



# (12)发明专利

(10)授权公告号 CN 105373955 B

(45)授权公告日 2020.07.10

(21)申请号 201510896821.2

(22)申请日 2015.12.08

(65)同一申请的已公布的文献号  
申请公布号 CN 105373955 A

(43)申请公布日 2016.03.02

(73)专利权人 布比(北京)网络技术有限公司  
地址 100085 北京市海淀区东北旺村南1号  
楼7层7590室

(72)发明人 蒋海 翟海滨 胡楠 赵正涌

(74)专利代理机构 北京献智知识产权代理事务  
所(特殊普通合伙) 11434  
代理人 杨献智

(51)Int.Cl.  
G06Q 30/06(2012.01)

(56)对比文件

CN 101751632 A,2010.06.23,说明书第18-20段.

CN 104881791 A,2015.09.02,说明书第7、20-24段,图1a,1b.

CN 1516048 A,2004.07.28,说明书第1页.

CN 102789607 A,2012.11.21,全文.

CN 102801710 A,2012.11.28,全文.

审查员 曹妹妹

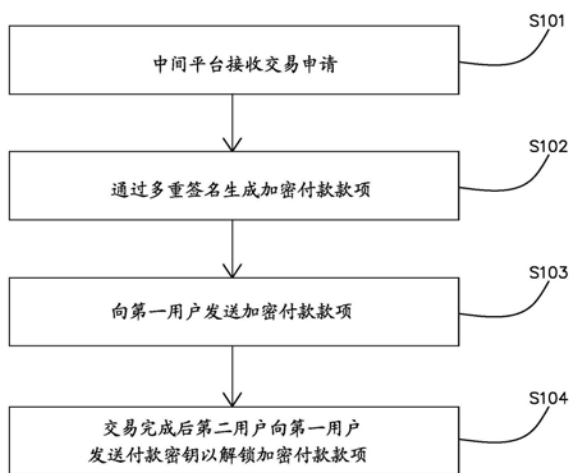
权利要求书2页 说明书6页 附图1页

## (54)发明名称

基于多重签名的数字资产处理方法及装置

## (57)摘要

本发明公开一种基于多重签名的数字资产处理方法及装置,该方法包括:中间平台接收交易申请;根据交易申请,通过多重签名生成加密付款款项;向第一用户终端发送加密付款款项,并通知第一用户终端和第二用户终端;在第一用户终端向第二用户终端发送商品或提供服务之后,第二用户终端向第一用户终端发送付款密钥,付款密钥用于解锁加密付款款项。通过买家、卖家和中间平台进行多重签名加密,中间平台既起到了居间担保作用,又不能单方转移数字资产,需要与卖家或者买家联合控制数字资产。因此,中间平台不再拥有数字资产完整的控制权,这能够在中间平台遭受攻击或中间平台恶意欺诈的情况下保证数字资产的安全性。



1. 一种基于多重签名的数字资产处理方法,其特征在于,包括:

中间平台接收第一用户终端与第二用户终端之间的交易申请,所述交易申请包括交易类型、第一用户标识和第二用户标识;

所述交易申请经所述中间平台确认后,所述中间平台、所述第一用户终端和所述第二用户终端通过多重签名生成加密付款款项;

所述中间平台向所述第一用户终端发送所述加密付款款项,并通知所述第一用户终端和所述第二用户终端;

在所述交易申请中设定的第一用户任务完成后,所述第二用户终端向所述第一用户终端发送付款密钥,所述付款密钥用于解锁所述加密付款款项;

其中,所述第一用户终端、所述第二用户终端、所述中间平台通过多方多重签名生成所述加密付款款项,设经过多重签名后的加密付款款项为Pay,设所述第二用户终端支付的款项为M,所述第二用户终端的公钥为B,所述第一用户终端的公钥为S,所述中间平台的公钥为P,签名算法为Sign,经过多重签名后的加密付款款项Pay为: $Pay = \text{Sign}_{B,S,P}(M)$ ;并且,签名公/私钥是变化的,每次交易通过公/私钥种子生成子公/私钥的方式动态变化;以及

