(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106982205 B
(45)授权公告日 2020.05.19

(21)申请号 201710118907.1

(22)申请日 2017.03.01

(65)同一申请的已公布的文献号
申请公布号 CN 106982205 A

(43)申请公布日 2017.07.25

(73)专利权人 中钞信用卡产业发展有限公司杭州区块链技术研究院
地址 310013 浙江省杭州市西湖区灵隐街道公元大厦南楼903室

(72)发明人 徐忠 姚前 张一锋

(74)专利代理机构 北京东方亿思知识产权代理有限责任公司 11258
代理人 彭琼

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/08(2006.01)
G06Q 20/06(2012.01)
G06Q 20/38(2012.01)
G06F 21/62(2013.01)

(56)对比文件
WO 2015179020 A3,2016.03.10,
CN 106341421 A,2017.01.18,
CN 106296138 A,2017.01.04,
WO 2016200885 A1,2016.12.15,
CN 106385315 A,2017.02.08,
elwingao.解决区块链三大问题的利器.《CSDN》.2016,
kyle.同态加密与智能合约可以完美结合私有和公有区块链的特性.《巴比特》.2016,

审查员 吴超

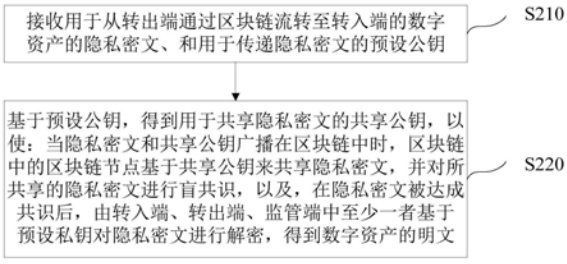
权利要求书5页 说明书11页 附图3页

(54)发明名称

基于区块链的数字资产处理方法和装置

(57)摘要

本发明公开了一种基于区块链的数字资产处理方法和装置。该方法包括:接收用于从转出端通过区块链流转至转入端的数字资产的隐私密文和预设公钥;基于预设公钥,得到用于共享隐私密文的共享公钥,以使:当隐私密文和共享公钥广播在区块链中时,区块链中的区块链节点基于共享公钥来共享隐私密文,并对所共享的隐私密文进行盲共识,以及,在隐私密文被达成共识后,由转入端、转出端、监管端中至少一者基于预设私钥对隐私密文进行解密,得到数字资产的明文。本发明实施例保障了用户的隐私权,并在隐私保护的前提下,可以实现单一通用数字资产在一个或者多个区块链中顺畅流通,保持货币总量不变,并且可以使除交易双方外的监管方随时监控交易信息。



CN 106982205 B

1.一种基于区块链的数字资产处理方法,应用于监管端,其特征在于,所述监管端作为中间跳转机构,所述方法包括:

接收用于从转出端通过区块链流转至转入端的数字资产的隐私密文、和用于传递所述隐私密文的预设公钥;

基于所述预设公钥,得到用于共享所述隐私密文的共享公钥,以使:当所述隐私密文和所述共享公钥广播在所述区块链中时,所述区块链中的区块链节点基于所述共享公钥来共享所述隐私密文,并对所共享的隐私密文进行盲共识,以及,在所述隐私密文被达成共识后,由所述转入端、所述转出端、所述监管端中至少一者基于预设私钥对所述隐私密文进行解密,得到所述数字资产的明文;

其中,所述监管端包括数字货币中心系统和监管系统,所述数字货币中心系统发行法定数字货币,所述监管系统设置有SDM APP和隐私保护中间层组件,所述隐私保护中间层组件为所述区块链上流转的数字货币提供隐私保护功能,所述SDM APP完成所述数字货币数据字段的加解密;

所述基于所述预设公钥,得到用于共享所述隐私密文的共享公钥,包括:

所述监管端接收由转出端提交的预设公钥;

所述监管端将所述预设公钥与指定私钥进行预设密码学运算,得到用于共享隐私密文的共享私钥;

所述监管端基于所述共享私钥,得到用于共享所述隐私密文的共享公钥。

2.根据权利要求1所述的方法,其特征在于,所述对所共享的隐私密文进行盲共识,包括:

利用同态加密方法和/或零知识证明方法对所共享的隐私密文的合法性进行验证,并对验证结果达成一致意见。

3.根据权利要求2所述的方法,其特征在于,所述隐私密文的合法性包括以下项中的至少一项:

所述转入端和所述转出端的身份的合法性、所述转入端和所述转出端的数字资产在流转前后总量保存不变、流转的数字资产量大于或者等于零、转出的数字资产量小于或者等于所述转出端所持有的数字资产量。

4.根据权利要求3所述的方法,其特征在于,所述数字资产是一个或者多个预定数值的Coin数据结构体的数据。

5.根据权利要求4所述的方法,其特征在于,还包括:

接收所述转入端所发送的接收受隐私保护的第一数值的数字资产的接收请求;

响应于所接收的接收请求,向所述转出端发送是否同意转出所述受隐私保护的第一数值的数字资产的指令;

当接收到来自所述转出端的包括同意转出和用于证明受隐私保护的第一数值的数字资产的合法性的密码学证明的应答时,在所述转入端的资产数据库内,写入增加一个或者多个预定受隐私保护的数值的Coin数据结构体的数据的记录,以及写入减少受隐私保护的指定数值的Coin数据结构体的数据的记录;以及,在所述转出端的资产数据库内,写入增加销毁所述一个或者多个受隐私保护的预定数值的Coin数据结构体的数据的记录,以及写入增加所述受隐私保护的指定数值的Coin数据结构体的数据的记录;或者,

接收所述转出端所发送的转出受隐私保护的第一数值的数字资产的转出请求；

响应于所接收的转出请求，向所述转入端发送是否同意接收所述受隐私保护的第一数值的数字资产的指令；

当接收到来自所述转入端的包括同意接收和用于证明受隐私保护的第一数值的数字资产的合法性的密码学证明的应答时，在所述转入端的资产数据库内，写入增加一个或者多个预定受隐私保护的数值的Coin数据结构体的数据的记录，以及写入减少受隐私保护的指定数值的Coin数据结构体的数据的记录；以及，在所述转出端的资产数据库内，写入增加销毁所述一个或者多个受隐私保护的预定数值的Coin数据结构体的数据的记录，以及写入增加所述受隐私保护的指定数值的Coin数据结构体的数据的记录。

6.根据权利要求5所述的方法，其特征在于，当在接收到所述转出端同意转出的应答之后，还包括：

采用同态加密和/或零知识证明的密码学方法验证所述一个或者多个受隐私保护的预定数值的和与所述受隐私保护的指定数值与所述受隐私保护的第一数值的和是否相等；

当验证通过时，

在所述转入端的资产数据库内，写入增加一个或者多个受隐私保护的预定数值的Coin数据结构体的数据的记录，以及写入减少受隐私保护的指定数值的Coin数据结构体的数据的记录；

在所述转出端的资产数据库内，写入增加销毁所述一个或者多个受隐私保护的预定数值的Coin数据结构体的数据的记录，以及写入增加所述受隐私保护后的指定数值的Coin数据结构体的数据的记录。

7.根据权利要求5所述的方法，其特征在于，还包括：

接收来自转入端所发送的接收转出端的受隐私保护的第一数量的数字资产的接收请求；

响应于所接收的接收请求，向所述转出端发送是否同意发送所述受隐私保护的第一数量的数字资产的指令；

当接收到来自所述转出端的拒绝向所述转入端发送第一数量的数字资产的应答时，向所述转入端发送拒绝的反馈。

8.根据权利要求5所述的方法，其特征在于，还包括：

接收来自所述转入端所发送的撤回所述接收请求；

将所接收的撤回所述接收请求反馈给所述转出端。

9.根据权利要求1-8中任一项所述的方法，其特征在于，还包括：

预先在所述一个或者多个区块链中部署智能合约程序，所述智能合约程序用于定义所述数字资产在所述一个或者多个区块链中入场、转账、出场、余额查询中的至少一种操作。

10.一种基于区块链的数字资产处理方法，应用于区块链节点侧，其特征在于，所述方法包括：

获取广播在区块链中的隐私密文和用于共享所述隐私密文的共享公钥；所述共享公钥由监管端生成，所述监管端用于对接收到的由转出端提交的预设公钥进行预设密码学运算，得到用于共享隐私密文的共享私钥，并基于所述共享私钥，得到用于共享所述隐私密文的共享公钥；

