

基于区块链的隐私交易及其应用方法和装置

技术领域

[01]本说明书涉及数据处理技术领域，尤其涉及一种基于区块链的隐私交易及其应用方法和装置。

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，使得区块链技术已在众多的领域中广泛的进行应用。

- 10 [03]但是，目前的主流区块链架构中，各个节点保存相同的数据；在有些实际场景中，区块链节点参与方不希望自己的数据被其它节点获知。

发明内容

- [04]针对以上提出的区块链数据处理流程的现状和问题，根据本说明书一个或多个实施例的第一方面，提出了一种基于区块链的隐私交易方法，应用于可信任用户的节点设备，
15 其中，所述可信任用户由区块链的分布式数据库存储的信任设置交易确定，所述信任设置交易包括所述区块链用户对应的所有可信任用户的标识；所述方法包括：

[05]接收所述区块链用户发送的第一消息，所述第一消息包括未隐私保护的第一数据信息和受隐私保护的所述第二数据信息；

[06]将所述未隐私保护的第一数据信息转化为受隐私保护的所述第二数据信息；

- 20 [07]将所述第一数据信息保存在所述可信任用户的节点设备的本地数据库；

[08]向所述区块链发送第二交易，所述第二交易包括所述第二数据信息，以使所述第二交易被验证后收录于所述区块链的分布式数据库中。

[09]根据本说明书一个或多个实施例的第二方面，提出了一种基于区块链的隐私交易的应用方法，包括：

- 25 [10]从所述区块链的分布式数据库获取由可信任用户的节点设备发送的第二交易，所述

第二交易包括受隐私保护的所述第二数据信息，其中，所述可信任用户由区块链的分布式数据库存储的信任设置交易确定，所述信任设置交易包括所述区块链用户对应的所有可信任用户的标识；

5 [11]接收所述可信任用户的节点设备发送的未隐私保护的第一数据信息，所述第一数据信息被保存在所述可信任用户的节点设备的本地数据库；

[12]验证所述受隐私保护的所述第二数据信息是否由所述未隐私保护的第一数据信息转化所得，如果是，执行对所述第二交易的应用逻辑。

10 [13]根据本说明书一个或多个实施例的第三方面，提出了一种基于区块链的隐私交易装置，应用于可信任用户的节点设备，其中，所述可信任用户由区块链的分布式数据库存储的信任设置交易确定，所述信任设置交易包括所述区块链用户对应的所有可信任用户的标识；所述装置包括：

[14]接收单元，接收所述区块链用户发送的第一消息，所述第一消息包括未隐私保护的第一数据信息；

[15]转化单元，将所述未隐私保护的第一数据信息转化为受隐私保护的所述第二数据信息；

15 [16]存储单元，将所述第一数据信息保存在所述可信任用户的节点设备的本地数据库；

[17]发送单元，向所述区块链发送第二交易，所述第二交易包括所述第二数据信息，以使所述第二交易被验证后收录于所述区块链的分布式数据库中。

[18]根据本说明书一个或多个实施例的第四方面，提出了一种基于区块链的隐私交易的应用装置，包括：

20 [19]获取单元，从所述区块链的分布式数据库获取由可信任用户的节点设备发送的第二交易，所述第二交易包括受隐私保护的所述第二数据信息，其中，所述可信任用户由区块链的分布式数据库存储的信任设置交易确定，所述信任设置交易包括所述区块链用户对应的所有可信任用户的标识；

25 [20]接收单元，接收所述可信任用户的节点设备发送的未隐私保护的第一数据信息，所述第一数据信息被保存在所述可信任用户的节点设备的本地数据库；

[21]验证单元，验证所述受隐私保护的所述第二数据信息是否由所述未隐私保护的第一数据信息转化所得；

[22]应用单元，执行对所述第二交易的应用逻辑。

[23]本说明书还提供了一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行上述基于区块链的隐私交易方法所述的步骤。

- 5 [24]本说明书还提供了一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行上述基于区块链的隐私数据应用方法所述的步骤。

[25]由以上技术方案可见，本说明书提供的基于区块链的隐私交易方法及装置，用户通过信任设置交易在区块链上设置其可信任的用户，并将其欲隐私的第一数据信息对其可信任用户公开，而其可信任用户将由上述第一数据信息转化来的、受隐私保护的第二数据信息上传至区块链的分布式数据库中，以使上述受隐私保护的第三数据信息在区块链上被共识验证。采用本说明书所提供的隐私交易方法，既可以保护用户未隐私保护的第一数据信息的隐私性，防止区块链上其他任意节点获得该第一数据信息，又可将第一数据信息数据转化获得的第二数据信息在区块链上予以存证保护；在以后任意节点需要应用或验证该第二数据信息时，可从上述用户设置的可信任节点处获取上述第一数据信息，并验证第一数据信息与第二数据信息的对应关系，从而既完成对区块链上存证的第二数据信息的验证、又可获取到第一数据信息的原文以对其应用。

