

基于区块链密钥的数据处理方法、装置、设备及存储介质

本申请要求于 2023 年 8 月 9 日提交中国专利局、申请号为 202310997066.1、申请名称为“基于区块链密钥的数据处理方法、装置、设备及存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及区块链技术领域，尤其涉及一种基于区块链密钥的数据处理方法、装置、设备及存储介质，该方法主要涉及数字资产管理技术，通过密钥管理方法与密钥使用方法实现签名处理。

背景技术

目前，随着区块链技术的发展，关于数字资产的应用越来越广泛，由于数字资产在进行业务交互时需要使用对应的密钥进行签名处理，因此数字资产若想成功进行业务交互需要生成安全且稳定的签名密钥。当前的密钥生成方法通常使用算法生成一对公私钥，进而通过私钥进行加密，通过私钥对应的公钥进行解密。当私钥破损或丢失时，数字资产将无法使用，因此当前使用的密钥签名方法增加了数字资产使用时的风险概率。

发明内容

本申请实施例提供一种基于区块链密钥的数据处理方法、装置、设备及存储介质，可以降低使用数字资产的风险概率。

本申请实施例一方面提供了一种基于区块链密钥的数据处理方法，该方法包括：

获取与 N 个客户端分别进行通信的通信信道，基于 N 个通信信道分别与 N 个客户端进行密钥分片协商，得到本地私钥分片和完整公钥；N 为大于 1 的正整数；完整公钥是本地私钥分片和 N 个目标私钥分片共同对应的唯一公钥；N 个目标私钥分片中的第 i 个目标私钥分片，是通过密钥分片协商后由 N 个客户端中的第 i 个客户端所独自持有的私钥分片；

接收 N 个客户端中的 M-1 个客户端发送的签名请求，获取 M-1 个签名请求中的身份关联信息；M 为基于完整公钥进行验签的私钥分片数量阈值，M 为小于等于 N+1 的正整数；

若 M-1 个签名请求中的身份关联信息均为合法身份信息，则将 M-1 个客户端中用于发起区块链业务的客户端，确定为目标客户端，获取目标客户端相关联的业务执行数据；

若业务执行数据符合目标客户端的身份关联信息对应的风险管理策略，则与 M-1 个客户端共同参与针对区块链业务的联合签名处理；联合签名处理所生成的联合签名结果是基于本地私钥分片和 M-1 个客户端分别持有的目标私钥分片共同生成，联合签名结果用于提供给目标客户端执行区块链业务。

本申请实施例一方面提供了一种基于区块链密钥的数据处理方法，该方法由用于发起区块链业务的目标客户端执行，该方法包括：

目标客户端获取分别与 N-1 个客户端以及服务端进行通信的通信信道，基于通信信道与服务端以及 N-1 个客户端进行密钥分片协商，得到目标客户端对应的目标私钥分片和完整公钥；N 为大于 1 的正整数；完整公钥是目标客户端对应的目标私钥分片、服务端私钥分片和 N-1 个客户端对应的目标私钥分片共同对应的唯一公钥；N-1 个客户端对应的目标私钥分片中的第 i 个目标私钥分片，是通过密钥分片协商后由 N-1 个客户端中的第 i 个客户端所独自持有的私钥分片；服务端私钥分片是通过密钥分片协商后由服务端所独自持有的私钥分片；

基于目标客户端对应的身份关联信息生成目标客户端对应的签名请求，将目标客户端对应的签名请求发送至服务端，以使服务端对接收到的 M-1 个签名请求中的身份关联信息进行合法身份验证；M-1 个签名请求包括目标客户端对应的签名请求；M 为基于完整公钥进行验签的私钥分片数量阈值，M 为小于等于 N+1 的正整数；

若检测到服务端确定 M-1 个签名请求中的身份关联信息均为合法身份信息，则向服务端发送目标客户端相关联的业务执行数据；

若业务执行数据符合目标客户端的身份关联信息对应的风险管理策略，则与发起签名请求的客户端以及服务端共同参与针对区块链业务的联合签名处理；联合签名处理所生成的联合签名结果是基于发起签名请求的客户端对应的目标私钥分片和服务端私钥分片共同生成，联合签名结果用于提供给目标客户端执行区块链业务。

本申请实施例一方面提供了一种基于区块链密钥的数据处理装置，该数据处理装置包括：

本地私钥分片获取模块, 用于获取与 N 个客户端分别进行通信的通信信道, 基于 N 个通信信道分别与 N 个客户端进行密钥分片协商, 得到本地私钥分片和完整公钥; N 为大于 1 的正整数; 完整公钥是本地私钥分片和 N 个目标私钥分片共同对应的唯一公钥; N 个目标私钥分片中的第 i 个目标私钥分片, 是通过密钥分片协商后由 N 个客户端中的第 i 个客户端所独自持有的私钥分片;

身份关联信息获取模块, 用于接收 N 个客户端中的 $M-1$ 个客户端发送的签名请求, 获取 $M-1$ 个签名请求中的身份关联信息; M 为基于完整公钥进行验签的私钥分片数量阈值, M 为小于等于 $N+1$ 的正整数;

目标客户端确定模块, 用于若 $M-1$ 个签名请求中的身份关联信息均为合法身份信息, 则将 $M-1$ 个客户端中用于发起区块链业务的客户端, 确定为目标客户端;

业务执行数据获取模块, 用于获取目标客户端相关联的业务执行数据;

第一联合签名模块, 用于若业务执行数据符合目标客户端的身份关联信息对应的风险管理策略, 则与 $M-1$ 个客户端共同参与针对区块链业务的联合签名处理; 联合签名处理所生成的联合签名结果是基于本地私钥分片和 $M-1$ 个客户端分别持有的目标私钥分片共同生成, 联合签名结果用于提供给目标客户端执行区块链业务。

其中, 本地私钥分片获取模块, 包括:

本地测试私钥生成单元, 用于随机生成用于进行密钥分片协商的本地测试私钥, 通过本地测试私钥对本地协商数据进行加密处理, 得到本地测试信息;

通信信道获取单元, 用于获取与 N 个客户端分别进行通信的通信信道, 通过每个通信信道向 N 个客户端发送本地测试信息;

目标解密数据获取单元, 用于接收 N 个客户端分别发送的目标测试公钥以及目标测试信息, 通过目标测试公钥对属于同一客户端的目标测试信息进行解密, 得到 N 个目标解密数据; 一个目标测试公钥是指一个客户端所生成的用于进行密钥分片协商的目标测试私钥对应的公钥, 一个目标测试信息是指在一个客户端中通过所生成的目标测试私钥对目标协商数据进行加密处理所得到的信息;

第一哈希结果确定单元, 用于基于本地测试私钥对应的本地测试公钥对本地测试信息进行解密, 得到本地解密数据, 将本地解密数据以及 N 个目标解密数据确定为第一哈希结果;

第二哈希结果获取单元, 用于对本地协商数据以及 N 个目标协商数据进行哈希运算, 得到第二哈希结果;

本地私钥分片确定单元, 用于若第一哈希结果与第二哈希结果相等, 则确定密钥协商成功, 将本地测试私钥确定为本地私钥分片;

完整公钥生成单元, 用于在与 N 个客户端进行密钥分片协商的过程中生成完整公钥。

其中, 数据处理装置, 还包括:

目标分片公钥获取模块, 用于获取 $M-1$ 个客户端分别对应的目标分片公钥; 一个客户端对应的目标分片公钥是基于该客户端对应的目标私钥分片所生成的;

签名验证模块, 用于通过 $M-1$ 个目标分片公钥分别对 $M-1$ 个客户端发送的分片签名结果进行签名验证, 得到 $M-1$ 个签名验证结果; 一个分片签名结果是指一个客户端通过该客户端对应的目标私钥分片对身份关联信息进行签名后的数据;

合法身份验证模块, 用于若 $M-1$ 个签名验证结果均为验证成功结果, 则对 $M-1$ 个客户端所发送的签名请求中的身份关联信息进行合法身份验证。

其中, $M-1$ 个客户端包括客户端 S_i , i 为小于或等于 $M-1$ 的正整数; 合法身份验证模块, 包括:

业务类型获取单元, 用于获取 $M-1$ 个客户端所关联发起的区块链业务的业务类型, 获取客户端 S_i 对应的身份关联信息中的身份标识以及身份特征数据;

身份验证策略确定单元, 用于确定业务类型所匹配的身份验证策略, 在身份标识以及身份特征数据中, 选取与身份验证策略所指示的验证维度匹配的数据, 作为待验证数据;

合法身份信息确定单元, 用于若待验证数据存在于身份数据库中, 则确定客户端 S_i 对应的签名请求中的身份关联信息为合法身份信息。

其中, 业务执行数据获取模块, 具体用于获取目标客户端的历史业务执行数据以及所发起的区块链业务中的目标业务执行数据, 将历史业务执行数据和目标业务执行数据确定为目标客户端相关联的业务执行数据;

其中, 数据处理装置, 还包括:

业务阈值设置模块, 用于对业务执行数据中的历史业务执行数据进行数据分析, 得到历史业务操作范

围，基于历史业务操作范围，设置业务阈值；

风险管理策略确定模块，用于若业务执行数据中的目标业务执行数据小于等于业务阈值，则确定业务执行数据符合目标客户端的身份关联信息对应的风险管理策略。

其中，数据处理装置，还包括：

地址风险检测模块，用于从业务执行数据中获取目标客户端对应的应用链上地址，对应用链上地址进行地址风险检测；

第一地址检测模块，用于若检测到应用链上地址存在于合法地址名单中，则确定业务执行数据符合目标客户端的身份关联信息对应的风险管理策略；

第二地址检测模块，用于若检测到应用链上地址不存在于合法地址名单中，则确定应用链上地址为风险性地址，禁止响应目标客户端所发起的区块链业务。

其中，M-1个客户端包括目标客户端；第一联合签名模块，包括：

服务端签名结果获取单元，用于接收目标客户端发送的经过目标客户端对应的目标私钥分片进行加密处理后的中间加密结果，通过本地私钥分片对接收到的中间加密结果进行签名，得到服务端签名结果；

联合签名结果生成单元，用于将服务端签名结果发送至目标客户端；服务端签名结果用于指示目标客户端生成联合签名结果。

其中，数据处理装置，还包括：

业务数据接收模块，用于接收目标客户端发送的待上链业务数据；待上链业务数据由区块链业务中的目标业务执行数据和联合签名结果组成；

业务数据转发模块，用于将待上链业务数据转发至区块链共识网络，以使区块链共识网络在共识过程中基于完整公钥对联合签名结果进行验签，在共识通过时，将目标业务执行数据所对应的执行结果数据存储至区块链账本中。

其中，数据处理装置，还包括：

目标业务地址生成模块，用于基于完整公钥生成目标业务地址；

待验证地址获取模块，用于获取N个客户端分别发送的待验证地址；一个客户端发送的待验证地址是基于完整公钥所生成的；

合法地址确定模块，用于若目标业务地址与N个待验证地址均相同，则确定目标业务地址为合法地址，且将目标业务地址确定为应用链上地址；

待验证地址删除模块，用于若N个待验证地址中存在与目标业务地址不同的待验证地址，则删除已生成的目标业务地址与N个待验证地址，向N个客户端发送重新生成应用链上地址请求；重新生成应用链上地址请求用于指示N个客户端重新基于完整公钥生成新的待验证地址。

本申请实施例一方面提供了一种基于区块链密钥的数据处理装置，该数据处理装置包括：

目标私钥分片获取模块，用于目标客户端获取分别与N-1个客户端以及服务端进行通信的通信信道，基于通信信道与服务端以及N-1个客户端进行密钥分片协商，得到目标客户端对应的目标私钥分片和完整公钥；N为大于1的正整数；完整公钥是目标客户端对应的目标私钥分片、服务端私钥分片和N-1个客户端对应的目标私钥分片共同对应的唯一公钥；N-1个客户端对应的目标私钥分片中的第i个目标私钥分片，是通过密钥分片协商后由N-1个客户端中的第i个客户端所独自持有的私钥分片；服务端私钥分片是通过密钥分片协商后由服务端所独自持有的私钥分片；

签名请求发送模块，用于基于目标客户端对应的身份关联信息生成目标客户端对应的签名请求，将目标客户端对应的签名请求发送至服务端，以使服务端对接收到的M-1个签名请求中的身份关联信息进行合法身份验证；M-1个签名请求包括目标客户端对应的签名请求；M为基于完整公钥进行验签的私钥分片数量阈值，M为小于等于N+1的正整数；

业务执行数据发送模块，用于若检测到服务端确定M-1个签名请求中的身份关联信息均为合法身份信息，则向服务端发送目标客户端相关联的业务执行数据；

第二联合签名模块，用于若业务执行数据符合目标客户端的身份关联信息对应的风险管理策略，则与发起签名请求的客户端以及服务端共同参与针对区块链业务的联合签名处理；联合签名处理所生成的联合签名结果是基于发起签名请求的客户端对应的目标私钥分片和服务端私钥分片共同生成，联合签名结果用于提供给目标客户端执行区块链业务。

