

基于区块链的交易处理方法及装置、电子设备

技术领域

[01] 本说明书一个或多个实施例涉及区块链技术领域，尤其涉及一种基于区块链的交易处理方法及装置、电子设备。

5 背景技术

[02] 区块链技术，也被称之为分布式账本技术，是一种由若干台计算设备共同参与“记账”，共同维护一份完整的分布式数据库的新兴技术。由于区块链技术具有去中心化、公开透明、每台计算设备可以参与数据库记录、并且各计算设备之间可以快速的进行数据同步的特性，利用区块链技术来搭建去中心化系统，并在区块链的分布式数据库中收
10 录各种执行程序进行自动执行，已在众多的领域中广泛的进行应用。

发明内容

- [03] 本申请提出一种基于区块链的交易处理方法，应用于客户端，所述区块链中维护了与用户账户对应的 Nonce 列表；其中，所述 Nonce 列表包括多条 Nonce 记录；所述 Nonce 记录包括所述 Nonce 列表的版本标识和 Nonce 值；所述方法包括：
- 15 [04] 从所述 Nonce 列表中为用户通过所述用户账户发起的目标交易获取可用 Nonce 记录；
- [05] 将获取到的所述可用 Nonce 记录添加至所述目标交易；
- [06] 将所述目标交易发布至所述区块链，以由所述区块链中的节点设备在确认所述可用 Nonce 记录中的版本标识，与所述区块链中维护的所述 Nonce 列表的版本标识不匹配时，向所述客户端返回所述目标交易为无效交易的提示信息；以及，在确认可用 Nonce 记录
20 中的版本标识，与所述区块链中维护的所述 Nonce 列表的版本标识不匹配时版本标识匹配时，进一步将所述可用 Nonce 记录与所述 Nonce 列表中的 Nonce 记录进行匹配对所述目标交易进行重放攻击检测，并在所述目标交易通过重放攻击检测时，受理所述目标交易。
- [07] 可选的，所述从所述 Nonce 列表中为用户通过所述用户账户发起的目标交易获取可用 Nonce 记录之前，还包括：
- 25 [08] 响应于针对所述客户端的初始化指令，获取所述区块链中维护的所述 Nonce 列表，

并将获取到的所述 Nonce 列表在所述客户端本地进行维护。

[09]可选的,所述从所述 Nonce 列表中为用户通过所述用户账户发起的目标交易获取可用 Nonce 记录,包括:

5 [10]从所述客户端本地维护的所述 Nonce 列表中,为用户通过所述用户账户发起的目标交易获取可用 Nonce 记录。

[11]可选的,所述客户端本地维护的所述 Nonce 列表中的 Nonce 记录默认被标记为可用;

[12]所述方法还包括:

[13]在从所述客户端本地维护的所述 Nonce 列表中为所述目标交易获取到了可用 Nonce 记录之后,在所述 Nonce 列表中将所述可用 Nonce 记录标记为不可用。

10 [14]可选的,还包括:

[15]确定是否接收到所述节点设备返回的所述目标交易被受理的通知消息;

[16]如果是,基于预设幅度对所述可用 Nonce 记录中的 Nonce 值进行单调递增,并在所述 Nonce 值单调递增之后,在所述 Nonce 列表中将所述可用 Nonce 记录重新标记为可用。

15 [17]可选的,所述客户端为多线程客户端;所述 Nonce 列表中的 Nonce 记录的数量,指示所述用户账户的交易并发能力。

[18]可选的,所述 Nonce 记录还包括:所述 Nonce 记录的索引标识。

[19]本申请还提出一种基于区块链的交易处理方法,应用于区块链中的节点设备,所述区块链维护了 Nonce 列表集合;所述 Nonce 列表集合包括与若干用户账户对应的 Nonce 列表;其中,所述 Nonce 列表包括多条 Nonce 记录;所述 Nonce 记录包括所述 Nonce 列表的版本标识和 Nonce 值;所述方法包括:

20

[20]接收客户端发送的用户通过用户账户发起的目标交易;其中,所述目标交易被添加了从所述区块链中维护的与所述用户账户对应的 Nonce 列表中获取到的可用 Nonce 记录;

[21]确定所述可用 Nonce 记录中的版本标识,与所述区块链中维护的与所述用户账户对应的 Nonce 列表的版本标识是否匹配;

25 [22]如果所述可用 Nonce 记录中的版本标识,与所述区块链中维护的与所述用户账户对应的 Nonce 列表的版本标识不匹配,向所述客户端返回所述目标交易为无效交易的提示信息;

[23]如果所述可用 Nonce 记录中的版本标识,与所述区块链中维护的与所述用户账户对应的 Nonce 列表的版本标识匹配,进一步将所述可用 Nonce 记录与所述 Nonce 列表中的 Nonce 记录进行匹配对所述目标交易进行重放攻击检测,并在所述目标交易通过重放攻击检测时,受理所述目标交易。

- 5 [24]可选的,所述将所述可用 Nonce 记录与所述 Nonce 列表中的 Nonce 记录进行匹配对所述目标交易进行重放攻击检测,包括:

[25]将所述可用 Nonce 记录与所述区块链中维护的与所述用户账户对应的 Nonce 列表中的 Nonce 记录进行匹配;

- 10 [26]如果所述可用 Nonce 记录与所述 Nonce 列表中的任一目标 Nonce 记录匹配,确定所述目标交易通过重放攻击检测。11. 根据权利要求 10 所述的方法,还包括:

[27]如果所述可用 Nonce 记录与所述 Nonce 列表中的任一目标 Nonce 记录匹配,基于预设幅度对所述目标 Nonce 记录的 Nonce 值进行单调递增;以及,

[28]向所述客户端返回所述目标交易被受理的通知消息。

[29]可选的,所述 Nonce 记录还包括:所述 Nonce 记录的索引标识。

- 15 [30]本说明书还提出一种基于区块链的交易处理装置,应用于客户端,所述区块链中维护了与用户账户对应的 Nonce 列表;其中,所述 Nonce 列表包括多条 Nonce 记录;所述 Nonce 记录包括所述 Nonce 列表的版本标识和 Nonce 值;所述方法包括:

[31]获取模块,从所述 Nonce 列表中为用户通过所述用户账户发起的目标交易获取可用 Nonce 记录;

- 20 [32]添加模块,将获取到的所述可用 Nonce 记录添加至所述目标交易;

