(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 118138254 A
(43)申请公布日 2024.06.04

(21)申请号 202410552122.5

(22)申请日 2024.05.07

(71)申请人 数盾信息科技股份有限公司
地址 100000 北京市丰台区汽车博物馆东路8号院7号楼9层901

(72)发明人 朱云 李元骅 可为

(74)专利代理机构 北京知汇宏图知识产权代理有限公司 11520
专利代理师 李媛

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/40(2022.01)
H04L 9/08(2006.01)
H04L 9/00(2022.01)
G06Q 20/40(2012.01)

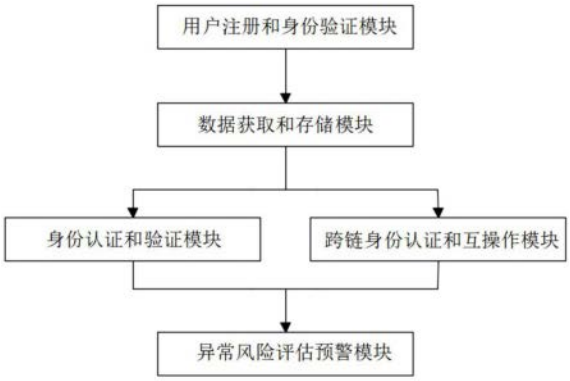
权利要求书2页 说明书9页 附图1页

(54)发明名称

一种基于区块链技术的数字货币身份认证系统

(57)摘要

本发明公开了一种基于区块链技术的数字货币身份认证系统,涉及区块链技术领域,该系统包括若干模块;其技术要点为:在本区块链上进行交易时,通过获取评估数据集中的交易频率差、交易时间差和交易对手方与黑名单地址的关联度数据,搭建对应的模型计算后,生成准确、有效的异常程度预估值Ead1,依据后续的对比结果,可以高效的检测到异常交易行为;在跨区块链进行交易时,通过同步获取用户交易过程中的评估数据集和网络波动系数Q,并基于预处理的数据集计算交易的异常程度预估值Ead2,依据后续的对比结果,可以得出在不同场景下交易时的异常程度,这有助于评估跨链交易的安全性和可信度,识别可能存在的风险和异常情况。



CN 118138254 A

1.一种基于区块链技术的数字货币身份认证系统,其特征在于,包括:

用户注册和身份验证模块,在注册时,获取用户的身份信息和证明材料数据,并进行初步身份验证;

数据获取和存储模块,在初步验证完用户身份后,提取用户的身份信息和证明材料数据,创建用户的数字身份,并将其存储至区块链上;

身份认证和验证模块,在用户进行交易前,采用公钥加密和数字签名技术,对用户提供的身份信息进行加密和签名,在本区块链上进行交易时,提供数字签名来验证用户身份和认证结果,并同步获取用户交易过程中的评估数据集;

跨链身份认证和互操作模块,在用户于其他区块链上进行交易时,通过跨链身份认证和互操作机制,将其身份信息和证明材料数据传递至目标区块链上,并同步获取用户交易过程中的评估数据集和网络波动系数Q;

异常风险评估预警模块,在本区块链上进行交易时,依据经过预处理后的评估数据集,搭建异常风险评估计算模型,生成本次交易的异常程度预估值Ead1,并将异常程度预估值Ead1与预设的第一评估阈值Emo_{δ}进行对比,若是异常程度预估值Ead1超过第一评估阈值Emo_{δ},则发出一级预警信号;反之,则不做响应动作;

在跨区块链进行交易时,依据经过预处理后的评估数据集和网络波动系数Q,二次搭建异常风险评估计算模型,生成本次交易的异常程度预估值Ead2,并将异常程度预估值Ead2与预设的第二评估阈值Emo_{θ}进行对比,若是异常程度预估值Ead2超过第二评估阈值Emo_{θ},则发出二级预警信号;反之,则不做响应动作。

2.根据权利要求1所述的一种基于区块链技术的数字货币身份认证系统,其特征在于:用户的身份信息包括用户本人的姓名、身份证号码以及联系电话,用户的身份信息是用户在注册时自行填写并提供的,证明材料数据包括护照、驾驶证和本人照片。

3.根据权利要求2所述的一种基于区块链技术的数字货币身份认证系统,其特征在于:进行初步身份验证的方式为:与预先准备的数据库进行比对。

4.根据权利要求3所述的一种基于区块链技术的数字货币身份认证系统,其特征在于:评估数据集包括交易频率差、交易时间差以及交易对手方与黑名单地址的关联度,其中,交易频率差表示本次交易频率与历史交易频率之间的差值,历史交易频率表示最近一个月的交易频率;交易时间差表示本次交易时间与正常工作时间范围的差值。

5.根据权利要求4所述的一种基于区块链技术的数字货币身份认证系统,其特征在于:交易对手方与黑名单地址的关联度表示对手方的网络IP地址与系统预设黑名单地址的关联指标I;

使用以下步骤获得具体的关联指标I:

S201、创建系统预设的黑名单地址列表,该列表包含已知被标记为不信任的地址;

S202、在交易过程中,获取交易对手方的IP地址,获取的方式为通过网络日志、访问日志以及审计记录中的任一种;

S203、将交易对手方的IP地址与预设的黑名单地址列表进行对比,直接对比交易对手方的IP地址与黑名单地址列表中每个地址,若存在匹配,将其作为关联数据;

S204、在找到匹配的IP地址后,使用以下公式计算关联指标I:

$$I = Ps/Zs;$$

式中,Ps表示匹配IP地址数量,Zs表示总IP地址数量。

6.根据权利要求5所述的一种基于区块链技术的数字货币身份认证系统,其特征在于:网络波动系数Q的获取过程如下:

在预设时间周期T内,采集每个时刻下交易时的网络传输速率Sv_t,计算T时间周期内不同时刻下的网络传输速率的平均值,根据平均值和网络传输速率Sv_t,计算网络波动系数Q,所依据的公式如下:

$$\begin{cases} Q = \sqrt{\left(\sum_{t=1}^{n}(Sv_t - \overline{Sv})^2\right)/(n-1)} \\ \overline{Sv} = \left(\sum_{t=1}^{n} Sv_t\right)/n \end{cases};$$

式中,$\overline{Sv}$表示T时间周期内不同时刻下的网络传输速率的平均值,t=1、2、…、n,n为正整数,且n=T。

7.根据权利要求6所述的一种基于区块链技术的数字货币身份认证系统,其特征在于:对评估数据集进行预处理的过程为:对各个数据进行无量纲化处理。

8.根据权利要求7所述的一种基于区块链技术的数字货币身份认证系统,其特征在于:在本区块链上进行交易时,计算本次交易的异常程度预估值Ead1,所依据的公式如下:

$$Ead1 = F1 * Xj + F2 * Xs + F3 * I;$$

式中,Xj、Xs分别为交易频率差和交易时间差,F1、F2、F3分别为交易频率差、交易时间差以及关联指标I的预设比例系数,且F3>F1>F2>0;

在跨区块链进行交易时,计算本次交易的异常程度预估值Ead2,所依据的公式如下:

$$Ead2 = Ead1 + G_1 * Q;$$

式中,G_1为常数修正系数。

9.一种计算机可读存储介质,其上存储有计算机程序,所述计算机程序被执行时,用于实现如权利要求1~8中任一所述的系统。

10.一种电子设备,包括处理器和存储器,用于执行如权利要求1~8中任一所述的系统。

一种基于区块链技术的数字货币身份认证系统

技术领域

[0001] 本发明涉及区块链技术领域,具体为一种基于区块链技术的数字货币身份认证系统。

背景技术

[0002] 区块链技术是一种去中心化的分布式数据库技术,它的核心概念是由多个节点共同维护一个不可篡改的、公开透明的数据链,它通过使用加密算法确保数据的安全性,并通过共识机制来解决节点之间的信任问题;将区块链技术应用于数字货币身份认证可以提供更安全、透明和去中心化的身份验证机制,表现的场景为用户注册和身份验证:用户在数字货币平台上注册账户时,需要提供基本的身份信息,这些信息会被加密并转化为一个唯一的身份标识,同时生成一个对应的公钥和私钥对;身份验证交易:用户进行身份验证时,会使用私钥对待验证的信息进行加密签名,并将签名后的数据和公钥发送给数字货币平台。平台会利用用户的公钥对签名进行验证,确保信息是由对应私钥的持有者创建。这种方式不需要用户将原始身份信息发送给平台,保护了用户的隐私。

[0003] 现有申请公布号为:CN117155582A,名称为一种基于区块链技术的数字货币身份认证系统的文件中指出的技术方案包括:密钥生成模块,生成密钥对同时被配置为生成第一溯源标识和/或生成第二溯源标识;证书生成模块生成证书;地址控制器模块接收证书,将数字货币单元化生成单元货币校验码写入证书中;溯源认证模块被配置为,获取来自参与交互的节点的匿名认证信息,将匿名认证信息至密钥生成模块和证书生成模块,由密钥生成模块生成对应公钥的第二私钥,由证书生成模块生成匿名证;异常校验模块被配置为检测异常监控交易,上述方案只是实现了对链上的交易的溯源性,并且通过对数字货币交易时产生溯源限制,避免了二次交易的发生,对任何不符合证书认证的交易均会发生拦截,保障了数字货币交易的安全性,但并未对交易场景下存在的异常情况进行有效检测。

[0004] 结合上述文件和现有技术,在网上进行的数字货币交易时,通常会存在不同场景的交易情况,结合区块链技术使用的认证系统时,在对用户的身份信息进行验证过后,通常会在区块链上进行交易处理,期间可以监测交易时的评估数据变化,以判断交易过程是否正常,但若是需要进行跨区块链交易时,由于在进行跨区块链交易时可能会存在外网接入的情况,导致交易的安全性降低,依旧监测原本评估数据的变化则无法准确的获知交易的异常状态,从而使得跨链交易的可信度大大降低。