10

15

[26]本说明书提供的上述技术方案，基于区块链技术的分布式数据库存储机制，用户的第二数据信息被去中心化地记录在所有节点中，由所有参与方的节点共同维护，实时进行同步，所有记录可回溯。而且，基于区块链的共识机制，每个用户提供的第二数据信息不会在提供后被篡改，从而保证了用户的第二数据信息的真实性和安全性。基于对可信任用户的信任，在使用第二数据信息对应的第一数据信息时，由可信任用户提供第一数据信息的原文，从而保证了上述第一数据的真实性、安全性和准确性。

20

附图说明

- 25 [27]图1为本说明书一示例性实施例提供的、可信任用户的节点设备执行的基于区块链的隐私交易方法的流程图；

[28]图2为本说明书一示例性实施例提供的、可信任用户的节点设备向其他可信任用户的节点设备传输未隐私消息的流程图；

[29]图 3 为本说明书一示例性实施例提供的区块链的任一节点设备执行的对被隐私保护的交易的交易的应用方法的流程图;

[30]图 4 为本说明书又一实施例提供的基于区块链的隐私交易方法及对被隐私保护的交易的交易的应用方法的流程图;

5 [31]图 5 为本说明书所提供的一实施例提供的基于区块链的隐私交易装置的示意图;

[32]图 6 为本说明书所提供的一实施例提供的基于区块链的隐私交易应用装置的示意图;

[33]图 7 为运行本说明书所提供的基于区块链的隐私交易装置实施例或隐私交易应用装置的一种硬件结构图。

具体实施方式

10 [34]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描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 [35]需要说明的是:在其他实施例中并不一定按照本发明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发明所描述的更多或更少。此外,本发明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;而本发明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 [36]如图 1 所示,本发明一示意性实施例提供了一种基于区块链的隐私交易方法。本实施例所述的区块链,具体可指一个各节点设备通过共识机制达成的、具有分布式数据存储结构的 P2P 网络系统,该区块链内的数据分布在时间上相连的一个个“区块(block)”之内,后一区块包含前一区块的数据摘要,且根据具体的共识机制(如 POW、POS、DPOS 或 PBFT 等)的不同,达成全部或部分节点设备的数据全备份。本领域的技术人
25 员熟知,由于区块链系统在相应共识机制下运行,已收录至区块链数据库内的数据很难被任意的节点设备篡改,例如采用 Pow 共识的区块链,至少需要全网 51%算力的攻击才有可能篡改已有数据,因此区块链系统有着其他中心化数据库系统所法比拟的保证数据安全、防攻击篡改的特性。

[37]在本说明书中所描述的交易（transaction），是指用户通过区块链的节点设备创建，并需要最终发布至区块链的分布式数据库中的一笔数据。其中，区块链中的交易，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

5 广义的交易是指用户向区块链发布的一笔任意的数据：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，租房业务、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；又如，在账户型的区块链中，该交易还可以是用户向区块链发送的、用以更改用

10 户的账户状态的数据（如账户余额等）。因此，只要是用户向区块链的分布式数据库发布的任意数据，无论该任意数据被保存在区块的区块体、区块头还是其他位置，均可属于本发明所述的“交易”。

[38]另外，值得注意的是，本说明书所述的节点设备，不仅可包括备份有区块链的分布式数据库的全量数据的全节点设备，还可包括备份有区块链的分布式数据库的部分数据

15 的轻节点设备，以及其他的终端设备或客户端，在本说明书中不做限定。

[39]图 1 所示的基于区块链的隐私交易方法应用于可信任用户的节点设备，其中，所述可信任用户由区块链的分布式数据库存储的信任设置交易确定，所述信任设置交易包括所述区块链用户确定的所有可信任用户的标识，如可信任用户的账户地址、可信任用户的公钥、或可信任用户的账户名称等可唯一确定可信任用户的信息。区块链用户可以基

20 于自身对其他用户的信任，选取设定其对应的可信任用户，例如可选用信用较高的金融机构、认证机构、监督机构用户或其他机构。上述信任设置交易可以由区块链用户直接向区块链发布，也可由区块链用户调用声明有可信任用户设置逻辑的智能合约来发布，在此不做限定。

[40]图 1 所示的方法包括：步骤 102，接收所述区块链用户发送的第一消息，所述第一

25 消息包括未隐私保护的第一数据信息。

[41]步骤 102 所述的接收所述区块链用户发送的第一消息，是上述可信任用户的节点设备通过链外通道与区块链用户通信而接收到的。所述链外通道，是指并非以向区块链的分布式数据库内发送交易的形式、而是以私下点对点通信、或通过其他中继节点的网络通信方式。值得注意的是，上述第一消息可以与区块链上发布的交易有着相同的数据内

容格式，之所以在此处被称为“消息”而非“交易”，是由于上述第一消息被非向区块链的分布式数据库内发送，而是链外通道发送。未隐私保护的第一数据信息，是指该第一数据信息是未经隐私保护加密的信息原文。