[33]发布模块,将所述目标交易发布至所述区块链,以由所述区块链中的节点设备在确认所述可用 Nonce 记录中的版本标识,与所述区块链中维护的所述 Nonce 列表的版本标识不匹配时,向所述客户端返回所述目标交易为无效交易的提示信息;以及,在确认可用 Nonce 记录中的版本标识,与所述区块链中维护的所述 Nonce 列表的版本标识不匹配

- 25 时版本标识匹配时,进一步将所述可用 Nonce 记录与所述 Nonce 列表中的 Nonce 记录进行匹配对所述目标交易进行重放攻击检测,并在所述目标交易通过重放攻击检测时,受理所述目标交易。

[34]可选的,所述获取模块进一步:

[35]在从所述 Nonce 列表中为用户通过所述用户账户发起的目标交易获取可用 Nonce 记录之前,响应于针对所述客户端的初始化指令,获取所述区块链中维护的所述 Nonce 列表,并将获取到的所述 Nonce 列表在所述客户端本地进行维护。

[36]可选的,所述获取模块:

- 5 [37]从所述客户端本地维护的所述 Nonce 列表中,为用户通过所述用户账户发起的目标交易获取可用 Nonce 记录。

[38]可选的,所述客户端本地维护的所述 Nonce 列表中的 Nonce 记录默认被标记为可用;

[39]所述获取模块进一步:

- 10 [40]在从所述客户端本地维护的所述 Nonce 列表中为所述目标交易获取到了可用 Nonce 记录之后,在所述 Nonce 列表中将所述可用 Nonce 记录标记为不可用。

[41]可选的,所述获取模块进一步:

[42]确定是否接收到所述节点设备返回的所述目标交易被受理的通知消息;如果是,基于预设幅度对所述可用 Nonce 记录中的 Nonce 值进行单调递增,并在所述 Nonce 值单调递增之后,在所述 Nonce 列表中将所述可用 Nonce 记录重新标记为可用。

- 15 [43]可选的,所述客户端为多线程客户端;所述 Nonce 列表中的 Nonce 记录的数量,指示所述用户账户的交易并发能力。

[44]可选的,所述 Nonce 记录还包括:所述 Nonce 记录的索引标识。

- 20 [45]本说明书还提出一种基于区块链的交易处理装置,应用于区块链中的节点设备,所述区块链维护了 Nonce 列表集合;所述 Nonce 列表集合包括与若干用户账户对应的 Nonce 列表;其中,所述 Nonce 列表包括多条 Nonce 记录;所述 Nonce 记录包括所述 Nonce 列表的版本标识和 Nonce 值;所述方法包括:

[46]接收模块,接收客户端发送的用户通过用户账户发起的目标交易;其中,所述目标交易被添加了从所述区块链中维护的与所述用户账户对应的 Nonce 列表中获取到的可用 Nonce 记录;

- 25 [47]确认模块,确定所述可用 Nonce 记录中的版本标识,与所述区块链中维护的与所述用户账户对应的 Nonce 列表的版本标识是否匹配;

[48]返回模块,如果所述可用 Nonce 记录中的版本标识,与所述区块链中维护的与所述用户账户对应的 Nonce 列表的版本标识不匹配,向所述客户端返回所述目标交易为无效

交易的提示信息;

[49]检测模块, 如果所述可用 Nonce 记录中的版本标识, 与所述区块链中维护的与所述用户账户对应的 Nonce 列表的版本标识匹配, 进一步将所述可用 Nonce 记录与所述 Nonce 列表中的 Nonce 记录进行匹配对所述目标交易进行重放攻击检测, 并在所述目标交易通过重放攻击检测时, 受理所述目标交易。

[50]可选的, 所述检测模块进一步:

[51]将所述可用 Nonce 记录与所述区块链中维护的与所述用户账户对应的 Nonce 列表中的 Nonce 记录进行匹配;

[52]如果所述可用 Nonce 记录与所述 Nonce 列表中的任一目标 Nonce 记录匹配, 确定所述目标交易通过重放攻击检测。

[53]可选的, 所述检测模块进一步:

[54]如果所述可用 Nonce 记录与所述 Nonce 列表中的任一目标 Nonce 记录匹配, 基于预设幅度对所述目标 Nonce 记录的 Nonce 值进行单调递增; 以及,

[55]向所述客户端返回所述目标交易被受理的通知消息。

[56]可选的, 所述 Nonce 记录还包括: 所述 Nonce 记录的索引标识。

[57]本说明书还提出一种电子设备, 包括:

[58]处理器;

[59]用于存储机器可执行指令的存储器;

[60]其中, 通过读取并执行所述存储器存储的与基于区块链的交易处理的控制逻辑对应的机器可执行指令, 所述处理器被促使:

[61]从区块链中维护的与用户账户对应的 Nonce 列表中, 为用户通过所述用户账户发起的目标交易获取可用 Nonce 记录; 其中, 所述 Nonce 列表包括多条 Nonce 记录; 所述 Nonce 记录包括所述 Nonce 列表的版本标识和 Nonce 值;

[62]将获取到的所述可用 Nonce 记录添加至所述目标交易;

[63]将所述目标交易发布至所述区块链, 以由所述区块链中的节点设备在确认所述可用 Nonce 记录中的版本标识, 与所述区块链中维护的所述 Nonce 列表的版本标识不匹配时, 向所述客户端返回所述目标交易为无效交易的提示信息; 以及, 在确认可用 Nonce 记录

中的版本标识,与所述区块链中维护的所述 Nonce 列表的版本标识不匹配时版本标识匹配时,进一步将所述可用 Nonce 记录与所述 Nonce 列表中的 Nonce 记录进行匹配对所述目标交易进行重放攻击检测,并在所述目标交易通过重放攻击检测时,受理所述目标交易。

5 [64]本说明书还提出一种电子设备,包括:

[65]处理器;

[66]用于存储机器可执行指令的存储器;

[67]其中,通过读取并执行所述存储器存储的与基于区块链的交易处理的控制逻辑对应的机器可执行指令,所述处理器被促使:

10 [68]接收客户端发送的用户通过用户账户发起的目标交易;其中,所述目标交易被添加了从所述区块链中维护的与所述用户账户对应的 Nonce 列表中获取到的可用 Nonce 记录;所述 Nonce 列表包括多条 Nonce 记录;所述 Nonce 记录包括所述 Nonce 列表的版本标识和 Nonce 值;

15 [69]确定所述可用 Nonce 记录中的版本标识,与所述区块链中维护的与所述用户账户对应的 Nonce 列表的版本标识是否匹配;

