清亦华知识产权代理事务所
Tsingyihua Intellectual Property LLC

北京市海淀区北洼路 45 号东配楼二层（邮编：100048）
Tel: 86-10-8288 6568
Fax:86-10-8260 0083
Email: ip@thuip.com
Web:www.thuip.com

清亦华知识产权代理事务所检索报告

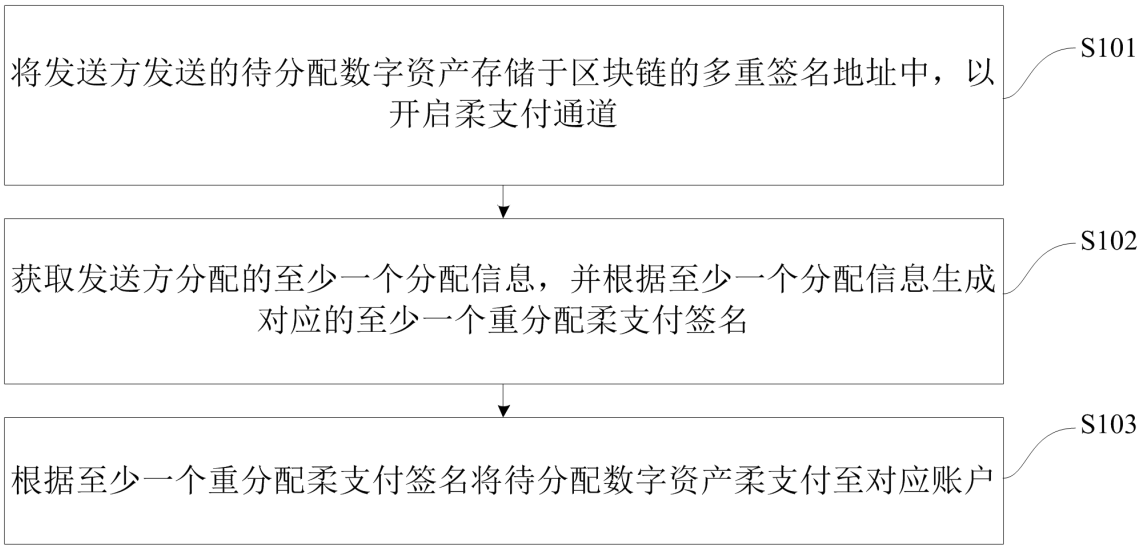
	检索过程和检索结果	
贵司卷号：ML-2018-001	清亦华卷号：PIDE3181370	
专利名称	一种多重签名的柔性区块链支付方法及网络系统	
发明点及解决的技术问题简述	本申请提供一种多重签名的柔性区块链支付方法及网络系统，通过发送方多重签名地址中发送有延迟返回的待分配数字资产形成柔支付通道，接受方可以验证签名是否正确来通过通道确认收到柔支付，并将这些通道有机的整合建立成柔支付网络，从而实现任意两陌生人间不需直接建立柔支付通道，解决了现有的区块链支付效率低、灵活性差，且十分繁琐，成本高的问题 。	
分类号	H04L29/	
关键词	多重签名　　区块链支付　　区块链	
检索式及文献数量	多重签名　AND 区块链支付	0
	多重签名 AND 区块链	4
	区块链支付 AND 区块链	9
接近的对比文献列表	对比文件 1：CN 107038578 A - 一种基于区块链的数据交易平台中多重签名交易信息处理方法 对比文件 2：CN 107682331 A - 一种基于区块链的物联网身份认证方法 对比文件 3：CN 107370606 A - 一种基于区块链的微博多重签名方法	

检索说明、初步结论以及提出申请的建议和意见	在检索到的对比文件中： 对比文件 1 提出了一种基于区块链的数据交易平台中多重签名交易信息处理方法，买家和卖家的每个在自身客户端生成交易密钥对，数据交易平台为每次交易过程生成分配单次交易密钥对；卖家通过数据交易平台在区块链上发布待交易数据；买家提交交易申请后，根据三方公钥生成中间地址，付款后资金转到中间地址，卖家在收到资金写入区块链后将数据加密发送买家；买家收到数据后若确认交易则双方签名，资金转到卖家地址；若存在异议，则由数据交易平台判定，根据判定结果决定将资金转至买家或卖家。 对本文件 1 公开了特殊的区域链方式对双方交易时的数据和交易信息进行处理，同时使得数据交易平台也无法挪用交易资金。但是并没有公开本申请中通过发送方多重签名地址中发送有延迟返回的待分配数字资产形成柔支付通道的技术特征。 对比文件 2 中提出了一种基于区块链的物联网身份认证方法，实体凭自身拥有的密钥调用智能合约，完成在身份认证系统中的注册；每个实体可以调用智能合约以设置访问策略来限制其他实体对其访问并形成物联网的信任网络；一个实体访问另一个实体的数据时需要向智能合约申请令牌以获得访问资格，智能合约根据实体间信任网络中被访问实体设置的访问策略核对发起访问的实体是否有访问资格，如果有则生成令牌返回给发起访问的实体；否则返回申请令牌失败。 对比文件 2 公布了去除了身份认证过程中的中心化的权威机构，保证了身份认证与数据访问的记录不会被恶意篡改，策略执行结果不会被人为操纵，对本申请没有技术性启示。 对比文件 3 提供了一种基于区块链的微博多重签名方法，包括以下步骤：1、用户注册，得到一对公私钥以及一个用来交易的由私钥生成的地址；2、m 个用户一起采用各自经过步骤 S1 得到的地址来创建多重签名地址；3、创建发送微博的交易，利用 OP_RETURN 操作符，使得在交易中插入所要发送的信息；OP_RETURN 操作符通过步骤 S2 创建的多重签名地址来操作；多重签名地址支持 n of m 的权限；4、在场的用户轮流对这笔微博交易进行数字签名，最后得到至少 n 个签名之后，广播此微博交易，交易成功之后，微博交易将永远的记录在区块链之中。 对比文件 3 公布了一种基于区块链的微博多重签名方法对本申请没有技术性启示。
	上述对比文件（1-3）未直接公开通过发送方多重签名地址中发送有延迟返回的待分配数字资产形成柔支付通道，接受方可以验证签名是否正确来通过通道确认收到柔支付，并将这些通道有机的整合建立成柔支付网络的技术特征。因此，本申请具有新颖性。

