(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 108921542 A
(43)申请公布日 2018.11.30

(21)申请号 201810543449.0

(22)申请日 2018.05.30

(71)申请人 招商银行股份有限公司
地址 518000 广东省深圳市福田区深南大道7088招商银行大厦

(72)发明人 张育明 潘海清 陈鹏

(74)专利代理机构 深圳市世纪恒程知识产权代理事务所 44287
代理人 胡海国

(51)Int.Cl.
G06Q 20/32(2012.01)

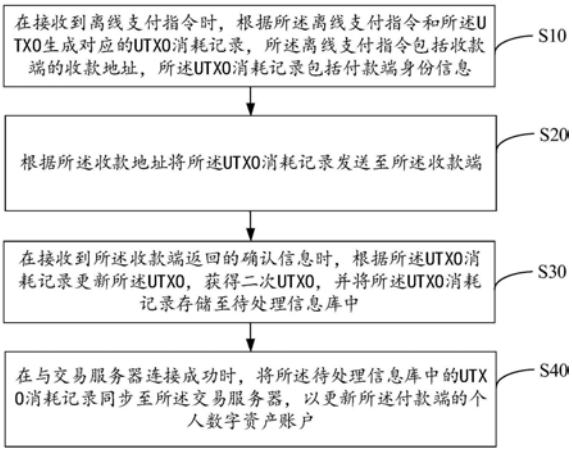
权利要求书2页 说明书10页 附图4页

(54)发明名称

数字资产的离线支付方法、付款端、收款端及存储介质

(57)摘要

本发明提供一种数字资产的离线支付方法，包括：付款端在接收到离线支付指令时，根据所述离线支付指令和本地UTXO生成对应的UTXO消耗记录；将所述UTXO消耗记录发送至收款端；在接收到所述收款端返回的确认信息时，根据所述UTXO消耗记录更新所述UTXO，获得二次UTXO，并将所述UTXO消耗记录存储至待处理信息库中；在与交易服务器连接成功时，将所述待处理信息库中的UTXO消耗记录同步至所述交易服务器，以更新所述付款端的个人数字资产账户。本发明还提供一种付款端、收款端及存储介质。本发明解决了移动终端在网络状态差或无网络时无法进行离线支付的技术问题。



CN 108921542 A

1.一种数字资产的离线支付方法，其特征在于，所述数字资产的离线支付方法应用于付款端，所述付款端的本地至少存储有一个未消耗的交易输出UTXO，所述数字资产的离线支付方法包括以下步骤：

在接收到离线支付指令时，根据所述离线支付指令和所述UTXO生成对应的UTXO消耗记录，所述离线支付指令包括收款端的收款地址，所述UTXO消耗记录包括付款端身份信息；

根据所述收款地址将所述UTXO消耗记录发送至所述收款端；

在接收到所述收款端返回的确认信息时，根据所述UTXO消耗记录更新所述UTXO，获得二次UTXO，并将所述UTXO消耗记录存储至待处理信息库中；

在与交易服务器连接成功时，将所述待处理信息库中的UTXO消耗记录同步至所述交易服务器，以更新所述付款端的个人数字资产账户。

2.如权利要求1所述的数字资产的离线支付方法，其特征在于，所述在接收到所述收款端返回的确认信息时，根据所述UTXO消耗记录更新所述UTXO，获得二次UTXO，并将所述UTXO消耗记录存储至待处理信息库中的步骤之后，还包括：

在接收到二次离线支付指令时，判断所述UTXO消耗记录是否已同步至所述交易服务器；

若所述UTXO消耗记录已同步至所述交易服务器，则允许使用所述二次UTXO进行二次离线支付；

若所述UTXO消耗记录未同步至所述交易服务器，则拒绝使用所述二次UTXO进行二次离线支付。

3.如权利要求1所述的数字资产的离线支付方法，其特征在于，所述数字资产的离线支付方法，还包括以下步骤：

在与交易服务器连接成功时，若接收到在线支付请求，则判断所述待处理信息库中是否存在未同步的UTXO消耗记录；

若所述待处理信息库中存在未同步的UTXO消耗记录，则将所述未同步的UTXO消耗记录同步至所述交易服务器，并在同步完成时进行在线支付。

4.如权利要求1至3中任一项所述的数字资产的离线支付方法，其特征在于，所述在接收到离线支付指令时，根据所述离线支付指令和所述UTXO生成对应的UTXO消耗记录的步骤包括：

在接收到离线支付指令时，判断所述离线支付指令包括的支付金额是否小于预设支付阈值，和/或判断所述付款端在预设周期内的离线支付指令接收次数是否小于预设接收阈值；

若所述支付金额小于预设支付阈值，和/或所述离线支付指令接收次数小于预设接收阈值，则根据所述离线支付指令和所述UTXO生成对应的UTXO消耗记录。

5.一种数字资产的离线支付方法，其特征在于，所述数字资产的离线支付方法应用于收款端，所述数字资产的离线支付方法包括以下步骤：

在接收到付款端发送的UTXO消耗记录时，根据所述UTXO消耗记录包括的付款端身份信息验证所述付款端是否可信；

若所述付款端可信，则向所述付款端返回对应的确认信息，并将所述UTXO消耗记录存储至待处理信息库中；

在与交易服务器连接成功时，将所述待处理信息库中的UTXO消耗记录同步至所述交易服务器，以更新所述收款端的个人数字资产账户。

6.如权利要求5所述的数字资产的离线支付方法，其特征在于，所述在与交易服务器连接成功时，将所述待处理信息库中的UTXO消耗记录存储同步至所述交易服务器，以更新所述收款端的个人资产账户的步骤之后，还包括：

根据已同步的UTXO消耗记录生成对应入账UTXO。

7.一种付款端，其特征在于，所述付款端的本地至少存储有一个UTXO，所述付款端还包括处理器、存储器、以及存储在所述存储器上并可被所述处理器执行的离线支付程序，其中所述离线支付程序被所述处理器执行时，实现如权利要求1至4中任一项所述的数字资产的离线支付方法的步骤。

8.一种收款端，其特征在于，所述收款端还包括处理器、存储器、以及存储在所述存储器上并可被所述处理器执行的离线支付程序，其中所述离线支付程序被所述处理器执行时，实现如权利要求5至6中任一项所述的数字资产的离线支付方法的步骤。

9.一种存储介质，其特征在于，所述存储介质上存储有离线支付程序，其中所述离线支付程序被处理器执行时，实现如权利要求1至4中任一项所述的数字资产的离线支付方法的步骤。