发明内容

[0005] (一)解决的技术问题

针对现有技术的不足,本发明提供了一种基于区块链技术的数字货币身份认证系统,在本区块链上进行交易时,通过获取评估数据集中的交易频率差、交易时间差和交易对手方与黑名单地址的关联度数据,搭建对应的模型计算后,生成准确、有效的异常程度预估值Ead1,依据后续的对比结果,可以高效的检测到异常交易行为;在跨区块链进行交易时,

通过同步获取用户交易过程中的评估数据集和网络波动系数Q,并基于预处理的数据集计算交易的异常程度预估值Ead2,依据后续的对比结果,可以得出在不同场景下交易时的异常程度,这有助于评估跨链交易的安全性和可信度,识别可能存在的风险和异常情况,解决了背景技术中提出的问题。

[0006] (二)技术方案

为实现以上目的,本发明通过以下技术方案予以实现:

一种基于区块链技术的数字货币身份认证系统,包括:

用户注册和身份验证模块,在注册时,获取用户的身份信息和证明材料数据,并进行初步身份验证;

数据获取和存储模块,在初步验证完用户身份后,提取用户的身份信息和证明材料数据,创建用户的数字身份,并将其存储至区块链上;

身份认证和验证模块,在用户进行交易前,采用公钥加密和数字签名技术,对用户提供的身份信息进行加密和签名,在本区块链上进行交易时,提供数字签名来验证用户身份和认证结果,并同步获取用户交易过程中的评估数据集;

跨链身份认证和互操作模块,在用户于其他区块链上进行交易时,通过跨链身份认证和互操作机制,将其身份信息和证明材料数据传递至目标区块链上,并同步获取用户交易过程中的评估数据集和网络波动系数Q;

异常风险评估预警模块,在本区块链上进行交易时,依据经过预处理后的评估数据集,搭建异常风险评估计算模型,生成本次交易的异常程度预估值Ead1,并将异常程度预估值Ead1与预设的第一评估阈值Emo_{δ}进行对比,若是异常程度预估值Ead1超过第一评估阈值Emo_{δ},则发出一级预警信号;反之,则不做响应动作;

在跨区块链进行交易时,依据经过预处理后的评估数据集和网络波动系数Q,二次搭建异常风险评估计算模型,生成本次交易的异常程度预估值Ead2,并将异常程度预估值Ead2与预设的第二评估阈值Emo_{θ}进行对比,若是异常程度预估值Ead2超过第二评估阈值Emo_{θ},则发出二级预警信号;反之,则不做响应动作。

[0007] 进一步的,用户的身份信息包括用户本人的姓名、身份证号码以及联系电话,用户的身份信息是用户在注册时自行填写并提供的,证明材料数据包括护照、驾驶证和本人照片。

[0008] 进一步的,进行初步身份验证的方式为:与法定机构数据库进行比对。

[0009] 进一步的,评估数据集包括交易频率差、交易时间差以及交易对手方与黑名单地址的关联度,其中,交易频率差表示本次交易频率与历史交易频率之间的差值,历史交易频率表示最近一个月的交易频率;交易时间差表示本次交易时间与正常工作时间范围的差值,正常工作时间范围为早9点至晚5点。

[0010] 进一步的,交易对手方与黑名单地址的关联度表示对手方的网络IP地址与系统预设黑名单地址的关联指标I;

使用以下步骤获得具体的关联指标I:

S201、创建系统预设的黑名单地址列表,该列表包含已知被标记为不信任的地址;

S202、在交易过程中,获取交易对手方的IP地址,获取的方式为通过网络日志、访

问日志以及审计记录中的任一种;

S203、将交易对手方的IP地址与预设的黑名单地址列表进行对比,直接对比交易对手方的IP地址与黑名单地址列表中每个地址,若存在匹配,将其作为关联数据;

S204、在找到匹配的IP地址后,使用以下公式计算关联指标I:

$$I = Ps/Zs$$

[0011] 式中,Ps表示匹配IP地址数量,Zs表示总IP地址数量。

[0012] 进一步的,网络波动系数Q的获取过程如下:

在预设时间周期T内,采集每个时刻下交易时的网络传输速率Sv_t,计算T时间周期内不同时刻下的网络传输速率的平均值,根据平均值和网络传输速率Sv_t,计算网络波动系数Q,所依据的公式如下:

$$\begin{cases} Q = \sqrt{\left(\sum_{t=1}^{n}(Sv_t - \overline{Sv})^2\right)/(n-1)} \\ \overline{Sv} = \left(\sum_{t=1}^{n} Sv_t\right)/n \end{cases};$$

