

基于区块链的业务数据加密方法及装置

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，尤其涉及一种基于区块链的业务数据加密方法及装置。

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。区块链账本分发给网络中的所有成员节点，在区块中永久记录网络中发生的业务数据的历史记录。由于账本是完全公开的，因此区块链账本本身无隐私保护功能，需通过额外的技术来保护业务数据的隐私。

发明内容

[03] 有鉴于此，本说明书一个或多个实施例提供一种基于区块链的业务数据加密方法及装置。

[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，提出了一种基于区块链的业务数据加密方法，应用于包括密钥分配方节点设备和密钥接收方节点设备的区块链，包括：

[06] 所述密钥接收方节点设备获取所述密钥分配方节点设备分配的第一派生密钥，所述第一派生密钥由所述密钥分配方的派生密钥基于所述密钥接收方的业务数据权限类型而派生生成，所述派生密钥可解密被所述第一派生密钥加密的业务数据；

[07] 基于所述第一派生密钥对业务数据进行加密以获得加密业务数据；

[08] 向所述区块链发送所述加密业务数据，以使所述加密业务数据被所述区块链共识验证后收录于所述区块链的分布式数据库。

[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业务数据加密装置，应用于包括密钥分配方节点设备和密钥接收方节点设备的区块链，包括：

- [10] 获取单元, 所述密钥接收方节点设备获取所述密钥分配方节点设备分配的第一派生密钥, 所述第一派生密钥由所述密钥分配方的派生密钥基于所述密钥接收方的业务数据权限类型而派生生成, 所述派生密钥可解密被所述第一派生密钥加密的业务数据;
- [11] 加密单元, 基于所述第一派生密钥对业务数据进行加密以获得加密业务数据;
- 5 [12] 发送单元, 向所述区块链发送所述加密业务数据, 以使所述加密业务数据被所述区块链共识验证后收录于所述区块链的分布式数据库。
- [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, 执行如上述基于区块链的业务数据加密方法。
- 10 [14] 本说明书提供的基于区块链的业务数据加密方法及装置, 用以进行业务数据加密的第一派生密钥是由密钥分配方的派生密钥基于密钥接收方的业务数据权限类型密钥派生而得到的; 由于所述密钥分配方的派生密钥可解密被所述第一派生密钥加密的业务数据, 所以所述密钥分配方可以对密钥接收方上传的业务数据进行解密、监督、及管理
- 15 生密钥也可以不相同, 因此基于上述不同的第一派生密钥加密的业务数据即可在不同业务数据权限类型的密钥接收方用户之间完成数据隐私隔离。

附图说明

- [15] 图 1 是一示例性实施例提供的一种基于区块链的业务数据加密方法的流程图;
- [16] 图 2 是一示例性实施例提供的密钥派生结构示意图;
- 20 [17] 图 3 是又一示例性实施例提供的密钥派生结构示意图;
- [18] 图 4 是一示例性实施例提供的一种基于区块链的业务数据加密装置的示意图;
- [19] 图 5 是运行本说明书所提供的基于区块链的业务数据加密装置实施例的一种硬件结构图。

具体实施方式

- 25 [20] 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说明书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、本说明书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。

[21] 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。

[22] 图 1 是一示例性实施例提供的一种基于区块链的业务数据加密方法的流程图，应用于包括密钥分配方节点设备和密钥接收方节点设备的区块链。

[23] 上述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的数据全备份。本领域的技术人员熟知，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无法比拟的保证数据安全、防攻击篡改的特性。

[24] 本实施例所述的密钥分配方节点设备和密钥接收方节点设备是在本实施例所提供的业务数据加密方法中分别执行密钥分配和密钥接收角色的节点设备；本领域的技术人员容易知道，对于同一用户，既可以作为密钥分配方向其他用户分配派生密钥，也可作为密钥接收方接收其他密钥分配方分配的派生密钥。

[25] 执行本实施例所述的基于区块链的业务数据加密方法的密钥接收方节点设备，既可以为备份有上述区块链的分布式数据库全部数据内容的全节点设备，也可仅为备份上述区块链的分布式数据库的部分数据内容的轻节点设备或客户端，在本说明书中不作限定。