10.一种存储介质，其特征在于，所述存储介质上存储有离线支付程序，其中所述离线支付程序被处理器执行时，实现如权利要求5至6中任一项所述的数字资产的离线支付方法的步骤。

数字资产的离线支付方法、付款端、收款端及存储介质

技术领域

[0001] 本发明涉及终端技术领域，尤其涉及一种数字资产的离线支付方法、付款端、收款端及存储介质。

背景技术

[0002] 随着终端技术的发展，移动支付已经成为了日常生活中一种重要的支付方式。目前，市面上的移动支付方案大多是采用在线支付方式，这种在线支付需要终端设备连接网络才能使用。然而这种支付方式的缺点也是显而易见的，当用户处于网络状况较差环境、甚至没有网络的情况下(比如地铁、偏远山区等)，就无法进行支付，这就给用户带来了不便。

发明内容

[0003] 本发明的主要目的在于提供一种数字资产的离线支付方法、付款端、收款端及存储介质，旨在解决网络状态差或无网络时无法进行移动支付的技术问题。

[0004] 为实现上述目的，本发明提供一种数字资产的离线支付方法，所述数字资产的离线支付方法应用于付款端，所述付款端的本地至少存储有一个未消耗的交易输出UTXO，所述数字资产的离线支付方法包括以下步骤：

[0005] 在接收到离线支付指令时，根据所述离线支付指令和所述UTXO生成对应的UTXO消耗记录，所述离线支付指令包括收款端的收款地址，所述UTXO消耗记录包括付款端身份信息；

[0006] 根据所述收款地址将所述UTXO消耗记录发送至所述收款端；

[0007] 在接收到所述收款端返回的确认信息时，根据所述UTXO消耗记录更新所述UTXO，获得二次UTXO，并将所述UTXO消耗记录存储至待处理信息库中；

[0008] 在与交易服务器连接成功时，将所述待处理信息库中的UTXO消耗记录同步至所述交易服务器，以更新所述付款端的个人数字资产账户。

[0009] 进一步的，所述在接收到所述收款端返回的确认信息时，根据所述UTXO消耗记录更新所述UTXO，获得二次UTXO，并将所述UTXO消耗记录存储至待处理信息库中的步骤之后，还包括：

[0010] 在接收到二次离线支付指令时，判断所述UTXO消耗记录是否已同步至所述交易服务器；

[0011] 若所述UTXO消耗记录已同步至所述交易服务器，则允许使用所述二次UTXO进行二次离线支付；

[0012] 若所述UTXO消耗记录未同步至所述交易服务器，则拒绝使用所述二次UTXO进行二次离线支付。

[0013] 进一步的，所述数字资产的离线支付方法，还包括以下步骤：

[0014] 在与交易服务器连接成功时，若接收到在线支付请求，则判断所述待处理信息库中是否存在未同步的UTXO消耗记录；

[0015] 若所述待处理信息库中存在未同步的UTXO消耗记录，则将所述未同步的UTXO消耗记录同步至所述交易服务器，并在同步完成时进行在线支付。

[0016] 进一步的，所述在接收到离线支付指令时，根据所述离线支付指令和所述UTXO生成对应的UTXO消耗记录的步骤，还包括：

[0017] 在接收到离线支付指令时，判断所述离线支付指令包括的支付金额是否小于预设支付阈值，和/或判断所述付款端在预设周期内的离线支付指令接收次数是否小于预设接收阈值；

[0018] 若所述支付金额小于预设支付阈值，和/或所述离线支付指令接收次数小于预设接收阈值，则根据所述离线支付指令和所述UTXO生成对应的UTXO消耗记录。

[0019] 此外，为实现上述目的，本发明还提供一种数字资产的离线支付方法，所述数字资产的离线支付方法应用于收款端，所述数字资产的离线支付方法包括以下步骤：

[0020] 在接收到付款端发送的UTXO消耗记录时，根据所述UTXO消耗记录包括的付款端身份信息验证所述付款端是否可信；

[0021] 若所述付款端可信，则向所述付款端返回对应的确认信息，并将所述UTXO消耗记录存储至待处理信息库中；

[0022] 在与交易服务器连接成功时，将所述待处理信息库中的UTXO消耗记录同步至所述交易服务器，以更新所述收款端的个人数字资产账户。

[0023] 进一步的，所述在与交易服务器连接成功时，将所述待处理信息库中的UTXO消耗记录存储同步至所述交易服务器，以更新所述收款端的个人数字资产账户的步骤之后，还包括：

[0024] 根据已同步的UTXO消耗记录生成对应入账UTXO。

[0025] 此外，为实现上述目的，本发明还提供一种付款端，所述付款端的本地至少存储有一个UTXO，所述付款端还包括处理器、存储器、以及存储在所述存储器上并可被所述处理器执行的离线支付程序，其中所述离线支付程序被所述处理器执行时，实现如上述应用于付款端的数字资产的离线支付方法的步骤。

[0026] 此外，为实现上述目的，本发明还提供一种收款端，所述收款端还包括处理器、存储器、以及存储在所述存储器上并可被所述处理器执行的离线支付程序，其中所述离线支付程序被所述处理器执行时，实现如上述应用于收款端的数字资产的离线支付方法的步骤。

[0027] 此外，为实现上述目的，本发明还提供一种存储介质，所述存储介质上存储有离线支付程序，其中所述离线支付程序被处理器执行时，实现如上述应用于付款端的数字资产的离线支付方法的步骤。

[0028] 此外，为实现上述目的，本发明还提供一种存储介质，所述存储介质上存储有离线支付程序，其中所述离线支付程序被处理器执行时，实现如上述应用于收款端的数字资产的离线支付方法的步骤。

[0029] 本发明的付款端可通过本地存储的资产信息实现离线支付操作和支付记录，并在网络恢复时根据相关的支付记录完成数字资产账户的更新变动，解决网络状态差或无网络时无法进行移动支付的问题，为用户的工作和生活提供了方便，提升了用户的使用体验。

附图说明

[0030] 图1为本发明实施例方案中涉及的付款端的硬件结构示意图；

[0031] 图2为本发明数字资产的离线支付方法第一实施例的流程示意图；

[0032] 图3为图2所示实施例涉及的付款端在转账前的本地存储示意图；

[0033] 图4为图2所示实施例涉及的付款端在转账后、同步前的本地存储示意图；

[0034] 图5为图2所示实施例涉及的付款端在同步后的本地存储示意图；

[0035] 图6为本发明数字资产的离线支付方法第二实施例的流程示意图；

[0036] 图7为图6所示实施例涉及的收款端在转账前的本地存储示意图；

[0037] 图8为图6所示实施例涉及的收款端在转账后、同步前的本地存储示意图；

[0038] 图9为图6所示实施例涉及的收款端在同步后的本地存储示意图。

[0039] 本发明目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

具体实施方式

[0040] 应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0041] 本发明实施例涉及的数字资产的离线支付方法主要应用于付款端，该付款端可以是手机、智能手环、平板电脑、可穿戴设备等移动终端。

