

权利要求书

1. 一种跨链数据的可信管理方法，应用于中继器，所述中继器上加载有可信执行环境，以在所述可信执行环境中实施如下步骤：
- 根据来自第一区块链的跨链请求，从作为请求对象的第二区块链调用相应的跨链数据，其中所述中继器配置有所述第二区块链的客户端；
- 加载预配置的管理规则集，以根据所述管理规则集包含的管理规则对所述跨链数据进行管理处理，得到处理后数据；
- 向所述第一区块链返回带有所述中继器的身份签名的响应结果，所述响应结果包含所述处理后数据。
2. 根据权利要求 1 所述的方法，所述响应结果还包含：所述管理规则集的信息和与所述管理规则集的信息唯一匹配的公钥，以用于证明所述处理后数据为所述跨链数据经由所述管理规则集的管理处理后得到。
3. 根据权利要求 2 所述的方法，还包括：
- 接收来自所述第一区块链的验证请求；
- 当所述验证请求包含与所述管理规则集唯一匹配的公钥时，返回所述管理规则集的信息，以用于与所述响应结果包含的管理规则集的信息进行比较。
4. 根据权利要求 2 所述的方法，还包括：
- 接收来自所述第一区块链的查询请求；
- 当所述查询请求包含所述管理规则集的信息时，返回所述管理规则集。
5. 根据权利要求 2 所述的方法，所述管理规则集的信息包括：所述管理规则集中的各条管理规则分别对应的哈希值按照预设算法形成的哈希值。
6. 根据权利要求 5 所述的方法，所述预设算法用于将所述管理规则集中的各条管理规则分别对应的哈希值组织为哈希树；其中，所述管理规则集的信息包括所述哈希树的根哈希值。
7. 根据权利要求 1 所述的方法，所述响应结果还包含：通过与所述管理规则集的信息唯一匹配的私钥对所述处理后数据的签名，以用于验证所述处理后数据的数据完整性。
8. 根据权利要求 1 所述的方法，所述响应结果还包含：所述跨链数据命中的监控规则的信息。
9. 一种跨链数据的可信管理方法，应用于第一区块链的区块链节点，所述方法包括：

创建跨链请求，所述跨链请求的请求对象为第二区块链，使中继器通过配置的所述第二区块链的客户端从所述第二区块链调用相应的跨链数据，且所述中继器用于根据管理规则集包含的管理规则对所述跨链数据进行管理处理而得到处理后数据；

5 获取所述中继器返回的响应结果，所述响应结果由所述中继器在可信执行环境中生成；其中，所述响应结果包含所述处理后数据，且所述响应结果带有所述中继器的身份签名。

10. 根据权利要求 9 所述的方法，所述响应结果还包含：管理规则集的信息和与所述管理规则集唯一匹配的公钥，以表明所述处理后数据为所述跨链数据经由所述管理规则集的管理处理后得到。

10 11. 根据权利要求 10 所述的方法，还包括：

向所述中继器发起验证请求，所述验证请求中包含来自所述响应结果的公钥；

其中，当所述中继器返回与所述公钥相对应的管理规则集的信息，且该信息与所述响应结果包含的管理规则集的信息一致时，所述响应结果包含的公钥被确认为来自所述中继器，且所述处理后数据被确认为所述跨链数据经由所述管理规则集的管理处理后得到。

15

12. 根据权利要求 10 所述的方法，还包括：

向所述中继器发起查询请求，所述查询请求中包含所述管理规则集的信息，以获得所述管理规则集。

13. 根据权利要求 10 所述的方法，所述响应结果还包含：通过与所述管理规则集唯一匹配的私钥对所述处理后数据的签名；所述方法还包括：

20

通过所述响应结果包含的公钥对所述签名进行验证，以确定所述响应结果包含的处理后数据的数据完整性。

14. 根据权利要求 9 所述的方法，所述响应结果还包含：所述跨链数据命中的监控规则的信息。

25 15. 一种跨链数据的可信管理装置，应用于中继器，所述中继器上加载有可信执行环境，以在所述可信执行环境中实现：

调用单元，根据来自第一区块链的跨链请求，从作为请求对象的第二区块链调用相应的跨链数据，其中所述中继器配置有所述第二区块链的客户端；

30 管理单元，加载预配置的管理规则集，以根据所述管理规则集包含的管理规则对所述跨链数据进行管理处理，得到处理后数据；

第一返回单元，向所述第一区块链返回带有所述中继器的身份签名的响应结果，所

述响应结果包含所述处理后数据。

16. 根据权利要求 15 所述的装置, 所述响应结果还包含: 所述管理规则集的信息和与所述管理规则集的信息唯一匹配的公钥, 以用于证明所述处理后数据为所述跨链数据经由所述管理规则集的管理处理后得到。