当所述第一用户终端和所述第二用户终端发生纠纷时,所述中间平台根据判定结果,向所述第一用户终端或所述第二用户终端发送解密密钥,所述中间平台赞成哪一方,就创建一笔对方的付款解密签名Pay\_p,设所述中间平台的私钥为p,则: $Pay\_p = \text{Dec}_p(\text{Pay})$ ;如果所述中间平台判定为所述第二用户终端收回付款,则所述第二用户终端收到Pay\_p后,通过再一次付款解密即可获取款项M: $M = \text{Dec}_{b,p}(\text{Pay})$ ;如果所述中间平台判定所述第一用户终端收回付款,则所述第一用户终端收到Pay\_p后,通过再一次付款解密即可获取款项M: $M = \text{Dec}_{s,p}(\text{Pay})$ ;其中,所述第二用户终端的私钥为b,所述第一用户终端的私钥为s。

2. 如权利要求1所述的基于多重签名的数字资产处理方法,其特征在于,在所述中间平台接收所述交易申请后,还包括:

所述中间平台根据所述第一用户标识和所述第二用户标识分别估算第一用户交易风险和第二用户交易风险,若所述第一用户交易风险和所述第二用户交易风险中任一个大于等于设定阈值,则终止所述交易申请。

3. 如权利要求1所述的基于多重签名的数字资产处理方法,其特征在于,在通过多重签名生成所述加密付款款项后,还包括:

判断所述第一用户终端和所述第二用户终端是否处于同一中间平台;

若是,则所述同一中间平台向所述第一用户终端发送所述加密付款款项;

若否,则首先所述第二用户终端所在的中间平台先向所述第一用户终端所在的中间平台发送所述加密付款款项,然后所述第一用户终端所在的中间平台向所述第一用户终端发送所述加密付款款项。

4. 如权利要求1所述的基于多重签名的数字资产处理方法,其特征在于,所述中间平台向所述第一用户终端发送加密付款款项后,还包括:

当所述第一用户终端和所述第二用户终端发出并共同确认退款请求后,所述第一用户终端向所述第二用户终端发送退款密钥,所述第二用户终端通过所述退款密钥解锁所述加密付款款项,得到退款。

5. 如权利要求1所述的基于多重签名的数字资产处理方法,其特征在于,还包括:

根据所述交易申请,在第一用户数字资产或第二用户数字资产中转移出指定数量的数字资产到所述中间平台的指定账号中。

6. 如权利要求1所述的基于多重签名的数字资产处理方法,其特征在于,在所述中间平台接收所述交易申请前,还包括:

所述中间平台接收所述第一用户终端和所述第二用户终端的注册和登陆请求,并更新第一用户账户信息和第二用户账户信息。

7. 如权利要求1所述的基于多重签名的数字资产处理方法,其特征在于,所述中间平台接收所述交易申请包括:

接收所述第一用户终端的出售商品请求和接收所述第二用户终端的购买商品请求;  
当所述出售商品请求和所述购买商品请求匹配时,生成所述交易申请。

8. 如权利要求1所述的基于多重签名的数字资产处理方法,其特征在于,还包括:

当所述交易申请不能完成或不能撤销时,所述中间平台根据所述交易申请的交易过程来确定向所述第一用户终端或所述第二用户终端发送解密密钥。

9. 一种用于如权利要求1~8之一所述方法的基于多重签名的数字资产处理装置,其特征在于,包括:

交易接收模块,其设置在中间平台内用于接收第一用户终端与第二用户终端之间的交易申请,所述交易申请包括交易类型、第一用户标识和第二用户标识;

付款加密生成模块,其分别设置在所述中间平台、所述第一用户终端和所述第二用户终端中,用于根据所述交易申请通过多重签名生成加密付款款项;

付款模块,其设置在所述中间平台中,用于向所述第一用户终端发送所述加密付款款项,并通知所述第一用户终端和所述第二用户终端;