[0042] 参照图1，图1为本发明实施例方案中涉及的付款端的硬件结构示意图。本发明实施例中，付款端可以包括处理器1001(例如中央处理器Central Processing Unit，CPU)，通信总线1002，用户接口1003，网络接口1004，存储器1005。其中，通信总线1002用于实现这些组件之间的连接通信；用户接口1003可以包括显示屏(Display)、输入单元比如键盘(Keyboard)；网络接口1004可选的可以包括标准的有线接口、无线接口(如无线保真WIreless-FIdelity，WI-FI接口)；存储器1005可以是高速随机存取存储器(random access memory，RAM)，也可以是稳定的存储器(non-volatile memory)，例如磁盘存储器，存储器1005可选的还可以是独立于前述处理器1001的存储装置。本领域技术人员可以理解，图1中示出的硬件结构并不构成对本发明的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

[0043] 继续参照图1，图1中作为一种计算机可读存储介质的存储器1005可以包括操作系统、网络通信模块以及离线支付程序。在图1中，网络通信模块主要用于连接交易服务器和其它移动端进行数据通信；而处理器1001可以调用存储器1005中存储的离线支付程序，并执行以下步骤：

[0044] 在接收到离线支付指令时，根据所述离线支付指令和本地存储的UTXO生成对应的UTXO消耗记录，所述离线支付指令包括收款端的收款地址，所述UTXO消耗记录包括付款端身份信息；

[0045] 根据所述收款地址将所述UTXO消耗记录发送至所述收款端；

[0046] 在接收到所述收款端返回的确认信息时，根据所述UTXO消耗记录更新所述UTXO，获得二次UTXO，并将所述UTXO消耗记录存储至待处理信息库中；

[0047] 在与交易服务器连接成功时，将所述待处理信息库中的UTXO消耗记录同步至所述交易服务器，以更新所述付款端的个人数字资产账户。

[0048] 进一步的，所述处理器1001还可以调用存储器1005中存储的离线支付程序，并执行以下步骤：

[0049] 在接收到二次离线支付指令时，判断所述UTXO消耗记录是否已同步至所述交易服务器；

[0050] 若所述UTXO消耗记录已同步至所述交易服务器，则允许使用所述二次UTXO进行二次离线支付；

[0051] 若所述UTXO消耗记录未同步至所述交易服务器，则拒绝使用所述二次UTXO进行二次离线支付。

[0052] 进一步的，所述处理器1001还可以调用存储器1005中存储的离线支付程序，并执行以下步骤：

[0053] 在与交易服务器连接成功时，若接收到在线支付请求，则判断所述待处理信息库中是否存在未同步的UTXO消耗记录；

[0054] 若所述待处理信息库中存在未同步的UTXO消耗记录，则将所述未同步的UTXO消耗记录同步至所述交易服务器，并在同步完成时进行在线支付。

[0055] 进一步的，所述在接收到离线支付指令时，根据所述离线支付指令和所述UTXO生成对应的UTXO消耗记录的步骤包括：

[0056] 在接收到离线支付指令时，判断所述离线支付指令包括的支付金额是否小于预设支付阈值，和/或判断所述付款端在预设周期内的离线支付指令接收次数是否小于预设接收阈值；

[0057] 若所述支付金额小于预设支付阈值，和/或所述离线支付指令接收次数小于预设接收阈值，则根据所述离线支付指令和所述UTXO生成对应的UTXO消耗记录。

[0058] 本发明实施例涉及的投保方法还应用于收款端，该收款端也可以是手机、智能手环、平板电脑、可穿戴设备等。

[0059] 对于收款端的硬件结构，可参照上述付款端的硬件结构，即收款端可以包括处理器(例如CPU)、通信总线、用户接口、网络接口、存储器。对于处理器(例如CPU)、通信总线、用户接口、网络接口，其功能与付款端中对应部分的功能类似。对于存储器部分，包括操作系统、网络通信模块以及离线支付程序；收款端的操作系统可与付款端的操作系统相同，也可以是采用不同的操作系统；网络通信模块则主要用于连接交易服务器和其它移动端进行数据通信；而处理器可以调用存储器1005中存储的离线支付程序，并执行以下步骤：

[0060] 在接收到付款端发送的UTXO消耗记录时，根据所述UTXO消耗记录包括的付款端身份信息验证所述付款端是否可信；

[0061] 若所述付款端可信，则向所述付款端返回对应的确认信息，并将所述UTXO消耗记录存储至待处理信息库中；

[0062] 在与交易服务器连接成功时，将所述待处理信息库中的UTXO消耗记录同步至所述交易服务器，以更新所述收款端的个人数字资产账户。

[0063] 进一步的，处理器还可以调用存储器1005中存储的离线支付程序，并执行以下步骤：

[0064] 根据已同步的UTXO消耗记录生成对应入账UTXO。

[0065] 基于上述付款端和收款端的硬件结构，提出本发明数字资产的离线支付方法的各

实施例。

[0066] 本发明实施例提供了一种数字资产的离线支付方法。

[0067] 参照图2,图2为本发明数字资产的离线支付方法第一实施例的流程示意图。

[0068] 本实施例中,所述数字资产的离线支付方法应用于付款端,所述付款端的本地至少存储有一个未消耗的交易输出UTXO,所述数字资产的离线支付包括以下步骤:

[0069] 步骤S10,在接收到离线支付指令时,根据所述离线支付指令和所述UTXO生成对应的UTXO消耗记录,所述离线支付指令包括收款端的收款地址,所述UTXO消耗记录包括付款端身份信息。

[0070] 随着终端技术的发展,移动支付已经成为了日常生活中一种重要的支付方式。目前,市面上的移动支付方案大多是采用在线支付方式,这种在线支付需要终端设备连接网络才能使用。然而这种支付方式的缺点也是显而易见的,当用户处于网络状况较差环境、甚至没有网络的情况下(比如地铁、偏远山区等),就无法进行支付,这就给用户带来了不便。对此,本实施例提出一种数字资产的离线支付方案,移动终端可在本地存储部分资产信息,在进行离线支付使用这些本地资产信息进行支付交易。

