(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 115811412 B
(45)授权公告日 2024.12.24

(21)申请号 202210837363.5
(22)申请日 2022.07.15
(65)同一申请的已公布的文献号
申请公布号 CN 115811412 A
(43)申请公布日 2023.03.17
(73)专利权人 中国电信股份有限公司
地址 100033 北京市西城区金融大街31号
(72)发明人 梁伟 卢毅 刘岩
(74)专利代理机构 北京律智知识产权代理有限公司 11438
专利代理师 孙宝海
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/32(2006.01)
H04L 9/06(2006.01)

(56)对比文件
CN 108696870 A,2018.10.23
CN 111787530 A,2020.10.16

审查员 郭风顺

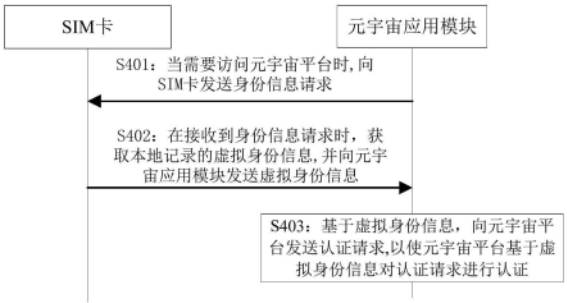
权利要求书5页 说明书14页 附图7页

(54)发明名称

一种通信方法、装置、SIM卡、电子设备和终端设备

(57)摘要

本公开实施例提供了一种通信方法、装置、SIM卡、电子设备和终端设备,涉及元宇宙技术领域。元宇宙应用模块,用于当需要访问元宇宙平台时,向SIM卡发送身份信息请求;还用于基于虚拟身份信息,向元宇宙平台发送认证请求,以使元宇宙平台基于虚拟身份信息对认证请求进行认证。SIM卡,用于在接收到身份信息请求时,获取本地记录的虚拟身份信息,并向元宇宙应用模块发送虚拟身份信息;其中,虚拟身份信息为:登录元宇宙应用模块的第一用户在注册SIM卡时,SIM卡基于第一用户的私钥生成得到的;第一用户的私钥为对预设随机数进行哈希计算得到的。能够降低虚拟身份信息泄露的风险,有利于用户的隐私保护。



CN 115811412 B

1.一种终端设备,其特征在于,包括:区块链用户身份模块BSIM卡;并安装有元宇宙应用模块,其中:

所述元宇宙应用模块,用于当需要访问元宇宙平台时,向所述BSIM卡发送身份信息请求;

所述BSIM卡,用于在接收到所述身份信息请求时,获取本地记录的虚拟身份信息,并向所述元宇宙应用模块发送所述虚拟身份信息;其中,所述虚拟身份信息为:登录所述元宇宙应用模块的第一用户在注册所述BSIM卡时,所述BSIM卡基于所述第一用户的私钥生成得到的,其包括:基于哈希算法对所述第一用户的私钥进行处理,得到一个固定长度的字符串,作为第一哈希值;获取第一哈希值的第一数值长度的字节,将所述第一数值长度的字节作为第二哈希值;在所述第二哈希值前添加DID角色类型字节,将添加DID角色类型字节后的第二哈希值作为第三哈希值;基于哈希算法对所述第三哈希值进行计算,得到第四哈希值;获取第四哈希值的第二数值长度的字节,并将第二数值长度的字节与所述第三哈希值拼接,得到的拼接后的值作为第五哈希值;对所述第五哈希值进行编码处理,得到所述第一用户对应的DID,作为第一用户的虚拟身份信息;所述第一用户的私钥为对预设随机数进行哈希计算得到的;

所述元宇宙应用模块,还用于基于所述虚拟身份信息,向所述元宇宙平台发送认证请求,以使所述元宇宙平台基于所述虚拟身份信息对所述认证请求进行认证。

2.一种通信方法,其特征在于,应用于终端设备中的元宇宙应用模块,所述终端设备还包括BSIM卡,所述方法包括:

当需要访问元宇宙平台时,向所述BSIM卡发送身份信息请求,以使所述BSIM卡在接收到所述身份信息请求时,获取本地记录的虚拟身份信息,并向所述元宇宙应用模块发送所述虚拟身份信息;其中,所述虚拟身份信息为:登录所述元宇宙应用模块的第一用户在注册所述BSIM卡时,所述BSIM卡基于所述第一用户的私钥生成得到的,其包括:基于哈希算法对所述第一用户的私钥进行处理,得到一个固定长度的字符串,作为第一哈希值;获取第一哈希值的第一数值长度的字节,将所述第一数值长度的字节作为第二哈希值;在所述第二哈希值前添加DID角色类型字节,将添加DID角色类型字节后的第二哈希值作为第三哈希值;基于哈希算法对所述第三哈希值进行计算,得到第四哈希值;获取第四哈希值的第二数值长度的字节,并将第二数值长度的字节与所述第三哈希值拼接,得到的拼接后的值作为第五哈希值;对所述第五哈希值进行编码处理,得到所述第一用户对应的DID,作为第一用户的虚拟身份信息;所述第一用户的私钥为对预设随机数进行哈希计算得到的;

基于所述虚拟身份信息,向所述元宇宙平台发送认证请求,以使所述元宇宙平台基于所述虚拟身份信息对所述认证请求进行认证。

3.根据权利要求2所述的方法,其特征在于,所述方法还包括:

获取所述第一用户在所述元宇宙平台中的交易记录;

向所述BSIM卡发送所述交易记录,以使所述BSIM卡基于所述第一用户的私钥对所述交易记录进行加密处理,得到对应的数字签名,并向所述元宇宙应用模块发送所述数字签名;

从所述BSIM卡获取所述数字签名,并向所述元宇宙平台发送所述交易记录和所述数字签名。

4.根据权利要求2所述的方法,其特征在于,所述方法还包括:

当检测到所述第一用户在所述元宇宙平台中获取到虚拟资产时,向所述BSIM卡发送所述虚拟资产,以使所述BSIM卡基于所述虚拟身份信息生成所述虚拟资产的唯一标识,并在本地对应记录所述虚拟资产和唯一标识。

5.一种通信方法,其特征在于,所述方法应用于终端设备中的BSIM卡,所述终端设备还包括元宇宙应用模块,所述方法包括:

当接收到身份信息请求时,获取本地记录的虚拟身份信息;其中,所述身份信息请求为所述元宇宙应用模块需要访问元宇宙平台时向所述BSIM卡发送的;

向所述元宇宙应用模块发送所述虚拟身份信息;其中,所述虚拟身份信息为:登录所述元宇宙应用模块的第一用户在注册所述BSIM卡时,所述BSIM卡基于所述第一用户的私钥生成得到的,其包括:基于哈希算法对所述第一用户的私钥进行处理,得到一个固定长度的字符串,作为第一哈希值;获取第一哈希值的第一数值长度的字节,将所述第一数值长度的字节作为第二哈希值;在所述第二哈希值前添加DID角色类型字节,将添加DID角色类型字节后的第二哈希值作为第三哈希值;基于哈希算法对所述第三哈希值进行计算,得到第四哈希值;获取第四哈希值的第二数值长度的字节,并将第二数值长度的字节与所述第三哈希值拼接,得到的拼接后的值作为第五哈希值;对所述第五哈希值进行编码处理,得到所述第一用户对应的DID,作为第一用户的虚拟身份信息;所述第一用户的私钥为对预设随机数进行哈希计算得到的;以使所述元宇宙应用模块基于所述虚拟身份信息,向所述元宇宙平台发送认证请求,以使所述元宇宙平台基于所述虚拟身份信息对所述认证请求进行认证。

6.根据权利要求5所述的方法,其特征在于,所述方法还包括:

接收所述元宇宙应用模块发送的交易记录;其中,所述交易记录为所述第一用户在所述元宇宙平台中的交易记录;

基于所述第一用户的私钥对所述交易记录进行加密处理,得到对应的数字签名;

向所述元宇宙应用模块发送所述数字签名,以使所述元宇宙应用模块向所述元宇宙平台发送所述交易记录和所述数字签名。

7.根据权利要求5所述的方法,其特征在于,所述方法还包括:

接收所述元宇宙应用模块发送的虚拟资产;其中,所述虚拟资产为所述第一用户在所述元宇宙平台中获取到的;

基于所述虚拟身份信息生成所述虚拟资产的唯一标识,并在本地对应记录所述虚拟资产和唯一标识。

8.根据权利要求5所述的方法,其特征在于,所述虚拟身份信息的生成过程包括:

生成随机数;

基于预设的哈希算法,计算所述随机数的哈希值,得到所述第一用户的私钥;

基于所述第一用户的私钥,生成所述第一用户的去中心化身份DID,作为所述第一用户的虚拟身份信息。

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:

当需要对待验证用户的用户身份进行验证时,获取所述待验证用户提供的用户密码和用户真实身份信息;

基于预先记录的用户真实身份信息、加密随机数与运营商密码的对应关系,确定所述待验证用户提供的用户真实身份信息对应的加密随机数与运营商密码;其中,所述对应关

系中记录的加密随机数为:基于注册用户提供的用户密码和对应的运营商密码进行加密得到的;

判断基于确定出的运营商密码和所述待验证用户提供的用户密码,是否能够成功对确定出的加密随机数进行解密;

若是,则确定所述待验证用户通过身份验证;

若否,确定所述待验证用户未通过身份验证。

10.一种通信装置,其特征在于,所述装置应用于终端设备中的元宇宙应用模块,所述终端设备还包括BSIM卡,所述装置包括:

身份信息请求发送模块,用于当需要访问元宇宙平台时,向所述BSIM卡发送身份信息请求,以使所述BSIM卡在接收到所述身份信息请求时,获取本地记录的虚拟身份信息,并向所述元宇宙应用模块发送所述虚拟身份信息;其中,所述虚拟身份信息为:登录所述元宇宙应用模块的第一用户在注册所述BSIM卡时,所述BSIM卡基于所述第一用户的私钥生成得到的,其包括:基于哈希算法对所述第一用户的私钥进行处理,得到一个固定长度的字符串,作为第一哈希值;获取第一哈希值的第一数值长度的字节,将所述第一数值长度的字节作为第二哈希值;在所述第二哈希值前添加DID角色类型字节,将添加DID角色类型字节后的第二哈希值作为第三哈希值;基于哈希算法对所述第三哈希值进行计算,得到第四哈希值;获取第四哈希值的第二数值长度的字节,并将第二数值长度的字节与所述第三哈希值拼接,得到的拼接后的值作为第五哈希值;对所述第五哈希值进行编码处理,得到所述第一用户对应的DID,作为第一用户的虚拟身份信息;所述第一用户的私钥为对预设随机数进行哈希计算得到的;

