

跨链数据的可信管理方法及装置、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，尤其涉及一种跨链数据的可信管理方法及装置、电子设备。

5 背景技术

[02] 在相关技术中，通过中继链可以实现不同区块链之间的跨链交互。中继链可以分别与各个区块链进行对接，并由该中继链上设置的若干验证者通过共识算法对各个区块链上的跨链数据进行验证，而其他区块链只需对接该中继链即可获得跨链数据。

发明内容

10 [03] 有鉴于此，本说明书一个或多个实施例提供一种跨链数据的可信管理方法及装置、电子设备。

[04] 为实现上述目的，本说明书一个或多个实施例提供技术方案如下：

[05] 根据本说明书一个或多个实施例的第一方面，提出了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
15 步骤：

[06] 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；

[07] 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；

20 [08] 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。

[09] 根据本说明书一个或多个实施例的第二方面，提出了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：

[10] 创建跨链请求，所述跨链请求的请求对象为第二区块链，使中继器从所述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；
25

- [11]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加载的可信执行环境中生成；其中，所述响应结果包含处理后数据，且所述响应结果带有所述中继器的身份签名。
- 5 [12]根据本说明书一个或多个实施例的第三方面，提出了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：
- [13]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；
- [14]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；
- 10 [15]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]根据本说明书一个或多个实施例的第四方面，提出了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：
- [17]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，使中继器从所述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；
- 15 [18]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加载的可信执行环境中生成；其中，所述响应结果包含处理后数据，且所述响应结果带有所述中继器的身份签名。
- [19]根据本说明书一个或多个实施例的第五方面，提出了一种电子设备，包括：
- 20 [20]处理器；
- [21]用于存储处理器可执行指令的存储器；
- [22]其中，所述处理器通过运行所述可执行指令以实现上述第一方面所述的方法。
- [23]根据本说明书一个或多个实施例的第六方面，提出了一种电子设备，包括：
- [24]处理器；
- 25 [25]用于存储处理器可执行指令的存储器；
- [26]其中，所述处理器通过运行所述可执行指令以实现上述第二方面所述的方法。

附图说明

[27]图 1 是一示例性实施例提供的一种跨链数据的可信管理方法的流程图。

[28]图 2 是一示例性实施例提供的另一种跨链数据的可信管理方法的流程图。

[29]图 3 是一示例性实施例提供的一种实现跨链交互的示意图。

5 [30]图 4 是一示例性实施例提供的一种 TEE 程序的功能架构的示意图。

[31]图 5 是一示例性实施例提供的一种设备的结构示意图。

[32]图 6 是一示例性实施例提供的一种跨链数据的可信管理装置的框图。

[33]图 7 是一示例性实施例提供的另一种设备的结构示意图。

[34]图 8 是一示例性实施例提供的另一种跨链数据的可信管理装置的框图。

10 具体实施方式

[35]这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所述的实施方式并不代表与本发明一个或多个实施例相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本发明一个或多个实施例的一些方面相一致的装置和方法的例子。

15

[36]需要说明的是：在其他实施例中并不一定按照本说明书示出和描述的顺序来执行相应方法的步骤。在一些其他实施例中，其方法所包括的步骤可以比本说明书所描述的更多或更少。此外，本说明书中所描述的单个步骤，在其他实施例中可能被分解为多个步骤进行描述；而本说明书中所描述的多个步骤，在其他实施例中也可能被合并为单个步骤进行描述。

20

[37]图 1 是一示例性实施例提供的一种跨链数据的可信管理方法的流程图。如图 1 所示，该方法应用于中继器，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：

[38]步骤 102，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。

25

[39]在一实施例中，第一区块链作为调用方、第二区块链作为被调用方，通过第一区块

链与第二区块链之间的跨链交互，使得第一区块链调用来自第二区块链的区块链数据（即跨链数据）；较为具体的，可以为第一区块链上的某一区块链节点请求调用第二区块链上的区块链数据。