其中，M-1个客户端包括目标客户端与签名客户端；数据处理装置，还包括：

第一加密模块，用于若接收到服务端发送的服务端故障信息，则通过目标客户端对应的目标私钥分片，

对获取到的待签名信息进行加密处理，得到初始签名结果；

第二加密模块，用于将初始签名结果发送至签名客户端，以使签名客户端通过签名客户端对应的目标私钥分片对初始签名结果进行加密处理，得到目标签名结果；

目标签名结果接收模块，用于接收签名客户端发送的目标签名结果，基于目标签名结果生成联合签名结果。

其中，签名请求发送模块，包括：

数据显示单元，用于在区块链功能界面中显示业务发起控件、目标客户端对应的应用链上地址与虚拟资源数据；虚拟资源数据用于表示目标客户端对应的区块链业务账号中的业务数据；

操作响应单元，用于响应针对区块链功能界面中的业务发起控件的发起区块链业务操作，将基于目标客户端对应的身份关联信息生成的目标客户端对应的签名请求发送至服务端；

其中，数据处理装置，还包括：

数据发送模块，用于将待上链业务数据向服务端进行发送；待上链业务数据由区块链业务中的目标业务执行数据和联合签名结果组成；

反馈数据接收模块，用于若区块链共识网络基于完整公钥对联合签名结果验签成功，且对待上链业务数据共识通过，则接收服务端发送的针对待上链业务数据的反馈数据，在区块链功能界面中基于反馈数据更新显示虚拟资源数据。

本申请一方面提供了一种计算机设备，包括：处理器、存储器、网络接口；

上述处理器与上述存储器、上述网络接口相连，其中，上述网络接口用于提供数据通信功能，上述存储器用于存储计算机程序，上述处理器用于调用上述计算机程序，以使得计算机设备执行本申请实施例中的方法。

本申请实施例一方面提供了一种计算机可读存储介质，上述计算机可读存储介质中存储有计算机程序，上述计算机程序适于由处理器加载并执行本申请实施例中的方法。

本申请实施例一方面提供了一种计算机程序产品或计算机程序，该计算机程序产品或计算机程序包括计算机指令，该计算机指令存储在计算机可读存储介质中；计算机设备的处理器从计算机可读存储介质读取该计算机指令，处理器执行该计算机指令，使得该计算机设备执行本申请实施例中的方法。

本申请实施例中，通过获取与N个客户端分别进行通信的通信信道，基于N个通信信道分别与N个客户端进行密钥分片协商，得到本地私钥分片和完整公钥。其中，N为大于1的正整数。具体的，完整公钥是本地私钥分片和N个目标私钥分片共同对应的唯一公钥。其中，N个目标私钥分片中的第i个目标私钥分片，是通过密钥分片协商后由N个客户端中的第i个客户端所独自持有的私钥分片。进一步地，接收N个客户端中的M-1个客户端发送的签名请求，获取M-1个签名请求中的身份关联信息。其中，M为基于完整公钥进行验签的私钥分片数量阈值，M为小于等于N+1的正整数。进一步地，若M-1个签名请求中的身份关联信息均为合法身份信息，则将M-1个客户端中用于发起区块链业务的客户端，确定为目标客户端，获取目标客户端相关联的业务执行数据。进一步地，若业务执行数据符合目标客户端的身份关联信息对应的风险管理策略，则与M-1个客户端共同参与针对区块链业务的联合签名处理。其中，联合签名处理所生成的联合签名结果是基于本地私钥分片和M-1个客户端分别持有的目标私钥分片共同生成，联合签名结果用于提供给目标客户端执行区块链业务。本申请实施例通过将密钥分片协商得到本地私钥分片与目标私钥分片，并且对于参加签名的客户端或者服务端进行身份关联信息验证，在身份关联信息验证为合法身份信息后进行多端私钥分片的联合签名处理，可以不再单独使用一个私钥进行数字资产的签名处理，从而降低了因私钥问题而出现签名出错的概率，即某些客户端或服务器中的私钥分片不可用时，依然可以通过其他M个可用的私钥分片来实现签名功能，提升了数字资产签名的安全概率，即降低了使用数字资产的风险概率。而且身份关联信息的合法检测以及风险管理策略的应用，可以降低进行数字资产业务交互的风险性，提升进行数字资产业务交互的安全性。

附图说明

为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例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，下面描述中的附图仅仅是本申请的一些实施例，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。

图1是本申请实施例提供的一种区块链网络的结构示意图；

图2是本申请实施例提供的一种关于数字资产签名的场景示意图；

图3是本申请实施例提供的一种数据处理方法的流程示意图；

图 4 是本申请实施例提供的另一种数据处理方法的流程示意图；
图 5 是本申请实施例提供的一种关于目标客户端的界面示意图；
图 6 是本申请实施例提供的一种关于数字资产签名的交互流程图；
图 7 是本申请实施例提供的一种数据处理装置的结构示意图；
图 8 是本申请实施例提供的另一种数据处理装置的结构示意图；
图 9 是本申请实施例提供的一种计算机设备的结构示意图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请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本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，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，都属于本申请保护的范围。

可以理解的是，在本申请的具体实施方式中，涉及到对象或用户相关的数据（如支付数据），当本申请以下实施例运用到具体产品或技术中时，需要获得用户许可或者同意，且相关数据的收集、使用和处理需要遵守相关国家和地区的相关法律法规和标准。

本申请实施例提供的方案涉及区块链技术，具体过程通过如下实施例进行说明。

请参见图 1，图 1 是本申请实施例提供的一种区块链网络的结构示意图。如图 1 所示的区块链网络可以包括但不限于区块链业务所对应的分布式网络。该区块链网络中可以包括多个区块链节点，多个区块链节点具体可以包括区块链节点 10a、区块链节点 10b、区块链节点 10c、区块链节点 10d、...、区块链节点 10n。例如，区块链节点可以是区块链业务所对应的分布式网络中的客户端或服务端。其中，每个区块链节点在进行正常工作时可以接收到外界发送的数据，并基于接收到的数据进行区块上链处理，也可以向外界发送数据。为了保证各个区块链节点之间的数据互通，每个区块链节点之间可以存在数据连接，例如区块链节点 10a 和区块链节点 10b 之间存在数据连接，区块链节点 10a 和区块链节点 10c 之间存在数据连接，区块链节点 10b 和区块链节点 10c 之间存在数据连接。

可以理解的是，区块链节点之间可以通过上述数据连接进行数据或者区块传输。区块链网络可以基于节点标识实现区块链节点之间的数据连接，对于区块链网络中的每个区块链节点，均具有与其对应的节点标识，而且上述每个区块链节点均可以存储与自身有相连关系的其他区块链节点的节点标识，以便后续根据其他区块链节点的节点标识，将获取到的数据或生成的区块广播至其他区块链节点，例如区块链节点 10a 中可以维护一个如表 1 所示的节点标识列表，该节点标识列表保存着其他节点的节点名称和节点标识：

表 1

节点名称	节点标识
节点 10a	AAA.AAA.AAA.AAA
节点 10b	BBB.BBB.BBB.BBB
节点 10c	CCC.CCC.CCC.CCC
节点 10d	DDD.DDD.DDD.DDD
...	...
节点 10n	EEE.EEE.EEE.EEE

其中，节点标识可为网络之间互联的协议（Internet Protocol，IP）地址以及其他任意一种能够用于标识区块链网络中节点的信息，表 1 中仅以 IP 地址为例进行说明。例如，区块链节点 10a 可以通过节点标识 BBB.BBB.BBB.BBB 向区块链节点 10b 发送区块链数据（例如，包装成区块格式的加密数据），且区块链节点 10b 可以通过节点标识 AAA.AAA.AAA.AAA 确定该信息是由区块链节点 10a 所发送的。

在区块链中，在将一个区块进行上链之前，该区块必须经过区块链网络中的共识节点进行共识，在共识通过后才能将该区块添加到区块链上。可以理解的是，当区块链被用于商业机构的一些场景中时，并非区块链中的所有参与节点（即上述区块链网络中的区块链节点）都有足够的资源和必要性成为区块链的共识节点。例如，在图 1 所示的区块链网络中，可以将区块链节点 10a、区块链节点 10b、区块链节点 10c 和区块链节点 10d 作为该区块链网络中的共识节点。区块链网络中的共识节点参与共识，也就是对区块（包含一批交易）进行共识，即对区块进行投票；而非共识节点不参与共识，但会帮助传播区块和投票消息，以及相互同步状态等。

可以理解的是，本申请实施例提供的方法可以由计算机设备执行，计算机设备包括但不限于上述区块链节点（本申请实施例中可以为客户端或者服务端）。其中，在本申请实施例中，服务端可以是独立的物

理服务器,也可以是多个物理服务器构成的服务器集群或者分布式系统,还可以是提供云数据库、云服务、云计算、云函数、云存储、网络服务、云通信、中间件服务、域名服务、安全服务、CDN、以及大数据和人工智能平台等基础云计算服务的云服务器。其中,以上所提及的客户端可以是一种电子设备,包括但不限于手机、平板电脑、台式电脑、笔记本电脑、掌上电脑、车载设备、增强现实/虚拟现实(Augmented Reality/Virtual Reality, AR/VR)设备、头显显示器、智能电视、可穿戴设备、智能音箱、数码相机、摄像头及其他具备网络接入能力的移动互联网设备(mobile internet device, MID),或者火车、轮船、飞行等场景下的终端设备等。

可以理解的是,本申请实施例可应用于各种场景,包括但不限于云技术、人工智能、智慧交通等场景。例如,区块链节点系统可以对车载终端所发送的一些驾驶行为数据、道路轨迹数据等等进行共识,共识通过后对其进行上链存储。

可以理解的是,本申请实施例中的多个不同的私钥分片的存储以及运算可以由包括服务器、个人电脑、个人智能穿戴设备以及拥有计算和存储能力的其他设备(如智能汽车、智能无人机)进行存储以及运算。例如,在业务对象需要通过自己的智能设备管理数据资产时,可以通过个人智能汽车或者智能手表、VR设备等发起数字资产处理流程,基于该智能设备对应的本地私钥分片与其他设备对应的私钥分片进行联合计算完成签名。

其中,本申请中所提及的计算机设备可以是服务端或客户端,也可以是由服务端和客户端所组成的系统。

进一步地,请参见图2,图2是本申请实施例提供的一种关于数字资产签名的场景示意图。如图2所示,其中,服务器300可以是本申请实施例中的安装有支付应用的客户端所对应的后台服务器(即服务端),业务设备400a可以是本申请实施例中的安装有支付应用的客户端。同时,服务器300可以是图1中的区块链节点10b,业务设备400a可以是图1中的区块链节点10a。具体的,服务器300可以获取与N个客户端分别进行通信的通信信道。其中,N个客户端可以包括业务设备400a。进一步地,服务器300可以基于N个通信信道分别与N个客户端进行密钥分片协商,得到由服务器300单独持有的本地私钥分片和完整公钥。举例来说,服务器300可以与业务设备400a、业务设备401a、...、业务设备402a等N个业务设备进行密钥分片协商,得到由服务器300单独持有的本地私钥分片、由业务设备400a单独持有的第一目标私钥分片、由业务设备401a单独持有的第二目标私钥分片、...、由业务设备402a单独持有的第三目标私钥分片与完整公钥。其中,N为大于1的正整数。可以理解,完整公钥是本地私钥分片和N个目标私钥分片共同对应的唯一公钥。其中,N个目标私钥分片中的第i个目标私钥分片,是通过密钥分片协商后由N个客户端中的第i个客户端所独自持有的私钥分片,换言之,每个客户端只能单独持有其中一个目标私钥分片。进一步地,服务器300接收N个客户端中的M-1个客户端发送的签名请求,获取M-1个签名请求中的身份关联信息。其中,M为基于完整公钥进行验签的私钥分片数量阈值,M为小于等于N+1的正整数。具体的,私钥分片数量阈值可以是指构成完整公钥对应的完整私钥的最小私钥分片数量。例如,若在区块链业务对应的分布式系统中,包括1个服务端与4个客户端,该分布式系统的私钥分片数量阈值为3,则表示分布式系统需要基于3个参与方(如1个服务端与2个客户端)对应的私钥分片生成完整私钥。也就是说,若分布式系统基于2个参与方对应的私钥分片不能生成完整私钥。进一步地,若M-1个签名请求中的身份关联信息均为合法身份信息,则将M-1个客户端中用于发起区块链业务的客户端,确定为目标客户端,获取目标客户端相关联的业务执行数据。举例来说,目标客户端相关联的业务执行数据可以包括具有支付功能的应用中的转账数据,具体的,该转账数据可以包括转账对象、转账数值以及目标客户端的身份信息等数据。可选的,目标客户端相关联的业务执行数据还可以是指车载终端所发送的一些驾驶行为数据、道路轨迹数据等等。进一步地,若业务执行数据符合目标客户端的身份关联信息对应的风险管理策略,则与M-1个客户端共同参与针对区块链业务的联合签名处理。其中,联合签名处理所生成的联合签名结果是基于本地私钥分片和M-1个客户端分别持有的目标私钥分片共同生成,联合签名结果用于提供给目标客户端执行区块链业务。