认证请求发送模块,用于基于所述虚拟身份信息,向所述元宇宙平台发送认证请求,以使所述元宇宙平台基于所述虚拟身份信息对所述认证请求进行认证。

11.根据权利要求10所述的装置,其特征在于,所述装置还包括:

交易记录获取模块,用于获取所述第一用户在所述元宇宙平台中的交易记录;

交易记录发送模块,用于向所述BSIM卡发送所述交易记录,以使所述BSIM卡基于所述第一用户的私钥对所述交易记录进行加密处理,得到对应的数字签名,并向所述元宇宙应用模块发送所述数字签名;

数字签名获取模块,用于从所述BSIM卡获取所述数字签名,并向所述元宇宙平台发送所述交易记录和所述数字签名。

12.根据权利要求10所述的装置,其特征在于,所述装置还包括:

虚拟资产发送模块,用于当检测到所述第一用户在所述元宇宙平台中获取到虚拟资产时,向所述BSIM卡发送所述虚拟资产,以使所述BSIM卡基于所述虚拟身份信息生成所述虚拟资产的唯一标识,并在本地对应记录所述虚拟资产和唯一标识。

13.一种通信装置,其特征在于,所述装置应用于终端设备中的BSIM卡,所述终端设备还包括元宇宙应用模块,所述装置包括:

虚拟身份信息获取模块,用于当接收到身份信息请求时,获取本地记录的虚拟身份信息;其中,所述身份信息请求为所述元宇宙应用模块需要访问元宇宙平台时向所述BSIM卡发送的;

虚拟身份信息发送模块,用于向所述元宇宙应用模块发送所述虚拟身份信息;其中,所

述虚拟身份信息为:登录所述元宇宙应用模块的第一用户在注册所述BSIM卡时,所述BSIM卡基于所述第一用户的私钥生成得到的,其包括:基于哈希算法对所述第一用户的私钥进行处理,得到一个固定长度的字符串,作为第一哈希值;获取第一哈希值的第一数值长度的字节,将所述第一数值长度的字节作为第二哈希值;在所述第二哈希值前添加DID角色类型字节,将添加DID角色类型字节后的第二哈希值作为第三哈希值;基于哈希算法对所述第三哈希值进行计算,得到第四哈希值;获取第四哈希值的第二数值长度的字节,并将第二数值长度的字节与所述第三哈希值拼接,得到的拼接后的值作为第五哈希值;对所述第五哈希值进行编码处理,得到所述第一用户对应的DID,作为第一用户的虚拟身份信息;所述第一用户的私钥为对预设随机数进行哈希计算得到的;以使所述元宇宙应用模块基于所述虚拟身份信息,向所述元宇宙平台发送认证请求,以使所述元宇宙平台基于所述虚拟身份信息对所述认证请求进行认证。

14.根据权利要求13所述的装置,其特征在于,所述装置还包括:

交易记录接收模块,用于接收所述元宇宙应用模块发送的交易记录;其中,所述交易记录为所述第一用户在所述元宇宙平台中的交易记录;

数字签名生成模块,用于基于所述第一用户的私钥对所述交易记录进行加密处理,得到对应的数字签名;

数字签名发送模块,用于向所述元宇宙应用模块发送所述数字签名,以使所述元宇宙应用模块向所述元宇宙平台发送所述交易记录和所述数字签名。

15.根据权利要求13所述的装置,其特征在于,所述装置还包括:

虚拟资产接收模块,用于接收所述元宇宙应用模块发送的虚拟资产;其中,所述虚拟资产为所述第一用户在所述元宇宙平台中获取到的;

唯一标识生成模块,用于基于所述虚拟身份信息生成所述虚拟资产的唯一标识,并在本地对应记录所述虚拟资产和唯一标识。

16.根据权利要求13所述的装置,其特征在于,所述装置还包括:

随机数生成模块,用于生成随机数;

私钥生成模块,用于基于预设的哈希算法,计算所述随机数的哈希值,得到所述第一用户的私钥;

DID生成模块,用于基于所述第一用户的私钥,生成所述第一用户的去中心化身份DID,作为所述第一用户的虚拟身份信息。

17.根据权利要求16所述的装置,其特征在于,所述装置还包括:

第一获取模块,用于当需要对待验证用户的用户身份进行验证时,获取所述待验证用户提供的用户密码和用户真实身份信息;

第一确定模块,用于基于预先记录的用户真实身份信息、加密随机数与运营商密码的对应关系,确定所述待验证用户提供的用户真实身份信息对应的加密随机数与运营商密码;其中,所述对应关系中记录的加密随机数为:基于注册用户提供的用户密码和对应的运营商密码进行加密得到的;

第一判断模块,用于判断基于确定出的运营商密码和所述待验证用户提供的用户密码,是否能够成功对确定出的加密随机数进行解密;若是,则确定所述待验证用户通过身份验证;若否,确定所述待验证用户未通过身份验证。

18.一种BSIM卡,其特征在于,所述BSIM卡包括计算芯片、通信模块和SIM卡模块;

所述计算芯片,用于通过所述通信模块与终端设备中的元宇宙应用模块进行数据通信,以实现权利要求5-9任一所述的方法。

19.一种电子设备,其特征在于,包括处理器、通信接口、存储器和通信总线,其中,处理器,通信接口,存储器通过通信总线完成相互间的通信;

存储器,用于存放计算机程序;

处理器,用于执行存储器上所存放的程序时,实现权利要求2-9任一所述的方法步骤。

20.一种计算机可读存储介质,其特征在于,所述计算机可读存储介质内存储有计算机程序,所述计算机程序被处理器执行时实现权利要求2-9任一所述的方法步骤。

一种通信方法、装置、SIM卡、电子设备和终端设备

技术领域

[0001] 本公开涉及元宇宙技术领域,特别是涉及一种通信方法、装置、SIM卡、电子设备和终端设备。

背景技术

[0002] 元宇宙(Metaverse)是与现实世界映射与交互的虚拟世界。基于元宇宙,可以将虚拟世界与现实世界在经济系统、社交系统、身份系统上密切融合,并且允许用户进行内容生产和世界编辑。

[0003] 相关技术中,用户可以通过互联网平台进行注册,互联网平台可以生成用户用于访问元宇宙的虚拟身份信息,进而,用户可以基于该虚拟身份信息访问元宇宙平台。

[0004] 然而,相关技术中,互联网平台会记录用户的虚拟身份信息,虚拟身份信息缺乏隐私保护,导致虚拟身份信息存在泄露的风险,不利于用户的隐私保护。

发明内容

[0005] 本公开实施例的目的在于提供一种通信方法、装置、SIM卡、电子设备和终端设备,能够降低虚拟身份信息泄露的风险,有利于用户的隐私保护。具体技术方案如下:

[0006] 本公开实施例的第一方面,首先提供了一种终端设备,所述终端设备包括:用户身份模块SIM卡;并安装有元宇宙应用模块,其中:

[0007] 所述元宇宙应用模块,用于当需要访问元宇宙平台时,向所述SIM卡发送身份信息请求;

[0008] 所述SIM卡,用于在接收到所述身份信息请求时,获取本地记录的虚拟身份信息,并向所述元宇宙应用模块发送所述虚拟身份信息;其中,所述虚拟身份信息为:登录所述元宇宙应用模块的第一用户在注册所述SIM(Subscriber Identity Module,用户身份模块)卡时,所述SIM卡基于所述第一用户的私钥生成得到的;所述第一用户的私钥为对预设随机数进行哈希计算得到的;

[0009] 所述元宇宙应用模块,还用于基于所述虚拟身份信息,向所述元宇宙平台发送认证请求,以使所述元宇宙平台基于所述虚拟身份信息对所述认证请求进行认证。

[0010] 本公开实施例的第二方面,提供了一种通信方法,所述方法应用于终端设备中的元宇宙应用模块,所述终端设备还包括SIM卡,所述方法包括:

[0011] 当需要访问元宇宙平台时,向所述SIM卡发送身份信息请求,以使所述SIM卡在接收到所述身份信息请求时,获取本地记录的虚拟身份信息,并向所述元宇宙应用模块发送所述虚拟身份信息;其中,所述虚拟身份信息为:登录所述元宇宙应用模块的第一用户在注册所述SIM卡时,所述SIM卡基于所述第一用户的私钥生成得到的;所述第一用户的私钥为对预设随机数进行哈希计算得到的;

[0012] 基于所述虚拟身份信息,向所述元宇宙平台发送认证请求,以使所述元宇宙平台基于所述虚拟身份信息对所述认证请求进行认证。

[0013] 在一些实施例中,所述方法还包括:

[0014] 获取所述第一用户在所述元宇宙平台中的交易记录;

[0015] 向所述SIM卡发送所述交易记录,以使所述SIM卡基于所述第一用户的私钥对所述交易记录进行加密处理,得到对应的数字签名,并向所述元宇宙应用模块发送所述数字签名;

[0016] 从所述SIM卡获取所述数字签名,并向所述元宇宙平台发送所述交易记录和所述数字签名。

[0017] 在一些实施例中,所述方法还包括:

[0018] 当检测到所述第一用户在所述元宇宙平台中获取到虚拟资产时,向所述SIM卡发送所述虚拟资产,以使所述SIM卡基于所述虚拟身份信息生成所述虚拟资产的唯一标识,并在本地对应记录所述虚拟资产和唯一标识。

[0019] 本公开实施例的第三方面,提供了一种通信方法,所述方法应用于终端设备中的SIM卡,所述终端设备还包括元宇宙应用模块,所述方法包括:

[0020] 当接收到身份信息请求时,获取本地记录的虚拟身份信息;其中,所述身份信息请求为所述元宇宙应用模块需要访问元宇宙平台时向所述SIM卡发送的;

[0021] 向所述元宇宙应用模块发送所述虚拟身份信息;其中,所述虚拟身份信息为:登录所述元宇宙应用模块的第一用户在注册所述SIM卡时,所述SIM卡基于所述第一用户的私钥生成得到的;所述第一用户的私钥为对预设随机数进行哈希计算得到的;以使所述元宇宙应用模块基于所述虚拟身份信息,向所述元宇宙平台发送认证请求,以使所述元宇宙平台基于所述虚拟身份信息对所述认证请求进行认证。