5 [40]容易理解的是，“第一区块链”与“第二区块链”只是作为不同角色的区块链的代称，而并不特指某一个或某几个区块链。例如，当任一区块链作为调用方时属于上述的第一区块链，而当该任一区块链作为被调用方时属于上述的第二区块链。

[41]在一实施例中，通过在中继器上配置第二区块链的客户端，使得中继器可以通过该客户端调用第二区块链上的区块链数据，以提供至第一区块链、完成跨链交互。其中，中继器上配置的客户端可以为完整客户端；或者，中继器上配置的客户端可以为
10 SPV(Simplified Payment Verification, 简单支付验证)客户端，从而在完成数据调用的同时，有助于实现中继器的轻量化。

[42]在一实施例中，中继器的数量可以为一个或多个。对于每一中继器而言，并不需要安装所有区块链的客户端，而只有当某一区块链确定需要通过该中继器实现跨链交互时，才需要在该中继器上配置相应区块链的客户端，这有助于实现中继器的轻量化。同时，
15 通过采用多个中继器，一方面可以对众多区块链的跨链交互需求进行合理分流、避免受到单个中继器的性能瓶颈限制，另一方面可以根据实际需求对中继器进行便捷地弹性部署，具有极佳的可扩展性。

[43]在一实施例中，中继器可以为公共类型或私有类型。对于公共类型的中继器而言，上述的第二区块链与其他区块链均具有操作权限，从而由这些区块链进行共享，有助于
20 减少中继器的部署量、简化系统复杂度。对于私有类型的中继器而言，仅上述的第二区块链具有操作权限，而其他区块链则不需要操作权限、无法使用该中继器，可以确保从第二区块链上调用的跨链数据不会被其他区块链获得，有助于提升数据私密性。

[44]在一实施例中，可以通过在中继器内安装第一区块链的客户端，使得该中继器能够监听第一区块链上创建的跨链请求。在另一实施例中，可以部署锚定器，该锚定器中安
25 装有第一区块链的客户端，使得该锚定器能够监听第一区块链上创建的跨链请求，并将该跨链请求提供至中继器；以及，中继器可以将返回的响应结果提供至锚定器，并由锚定器将该响应结果返回至第一区块链。其中，上述中继器或锚定器中安装的第一区块链的客户端可以为完整客户端或 SPV 客户端，本说明书并不对此进行限制。

[45]在一实施例中，锚定器可以为公共类型或私有类型。对于公共类型的锚定器，上述

的第一区块链与其他区块链均具有操作权限，从而由这些区块链进行共享，有助于减少锚定器的部署量、简化系统复杂度。对于私有类型的锚定器而言，仅上述的第一区块链具有操作权限，其他区块链则不具有操作权限、无法使用该锚定器，可以确保中继器提供的响应结果不会被其他区块链获得，有助于提升数据私密性。

- 5 [46] 步骤 104，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。

[47] 在一实施例中，管理规则集中包含一条或多条管理规则，以用于对跨链数据进行内容管理。管理规则可以来自于管理部门，或者管理规则可以为区块链成员自身或区块链成员之间约定的管理条例，或者管理规则可以具备其他来源，本说明书并不对此进行限制。

10

[48] 在一实施例中，基于管理规则集对跨链数据进行管理处理时，如果跨链数据命中一条或多个管理规则，可能需要基于该管理规则对跨链数据实施一定的调整，比如对敏感词进行标注、对敏感内容进行脱敏（如采用“*”代替或直接删除）等，这取决于管理规则自身的定义，本说明书并不对此进行限制。因此，处理后数据与跨链数据之间可能

15 相同，也可能存在一定差异，这取决于对管理规则的命中情况以及管理规则定义的内容。

[49] 步骤 106，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。

[50] 在一实施例中，中继器可以支持相关技术中的可信执行环境（Trusted Execution Environment, TEE）技术，比如 SGX (Software Guard Extensions, 软件保护扩展) 等，本说明书并不对此进行限制。通过该 TEE 技术可以在中继器上加载可信执行环境，使得

