

权利要求书

1. 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:
 - 5 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; 将获取到的所述可用 Nonce 记录添加至所述目标交易; 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;
 - 10 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。
2. 根据权利要求 1 所述的方法, 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:
 - 15 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。
3. 根据权利要求 2 所述的方法, 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:
 - 20 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。
4. 根据权利要求 3 所述的方法, 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; 所述方法还包括:
 - 25 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。
5. 根据权利要求 4 所述的方法, 还包括:
 - 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。
 - 30

6. 根据权利要求 1 所述的方法, 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。

7. 根据权利要求 1 所述的方法, 所述 Nonce 记录还包括: 所述 Nonce 记录的索引标识。

5 8. 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:

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
10 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;

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;

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
15 信息;

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。

20 9. 根据权利要求 8 所述的方法, 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:

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;

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
25 所述目标交易通过重放攻击检测。

10. 根据权利要求 9 所述的方法, 还包括:

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,

向所述客户端返回所述目标交易被受理的通知消息。

30 11. 根据权利要求 9 所述的方法, 所述 Nonce 记录还包括: 所述 Nonce 记录的索引标识。

12. 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:

5 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;

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;

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。

13. 根据权利要求 12 所述的装置,所述获取模块进一步:
15 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。

14. 根据权利要求 13 所述的装置,所述获取模块:
20 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。

15. 根据权利要求 14 所述的装置,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;

所述获取模块进一步:

25 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。

16. 根据权利要求 15 所述的装置,所述获取模块进一步:

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。

30 17. 根据权利要求 12 所述的装置,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. 根据权利要求 17 所述的装置, 所述 Nonce 记录还包括: 所述 Nonce 记录的索引标识。

19. 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;
- 5 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:

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;

- 10 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;

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;

- 15 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。

20. 根据权利要求 19 所述的装置, 所述检测模块进一步:

- 20 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;

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。

21. 根据权利要求 20 所述的装置, 所述检测模块进一步:

- 25 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,

向所述客户端返回所述目标交易被受理的通知消息。

22. 根据权利要求 21 所述的装置, 所述 Nonce 记录还包括: 所述 Nonce 记录的索引标识。

- 30 23. 一种电子设备, 包括:
处理器;

用于存储机器可执行指令的存储器;

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:

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
5 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;

将获取到的所述可用 Nonce 记录添加至所述目标交易;

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,
10 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。

15 24. 一种电子设备,包括:

处理器;

用于存储机器可执行指令的存储器;

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
的机器可执行指令,所述处理器被促使:

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;
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;

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
25 应的 Nonce 列表的版本标识是否匹配;

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;

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
30 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。