[26] 本实施例所述的业务数据可以是所述区块链可共识收录至分布式数据库的业务相关数据。上述区块链可用于为一种或多种业务类型下产生的业务数据进行备份，上述业务类型可包括租房业务、车辆调度业务、保险理赔业务、信用服务、医疗服务等。该

区块链上的一些节点设备可能并不参与某种业务类型的运营交互，因此，为保证被区块链的分布式数据库收录的该种业务类型相关的业务数据的安全及隐私，该业务类型相关的业务数据需对上述一些节点设备保密；或者，该区块链上的一些节点设备即使参与了某种或某些业务类型的运营交互，其他参与方上传至区块链进行存证备份的业务数据出于安全性及隐私性的考量，仍需对上述一些节点设备保密。

[27] 鉴于以上所述的对业务数据的保密需求，如图 1 所示，本实施例提供的基于区块链的业务数据加密方法包括：

[28] 步骤 102，所述密钥接收方节点设备获取所述密钥分配方节点设备分配的第一派生密钥，所述第一派生密钥由所述密钥分配方的派生密钥基于所述密钥接收方的业务数据权限类型而派生生成，所述派生密钥可解密被所述第一派生密钥加密的业务数据。

[29] 本实施例所述的业务数据权限类型用于表征具有获知业务数据明文信息的权限的用户集合类型，例如，上述区块链可包括参与一种业务类型的多个用户，或参与多种业务类型的多个用户，因此不同的业务数据可分别对应有不同的用户集合，该不同的用户集合具有获知相应的业务数据的明文信息的权限，例如区块链用户 A、B、C 具有获知租房业务内的业务数据的权限；区块链用户 C、D、E 具有获知租车业务内的业务数据的权限；用户 A、B 具有获知北京地区租房业务的业务数据的权限，用户 C 具有获知上海地区租房业务的业务数据的权限。针对上述不同的业务数据所对应的不同的用户集合类型（如用户集合类型[A、B、C]、[C、D、E]、[A、B]、[C]等），即可划分出相应的业务数据权限类型。

[30] 上述业务数据权限类型还可进一步包括在时间、空间、或组织结构等多重维度上对具有获知业务数据明文信息的权限的用户集合的划分，例如区块链用户 A、B、C 在 2018 年具有获知租房业务内的业务数据的权限，属于司法部组织结构的区块链用户 C、D 具有获知法院判决书的业务数据的权限等等。本领域技术人员可以从区块链所运营的具体业务、及相关业务数据的具体划分或隔离模式设置多种多样的业务数据权限类型，均在本说明书的保护范围内。在本实施例中，上述用户对业务数据明文信息的获知，即可通过从区块链上获取被加密的业务数据，并基于用户接受到的派生密钥进行解密以达成。

[31] 密钥分配方是可由用户自身所持的派生密钥基于所述密钥接收方的业务数据权限类型而派生生成下级派生密钥（如本实施例所述的第一派生密钥）的用户；所述密钥分配方的派生密钥可解密其所派生出的任何下级派生密钥所加密的业务数据。上述密钥接

收方接收的第一派生密钥可由所述密钥分配方的派生密钥经过一级派生得出，也可由所述密钥分配方的派生密钥经过多级派生而得出，在此不作限定。

[32] 值得注意的是，本实施例所述密钥分配方的派生密钥，既可以是由其他密钥分配方派生分配至所述密钥分配方的子派生密钥，也可以是所述密钥分配方自持的根派生密钥，在此不做限定。无论是所述密钥分配方的派生密钥属于子派生密钥还是根派生密钥，均可再继续派生出下级派生密钥（如第一派生密钥）以进行密钥分配。

[33] 由于密钥分配方的派生密钥可解密被其下级派生密钥（如密钥接收方的第一派生密钥）加密的业务数据，因此本实施例所述的密钥分配方可以作为密钥接收方的上级监管机构或平台，用以对上述密钥接收方发送的加密业务数据进行监督和管理。上述密钥分配方基于上述密钥接收方所属的业务数据权限类型，为上述密钥接收方分配相应的第一派生密钥；对应于同一业务数据权限类型的多个密钥接收方，均获得相同的第一派生密钥；对应于不同业务数据权限类型的多个密钥接收方，将获得不同的第一派生密钥。