20 中继器在加载管理规则集对跨链数据进行管理处理时，可以避免受到恶意软件的干扰或影响，从而确保中继器能够忠实地按照预定义的管理规则集对跨链数据实施管理处理，得到上述的处理后数据。

[51] 在一实施例中，通过向第一区块链返回带有该中继器的身份签名的响应结果，使得

25 第一区块链通过使用对该身份签名进行验签，确定相应的响应结果确实由上述的中继器生成。同时，由于第一区块链可以预先获知各个中继器所采用的处理方案，包括是否采用 TEE 环境等；因此，第一区块链可以确定该响应结果由相应的中继器在 TEE 环境下生成，从而确定该响应结果所包含的处理后数据由该中继器按照预定义的管理规则集对跨链数据实施管理处理而得到，即中继器对跨链数据的管理结果准确、有效。

[52]在一实施例中，中继器记录了与管理规则集唯一匹配的公私钥对，这里的“唯一匹配”与管理规则集的内容相关，而并不仅局限于“管理规则集”这一概念；换言之，当中继器中的管理规则集发生变化时，比如所包含的管理规则发生增加、删除或修改，中继器都需要对相应的公私钥对进行更新。

- 5 [53]在一实施例中，可以根据管理规则集所包含的所有管理规则，生成与所有管理规则的内容唯一对应的信息，并记录该信息与公私钥对之间的唯一匹配关系。例如，可以将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一哈希值，以作为管理规则集的信息；譬如，该预设算法可以用于将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（Merkle Tree 或 Merkle Hash Tree），而管理规则集的信息可以
- 10 为该哈希树的根哈希值（Root Hash）。

- [54]在一实施例中，响应结果中还可以包含管理规则集的信息、与管理规则集唯一匹配的公钥，使得第一区块链可以据此证明响应结果包含的处理后数据与管理规则集之间的关系，确保中继器忠实地按照预先定义的管理规则对跨链数据实施了管理处理，而并未针对管理规则集包含的管理规则实施私自篡改。例如，第一区块链处可以向中继器发送
- 15 验证请求，该验证请求包含响应结果中提供的公钥。一种情况下，如果中继器查找到验证请求中的公钥对应的管理规则集的信息，可以将确定出的管理规则集的信息返回第一区块链；相应地，根据收到的管理规则集的信息，第一区块链可以确定响应结果中提供的公钥确实来自于该中继器。然后，第一区块链可以将中继器返回的管理规则集的信息与响应结果中包含的管理规则集的信息进行比较，如果两者一致，可以确定中继器通过
- 20 该管理规则集对跨链数据实施管理处理而得到了上述的处理后数据，而未针对管理规则集进行私自篡改；而如果两者不一致，则表明中继器可能私自篡改了管理规则集，响应结果中的处理后数据不可信。另一种情况下，如果中继器未查找到该公钥对应的管理规则集的信息，可以返回用于表明未查找到的通知消息，使得第一区块链确定该公钥并非来自于该中继器，因而响应结果存在异常，可能是中继器私自篡改了管理规则集而导致
- 25 对应的公钥发生变化，表明响应结果中的处理后数据不可信。

[55]在一实施例中，中继器可以接收来自所述第一区块链的查询请求，并在该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，以便第一区块链侧的管理方或其他角色能够了解中继器实施管理处理时具体采用的管理规则。

- [56]在一实施例中，中继器在向第一区块链返回响应结果后，可能基于正常流程对管理
- 30 规则集实施了更新，导致管理规则集的信息、与管理规则集的信息唯一匹配的公私钥对

发生了变更，但中继器仍然可以保存历史版本的管理规则集、该历史版本的管理规则集的信息、与该历史版本的管理规则集的信息唯一匹配的公私钥对，使得第一区块链向中继器发起上述的验证请求或查询请求时，中继器能够返回相应的信息或数据，以满足第一区块链的需求，避免第一区块链误认为响应结果所包含的处理后数据不可信。

5 [57]在一实施例中，响应结果还可以包含：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。例如，第一区块链可以通过预先获知或响应结果中提供的公钥（即与所述管理规则集的信息唯一匹配的公钥）对签名进行验证，以确保处理后数据的数据完整性，避免在传输过程中发生数据缺失或被篡改。

