

一种构建梅克尔树、简单支付验证方法及装置

技术领域

[01] 本说明书实施例涉及信息技术领域，尤其涉及一种构建梅克尔树、简单支付验证方法及装置。

5 背景技术

[02] 区块链网络是一种去中心化的、由多个节点参与的分布式数据存储系统。数据一旦被写入每个节点上的区块链，一方面，意味着数据在全网公开，另一方面，写入区块链的数据也难以被删除与篡改。基于此，在数据存证领域，区块链技术具有很大的应用前景。

- 10 [03] 然而，一方面，在实际应用中，有些数据（本文称之为敏感数据）一旦被写入区块链，就会造成不可消除的危害后果。例如，张三对李四进行诽谤，并将诽谤言论的文本文件上传到区块链网络进行存证，导致该文本文件被写入区块链，这相当于给李四的名誉造成不可消除的伤害。又如，A公司盗取B公司的商业机密，并将盗取的商业机密上传到区块链网络进行存证，导致该商业机密被写入区块链，这相当于给B公司造成不可挽回的损失。

[04] 另一方面，假设将上述的敏感数据从区块链中删除，那么很容易影响到针对其他数据（与所述敏感数据位于同一区块中的数据）的简单支付验证（Simplified Payment Verification, SPV）的准确性，从而影响数据存证业务的正常运行。

- 20 [05] 基于以上，如何既使得写入区块链的敏感数据不会被公开，又不会影响针对所述其他数据的存证业务的正常运行，是亟待解决的技术问题。

发明内容

[06] 为了使得写入区块链的敏感数据不会被公开，又不会影响针对所述其他数据的存证业务的正常运行，本说明书实施例提供一种构建梅克尔树、简单支付验证方法及装置，技术方案如下：

- 25 [07] 根据本说明书实施例的第1方面，提供一种构建梅克尔树的方法，包括：

[08] 目标全节点针对目标区块中的每个交易存储位置，从该交易存储位置读取数据；

所述目标全节点是区块链网络中的任一全节点，所述目标区块是所述目标全节点的区块链中的任一区块；

[09] 对从该交易存储位置读取的数据进行分析；

5 [10] 若确定从该交易存储位置读取的数据为交易，则对读取的交易进行哈希计算，得到交易哈希；

[11] 若确定从该交易存储位置读取的数据为隐匿化数据，则从所述隐匿化数据中提取交易哈希；其中，从所述隐匿化数据中提取的交易哈希，是该交易存储位置原本存储的交易的交易哈希；将该交易存储位置原本存储的交易替换成所述隐匿化数据的操作，是所述区块链网络中具有交易隐匿权限的节点指令各节点执行的；

10 [12] 基于所述目标区块中各交易存储位置分别对应的交易哈希，构建所述目标区块对应的梅克尔树。

[13] 根据本说明书实施例的第2方面，提供一种简单支付验证方法，包括：

[14] 目标全节点接收验证请求；所述验证请求包含目标交易标识；所述目标全节点是区块链网络中的任一全节点；

15 [15] 根据所述验证请求，在自身的区块链中确定所述目标交易标识对应的交易所在的区块，并基于上述的构建梅克尔树的方法构建所述区块对应的梅克尔树；

[16] 基于构建的梅克尔树，触发针对所述目标交易标识对应的交易的简单支付验证SPV流程。

20 [17] 根据本说明书实施例的第3方面，提供一种构建梅克尔树的装置，所述装置是区块链网络中的任一全节点，所述装置包括：

[18] 读取模块，针对目标区块中的每个交易存储位置，从该交易存储位置读取数据；所述目标区块是所述装置的区块链中的任一区块；

[19] 分析模块，对从该交易存储位置读取的数据进行分析；

25 [20] 交易哈希确定模块，若确定从该交易存储位置读取的数据为交易，则对读取的交易进行哈希计算，得到交易哈希；若确定从该交易存储位置读取的数据为隐匿化数据，则从所述隐匿化数据中提取交易哈希；其中，从所述隐匿化数据中提取的交易哈希，是该交易存储位置原本存储的交易的交易哈希；将该交易存储位置原本存储的交易替换成所述隐匿化数据的操作，是所述区块链网络中具有交易隐匿权限的节点指令各节点执行

的;

[21] 梅克尔树构建模块, 基于所述目标区块中各交易存储位置分别对应的交易哈希, 构建所述目标区块对应的梅克尔树。

[22] 根据本说明书实施例的第 4 方面, 提供一种简单支付验证装置, 所述装置是区块
5 链网络中的任一全节点, 所述装置包括:

[23] 接收模块, 接收验证请求; 所述验证请求包含目标交易标识;

[24] 确定构建模块, 根据所述验证请求, 在自身的区块链中确定所述目标交易标识对应的交易所在的区块, 并基于上述的构建梅克尔树的方法构建所述区块对应的梅克尔树;

