(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 106790253 A
(43)申请公布日 2017.05.31

(21)申请号 201710056607.5

(22)申请日 2017.01.25

(71)申请人 中钞信用卡产业发展有限公司北京智能卡技术研究院
地址 100088 北京市西城区德胜门外大街79号德胜国际中心C座7层

(72)发明人 张一锋

(74)专利代理机构 北京东方亿思知识产权代理有限责任公司 11258
代理人 彭琼

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
G06Q 20/40(2012.01)
G06Q 20/38(2012.01)

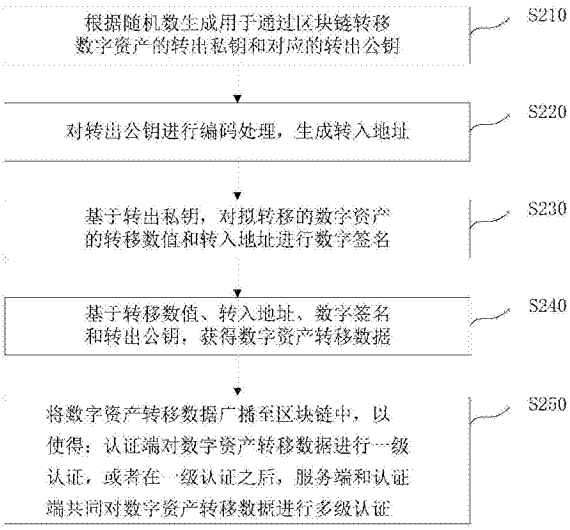
权利要求书3页 说明书9页 附图5页

(54)发明名称

基于区块链的认证方法和装置

(57)摘要

本发明公开了一种基于区块链的认证方法和装置。该方法包括：根据随机数生成用于通过区块链转移数字资产的转出私钥和对应的转出公钥；对转出公钥进行编码处理，生成转入地址；基于转出私钥，对拟转移的数字资产的转移数值和转入地址进行数字签名；基于转移数值、转入地址、数字签名和转出公钥，获得数字资产转移数据；将数字资产转移数据广播至区块链中，以使得：认证端对所述数字资产转移数据进行一级认证，或者在所述一级认证之后，所述服务端和认证端共同对所述数字资产转移数据进行多级认证。由此，本实施例可以提高黑客攻击的能力，可以满足在区块链开放环境下数据和交易的安全需求。



CN 106790253 A

1.一种基于区块链的认证方法，应用于终端侧，其特征在于，该方法包括：

根据随机数生成用于通过区块链转移数字资产的转出私钥和对应的转出公钥；

对所述转出公钥进行编码处理，生成转入地址；

基于所述转出私钥，对拟转移的数字资产的转移数值和所述转入地址进行数字签名；

基于所述转移数值、所述转入地址、所述数字签名和所述转出公钥，获得数字资产转移数据；

将所述数字资产转移数据广播至所述区块链中，以使得：

认证端对所述数字资产转移数据进行一级认证，或者

在所述一级认证之后，所述服务端和认证端共同对所述数字资产转移数据进行多级认证。

2.根据权利要求1所述的方法，其特征在于，还包括：

接收来自所述认证端的加密数据，所述加密数据是所述认证端利用所述转出公钥对随机数种子进行加密所生成的；

利用所述转出私钥对所接收的加密数据进行解密，获取所述随机数种子。

3.根据权利要求2所述的方法，其特征在于，还包括：

接收来自所述认证端的当前时间参数和第一动态口令OTP值，所述第一OTP值是对所述随机数种子和所述当前时间参数进行哈希运算得到的。

4.根据权利要求3所述的方法，其特征在于，还包括：

对所述随机数种子和所述当前时间参数进行哈希运算得到的第二OTP值；

验证所述第一OTP值和所述第二OTP值是否相等；

当验证结果指示相等时，所述数字资产转移数据通过所述多级认证。

5.根据权利要求1-4中任意一项所述的方法，其特征在于，所述生成转入地址包括：

对所述转出公钥通过哈希运算得到公钥哈希值；

为所述公钥哈希值设置首部版本数据；

为所述公钥哈希值设置尾部校验数据；

对设置了所述首部版本数据和所述尾部校验数据的公钥哈希值进行编码处理，生成所述转入地址。

6.根据权利要求5所述的方法，其特征在于，为所述公钥哈希值设置尾部校验数据包括：

对设置了所述首部版本数据的公钥哈希值进行预设次数的哈希运算；

提取运算的结果中的指定部分数据，生成所述尾部校验数据。

7.根据权利要求6所述的方法，其特征在于，所述预设次数为2次，所述多级为2级。

8.根据权利要求1-4中任一项所述的方法，其特征在于，生成所述对应的转出公钥包括：

基于所述转出私钥，通过椭圆曲线加密算法ECC、RSA加密算法、Elgamal加密算法、D-H加密算法、国密SM2算法中至少一种非对称加密算法生成所述对应的转出公钥。

9.一种基于区块链的认证方法，应用于认证端侧，其特征在于，该方法包括：

接收终端广播在区块链中的数字资产转移数据；

对所接收的数字资产转移数据进行一级认证，或者

在所述一级认证之后，与所述终端共同对所述数字资产转移数据进行多级认证；所述数字资产转移数据包括：拟转移的数字资产的转移数值、转入地址、数字签名、用于通过区块链转移数字资产的转出公钥。

