

一种基于区块链的用户要素认证的方法及装置

技术领域

[01]本说明书涉及计算机应用领域，尤其涉及一种基于区块链的用户要素认证方法及装置。

背景技术

[02]用户要素认证通常指，特定的用户要素认证机构通过判断用户提供的若干包含隐私信息的用户要素是否匹配，来确定上述若干个用户要素所指示的对象的身份的真实性；但是在实际应用场景中，可能同时存在较多数量的用户要素提供方、用户要素认证结果的使用方以及用户要素认证机构，因此，用户难以快速找到合适的认证机构，完成用户要素认证过程。

[03]在相关技术中，可以在上述交互情景中加入中介者角色，用户将待认证的用户要素发送给中介者，而无需操心后续流程；认证机构从中介者处获取待认证的用户要素并返回对应的用户要素认证结果，也不需要直接联系用户要素的提供方和认证结果的使用方。但是，此方案需要用户将包含隐私数据的用户要素发送给中介者，这可能会导致隐私信息的不必要泄露；因此，业界亟需一种能够兼顾高效率和高安全性的用户要素认证方案。

发明内容

[04]有鉴于此，本说明书公开了一种基于区块链的用户要素认证方法和装置。

[05]根据本说明书实施例的第一方面，公开了一种基于区块链的用户要素认证方法，应用于区块链中的节点设备；其中，所述区块链中部署有用于管理用户要素认证流程的智能合约；所述方法包括：接收智能合约调用交易；其中，所述智能合约调用交易中携带有来自用户客户端的已加密的用于确认用户身份真实性的待认证用户要素；响应于所述智能合约调用交易，调用所述智能合约中的加密转换逻辑，在所述节点设备搭载的可信计算环境中，对所述已加密待认证用户要素进行解密，并进一步对解密后的待认证用户要素进行二次加密处理，其中，所述二次加密处理对应的解密密钥由用户要素认证机构维护，以使所述用户要素认证机构获取二次加密处理后的待认证用户要素，基于所述解密密钥对所述待认证用户要素进行解密，并基于解密后的所述待认证用户要素进行用户要素认证；获取所述用户要素认证机构提交至所述智能合约的针对所述待认证用户要素

的认证结果，并在所述区块链的分布式账本中存储所述认证结果，以使与所述区块链对接的认证结果使用方从所述区块链的分布式账本中获取所述认证结果，并基于所述认证结果确认所述用户客户端提供的用户身份的真实性。

[06]根据本说明书实施例的第二方面，公开了一种基于区块链的用户要素认证装置，应用于区块链中的节点设备；其中，所述区块链中部署有用于管理用户要素认证流程的智能合约；所述装置包括：接收模块，接收智能合约调用交易；其中，所述智能合约调用交易中携带有来自用户客户端的已加密的用于确认用户身份真实性的待认证用户要素；认证模块，响应于所述智能合约调用交易，调用所述智能合约中的加密转换逻辑，在所述节点设备搭载的可信计算环境中，对所述已加密待认证用户要素进行解密，并进一步对解密后的待认证用户要素进行二次加密处理，其中，所述二次加密处理对应的解密密钥由用户要素认证机构维护，以使所述用户要素认证机构获取二次加密处理后的待认证用户要素，基于所述解密密钥对所述待认证用户要素进行解密，并基于解密后的所述待认证用户要素进行用户要素认证；存储模块，获取所述用户要素认证机构提交至所述智能合约的针对所述待认证用户要素的认证结果，并在所述区块链的分布式账本中存储所述认证结果，以使与所述区块链对接的认证结果使用方从所述区块链的分布式账本中获取所述认证结果，并基于所述认证结果确认所述用户客户端提供的用户身份的真实性。

[07]以上技术方案中，一方面，由于上述用户客户端、认证机构以及认证结果使用方均无需自行沟通业务、建立连接，只需要与区块链进行交互，即可完成用户要素认证的整个业务流程，因此可以显著提高用户要素认证这一业务的运营效率；另一方面，由于区块链节点对待认证用户要素进行的加密转换过程，是在可信执行环境下完成的，因而本方案中的区块链节点设备从原理上即不可能获取到明文形式的待认证用户要素，因此保证了用户的待认证用户要素中隐私信息不会被泄露，提高了用户要素认证这一业务的安全性。

附图说明

[08]此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本说明书的实施例，并与说明书文本一同用于解释原理。

[09]图 1 是本说明书所述基于区块链的用户要素认证的情景示例图；

[10]图 2 是本说明书所述智能合约的创建和调用过程的示意图；

[11]图 3 是本说明书所述基于区块链的用户要素认证方法的流程示例图；

[12]图4是本说明书所述基于区块链的用户要素认证装置的结构示例图;