[25] 触发模块, 基于构建的梅克尔树, 触发针对所述目标交易标识对应的交易的简单
10 支付验证 SPV 流程。

[26] 本说明书实施例所提供的技术方案, 如果写入区块链的某个交易是不宜公开的敏感数据, 那么, 区块链网络中的各节点可以将区块链中的该交易替换成该交易的交易哈希。一方面, 该交易的交易哈希是对该交易采用单向散列算法 (即哈希算法) 计算得到的, 由该交易的交易哈希无法逆推出该交易, 因此, 将该交易替换成该交易的交易哈希,
15 相当于将区块链中公示的该交易的明文内容加密后隐匿起来。另一方面, 将该交易替换成该交易的交易哈希, 并不会影响该交易所在区块对应的梅克尔树的稳定性, 也就不会影响到针对其他交易 (与该交易位于同一区块中的交易) 的简单支付验证 (Simplified Payment Verification, SPV) 的准确性, 从而保证了数据存证业务的正常运行。

[27] 应当理解的是, 以上的一般描述和后文的细节描述仅是示例性和解释性的, 并不能
20 限制本说明书实施例。

[28] 此外, 本说明书实施例中的任一实施例并不需要达到上述的全部效果。

附图说明

[29] 为了更清楚地说明本说明书实施例或现有技术中的技术方案, 下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍, 显而易见地, 下面描述中的附图仅仅
25 是本说明书实施例中记载的一些实施例, 对于本领域普通技术人员来讲, 还可以根据这些附图获得其他的附图。

[30] 图 1 是本说明提供的梅克尔树的结构示意图;

- [31] 图 2 是本说明书实施例提供的一种对写入区块链的交易进行隐匿的方法, 的流程示意图;
- [32] 图 3 是本说明书实施例提供的构造隐匿化数据的过程示意图;
- [33] 图 4 是本说明书实施例提供的构造隐匿化数据的另一过程示意图;
- 5 [34] 图 5 是本说明书实施例提供的一种区块链数据读取方法的流程示意图;
- [35] 图 6 是本说明书实施例提供的一种构建梅克尔树的方法的流程示意图;
- [36] 图 7 是本说明书实施例提供的一种简单支付验证方法的流程示意图;
- [37] 图 8 是本说明书实施例提供的一种对写入区块链的交易进行隐匿的装置的结构示意图;
- 10 [38] 图 9 本说明书实施例提供的一种对写入区块链的交易进行隐匿的装置的结构示意图;
- [39] 图 10 是本说明书实施例提供的一种区块链数据读取装置的结构示意图;
- [40] 图 11 是本说明书实施例提供的一种构建梅克尔树的装置的结构示意图;
- [41] 图 12 是本说明书实施例提供的一种简单支付验证装置的结构示意图;
- 15 [42] 图 13 是本说明书实施例提供的区块链系统的结构示意图;
- [43] 图 14 是用于配置本说明书实施例装置的一种计算机设备的结构示意图。

具体实施方式

- [44] 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。交易是区块链
- 20 协议中所约定的一种数据结构, 一笔数据要存入区块链, 就需要被封装成交易。
- [45] 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
- 25 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。

[46] 在基于区块链的数据存证场景下，交易一旦被写入区块链，就会被永久存证下来，不可被删除与篡改。然而，在实际应用中，如果写入区块链的交易后续被认定包含不宜公开的敏感数据，那么，如何使得写入区块链的敏感数据停止公开，就成为一个难以解决的技术问题。

[47] 假设将写入区块链的敏感交易（包含敏感数据的交易）直接删除，那么很容易导致基于区块链所运行的数据存证业务无法正常运行。原因具体为：

[48] 众所周知，考虑到有的节点的存储能力较弱，区块链网络中的节点存在全节点与轻节点之分。全节点的区块链中有完整的数据备份，即每个区块既包括区块头，也包括区块体；区块中的各交易存储于区块体中，基于区块中的各交易构建的梅克尔树的根哈希存储于区块头中。然而，轻节点的区块链中并没有完整的数据备份，即每个区块仅有区块头，并没有区块体。

[49] 当用户向某个轻节点请求验证自己之前上传的数据是否已被写入区块链时，由于轻节点的区块链中的每个区块仅包括区块头，因此，轻节点需要借助于全节点，才能针对某个交易是否已被写入区块链进行验证，这就是所谓的简单支付验证 SPV。

[50] 值得强调的是，在区块链技术领域，所谓简单支付验证，广义上是指针对某个交易，验证该交易是否已写入区块链。简单支付验证的原理是，轻节点向全节点请求验证某个交易（称为目标交易）是否已写入区块链，全节点首先会定位所述目标交易所在的区块（称为目标区块），然后基于目标区块中的各交易构建梅克尔树（Merkle trees），然后确定目标交易对应的梅克尔验证路径，并将目标交易对应的梅克尔路径所关联的哈希值返回给轻节点。轻节点会根据全节点返回的哈希值，验证目标交易对应的梅克尔路径是否正确，即根据目标交易的交易哈希与全节点返回的哈希值，计算梅克尔树的根哈希，并判断计算得到的根哈希与自身存储的目标区块的区块头中的根哈希是否一致，如果一致，就认定验证通过，证明目标交易确实已经被写入区块链中。

[51] 图 1 是本说明提供的梅克尔树的结构示意图。如图 1 所示，在梅克尔树中，各叶子节点与目标区块中存储的各交易一一对应。每个叶子节点上的哈希值是对相应的交易进行哈希运算得到的交易哈希。而针对每个父节点，该父节点上的哈希值是对该父节点的两个子节点上的哈希值进行哈希运算得到的。