[42] 步骤 104，将所述未隐私保护的第一数据信息转化为受隐私保护的第三数据信息。

- 5 [43] 上述受隐私保护的第三数据信息是由未隐私保护的第一数据信息转化所得，具体的数据转化规则可以由该区块链的底层协议设定，也可以由可信任用户自行设定。上述转化过程可以为将上述第一数据信息加密或编码运算以获得上述第三数据信息。在一示出的实施方式中，为保证第三数据信息仅可唯一地对应上述第一数据信息，第三数据信息可以为第一数据信息的哈希摘要。

- 10 [44] 步骤 106，将所述第一数据信息保存在所述可信任用户的节点设备的本地数据库。

[45] 上述可信任用户的节点设备的本地数据库是区别于该可信任用户的节点设备的区块链分布式数据库而言的，存储在节点设备的本地数据库的第一数据信息不会被区块链上的其他节点设备获知，因而保证了第一数据信息的隐私性。

- [46] 在又一示出的实施例，为保证上述第一消息所包含的内容的合法性，还可预先设置验证规则，由上述可信任用户的节点设备对上述第一消息进行验证，并在预设的验证规则规定的验证通过后，将所述第一数据信息保存在所述可信任用户的节点设备的本地数据库。例如，当所述第一消息包括所述区块链用户至少对所述未隐私保护的第一数据信息所作的第一数字签名时，上述预设的验证规则至少可包括验证所述第一数字签名是由所述区块链用户至少对所述未隐私保护的第一数据信息所作，以防止其他用户冒充上述区块链用户篡改上述第一数据信息。
- 15
- 20

[47] 步骤 108，向所述区块链发送第二交易，所述第二交易包括所述第三数据信息，以使所述第二交易被所述区块链中具有共识权限的节点设备验证后收录于所述区块链的分布式数据库中。

- [48] 该区块链上的任意节点设备均可通过访问区块链的分布式数据库的形式，获得上述第二交易中的第三数据信息；由于第三数据信息处于被隐私保护的状态，除了上述发送第一消息的区块链用户自身和上述区块链用户所信任的可信任用户，该区块链上的其他用户均不能获知该第三数据信息对应的第一数据信息，从而有效地保护了第一数据信息的隐私性。
- 25

[49]上述实施例所述的使所述第二交易被收录至所述区块链的分布式数据库中的详细过程，可依据所述区块链的共识机制及验证规则而具体设定。在一示出的实施方式中，所述第二交易被收录到所述区块链的分布式数据库中的具体步骤，可以包括：

[50]所述区块链中具有记账权限的节点设备将所述第二交易加入到候选区块；

- 5 [51]从所述具有记账权限的节点设备中确定满足所述区块链共识机制的共识记账节点设备；

[52]所述共识记账节点设备向所述区块链的节点设备广播所述候选区块；

[53]在所述候选区块通过所述区块链符合预设数量的节点设备的验证认可后，所述候选区块被视为最新区块，加入到所述区块链的分布式数据库中。

- 10 [54]在上述的实施例中，具有记账权限的节点设备是指具有生成候选区块权限的节点设备，可包括具有较高信用用户的节点设备、及上述区块链中的其他节点设备。根据所述区块链的共识机制，可从上述对所述候选区块具有记账权限的节点设备中确定共识记账节点设备，上述共识机制可以包括工作量证明机制（PoW）、或权利证明机制（PoS）、或股份授权证明机制（DPoS）等，或联盟链通常采用的 PBFT 等。

- 15 [55]关于对上述第二交易的验证，通常可包括对第二交易的数据内容格式的验证，或第二交易的全部或部分内容的验证，或对第二交易所包含的数字签名的验证等等。在一示出的实施例中，为保证发送上述第二交易的可信任用户的节点设备属于上述区块链用户设定的可信任用户，区块链的节点设备应验证上述可信任用户的标识是否包含在上述区块链用户发起的信任设置交易中；如果是，表明该第二交易的发起用户为合法的发起用
20 户。

- [56]在又一示出的实施例中，为防止其他任意节点设备冒充上述可信任用户的节点设备发起上述第二交易，上述第二交易还包括所述可信任用户至少对所述受隐私保护的第二数据信息所作的第二数字签名；为体现并存证上述第二交易中包含的第二数据信息最初是由上述区块链用户的节点设备生成作出的，上述第二交易还可包括上述第一消息所包
25 括的、所述区块链用户至少对所述未隐私保护的第一数据信息所作的第一数字签名。相应地，区块链中的节点设备对上述第二交易的验证，至少应包括基于可信任用户的公钥对第二数字签名的验证，以在验证通过后，将上述第二交易收录于区块链的分布式数据库中。

[57] 区块链用户在设置可信用户时，可以设置多个可信用户。区块链用户可从上述多个可信用户中选择一个可信用户，发送上述第一消息；相应地，上述一个可信用户除完成如上述实施例中步骤 102 至 108 所述的基于区块链的隐私交易方法，还应将上述区块链用户发来的上述第一消息传输至其他的可信任用户的节点设备处，以使其他的可信任用户在其节点设备的本地数据库中备份该第一消息中包含的未隐私保护的第一数据信息。具体说来，如图 2 所示，将上述区块链用户发来的上述第一消息传输至其他的可信任用户的节点设备处的步骤可以包括：