式中,$\overline{Sv}$表示T时间周期内不同时刻下的网络传输速率的平均值,t=1、2、…、n,n为正整数,且n=T。

[0013] 进一步的,对评估数据集进行预处理的过程为:对各个数据进行无量纲化处理。

[0014] 进一步的,在本区块链上进行交易时,计算本次交易的异常程度预估值Ead1,所依据的公式如下:

$$Ead1 = F1 * Xj + F2 * Xs + F3 * I$$

[0015] 式中,Xj、Xs分别为交易频率差和交易时间差,F1、F2、F3分别为交易频率差、交易时间差以及关联指标I的预设比例系数,且F3>F1>F2>0;

在跨区块链进行交易时,计算本次交易的异常程度预估值Ead2,所依据的公式如下:

$$Ead2 = Ead1 + G_1 * Q$$

[0016] 式中,G_1为常数修正系数。

[0017] (三)有益效果

本发明提供了一种基于区块链技术的数字货币身份认证系统,具备以下有益效果:

本发明在本区块链上进行交易时,通过获取评估数据集中的交易频率差、交易时间差和交易对手方与黑名单地址的关联度数据,搭建对应的模型计算后,生成准确、有效的异常程度预估值Ead1,依据后续的对比结果,可以高效的检测到异常交易行为,这有助于降低交易风险;在跨区块链进行交易时,通过同步获取用户交易过程中的评估数据集和网络波动系数Q,并基于预处理的数据集计算交易的异常程度预估值Ead2,依据后续的对比结果,可以得出在不同场景下交易时的异常程度,这有助于评估跨链交易的安全性和可信度,识别可能存在的风险和异常情况;

2、本发明采用公钥加密、数字签名技术和评估数据集的方法，可以提高数据的完整性、真实性和身份验证的准确性，同时检测和预防异常交易行为，增强跨链交易的安全性和可信度，有助于保护用户隐私、防范风险和维护整体系统的安全运行。

附图说明

[0018] 图1为本发明中一种基于区块链技术的数字货币身份认证系统的模块结构示意图；

图2为本发明的电子设备图。

具体实施方式

[0019] 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、完整的描述，显然，所描述的实施例仅仅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做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。

实施例1

[0020] 请参阅图1，本实施例提供一种基于区块链技术的数字货币身份认证系统，该系统包括用户注册和身份验证模块、数据获取和存储模块、身份认证和验证模块、跨链身份认证和互操作模块以及异常风险评估预警模块，该系统针对不同情况下进行的身份认证和交易进行异常检测处理，并对交易过程中存在的风险进行有效评估，以提示用户并通过线上监管人员进行远程监管，保证在不同身份认证情况下进行数字货币交易的安全性；

用户注册和身份验证模块，在注册时，获取用户的身份信息和证明材料数据，并进行初步身份验证；

其中，用户的身份信息包括用户本人的姓名、身份证号码以及联系电话，用户的身份信息是用户在注册时自行填写并提供的，证明材料数据包括护照、驾驶证和本人照片；

进行初步身份验证的方式为：使用传统的身份验证方式，如与法定机构数据库进行比对或使用第三方身份验证服务，本方案中使用的身份验证方式为：与法定机构数据库进行比对，这种方式通常涉及与其他法定机构的身份验证数据库进行比对，以验证个人提供的身份信息的准确性和合法性；

具体的实施方式包括以下步骤：

收集身份信息：用户在进行身份验证时，需要提供一些个人身份信息，例如姓名、出生日期、身份证号码；数据库查询：身份验证服务提供商会将用户提供的身份信息与相应的法定机构数据库进行比对，这些数据库可能包括国家人口登记数据库、驾驶执照数据库、护照数据库；数据比对：身份验证服务将用户提供的身份信息与数据库中存储的相应信息进行比对，比对过程通常涉及验证数据的一致性、有效性和合法性；例如，验证身份证号码是否有效、姓名与数据库记录是否匹配；验证结果：根据比对结果，身份验证服务会生成一个验证结果，指示提供的身份信息是否通过验证，验证结果可能是通过、未通过或需要进一步验证；值得注意的是，具体的身份验证方式和使用的法定机构数据库可能因国家和地区而异；在某些国家可能提供身份验证接口，允许第三方服务提供商进行在线验证；而在其他地方，可能需要用户提供身份证明文件的副本，并由服务提供商进行手动验证。

[0021] 数据获取和存储模块,在初步验证完用户身份后,提取用户的身份信息和证明材料数据,创建用户的数字身份,并将其存储至区块链上;

其中,创建用户的数字身份并将其存储至区块链上是一种保护用户隐私和确保身份信息安全的方式,具体过程如下:

S101、用户成功通过基本的身份验证,提供手机号码和邮箱地址,并验证其有效性;

S102、用户提供身份证明材料,如身份证、护照、驾驶执照,平台利用OCR技术或其他手段提取身份证明材料中的关键信息,如姓名、身份证号码、国籍等;

S103、使用加密算法将用户的身份信息编码为唯一的数字身份标识符,例如,可以使用Hash函数将身份信息哈希化,得到一个独一无二的数字标识;

