(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 108564353 A
(43)申请公布日 2018.09.21

(21)申请号 201810390212.3

(22)申请日 2018.04.27

(71)申请人 数字乾元科技有限公司
地址 200082 上海市杨浦区伟德路6号1003-16室

(72)发明人 李杰 张宇 周海京 张哲

(74)专利代理机构 北京超凡志成知识产权代理事务所(普通合伙) 11371
代理人 吴迪

(51)Int.Cl.
G06Q 20/06(2012.01)
G06Q 20/36(2012.01)
G06Q 20/38(2012.01)
G06Q 20/40(2012.01)

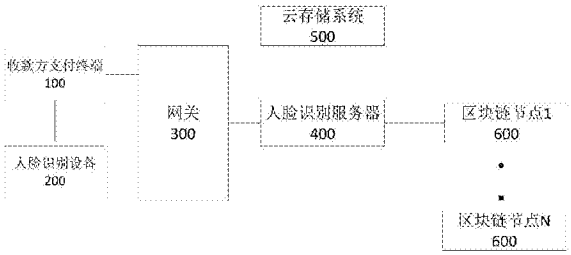
权利要求书2页 说明书9页 附图5页

(54)发明名称

基于区块链的支付系统及方法

(57)摘要

本发明提供一种基于区块链的支付系统及方法，涉及支付技术领域，包括：收款方支付终端、人脸识别服务器、区块链节点和云存储系统，收款方支付终端将交易信息和人脸识别设备发送的人脸数据执行属性加密，通过网关发送第一数据密文给人脸识别服务器，人脸识别服务器解密得到人脸数据和支付方钱包地址，并从云存储系统中获取与支付方钱包地址对应的私钥和预设人脸数据，若人脸数据与预设人脸数据满足预设识别条件，调用私钥对交易进行签名，向系统内广播属性加密后的交易信息，区块链节点解密交易信息并验证，若通过将交易信息记录在区块链中。本发明的基于区块链的支付系统，引入刷脸支付，对交易信息进行加密，可满足多样化支付需求和安全性需求。



CN 108564353 A

1.一种基于区块链的支付系统，其特征在于，包括：收款方支付终端、人脸识别设备、网关、人脸识别服务器、区块链节点和云存储系统；

所述收款方支付终端，用于将交易信息和所述人脸识别设备采集的人脸数据执行属性加密，将加密得到的第一数据密文通过所述网关发送给所述人脸识别服务器；

所述人脸识别服务器，用于根据与自身对应的预设属性密码私钥进行解密，从解密得到的第一数据明文中获取人脸数据和交易信息中的支付方钱包地址，并从所述云存储系统中获取与所述支付方钱包地址对应的私钥和预设人脸数据；以及，若所述人脸数据与预设人脸数据满足预设识别条件，调用所述私钥对交易信息进行签名，执行属性加密后向系统内广播加密且签名的交易信息；

所述区块链节点，用于根据与自身对应的预设属性密码私钥解密加密且签名的交易信息，并对解密得到的交易信息进行验证，若验证通过，将验证通过的交易信息记录在区块链网络中。

2.根据权利要求1所述的系统，其特征在于，还包括：支付方支付终端、中央数字货币系统和CA系统；

所述支付方支付终端，用于根据支付用户的用户信息生成公私钥对和支付方钱包地址，从与自身对应的人脸识别设备接收预设人脸数据，并将支付方钱包地址，以及经过属性加密的私钥和预设人脸数据通过所述网关发送给云存储系统；

所述中央数字货币系统，用于根据所述支付方支付终端发送的含有支付方钱包地址的注册请求生成与所述支付方钱包地址对应的数字货币账户；

所述CA系统，还用于根据所述支付终端发送的支付方钱包地址生成身份数字证书，将与支付方钱包地址相关联的身份数字证书通过所述网关传输至所述支付方支付终端，并将所述身份数字证书加入到区块链网络中；以及，向所述人脸识别服务器和所述区块链节点分发各自对应的预设属性密码私钥。

3.一种基于区块链的支付方法，应用于人脸识别服务器，其特征在于，包括：

根据与自身对应的预设属性密码私钥解密从网关接收的第一数据密文；

从解密得到的第一数据明文中获取人脸数据和交易信息中的支付方钱包地址；

从云存储系统中获取与所述支付方钱包地址对应的私钥和预设人脸数据；

若所述人脸数据与预设人脸数据满足预设识别条件，调用所述私钥对交易信息进行签名，执行属性加密后向系统内广播加密且签名的交易信息。

4.根据权利要求3所述的方法，其特征在于，从云存储系统中获取与所述支付方钱包地址对应的私钥和预设人脸数据，包括：

向所述云存储系统发送查询请求，所述查询请求包括：支付方钱包地址；

接收所述云存储系统根据所述查询请求返回的查询信息，所述查询信息包括：含有与所述支付方钱包地址相关联的私钥和预设人脸数据的第二数据密文；

根据自身对应的预设属性密码私钥对所述第二数据密文进行解密，并从解密得到的第二数据明文中获取与所述支付方钱包地址对应的私钥和预设人脸数据。

5.根据权利要求4所述的方法，其特征在于，所述方法还包括：

判断所述人脸数据与预设人脸数据之间的相似值是否大于预设相似阈值；

当所述人脸数据与预设人脸数据之间的相似值大于预设相似阈值时，确定所述人脸数

据与预设人脸数据满足预设识别条件；

当确定所述人脸数据与预设人脸数据满足预设识别条件之后，还包括；

在向系统内广播加密且签名的交易信息后，向所述网关返回支付成功信息。

6.根据权利要求5所述的方法，其特征在于，根据预设属性密码私钥解密从网关接收的第一数据密文之前，包括：

接收CA系统发送的与自身对应的预设属性密码私钥。

7.一种基于区块链的支付方法，应用于网关，其特征在于，包括：

接收收款方支付终端发送的第一数据密文，所述第一数据密文包含经过属性加密的交易信息和人脸数据，所述交易信息包含支付方钱包地址；

将所述第一数据密文发送给人脸识别服务器。

8.根据权利要求7所述的方法，其特征在于，在接收收款方支付终端发送的第一数据密文之前，包括：

接收支付方支付终端发送的支付方钱包地址，以及经过属性加密后的预设人脸数据和私钥；

将所述支付方钱包地址，以及经过属性加密后的预设人脸数据和私钥按照预设数据格式上传至云存储系统。

9.根据权利要求8所述的方法，其特征在于，所述方法还包括：

接收所述人脸识别服务器发送的支付成功信息；

将所述支付成功信息发送给所述收款方支付终端。

10.一种具有处理器可执行的非易失的程序代码的计算机可读介质，其特征在于，所述程序代码使所述处理器执行所述权利要求3至6任一项或者权利要求7至9任一项所述的方法。