当所述隐私密文和所述共享公钥广播在所述区块链中时，基于所述共享公钥来共享所述隐私密文，并对所共享的隐私密文进行盲共识，以及，在所述隐私密文被达成共识后，由转入端、转出端、监管端中至少一者基于预设私钥对所述隐私密文进行解密，得到所述数字资产的明文；

其中，所述监管端包括数字货币中心系统和监管系统，所述数字货币中心系统发行法定数字货币，所述监管系统设置有SDM APP和隐私保护中间层组件，所述隐私保护中间层组件为所述区块链上流转的数字货币提供隐私保护功能，所述SDM APP完成所述数字货币数据字段的加解密。

11.根据权利要求10所述的方法，其特征在于，对所述隐私密文进行盲共识包括：

利用同态加密方法和/或零知识证明方法对所共享的隐私密文的合法性进行验证，并对验证结果达成一致意见。

12.一种基于区块链的数字资产处理装置，应用于监管端，其特征在于，所述装置包括：

数据接收单元，用于接收用于从转出端通过区块链流转至转入端的数字资产的隐私密文、和由转出端提交的用于传递所述隐私密文的预设公钥；

隐私处理单元，用于基于所述预设公钥，得到用于共享所述隐私密文的共享公钥，以使：所述隐私密文和所述共享公钥广播在所述区块链中时，所述区块链中的区块链节点基于所述共享公钥来共享所述隐私密文，并对所共享的隐私密文进行盲共识，以及，在所述隐私密文被达成共识后，由所述转入端、所述转出端和所述监管端基于预设私钥对所述隐私密文进行解密，得到所述数字资产的明文；

其中，所述监管端包括数字货币中心系统和监管系统，所述数字货币中心系统发行法定数字货币，所述监管系统设置有SDM APP和隐私保护中间层组件，所述隐私保护中间层组件为所述区块链上流转的数字货币提供隐私保护功能，所述SDM APP完成所述数字货币数据字段的加解密；

隐私处理单元，用于将所述预设公钥与指定私钥进行预设密码学运算，得到用于共享隐私密文的共享私钥；基于所述共享私钥，得到用于共享所述隐私密文的共享公钥。

13.根据权利要求12所述的装置，其特征在于，所述数字资产是一个或者多个预定数值的Coin数据结构体的数据。

14.根据权利要求13所述的装置，其特征在于，还包括：

请求接收单元，用于接收所述转入端所发送的接收受隐私保护的第一数值的数字资产的接收请求；或者，

用于接收所述转出端所发送的转出受隐私保护的第一数值的数字资产的转出请求；

指令发送单元，用于响应于所接收的接收请求，向所述转出端发送是否同意转出所述受隐私保护的第一数值的数字资产的指令；或者，

用于响应于所接收的转出请求，向所述转入端发送是否同意接收所述受隐私保护的第一数值的数字资产的指令；数据处理单元，用于当接收到来自所述转出端的包括同意转出和用于证明受隐私保护的第一数值的数字资产的合法性的密码学证明的应答时，在所述转入端的资产数据库内，写入增加一个或者多个预定受隐私保护的数值的Coin数据结构体的数据的记录，以及写入减少受隐私保护的指定数值的Coin数据结构体的数据的记录；以及，在所述转出端的资产数据库内，写入增加销毁所述一个或者多个受隐私保护的预定数值的

Coin数据结构体的数据的记录,以及写入增加所述受隐私保护的指定数值的Coin数据结构体的数据的记录;或者,

用于当接收到来自所述转入端的包括同意接收和用于证明受隐私保护的第一数值的数字资产的合法性的密码学证明的应答时,在所述转入端的资产数据库内,写入增加一个或者多个预定受隐私保护的数值的Coin数据结构体的数据的记录,以及写入减少受隐私保护的指定数值的Coin数据结构体的数据的记录;以及,在所述转出端的资产数据库内,写入增加销毁所述一个或者多个受隐私保护的预定数值的Coin数据结构体的数据的记录,以及写入增加所述受隐私保护的指定数值的Coin数据结构体的数据的记录。

15.根据权利要求14所述的装置,其特征在于,还包括:

数据验证单元,用于采用同态加密和/或零知识证明的密码学方法验证所述一个或者多个受隐私保护的预定数值的和与所述受隐私保护的指定数值与所述受隐私保护的第一数值的和是否相等;

所述数据处理单元,还用于当验证通过时,

在所述转入端的资产数据库内,写入增加一个或者多个受隐私保护的预定数值的Coin数据结构体的数据的记录,以及写入减少受隐私保护的指定数值的Coin数据结构体的数据的记录;

在所述转出端的资产数据库内,写入增加销毁所述一个或者多个受隐私保护的预定数值的Coin数据结构体的数据的记录,以及写入增加所述受隐私保护后的指定数值的Coin数据结构体的数据的记录。

16.根据权利要求14所述的装置,其特征在于,还包括:

所述请求接收单元,还用于接收来自转入端所发送的接收转出端的受隐私保护的第一数量的数字资产的接收请求;

所述指令发送单元,还用于响应于所接收的接收请求,向所述转出端发送是否同意发送所述受隐私保护的第一数量的数字资产的指令;

反馈发送单元,用于当接收到来自所述转出端的拒绝向所述转入端发送第一数量的数字资产的应答时,向所述转入端发送拒绝的反馈。

17.根据权利要求14所述的装置,其特征在于,其中:

所述请求接收单元,还用于接收来自所述转入端所发送的撤回所述接收请求;

反馈发送单元,还用于将所接收的撤回所述接收请求反馈给所述转出端。

18.根据权利要求12-17中任一项所述的装置,其特征在于,还包括:

合约部署单元,用于预先在所述一个或者多个区块链中部署智能合约程序,所述智能合约程序用于定义所述数字资产在所述一个或者多个区块链中入场、转账、出场、余额查询中的至少一种操作。

19.一种基于区块链的数字资产处理装置,应用于区块链节点侧,其特征在于,所述装置包括:

数据获取单元,用于获取广播在区块链中的隐私密文和用于共享所述隐私密文的共享公钥;所述共享公钥由监管端生成,所述监管端用于对接收到的由转出端提交的预设公钥进行预设密码学运算,得到用于共享隐私密文的共享私钥,并基于所述共享私钥,得到用于共享所述隐私密文的共享公钥

数据处理单元，用于当所述隐私密文和所述共享公钥广播在所述区块链中时，基于所述共享公钥来共享所述隐私密文，并对所共享的隐私密文进行盲共识，以及，在所述隐私密文被达成共识后，由转入端、所述转出端、所述监管端中至少一者基于预设私钥对所述隐私密文进行解密，得到所述数字资产的明文；

其中，所述监管端包括数字货币中心系统和监管系统，所述数字货币中心系统发行法定数字货币，所述监管系统设置有SDM APP和隐私保护中间层组件，所述隐私保护中间层组件为所述区块链上流转的数字货币提供隐私保护功能，所述SDM APP完成所述数字货币数据字段的加解密。

20.根据权利要求19所述的装置，其特征在于，所述数据处理单元还用于：利用同态加密方法和/或零知识证明方法对所共享的隐私密文的合法性进行验证，并对验证结果达成一致意见。

