交易信息有效时，确定身份交易合法，否则确定身份交易不合法。

[0046] 需要说明的是，上述(1)和(2)可以同时执行，也可以先执行(1)，确定交易公钥具有身份交易权限再执行(2)，本申请对此不做限定。

[0047] 步骤2：在身份交易合法时，区块链平台中的各个节点将身份交易的交易信息添加到区块链上。各个业务平台都可以使用该方法将交易信息添加到区块链平台上，基于区块链平台去中心化、防篡改、共享等特点，其他业务平台只要接入区块链平台中的节点就能获取到与用户相关的所有业务及各个业务内的账户标识等各类信息，实现了信息共享，同时由于由于区块链平台的特点，身份交易无法抵赖和破坏，也能保证用户信息和记录的隐私性。

[0048] 步骤3：在身份交易不合法时，区块链平台中的各个节点可以直接丢弃该身份交易的交易数据。

[0049] 在一个实际的例子中，以图1中的用户设备A和业务平台A为例，本申请公开的身份管理方法过程如下：业务平台A连接区块链平台中的第一节点11并生成交易密钥对，储存交易私钥K1并将交易公钥K2发送给第一节点11，并通过第一节点11转发给其他各个节点。

[0050] 用户设备A将用户设备标识HID以及设备公钥的公钥地址AddrA上传到业务平台A，业务平台A也会生成该平台内用户的账户标识IDA。业务平台A发起一笔身份交易，叫身份交易的目的地址即为AddrA，同时该身份交易还包括其他附属的交易信息：Type||AppA||HID||IDA||Status，Type为交易类型标识，AppA为业务平台标识，Status为用户设备状态标识。业务平台A使用交易私钥K1对交易信息签名，并将交易信息、签名结果和交易公钥K2通过第一节点11发送至其他各个节点从而在整个区块链平台上广播。第一节点11、第二节点12和第三节点13查询到存储有交易公钥K2，确定交易公钥K2具有身份交易权限，并使用交易公钥K2验证得到签名结果和交易信息没有被篡改，则第一节点11、第二节点12和第三节点13达成共识并将交易信息记录在区块链的区块中。

[0051] 以上所述的仅是本申请的优选实施方式，本发明不限于以上实施例。可以理解，本领域技术人员在不脱离本发明的精神和构思的前提下直接导出或联想到的其他改进和变化，均应认为包含在本发明的保护范围之内。

