(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108510281 A
(43)申请公布日 2018.09.07

(21)申请号 201810276790.4

(22)申请日 2018.03.30

(71)申请人 北京金山安全软件有限公司
地址 100123 北京市朝阳区姚家园南路1号惠通时代广场8号楼

(72)发明人 黄献德

(74)专利代理机构 北京柏杉松知识产权代理事务所(普通合伙) 11413
代理人 李欣 马敬

(51)Int.Cl.
G06Q 20/40(2012.01)
G06Q 20/06(2012.01)
G06N 3/04(2006.01)

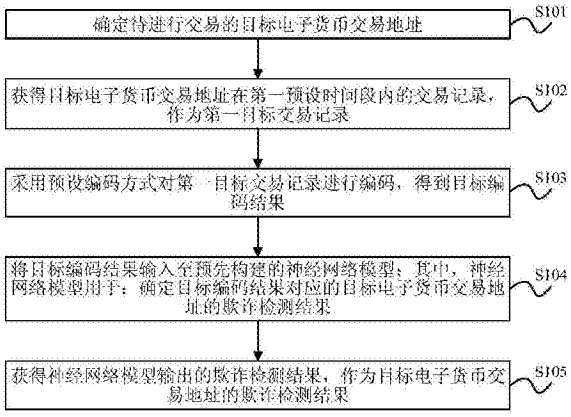
权利要求书2页 说明书12页 附图2页

(54)发明名称

数据检测方法、装置、电子设备及存储介质

(57)摘要

本发明实施例提供了一种数据检测方法、装置、电子设备及存储介质。该方法包括：确定待进行交易的目标电子货币交易地址；获得目标电子货币交易地址在第一预设时间段内的交易记录，作为第一目标交易记录；采用预设编码方式对第一目标交易记录进行编码，得到目标编码结果；将目标编码结果输入至预先构建的神经网络模型；该神经网络模型用于：确定目标编码结果对应的电子货币交易地址的欺诈检测结果；获得神经网络模型输出的欺诈检测结果，作为目标电子货币交易地址的欺诈检测结果。应用本发明实施例，能够确定待进行的交易是否为欺诈交易，从而减少欺诈交易，保护了用户的资产安全。



CN 108510281 A

1.一种数据检测方法,其特征在于,所述方法包括:

确定待进行交易的目标电子货币交易地址;

获得所述目标电子货币交易地址在第一预设时间段内的交易记录,作为第一目标交易记录;

采用预设编码方式对所述第一目标交易记录进行编码,得到目标编码结果;

将所述目标编码结果输入至预先构建的神经网络模型;其中,所述神经网络模型用于:确定所述目标编码结果对应的目标电子货币交易地址的欺诈检测结果;

获得所述神经网络模型输出的欺诈检测结果,作为所述目标电子货币交易地址的欺诈检测结果。

2.根据权利要求1所述的方法,其特征在于,在所述将所述目标编码结果输入至预先构建的神经网络模型之前,所述方法还包括:

构建所述神经网络模型;

所述构建所述神经网络模型,包括:

确定N个预设电子货币交易地址,其中,所述N个预设电子货币交易地址中包括:具有欺诈行为的电子货币交易地址,和/或,不具有欺诈行为的电子货币交易地址;其中,所述N≥2;

分别获得每个预设电子货币交易地址在第二预设时间段内的交易记录,作为每个预设电子货币交易地址对应的第二目标交易记录;

采用所述预设编码方式分别对每个第二目标交易记录进行编码,得到每个第二目标交易记录对应的编码结果;

利用预设神经网络算法和N个训练样本训练得到所述神经网络模型,其中,一个训练样本中包括:一个第二目标交易记录对应的编码结果和欺诈标识信息;所述欺诈标识信息用于:标识该第二目标交易记录对应的预设电子货币交易地为欺诈地址或非欺诈地址。

3.根据权利要求2所述的方法,其特征在于,所述分别获得每个预设电子货币交易地址在第二预设时间段内的交易记录,作为每个预设电子货币交易地址对应的第二目标交易记录,包括:

分别获得具有欺诈行为的预设电子货币交易地址的第一延伸交易记录和在所述第二预设时间段内的交易记录,和/或,分别获得不具有欺诈行为的预设电子货币交易地址在所述第二预设时间段内的交易记录,作为相应预设电子货币交易地址对应的第二目标交易记录;所述第一延伸交易记录包括:接收所述预设电子货币交易地址汇款的电子货币交易地址的交易记录。

4.根据权利要求3所述的方法,其特征在于,所述获得所述目标电子货币交易地址在第一预设时间段内的交易记录,作为第一目标交易记录的步骤,包括:

获得所述目标电子货币交易地址的第二延伸交易记录和在所述第一预设时间段内的交易记录,作为第一目标交易记录;所述第二延伸交易记录包括:接收所述目标电子货币交易地址汇款的电子货币交易地址的交易记录。

5.根据权利要求2所述的方法,其特征在于,当所述N个预设电子货币交易地址中包括:具有欺诈行为的电子货币交易地址和不具有欺诈行为的电子货币交易地址时,所述具有欺诈行为的电子货币交易地址的总数目与所述不具有欺诈行为的电子货币交易地址的总数

目的差值绝对值小于预设数目。

6.根据权利要求2所述的方法，其特征在于，在训练得到所述神经网络模型之后，所述方法还包括：

利用M个优化样本对所述神经网络模型进行调优，得到调优神经网络模型；其中，一个优化样本中包括：用于优化模型的电子货币交易地址对应的编码结果和欺诈标识信息；其中，所述M≥2；

所述将所述目标编码结果输入至预先构建的神经网络模型，包括：

将所述目标编码结果输入至所述调优神经网络模型。

7.根据权利要求2所述的方法，其特征在于，所述预设神经网络算法包括：循环神经网络算法、深度神经网络算法和卷积神经网络算法中的任意一项。

8.一种数据检测装置，其特征在于，所述装置包括：

确定单元，用于确定待进行交易的目标电子货币交易地址；

第一获得单元，用于获得所述目标电子货币交易地址在第一预设时间段内的交易记录，作为第一目标交易记录；

编码单元，用于采用预设编码方式对所述第一目标交易记录进行编码，得到目标编码结果；

输入单元，用于将所述目标编码结果输入至预先构建的神经网络模型；其中，所述神经网络模型用于：确定所述目标编码结果对应的目标电子货币交易地址的欺诈检测结果；

第二获得单元，用于获得所述神经网络模型输出的欺诈检测结果，作为所述目标电子货币交易地址的欺诈检测结果。

9.一种电子设备，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1-7中任一项所述的方法步骤。

10.一种可读存储介质，其特征在于，所述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1-7中任一项所述的方法步骤。