说明书摘要

本发明公开了一种多重签名的柔性区块链支付方法、装置及电子设备，其中，方法包括：将发送方发送的待分配数字资产存储于区块链的多重签名地址中，以开启柔支付通道；获取发送方分配的至少一个分配信息，并根据至少一个分配信息生成对应的至少一个重分配柔支付签名；根据至少一个重分配柔支付签名将待分配数字资产柔支付至对应账户。该方法可以通过将待分配数字资产发送到区块链的多重签名地址上，并通过建立柔支付网络，而实现双方不需要直接建立柔支付通道便可以实现柔支付，不但有效保证支付的可靠性和安全性，而且具有支付成本较低、确认时间短、灵活性较高等优点，有效提升用户使用体验，且简单易实现。

摘要附图


将发送方发送的待分配数字资产存储于区块链的多重签名地址中，以开启柔支付通道
S101
获取发送方分配的至少一个分配信息，并根据至少一个分配信息生成对应的至少一个重分配柔支付签名
S102
根据至少一个重分配柔支付签名将待分配数字资产柔支付至对应账户
S103

权利要求书

1、一种多重签名的柔性区块链支付方法，其特征在于，包括以下步骤：

将发送方发送的待分配数字资产存储于区块链的多重签名地址中，以开启柔支付通道；

获取所述发送方分配的至少一个分配信息，并根据所述至少一个分配信息生成对应的至少一个重分配柔支付签名；以及

根据所述至少一个重分配柔支付签名将所述待分配数字资产柔支付至对应账户。

2、根据权利要求 1 所述的多重签名的柔性区块链支付方法，其特征在于，还包括：

在将发送方发送的待分配数字资产存储于区块链的多重签名地址中之前，获取所述接收方签名的延时转回签名，并根据所述接收方签名的延时转回签名关闭所述柔支付通道，以将所述多重签名地址中的部分或全部待分配数字资产在预设时间戳或预设区块高度后转回所述发送方；或

根据所述接收方签名的分配信息发送的区块链广播关闭所述柔支付通道，按所述分配信息进行分配所述待分配数字资产。

3、根据权利要求 1 所述的多重签名的柔性区块链支付方法，其特征在于，所述区块链的多重签名地址为 2of2 模式多重签名地址或者 2of3 模式多重签名地址，以在所述发送方和所述接受方均签名，或者所述发送方、所述接收方和第三方中任意两方签名后，支付所述待分配数字资产。

4、根据权利要求 2 所述的多重签名的柔性区块链支付方法，其特征在于，还包括：

通过多个柔支付节点之间建立双向或者单向的所述柔支付通道，以生成柔支付网络。

5、根据权利要求 4 所述的多重签名的柔性区块链支付方法，其特征在于，所述柔支付节点分包括至少一个中心节点和多个第一用户节点，所述多个第一用户节点均与所述至少一个中心节点相连，且所述多个第一用户节点之间不相连，以生成星型拓扑的柔支付网络。

6、根据权利要求 4 所述的多重签名的柔性区块链支付方法，其特征在于，所述柔支付节点包括中转根节点、多个柔网关节点和多个第二用户节点，其中，所述中转根节点与所述多个柔网关节点相连，所述多个柔网关节点与所述多个第二用户节点相连，且各柔网关节点相互之间不相连，所述多个第二用户节点的每个用户节点与所述中转根节点、柔网关节点和其它第二用户节点均可相连，以生成分层树状拓扑的柔支付网络。

7、一种多重签名的柔性区块链支付装置，其特征在于，包括：

存储模块，用于将发送方发送的待分配数字资产存储于区块链的多重签名地址中，以开启柔支付通道；

处理模块，用于获取所述发送方分配的至少一个分配信息，并根据所述至少一个分配信息生成对应的至少一个重分配柔支付签名；以及

支付模块，用于根据所述至少一个重分配柔支付签名将所述待分配数字资产柔支付至对应账户。

8、根据权利要求 7 所述的多重签名的柔性区块链支付装置，其特征在于，还包括：

控制模块，用于在将发送方发送的待分配数字资产存储于区块链的多重签名地址中之前，获取所述接收方签名的延时转回签名，并根据所述接收方签名

的延时转回签名关闭所述柔支付通道，以将所述多重签名地址中的部分或全部待分配数字资产在预设时间戳或预设区块高度后转回所述发送方，或在需要时，根据所述接收方签名的分配信息发送的区块链广播关闭所述柔支付通道，按所述分配信息进行分配所述待分配数字资产。

9、一种电子设备，包括：

存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时实现如权利要求 1-6 中任一所述的多重签名的柔性区块链支付方法。

10、一种计算机可读存储介质，其上存储有计算机程序，其特征在于，所述程序被处理器执行时实现如权利要求 1-6 中任一所述的多重签名的柔性区块链支付方法。

说明书

多重签名的柔性区块链支付方法、装置及电子设备

技术领域

本发明涉及互联网金融技术领域，特别涉及一种多重签名的柔性区块链支付方法、装置及电子设备。

背景技术

目前，区块链技术在飞速地发展中，以其去中心化、方便快捷、高安全性、成本较低等优势，引起了金融领域甚至整个社会的关注。

其中，区块链的具体重要技术落地应用之一就是区块链支付，然而随着区块链支付行业的发展新的问题出现，一方面为了维持区块链数据的简捷和去中心化而限制了区块大小，采用市场竞争手续费高者优先打包确认的模式，即为了尽快确认往往在繁忙时会需要支付较高的交易手续费，有时甚至高到难以接受。另一方面，由于区块链的全球全节点同步确认的特点，需要区块数据在全球传播的时间，因此即使足够高手续费，也需要约十几分钟来确认，难以满足一些高频快速交易的应用场景的需求。

在相关技术中，为了降低使用的区块链支付的成本，且加速确认时间提高灵活性，往往使用闪电网络、雷电网络和侧链技术等解决上述问题，但是由于过于复杂繁琐，均导致未能成熟落地，尤其是相关技术的支付方法存在支付成本较高、确认时间较长、灵活性较差等一系列问题，无法满足越来越多的区块链支付需求，降低了用户使用体验，亟待改进。

发明内容

本发明旨在至少在一定程度上解决相关技术中的技术问题之一。

为此，本发明的第一个目的在于提出一种多重签名的柔性区块链支付方法，该方法可以有效保证支付的可靠性和安全性，而且具有支付成本较低、确认时间短、灵活性较高等优点，有效提升用户使用体验，且简单易实现。