基于区块链的数字资产处理方法和装置

技术领域

[0001] 本发明涉及通信技术领域，尤其涉及一种基于区块链的数字资产处理方法和装置。

背景技术

[0002] 随着通信技术的发展，区块链由于去中心化、公开、透明、无法篡改等优点而逐渐被应用于数据处理的应用场景中。区块链由于其技术本身的限制难以承载海量的数据交易，同时不同的区块链承载不同类型的数据业务也符合实际的业务需求。例如股权区块链、不动产区块链、小额支付区块链等分别承载对应的数字资产业务。

[0003] 现有的不同区块链各自使用本区块链的特有货币。不同区块链上使用数字货币进行资产交易就需要将不同数字货币进行转换，例如，比特币需要进入以太网就需要转化为以太币。现有的区块链数字资产处理方法存在操作繁琐、不同币种相互转化会产生货币损耗、缺乏央行等权威机构监管、用户的数字资产的隐私得不到保护。

[0004] 如何保障用户的隐私权，并在隐私保护的前提下实现单一通用法定货币在不同区块链中顺畅流通、并保持货币总量不变，是业界需要解决的问题。

发明内容

[0005] 鉴于以上所述一个或多个问题，本发明实施例提供了一种数字资产处理方法和装置。

[0006] 第一方面，提供了一种基于区块链的数字资产处理方法。该方法包括以下步骤：

[0007] 接收用于从转出端通过区块链流转至转入端的数字资产的隐私密文、和用于传递隐私密文的预设公钥；

[0008] 基于预设公钥，得到用于共享隐私密文的共享公钥，以使：当隐私密文和共享公钥广播在区块链中时，区块链中的区块链节点基于共享公钥来共享隐私密文，并对所共享的隐私密文进行盲共识，以及，在隐私密文被达成共识后，由转入端、转出端、监管端中至少一者基于预设私钥对隐私密文进行解密，得到数字资产的明文。

[0009] 第二方面，提供了一种基于区块链的数字资产处理方法。该方法包括以下步骤：

[0010] 获取广播在区块链中的隐私密文和用于共享所述隐私密文的共享公钥；

[0011] 当所述隐私密文和所述共享公钥广播在所述区块链中时，基于所述共享公钥来共享所述隐私密文，并对所共享的隐私密文进行盲共识，以及，在所述隐私密文被达成共识后，由所述转入端、所述转出端、所述监管端中至少一者基于预设私钥对所述隐私密文进行解密，得到所述数字资产的明文。

[0012] 第三方面，提供了一种基于区块链的数字资产处理装置。该装置包括：

[0013] 数据接收单元，用于接收用于从转出端通过区块链流转至转入端的数字资产的隐私密文、和用于传递所述隐私密文的预设公钥；

[0014] 隐私处理单元，用于基于所述预设公钥，得到用于共享所述隐私密文的共享公钥，

以使:所述隐私密文和所述共享公钥广播在所述区块链中时,所述区块链中的区块链节点基于所述共享公钥来共享所述隐私密文,并对所共享的隐私密文进行盲共识,以及,在所述隐私密文被达成共识后,由所述转入端、所述转出端和所述监管端基于预设私钥对所述隐私密文进行解密,得到所述数字资产的明文。

[0015] 第四方面,提供了一种基于区块链的数字资产处理装置。该装置包括:

[0016] 数据获取单元,用于获取广播在区块链中的隐私密文和用于共享隐私密文的共享公钥;

[0017] 数据处理单元,用于当所述隐私密文和所述共享公钥广播在所述区块链中时,基于所述共享公钥来共享所述隐私密文,并对所共享的隐私密文进行盲共识,以及,在所述隐私密文被达成共识后,由所述转入端、所述转出端、所述监管端中至少一者基于预设私钥对所述隐私密文进行解密,得到所述数字资产的明文。

[0018] 由此,本发明实施例通过明文消息进行加密,生成隐私密文,并基于预设公钥,得到用于共享隐私密文的共享公钥,将隐私密文和共享公钥广播在区块链中,以使:转入端、转出端和监管端基于预设私钥对隐私密文进行解密,得到明文;区块链中的节点基于共享公钥来共享隐私密文,并对所共享的隐私密文进行盲共识,保障了用户的隐私权。另外,本实施例可以通过设置监管方(监管端)作为中间跳转机构,将转出端发出的数字资产进行隐私处理,然后再通过区块链转至转入端,在隐私保护的前提下,可以实现单一通用数字资产在一个或者多个区块链中顺畅流通,并保持货币总量不变。

附图说明

[0019] 为了更清楚地说明本发明实施例的技术方案,下面将对本发明实施例中所需要使用的附图作简单地介绍,显而易见地,下面所描述的附图仅仅是本发明的一些实施例,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。

[0020] 图1是本发明一实施例的基于区块链的数字资产处理的系统架构示意图。

[0021] 图2是本发明一实施例的基于区块链的数字资产处理的流程示意图。

[0022] 图3是本发明另一实施例的基于区块链的数字资产处理的流程示意图。

[0023] 图4是本发明一实施例的基于区块链的数字资产处理的结构示意图。

[0024] 图5是本发明另一实施例的基于区块链的数字资产处理的结构示意图。

具体实施方式

[0025] 为使本发明实施例的目的、技术方案和优点更加清楚,下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0026] 需要说明的是,在不冲突的情况下,本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

[0027] 数字资产可以是区块链上可转移的数字信息,往往与现实世界的某种实物对应,它由前述账户地址或智能合约地址持有。数字资产可以包括但不限于法定数字货币。法定

数字货币可以是由政府央行发行的数字货币。下面以数字货币在区块链中进行交易为例说明基于区块链的数字资产处理方法的实现方式。

[0028] 图1是本发明一实施例的基于区块链的数字资产处理的系统架构示意图。

[0029] 如图1所示，该系统架构可以包括：监管方(即监管端)110、转出端120、转入端130、网络140和区块链150。区块链150可以包括：区块链节点151-154和部署在区块链150中的智能合约程序155。监管方110可以央行、票交所等权威机构。监管方110可以包括：数字货币中心系统111和监管系统112。数字货币中心系统111可以用于发行法定数字货币，存储支付准备数据库，支付准备数据库用于记录支付准备数字资产的发行(创建)和回收(转出)等数据。

[0030] 转出端120和转入端130分别是交易的付款方和收款方。例如，转出端120需要想转100万数字货币给转入端130。转出端120需要先将这笔钱“出场”到数字货币中心系统111内部，由数字货币中心系统111的支付准备数据库记录这笔钱并转换变为通用数字货币(央行发行的法定数字货币)，然后再将通用数字货币支付给转入端130。

[0031] 监管系统112可以设置有SDM APP和隐私保护中间层组件(SDDS-Middleware)。SDDS-Middleware可以为区块链150(例如，数字票据链)上流转的数字货币提供隐私保护功能。因此在区块链上的数字货币包含隐私保护后的数据字段。监管系统112需要对数字货币的明文信息进行处理，具体数字货币数据字段的加解密可以由SDM APP完成。具体来说，区块链团队可以提供数字货币管理合约SDMFrontEnd与隐私保护相关的基础功能，并提供给监管方110做进一步开发以加入SDM所需的其他功能。同时，票据链团队以隐私保护中间层组件(SDDS-Middleware)的方式提供SDM APP所需的隐私保护加解密功能，SDDS-Middleware还将进一步提供从区块链上即时同步交易详细信息的API。与带隐私保护功能的区块链交互时，数字货币中心系统110可以通过监管方120的隐私保护中间层(SDDS Middleware)进行隐私数据转换。数字货币中心系统111中登记的是明文数字货币，在区块链150上登记的则是密文数字货币。

[0032] 垂直虚线部分可以是隐私秘文和明文的分界线，虚线左侧所有的业务操作都是采用明文操作，虚线右侧出现的金额相关的操作都是密文。具体来说，业务方(包括参与者和管理者)在自己的子系统内部处理的金额相关业务都是明文的，一旦上链，为了保障隐私，提交到区块链上的数据都是隐私数据，只有交易对手方和监管方有能力解码。SDM APP是用来做隐私明文、隐私密文互相转换的中间件，通过这个中间件(包括预设的公钥、私钥数据)业务方可以不关心区块链上隐私数据加解密的细节，只需要向SDM APP写入明文数据或者读取明文数据即可。