数据检测方法、装置、电子设备及存储介质

技术领域

[0001] 本发明涉及计算机技术领域，特别是涉及数据检测方法、装置、电子设备及存储介质。

背景技术

[0002] 随着技术的发展，越来越多的用户使用电子货币来替代传统货币进行交易。其中，部分电子货币是基于区块链技术的加密货币，例如比特币和以太币等。

[0003] 但是，由于区块链技术中的交易为匿名交易，因而当用户想要进行电子货币交易时，用户无法获知交易对方的身份信息。从而使得用户很难辨别将进行的交易是否为欺诈交易，导致常常产生欺诈交易，使用户资产遭受损失。

发明内容

[0004] 本发明实施例的目的在于提供一种数据检测方法、装置、电子设备及存储介质，以能够确定待进行的交易是否为欺诈交易，从而减少欺诈交易，保护用户的资产安全。具体技术方案如下：

[0005] 第一方面，本发明实施例提供了一种数据检测方法，该方法可以包括：

[0006] 确定待进行交易的目标电子货币交易地址；

[0007] 获得目标电子货币交易地址在第一预设时间段内的交易记录，作为第一目标交易记录；

[0008] 采用预设编码方式对第一目标交易记录进行编码，得到目标编码结果；

[0009] 将目标编码结果输入至预先构建的神经网络模型；其中，神经网络模型用于：确定目标编码结果对应的目标电子货币交易地址的欺诈检测结果；

[0010] 获得神经网络模型输出的欺诈检测结果，作为目标电子货币交易地址的欺诈检测结果。

[0011] 可选地，在将目标编码结果输入至预先构建的神经网络模型之前，方法还可以包括：

[0012] 构建神经网络模型；

[0013] 相应地，构建神经网络模型，可以包括：

[0014] 确定N个预设电子货币交易地址，其中，N个预设电子货币交易地址中包括：具有欺诈行为的电子货币交易地址，和/或，不具有欺诈行为的电子货币交易地址；其中，$N \geq 2$；

[0015] 分别获得每个预设电子货币交易地址在第二预设时间段内的交易记录，作为每个预设电子货币交易地址对应的第二目标交易记录；

[0016] 采用预设编码方式分别对每个第二目标交易记录进行编码，得到每个第二目标交易记录对应的编码结果；

[0017] 利用预设神经网络算法和N个训练样本训练得到神经网络模型，其中，一个训练样本中包括：一个第二目标交易记录对应的编码结果和欺诈标识信息；欺诈标识信息用于：标

识该第二目标交易记录对应的预设电子货币交易地为欺诈地址或非欺诈地址。

[0018] 可选地，分别获得每个预设电子货币交易地址在第二预设时间段内的交易记录，作为每个预设电子货币交易地址对应的第二目标交易记录，可以包括：

[0019] 分别获得具有欺诈行为的预设电子货币交易地址的第一延伸交易记录和在第二预设时间段内的交易记录，和/或，分别获得不具有欺诈行为的预设电子货币交易地址在第二预设时间段内的交易记录，作为相应预设电子货币交易地址对应的第二目标交易记录；第一延伸交易记录包括：接收预设电子货币交易地址汇款的电子货币交易地址的交易记录。

[0020] 可选地，获得目标电子货币交易地址在第一预设时间段内的交易记录，作为第一目标交易记录的步骤，可以包括：

[0021] 获得目标电子货币交易地址的第二延伸交易记录和在第一预设时间段内的交易记录，作为第一目标交易记录；第二延伸交易记录包括：接收目标电子货币交易地址汇款的电子货币交易地址的交易记录。

[0022] 可选地，当N个预设电子货币交易地址中包括：具有欺诈行为的电子货币交易地址和不具有欺诈行为的电子货币交易地址时，具有欺诈行为的电子货币交易地址的总数目与不具有欺诈行为的电子货币交易地址的总数目的差值绝对值小于预设数目。

[0023] 可选地，在训练得到神经网络模型之后，该方法还可以包括：

[0024] 利用M个优化样本对神经网络模型进行调优，得到调优神经网络模型；其中，一个优化样本中包括：用于优化模型的电子货币交易地址对应的编码结果和欺诈标识信息；其中，$M \geq 2$；

[0025] 相应地，将目标编码结果输入至预先构建的神经网络模型，可以包括：

[0026] 将目标编码结果输入至调优神经网络模型。

[0027] 可选地，预设神经网络算法可以包括：循环神经网络算法、深度神经网络算法和卷积神经网络算法中的任意一项。

[0028] 可选地，预设编码方式可以包括：词向量编码item2vec方式或独热编码one-hot encoding方式。

[0029] 可选地，第一目标交易记录包括至少一个子交易记录，第一子交易记录包括：目标电子货币交易地址、电子货币交易对方地址、目标电子货币交易地址的收支类型、交易金额、目标电子货币交易地址的交易余额和交易时间；第一子交易记录为第一目标交易记录中的任意一个子交易记录；

[0030] 其中，电子货币交易对方地址包括：接收目标电子货币交易地址汇款或汇款至目标电子货币交易地址的电子货币交易地址。

[0031] 第二方面，本发明实施例还提供了一种数据检测装置，该装置可以包括：

[0032] 确定单元，用于确定待进行交易的目标电子货币交易地址；

[0033] 第一获得单元，用于获得目标电子货币交易地址在第一预设时间段内的交易记录，作为第一目标交易记录；

[0034] 编码单元，用于采用预设编码方式对第一目标交易记录进行编码，得到目标编码结果；

[0035] 输入单元，用于将目标编码结果输入至预先构建的神经网络模型；其中，神经网络

模型用于：确定目标编码结果对应的目标电子货币交易地址的欺诈检测结果；

[0036] 第二获得单元，用于获得神经网络模型输出的欺诈检测结果，作为目标电子货币交易地址的欺诈检测结果。

[0037] 可选地，该装置还可以包括构建单元；

[0038] 构建单元，用于在输入单元将目标编码结果输入至预先构建的神经网络模型之前，构建神经网络模型；

[0039] 相应地，构建单元可以包括：

[0040] 确定子模块，用于确定N个预设电子货币交易地址，其中，N个预设电子货币交易地址中包括：具有欺诈行为的电子货币交易地址，和/或，不具有欺诈行为的电子货币交易地址；其中，$N \geq 2$；