S104、将用户的数字身份存储到区块链上,确保该数据不可篡改和删除,可以选择公有区块链,如以太坊或私有区块链来存储用户数字身份,取决于具体需求和安全性要求;

S105、为保护用户隐私,存储在区块链上的数字身份可以进行加密,只有拥有相应私钥的用户才能解密和访问其个人身份信息;

举例来说,假设XX是一个新用户,她通过提供手机号码和邮箱地址成功通过初步验证,接下来,XX提供了她的身份证明材料,包括身份证照片,平台使用OCR技术提取身份证的姓名、身份证号码和国籍信息;然后,使用加密算法,如SHA-256将XX的身份信息编码为一个唯一的数字身份标识符,例如,经过哈希处理,Alice的身份信息生成的数字标识符为"abc123";最后,平台将"abc123"存储在区块链上,确保数据的不可篡改和安全性;只有XX及其他拥有相应私钥的授权用户才能解密和访问该信息,当其他服务方需要验证XX的身份时,可以通过请求区块链上的数字身份数据获得必要的身份信息,并进行验证。

[0022] 身份认证和验证模块,在用户进行交易前,采用公钥加密和数字签名技术,对用户提供的身份信息进行加密和签名,以保证数据的完整性和真实性,便于后续在本区块链上进行交易时,要求用户提供数字签名来验证其身份和认证结果;并同步获取用户交易过程中的评估数据集,且评估数据集包括交易频率差、交易时间差以及交易对手方与黑名单地址的关联度;

其中,公钥加密和数字签名技术是密码学中常用的两种加密和验证技术,它们可以用于确保数据的机密性、完整性和身份认证性;

公钥加密:公钥加密是一种加密技术,使用了一对密钥,包括公钥和私钥,公钥可以公开分发给任何人,而私钥则由密钥的所有者保密,使用公钥加密算法,可以使用公钥对消息进行加密,而只有持有对应私钥的人能够解密消息;简单来说,如果X1想要向X2发送加密消息,X2可以提供他的公钥给X1,X1将使用该公钥对消息进行加密,得到一个只有X2能够解密的密文,即使在传输过程中,其他人获取了该加密消息,他们也无法解密它,因为只有X2持有私钥,常见的公钥加密算法有RSA和椭圆曲线加密算法ECC;

数字签名:数字签名是用于验证数据完整性和身份认证的技术,它基于一对密钥,包括私钥和公钥,与公钥加密不同,数字签名使用私钥对数据进行签名,而公钥用于验证签名的真实性,当X1要发送一份被签名的消息给X2时,X1首先使用她的私钥对消息进行签名,创建一个唯一的数字签名,然后,她将消息和数字签名发送给X2,X2可以使用X1的公钥来验证签名的真实性,如果数字签名验证成功,这意味着消息确实由X1签名,并且在传输过程中

没有被篡改,数字签名常用于保证文件的原始性、验证身份(通过公钥认证),或者确保数据在传输过程中没有被篡改;常见的数字签名算法包括RSA和椭圆曲线数字签名算法ECDSA;

总结起来,公钥加密技术用于数据加密和解密,而数字签名技术用于数据完整性验证和身份认证,这两种技术结合使用,可以在网络通信中确保数据的保密性、完整性和身份真实性;

交易频率差:分析用户的交易频率,检测是否存在异常频繁的交易行为,交易频率差表示本次交易频率与历史交易频率之间的差值,历史交易频率表示最近一个月的交易频率;例如:本次交易频率为10次/天,最近一个月的交易频率为5次/天,则差值即为5

交易时间差:检查交易时间是否存在正常的工作范围内,以防止异常的交易行为,交易时间差表示本次交易时间与正常工作时间范围的差值,正常工作时间范围为早9点至晚5点;例如:本次交易时间为早上8点,则交易时间差为9-8=1小时;

交易对手方与黑名单地址的关联度:表示对交易对手方进行分析,检测对手方的网络IP地址与系统预设黑名单地址的关联指标I;

使用以下步骤获得具体的关联指标I:

S201、收集黑名单地址列表:首先,需要创建一个系统预设的黑名单地址列表,该列表包含已知的恶意IP地址或被标记为不信任的地址;

S202、获取交易对手方的IP地址:在交易过程中,获取交易对手方的IP地址,这可以通过网络日志、访问日志或审计记录等方式获得;

S203、对比IP地址:将交易对手方的IP地址与预设的黑名单地址列表进行对比,可以使用以下两种方法之一:a) 精确匹配:直接对比交易对手方的IP地址与黑名单地址列表中每个地址,如果存在匹配,将其作为关联指标之一;b) 子网匹配:根据IP地址的子网掩码,将交易对手方的IP地址与黑名单地址列表中的地址进行子网匹配,如果存在匹配,将其作为关联指标之一;

S204、计算关联系数:在找到匹配的IP地址后,可以使用以下公式计算关联指标I:

$$I = Ps/Zs$$

[0023] 式中,Ps表示匹配IP地址数量,Zs表示总IP地址数量;