[34] 所述密钥接收方节点设备获取所述密钥分配方节点设备分配的第一派生密钥的具体方式，即可以通过区块链的分布式数据库进行链上获取，也可以通过链外通道进行点对点通信传输；相较于通过链外通道进行点对点通信传输的获取方式，通过链上获取第一派生密钥，由于第一派生密钥被区块链的节点共识验证后收录于区块链的分布式数据库，因此可保证上述第一派生密钥的准确性，防止上述第一派生密钥被篡改。

[35] 值得注意的是，为保证基于上述链上获取的方式获取上述第一派生密钥时，该第一派生密钥不被其他用户从链上获得后危及被加密的业务数据的私密安全性，上述全部或部分的第一派生密钥可被具有获得该第一派生密钥权限（即相应的业务数据权限）的密钥接收方的用户公钥加密，由此，密钥接收方可基于用户私钥进行解密而获知该第一派生密钥。

[36] 关于数据的加密方式通常可分为对称加密和非对称加密。在一种示出的实施方式中，所述密钥分配方的派生密钥为对称加密密钥，相应地，由所述派生密钥派生出的第一派生密钥也为对称加密密钥，亦即上述派生密钥或第一派生密钥既可用于对业务数据进行加密，也可用于对被上述派生密钥或第一派生密钥加密的业务数据进行解密。当所述密钥接收方节点设备从如上所述的链上通道获取第一派生密钥时，为保证上述第一派生密钥的安全隐私性，上述密钥接收方节点设备从所述区块链的分布式数据库中获取被加密的第一派生密钥，所述第一派生密钥被基于所述密钥接收方的用户公钥加密；相应地，上述密钥接收方节点设备基于所述密钥接收方的用户私钥解密上述被加密的第一派

生密钥，以获取所述第一派生密钥。

[37] 在又一示出的实施方式中，所述密钥分配方的派生密钥为非对称加密的密钥对，即公钥-私钥对，相应地，由所述派生密钥派生出的密钥也应为非对称加密密钥对：上述第一派生密钥包括的一对密钥分别为第一派生公钥和与该第一派生公钥对应的第一派生私钥。由于被上述第一派生公钥加密的业务数据需要被第一派生私钥来解密以获取业务数据的明文，因此，具有业务数据解密需求的密钥接收方通常仍需获取与上述第一派生密钥对应的第一派生私钥。同理，上述第一派生私钥既可以通过区块链的分布式数据库进行链上获取，也可以通过链外通道进行点对点通信传输；相较于通过链外通道进行点对点通信传输的获取方式，通过链上获取第一派生私钥，由于第一派生私钥被区块链的节点共识验证后收录于区块链的分布式数据库，因此可保证上述第一派生私钥的准确性，防止上述第一派生私钥被篡改。

[38] 相似地，为保证基于上述链上获取的方式获取上述第一派生私钥时，该第一派生私钥不被其他用户从链上获得后危及被加密的业务数据的私密安全性，上述第一派生私钥可被具有获得该第一派生密钥权限（即相应的业务数据权限）的密钥接收方的用户公钥加密，由此，密钥接收方可基于用户私钥进行解密而获知该第一派生私钥。

[39] 可选的，上述密钥分配方向区块链的分布式数据库上发布被密钥接收方的用户公钥加密的第一派生私钥，可基于上述密钥接收方的请求而启动：上述密钥接收方应向所述区块链发送对所述第一派生私钥的请求交易，其中，所述请求交易被所述密钥接收方的用户私钥加密，以使所述密钥分配方节点设备在基于所述密钥接收方的用户公钥对所请求交易验证通过后，向所述区块链发送被所述密钥接收方的用户公钥加密的第一派生私钥。上述对请求交易的验证可以包括对密钥接收方的身份验证，及对密钥接收方对应的业务数据权限类型是否与该第一派生私钥对应的验证，等等。