付款密钥模块,其分别设置在所述第一用户终端和所述第二用户终端中,在所述交易申请中设定的第一用户任务完成后,所述第二用户终端的付款密钥模块生成付款密钥并发送至所述第一用户终端,所述第一用户终端的付款密钥模块利用所述付款密钥解锁所述加密付款款项。

10. 如权利要求9所述的基于多重签名的数字资产处理装置,其特征在于,还包括:

风险处理模块,其设置在所述中间平台中,用于根据所述第一用户标识和所述第二用户标识分别估算第一用户交易风险和第二用户交易风险,若所述第一用户交易风险和所述第二用户交易风险中任一个大于等于设定阈值,则终止所述交易申请。

## 基于多重签名的数字资产处理方法及装置

### 技术领域

[0001] 本发明属于互联网金融领域,尤其涉及一种数字资产交易方法及系统。

### 背景技术

[0002] 随着全球信息技术的飞速发展,互联网数字资产越来越被人们关注和重视。现有互联网数字资产通常包括电子货币、虚拟货币、甚至网络账户内容等一切可用于交易的数字形式资产。

[0003] 现有互联网数字资产交易过程中,买家、卖家完全依赖于中间平台,包括价款对付、资产交割、信息更新等。在上述交易环节,中间平台对数字资产拥有完整的控制权,如支付宝等平台,虽然买方可以选择在收到商品或者服务后再确认付款,但是在交易过程中,如果中间平台被攻击,攻击者仍将能够获取交易中的全部数字资产。

[0004] 此外,对于一些存在恶意欺诈的中间平台,该中间平台运营者能够“窃走”交易中的全部数字资产。

[0005] 因此,提供一种更加安全可靠的数字资产交易方法及系统成为业内急需解决的问题。

### 发明内容

[0006] 本发明的目的在于提供一种基于多重签名的数字资产处理方法及装置,以限制中间平台对数字资产的控制权,从而避免在中间平台遭受攻击或恶意欺诈时导致用户数字资产损失。

[0007] 根据本发明的一个方面,提供一种基于多重签名的数字资产处理方法,包括:中间平台接收第一用户终端与第二用户终端之间的交易申请,交易申请包括交易类型、第一用户标识和第二用户标识;交易申请经中间平台确认后,中间平台、第一用户终端和第二用户终端通过多重签名生成加密付款款项;中间平台向第一用户终端发送加密付款款项,并通知第一用户终端和第二用户终端;以及在交易申请中设定的第一用户任务完成后,第二用户终端向第一用户终端发送付款密钥,付款密钥用于解锁加密付款款项。

[0008] 其中,交易类型包括出售商品、出售服务、购买商品、购买服务等类型中的任一个或任意组合。第一用户标识和第二用户标识可分别包括账户信息、信誉度、交易历史、交易额等信息中的任一个或任意组合。

[0009] 优选地,在中间平台接收交易申请后,还包括:中间平台根据第一用户标识和第二用户标识分别估算第一用户交易风险和第二用户交易风险,若第一用户交易风险和第二用户交易风险中任一个大于等于设定阈值,则终止交易申请。

[0010] 可选择地,在通过多重签名生成加密付款款项后,还包括:判断第一用户终端和第二用户终端是否处于同一中间平台;若是,则同一中间平台向第一用户终端发送加密付款款项;若否,则首先第二用户终端所在的中间平台先向第一用户终端所在的中间平台发送加密付款款项,然后第一用户终端所在的中间平台向第一用户终端发送加密付款款项。

[0011] 可选择地,中间平台向第一用户终端发送加密付款款项后,还包括:当第一用户终端和第二用户终端发出并共同确认退款请求后,第一用户终端向第二用户终端发送退款密钥,第二用户终端通过退款密钥解锁加密付款款项,得到退款。