其中,公钥与私钥是通过一种密钥生成算法得到的一个密钥对(即一个公钥和一个私钥),公钥是密钥对中公开的密钥部分,私钥则是非公开的密钥部分。具体的,公钥通常用于加密数据、验证数字签名等。通过该密钥生成算法能够确保得到的密钥对是唯一的,在使用该密钥对时,若使用其中一个密钥加密一段数据,则需要用另一个密钥进行解密,例如,用公钥加密一段数据就必须用私钥解密,如果用私钥加密也必须用公钥解密,否则解密失败。

具体的,以服务器300和业务设备400a共同参与针对区块链业务的联合签名处理为例,该数据处理

方法至少可以包括以下步骤 S21-步骤 S27:

步骤 S21, 业务设备 400a 通过所持有的目标私钥分片对待签名内容进行签名, 得到中间加密结果。

其中, 待签名内容可以是指需要进行签名确认的业务数据, 例如, 业务数据可以是支付应用中的转账业务的相关数据, 如包含转账对象、转账金额以及转账机构等等。

步骤 S22, 服务器 300 接收中间加密结果。

步骤 S23, 服务器 300 通过本地私钥分片对中间加密结果进行签名, 得到服务端签名结果。

步骤 S24, 服务器 300 发送服务端签名结果。

步骤 S25, 业务设备 400a 基于服务端签名结果生成联合签名结果, 基于待签名内容和联合签名结果生成待上链业务数据。

步骤 S26, 服务器 300 接收待上链业务数据。

步骤 S27, 服务器 300 发送待上链业务数据至区块链共识网络。

可选的, 服务器 300 也可以接收区块链共识网络上的数据 (即服务器 300 也可以为区块链共识网络中的其中一个共识节点), 并对接收到的数据进行数据处理, 具体的数据处理过程请参见下文图 3 中服务端对接收到的客户端的区块链业务数据的处理过程的详细描述。

应当理解, 在分布式系统 200S (即服务器 300 和业务设备 400a 构成的系统) 中, 任何机器 (如服务端、客户端) 都可以加入而成为节点, 且一个节点可以对应一个角色 (也可以称之为一个对象)。换言之, 该分布式系统可以用于为加入该区块链系统中的角色提供相应的接入接口。比如, 可以针对税局 (即税务局)、开票企业、消费者以及报销企业等角色分别提供相应的接入接口。比如, 税局中的税务人员可以通过浏览器中的目标网页面访问相应的节点, 又比如, 消费者在通过目标应用完成数据交互业务时, 可以通过该目标应用所提供的子应用程序 (例如, 嵌入在支付应用中的小程序等) 访问相应的节点等。其中, 可以理解的是, 每个节点均可以包括硬件层、中间层、操作系统层和应用层。

进一步地, 请参见图 3, 图 3 是本申请实施例提供的一种数据处理方法的流程示意图。如图 3 所示, 该方法可以由服务端执行, 该服务端可以为上述图 1 所示的区块链节点 10b, 在此不做限定。为便于理解, 本申请实施例以该方法由服务端执行为例进行说明, 该数据处理方法至少可以包括以下步骤 S101-步骤 S104:

步骤 S101, 获取与 N 个客户端分别进行通信的通信信道, 基于 N 个通信信道分别与 N 个客户端进行密钥分片协商, 得到本地私钥分片和完整公钥; N 为大于 1 的正整数; 完整公钥是本地私钥分片和 N 个目标私钥分片共同对应的唯一公钥; N 个目标私钥分片中的第 i 个目标私钥分片, 是通过密钥分片协商后由 N 个客户端中的第 i 个客户端所独自持有的私钥分片。

具体的, 服务端可以通过与 N 个客户端分别进行通信的通信信道向 N 个客户端进行通信消息的传递 (例如, 向 N 个客户端发送广播)。进一步地, 服务端可以通过该通信信道进行业务协商以及业务请求确认等操作。其中, 通信信道可以是指用于进行服务端与客户端之间会话的会话信道。广义上讲, 通信信道可以包括进行通信的虚拟信道以及构成通信线路的实体信道。例如, 通信信道可以包括传输电缆等实体信道。具体来说, 通信信道可以指用于进行广播等用途的通信信道。例如, 在一个通信线路构成的局域网中, 通信信道可以指构成该局域网的虚拟线路以及硬件线路等。

具体的, 本申请实施例不对客户端的总数量进行限定, 客户端可以为一个或多个, 即 N 可以大于等于 1, N 的具体取值是由在区块链业务对应的分布式系统中, 共同生成一个完整公钥对应的完整私钥时, 生成完整私钥过程的参与方 (即区块链节点) 的数量所确定。此处以 1 个客户端与 1 个服务端共同参与支付应用的签名进行示例, 即业务对象请求 2 个参与方分别持有私钥分片 (即一个本地私钥分片与一个目标私钥分片)。也就是说, 服务端可以与客户端进行密钥分片协商, 生成两个分别独立的私钥分片 (即服务端单独持有本地私钥分片, 客户端单独持有目标私钥分片)。应当理解, 生成的私钥分片仅在生成该私钥分片的设备内部可知, 是生成该私钥分片的设备独自持有, 不会对外公布。其中, 该私钥分片为该区块链系统的完整私钥的一部分 (任意一个参与方都不能获知完整私钥), 该完整私钥由多个私钥片段组成, 该完整私钥与完整公钥相对应, 且完整公钥和私钥分片可以基于分布式密钥生成协议 (Distributed Key Generation, DKG) 生成。具体的, 在 DKG 协议中, 多个参与的服务端或客户端根据预先设定的加密系统, 共同生成完整公钥和各自的私钥分片, 基于超过一定阈值数量的私钥分片即可合成与该完整公钥对应的完整私钥, 而基于小于上述阈值数量的私钥分片将无法获取到完整私钥的任何信息, DKG 协议生成的完整公钥以公开的形式输出, 而各个私钥分片将被参与者按照某一种秘密分享方案所分享, 被分享的私钥分片可以用于面向群体的密码系统, 比如群体签名或者群体解密等。可选的, N 可以为 2。也就是说, 分布式

系统(如图2中所示的分布式系统200S)可以由2个客户端与1个服务端共同参与支付应用的签名进行示例,即业务对象请求3个参与方分别持有私钥分片(即一个本地私钥分片与两个目标私钥分片)。也就是说,服务端可以与两个客户端进行密钥分片协商,生成三个分别独立的私钥分片(即服务端对应的一个本地私钥分片与2个客户端分别对应的目标私钥分片)。可选的,密钥协商处理的过程还可以包括阈值签名(Threshold Signature Scheme, TSS)的过程。也就是说,在密钥协商处理的过程中,服务端可以通过阈值签名的方法以使从多个签名者(区块链节点)生成单个数字签名。进一步地,阈值签名的具体实现方案可以包括Lindell算法(一种阈值签名算法)、DKLS算法(一种阈值签名算法)、CCLST算法(一种阈值签名算法)、GKSS算法(一种阈值签名算法)、GG18算法(一种阈值签名算法)、GG20算法(一种阈值签名算法)等算法。

具体的,分布式系统(如图2中所示的分布式系统200S)可以通过非对称加密算法创建密钥对。其中,非对称加密算法可包括但不限于:ElGamal算法(一种非对称加密算法)、Rabin算法(一种非对称加密算法)、Diffie-Hellman算法(一种非对称加密算法)、ECC算法(椭圆曲线加密算法)。具体的,Diffie-Hellman算法是一种基于离散对数问题的公开密钥加密算法,它可以让两个节点在不共享任何信息的情况下协商出一个共同的秘密。进一步地,RSA算法是一种基于大质数来生成公私钥对,并利用这些数字进行解密操作的算法。此外,ECC算法则是一种基于椭圆曲线离散对数问题的公开密钥加密算法,它具有短密钥长度和高安全性等优点。

具体的,服务端可以随机生成用于进行密钥分片协商的本地测试私钥,通过本地测试私钥对本地协商数据(本地协商数据可以为随机数据)进行加密处理,得到本地测试信息。进一步地,服务端可以获取与N个客户端分别进行通信的通信信道,通过每个通信信道向N个客户端发送本地测试信息。进一步地,服务端可以接收N个客户端分别发送的目标测试公钥以及目标测试信息,通过目标测试公钥对属于同一客户端的目标测试信息进行解密,得到N个目标解密数据。其中,一个目标测试公钥是指一个客户端所生成的用于进行密钥分片协商的目标测试私钥对应的公钥,一个目标测试信息是指在一个客户端中通过所生成的目标测试私钥对目标协商数据进行加密处理所得到的信息。例如,若在客户端中生成了一对密钥,且该对密钥中的私钥为目标测试私钥Z1,则该对密钥中的公钥可以为目标测试公钥Z2。在此基础上,目标测试信息Y即为通过目标测试私钥Z1对客户端中的目标协商数据进行加密处理后的信息,该加密处理后的信息可以用于在区块链节点系统中进行发送或传递。进一步地,服务端可以基于本地测试私钥对应的本地测试公钥对本地测试信息进行解密,得到本地解密数据,将本地解密数据以及N个目标解密数据确定为第一哈希结果。进一步地,服务端可以对本地协商数据以及N个目标协商数据进行哈希运算,得到第二哈希结果。进一步地,若第一哈希结果与第二哈希结果相等,则确定密钥协商成功,将本地测试私钥确定为本地私钥分片。进一步地,服务端可以在与N个客户端进行密钥分片协商的过程中生成完整公钥。依此类推,在N个客户端中也可以通过与生成本地私钥分片近似的方法,分别生成N个在各自客户端中独自持有的目标私钥分片。

其中,服务端可以通过随机生成的算法在服务端生成一个伪随机数,并作为服务端的本地私钥分片。生成一个伪随机数的具体实施方式不做限制,例如以一个随机数种子(真随机数)作为初始条件,然后采用算法不停迭代产生随机数。其中,服务端可以通过本地测试私钥对本地协商数据进行加密处理。具体的,加密处理所对应的数字签名算法可以包括但不限于:ElGamal(一种签名算法),Fiat-Shamir(一种签名算法),Guillou-Quisquater(一种签名算法),Schnorr(一种签名算法),Ong-Schnorr-Shamir(一种签名算法),椭圆曲线数字签名算法和有限自动机数字签名算法,等等。其中,本地协商数据是指服务端中需要进行加密的业务数据。相应的,每个客户端可以通过每个客户端对应的目标测试私钥对目标协商数据进行加密处理,得到目标测试信息。其中,目标协商数据是指客户端中需要进行加密的业务数据。进一步地,通过每个客户端对应的目标测试公钥对属于同一客户端的目标测试信息进行解密,得到每个客户端对应的目标解密数据。应当理解,若第一哈希结果与第二哈希结果相等,则表示通过本地测试私钥对本地协商数据进行加密的过程、通过本地测试私钥对应的本地测试公钥对本地测试信息进行解密的过程、通过目标测试私钥对目标协商数据进行加密的过程以及通过目标测试私钥对应的目标测试公钥对目标测试信息进行解密的过程均无误。

进一步地,服务端可以基于完整公钥生成目标业务地址。进一步地,服务端可以获取N个客户端分别发送的待验证地址。其中,一个客户端发送的待验证地址是基于完整公钥所生成的。进一步地,若目标业务地址与N个待验证地址均相同,则确定目标业务地址为合法地址,且将目标业务地址确定为应用链上地址。相应的,若N个待验证地址中存在与目标业务地址不同的待验证地址,则删除已生成的目标业务地址

与 N 个待验证地址, 向 N 个客户端发送重新生成应用链上地址请求。其中, 重新生成应用链上地址请求用于指示 N 个客户端重新基于完整公钥生成新的待验证地址。

具体的, 服务端可以通过完整公钥进行推算, 得到目标业务地址。进一步地, 若目标业务地址与获取到的 N 个待验证地址均相同, 则确定目标业务地址为合法地址, 且将目标业务地址确定为应用链上地址。其中, 应用链上地址即为区块链业务对应的应用的地址 (如支付应用的地址)。例如, 若图 2 中的分布式系统 200S 由一个客户端与一个服务端构成, 则若服务端生成的目标业务地址与客户端生成的待验证地址相同, 则表示目标业务地址即为区块链业务对应的应用 (如客户端上的支付应用) 的地址。进一步地, 目标业务地址可以用于在区块链节点网络中进行区块链数据交互对象的定位。例如, 在本申请实施例中, 目标节点 (即服务端) 在获取到游戏客户端 (即目标客户端) 发送的完整公钥和游戏资源账号的地址 (即目标业务地址) 后, 可以向区块链网络中的每个节点发送该完整公钥和游戏资源账号的地址, 任一节点接收到该完整公钥和游戏资源账号的地址后, 可以通过该游戏资源账号地址进行游戏资源相关数据 (例如需要更新的虚拟游戏装备数据) 的交互。此外, 该节点在接收到该完整公钥和游戏资源账号的地址后, 还可以通过共识算法对该完整公钥和游戏资源账号的地址进行共识处理后再次广播至区块链网络, 不断执行该共识处理, 直至各个节点存储的公钥和游戏资源账号的地址达成一致, 这样一来, 可以保证各个节点存储的公钥和游戏资源账号的地址的一致性。