[0022] 在一些实施例中,所述方法还包括:

[0023] 接收所述元宇宙应用模块发送的交易记录;其中,所述交易记录为所述第一用户在所述元宇宙平台中的交易记录;

[0024] 基于所述第一用户的私钥对所述交易记录进行加密处理,得到对应的数字签名;

[0025] 向所述元宇宙应用模块发送所述数字签名,以使所述元宇宙应用模块向所述元宇宙平台发送所述交易记录和所述数字签名。

[0026] 在一些实施例中,所述方法还包括:

[0027] 接收所述元宇宙应用模块发送的虚拟资产;其中,所述虚拟资产为所述第一用户在所述元宇宙平台中获取到的;

[0028] 基于所述虚拟身份信息生成所述虚拟资产的唯一标识,并在本地对应记录所述虚拟资产和唯一标识。

[0029] 在一些实施例中,所述虚拟身份信息的生成过程包括:

[0030] 生成随机数;

[0031] 基于预设的哈希算法,计算所述随机数的哈希值,得到所述第一用户的私钥;

[0032] 基于所述第一用户的私钥,生成所述第一用户的DID(Decentralized Identity,去中心化身份),作为所述第一用户的虚拟身份信息。

[0033] 在一些实施例中,所述方法还包括:

[0034] 当需要对待验证用户的用户身份进行验证时,获取所述待验证用户提供的用户密码和用户真实身份信息;

[0035] 基于预先记录的用户真实身份信息、加密随机数与运营商密码的对应关系,确定所述待验证用户提供的用户真实身份信息对应的加密随机数与运营商密码;其中,所述对应关系中记录的加密随机数为:基于注册用户提供的用户密码和对应的运营商密码进行加密得到的;

[0036] 判断基于确定出的运营商密码和所述待验证用户提供的用户密码,是否能够成功对确定出的加密随机数进行解密;

[0037] 若是,则确定所述待验证用户通过身份验证;

[0038] 若否,确定所述待验证用户未通过身份验证。

[0039] 本公开实施例的第四方面,提供了一种通信装置,所述装置应用于终端设备中的元宇宙应用模块,所述终端设备还包括SIM卡,所述装置包括:

[0040] 身份信息请求发送模块,用于当需要访问元宇宙平台时,向所述SIM卡发送身份信息请求,以使所述SIM卡在接收到所述身份信息请求时,获取本地记录的虚拟身份信息,并向所述元宇宙应用模块发送所述虚拟身份信息;其中,所述虚拟身份信息为:登录所述元宇宙应用模块的第一用户在注册所述SIM卡时,所述SIM卡基于所述第一用户的私钥生成得到的;所述第一用户的私钥为对预设随机数进行哈希计算得到的;

[0041] 认证请求发送模块,用于基于所述虚拟身份信息,向所述元宇宙平台发送认证请求,以使所述元宇宙平台基于所述虚拟身份信息对所述认证请求进行认证。

[0042] 在一些实施例中,所述装置还包括:

[0043] 交易记录获取模块,用于获取所述第一用户在所述元宇宙平台中的交易记录;

[0044] 交易记录发送模块,用于向所述SIM卡发送所述交易记录,以使所述SIM卡基于所述第一用户的私钥对所述交易记录进行加密处理,得到对应的数字签名,并向所述元宇宙应用模块发送所述数字签名;

[0045] 数字签名获取模块,用于从所述SIM卡获取所述数字签名,并向所述元宇宙平台发送所述交易记录和所述数字签名。

[0046] 在一些实施例中,所述装置还包括:

[0047] 虚拟资产发送模块,用于当检测到所述第一用户在所述元宇宙平台中获取到虚拟资产时,向所述SIM卡发送所述虚拟资产,以使所述SIM卡基于所述虚拟身份信息生成所述虚拟资产的唯一标识,并在本地对应记录所述虚拟资产和唯一标识。

[0048] 本公开实施例的第五方面,提供了一种通信装置,所述装置应用于终端设备中的SIM卡,所述终端设备还包括元宇宙应用模块,所述装置包括:

[0049] 虚拟身份信息获取模块,用于当接收到身份信息请求时,获取本地记录的虚拟身份信息;其中,所述身份信息请求为所述元宇宙应用模块需要访问元宇宙平台时向所述SIM卡发送的;

[0050] 虚拟身份信息发送模块,用于向所述元宇宙应用模块发送所述虚拟身份信息;其中,所述虚拟身份信息为:登录所述元宇宙应用模块的第一用户在注册所述SIM卡时,所述SIM卡基于所述第一用户的私钥生成得到的;所述第一用户的私钥为对预设随机数进行哈希计算得到的;以使所述元宇宙应用模块基于所述虚拟身份信息,向所述元宇宙平台发送认证请求,以使所述元宇宙平台基于所述虚拟身份信息对所述认证请求进行认证。

[0051] 在一些实施例中,所述装置还包括:

[0052] 交易记录接收模块,用于接收所述元宇宙应用模块发送的交易记录;其中,所述交易记录为所述第一用户在所述元宇宙平台中的交易记录;

[0053] 数字签名生成模块,用于基于所述第一用户的私钥对所述交易记录进行加密处理,得到对应的数字签名;

[0054] 数字签名发送模块,用于向所述元宇宙应用模块发送所述数字签名,以使所述元宇宙应用模块向所述元宇宙平台发送所述交易记录和所述数字签名。

[0055] 在一些实施例中,所述装置还包括:

[0056] 虚拟资产接收模块,用于接收所述元宇宙应用模块发送的虚拟资产;其中,所述虚拟资产为所述第一用户在所述元宇宙平台中获取到的;

[0057] 唯一标识生成模块,用于基于所述虚拟身份信息生成所述虚拟资产的唯一标识,并在本地对应记录所述虚拟资产和唯一标识。

[0058] 在一些实施例中,所述装置还包括:

[0059] 随机数生成模块,用于生成随机数;

[0060] 私钥生成模块,用于基于预设的哈希算法,计算所述随机数的哈希值,得到所述第一用户的私钥;

[0061] DID生成模块,用于基于所述第一用户的私钥,生成所述第一用户的去中心化身份DID,作为所述第一用户的虚拟身份信息。

[0062] 在一些实施例中,所述装置还包括:

[0063] 第一获取模块,用于当需要对待验证用户的用户身份进行验证时,获取所述待验证用户提供的用户密码和用户真实身份信息;

[0064] 第一确定模块,用于基于预先记录的用户真实身份信息、加密随机数与运营商密码的对应关系,确定所述待验证用户提供的用户真实身份信息对应的加密随机数与运营商密码;其中,所述对应关系中记录的加密随机数为:基于注册用户提供的用户密码和对应的运营商密码进行加密得到的;

[0065] 第一判断模块,用于判断基于确定出的运营商密码和所述待验证用户提供的用户密码,是否能够成功对确定出的加密随机数进行解密;若是,则确定所述待验证用户通过身份验证;若否,确定所述待验证用户未通过身份验证。

[0066] 本公开实施例的第六方面,提供了一种SIM卡,所述SIM卡包括计算芯片、通信模块和SIM卡模块;

[0067] 所述计算芯片,用于通过所述通信模块与终端设备中的元宇宙应用模块进行数据通信,以实现上述任一应用于SIM卡的通信方法步骤。

[0068] 本公开实施例的第七方面,提供了一种电子设备,其特征在于,包括处理器、通信接口、存储器和通信总线,其中,处理器,通信接口,存储器通过通信总线完成相互间的通信;

[0069] 存储器,用于存放计算机程序;

[0070] 处理器,用于执行存储器上所存放的程序时,实现上述任一通信方法步骤。

[0071] 本公开实施例还提供了一种包含指令的计算机程序产品,当其在计算机上运行时,使得计算机执行上述任一通信方法。

[0072] 本公开实施例有益效果:

[0073] 本公开实施例提供的终端设备包括用户身份模块SIM卡和元宇宙应用模块,其中:元宇宙应用模块,用于当需要访问元宇宙平台时,向SIM发送身份信息请求;SIM卡,用于在接收到身份信息请求时,获取本地记录的虚拟身份信息,并向元宇宙应用模块发送虚拟身份信息;其中,虚拟身份信息为:登录元宇宙应用模块的第一用户在注册SIM卡时,SIM卡基于第一用户的私钥生成得到的;第一用户的私钥为对预设随机数进行哈希计算得到的;元宇宙应用模块,还用于基于虚拟身份信息,向元宇宙平台发送认证请求,以使元宇宙平台基于虚拟身份信息对认证请求进行认证。

[0074] 基于本公开实施例提供的终端设备,可以在用户注册SIM卡时,生成用户的虚拟身份信息,并存储在SIM卡中,后续,基于SIM卡中记录的虚拟身份信息,可以实现用户访问元宇宙平台,而无需在各互联网平台会记录用户的虚拟身份信息,进而,降低虚拟身份信息泄露的风险,有利于用户的隐私保护。

[0075] 当然,实施本公开的任一产品或方法并不一定需要同时达到以上所述的所有优点。

附图说明

[0076] 为了更清楚地说明本公开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公开的一些实施例,对于本领域普通技术人员来讲,还可以根据这些附图获得其他的实施例。

[0077] 图1为本公开实施例提供的一种终端设备的架构图;

[0078] 图2为本申请实施例提供的一种SIM卡的结构图;

[0079] 图3为本公开实施例提供的一种BSIM卡的硬件结构示意图;

[0080] 图4为本公开实施例提供的一种通信方法的交互图;

[0081] 图5为本公开实施例提供的一种访问元宇宙平台的示意图;

[0082] 图6为本公开实施例提供的另一种通信方法的交互图;

[0083] 图7为本公开实施例提供的又一种通信方法的交互图;

[0084] 图8为本公开实施例提供的一种虚拟身份信息的生成过程的流程图;

[0085] 图9为本公开实施例提供的一种用户身份验证过程的流程图;

[0086] 图10为本公开实施例提供的一种待验证用户验证示意图;

[0087] 图11为本公开实施例提供的一种智能终端的操作系统与SIM卡的通信示意图;

[0088] 图12为本公开实施例提供的一种SIM卡对虚拟资产进行管理的示意图;