基于区块链的支付系统及方法

技术领域

[0001] 本发明涉及交易支付技术领域，尤其是涉及一种基于区块链的支付系统及方法。

背景技术

[0002] 目前，当用户使用现有技术中基于区块链技术实现的支付系统进行交易支付时，用户通常需要借助存储自身私钥的硬件设备(如手机)完成对交易的数字签名，支付方式单一，无法满足用户多样化的支付需求。并且，在现有的支付技术中，大多缺乏对交易信息的保护，容易泄露用户的隐私，给用户带来不便。

发明内容

[0003] 有鉴于此，本发明的目的在于提供一种基于区块链的支付系统及方法，以缓解在现有的支付过程中，用户通常需要借助存储其私钥的硬件设备完成对交易的数字签名，支付方式单一，并且对交易信息缺乏保护，不能满足用户多样化支付需求和安全需求，给用户带来不便等技术问题。

[0004] 第一方面，本发明实施例提供了一种基于区块链的支付系统，包括：收款方支付终端、人脸识别设备、网关、人脸识别服务器、区块链节点和云存储系统；

[0005] 所述收款方支付终端，用于组织交易信息，接收所述人脸识别设备采集的人脸数据，将所述交易信息和人脸数据按照指定访问控制规则进行属性加密，并将加密得到的第一数据密文发送给所述网关，以使所述网关将所述第一数据密文发送给人脸识别服务器；

[0006] 所述人脸识别服务器，用于根据与自身对应的预设属性密码私钥进行解密，从解密得到的第一数据明文中获取人脸数据和交易信息中的支付方钱包地址，并从所述云存储系统中获取与所述支付方钱包地址对应的私钥和预设人脸数据；以及，若所述人脸数据与预设人脸数据满足预设识别条件，调用所述私钥对交易信息进行签名，执行属性加密后向系统内广播加密且签名的交易信息；

[0007] 所述区块链节点，用于根据与自身对应的预设属性密码私钥解密加密且签名的交易信息，并利用与所述私钥相关联的数字身份证书对解密得到的交易信息进行验证，若验证通过，将验证通过的交易信息记录在区块链网络中。

[0008] 结合第一方面，本发明实施例提供了第一方面的第一种可能的实施方式，其中，还包括：支付方支付终端、中央数字货币系统和CA系统；

[0009] 所述支付方支付终端，用于根据支付用户的用户信息生成公私钥对和支付方钱包地址；以及，当用户确定开通刷脸支付时，用于将与自身对应的人脸识别设备采集的人脸数据和私钥按照指定访问控制规则进行属性加密，并将得到的数据密文(包含支付方钱包地址，以及经过属性加密的私钥和预设人脸数据)发送给所述网关，以使所述网关将所述数据密文发送给云存储系统；

[0010] 所述中央数字货币系统，用于根据所述支付方支付终端发送的含有支付方钱包地址的注册请求生成与所述支付方钱包地址对应的数字货币账户；

[0011] 所述CA系统，还用于根据所述支付终端发送的支付方钱包地址生成身份数字证书，将与支付方钱包地址相关联的身份数字证书通过所述网关传输至所述支付方支付终端，并将所述身份数字证书加入到区块链网络中；以及，向所述人脸识别服务器和所述区块链节点分发各自对应的预设属性密码私钥。

[0012] 第二方面，本发明实施例还提供一种基于区块链的支付方法，应用于人脸识别服务器，包括：

[0013] 根据与自身对应的预设属性密码私钥解密从网关接收的第一数据密文；

[0014] 从解密得到的第一数据明文中获取人脸数据和交易信息中的支付方钱包地址；

[0015] 从云存储系统中获取与所述支付方钱包地址对应的私钥和预设人脸数据；

[0016] 若所述人脸数据与预设人脸数据满足预设识别条件，调用所述私钥对交易信息进行签名，执行属性加密后向系统内广播加密且签名的交易信息。

[0017] 结合第二方面，本发明实施例提供了第二方面的第一种可能的实施方式，其中，从云存储系统中获取与所述支付方钱包地址对应的私钥和预设人脸数据，包括：

[0018] 向所述云存储系统发送查询请求，所述查询请求包括：支付方钱包地址；

[0019] 接收所述云存储系统根据所述查询请求返回的查询信息，所述查询信息包括：含有与所述支付方钱包地址相关联的私钥和预设人脸数据的第二数据密文；

[0020] 根据自身对应的预设属性密码私钥对所述第二数据密文进行解密，并从解密得到的第二数据明文中获取与所述支付方钱包地址对应的私钥和预设人脸数据。

[0021] 结合第二方面，本发明实施例提供了第二方面的第二种可能的实施方式，其中，所述方法还包括：

[0022] 判断所述人脸数据与预设人脸数据之间的相似值是否大于预设相似阈值；

[0023] 当所述人脸数据与预设人脸数据之间的相似值大于预设相似阈值时，确定所述人脸数据与预设人脸数据满足预设识别条件；

[0024] 当确定所述人脸数据与预设人脸数据满足预设识别条件之后，还包括；

[0025] 在向系统内广播加密且签名的交易信息后，向所述网关返回支付成功信息。

[0026] 结合第二方面，本发明实施例提供了第二方面的第三种可能的实施方式，其中，根据预设属性密码私钥解密从网关接收的第一数据密文之前，包括：

[0027] 接收CA系统发送的与自身对应的预设属性密码私钥。

[0028] 第三方面，本发明实施例还提供一种基于区块链的支付方法，应用于网关，包括：

[0029] 接收收款方支付终端发送的第一数据密文，所述第一数据密文包含经过属性加密的交易信息和人脸数据，所述交易信息包含支付方钱包地址；

[0030] 将所述第一数据密文发送给人脸识别服务器。

[0031] 结合第三方面，本发明实施例提供了第三方面的第一种可能的实施方式，其中，在接收收款方支付终端发送的第一数据密文之前，包括：

[0032] 接收支付方支付终端发送的支付方钱包地址，以及经过属性加密的预设人脸数据和私钥；

[0033] 将所述支付方钱包地址，以及经过属性加密后的预设人脸数据和私钥按照预设数据格式上传至云存储系统。

[0034] 结合第三方面，本发明实施例提供了第三方面的第二种可能的实施方式，其中，所

述方法还包括：

[0035] 接收所述人脸识别服务器发送的支付成功信息；

[0036] 将所述支付成功信息发送给所述收款方支付终端。

[0037] 第四方面，本发明实施例还提供一种具有处理器可执行的非易失的程序代码的计算机可读介质，所述程序代码使所述处理器执行所述第二方面或者第三方面所述的方法。