步骤 S102, 接收 N 个客户端中的 $M-1$ 个客户端发送的签名请求, 获取 $M-1$ 个签名请求中的身份关联信息; M 为基于完整公钥进行验签的私钥分片数量阈值, M 为小于等于 $N+1$ 的正整数。

具体的, 服务端可以通过接收 N 个客户端中的 $M-1$ 个客户端发送的签名请求进而触发服务端进行签名的过程。进一步地, 服务端可以通过获取 $M-1$ 个签名请求中的身份关联信息进而对于 $M-1$ 个客户端进行签名验证。

具体的, 服务端可以获取 $M-1$ 个客户端分别对应的目标分片公钥。其中, 一个客户端对应的目标分片公钥是基于该客户端对应的目标私钥分片所生成的。进一步地, 服务端可以通过 $M-1$ 个目标分片公钥分别对 $M-1$ 个客户端发送的分片签名结果进行签名验证, 得到 $M-1$ 个签名验证结果。其中, 一个分片签名结果是指一个客户端通过该客户端对应的目标私钥分片对身份关联信息进行签名后的数据。进一步地, 若 $M-1$ 个签名验证结果均为验证成功结果, 则对 $M-1$ 个客户端所发送的签名请求中的身份关联信息进行合法身份验证。

其中, 服务端可以通过目标分片公钥的验证进而确定该客户端的身份, 具体的, 服务端可以在生成本地私钥分片时将构成一个完整私钥的目标私钥分片对应的客户端与该服务端进行关联。由此, 服务端可以通过验证目标分片公钥进而验证客户端与服务端之间的关联关系, 换言之, 服务端可以通过验证目标分片公钥进而验证客户端与服务端之间是否属于同一个完整公钥对应的分布式系统。若 $M-1$ 个签名验证结果均为验证成功结果, 则证明服务端与 $M-1$ 个签名验证结果对应的客户端具有关联关系, 也就是说, 服务端与 $M-1$ 个签名验证结果对应的客户端可以构成属于同一个完整公钥 (或完整私钥) 的分布式系统。

进一步地, 若验证通过, 则表示服务端可以根据接收到的签名请求进行服务端签名处理。其中, 服务端接收到的签名请求为验证通过的客户端发送的。进一步地, 具体的服务端签名处理的过程请参见下文步骤 S103-步骤 S104 中的详细描述。

步骤 S103, 若 $M-1$ 个签名请求中的身份关联信息均为合法身份信息, 则将 $M-1$ 个客户端中用于发起区块链业务的客户端, 确定为目标客户端, 获取目标客户端相关联的业务执行数据。

具体的, 其中, $M-1$ 个签名请求所对应的 $M-1$ 个客户端可以包括客户端 S_i , i 为小于或等于 $M-1$ 的正整数。具体的, 服务端可以获取 $M-1$ 个客户端所关联发起的区块链业务的业务类型, 获取客户端 S_i 对应的身份关联信息中的身份标识以及身份特征数据。进一步地, 服务端可以确定业务类型所匹配的身份验证策略, 在身份标识以及身份特征数据中, 选取与身份验证策略所指示的验证维度匹配的数据, 作为待验证数据。进一步地, 若待验证数据存在于身份数据库中, 则确定客户端 S_i 对应的签名请求中的身份关联信息为合法身份信息。

其中, 业务类型可以包括业务查询、转账与账户管理等操作类型。具体的, 服务器可以在业务对象进行账户注册时, 进行身份标识以及身份特征数据的绑定, 具体的, 身份特征数据可以包括但不限于多个关键部位所对应的特征等。具体的, 服务端可以根据业务类型所匹配的身份验证策略确定需要验证的身份标识或者身份特征信息。例如, 若服务端获取到客户端所发起的业务类型为业务查询 (具体可以为账户余额查询), 则服务端可以确定业务类型所匹配的身份验证策略为验证身份特征数据。进一步地, 服务端可以选取业务对象的身份特征数据作为与身份验证策略所指示的验证维度匹配的数据, 即服务端可以选取业务

对象的身份特征数据作为待验证数据。进一步地,若该业务对象的身份特征数据存在于身份数据库中,则确定客户端 S_i 对应的签名请求中的身份关联信息为合法身份信息。其中,服务端验证身份特征数据的方式可以为仅验证多个关键部位中的任意一个,该验证方式可以由业务对象在支付应用中进行设置,这里不对其进行具体限制。再例如,若服务端获取到客户端所发起的业务类型为转账,则服务端可以确定业务类型所匹配的身份验证策略为验证身份特征数据与身份标识。进一步地,服务端可以选取业务对象的身份特征数据与业务对象的身份标识一起作为与身份验证策略所指示的验证维度匹配的数据,即服务端可以选取业务对象的身份特征数据与业务对象的身份标识作为待验证数据。进一步地,若该业务对象的身份特征数据与业务对象的身份标识皆存在于身份数据库中,则确定客户端 S_i 对应的签名请求中的身份关联信息为合法身份信息。相应的,若该业务对象的身份特征数据与业务对象的身份标识中的任意一个未存在与身份数据库中,则确定客户端 S_i 对应的签名请求中的身份关联信息为非法身份信息,并且服务器可以拒绝响应客户端发起的该笔转账业务。应当理解,前文列举的身份验证策略为可能的两种身份验证策略,关于本申请实施例中具体的身份验证策略可以由支付应用的维护对象进行设定,这里不对其进行具体限定。依此类推,可以理解的,M-1个客户端中除客户端 S_i 之外的其他客户端的确定身份关联信息的具体过程可以参考上文客户端 S_i 的确定身份关联信息的具体过程,这里不再进行赘述。进一步地,直至对M-1个客户端所对应的身份关联信息进行验证处理后,若确定M-1个客户端所对应的身份关联信息皆为合法身份信息,则确定M-1个签名请求中的身份关联信息均为合法身份信息。

进一步地,若M-1个签名请求中的身份关联信息均为合法身份信息,则服务端可以获取目标客户端的历史业务执行数据以及所发起的区块链业务中的目标业务执行数据,将历史业务执行数据和目标业务执行数据确定为目标客户端相关联的业务执行数据。其中,服务端可以获取目标客户端的历史业务交互记录(如历史交易记录)、目标客户端的历史设置变更、目标客户端的历史业务交互对象等数据确定为历史业务执行数据。其中,服务端可以获取区块链业务关联的所有客户端的业务信息作为目标业务执行数据。具体的,服务端可以将业务交互对象(如转账对象标识)、业务交互内容(如转账金额)与业务交互地址(如转账对象的地址)等信息确定为与区块链业务关联的客户端的业务信息,也就是说,服务端可以将业务交互对象(如转账对象标识)、业务交互内容(如转账金额)与业务交互地址(如转账对象的地址)等信息确定为目标业务执行数据。

进一步地,服务端可以对业务执行数据中的历史业务执行数据进行数据分析,得到历史业务操作范围,基于历史业务操作范围,设置业务阈值。进一步地,若业务执行数据中的目标业务执行数据小于等于业务阈值,则确定业务执行数据符合目标客户端的身份关联信息对应的风险管理策略。例如,若与服务端进行业务交互的客户端上对于的应用为支付应用,则服务端对业务执行数据中的历史业务执行数据进行数据分析,得到的历史业务操作范围可以是支付应用的历史转账额度,基于支付应用的历史转账额度设置转账阈值(即业务阈值)。进一步地,若业务执行数据中的目标业务执行数据(即支付应用中的当前转账额度)小于等于业务阈值(即转账阈值),则确定业务执行数据符合目标客户端的身份关联信息对应的风险管理策略。也就是说,确定该支付应用的当前转账数据符合目标客户端的身份关联信息对应的风险管理策略。举例来说,服务端可以设置固定时间段内单笔业务交互数据的额度上线,这里的固定时间段可以包括小时、日与月等。可选的,服务端可以设置固定时间段内业务交互数据的次数上线。可选的,服务端还可以针对某些业务对象预先设置的特定场景进行限制区块链业务交互的风险管理策略。

具体的,服务端可以从业务执行数据中获取目标客户端对应的应用链上地址,对应用链上地址进行地址风险检测。进一步地,若检测到应用链上地址存在于合法地址名单中,则确定业务执行数据符合目标客户端的身份关联信息对应的风险管理策略。相应的,若检测到应用链上地址不存在于合法地址名单中,则确定应用链上地址为风险性地址,禁止响应目标客户端所发起的区块链业务。其中,服务端通过对应用链上地址进行地址风险检测,可以将监管单位发布的黑名单地址以及管制实体的地址进行过滤,从而降低进行数字资产业务交互的风险性,提升进行数字资产业务交互的安全性。

步骤S104,若业务执行数据符合目标客户端的身份关联信息对应的风险管理策略,则与M-1个客户端共同参与针对区块链业务的联合签名处理:联合签名处理所生成的联合签名结果是基于本地私钥分片和M-1个客户端分别持有的目标私钥分片共同生成,联合签名结果用于提供给目标客户端执行区块链业务。

具体的,其中,M-1个客户端包括目标客户端。具体的,服务端可以接收目标客户端发送的经过目标客户端对应的目标私钥分片进行加密处理后的中间加密结果,通过本地私钥分片对接收到的中间加密结果进行签名,得到服务端签名结果。进一步地,服务端可以将服务端签名结果发送至目标客户端。其中,服务端签名结果用于指示目标客户端生成联合签名结果。

进一步地,服务端可以接收目标客户端发送的待上链业务数据。其中,待上链业务数据由区块链业务中的目标业务执行数据和联合签名结果组成。进一步地,服务端可以将待上链业务数据转发至区块链共识网络,以使区块链共识网络在共识过程中基于完整公钥对联合签名结果进行验签,在共识通过时,将目标业务执行数据所对应的执行结果数据存储至区块链账本中。其中,区块链账本用于提供账目数据的存储、查询和修改等操作的功能,将对账目数据的操作的记录数据发送到区块链系统(如图2中的分布式系统200S)中的其他节点,其他节点验证有效后,作为承认账目数据有效的响应,将记录数据存入临时区块中,还可以向发起操作的节点发送确认。其中,节点可以是指接入网络中的任意形式的计算设备,如服务器或客户端。

应当理解,在本申请实施例中,服务端所持有的私钥分片数量(即一片)占区块链业务对应的分布式系统中的全部私钥分片数量的比值小于等于50%,也就是说,服务端所持有的私钥分片的分片份额小于等于50%,这就保障了若客户端未参与联合签名,则服务端无法独立完成联合签名,因此服务端也就无法私自动用数字资产,降低了使用数字资产的风险概率。

可以理解的是,在本申请的具体实施方式中,涉及到的如支付应用的关联数据等区块链业务数据,当本申请以上以及以下实施例运用到具体产品或技术中时,相关数据收集处理在实例应用时应该严格根据相关国家法律法规的要求,获取个人信息主体的知情同意或单独同意(或具备合法性基础),并在法律法规及个人信息主体的授权范围内,开展后续数据使用及处理行为。涉及到的人脸(或其他生物特征)识别技术时,相关数据收集、使用和处理过程应该遵守国家法律法规要求,收集人脸信息前应该告知信息处理规则并征求目标对象的单独同意(或具备合法性基础),并严格遵照法律法规要求和个人信息处理规则处理人脸信息,采取技术措施保障相关数据安全。

本申请实施例中,通过获取与N个客户端分别进行通信的通信信道,基于N个通信信道分别与N个客户端进行密钥分片协商,得到本地私钥分片和完整公钥。进一步地,接收N个客户端中的M-1个客户端发送的签名请求,获取M-1个签名请求中的身份关联信息。进一步地,若M-1个签名请求中的身份关联信息均为合法身份信息,则将M-1个客户端中用于发起区块链业务的客户端,确定为目标客户端,获取目标客户端相关联的业务执行数据。进一步地,若业务执行数据符合目标客户端的身份关联信息对应的风险管理策略,则与M-1个客户端共同参与针对区块链业务的联合签名处理。其中,联合签名处理所生成的联合签名结果是基于本地私钥分片和M-1个客户端分别持有的目标私钥分片共同生成,联合签名结果用于提供给目标客户端执行区块链业务。本申请实施例通过将密钥分片协商得到本地私钥分片与目标私钥分片,并且对于参加签名的客户端或者服务端进行身份关联信息验证,在身份关联信息验证为合法身份信息后进行多端私钥分片的联合签名处理,可以不再单纯使用一个私钥进行数字资产的签名处理过程,从而降低了因私钥问题而出现签名出错的概率,降低了使用数字资产的风险概率。应当理解,本申请实施例中通过进行身份关联信息验证可以对客户端的身份关联信息进行安全性确认,进而降低进行签名过程的风险概率。而且,本申请实施例中通过风险管理策略的验证对应用链上地址进行地址风险检测,可以将监管单位发布的黑名单地址以及管制实体的地址进行过滤与拦截,从而降低进行数字资产业务交互的风险性,提升进行数字资产业务交互的安全性。本申请实施例中,降低了使用数字资产的风险概率。