[0033] 网络140用以在各种电子设备之间提供通信链路的介质。具体的，网络设备可以包括各种连接类型，例如有线、无线通信链路或者光纤电缆等。

[0034] 区块链150可以是分布式统一账本，由所有参与方(例如各区块链节点151-154)共同决定记账内容，每个参与方都保存有全量数据，任何个体无法对数据进行篡改。区块链150可以是联盟链。联盟链与公有链相对，是区块链的一种。特点是具有准入制度，只有获得批准的参与方才能加入。对应的，联盟链中会有监管方和普通参与方两种角色。

[0035] 智能合约程序155可以是数字货币管理智能合约。数字货币管理智能合约是部署在特定区块链上的智能合约，只有部署了该合约的区块链可以进行资产数据处理。数字货

币管理智能合约可以包括:SDMFrontEnd货币合约、票据合约和业务合约。

[0036] 转出端120可以通过区块链150将数字资产通过区块链150转给转入端130。转出端120和转入端130可以是区块链150之外的节点,也可以是区块链150中的节点,此方面内容不做限制。

[0037] 可以理解,图1中的设备的数目仅仅是示意性的。根据实现需要,进行调整。其中,区块链节点151-154、转出端120和转入端130可以是各种电子设备。这些电子设备包括但不限于个人电脑、智能手机、平板电脑、个人数字助理、服务器等。这些电子设备可以安装有各种通讯客户端应用,例如即时通信工具、邮箱客户端、社交平台软件、音频视频软件等。其中,这些电子设备具有存储器和逻辑运算处理器、控制元件等。这些电子设备可以发送数据请求,或者可以接收数据请求,还可以对数据进行分析、验证和存储等处理。

[0038] 另外,该架构还可以其他基础设备,例如,网络交互和路由设备。

[0039] 下面各实施例均可以应用于图1所示架构,为了描述简洁,各实施例可以相互参考引用。

[0040] 图2是本发明一实施例的基于区块链的数字资产处理的流程示意图。

[0041] 如图2所示,该方法包括以下步骤:S210,接收用于从转出端通过区块链流转至转入端的数字资产的隐私密文、和用于传递隐私密文的预设公钥;S220,基于预设公钥,得到用于共享隐私密文的共享公钥,以使:当隐私密文和共享公钥广播在区块链中时,区块链中的区块链节点基于共享公钥来共享隐私密文,并对所共享的隐私密文进行盲共识,以及,在隐私密文被达成共识后,由转入端、转出端、监管端中至少一者基于预设私钥对隐私密文进行解密,得到数字资产的明文。本实施例可以应用于图1所述监管方(监管端)110。监管方可以作为本实施例的各个步骤的执行主体,执行基于区块链的数字资产处理。监管方(SDM与票交所)具有看穿机制,可以即时追踪票据链上每一笔交易。一旦发现参与方具有违法动作,SDM或票交所(SDMFrontEnd的内部设计决定)有权冻结对应参与方的数字货币,也因此该参与方无法参与后续的票据交易。数字票据链上部署SDM提供的数字货币管理合约SDMFrontEnd,同时数字货币中心系统通过SDM的软件APP对数字票据区块链数据进行处理、操作。数字货币管理合约SDMFrontEnd集中管理票据链上的数字货币。

[0042] 在步骤S210中,为了使消息加密机制有效,首先,转出端向监管方提交自己的消息传递预公钥,然后由监管方设定正式的消息传递公钥;然后,交易双方(转出端和转入端)根据公开可查的消息传递公钥可以进行消息的点对点传递。需要指出的是,监管方设定消息传递公钥的过程只需要操作一次,后续的参与方之间的交易无需重复向监管方申请新的消息传递公钥。

[0043] 本实施例的数字票据链(即区块链)上流转的数字货币接受了隐私保护,因此在区块链上的数字货币包含隐私保护(即加密)后的数据字段。转出端与转出端的交易详细信息可以包括但不限于下列字段:

[0044]

汇款人	收款人	密文金额	明文金额	隐私秘钥	交易哈希	所在区块	上笔交易
From	To	Value	Amount	Key	TxHash	BlockN	PreTxHash

[0045] 在步骤S220中,上述两个步骤可以用两个函数来实现。第一个函数可以由参与方

发起，用来提交自己的消息传递预公钥$Pk_0^i = x_0^i G$，智能合约只做基本的重复调用检测，并将该数据存储。第二个函数可以由监管方调用，监管方计算自己与参与方的消息传递共享私钥，并将对应的公钥公布。具体步骤如下：

[0046] 1、链外计算$x_i = hash(x_0 \cdot Pk_0^i) = hash(x_0 x_0^i G)$，其中，Pk可以是公钥，Xi可以是私钥，hash为哈希运算；

[0047] 2、链外计算$Pk^i = x_i G$，记为messagePk，作为参数提交给智能合约；

[0048] 3、智能合约记录Pk^i和holder(收款方)的对应关系备查。

[0049] 通过上述步骤，完成了参与方与监管方关于消息传递共享私钥的分发问题。同时，参与方之间进行消息传递私钥共享时，只需要根据对手方的消息公钥Pk^j和自己持有的消息私钥x_i即可计算出二者的共享消息私钥。同时该共享消息私钥监管方也可以轻易计算出，并对交易进行跟踪。

[0050] 为了完成隐私共识，在转出端账号初始化时公布用户持有的消息传递公钥。该公钥用来实现对手方之间的私钥共享，进而保证在点对点转账时可以安全传递信息，并且给予监管方看穿能力。例如，利用m_PBOCpk用来保存监管方公布的消息传递公钥：$Pk_0 = x_0 G$，利用m_msgPK用来保存每个参与方的消息传递公钥，在执行隐私支付时，对手方使用该公钥加密后传递给参与方。

[0051] 由此，本发明实施例基于预设公钥，得到用于共享隐私密文的共享公钥以使：当隐私密文和共享公钥广播在区块链中时，区块链中的区块链节点基于共享公钥来共享隐私密文，并对所共享的隐私密文进行盲共识，以及，在隐私密文被达成共识后，由转入端、转出端、监管端中至少一者基于预设私钥对隐私密文进行解密，得到数字资产的明文，保障了用户的隐私权。另外，本实施例可以通过设置监管方作为中间跳转机构，将转出端发出的数字资产进行隐私处理，然后再通过区块链转至转入端，在隐私保护的前提下，可以实现单一通用数字资产在一个或者多个区块链中顺畅流通，并保持货币总量不变。

[0052] 在一些实施例中，对所共享的隐私密文进行盲共识，可以包括：利用同态加密方法和/或零知识证明方法对所共享的隐私密文的合法性进行验证，并对验证结果达成一致意见。票据链上的数字货币是以隐私保护密文存在的，本实施例可以采取同态加密、零知识证明和密钥共享的密码学技术保障了对交易行为的盲共识。各个区块链节点在验证时，无法知晓数字资产的金额等敏感信息。

[0053] 由此，本实施例通过盲共识，保证了数字资产不仅可以通过区块链中的各个节点进行验证，而且可以保护用户的隐私，改善了用户的体验。

[0054] 在一些实施例中，隐私密文的合法性包括以下项中的至少一项：转入端和转出端的身份的合法性、转入端和转出端的数字资产在流转前后总量保存不变、流转的数字资产量大于或者等于零、转出的数字资产量小于或者等于转出端所持有的数字资产量。

[0055] 由此，本实施例可以保障转入端和转出端的数字资产合法且在流转前后总量保存不变，保障了数据转换的安全性，防止了数据转换的损耗。

[0056] 在一些实施例中，基于预设公钥，得到用于共享隐私密文的共享公钥，可以包括：将预设公钥与指定私钥进行预设密码学运算，得到用于共享隐私密文的共享私钥；基于共享私钥，得到用于共享隐私密文的共享公钥。