[58] 步骤 202，从所述区块链的分布式数据库中获取所述信任设置交易；

[59] 步骤 204，基于所述信任设置交易确认所述区块链用户信任的其他可信用户；

10 [60] 步骤 206，将所述未隐私保护的第一数据信息和受隐私保护的第二数据信息链外传输至所述用户信任的其他可信用户的节点设备，以使所述第一数据信息被验证由所述第二数据信息转化所得后，保存在所述其他可信用户的节点设备的本地数据库中。

[61] 如上述实施例所述，信任设置交易包括所述区块链用户确定的所有可信用户的标识，如可信用户的账户地址、可信用户的公钥、或可信用户的账户名称等可唯一
15 确定可信用户的信息。因此，基于上述信任设置交易可确认除自身之外所述区块链用户信任的其他可信用户。

[62] 为防止第一数据信息被区块链上的任意节点设备获知而失去隐私性，上述可信用户的节点设备通过链外通道将其获得的第一数据信息传输至其他可信用户的节点设备；为方便其他可信用户验证上述第二数据信息的是否与第一数据信息对应，上述可
20 信用户的节点设备也应通过链外通道将其转化所得的第二数据信息传输至其他可信用户的节点设备。上述链外传输方式包括但不限于链外点对点通信、广播等形式。

[63] 类似地，其他可信用户的节点设备也可基于预设的验证规则验证所述第一数据信息，以在所述验证通过后将所述第一数据信息保存在所述其他可信用户的节点设备的本地数据库，其中所述预设的验证规则包括验证所述受隐私保护的所述第二数据信息是由所述未隐私保护的第一数据信息转化所得。当上述可信用户还将上述实施例所述的第一数字签名或第二数字签名链外发送至其他可信用户时，其他可信用户还应验证所述
25 第一数字签名是由所述区块链用户至少对所述未隐私保护的第一数据信息所作，或验证所述第二数字签名是由所述可信用户至少对所述受隐私保护的所述第二数据信息所作，等等，在此不再赘述。

[64]值得注意的是，当各个其他可信任用户的节点设备接收到上述第一数据信息和第二数据信息后，各个其他可信任用户的节点设备可向上述可信任用户传递信息接收完毕、或验证通过、或同意存储上述第一数据信息等回复。在又一示出的实施方式中，上述各个其他可信任用户的节点设备向上述可信任用户发送各个其他可信任用户至少对所述受隐私保护的5 第二数据信息所作的各个数字签名，上述各个数字签名，既可以向上述可信任用户表达各个其他可信任用户的节点设备对上述第一消息的验证通过指示、或已存储第一数据信息的提示，上述可信任用户的节点设备还可将上述各个数字签名收录纳入其向区块链的分布式数据库发布的第二交易中，从而与上述可信任用户的节点设备作出的10 第四电子签名一起，为区块链的其他任意节点设备对第二交易所包括的第二数据信息的合法性验证作出支持。

[65]本说明书所提供的以上实施例提供了可信任用户的节点设备所执行的基于区块链的隐私交易方法，通过在可信任用户的节点设备的本地数据库中存储未隐私保护的第一数据15 信息，可信任用户的节点设备向区块链的分布式数据库中发送受隐私保护的20 第二数据信息，使得区块链的节点设备均可备份上述受隐私保护的25 第二数据信息，达到了隐私保护上述第一数据信息的效果。

[66]相应地，本说明书还提供了一种基于区块链的隐私交易的应用方法。如图3所示，在区块链的任一节点设备需要应用上述第二交易时，该任一节点设备可执行以下步骤：

[67]步骤302，从所述区块链的分布式数据库获取由可信任用户的节点设备发送的第二交易，所述第二交易包括受隐私保护的20 第二数据信息，所述可信任用户由区块链的分布式数据库存储的信任设置交易确定，所述信任设置交易包括所述区块链用户对应的所有可信任用户的标识。

[68]步骤304，接收所述可信任用户的节点设备发送的未隐私保护的第一数据信息，所述25 第一数据信息被保存在所述可信任用户的节点设备的本地数据库。该区块链的任一节点设备通过与发送上述第二交易的可信任用户的节点设备进行链外通信，可获得该可信任用户的节点设备在本地数据库中存储的第一数据信息。

[69]步骤306，验证所述受隐私保护的20 第二数据信息是否由所述未隐私保护的第一数据信息转化所得。

[70]如果是，

[71]步骤308，执行对所述第二交易的应用逻辑。

[72]关于上述信任设置交易的设置方式、第一数据信息和第二数据信息的转化规则或方式、可信任用户的选择方式等，均已在上述基于区块链的隐私交易方法所述的多个实施例中描述过，在此不再赘述。上述对第二交易的应用逻辑，包括获取第二交易中受隐私保护的