[70]如果所述可用 Nonce 记录中的版本标识,与所述区块链中维护的与所述用户账户对应的 Nonce 列表的版本标识不匹配,向所述客户端返回所述目标交易为无效交易的提示信息;

20 [71]如果所述可用 Nonce 记录中的版本标识,与所述区块链中维护的与所述用户账户对应的 Nonce 列表的版本标识匹配,进一步将所述可用 Nonce 记录与所述 Nonce 列表中的 Nonce 记录进行匹配对所述目标交易进行重放攻击检测,并在所述目标交易通过重放攻击检测时,受理所述目标交易。

25 [72]通过以上实施例,不仅可以在有效防护重放攻击的基础上,引入交易无效机制,在 Nonce 列表的版本标识发生更新后,及时无效掉携带旧版本标识的交易;而且,还可以在有效防护重放攻击的基础上,提升单账户的交易并发能力。

附图说明

[73]图 1 是一示例性实施例提供的一种对交易进行重放攻击检测的示意图。

[74]图 2 是一示例性实施例提供的一种基于区块链的交易处理方法的流程图。

[75]图 3 是一示例性实施例提供的一种在区块链中维护的 Nonce 列表集合的结构示意图。

[76]图 4 是一示例性实施例提供的另一种对交易进行重放攻击检测的示意图。

[77]图 5 是一示例性实施例提供的一种客户端维护的 Nonce 列表的结构示意图。

5 [78]图 6 是一示例性实施例提供的一种电子设备的结构示意图。

[79]图 7 是一示例性实施例提供的一种基于区块链的交易处理装置的框图。

[80]图 8 是一示例性实施例提供的另一种基于区块链的交易处理装置的框图。

具体实施方式

[81]区块链领域的重放攻击，是指通过在区块链中发布重复的交易，进而导致一笔相同
10 的交易被执行多次，对用户造成损失的攻击行为；

[82]例如，比特币网络中经典的“双花”（double spending）问题，就是一种较为典型的重放攻击行为。一笔转账交易在经过用户私钥的签名许可后，如果被非法节点截获，那么该非法节点可以在该笔交易执行完毕后，基于截获的该笔交易，发起重放攻击，在区块链中重复发布并执行该笔交易，造成一笔转账交易被执行多次，进而对用户造成资
15 金损失。

[83]在示出的一种实施方式中，通常可以在交易中携带一个致密递增的 Nonce 值（致密递增的整数）的方式，来应对针对该笔交易的重放攻击风险；

[84]请参见图 1，图 1 为本说明书示出的一种对交易进行重放攻击检测的示意图。

[85]如图 1 所示，用户在客户端上通过个人的用户账户发起的每笔交易，都可以指定一个 Nonce 值，并使用用户持有的私钥对该笔交易的交易体和指定的 Nonce 值进行签名。
20 其中，签名是对[交易体,Nonce 值]的整体签名,这样可以保障该笔交易中的 Nonce 无法被篡改。

[86]当签名完成后，客户端可以将该笔交易在区块链中进行发布。而区块链中的节点设备，在收到该笔交易后，除了需要验证该笔交易的签名是否合法以外，还需要检测该笔
25 交易中的 Nonce 值，是否与之前已经成功受理的最近一笔交易中的 Nonce 值保持严格的致密递增；如果该笔交易与已经成功受理的最近一笔交易中的 Nonce 值保持致密递增，则可以受理该笔交易；反之，可以认定该比较交易为非法的交易。

[87]例如,假设用户在客户端上通过个人的用户账户 Account1 发起了一笔 Nonce 值为 1 的交易,该笔交易在被区块链成功受理后,用户在客户端上通过 Account1 再次发起交易的时候,必须将该交易中的 Nonce 值指定为 2,才会被区块链中的节点设备认定为一笔合法的交易进行受理。

- 5 [88]相应的,区块链系统会维护用户个人的用户账户的 Nonce 状态,每成功受理 Account1 发起的一笔交易,区块链系统会将该用户账户的 Nonce 值自增 1;区块链中的节点设备在收到客户端发布的一笔交易后,会将该笔交易中的 Nonce 值,与维护的 Nonce 状态中的 Nonce 值进行比较,来判断该笔交易中的 Nonce 值,是否与已经成功受理的最近一笔交易中的 Nonce 值严格递增 1;如果是,则可以受理该笔交易。

- 10 [89]通过以上方式,虽然在某种程度上可以避免交易的重放攻击风险,但对于用户账户而言,需要在前一笔交易被受理后,才可以继续发起下一笔交易,因此单账户的交易并发能力不足,无法在高并发的场景下进行应用。

[90]基于此,在本说明书中,提出一种能够在高并发的场景下进行应用的重放攻击防护方案。

- 15 [91]在实现时,可以在区块链中维护一个 Nonce 列表集合,在该 Nonce 列表集合中,可以包括与若干用户账户对应的 Nonce 列表;而在上述 Nonce 列表中,可以包括若干条 Nonce 记录;每一条 Nonce 记录由上述 Nonce 列表的版本标识和 Nonce 值构成。

- [92]当用户在客户端上通过个人的用户账户发起一笔目标交易后,客户端可以从上述 Nonce 列表为该目标交易获取一条可用 Nonce 记录,并将获取到的该可用 Nonce 记录添
20 加至该目标交易,然后再将该目标交易发布至区块链。

- [93]而区块链中的节点设备在收到该笔目标交易之后,首先可以将上述可用 Nonce 记录中的版本标识,与区块链中维护的与该用户账户对应的上述 Nonce 列表的版本标识进行匹配;如果二者不匹配,可以向客户端返回该目标交易为无效交易的提示信息;如果二者匹配,可以进一步将该笔交易中携带的可用 Nonce 记录,与区块链中维护的与该用户
25 账户对应的上述 Nonce 列表中的 Nonce 记录进行匹配,来对该目标交易进行重放攻击检测;

[94]如果该笔交易中携带的可用 Nonce 记录,与区块链中维护的与该用户账户对应的上述 Nonce 列表中的任一目标 Nonce 记录匹配,则可以确认该笔交易通过重放攻击检测,此时节点设备可以受理该笔目标交易进行执行,并在该笔目标交易被成功受理后,将该

目标 Nonce 记录中的 Nonce 值按照预设幅度进行单调递增；比如，仍然可以将该目标 Nonce 记录中的 Nonce 值自增 1。

[95]通过上述技术方案，一方面，由于在对用户在客户端上通过用户账户发起的每一笔交易进行重放攻击检测之前，会将该笔交易所使用的 Nonce 记录的版本标识与区块链中维护的与该用户账户对应的 Nonce 列表的版本标识进行匹配，来对该笔交易进行无效检测，因此可以在有效避免重放攻击的基础上，引入交易无效机制，在 Nonce 列表的版本标识发生更新后，及时无效掉携带旧版本标识的交易。