5 17. 根据权利要求 16 所述的装置, 还包括:

第一接收单元, 接收来自所述第一区块链的验证请求;

第二返回单元, 当所述验证请求包含与所述管理规则集唯一匹配的公钥时, 返回所述管理规则集的信息, 以用于与所述响应结果包含的管理规则集的信息进行比较。

18. 根据权利要求 16 所述的装置, 还包括:

10 第二接收单元, 接收来自所述第一区块链的查询请求;

第三返回单元, 当所述查询请求包含所述管理规则集的信息时, 返回所述管理规则集。

19. 根据权利要求 16 所述的装置, 所述管理规则集的信息包括: 所述管理规则集中的各条管理规则分别对应的哈希值按照预设算法形成的哈希值。

15 20. 根据权利要求 19 所述的装置, 所述预设算法用于将所述管理规则集中的各条管理规则分别对应的哈希值组织为哈希树; 其中, 所述管理规则集的信息包括所述哈希树的根哈希值。

21. 根据权利要求 15 所述的装置, 所述响应结果还包含: 通过与所述管理规则集的信息唯一匹配的私钥对所述处理后数据的签名, 以用于验证所述处理后数据的数据完整性。

20 22. 根据权利要求 15 所述的装置, 所述响应结果还包含: 所述跨链数据命中的监控规则的信息。

23. 一种跨链数据的可信管理装置, 应用于第一区块链的区块链节点, 所述装置包括:

25 创建单元, 创建跨链请求, 所述跨链请求的请求对象为第二区块链, 使中继器通过配置的所述第二区块链的客户端从所述第二区块链调用相应的跨链数据, 且所述中继器用于根据管理规则集包含的管理规则对所述跨链数据进行管理处理而得到处理后数据;

获取单元, 获取所述中继器返回的响应结果, 所述响应结果由所述中继器在可信执行环境中生成; 其中, 所述响应结果包含所述处理后数据, 且所述响应结果带有所述中继器的身份签名。

30 24. 根据权利要求 23 所述的装置, 所述响应结果还包含: 管理规则集的信息和与

所述管理规则集唯一匹配的公钥，以表明所述处理后数据为所述跨链数据经由所述管理规则集的管理处理后得到。

25. 根据权利要求 24 所述的装置，还包括：

5 第一请求单元，向所述中继器发起验证请求，所述验证请求中包含来自所述响应结果的公钥；

其中，当所述中继器返回与所述公钥相对应的管理规则集的信息，且该信息与所述响应结果包含的管理规则集的信息一致时，所述响应结果包含的公钥被确认为来自所述中继器，且所述处理后数据被确认为所述跨链数据经由所述管理规则集的管理处理后得到。

10 26. 根据权利要求 24 所述的装置，还包括：

第二请求单元，向所述中继器发起查询请求，所述查询请求中包含所述管理规则集的信息，以获得所述管理规则集。

27. 根据权利要求 24 所述的装置，所述响应结果还包含：通过与所述管理规则集唯一匹配的私钥对所述处理后数据的签名；所述方法还包括：

15 验证单元，通过所述响应结果包含的公钥对所述签名进行验证，以确定所述响应结果包含的处理后数据的数据完整性。

28. 根据权利要求 23 所述的装置，所述响应结果还包含：所述跨链数据命中的监控规则的信息。

29. 一种电子设备，包括：

20 处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器通过运行所述可执行指令以实现如权利要求 1-8 中任一项所述的方法。

30. 一种电子设备，包括：

25 处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器通过运行所述可执行指令以实现如权利要求 9-14 中任一项所述的方法。