[0089] 图13为本公开实施例提供的一种元宇宙资产管理流程示意图;

[0090] 图14为本公开实施例提供的一种通信装置的结构图;

[0091] 图15为本公开实施例提供的又一种通信装置的结构图;

[0092] 图16为本申请实施例提供的一种电子设备的结构图。

具体实施方式

[0093] 下面将结合本公开实施例中的附图,对本公开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公开一部分实施例,而不是全部的实施例。基于

本公开中的实施例,本领域普通技术人员基于本公开所获得的所有其他实施例,都属于本公开保护的范围。

[0094] 相关技术中,互联网平台会记录用户的虚拟身份信息,导致虚拟身份信息存在泄露的风险,不利于用户的隐私保护。

[0095] 为了解决上述问题,本公开实施例提供了一种终端设备,参见图1,图1为本公开实施例提供的一种终端设备的架构图,该终端设备包括SIM(用户身份模块,Subscriber Identity Module)卡101和元宇宙应用模块102,其中:

[0096] 元宇宙应用模块102,用于当需要访问元宇宙平台时,向SIM卡101发送身份信息请求。

[0097] SIM卡101,用于在接收到身份信息请求时,获取本地记录的虚拟身份信息,并向元宇宙应用模块102发送虚拟身份信息。

[0098] 其中,虚拟身份信息为:登录元宇宙应用模块102的第一用户在注册SIM卡时,SIM卡101基于第一用户的私钥生成得到的;第一用户的私钥为对预设随机数进行哈希计算得到的。

[0099] 元宇宙应用模块102,还用于基于虚拟身份信息,向元宇宙平台发送认证请求,以使元宇宙平台基于虚拟身份信息对认证请求进行认证。

[0100] 本公开实施例提供的终端设备,可以在用户注册SIM卡时,生成用户的虚拟身份信息,并存储在SIM卡中,后续,基于SIM卡中记录的虚拟身份信息,可以实现用户访问元宇宙平台,而无需在各互联网平台会记录用户的虚拟身份信息,进而,降低虚拟身份信息泄露的风险,有利于用户的隐私保护。

[0101] 本公开实施例提供的终端设备可以应用于不同的场景,例如,该终端设备可以为手机,用户可以通过手机与元宇宙平台进行通信。相应的,该终端设备中的SIM卡表示内置于该手机的SIM卡,元宇宙应用模块可以包括该手机中安装的用于访问元宇宙平台的应用程序。

[0102] 本公开实施例还提供了一种SIM卡,如图2所示,图2为本申请实施例提供的一种SIM卡的结构图,包括:计算芯片201、SIM卡模块202和通信模块203;

[0103] 计算芯片201,用于通过通信模块203与终端设备中的元宇宙应用模块进行数据通信。

[0104] 本公开中的SIM卡也可以称为BSIM(区块链用户身份模块,Blockchain Subscriber Identity Module)卡。元宇宙平台应用模块可以为终端设备安装的元宇宙软件。

[0105] 一种实现方式中,如图3所示,图3为本公开实施例提供的一种BSIM卡的硬件结构示意图。在图3中,BSIM卡包括SIM卡模块301、蓝牙模块302、计算芯片303和接口模块304。SIM卡模块301包括传统SIM卡的硬件结构,蓝牙模块302即为上述实施例中的通信模块,接口模块304包含后文中的特定接口。计算芯片303用于生成用户的虚拟身份信息、对交易记录进行签名、生成虚拟资产的唯一标识,以及对用户身份进行验证等,具体地,将在后续实施例中详细接收。该计算芯片303具备金融安全等级。

[0106] 一种实现方式中,BSIM卡可以支持ECC-secp256k1(椭圆曲线算法,Elliptic Curve Cryptography)、AES(高级加密标准算法,Advanced Encryption Standard)、ECDSA-

secp256k1(椭圆曲线数字签名算法,Elliptic Curve Digital Signature Algorithm)、HMAC-SHA512(基于消息认证码的哈希算法,Hash-based Message Authentication Code)等区块链算法。BSIM卡中的存储空间大于1M,用户空间大于450K;签名速度小于150ms。其中,用户空间用于存储用户的虚拟身份信息、虚拟资产、手机号、加密种子和私钥。

[0107] 一种实现方式中,BSIM可以通过以下架构实现:JAVA应用层、JAVA平台、硬件接口层和硬件层。JAVA应用层用于BSIM卡内实现区块链应用逻辑,包括种子生成、公私钥生成、加密存储、数字签名生成、私钥找回、备份等。JAVA平台层可以实现JAVACARD虚拟机及卡片内容管理功能,提供应用调用的JAVA接口。BSIM卡通过JAVA接口与元宇宙平台用于模块进行通信。硬件接口层可以基于C语言调用硬件接口,以生成用户的虚拟身份信息、对交易记录进行签名、生成虚拟资产的唯一标识,以及对用户身份进行验证等处理。硬件层可以通过硬件算法IP协处理器,提升算法性能。硬件算法IP协处理器即上述实施例中的计算芯片。

[0108] 基于相同的发明构思,本公开实施例还提供了一种通信方法,该方法可以应用于终端设备中的SIM卡和元宇宙应用模块。该SIM卡和元宇宙应用模块可以分别为图1中终端设备中的SIM卡101和元宇宙应用模块102。参见图4,图4为本公开实施例提供的一种通信方法的交互图,该方法可以包括以下步骤:

[0109] S401:当需要访问元宇宙平台时,元宇宙应用模块向SIM卡发送身份信息请求。

[0110] S402:SIM卡在接收到身份信息请求时,获取本地记录的虚拟身份信息,并向元宇宙应用模块发送虚拟身份信息。

[0111] 其中,虚拟身份信息为:登录元宇宙应用模块的第一用户在注册SIM卡时,SIM卡基于第一用户的私钥生成得到的;第一用户的私钥为对预设随机数进行哈希计算得到的。

[0112] S403:元宇宙应用模块基于虚拟身份信息,向元宇宙平台发送认证请求,以使元宇宙平台基于虚拟身份信息对认证请求进行认证。

[0113] 本公开实施例提供的通信方法,可以在用户注册SIM卡时,生成用户的虚拟身份信息,并存储在SIM卡中,后续,基于SIM卡中记录的虚拟身份信息,可以实现用户访问元宇宙平台,而无需在各互联网平台会记录用户的虚拟身份信息,进而,降低虚拟身份信息泄露的风险,有利于用户的隐私保护。

[0114] 另外,相关技术中,虚拟资产和虚拟身份是元宇宙的核心,承载了元宇宙中用户的资产权益和社交身份。但由于用户的虚拟身份解释权在互联网平台机构,所有权属性不明确,阻碍了元宇宙的发展。

[0115] 而基于本公开实施例的方法,用户的虚拟身份信息记录在用户注册的SIM卡中,使得用户能够拥有虚拟身份信息的所有权,即,能够明确虚拟身份信息的所有权,促进元宇宙的发展。

[0116] 针对步骤S401,该元宇宙平台与元宇宙应用模块对应,即,用户可以通过不同的元宇宙应用模块访问不同的元宇宙平台。

[0117] 一种实现方式中,当用户在智能终端中开启元宇宙应用模块时,该元宇宙应用模块可以向SIM卡发送身份信息请求。例如,元宇宙应用模块可以通过特定接口调用SDK(软件开发工具包,Software Development Kit),进而,通过SDK向SIM卡发送身份信息请求,以获取SIM卡中储存的身份信息。上述特定接口可以为智能终端的操作系统提供的接口。

[0118] 针对步骤S402,第一用户为当前使用智能终端需要通过元宇宙应用模块访问元宇

宙平台的用户。一种实现方式中,第一用户可以向运营商申请注册SIM卡,在注册SIM卡时,SIM卡可以生成第一用户的虚拟身份信息。

[0119] 针对步骤S403,一种实现方式中,第一用户的虚拟身份信息可以包含DID。即,第一用户在注册SIM卡时,运营商可以将该第一用户的DID存储至运营商构建的区块链中。相应的,元宇宙应用模块可以基于第一用户的DID生成DID可验证声明,并向元宇宙平台发送携带有该DID可验证声明的认证请求。相应的,元宇宙平台可以获取运营商构建的区块链中存储的第一用户的DID,并基于该DID对DID可验证声明进行验证,也就可以对认证请求进行认证。其中,对认证请求进行认证,也就是对第一用户进行认证。

[0120] 例如,DID可以包含DID标识符和DID文档,该DID文档包括:该第一用户的公钥、加密协议的集合、服务端点的集合、该DID文档的创建时间戳和JSON-LD(JavaScript Object Notation-Linked Data,一种基于JSON表示和传输互联数据的方法)签名。其中,JSON-LD签名用于验证该DID文档的合法性。该第一用户的公钥与后文中提到的第一用户的私钥对应。

[0121] 一种实现方式中,元宇宙平台可以基于W3C(万维网联盟,World Wide Web Consortium)的DID规范,对认证请求中携带的DID可验证声明进行验证。例如,可以判断该DID可验证声明中的签名是否合法,或,可以判断该DID可验证声明中的DID是否为该元宇宙平台信任的DID,即,该DID可验证声明表征的DID标识符和DID文档是否为运营商构建的区块链中存储的DID标识符和DID文档。也就是说,当第一用户通过元宇宙应用模块访问元宇宙平台时,元宇宙平台可以获取第一用户的DID可验证声明,若该DID可验证声明通过验证,则可以确定对第一用户认证成功;反之,确定对第一用户认证失败。

[0122] 一种实现方式中,参见图5,图5为本公开实施例提供的一种访问元宇宙平台的示意图。图5中的各元宇宙表示元宇宙平台,自然人(即用户)通过运营商进行实名认证后,可以登录元宇宙平台,并可以切换访问多个不同的元宇宙平台。运营商将用户的DID密钥(即DID)存储在BSIM卡芯片内,元宇宙平台可以从运营商获取该用户的DID,后续,当该用户访问元宇宙平台时,元宇宙平台可以对DID可验证声明进行解析、验证,进而对用户进行认证。基于W3C的DID标识规范定义,可以实现统一规范的DID在元宇宙平台之间互联互通互认,用户可以实现在多个元宇宙平台间无缝切换,即,用户可以基于一个DID通过访问不同的元宇宙平台,无需在不同的元宇宙平台注册不同的DID。区块链基础设施是一个基于区块链技术运行的网络,运营商可以参与区块链基础设施的构建,同时,区块链中也可以存储DID。另外,区块链中还可以存储元宇宙平台中的每一DID的交易记录。利用BSIM卡对用户的虚拟身份信息进行存储,可以打通多个元宇宙平台之间的数字身份,实现跨元宇宙平台的统一身份认证协议,为云宇宙平台构建权威、标准、可信的用户身份体系基础设施。