5 第二数据信息所对应的未隐私保护的第一数据信息、或基于该第一数据信息开展的数据应用或业务应用等；该应用即可包括区块链外的数据应用也可包括区块链上的数据应用，如发布基于该第一数据信息的交易等，在本说明书中不作限定。

[73]相较于一般的设置参数状态、或发布被隐私保护的数据信息的交易，区块链中的转账交易由于需要涉及至少两个用户的账户余额状态发生联动变化而有着一些独有的特征步骤。以下，本说明书以区块链用户 A 向区块链用户 B 发送转账交易为例，详细阐述本说明书所提供的隐私交易方法。基于对自身账户的隐私安全考虑，区块链用户 A 协

10 同其可信任用户 SA 通过上述一个或多个实施例所述的方法，将其账户状态中的余额(假设为 100)设置为受隐私保护的状态(例如为余额 100 所对应的哈希摘要值 hash(100))。

[74]如图 4 所示，将区块链用户 A 账户状态中的余额 100 设置为 hash(100)的过程可包括：

15 [75]步骤 401，区块链用户 A 的节点设备向区块链的分布式数据库中发送信任设置交易，将用户 SA 设置为其可信任用户。

[76]步骤 402，区块链用户 A 的节点设备通过链外通道向可信任用户 SA 的节点设备发送第一消息，该第一消息可包括：第一数据信息——余额 100，用户 A 对第一数据信息的数字签名 Sign 1。

20 [77]步骤 403，可信任用户 SA 的节点设备根据数据转化规则将第一数据信息——余额 100，转化为第二数据信息——被隐私保护的余额 hash(100)，并验证上述 Sign 1。

[78]步骤 404，在步骤 403 所述的验证都通过后，可信任用户 SA 的节点设备将第一消息所包含的第一数据信息——余额 100 保存在本地数据库中。可选的，可信任用户 SA 的节点设备可在本地数据库中设置一映射表格，用以记录上述第一数据信息和第二数据信息。

25

[79]步骤 405，可信任用户 SA 的节点设备对通过验证的第二数据信息进行数字签名 Sign 2。

[80]步骤 406，可信任用户 SA 的节点设备向区块链发送第二交易，该第二交易包括第二

数据信息——被保护余额 hash (100)，用户 A 对第一数据信息的数字签名 Sign1，用户 SA 对第二数据信息的数字签名 Sign 2。

[81]步骤 407，根据该区块链的共识规则，区块链上的共识节点对上述第二交易进行验证，上述验证包括验证用户 SA 是否属于用户 A 通过信任设置交易确定的可信任用户，
5 验证第二交易包括的数字签名分别是用户 A 和用户 A 确认的可信任用户 SA 所作出的。

[82]步骤 408，当步骤 407 所述的所有验证均通过后，该区块链的共识节点（具有共识权限的节点）将包括上述第二交易的区块收录到上述区块链的分布式数据库中，该区块链上的所有节点在其数据库中将用户 A 的余额状态更新为 hash (100)。

[83]同理，用户 B 也可将其账户中的余额状态隐私保护起来，具体方法可与步骤 401 至
10 408 类似，在此不再赘述。

[84]值得注意的是，在本说明书所提供的隐私交易方法为隐私转账交易时，为保证转出方用户的账户余额及转入方用户的账户余额可被可信任用户的节点设备验证，并发生相应的余额变动，转出方用户与转入方用户应至少信任一个相同的可信任用户，亦即转出方用户与转入方用户发送的信任设置交易中应包括至少一个相同的可信任用户的标识，
15 在本实施例中，可信任用户 SA 即为用户 A 的可信任用户，也为用户 B 的可信任用户。

[85]用户 A 完成向用户 B 转账的过程可具体包括：

[86]步骤 409，用户 A 的节点设备将用户 A 向用户 B 转账的交易消息 Txab 发送至用户 A 与用户 B 共同的可信任用户 SA 的节点设备；上述交易消息 Txab 包括用户 A、用户 B 的账户标识（账户地址或公钥）、转账金额 10，用户 A 对转账金额 10 的数字签名 Sign
20 (10)。

[87]步骤 410，可信任用户 SA 的节点设备根据数据转化规则将上述转账金额 10 转化为哈希摘要 hash (10)，验证用户 A 的账户余额 100 是否足以支付本次转账、验证上述 Sign (10)。

[88]步骤 411，在步骤 410 所述的验证都通过后，可信任用户 SA 的节点设备将上述转账消息中的转账金额 10 保存在本地数据库中；基于本次转账，可信任用户 SA 的节点设备还应在本地数据库中更改用户 A 和用户 B 的账户余额。
25

[89]步骤 412，可信任用户 SA 的节点设备对通过验证的受隐私保护的转账金额 hash(10) 进行数字签名 Sign 2 (hash (10))；并为转账完成后的用户 A 和用户 B 的账户余额生

成新的哈希摘要 hash (account A)、hash (account B) 进行数字签名 Sign (hash (account A))、Sign (hash (account B))。