[96]另一方面，由于区块链中维护的与用户账户对应的 Nonce 列表中，可以包括多条可用 Nonce 记录；因此，用户可以在客户端上通过用户账户发起多笔包含可用 Nonce 记录，并且能够通过区块链系统的重放攻击检测的合法交易，从而可以显著的提升用户账户的交易并发能力。

[97]下面通过具体实施例并结合具体的应用场景对本说明书进行描述。

[98]请参考图 2，图 2 是本说明书一实施例提供的一种基于区块链的交易处理方法；所述方法执行以下步骤：

15 [99]步骤 202，客户端从区块链中维护的与用户账户对应的 Nonce 列表中，为用户通过所述用户账户发起的目标交易获取可用 Nonce 记录；其中，所述 Nonce 列表包括多条 Nonce 记录；所述 Nonce 记录包括所述 Nonce 列表的版本标识和 Nonce 值；

[100] 步骤 204，客户端将获取到的所述可用 Nonce 记录添加至所述目标交易；

[101] 步骤 206，客户端将所述目标交易发布至所述区块链；

20 [102] 步骤 208，区块链中的节点设备接收客户端发送的所述目标交易，并确定所述可用 Nonce 记录中的版本标识，与所述区块链中维护的与用户账户对应的 Nonce 列表的版本标识是否匹配；

[103] 步骤 210，如果所述可用 Nonce 记录中的版本标识，与所述区块链中维护的与用户账户对应的 Nonce 列表的版本标识不匹配，向所述客户端返回所述目标交易为无效交易的提示信息；

[104] 步骤 212，如果所述可用 Nonce 记录中的版本标识，与所述区块链中维护的与用户账户对应的 Nonce 列表的版本标识匹配，进一步将所述可用 Nonce 记录与所述 Nonce 列表中的 Nonce 记录进行匹配对所述目标交易进行重放攻击检测，并在所述目标

交易通过重放攻击检测时，受理所述目标交易。

[105] 在本说明书所描述的区块链，具体可以包括私有链、共有链以及联盟链等，在本说明书中不进行特别限定。

5 [106] 例如，在一个场景中，上述区块链具体可以是由第三方支付平台的服务器、境内银行服务器、境外银行服务器、以及若干用户节点设备作为成员设备组成的一个联盟链。该联盟链的运营方可以依托于该联盟链，来在线部署诸如基于联盟链的跨境转账、资产转移等在线业务。

[107] 其中，需要说明的是，在本说明书中所描述的交易（Transaction），是指用户通过区块链的客户端创建，并需要最终发布至区块链的分布式数据库中的一笔数据。

10 [108] 区块链中的交易，通常存在狭义的交易以及广义的交易之分。狭义的交易是指用户向区块链发布的一笔价值转移；例如，在传统的比特币区块链网络中，交易可以是用户在区块链中发起的一笔转账。而广义的交易是指用户向区块链发布的一笔具有业务意图的业务数据；例如，运营方可以基于实际的业务需求搭建一个联盟链，依托于联盟链部署一些与价值转移无关的其它类型的在线业务（比如，防伪校验业务、租房业务、
15 车辆调度业务、保险理赔业务、信用服务、医疗服务等），而在这类联盟链中，交易可以是用户在联盟链中发布的一笔具有业务意图的业务消息或者业务请求。

[109] 在本说明书中，可以在区块链中维护一个 Nonce 列表集合，在该 Nonce 列表集合中，可以包括与若干用户账户对应的 Nonce 列表。在上述 Nonce 列表中，均可以包括多条 Nonce 记录。而每一条 Nonce 记录可以包括辅助参数和 Nonce 值。

20 [110] 也即，在本说明书中，上述 Nonce 记录具体可以是一条由包含 Nonce 值在内的多个字段构成的复合结构。

[111] 在实现时，上述区块链的运营方，可以预先为每一个用户账户分配可用的 Nonce 值，并在分配的可用的 Nonce 值的基础上，为每一个 Nonce 值设置对应的辅助字段，再基于每一个可用的 Nonce 值和对应的辅助字段，来构造出多条 Nonce 记录；

25 [112] 然后，可以基于生成的多条 Nonce 记录为该用户账户构造 Nonce 列表；最后，可以基于为各个用户账户构造的 Nonce 列表，创建上述 Nonce 列表集合，并将上述 Nonce 列表集合发布至上述区块链，由上述区块链中的节点设备进行共识处理，并在共识通过后，将上述 Nonce 列表集合存储在上述区块链的分布式数据进行存储和维护。

[113] 其中，需要说明的是，上述辅助参数的具体参数内容，在本说明书中不进行特

别限定；在实际应用中，上述辅助参数，具体可以包括上述区块链的运营方基于实际的需求，在用户账户可用的 Nonce 值的基础上扩展出的任意形式的参数；或者参数组合。

[114] 也即，在实际应用中，上述辅助参数中所能包含的参数数量以及类别，可以不固定；可以在 Nonce 值的基础上扩展出任意一种参数来作为辅助参数；也可以在 Nonce 5 值的基础上扩展出多种参数进行组合来作为辅助参数。

[115] 在本说明书中，上述 Nonce 列表中的 Nonce 记录中的辅助参数，具体可以包括上述 Nonce 列表的版本标识（比如版本编号）；其中，上述版本标识，具体用于表示上述 Nonce 列表当前的版本；对于上述 Nonce 列表集合中的与各个用户账户对应的 Nonce 列表而言，上述版本标识可以相同，也可以不相同。

10 [116] 在实际应用中，上述 Nonce 列表的版本标识，可以由区块链的运营方在上述 Nonce 列表满足了特定的版本更换条件时，进行修改更新；或者，也可以由用户通过客户端向区块链发布交易的形式，进行手动更新。

[117] 在实际应用中，如果上述 Nonce 列表的版本标识发生更新，此时已经在区块链中发布，但还尚未被受理的交易（携带上述 Nonce 列表更新前的版本标识），则可能会
15 由于所携带的上述 Nonce 列表的版本标识（更新前的旧版本标识），与上述 Nonce 列表更新后的版本标识不匹配，而被认定为无效交易，无法被区块链系统进行交易受理。