[0038] 本发明实施例带来了以下有益效果：本发明提供一种基于区块链的支付系统及方法，除传统的基于支付终端的支付方式外，引入了刷脸支付，能适应多样化的支付场景，且对交易信息和人脸数据进行属性加密，不仅可以满足用户的多样化支付需求，还提高支付安全性。

[0039] 本发明的其他特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明而了解。本发明的目的和其他优点在说明书、权利要求书以及附图中所特别指出的结构来实现和获得。

[0040] 为使本发明的上述目的、特征和优点能更明显易懂，下文特举较佳实施例，并配合所附附图，作详细说明如下。

附图说明

[0041] 为了更清楚地说明本发明具体实施方式或现有技术中的技术方案，下面将对具体实施方式或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施方式，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。

[0042] 图1为现有技术的支付流程图；

[0043] 图2为本发明实施例提供的基于区块链的支付系统的结构示意图；

[0044] 图3为本发明实施例提供的基于区块链的支付系统的数据流程图；

[0045] 图4为本发明另一个实施例提供的基于区块链的支付方法的流程图；

[0046] 图5为本发明另一个实施例提供的基于区块链的支付方法的流程图；

[0047] 图6为本发明另一个实施例提供的用户注册处理流程图；

[0048] 图7为本发明另一个实施例提供的刷脸支付流程图。

[0049] 图标：

[0050] 100-收款方支付终端；200-人脸识别设备；300-网关；400-人脸识别服务器；500-云存储系统；600-区块链节点。

具体实施方式

[0051] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合附图对本发明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做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。

[0052] 名词解释：

[0053] 属性加密，将文件标记为不同的属性，并使用属性对文件进行加密。其特点是，用户的私钥和密文由一个属性集标记。

[0054] 现有基于区块链技术实现的支付系统，用户通常需要借助存储其私钥的硬件设备(如手机)完成对交易的数字签名，方式单一。例如，如图1所示，当用户1通过智能终端要转账给用户2时，需要执行以下几个步骤。

[0055] 1.获取用户2的收款地址；

[0056] 2.利用手机组织交易信息并签名；

[0057] 3.将签名后的交易信息向系统内广播；

[0058] 4.节点验证交易信息，通过后将其记录到区块链中；

[0059] 5.用户2检索区块链记录，确认转账完成。

[0060] 目前，在现有的支付过程中，用户通常需要借助存储其私钥的硬件设备完成对交易的数字签名，支付方式单一，并且对交易信息缺乏保护，容易泄露用户隐私，不能满足用户多样化支付需求和安全需求，给用户带来不便，基于此，本发明实施例提供的一种基于区块链的支付系统及方法，除传统的基于支付终端的支付方式外，引入了刷脸支付，能够适应多样化的支付场景，且对交易信息和人脸数据进行属性加密，不仅可以满足用户的多样化支付需求，还提高支付安全性。

[0061] 本发明实施例中的属性加密算法，是按照访问者的属性来确认属性集合，例如区块链节点和人脸识别服务器。加密时，使用该属性集合中元素的组合来指定具体访问控制规则(即解密规则)，例如，加密交易数据时，应指定访问控制规则为(“区块链节点”或者“人脸识别服务器”)，也就是说区块链节点或者人脸识别服务器可以解密加密的交易数据；加密人脸数据时，指定访问控制规则为(“人脸识别服务器”)，也就是说人脸识别服务器可以解密加密的人脸数据。

[0062] 为便于对本实施例进行理解，首先对本发明实施例所公开的一种基于区块链的支付系统进行详细介绍。

[0063] 如图2和图3所示，本发明实施例中，提供了一种基于区块链的支付系统，该系统包括：收款方支付终端100、人脸识别设备200、网关300、人脸识别服务器400、区块链节点600、CA系统、数字货币系统和云存储系统500。

[0064] 每个用户通过自身拥有的支付终端完成用户注册，在注册过程中，支付终端生成用户的公私钥对，以及根据公钥生成用户钱包地址。之后，用户通过自己的支付终端向数字货币系统和系统发送包含有用户钱包地址和用户信息的注册请求，以完成钱包账号注册，并接收CA系统发送的数字身份证书。在实际应用中，支付终端可以为手机和PAD等智能设备。

[0065] 具体的，根据实际需求，每个支付终端可以对应自身配置一个用于采集人脸数据的人脸识别设备200，用于在注册过程中采集注册用户的人脸数据，以及在支付过程中采集支付方用户的人脸数据。优选的，人脸识别设备200可以为高清摄像头，高清摄像头可以与支付终端相互独立设置，也可以将摄像头集成在支付终端内。在用户注册过程中，支付终端将经过属性加密保护的私钥、经过属性加密保护的人脸数据和用户钱包地址明文三者级联，并通过网关300上传到云存储系统500进行存储。

[0066] 在支付方向收款方支付款项时，支付方用户可以选择用自己的支付终端支付，也可以选择刷脸支付。当支付方用户选择刷脸支付时，收款用户通过自己的收款方支付终端100生成交易信息，接收人脸识别设备采集的人脸数据，将所述交易信息、人脸数据分别执

行属性加密算法，即加密交易信息时，指定访问控制规则为（“人脸识别服务器”或者“区块链节点”）；加密人脸数据时，指定访问控制规则为：（“人脸识别服务器”）。将加密得到的第一数据密文上传给网关300。

[0067] 所述网关300，在用户注册过程中，发送设备注册请求、网关注册请求和钱包注册请求给CA系统，CA系统根据各个注册请求分发身份数字证书、企业证书、个人小额证书、设备证书和网关300证书等，以及将各类证书登记在区块链中。