[13]图5是本说明书所述计算机设备的结构示例图。

具体实施方式

[14]为了使本技术领域的人员更好地理解本说明书一个或多个实施例中的技术方案,下面将结合本说明书一个或多个实施例中的附图,对本说明书一个或多个实施例中的技术方案进行清楚、完整地描述。显然,所描述的实施例仅仅是一部分实施例,而不是全部的实施例。基于本说明书一个或多个实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都应当属于本说明书保护的范围。

[15]下面的描述涉及附图时,除非另有表示,不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本说明书相一致的所有实施方式。相反,它们仅是与如所附权利要求书中所详述的、本说明书的一些方面相一致的系统和方法的例子。

[16]在本说明书使用的术语是仅仅出于描述特定实施例的目的,而非旨在限制本说明书。在本说明书和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式,除非上下文清楚地表示其他含义。还应当理解,本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[17]应当理解,尽管在本说明书可能采用术语第一、第二、第三等来描述各种信息,但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如,在不脱离本说明书范围的情况下,第一信息也可以被称为第二信息,类似地,第二信息也可以被称为第一信息。取决于语境,如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[18]用户要素认证通常指,特定的用户要素认证机构通过判断用户提供的若干包含隐私信息的用户要素信息是否匹配,来确定上述若干个用户要素信息所指示的对象的身份的真实性;举例而言,公民可以通过提供姓名、身份证号、住址等信息的方式,来证明本人的身份;商户可以通过提供经营个体名称、许可证编号等信息的方式,来证明所经营的个体的身份。通常而言,通信运营商、公安网络数据库、银行数据库、工商管理数据库等能存储有够作为上述用户要素的对应关系的个体,都可以作为上述用户要素认证机构,提供用户要素认证服务;但是在实际应用场景中,可能同时存在较多数量的用户要素提供方、用户要素认证结果的使用方以及用户要素认证机构,因此,用户难以快速找

到合适的认证机构，完成用户要素认证过程。

[19]在相关技术中，可以在上述交互情景中加入中介者角色，用户只需要将待认证的用户要素发送给中介者，而无需操心后续流程；认证机构只需要从中介者处获取待认证的用户要素并返回对应的用户要素认证结果，也不需要直接联系用户要素的提供方和认证结果的使用方。采用此方案，可以明显提高用户要素认证这类业务的执行效率，极大改善用户的体验。但是，此方案需要用户将包含隐私数据的用户要素发送给中介者，这可能会导致隐私信息的不必要泄露；而由于通常情况下，用户提供的用户要素信息隐私程度越高，就意味着身份伪造者更难以获取、冒用用户要素信息，因而用户要素认证的结果的可靠性也越高，因而为了保证用户要素认证最终的效果，用户也不可能通过降低用户要素的隐私程度的方式来减少隐私信息的泄露；因此，业界亟需一种能够兼顾高效率和高安全性的用户要素认证方案。

[20]基于此，本说明书公开了一种通过区块链上可信执行环境内执行的智能合约管理用户要素认证流程的技术方案。

[21]在实现时，请参见图 1，图 1 为本说明书所述基于区块链的用户要素认证的情景示例图；一方面，该例中将区块链作为用户要素认证的情景中的中介者，无需上述用户客户端、用户要素认证机构以及认证结果使用方自行沟通业务、建立连接；另一方面，该例中从用户客户端到区块链，再到用户要素认证机构，涉及到的待认证用户要素可以全程加密，并由区块链中的智能合约在可信执行环境 TEE(Trusted execution environment)下完成加密形式的转换。

[22]以上技术方案中，一方面，由于上述用户客户端、用户要素认证机构以及认证结果使用方均无需自行沟通业务、建立连接，只需要与区块链进行交互，即可完成用户要素认证的整个业务流程，因此可以显著提高用户要素认证这一业务的运营效率；另一方面，由于区块链节点对待认证用户要素进行的加密转换过程，是在可信执行环境下完成的，因而本方案中的区块链节点设备从原理上即不可能获取到明文形式的待认证用户要素，因此保证了用户的待认证用户要素中隐私信息不会被泄露，提高了用户要素认证这一业务的安全性。

[23]区块链一般被划分为三种类型：公有链(Public Blockchain)，私有链(Private Blockchain)和联盟链(Consortium Blockchain)。此外，还可以有上述多种类型的结合，比如私有链+联盟链、联盟链+公有链等。

[24]其中，去中心化程度最高的是公有链。公有链以比特币、以太坊为代表，加入公有链的参与者（也可称为区块链中的节点）可以读取链上的数据记录、参与交易、以及竞争新区块的记账权等。而且，各节点可自由加入或者退出网络，并进行相关操作。