[0123] 一种实现方式中,参见图6,图6为本公开实施例提供的另一种通信方法的交互图,在图4的基础上,该方法可以包括以下步骤:

[0124] S404:元宇宙应用模块获取第一用户在元宇宙平台中的交易记录。

[0125] S405:元宇宙应用模块向SIM卡发送交易记录。

[0126] S406:SIM卡基于第一用户的私钥对交易记录进行加密处理,得到对应的数字签名,并向元宇宙应用模块发送数字签名。

[0127] S407:元宇宙应用模块从SIM卡获取数字签名,并向元宇宙平台发送交易记录和数字签名。

[0128] 元宇宙平台可以使用区块链作为基础设施,例如,元宇宙平台可以基于区块链发行虚拟资产。

[0129] 当用户在元宇宙平台中购买或出售一件虚拟资产时,元宇宙平台可以产生一条交易记录,用来表示第一用户在该元宇宙平台中进行虚拟资产交易。例如,交易记录可以包含交易的时间、交易双方的虚拟身份信息和交易的虚拟资产原有的标识。虚拟资产原有的标识表示生成该虚拟资产时得到的标识。

[0130] 一种实现方式中,SIM卡可以基于数字摘要算法对交易记录进行处理,得到固定长度的字符串,然后,基于第一用户的私钥对字符串进行加密,形成数字签名。SIM卡可以通过区块链接口,将数字签名发送至元宇宙应用模块。例如,数字摘要算法可以为Hash(哈希)算法。其中,区块链接口可以为SIM卡提供的硬件接口,SIM卡可以通过该硬件接口接入各元宇宙平台对应的区块链。

[0131] 元宇宙应用模块可以基于SIM卡中的区块链接口获取数字签名,并将该数字签名和其对应的交易记录发送至元宇宙平台。

[0132] 本公开实施例提供的通信方法,在用户进行虚拟资产交易时,使用SIM卡中存储的第一用户的私钥对交易记录进行签名,将得到的数字签名和交易记录发送至元宇宙平台,可以避免用户的交易记录被篡改,且交易的成本低、不受时间和空间的限制。

[0133] 一种实现方式中,参见图7,图7为本公开实施例提供的又一种通信方法的交互图,在图4的基础上,该方法可以包括以下步骤:

[0134] S408:当检测到第一用户在元宇宙平台中获取到虚拟资产时,元宇宙应用模块向SIM卡发送虚拟资产。

[0135] S409:SIM卡基于虚拟身份信息生成虚拟资产的唯一标识,并在本地对应记录虚拟资产和唯一标识。

[0136] 第一用户可以通过元宇宙应用模块在元宇宙平台中购买虚拟资产、交换虚拟资产,相应的,元宇宙应用模块可以将第一用户得到的虚拟资产发送至SIM卡中。

[0137] 一种实现方式中,第一用户可以使用积分购买数字艺术品、游戏道具等。其中,积分可以为第一用户在运营商的业务运营平台进行充值得到的虚拟资产;或者,也可以为运营商根据用户的历史消费记录,向用户赠送的虚拟资产。

[0138] 一种实现方式中,SIM卡可以对虚拟身份信息和虚拟资产原有的标识进行拼接,作为虚拟资产的唯一标识。

[0139] 相关技术中,虚拟资产和虚拟身份是元宇宙的核心,承载了元宇宙中用户的资产权益和社交身份。但由于虚拟身份信息及衍生的相关资产、活动等数据缺乏隐私,不利于用户隐私的保护。本公开实施例提供的通信方法,可以基于SIM卡中存储的虚拟身份信息对不同元宇宙中的不同资产生成唯一标识,有利于用户对虚拟资产进行管理,进而,有利于打造元宇宙交易生态和用户的隐私保护。

[0140] 一种实现方式中,如图8所示,图8为本公开实施例提供的一种虚拟身份信息的生成过程的流程图,SIM卡生成虚拟身份信息的过程包括:

[0141] S801:生成随机数。

[0142] S802:基于预设的哈希算法,计算随机数的哈希值,得到第一用户的私钥。

[0143] S803:基于第一用户的私钥,生成第一用户的DID,作为第一用户的虚拟身份信息。

[0144] 一种实现方式中,在第一用户注册SIM卡时,SIM卡可以通过硬件随机数发生器(TRNG,True Random Number Generator)生成指定字节的随机数。基于预设的哈希算法对随机数进行处理,得到第一用户的私钥。

[0145] 基于哈希算法对第一用户的私钥进行处理,得到一个固定长度的字符串,作为第一哈希值。获取第一哈希值的第一数值长度的字节,将该第一数值长度的字节作为第二哈希值。在第二哈希值前添加DID角色类型字节,将添加DID角色类型字节后的第二哈希值作为第三哈希值。基于哈希算法对第三哈希值进行计算,得到第四哈希值。获取第四哈希值的第二数值长度的字节,并将第二数值长度的字节与第三哈希值拼接,得到的拼接后的值作为第五哈希值。对第五哈希值进行编码处理,得到该第一用户对应的DID,作为第一用户的虚拟身份信息。

[0146] 其中,第一数值长度的字节可以为前20个字节,第二数值长度的字节可以为前4个字节。哈希算法可以为SHA-512(Secure Hash Algorithm-512,安全散列算法)。DID角色类型字节表示该DID代表的角色类型,其中,角色类型可以为应用程序、个人或设备等。对第五哈希值进行编码处理可以使用Base58编码方法。

[0147] 指定字节可以为64字节,私钥的长度可以为512位,也就使得能够存在2的512次方个不同的私钥,即,私钥的个数接近于10的150次方,随机选取出的私钥相同的概率为10的150次方分之一,接近于0,进而,能够提高私钥的唯一性和安全性。

[0148] 本公开实施例提供的通信方法,可以基于随机数生成第一用户的私钥,确保了私钥的唯一性、安全性,且在用户注册SIM卡时生成用户的虚拟身份信息,明确了用户的虚拟身份信息的所有权,保障了用户的虚拟身份解释权在用户本人而非互联网平台,有利于用户的隐私保护,促进元宇宙的发展。

[0149] 一种实现方式中,当SIM卡被遗失或损坏时,用户可以恢复SIM卡,相应的,可以对用户身份进行验证。如图9所示,图9为本公开实施例提供的一种用户身份验证过程的流程图,包括:

[0150] S901:当需要对待验证用户的用户身份进行验证时,获取待验证用户提供的用户密码和用户真实身份信息。

[0151] S902:基于预先记录的用户真实身份信息、加密随机数与运营商密码的对应关系,确定待验证用户提供的用户真实身份信息对应的加密随机数与运营商密码。

[0152] 其中,对应关系中记录的加密随机数为:基于注册用户提供的用户密码和对应的运营商密码进行加密得到的。

[0153] S903:判断基于确定出的运营商密码和待验证用户提供的用户密码,是否能够成功对确定出的加密随机数进行解密;若是,则执行步骤S904;若否,则执行步骤S905。

[0154] S904:确定待验证用户通过身份验证。

[0155] S905:确定待验证用户未通过身份验证。

[0156] 在本公开中,随机数也可以称为种子,加密随机数也可以称为加密种子。

[0157] 一种实现方式中,用户在注册SIM卡时,可以提供用户密码。例如,用户密码可以为固定长度的字符串。另外,用户可以提供真实身份信息。真实身份信息可以包括用户的姓名和身份证号。运营商密码为运营商在用户在注册SIM卡时生成的。不同的用户对应的运营商密码可以相同,也可以不同。针对每一用户,在该用户注册SIM卡时,SIM卡在得到对应加密

随机数后,可以将该用户对应的加密随机数、运营商密码和该用户提供的真实身份信息存储在运营商的业务运营平台。

[0158] 待验证用户为当前需要进行用户身份验证的用户,当需要对待验证用户的用户身份进行验证时,SIM卡可以获取业务运营平台中记录的与待验证用户提供真实身份信息对应的加密随机数、运营商密码。进而,SIM卡结合待验证用户提供的用户密码和运营商密码对加密随机数进行解密;若解密成功,则确定待验证用户通过身份验证;若解密未成功,则确定待验证用户未通过身份验证。

[0159] 本公开实施例提供的通信方法,由于业务运营平台存储的为加密种子,并未存储用户的用户密码,因此,仅基于运营商密码,运营商无法得到用户的种子、私钥和资产,保证了用户资产安全,有利于用户的隐私保护。

[0160] 一种实现方式中,参见图10,图10为本公开实施例提供的一种待验证用户验证示意图。图10中,当SIM卡丢失或损坏时,待验证用户可以向运营商申请恢复卡。运营商可以将记录的与待验证用户提供的手机号等真实身份信息对应的加密种子和运营商密码写入SIM卡中。另外,SIM卡可以获取待验证用户输入的用户密码,进而,SIM卡基于运营商密码和用户密码对加密种子进行解密,若解密成功,则确定待验证用户通过身份验证,相应的,运营商可以为待验证用户恢复SIM卡,即,待验证用户得到新卡,找回钱包(即待验证用户的私钥);若解密未成功,则确定待验证用户未通过身份验证。

[0161] 一种实现方式中,参见图11,图11为本公开实施例提供的一种智能终端的操作系统与SIM卡的通信示意图。如图11所示,智能终端可以为手机,手机OS(操作系统)可以通过特定接口调用SDK(软件开发工具包,Software Development Kit),与SIM卡进行通信,SIM卡存储有用户的手机号、加密种子、私钥、加密数字资产和SIM卡计算程序。其中,通过SIM卡计算程序可以生成用户的虚拟身份信息、对交易记录进行签名、生成虚拟资产的唯一标识,以及对用户身份进行验证。