[0068] 而在刷脸支付过程中，所述网关300用于将收款方支付终端100发送的第一数据密文上传至人脸识别服务器400。

[0069] 所述人脸识别服务器400，用于在每个用户注册完成后，管理该用户托管的支付私钥。而在刷脸支付过程中，人脸识别服务器400对支付方用户进行身份认证(即人脸验证)，首先根据与自身对应的预设属性密码私钥进行解密，从解密得到的第一数据明文中获取人脸数据和交易信息中的支付方钱包地址，并从所述云存储系统500系统中获取与所述支付方钱包地址对应的私钥和预设人脸数据。之后判断所述人脸数据与预设人脸数据是否满足预设识别条件，当所述人脸数据与预设人脸数据满足预设识别条件(即当前人脸数据与预设人脸数据对应同一支付用户)，调用所述私钥对交易信息进行签名，执行属性加密后向系统内广播加密且签名的交易信息。此外，在向系统内广播加密且签名的交易信息后，向所述网关300返回支付成功信息。

[0070] 其中，上述的人脸识别服务器400是集成人脸识别和实现交易两个功能的智能设备。而在实际应用中，上述人脸识别服务器400实现的两个功能：人脸识别；交易模块(包含获取用户私钥和使用私钥签名)，还可以由几个相互独立的设备实现，例如，只用于识别人脸的人脸识别服务器A，部署有代理云钱包的交易服务器B负责交易，若人脸识别服务器A识别成功，人脸识别服务器A用自己的私钥对交易信息进行签名后，将签名后的交易信息发送给代理云钱包，代理云钱包再检索用户私钥，使用用户的私钥签名交易信息。

[0071] 所述区块链节点600，用于对交易进行验证，存证交易记录，执行智能合约，区块链的维护等。

[0072] 所述CA系统，用于负责分发各类证书和证书管理，以及向人脸识别服务器400和各个区块链节点600分发属性密码私钥。

[0073] 在实际应用中，所述CA系统，还用于根据任一支付终端发送的用户钱包地址生成身份数字证书，将与用户钱包地址相关联的身份数字证书通过所述网关300传输至所述支付终端，并将所述身份数字证书加入到区块链网络中。并且，CA系统用于向所述人脸识别服务器400和所述区块链节点600分发各自对应的预设属性密码私钥。

[0074] 例如，CA系统向所述人脸识别服务器400发送包含“人脸识别服务器”属性的私钥，向区块链节点600发送包含“区块链节点”属性的私钥，加密交易信息时，指定访问控制规则为（“人脸识别服务器”或者“区块链节点”）；加密人脸数据时，指定访问控制规则为（“人脸识别服务器”）。

[0075] 所述数字货币系统(即中央数字货币系统)，用于根据所述支付终端发送的含有用户钱包地址的注册请求生成与所述用户钱包地址对应的数字货币账户。

[0076] 本发明实施例提供的一种基于区块链的支付系统，除传统的基于支付终端的支付方式外，还引入了刷脸支付，能够适应多样化的支付场景，且对交易信息和人脸数据进行属

性加密，不仅可以满足用户的多样化支付需求，还提高支付安全性。

[0077] 如图4所示，在本发明的另一个实施例中，提供了一种应用于上述基于区块链的支付系统中人脸识别服务器的支付方法，所述方法包括以下几个步骤。

[0078] S101，根据与自身对应的预设属性密码私钥解密从网关接收的第一数据密文。

[0079] 具体的，在刷脸支付过程中，人脸识别服务器从网关接收含有人脸数据和交易信息的第一数据密文之前，人脸识别服务器接收CA系统发送的与人脸识别服务器对应的预设属性密码私钥，利用该属性密码私钥可以解密第一数据密文，得到人脸数据和交易信息。

[0080] S102，从解密得到的第一数据明文中获取人脸数据和交易信息中的支付方钱包地址。

[0081] S103，从云存储系统中获取与所述支付方钱包地址对应的私钥和预设人脸数据。

[0082] 具体的，从云存储系统中获取与所述支付方钱包地址对应的私钥和预设人脸数据包括以下几个步骤。

[0083] 人脸识别服务器向所述云存储系统发送查询请求，所述查询请求包括：支付方钱包地址。

[0084] 接收所述云存储系统根据所述查询请求返回的查询信息，所述查询信息包括：含有与所述支付方钱包地址相关联的私钥和预设人脸数据的第二数据密文。

[0085] 根据自身对应的预设属性密码私钥对所述第二数据密文进行解密，并从解密得到的第二数据明文中获取与所述支付方钱包地址对应的私钥和预设人脸数据。

[0086] S104，若所述人脸数据与预设人脸数据满足预设识别条件，调用所述私钥对交易信息进行签名，执行属性加密后向系统内广播加密且签名的交易信息。

[0087] 在实际应用中，当人脸识别服务器接收到云存储系统发送的预设人脸数据和私钥后，先判断所述人脸数据与预设人脸数据是否满足预设识别条件。具体判断过程如下：示例性的，判断所述人脸数据与预设人脸数据之间的相似值是否大于预设相似阈值，只有当所述人脸数据与预设人脸数据之间的相似值大于预设相似阈值时，确定所述人脸数据与预设人脸数据满足预设识别条件，即当前人脸数据和预设人脸数据对应同一支付用户，完成对支付方用户身份的认证。值得注意的是，在这里示出和描述的所有示例中，任何具体值应被解释为仅仅是示例性的，而不是作为限制，因此，示例性实施例的其他示例可以具有不同的值。

[0088] 当对支付方用户的身份认证通过后，调用该支付方用户的私钥对交易信息进行签名，并对签名后的交易信息进行属性加密，向系统内广播加密且签名的交易信息，以使各个区块链节点接收加密且签名的交易信息。每个区块链节点根据CA系统发送给自身的预设属性密码私钥，解密加密且签名的交易信息，解密后利用数字身份证书对解密得到的交易信息进行验证。其中，对交易信息的验证，不仅包含对签名的认证，还包括对交易是否满足交易条件进行验证，如用户A向用户B转账100元，不仅要验证该交易是否由A签名，还要验证用户A的账户余额是否不小于100元，只有当确定该交易是由用户A签名和用户A的账户余额不小于100元时，才能实现成功转账，完成这笔交易。在验证通过后，将验证通过的交易信息记录在区块链网络中。