进一步地,请参见图4,图4是本申请实施例提供的另一种数据处理方法的流程示意图。如图4所示,该方法可以由客户端执行,该客户端可以为上述图1所示的区块链节点系统中的任意一个区块链节点,例如,区块链节点10a,在此不做限定。为便于理解,本申请实施例以该方法由客户端执行为例进行说明,该数据处理方法至少可以包括以下步骤S201-步骤S204:

步骤S201,目标客户端获取分别与N-1个客户端以及服务端进行通信的通信信道,基于通信信道与服务端以及N-1个客户端进行密钥分片协商,得到目标客户端对应的目标私钥分片和完整公钥;N为大于1的正整数;完整公钥是目标客户端对应的目标私钥分片、服务端私钥分片和N-1个客户端对应的目标私钥分片共同对应的唯一公钥;N-1个客户端对应的目标私钥分片中的第i个目标私钥分片,是通过密钥分片协商后由N-1个客户端中的第i个客户端所独自持有的私钥分片;服务端私钥分片是通过密钥分片协商后由服务端所独自持有的私钥分片。

具体的,目标客户端可以通过获取到的通信信道进行会话。通过该通信信道进行密钥协商过程中的广播,以及消息回复。进一步地,目标客户端可以基于通信信道进行密钥分片协商,得到唯一公钥。本步骤为以客户端为执行主体的响应过程,具体过程可以参见上述图3所对应实施例中的S101中以服务端为执行主体的步骤S201对应的内容的详细描述,这里不再进行赘述。

步骤S202,基于目标客户端对应的身份关联信息生成目标客户端对应的签名请求,将目标客户端对应

的签名请求发送至服务端,以使服务端对接收到的 M-1 个签名请求中的身份关联信息进行合法身份验证; M-1 个签名请求包括目标客户端对应的签名请求; M 为基于完整公钥进行验签的私钥分片数量阈值, M 为小于等于 N+1 的正整数。

本步骤的具体过程可以参见上述图 3 所对应实施例中的 S102, 这里不再进行赘述。

步骤 S203, 若检测到服务端确定 M-1 个签名请求中的身份关联信息均为合法身份信息, 则向服务端发送目标客户端相关联的业务执行数据。

本步骤的具体过程可以参见上述图 3 所对应实施例中的 S103, 这里不再进行赘述。

步骤 S204, 若业务执行数据符合目标客户端的身份关联信息对应的风险管理策略, 则与发起签名请求的客户端以及服务端共同参与针对区块链业务的联合签名处理; 联合签名处理所生成的联合签名结果是基于发起签名请求的客户端对应的目标私钥分片和服务端私钥分片共同生成, 联合签名结果用于提供给目标客户端执行区块链业务。

进一步地, M-1 个客户端包括目标客户端与签名客户端。具体的, 目标客户端若接收到服务端发送的服务端故障信息, 则通过目标客户端对应的目标私钥分片, 对获取到的待签名信息进行加密处理, 得到初始签名结果。进一步地, 目标客户端可以将初始签名结果发送至签名客户端, 以使签名客户端通过签名客户端对应的目标私钥分片对初始签名结果进行加密处理, 得到目标签名结果。进一步地, 目标客户端可以接收签名客户端发送的目标签名结果, 基于目标签名结果生成联合签名结果。应当理解, 通过目标客户端与签名客户端进行联合签名, 可以使得当服务端永久不可用或服务端存证拒绝服务时, 将数字资产转移到新的可控的用于进行区块链业务的地址, 保障了数字资产的安全, 降低了使用数字资产的风险概率。

进一步地, 目标客户端可以将待上链业务数据向服务端进行发送。其中, 待上链业务数据由区块链业务中的目标业务执行数据和联合签名结果组成。进一步地, 若区块链共识网络基于完整公钥对联合签名结果验签成功, 且对待上链业务数据共识通过, 则目标客户端可以接收服务端发送的针对待上链业务数据的反馈数据, 在区块链功能界面中基于反馈数据更新显示虚拟资源数据。

具体的, 目标客户端可以在区块链功能界面中显示业务发起控件、目标客户端对应的应用链上地址与虚拟资源数据, 其中, 虚拟资源数据用于表示目标客户端对应的区块链业务账号中的业务数据。进一步地, 目标客户端可以响应针对区块链功能界面中的业务发起控件的发起区块链业务操作, 将基于目标客户端对应的身份关联信息生成的目标客户端对应的签名请求发送至服务端, 以使服务端进行签名处理。具体的, 服务端进行签名处理的其他具体过程可以参加上文图 3 中的步骤 S104 的详细描述, 这里不再赘述。

请参见图 5, 图 5 是本申请实施例提供的一种关于目标客户端的界面示意图。如图 5 所示, 业务设备 500a 可以是本申请实施例中的安装有支付应用的客户端。同时, 业务设备 500a 可以是图 1 中的区块链节点 10b。具体的, 在图 5 中, 客户端界面 50D 即为区块链功能界面, 客户端界面 50D 可以包括可以展示目标客户端对应的应用链上地址 51A。例如, 目标客户端对应的应用链上地址 51A 可以是支付应用对应的客户端的地址。进一步地, 客户端界面 50D 可以显示核心功能对应的控件, 如图 5 所示的转出控件 52G 可以用于发起当前支付应用所对应的账户余额的转出过程。相应的, 转入控件 53G 可以用于发起当前支付应用所对应的账户余额的转入过程。相应的, 兑换控件 54G 可以用于发起当前支付应用所对应的账户余额的数字资产种类(如在不同地域通用的数字资产类别)的兑换过程。例如, 若地域 W 与地域 V 之间的数字资产种类不同, 则通过兑换控件 54G 可以将支付应用账户余额在地域 W 的数字资产种类与地域 V 的数字资产种类之间转换。进一步地, 客户端界面 50D 可以显示虚拟资源数据, 举例来说, 虚拟资源数据可以是如图 5 中的数字藏品 55S 与数字藏品 56S。其中, 不同的数字藏品可以具有不同的数字藏品标识。具体的, 可以通过对虚拟资源数据所在区域进行触发操作进而查看该支付应用中的其他数字藏品。其中, 触发操作可以包括点击、双击、长按、放大与缩小等触发操作, 这里不对其进行具体限定, 且该触发操作的设置可以在客户端界面 50D 的功能菜单 57D 中进行设定。进一步地, 客户端界面 50D 可以显示功能菜单 57D, 通过触发功能菜单 57D 可以进行该支付应用所对应的账号切换、账号复制、账号回复与账号托管等功能。具体的, 这里的触发操作也可以参加上文的触发操作, 在此不对其进行具体限定。进一步地, 客户端界面 50D 可以显示链网络状态 58D, 并通过对链网络状态 58D 所对应区域的触发操作实现链网络的切换, 这里不对其具体触发操作进行限定。进一步地, 客户端界面 50D 可以显示业务发起控件 59D, 通过业务发起控件 59D 发起区块链业务操作。举例来说, 业务发起控件 59D 可以通过支付应用所对应硬件设备的摄像头, 以扫码的方式发起区块链业务操作。此外, 客户端界面 50D 还可以显示当前的时间以及支付应用所对应的硬件设备的电量等数据。

本申请实施例中, 通过目标客户端获取分别与 N-1 个客户端以及服务端进行通信的通信信道, 基于通

信信道与服务端以及 $N-1$ 个客户端进行密钥分片协商, 得到目标客户端对应的目标私钥分片和完整公钥。进一步地, 基于目标客户端对应的身份关联信息生成目标客户端对应的签名请求, 将目标客户端对应的签名请求发送至服务端, 以使服务端对接收到的 $M-1$ 个签名请求中的身份关联信息进行合法身份验证。进一步地, 若检测到服务端确定 $M-1$ 个签名请求中的身份关联信息均为合法身份信息, 则向服务端发送目标客户端相关联的业务执行数据。进一步地, 若业务执行数据符合目标客户端的身份关联信息对应的风险管理策略, 则与发起签名请求的客户端以及服务端共同参与针对区块链业务的联合签名处理。其中, 联合签名处理所生成的联合签名结果是基于发起签名请求的客户端对应的目标私钥分片和服务端私钥分片共同生成, 联合签名结果用于提供给目标客户端执行区块链业务。本申请实施例通过将密钥分片协商得到本地私钥分片与目标私钥分片, 并且对于参加签名的客户端或者服务端进行身份关联信息验证, 在身份关联信息验证为合法身份信息后进行多端私钥分片的联合签名处理, 可以不再单纯使用一个私钥进行数字资产的签名处理过程, 从而降低了因私钥问题而出现签名出错的概率, 降低了使用数字资产的风险概率。应当理解, 本申请实施例中通过进行身份关联信息验证可以实现服务端对客户端身份信息的检测, 若客户端提供的身份信息不符合服务端身份数据库中存储的身份信息, 则对该客户端的签名请求进行拦截, 提升了服务端对于签名过程的安全掌控程度, 进而降低了使用数字资产的风险概率。而且, 本申请实施例中通过风险管理策略的验证对应用链上地址进行地址风险检测, 可以将监管单位发布的黑名单地址以及管制实体的地址进行过滤与拦截, 从而降低进行数字资产业务交互的风险性, 降低了使用数字资产的风险概率。此外, 本申请实施例还可以用于若服务端出现设备问题时, 通过两个客户端进行签名, 从而绕过出现故障的服务端进行签名处理, 提升了区块链业务的分布式系统应对风险的能力, 增加了区块链业务的分布式系统的安全性。本申请实施例中, 降低了使用数字资产的风险概率。

进一步地, 请参见图 6, 图 6 是本申请实施例提供的一种关于数字资产签名的交互流程图。如图 6 所示, 该方法可以由计算机设备执行, 该计算机设备可以包括图 6 中的客户端 600a 或者服务端 610。具体的, 该客户端 600a 可以为上述图 1 所示的区块链节点系统中的任意一个区块链节点, 例如, 区块链节点 10a, 服务端 610 可以为上述图 1 所示的区块链节点 10b, 在此不做限定。为便于理解, 本申请实施例以该方法由计算机设备执行为例进行说明, 该数据处理方法至少可以包括以下步骤 S60-步骤 S68:

步骤 S60, 获取与 N 个客户端分别进行通信的通信信道。

本步骤的具体过程可以参见上述图 3 所对应实施例中的 S101, 这里不再进行赘述。

步骤 S61, 基于 N 个通信信道分别与 N 个客户端进行密钥分片协商。

本步骤的具体过程可以参见上述图 3 所对应实施例中的 S101, 这里不再进行赘述。

步骤 S62, 得到本地私钥分片和完整公钥。

本步骤的具体过程可以参见上述图 3 所对应实施例中的 S101, 这里不再进行赘述。

步骤 S63, 得到目标私钥分片和完整公钥。

本步骤的具体过程可以参见上述图 4 所对应实施例中的 S201, 这里不再进行赘述。

步骤 S64, 获取目标分片公钥, 通过目标分片公钥进行对客户端的分片签名结果验证。

本步骤的具体过程可以参见上述图 3 所对应实施例中的 S101, 这里不再进行赘述。

步骤 S65, 获取本地分片公钥, 通过本地分片公钥进行对服务端的分片签名结果验证。

本步骤的具体过程可以参见上述图 4 所对应实施例中的 S201, 这里不再进行赘述。

步骤 S66, 若 $M-1$ 个签名验证结果均为验证成功结果, 则对 $M-1$ 个客户端所发送的签名请求中的身份关联信息进行合法身份验证。

本步骤的具体过程可以参见上述图 3 所对应实施例中的 S101, 这里不再进行赘述。

步骤 S67, 若 $M-1$ 个签名请求中的身份关联信息均为合法身份信息, 则获取目标客户端相关联的业务执行数据。

本步骤的具体过程可以参见上述图 3 所对应实施例中的 S103, 这里不再进行赘述。

步骤 S68, 若业务执行数据符合风险管理策略, 则进行联合签名处理。

本步骤的具体过程可以参见上述图 3 所对应实施例中的 S104, 这里不再进行赘述。

可选的, 客户端可以是一个或多个, 即 N 可以大于等于 1, N 的具体取值是由业务对象在应用客户端 (例如支付应用) 中请求多方共同生成一个完整公钥对应的完整私钥中参与方的数量所确定。此处以 4 个客户端与 1 个服务端共同参与支付应用的签名进行示例, 即业务对象请求 5 个参与方分别持有私钥分片 (即一个本地私钥分片与四个目标私钥分片)。也就是说, 服务端可以与 4 个客户端分别进行密钥分片协商, 生成五个分别独立的私钥分片 (即 1 个服务端对应的本地私钥分片与 4 个客户端对应的目标私钥分片)。