[0162] 一种实现方式中,参见图12,图12为本公开实施例提供的一种SIM卡对虚拟资产进行管理的示意图。图12中,BSIM卡中可以存储用户的用户身份(即,虚拟身份信息)、用户资产(虚拟资产)、原生资产(运营商下发的积分)。基于区块链可以实现数字身份的认证、构建数字资产交易商城(例如,积分交易平台),以及对数字艺术品(包括音乐、视频、图片等)、游戏资产(包括装备、物品、能力、皮肤等)和元宇宙资产进行交易。例如,针对数字艺术品,可定义所有权和使用权;能够实现对元宇宙的权力与资产的管理,保证资产归属与价值在元宇宙中得到无边界的广泛确认。区块链节点包括:联盟链区块链节点、区块链共识节点、版权保护节点、跨链节点等,各节点基于智能合约分别实现不同的业务功能。

[0163] 一种实现方式中,如图13所示,图13为本公开实施例提供的一种元宇宙资产管理流程示意图。图13中,BSIM卡可以作为元宇宙的入口装置,基于BSIM卡,可以实现区块链分布式数字身份的认证、元宇宙数字资产管理,以及基于通证的数字资产交易。使得构建的元宇宙能够服务于数据权益与资产流转,打造元宇宙数字身份及资产交易生态。BSIM卡具有支持多种区块链算法、性能高、安全性好、使用便捷等优点。有利于拉动5G大网流量收入,且区块链上数字资产不易迁移,提供用户粘性,有利于现有高净值用户的运营和吸引异网用户。

[0164] 基于相同的发明构思,本公开实施例还提供了一种通信装置,参见图14,图14为本

公开实施例提供的一种通信装置的结构图,该装置应用于终端设备中的元宇宙应用模块,终端设备还包括SIM卡,装置包括:

[0165] 身份信息请求发送模块1401,用于当需要访问元宇宙平台时,向SIM卡发送身份信息请求,以使SIM卡在接收到身份信息请求时,获取本地记录的虚拟身份信息,并向元宇宙应用模块发送虚拟身份信息;其中,虚拟身份信息为:登录元宇宙应用模块的第一用户在注册SIM卡时,SIM卡基于第一用户的私钥生成得到的;第一用户的私钥为对预设随机数进行哈希计算得到的;

[0166] 认证请求发送模块1402,用于基于虚拟身份信息,向元宇宙平台发送认证请求,以使元宇宙平台基于虚拟身份信息对认证请求进行认证。

[0167] 在一些实施例中,装置还包括:

[0168] 交易记录获取模块,用于获取第一用户在元宇宙平台中的交易记录;

[0169] 交易记录发送模块,用于向SIM卡发送交易记录,以使SIM卡基于第一用户的私钥对交易记录进行加密处理,得到对应的数字签名,并向元宇宙应用模块发送数字签名;

[0170] 数字签名获取模块,用于从SIM卡获取数字签名,并向元宇宙平台发送交易记录和数字签名。

[0171] 在一些实施例中,装置还包括:

[0172] 虚拟资产发送模块,用于当检测到第一用户在元宇宙平台中获取到虚拟资产时,向SIM卡发送虚拟资产,以使SIM卡基于虚拟身份信息生成虚拟资产的唯一标识,并在本地对应记录虚拟资产和唯一标识。

[0173] 基于相同的发明构思,本公开实施例还提供了一种通信装置,参见图15,图15为本公开实施例提供的又一种通信装置的结构图,该装置应用于终端设备中的SIM卡,终端设备还包括元宇宙应用模块,装置包括:

[0174] 虚拟身份信息获取模块1501,用于当接收到身份信息请求时,获取本地记录的虚拟身份信息;其中,身份信息请求为元宇宙应用模块需要访问元宇宙平台时向SIM卡发送的;

[0175] 虚拟身份信息发送模块1502,用于向元宇宙应用模块发送虚拟身份信息;其中,虚拟身份信息为:登录元宇宙应用模块的第一用户在注册SIM卡时,SIM卡基于第一用户的私钥生成得到的;第一用户的私钥为对预设随机数进行哈希计算得到的;以使元宇宙应用模块基于虚拟身份信息,向元宇宙平台发送认证请求,以使元宇宙平台基于虚拟身份信息对认证请求进行认证。

[0176] 在一些实施例中,装置还包括:

[0177] 交易记录接收模块,用于接收元宇宙应用模块发送的交易记录;其中,交易记录为第一用户在元宇宙平台中的交易记录;

[0178] 数字签名生成模块,用于基于第一用户的私钥对交易记录进行加密处理,得到对应的数字签名;

[0179] 数字签名发送模块,用于向元宇宙应用模块发送数字签名,以使元宇宙应用模块向元宇宙平台发送交易记录和数字签名。

[0180] 在一些实施例中,装置还包括:

[0181] 虚拟资产接收模块,用于接收元宇宙应用模块发送的虚拟资产;其中,虚拟资产为

第一用户在元宇宙平台中获取到的;

[0182] 唯一标识生成模块,用于基于虚拟身份信息生成虚拟资产的唯一标识,并在本地对应记录虚拟资产和唯一标识。

[0183] 在一些实施例中,装置还包括:

[0184] 随机数生成模块,用于生成随机数;

[0185] 私钥生成模块,用于基于预设的哈希算法,计算随机数的哈希值,得到第一用户的私钥;

[0186] DID生成模块,用于基于第一用户的私钥,生成第一用户的去中心化身份DID,作为第一用户的虚拟身份信息。

[0187] 在一些实施例中,装置还包括:

[0188] 第一获取模块,用于当需要对待验证用户的用户身份进行验证时,获取待验证用户提供的用户密码和用户真实身份信息;

[0189] 第一确定模块,用于基于预先记录的用户真实身份信息、加密随机数与运营商密码的对应关系,确定待验证用户提供的用户真实身份信息对应的加密随机数与运营商密码;其中,对应关系中记录的加密随机数为:基于注册用户提供的用户密码和对应的运营商密码进行加密得到的;

[0190] 第一判断模块,用于判断基于确定出的运营商密码和待验证用户提供的用户密码,是否能够成功对确定出的加密随机数进行解密;若是,则确定待验证用户通过身份验证;若否,确定待验证用户未通过身份验证。

[0191] 本公开实施例还提供了一种电子设备,如图16所示,图16为本申请实施例提供的一种电子设备的结构图。包括处理器1601、通信接口1602、存储器1603和通信总线1604,其中,处理器1601,通信接口1602,存储器1603通过通信总线1604完成相互间的通信,

[0192] 存储器1603,用于存放计算机程序;

[0193] 处理器1601,用于执行存储器1603上所存放的程序时,实现上述实施例中任一通信方法的步骤。

[0194] 上述电子设备提到的通信总线可以是外设部件互连标准(Peripheral Component Interconnect,PCI)总线或扩展工业标准结构(Extended Industry Standard Architecture,EISA)总线等。该通信总线可以分为地址总线、数据总线、控制总线等。为便于表示,图中仅用一条粗线表示,但并不表示仅有一根总线或一种类型的总线。

[0195] 通信接口用于上述电子设备与其他设备之间的通信。

[0196] 存储器可以包括随机存取存储器(Random Access Memory,RAM),也可以包括非易失性存储器(Non-Volatile Memory,NVM),例如至少一个磁盘存储器。可选的,存储器还可以是至少一个位于远离前述处理器的存储装置。

[0197] 上述的处理器可以是通用处理器,包括中央处理器(Central Processing Unit,CPU)、网络处理器(Network Processor,NP)等;还可以是数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现场可编程门阵列(Field-Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。

[0198] 在本公开提供的又一实施例中,还提供了一种计算机可读存储介质,该计算机可

读存储介质内存储有计算机程序,所述计算机程序被处理器执行时实现上述任一通信方法的步骤。

[0199] 在本公开提供的又一实施例中,还提供了一种包含指令的计算机程序产品,当其在计算机上运行时,使得计算机执行上述实施例中任一通信方法。

[0200] 在上述实施例中,可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时,可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时,全部或部分地产生按照本公开实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中,或者从一个计算机可读存储介质向另一个计算机可读存储介质传输,例如,所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线(例如同轴电缆、光纤、数字用户线(DSL))或无线(例如红外、无线、微波等)方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质,(例如,软盘、硬盘、磁带)、光介质(例如,DVD)、或者半导体介质(例如固态硬盘Solid State Disk(SSD))等。

[0201] 需要说明的是,在本文中,诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来,而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且,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、物品或者设备不仅包括那些要素,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、物品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0202] 本说明书中的各个实施例均采用相关的方式描述,各个实施例之间相同相似的部分互相参见即可,每个实施例重点说明的都是与其他实施例的不同之处。尤其,对于装置、SIM卡、电子设备和终端设备实施例而言,由于其基本相似于方法实施例,所以描述的比较简单,相关之处参见方法实施例的部分说明即可。

[0203] 以上所述仅为本公开的较佳实施例,并非用于限定本公开的保护范围。凡在本公开的精神和原则之内所作的任何修改、等同替换、改进等,均包含在本公开的保护范围内。