[0071] 本实施例中,为了描述的方便,用于付款的付款端可称为A端,用于收款的收款端可称为B端;A端和B端均以手机为例进行说明。A端网络正常、并与交易服务器连接成功时,通过A端所安装的数字资产钱包客户端,可查看到A端的个人数字资产账户信息,该个人数字资产账户信息是全网同步的。同时,A端的本地还存储有未消耗的交易输出(Unspent Transaction Output,UTXO),该UTXO代表了个人数字资产账户中的部分资产;本实施例中在进行离线交易时,仅能通过该UTXO进行,也就是说,该UTXO也可认为是A端的离线交易资产。值得说明的是,A端中可以是仅存储有一个UTXO,也可以两个以上(此处"以上"包括本数,下同)的UTXO,每个UTXO所代表的金额可以不同的;例如,如图3所示,图3为本实施例A端转账前本地存储示意图,在离线支付开始前,A端的本地UTXO列表存储有4个UTXO,分别记为$UTXO_{A1}$、$UTXO_{A2}$、$UTXO_{A3}$和$UTXO_{A4}$,所代表的金额分别为1000元、2000元、3000元和4000元;此外,A端中还设置有待处理信息库,该待处理信息库可用于存储交易记录,其中UTXO和待处理信息库的作用在后续的实施例中进行说明。

[0072] 本实施例中,当支付用户需要通过A端在离线状态(即不使用网络,或不连接交易服务器)下向B端进行支付时,可在A端进行操作,通过扫描B端所提供的二维码、或者是通过NFC(Near Field Communication,近距离无线通讯技术)、又或者是蓝牙、无线热点等方式与B端建立点对点的通信连接,并触发离线支付指令,输入相关的支付金额。而在于B端建立点对点的通信连接时,A端也会获取到B端的通信地址,即收款地址,且该收款地址会存在与该离线支付指令中。A端在接收到该离线支付指令时,将会根据该离线支付指令中的支付金额查询本地的UTXO表,从而获取UTXO的相关信息,然后选择一个或两个以上的UTXO,用以进行转账;在选择了某一个或两个以上的UTXO时,A端将根据所选择的UTXO和离线支付指令生成对应的UTXO消耗记录,该消耗记录包括了所选择的UTXO支付后的变化情况。例如,本实施例中A端要向B端离线支付3500元,则在如图3所示的UTXO列表中,A选择使用$UTXO_{A4}$,并生成了$UTXO_{A4}$的消耗记录,该消耗记录的表示形式可以为A4→B4+A5(即代表$4UTXO_{A4}\rightarrow UTXO_{B4}+UTXO_{A5}$),其中$UTXO_{A5}$代表的金额为500元,$UTXO_{B4}$代表的金额为3500元;同时,对于该消耗记录,A端还会添加A端的身份信息(如签名、证书等)用以证明A端的付款者身份。当然该消耗

记录还可以根据实际使用情况，添加其它内容。

[0073] 进一步的，在于B端建立点对点的通信连接时，A端还会获取到B端的身份信息(如证书、签名等)；A端首先会根据该身份信息对B端进行验证，判断B端是否可信；若B端可信，A端才会根据离线支付指令和UTXO生成对应的UTXO消耗记录。

[0074] 步骤S20，根据所述收款地址将所述UTXO消耗记录发送至所述收款端；

[0075] 本实施例中，在得到$UTXO_{A4}$的消耗记录时，A端将会获取B端的收款地址；该收款地址可以是A端与B端的建立点对点连接时B端的通信地址。在获取到该收款地址时，A端会把该$UTXO_{A4}$的消耗记录发送至B端，以供B端进行确认。此时，该$UTXO_{A4}$的消耗记录也可认为是A端向B端发出的交易请求，从而将A端的个人数字资产账户中的部分资产转移至B端的个人数字资产账户中。B端在接收到该$UTXO_{A4}$的消耗记录时，将根据其中的A端身份信息对A端的身份进行验证，判断其是否可信；当然对B端的操作用户而言，还可以判断其支付金额是否满足约定要求。当B端确认A端的身份可信时，将会向A端返回对应的确认信息(该确认信息也含有B端身份信息，以供A端验证B端身份)，以表示确认支付。

[0076] 步骤S30，在接收到所述收款端返回的确认信息时，根据所述UTXO消耗记录更新所述UTXO，获得二次UTXO，并将所述UTXO消耗记录存储至待处理信息库中；

[0077] 本实施例中，当A端接收到B端返回的确认信息时，即可根据该确认信息对UTXO列表中的$UTXO_{A4}$，将其替换为$UTXO_{A5}$(即二次UTXO)，其中$UTXO_{A5}$代表的金额为500元；同时，A端还会将$UTXO_{A4}$的消耗记录存储到A端的待处理信息库中，具体如图4所示，图4为本实施例A端转账后、同步前的本地存储示意图。此时，A端本地的UTXO列表中的UTXO分别为$UTXO_{A1}$、$UTXO_{A2}$、$UTXO_{A3}$和$UTXO_{A5}$。此时，可认为A端向B端的离线支付动作完成，双方达成了支付的合意并进行了对应的记录。

[0078] 步骤S40，在与交易服务器连接成功时，将所述待处理信息库中的UTXO消耗记录同步至所述交易服务器，以更新所述付款端的个人数字资产账户。

[0079] 本实施例中，虽然A端与B端之间达成了支付的合意并进行了对应的记录，但是该记录并未没有与交易服务器同步，因此并未改变交易服务器(或是数字资产网络)的个人资产情况，对此，当A端恢复与交易服务器的连接时，A端需要将待处理信息库中的$UTXO_{A4}$消耗记录同步至交易服务器中，从而使得交易服务器根据该$UTXO_{A4}$消耗记录对A端的个人数字资产账户情况进行更新。当A端在完成$UTXO_{A4}$消耗记录记录的同步时，即可将该$UTXO_{A4}$从待处理信息库中删除，具体如图5所示，图5为本实施例A端在UTXO消耗记录同步后本地存储示意图；当然A端也可以不将$UTXO_{A4}$消耗记录删除，而是对其同步状态进行标记。此外，交易服务器根据UTXO对A端的个人数字资产账户进行更新的同时，也可以同时对B端的个人数字资产进行更新；当然也可以是仅对A端的数字资产信息进行更新。而在实际中，为了保证数字资产网络的有序性，避免欺诈的发生，A端在于交易服务器进行UTXO同步时，往往还需要将A端的身份信息和B端的身份信息共同发送至交易服务器；交易服务器在首先会根据这些身份信息验证收款端身份、付款端身份的合法性、以及要同步的UTXO的合法性后，才会更新个人数字资产账户。