应当理解,生成的私钥分片仅在生成该私钥分片的设备内部可知,是生成该私钥分片的设备独自持有,不会对外公布。若构成完整私钥要求的参与方为3,则参与方可以是一个服务端与两个客户端,例如,一个服务端即为服务后台,两个客户端可以分别为手机端与电脑端(pc端),具体的,进行联合签名的过程可以参加上文图3与图4中的联合签名过程,进行类推,这里不再赘述。

应当理解的是,在本申请实施例中,通过设置私钥分片数量阈值,结合以服务端为中心的中心化风险管理策略,比现有的中心化托管方式的签名方案与现有的去中心化托管方式的签名方案,具有更加突出的优点,通过服务端侧的风险管理策略,可以降低业务对象对于区块链业务所对应的应用(如支付应用)的使用门槛,增加了使用区块链业务所对应的应用的便捷性。而且,本申请实施例中的通过目标客户端与签名客户端进行联合签名的方式,可以保障业务对象对于数字资产的自主性与可控性,降低了使用数字资产的风险概率。

本申请实施例中,通过获取与N个客户端分别进行通信的通信信道,基于N个通信信道分别与N个客户端进行密钥分片协商,得到本地私钥分片和完整公钥。进一步地,接收N个客户端中的M-1个客户端发送的签名请求,获取M-1个签名请求中的身份关联信息。进一步地,若M-1个签名请求中的身份关联信息均为合法身份信息,则将M-1个客户端中用于发起区块链业务的客户端,确定为目标客户端,获取目标客户端相关联的业务执行数据。进一步地,若业务执行数据符合目标客户端的身份关联信息对应的风险管理策略,则与M-1个客户端共同参与针对区块链业务的联合签名处理。其中,联合签名处理所生成的联合签名结果是基于本地私钥分片和M-1个客户端分别持有的目标私钥分片共同生成,联合签名结果用于提供给目标客户端执行区块链业务。本申请实施例通过将密钥分片协商得到本地私钥分片与目标私钥分片,并且对于参加签名的客户端或者服务端进行身份关联信息验证,在身份关联信息验证为合法身份信息后进行多端私钥分片的联合签名处理,可以不再单纯使用一个私钥进行数字资产的签名处理过程,从而降低了因私钥问题而出现签名出错的概率,降低了使用数字资产的风险概率。应当理解,本申请实施例中通过进行身份关联信息验证可以对客户端的身份关联信息进行安全性确认,进而降低了使用数字资产的风险概率。而且,本申请实施例中通过风险管理策略的验证对应用链上地址进行地址风险检测,可以将监管单位发布的黑名单地址以及管制实体的地址进行过滤与拦截,从而降低进行数字资产业务交互的风险性。本申请实施例中,降低了使用数字资产的风险概率。

进一步地,请参见图7,图7是本申请实施例提供的一种数据处理装置的结构示意图。上述数据处理装置可以是运行于计算机设备中的一个计算机程序(包括程序代码),例如该数据处理装置为一个应用软件;该装置可以用于执行本申请实施例提供的方法中的相应步骤。如图7所示,该数据处理装置1应用于业务管理平台,该数据处理装置1可以包括:本地私钥分片获取模块11、身份关联信息获取模块12、目标客户端确定模块13、业务执行数据获取模块14以及第一联合签名模块15。

本地私钥分片获取模块11,用于获取与N个客户端分别进行通信的通信信道,基于N个通信信道分别与N个客户端进行密钥分片协商,得到本地私钥分片和完整公钥;N为大于1的正整数;完整公钥是本地私钥分片和N个目标私钥分片共同对应的唯一公钥;N个目标私钥分片中的第i个目标私钥分片,是通过密钥分片协商后由N个客户端中的第i个客户端所独自持有的私钥分片;

身份关联信息获取模块12,用于接收N个客户端中的M-1个客户端发送的签名请求,获取M-1个签名请求中的身份关联信息;M为基于完整公钥进行验签的私钥分片数量阈值,M为小于等于N+1的正整数;

目标客户端确定模块13,用于若M-1个签名请求中的身份关联信息均为合法身份信息,则将M-1个客户端中用于发起区块链业务的客户端,确定为目标客户端;

业务执行数据获取模块14,用于获取目标客户端相关联的业务执行数据;

第一联合签名模块15,用于若业务执行数据符合目标客户端的身份关联信息对应的风险管理策略,则与M-1个客户端共同参与针对区块链业务的联合签名处理;联合签名处理所生成的联合签名结果是基于本地私钥分片和M-1个客户端分别持有的目标私钥分片共同生成,联合签名结果用于提供给目标客户端执行区块链业务。

其中,本地私钥分片获取模块11、身份关联信息获取模块12、目标客户端确定模块13、业务执行数据获取模块14以及第一联合签名模块15的具体功能实现方式可以参见上述图3对应实施例中的步骤S101-步骤S104,这里不再进行赘述。

再请参见图7,其中,本地私钥分片获取模块11,包括:

本地测试私钥生成单元111,用于随机生成用于进行密钥分片协商的本地测试私钥,通过本地测试私

钥对本地协商数据进行加密处理,得到本地测试信息;

通信信道获取单元 112,用于获取与 N 个客户端分别进行通信的通信信道,通过每个通信信道向 N 个客户端发送本地测试信息;

目标解密数据获取单元 113,用于接收 N 个客户端分别发送的目标测试公钥以及目标测试信息,通过目标测试公钥对属于同一客户端的目标测试信息进行解密,得到 N 个目标解密数据;一个目标测试公钥是指一个客户端所生成的用于进行密钥分片协商的目标测试私钥对应的公钥,一个目标测试信息是指在一个客户端中通过所生成的目标测试私钥对目标协商数据进行加密处理所得到的信息;

第一哈希结果确定单元 114,用于基于本地测试私钥对应的本地测试公钥对本地测试信息进行解密,得到本地解密数据,将本地解密数据以及 N 个目标解密数据确定为第一哈希结果;

第二哈希结果获取单元 115,用于对本地协商数据以及 N 个目标协商数据进行哈希运算,得到第二哈希结果;

本地私钥分片确定单元 116,用于若第一哈希结果与第二哈希结果相等,则确定密钥协商成功,将本地测试私钥确定为本地私钥分片;

完整公钥生成单元 117,用于在与 N 个客户端进行密钥分片协商的过程中生成完整公钥。

其中,本地测试私钥生成单元 111、通信信道获取单元 112、目标解密数据获取单元 113、第一哈希结果确定单元 114、第二哈希结果获取单元 115、本地私钥分片确定单元 116 以及完整公钥生成单元 117 的具体功能实现方式可以参见上述图 3 对应实施例中的步骤 S101,这里不再进行赘述。

再请参见图 7,其中,数据处理装置 1,还包括:

目标分片公钥获取模块 16,用于获取 M-1 个客户端分别对应的目标分片公钥;一个客户端对应的目标分片公钥是基于该客户端对应的目标私钥分片所生成的;

签名验证模块 17,用于通过 M-1 个目标分片公钥分别对 M-1 个客户端发送的分片签名结果进行签名验证,得到 M-1 个签名验证结果;一个分片签名结果是指一个客户端通过该客户端对应的目标私钥分片对身份关联信息进行签名后的数据;

合法身份验证模块 18,用于若 M-1 个签名验证结果均为验证成功结果,则对 M-1 个客户端所发送的签名请求中的身份关联信息进行合法身份验证。

其中,目标分片公钥获取模块 16、签名验证模块 17 以及合法身份验证模块 18 的具体功能实现方式可以参见上述图 3 对应实施例中的步骤 S101,这里不再进行赘述。

再请参见图 7,其中,M-1 个客户端包括客户端 S_i ,i 为小于或等于 M-1 的正整数;合法身份验证模块 18,包括:

业务类型获取单元 181,用于获取 M-1 个客户端所关联发起的区块链业务的业务类型,获取客户端 S_i 对应的身份关联信息中的身份标识以及身份特征数据;

身份验证策略确定单元 182,用于确定业务类型所匹配的身份验证策略,在身份标识以及身份特征数据中,选取与身份验证策略所指示的验证维度匹配的数据,作为待验证数据;

合法身份信息确定单元 183,用于若待验证数据存在于身份数据库中,则确定客户端 S_i 对应的签名请求中的身份关联信息为合法身份信息。

其中,业务类型获取单元 181、身份验证策略确定单元 182 以及合法身份信息确定单元 183 的具体功能实现方式可以参见上述图 3 对应实施例中的步骤 S101,这里不再进行赘述。

再请参见图 7,其中,业务执行数据获取模块 14,具体用于获取目标客户端的历史业务执行数据以及所发起的区块链业务中的目标业务执行数据,将历史业务执行数据和目标业务执行数据确定为目标客户端相关联的业务执行数据;

其中,数据处理装置 1,还包括:

业务阈值设置模块 19,用于对业务执行数据中的历史业务执行数据进行数据分析,得到历史业务操作范围,基于历史业务操作范围,设置业务阈值;

风险管理策略确定模块 20,用于若业务执行数据中的目标业务执行数据小于等于业务阈值,则确定业务执行数据符合目标客户端的身份关联信息对应的风险管理策略。

其中,业务阈值设置模块 19 以及风险管理策略确定模块 20 的具体功能实现方式可以参见上述图 3 对应实施例中的步骤 S101,这里不再进行赘述。

再请参见图 7,其中,数据处理装置 1,还包括:

地址风险检测模块 21,用于从业务执行数据中获取目标客户端对应的应用链上地址,对应用链上地址

进行地址风险检测；

第一地址检测模块 22，用于若检测到应用链上地址存在于合法地址名单中，则确定业务执行数据符合目标客户端的身份关联信息对应的风险管理策略；

第二地址检测模块 23，用于若检测到应用链上地址不存在于合法地址名单中，则确定应用链上地址为风险性地址，禁止响应目标客户端所发起的区块链业务。

其中，地址风险检测模块 21、第一地址检测模块 22 以及第二地址检测模块 23 的具体功能实现方式可以参见上述图 3 对应实施例中的步骤 S101，这里不再进行赘述。

再请参见图 7，其中，M-1 个客户端包括目标客户端；第一联合签名模块 15，包括：

服务端签名结果获取单元 151，用于接收目标客户端发送的经过目标客户端对应的目标私钥分片进行加密处理后的中间加密结果，通过本地私钥分片对接收到的中间加密结果进行签名，得到服务端签名结果；

联合签名结果生成单元 152，用于将服务端签名结果发送至目标客户端；服务端签名结果用于指示目标客户端生成联合签名结果。

其中，服务端签名结果获取单元 151 以及联合签名结果生成单元 152 的具体功能实现方式可以参见上述图 3 对应实施例中的步骤 S104，这里不再进行赘述。

再请参见图 7，其中，数据处理装置 1，还包括：

业务数据接收模块 24，用于接收目标客户端发送的待上链业务数据；待上链业务数据由区块链业务中的目标业务执行数据和联合签名结果组成；

业务数据转发模块 25，用于将待上链业务数据转发至区块链共识网络，以使区块链共识网络在共识过程中基于完整公钥对联合签名结果进行验签，在共识通过时，将目标业务执行数据所对应的执行结果数据存储至区块链账本中。

其中，业务数据接收模块 24 以及业务数据转发模块 25 的具体功能实现方式可以参见上述图 3 对应实施例中的步骤 S104，这里不再进行赘述。

再请参见图 7，其中，数据处理装置 1，还包括：

目标业务地址生成模块 26，用于基于完整公钥生成目标业务地址；

待验证地址获取模块 27，用于获取 N 个客户端分别发送的待验证地址；一个客户端发送的待验证地址是基于完整公钥所生成的；

合法地址确定模块 28，用于若目标业务地址与 N 个待验证地址均相同，则确定目标业务地址为合法地址，且将目标业务地址确定为应用链上地址；

待验证地址删除模块 29，用于若 N 个待验证地址中存在与目标业务地址不同的待验证地址，则删除已生成的目标业务地址与 N 个待验证地址，向 N 个客户端发送重新生成应用链上地址请求；重新生成应用链上地址请求用于指示 N 个客户端重新基于完整公钥生成新的待验证地址。

其中，目标业务地址生成模块 26、待验证地址获取模块 27、合法地址确定模块 28 以及待验证地址删除模块 29 的具体功能实现方式可以参见上述图 3 对应实施例中的步骤 S104，这里不再进行赘述。

进一步地，请参见图 8，图 8 是本申请实施例提供的一种数据处理装置的结构示意图。上述数据处理装置可以是运行于计算机设备中的一个计算机程序（包括程序代码），例如该数据处理装置为一个应用软件；该装置可以用于执行本申请实施例提供的方法中的相应步骤。如图 8 所示，该数据处理装置 3 应用于业务管理平台，该数据处理装置 3 可以包括：目标私钥分片获取模块 31、签名请求发送模块 32、业务执行数据发送模块 33 以及第二联合签名模块 34。