本发明的第二个目的在于提出一种多重签名的柔性区块链支付装置。

本发明的第三个目的在于提出一种电子设备。

本发明的第四个目的在于提出一种计算机可读存储介质。

为达到上述目的，本发明第一方面实施例提出了一种多重签名的柔性区块链支付方法，包括以下步骤：将发送方发送的待分配数字资产存储于区块链的多重签名地址中，以开启柔支付通道；获取所述发送方分配的至少一个分配信息，并根据所述至少一个分配信息生成对应的至少一个重分配柔支付签名；根据所述至少一个重分配柔支付签名将所述待分配数字资产柔支付至对应账户。

本发明实施例的多重签名的柔性区块链支付方法，可以通过将待分配数字资产发送到区块链的多重签名地址上，并通过建立柔支付网络，而实现双方不需要直接建立柔支付通道便可以实现柔支付，不但有效保证支付的可靠性和安全性，而且具有支付成本较低、确认时间短、灵活性较高等优点，有效提升用户使用体验，且简单易实现。

另外，根据本发明上述实施例的多重签名的柔性区块链支付方法还可以具有以下附加的技术特征：

进一步地，在本发明的一个实施例中，上述方法还包括：在将发送方发送的待分配数字资产存储于区块链的多重签名地址中之前，获取所述接收方签名

的延时转回签名，并根据所述接收方签名的延时转回签名关闭所述柔支付通道，以将所述多重签名地址中的部分或全部待分配数字资产在预设时间戳或预设区块高度后转回所述发送方；或根据所述接收方签名的分配信息发送的区块链广播关闭所述柔支付通道，按所述分配信息进行分配所述待分配数字资产。

进一步地，在本发明的一个实施例中，所述区块链的多重签名地址为 2of2 模式多重签名地址或者 2of3 模式多重签名地址，以在所述发送方和所述接受方均签名，或者所述发送方、所述接收方和第三方中任意两方签名后，支付所述待分配数字资产。

进一步地，在本发明的一个实施例中，上述还包括：通过多个柔支付节点之间建立双向或者单向的所述柔支付通道，以生成柔支付网络。

进一步地，在本发明的一个实施例中，所述柔支付节点分包括至少一个中心节点和多个第一用户节点，所述多个第一用户节点均与所述至少一个中心节点相连，且所述多个第一用户节点之间不相连，以生成星型拓扑的柔支付网络。

进一步地，在本发明的一个实施例中，所述柔支付节点包括中转根节点、多个柔网关节点和多个第二用户节点，其中，所述中转根节点与所述多个柔网关节点相连，所述多个柔网关节点与所述多个第二用户节点相连，且各柔网关节点相互之间不相连，所述多个第二用户节点的每个用户节点与所述中转根节点、柔网关节点和其它第二用户节点均可相连，以生成分层树状拓扑的柔支付网络。

为达到上述目的，本发明第二方面实施例提出了一种多重签名的柔性区块链支付装置包括：存储模块，用于将发送方发送的待分配数字资产存储于区块链的多重签名地址中，以开启柔支付通道；处理模块，用于获取所述发送方分配的至少一个分配信息，并根据所述至少一个分配信息生成对应的至少一个重

分配柔支付签名；支付模块，用于根据所述至少一个重分配柔支付签名将所述待分配数字资产柔支付至对应账户。

本发明实施例的多重签名的柔性区块链支付装置，可以通过将待分配数字资产发送到区块链的多重签名地址上，并通过建立柔支付网络，而实现双方不需要直接建立柔支付通道便可以实现柔支付，不但有效保证支付的可靠性和安全性，而且具有支付成本较低、确认时间短、灵活性较高等优点，有效提升用户使用体验，且简单易实现。

另外，根据本发明上述实施例的多重签名的柔性区块链支付装置还可以具有以下附加的技术特征：

进一步地，在本发明的一个实施例中，上述装置还包括：控制模块，用于在将发送方发送的待分配数字资产存储于区块链的多重签名地址中之前，获取所述接收方签名的延时转回签名，并根据所述接收方签名的延时转回签名关闭所述柔支付通道，以将所述多重签名地址中的部分或全部待分配数字资产在预设时间戳或预设区块高度后转回所述发送方，或在需要时，根据所述接收方签名的分配信息发送的区块链广播关闭所述柔支付通道，按所述分配信息进行分配所述待分配数字资产。

本发明第三方面实施例提出了一种电子设备，包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述处理器执行所述程序时实现如第一方面实施例所述的多重签名的柔性区块链支付方法。

本发明第四方面实施例提出了一种计算机可读存储介质，其上存储有计算机程序，所述程序被处理器执行时实现如第一方面实施例所述的多重签名的柔性区块链支付方法。

本发明附加的方面和优点将在下面的描述中部分给出，部分将从下面的描

述中变得明显，或通过本发明的实践了解到。

附图说明

本发明上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中：

图 1 为根据本发明一个实施例的多重签名的柔性区块链支付方法的流程图；

图 2 为根据本发明一个实施例的柔性区块链支付方法的柔支付通道原理示意图；

图 3 为根据本发明一个实施例的用户 A 与用户 B 之间建立的柔支付通道示意图；

图 4 为根据本发明一个实施例的柔网关 X 与用户间建立的柔支付通道示意图；

图 5 为根据本发明一个实施例的根柔网关与各柔网关及用户间建立柔支付网络示意图；

图 6 为根据本发明一个实施例的多重签名的柔性区块链支付装置的结构示意图；

图 7 为根据本发明一个实施例的电子设备的结构示意图。

附图标记说明：

发送方 1，接受方 2，多重签名地址 3，延时转回签名 4 和重分配柔支付签名 5。

具体实施方式

下面详细描述本发明的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，旨在用于解释本发明，而不能理解为对本发明的限制。