[0041] 获得子模块，用于分别获得每个预设电子货币交易地址在第二预设时间段内的交易记录，作为每个预设电子货币交易地址对应的第二目标交易记录；

[0042] 编码子模块，用于采用预设编码方式分别对每个第二目标交易记录进行编码，得到每个第二目标交易记录对应的编码结果；

[0043] 训练子模块，用于利用预设神经网络算法和N个训练样本训练得到神经网络模型，其中，一个训练样本中包括：一个第二目标交易记录对应的编码结果和欺诈标识信息；欺诈标识信息用于：标识该第二目标交易记录对应的预设电子货币交易地为欺诈地址或非欺诈地址。

[0044] 可选地，获得子模块具体用于：

[0045] 分别获得具有欺诈行为的预设电子货币交易地址的第一延伸交易记录和在第二预设时间段内的交易记录，和/或，分别获得不具有欺诈行为的预设电子货币交易地址在第二预设时间段内的交易记录，作为相应预设电子货币交易地址对应的第二目标交易记录；第一延伸交易记录包括：接收预设电子货币交易地址汇款的电子货币交易地址的交易记录。

[0046] 可选地，第一获得单元具体用于：

[0047] 获得目标电子货币交易地址的第二延伸交易记录和在第一预设时间段内的交易记录，作为第一目标交易记录；第二延伸交易记录包括：接收目标电子货币交易地址汇款的电子货币交易地址的交易记录。

[0048] 可选地，当N个预设电子货币交易地址中包括：具有欺诈行为的电子货币交易地址和不具有欺诈行为的电子货币交易地址时，具有欺诈行为的电子货币交易地址的总数目与不具有欺诈行为的电子货币交易地址的总数目的差值绝对值小于预设数目。

[0049] 可选地，在本发明实施例中，该装置还可以包括：

[0050] 调整单元，用于在训练得到神经网络模型之后，利用M个优化样本对神经网络模型进行调优，得到调优神经网络模型；其中，一个优化样本中包括：用于优化模型的电子货币交易地址对应的编码结果和欺诈标识信息；其中，$M \geq 2$；

[0051] 输入单元具体用于：将目标编码结果输入至调优神经网络模型。

[0052] 可选地，预设神经网络算法可以包括：循环神经网络算法、深度神经网络算法和卷积神经网络算法中的任意一项。

[0053] 可选地，预设编码方式包括：词向量编码item2vec方式或独热编码one-hot

encoding方式。

[0054] 可选地，第一目标交易记录包括至少一个子交易记录，第一子交易记录包括：目标电子货币交易地址、电子货币交易对方地址、目标电子货币交易地址的收支类型、交易金额、目标电子货币交易地址的交易余额和交易时间；第一子交易记录为第一目标交易记录中的任意一个子交易记录；

[0055] 其中，电子货币交易对方地址为：接收目标电子货币交易地址汇款或汇款至目标电子货币交易地址的电子货币交易地址

[0056] 第三方面，本发明实施例还提供了一种电子设备，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；

[0057] 存储器，用于存放计算机程序；

[0058] 处理器，用于执行存储器上所存放的程序时，实现上述任一项数据检测方法的方法步骤。

[0059] 第四方面，本发明实施例还提供了一种可读存储介质，该可读存储介质内存储有计算机程序，计算机程序被处理器执行时实现上述任一项数据检测方法的方法步骤。

[0060] 第五方面，本发明实施例还提供了一种包含指令的计算机程序产品，当其在电子设备上运行时，使得电子设备执行：上述任一项数据检测方法的方法步骤。

[0061] 在本发明实施例中，当需要确定待进行的交易是否为欺诈交易时，可以先确定待进行交易的目标电子货币交易地址。然后，获得该目标电子货币交易地址在第一预设时间段内的交易记录，并将获得的交易记录记为第一目标交易记录。之后，采用预设编码方式对第一目标交易记录进行编码，得到目标编码结果。再将得到目标编码结果输入至神经网络模型中。其中，由于该神经网络模型可以用于确定编码结果对应的电子货币交易地址的欺诈检测结果。因而可以获得该神经网络模型输出的、对于该目标电子货币交易地址的欺诈检测结果。另外，由于当一个电子货币交易地址为欺诈地址时，则与该电子货币交易地址进行的交易很可能为欺诈交易，因而该目标电子货币交易地址的欺诈检测结果也就是待进行的交易的欺诈检测结果。这样，可以通过该欺诈检测结果来确定待进行的交易是否为欺诈交易，从而减少欺诈交易，保护用户的资产安全。

附图说明

[0062] 为了更清楚地说明本发明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。

[0063] 图1为本发明实施例提供的一种数据检测方法的流程图；

[0064] 图2为本发明实施例提供的一种构建神经网络模型的流程图；

[0065] 图3为本发明实施例提供的一种数据检测装置的结构示意图；

[0066] 图4为本发明实施例提供的一种电子设备的结构示意图。

具体实施方式

[0067] 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。

[0068] 为了解决现有技术中难以确定待进行的电子货币交易是否为欺诈交易的问题，本发明实施例提供了一种数据检测方法、装置、电子设备及存储介质。

[0069] 下面首先对本发明实施例提供的数据检测方法进行说明。

[0070] 参见图1，本发明实施例提供的数据检测方法可以包括如下步骤：

[0071] S101：确定待进行交易的目标电子货币交易地址；

[0072] S102：获得目标电子货币交易地址在第一预设时间段内的交易记录，作为第一目标交易记录；

[0073] S103：采用预设编码方式对第一目标交易记录进行编码，得到目标编码结果；

[0074] S104：将目标编码结果输入至预先构建的神经网络模型；其中，神经网络模型用于：确定目标编码结果对应的目标电子货币交易地址的欺诈检测结果；

[0075] S105：获得神经网络模型输出的欺诈检测结果，作为目标电子货币交易地址的欺诈检测结果。

[0076] 在本发明实施例中，当需要确定待进行的交易是否为欺诈交易时，可以先确定待进行交易的目标电子货币交易地址。然后，获得该目标电子货币交易地址在第一预设时间段内的交易记录，并将获得的交易记录记为第一目标交易记录。之后，采用预设编码方式对第一目标交易记录进行编码，得到目标编码结果。再将得到目标编码结果输入至神经网络模型中。其中，由于该神经网络模型用于确定目标编码结果对应的目标电子货币交易地址的欺诈检测结果。因而可以获得该神经网络模型输出的、对于该目标电子货币交易地址的欺诈检测结果。另外，由于当一个电子货币交易地址为欺诈地址时，则与该电子货币交易地址进行的交易很可能为欺诈交易，因而该目标电子货币交易地址的欺诈检测结果也就是待进行的交易的欺诈检测结果。这样，可以通过该欺诈检测结果来确定待进行的交易是否为欺诈交易，从而减少欺诈交易，保护用户的资产安全。