[52] 假设目标交易包括交易 1。轻节点需要验证交易 1 是否被写入区块链中。于是，轻

节点向任一全节点发送请求，全节点首先会确定目标区块并构建出如图 1 所示的梅克尔树。然后，全节点会确定交易 1 对应的梅克尔路径所关联的哈希值为 Hash2、Hash10、Hash14，并将 Hash2、Hash10、Hash14 返回给轻节点。轻节点根据 Hash1（交易 1 的交易哈希）、Hash2、Hash10、Hash14，就可以计算得到梅克尔树的根哈希，然后，轻节点若发现计算得到的根哈希与目标区块的区块头中存储的根哈希一致，就认定交易 1 确实已经被写入区块链。

[53] 显然，在触发针对目标交易的简单支付验证之前，全节点通常需要基于目标区块中的各交易构建梅克尔树。这样，才能把目标交易对应的梅克尔路径所关联的哈希值返回给轻节点，从而触发针对目标交易的简单支付验证。这也意味着，交易 1~交易 8 中的任一交易被篡改或被删除，梅克尔树的根哈希（即 Hash1-8）就会发生改变，从而影响到简单支付验证的准确性。

[54] 例如，如图 1 所示，交易 2 包含敏感数据，如果直接将交易 2 从区块链中删除，那么，当需要针对交易 1、交易 3~8 中的任一交易进行简单支付验证时，由于缺少交易 2，只能基于交易 1、交易 3~8 构建梅克尔树，如此，构建的梅克尔树的根哈希与目标区块的区块头中存储的根哈希是不一致的，会导致简单支付验证出错。

[55] 为此，本说明书可以在对区块链系统中的简单支付验证不构成干扰的前提下，实现了对区块链中某个交易的隐匿。本说明书的核心技术手段是将区块链中需要被隐匿的交易替换成该交易的交易哈希。如此，既可以停止公开该交易的明文内容，又不会干扰到区块链系统中的简单支付验证体系的平稳运行。

[56] 为了使本领域技术人员更好地理解本说明书实施例中的技术方案，下面将结合本说明书实施例中的附图，对本说明书实施例中的技术方案进行详细地描述，显然，所描述的实施例仅仅是本说明书的一部分实施例，而不是全部的实施例。基于本说明书中的实施例，本领域普通技术人员所获得的所有其他实施例，都应当属于保护的范围。

[57] 以下结合附图，详细说明本说明书各实施例提供的技术方案。

[58] 图 2 是本说明书实施例提供的一种对写入区块链的交易进行隐匿的方法，的流程示意图，包括以下步骤：

[59] S200：执行节点获取目标交易标识。

[60] 本说明书所应用的场景为基于区块链的数据存证场景。在此场景下，由包括多个节点的区块链网络对数据进行分布式存证。

[61] 在本说明书实施例中，可以将交易隐匿权限授予区块链网路中的至少一个节点。本文将具有交易隐匿权限的节点称为执行节点。进一步地，区块链网络中的每个节点都可以是执行节点。

5 [62] 在本说明书实施例中，交易的交易标识用于唯一标识交易。具体地，交易的交易标识可以是对交易进行哈希运算后得到的交易哈希，也可以是为交易分配的唯一编号。

[63] 在步骤 S200 中，所述目标交易标识可以是某个用户发送给执行节点的。该用户可以是上传敏感数据的用户，也可以是有权要求隐匿敏感数据的主体（如法院、受害人等）。也就是说，在需要隐匿敏感数据的场景下，所述目标交易标识可以是包含所述敏感数据的交易的交易标识。

10 [64] 当然，本方案不仅可以实现对敏感数据的隐匿，也可以实现对非敏感数据的隐匿。因此，广义上讲，所述目标交易标识可以是任一交易的交易标识。

[65] S202：所述执行节点构建包含所述目标交易标识的隐匿指令，并向所述区块链网络广播所述隐匿指令。

15 [66] 具体地，所述执行节点可以对所述隐匿指令进行签名，并向所述区块链网络广播签名后的所述隐匿指令。

[67] S204：针对所述区块链网络中的每个节点，该节点根据所述隐匿指令，将区块链中对应于所述目标交易标识的交易替换成隐匿化数据。

[68] 针对区块链网络中的每个节点，该节点具体可以先对所述隐匿指令进行签名验证，若签名验证通过，则确认所述隐匿指令是所述执行节点发出的，并且，该节点需要确认
20 所述执行节点确实具有交易隐匿权限。然后，该节点才会执行交易隐匿操作。

[69] 进一步地，在实际应用中，如果每次交易隐匿操作的记录也需要写入区块链进行存证，那么，所述执行节点具体可以将所述隐匿指令封装成交易并向所述区块链网络广播。这样，区块链网络中的每个节点可以将封装成交易的所述隐匿指令写入区块链。

[70] 此处需要说明，在本说明书实施例，用于存储数据存证交易的区块链与用于存储
25 隐匿指令交易的区块链可以不是同一区块链。这样，针对所述区块链网络中的每个节点，该节点上需要维护两个区块链。