10 [58]在一实施例中，响应结果还可以包含：所述跨链数据命中的监控规则的信息，以便于第一区块链侧的管理方或其他角色能够了解跨链数据的规则命中情况。

[59]图2是一示例性实施例提供的另一种跨链数据的可信管理方法的流程图。如图2所示，该方法应用于第一区块链的区块链节点，可以包括以下步骤：

[60]步骤202，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
15 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处理而得到处理后数据。

[61]在一实施例中，第一区块链作为调用方、第二区块链作为被调用方，通过第一区块链与第二区块链之间的跨链交互，使得第一区块链调用来自第二区块链的区块链数据（即跨链数据）；较为具体的，可以为第一区块链上的某一区块链节点请求调用第二区块链上的区块链数据。
20

[62]容易理解的是，“第一区块链”与“第二区块链”只是作为不同角色的区块链的代称，而并不特指某一个或某几个区块链。例如，当任一区块链作为调用方时属于上述的第一区块链，而当该任一区块链作为被调用方时属于上述的第二区块链。

[63]在一实施例中，通过在中继器上配置第二区块链的客户端，使得中继器可以通过该
25 客户端调用第二区块链上的区块链数据，以提供至第一区块链、完成跨链交互。其中，中继器上配置的客户端可以为完整客户端；或者，中继器上配置的客户端可以为SPV客户端，从而在完成数据调用的同时，有助于实现中继器的轻量化。

[64]在一实施例中，可以通过在中继器内安装第一区块链的客户端，使得该中继器能够监听第一区块链上创建的跨链请求。在另一实施例中，可以部署锚定器，该锚定器中安

装有第一区块链的客户端，使得该锚定器能够监听第一区块链上创建的跨链请求，并将该跨链请求提供至中继器；以及，中继器可以将返回的响应结果提供至锚定器，并由锚定器将该响应结果返回至第一区块链。其中，上述中继器或锚定器中安装的第一区块链的客户端可以为完整客户端或 SPV 客户端，本说明书并不对此进行限制。

- 5 [65]在一实施例中，锚定器可以为公共类型或私有类型。对于公共类型的锚定器，上述的第一区块链与其他区块链均具有操作权限，从而由这些区块链进行共享，有助于减少锚定器的部署量、简化系统复杂度。对于私有类型的锚定器而言，仅上述的第一区块链具有操作权限，其他区块链则不具有操作权限、无法使用该锚定器，可以确保中继器提供的响应结果不会被其他区块链获得，有助于提升数据私密性。
- 10 [66]在一实施例中，管理规则集中包含一条或多条管理规则，以用于对跨链数据进行内容管理。管理规则可以来自于管理部门，或者管理规则可以为区块链成员自身或区块链成员之间约定的管理条例，或者管理规则可以具备其他来源，本说明书并不对此进行限制。

- [67]在一实施例中，基于管理规则集对跨链数据进行处理时，如果跨链数据命中一条或多个管理规则，可能需要基于该管理规则对跨链数据实施一定的调整，比如对敏感词进行标注、对敏感内容进行脱敏（如采用“*”代替或直接删除）等，这取决于管理规则自身的定义，本说明书并不对此进行限制。因此，处理后数据与跨链数据之间可能相同，也可能存在一定差异，这取决于对管理规则的命中情况以及管理规则定义的内容。
- 15

- [68]步骤 204，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。
- 20

- [69]在一实施例中，中继器可以支持相关技术中的 TEE 技术，比如 SGX 等，本说明书并不对此进行限制。通过该 TEE 技术可以在中继器上加载可信执行环境，使得中继器在加载管理规则集对跨链数据进行处理时，可以避免受到恶意软件的干扰或影响，从而确保中继器能够忠实地按照预定义的管理规则集对跨链数据实施管理处理，得到上述的处理后数据。
- 25