[0077] 其中，本发明实施例中的部分电子货币是基于区块链技术的加密货币。其中，虚拟币是电子货币中的一种，虚拟币包括但并不局限于比特币、以太币和莱特币。另外，本发明实施例中的一个电子货币交易地址为一个电子货币交易账号。

[0078] 另外，本发明实施例提供的神经网络模型可以对输入至该神经网络模型的、任意电子货币交易地址对应的交易记录的编码结果进行检测，从而输出相应电子货币交易地址的欺诈检测结果。

[0079] 下面以太币为示例，对本发明实施例提供的数据检测方法进行详细说明。

[0080] 在以太币交易中，当用户A(假设用户A对应的电子货币交易地址为a)在向用户B(假设用户B对应的电子货币交易地址为b)支付以太币之前，由于用户A无法获知用户B的身份信息导致无法确定用户B是否可信，因而无法确定待进行的交易是否为欺诈交易。

[0081] 为了确定该待进行的交易是否为欺诈交易，从而避免欺诈交易给用户A带来资产损失。在用户A执行该交易之前，电子设备可以确定用户A待进行交易的目标电子货币交易地址，即电子货币交易地址b。

[0082] 然后，电子设备可以通过以太坊API(Application Programming Interface，应用

程序编程接口)，获取电子货币交易地址b在第一预设时间段内的交易记录，并将获得的交易记录记为第一目标交易记录。其中，以太坊是一个基于区块链的、去中心化的应用平台，此为现有概念，在此不做详述。

[0083] 其中，为了能够获得较为准确的欺诈检测结果，可以尽量多的获得电子货币交易地址b的交易记录。而为了获得较多的交易记录，可以设置第一预设时间段对应较长的时长。例如设置第一预设时间段为：当前时刻至五年前当前时刻所对应的时间段，当然并不局限于此。

[0084] 另外，为了提高获得欺诈检测结果的速度，也可以将第一预设时间段设置为一个年度(例如2017年度)，当然并不局限于此。本领域技术人员可以根据实际需要来设置该第一预设时间段，在此不做具体限定。

[0085] 举例而言，获得的电子货币交易地址b的一条交易记录中可以包括：电子货币交易地址b、电子货币交易对方地址c、电子货币交易地址b的的收支类型：支出、交易金额：5个以太币、目标电子货币交易地址的交易余额：1个以太币、交易时间：20180316。

[0086] 其中，电子货币交易对方地址除了可以为：接收电子货币交易地址b汇款的电子货币交易对方地址c，还可以为：汇款至电子货币交易地址b的电子货币交易地址e或f等，这是合理的。

[0087] 当然，该条交易记录中还可以包括交易总次数，例如1000次，当然交易记录中包含的元素并不局限于此。其中，该交易总次数是指：电子货币交易地址b在将5个以太币汇入电子货币交易对方地址c之前所执行的总交易次数。

[0088] 在获得电子货币交易地址b对应的第一目标交易记录之后，可以利用词向量编码item2vec方式或独热编码one-hot encoding方式，对该第一目标交易记录进行编码，将编码结果记为目标编码结果，得到目标编码结果。

[0089] 其中，独热编码one-hot encoding方式可以以向量形式来表示交易记录中的元素，即可以利用一个多维度的向量表示一个元素。其中，该向量中的多个维度的值为0，只有一个维度的值为1。采用词向量编码item2vec方式进行编码，可以降低维度，并且可以挖掘交易记录中各个元素的上下文关系，从而提高向量语义上的准确度。

[0090] 在获得目标编码结果之后，可以构建神经网络模型，并将该目标编码结果输入至构建得到的神经网络模型中，由于该神经网络模型可以确定编码结果对应的电子货币交易地址的欺诈检测结果，因而可以获得该神经网络模型输出的、对于电子货币交易地址b的欺诈检测结果。为了清晰布局，后续对构建该神经网络模型的方式进行详细说明。

[0091] 其中，在一种实现方式中，该欺诈检测结果具体可以包括：可信度很高、可信度高、可信度一般、可信度低和可信度很低中的一种。在另一种实现方式中，该欺诈检测结果也可以为：欺诈风险高或欺诈风险低。当然并不局限于此。

[0092] 假设神经网络模型输出的、对于电子货币交易地址b的欺诈检测结果为：可信度低，即欺诈风险程度为：可信度低。此时，表明电子货币交易地址b的交易行为与欺诈地址的交易行为相似度较高，或与非欺诈地址的交易行为相似度较低。也就是说，电子货币交易地址b很可能为欺诈地址。此时，与电子货币交易地址b待进行的交易很可能为欺诈交易，为了保证用户的资产安全，可以将可信度低(即欺诈风险)作为待进行的交易的欺诈检测结果。这样，当用户A在得知该待进行的交易的可信度低后，可以停止交易，从而保证用户A的资产

安全。

[0093] 另外，当电子货币交易地址b的欺诈检测结果为：可信度高时，表明电子货币交易地址b的交易行为与欺诈地址的交易行为相似度较低，或与非欺诈地址的交易行为相似度较高。这样，当用户A在得知该待进行的交易的可信度高后，可以进行交易，保证了用户A的资产安全。

[0094] 下面对本发明实施例提供的神经网络模型的构建过程进行详细说明。

[0095] 参见图2，该神经网络模型的构建步骤可以包括：

[0096] S201：确定N个预设电子货币交易地址，其中，N个预设电子货币交易地址中包括：具有欺诈行为的电子货币交易地址，和/或，不具有欺诈行为的电子货币交易地址；其中，N≥2；