[118] 通过这种方式，使得区块链的运营方或者用户，可以通过对上述 Nonce 列表的版本标识进行更新的方式，将一些已经发布但还尚未被受理的交易设置为无效状态，从而可以及时终止一些长时间无法被受理的交易。

20 [119] 在示出的一种实施方式中，上述 Nonce 列表中的 Nonce 记录中的辅助参数，除了可以包括上述 Nonce 列表的版本标识以外，还可以进一步包括上述 Nonce 记录的索引标识（比如索引编号）。其中，上述索引标识，具体用于表示 Nonce 记录在 Nonce 列表中的顺序以及位置。

[120] 例如，请参见图 3，以上述 Nonce 列表中的 Nonce 记录中的辅助参数，同时包
25 含上述 Nonce 列表的版本标识和上述 Nonce 记录的索引标识为例，此时上述 Nonce 记录具体可以是一个 Version（版本标识）、Index（索引标识）、Value（Nonce 值）等字段组成的复合结构。在这种情况下，在区块链中维护的 Nonce 列表集合，可以表示成如图 3 所示出的形式。

[121] 其中，上述 Nonce 记录以及上述 Nonce 记录中的 Nonce 值和上述辅助参数的具

体的字节长度,在本说明书中不进行特别限定;在实际应用中,可以基于上述区块链的运营方的实际需求,进行灵活的设定(比如,运营方可以通过所占用的字节长度,来控制 Nonce 值以及辅助参数的具体取值范围);

5 [122] 例如,在一种实现方式中,上述 Nonce 记录具体可以是一个 16 字节组成的复合结构;其中,4 字节表示 Version (版本标识)、4 字节表示 Index (索引标识)、8 字节表示 Value (Nonce 值)。

[123] 通过在 Nonce 值的基础上扩展出多种参数进行组合来作为辅助参数,使得上述 Nonce 表中的 Nonce 记录能够涵盖丰富的取值字段,从而可以降低上述 Nonce 表中的多条 Nonce 记录由于取值相同发生冲突的概率;

10 [124] 例如,两条由 Version (版本标识)和 Value (Nonce 值)构成的总长度为 12 字节的 Nonce 记录完全相同发生冲突的概率,会远低于,两条由 Version (版本标识)、Index (索引标识)和 Value (Nonce 值)构成的总长度为 16 字节的 Nonce 记录完全相同发生冲突的概率。

15 [125] 在本说明书中,上述客户端具体可以是一个多线程客户端;也即,客户端可以同时启用多个线程,每一个线程都可以独立运行,从而用户可以通过调用客户端的多个线程,通过个人的用户账户来同时发起多笔交易。

[126] 请参见图 4,当用户在客户端上调用客户端启用的线程,通过个人的用户账户发起一笔目标交易后,该线程可以从区块链上维护的与该用户账户对应的上述 Nonce 列表中,为该目标交易获取一条可用 Nonce 记录。

20 [127] 由于上述 Nonce 列表中包括多条 Nonce 记录,使得客户端启动的多线程均能够从上述 Nonce 列表中为发起的交易获取到可用 Nonce 记录,进而用户可以使用个人的用户账户通过上述客户端同时发起多笔交易;因此,在本说明书中,上述 Nonce 列表中的 Nonce 记录的数量,实际上可以用于指示用户个人的用户账户的交易并发能力。比如,上述 Nonce 列表包括 4 条 Nonce 记录,那么用户可以通过用户账户同时发起 4 笔交易。

25 [128] 基于这一点,在实际应用中,区块链的运营方,可以基于客户端自身的性能,来灵活的为上述 Nonce 列表指定所包含的 Nonce 记录的数量;或者,客户端可以向区块链系统主动上报自身的性能,由区块链的运营方来灵活的指定上述 Nonce 列表所包含的 Nonce 记录的数量;

[129] 例如,假设客户端的性能决定,该客户端可以同时启动 4 个线程来发起交易,

那么在为登录该客户端的用户账户创建上述 Nonce 列表时，可以为该 Nonce 列表添加 4 条可用 Nonce 记录。

[130] 在示出的一种实施方式中，客户端可以在初始化阶段，预先将区块链上维护的上述 Nonce 列表“下载”到本地进行维护；

5 [131] 例如，在实现时，客户端在启动运行，或者与区块链中的节点设备之间的连接断开需要重新进行连接时，通过都需要进行初始化操作。在这种情况下，当客户端收到用户触发的针对该客户端的初始化指令（比如启动指令、重连指令等）时，则可以响应该初始化指令，与区块链中的节点设备建立连接，并基于该连接访问区块链的分布式数据库，获取区块链中维护的上述 Nonce 列表，然后可以将获取到的上述 Nonce 列表本地
10 进行存储和维护。

[132] 在这种情况下，当客户端上启用的线程，需要为该目标交易获取可用 Nonce 记录时，可以直接从本地维护的上述 Nonce 列表中获取可用 Nonce 记录。

[133] 通过这种方式，可以避免与区块链上的节点设备进行数据交互，从区块链中维护的上述 Nonce 列表中读取数据，为该目标交易获取可用 Nonce 记录，可以提升客户端
15 的处理性能。

[134] 在示出的一种实施方式中，对于客户端在本地维护的上述 Nonce 列表，可以由客户端为该 Nonce 列表中的 Nonce 记录，均默认添加一个表示“可用”的标记。

[135] 例如，请参见图 5，仍以上述 Nonce 记录为图 4 中示出的 16 字节组成的复合结构为例，可以为 Nonce 列表中的 Nonce 记录，扩展出一个 1 字节的 Available 字段；其中，当 Available 字段取值为 T 时，表示该条 Nonce 记录“可用”；当 Available 字段取
20 值为 F 时，表示该条 Nonce 记录“不可用”。

[136] 一方面，当客户端上启用的线程，在从客户端本地维护的上述 Nonce 列表中为用户发起的目标交易获取可用 Nonce 记录时，可以从上述 Nonce 列表中所有被标记为“可用”的 Nonce 记录来随机选择一个 Nonce 记录作为可用 Nonce 记录。

25 [137] 另一方面，当客户端上启用的线程，从客户端本地维护的上述 Nonce 列表中为用户发起的目标交易获取到可用 Nonce 记录之后，可以对该可用 Nonce 记录携带的标记进行修改更新，为该可用 Nonce 记录重新添加一个表示“不可用”的标记，以将该可用 Nonce 记录标记为不可用。

[138] 在本说明书中，当客户端上启用的线程，为上述目标交易获取到可用 Nonce 记

录之后, 可以将获取到的可用 Nonce 记录添加至上述目标交易;