下面参照附图描述根据本发明实施例提出的多重签名的柔性区块链支付方法、装置及电子设备，首先将参照附图描述根据本发明实施例提出的多重签名的柔性区块链支付方法。

图 1 是本发明一个实施例的多重签名的柔性区块链支付方法的流程图。

如图 1 所示，该多重签名的柔性区块链支付方法包括以下步骤：

在步骤 S101 中，将发送方发送的待分配数字资产存储于区块链的多重签名地址中，以开启柔支付通道。

可以理解的是，发送方通过区块链发送数字资产到区块链的多重签名地址中。多重签名地址为通过多重签名技术生成的地址，且需要由发送方和接受方都签名同意后，才可以交易向外支付，仅仅一方的签名则无法动用多重签名地址里的数字资产，从而可以有效保障数字资产的安全。也就是说，本发明实施例首先将待分配数字资产存储至多重签名地址中，然后再开启柔支付通道，从而可以有效保障发送方的数字资产的安全，提高数字资产的安全性，有效保证支付的便捷性和可靠性。

具体地，柔支付通道底层会具有通道时间参数，以及单向支付的特性，通道的发送方和接收方在开启通道时可以根据实际需要自由的设置柔支付通道的通道维持时间，从而使得柔支付通道更加灵活，有效适应不同应用场合需求，进而可以有效提高支付的灵活性，而支付会在实现时需要的底层技术支持不多

（例如，仅仅只需要多重签名和延迟签名交易技术，而不需要智能合约技术或隔离验证技术等支持），更加简单便捷简捷，从而使得柔支付通道简捷可靠，进而有效提高支付的可靠性。

综上，本发明实施例可以在将发送方数字资产存入多重签名地址中后，开通柔支付通道，多重签名地址能够保障数字资产的安全，柔支付通道能够保障支付通道的安全可靠，进而能够保障支付的安全可靠，有效提高支付的安全性和可靠性，简单易实现。

其中，在本发明的一个实施例中，区块链的多重签名地址可以为 2of2 模式多重签名地址，以在发送方和接受方均签名后，支付待分配数字资产。可以理解的是，区块链多重签名地址可以为 2of2 模式多重签名地址，需要发送方和接受方都签名才能动用区块链多重签名地址中的数字资产，从而有效保障数字资产的安全性，提高支付的可靠性。

此外，在本发明的另一个实施例中，区块链多重签名地址也可以为 2of3 模式多重签名地址，除了发送方和接受方外还有第三方，需要收集发送方、接受方和第三方中的任意两者的签名即可动用区块链多重签名地址中的数字资产。其中，第三方可以视为发送方或者接受方中的一方，即可有不只一个发送方或不只一个接受方，从而可以灵活的进行签名的组合，有效提高支付的安全性和可靠性。

举例而言，如果只有发送方和接收方，在任何一方想动用区块链多重签名地址中的数字资产时，由于多重签名地址是通过多重签名技术生成的地址，需要由发送方和接受方都签名同意后，才可以交易向外支付，因此，必须双发都要签字在能够动用区块链多重签名地址中的数字资产，而本发明实施例在发送方和接收方的基础上增加了第三方，第三方可以视为发送

方或者接受方中的一方，即可有不只一个发送方或不只一个接受方，因此，在动用区块链多重签名地址中的数字资产时，就可以通过第三方的签字而分配数字资产，从而大大提高了支付的安全性和可靠性，简单便捷。

在步骤 S102 中，获取发送方分配的至少一个分配信息，并根据至少一个分配信息生成对应的至少一个重分配柔支付签名。

可以理解的是，发送方签名分配多重签名地址中发送方和接受方占有的币量，并将签名好的字串发给接受方作为柔支付通道内实现的柔支付，从而有效保障支付的安全性和可靠性的同时，有效提升支付的便捷性和实用性，从而通过签名好的字串进行柔支付，接收方只需要确认发送方的签名是否正确即可，确认时间短，有效提高便捷性和实用性，提高支付效率，大大提升了用户的使用体验。其中，一个分配信息一般只能生成一个重分配柔支付签名，是多个更新的分配信息生成多个重分配签名

具体而言，发送方将币发到多重签名地址中，然后靠多次重新分配币量柔支付签名，将多重签名地址中的币越来越多的签名分配给接受方，接受方只要确认发送方的签名正确，从而大大简化了支付流程，在保障支付安全可靠的同时，简单易实现。

在步骤 S103 中，根据至少一个重分配柔支付签名将待分配数字资产柔支付至对应账户。

可以理解的是，在接受方确认发送方的签名正确之后，本发明实施例便可以根据确认过的柔支付签名进行柔支付，从而有效提高支付的便捷性。其中，根据通过刷新分配信息，新旧分配之间的差额相当于支付，即为柔支付。

进一步地，在本发明的一个实施例中，本发明实施例的方法还包括：在将

发送方发送的待分配数字资产存储于区块链的多重签名地址中之前，获取接收方签名的延时转回签名，并根据接收方签名的延时转回签名关闭柔支付通道，以将多重签名地址中的部分或全部待分配数字资产在预设时间戳或预设区块高度后转回发送方；或根据接收方签名的分配信息发送的区块链广播关闭柔支付通道，按分配信息进行分配待分配数字资产。

可以理解的是，延时转回签名最好是在“待分配数字资产发送区块链的多重签名地址”之前就已经签名好。发送方有这个签名后，才可以更加放心地将币发到多重签名地址，否则一旦接收方不关闭或者消失，那么难以关闭柔支付通道拿回分配资产中自己的资产。

发送方将数字资产存放在需要多重签名才能支付的区块链多重签名地址中，且接受方签名同意将多重签名地址中的部分或全部币在某时间戳或区块高度后转回发送方。其中，某时间戳或区块高度，具体可由发送方或者接受方来选择设定，柔支付通道内签名好的支付字串，可以交给平台进行管理维护防止丢失，从而避免损失在多重签名地址未支付的币，有效保障用户数字资产的安全，提升用户的信任感，从而适用于多种使用场合。

其中，延时转回签名是一种时间戳交易或者区块高度交易，即使签名正确，也需要在当前时间戳超过交易中设的时间戳，或者区块高度高于交易中设的区块高度，才可以在区块链上广播确认，有效提高支付的可靠性。

另外，接受方可以验证签名是否正确来确认收到柔支付币量，之后可选择增加自己签名后区块链广播关闭柔支付通道或者不广播继续维持柔支付通道的开启状态，从而有效保障支付的可控性，保证接收方的使用意愿，有效提升使用体验。