[0097] 其中，在一种实现方式中，确定的N个预设电子货币交易地址均为具有欺诈行为的电子货币交易地址。在另一种实现方式中，确定的N个预设电子货币交易地址均为不具有欺诈行为的电子货币交易地址。在又一种实现方式中，确定的N个预设电子货币交易地址既包括具有欺诈行为的电子货币交易地址，又包括不具有欺诈行为的电子货币交易地址。在又一种实现方式中，确定的N个预设电子货币交易地址既包括具有欺诈行为的电子货币交易地址，又包括具有欺诈行为的电子货币交易地址的第一延伸交易地址。这都是合理的。

[0098] 其中，具有欺诈行为的电子货币交易地址的第一延伸交易地址是指：接收该具有欺诈行为的电子货币交易地址汇款的电子货币交易地址。

[0099] 可以理解的是，确定的每一个预设电子货币交易地址均对应有一个欺诈标识信息。该欺诈标识信息用于标识预设电子货币交易地是欺诈地址，还是非欺诈地址。例如用1标识为欺诈地址，用0标识非欺诈地址，这都是合理的。当然并不局限于此。

[0100] 当N个预设电子货币交易地址中包括：具有欺诈行为的电子货币交易地址和不具有欺诈行为的电子货币交易地址时，为了避免训练得到的模型的检测结果不准确，可以设置具有欺诈行为的电子货币交易地址的总数目与不具有欺诈行为的电子货币交易地址的总数目的差值绝对值小于预设数目。

[0101] 其中，本领域技术人员可以根据具体需求来设置该预设数目，在此不做限定。

[0102] S202：分别获得每个预设电子货币交易地址在第二预设时间段内的交易记录，作为每个预设电子货币交易地址对应的第二目标交易记录；

[0103] 其中，为了能够训练得到能够准确检测欺诈的神经网络模型，可以尽量多的获得每个预设电子货币交易地址的交易记录。而为了获得较多的交易记录，可以设置第二预设时间段对应较长的时长。例如设置第一预设时间段为：当前时刻至十年前当前时刻所对应的时间段，当然并不局限于此。本领域技术人员可以根据实际需要来设置该第二预设时间段，在此不做具体限定。

[0104] 由于具有欺诈行为的电子货币交易地址(即欺诈地址)在接收到汇款后，常常会给其他N个电子货币交易地址转账，而这N个电子货币交易地址又会执行类似转账操作，最后转账至便于体现的钱包地址中。

[0105] 因此，为了能够训练得到能够准确检测欺诈地址的神经网络模型，还可以在确定的预设电子货币交易地址为具有欺诈行为的电子货币交易地址时，分别获取具有欺诈行为的预设电子货币交易地址的第一延伸交易记录和在第二预设时间段内的交易记录，作为相

应预设电子货币交易地址对应的第二目标交易记录。在确定的预设电子货币交易地址为不具有欺诈行为的电子货币交易地址时，分别获得不具有欺诈行为的预设电子货币交易地址在第二预设时间段内的交易记录，作为相应预设电子货币交易地址对应的第二目标交易记录。在确定的预设电子货币交易地址为具有欺诈行为和不具有欺诈行为的电子货币交易地址时，分别获取具有欺诈行为的预设电子货币交易地址的第一延伸交易记录和在第二预设时间段内的交易记录，并分别获得不具有欺诈行为的预设电子货币交易地址在第二预设时间段内的交易记录，作为相应预设电子货币交易地址对应的第二目标交易记录。

[0106] 其中，第一延伸交易记录包括：接收该预设电子货币交易地址汇款的电子货币交易地址的交易记录。

[0107] 相应地，为了保证检测结果的准确性，在利用该神经网络模型检测待进行的交易是否为欺诈交易的过程中，获得目标电子货币交易地址的第二延伸交易记录和在第一预设时间段内的交易记录，作为第一目标交易记录。其中，第二延伸交易记录包括：接收该目标电子货币交易地址汇款的电子货币交易地址的交易记录。这是合理的。

[0108] S203：采用预设编码方式分别对每个第二目标交易记录进行编码，得到每个第二目标交易记录对应的编码结果；

[0109] 其中，预设编码方式可以包括：词向量编码item2vec方式或独热编码one-hot encoding方式。当然并不局限于此。

[0110] S204：利用预设神经网络算法和N个训练样本训练得到神经网络模型，其中，一个训练样本中包括：一个第二目标交易记录对应的编码结果和欺诈标识信息；欺诈标识信息用于：标识该第二目标交易记录对应的预设电子货币交易地为欺诈地址或非欺诈地址。

[0111] 其中，预设神经网络算法包括：循环神经网络算法(Recurrent neural networks，RNN)、深度神经网络算法(Deep Neural Networks，DNN)和卷积神经网络算法(Convolutional Neural Network，CNN)中的任意一项。相应地，当利用循环神经网络算法时，可以训练得到循环神经网络模型；当利用深度神经网络算法时，可以训练得到深度神经网络模型；当利用卷积神经网络算法时，可以训练得到卷积神经网络模型。

[0112] 这些神经网络模型能够计算输入至该神经网络模型的目标编码结果与欺诈地址或非欺诈地址的相似度，从而输出目标编码结果对应的目标电子货币交易地址的欺诈检测结果。从而，可以根据该确定与该目标电子货币交易地址待进行的交易的欺诈检测结果。

[0113] 另外，为了提高神经网络模型输出的欺诈检测结果的准确性，在训练得到神经网络模型之后，还可以利用M个优化样本对所述神经网络模型进行调优，其中，$M \geq 2$。其中，一个优化样本中包括：用于优化模型的电子货币交易地址对应的编码结果和欺诈标识信息。这样，可以对神经网络模型中的参数进行优化，从而提高输出结果的准确性。