[0057] 在一些实施例中，数字资产是一个或者多个预定数值的Coin数据结构体的数据。例如，采用单一智能合约存储和管理票据链上的数字货币，每个用户持有多个表现为Coin结构体的数字货币，每个数字货币具备不同的面额，用户对数字货币进行转账时，需要指定欲花费的Coin列表，同时用户指定找零金额信息，智能合约验证欲花费的Coin金额之和与收款金额加找零金额相等后完成转账，并利用找零金额数据生成一个新的Coin划拨给付款方。

[0058] 其中，Coin结构体可以是数字货币的主要存储结构；PendingCoin结构体用来存储收款方发起的但付款方尚未同意的收款请求；MoneySet结构体可以看做隐私保护后的转账金额(附带一些零知识信息)。本实施例可以用m_account保存账户当前持有的数字货币的ID列表；还可以用m_cashBank记录每张数字货币的面额(隐私值)、归属权等信息；也可以用m_pendingTx记录当前尚未确认付款的交易信息。

[0059] 在一些实施例中，在上述各实施例的基础上，基于区块链的数字资产的处理方法还可以包括：预先在一个或者多个区块链中部署智能合约程序，智能合约程序用于定义数字资产在一个或者多个区块链中入场、转账、出场、余额查询中的至少一种操作。数字货币智能合约的基本函数可以包括：数字货币入场、数字货币出场、转账(包含发起收款、同意付款、拒绝/撤回付款等子步骤)等。

[0060] 下面以票据业务参与方生命周期时间顺序，来描述利用智能合约程序来实现数字资产处理的实现方式。

[0061] 步骤1：票据账号注册。

[0062] 在本实施例中，数字票据参与方(例如转出端和转入端)向监管方(即票交所)提供相应身份证明材料和自己持有信息传递私钥对应的公钥Pk，该Pk用来做信息传递使用。票交所为该参与方创建对应的账号智能合约，对应的合约ID(即合约地址)为SDDS-ID。其后该账号即可参与票据交易并持有数字货币。

[0063] 步骤2：数字货币账号绑定。

[0064] 在本实施例中，参与方向SDM提供相应的身份证明材料和票据链上的身份SDDS-ID，SDM通过SDM APP查阅票据链上公布的对应参与方的身份证明材料，确认一致符合后将票据链上的SDDS-ID同数字货币系统中对应参与方的SDM-ID进行绑定。

[0065] 步骤3：数字货币入场。

[0066] 在本实施例中，参与方(例如转出端，即付款方)调用SDM业务接口做数字货币入场申请，申请通过并完成数字货币中心相关的一系列内部操作后，SDM APP调用SDMFrontEnd智能合约为参与方在票据链上增加对应数额的基于隐私保护的数字货币。

[0067] 步骤4：数字货币转账。

[0068] 在本实施例中，手动转账和智能合约DVP转账类似，区别是前者由参与方账户直接调用SDMFrontEnd智能合约发起交易，后者由参与方账户调用其他智能合约然后简介调用SDMFrontEnd智能合约发起交易。对于SDMFrontEnd智能合约来说，二者没有本质区别，下面统称为“转账”。每一笔转账和数字货币的入场、出场，SDDS-Middleware中间件都会即时解密、记录并输出到指定数据库中。同时SDDS-Middleware还将提供回溯功能，即指定票据链上的区块序号即可读取该区块内发生的所有交易详细列表。通过该回溯功能，监管方可以掌握票据链上的所有交易细节。

[0069] 步骤5:数字货币出场。

[0070] 在本实施例中,与数字货币入场步骤类似,参与方调用SDM业务接口做数字货币出场申请。SDM APP调用SDMFrontEnd智能合约为参与方在票据链上减少对应数值的基于隐私保护的数字货币。

[0071] 步骤6:数字货币余额查询。

[0072] 在本实施例中,参与方可以通过本地区块链节点直接查询自己的数字货币余额和历史记录。监管方(票交所节点、SDM节点)具有看穿机制,可以通过本地区块链节点直接明文查询所有参与方的数字货币余额和历史记录。SDMFrontEnd需要提供给予隐私保护的数字货币余额直接读取功能,即密文查询功能。参与方只拥有自己的隐私保护私钥,因此只能解开自己的基于隐私保护的数字货币的余额密文。

[0073] 考虑票据链隐私保护的需求,在上述业务逻辑基础上将转账动作分割成:收款方发起收款、付款方同意付款两步进行。另外,可以在增加付款方拒绝付款、收款方撤回请求的步骤。

[0074] 在一些实施例中,在上述各实施例的基础上,基于区块链的数字资产的处理方法还可以包括:接收转入端所发送的接收受隐私保护的第一数值的数字资产的接收请求;响应于所接收的接收请求,向转出端发送是否同意转出受隐私保护的第一数值的数字资产的指令;当接收到来自转出端的包括同意转出和用于证明受隐私保护的第一数值的数字资产的合法性的密码学证明的应答时,在转入端的资产数据库内,写入增加一个或者多个预定受隐私保护的数值的Coin数据结构体的数据的记录,以及写入减少受隐私保护的指定数值的Coin数据结构体的数据的记录;以及,在转出端的资产数据库内,写入增加销毁一个或者多个受隐私保护的预定数值的Coin数据结构体的数据的记录,以及写入增加受隐私保护的指定数值的Coin数据结构体的数据的记录;

[0075] 或者,接收转出端所发送的转出受隐私保护的第一数值的数字资产的转出请求;响应于所接收的转出请求,向转入端发送是否同意接收受隐私保护的第一数值的数字资产的指令;当接收到来自转入端的包括同意接收和用于证明受隐私保护的第一数值的数字资产的合法性的密码学证明的应答时,在转入端的资产数据库内,写入增加一个或者多个预定受隐私保护的数值的Coin数据结构体的数据的记录,以及写入减少受隐私保护的指定数值的Coin数据结构体的数据的记录;以及,在转出端的资产数据库内,写入增加销毁一个或者多个受隐私保护的预定数值的Coin数据结构体的数据的记录,以及写入增加受隐私保护的指定数值的Coin数据结构体的数据的记录。

[0076] 例如,数字资产可以是由A转给B的,但可以A先发起转让动作,B确认;也可由B发起接受动作,再由A确认。

[0077] 在一些实施例中,在上述各实施例的基础上,基于区块链的数字资产的处理方法还可以包括:采用同态加密和/或零知识证明的密码学方法验证一个或者多个受隐私保护的预定数值的和与受隐私保护的指定数值与受隐私保护的第一数值的和是否相等;当验证通过时,在转入端的资产数据库内,写入增加一个或者多个受隐私保护的预定数值的Coin数据结构体的数据的记录,以及写入减少受隐私保护的指定数值的Coin数据结构体的数据的记录;在转出端的资产数据库内,写入增加销毁一个或者多个受隐私保护的预定数值的Coin数据结构体的数据的记录,以及写入增加受隐私保护后的指定数值的Coin数据结构体

的数据的记录。

[0078] 在一些实施例中，在上述各实施例的基础上，基于区块链的数字资产的处理方法还可以包括：接收来自转入端所发送的接收转出端的受隐私保护的第一数量的数字资产的接收请求；响应于所接收的接收请求，向转出端发送是否同意发送受隐私保护的第一数量的数字资产的指令；当接收到来自转出端的拒绝向转入端发送第一数量的数字资产的应答时，向转入端发送拒绝的反馈。

[0079] 在一些实施例中，在上述各实施例的基础上，基于区块链的数字资产的处理方法还可以包括：接收来自转入端所发送的撤回接收请求；将所接收的撤回接收请求反馈给转出端。

[0080] 数字货币智能合约的基本函数有：数字货币入场、数字货币出场、转账(包含发起收款、同意付款、拒绝/撤回付款等子步骤)等。下面用五个实施例来详细说明各个函数的实现方式。