[90] 步骤 413, 可信任用户 SA 的节点设备向区块链发送第二交易, 该第二交易包括被隐私保护的转账金额 hash (10), 转账完成后的用户 A 和用户 B 的账户余额生成新的哈希摘要 hash (account A) 和 hash (account B), 用户 A 对转账金额 10 的数字签名 Sign 1(10), 和用户 SA 的数字签名 Sign 2 (hash (10))、Sign (hash (account A))、Sign (hash (account B))。

[91] 步骤 414, 根据该区块链的共识规则, 区块链上的共识节点对上述第二交易进行验证, 上述验证包括验证用户 SA 是否属于用户 A 和用户 B 通过信任设置交易确定的可信任用户, 验证第二交易包括的数字签名 Sign 2 (hash (10)) 是用户 A 确认的可信任用户 SA 对上述转账金额的哈希摘要 hash(10) 所作出的、且用户 SA 的数字签名 Sign (hash (account A))、Sign (hash (account B)) 是用户 SA 分别对用户 A 和用户 B 的新的账户余额的哈希摘要 hash (account A)、hash (account B) 所作出的。

[92] 步骤 415, 当步骤 414 所述的所有验证均通过后, 该区块链的共识节点 (具有共识权限的节点) 将包括上述第二交易的区块收录到上述区块链的分布式数据库中, 该区块链上的所有节点在其数据库中将用户 A 的余额状态更新为 hash (account A), 将用户 B 的余额状态更新为 hash (account B)。

[93] 可选的, 为保证上述可信任用户 SA 的节点设备对转账发生后用户 A 和用户 B 的账户余额的更新经过用户 A 和用户 B 的认可, 用户 A 和用户 B 还可分别向上述可信任用户 SA 的节点设备发送自身更新后的账户余额、及基于上述更新后的账户余额的数字签名。以上具体的过程与本说明书各实施例所述的用户选择的可信任用户在区块链的分布式数据库中存储用户的受隐私保护的第二数据信息的过程类似, 在此不再赘述。

[94] 与上述流程实现对应, 本说明书的实施例还提供了一种基于区块链的隐私交易装置和一种基于区块链的隐私交易的应用装置。上述装置可以通过软件实现, 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, 作为逻辑意义上的装置, 是通过所在设备的 CPU (Central Process Unit, 中央处理器) 将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, 除了图 7 所示的 CPU、内存以及存储器之外, 网络风险业务的实现装置所在的设备通常还包括用于进行无线信号收发的芯片等其他硬件, 和/或用于实现网络通信功能的板卡等其他硬件。

[95]图 5 所示为一种基于区块链的隐私交易装置 50，应用于可信任用户的节点设备，其中，所述可信任用户由区块链的分布式数据库存储的信任设置交易确定，所述信任设置交易包括所述区块链用户对应的所有可信任用户的标识；所述装置 50 包括：

5 [96]接收单元 502，接收所述区块链用户发送的第一消息，所述第一消息包括未隐私保护的第一数据信息；

[97]转化单元 504，将所述未隐私保护的第一数据信息转化为受隐私保护的所述第二数据信息；

[98]存储单元 506，将所述第一数据信息保存在所述可信任用户的节点设备的本地数据库；

10 [99]发送单元 508，向所述区块链发送第二交易，所述第二交易包括所述第二数据信息，以使所述第二交易被验证后收录于所述区块链的分布式数据库中。

[100] 在又一示出的实施方式中，所述第一消息包括所述区块链用户至少对所述未隐私保护的第一数据信息所作的所述第一数字签名；

15 [101] 所述的装置 50 还包括验证单元 510：基于预设的验证规则验证所述第一消息，以在所述验证通过后将所述第一数据信息保存在所述可信任用户的节点设备的本地数据库，其中，所述预设的验证规则还包括：验证所述第一数字签名是由所述区块链用户至少对所述未隐私保护的第一数据信息所作。

[102] 在又一示出的实施方式中，所述第二交易还包括所述可信任用户至少对所述受隐私保护的所述第二数据信息所作的第二数字签名和所述区块链用户至少对所述未隐私保护的所述第一数据信息所作的所述第一数字签名。

20 [103] 在又一示出的实施方式中，所述的装置 50 还包括：

[104] 获取单元 512，从所述区块链的分布式数据库中获取所述信任设置交易；

[105] 确认单元 514，基于所述信任设置交易确认所述用户信任的其他可信任用户；

25 [106] 传输单元 516，将所述未隐私保护的第一数据信息和受隐私保护的所述第二数据信息链外传输至所述用户信任的其他可信任用户的节点设备，以使所述第一数据信息被验证由所述第二数据信息转化所得后，保存在所述其他可信任用户的节点设备的本地数据库中。