[40] 在本实施例中，第一派生公钥由于作为公钥可以被任何用户获知，因此密钥分配方可将第一派生密钥以明文的形式发布于区块链的分布式数据库上，以供密钥接收方直接获取。当然，上述第一派生密钥可以与其对应的第一派生私钥在密钥分配方发送的同一交易中被发布，也可在密钥分配方发送的不同交易中被发布，在此不作限定。

[41] 值得注意的是，由于本实施例中的第一派生密钥所包括的两个密钥（第一派生公钥和第一派生私钥）均是由密钥分配方的派生密钥计算派生的，可选择第一派生密钥中任意一个密钥为第一派生公钥，另一个密钥则为第一派生私钥。

[42] 更优地，区块链系统可为不同的业务数据权限类型设置标识，为方便区块链上具有相同业务数据权限类型的用户使用其第一派生密钥以解密或加密相应的业务数据，本实施例所述的密钥接收方在获得上述第一派生密钥后，可在本地数据库存储上述第一派生密钥与其业务数据权限类型的标识的映射关系，以方便用户对第一派生密钥的查询及使用。

[43] 关于以上实施例所述的由上述派生密钥派生出第一派生密钥的过程，可以基于相关的密钥派生函数计算获得，在一种示出的实施方式中，上述第一派生密钥是由上述密钥分配方的派生密钥基于所述密钥接收方的业务数据查看权限类型进行 KDF 计算而派生生成的密钥。

10 [44] 本领域的技术人员应知，通过 KDF 技术可以任意生成密钥树，只需要保管一把根密钥即可根据派生路径实时派生计算出各级节点具体的派生密钥，密钥树上各级节点的派生密钥可以由其父节点的派生密钥派生生成，子节点无法计算出其父节点的派生密钥。由于本说明书所提供的各个实施例并不限定由所述密钥分配方的派生密钥基于所述密钥接收方的业务数据权限类型而派生生成第一派生密钥的具体派生级数（至少为一级派生），因此本说明书各实施例所述的密钥分配方的派生密钥既可以为 KDF 密钥树的根密钥，也可以为 KDF 密钥树的任意非叶子节点的派生密钥。由于区块链用户在具体的业务处理中可以有多种不同的业务数据权限类型，KDF 密钥树的不同节点可以相应配置不同的业务数据权限类型所对应的派生密钥、或派生公钥-私钥对。

20 [45] 图 2 和图 3 分别示意了一种具体业务模式中的 KDF 密钥树派生结构示意图。图 2 所示的 KDF 密钥树的根密钥为公钥-私钥对，则由该根密钥派生而出的任何节点的派生密钥均为公钥-私钥对，KDF 密钥树的父节点可以推导派生出其任意子节点，因此父节点可解密其任意子节点所加密的业务数据，获得父节点派生密钥的区块链用户即可对获得子节点派生密钥的区块链用户所加密的业务数据进行解密、监管等。

25 [46] 为保证派生密钥的安全性，密钥分配方可定期更新派生密钥，在图 2 所示的 KDF 密钥树结构中，获得根节点密钥的密钥分配方用户为不同的年份时间内的业务数据分别派生了不同的派生密钥，如 2017 年、2018 年、2019 年、2020 年，以上各个年份均对应相应的业务数据权限类型。上述不同年份的派生密钥可在区块链中作备份，例如，以获得上述对应年份的密钥分配方的用户公钥作加密并备份在区块链的分布式数据库中，从而协助上述密钥分配方为历史业务数据进行查阅。值得注意的是，图 2 所示的获得不同年份的派生密钥（第二级派生密钥）的区块链用户作为密钥接收方，既可以仍是

持有获得根节点密钥的密钥分配方自身，也可以是持有根节点密钥的密钥分配方基于业务数据权限类型为其分配密钥的其他区块链用户。

[47] 图 2 所示的 KDF 密钥树结构中的不同叶子节点与不同的业务数据权限类型相对应，具有相同的业务数据权限类型的区块链用户可共享该叶子节点对应的公私钥对。本领域的技术人员应知，图 2 所示的第三级派生密钥（此时的叶子节点）还可继续向下扩充派生（图中未示），由具有相应业务数据权限的用户作为密钥分配方，为其监管的业务数据进行进一步的数据隐私隔离管理，亦即，上述第三级派生密钥作为父级派生密钥，由持有该第三级派生密钥的某区块链用户（作为密钥分配方），基于其他区块链用户对上述某区块链用户可获知的业务数据（即其监管的业务数据）所具有的、不同的业务数据权限类型进行下级密钥派生。