[0080] 进一步的，如果A端在通过消耗$UTXO_{A4}$进行离线支付，并将$UTXO_{A4}$更新替换为$UTXO_{A5}$后，为了降低离线资产多次交易带来的潜在危险性，保证各个用户的资产安全，对于新生成$UTXO_{A5}$(二次UTXO)，将会对其进行一定的离线使用限制。具体的，A端在获取$UTXO_{A5}$，并将

$UTXO_{A4}$的消耗记录存储至待处理信息库后，如果再次接收了离线支付指令，则首先A端判断待处理信息库中$UTXO_{A4}$消耗记录是否已经同步至交易服务器；如果该$UTXO_{A4}$消耗记录已经同步至交易服务器中，则可认为$UTXO_{A5}$已经被交易服务器所认可和记录的，此时可允许使用该$UTXO_{A5}$进行离线支付，具体的离线支付过程可参照$UTXO_{A4}$的消耗过程，此处不再赘述；而如果该$UTXO_{A4}$消耗记录没有同步至交易服务器中，则认为$UTXO_{A5}$尚未被交易服务器所认可和记录的，此时为了保证各个用户的资产安全，A端将拒绝使用$UTXO_{A5}$进行离线支付，即限定$UTXO_{A5}$的离线使用，此时A端将使用其它的UTXO进行离线支付，或直接返回离线支付功能锁定提示。

[0081] 再进一步的，为了降低离线支付带来的潜在危险性，保证各个用户的资产安全，在A端恢复网络后，还可以对其在线支付功能进行限制，以使其及时进行UTXO消耗记录的同步。具体的，A端在获取$UTXO_{A5}$，并将$UTXO_{A4}$的消耗记录存储至待处理信息库后，如果A端与交易服务器连接成功了，并在与交易服务器连接成功的情况下接收到了在线支付请求，则A端首先会判断待处理信息库中是否存在有任何未同步至服务器的消耗记录(包括但不局限于$UTXO_{A4}$消耗记录)；如果待处理信息库中存储任何未同步的消耗记录，则A端首先会将这些未同步的UTXO消耗记录同步至交易服务器中，以进行个人账户的更新，在同步完成时才会根据在线支付请求进行在线支付，从而对离线支付后的在线支付功能进行限制，保护数字资产账户的安全。

[0082] 本实施例中，付款端在接收到离线支付指令时，根据所述离线支付指令和本地UTXO生成对应的UTXO消耗记录，所述离线支付指令包括收款端的收款地址，所述UTXO消耗记录包括付款端身份信息；根据所述收款地址将所述UTXO消耗记录发送至所述收款端；在接收到所述收款端返回的确认信息时，根据所述UTXO消耗记录更新所述UTXO，获得二次UTXO，并将所述UTXO消耗记录存储至待处理信息库中；在与交易服务器连接成功时，将所述待处理信息库中的UTXO消耗记录同步至所述交易服务器，以更新所述付款端的个人数字资产账户。通过以上方式，本实施例的付款端可通过本地存储的资产信息实现离线支付操作和支付记录，并在网络恢复时根据相关的支付记录完成数字资产账户的更新变动，解决网络状态差或无网络时无法进行移动支付的问题，为用户的工作和生活提供了方便，提升了用户的使用体验。

[0083] 进一步的，在上述图2所示的数字资产的离线支付方法第一实施例中，所述步骤S10还包括：

[0084] 步骤S11，在接收到离线支付指令时，判断所述离线支付指令包括的支付金额是否小于预设支付阈值，和/或判断所述付款端在预设周期内的离线支付指令接收次数是否小于预设接收阈值；

[0085] 步骤S12，若所述支付金额小于预设支付阈值，和/或所述离线支付指令接收次数小于预设接收阈值，则根据所述离线支付指令和所述UTXO生成对应的UTXO消耗记录。

[0086] 本实施例中，为了降低离线支付带来的潜在危险性，保证各个用户的资产安全，还可以对移动支付端(A端)中UTXO的读写权限进行控制，从而对离线支付进行一定的限制。

[0087] 具体的，在本实施例中可以是对离线支付的金额进行限制。当A端在接收到离线支付指令时，首先会根据该离线支付指令中包括的支付金额，然后判断该支付金额是否小于预设支付阈值，其中该预设支付阈值可以是交易服务器预先设置并同步至各付款端中(当

然交易服务器也可以为不同的付款端设置不同的预设支付阈值)，也可以是由A端所有者进行设置；如果该支付金额小于预设支付阈值，则A端会认为本次离线支付满足要求，此时A端才会根据该离线支付指令和本地的UTXO生成对应的UTXO消耗记录，并进行后续的离线支付步骤；而如果该支付金额等于或大于预设支付阈值，则A端会认为本次离线支付不满足要求，可能会导致危险情况的发生，此时A端将不会执行离线支付的各步骤，并进行对应的安全提示。当然，在以支付金额为维度对离线支付功能的使用进行把控和限制的同时，对于该预设支付阈值，可以是单次支付时的单次安全支付阈值，也可以是多次支付的累计安全支付阈值，也可以是将单次支付的安全支付阈值和多次支付的累计安全支付阈值进行结合，从而对离线支付功能的使用进行把控和限制。

[0088] 此外，本实施例中还可以是对离线支付功能的使用次数进行限制。当A端在接收到离线支付指令时，首先会统计A端在预设周期内接收到离线支付指令的次数，然后判断该离线支付指令接收次数是否小于预设接收阈值，其中该预设周期和预设接收阈值可以是交易服务器预先设置并同步至各移动支付端中(当然交易服务器也可以为不同的移动支付端设置不同的预设周期和/或预设接收阈值)，也可以是由A端所有者进行设置的；如果A端在预设周期内的离线支付指令接收次数小于该预设接收阈值，则A端会认为本次离线支付满足要求，此时A端才会根据该离线支付指令和本地的UTXO生成对应的UTXO消耗记录，并进行后续的离线支付步骤；而如果A端在预设周期内的离线支付指令接收次数等于或大于该预设接收阈值，则A端会认为本次离线支付不满足要求，可能会导致危险情况的发生，此时A端将不会执行离线支付的各步骤，并进行对应的安全提示。