10.根据权利要求9所述的方法，其特征在于，对所接收的数字资产转移数据进行一级认证包括：对所接收的数字资产转移数据进行合法性验证。

11.根据权利要求10所述的方法，其特征在于，与所述终端共同对所述数字资产转移数据进行多级认证包括：

生成随机数种子；

基于所述转出公钥，对所述随机数种子进行加密并生成加密数据；

将所述加密数据发送给所述终端侧，以供所述终端对所述加密数据进行解密，并获取所述随机数种子；

对所述随机数种子和当前时间参数进行哈希运算得到第一OTP值；

将所述第一OTP值发送给所述终端，以供所述终端：

对所述随机数种子和所述当前时间参数进行哈希运算得到的第二OTP值，验证所述第一OTP值和所述第二OTP值是否相等，当验证结果指示相等时，通过所述多级认证。

12.一种基于区块链的认证装置，应用于终端侧，其特征在于，该装置包括：

密钥生成单元，用于根据随机数生成用于通过区块链转移数字资产的转出私钥和对应的转出公钥；

地址生成单元，用于对所述转出公钥进行编码处理，生成转入地址；

数字签名单元，用于基于所述转出私钥，对拟转移的数字资产的转移数值和所述转入地址进行数字签名；

数据生成单元，用于基于所述转移数值、所述转入地址、所述数字签名和所述转出公钥，获得数字资产转移数据；

数据广播单元，用于将所述数字资产转移数据广播至所述区块链中，以使得：

认证端对所述数字资产转移数据进行一级认证，或者

在所述一级认证之后，所述服务端和认证端共同对所述数字资产转移数据进行多级认证。

13.根据权利要求12所述的装置，其特征在于，还包括：

数据接收单元，用于接收来自所述认证端的加密数据，所述加密数据是所述认证端利用所述转出公钥对随机数种子进行加密所生成的；

数据解密单元，用于利用所述转出私钥对所接收的加密数据进行解密，获取所述随机数种子。

14.根据权利要求13所述的装置，其特征在于，其中：

所述数据接收单元，还用于接收来自所述认证端的当前时间参数和第一OTP值，所述第一OTP值是对所述随机数种子和所述当前时间参数进行哈希运算得到的。

15.根据权利要求14所述的装置，其特征在于，还包括：

哈希运算单元，用于对所述随机数种子和所述当前时间参数进行哈希运算得到的第二OTP值；

数据验证单元，用于验证所述第一OTP值和所述第二OTP值是否相等，当验证结果指示

相等时，所述数字资产转移数据通过所述多级认证。

16.根据权利要求12-15中任意一项所述的装置，其特征在于，所述地址生成单元包括：

哈希运算模块，用于对所述转出公钥通过哈希运算得到公钥哈希值；

首部设置模块，用于为所述公钥哈希值设置首部版本数据；

尾部设置模块，用于为所述公钥哈希值设置尾部校验数据；

数据编码模块，用于对设置了所述首部版本数据和所述尾部校验数据的公钥哈希值进行编码处理，生成所述转入地址。

17.根据权利要求16所述的装置，其特征在于，所述尾部设置模块包括：

哈希运算元件，用于对设置了所述首部版本数据的公钥哈希值进行预设次数的哈希运算；

数据提取元件，用于提取运算的结果中的指定部分数据，生成所述尾部校验数据。

18.根据权利要求6所述的装置，其特征在于，所述预设次数为2次，所述多级为2级。

19.根据权利要求12-15中任一项所述的装置，其特征在于，所述密钥生成单元还用于：基于所述转出私钥，通过椭圆曲线加密算法ECC、RSA加密算法、Elgamal加密算法、D-H加密算法、国密SM2算法中至少一种非对称加密算法生成所述对应的转出公钥。

20.一种基于区块链的认证装置，应用于认证端侧，其特征在于，该装置包括：

数据接收单元，用于接收终端广播在区块链中的数字资产转移数据；

数据认证单元，用于对所接收的数字资产转移数据进行一级认证，或者

在所述一级认证之后，与所述终端共同对所述数字资产转移数据进行多级认证：所述数字资产转移数据包括：拟转移的数字资产的转移数值、转入地址、数字签名、用于通过区块链转移数字资产的转出公钥。

21.根据权利要求20所述的装置，其特征在于，所述数据认证单元包括：一级认证模块，所述一级认证模块用于：对所接收的数字资产转移数据进行合法性验证。

22.根据权利要求21所述的装置，其特征在于，所述数据认证单元包括：多级认证模块，所述多级认证模块包括：

种子生产元件，用于生成随机数种子；

数据加密元件，用于基于所述转出公钥，对所述随机数种子进行加密并生成加密数据；

数据发送元件，用于将所述加密数据发送给所述终端侧，以供所述终端对所述加密数据进行解密，并获取所述随机数种子；

哈希运算元件，用于对所述随机数种子和当前时间参数进行哈希运算得到第一OTP值；

数值发送元件，用于将所述第一OTP值发送给所述终端，以供所述终端：对所述随机数种子和所述当前时间参数进行哈希运算得到的第二OTP值，验证所述第一OTP值和所述第二OTP值是否相等，当验证结果指示相等时，通过所述多级认证。

基于区块链的认证方法和装置

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及一种基于区块链的认证方法和装置。

背景技术

[0002] 传统的数字资产交互(例如电子货币交易)通常由中心化的机构来完成。中心化的机构主要涉及到第三方交易支付平台、银行的账户管理系统、远程支付系统、转接清算系统等。传统的数字资产交互方式存在操作繁琐，数据不透明，容易篡改等问题。

[0003] 随着通信技术的发展，区块链由于去中心化、公开、透明、无法篡改等优点而逐渐被应用于各种数据处理的应用场景中。区块链可以看作分布式统一账本，由所有参与方共同决定记账内容，每个参与方都保存有全量数据，任何个体参与方无法对数据进行篡改。根据不同的交互场景，基于区块链的数字资产转移可能涉及个人、商户、第三方、银行等多个参与方。

[0004] 目前，数字资产交互的数据(例如转账地址和用于转账的私钥)都保存在交易文件中，而交易文件通常采用软件加密或云加密的方式保存。软件加密或者云端加密都存在以下数据转移过程不安全、交互环境不安全，容易出现私钥丢失、遗忘、暴力破解等问题。一旦出现问题，该私钥对应的区块链上的账号所持有的数字资产，如数字货币、数字化实物资产等资产，就会出现无法证明所有权的问题，进而造成数字资产流失。

[0005] 如何基于区块链进行安全、可靠地转移数字资产，成为业界需要解决的问题。

发明内容

[0006] 鉴于以上所述一个或多个问题，本发明实施例提供了一种基于区块链的认证方法和装置。

[0007] 第一方面，提供了一种基于区块链的认证方法。该方法包括：

[0008] 根据随机数生成用于通过区块链转移数字资产的转出私钥和对应的转出公钥；

[0009] 对转出公钥进行编码处理，生成转入地址；

[0010] 基于转出私钥，对拟转移的数字资产的转移数值和转入地址以及其他必要信息进行数字签名；

[0011] 基于转移数值、转入地址、数字签名和转出公钥，获得数字资产转移数据；

[0012] 将数字资产转移数据广播至区块链中，以使得：

[0013] 认证端对所述数字资产转移数据进行一级认证，或者

[0014] 在所述一级认证之后，所述服务端和认证端共同对所述数字资产转移数据进行多级认证。

[0015] 第二方面，提供了一种基于区块链的认证方法。该方法包括：

[0016] 接收终端广播在区块链中的数字资产转移数据；

[0017] 对所接收的数字资产转移数据进行一级认证，或者

[0018] 在所述一级认证之后，与所述终端共同对所述数字资产转移数据进行多级认证；

所述数字资产转移数据包括：拟转移的数字资产的转移数值、转入地址、数字签名、用于通过区块链转移数字资产的转出公钥。

[0019] 第三方面，提供了一种基于区块链的认证装置。该装置包括：

[0020] 密钥生成单元，用于根据随机数生成用于通过区块链转移数字资产的转出私钥和对应的转出公钥；

[0021] 地址生成单元，用于对转出公钥进行编码处理，生成转入地址；

[0022] 数字签名单元，用于基于转出私钥，对拟转移的数字资产的转移数值和转入地址进行数字签名；

[0023] 数据生成单元，用于基于转移数值、转入地址、数字签名和转出公钥，获得数字资产转移数据；

[0024] 数据广播单元，用于将数字资产转移数据广播至区块链中，以使得：

[0025] 认证端对所述数字资产转移数据进行一级认证，或者

[0026] 在所述一级认证之后，所述服务端和认证端共同对所述数字资产转移数据进行多级认证。

[0027] 第四方面，提供了一种基于区块链的认证装置。该装置包括：

[0028] 数据接收单元，用于接收终端广播在区块链中的数字资产转移数据；

[0029] 数据认证单元，用于对所接收的数字资产转移数据进行一级认证，或者

[0030] 在所述一级认证之后，与所述终端共同对所述数字资产转移数据进行多级认证：所述数字资产转移数据包括：拟转移的数字资产的转移数值、转入地址、数字签名、用于通过区块链转移数字资产的转出公钥。