[25]私有链则相反，该网络的写入权限由某个组织或者机构控制，数据读取权限受组织规定。简单来说，私有链可以为一个弱中心化系统，其对节点具有严格限制且节点数量较少。这种类型的区块链更适合于特定机构内部使用。

[26]联盟链则是介于公有链以及私有链之间的区块链，可实现“部分去中心化”。联盟链中各个节点通常有与之相对应的实体机构或者组织；节点通过授权加入网络并组成利益相关联盟，共同维护区块链运行。

[27]基于区块链的基本特性，区块链通常是由若干个区块构成。在这些区块中分别记录有与该区块的创建时刻对应的时间戳，所有的区块严格按照区块中记录的时间戳，构成一条在时间上有序的数据链条。

[28]对于物理世界产生的真实数据，可以将其构建成区块链所支持的标准的交易（transaction）格式，然后发布至区块链，由区块链中的节点设备对收到的交易进行共识处理，并在达成共识后，由区块链中作为记账节点的节点设备，将这笔交易打包进区块，在区块链中进行持久化存证。

[29]在实际应用中，不论是公有链、私有链还是联盟链，都可能提供智能合约（Smart contract）的功能。区块链上的智能合约是在区块链上可以被交易触发执行的合约。智能合约可以通过代码的形式定义。

[30]以以太坊为例，支持用户在以太坊网络中创建并调用一些复杂的逻辑。以太坊作为一个可编程区块链，其核心是以太坊虚拟机（EVM），每个以太坊节点都可以运行EVM。EVM是一个图灵完备的虚拟机，通过它可以实现各种复杂的逻辑。用户在以太坊中发布和调用智能合约就是在EVM上运行的。实际上，EVM直接运行的是虚拟机代码（虚拟机字节码，下简称“字节码”），所以部署在区块链上的智能合约可以是字节码。

[31]请参见图2，图2是创建智能合约和调用智能合约的一示意图；如图2所示，以太坊中要创建一个智能合约，需要经过编写智能合约、变成字节码、部署到区块链等过程。以太坊中调用智能合约，是发起一笔指向智能合约地址的交易，各个节点的EVM可以分别执行该交易，将智能合约代码分布式的运行在以太坊网络中每个节点的虚拟机中。

[32]下面通过具体实施例并结合具体的应用场景对本说明书进行描述。

[33]请参考图 3，图 3 是本说明书所述基于区块链的用户要素认证方法的流程示例图；该方法可以应用于区块链中的节点设备；其中，所述区块链中部署有用于管理用户要素认证流程的智能合约；该方法可以包括以下步骤：S301，接收智能合约调用交易；其中，所述智能合约调用交易中携带有来自用户客户端的已加密的用于确认用户身份真实性的待认证用户要素；S302，响应于所述智能合约调用交易，调用所述智能合约中的加密转换逻辑，在所述节点设备搭载的可信计算环境中，对所述已加密待认证用户要素进行解密，并进一步对解密后的待认证用户要素进行二次加密处理，其中，所述二次加密处理对应的解密密钥由用户要素认证机构维护，以使所述用户要素认证机构获取二次加密处理后的待认证用户要素，基于所述解密密钥对所述待认证用户要素进行解密，并基于解密后的所述待认证用户要素进行用户要素认证；S303，获取所述用户要素认证机构提交至所述智能合约的针对所述待认证用户要素的认证结果，并在所述区块链的分布式账本中存储所述认证结果，以使与所述区块链对接的认证结果使用方从所述区块链的分布式账本中获取所述认证结果，并基于所述认证结果确认所述用户客户端提供的用户身份的真实性。

[34]上述区块链，可以包括任意形式的区块链；如前文所述，公有链具有更高的去中心化程度，这意味着其可靠程度更高，但执行效率也偏低；而私有链则相反，由于规模较小且范围受限，一般执行效率较高，但可靠性不及大规模的公有链；因此，本领域技术人员可以根据具体的业务需求，以及各种形式的区块链的特性，自行选择并完成具体的区块链构建，本说明书不作进一步限定。

[35]上述用户客户端，可以包括任意的能够提供上述相关功能的软硬件；例如，其既可以是专用的硬件客户端，也可以是独立设计的软件客户端，或者依托于其他应用程序的小程序，又或者具有交互能力的网页等等；本领域技术人员可以根据具体的业务需求，参照相关技术文献完成具体开发设计，本说明书不作进一步限定。

[36]上述用户要素，可以包括用于用户要素认证的任意用户要素；可以理解的是，上述用户要素认证机构的具体类型可以与上述待认证用户要素相匹配；例如，上述待认证的用户要素中包含用户的姓名和身份证号，那么对应的用户要素认证机构就可以是公安网络等存储有用户的姓名和身份证号的对应关系的相关机构；又例如，上述待认证的用户要素中包含商户的公司名称以及营业执照编号，那么对应的用户要素认证机构就可以是工商管理部门等存储有公司名称和营业执照编号的对应关系的机构；本领域技术人员可以根据具体需求，自行选择应用场景以及用户要素类型，本说明书无需进行详细列举。