[139] 例如, 请继续参见图 4, 客户端在为上述目标交易获取到可用 Nonce 记录之后, 可以对上述目标交易的交易体, 和上述可用 Nonce 记录进行打包, 然后提示用户基于持有的私钥对打包后的 [交易体, Nonce 记录] 进行整体签名, 这样可以保障该笔交易中的 Nonce 记录无法被篡改。

[140] 进一步的, 当客户端上启用的线程, 将获取到的可用 Nonce 记录添加至上述目标交易之后, 客户端可以将上述目标交易发布至区块链;

[141] 例如, 将上述目标交易发布至该客户端接入的节点设备, 或者将该目标交易在区块链中进行广播发布; 其中, 客户端将上述目标交易发布至区块链的具体方式, 通常取决于区块链所采用的共识机制, 在本说明书中不进行特别限定。

[142] 而当区块链中的节点设备在收到客户端发布的上述目标交易之后, 首先可以在区块链采用的共识算法, 发起针对该目标交易的共识处理;

[143] 其中, 区块链采用的共识算法, 以及基于共识算法对上述目标交易的共识处理过程, 在本说明书中不再进行详述, 本领域技术人员在将本说明书记载的技术方案付诸实现时, 可以参考相关技术中的记载。

[144] 当上述目标交易共识通过后, 此时上述区块链中的节点设备, 可以进一步发起针对该目标交易的合法性检测。

[145] 其中, 在本说明书中, 针对上述目标交易的合法性检测至少可以包括, 针对该目标交易携带的签名的合法性检测、针对该目标交易的有效性检测、以及, 针对上述目标交易的重放攻击检测。

[146] 在实现时, 上述区块链中的节点设备首先可以基于与上述用户持有的私钥对应的公钥, 对该目标交易的签名进行验证; 如果该目标交易的签名失败, 可以认定该目标交易为不合法的交易, 上述节点设备可以直接通过客户端向用户返回交易执行失败的提示消息。

[147] 如果目标交易的签名验证通过, 此时上述节点设备, 可以将该目标交易中携带的可用 Nonce 记录中的版本标识, 与区块链中维护的与该用户个人的用户账户对应的 Nonce 列表的版本标识进行匹配, 以确定该目标交易中携带的 Nonce 列表的版本标识, 与区块链中维护的与该用户个人的用户账户对应的 Nonce 列表的版本标识是否相同;

- [148] 如果该目标交易中携带的可用 Nonce 记录中的版本标识, 与区块链中维护的与该用户个人的用户账户对应的 Nonce 列表的版本标识并不匹配, 表明当前区块链中维护的与该用户个人的用户账户对应的 Nonce 列表的版本标识可能已经发生更新; 此时, 该节点设备可以认定该目标交易为无效交易, 向客户端返回一个该目标交易为无效交易的提示信息。
- [149] 如果该目标交易中携带的可用 Nonce 记录中的版本标识, 与区块链中维护的与该用户个人的用户账户对应的 Nonce 列表的版本标识匹配, 此时该节点设备可以认定该目标交易有效交易, 可以进一步基于该目标交易中携带的可用 Nonce 记录, 和区块链中维护的与该用户个人的用户账户对应的 Nonce 列表, 针对该目标交易进行重放攻击检测。
- 10 [150] 一方面, 请继续参见图 4, 上述节点设备可以将上述目标交易中携带的 Nonce 记录, 从区块链上维护的与该用户账户对应的 Nonce 列表中的 Nonce 记录逐一进行匹配; 如果上述目标交易中携带的 Nonce 记录, 与上述 Nonce 列表中的任一目标 Nonce 记录匹配, 可以确定该目标交易通过重放攻击检测; 在这种情况下, 该节点设备可以受理该目标交易。
- 15 [151] 另一方面, 当上述目标交易被受理后, 该节点设备可以基于预设幅度对上述目标 Nonce 记录中的 Nonce 值进行单调递增; 其中, 上述预设幅度可以基于实际需求进行自定义;
- [152] 例如, 上述预设幅度仍然可以是 1, 上述节点设备可以在上述目标交易被受理后, 将在上述 Nonce 列表中匹配到的上述目标 Nonce 记录中的 Nonce 值自增 1。
- 20 [153] 通过这种方式, 如果上述目标交易在被受理之后, 又再次在区块链中进行了重复发布, 由于上述 Nonce 列表中与该目标交易携带的可用 Nonce 记录匹配的目标 Nonce 记录中的 Nonce 值, 已经发生了更新, 该重复发布的该目标交易在重放攻击检测阶段, 将无法在上述 Nonce 列表中匹配到对应的 Nonce 记录; 因此, 该重复发布的目标交易将不会被再次受理, 从而可以有效的避免通过在区块链中重复发布该目标交易进行重放攻击。
- 25 [154] 在示出的一种实施方式中, 当上述目标交易被受理后, 可以向上述客户端返回上述目标交易被受理的通知消息; 而客户端在将上述目标交易发布至区块链后, 可以确定是否接收到节点设备返回的该目标交易被受理的通知消息。
- [155] 如果确认收到上述目标交易被受理的通知消息:

[156] 一方面，可以基于预设幅度，对从客户端本地维护的上述 Nonce 列表中为上述目标交易获取到的上述可用 Nonce 记录中的 Nonce 值进行单调递增；比如，将在上述可用 Nonce 记录中的 Nonce 值也自增 1，以与区块链中维护的上述 Nonce 列表保持内容同步。

- 5 [157] 另一方面，由于此前该可用 Nonce 记录已经被标记为了“不可用”；因此，在基于预设幅度，对该可用 Nonce 记录中的 Nonce 值进行单调递增后，可以将该可用 Nonce 记录的 Available 字段的取值，置位为“T”。

- 10 [158] 通过以上技术方案，一方面，由于在对用户在客户端上通过用户账户发起的每一笔交易进行重放攻击检测之前，会将该笔交易所使用的 Nonce 记录的版本标识与区块链中维护的与该用户账户对应的 Nonce 列表的版本标识进行匹配，来对该笔交易进行无效检测，因此可以在有效避免重放攻击的基础上，引入交易无效机制，在 Nonce 列表的版本标识发生更新后，及时无效掉携带旧版本标识的交易。

- 15 [159] 另一方面，由于区块链中维护的与用户账户对应的 Nonce 列表中，可以包括多条可用 Nonce 记录；因此，用户可以在客户端上通过用户账户发起多笔包含可用 Nonce 记录，并且能够通过区块链系统的重放攻击检测的合法交易，从而可以显著的提升用户账户的交易并发能力。