[71] 在本说明书实施例中，针对每个节点，该节点在接收到所述隐匿指令之后，需要构造隐匿化数据，并将所述目标交易标识对应的交易替换成构造的隐匿化数据。所述隐

匿化数据包括所述目标交易标识对应的交易的交易哈希。在本文中，交易的交易哈希是指，对交易进行一次哈希运算后得到的运算结果。

[72] 具体地，如果所述目标交易标识是相应的交易的交易哈希，那么，每个节点可以直接将所述交易哈希作为所述隐匿化数据。如果所述目标交易标识不是相应的交易的交易哈希，那么，每个节点可以先对所述目标交易标识对应的交易进行哈希运算，得到交易哈希，然后将所述交易哈希作为所述隐匿化数据。

[73] 随后，每个节点会将区块链中对应于所述目标交易标识的交易替换成隐匿化数据。

[74] 在本文中，所谓交易存储位置，是指区块链中，用于存储交易的存储空间或存储地址。假设区块链中写入了N个交易（N为大于1的自然数），那么，区块链中也同时有N个交易存储位置，分别用于存储这N个交易。

[75] 在本说明书实施例中，每个节点可以根据所述目标交易标识，在区块链中的各交易中进行遍历，以搜索所述目标交易标识对应的交易，也就是定位到所述目标交易标识对应的交易所在的交易存储位置。随后，从定位到的交易存储位置删除所述目标交易标识对应的交易，并向定位到的交易存储位置存入所述目标交易标识对应的交易的交易哈希。

[76] 进一步地，由于对于节点而言，根据目标交易标识在区块链中以遍历的方式定位交易效率较低，因此，在本说明书实施例中，每个节点可以预先针对写入区块链的任一交易，在区块链之外，另行记录该交易的交易标识与区块链中该交易所在的交易存储位置之间的对应关系。

[77] 其中，针对写入区块链的任一交易，区块链中该交易所在的交易存储位置，一般是该交易所在的区块的高度（即区块链中区块的顺位号）以及该交易在区块中的顺位号。例如，打包有交易A的区块被写入到区块链中第4个区块之后，即打包有交易A的区块的高度是5，并且，交易A是区块中的第10个交易。因此，交易A对应的交易存储位置可以是（5，10）。

[78] 区块链网络中的每个节点可以根据所述隐匿指令中包含的目标交易标识以及预先记录的交易标识与交易存储位置的对应关系，确定所述目标交易标识对应的交易存储位置，作为目标交易存储位置；然后，在区块链中直接定位到所述目标交易存储位置，并将区块链中存储于所述目标交易存储位置的交易替换成隐匿化数据。

[79] 此外，在本说明书实施例中，所述隐匿化数据除了包括所述目标交易标识对应的

交易的交易哈希之外，还可以包括更多信息。

[80] 具体地，图 3 是本说明书实施例提供的构造隐匿化数据的过程示意图。每个节点在构造隐匿化数据时，可以获取所述目标交易标识对应的交易的交易哈希；将预设的前标记字符拼接所述交易哈希的首部；根据所述前标记字符与所述交易哈希拼接成的数据，确定所述隐匿化数据。

[81] 进一步地，图 4 是本说明书实施例提供的构造隐匿化数据的另一过程示意图。每个节点在构造隐匿化数据时，可以获取所述目标交易标识对应的交易的交易哈希；将预设的前标记字符拼接所述交易哈希的首部，将预设的后标记字符拼接所述交易哈希的尾部，并且，将备注信息拼接所述后标记字符的尾部；然后，将所述前标记字符、所述交易哈希、所述后标记字符以及所述备注信息拼接成的数据确定为所述隐匿化数据。

[82] 需要说明的是，上述的前标记字符与后标记字符可以根据实际需要进行指定。例如，所述前标记字符可以为“OE”，所述后标记字符可以为“OF”。

[83] 还需要说明的是，所述备注信息具体可以是为实现特定业务需要所添加的信息。例如，所述备注信息可以是“hidden”，表明所述目标交易标识对应的交易已经被隐匿。

15 当用户查询所述目标交易标识对应的交易时，所述备注信息可以提示用户交易是不可见的。

[84] 值得强调的是，上述的前标记字符的作用是，当节点针对某个交易存储位置进行数据读取时，如果该交易存储位置的交易已经被替换成了隐匿化数据，那么，相当于所述隐匿化数据中的前标记字符向节点透露出信息：“该交易存储位置所存储的不是交易的明文内容，而是交易哈希”。此外，上述的后标记字符的作用是，当隐匿化数据中包括备注信息时，将隐匿化数据中的交易哈希与备注信息进行区隔，以便节点进行区分。

[85] 另外需要说明的是，在本说明书实施例中，每个节点执行的交易隐匿操作所对应的逻辑代码，可以预先被写入每个节点的固件中，也可以预先以智能合约的形式部署于每个节点上。

25 [86] 图 5 是本说明书实施例提供的一种区块链数据读取方法的流程示意图，包括如下步骤：

[87] S500：所述区块链网络中的任一节点接收数据读取请求。

[88] 在图 5 所示的方法中，所述数据读取请求可以是用户发送的。当用户想要查询区块链中的某个交易时，需要将包含该交易的交易标识的交易查询请求发送给所述区块链

网络中的任一节点。为了描述的方便，在对图 5 所示的方法的说明中，将用户想要查询的任一交易的交易标识称为目标交易标识。

5 [89] S502: 根据所述数据读取请求包含的目标交易标识以及预先记录的交易标识与交易存储位置的对应关系，确定所述目标交易标识对应的交易存储位置，作为目标交易存储位置。