其中，在已经有了发送方分配和签名之后，接受方再补充自己签名后即可

在区块链上广播，按分配信息进行执行。而这一步是非每次柔支付都需要的，接收方可以根据实际情况进行设置。

下面以一个具体实施例对本发明的多重签名的柔性区块链支付方法进行详细描述。

在本发明的一个具体实施例中，如图 2 所示，柔支付底层原理是，发送方 1 和接受方 2，生成只有两方签名才可以转出的多重签名地址 3，从而可以有效保障数字资产的安全。然后在接受方 2 签名同意延时转回签名 4 的前提下，发送方 1 将币发到多重签名地址 3 中，从而可以有效保障发送方的数字资产的安全，提高数字资产的安全性，有效保证支付的便捷性和可靠性。然后靠多次重新分配币量柔支付签名 5，将多重签名地址 3 中的币越来越多的签名分配给接受方 2，接受方 2 只要确认发送方 1 的签名正确即可，从而有效保障支付的安全性和可靠性的同时，有效提升支付的便捷性和实用性，确认时间短，有效提高便捷性和实用性，提高支付效率，大大提升了用户的使用体验。在时间戳或区块高度到来前，没有必要立即到区块链上广播，若接受方 2 补充签名后区块链上广播交易即关闭了柔支付通道，从而有效保障支付的可控性，保证接收方的使用意愿，有效提升使用体验。而若接受方 2 因意外忘记或其它原因而一直不去广播，在时间戳或区块高度到来之后，发送方 1 也可发布延时转回签名 4 的交易，收回多重签名地址 3 中的全部币，避免损失在多重签名地址 3 中自己未支付的币，从而有效保障用户数字资产的安全，提升用户的信任感，从而适用于多种使用场合。

因此，柔支付通道底层会具有通道时间参数，以及单向支付的特性。柔支付通道的通道时间可根据需要自由的设置更加灵活，适应不同应用场合需求，有效提高柔支付通道的适用性。而单向支付会在实现时更加简捷，自动将之前

的分配交易无用化，因接受方也不会去将对自己不利的之前的分配交易补充签名发布广播，因此不需要额外再进行作废之前分配交易的设计，更简捷可靠，简单易实现。

进一步地，在本发明的一个实施例中，本发明实施例的方法还包括：通过多个柔支付节点之间建立双向或者单向的柔支付通道，以生成柔支付网络。

可以理解的是，本发明实施例通过柔支付节点相互之间建立双向或者单向柔支付通道，并通过柔支付通道使节点之间建立连接，形成一定拓扑形状的柔支付网络。其中，各节点之间相互平等，任意节点之间都有可能连接，从而形成网状拓扑形状的高去中心化的柔支付网络，从而实现了两个陌生人之间不需要直接建立柔支付通道，就可以实现秒速确认和几乎零手续费的柔支付区块链数字资产，大大降低了支付的成本，缩短了支付时间，简单便捷。

下面以一个具体实施例对本发明的多重签名的柔性区块链支付方法中的柔性网络的原理进行详细描述。

具体而言，如图 3 所示，因为在基础原理层是单向的，而实际的支付需要中多会需要双向支付，因此需要将单向拓展为双向。方法也很简单，A 到 B 建立个通道，再建立另外一个 B 到 A 通道即可。

例如，用户 A 与用户 B 之间建立双向柔支付通道的参考步骤：

第一步：扫码或网络连接或者直接内置，获得对方地址的公钥数据，用交换顺序来生成两个 2of2 多重签名分配地址，A 到 B 用一个，B 到 A 用另外一个。

第二步：构造自己发向分配地址和从分配地址延时回自己的两个交易，发送给对方。

第三步：签名延时转回签名后发给对方，收到且验证通过后可广播自己发向分配地址的交易，形成双向柔支付通道。

进一步地，在本发明的一个实施例中，柔支付节点分包括至少一个中心节点和多个第一用户节点，多个第一用户节点均与至少一个中心节点相连，且多个第一用户节点之间不相连，以生成星型拓扑的柔支付网络。

可以理解的是，柔支付节点分为中心节点和用户节点，所有用户节点与中心节点相连接，用户节点之间不连接，从而形成星型拓扑支付网络，其中，中心节点可以为一个或者多个，若为多个中心节点相互之间相互连接形成一个整体。从而就可以实现秒速确认和几乎零手续费的柔支付区块链数字资产，大大降低了支付的成本，缩短了支付时间，简单便捷。

具体而言，如图 4 所示，柔网关与用户间建立的柔支付通道要先建立有柔支付通道，才能进行柔支付。本发明实施例通过有些特殊的柔支付节即为柔网关节点建立柔支付网络，柔网关节点同时会和很多用户节点之间建立柔支付通道，从而大大降低柔支付网络的复杂性，有效提高支付的效率，简单易实现。

举例而言，如图 4 所示，若 A、B、C、D 四个用户节点都与柔网关 X 建立了双向柔支付通道，那么可以通过柔网关的中转可轻易实现这四个用户间的任意收发柔支付。例如 A 要支付给 D，那么 A 先支付给 X，X 再支付给 D 即可。柔支付可以中间收取少量地手续费作为中转服务回报，也可以免费提供中转服务来吸引更多用户来建立柔支付通道，毕竟柔支付通道内的柔支付本身的支付成本几乎为零，从而大大降低支付成本，提升用户的使用体验，而柔网关连接的用户越多其价值越大。其中，数字资产交易平台，钱包平台，算力矿池，资讯社区平台，各币种资源甚至知名个人等等都可以成为广义的柔网关，只要能有足够多的人愿意与其建立柔支付通道，从而大大提升了柔性网络的实用性。

进一步地，在本发明的一个实施例中，柔支付节点包括中转根节点、多个柔网关节点和多个第二用户节点，其中，中转根节点与多个柔网关节点相连，多个柔网关节点与多个第二用户节点相连，且各柔网关节点相互之间不相连，多个第二用户节点的每个用户节点与中转根节点、柔网关节点和其它第二用户节点均可相连，以生成分层树状拓扑的柔支付网络。

可以理解的是，节点分为中转根节点，柔网关节点和用户节点。其中，中转根节点与柔网关节点，以中转根节点为中心星型拓扑连接，一般仅有一个，且在出现特殊情况时，可共识认可下将某个柔网关节点升级为中转根节点。柔网关节点有多个，与用户节点和中转根节点相链接，但各柔网关节点相互之间一般不连接。用户节点一般可与柔网关节点连接，也可以直接和中转根节点连接，用户节点相互之间也可以直接连接，从而形成分层树状拓扑的柔支付网络。本发明实施例将中转根节点、各柔网关及用户联系起来，从而实现秒速确认和几乎零手续费的柔支付区块链数字资产，大大降低了支付的成本，缩短了支付时间，简单便捷。