[70]在一实施例中，通过向第一区块链返回带有该中继器的身份签名的响应结果，使得第一区块链通过使用对该身份签名进行验签，确定相应的响应结果确实由上述的中继器生成。同时，由于第一区块链可以预先获知各个中继器所采用的处理方案，包括是否采

用 TEE 环境等；因此，第一区块链可以确定该响应结果由相应的中继器在 TEE 环境下生成，从而确定该响应结果所包含的处理后数据由该中继器按照预定义的管理规则集对跨链数据实施管理处理而得到，即中继器对跨链数据的管理结果准确、有效。

[71]在一实施例中，中继器记录了与管理规则集唯一匹配的公私钥对，这里的“唯一匹
5 配”与管理规则集的内容相关，而并不仅限于“管理规则集”这一概念；换言之，当中继器中的管理规则集发生变化时，比如所包含的管理规则发生增加、删除或修改，中继器都需要对相应的公私钥对进行更新。

[72]在一实施例中，可以根据管理规则集所包含的所有管理规则，生成与所有管理规则的内容唯一对应的信息，并记录该信息与公私钥对之间的唯一匹配关系。例如，可以将
10 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一哈希值，以作为管理规则集的信息；譬如，该预设算法可以用于将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，而管理规则集的信息可以为该哈希树的根哈希值。

[73]在一实施例中，响应结果中还可以包含管理规则集的信息、与管理规则集唯一匹配的公钥，使得第一区块链可以据此证明响应结果包含的处理后数据与管理规则集之间的
15 关系，确保中继器忠实地按照预先定义的管理规则对跨链数据实施了管理处理，而并未针对管理规则集包含的管理规则实施私自篡改。例如，第一区块链处可以向中继器发送验证请求，该验证请求包含响应结果中提供的公钥。一种情况下，如果中继器查找到验证请求中的公钥对应的管理规则集的信息，可以将确定出的管理规则集的信息返回第一区块链；相应地，根据收到的管理规则集的信息，第一区块链可以确定响应结果中提供
20 的公钥确实来自于该中继器。然后，第一区块链可以将中继器返回的管理规则集的信息与响应结果中包含的管理规则集的信息进行比较，如果两者一致，可以确定中继器通过该管理规则集对跨链数据实施管理处理而得到了上述的处理后数据，而未针对管理规则集进行私自篡改；而如果两者不一致，则表明中继器可能私自篡改了管理规则集，响应结果中的处理后数据不可信。另一种情况下，如果中继器未查找到该公钥对应的管理规
25 则集的信息，可以返回用于表明未查找到的通知消息，使得第一区块链确定该公钥并非来自于该中继器，因而响应结果存在异常，可能是中继器私自篡改了管理规则集而导致对应的公钥发生变化，表明响应结果中的处理后数据不可信。

[74]在一实施例中，中继器可以接收来自所述第一区块链的查询请求，并在该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，以便第一区块链侧的管理方或其他角色能够了解中继器实施管理处理时具体采用的管理规则。
30

[75]在一实施例中，中继器在向第一区块链返回响应结果后，可能基于正常流程对管理规则集实施了更新，导致管理规则集的信息、与管理规则集的信息唯一匹配的公私钥对发生了变更，但中继器仍然可以保存历史版本的管理规则集、该历史版本的管理规则集的信息、与该历史版本的管理规则集的信息唯一匹配的公私钥对，使得第一区块链向中
5 继器发起上述的验证请求或查询请求时，中继器能够返回相应的信息或数据，以满足第一区块链的需求，避免第一区块链误认为响应结果所包含的处理后数据不可信。

[76]在一实施例中，响应结果还可以包含：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。例如，第一区块链可以通过预先获知或响应结果中提供的公钥（即与所述管理规则集的信息唯一匹配的
10 的公钥）对签名进行验证，以确保处理后数据的数据完整性，避免在传输过程中发生数据缺失或被篡改。