[37]在示出的一种实施方式中，上述待认证用户要素可以是用户的身份信息。由于用户通常更加注重保护自身的隐私数据，因此在需要将涉及隐私的身份信息作为待认证用户要素时，应用上述方案进行用户要素认证，可以免除“中介者”攫取身份信息，导致隐私泄露的可能。

[38]在示出的一种实施方式中，上述用户的身份信息，可以包括用户的姓名、身份证号码以及手机号码；与上述身份信息对应的，上述用户要素认证机构则可以是手机运营商。例如，用户张三需要到银行办理开户业务，则需要向银行提供自己的姓名、身份证号码以及手机号码，并完成基于该姓名、身份证号码以及手机号码的用户要素认证；一般而言，此三种用户要素的对应关系可以在手机运营商的数据库中存储，因此手机运营商可以作为此次用户要素认证的用户要素认证机构；可以理解的是，基于手机运营商的用户要素认证仅仅是用户要素认证的一个常见实现形式，不应视为对本说明书方案构成不当限定。

[39]在本说明书中，上述区块链中的节点设备可以首先接收携带有来自用户客户端的智能合约调用交易，其中，该智能合约调用交易可以携带用于确认用户身份真实性的已加密的待认证用户要素；如前所述，区块链上预先部署的智能合约可以通过交易来进行调用，而且可以将智能合约执行中所需要的数据携带在调用交易中，完成信息的交互。由于需要保证待认证用户要素不被泄露，区块链的节点设备不能直接读取到待认证用户要素的明文，所以在该智能合约调用交易中，待认证用户要素可以由用户客户端加密后的密文。可以理解的是，上述智能合约调用交易，可以是上述客户端直接发起，也可以是由其他的服务端、中转平台等间接发起；例如，为了保证区块链的运行效率以及安全，可以设定只有特定的服务端具有向区块链中发起智能合约调用交易的权限，在此种情况下，上述用户客户端即可首先将上述待认证用户要素的密文发送至有权限的服务端，再由服务端生成对应的智能合约调用交易，并发送到区块链上。

[40]在示出的一种实施方式中，上述节点设备可以与服务端对接；在此种环境下，上述用户客户端可以首先将上述待认证用户要素的密文携带在一个用户要素认证请求中，并发送给上述服务端，上述服务端再基于已加密的待认证用户要素构建智能合约调用交易，并发送到与其对接的节点设备上。应用此种设计，可以在上述服务端上进一步开发设计权限控制、资费计算等功能，以适应更加复杂的业务环境需求，本说明书无需进行进一步限定，本领域技术人员可以参考相关技术文献，完成具体设计。

[41]在本说明书中，上述节点设备可以响应于上述智能合约调用交易，调用上述智能合

约中的加密转换逻辑,在上述节点设备搭载的可信计算环境中对上述已加密待认证用户要素进行解密;由于可信计算环境对外界而言是不可观测的黑盒状态,因此即使在可信计算环境下完成了上述解密过程,也不会导致待认证用户要素中的隐私数据的泄露;在完成解密后,可以进一步对解密后的待认证用户要素进行二次加密处理;其中,此次二次加密处理对应的解密密钥可以由用户要素认证机构维护;举例而言,上述两次加解密可以均采用非对称加密方式进行,假设上述节点设备搭载的可信计算环境中维护有一私钥 A1,对应的公钥 A2 则由用户客户端持有,上述用户要素认证机构可以持有一私钥 B1,对应的公钥 B2 则由上述节点设备搭载的可信计算环境持有;在实现上述方案时,上述用户客户端可以首先使用公钥 A2 对待认证用户要素进行加密,并通过智能合约调用交易的形式发送至上述节点设备,上述节点设备则可以在其搭载的可信计算环境中,利用维护的私钥 A1 完成第一次解密,并使用公钥 B2 对解密后的待认证用户要素进行二次加密,得到只有持有私钥 B1 的用户要素认证机构可以解密的二次加密处理后的待认证用户要素。