[0089] 值得说明的是，在具体实施中，也可以是将上述两种方式结合使用，或是配合其它的离线支付限制方式，以保护各用户的资产安全。

[0090] 参照图6，图6为本发明数字资产的离线支付方法第二实施例的流程示意图。

[0091] 本实施例中的离线支付方法应用于收款端，所述数字资产的离线支付方法包括以下步骤：

[0092] 步骤S50，在接收到付款端发送的UTXO消耗记录时，根据所述UTXO消耗记录包括的付款端身份信息验证所述付款端是否可信；

[0093] 本实施例中，用于付款的付款端可称为A端，用于收款的收款端可称为B端；对于A端的基本配置、以及其功能介绍可参照上述图2所示实施例，此处不在赘述。对于B端可参照图7，图7为B端在接收A端的离线转账前的存储示意图，其中B端在本地也存储有UTXO列表，该UTXO列表用于记录B端的UTXO信息，其中包括有$UTXO_{B1}$、$UTXO_{B2}$和$UTXO_{B3}$；此外，B端中也设置有待处理信息库，该待处理信息库可用于存储交易记录。当A端通过使用其本地的$UTXO_{A4}$开始向B端进行离线支付时(A端的离线支付流程可参照图2所示实施例)，会向B端发送对应的$UTXO_{A4}$消耗记录，其中该$UTXO_{A4}$消耗记录中包括有A端的身份信息(如A端的签名、证书等)。B端在接收到该$UTXO_{A4}$消耗记录时，将会根据其中的身份信息验证A端是否可信(如验证A端的签名是否正确等)；当然B端还可以根据该$UTXO_{A4}$消耗记录显示对应的支付金额，以供B端的操作用户判断其支付金额是否满足约定要求。

[0094] 步骤S60，若所述付款端可信，则向所述付款端返回对应的确认信息，并将所述UTXO消耗记录存储至待处理信息库中；

[0095] 本实施例中，B端在判断A端可信时，将会向A端返回对应的确认信息，以表示确认

支付;此外,B端还会将该$UTXO_{A4}$消耗记录存储至B端本地的待处理信息库中,具体如图8所示,图8为本实施例B端转账后、同步前的本地存储示意图。当然,B端在判断A端身份可信的同时,还需要判断$UTXO_{A4}$消耗记录显示对应的支付金额正确,才会返回对应的确认信息。此时,可认为A端向B端的离线支付动作完成,双方达成了支付的合意并进行了对应的记录。而对于B端所返回的确认信息中,还可包括有B端的身份信息(如B端的签名、证书等),以供A端根据该身份信息验证B端的身份、或该确认信息是否由B端发出。

[0096] 步骤S70,在与交易服务器连接成功时,将所述待处理信息库中的UTXO消耗记录同步至所述交易服务器,以更新所述收款端的个人数字资产账户。

[0097] 本实施例中,虽然A端与B端之间达成了支付的合意并进行了对应的记录,但是该记录并未没有与交易服务器同步,因此并未改变交易服务器(或是数字资产网络)的个人数字资产情况,对此,当B端恢复与交易服务器的连接时,B端需要将待处理信息库中的$UTXO_{A4}$消耗记录同步至交易服务器中,从而使得交易服务器根据该$UTXO_{A4}$消耗记录对B端的个人数字资产账户情况进行更新。此外,交易服务器根据UTXO对B端的个人数字资产账户进行更新的同时,也可以同时对A端的个人数字资产进行更新;也可以是仅对B端的数字资产信息进行更新。而在实际中,为了保证数字资产网络的有序性,避免欺诈的发生,A端在于交易服务器进行UTXO同步时,往往还需要将A端的身份信息和B端的身份信息共同发送至交易服务器;交易服务器在首先会对根据这些身份信息验证收款端身份、付款端身份的合法性、以及要同步的UTXO的合法性后,才会更新个人数字资产账户。

[0098] 进一步的,在B端完成$UTXO_{A4}$消耗记录的同步时,还可以在本地的UTXO列表中生成对应的$UTXO_{B4}$;同时,对于待处理信息库中的$UTXO_{A4}$消耗记录,B端可以是将其删除,具体如图9所示,图9为B端在UTXO消耗记录同步后本地存储示意图。当然,B端在进行UTXO消耗记录同步后,也可以不删除UTXO消耗记录,而是对其同步状态进行标记。

[0099] 值得说明的是,作为A端与B端在离线支付过程中,在对UTXO消耗记录进行处理后,其对各自本地的UTXO的处理具有一定区别。对于A端,其作为付款端,A端在接收到B端的确认信息后,即使当前没有与交易服务器连接,也会根据UTXO消耗记录对本地的UTXO进行更新操作(将原$UTXO_{A4}$更新为$UTXO_{A5}$);而对于B端,其作为收款端,B端向A端返回确认信息时,并不是立即在本地生成对应的入账UTXO($UTXO_{B4}$),而是需要将UTXO同步至交易服务器中才会在本地生成对应的入账UTXO。如此,假如A端是欺诈方,B端被欺诈,由于B端是在与服务器同步后才能够生成对应的入账UTXO并用以进行离线支付,这样就可以在于服务器同步时及时发现A端欺诈的情况,而B端不是与A端(欺诈者)进行离线支付时立即生成入账UTXO并用以进行离线支付,避免了单次欺诈引起的多方受害的情况,从而降低欺诈所带来的危及范围。

[0100] 在具体实施中,上述A端和B端,其在不同的离线支付场合中可能是作为了不同的角色存在。例如在上述的A端与B端之间的离线支付过程中,A端是作为付款端,B端是作为收款端;而A端在与另一移动终端C端进行离线支付时,A端可以是作为收款端;类似的,B端在与另一移动终端D端进行离线支付时,B端可以是作为付款端。

[0101] 此外,本发明实施例还提供一种存储介质。

[0102] 本发明存储介质上存储有离线支付程序,其中所述离线支付程序被处理器执行时,实现如上述应用于付款端的数字资产的离线支付方法的步骤。

[0103] 其中，离线支付程序被执行时所实现的方法可参照本发明数字资产的离线支付方法的各个实施例，此处不再赘述。

[0104] 此外，本发明实施例还提供一种存储介质。

[0105] 本发明存储介质上存储有离线支付程序，其中所述离线支付程序被处理器执行时，实现如上述应用于收款端的数字资产的离线支付方法的步骤。

[0106] 其中，离线支付程序被执行时所实现的方法可参照本发明数字资产的离线支付方法的各个实施例，此处不再赘述。

[0107] 需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者系统不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者系统所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者系统中还存在另外的相同要素。

[0108] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0109] 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上述实施例方法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，但很多情况下前者是更佳的实施方式。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如上所述的一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，空调器，或者网络设备等)执行本发明各个实施例所述的方法。