- 20 [160] 与上述方法实施例相对应，本说明书还提供了一种基于区块链的交易处理装置的实施例。本说明书的基于区块链的交易处理装置的实施例可以应用在电子设备上。装置实施例可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现。以软件实现为例，作为一个逻辑意义上的装置，是通过其所在电子设备的处理器将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言，如图 6 所示，为本说明书的基于区块链的交易处理装置所在电子设备的一种硬件结构图，除了图 6 所示的处理器、内存、网络接口、以及非易失性存储器之外，实施例中装置所在的电子设备通常根据该电子设备的实际功能，还可以包括其他硬件，对此不再赘述。

- 25 [161] 图 7 是本说明书一示例性实施例示出的一种基于区块链的交易处理装置的框图。

[162] 请参考图 7，所述基于区块链的交易处理装置 70 可以应用在前述图 6 所示的电子设备中，包括有：获取模块 701、添加模块 702 和发布模块 703。

[163] 获取模块 701，从区块链中维护的与用户账户对应的 Nonce 列表中，为用户通过所述用户账户发起的目标交易获取可用 Nonce 记录；其中，所述 Nonce 列表包括多条

Nonce 记录; 所述 Nonce 记录包括辅助参数和 Nonce 值;

[164] 添加模块 702, 将获取到的所述可用 Nonce 记录添加至所述目标交易;

[165] 发布模块 703, 将所述目标交易发布至所述区块链, 以由所述区块链中的节点设备在确认所述可用 Nonce 记录中的版本标识, 与所述区块链中维护的所述 Nonce 列表的版本标识不匹配时, 向所述客户端返回所述目标交易为无效交易的提示信息; 以及, 在确认可用 Nonce 记录中的版本标识, 与所述区块链中维护的所述 Nonce 列表的版本标识不匹配时版本标识匹配时, 进一步将所述可用 Nonce 记录与所述 Nonce 列表中的 Nonce 记录进行匹配对所述目标交易进行重放攻击检测, 并在所述目标交易通过重放攻击检测时, 受理所述目标交易。

10 [166] 在本实施例中, 所述获取模块 701 进一步:

[167] 在从所述 Nonce 列表中为用户通过所述用户账户发起的目标交易获取可用 Nonce 记录之前, 响应于针对所述客户端的初始化指令, 获取所述区块链中维护的所述 Nonce 列表, 并将获取到的所述 Nonce 列表在所述客户端本地进行维护。

[168] 在本实施例中, 所述获取模块 701:

15 [169] 从所述客户端本地维护的所述 Nonce 列表中, 为用户通过所述用户账户发起的目标交易获取可用 Nonce 记录。

[170] 在本实施例中, 所述客户端本地维护的所述 Nonce 列表中的 Nonce 记录默认被标记为可用;

[171] 所述获取模块 701 进一步:

20 [172] 在从所述客户端本地维护的所述 Nonce 列表中为所述目标交易获取到了可用 Nonce 记录之后, 在所述 Nonce 列表中将所述可用 Nonce 记录标记为不可用。

[173] 在本实施例中, 所述获取模块 701 进一步:

[174] 确定是否接收到所述节点设备返回的所述目标交易被受理的通知消息; 如果是, 基于预设幅度对所述可用 Nonce 记录中的 Nonce 值进行单调递增, 并在所述 Nonce 值单调递增之后, 在所述 Nonce 列表中将所述可用 Nonce 记录重新标记为可用。

[175] 在本实施例中, 所述客户端为多线程客户端; 所述 Nonce 列表中的 Nonce 记录的数量, 指示所述用户账户的交易并发能力。

[176] 在本实施例中, 所述 Nonce 记录还包括: 所述 Nonce 记录的索引标识。

[177] 图 8 是本说明书一示例性实施例示出的另一种基于区块链的交易处理装置的框图。

[178] 请参考图 8, 所述基于区块链的交易处理装置 80 也可以应用在前述图 6 所示的电子设备中, 包括有: 接收模块 801、确认模块 802、返回模块 803 和检测模块 804。

5 [179] 接收模块 801, 接收客户端发送的用户通过用户账户发起的目标交易; 其中, 所述目标交易被添加了从所述区块链中维护的与所述用户账户对应的 Nonce 列表中获取到的可用 Nonce 记录; 所述 Nonce 列表包括多条 Nonce 记录; 所述 Nonce 记录包括所述 Nonce 列表的版本标识和 Nonce 值和 Nonce 值;

10 [180] 确认模块 802, 确定所述可用 Nonce 记录中的版本标识, 与所述区块链中维护的与所述用户账户对应的 Nonce 列表的版本标识是否匹配;

[181] 返回模块 803, 如果所述可用 Nonce 记录中的版本标识, 与所述区块链中维护的与所述用户账户对应的 Nonce 列表的版本标识不匹配, 向所述客户端返回所述目标交易为无效交易的提示信息;

15 [182] 检测模块 804, 如果所述可用 Nonce 记录中的版本标识, 与所述区块链中维护的与所述用户账户对应的 Nonce 列表的版本标识匹配, 进一步将所述可用 Nonce 记录与所述 Nonce 列表中的 Nonce 记录进行匹配对所述目标交易进行重放攻击检测, 并在所述目标交易通过重放攻击检测时, 受理所述目标交易。

[183] 在本实施例中, 所述检测模块 804 进一步:

20 [184] 将所述可用 Nonce 记录与所述区块链中维护的与所述用户账户对应的 Nonce 列表中的 Nonce 记录进行匹配;

[185] 如果所述可用 Nonce 记录与所述 Nonce 列表中的任一目标 Nonce 记录匹配, 确定所述目标交易通过重放攻击检测。

[186] 在本实施例中, 所述检测模块 804 进一步:

25 [187] 如果所述可用 Nonce 记录与所述 Nonce 列表中的任一目标 Nonce 记录匹配, 基于预设幅度对所述目标 Nonce 记录的 Nonce 值进行单调递增; 以及,

[188] 向所述客户端返回所述目标交易被受理的通知消息。

[189] 在本实施例中, 所述 Nonce 记录还包括: 所述 Nonce 记录的索引标识。

[190] 上述装置中各个模块的功能和作用的实现过程具体详见上述方法中对应步骤的

实现过程，在此不再赘述。

[191] 对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，作为模块显示的部件可以是或者也可以不是物理模块，即可以位于一个地方，或者也可以分布到多个网络模块上。可以根据实际的需要选择其中的部分或者全部模块来实现本说明书方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[192] 上述实施例阐明的系统、装置、模块或模块，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机，计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