[42]可以理解的是,上述密钥使用过程仅为一个可行示例,具体的密码机制可以根据具体的业务需求进行选择和设计,本说明书不作进一步限定。

[43]在本说明书中,上述节点设备可以执行上述二次加密处理的过程,以使上述用户要素认证机构获取二次加密处理后的待认证用户要素,基于上述解密密钥对上述待认证用户要素进行解密,并基于解密后的上述待认证用户要素进行用户要素认证;具体而言,由于上述区块链的节点设备在上述业务场景中扮演了中介者的角色,因此在发起用户要素认证的用户以及用户要素认证机构的数量较多时,可以基于预设的匹配机制,为发起用户要素认证的用户分配对应的用户要素认证机构,以保证用户要素认证业务的顺利进行;具体而言,选择用户要素认证机构的方式可以是基于待认证用户要素类型的,例如涉及手机号的待认证用户要素,可以为其匹配手机运营商作为对应的用户要素认证机构,涉及银行卡号的待认证用户要素,可以为其匹配银行作为对应的用户要素认证机构,等等。可以理解的是,虽然待认证用户要素本身的内容可以进行加密,但待认证用户要素的类型可以通过预设标志位或者附带标签等方式进行标识,因此本领域技术人员可以自行根据具体需求,设计选择用户要素认证机构的方式。

[44]在示出的一种实施方式中,上述智能合约调用交易中还可以携带有用户客户端指定的目标用户要素认证机构的标识;在此种情况下,可以设计只有上述目标用户要素认证机构可以解密该节点设备二次加密后的待认证用户要素,因此,可以在接收到上述智能

合约调用交易后，查询预设的加密密钥表得到与上述目标用户要素认证机构对应的二次加密密钥，在对解密后的待认证用户要素进行二次加密处理时，即可以采用确定出的、与上述目标用户要素认证机构对应的二次加密密钥；相对应的，在令用户要素认证机构获取二次加密处理后的待认证用户要素，对上述待认证用户要素进行二次解密，并基于解密后的上述待认证用户要素进行用户要素认证时，就可以直接指定上述标识对应的目标用户要素认证机构获取二次加密处理后的待认证用户要素，对上述待认证用户要素进行二次解密，并基于解密后的上述待认证用户要素进行用户要素认证。

[45]可以理解的是，用户要素认证机构内部基于待认证用户要素生成用户要素认证结果的方式，例如查询存储有待认证用户要素的对应关系的数据库等等，本说明书无需进行详细限定，本领域技术人员可以根据具体实施环境，以及相关需求自行确定实现方式。

[46]在本说明书中，在上述用户要素认证机构完成用户要素认证后，上述节点设备获取所述用户要素认证机构提交至所述智能合约的针对所述待认证用户要素的认证结果，并在所述区块链的分布式账本中存储所述认证结果，以使与所述区块链对接的认证结果使用方从所述区块链的分布式账本中获取所述认证结果，并基于所述认证结果确认所述用户客户端提供的用户身份的真实性；具体而言，如前所述，区块链在该用户要素认证的业务场景中扮演中介者的角色，因此上述用户要素认证机构生成的用户要素认证结果可以通过该区块链发送给认证结果的使用方。可以理解的是，上述认证结果的使用方，可以是用户自身；例如，用户可以通过上述用户要素认证过程，得到用户要素认证机构针对某一组待认证用户要素给出的认证通过证明，从而可以直接自行持有该证明办理其他需要保证用户要素认证通过的业务。

[47]在示出的一种实施方式中，上述使认证结果的使用方从区块链的分布式账本中获取认证结果的具体方式，可以是首先由该节点设备在该区块链的分布式账本中存储上述认证结果，并生成与所述认证结果对应的结果返回事件，再由上述服务端响应于上述结果返回事件，从上述区块链的分布式账本中获取上述认证结果，并将上述认证结果发送至上述认证结果的使用方。

[48]可以理解的是，上述通过服务端进行中转的方式，仅是一返回认证结果的可行示例，上述认证结果的使用方也可以直接响应于上述结果返回事件，从区块链的分布式账本中获取上述认证结果，又或者通过预设的识别逻辑，直接从区块链分布式账本的新增内容中抓取上述认证结果；此外，该过程中也可以通过加密的方式进一步提高认证结果的私密性；因此，本领域技术人员可以根据具体需求，自行设计上述用户要素认证机构将认

证结果通过区块链发送给认证结果的使用方的具体形式，本说明书不作进一步限定。

[49]上述内容即为本说明书针对所述基于区块链的用户要素认证方法的全部实施例。本说明书还提供了对应的基于区块链的用户要素认证装置的实施例如下：本说明书提出一种基于区块链的用户要素认证装置，其结构示例如图4所示；该装置可以应用于区块链中的节点设备；其中，所述区块链中部署有用于管理用户要素认证流程的智能合约；所述装置包括：接收模块401，接收智能合约调用交易；其中，所述智能合约调用交易中携带有来自用户客户端的已加密的用于确认用户身份真实性的待认证用户要素；认证模块402，响应于所述智能合约调用交易，调用所述智能合约中的加密转换逻辑，在所述节点设备搭载的可信计算环境中，对所述已加密待认证用户要素进行解密，并进一步对解密后的待认证用户要素进行二次加密处理，其中，所述二次加密处理对应的解密密钥由用户要素认证机构维护，以使所述用户要素认证机构获取二次加密处理后的待认证用户要素，基于所述解密密钥对所述待认证用户要素进行解密，并基于解密后的所述待认证用户要素进行用户要素认证；存储模块403，获取所述用户要素认证机构提交至所述智能合约的针对所述待认证用户要素的认证结果，并在所述区块链的分布式账本中存储所述认证结果，以使与所述区块链对接的认证结果使用方从所述区块链的分布式账本中获取所述认证结果，并基于所述认证结果确认所述用户客户端提供的用户身份的真实性。