- [107] 在又一示出的实施方式中，所述接收单元 502，接收所述其他可信任用户至少基于所述第二数据信息所作的数字签名；
- [108] 所述第二交易还包括所述其他可信任用户至少基于所述第二数据信息所作的数字签名。
- 5 [109] 在又一示出的实施方式中，所述受隐私保护的所述第二数据信息为所述未隐私保护的第一数据信息的数据摘要。
- [110] 在又一示出的实施方式中，所述第一消息包括所述区块链用户向其他区块链用户的转账金额；所述第二交易包括受隐私保护的所述转账金额和所述区块链用户和所述其他区块链用户的受隐私保护的账户余额；
- 10 [111] 所述可信任用户也是所述其他区块链用户在信任设置交易中对应的可信任用户。
- [112] 图 6 所示为本说明书提供了一种基于区块链的隐私交易的应用装置 60，包括：
- [113] 获取单元 602，从所述区块链的分布式数据库获取由可信任用户的节点设备发送的第二交易，所述第二交易包括受隐私保护的所述第二数据信息，其中，所述可信任用户由区块链的分布式数据库存储的信任设置交易确定，所述信任设置交易包括所述区块链用户对应的所有可信任用户的标识；
- 15 [114] 接收单元 604，接收所述可信任用户的节点设备发送的未隐私保护的第一数据信息，所述第一数据信息被保存在所述可信任用户的节点设备的本地数据库；
- [115] 验证单元 606，验证所述受隐私保护的所述第二数据信息是否由所述未隐私保护的第一数据信息转化所得；
- 20 [116] 应用单元 608，执行对所述第二交易的应用逻辑。
- [117] 上述装置中各个单元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，相关之处参见方法实施例的部分说明即可，在此不再赘述。
- [118] 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
- 25 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单元或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。

[119] 上述实施例阐明的装置、单元、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
5 这些设备中的任意几种设备的组合。

[120] 与上述方法实施例相对应，本说明书的实施例还提供了一种计算机设备，该计算机设备包括存储器和处理器。其中，存储器上存储有能够由处理器运行的计算机程序；处理器在运行存储的计算机程序时，执行本说明书实施例中基于区块链的隐私交易方法的各个步骤。对基于区块链的隐私交易方法的各个步骤的详细描述请参见之前的内容，
10 不再重复。

[121] 与上述方法实施例相对应，本说明书的实施例还提供了一种计算机设备，该计算机设备包括存储器和处理器。其中，存储器上存储有能够由处理器运行的计算机程序；处理器在运行存储的计算机程序时，执行本说明书实施例中基于区块链的隐私交易的应用方法的各个步骤。对基于区块链的隐私交易的应用方法的各个步骤的详细描述请参见
15 之前的内容，不再重复。

[122] 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范围之内。

[123] 在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、
20 网络接口和内存。

[124] 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。

[125] 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。
25 数据。

[126] 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、磁盒式磁带, 磁带磁磁盘存储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。

- 5 [127] 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, 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。
- 10 [128] 本领域技术人员应明白, 本说明书的实施例可提供为方法、系统或计算机程序产品。因此, 本说明书的实施例可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且, 本说明书的实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

权利要求书

- 1、一种基于区块链的隐私交易方法，应用于可信任用户的节点设备，其中，所述可信任用户由区块链的分布式数据库存储的信任设置交易确定，所述信任设置交易包括所述区块链用户对应的所有可信任用户的标识；所述方法包括：
- 5 接收所述区块链用户发送的第一消息，所述第一消息包括未隐私保护的第一数据信息；
- 将所述未隐私保护的第一数据信息转化为受隐私保护的所述第二数据信息；
- 将所述第一数据信息保存在所述可信任用户的节点设备的本地数据库；
- 向所述区块链发送第二交易，所述第二交易包括所述第二数据信息，以使所述第二
- 10 交易被验证后收录于所述区块链的分布式数据库中。
- 2、根据权利要求 1 所述的方法，所述第一消息包括所述区块链用户至少对所述未隐私保护的第一数据信息所作的所述第一数字签名；
- 所述的方法，还包括：
- 基于预设的验证规则验证所述第一消息，以在所述验证通过后将所述第一数据信息
- 15 保存在所述可信任用户的节点设备的本地数据库，其中，所述预设的验证规则还包括：验证所述第一数字签名是由所述区块链用户至少对所述未隐私保护的第一数据信息所作。
- 3、根据权利要求 2 所述的方法，所述第二交易还包括所述可信任用户至少对所述受隐私保护的所述第二数据信息所作的第二数字签名和所述区块链用户至少对所述未隐私
- 20 保护的第一数据信息所作的所述第一数字签名。
- 4、根据权利要求 1 至 3 中任一权利要求所述的方法，还包括：
- 从所述区块链的分布式数据库中获取所述信任设置交易；
- 基于所述信任设置交易确认所述用户信任的其他可信任用户；
- 将所述未隐私保护的第一数据信息和受隐私保护的所述第二数据信息链外传输至所述
- 25 用户信任的其他可信任用户的节点设备，以使所述第一数据信息被验证由所述第二数据信息转化所得后，保存在所述其他可信任用户的节点设备的本地数据库中。
- 5、根据权利要求 4 所述的方法，还包括：
- 接收所述其他可信任用户至少基于所述第二数据信息所作的数字签名；
- 所述第二交易还包括所述其他可信任用户至少基于所述第二数据信息所作的数字
- 30 签名。
- 6、根据权利要求 1 所述的方法，所述受隐私保护的所述第二数据信息为所述未隐私保