[193] 与上述方法实施例相对应，本说明书还提供了一种电子设备的实施例。该电子设备包括：处理器以及用于存储机器可执行指令的存储器；其中，处理器和存储器通常通过内部总线相互连接。在其他可能的实现方式中，所述设备还可能包括外部接口，以能够与其他设备或者部件进行通信。

[194] 在本实施例中，通过读取并执行所述存储器存储的与基于区块链的交易处理的控制逻辑对应的机器可执行指令，所述处理器被促使：

[195] 从区块链中维护的与用户账户对应的 Nonce 列表中，为用户通过所述用户账户发起的目标交易获取可用 Nonce 记录；其中，所述 Nonce 列表包括多条 Nonce 记录；所述 Nonce 记录包括所述 Nonce 列表的版本标识和 Nonce 值；

[196] 将获取到的所述可用 Nonce 记录添加至所述目标交易；

[197] 将所述目标交易发布至所述区块链，以由所述区块链中的节点设备在确认所述可用 Nonce 记录中的版本标识，与所述区块链中维护的所述 Nonce 列表的版本标识不匹配时，向所述客户端返回所述目标交易为无效交易的提示信息；以及，在确认可用 Nonce 记录中的版本标识，与所述区块链中维护的所述 Nonce 列表的版本标识不匹配时版本标识匹配时，进一步将所述可用 Nonce 记录与所述 Nonce 列表中的 Nonce 记录进行匹配对所述目标交易进行重放攻击检测，并在所述目标交易通过重放攻击检测时，受理所述目标交易。

[198] 在本实施例中，通过读取并执行所述存储器存储的与基于区块链的交易处理的控制逻辑对应的机器可执行指令，所述处理器被促使：

[199] 从所述 Nonce 列表中为用户通过所述用户账户发起的目标交易获取可用 Nonce 记录之前，响应于针对所述客户端的初始化指令，获取所述区块链中维护的所述 Nonce
5 列表，并将获取到的所述 Nonce 列表在所述客户端本地进行维护。

[200] 在本实施例中，通过读取并执行所述存储器存储的与基于区块链的交易处理的控制逻辑对应的机器可执行指令，所述处理器被促使：

[201] 从所述客户端本地维护的所述 Nonce 列表中，为用户通过所述用户账户发起的目标交易获取可用 Nonce 记录。

10 [202] 在本实施例中，所述客户端本地维护的所述 Nonce 列表中的 Nonce 记录默认被标记为可用；

[203] 通过读取并执行所述存储器存储的与基于区块链的交易处理的控制逻辑对应的机器可执行指令，所述处理器被促使：

[204] 在从所述客户端本地维护的所述 Nonce 列表中为所述目标交易获取到了可用
15 Nonce 记录之后，在所述 Nonce 列表中将所述可用 Nonce 记录标记为不可用。

[205] 在本实施例中，通过读取并执行所述存储器存储的与基于区块链的交易处理的控制逻辑对应的机器可执行指令，所述处理器被促使：

[206] 确定是否接收到所述节点设备返回的所述目标交易被受理的通知消息；

[207] 如果是，基于预设幅度对所述可用 Nonce 记录中的 Nonce 值进行单调递增，并在
20 所述 Nonce 值单调递增之后，在所述 Nonce 列表中将所述可用 Nonce 记录重新标记为可用。

[208] 与上述方法实施例相对应，本说明书还提供了另一种电子设备的实施例。该电子设备包括：处理器以及用于存储机器可执行指令的存储器；其中，处理器和存储器通常通过内部总线相互连接。在其他可能的实现方式中，所述设备还可能包括外部接口，
25 以能够与其他设备或者部件进行通信。

[209] 在本实施例中，通过读取并执行所述存储器存储的与基于区块链的交易处理的控制逻辑对应的机器可执行指令，所述处理器被促使：

[210] 接收客户端发送的用户通过用户账户发起的目标交易；其中，所述目标交易被

添加了从所述区块链中维护的与所述用户账户对应的 Nonce 列表中获取到的可用 Nonce 记录；所述 Nonce 列表包括多条 Nonce 记录；所述 Nonce 记录包括所述 Nonce 列表的版本标识和 Nonce 值；

5 [211] 确定所述可用 Nonce 记录中的版本标识，与所述区块链中维护的与所述用户账户对应的 Nonce 列表的版本标识是否匹配；

[212] 如果所述可用 Nonce 记录中的版本标识，与所述区块链中维护的与所述用户账户对应的 Nonce 列表的版本标识不匹配，向所述客户端返回所述目标交易为无效交易的提示信息；

10 [213] 如果所述可用 Nonce 记录中的版本标识，与所述区块链中维护的与所述用户账户对应的 Nonce 列表的版本标识匹配，进一步将所述可用 Nonce 记录与所述 Nonce 列表中的 Nonce 记录进行匹配对所述目标交易进行重放攻击检测，并在所述目标交易通过重放攻击检测时，受理所述目标交易。

[214] 在本实施例中，通过读取并执行所述存储器存储的与基于区块链的交易处理的控制逻辑对应的机器可执行指令，所述处理器被促使：

15 [215] 将所述可用 Nonce 记录与所述区块链中维护的与所述用户账户对应的 Nonce 列表中的 Nonce 记录进行匹配；

[216] 如果所述可用 Nonce 记录与所述 Nonce 列表中的任一目标 Nonce 记录匹配，确定所述目标交易通过重放攻击检测。

20 [217] 在本实施例中，通过读取并执行所述存储器存储的与基于区块链的交易处理的控制逻辑对应的机器可执行指令，所述处理器被促使：

[218] 如果所述可用 Nonce 记录与所述 Nonce 列表中的任一目标 Nonce 记录匹配，基于预设幅度对所述目标 Nonce 记录的 Nonce 值进行单调递增；以及，

[219] 向所述客户端返回所述目标交易被受理的通知消息。

25 [220] 本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本说明书的其它实施方案。本说明书旨在涵盖本说明书的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本说明书的一般性原理并包括本说明书未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本说明书的真正范围和精神由下面的权利要求指出。

[221] 应当理解的是，本说明书并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本说明书的范围仅由所附的权利要求来限制。

[222] 以上所述仅为本说明书的较佳实施例而已，并不用以限制本说明书，凡在本说明书的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书保护的5 范围之内。