[0081] 第一实施例，用于说明数字货币入场函数的实现方式。

[0082] 本实施例可以由监管方调用，输入入场后的收款方地址与转账金额结构体_amount。函数内部做如下操作：

[0083] 1、对_amount进行必要的隐私保护验证(即验证RangeProof)；

[0084] 2、在m_cashBank创建新的Coin，金额为_amount；

[0085] 3、在m_account将新Coin的ID分配给_holder；

[0086] 4、记录相应EventLog；

[0087] 5、返回该新创建的Coin的ID；

[0088] 第二实施例，用于说明数字货币出场函数的实现方式。

[0089] 本实施例可以由监管方调用，输入出场方地址、出场方持有的部分数字货币的ID列表，扣款金额_amount和找零金额_change。函数内部做如下操作：

[0090] 1、对_amount和_change进行必要的隐私保护验证(即验证RangeProof)；

[0091] 2、验证：Σ(Coin.value)＝＝_amount.value+_change.value；

[0092] 3、销毁输入的coin列表对应的coin；

[0093] 4、创建新的Coin，金额为_change作为找零；

[0094] 5、将上述Coin所有权分配给_holder；

[0095] 6、记录相应EventLog；

[0096] 7、返回上述找零Coin的ID。

[0097] 在本实施例中，如果Σ(Coin.value)恰好等于_amount.value，则似乎不必要出现_change，但由于隐私保护的需求，此时_change依然存在。后续可以通过附带花费零值Coin来删除这些冗余数据。

[0098] 第三实施例，用于说明发起收款函数的实现方式。

[0099] 本实施例可以由收款方调用，输入参数为付款方地址、付款金额结构体等。函数内部完成如下步骤：

[0100] 1、对_amount进行必要的隐私保护验证(即验证RangeProof)；

[0101] 2、在m_pendingTx中增加一条记录；

[0102] 3、记录相应EventLog；

[0103] 4、返回上述记录的ID。

[0104] 第四实施例，用于说明确认付款函数的实现方式。

[0105] 本实施例可以由付款方发起，发起后即完成支付业务。输入参数为欲花费的数字货币列表、欲支付的待付款请求(可以支持同时支付多笔请求)、找零信息等。函数内部完成如下步骤：

[0106] 1、对_changeMoney进行必要的隐私保护验证；

[0107] 2、验证：∑(Coin.value)＝＝∑(Pending.value)+_changeMoney.value；

[0108] 3、销毁输入的Coin列表对应的Coin；

[0109] 4、利用_pending_ids中的数据分别创建Coin并分配给对应的收款方；

[0110] 利用_changeMoney的信息创建找零Coin并分配给付款方；

[0111] 5、记录相应EventLog；

[0112] 6、返回找零Coin对应的ID。

[0113] 在本实施例中，收款方利用EventLog来收到付款通知，并获知得到的Coin的ID。

[0114] 第五实施例，用于说明确认付款函数的实现方式。

[0115] 本实施例可以由交易双方的任一方发起，发起后删除pending数据。

[0116] 图3是本发明另一实施例的基于区块链的数字资产处理的流程示意图。

[0117] 如图3所示，该方法可以包括以下步骤：S310，获取广播在区块链中的隐私密文和用于共享隐私密文的共享公钥；S320，当隐私密文和共享公钥广播在区块链中时，基于共享公钥来共享隐私密文，并对所共享的隐私密文进行盲共识，以及，在隐私密文被达成共识后，由转入端、转出端、监管端中至少一者基于预设私钥对隐私密文进行解密，得到数字资产的明文。

[0118] 在一些实施例中，对隐私密文进行盲共识包括：利用同态加密方法和/或零知识证明方法对所共享的隐私密文的合法性进行验证，并对验证结果达成一致意见。

[0119] 在一些实施例中，隐私密文的合法性包括以下项中的至少一项：转入端和转出端的身份的合法性、转入端和转出端的数字资产在流转前后总量保存不变、流转的数字资产量大于或者等于零、转出的数字资产量小于或者等于转出端所持有的数字资产量。

[0120] 需要说明的是，在不冲突的情况下，本领域的技术人员可以按实际需要将上述的操作步骤的顺序进行灵活调整，或者将上述步骤进行灵活组合等操作。为了简明，不再赘述各种实现方式。另外，各实施例的内容可以相互参考引用。

[0121] 图4是本发明一实施例的基于区块链的数字资产处理的结构示意图。

[0122] 如图4所示，基于区块链的数字资产处理装置400可以包括：数据接收单元410和隐私处理单元420。其中，数据接收单元410可以用于接收用于从转出端通过区块链流转至转入端的数字资产的隐私密文、和用于传递隐私密文的预设公钥；隐私处理单元420可以用于基于预设公钥，得到用于共享隐私密文的共享公钥，以使：隐私密文和共享公钥广播在区块链中时，区块链中的区块链节点基于共享公钥来共享隐私密文，并对所共享的隐私密文进行盲共识，以及，在隐私密文被达成共识后，由转入端、转出端和监管端基于预设私钥对隐私密文进行解密，得到数字资产的明文。

[0123] 在一些实施例中，数字资产是一个或者多个预定数值的Coin数据结构体的数据。

[0124] 在一些实施例中，在上述实施例的基础上，基于区块链的数字资产处理装置400还

可以包括:请求接收单元、指令发送单元和数据处理单元。其中,请求接收单元可以用于接收转入端所发送的接收来自转出端的受隐私保护的第一数值的数字资产的接收请求;或者,用于接收转出端所发送的转出受隐私保护的第一数值的数字资产的转出请求。

[0125] 指令发送单元可以用于响应于所接收的接收请求,向转出端发送是否同意转出受隐私保护的第一数值的数字资产的指令;或者,用于响应于所接收的转出请求,向转入端发送是否同意接收受隐私保护的第一数值的数字资产的指令。

[0126] 数据处理单元可以用于当接收到来自转出端的包括同意转出和用于证明受隐私保护的第一数值的数字资产的合法性的密码学证明的应答时,在转入端的资产数据库内,写入增加一个或者多个预定受隐私保护的数值的Coin数据结构体的数据的记录,以及写入减少受隐私保护的指定数值的Coin数据结构体的数据的记录;以及,在转出端的资产数据库内,写入增加销毁一个或者多个受隐私保护的预定数值的Coin数据结构体的数据的记录,以及写入增加受隐私保护的指定数值的Coin数据结构体的数据的记录;或者,用于当接收到来自转入端的包括同意接收和用于证明受隐私保护的第一数值的数字资产的合法性的密码学证明的应答时,在转入端的资产数据库内,写入增加一个或者多个预定受隐私保护的数值的Coin数据结构体的数据的记录,以及写入减少受隐私保护的指定数值的Coin数据结构体的数据的记录;以及,在转出端的资产数据库内,写入增加销毁一个或者多个受隐私保护的预定数值的Coin数据结构体的数据的记录,以及写入增加受隐私保护的指定数值的Coin数据结构体的数据的记录。

[0127] 在一些实施例中,在上述实施例的基础上,基于区块链的数字资产处理装置400还可以包括:数据验证单元和数据处理单元。其中,数据验证单元可以用于采用同态加密和/或零知识证明的密码学方法验证一个或者多个受隐私保护的预定数值的和与受隐私保护的指定数值与受隐私保护的第一数值的和是否相等;数据处理单元可以还用于当验证通过时,在转入端的资产数据库内,写入增加一个或者多个受隐私保护的预定数值的Coin数据结构体的数据的记录,以及写入减少受隐私保护的指定数值的Coin数据结构体的数据的记录;在转出端的资产数据库内,写入增加销毁一个或者多个受隐私保护的预定数值的Coin数据结构体的数据的记录,以及写入增加受隐私保护后的指定数值的Coin数据结构体的数据的记录。