护的第一数据信息的数据摘要。

7、根据权利要求1所述的方法，所述第一消息包括所述区块链用户向其他区块链用户的转账金额；所述第二交易包括受隐私保护的所述转账金额和所述区块链用户和所述其他区块链用户的受隐私保护的账户余额；

5 所述可信任用户也是所述其他区块链用户在信任设置交易中对应的可信任用户。

8、一种基于区块链内的隐私交易的应用方法，包括：

从所述区块链的分布式数据库获取由可信任用户的节点设备发送的第二交易，所述第二交易包括受隐私保护的所述第二数据信息，其中，所述可信任用户由区块链的分布式数据库存储的信任设置交易确定，所述信任设置交易包括所述区块链用户对应的所有可信任用户的标识；

10 接收所述可信任用户的节点设备发送的未隐私保护的第一数据信息，所述第一数据信息被保存在所述可信任用户的节点设备的本地数据库；

验证所述受隐私保护的所述第二数据信息是否由所述未隐私保护的第一数据信息转化所得，如果是，执行对所述第二交易的应用逻辑。

15 9、一种基于区块链的隐私交易装置，应用于可信任用户的节点设备，其中，所述可信任用户由区块链的分布式数据库存储的信任设置交易确定，所述信任设置交易包括所述区块链用户对应的所有可信任用户的标识；所述装置包括：

接收单元，接收所述区块链用户发送的第一消息，所述第一消息包括未隐私保护的第一数据信息；

20 转化单元，将所述未隐私保护的第一数据信息转化为受隐私保护的所述第二数据信息；
存储单元，将所述第一数据信息保存在所述可信任用户的节点设备的本地数据库；
发送单元，向所述区块链发送第二交易，所述第二交易包括所述第二数据信息，以使所述第二交易被验证后收录于所述区块链的分布式数据库中。

25 10、根据权利要求9所述的装置，所述第一消息包括所述区块链用户至少对所述未隐私保护的第一数据信息所作的所述第一数字签名；

所述的装置还包括验证单元：基于预设的验证规则验证所述第一消息，以在所述验证通过后将所述第一数据信息保存在所述可信任用户的节点设备的本地数据库，其中，所述预设的验证规则还包括：验证所述第一数字签名是由所述区块链用户至少对所述未隐私保护的第一数据信息所作。

30 11、根据权利要求10所述的装置，所述第二交易还包括所述可信任用户至少对所述受隐私保护的所述第二数据信息所作的所述第一数字签名和所述区块链用户至少对所述未隐

私保护的第一数据信息所作的第二数字签名。

12、根据权利要求 9 至 11 中任一权利要求所述的装置，还包括：

获取单元，从所述区块链的分布式数据库中获取所述信任设置交易；

确认单元，基于所述信任设置交易确认所述用户信任的其他可信任用户；

5 传输单元，将所述未隐私保护的第一数据信息和受隐私保护的所述第二数据信息链外传输至所述用户信任的其他可信任用户的节点设备，以使所述第一数据信息被验证由所述第二数据信息转化所得后，保存在所述其他可信任用户的节点设备的本地数据库中。

13、根据权利要求 12 所述的装置，

10 所述接收单元，接收所述其他可信任用户至少基于所述第二数据信息所作的数字签名；

所述第二交易还包括所述其他可信任用户至少基于所述第二数据信息所作的数字签名。

14、根据权利要求 9 所述的装置，所述受隐私保护的所述第二数据信息为所述未隐私保护的第一数据信息的数据摘要。

15 15、根据权利要求 9 所述的装置，所述第一消息包括所述区块链用户向其他区块链用户的转账金额；所述第二交易包括受隐私保护的所述转账金额和所述区块链用户和所述其他区块链用户的受隐私保护的账户余额；

所述可信任用户也是所述其他区块链用户在信任设置交易中对应的可信任用户。

16、一种基于区块链的隐私交易的应用装置，包括：

20 获取单元，从所述区块链的分布式数据库获取由可信任用户的节点设备发送的第二交易，所述第二交易包括受隐私保护的所述第二数据信息，其中，所述可信任用户由区块链的分布式数据库存储的信任设置交易确定，所述信任设置交易包括所述区块链用户对应的所有可信任用户的标识；

25 接收单元，接收所述可信任用户的节点设备发送的未隐私保护的第一数据信息，所述所述第一数据信息被保存在所述可信任用户的节点设备的本地数据库；

验证单元，验证所述受隐私保护的所述第二数据信息是否由所述未隐私保护的第一数据信息转化所得；

应用单元，执行对所述第二交易的应用逻辑。

30 17、一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行如权利要求 1 到 7 任意一项所述的方法。

18、一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行如权利要求 8 所述的方法。