[90] 如前文所述，在本说明书实施例中，针对写入区块链的任一交易，区块链网络中的各节点上可以预先记录该交易的交易标识与区块链中该交易所在的交易存储位置之间的对应关系。如此，节点可以直接根据所述交易查询请求中的目标交易标识，定位到区块链中所述用户所要查询的交易存储位置。

10 [91] S504: 从区块链中的所述目标交易存储位置读取数据，作为查询到的数据。

[92] 节点在定位到目标交易存储位置之后，可以直接从目标交易存储位置读取数据，然后针对所述数据读取请求，返回读取到的数据。

[93] 其中，若区块链中对应于所述目标交易标识的交易已被替换成隐匿化数据，则节点读取到的数据为隐匿化数据。若区块链中对应于所述目标交易标识的交易未已被替换成隐匿化数据，则节点读取到的数据为所述目标交易标识对应的交易。

[94] 显然，如果所述目标交易标识对应的交易因为包含有敏感数据已经被隐匿，那么，用户查询所述目标交易标识对应的交易时，节点返回给所述用户的实际上是隐匿化数据，用户并不能看到所述目标交易标识对应的交易的明文内容。

20 [95] 此外，如果隐匿化数据中不仅包括交易哈希，还包括前标记字符，那么，节点从所述目标交易存储位置读取隐匿化数据之后，可以分析出所述隐匿化数据中包含前标记字符，于是，节点可以针对所述数据读取请求，返回提示信息，以表明所述用户所述目标交易标识对应的交易已被替换成隐匿化数据。这种情况下，节点可以不返回隐匿化数据，仅返回一个提示信息进行说明即可。

25 [96] 或者，如果隐匿化数据中不仅包括交易哈希，还包括前标记字符、后标记字符与备注信息，节点从所述目标交易存储位置读取隐匿化数据之后，可以将所述备注信息返回给所述用户。这种情况下，节点也可以不向用户返回隐匿化数据。例如，所述备注信息是“hidden”，用户节点返回的备注信息后，就会得知所述目标交易标识对应的交易已经被隐匿。

[97] 此外，众所周知，针对区块链中的每个区块，在该区块被创设之初，会基于该区

块中的各交易构建如图 1 所示的梅克尔树，并计算梅克尔树的根哈希，将根哈希写入该区块的区块头中。该区块被写入区块链之后，一旦该区块中的交易被篡改或删除，就会导致基于区块中的各交易构建的梅克尔树的根哈希发生变化，与区块头中的根哈希不一致。正是因为如此，区块链中的数据是难以篡改与删除的。

- 5 [98] 当轻节点需要借助全节点进行简单支付验证时，全节点会根据轻节点提供的目标交易标识，确定所述目标交易标识对应的交易所在的区块，并基于该区块中的各交易构建梅克尔树。随后，才会基于构建的梅克尔树触发针对所述目标交易标识对应的交易的简单支付验证。

- 10 [99] 然而，在本说明书实施例中，针对区块链中的任一区块，该区块中的某个交易可能被替换成了隐匿化数据，基于此，本说明书相应提供一种改进后的构建梅克尔树的方法以及一种改进后的简单支付验证方法。

[100] 图 6 是本说明书实施例提供的一种构建梅克尔树的方法的流程示意图，包括如下步骤：

- 15 [101] S600：目标全节点针对目标区块中的每个交易存储位置，从该交易存储位置读取数据。

[102] 在图 6 所示的方法中，所述目标全节点是区块链网络中的任一全节点，所述目标区块是所述目标全节点的区块链中的任一区块。

[103] 在目标区块中，通常，每个交易都存储于各自的交易存储位置。如果某个交易被替换成了隐匿化数据，则原本存储该交易的交易存储位置当前存储的是该隐匿化数据。

- 20 [104] 目标全节点当需要构建所述目标区块对应的梅克尔树时，会从所述目标区块的每个交易存储位置读取数据。

[105] S602：对从该交易存储位置读取的数据进行分析。

[106] 目标全节点会针对每个交易存储位置，对从该交易存储位置读取的数据进行分析，以判断从该交易存储位置读取的数据是交易还是隐匿化数据。

- 25 [107] 具体地，由于交易是区块链协议中约定的一种数据结构，因此，目标全节点可以据此判断从该交易存储位置读取的数据是否为交易，如果不是交易，则是隐匿化数据。

[108] 此外，如果隐匿化数据不仅包括交易哈希，还包括前标记字符，那么，目标全节点也可以判断从该交易存储位置读取的数据是否为隐匿化数据，如果包含前标记字符，

就是隐匿化数据，如果不包含前标记字符，就是交易。

[109] S604: 若确定从该交易存储位置读取的数据为交易，则对读取的交易进行哈希计算，得到交易哈希。

5 [110] S606: 若确定从该交易存储位置读取的数据为隐匿化数据，则从所述隐匿化数据中提取交易哈希。

[111] 其中，从所述隐匿化数据中提取的交易哈希，是该交易存储位置原本存储的交易的交易哈希。将该交易存储位置原本存储的交易替换成所述隐匿化数据的操作，是所述区块链网络中具有交易隐匿权限的节点指令各节点执行的。