[0089] 并且，在广播加密签名的交易信息后，向网关发送支付成功信息，以使所述网关将所述支付成功信息发送给收款方支付终端。

[0090] 而当对支付方的身份认证失败后，人脸识别服务器向网关发送支付失败信息，以使所述网关发送支付失败信息给收款方支付终端。

[0091] 如图5所示，在本发明的另一个实施例中，提供了一种应用于上述基于区块链的支付系统中网关的支付方法，所述方法包括以下几个步骤。

[0092] S201，接收收款方支付终端发送的第一数据密文，所述第一数据密文包含经过属性加密的交易信息和人脸数据，所述交易信息包含支付方钱包地址。

[0093] 具体的，在网关接收收款方支付终端发送的所述第一数据密文之前，支付方用户需要完成人脸注册，具体注册方法包括以下步骤。

[0094] 支付方支付终端将支付方钱包地址明文和经过属性加密后的私钥、经过属性加密后的预设人脸数据按照预设数据格式上传至云存储系统。

[0095] 在实际应用中，在支付方用户进行注册时，支付方支付终端将支付方用户的人脸数据、私钥进行属性加密，将密文和支付方钱包地址明文级联后上传。

[0096] S202，将所述第一数据密文发送给人脸识别服务器。

[0097] 在前述实施例的基础上，所述应用于网关的支付方法还包括以下步骤。

[0098] 接收所述人脸识别服务器发送的支付成功信息。

[0099] 将所述支付成功信息发送给所述收款方支付终端。

[0100] 以下以举例方式说明本发明实施例提供的一种基于区块链的支付方法的具体流程：

[0101] 1)系统初始化，CA系统为相关方颁发证书(身份数字证书、企业证书、个人小额证书、设备证书和网关证书等)，以及为人脸识别服务器和各个区块链节点生成并分发各自对应的属性密码私钥。

[0102] 2)用户注册：如图6所示，用户通过自己的支付终端生成公私钥对及用户钱包地址。若用户选择开通刷脸支付功能，则需要通过人脸识别设备录入人脸数据。支付终端将用户的人脸数据进行属性加密，将加密后的人脸数据，以及经过属性加密保护的私钥和用户钱包地址明文三者级联后，按照如下表1的数据格式通过网关上传给云存储系统。云存储系统发送存储已完成提示信息给支付终端，提示用户人脸注册已完成。

[0103] 表1

[0104]

Addr	$E_{ABE}(Key_{sign})$	$E_{ABE}(Data_{face})$

[0105] 3)支付过程：如图7所示，当支付方用户选择刷脸支付时，收款方支付终端将交易信息和人脸识别设备发送的人脸数据分别进行属性加密，并将交易信息密文和人脸数据密文组合得到第一数据密文，最后将第一数据密文通过网关发送给人脸识别服务器。

[0106] 人脸识别服务器根据CA系统发送给自身的属性密码私钥对第一数据密文进行解密，得到人脸数据和交易信息中的支付方钱包地址。之后人脸识别服务器向云存储系统发送含有支付方钱包地址的查询请求，云存储系统向人脸识别服务器返回查询结果，所示查询结果包括：含有与所述支付方钱包地址相关联的私钥和预设人脸数据的第二数据密文。人脸识别服务器利用自身的属性密码私钥对第二数据密文进行解密，从而得到与所述支付方钱包地址相关联的私钥和预设人脸数据。最后调用人脸识别算法，对人脸数据和预设人脸数据进行识别。若人脸数据和预设人脸数据对应同一支付用户，即对支付方的身份认证

通过，则调用支付方用户私钥对交易进行签名，并对签名后的交易信息进行属性加密后，向包含有多个区块链节点的系统内广播加密且签名的交易信息。每个区块链节点根据CA系统发送给自身的预设属性密码私钥对加密且签名的交易信息进行解密，解密后利用数字身份证书对交易信息进行验证，即对签名的认证和交易条件的验证，若验证通过，将验证通过的交易信息记录在区块链网络中。

[0107] 并且，在人脸识别服务器广播加密签名的交易信息后，向网关发送支付成功信息，以使所述网关将支付成功信息发送给收款方支付终端，收款方支付终端接收支付成功信息后提示收款方支付成功，支付流程结束。若对用户的身份认证失败时，人脸识别服务器向所述网关返回支付失败信息，以使网关将所述支付失败信息发送给收款方支付终端提示收款方支付失败，支付流程结束。

[0108] 此外，当支付方用户选择使用自己的支付终端支付时，利用支付终端生成交易信息，并使用用户私钥签名并执行属性加密后进行系统内广播。区块链节点接收到交易信息，解密后验证该交易信息。若验证通过则将交易信息记录在区块链中。

[0109] 4)查询：支付终端，还用于根据用户输入的查询信息，向区块链节点发送查询请求，区块链节点验证查询权限后检索区块链数据，将检索得到的数据解密后，并将查询结果明文通过网关传输至支付终端。

[0110] 例如，用户输入自己的身份信息，可以查询自己钱包账户内的余额。

[0111] 本发明实施例提供一种基于区块链的支付系统及方法具有以下优势：

[0112] a)支付多样性：

[0113] 除传统的基于支付终端的支付方式外，本发明实施例引入了刷脸支付，能适应多样化的支付场景，满足用户的多样化支付需求。

[0114] b)高安全性：

[0115] 交易信息均经过加密保护，安全性大大提高，保护用户的隐私。

[0116] c)高效性：

[0117] 使用属性加密算法加密存在多个潜在访问者的数据(如交易数据或者人脸数据)，能够实现一份基于属性加密的密文，多人解密，从而大大提升了效率。

[0118] 在本发明的另一个实施例中，还提供了一种具有处理器可执行的非易失的程序代码的计算机可读介质，所述程序代码使所述处理器执行所述基于区块链的支付方法。

[0119] 除非另外具体说明，否则在这些实施例中阐述的部件和步骤的相对步骤、数字表达式和数值并不限制本发明的范围。

[0120] 本发明实施例所提供的装置，其实现原理及产生的技术效果和前述方法实施例相同，为简要描述，装置实施例部分未提及之处，可参考前述方法实施例中相应内容。

[0121] 应注意到：相似的标号和字母在下面的附图中表示类似项，因此，一旦某一项在一个附图中被定义，则在随后的附图中不需要对其进行进一步定义和解释。

[0122] 附图中的流程图和框图显示了根据本发明的多个实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段或代码的一部分，所述模块、程序段或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个连续的方框实际上可以基

本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或动作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0123] 本发明实施例所提供的基于区块链的支付系统的计算机程序产品，包括存储了程序代码的计算机可读存储介质，所述程序代码包括的指令可用于执行前面方法实施例中所述的方法，具体实现可参见方法实施例，在此不再赘述。