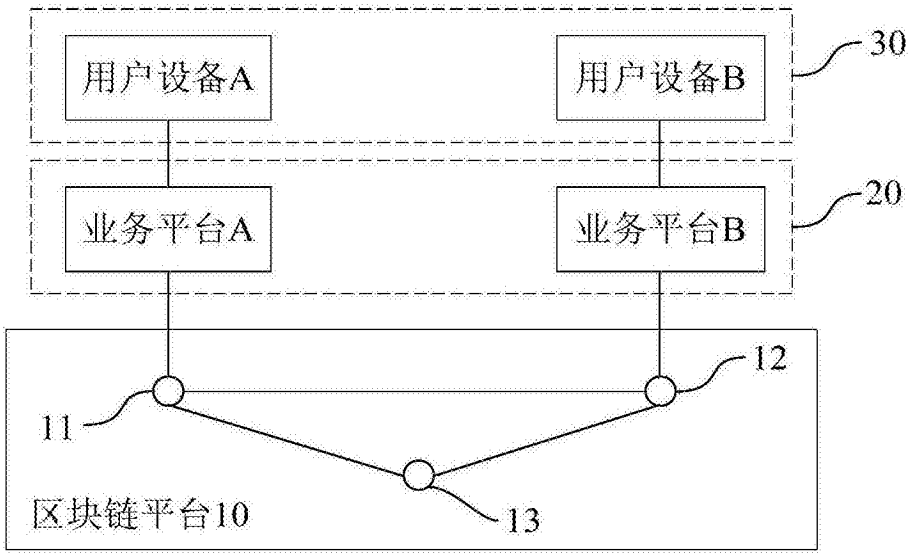


图1

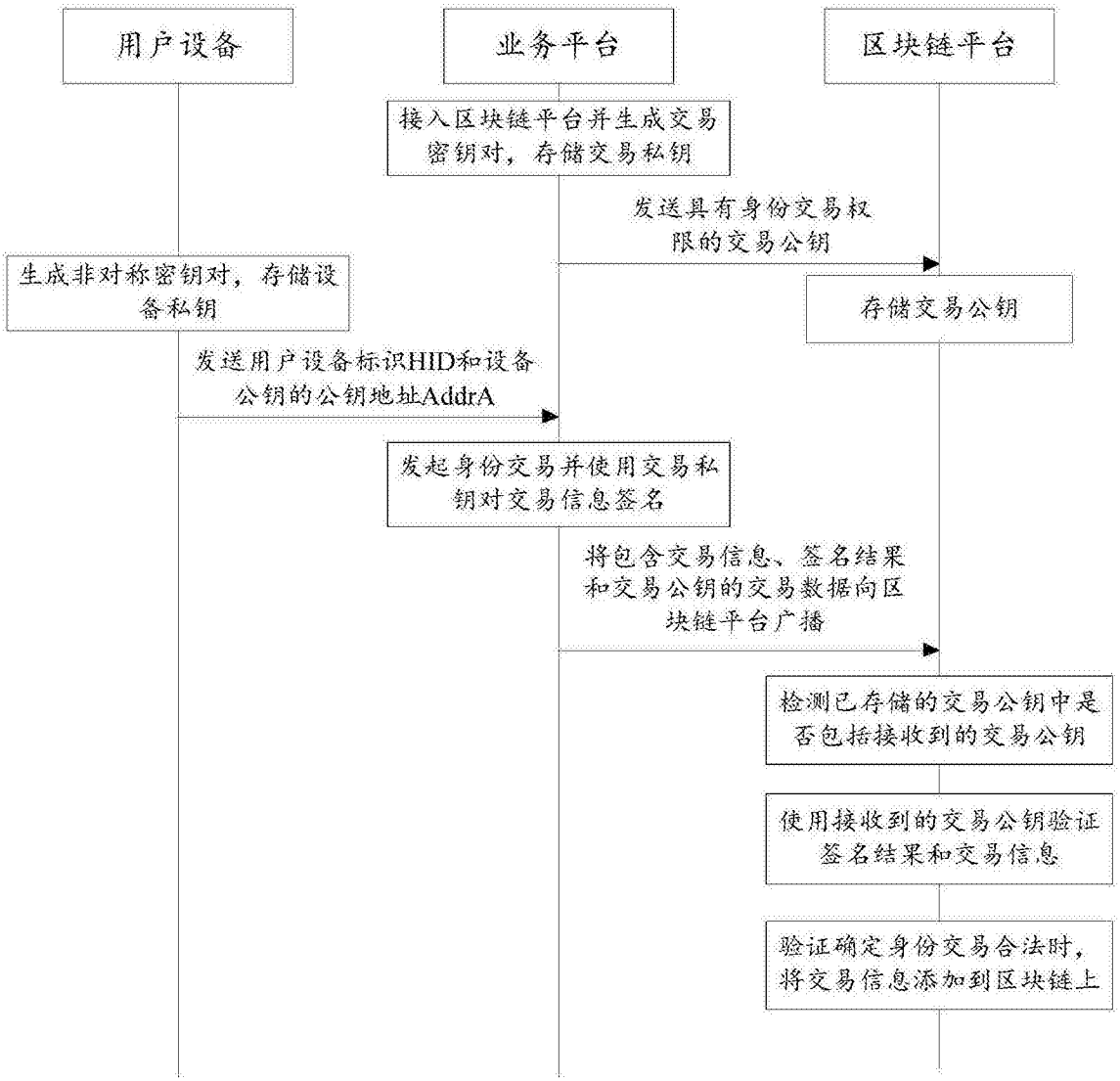

用户设备
业务平台
区块链平台
接入区块链平台并生成交易密钥对，存储交易私钥
发送具有身份交易权限的交易公钥
生成非对称密钥对，存储设备私钥
存储交易公钥
发送用户设备标识HID和设备公钥的公钥地址AddrA
发起身份交易并使用交易私钥对交易信息签名
将包含交易信息、签名结果和交易公钥的交易数据向区块链平台广播
检测已存储的交易公钥中是否包括接收到的交易公钥
使用接收到的交易公钥验证签名结果和交易信息
验证确定身份交易合法时，将交易信息添加到区块链上

图2