[50]在示出的一种实施方式中，上述节点设备可以与服务端对接；在此种环境下，上述用户客户端可以首先将上述待认证用户要素的密文携带在一个用户要素认证请求中，并发送给上述服务端，上述服务端再基于已加密的待认证用户要素构建智能合约调用交易，并发送到与其对接的节点设备上。应用此种设计，可以在上述服务端上进一步开发设计权限控制、资费计算等功能，以适应更加复杂的业务环境需求，本说明书无需进行进一步限定，本领域技术人员可以参考相关技术文献，完成具体设计。

[51]在示出的一种实施方式中，上述智能合约调用交易中还可以携带有用户客户端指定的目标用户要素认证机构的标识；在此种情况下，上述目标用户要素认证机构可以解密该节点设备二次加密后的待认证用户要素，因此，上述装置还可以包括查询模块，该模块可以在接收到上述智能合约调用交易后，查询预设的加密密钥表得到与上述目标用户要素认证机构对应的二次加密密钥；上述认证模块402对解密后的待认证用户要素进行二次加密处理时，可以采用与上述目标用户要素认证机构对应的二次加密密钥；相对应的，在令用户要素认证机构获取二次加密处理后的待认证用户要素，对上述待认证用户要素进行二次解密，并基于解密后的上述待认证用户要素进行用户要素认证时，上述转

换模块402就可以直接指定上述标识对应的目标用户要素认证机构获取二次加密处理后的待认证用户要素，对上述待认证用户要素进行二次解密，并基于解密后的上述待认证用户要素进行用户要素认证。

[52]在示出的一种实施方式中，上述存储模块403使认证结果的使用方从区块链的分布式账本中获取认证结果的具体方式，可以是首先在上述区块链的分布式账本中存储上述认证结果，并生成与上述认证结果对应的结果返回事件，再由上述服务端响应于上述结果返回事件，从上述区块链的分布式账本中获取上述认证结果，并将上述认证结果发送至上述认证结果的使用方。

[53]可以理解的是，上述通过服务端进行中转的方式，仅是一返回认证结果的可行示例，上述认证结果的使用方也可以直接响应于上述结果返回事件，从区块链的分布式账本中获取上述认证结果，又或者通过预设的识别逻辑，直接从区块链分布式账本的新增内容中抓取上述认证结果；此外，该过程中也可以通过加密的方式进一步提高认证结果的私密性；因此，本领域技术人员可以根据具体需求，自行设计上述用户要素认证机构将认证结果通过区块链发送给认证结果的使用方的具体形式，本说明书不作进一步限定。

[54]在示出的一种实施方式中，上述待认证用户要素可以是用户的身份信息。由于用户通常更加注重保护自身的隐私数据，因此在需要将涉及隐私的身份信息作为待认证用户要素时，应用上述方案进行用户要素认证，可以免除“中介者”攫取身份信息，导致隐私泄露的可能。

[55]在示出的一种实施方式中，上述用户的身份信息，可以包括用户的姓名、身份证号码以及手机号码；与上述身份信息对应的，上述用户要素认证机构则可以是手机运营商。例如，用户张三需要到银行办理开户业务，则需要向银行提供自己的姓名、身份证号码以及手机号码，并完成基于该姓名、身份证号码以及手机号码的用户要素认证；一般而言，此三种用户要素的对应关系可以在手机运营商的数据库中存储，因此手机运营商可以作为此次用户要素认证的用户要素认证机构；可以理解的是，基于手机运营商的用户要素认证仅仅是用户要素认证的一个常见实现形式，不应视为对本说明书方案构成不当限定。

[56]本说明书实施例还提供一种计算机设备，其至少包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，处理器执行所述程序时实现前述的基于区块链的用户要素认证方法。

[57]图 5 示出了本说明书实施例所提供的一种更为具体的计算设备硬件结构示意图，该设备可以包括：处理器 1010、存储器 1020、输入/输出接口 1030、通信接口 1040 和总线 1050。其中处理器 1010、存储器 1020、输入/输出接口 1030 和通信接口 1040 通过总线 1050 实现彼此之间在设备内部的通信连接。