[0124] 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，上述描述的系统和装置的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0125] 另外，在本发明实施例的描述中，除非另有明确的规定和限定，术语“安装”、“相连”、“连接”应做广义理解，例如，可以是固定连接，也可以是可拆卸连接，或一体地连接；可以是机械连接，也可以是电连接；可以是直接相连，也可以通过中间媒介间接相连，可以是两个元件内部的连通。对于本领域的普通技术人员而言，可以具体情况理解上述术语在本发明中的具体含义。

[0126] 所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，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)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0127] 在本发明的描述中，需要说明的是，术语“中心”、“上”、“下”、“左”、“右”、“竖直”、“水平”、“内”、“外”等指示的方位或位置关系为基于附图所示的方位或位置关系，仅是为了便于描述本发明和简化描述，而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作，因此不能理解为对本发明的限制。此外，术语“第一”、“第二”、“第三”仅用于描述目的，而不能理解为指示或暗示相对重要性。

[0128] 最后应说明的是：以上所述实施例，仅为本发明的具体实施方式，用以说明本发明的技术方案，而非对其限制，本发明的保护范围并不局限于此，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：任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，其依然可以对前述实施例所记载的技术方案进行修改或可轻易想到变化，或者对其中部分技术特征进行等同替换；而这些修改、变化或者替换，并不使相应技术方案的本质脱离本发明实施例技术方案的精神和范围，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应所述以权利要求的保护范围为准。