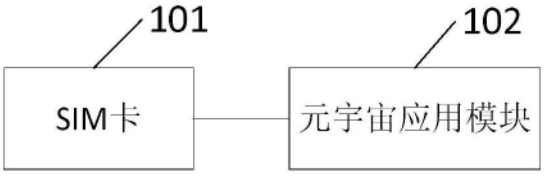

101
102
SIM卡
元宇宙应用模块

图1

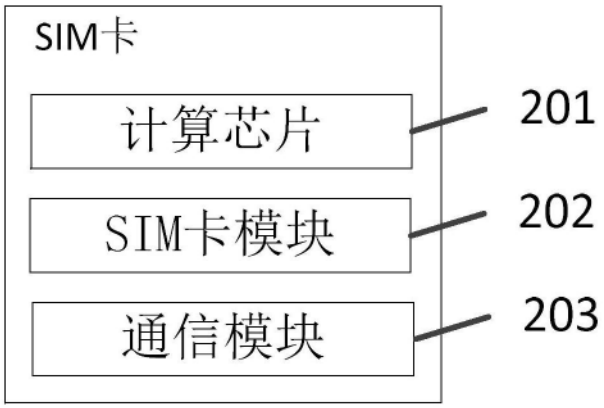

SIM卡
计算芯片
201
SIM卡模块
202
通信模块
203

图2

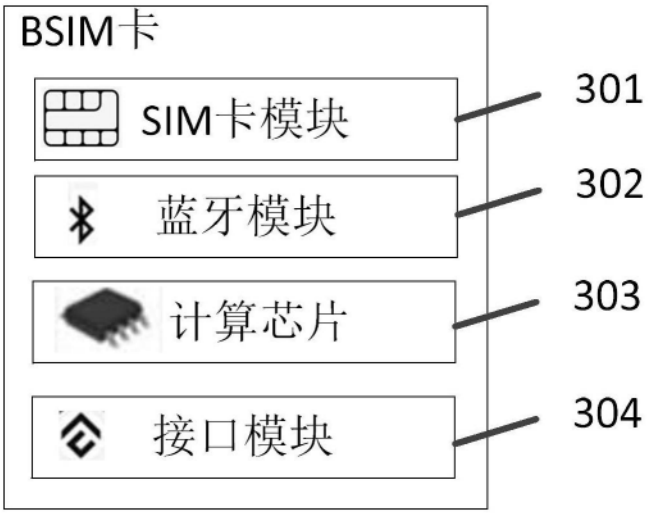

BSIM卡
SIM卡模块
301
蓝牙模块
302
计算芯片
303
接口模块
304

图3

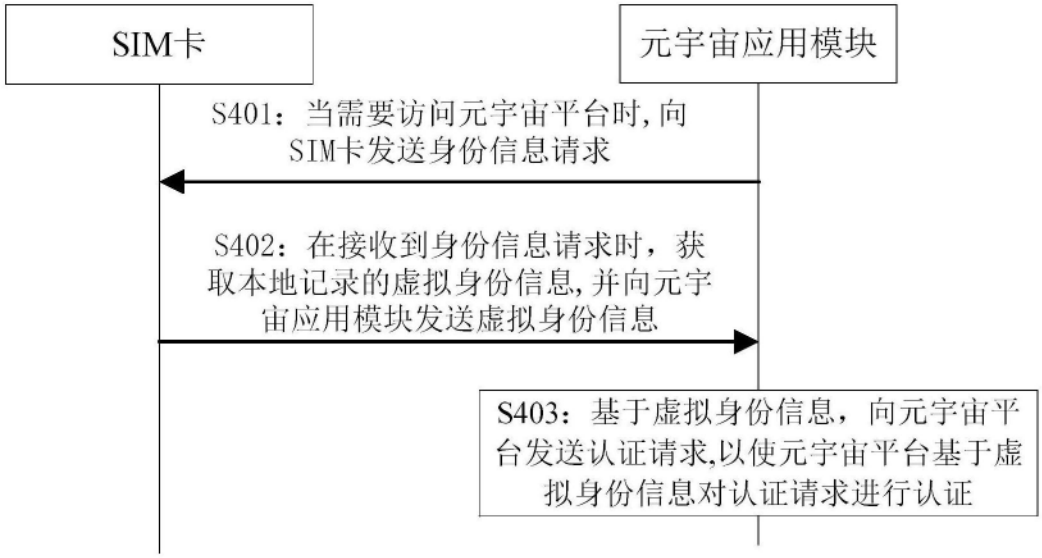

SIM卡
元宇宙应用模块
S401：当需要访问元宇宙平台时，向SIM卡发送身份信息请求
S402：在接收到身份信息请求时，获取本地记录的虚拟身份信息，并向元宇宙应用模块发送虚拟身份信息
S403：基于虚拟身份信息，向元宇宙平台发送认证请求，以使元宇宙平台基于虚拟身份信息对认证请求进行认证

图4

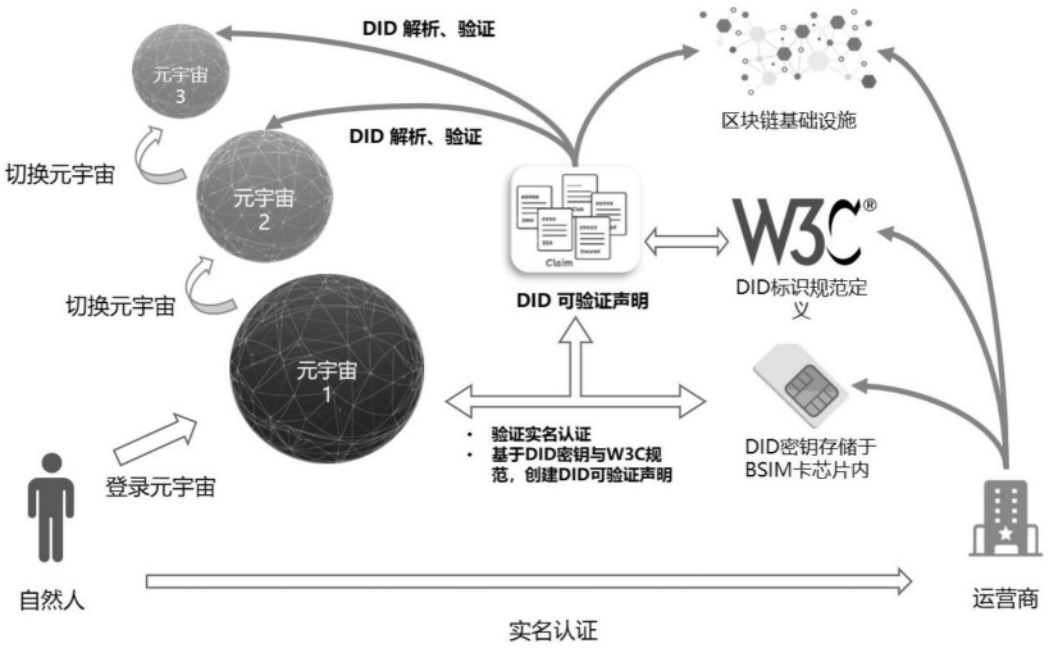

DID 解析、验证
DID 解析、验证
元宇宙3
元宇宙2
元宇宙1
切换元宇宙
切换元宇宙
区块链基础设施
DID 可验证声明
DID标识规范定义
验证实名认证
基于DID密钥与W3C规范，创建DID可验证声明
DID密钥存储于BSIM卡芯片内
登录元宇宙
自然人
运营商
实名认证

图5

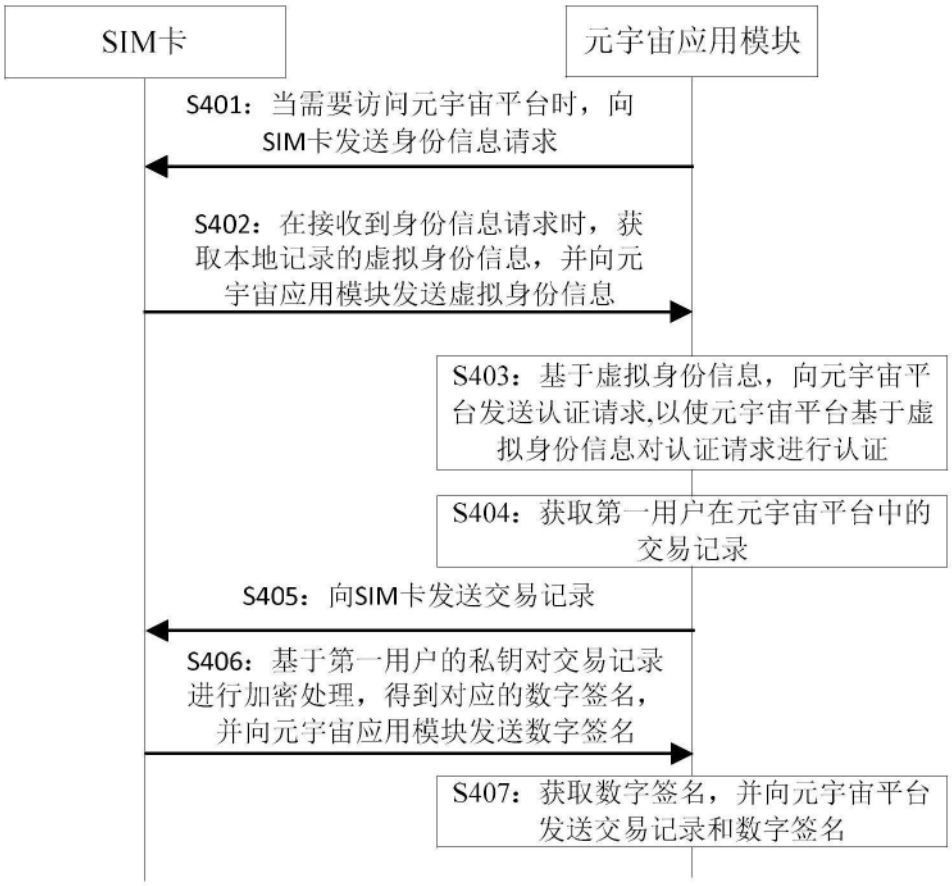

SIM卡
元宇宙应用模块
S401：当需要访问元宇宙平台时，向SIM卡发送身份信息请求
S402：在接收到身份信息请求时，获取本地记录的虚拟身份信息，并向元宇宙应用模块发送虚拟身份信息
S403：基于虚拟身份信息，向元宇宙平台发送认证请求,以使元宇宙平台基于虚拟身份信息对认证请求进行认证
S404：获取第一用户在元宇宙平台中的交易记录
S405：向SIM卡发送交易记录
S406：基于第一用户的私钥对交易记录进行加密处理，得到对应的数字签名，并向元宇宙应用模块发送数字签名
S407：获取数字签名，并向元宇宙平台发送交易记录和数字签名