10 [112] 此处需要说明的是，如果所述隐匿化数据是由前标记字符与交易哈希拼接成的，那么，目标全节点具体可以将所述隐匿化数据中位于所述前标记字符之后的数据确定为交易哈希并提取。

[113] 如果所述隐匿化数据是由前标记字符、交易哈希、后标记字符、备注信息拼接成的，那么，目标全节点具体可以将所述隐匿化数据中位于所述前标记字符与所述后标记字符之间的数据确定为交易哈希并提取。

15 [114] S608: 基于所述目标区块中各交易存储位置分别对应的交易哈希，构建所述目标区块对应的梅克尔树。

[115] 图 7 是本说明书实施例提供的一种简单支付验证方法的流程示意图，包括如下步骤：

[116] S700: 目标全节点接收验证请求。

20 [117] 所述目标全节点是区块链网络中的任一全节点。所述验证请求具体可以是所述区块链网络中的任一轻节点发送的。

[118] S702: 根据所述验证请求，在自身的区块链中确定所述目标交易标识对应的交易所在的区块，构建所述区块对应的梅克尔树。

25 [119] 一般而言，目标全节点在触发针对所述目标交易标识对应的交易的简单支付验证流程之前，需要先定位所述目标交易标识对应的交易所在的区块，并基于该区块中当前包括的各交易，构建梅克尔树。需要说明的是，在步骤 S702 中，目标全节点基于图 5 所示的方法构建梅克尔树。

[120] 在步骤 S702 中，目标全节点可以根据所述目标交易标识以及预先记录的交易标识

与交易存储位置的对应关系，确定所述目标交易标识对应的交易存储位置，作为目标交易存储位置；然后，确定所述目标交易存储位置所属的区块，作为所述目标交易标识对应的交易所在的区块。

5 [121] S704：基于构建的梅克尔树，触发针对所述目标交易标识对应的交易的简单支付验证 SPV 流程。

[122] 在构建梅克尔树之后，目标全节点就可以触发针对所述目标交易标识对应的交易的简单支付验证 SPV 流程。

10 [123] 具体地，目标全节点会根据构建的梅克尔树，确定所述目标交易标识对应交易的梅克尔验证路径，并将所述梅克尔路径所关联的哈希值返回给轻节点，以便所述轻节点根据所述目标交易标识对应的交易的交易哈希以及所述目标全节点返回的哈希值，计算梅克尔树的根哈希，并将计算的根哈希与所述目标交易标识对应的交易所在的区块的区块头中的根哈希进行比对，如果一致，就认定通过验证，如果不一致，就认定未通过验证。

15 [124] 图 8 是本说明书实施例提供的一种对写入区块链的交易进行隐匿的装置的结构示意图，所述装置是区块链网络中具有交易隐匿权限的节点，所述装置包括：

[125] 获取模块 801，获取目标交易标识；

20 [126] 执行模块 802，构建包含所述目标交易标识的隐匿指令，并向所述区块链网络广播所述隐匿指令，以使所述区块链网络中的每个节点根据所述隐匿指令，将区块链中对应于所述目标交易标识的交易替换成隐匿化数据；所述隐匿化数据包括所述目标交易标识对应的交易的交易哈希。

[127] 图 9 本说明书实施例提供的一种对写入区块链的交易进行隐匿的装置的结构示意图，所述装置是区块链网络中的任一节点，所述装置包括：

[128] 处理模块 901，根据隐匿指令，将区块链中对应于所述目标交易标识的交易替换成隐匿化数据；所述隐匿化数据包括所述目标交易标识对应的交易的交易哈希；

25 [129] 其中，所述隐匿指令是执行节点根据获取的目标交易标识构建并向所述区块链网络广播的；所述执行节点是所述区块链网络中具有交易隐匿权限的节点。

[130] 本说明书实施例提供的一种区块链系统，包括由多个节点组成的区块链网络；

[131] 所述区块链网络中具有交易隐匿权限的节点，获取目标交易标识；构建包含所述

目标交易标识的隐匿指令，并向所述区块链网络广播所述隐匿指令；

[132] 所述区块链网络中的每个节点，根据所述隐匿指令，将区块链中对应于所述目标交易标识的交易替换成隐匿化数据；所述隐匿化数据包括所述目标交易标识对应的交易的交易哈希。

- 5 [133] 图 10 是本说明书实施例提供的一种区块链数据读取装置的结构示意图，所述装置为所述区块链网络中的任一节点，针对写入区块链的任一交易，区块链网络中的各节点上预先记录有该交易的交易标识与区块链中该交易所在的交易存储位置之间的对应关系，所述装置包括：

[134] 接收模块 1001，接收数据读取请求；

- 10 [135] 确定模块 1002，根据所述数据读取请求包含的目标交易标识以及预先记录的交易标识与交易存储位置的对应关系，确定所述目标交易标识对应的交易存储位置，作为目标交易存储位置；

[136] 读取模块 1003，从区块链中的所述目标交易存储位置读取数据，作为查询到的数据；

- 15 [137] 其中，若区块链中对应于所述目标交易标识的交易已被替换成隐匿化数据，则读取到的数据为所述隐匿化数据；所述隐匿化数据包括所述目标交易标识对应的交易的交易哈希；将所述目标交易标识对应的交易替换成隐匿化数据的操作，是所述区块链网络中具有交易隐匿权限的节点指令各节点执行的。