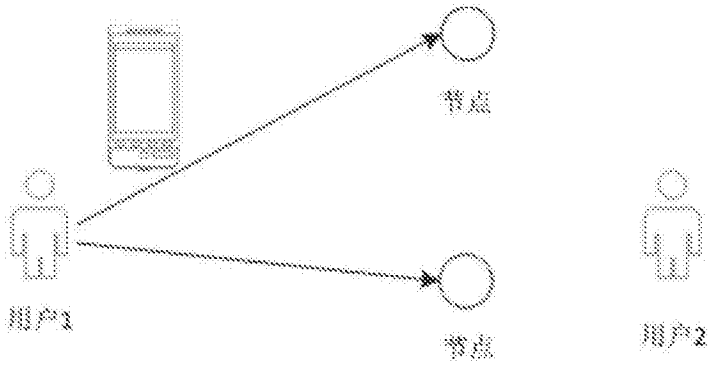

节点
用户1
节点
用户2

图1

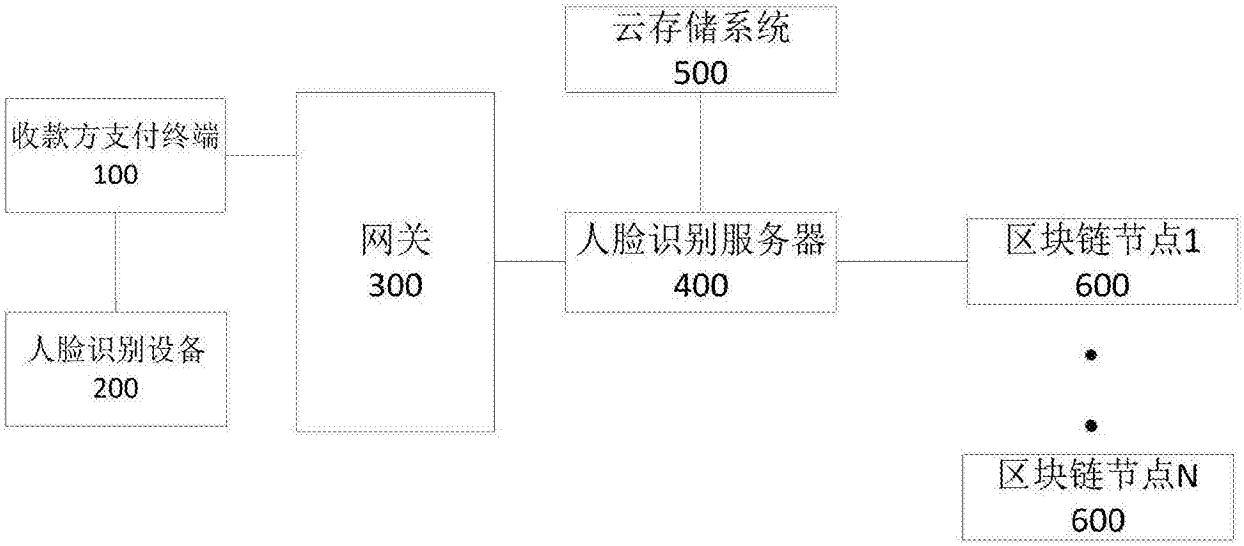

云存储系统
500
收款方支付终端
100
网关
300
人脸识别服务器
400
区块链节点1
600
人脸识别设备
200
区块链节点N
600

图2

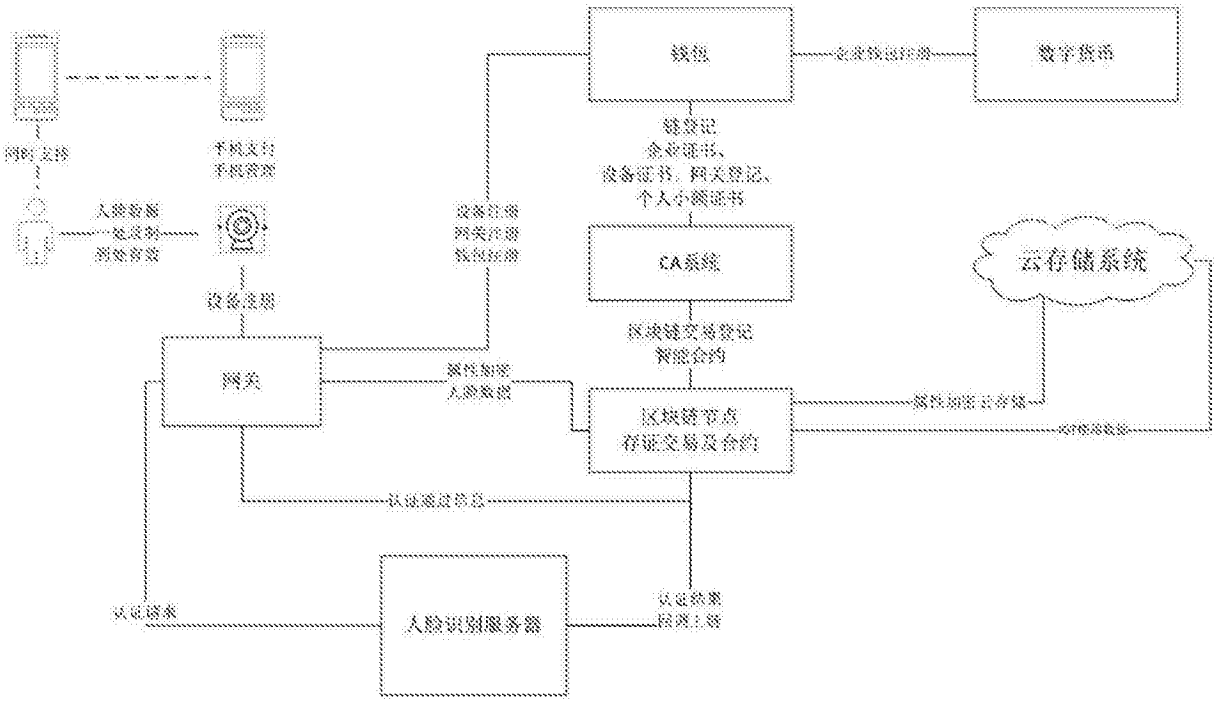

钱包
数字货币
CA系统
云存储系统
网关
区块链节点
存储交易及合约
人脸识别服务器

图3

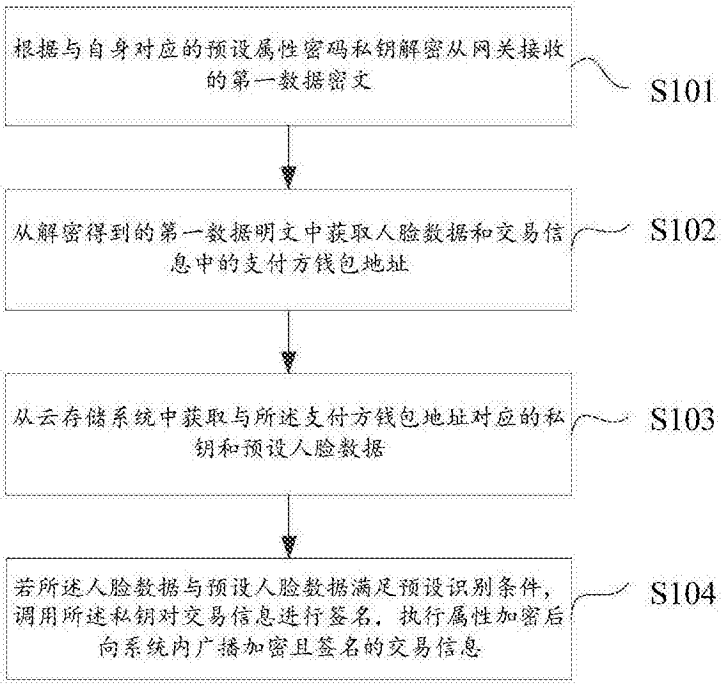

根据与自身对应的预设属性密码私钥解密从网关接收的第一数据密文
S101
从解密得到的第一数据明文中获取人脸数据和交易信息中的支付方钱包地址
S102
从云存储系统中获取与所述支付方钱包地址对应的私钥和预设人脸数据
S103
若所述人脸数据与预设人脸数据满足预设识别条件，调用所述私钥对交易信息进行签名，执行属性加密后向系统内广播加密且签名的交易信息
S104

图4

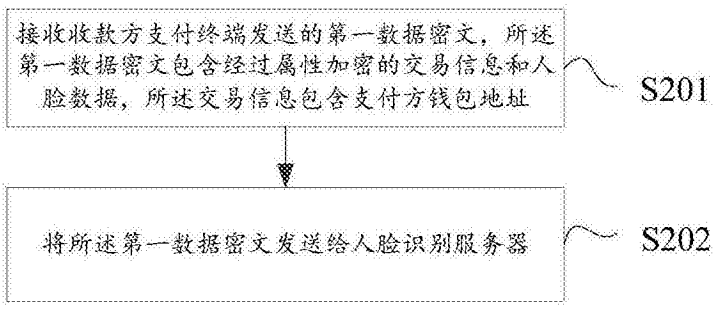

接收收款方支付终端发送的第一数据密文，所述第一数据密文包含经过属性加密的交易信息和人脸数据，所述交易信息包含支付方钱包地址
S201
将所述第一数据密文发送给人脸识别服务器
S202