[0128] 在一些实施例中,在上述实施例的基础上,基于区块链的数字资产处理装置400还可以包括:请求接收单元、指令发送单元和反馈发送单元。其中,请求接收单元可以还用于接收来自转入端所发送的接收转出端的受隐私保护的第一数量的数字资产的接收请求;指令发送单元可以还用于响应于所接收的接收请求,向转出端发送是否同意发送受隐私保护的第一数量的数字资产的指令;反馈发送单元可以用于当接收到来自转出端的拒绝向转入端发送第一数量的数字资产的应答时,向转入端发送拒绝的反馈。

[0129] 在一些实施例中,请求接收单元还可以用于接收来自转入端所发送的撤回接收请求;反馈发送单元还可以用于将所接收的撤回接收请求反馈给转出端。

[0130] 在一些实施例中,在上述实施例的基础上,基于区块链的数字资产处理装置400还可以包括:合约部署单元。合约部署单元可以用于预先在一个或者多个区块链中部署智能合约程序,智能合约程序用于定义数字资产在一个或者多个区块链中入场、转账、出场、余额查询中的至少一种操作。

[0131] 需要说明的是，本实施例中所示的功能单元或者功能模块的实现方式可以为硬件、软件、固件或者它们的组合。当以硬件方式实现时，其可以例如是电子电路、专用集成电路(ASIC)、适当的固件、插件、功能卡等等。当以软件方式实现时，本发明的元素是被用于执行所需任务的程序或者代码段。程序或者代码段可以存储在机器可读介质中，或者通过载波中携带的数据信号在传输介质或者通信链路上传送。“机器可读介质”可以包括能够存储或传输信息的任何介质。机器可读介质的例子包括电子电路、半导体存储器设备、ROM、闪存、可擦除ROM(EROM)、软盘、CD-ROM、光盘、硬盘、光纤介质、射频(RF)链路，等等。代码段可以经由诸如因特网、内联网等的计算机网络被下载。

[0132] 图5是本发明另一实施例的基于区块链的数字资产处理的结构示意图。

[0133] 如图5所示，基于区块链的数字资产处理装置500可以包括：数据获取单元510和数据处理单元520。其中，数据获取单元510可以用于当隐私密文和共享公钥广播在区块链中时，基于共享公钥来共享隐私密文，并对所共享的隐私密文进行盲共识，以及，在隐私密文被达成共识后，由转入端、转出端、监管端中至少一者基于预设私钥对隐私密文进行解密，得到数字资产的明文。需要说明的是，上述各实施例的装置可作为上述各实施例的用于各实施例的方法中的执行主体，可以实现各个方法中的相应流程，为了简洁，此方面内容不再赘述。

[0134] 在一些实施例中，数据处理单元还可以用于：利用同态加密方法和/或零知识证明方法对所共享的隐私密文的合法性进行验证，并对验证结果达成一致意见。

[0135] 以上所描述的装置实施例仅仅是示意性的，其中作为分离部件说明的单元可以是或者也可以不是物理上分开的，可以分布到多个网络单元上，可以根据实际的需要选择其中部分或者全部模块来实现实施例方案的目的。

[0136] 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各实施方式可借助软件加必需的通用硬件平台的方式来实现，当然也可以直接通过硬件来实现。基于这样的理解，上述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，该计算机软件产品可以存储在计算机可读存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行各个实施例或者实施例的某些部分所述的方法。