[138] 将所述目标交易标识对应的交易替换成隐匿化数据的操作如下：

- 20 [139] 获取所述目标交易标识对应的交易的交易哈希；

[140] 将预设的前标记字符拼接到所述交易哈希的首部；

[141] 根据所述前标记字符与所述交易哈希拼接成的数据，确定隐匿化数据；

[142] 将所述目标交易标识对应的交易替换成隐匿化数据。

[143] 根据所述前标记字符与所述交易哈希拼接成的数据，确定隐匿化数据，具体包括：

- 25 [144] 将预设的后标记字符拼接到所述交易哈希的尾部，并且，将备注信息拼接到所述后标记字符的尾部；

[145] 将所述前标记字符、所述交易哈希、所述后标记字符以及所述备注信息拼接成的

数据确定为所述隐匿化数据。

[146] 所述装置还包括:

[147] 提示模块 1004, 若读取到的数据包含所述前标记字符, 则针对所述数据读取请求, 返回提示信息, 以表明所述目标交易标识对应的交易已被替换成隐匿化数据。

5 [148] 所述装置还包括:

[149] 返回模块 1005, 针对所述数据读取请求, 返回读取到的数据。

[150] 一种区块链系统, 包括由多个节点组成的区块链网络; 针对写入区块链的任一交易, 区块链网络中的各节点上预先记录有该交易的交易标识与区块链中该交易所在的交易存储位置之间的对应关系;

10 [151] 所述区块链网络中的任一节点, 接收数据读取请求; 根据所述数据读取请求包含的目标交易标识以及预先记录的交易标识与交易存储位置的对应关系, 确定所述目标交易标识对应的交易存储位置, 作为目标交易存储位置; 从区块链中的所述目标交易存储位置读取数据;

[152] 其中, 若区块链中对应于所述目标交易标识的交易已被替换成隐匿化数据, 则读
15 取到的数据为所述隐匿化数据; 所述隐匿化数据包括所述目标交易标识对应的交易的交易哈希; 将所述目标交易标识对应的交易替换成隐匿化数据的操作, 是所述区块链网络中具有交易隐匿权限的节点指令各节点执行的。

[153] 图 11 是本说明书实施例提供的一种构建梅克尔树的装置的结构示意图, 所述装置是区块链网络中的任一全节点, 所述装置包括:

20 [154] 读取模块 1101, 针对目标区块中的每个交易存储位置, 从该交易存储位置读取数据; 所述目标区块是所述装置的区块链中的任一区块;

[155] 分析模块 1102, 对从该交易存储位置读取的数据进行分析;

[156] 交易哈希确定模块 1103, 若确定从该交易存储位置读取的数据为交易, 则对所述交易进行哈希计算, 得到交易哈希; 若确定从该交易存储位置读取的数据为隐匿化数据,
25 则从所述隐匿化数据中提取交易哈希; 其中, 从所述隐匿化数据中提取的交易哈希, 是该交易存储位置原本存储的交易的交易哈希; 将该交易存储位置存储的交易替换成所述隐匿化数据的操作, 是所述区块链网络中具有交易隐匿权限的节点指令各节点执行的;

[157] 梅克尔树构建模块 1104, 基于所述目标区块中各交易存储位置分别对应的交易哈

希，构建所述目标区块对应的梅克尔树。

[158] 将该交易存储位置存储的交易替换成所述隐匿化数据的操作如下：

[159] 获取该交易存储位置存储的交易的交易哈希；

[160] 将预设的前标记字符拼接到所述交易哈希的首部；

5 [161] 根据所述前标记字符与所述交易哈希拼接成的数据，确定隐匿化数据；

[162] 将该交易存储位置存储的交易替换成所述隐匿化数据。

[163] 根据所述前标记字符与所述交易哈希拼接成的数据，确定隐匿化数据，具体包括：

[164] 将预设的后标记字符拼接到所述交易哈希的尾部，并且，将备注信息拼接到所述后标记字符的尾部；

10 [165] 将所述前标记字符、所述交易哈希、所述后标记字符以及所述备注信息拼接成的数据确定为所述隐匿化数据。

[166] 所述分析模块 1102，若从该交易存储位置读取的数据不包含所述前标记字符，则确定从该交易存储位置读取的数据为交易；若从该交易存储位置读取的数据包含所述前标记字符，则确定从该交易存储位置读取的数据为隐匿化数据。