[0012] 可选择地,该方法还包括:根据交易申请,在第一用户数字资产或第二用户数字资产中转移出指定数量的数字资产到中间平台的指定账号中。

[0013] 可选择地,在中间平台接收交易申请前,还包括:中间平台接收第一用户终端和第二用户终端的注册和登陆请求,并更新第一用户账户信息和第二用户账户信息。

[0014] 可选择地,中间平台接收交易申请包括:接收第一用户终端的出售商品请求和接收第二用户终端的购买商品请求;当出售商品请求和购买商品请求匹配时,生成交易申请。

[0015] 可选择地,该方法还包括:当交易申请不能完成或不能撤销时,中间平台根据交易申请的交易过程来确定向第一用户终端或第二用户终端发送解密密钥。

[0016] 根据本发明的第二方面,提供一种基于多重签名的数字资产处理装置,包括:交易接收模块,其设置在中间平台内用于接收第一用户终端与第二用户终端之间的交易申请,交易申请包括交易类型、第一用户标识和第二用户标识;付款加密生成模块,其分别设置在中间平台、第一用户终端和第二用户终端中,用于根据交易申请通过多重签名生成加密付款款项;付款模块,其设置在中间平台中,用于向第一用户终端发送加密付款款项,并通知第一用户终端和第二用户终端;付款密钥模块,其分别设置在第一用户终端和第二用户终端中,在交易申请中设定的第一用户任务完成后,第二用户终端的付款密钥模块生成付款密钥并发送至第一用户终端,第一用户终端的付款密钥模块利用付款密钥解锁加密付款款项。

[0017] 优选地,该装置还包括:风险处理模块,其设置在中间平台中,用于根据第一用户标识和第二用户标识分别估算第一用户交易风险和第二用户交易风险,若第一用户交易风险和第二用户交易风险中任一个大于等于设定阈值,则终止交易申请。

[0018] 可选择地,该装置还包括:退款模块,用于在第一用户终端和第二用户终端发出并共同确认退款请求之后,根据第一用户终端向第二用户终端发送的退款密钥,解锁加密付款款项,得到退款。

[0019] 可选择地,该装置还包括:交易费用模块,用于根据交易申请,在第一用户终端或者第二用户终端数字资产中转移出指定数量的数字资产到中间平台的指定账号中。

[0020] 可选择地,该装置还包括:交易生成模块,用于在接收第一用户终端的出售商品请求和接收第二用户终端的购买商品请求之后,匹配售商品请求和购买商品请求,并生成交易申请。

[0021] 可选择地,该装置还包括:纠纷处理模块,用于在第一用户终端和第二用户终端发生纠纷时,根据判定结果,向第一用户终端或第二用户终端发送解密密钥。

[0022] 本发明的有益效果是:本发明提供的基于多重签名的数字资产处理方法及装置中,通过买家、卖家和中间平台进行多重签名加密,中间平台即起到了居间担保作用,又不能单方转移数字资产,需要与卖家或者买家联合控制数字资产,因此,中间平台不再拥有数字资产完整的控制权,能够保证中间平台在被攻击或者欺诈的情况下数字资产的安全性。

## 附图说明

[0023] 图1为实施例1基于多重签名的数字资产处理方法的流程示意图。

[0024] 图2为实施例2基于多重签名的数字资产处理装置的构造示意图。

## 具体实施方式

[0025] 下面详细描述本发明的实施例,所述实施例的示例在附图中示出,其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的,旨在用于解释本发明,而不能理解为对本发明的限制。

[0026] 本发明提供了一种基于多重签名的数字资产处理方法及装置。

[0027] 实施例1

[0028] 如图1所示,为本实施例提供的基于多重签名的数字资产处理方法的流程示意图,具体包括以下步骤:

[0029] 在步骤S101,中间平台接收交易申请,交易申请包括交易类型、第一用户标识和第二用户标识。其中,交易申请中包括买方和卖方账户信息、交易金额、以及所购买或者出售的商品/服务等交易信息。