图5

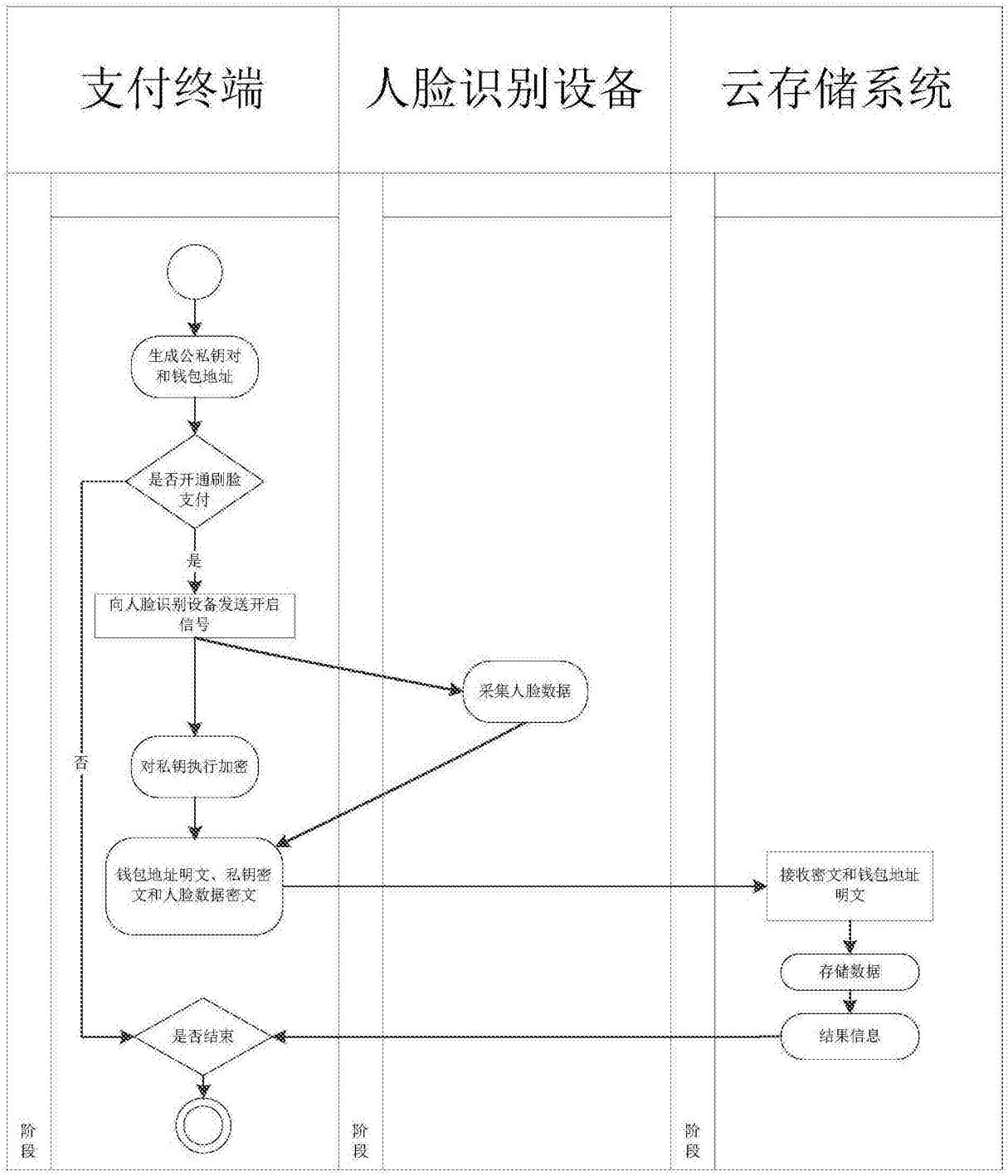

支付终端
人脸识别设备
云存储系统
生成公私钥对和钱包地址
是否开通刷脸支付
是
否
向人脸识别设备发送开启信号
采集人脸数据
对私钥执行加密
钱包地址明文、私钥密文和人脸数据密文
接收密文和钱包地址明文
存储数据
结果信息
是否结束
阶段
阶段
阶段

图6

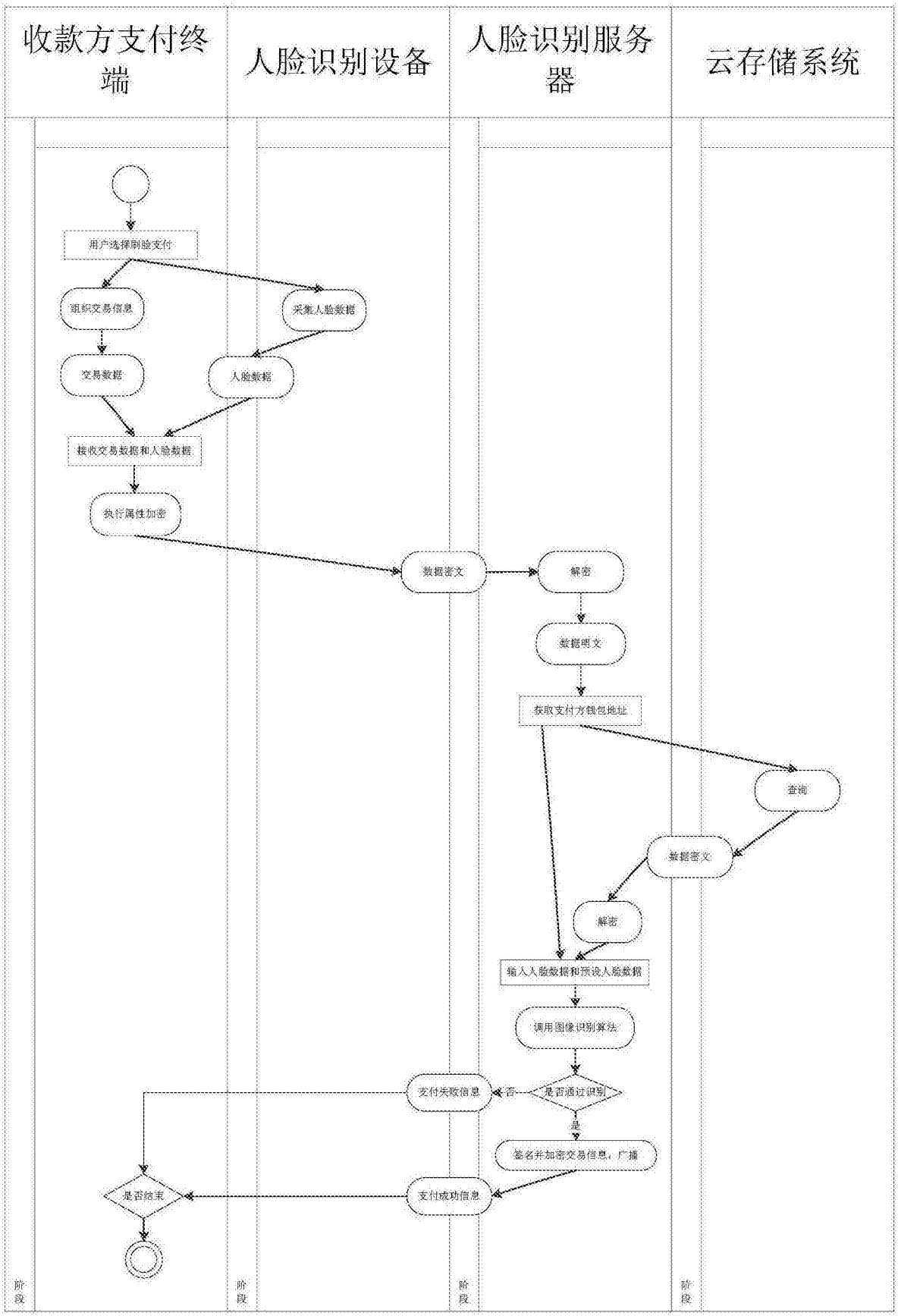

收款方支付终端
人脸识别设备
人脸识别服务器
云存储系统
用户选择刷脸支付
组织交易信息
采集人脸数据
交易数据
人脸数据
接收交易数据和人脸数据
执行属性加密
数据密文
解密
数据明文
获取支付方钱包地址
查询
数据密文
解密
输入人脸数据和预设人脸数据
调用图像识别算法
是否通过识别
否
支付失败信息
是
签名并加密交易信息，广播
支付成功信息
是否结束
阶段
阶段
阶段
阶段

图7