[0031] 第一方面，本实施例在需要转移数字资产时，通过对随机数进行系列处理生成密钥和转入地址，从而解决了现有密钥和转入地址丢失、遗忘或者暴力破解等问题，可以提高黑客攻击的能力。

[0032] 第二方面，本实施例通过一级或者多级认证，提高了认证的准确性，可以满足在区块链开放环境下数据和交易的安全需求。

[0033] 第三方面，本实施例通过区块链转移数字资产可以快速处理数据、使得数据公开、透明、无法篡改。

附图说明

[0034] 为了更清楚地说明本发明实施例的技术方案，下面将对本发明实施例中所需要使用的附图作简单地介绍，显而易见地，下面所描述的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0035] 图1(a)是本发明一实施例的基于区块链的认证系统架构示意图。

[0036] 图1(b)是本发明一实施例的区块链节点结构示意图。

[0037] 图2是本发明一实施例的基于区块链的认证方法流程示意图。

[0038] 图3是本发明一实施例的获得数字资产转移数据的流程示意图。

[0039] 图4是本发明另一实施例的基于区块链的认证方法流程示意图。

[0040] 图5是本发明又一实施例的基于区块链的认证方法流程示意图。

[0041] 图6是本发明一实施例的基于区块链的认证装置的结构示意图。

[0042] 图7是本发明另一实施例的基于区块链的认证装置的结构示意图。

具体实施方式

[0043] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0044] 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。下面将参考附图并结合实施例来详细说明本申请。

[0045] 图1(a)是本发明一实施例的基于区块链的认证系统架构示意图。

[0046] 如图1(a)所示，该系统架构可以包括：区块链100、网络200、区块链节点110、120、130、140、150和160。区块链100可以看作分布式统一账本，由所有参与方(区块链节点110-160)共同决定记账内容。每个参与方都保存有全量数据，任何个体参与方无法对数据进行篡改。根据不同的交互场景，区块链节点可以是终端节点、认证服务器节点、商户节点、第三方节点和银行节点等。各个节点可以是各种电子设备。这些电子设备包括但不限于个人电脑、智能手机、平板电脑、个人数字助理、服务器等。这些电子设备可以安装有各种通讯客户端应用，例如即时通信工具、邮箱客户端、社交平台软件、音频视频软件等。其中，这些电子设备具有存储器和逻辑运算处理器、控制元件等。这些电子设备可以发送数据请求，或者可以接收数据请求，还可以对数据进行分析、验证和存储等处理。

[0047] 网络200用以在区块链节点110-160之间提供通信链路的介质。具体的，网络可以包括各种连接类型，例如有线、无线通信链路或者光纤电缆等。

[0048] 可以理解图1(a)中的区块链100、网络200和区块链节点110-160的数量是示意性的，可以根据实际需要进行灵活配置。

[0049] 图1(b)是本发明一实施例的区块链节点结构示意图。

[0050] 如图1(b)区块链节点110可以是终端，例如安卓系统的智能手机。该终端可以包括：数字货币客户端、时钟clock、安全芯片SE、Javacard API接口、Javacard运行环境、Javacard虚拟机、底层OS。可以理解，区块链节点120-160也可以是上述的智能手机，还可以是用于认证数据的服务器。时钟clock可以提供当前时间参数。安全芯片SE可以存储有程序，用于执行认证的各步骤的操作。

[0051] 在本实施例中，终端可以对待转移的数字资产进行加密，以确保数字资产可以安全、可靠地从一个区块链节点转移至另一个区块链节点，或者从区块链之外的一个转出端通过区块链转至区块链之外的转入端。其中，加密技术可以依托成熟Javacard框架，通过加密算法类JAVACard API组成加密算法结构框架。该框架可以包括各种密钥、各种签名算法、各种加密算法等。基于硬件SE的数字货币身份认证Applet可以使用这些加密算法类建立与Applet有关的安全逻辑，提高Applet运行时的安全级别。同时也可以使用这些加密算法类为SE外部应用提供加解密服务，以体现SE在整个系统中作为安全保障的这一特征。Javacard技术有成熟的国际标准，并通过国际检测认证取得资质。Javacard规范(包括JCVM、JCRE、JCAPI规范)和GlobalPlatform规范中的安全域管理、逻辑通道和防火墙机制安

全机制，能有效抵御非法代码攻击，保证Applet中的敏感数据不被暴露。

[0052] 下面各实施例均可以应用图1(a)、图1(b)所示系统架构来进行数据认证。为了描述简洁，各个实施例可以相互参考引用。

[0053] 图2是本发明一实施例的基于区块链的认证方法流程示意图。

[0054] 如图2所示，该方法包括以下步骤：S210，根据随机数生成用于通过区块链转移数字资产的转出私钥和对应的转出公钥；S220，对转出公钥进行编码处理，生成转入地址；S230，基于转出私钥，对拟转移的数字资产的转移数值、转入地址和其他必要数据进行数字签名；S240，基于转移数值、转入地址、数字签名和转出公钥，获得数字资产转移数据；S250，将数字资产转移数据广播至区块链中，以使得：认证端对所述数字资产转移数据进行一级认证，或者在所述一级认证之后，所述服务端和认证端共同对所述数字资产转移数据进行多级认证。

[0055] 本实施例可以应用于终端侧，终端可以作为本实施例的动作执行主体，具体执行各个步骤操作。终端的安全芯片SE可以存储有数字货币身份认证Applet应用程序，该程序可以实现如下功能：初始化公钥、生成转入地址、签名、验证等功能。

[0056] 在步骤S210中，安全芯片SE可以使用随机数发生器生成私钥Sk。将私钥Sk经过非对称加密算法处理可以得到公钥Pk。

[0057] 生成对应的转出公钥可以包括：基于所述转出私钥，通过椭圆曲线加密算法ECC、RSA加密算法、Elgamal加密算法、D-H加密算法、国密SM2算法中至少一种非对称加密算法生成所述对应的转出公钥。

[0058] 在步骤S220中，编码处理可以是使用上述加密算法进行编码处理。转入地址可以是待转入的钱包地址。

[0059] 在步骤S230中，数字签名可以是利用私钥Sk对原始数据进行签名。交易(或者转移)的原始数据可以包括：转账数额和转入钱包地址。

[0060] 在步骤S240中，数字资产转移数据可以包括：转移数值、转入地址、数字签名和转出公钥。本实施例可以将转出签名和转出公钥添加到原始数据中生成优化的交易数据。优化的交易数据可以包括：转账数额、转入钱包地址、转出签名和转出公钥。