[77]在一实施例中，响应结果还可以包含：所述跨链数据命中的监控规则的信息，以便于第一区块链侧的管理方或其他角色能够了解跨链数据的规则命中情况。

[78]为了便于理解，下面以采用 TEE 技术的中继器为例，对本说明书的跨链数据管理方案进行描述。图 3 是一示例性实施例提供的一种实现跨链交互的示意图。如图 3 所示，
15 区块链 1 与区块链 2 可以通过中继器实现跨链交互，该区块链 1 可以发起针对区块链 2 的跨链请求，而中继器可以将跨链请求传递至区块链 2，使得区块链 2 针对该跨链请求生成相应的跨链数据。而中继器上配置有区块链 2 的客户端，使得该中继器可以据此调用区块链 2 生成的上述跨链数据，并针对该跨链数据实施管理处理后，将相应的响应结果
20 返回至区块链 1。

[79]在一实施例中，中继器可以支持 TEE 技术，使得该中继器运行的、用于实施上述管理处理的程序可以被配置为 TEE 程序，而该 TEE 程序可以安全运行于中继器加载的可信执行环境中，避免受到恶意软件等的影响。以相关技术中的 SGX 技术为例，中继器的 CPU 在发现所需执行的程序为 TEE 程序时，可以从预配置的安全元件中读取密钥，
25 以用于对分配的内存空间进行加密，该内存空间可以形成用于执行上述 TEE 程序的可信执行环境，即图 3 所示的 Enclave 空间。

[80]通过将 TEE 程序封装在 Enclave 空间中，且只有 CPU 能够获得该 enclave 的密钥（即上述安全元件中的密钥），使得该 Enclave 的安全边界只有 CPU 和 TEE 程序自身，可以避免受到恶意软件的攻击，而不论该恶意软件是否为特权软件，甚至操作系统和 VMM
30 （Virtual Machine Monitor，虚拟机监控器）也无法对 Enclave 造成影响。因此，可以避

免外部因素影响中继器对跨链数据实施管理处理。

[81]图 4 是一示例性实施例提供的一种 TEE 程序的功能架构的示意图。如图 4 所示,该 TEE 程序可以包含 TEE 身份密钥对、区块链 2 客户端、管理规则根哈希、管理规则执行器、锁定根哈希的密钥对等若干功能模块,以供中继器实现相关处理功能。

- 5 [82]在一实施例中,区块链 2 客户端可以为区块链 2 的 SPV 客户端,中继器可以基于该区块链 2 客户端从区块链 2 中调用上述的跨链数据,此处不再赘述。然后,中继器可以通过管理规则执行器加载预定义的管理规则,比如图 4 所示的管理规则 1~4,以用于针对跨链数据实施管理处理,得到处理后数据。其中,根据管理规则所定义的内容,对跨链数据实施的管理处理也存在差异,比如某一管理规则可以用于对跨链数据中的一部分敏感词进行脱敏(如删除或替换为“*”等)、另一管理规则可以用于对跨链数据中的另一部分敏感词进行标注等,本说明书并不对此进行限制。当然,跨链数据也可能不会命中任何管理规则,使得处理后数据与跨链数据一致。
- 10

- [83]在一实施例中,可以将中继器中的规则 1~4 分别生成对应的哈希值,比如 hash1~hash4,并进一步组织为如图 4 所示的 Merkle Tree 形式,从而最终得到根哈希(比如由 hash1 与 hash2 进行哈希计算得到 hash5、由 hash3 与 hash4 进行哈希计算得到 hash6,并进一步由 hash5 与 hash6 进行哈希计算得到根哈希)。而管理规则执行器可以根据根哈希以及上述的 Merkle Tree,调用中继器中对应的规则 1~4(即根哈希在 Merkle Tree 中对应的所有叶子哈希对应的管理规则),以针对跨链数据实施上述的管理处理。
- 15