[0137] 最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

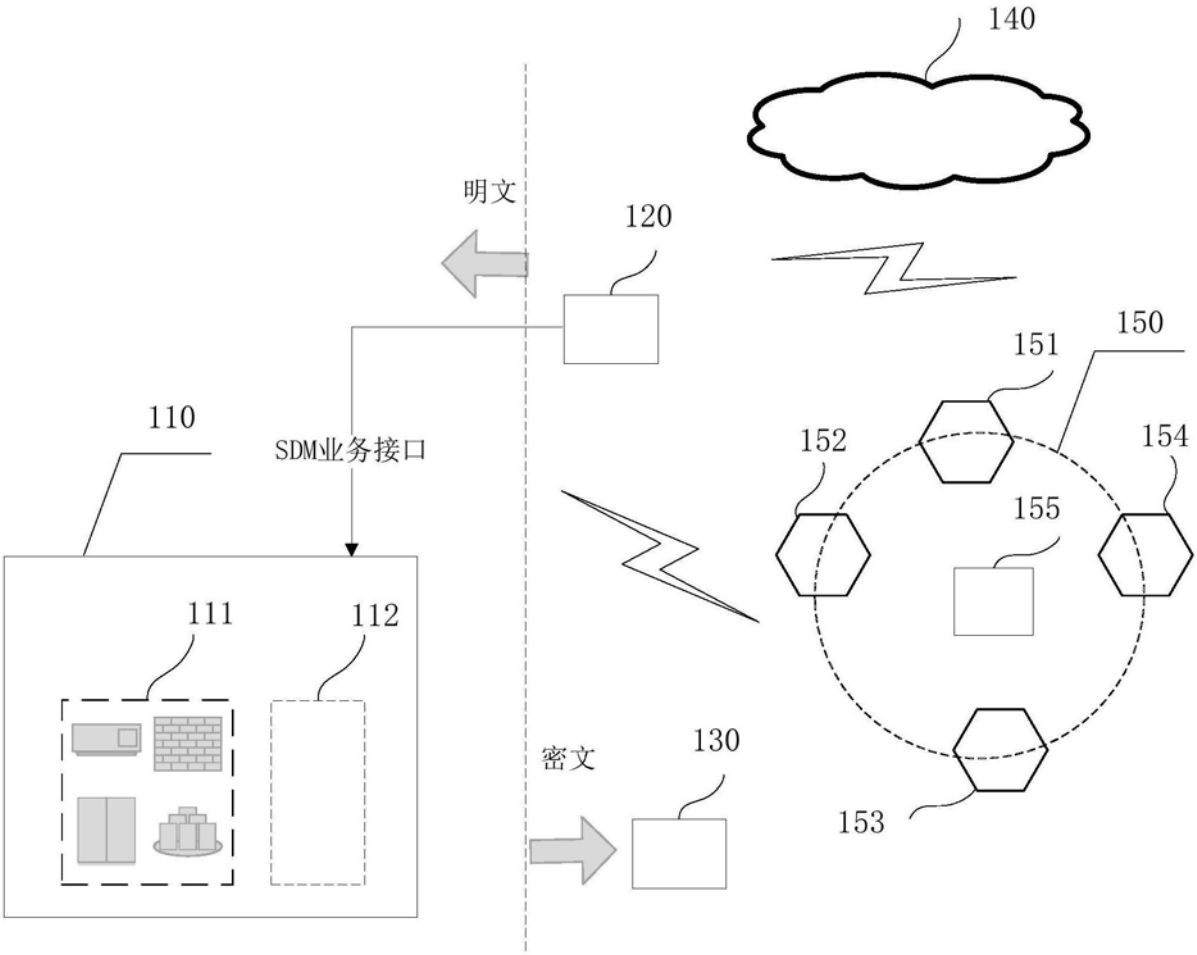

140
明文
120
150
151
110
SDM业务接口
152
154
155
111
112
密文
130
153

图1

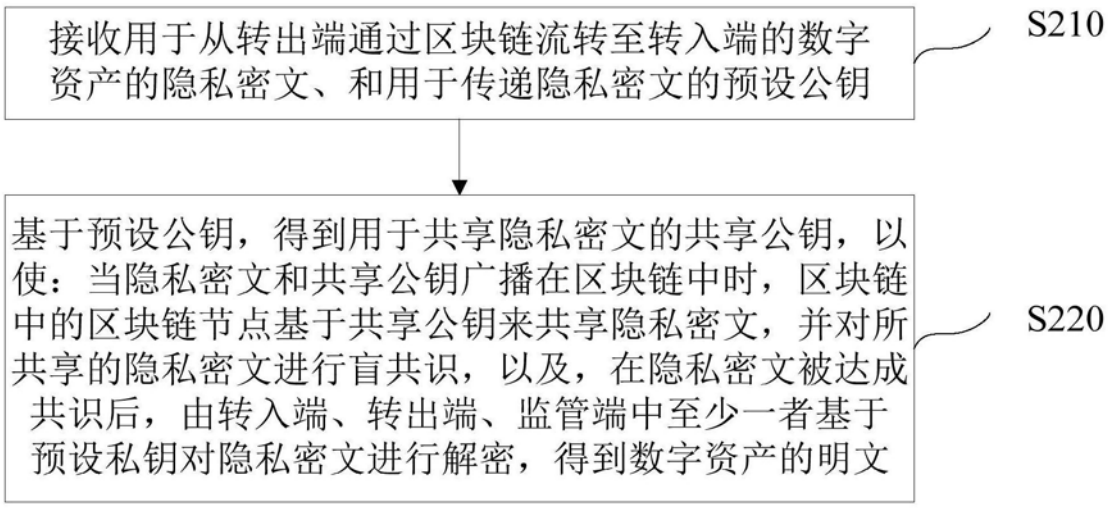

接收用于从转出端通过区块链流转至转入端的数字资产的隐私密文、和用于传递隐私密文的预设公钥
S210
基于预设公钥，得到用于共享隐私密文的共享公钥，以使：当隐私密文和共享公钥广播在区块链中时，区块链中的区块链节点基于共享公钥来共享隐私密文，并对所共享的隐私密文进行盲共识，以及，在隐私密文被达成共识后，由转入端、转出端、监管端中至少一者基于预设私钥对隐私密文进行解密，得到数字资产的明文
S220

图2

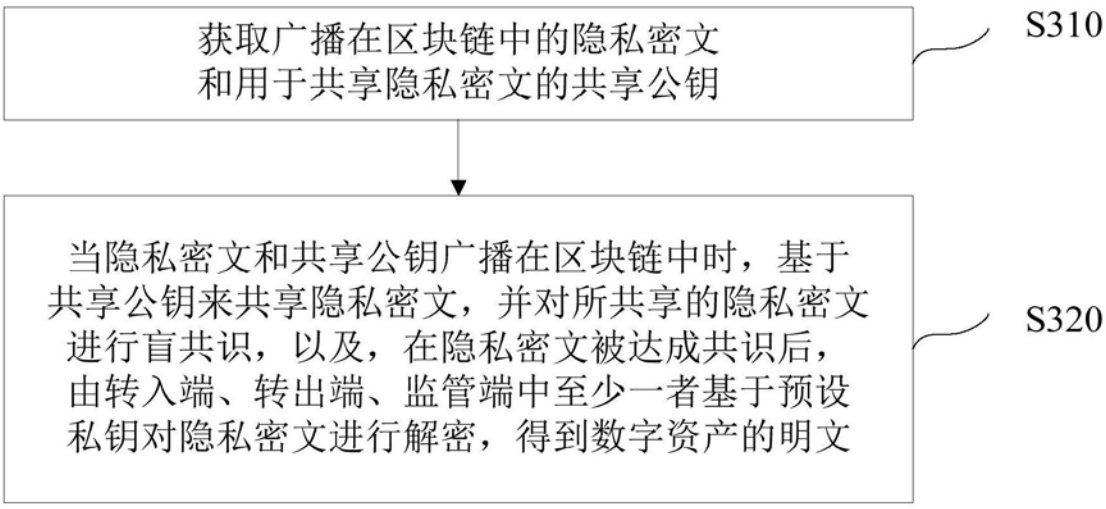

获取广播在区块链中的隐私密文
和用于共享隐私密文的共享公钥
S310
当隐私密文和共享公钥广播在区块链中时，基于
共享公钥来共享隐私密文，并对所共享的隐私密文
进行盲共识，以及，在隐私密文被达成共识后，
由转入端、转出端、监管端中至少一者基于预设
私钥对隐私密文进行解密，得到数字资产的明文
S320

图3

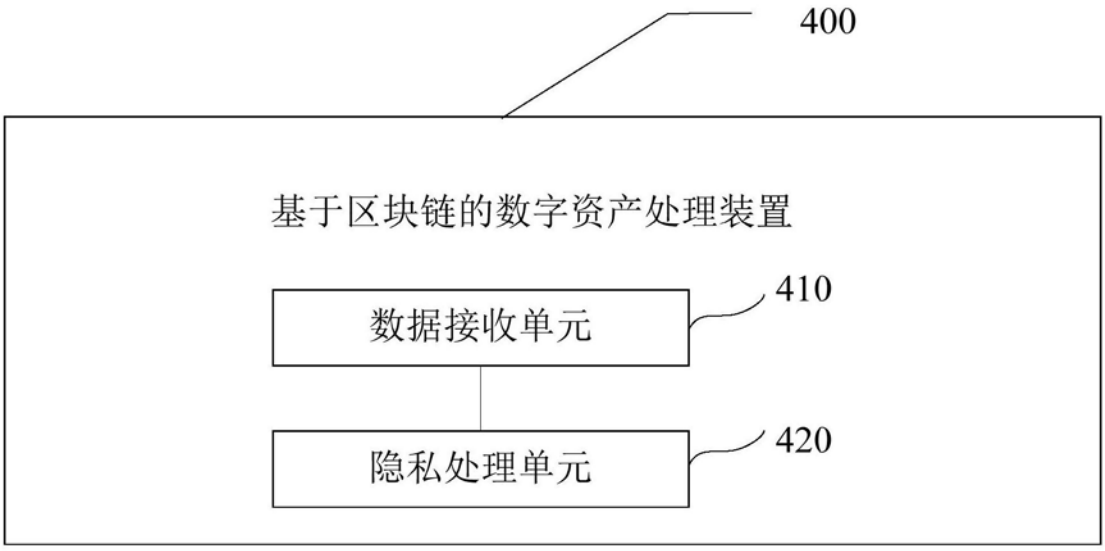

400
基于区块链的数字资产处理装置
数据接收单元
410
隐私处理单元
420

图4

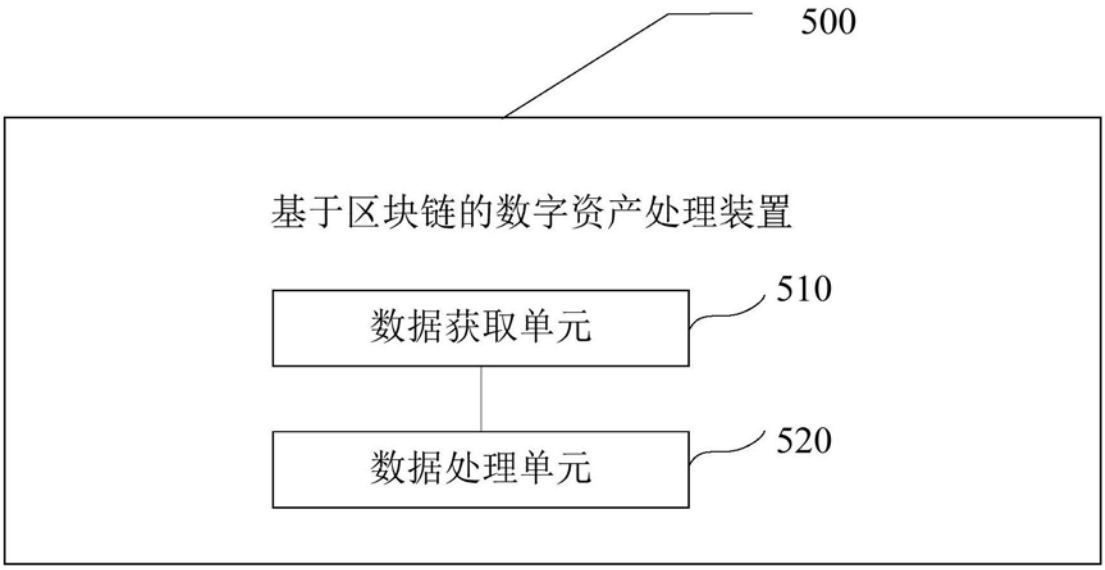


图5