具体而言，如图 5 所示，各个柔网关及其用户就像是局域网，要实现全球范围的互联，需要一个连接各柔网关得节点，称为中转根节点。本发明实施例采用树状的拓扑模式，中转根节点是树根树干，各柔网关是各个树分枝，而用户就是树叶。分三层当系统过于庞大而中转根节点较大压力时，也可考虑四层或更多层，即柔网关下再增设一些子柔网关。不过一般还是维持三层会更简捷高效，这种构架下任意两人最多中间中转三次即可进行柔支付，从而有效提升支付的便捷性和实用性，支付效率高，大大提升用户的使用体验。

例如，图 5 中 A 想柔支付付给 F，可通过 A 付 X，X 付 T，T 付 Y，Y

付 F 实现。需要注意的是，要尽量减少且最好能完全杜绝柔网关之间相互连接，否则会导致路由情况增多而增加系统的复杂度和降低中转根节点的地位，甚至演变成点对点的网状拓扑的柔支付网络，而失去树状拓扑的一些优势。

根据本发明实施例提出的多重签名的柔性区块链支付方法，通过发送方多重签名地址中发送有延迟返回的待分配数字资产形成柔支付通道，从而可以有效保障发送方的数字资产的安全，提高数字资产的安全性，有效保证支付的便捷性和可靠性；接受方可以验证签名是否正确来通过通道确认收到柔支付，确认时间短，有效提高便捷性和实用性，提高支付效率，大大提升了用户的使用体验；接受方可补充签名后通过区块链广播关闭柔支付通道或不广播继续维持柔支付通道，从而有效保障支付的可控性，保证接收方的使用意愿，有效提升使用体验，并将这些通道有机的整合建立成柔支付网络，从而实现任意两陌生人间不需直接建立柔支付通道，就可以实现秒速确认和几乎零手续费的柔支付区块链数字资产，不仅提升了用户的信任感，而且大大降低了支付成本，支付效率高，简单易实现，适用于多种使用场合。

其次参照附图描述根据本发明实施例提出的多重签名的柔性区块链支付装置。

图 6 是本发明一个实施例的多重签名的柔性区块链支付装置的结构示意图。

如图 6 所示，该多重签名的柔性区块链支付装置 10 包括：存储模块 100、处理模块 200 和支付模块 300。

其中，存储模块 100 用于将发送方发送的待分配数字资产存储于区块链的多重签名地址中，以开启柔支付通道。处理模块 200 用于获取发送方分配的至

少一个分配信息，并根据至少一个分配信息生成对应的至少一个重分配柔支付签名。支付模块 300 用于根据至少一个重分配柔支付签名将待分配数字资产柔支付至对应账户。本发明实施例的装置 10 通过将待分配数字资产发送到区块链的多重签名地址上，智能的开启柔支付通道，发送方和接收方不需要直接建立柔支付通道便可以实现数字资产的分配和确认，从而有效提高区域链支付的灵活性和高效性，支付成本低，简单易实现。

进一步地，在本发明的一个实施例中，本发明实施例的装置 10 还包括：控制模块。其中，控制模块用于在将发送方发送的待分配数字资产存储于区块链的多重签名地址中之前，获取接收方签名的延时转回签名，并根据接收方签名的延时转回签名关闭柔支付通道，以将多重签名地址中的部分或全部待分配数字资产在预设时间戳或预设区块高度后转回发送方，或在需要时，根据接收方签名的分配信息发送的区块链广播关闭柔支付通道，按分配信息进行分配待分配数字资产。

需要说明的是，前述对多重签名的柔性区块链支付方法实施例的解释说明也适用于该实施例的多重签名的柔性区块链支付装置，此处不再赘述。

根据本发明实施例提出的多重签名的柔性区块链支付装置，通过发送方多重签名地址中发送有延迟返回的待分配数字资产形成柔支付通道，从而可以有效保障发送方的数字资产的安全，提高数字资产的安全性，有效保证支付的便捷性和可靠性；接受方可以验证签名是否正确来通过通道确认收到柔支付，确认时间短，有效提高便捷性和实用性，提高支付效率，大大提升了用户的使用体验；接受方可补充签名后区块链广播关闭柔支付通道或不广播继续维持柔支付通道，从而有效保障支付的可控性，保证接收方的使用意愿，有效提升使用体验，并将这些通道有机的整合建立成柔支付网络，从而实现任意两陌

生人间不需直接建立柔支付通道，就可以实现秒速确认和几乎零手续费的柔支付区块链数字资产，不仅提升了用户的信任感，而且大大降低了支付成本，支付效率高，简单易实现，适用于多种使用场合。

图 7 为本发明实施例提供的一种电子设备的结构示意图。

如图 7 所示，该电子设备包括：存储器 71、处理器 72 及存储在存储器 71 上并可在处理器 72 上运行的计算机程序。

处理器 72 执行程序时实现上述实施例中提供的多重签名的柔性区块链支付方法。其中，电子设备可以是电脑、手机、可穿戴设备等。

存储器 71 可能包含高速 RAM 存储器，也可能还包括非易失性存储器（non-volatile memory），例如至少一个磁盘存储器。处理器 72，用于执行程序时实现上述实施例的多重签名的柔性区块链支付方法。

进一步地，电子设备还包括：通信接口 73、存储器 71。

其中，通信接口 73 用于存储器 71 和处理器 72 之间的通信。存储器 71，用于存放可在处理器 72 上运行的计算机程序。

如果存储器 71、处理器 72 和通信接口 73 独立实现，则通信接口 73、存储器 71 和处理器 72 可以通过总线相互连接并完成相互间的通信。总线可以是 ISA（Industry Standard Architecture，工业标准体系结构）总线、PCI（PeripheralComponentInterconnect，外部设备互连）总线或 EISA（Extended Industry Standard Architecture，扩展工业标准体系结构）总线等。总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 5 中仅以一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

可选地，在具体实现时，如果存储器 71、处理器 72 及通信接口 73，集成在一块芯片上实现，则存储器 71、处理器 72 及通信接口 73 可以通过内部接

口完成相互间的通信。

处理器 72 可以是一个中央处理器（Central Processing Unit，简称 CPU），或者是特定集成电路（Application Specific Integrated Circuit，简称 ASIC），或者是被配置成实施本发明实施例的一个或多个集成电路。