[0061] 在步骤S250中，终端可以通过区块链将数字资产转移数据发送到用于认证数据的认证端(即认证服务器)。

[0062] 第一方面，本实施例在需要转移数字资产时，通过对随机数进行系列处理生成密钥和转入地址，从而解决了现有密钥和转入地址丢失、遗忘或者暴力破解等问题，可以提高黑客攻击的能力。

[0063] 第二方面，本实施例通过一级或者多级认证，提高了认证的准确性，可以满足在区块链开放环境下数据和交易的安全需求。

[0064] 第三方面，本实施例通过区块链转移数字资产可以快速处理数据、使得数据公开、透明、无法篡改。

[0065] 作为图1所示实施例的第一变形实施例，在图2所示实施例的基础上增加以下步骤：S260，接收来自认证端的加密数据，加密数据是认证端利用转出公钥对随机数种子进行加密所生成的；S270，利用转出私钥对所接收的加密数据进行解密，获取随机数种子。本实施例可以应用于转账数额较小(例如转账上限为999元)的场景。在本实施例中仅需认证端

的服务器进行一级认证即可。

[0066] 在本实施例中，公钥Pk经数字货币APP通过区块链发送到认证服务器，认证服务器生成随机数种子Seed并使用Pk加密E(seed,PK)，并通过区块链返回到数字货币APP，安全芯片SE数字货币applet用私钥Sk解密E(seed,PK)并保存随机数种子seed。

[0067] 作为图1所示实施例的第二变形实施例，可以在第一变形实施例的基础上增加以下步骤：S280，接收来自认证端的当前时间参数和第一OTP(One-time Password，动态口令)值，第一OTP值是对随机数种子和当前时间参数进行哈希运算得到的。

[0068] 作为图1所示实施例的第三变形实施例，可以在第二变形实施例的基础上增加以下步骤：S2100，对随机数种子和当前时间参数进行哈希运算得到的第二OTP值；S2110，验证第一OTP值和第二OTP值是否相等；S2120，当验证结果指示相等时，数字资产转移数据通过多级认证。本实施例可以是2级认证，即认证端进行第一次认证，然后客户端进行第二次认证。本实施例可以应用于当转账数额较大(例如，大于1000元)时，引入提供额外身份认证的手段。在这种情况下，由接收方数字货币APP向认证服务器发起大额交易认证申请，认证服务器对初始随机数种子seed和当前时间time进行Hash计算，生成OTP值，返回给数字货币APP。数字货币APP将收到的OTP值和当前时间一起返回给安全芯片SE身份认证Applet，Applet使用自己保存的初始随机数种子seed和当前时间一起计算得到OTP'，当得到OTP＝OTP'一致结果时，通过验证，对交易数据进行数字签名，并通过区块链返回交易发起方，从而完成交易。

[0069] 本实施例通过端生成OTP数值，由客户端(SE)进行认证的大额支付方案，增强了客户端的认证权利，比客户端生成OTP数值，由服务器认证更加科学合理。

[0070] 在一些实施例中，对转出公钥进行编码处理，生成转入地址(即，S220)可以包括以下步骤：S221，对转出公钥通过哈希运算得到公钥哈希值；S222，为公钥哈希值设置首部版本数据；S223，为公钥哈希值设置尾部校验数据；S224，对设置了首部版本数据和尾部校验数据的公钥哈希值进行编码处理，生成转入地址。

[0071] 在一些实施例中，为公钥哈希值设置尾部校验数据(即，S223)的步骤可以包括：S2231，对设置了首部版本数据的公钥哈希值进行预设次数的哈希运算；S2232，提取运算的结果中的指定部分数据，生成尾部校验数据。

[0072] 在一些实施例中，预设次数为2次，多级为2级。

[0073] 例如，首先使用随机数发生器生成“私钥”，“私钥”经过ECC算法处理成“公钥”。通过已知的“私钥”可以算出“公钥”，而“公钥”已知时无法反向推出“私钥”。公钥通过哈希算法得到“公钥哈希”，但通过“公钥哈希”不能得到“公钥”，将一个字节的地址版本号链接到“公钥哈希”头部，对其进行两次哈希运算，将结果的前4字节作为公钥哈希的校验值，连接在其尾部。将这一结果使用加密算法进行编码，就得到了“钱包地址”。

[0074] 上述实施例可以通过硬件SE中加载的数字货币身份认证Applet进行区块链(数字货币交易)上交易签名，提高了交易的安全性和可靠性。

[0075] 图3是本发明一实施例的获得数字资产转移数据的流程示意图。

[0076] 如图3所示，获得数字资产转移数据可以包括：S310，根据随机数RADOM生成转出私钥Sk；S320，对转出私钥Sk进行加密算法处理；S330，生成转出公钥Pk；S340，设置原始数据：转账数额和转入地址；S350，对转出私钥Sk与原始数据进行数字签名；S360，生成转出签名；

S370，将转出签名和转出公钥Pk添加到原始数据中生成了优化的交易数据，优化的交易数据包括：转账数额、转入地址、转出签名和转出公钥Pk。

[0077] 图4是本发明另一实施例的基于区块链的认证方法流程示意图。

[0078] 如图4所示，该方法包括以下步骤：S410，接收终端广播在区块链中的数字资产转移数据；S420，在一级认证之后，与终端共同对数字资产转移数据进行多级认证；数字资产转移数据包括：拟转移的数字资产的转移数值、转入地址、数字签名、用于通过区块链转移数字资产的转出公钥。

[0079] 在一些实施例中，对所接收的数字资产转移数据进行一级认证包括：对所接收的数字资产转移数据进行合法性验证。例如，接收方数字货币身份认证Applet收到交易数据后通过转算法对交易数据进行解密得到原始交易数据，当转账数额小于1000元(即上限为999元)时，对数据进行检验，其中包括对数字签名、交易数据是否大于零等进行的检验，如果校验正确，数字货币就成功的从“转出钱包”转移到“转入钱包”，完成交易。交易文件中生成唯一序列号，通过区块链全网同步。

[0080] 本实施例可以应用于认证端侧，服务器可以作为本实施例的动作执行主体，具体执行各个步骤操作。本实施例与图2所示实施例构思相同，但从不同的角度(认证端的角度与终端的角度)来描述基于区块链的认证方法。

[0081] 在一些实施例中，与终端共同对数字资产转移数据进行多级认证包括：生成随机数种子；基于转出公钥，对随机数种子进行加密并生成加密数据；将加密数据发送给终端侧，以供终端对加密数据进行解密，并获取随机数种子。

[0082] 对随机数种子和当前时间参数进行哈希运算得到第一OTP值；将第一OTP值发送给终端，以供终端：对随机数种子和当前时间参数进行哈希运算得到的第二OTP值，验证第一OTP值和第二OTP值是否相等，当验证结果指示相等时，通过多级认证。