目标私钥分片获取模块 31，用于目标客户端获取分别与 N-1 个客户端以及服务端进行通信的通信信道，基于通信信道与服务端以及 N-1 个客户端进行密钥分片协商，得到目标客户端对应的目标私钥分片和完整公钥；N 为大于 1 的正整数；完整公钥是目标客户端对应的目标私钥分片、服务端私钥分片和 N-1 个客户端对应的目标私钥分片共同对应的唯一公钥；N-1 个客户端对应的目标私钥分片中的第 i 个目标私钥分片，是通过密钥分片协商后由 N-1 个客户端中的第 i 个客户端所独自持有的私钥分片；服务端私钥分片是通过密钥分片协商后由服务端所独自持有的私钥分片；

签名请求发送模块 32，用于基于目标客户端对应的身份关联信息生成目标客户端对应的签名请求，将目标客户端对应的签名请求发送至服务端，以使服务端对接收到的 M-1 个签名请求中的身份关联信息进行合法身份验证；M-1 个签名请求包括目标客户端对应的签名请求；M 为基于完整公钥进行验签的私钥分片数量阈值，M 为小于等于 N+1 的正整数；

业务执行数据发送模块 33，用于若检测到服务端确定 M-1 个签名请求中的身份关联信息均为合法身

份信息, 则向服务端发送目标客户端相关联的业务执行数据;

第二联合签名模块 34, 用于若业务执行数据符合目标客户端的身份关联信息对应的风险管理策略, 则与发起签名请求的客户端以及服务端共同参与针对区块链业务的联合签名处理; 联合签名处理所生成的联合签名结果是基于发起签名请求的客户端对应的目标私钥分片和服务端私钥分片共同生成, 联合签名结果用于提供给目标客户端执行区块链业务。

其中, 目标私钥分片获取模块 31、签名请求发送模块 32、业务执行数据发送模块 33 以及第二联合签名模块 34 的具体功能实现方式可以参见上述图 4 应实施例中的步骤 S201-步骤 S204, 这里不再进行赘述。

再请参见图 8, 其中, M-1 个客户端包括目标客户端与签名客户端; 数据处理装置 3, 还包括:

第一加密模块 35, 用于若接收到服务端发送的服务端故障信息, 则通过目标客户端对应的目标私钥分片, 对获取到的待签名信息进行加密处理, 得到初始签名结果;

第二加密模块 36, 用于将初始签名结果发送至签名客户端, 以使签名客户端通过签名客户端对应的目标私钥分片对初始签名结果进行加密处理, 得到目标签名结果;

目标签名结果接收模块 37, 用于接收签名客户端发送的目标签名结果, 基于目标签名结果生成联合签名结果。

其中, 第一加密模块 35、第二加密模块 36 以及目标签名结果接收模块 37 的具体功能实现方式可以参见上述图 4 应实施例中的步骤 S201, 这里不再进行赘述。

其中, 签名请求发送模块 32, 包括:

数据显示单元 321, 用于在区块链功能界面中显示业务发起控件、目标客户端对应的应用链上地址与虚拟资源数据; 虚拟资源数据用于表示目标客户端对应的区块链业务账号中的业务数据;

操作响应单元 322, 用于响应针对区块链功能界面中的业务发起控件的发起区块链业务操作, 将基于目标客户端对应的身份关联信息生成的目标客户端对应的签名请求发送至服务端;

其中, 数据显示单元 321 以及操作响应单元 322 的具体功能实现方式可以参见上述图 4 应实施例中的步骤 S202, 这里不再进行赘述。

其中, 数据处理装置 3, 还包括:

数据发送模块 38, 用于将待上链业务数据向服务端进行发送; 待上链业务数据由区块链业务中的目标业务执行数据和联合签名结果组成;

反馈数据接收模块 39, 用于若区块链共识网络基于完整公钥对联合签名结果验签成功, 且对待上链业务数据共识通过, 则接收服务端发送的针对待上链业务数据的反馈数据, 在区块链功能界面中基于反馈数据更新显示虚拟资源数据。

其中, 数据发送模块 38 以及反馈数据接收模块 39 的具体功能实现方式可以参见上述图 4 应实施例中的步骤 S201, 这里不再进行赘述。

进一步地, 请参见图 9, 图 9 是本申请实施例提供的一种计算机设备的结构示意图。如图 9 所示, 该计算机设备 1000 可以包括: 至少一个处理器 1001, 例如 CPU, 至少一个网络接口 1004, 用户接口 1003, 存储器 1005, 至少一个通信总线 1002。其中, 通信总线 1002 用于实现这些组件之间的连接通信。其中, 用户接口 1003 可以包括显示屏 (Display)、键盘 (Keyboard), 网络接口 1004 可选地可以包括标准的有线接口、无线接口 (如 WI-FI 接口)。存储器 1005 可以是高速 RAM 存储器, 也可以是非不稳定的存储器 (non-volatile memory), 例如至少一个磁盘存储器。存储器 1005 可选地还可以是至少一个位于远离前述处理器 1001 的存储装置。如图 9 所示, 作为一种计算机存储介质的存储器 1005 可以包括操作系统、网络通信模块、用户接口模块以及设备控制应用程序。

在图 9 所示的计算机设备 1000 中, 网络接口 1004 可提供网络通讯功能; 而用户接口 1003 主要用于为用户提供输入的接口; 而处理器 1001 可以用于调用存储器 1005 中存储的设备控制应用程序, 以实现:

获取与 N 个客户端分别进行通信的通信信道, 基于 N 个通信信道分别与 N 个客户端进行密钥分片协商, 得到本地私钥分片和完整公钥; N 为大于 1 的正整数; 完整公钥是本地私钥分片和 N 个目标私钥分片共同对应的唯一公钥; N 个目标私钥分片中的第 i 个目标私钥分片, 是通过密钥分片协商后由 N 个客户端中的第 i 个客户端所独自持有的私钥分片; 接收 N 个客户端中的 M-1 个客户端发送的签名请求, 获取 M-1 个签名请求中的身份关联信息; M 为基于完整公钥进行验签的私钥分片数量阈值, M 为小于等于 N+1 的正整数; 若 M-1 个签名请求中的身份关联信息均为合法身份信息, 则将 M-1 个客户端中用于发起区块链业务的客户端, 确定为目标客户端, 获取目标客户端相关联的业务执行数据; 若业务执行数据符合目标客户端的身份关联信息对应的风险管理策略, 则与 M-1 个客户端共同参与针对区块链业务的联合签名处理;

联合签名处理所生成的联合签名结果是基于本地私钥分片和 $M-1$ 个客户端分别持有的目标私钥分片共同生成, 联合签名结果用于提供给目标客户端执行区块链业务。

在图 9 所示的计算机设备 1000 中, 网络接口 1004 可提供网络通讯功能; 而用户接口 1003 主要用于为用户提供输入的接口; 而处理器 1001 可以用于调用存储器 1005 中存储的设备控制应用程序, 以实现:

目标客户端获取分别与 $N-1$ 个客户端以及服务端进行通信的通信信道, 基于通信信道与服务端以及 $N-1$ 个客户端进行密钥分片协商, 得到目标客户端对应的目标私钥分片和完整公钥; N 为大于 1 的正整数: 完整公钥是目标客户端对应的目标私钥分片、服务端私钥分片和 $N-1$ 个客户端对应的目标私钥分片共同对应的唯一公钥; $N-1$ 个客户端对应的目标私钥分片中的第 i 个目标私钥分片, 是通过密钥分片协商后由 $N-1$ 个客户端中的第 i 个客户端所独自持有的私钥分片; 服务端私钥分片是通过密钥分片协商后由服务端所独自持有的私钥分片; 基于目标客户端对应的身份关联信息生成目标客户端对应的签名请求, 将目标客户端对应的签名请求发送至服务端, 以使服务端对接收到的 $M-1$ 个签名请求中的身份关联信息进行合法身份验证; $M-1$ 个签名请求包括目标客户端对应的签名请求; M 为基于完整公钥进行验签的私钥分片数量阈值, M 为小于等于 $N+1$ 的正整数; 若检测到服务端确定 $M-1$ 个签名请求中的身份关联信息均为合法身份信息, 则向服务端发送目标客户端相关联的业务执行数据; 若业务执行数据符合目标客户端的身份关联信息对应的风险管理策略, 则与发起签名请求的客户端以及服务端共同参与针对区块链业务的联合签名处理; 联合签名处理所生成的联合签名结果是基于发起签名请求的客户端对应的目标私钥分片和服务端私钥分片共同生成, 联合签名结果用于提供给目标客户端执行区块链业务。

应当理解, 本申请实施例中所描述的计算机设备 1000 可执行前文图 2、图 3、图 4、图 5 以及图 6 所对应实施例中对数据处理方法的描述, 也可执行前文图 7 所对应实施例中对数据处理装置 1 的描述, 也可执行前文图 8 所对应实施例中对数据处理装置 3 的描述, 在此不再赘述。另外, 对采用相同方法的有益效果描述, 也不再进行赘述。

本申请实施例还提供一种计算机可读存储介质, 该计算机可读存储介质存储有计算机程序, 该计算机程序包括程序指令, 该程序指令被处理器执行时实现图 2、图 3、图 4、图 5 以及图 6 中各个步骤所提供的数据处理方法, 具体可参见上述图 2、图 3、图 4、图 5 以及图 6 各个步骤所提供的实现方式, 在此不再赘述。另外, 对采用相同方法的有益效果描述, 也不再进行赘述。

上述计算机可读存储介质可以是前述任一实施例提供的数据处理装置或者上述计算机设备的内部存储单元, 例如计算机设备的硬盘或内存。该计算机可读存储介质也可以是该计算机设备的外部存储设备, 例如该计算机设备上配备的插接式硬盘, 智能存储卡 (smart media card, SMC), 安全数字 (secure digital, SD) 卡, 闪存卡 (flash card) 等。进一步地, 该计算机可读存储介质还可以既包括该计算机设备的内部存储单元也包括外部存储设备。该计算机可读存储介质用于存储该计算机程序以及该计算机设备所需的其他程序和数据。该计算机可读存储介质还可以用于暂时地存储已经输出或者将要输出的数据。

本申请实施例还提供了一种计算机程序产品或计算机程序, 该计算机程序产品或计算机程序包括计算机指令, 该计算机指令存储在计算机可读存储介质中。计算机设备的处理器从计算机可读存储介质读取该计算机指令, 处理器执行该计算机指令, 使得该计算机设备可执行前文图 2、图 3、图 4、图 5 以及图 6 所对应实施例中对数据处理方法的描述, 在此不再赘述。另外, 对采用相同方法的有益效果描述, 也不再进行赘述。

本申请实施例的说明书和权利要求书及附图中的术语“包括”以及它们任何变形, 意图在于覆盖不排除他的包含。例如包含了一系列步骤或单元的过程、方法、装置、产品或设备没有限定于已列出的步骤或模块, 而是可选地还包括没有列出的步骤或模块, 或可选地还包括对于这些过程、方法、装置、产品或设备固有的其他步骤单元。

本领域普通技术人员可以意识到, 结合本文中所公开的实施例描述的各示例的单元及算法步骤, 能够以电子硬件、计算机软件或者二者的结合来实现, 为了清楚地说明硬件和软件的可互换性, 在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行, 取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能, 但是这种实现不应认为超出本申请的范围。

本申请实施例提供的方法及相关装置是参照本申请实施例提供的方法流程图和/或结构示意图来描述的, 具体可由计算机程序指令实现方法流程图和/或结构示意图的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。这些计算机程序指令可提供到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器, 使得通过计算机或其他可编程数据处理设备的处理器

执行的指令产生用于实现在流程图一个流程或多个流程和/或结构示意图一个方框或多个方框中指定的功能的装置。这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或结构示意图一个方框或多个方框中指定的功能。这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或结构示意图一个方框或多个方框中指定的功能的步骤。

以上所揭露的仅为本申请较佳实施例而已，当然不能以此来限定本申请之权利范围，因此依本申请权利要求所作的等同变化，仍属本申请所涵盖的范围。

权利要求书

1、一种基于区块链密钥的数据处理方法，其特征在于，包括：

获取与N个客户端分别进行通信的通信信道，基于N个通信信道分别与所述N个客户端进行密钥分片协商，得到本地私钥分片和完整公钥；N为大于1的正整数；所述完整公钥是所述本地私钥分片和N个目标私钥分片共同对应的唯一公钥；所述N个目标私钥分片中的第i个目标私钥分片，是通过所述密钥分片协商后由所述N个客户端中的第i个客户端所独自持有的私钥分片；

接收所述N个客户端中的M-1个客户端发送的签名请求，获取M-1个签名请求中的身份关联信息；所述M为基于所述完整公钥进行验签的私钥分片数量阈值，M为小于等于N+1的正整数；

若M-1个签名请求中的身份关联信息均为合法身份信息，则将所述M-1个客户端中用于发起区块链业务的客户端，确定为目标客户端，获取所述目标客户端相关联的业务执行数据；

若所述业务执行数据符合所述目标客户端的身份关联信息对应的风险管理策略，则与所述M-1个客户端共同参与针对所述区块链业务的联合签名处理；所述联合签名处理所生成的联合签名结果是基于所述本地私钥分片和所述M-1个客户端分别持有的目标私钥分片共同生成，所述联合签名结果用于提供给所述目标客户端执行所述区块链业务。