本发明第四方面实施例提出了一种计算机可读存储介质，其上存储有计算机程序，当该程序被处理器执行时实现如前述实施例中的多重签名的柔性区块链支付方法。

本发明第五方面实施例提出了一种计算机程序产品，当计算机程序产品中的指令由处理器执行时，执行如前述实施例中的多重签名的柔性区块链支付方法。

此外，术语“第一”、“第二”仅用于描述目的，而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此，限定有“第一”、“第二”的特征可以明示或者隐含地包括至少一个该特征。在本发明的描述中，“多个”的含义是至少两个，例如两个，三个等，除非另有明确具体的限定。

在本发明中，除非另有明确的规定和限定，第一特征在第二特征 “上”或“下”可以是第一和第二特征直接接触，或第一和第二特征通过中间媒介间接接触。而且，第一特征在第二特征“之上”、“上方”和“上面”可是第一特征在第二特征正上方或斜上方，或仅仅表示第一特征水平高度高于第二特征。第一特征在第二特征“之下”、“下方”和“下面”可以是第一特征在第二特征正下方或斜下方，或仅仅表示第一特征水平高度小于第二特征。

在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、 “示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，

对上述术语的示意性表述不必须针对的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任一个或多个实施例或示例中以合适的方式结合。此外，在不相互矛盾的情况下，本领域的技术人员可以将本说明书中描述的不同实施例或示例以及不同实施例或示例的特征进行结合和组合。

尽管上面已经示出和描述了本发明的实施例，可以理解的是，上述实施例是示例性的，不能理解为对本发明的限制，本领域的普通技术人员在本发明的范围内可以对上述实施例进行变化、修改、替换和变型。

说明书附图

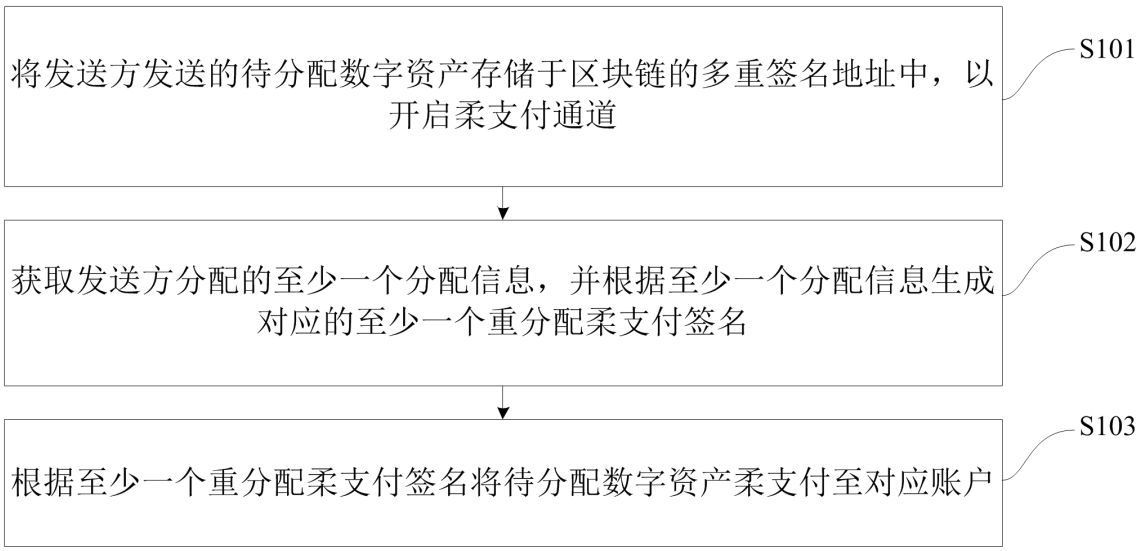

将发送方发送的待分配数字资产存储于区块链的多重签名地址中，以开启柔支付通道
S101
获取发送方分配的至少一个分配信息，并根据至少一个分配信息生成对应的至少一个重分配柔支付签名
S102
根据至少一个重分配柔支付签名将待分配数字资产柔支付至对应账户
S103