- [84]基于哈希值的特点,使得上述的根哈希与管理规则的内容之间唯一对应;换言之,当 TEE 程序所采用的管理规则不变时,对应的根哈希也不变,而当任一管理规则发生变化时,即可反映为对应的根哈希的取值变化。而“锁定根哈希的密钥对”与“根哈希”之间唯一匹配,使得当 TEE 程序所采用的管理规则不变时,根哈希和锁定根哈希的密钥对也不变,而当任一管理规则发生变化时,即可反映为对应的根哈希、锁定根哈希的密钥对均发生变化。例如,当确定根哈希发生变化时,中继器可以重新生成密钥对,并配置为新的根哈希对应的锁定根哈希密钥对。
- 20
- 25

[85]在一实施例中,TEE 根据上述内容,可以生成中继器向区块链 1 返回的响应结果,该响应结果可以包括下述内容:

[86]i.处理后数据

[87]ii.通过锁定根哈希的私钥对处理后数据的签名

[88]iii.锁定根哈希的公钥

[89]iv.管理规则根哈希

[90]v.跨链数据命中的管理规则

[91]同时，TEE 程序可以通过上述的 TEE 身份密钥对中的私钥，对响应结果进行签名，

5 然后由中继器返回至区块链 1。

[92]相应地，针对收到的响应结果，区块链 1 可以对该响应结果进行验证，以确定其包含的处理后数据是否可靠，比如是否确实是根据管理规则对跨链数据进行处理而得到该处理后数据。例如，区块链 1 针对响应结果的验证过程可以包括：

[93]I.区块链 1 根据中继器的 TEE 身份公钥对响应结果的签名进行验证，以确定该响应
10 结果确实来自于该中继器。

[94]其中，TEE 身份公钥可以由中继器预先对外或向区块链 1 公布。而区块链 1 可以预先获知该中继器对 TEE 技术的支持情况，因而当确定该响应结果来自于该中继器时，区块链 1 可以确定该响应结果是由中继器在可信执行环境中处理得到，从而排除了恶意软件等外部因素对该响应结果的不利影响。

15 [95]II.区块链 1 读取响应结果包含的处理后数据、锁定根哈希的公钥、通过锁定根哈希的私钥对处理后数据的签名，并通过锁定根哈希的公钥对该通过锁定根哈希的私钥对处理后数据的签名进行验证。若通过验证，则可以确定处理后数据在传输过程中未发生数据丢失或被篡改，从而确认该处理后数据的完整性。

[96]III.区块链 1 向中继器发起验证请求，该验证请求中包含响应结果中提供的锁定根哈
20 希的公钥。

[97]其中，中继器在收到验证请求后，如果查找到与该锁定根哈希的公钥相对应的管理规则根哈希 HashX，可以将查找到的管理规则根哈希 HashX 返回至区块链 1。相应地，区块链 1 在接收到中继器返回的管理规则根哈希 HashX 时，至少可以确定响应结果中提供的锁定根哈希的公钥确实来自于该中继器，且确定该锁定根哈希的公钥锁定的管理规
25 则根哈希为 HashX。相反地，如果中继器并未查找到与验证请求中的锁定根哈希的公钥相对应的管理规则根哈希，那么中继器将无法返回对应的管理规则根哈希，比如可以返回“未查找到对应信息”或类似内容，使得区块链 1 确定响应结果中提供的锁定根哈希的公钥并非来自于该中继器，从而推断出响应结果中的处理后数据极可能不可靠。

[98]进一步地，区块链 1 可以将获得的 HashX 与响应结果中包含的管理规则根哈希进行比较；当两者一致时，区块链 1 可以确定：中继器通过运行 TEE 程序，忠实地执行了管理规则根哈希对应的管理规则（如规则 1~4），而并未针对管理规则实施私自篡改；当两者不一致时，表明中继器极可能私自篡改了所采用的管理规则，从而推断出响应结果中的处理后数据极可能不可靠。

[99]另外，区块链 1 还可以向中继器发送管理规则根哈希，使得中继器可以将对应的所有管理规则返回至区块链 1，以便于区块链 1 了解用于对跨链数据实施管理处理的管理规则。区块链 1 还可以通过响应结果中包含的跨链数据命中的管理规则，确定跨链数据对管理规则的命中情况。