[0110] 以上仅为本发明的优选实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

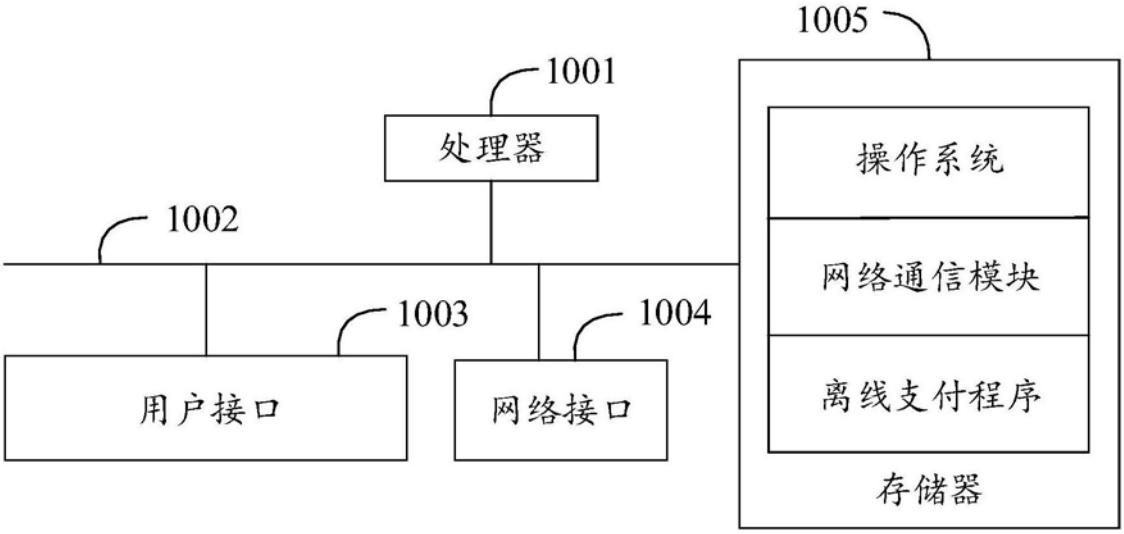

1005
1001
处理器
操作系统
1002
网络通信模块
1003
1004
离线支付程序
用户接口
网络接口
存储器

图1

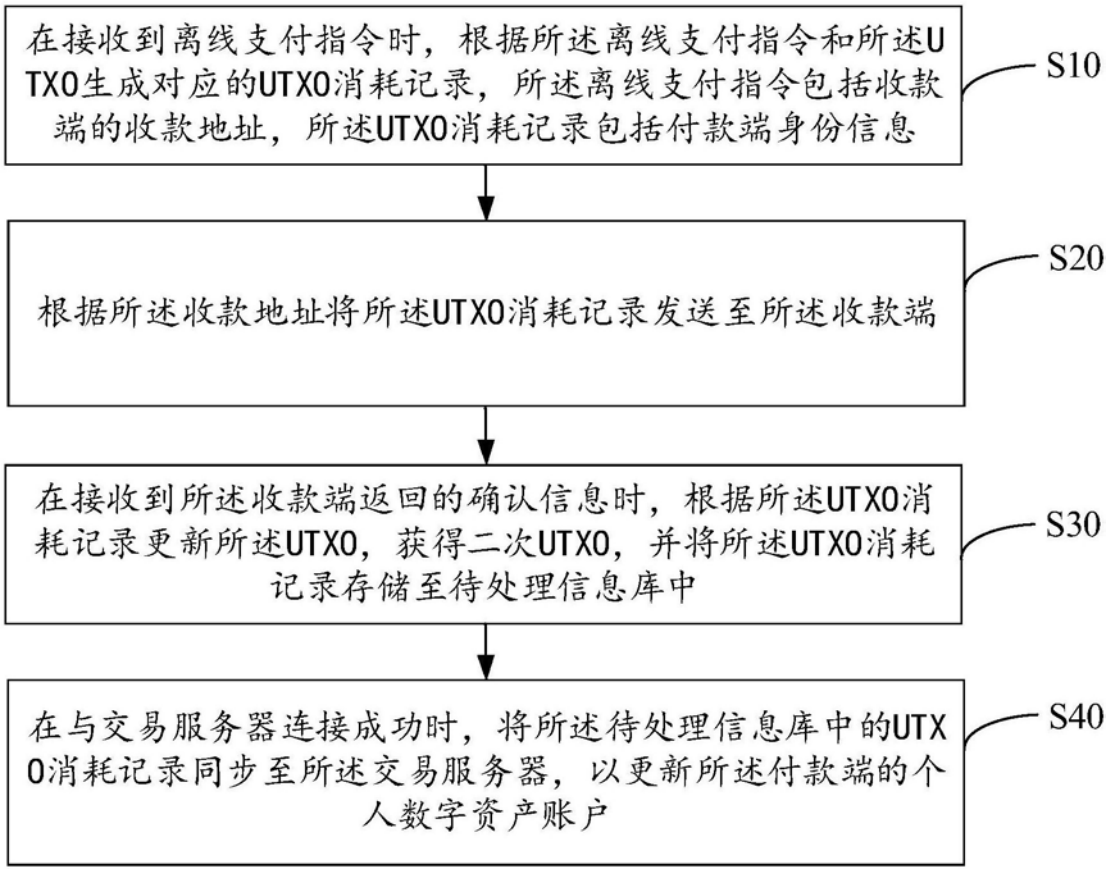

在接收到离线支付指令时，根据所述离线支付指令和所述UTXO生成对应的UTXO消耗记录，所述离线支付指令包括收款端的收款地址，所述UTXO消耗记录包括付款端身份信息
S10
根据所述收款地址将所述UTXO消耗记录发送至所述收款端
S20
在接收到所述收款端返回的确认信息时，根据所述UTXO消耗记录更新所述UTXO，获得二次UTXO，并将所述UTXO消耗记录存储至待处理信息库中
S30
在与交易服务器连接成功时，将所述待处理信息库中的UTXO消耗记录同步至所述交易服务器，以更新所述付款端的个人数字资产账户
S40