[0030] 在本步骤之前,还可以包括:在中间平台上,接收第一用户(卖家)和第二用户(买家)的注册和登陆请求,并更新其对应的账户信息。

[0031] 具体的,用户在选择的交易中间平台上进行注册以获得合法交易身份,如用户账户id。需要说明的是,买家和卖家并不一定在同一中间平台注册,如果在不同中间平台注册,则要求不同中间平台之间相互信任且均支持基于本实施例提供的基于多重签名的数字资产处理的技术方案。

[0032] 用户登录交易中间平台之后,通过验证,并可以通过转账等方式进行充值,充值包括多种类型(可以为数字货币,也可以为虚拟货币等),中间平台相应地更新用户对应的账户信息。

[0033] 上述步骤中,交易申请根据买家或者卖家的交易请求生成,具体的,中间平台接收第一用户终端的出售商品请求和接收第二用户终端的购买商品请求,当出售商品请求和购买商品请求匹配时,生成交易申请。

[0034] 此外,为提高交易的安全性,在接收交易申请之后,还可以包括:根据交易申请,计算交易风险,若交易风险大于设定值,则终止交易。

[0035] 其中,若卖家需要出售商品或服务,则中间平台根据交易者信誉度、交易历史、交易额度等进行交易风险评估,以决定是否接受交易,如果未通过评估,则交易结束;如果通过评估,则将用户需要出售的商品或服务与用户信息进行关联,形成交易包,并将当前交易包添加到出售商品包列表,并更新出售商品包的索引列表。

[0036] 若用户需要购买商品或服务,购买用户通过中间平台获取出售商品包索引列表,并查找所需要的商品,在找到期望购买的商品之后,向中间平台发送包含该商品包索引信息的交易请求。中间平台根据交易者信誉度、交易历史、交易额度等进行交易风险评估,以决定是否接受交易,如果未通过评估,则交易结束;如果通过评估,则转到步骤S102。

[0037] 在步骤S102,根据交易申请,通过多重签名生成加密付款款项;卖家(第一用户终端)、买家(第二用户终端)、中间平台通过多方多重签名生成买家付款,令经过多重签名后

的加密付款款项为Pay。设买家支付的款项为M,买家的公钥为B,卖家的公钥为S,中间平台的公钥为P,签名算法为Sign,经过多重签名后的加密付款款项Pay为:Pay=Sign<sub>B,S,P</sub>(M)。

[0038] 其中,签名公私钥并非确定不变,每次交易可以通过公(私)钥种子生成子公(私)钥的方式(如分层确定性签名)动态变化。

[0039] 在步骤S103,向第一用户终端发送加密付款款项,并通知第一用户终端和第二用户终端;

[0040] 本步骤中,可以首先判断第一用户终端和第二用户终端是否处于同一平台;如果是,则由该中间平台直接将加密付款款项Pay划拨给第一用户终端(卖家),并通知双方;如果第一用户终端和第二用户终端处于不同平台,则首先第二用户终端所在的平台先向第一用户终端所在的平台发送加密付款款项,然后第一用户终端所在的平台向该第一用户终端发送加密付款款项。

[0041] 在步骤S104,在第一用户终端向第二用户终端发送商品或提供服务之后,第二用户终端向第一用户终端发送付款密钥,付款密钥用于解锁加密付款款项。

[0042] 第一用户终端(卖家)收到加密付款款项Pay后,即向买家发送商品或服务;第二用户终端(买家)收到所需商品或服务后,协助卖家利用付款密钥解密获取款项,具体步骤如下:设付款解密算法为Dec,买家私钥为b;则首先生成Pay<sub>b</sub>=Dec<sub>b</sub>(Pay);设卖家的私钥为s,卖家收到Pay<sub>b</sub>后,通过再一次付款解密即可获取款项M:M=Dec<sub>b,s</sub>(Pay)。

[0043] 此外,在交易结束后,中间平台可以收取一笔付款作为交易费,其中交易费可以与申请交易额度成正比,具体的,该方法还包括以下步骤:根据交易申请,在第一用户或者第二用户数字资产中转移出指定数量的数字资产到中间平台的指定账号中。