10 [100] 综上所述，通过采用基于 TEE 技术的中继器，使得该中继器可以提供安全可靠的可信执行环境，以确保在该可信执行环境下实施的处理操作不会受到恶意软件等外部因素的影响，并且由于中继器在逻辑上属于单点设备，因而能够高效、安全地执行管理处理，从而在跨链交互过程中对跨链数据实施有效管理。同时，通过在响应结果中包含上文所述的其他证明信息，使得区块链 1 能够证明处理后数据与跨链数据之间的关系，
15 可以对中继器实现有效的监督作用，使得中继器难以篡改管理规则，或者使得区块链 1 或第三方的管理方能够发现篡改行为，从而实现可信的跨链数据管理方案。

[101] 图 5 是一示例性实施例提供的一种设备的示意结构图。请参考图 5，在硬件层面，该设备包括处理器 502、内部总线 504、网络接口 506、内存 508 以及非易失性存储器 510，当然还可能包括其他业务所需要的硬件。处理器 502 从非易失性存储器 510 中读取对应的计算机程序到内存 508 中然后运行，在逻辑层面上形成跨链数据的可信管理装置。当然，除了软件实现方式之外，本说明书一个或多个实施例并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

25 [102] 请参考图 6，在软件实施方式中，该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：

[103] 调用单元 61，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；

[104] 管理单元 62，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；

- [105] 第一返回单元 63, 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。
- [106] 可选的, 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 [107] 可选的, 还包括:
- [108] 第一接收单元 64, 接收来自所述第一区块链的验证请求;
- [109] 第二返回单元 65, 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。
- 10 [110] 可选的, 还包括:
- [111] 第二接收单元 66, 接收来自所述第一区块链的查询请求;
- [112] 第三返回单元 67, 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。
- [113] 可选的, 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 [114] 可选的, 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。
- [115] 可选的, 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 [116] 可选的, 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。
- [117] 图 7 是一示例性实施例提供的一种设备的示意结构图。请参考图 7, 在硬件层面, 该设备包括处理器 702、内部总线 704、网络接口 706、内存 708 以及非易失性存储器 710, 当然还可能包括其他业务所需要的硬件。处理器 702 从非易失性存储器 710 中读取对应的计算机程序到内存 708 中然后运行, 在逻辑层面上形成跨链数据的可信管理装置。当然, 除了软件实现方式之外, 本说明书一个或多个实施例并不排除其他实现方式, 比如逻辑器件抑或软硬件结合的方式等等, 也就是说以下处理流程的执行主体并不限定于各个逻辑单元, 也可以是硬件或逻辑器件。
- 25 [118] 请参考图 8, 在软件实施方式中, 该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，可以包括：

[119] 创建单元 81，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；

[120] 获取单元 82，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。

[121] 可选的，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。

[122] 可选的，还包括：

[123] 第一请求单元 83，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；

[124] 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。

[125] 可选的，还包括：

[126] 第二请求单元 84，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。

[127] 可选的，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：

[128] 验证单元 85，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。

[129] 可选的，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。

[130] 上述实施例阐明的系统、装置、模块或单元，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。

5 [131] 在一个典型的配置中，计算机包括一个或多个处理器 (CPU)、输入/输出接口、网络接口和内存。

[132] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器 (RAM) 和/或非易失性内存等形式，如只读存储器 (ROM) 或闪存(flash RAM)。内存是计算机可读介质的示例。

10 [133] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器 (CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒
15 式磁带、磁盘存储、量子存储器、基于石墨烯的存储介质或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体 (transitory media)，如调制的数据信号和载波。

[134] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，
20 而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[135] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理
25 也是可以的或者可能是有利的。

[136] 在本说明书一个或多个实施例使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本说明书一个或多个实施例。在本说明书一个或多个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。

5 [137] 应当理解，尽管在本说明书一个或多个实施例可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本说明书一个或多个实施例范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。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”。

10 [138] 以上所述仅为本说明书一个或多个实施例的较佳实施例而已，并不用以限制本说明书一个或多个实施例，凡在本说明书一个或多个实施例的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书一个或多个实施例保护的范围之内。