图2

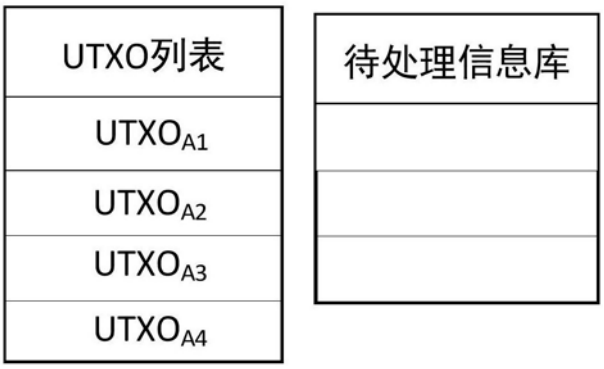

UTXO列表
UTXO$_{A1}$
UTXO$_{A2}$
UTXO$_{A3}$
UTXO$_{A4}$
待处理信息库

图3

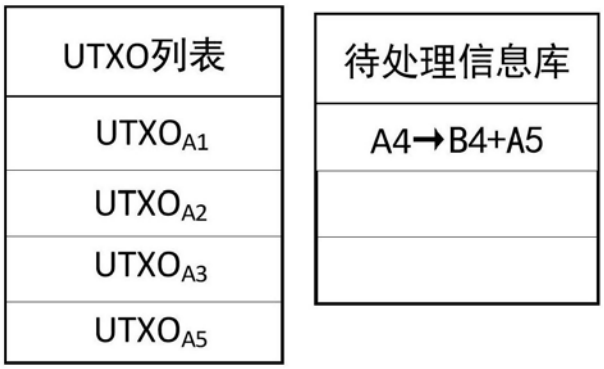

UTXO列表
UTXO$_{A1}$
UTXO$_{A2}$
UTXO$_{A3}$
UTXO$_{A5}$
待处理信息库
A4→B4+A5

图4

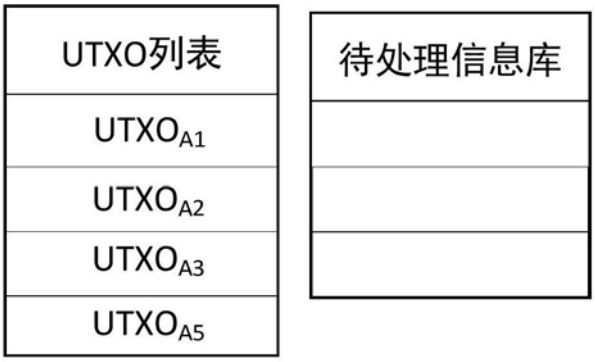

UTXO列表
UTXO$_{A1}$
UTXO$_{A2}$
UTXO$_{A3}$
UTXO$_{A5}$
待处理信息库

图5

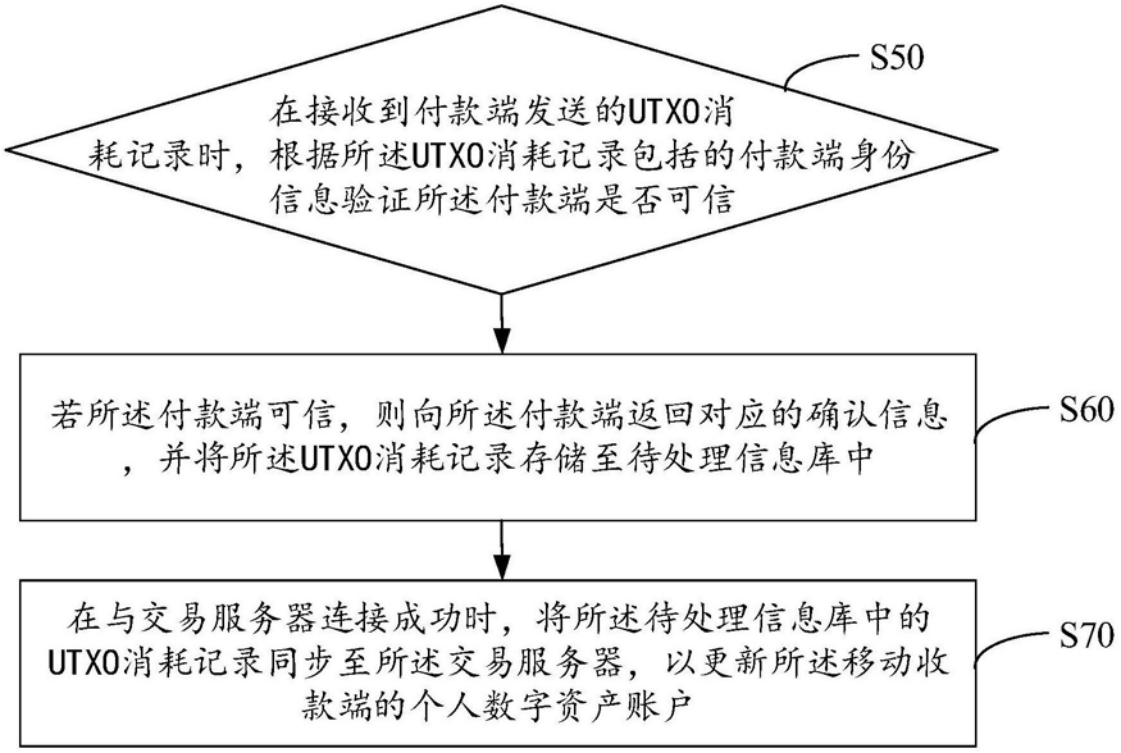

S50
在接收到付款端发送的UTXO消耗记录时，根据所述UTXO消耗记录包括的付款端身份信息验证所述付款端是否可信
若所述付款端可信，则向所述付款端返回对应的确认信息，并将所述UTXO消耗记录存储至待处理信息库中
S60
在与交易服务器连接成功时，将所述待处理信息库中的UTXO消耗记录同步至所述交易服务器，以更新所述移动收款端的个人数字资产账户
S70

图6


UTXO列表
待处理信息库
$UTXO_{B1}$
$UTXO_{B2}$
$UTXO_{B3}$

图7

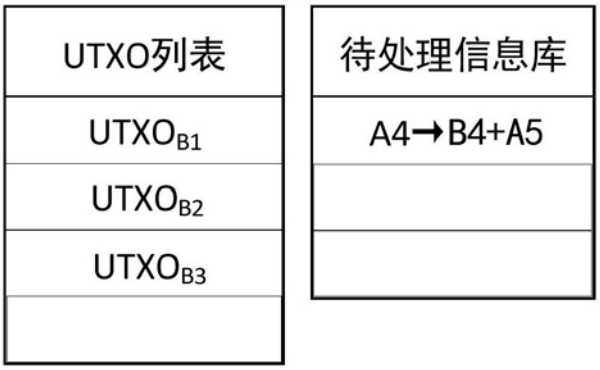

UTXO列表
UTXO$_{B1}$
UTXO$_{B2}$
UTXO$_{B3}$
待处理信息库
A4→B4+A5

图8


UTXO列表
UTXO$_{B1}$
UTXO$_{B2}$
UTXO$_{B3}$
UTXO$_{B4}$
待处理信息库

图9