[0114] 综上，能够通过本发明实施例提供的神经网络模型确定待进行的交易是否为欺诈交易，从而减少欺诈交易，保护用户的资产安全。

[0115] 相应于上述方法实施例，本发明实施例还提供了一种数据检测装置，参见图3，该装置可以包括：

[0116] 确定单元301，用于确定待进行交易的目标电子货币交易地址；

[0117] 第一获得单元302，用于获得目标电子货币交易地址在第一预设时间段内的交易记录，作为第一目标交易记录；

[0118] 编码单元303，用于采用预设编码方式对第一目标交易记录进行编码，得到目标编码结果；

[0119] 输入单元304，用于将目标编码结果输入至预先构建的神经网络模型；其中，神经网络模型用于：确定目标编码结果对应的目标电子货币交易地址的欺诈检测结果；

[0120] 第二获得单元305，用于获得神经网络模型输出的欺诈检测结果，作为目标电子货币交易地址的欺诈检测结果。

[0121] 应用本发明实施例提供的装置，当需要确定待进行的交易是否为欺诈交易时，可以先确定待进行交易的目标电子货币交易地址。然后，获得该目标电子货币交易地址在第一预设时间段内的交易记录，并将获得的交易记录记为第一目标交易记录。之后，采用预设编码方式对第一目标交易记录进行编码，得到目标编码结果。再将得到目标编码结果输入至神经网络模型中。其中，由于该神经网络模型可以用于确定编码结果对应的电子货币交易地址的欺诈检测结果。因而可以获得该神经网络模型输出的、对于该目标电子货币交易地址的欺诈检测结果。另外，由于当一个电子货币交易地址为欺诈地址时，则与该电子货币交易地址进行的交易很可能为欺诈交易，因而该目标电子货币交易地址的欺诈检测结果也就是待进行的交易的欺诈检测结果。这样，可以通过该欺诈检测结果来确定待进行的交易是否为欺诈交易，从而减少欺诈交易，保护用户的资产安全。

[0122] 可选地，在本发明实施例中，该装置还可以包括构建单元；

[0123] 构建单元用于在输入单元304将目标编码结果输入至预先构建的神经网络模型之前，构建该神经网络模型；

[0124] 该构建单元具体可以包括：

[0125] 确定子模块，用于确定N个预设电子货币交易地址，其中，N个预设电子货币交易地址中包括：具有欺诈行为的电子货币交易地址，和/或，不具有欺诈行为的电子货币交易地址；其中，$N \geq 2$；

[0126] 获得子模块，用于分别获得每个预设电子货币交易地址在第二预设时间段内的交易记录，作为每个预设电子货币交易地址对应的第二目标交易记录；

[0127] 编码子模块，用于采用预设编码方式分别对每个第二目标交易记录进行编码，得到每个第二目标交易记录对应的编码结果；

[0128] 训练子模块，用于利用预设神经网络算法和N个训练样本训练得到神经网络模型，其中，一个训练样本中包括：一个第二目标交易记录对应的编码结果和欺诈标识信息；欺诈标识信息用于：标识该第二目标交易记录对应的预设电子货币交易地为欺诈地址或非欺诈地址。

[0129] 可选地，获得子模块具体用于：

[0130] 分别获得具有欺诈行为的预设电子货币交易地址的第一延伸交易记录和在第二预设时间段内的交易记录，和/或，分别获得不具有欺诈行为的预设电子货币交易地址在第二预设时间段内的交易记录，作为相应预设电子货币交易地址对应的第二目标交易记录；第一延伸交易记录包括：接收预设电子货币交易地址汇款的电子货币交易地址的交易记录。

[0131] 可选地，在本发明实施例中，第一获得单元302具体可以用于：

[0132] 获得目标电子货币交易地址的第二延伸交易记录和在第一预设时间段内的交易

记录，作为第一目标交易记录；第二延伸交易记录包括：接收目标电子货币交易地址汇款的电子货币交易地址的交易记录。

[0133] 可选地，当N个预设电子货币交易地址中包括：具有欺诈行为的电子货币交易地址和不具有欺诈行为的电子货币交易地址时，具有欺诈行为的电子货币交易地址的总数目与不具有欺诈行为的电子货币交易地址的总数目的差值绝对值小于预设数目。

[0134] 可选地，在本发明实施例中，该装置还可以包括：

[0135] 调整单元，用于在训练得到神经网络模型之后，利用M个优化样本对神经网络模型进行调优，得到调优神经网络模型；其中，一个优化样本中包括：用于优化模型的电子货币交易地址对应的编码结果和欺诈标识信息；其中，$M \geq 2$；

[0136] 输入单元具体用于：将所述目标编码结果输入至所述调优神经网络模型。

[0137] 可选地，在本发明实施例中，预设神经网络算法可以包括：循环神经网络算法、深度神经网络算法和卷积神经网络算法中的任意一项。

[0138] 可选地，在本发明实施例中，预设编码方式包括：词向量编码item2vec方式或独热编码one-hot encoding方式。

[0139] 可选地，第一目标交易记录包括至少一个子交易记录，第一子交易记录包括：目标电子货币交易地址、电子货币交易对方地址、目标电子货币交易地址的收支类型、交易金额、目标电子货币交易地址的交易余额和交易时间；第一子交易记录为第一目标交易记录中的任意一个子交易记录；

[0140] 其中，电子货币交易对方地址包括：接收目标电子货币交易地址汇款或汇款至目标电子货币交易地址的电子货币交易地址。

[0141] 相应于上述方法实施例，本发明实施例还提供了一种电子设备，参见图4，该电子设备包括处理器401、通信接口402、存储器403和通信总线404，其中，处理器401，通信接口402，存储器403通过通信总线404完成相互间的通信；

[0142] 存储器403，用于存放计算机程序；

[0143] 处理器401，用于执行存储器403上所存放的程序时，实现上述任一项数据检测方法的方法步骤。

[0144] 当需要确定待进行的交易是否为欺诈交易时，本发明实施例提供的电子设备可以先确定待进行交易的目标电子货币交易地址。然后，获得该目标电子货币交易地址在第一预设时间段内的交易记录，并将获得的交易记录记为第一目标交易记录。之后，采用预设编码方式对第一目标交易记录进行编码，得到目标编码结果。再将得到目标编码结果输入至神经网络模型中。其中，由于该神经网络模型可以用于确定编码结果对应的电子货币交易地址的欺诈检测结果。因此，可以获得该神经网络模型输出的、对于该目标电子货币交易地址的欺诈检测结果。另外，由于当一个电子货币交易地址为欺诈地址时，则与该电子货币交易地址进行的交易很可能为欺诈交易，因而该目标电子货币交易地址的欺诈检测结果也就是待进行的交易的欺诈检测结果。这样，可以通过该欺诈检测结果来确定待进行的交易是否为欺诈交易，从而减少欺诈交易，保护用户的资产安全。

[0145] 相应于上述方法实施例，本发明实施例还提供了一种可读存储介质，该可读存储介质内存储有计算机程序，计算机程序被处理器执行时实现上述任一项数据检测方法的方法步骤。