[0044] 当买方对商品或者服务不满意或者其它情形需要退款时,该方法中,在向第一用户终端发送加密付款款项之后,还可以包括:当第一用户终端和第二用户终端发出并共同确认退款请求之后,第一用户终端向第二用户终端发送退款密钥,该第二用户终端通过退款密钥解锁加密付款款项,得到退款。

[0045] 具体的,卖家创建一个付款解密签名Pay<sub>s</sub>给买家,买家收到Pay<sub>s</sub>后,对付款进行再次解密,即可获取到退款款项M:M=Dec<sub>b,s</sub>(Pay)。

[0046] 上述交易的成功或者失败退款等信息均可以被交易中间平台收集,并作为信誉度纳入中间平台交易风险评估模型。

[0047] 为了应对交易过程中出现的交易纠纷,本实施例提供的基于多重签名的数字资产处理方法,还可以包括:当第一用户和第二用户发生纠纷时,中间平台根据判定结果,向第一用户终端或第二用户终端发送解密密钥。

[0048] 具体的实现方式如下:如果交易双方出现纠纷,买卖双方需要联系仲裁者—中间平台,并提供相关证据,由中间平台来决定相信哪一方。中间平台赞成哪一方,就创建一笔对方的付款解密签名Pay<sub>p</sub>。设中间平台的私钥为p,则:Pay<sub>p</sub>=Dec<sub>p</sub>(Pay);如果中间平台判定为买家收回付款,则收到Pay<sub>p</sub>后,通过再一次付款解密即可获取款项M:M=Dec<sub>b,p</sub>(Pay);如果为中间平台判定卖家收回付款,则收到Pay<sub>p</sub>后,通过再一次付款解密即可获取款项M:M=Dec<sub>s,p</sub>(Pay)。

[0049] 本实施例提供的基于多重签名的数字资产处理方法中,通过买家、卖家和中间平台进行多重签名加密,中间平台既起到了居间担保作用,又不能单方转移数字资产,需要与

卖家或者买家联合控制数字资产,因此,中间平台不再拥有数字资产完整的控制权,能够在中间平台被攻击或者欺诈的情况下保证数字资产的安全性。

[0050] 在具体应用过程中,用户首先选择值得信任的中间平台,并完成注册、账户创建、信息更新、充值等操作。进而,用户可以提交交易申请:(1) 如果为出售交易,则用户为卖家,将需要出售的商品或服务信息提交给中间平台,中间平台将根据用户历史交易行为、信誉度等信息评估是否接受该交易,如果通过评估则将该出售信息加入出售商品列表,否则交易结束。(2) 如果为购买交易,则用户为买家,需要支付付款,该付款由买卖双方以及中间平台生成多重签名并加密,进而将经过加密签名的付款发送给卖家。卖家收到该款项后,向买家发送商品或服务;如果买家收到商品或服务后,如果满足要求则对款项进行首次解密签名并发送给卖家,交易顺利完成;如果买卖双方达成一致退款,则卖家对款项进行首次解密签名并发送给买家,交易结束;如果买卖双方出现交易纠纷,则需提供相关证据提交中间平台,由中间平台评估相信哪一方并协助其取得付款款项。

[0051] 实施例2

[0052] 本实施例提供了一种基于多重签名的数字资产处理装置,如图2所示,其包括中间平台100、第一用户终端300及第二用户终端500,其中,中间平台100、第一用户终端300及第二用户终端500均示意性显示一个,而实际上可以包括两个或两个以上的中间平台、若干第一用户终端及若干第二用户终端。

[0053] 交易接收模块201设置于中间平台100中,用于接收第一用户终端300与第二用户终端500之间的交易申请,交易申请包括交易类型、第一用户标识和第二用户标识。