关联指标I表示交易对手方的IP地址与系统预设黑名单地址的关联程度,如果关联系数接近或达到1,则表示交易对手方的IP地址与黑名单地址高度关联,可能存在风险;需要注意的是,关联系数仅表示IP地址之间的匹配程度,并不能直接确定交易对手方的可信度,可能存在假阳性或假阴性的情况;因此,综合其他安全措施和认证方式进行综合评估才能做出最终判断。

[0024] 跨链身份认证和互操作模块,在用户于其他区块链上进行交易时,通过跨链身份认证和互操作机制,将其身份信息和证明材料数据传递至目标区块链上,并同步获取用户交易过程中的评估数据集和网络波动系数Q;

其中,跨链身份认证和互操作机制是一种在不同区块链之间实现身份验证和信息共享的技术解决方案,下面是本实施例中的实现方式,展示了跨链身份认证和互操作的过程:

跨链身份认证:a) 用户发起身份认证请求:当用户需要在目标区块链上进行交易或使用服务时,首先向目标区块链发送身份认证请求,请求包括用户的身份信息以及需要

验证的信息;b) 跨链身份认证机制:目标区块链使用特定的跨链身份认证机制来验证用户的身份,这可能涉及与用户的原始区块链进行通信验证,或使用特定的跨链身份验证协议,在验证成功后,目标区块链确认用户的身份;c) 返回身份认证结果:目标区块链向用户返回身份认证结果,通常是一个身份认证令牌或其他标识;

跨链信息共享:a) 用户请求信息共享:用户在目标区块链上完成身份认证后,可以发送信息共享的请求,包括期望共享的数据和接收者的地址;b) 跨链互操作机制:目标区块链使用跨链互操作机制将请求传递到源区块链,以获取需要共享的数据,这可能涉及特定的跨链通信协议或智能合约的调用;c) 源区块链数据共享:源区块链收到共享请求后,根据请求的合法性和权限,将相应的数据共享给目标区块链,这可能需要使用特定的数据转换或加密技术来确保数据在跨链过程中的安全性和一致性;d) 返回共享结果:源区块链将共享的数据传递给目标区块链并返回共享结果,目标区块链收到数据后可以继续进行交易或服务;

具体的跨链身份认证和互操作机制可以根据区块链平台的不同而异,一些开源的跨链解决方案,如Cosmos、Polkadot和Interledger,提供了特定的协议和机制来实现跨链身份验证和共享;总结起来,跨链身份认证和互操作机制允许用户在不同区块链之间进行身份验证和信息共享,通过特定的协议和机制确保安全性和一致性,这为用户提供了跨区块链之间的无缝体验,并促进了区块链之间的互操作性和数据共享;

网络波动系数Q表现在交易时系统内网络的波动程度,波动程度越高,则表示交易在传输过程越不稳定,交易时存在外来网络接入的风险越大;

网络波动系数Q的获取过程如下:

在预设时间周期T内,采集每个时刻下交易时的网络传输速率Sv_t,计算T时间周期内不同时刻下的网络传输速率的平均值,根据平均值和网络传输速率Sv_t,计算网络波动系数Q,所依据的公式如下:

$$\begin{cases} Q = \sqrt{\left(\sum_{t=1}^{n}(Sv_t - \overline{Sv})^2\right)/(n-1)} \\ \overline{Sv} = \left(\sum_{t=1}^{n} Sv_t\right)/n \end{cases}$$

[0025] 式中,$\overline{Sv}$表示T时间周期内不同时刻下的网络传输速率的平均值,t=1、2、…、n,n为正整数,且n=T。

[0026] 异常风险评估预警模块,在本区块链上进行交易时,依据经过预处理后的评估数据集,搭建异常风险评估计算模型,生成本次交易的异常程度预估值Ead1,并将异常程度预估值Ead1与预设的第一评估阈值Emo_{δ}进行对比,若是异常程度预估值Ead1超过第一评估阈值Emo_{δ},则表示交易存在异常,发出一级预警信号;反之,则系统不做响应动作;

在跨区块链进行交易时,依据经过预处理后的评估数据集和网络波动系数Q,二次搭建异常风险评估计算模型,生成本次交易的异常程度预估值Ead2,并将异常程度预估值Ead2与预设的第二评估阈值Emo_{θ}进行对比,若是异常程度预估值Ead2超过第二评估阈值Emo_{θ},则表示交易存在异常,发出二级预警信号;反之,则系统不做响应动作;

其中,对评估数据集进行预处理的过程为:对各个数据进行无量纲化处理;

在本区块链上进行交易时,计算本次交易的异常程度预估值Ead1,所依据的公式如下:

$$Ead1 = F1 * Xj + F2 * Xs + F3 * I$$

[0027] 式中,Xj、Xs分别为交易频率差和交易时间差,F1、F2、F3分别为交易频率差、交易时间差以及关联指标I的预设比例系数,且F3>F1>F2>0,F1、F2、F3的取值范围均为0~1;