[0146] 本发明实施例提供的可读存储介质中存储的计算机程序被电子设备的处理器执行后，电子设备可以先确定待进行交易的目标电子货币交易地址。然后，获得该目标电子货币交易地址在第一预设时间段内的交易记录，并将获得的交易记录记为第一目标交易记录。之后，采用预设编码方式对第一目标交易记录进行编码，得到目标编码结果。再将得到目标编码结果输入至神经网络模型中。其中，由于该神经网络模型可以用于确定编码结果对应的电子货币交易地址的欺诈检测结果。因此，可以获得该神经网络模型输出的、对于该目标电子货币交易地址的欺诈检测结果。另外，由于当一个电子货币交易地址为欺诈地址时，则与该电子货币交易地址进行的交易很可能为欺诈交易，因而该目标电子货币交易地址的欺诈检测结果也就是待进行的交易的欺诈检测结果。这样，可以通过该欺诈检测结果来确定待进行的交易是否为欺诈交易，从而减少欺诈交易，保护用户的资产安全。

[0147] 相应于上述方法实施例，本发明实施例还提供了一种包含指令的计算机程序产品，当其在电子设备上运行时，使得电子设备执行：上述任一项数据检测方法的方法步骤。

[0148] 本发明实施例提供的包含指令的计算机程序产品，当其在电子设备上运行时，使得电子设备可以先确定待进行交易的目标电子货币交易地址。然后，获得该目标电子货币交易地址在第一预设时间段内的交易记录，并将获得的交易记录记为第一目标交易记录。之后，采用预设编码方式对第一目标交易记录进行编码，得到目标编码结果。再将得到目标编码结果输入至神经网络模型中。其中，由于该神经网络模型可以用于确定编码结果对应的电子货币交易地址的欺诈检测结果。因此，可以获得该神经网络模型输出的、对于该目标电子货币交易地址的欺诈检测结果。另外，由于当一个电子货币交易地址为欺诈地址时，则与该电子货币交易地址进行的交易很可能为欺诈交易，因而该目标电子货币交易地址的欺诈检测结果也就是待进行的交易的欺诈检测结果。这样，可以通过该欺诈检测结果来确定待进行的交易是否为欺诈交易，从而减少欺诈交易，保护用户的资产安全。

[0149] 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。

[0150] 通信接口用于上述电子设备与其他设备之间的通信。

[0151] 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。

[0152] 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 Processing，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。

[0153] 在本申请实施例中使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本申请。在本申请实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[0154] 应当理解，尽管在本申请实施例中可能采用术语“第一”、“第二”、“第三”等来描述各种连接端口和标识信息等，但这些连接端口和标识信息等不应限于这些术语。这些术语仅用来将连接端口和标识信息等彼此区分开。例如，在不脱离本申请实施例范围的情况下，第一连接端口也可以被称为第二连接端口，类似地，第二连接端口也可以被称为第一连接端口。

[0155] 取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”或“响应于检测”。类似地，取决于语境，短语“如果确定”或“如果检测(陈述的条件或事件)”可以被解释成为“当确定时”或“响应于确定”或“当检测(陈述的条件或事件)时”或“响应于检测(陈述的条件或事件)”。

[0156] 通过以上的实施方式的描述，所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将装置的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。上述描述的系统，装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0157] 在本申请所提供的几个实施例中，应该理解到，所揭露的电子设备，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述模块或单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0158] 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，即可以位于一个地方，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。

[0159] 另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0160] 所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，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)或处理器(processor)执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(Read Only Memory；以下简称：ROM)、随机存取存储器(Random Access Memory；以下简称：RAM)、磁碟或者光盘等各种可以存储程序代码的介质。

[0161] 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。因此，本申请的保护范围应以所述权利要求的保护范围为准。

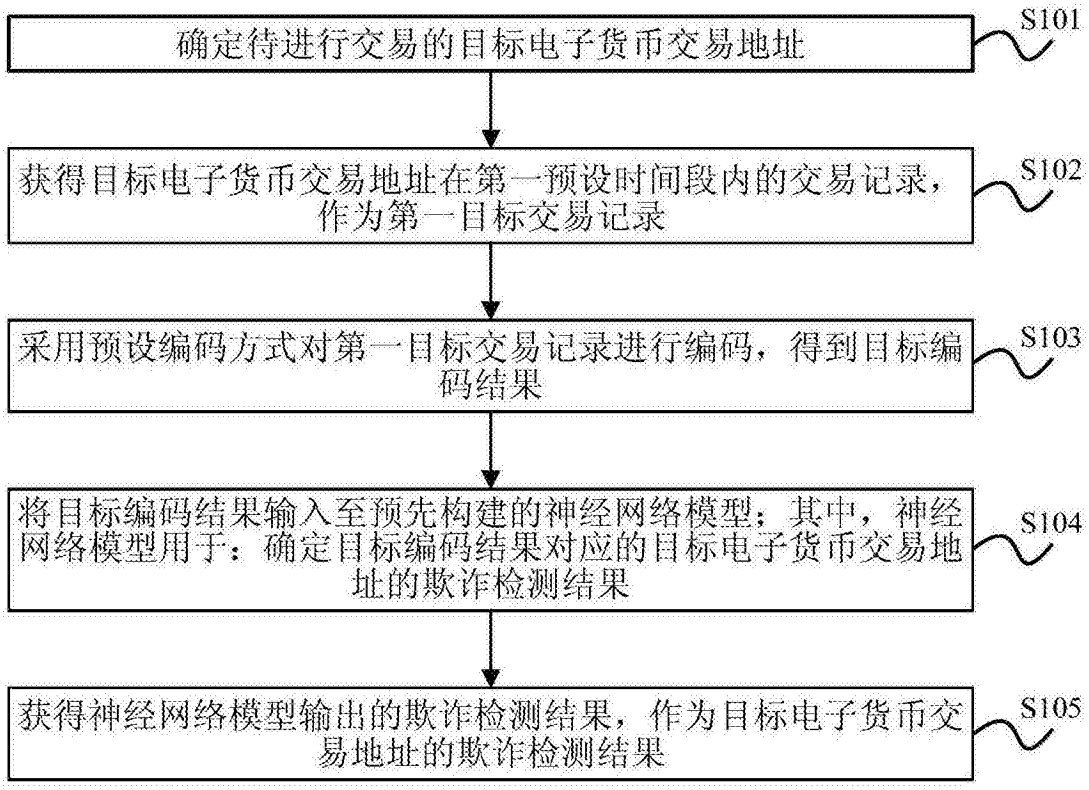

确定待进行交易的目标电子货币交易地址
S101
获得目标电子货币交易地址在第一预设时间段内的交易记录，作为第一目标交易记录
S102
采用预设编码方式对第一目标交易记录进行编码，得到目标编码结果
S103
将目标编码结果输入至预先构建的神经网络模型；其中，神经网络模型用于：确定目标编码结果对应的目标电子货币交易地址的欺诈检测结果
S104
获得神经网络模型输出的欺诈检测结果，作为目标电子货币交易地址的欺诈检测结果
S105