[0054] 付款加密生成模块202分别设置在中间平台100、第一用户终端300和第二用户终端500中,用于根据交易申请通过多重签名生成加密付款款项。

[0055] 付款模块203设置在中间平台100中,用于向第一用户终端300发送加密付款款项,并通知第一用户终端300和第二用户终端500。

[0056] 付款密钥模块204分别设置在第一用户终端300和第二用户终端500中,在交易申请中设定的第一用户任务完成后,第二用户终端500通过付款密钥模块204生成付款密钥并发送至第一用户终端300,第一用户终端300的付款密钥模块204利用付款密钥解锁加密付款款项。

[0057] 此外,为提高交易的安全性,基于多重签名的数字资产处理装置中还包括:风险处理模块205,其设置在中间平台100中用于根据交易申请计算交易风险,若交易风险大于设定值,则终止交易。

[0058] 作为一种可替代实施方式,为应对买方对商品或者服务不满意或者其它情形需要退款,基于多重签名的数字资产处理装置中还包括:退款模块,其设于第一用户终端和第二用户终端中,用于在第一用户终端和第二用户终端发出并共同确认退款请求之后,根据第一用户终端向第二用户终端发送的退款密钥,解锁加密付款款项,得到退款。

[0059] 作为另一种可替代实施方式,在交易结束后,中间平台可以收取一笔付款作为交易费,其中交易费可以与申请交易额度成正比,具体的,基于多重签名的数字资产处理装置中还包括:交易费用模块,其设于第一用户终端和第二用户终端中,用于根据交易申请,在第一用户终端或者第二用户终端数字资产中转移出指定数量的数字资产到中间平台的指定账号中。



[0060] 作为又一种可替代实施方式,交易申请可以根据买家或者卖家的交易请求生成,因此该装置中还包括:交易生成模块,其设置在中间平台中用于在接收第一用户终端的出售商品请求和接收第二用户终端的购买商品请求之后,匹配售商品请求和购买商品请求,并生成交易申请。

[0061] 作为再一种可替代实施方式,为了应对交易过程中出现的交易纠纷,基于多重签名的数字资产处理装置还包括:纠纷处理模块,其设置在中间平台中用于在第一用户终端和第二用户终端发生纠纷时,根据判定结果,向第一用户终端或第二用户终端发送解密密钥。

[0062] 本发明提供的基于多重签名的数字资产处理装置中,通过买家、卖家和中间平台进行多重签名加密,中间平台既起到了居间担保作用,又不能单方转移数字资产,需要与卖家或者买家联合控制数字资产,因此,中间平台不再拥有数字资产完整的控制权,能够在中间平台被攻击或者欺诈的情况下保证数字资产的安全性。

[0063] 最后应说明的是:以上各实施例仅用以说明本发明的技术方案,而非对其限制;尽管参照前述各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,或者对其中部分或者全部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范围。