[0083] 图5是本发明又一实施例的基于区块链的认证方法流程示意图。本实施例是从终端和服务器两侧进行数据交互的角度来描述认证方法的实现方式。

[0084] 如图5所示，该方法包括以下步骤：

[0085] S501，终端根据随机数生成用于通过区块链转移数字资产的转出私钥Sk；

[0086] S502，终端利用非对称加密算法对转出私钥进行一系列运算处理，生成转出公钥Pk，将公钥Pk发送给服务器；

[0087] S503，服务器生成随机数种子Seed，基于转出公钥Pk，对随机数种子进行加密并生成加密数据E(Seed,Pk)，将加密数据发送给终端；

[0088] S504，终端用私钥Sk对加密数据进行解密，并获取并保存随机数种子Seed。终端向服务器发送优化的交易数据；

[0089] S505，服务器判断转账数额是否达到阈值(例如阈值为1000元)；

[0090] S506，当没有达到阈值时，服务器对优化的交易数据进行一级认证；

[0091] S507，当达到阈值时，服务器对随机数种子Seed和当前时间进行哈希运算得到OTP值，将当前时间和OTP值发送给终端；

[0092] S508，终端对随机数种子Seed和当前时间参数进行哈希运算得到的OTP’值；

[0093] S509，终端验证OTP值和OTP’值是否相等；

[0094] S510，当验证结果指示相等时，通过二级认证。

[0095] 在本实施例中，可以终端的安全芯片使用随机数发生器生成私钥Sk，私钥经过ECC算法处理成公钥Pk。公钥Pk经数字货币APP通过区块链发送到认证服务器，认证服务器生成随机数种子Seed并使用Pk加密E(seed，Pk)，并通过区块链返回到数字货币APP，安全芯片SE数字货币applet用私钥Sk解密E(seed，Pk)并保存随机数种子seed。

[0096] 发起交易时，交易数据由转出钱包私钥Sk'生成。交易的原始数据包括“转账数额”和“转入钱包地址”，然后用私钥Sk'对原始数据签名。转出私钥通过ECC算法处理后，得到转出公钥Pk'。转出签名和转出公钥添加到原始数据中生成了优化的交易数据，通过区块链发送到接收方节点数字货币APP。

[0097] 接收方数字货币身份认证Applet收到交易数据后通过转算法对交易数据进行解密得到原始交易数据，当转账数额小于1000元(即上限为999元)时，对数据进行检验，其中包括对数字签名的检验，如果校验正确，数字货币就成功的从“转出钱包”转移到“转入钱包”，完成交易。交易文件中生成唯一序列号，通过区块链全网同步。

[0098] 当转账数额大于1000元时，引入提供额外身份认证的手段。在这种情况下，由接收方数字货币APP向认证服务器发起大额交易认证申请，认证服务器对初始随机数种子seed和当前时间time进行Hash计算，生成OTP值(即第一OTP值)，返回给数字货币APP。数字货币APP将收到的OTP值和当前时间一起返回给安全芯片SE身份认证Applet，Applet使用自己保存的初始随机数种子seed和当前时间一起计算得到OTP'(即第二OTP值)，当得到OTP＝OTP'一致结果时，通过验证，完成交易。

[0099] 需要说明的是，在不冲突的情况下，本领域的技术人员可以按实际需要将上述的操作步骤的顺序进行灵活调整，或者将上述步骤进行灵活组合等操作。为了简明，不再赘述各种实现方式。另外，各实施例的内容可以相互参考引用。

[0100] 图6是本发明一实施例的基于区块链的认证装置的结构示意图。本实施例可以应用于终端侧。

[0101] 如图6所示，基于区块链的认证装置600可以包括：密钥生成单元610、地址生成单元620、数字签名单元630、数据生成单元640和数据广播单元650。其中，密钥生成单元610可以用于根据随机数生成用于通过区块链转移数字资产的转出私钥和对应的转出公钥；地址生成单元620可以用于对转出公钥进行编码处理，生成转入地址；数字签名单元630可以用于基于转出私钥，对拟转移的数字资产的转移数值和转入地址进行数字签名；数据生成单元640可以用于基于转移数值、转入地址、数字签名和转出公钥，获得数字资产转移数据；数据广播单元650可以用于将数字资产转移数据广播至区块链中，以使得：认证端对数字资产转移数据进行一级认证，或者在一级认证之后，服务端和认证端共同对数字资产转移数据进行多级认证。可以理解，数字签名单元630还可以对其他必要数据进行数字签名。

[0102] 需要说明的是，本实施例中所示的功能单元或者功能模块的实现方式可以为硬件、软件、固件或者它们的组合。当以硬件方式实现时，其可以例如是电子电路、专用集成电路(ASIC)、适当的固件、插件、功能卡等等。当以软件方式实现时，本发明的元素是被用于执行所需任务的程序或者代码段。程序或者代码段可以存储在机器可读介质中，或者通过载波中携带的数据信号在传输介质或者通信链路上传送。“机器可读介质”可以包括能够存储或传输信息的任何介质。机器可读介质的例子包括电子电路、半导体存储器设备、ROM、闪存、可擦除ROM(EROM)、软盘、CD-ROM、光盘、硬盘、光纤介质、射频(RF)链路，等等。代码段可

以经由诸如因特网、内联网等的计算机网络被下载。

[0103] 作为图6所示实施例的第一变形实施例，可以在图6实施例的基础上增加：数据接收单元和数据解密单元。其中，数据接收单元可以用于接收来自认证端的加密数据，加密数据是认证端利用转出公钥对随机数种子进行加密所生成的；数据解密单元可以用于利用转出私钥对所接收的加密数据进行解密，获取随机数种子。

[0104] 作为图6所示实施例的第二变形实施例，可以在第一变形实施例的基础上增加：数据接收单元。其中，数据接收单元可以还用于接收来自认证端的当前时间参数和第一OTP值，第一OTP值是对随机数种子和当前时间参数进行哈希运算得到的。

[0105] 作为图6所示实施例的第三变形实施例，可以在第三变形实施例的基础上增加：哈希运算单元和数据验证单元。其中，哈希运算单元可以用于对随机数种子和当前时间参数进行哈希运算得到的第二OTP值；数据验证单元可以用于验证第一OTP值和第二OTP值是否相等，当验证结果指示相等时，数字资产转移数据通过多级认证。

[0106] 在一些实施例中，地址生成单元可以包括：哈希运算模块、首部设置模块、尾部设置模块和数据编码模块。其中，哈希运算模块可以用于对转出公钥通过哈希运算得到公钥哈希值；首部设置模块可以用于为公钥哈希值设置首部版本数据；尾部设置模块可以用于为公钥哈希值设置尾部校验数据；数据编码模块可以用于对设置了首部版本数据和尾部校验数据的公钥哈希值进行编码处理，生成转入地址。

[0107] 在一些实施例中，尾部设置模块可以包括：哈希运算元件和数据提取元件。其中，哈希运算元件可以用于对设置了首部版本数据的公钥哈希值进行预设次数的哈希运算；数据提取元件可以用于提取运算的结果中的指定部分数据，生成尾部校验数据。