在跨区块链进行交易时,计算本次交易的异常程度预估值Ead2,所依据的公式如下:

$$Ead2 = Ead1 + G_1 * Q$$

[0028] 式中,G_1为常数修正系数,且其具体值可由用户调整设置,或者由分析函数拟合生成,且G_1的取值范围为1~2;

需要说明的是,一级预警信号和二级预警信号只是用于区分预警信号形式;

在工作人员收到一级预警信号和二级预警信号时,做出的响应动作为,立即关闭当前交易进程,并保存证据,便于后续的调查和取证。

[0029] 具体的,在本区块链上进行交易时,通过获取评估数据集中的交易频率差、交易时间差和交易对手方与黑名单地址的关联度数据,搭建对应的模型计算后,生成准确、有效的异常程度预估值Ead1,依据后续的对比结果,可以高效的检测到异常交易行为,这有助于降低交易风险;在跨区块链进行交易时,通过同步获取用户交易过程中的评估数据集和网络波动系数Q,并基于预处理的数据集计算交易的异常程度预估值Ead2,依据后续的对比结果,可以得出在不同场景下交易时的异常程度,这有助于评估跨链交易的安全性和可信度,识别可能存在的风险和异常情况;

综合本实施例的整体方案,采用公钥加密、数字签名技术和评估数据集的方法,可以提高数据的完整性、真实性和身份验证的准确性,同时检测和预防异常交易行为,增强跨链交易的安全性和可信度,有助于保护用户隐私、防范风险和维护区块链系统的安全运行。

[0030] 请参阅图2,本实施例运行基于区块链技术的数字货币身份认证系统需要使用到对应的电子设备,该电子设备包括处理器和存储器,用于执行基于区块链技术的数字货币身份认证系统。

实施例2

[0031] 以实施例1为基础,本实施例还提供一种基于区块链技术的数字货币身份认证的过程:S1、在注册时,获取用户的身份信息和证明材料数据,并进行初步身份验证;

S2、在初步验证完用户身份后,提取用户的身份信息和证明材料数据,创建用户的数字身份,并将其存储至区块链上;

S3、在用户进行交易前,采用公钥加密和数字签名技术,对用户提供的身份信息进行加密和签名,在本区块链上进行交易时,提供数字签名来验证用户身份和认证结果,并同步获取用户交易过程中的评估数据集;

S4、在用户于其他区块链上进行交易时,通过跨链身份认证和互操作机制,将其身

份信息和证明材料数据传递至目标区块链上,并同步获取用户交易过程中的评估数据集和网络波动系数Q;

S5、在本区块链上进行交易时,依据经过预处理后的评估数据集,搭建异常风险评估计算模型,生成本次交易的异常程度预估值Ead1,并将异常程度预估值Ead1与预设的第一评估阈值Emo_{δ}进行对比,若是异常程度预估值Ead1超过第一评估阈值Emo_{δ},则发出一级预警信号;反之,则不做响应动作;

在跨区块链进行交易时,依据经过预处理后的评估数据集和网络波动系数Q,二次搭建异常风险评估计算模型,生成本次交易的异常程度预估值Ead2,并将异常程度预估值Ead2与预设的第二评估阈值Emo_{θ}进行对比,若是异常程度预估值Ead2超过第二评估阈值Emo_{θ},则发出二级预警信号;反之,则不做响应动作。

[0032] 在申请中,所述涉及到的若干个公式均是去量纲后取其数值计算,而所述公式是由采集大量数据进行软件模拟得到最近真实情况的一个公式,公式中的由本领域的技术人员根据实际情况进行设置。

[0033] 上述实施例,可以全部或部分地通过软件、硬件、固件或其他任意组合来实现。当使用软件实现时,上述实施例可以全部或部分地以计算机程序产品的形式实现。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,或者计算机软件和电子硬件的结合来实现。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。

[0034] 所述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,作为单元显示的部件可以是或者也可以不是物理单元,既可以位于一个地方,或者也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的部分或者全部单元来实现本实施例方案的目的。

[0035] 以上所述,仅为本申请的具体实施方式,但本申请的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本申请揭露的技术范围内,可轻易想到变化或替换,都应涵盖在本申请的保护范围之内。