[58]处理器 1010 可以采用通用的 CPU（Central Processing Unit，中央处理器）、微处理器、应用专用集成电路（Application Specific Integrated Circuit，ASIC）、或者一个或多个集成电路等方式实现，用于执行相关程序，以实现本说明书实施例所提供的技术方案。

[59]存储器 1020 可以采用 ROM（Read Only Memory，只读存储器）、RAM（Random Access Memory，随机存取存储器）、静态存储设备，动态存储设备等形式实现。存储器 1020 可以存储操作系统和其他应用程序，在通过软件或者固件来实现本说明书实施例所提供的技术方案时，相关的程序代码保存在存储器 1020 中，并由处理器 1010 来调用执行。

[60]输入/输出接口 1030 用于连接输入/输出模块，以实现信息输入及输出。输入输出/模块可以作为组件配置在设备中（图中未示出），也可以外接于设备以提供相应功能。其中输入设备可以包括键盘、鼠标、触摸屏、麦克风、各类传感器等，输出设备可以包括显示器、扬声器、振动器、指示灯等。

[61]通信接口 1040 用于连接通信模块（图中未示出），以实现本设备与其他设备的通信交互。其中通信模块可以通过有线方式（例如 USB、网线等）实现通信，也可以通过无线方式（例如移动网络、WIFI、蓝牙等）实现通信。

[62]总线 1050 包括一通路，在设备的各个组件（例如处理器 1010、存储器 1020、输入/输出接口 1030 和通信接口 1040）之间传输信息。

[63]需要说明的是，尽管上述设备仅示出了处理器 1010、存储器 1020、输入/输出接口 1030、通信接口 1040 以及总线 1050，但是在具体实施过程中，该设备还可以包括实现正常运行所必需的其他组件。此外，本领域的技术人员可以理解的是，上述设备中也可仅包含实现本说明书实施例方案所必需的组件，而不必包含图中所示的全部组件。

[64]本说明书实施例还提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现前述的基于区块链的用户要素认证方法。

[65]计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存（PRAM）、静态随机存取存储器

(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带、磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质,可用于存储可以被计算设备访问的信息。按照本文中的界定,计算机可读介质不包括暂存电脑可读媒体(transitory media),如调制的数据信号和载波。

[66]通过以上的实施方式的描述可知,本领域的技术人员可以清楚地了解到本说明书实施例可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解,本说明书实施例的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品可以存储在存储介质中,如ROM/RAM、磁碟、光盘等,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行本说明书实施例各个实施例或者实施例的某些部分所述的方法。

[67]上述实施例阐明的系统、装置、模块或单元,具体可以由计算机芯片或实体实现,或者由具有某种功能的产品来实现。一种典型的实现设备为计算机,计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

[68]本说明书中的各个实施例均采用递进的方式描述,各个实施例之间相同相似的部分互相参见即可,每个实施例重点说明的都是与其他实施例的不同之处。尤其,对于装置实施例而言,由于其基本相似于方法实施例,所以描述得比较简单,相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的,其中所述作为分离部件说明的模块可以是或者也可以不是物理上分开的,在实施本说明书实施例方案时可以把各模块的功能在同一个或多个软件和/或硬件中实现。也可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性劳动的情况下,即可以理解并实施。

[69]以上所述仅是本说明书实施例的具体实施方式,应当指出,对于本技术领域的普通技术人员来说,在不脱离本说明书实施例原理的前提下,还可以做出若干改进和润饰,这些改进和润饰也应视为本说明书实施例的保护范围。

权利要求书

1、一种基于区块链的用户要素认证方法，应用于区块链中的节点设备；其中，所述区块链中部署有用于管理用户要素认证流程的智能合约；所述方法包括：

接收智能合约调用交易；其中，所述智能合约调用交易中携带有来自用户客户端的已加密的用于确认用户身份真实性的待认证用户要素；

响应于所述智能合约调用交易，调用所述智能合约中的加密转换逻辑，在所述节点设备搭载的可信计算环境中，对所述已加密待认证用户要素进行解密，并进一步对解密后的待认证用户要素进行二次加密处理，其中，所述二次加密处理对应的解密密钥由用户要素认证机构维护，以使所述用户要素认证机构获取二次加密处理后的待认证用户要素，基于所述解密密钥对所述待认证用户要素进行解密，并基于解密后的所述待认证用户要素进行用户要素认证；

获取所述用户要素认证机构提交至所述智能合约的针对所述待认证用户要素的认证结果，并在所述区块链的分布式账本中存储所述认证结果，以使与所述区块链对接的认证结果使用方从所述区块链的分布式账本中获取所述认证结果，并基于所述认证结果确认所述用户客户端提供的用户身份的真实性。