图6

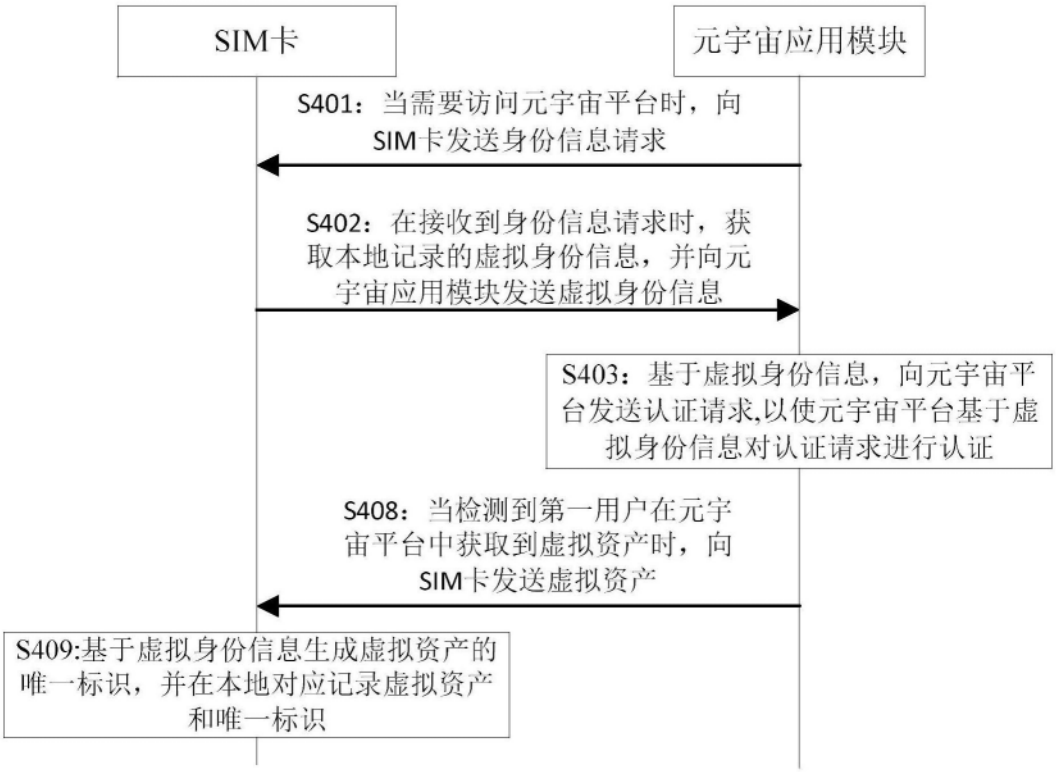

SIM卡
元宇宙应用模块
S401：当需要访问元宇宙平台时，向SIM卡发送身份信息请求
S402：在接收到身份信息请求时，获取本地记录的虚拟身份信息，并向元宇宙应用模块发送虚拟身份信息
S403：基于虚拟身份信息，向元宇宙平台发送认证请求,以使元宇宙平台基于虚拟身份信息对认证请求进行认证
S408：当检测到第一用户在元宇宙平台中获取到虚拟资产时，向SIM卡发送虚拟资产
S409:基于虚拟身份信息生成虚拟资产的唯一标识，并在本地对应记录虚拟资产和唯一标识

图7


生成随机数
S801
基于预设的哈希算法，计算随机数的哈希值，得到第一用户的私钥
S802
基于第一用户的私钥，生成第一用户的DID，作为第一用户的虚拟身份信息
S803

图8

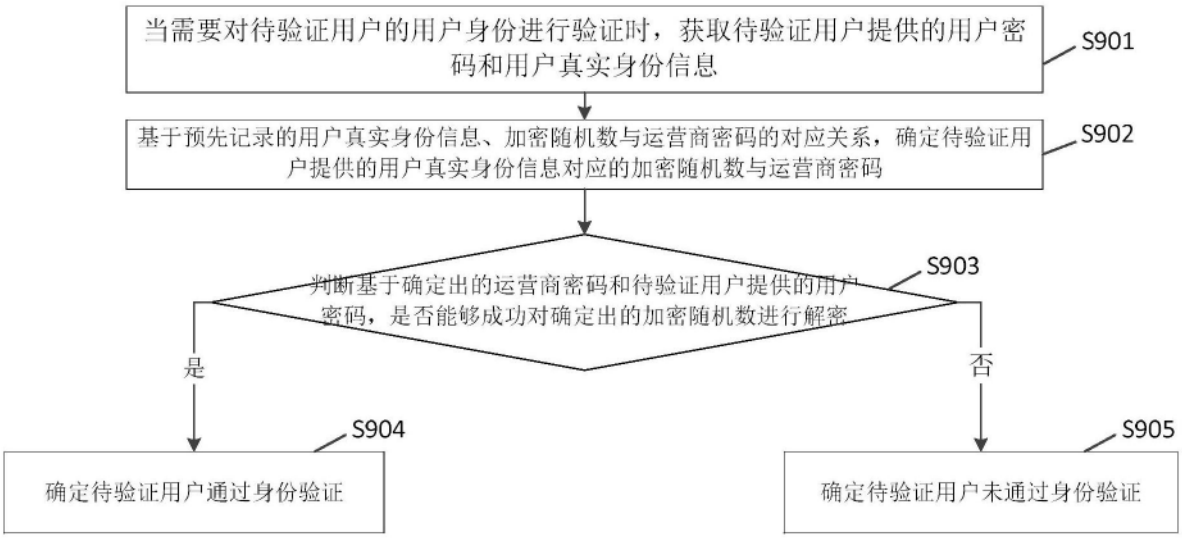

当需要对待验证用户的用户身份进行验证时，获取待验证用户提供的用户密码和用户真实身份信息
S901
基于预先记录的用户真实身份信息、加密随机数与运营商密码的对应关系，确定待验证用户提供的用户真实身份信息对应的加密随机数与运营商密码
S902
判断基于确定出的运营商密码和待验证用户提供的用户密码，是否能够成功对确定出的加密随机数进行解密
S903
是
否
S904
确定待验证用户通过身份验证
S905
确定待验证用户未通过身份验证

图9

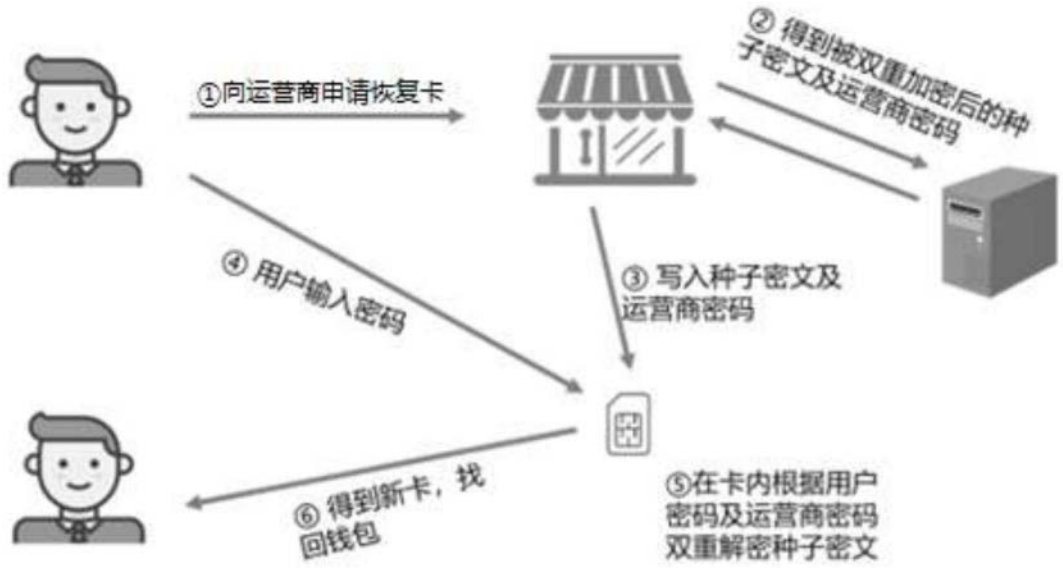

①向运营商申请恢复卡
② 得到被双重加密后的种子密文及运营商密码
③ 写入种子密文及运营商密码
④ 用户输入密码
⑤在卡内根据用户密码及运营商密码双重解密种子密文
⑥ 得到新卡，找回钱包

图10


手机OS（操作系统）
特定接口调用SDK
SIM卡
手机号
加密种子、私钥
加密数字资产
SIM卡计算程序

图11


数字身份
数字资产交易商城
(积分交易平台)
数字艺术品
(音乐、视频、图片等)
可定义所有权和使用权
游戏资产
(装备、物品、能力、皮肤等)
区块链
BSIM
Address:
用户身份
Token:
用户资产
原生资产：积分
智能合约
联盟链
区块链
节点
智能合约
区块链
共识
节点
智能合约
版权保护
节点
智能合约
跨链
节点

图12


BSIM卡
支持多种区块链算法、性能高、
安全性好、使用便捷
可打通对接多种区块链
元宇宙
数字资产管理
元宇宙
数字资产生态
区块链分布式
数字身份
基于通证的数
字资产交易

图13

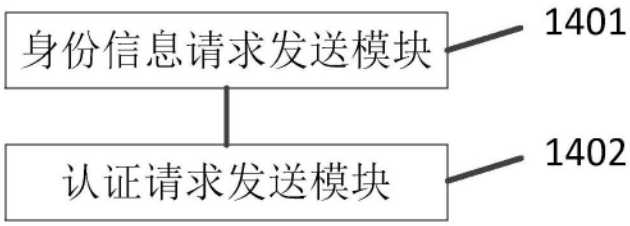

身份信息请求发送模块
1401
认证请求发送模块
1402

图14

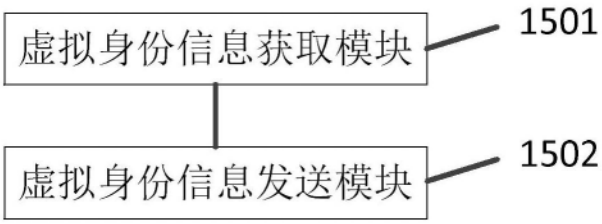

虚拟身份信息获取模块
1501
虚拟身份信息发送模块
1502

图15

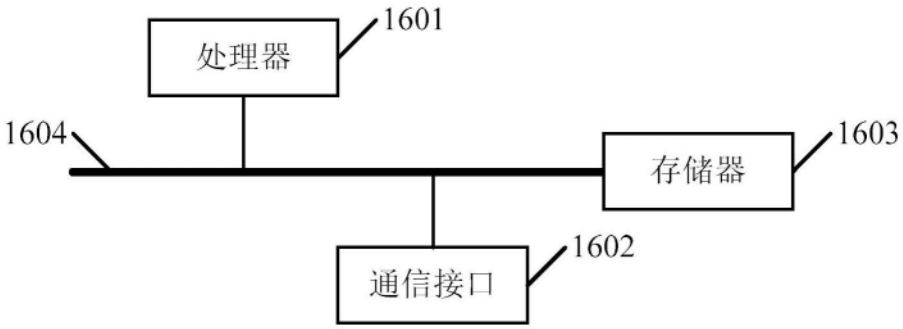

处理器
1601
1604
存储器
1603
通信接口
1602

图16