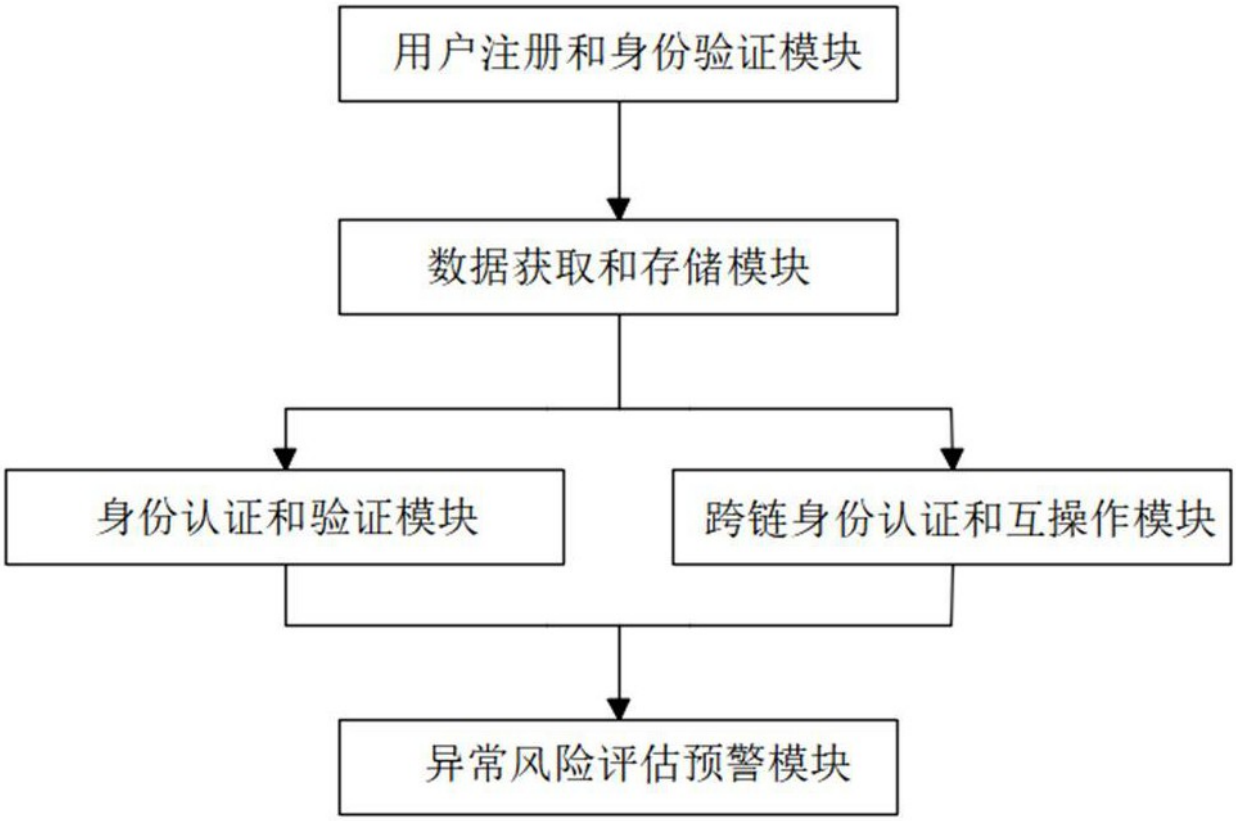

用户注册和身份验证模块
数据获取和存储模块
身份认证和验证模块
跨链身份认证和互操作模块
异常风险评估预警模块

图 1

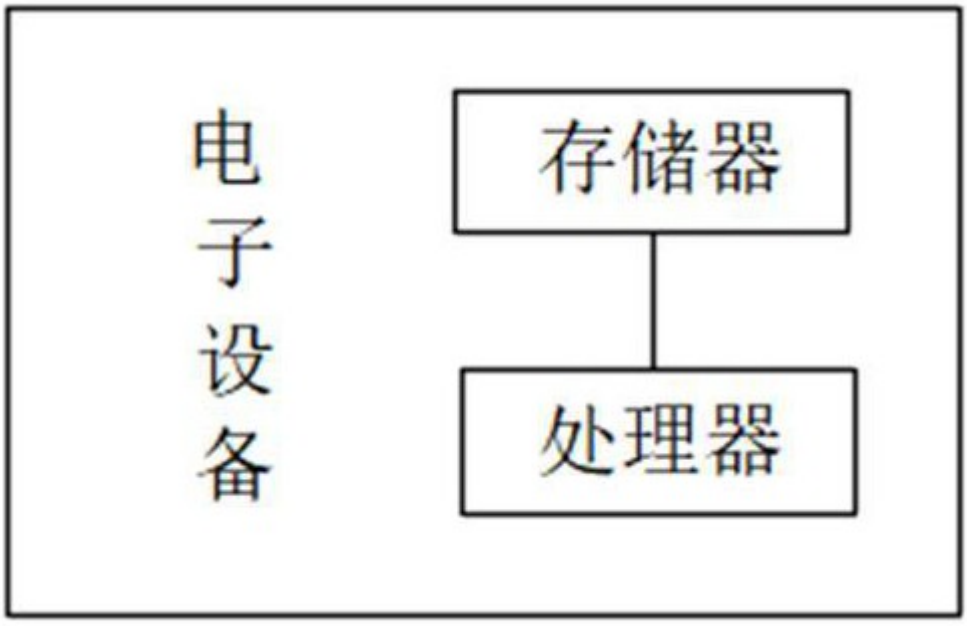

电子设备
存储器
处理器

图 2