[48] 图 3 示意了多链共享根节点的 KDF 密钥派生结构，不同的区块链内的派生密钥可由同一根节点密钥派生而来。该种密钥派生结构特别适用于包括基于多种业务类型而构建的多条联盟链的多链系统，例如区块链 1 为运营房屋租赁业务的联盟链，区块链 2 为运营共享租车业务的联盟链，上述多链系统可具有一个统一的密钥分配方以持有该根节点密钥，该密钥分配方可以为上述多链系统的总监管机构（如政府行政机构）、或该多链系统的建设机构等等。

[49] 由于同一密钥接收方可能具有不同的业务数据权限类型，如图 3 所示的区块链用户 A 既具有联盟链 1 中的一种业务数据权限类型，也具有联盟链 2 中的一种业务数据权限类型；区块链用户 B 既具有联盟链 2 中的两种业务数据权限类型。为方便作为密钥接收方的区块链用户 A 或 B 为相应的业务数据进行加密而不混淆其应使用的派生密钥（即上述实施例所述的第一派生密钥），密钥接收方的节点设备可以本地数据库中存储关于第一派生密钥与其对应的业务数据权限类型的映射关系表。

[50] 值得注意的是，在 KDF 密钥树中由父节点（对应有密钥分配方）生成子节点（对应有密钥接收方）的过程通常可采用注记词（seed）协助派生的方式，具体的注记词由密钥分配方定义，以协助其计算生生子节点。助记词通常可选用一些易于记忆的词语，便于密钥分配方管理基于各种业务数据权限类型而生成的多个派生密钥，而且在除根密钥外的任何派生密钥丢失的情况下，可以由持有根密钥的密钥分配方根据助记词重新派生或恢复出各级别的派生密钥。例如，以规则：/联盟链标识/时间（年）/业务类型/构建的 KDF 密钥树，可选用示例为/溯源行业链/2018/ABC/的助记词，即该联盟链名称为“溯源行业链”，派生密钥用于 2018 年，业务数据权限类型是业务数据在联盟参与方 A、B、

C 间可见。

[51] 步骤 104, 基于所述第一派生密钥对业务数据进行加密以获得加密业务数据。

[52] 本实施例所述对业务数据的具体加密方式可以有多种, 例如, 当上述第一派生密钥为对称加密密钥时, 可使用所述第一派生密钥对所述业务数据进行加密以获得第一加密业务数据; 所述加密业务数据包括所述第一加密业务数据。具有相同业务数据权限类型的区块链用户, 即可利用上述一种或多种实施例所述的获取第一派生密钥的方法获取第一派生密钥, 并对从区块链的分布式数据库上获取的上述加密业务数据进行解密, 以获得该业务数据的明文信息。

[53] 又如, 当上述第一派生密钥为非对称密钥(对)时, 可使用所述第一派生公钥对所述业务数据进行加密以获得第一加密业务数据; 所述加密业务数据包括所述第一加密业务数据。由于被第一派生公钥加密的数据需使用第一派生私钥来解密, 具有相同业务数据权限类型的区块链用户, 即可利用上述一种或多种实施例所述的获取第一派生私钥的方法获取与第一派生密钥对应的第一派生私钥, 基于所述第一派生私钥对从区块链的分布式数据库上获取的上述加密业务数据进行解密, 以获得该业务数据的明文信息。

[54] 上述两种实施方式所述的利用第一派生密钥或第一派生公钥对业务数据加密, 既可以包括对一条交易内的全部业务数据进行加密, 也可以包括对一条交易内的部分业务数据进行加密; 既可以包括对业务数据进行直接加密, 也可以包括对业务数据的密文再进行加密。