15 [167] 所述交易哈希确定模块 1103，将所述隐匿化数据中位于所述前标记字符之后的数据确定为交易哈希并提取。

[168] 所述交易哈希确定模块 1103，将所述隐匿化数据中位于所述前标记字符与所述后标记字符之间的数据确定为交易哈希并提取。

20 [169] 图 12 是本说明书实施例提供的一种简单支付验证装置的结构示意图，所述装置是区块链网络中的任一全节点，所述装置包括：

[170] 接收模块 1201，接收验证请求；所述验证请求包含目标交易标识；

[171] 确定构建模块 1202，根据所述验证请求，在自身的区块链中确定所述目标交易标识对应的交易所在的区块，并基于前述方法构建所述区块对应的梅克尔树；

25 [172] 触发模块 1203，基于构建的梅克尔树，触发针对所述目标交易标识对应的交易的简单支付验证 SPV 流程。

[173] 针对写入区块链的任一交易，区块链网络中的各节点上预先记录有该交易的交易标识与区块链中该交易所在的交易存储位置之间的对应关系；

- [174] 所述确定构建模块 1202, 根据所述目标交易标识以及预先记录的交易标识与交易存储位置的对应关系, 确定所述目标交易标识对应的交易存储位置, 作为目标交易存储位置; 确定所述目标交易存储位置所属的区块, 作为所述目标交易标识对应的交易所在的区块。
- 5 [175] 一种区块链系统, 包括: 由多个节点组成的区块链网络;
- [176] 所述区块链网络中的任一全节点, 针对目标区块中的每个交易存储位置, 从该交易存储位置读取数据, 所述目标区块是所述目标全节点的区块链中的任一区块; 对从该交易存储位置读取的数据进行分析; 若确定从该交易存储位置读取的数据为交易, 则对所述交易进行哈希计算, 得到交易哈希; 若确定从该交易存储位置读取的数据为隐匿化数据, 则从所述隐匿化数据中提取交易哈希, 其中, 从所述隐匿化数据中提取的交易哈希, 是该交易存储位置原本存储的交易的交易哈希; 将该交易存储位置存储的交易替换成所述隐匿化数据的操作, 是所述区块链网络中具有交易隐匿权限的节点指令各节点执行的; 基于所述目标区块中各交易存储位置分别对应的交易哈希, 构建所述目标区块对应的梅克尔树。
- 10 [177] 一种区块链系统, 包括: 由多个节点组成的区块链网络;
- [178] 所述区块链网络中的任一全节点, 接收验证请求, 所述验证请求包含目标交易标识; 根据所述验证请求, 在自身的区块链中确定所述目标交易标识对应的交易所在的区块, 并基于前述方法构建所述区块对应的梅克尔树; 基于构建的梅克尔树, 触发针对所述目标交易标识对应的交易的简单支付验证 SPV 流程。
- 15 [179] 图 13 是本说明书实施例提供的区块链系统的结构示意图。
- [180] 本说明书实施例还提供一种计算机设备, 其至少包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序, 其中, 处理器执行所述程序时实现图 2, 5~7 所示方法的功能。
- [181] 图 14 示出了本说明书实施例所提供的一种更为具体的计算设备硬件结构示意图,
- 25 该设备可以包括: 处理器 1410、存储器 1420、输入/输出接口 1430、通信接口 1440 和总线 1450。其中处理器 1410、存储器 1420、输入/输出接口 1430 和通信接口 1440 通过总线 1450 实现彼此之间在设备内部的通信连接。
- [182] 处理器 1410 可以采用通用的 CPU (Central Processing Unit, 中央处理器)、微处理器、应用专用集成电路 (Application Specific Integrated Circuit, ASIC)、或者一个或

多个集成电路等方式实现，用于执行相关程序，以实现本说明书实施例所提供的技术方案。

[183] 存储器 1420 可以采用 ROM (Read Only Memory, 只读存储器)、RAM (Random Access Memory, 随机存取存储器)、静态存储设备、动态存储设备等形式实现。存储器 1420 可以存储操作系统和其他应用程序，在通过软件或者固件来实现本说明书实施例所提供的技术方案时，相关的程序代码保存在存储器 1420 中，并由处理器 1410 来调用执行。

[184] 输入/输出接口 1430 用于连接输入/输出模块，以实现信息输入及输出。输入输出/模块可以作为组件配置在设备中（图中未示出），也可以外接于设备以提供相应功能。其中输入设备可以包括键盘、鼠标、触摸屏、麦克风、各类传感器等，输出设备可以包括显示器、扬声器、振动器、指示灯等。

[185] 通信接口 1440 用于连接通信模块（图中未示出），以实现本设备与其他设备的通信交互。其中通信模块可以通过有线方式（例如 USB、网线等）实现通信，也可以通过无线方式（例如移动网络、WIFI、蓝牙等）实现通信。

[186] 总线 1450 包括一通路，在设备的各个组件（例如处理器 1410、存储器 1420、输入/输出接口 1430 和通信接口 1440）之间传输信息。

[187] 需要说明的是，尽管上述设备仅示出了处理器 1410、存储器 1420、输入/输出接口 1430、通信接口 1440 以及总线 1450，但是在具体实施过程中，该设备还可以包括实现正常运行所必需的其他组件。此外，本领域的技术人员可以理解的是，上述设备中也可以仅包含实现本说明书实施例方案所必需的组件，而不必包含图中所示的全部组件。

[188] 本说明书实施例还提供一种计算机可读存储介质，其上存储有计算机程序，该程序被处理器执行时实现图 2，5~7 所示方法的功能。

[189] 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 [190] 通过以上的实施方式的描述可知，本领域的技术人员可以清楚地了解到本说明书实施例可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本说明书实施例的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如 ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本说明书实施例各个实施例或者实施例的某些部分所述的方法。

10 [191] 上述实施例阐明的系统、方法、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。

15 [192] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于方法和设备实施例而言，由于其基本相似于方法实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。以上所描述的方法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，在实施本说明书实施例方案时可以把各模块的功能在同一个或多个软件和/或硬件中实现。也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实施例方案的目的。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。

20

[193] 以上所述仅是本说明书实施例的具体实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本说明书实施例原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本说明书实施例的保护范围。