图 1

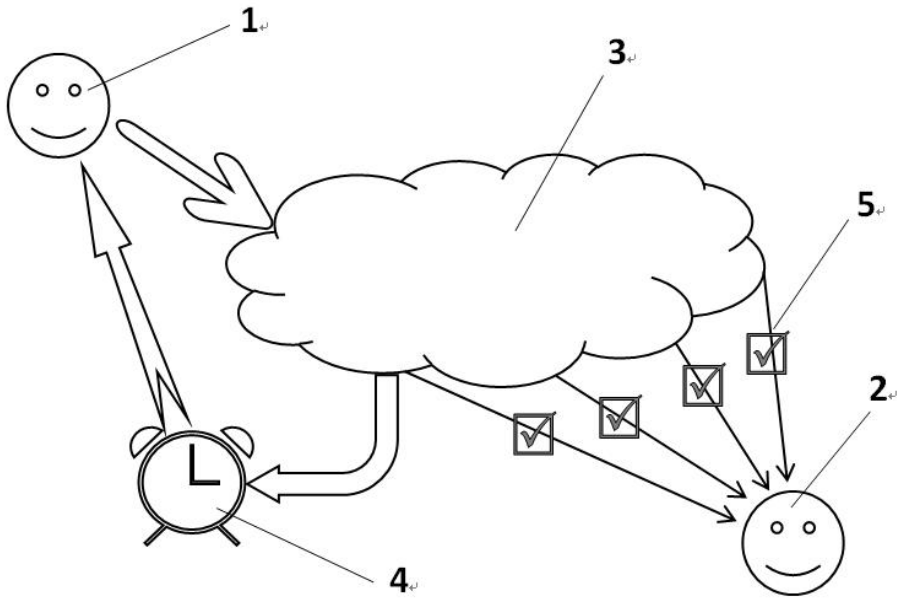

1
3
5
2
4

图 2

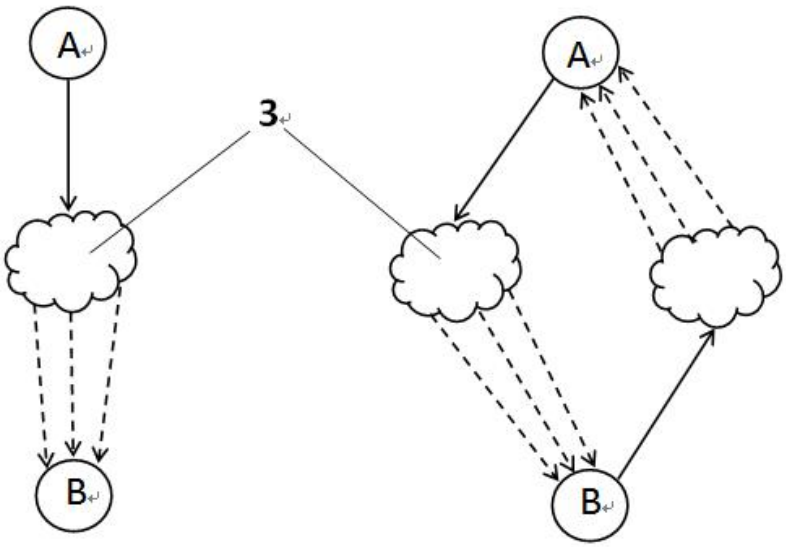


图 3

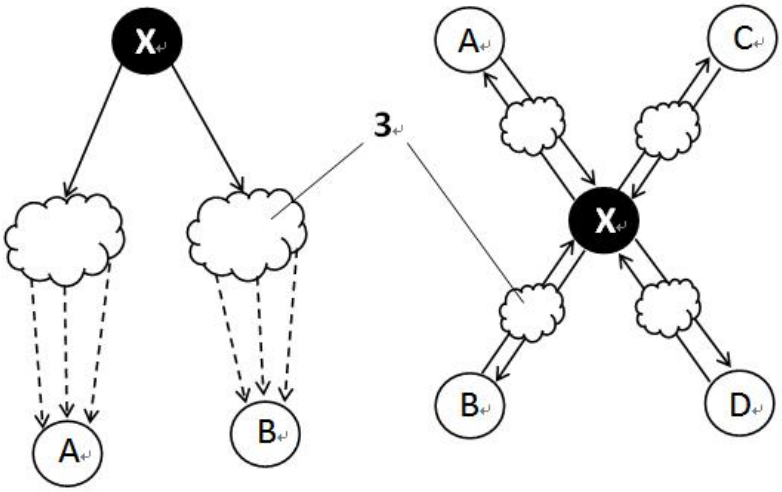


图 4

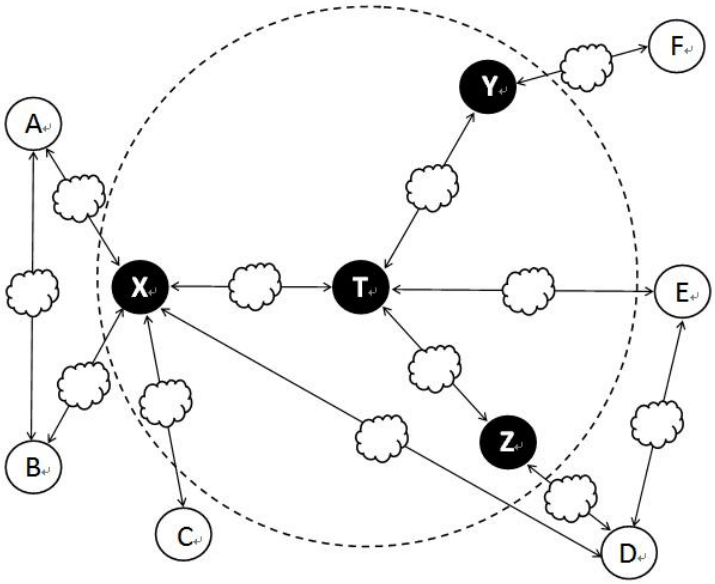


图 5

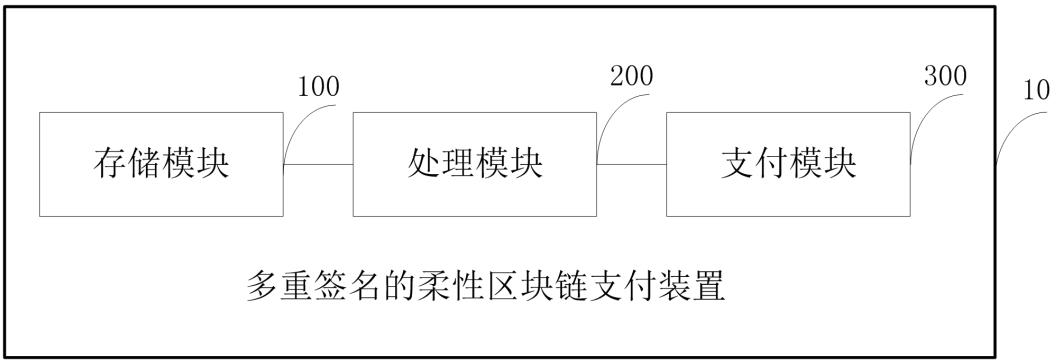


图 6

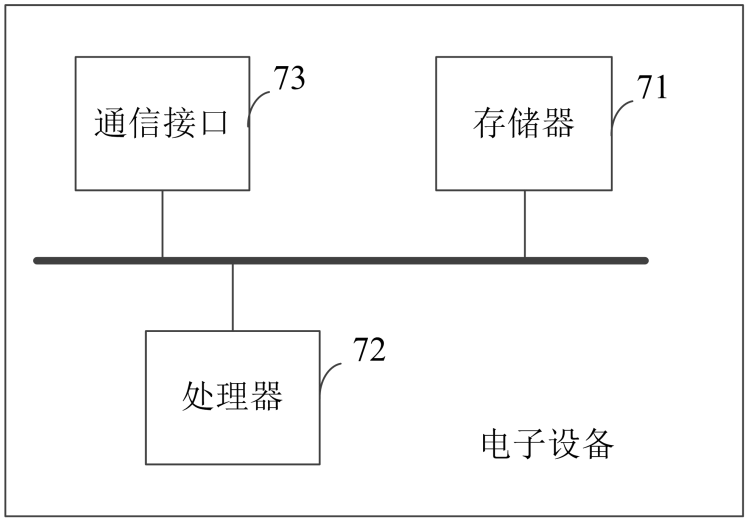


图 7