2、根据权利要求1所述的方法，其特征在于，所述方法还包括：

获取所述M-1个客户端分别对应的目标分片公钥；一个客户端对应的目标分片公钥是基于该客户端对应的目标私钥分片所生成的；

通过M-1个目标分片公钥分别对所述M-1个客户端发送的分片签名结果进行签名验证，得到M-1个签名验证结果；一个所述分片签名结果是指一个客户端通过该客户端对应的目标私钥分片对身份关联信息进行签名后的数据；

若所述M-1个签名验证结果均为验证成功结果，则对所述M-1个客户端所发送的签名请求中的身份关联信息进行合法身份验证。

3、根据权利要求1或2所述的方法，其特征在于，所述M-1个客户端包括客户端 S_i ，i为小于或等于M-1的正整数；所述对所述M-1个客户端所发送的签名请求中的身份关联信息进行合法身份验证，包括：

获取所述M-1个客户端所关联发起的区块链业务的业务类型，获取客户端 S_i 对应的身份关联信息中的身份标识以及身份特征数据；

确定所述业务类型所匹配的身份验证策略，在所述身份标识以及所述身份特征数据中，选取与所述身份验证策略所指示的验证维度匹配的数据，作为待验证数据；

若所述待验证数据存在于身份数据库中，则确定所述客户端 S_i 对应的签名请求中的身份关联信息为合法身份信息。

4、根据权利要求1至3任一项所述的方法，其特征在于，所述获取所述目标客户端相关联的业务执行数据，包括：

获取所述目标客户端的历史业务执行数据以及所发起的区块链业务中的目标业务执行数据，将所述历史业务执行数据和所述目标业务执行数据确定为所述目标客户端相关联的业务执行数据；

所述方法还包括：

对所述业务执行数据中的历史业务执行数据进行数据分析，得到历史业务操作范围，基于所述历史业务操作范围，设置业务阈值；

若所述业务执行数据中的目标业务执行数据小于等于所述业务阈值，则确定所述业务执行数据符合所述目标客户端的身份关联信息对应的风险管理策略。

5、根据权利要求1至4任一项所述的方法，其特征在于，还包括：

从所述业务执行数据中获取所述目标客户端对应的应用链上地址，对所述应用链上地址进行地址风险检测；

若检测到所述应用链上地址存在于合法地址名单中，则确定所述业务执行数据符合所述目标客户端的身份关联信息对应的风险管理策略；

若检测到所述应用链上地址不存在于所述合法地址名单中，则确定所述应用链上地址为风险性地址，禁止响应所述目标客户端所发起的区块链业务。

6、根据权利要求1至5任一项所述的方法，其特征在于，所述与所述M-1个客户端共同参与针对所述区块链业务的联合签名处理，包括：

接收所述目标客户端发送的经过所述目标客户端对应的目标私钥分片进行加密处理后的中间加密结

果,通过所述本地私钥分片对接收到的中间加密结果进行签名,得到服务端签名结果;

将所述服务端签名结果发送至所述目标客户端;所述服务端签名结果用于指示所述目标客户端生成联合签名结果。

7、根据权利要求1至6任一项所述的方法,其特征在于,还包括:

接收所述目标客户端发送的待上链业务数据;所述待上链业务数据由所述区块链业务中的目标业务执行数据和所述联合签名结果组成;

将所述待上链业务数据转发至区块链共识网络,以使所述区块链共识网络在共识过程中基于所述完整公钥对所述联合签名结果进行验签,在共识通过时,将所述目标业务执行数据所对应的执行结果数据存储至区块链账本中。

8、根据权利要求1至7任一项所述的方法,其特征在于,还包括:

基于所述完整公钥生成目标业务地址;

获取所述N个客户端分别发送的待验证地址;一个客户端发送的待验证地址是基于所述完整公钥所生成的;

若所述目标业务地址与N个待验证地址均相同,则确定所述目标业务地址为合法地址,且将所述目标业务地址确定为应用链上地址;

若所述N个待验证地址中存在与所述目标业务地址不同的待验证地址,则删除已生成的所述目标业务地址与所述N个待验证地址,向所述N个客户端发送重新生成应用链上地址请求;所述重新生成应用链上地址请求用于指示所述N个客户端重新基于所述完整公钥生成新的待验证地址。

9、根据权利要求1至8任一项所述的方法,其特征在于,所述获取与N个客户端分别进行通信的通信信道,基于N个通信信道分别与所述N个客户端进行密钥分片协商,得到本地私钥分片和完整公钥,包括:

随机生成用于进行密钥分片协商的本地测试私钥,通过所述本地测试私钥对本地协商数据进行加密处理,得到本地测试信息;

获取与N个客户端分别进行通信的通信信道,通过每个通信信道向所述N个客户端发送所述本地测试信息;

接收所述N个客户端分别发送的目标测试公钥以及目标测试信息,通过所述目标测试公钥对属于同一客户端的目标测试信息进行解密,得到N个目标解密数据;一个所述目标测试公钥是指一个客户端所生成的用于进行密钥分片协商的目标测试私钥对应的公钥,一个所述目标测试信息是指在一个客户端中通过所生成的目标测试私钥对目标协商数据进行加密处理所得到的信息;

基于所述本地测试私钥对应的本地测试公钥对所述本地测试信息进行解密,得到本地解密数据,将所述本地解密数据以及所述N个目标解密数据确定为第一哈希结果;

对所述本地协商数据以及N个目标协商数据进行哈希运算,得到第二哈希结果;

若所述第一哈希结果与所述第二哈希结果相等,则确定密钥协商成功,将所述本地测试私钥确定为本地私钥分片;

在与所述N个客户端进行密钥分片协商的过程中生成完整公钥。

10、一种基于区块链密钥的数据处理方法,其特征在于,所述方法由用于发起区块链业务的目标客户端执行,所述方法包括:

目标客户端获取分别与N-1个客户端以及服务端进行通信的通信信道,基于所述通信信道与所述服务端以及所述N-1个客户端进行密钥分片协商,得到所述目标客户端对应的目标私钥分片和完整公钥;N为大于1的正整数;所述完整公钥是所述目标客户端对应的目标私钥分片、服务端私钥分片和所述N-1个客户端对应的目标私钥分片共同对应的唯一公钥;所述N-1个客户端对应的目标私钥分片中的第i个目标私钥分片,是通过所述密钥分片协商后由所述N-1个客户端中的第i个客户端所独自持有的私钥分片;所述服务端私钥分片是通过所述密钥分片协商后由所述服务端所独自持有的私钥分片;

基于所述目标客户端对应的身份关联信息生成所述目标客户端对应的签名请求,将所述目标客户端对应的签名请求发送至所述服务端,以使所述服务端对接收到的M-1个签名请求中的身份关联信息进行合法身份验证;所述M-1个签名请求包括所述目标客户端对应的签名请求;所述M为基于所述完整公钥进行验签的私钥分片数量阈值,M为小于等于N+1的正整数;

若检测到所述服务端确定所述M-1个签名请求中的身份关联信息均为合法身份信息,则向所述服务端发送所述目标客户端相关联的业务执行数据;

若所述业务执行数据符合所述目标客户端的身份关联信息对应的风险管理策略,则与发起签名请求的客户端以及所述服务端共同参与针对所述区块链业务的联合签名处理;所述联合签名处理所生成的联合签名结果是基于所述发起签名请求的客户端对应的目标私钥分片和服务端私钥分片共同生成,所述联合签名结果用于提供给所述目标客户端执行所述区块链业务。

11、根据权利要求 10 所述的方法,其特征在于,所述 M-1 个客户端包括所述目标客户端与签名客户端;所述方法还包括:

若接收到所述服务端发送的服务端故障信息,则通过所述目标客户端对应的目标私钥分片,对获取到的待签名信息进行加密处理,得到初始签名结果;

将所述初始签名结果发送至所述签名客户端,以使所述签名客户端通过所述签名客户端对应的目标私钥分片对所述初始签名结果进行加密处理,得到目标签名结果;

接收所述签名客户端发送的所述目标签名结果,基于所述目标签名结果生成所述联合签名结果。

12、根据权利要求 10 或 11 所述的方法,其特征在于,所述基于所述目标客户端对应的身份关联信息生成所述目标客户端对应的签名请求,将所述目标客户端对应的签名请求发送至所述服务端,包括:

在区块链功能界面中显示业务发起控件、所述目标客户端对应的应用链上地址与虚拟资源数据;所述虚拟资源数据用于表示所述目标客户端对应的区块链业务账号中的业务数据;

响应针对所述区块链功能界面中的所述业务发起控件的发起区块链业务操作,将基于所述目标客户端对应的身份关联信息生成的所述目标客户端对应的签名请求发送至所述服务端;

所述方法还包括:

将待上链业务数据向所述服务端进行发送;所述待上链业务数据由所述区块链业务中的目标业务执行数据和所述联合签名结果组成;

若区块链共识网络基于所述完整公钥对所述联合签名结果验签成功,且对所述待上链业务数据共识通过,则接收所述服务端发送的针对所述待上链业务数据的反馈数据,在所述区块链功能界面中基于所述反馈数据更新显示所述虚拟资源数据。

13、一种基于区块链密钥的数据处理装置,其特征在于,所述数据处理装置,包括:

本地私钥分片获取模块,用于获取与 N 个客户端分别进行通信的通信信道,基于 N 个通信信道分别与 N 个客户端进行密钥分片协商,得到本地私钥分片和完整公钥;N 为大于 1 的正整数;完整公钥是本地私钥分片和 N 个目标私钥分片共同对应的唯一公钥;N 个目标私钥分片中的第 i 个目标私钥分片,是通过密钥分片协商后由 N 个客户端中的第 i 个客户端所独自持有的私钥分片;

身份关联信息获取模块,用于接收 N 个客户端中的 M-1 个客户端发送的签名请求,获取 M-1 个签名请求中的身份关联信息;M 为基于完整公钥进行验签的私钥分片数量阈值,M 为小于等于 N+1 的正整数;

目标客户端确定模块,用于若 M-1 个签名请求中的身份关联信息均为合法身份信息,则将 M-1 个客户端中用于发起区块链业务的客户端,确定为目标客户端;

业务执行数据获取模块,用于获取目标客户端相关联的业务执行数据;

第一联合签名模块,用于若业务执行数据符合目标客户端的身份关联信息对应的风险管理策略,则与 M-1 个客户端共同参与针对区块链业务的联合签名处理;联合签名处理所生成的联合签名结果是基于本地私钥分片和 M-1 个客户端分别持有的目标私钥分片共同生成,联合签名结果用于提供给目标客户端执行区块链业务。

14、一种基于区块链密钥的数据处理装置,其特征在于,所述数据处理装置,包括:

目标私钥分片获取模块,用于目标客户端获取分别与 N-1 个客户端以及服务端进行通信的通信信道,基于通信信道与服务端以及 N-1 个客户端进行密钥分片协商,得到目标客户端对应的目标私钥分片和完整公钥;N 为大于 1 的正整数;完整公钥是目标客户端对应的目标私钥分片、服务端私钥分片和 N-1 个客户端对应的目标私钥分片共同对应的唯一公钥;N-1 个客户端对应的目标私钥分片中的第 i 个目标私钥分片,是通过密钥分片协商后由 N-1 个客户端中的第 i 个客户端所独自持有的私钥分片;服务端私钥分片是通过密钥分片协商后由服务端所独自持有的私钥分片;

签名请求发送模块,用于基于目标客户端对应的身份关联信息生成目标客户端对应的签名请求,将目标客户端对应的签名请求发送至服务端,以使服务端对接收到的 M-1 个签名请求中的身份关联信息进行合法身份验证;M-1 个签名请求包括目标客户端对应的签名请求;M 为基于完整公钥进行验签的私钥分片数量阈值,M 为小于等于 N+1 的正整数;

业务执行数据发送模块,用于若检测到服务端确定 M-1 个签名请求中的身份关联信息均为合法身份信

息，则向服务端发送目标客户端相关联的业务执行数据；

第二联合签名模块，用于若业务执行数据符合目标客户端的身份关联信息对应的风险管理策略，则与发起签名请求的客户端以及服务端共同参与针对区块链业务的联合签名处理；联合签名处理所生成的联合签名结果是基于发起签名请求的客户端对应的目标私钥分片和服务端私钥分片共同生成，联合签名结果用于提供给目标客户端执行区块链业务。

15、一种的计算机设备，其特征在于，包括：处理器、存储器以及网络接口；

处理器与存储器、网络接口相连，其中，网络接口用于提供数据通信功能，存储器用于存储计算机程序，处理器用于调用计算机程序，以使得计算机设备执行权利要求 1-12 任一项所述的方法。

16、一种的计算机可读存储介质，其特征在于，计算机可读存储介质中存储有计算机程序，计算机程序适于由处理器加载并执行，以使得具有处理器的计算机设备执行权利要求 1-12 任一项所述的方法。