[0108] 在一些实施例中，预设次数为2次，多级为2级。可以理解，预设次数还可以是3次、4次，多级还可以是3级、4级，由于数量越大运算越复杂，当预设次数为2次，多级为2级时，在满足运算速度的条件下，认证效果最佳。

[0109] 在一些实施例中，密钥生成单元还用于：基于所述转出私钥，通过椭圆曲线加密算法ECC、RSA加密算法、Elgamal加密算法、D-H加密算法、国密SM2算法中至少一种非对称加密算法生成所述对应的转出公钥。

[0110] 在图6所示的各实施例中，基于区块链的认证装置600可以是移动终端。

[0111] 图7是本发明另一实施例的基于区块链的认证装置的结构示意图。本实施例可以应用于认证端侧。

[0112] 如图7所示，基于区块链的认证装置700可以包括：数据接收单元710和数据认证单元720。其中，数据接收单元710可以用于接收终端广播在区块链中的数字资产转移数据；数据认证单元720可以用于对所接收的数字资产转移数据进行一级认证，或者在一级认证之后，与终端共同对数字资产转移数据进行多级认证：数字资产转移数据包括：拟转移的数字资产的转移数值、转入地址、数字签名、用于通过区块链转移数字资产的转出公钥。

[0113] 在一些实施例中，数据认证单元可以包括：一级认证模块。一级认证模块可以用于：对所接收的数字资产转移数据进行合法性验证。

[0114] 多级认证模块可以包括：种子生产元件、数据加密元件、数据发送元件、哈希运算元件和数值发送元件。其中：种子生产元件可以用于生成随机数种子；数据加密元件可以用于基于转出公钥，对随机数种子进行加密并生成加密数据；数据发送元件可以用于将加密

数据发送给终端侧，以供终端对加密数据进行解密，并获取随机数种子；哈希运算元件可以用于对随机数种子和当前时间参数进行哈希运算得到第一OTP值；数值发送元件可以用于将第一OTP值发送给终端，以供终端：对随机数种子和当前时间参数进行哈希运算得到的第二OTP值，验证第一OTP值和第二OTP值是否相等，当验证结果指示相等时，通过多级认证。

[0115] 在图7所示的各实施例中，基于区块链的认证装置600可以是认证服务器。

[0116] 需要说明的是，上述各实施例的装置可作为上述各实施例的用于各实施例的方法中的执行主体，可以实现各个方法中的相应流程，为了简洁，此方面内容不再赘述。

[0117] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到各实施方式可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件。基于这样的理解，上述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计算机可读存储介质中，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)执行各个实施例或者实施例的某些部分所述的方法。

[0118] 最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

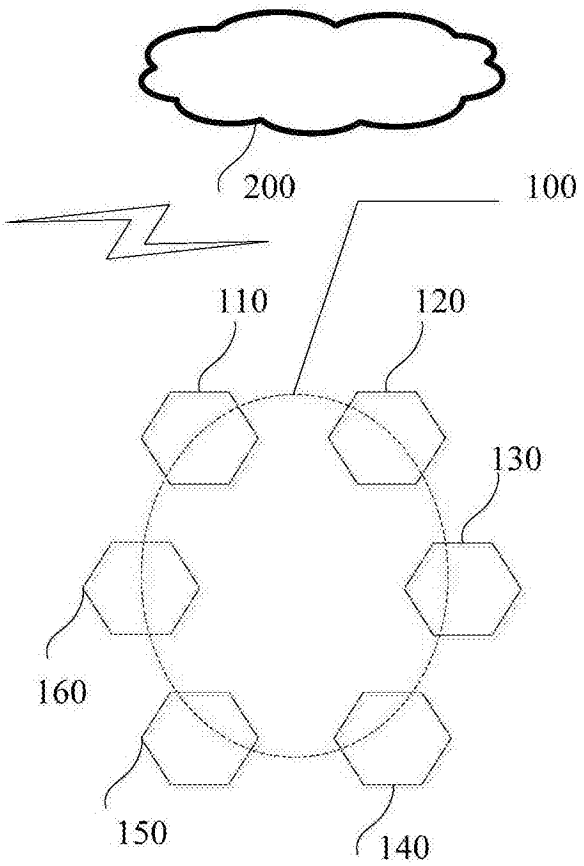

200
100
110
120
130
160
150
140

图1 (a)

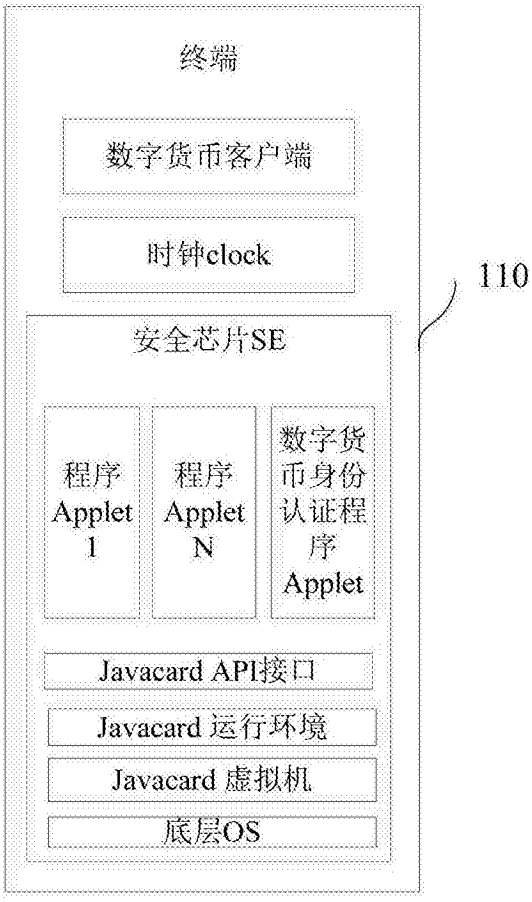

终端
数字货币客户端
时钟clock
110
安全芯片SE
程序 Applet 1
程序 Applet N
数字货币身份认证程序 Applet
Javacard API接口
Javacard 运行环境
Javacard 虚拟机
底层OS

图1 (b)


根据随机数生成用于通过区块链转移数字资产的转出私钥和对应的转出公钥
S210
对转出公钥进行编码处理，生成转入地址
S220
基于转出私钥，对拟转移的数字资产的转移数值和转入地址进行数字签名
S230
基于转移数值、转入地址、数字签名和转出公钥，获得数字资产转移数据
S240
将数字资产转移数据广播至区块链中，以使得：认证端对数字资产转移数据进行一级认证，或者在一级认证之后，服务端和认证端共同对数字资产转移数据进行多级认证
S250