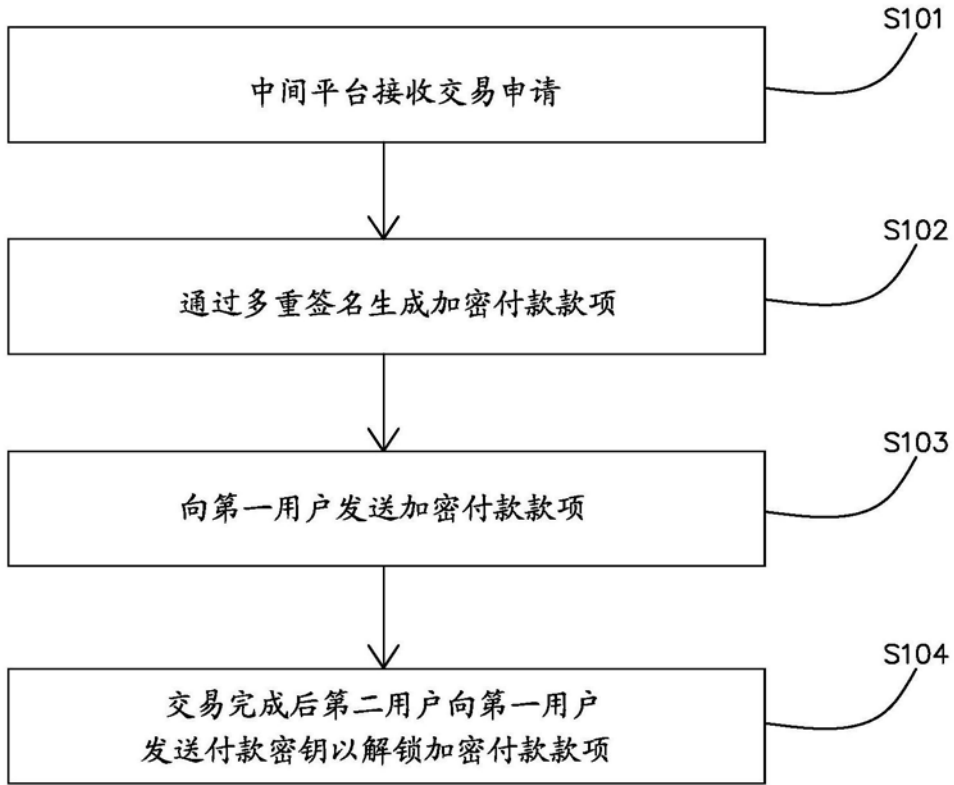


图1

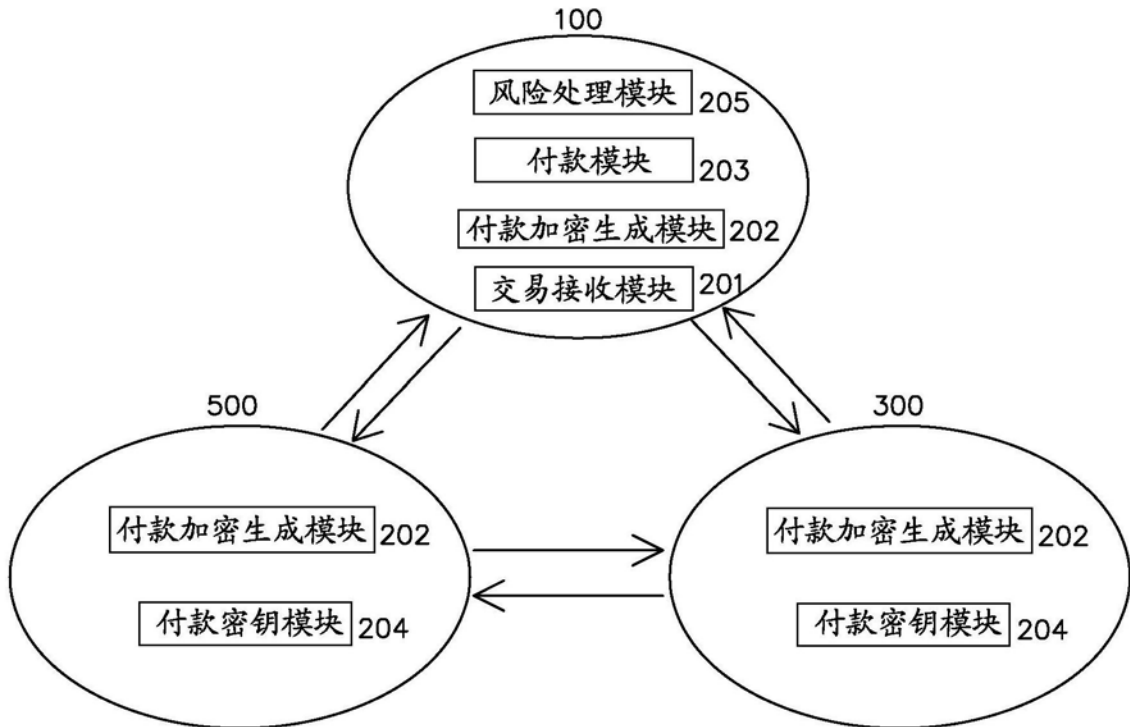


图2