2、根据权利要求1所述的方法，所述节点设备与服务端对接；

所述智能合约调用交易，包括所述服务端响应于用户客户端发送的用户要素认证请求，基于所述用户要素认证请求中携带的已加密待认证用户要素构建的智能合约调用交易。

3、根据权利要求2所述的方法，所述在所述区块链的分布式账本中存储所述认证结果，以使与所述区块链对接的认证结果使用方从所述区块链的分布式账本中获取所述认证结果，包括：

在所述区块链的分布式账本中存储所述认证结果，生成与所述认证结果对应的结果返回事件，以使所述服务端响应于所述结果返回事件，从所述区块链的分布式账本中获取所述认证结果，并将所述认证结果发送至与所述区块链对接的认证结果使用方。

4、根据权利要求1所述的方法，所述智能合约调用交易中还携带有用户客户端指定的目标用户要素认证机构的标识；

接收所述智能合约调用交易后，所述方法还包括：查询预设的加密密钥表，确定与所述目标用户要素认证机构对应的二次加密密钥；所述对解密后的待认证用户要素进行二次加密处理，其中，所述二次加密处理对应的解密密钥由用户要素认证机构维护，以使所述用户要素认证机构获取二次加密处理后的待认证用户要素，基于所述解密密钥对

所述待认证用户要素进行解密,并基于解密后的所述待认证用户要素进行用户要素认证,包括:

基于确定出的二次加密密钥,对解密后的待认证用户要素进行二次加密处理,其中,所述二次加密处理对应的解密密钥由所述目标用户要素认证机构维护,以使所述目标用户要素认证机构获取二次加密处理后的待认证用户要素,基于所述解密密钥对所述待认证用户要素进行解密,并基于解密后的所述待认证用户要素进行用户要素认证。

5、根据权利要求1所述的方法,所述待认证用户要素包括用户的身份信息。

6、根据权利要求5所述的方法,

所述用户的身份信息,包括用户的姓名、身份证号码以及手机号码;所述用户要素认证机构包括手机运营商。

7、一种基于区块链的用户要素认证装置,应用于区块链中的节点设备;其中,所述区块链中部署有用于管理用户要素认证流程的智能合约;所述装置包括:

接收模块,接收智能合约调用交易;其中,所述智能合约调用交易中携带有来自用户客户端的已加密的用于确认用户身份真实性的待认证用户要素;

认证模块,响应于所述智能合约调用交易,调用所述智能合约中的加密转换逻辑,在所述节点设备搭载的可信计算环境中,对所述已加密待认证用户要素进行解密,并进一步对解密后的待认证用户要素进行二次加密处理,其中,所述二次加密处理对应的解密密钥由用户要素认证机构维护,以使所述用户要素认证机构获取二次加密处理后的待认证用户要素,基于所述解密密钥对所述待认证用户要素进行解密,并基于解密后的所述待认证用户要素进行用户要素认证;

存储模块,获取所述用户要素认证机构提交至所述智能合约的针对所述待认证用户要素的认证结果,并在所述区块链的分布式账本中存储所述认证结果,以使与所述区块链对接的认证结果使用方从所述区块链的分布式账本中获取所述认证结果,并基于所述认证结果确认所述用户客户端提供的用户身份的真实性。

8、根据权利要求7所述的装置,所述节点设备与服务端对接;

所述智能合约调用交易,包括所述服务端响应于用户客户端发送的用户要素认证请求,基于所述用户要素认证请求中携带的已加密待认证用户要素构建的智能合约调用交易。

9、根据权利要求8所述的装置,所述存储模块进一步:

在所述区块链的分布式账本中存储所述认证结果,生成与所述认证结果对应的结果返回事件,以使所述服务端响应于所述结果返回事件,从所述区块链的分布式账本中获

取所述认证结果，并将所述认证结果发送至与所述区块链对接的认证结果使用方。

10、根据权利要求 7 所述的装置，所述智能合约调用交易中还携带有用户客户端指定的目标用户要素认证机构的标识；

所述装置还包括：查询模块，查询预设的加密密钥表，确定与所述目标用户要素认证机构对应的二次加密密钥；

所述认证模块进一步：

基于确定出的二次加密密钥，对解密后的待认证用户要素进行二次加密处理，其中，所述二次加密处理对应的解密密钥由所述目标用户要素认证机构维护，以使所述目标用户要素认证机构获取二次加密处理后的待认证用户要素，基于所述解密密钥对所述待认证用户要素进行解密，并基于解密后的所述待认证用户要素进行用户要素认证。

11、根据权利要求 7 所述的装置，所述待认证用户要素包括用户的身份信息。

12、根据权利要求 11 所述的装置，

所述用户的身份信息，包括用户的姓名、身份证号码以及手机号码；所述用户要素认证机构包括手机运营商。

13、一种计算机设备，其至少包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其中，处理器执行所述程序时实现权利要求 1 至 6 任一所述的方法。