图2

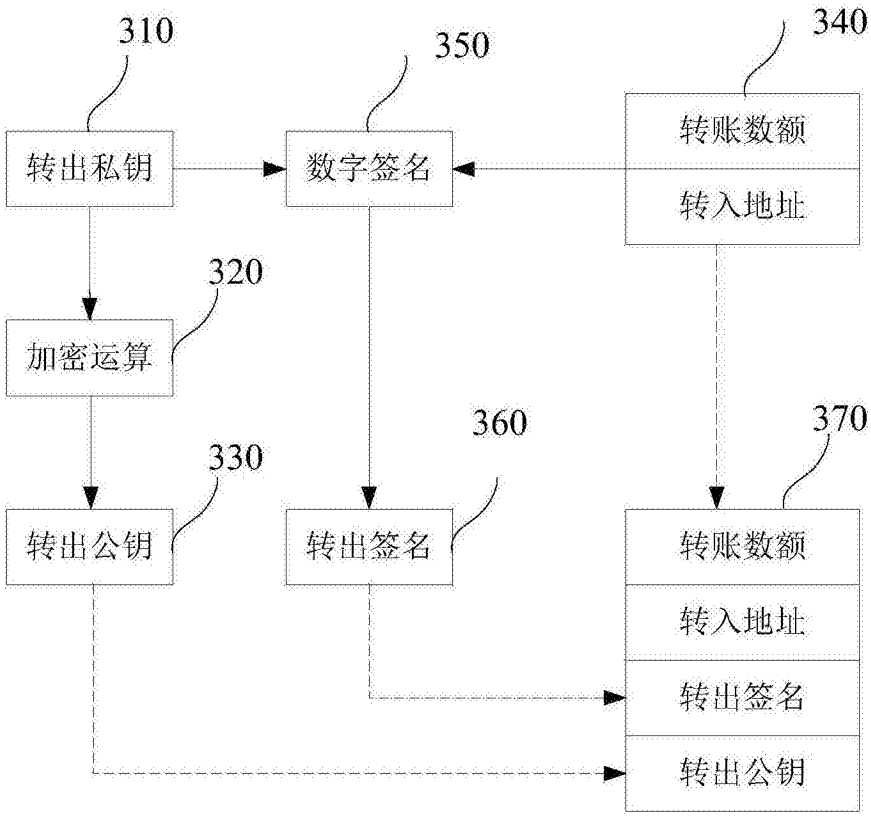

310
350
340
转出私钥
数字签名
转账数额
转入地址
320
加密运算
360
370
330
转出公钥
转出签名
转账数额
转入地址
转出签名
转出公钥

图3

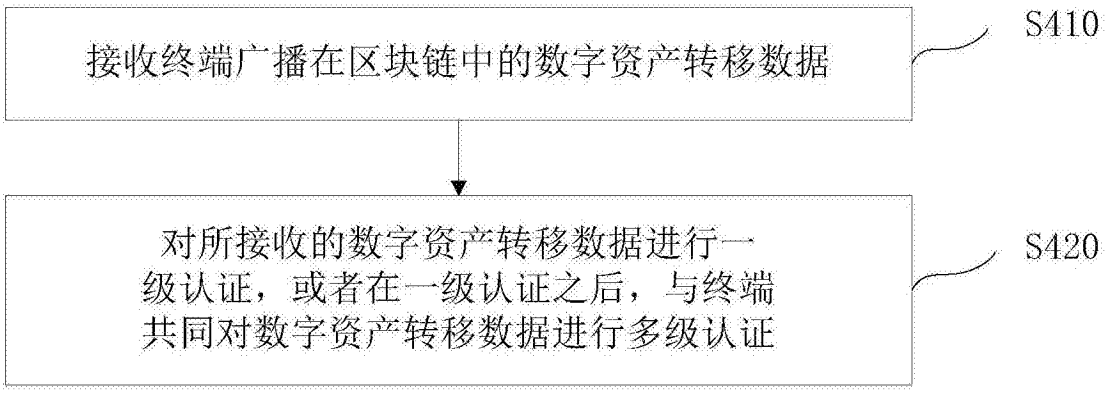

接收终端广播在区块链中的数字资产转移数据
S410
对所接收的数字资产转移数据进行一级认证，或者在一级认证之后，与终端共同对数字资产转移数据进行多级认证
S420