图1

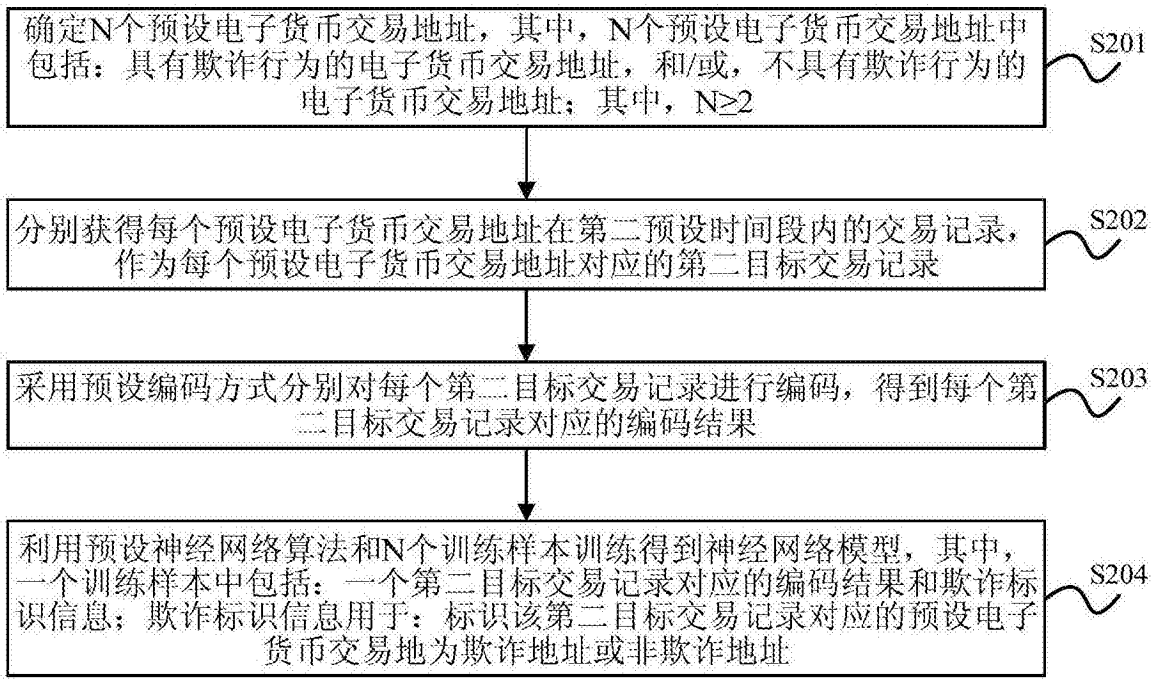

确定N个预设电子货币交易地址，其中，N个预设电子货币交易地址中包括：具有欺诈行为的电子货币交易地址，和/或，不具有欺诈行为的电子货币交易地址；其中，N≥2
S201
分别获得每个预设电子货币交易地址在第二预设时间段内的交易记录，作为每个预设电子货币交易地址对应的第二目标交易记录
S202
采用预设编码方式分别对每个第二目标交易记录进行编码，得到每个第二目标交易记录对应的编码结果
S203
利用预设神经网络算法和N个训练样本训练得到神经网络模型，其中，一个训练样本中包括：一个第二目标交易记录对应的编码结果和欺诈标识信息；欺诈标识信息用于：标识该第二目标交易记录对应的预设电子货币交易地为欺诈地址或非欺诈地址
S204

图2

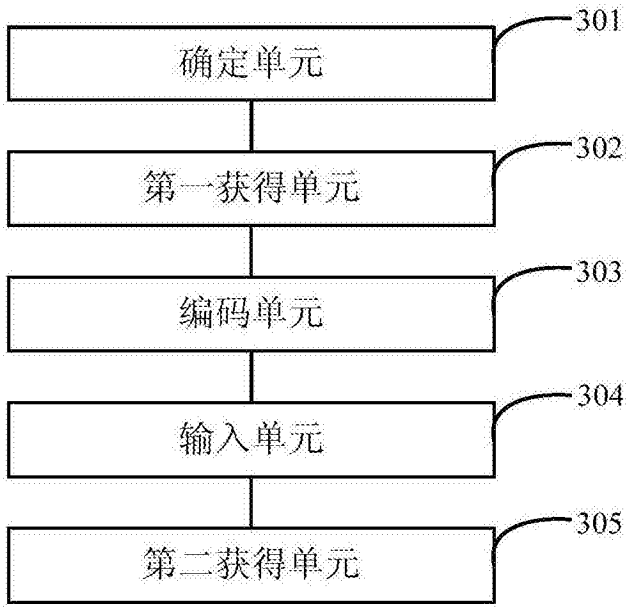

301
确定单元
302
第一获得单元
303
编码单元
304
输入单元
305
第二获得单元

图3

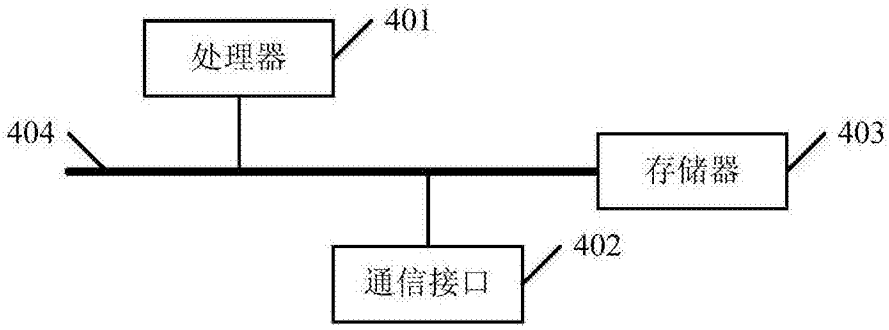

401
处理器
404
403
存储器
402
通信接口

图4