图4

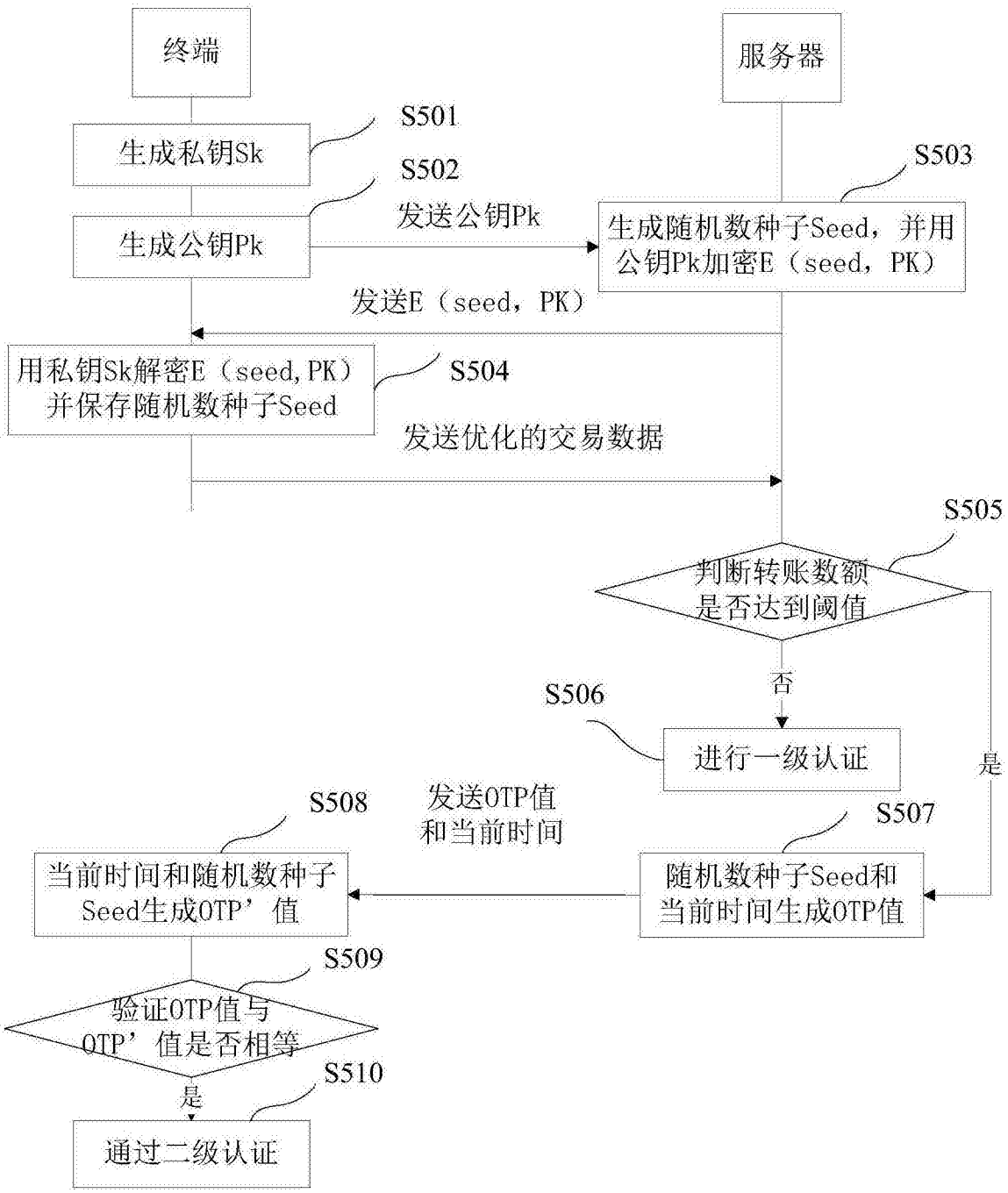

终端
服务器
S501
生成私钥Sk
S502
发送公钥Pk
生成公钥Pk
S503
生成随机数种子Seed，并用公钥Pk加密E（seed，PK）
发送E（seed，PK）
用私钥Sk解密E（seed,PK）并保存随机数种子Seed
S504
发送优化的交易数据
S505
判断转账数额是否达到阈值
否
是
S506
进行一级认证
S507
随机数种子Seed和当前时间生成OTP值
发送OTP值和当前时间
S508
当前时间和随机数种子Seed生成OTP’值
S509
验证OTP值与OTP’值是否相等
是
S510
通过二级认证

图5

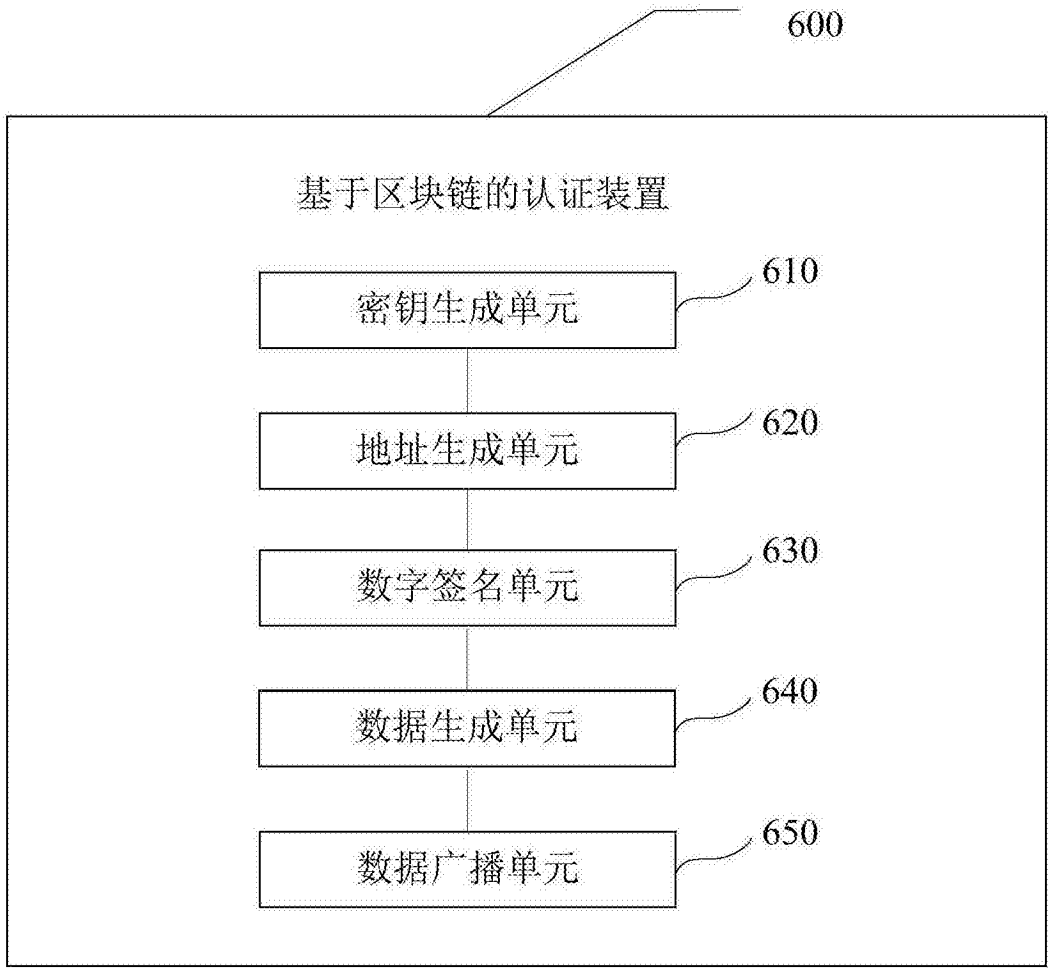

600
基于区块链的认证装置
密钥生成单元
610
地址生成单元
620
数字签名单元
630
数据生成单元
640
数据广播单元
650

图6

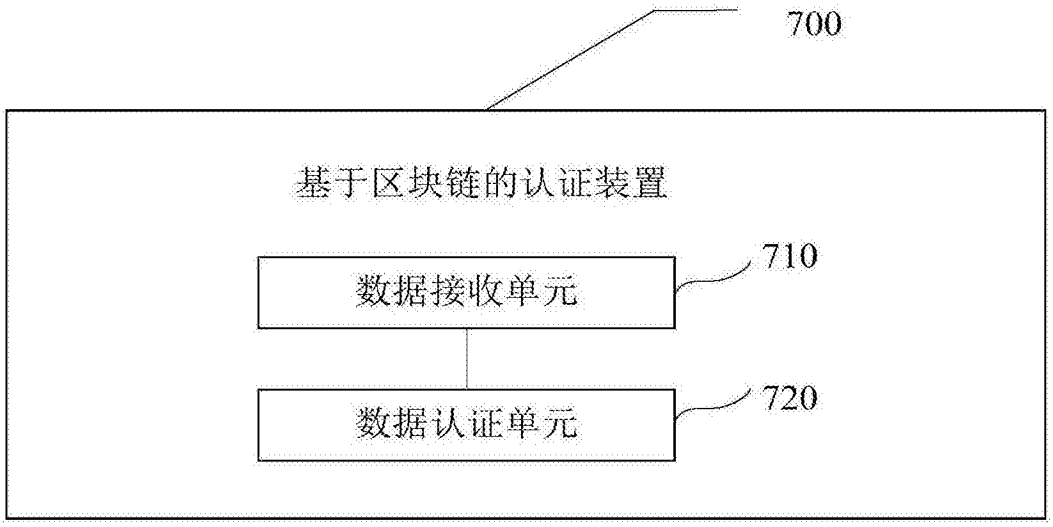

700
基于区块链的认证装置
数据接收单元
710
数据认证单元
720

图7