[55] 除了上述两种实施方式所述的使用第一派生密钥或第一派生公钥对全部或部分的业务数据进行加密以生成加密业务数据外, 还可使用第一派生密钥或第一派生公钥对全部或部分的业务数据的密文对应的解密密钥进行加密以生成加密业务数据。例如, 当上述第一派生密钥为对称加密密钥时, 持有第一派生密钥的密钥接收方可先使用第三加密密钥对业务数据进行加密以获得第二加密业务数据; 然后再使用第一派生密钥对上述第三加密密钥对应的第三解密密钥进行加密以获得第三加密密钥数据; 发往区块链的加密业务数据应包括上述第二加密业务数据和第三加密密钥数据。本领域技术人员容易知道的是, 上述利用第三加密密钥进行加密的方法, 既可以是对称加密也可以是非对称加密; 当第三加密密钥为对称加密方法所使用的密钥时, 上述第三解密密钥与第三加密密钥相同; 当第三加密密钥为非对称加密方法所使用的密钥时, 上述第三解密密钥为与第三加密密钥对应的私钥或公钥。

- [56] 又如，当上述第一派生密钥为非对称加密密钥（对）时，持有第一派生密钥的密钥接收方可先使用第三加密密钥对业务数据进行加密以获得第二加密业务数据；然后再使用第一派生公钥对上述第三加密密钥对应的第三解密密钥进行加密以获得第三加密密钥数据；发往区块链的加密业务数据应包括上述第二加密业务数据和第三加密密钥数据。
- 5 由于被第一派生公钥加密的数据需使用第一派生私钥来解密，具有相同业务数据权限类型的区块链用户，即可利用上述一种或多种实施例所述的获取第一派生私钥的方法获取与第一派生密钥对应的第一派生私钥，基于所述第一派生私钥对从区块链的分布式数据库上获取的上述第三加密密钥数据和第二加密业务数据依次进行解密，以获得该业务数据的明文信息。本领域技术人员容易知道的是，上述利用第三加密密钥进行加密的方法，既可以是对称加密也可以是非对称加密；当第三加密密钥为对称加密方法所使用的密钥时，上述第三解密密钥与第三加密密钥相同；当第三加密密钥为非对称加密方法所使用的密钥时，上述第三解密密钥为与第三加密密钥对应的私钥或公钥。
- 10 [57] 步骤 106，向所述区块链发送所述加密业务数据，以使所述加密业务数据被所述区块链共识验证后收录于所述区块链的分布式数据库。
- 15 [58] 在一示出的实施例中，将所述加密业务数据收录于所述区块链的分布式数据库中的具体过程，可以包括：
- [59] 确定满足所述区块链共识机制的共识记账节点；
- [60] 所述共识记账节点将所述加密业务数据加入到候选区块；
- [61] 所述共识记账节点向所述区块链的节点广播所述候选区块；
- 20 [62] 在所述候选区块通过所述区块链符合预设数量的节点的验证认可后，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。
- [63] 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。为降低交易或数据的确认时间、提高交易吞吐量、满足对安全性和性能的需求，尤其为基于不同的业务类型构建包含不同节点用户的区块链，本说明书所提供的实施例还可选用联盟链架构来构建该区块链。联盟链通常多采用权益证明或 PBFT、RAFT 等共识算法；由于采用该种算法共识的效率，可满足高频交易量的需求，且共识的时延很低，能快速地在区块链的新生区块中收录上述加密业务数据；而且，将联盟链网络中可信节点作为预选的记账节点，兼顾了安全性与稳定性；另外，采用 PBFT 算法不会消耗过多的计算机算力资源，也不一定需要代币流通，因此具有良
- 25

好的可使用性。

[64] 为方便区块链上具有相同业务数据权限类型的用户解密上述多种实施例所提供的加密业务数据，还可将上述第一派生密钥对应的业务数据权限类型标识与上述加密业务数据一起发送至区块链的分布式数据库；区块链用户在获取到上述业务数据权限类型标识后，可在本地数据库中查询该业务数据权限类型标识对应的解密密钥（第一派生密钥或第一派生私钥），从而方便快捷地对上述加密业务数据进行解密。

[65] 上述一个或多个实施例所述的基于区块链的数据加密方法，密钥分配方基于业务数据权限类型为密钥接收方派生分配密钥，由于密钥分配方的派生密钥可以解密其派生出的任意一级的派生密钥，所以密钥分配方即可监督管理其对应的密钥接收方的业务数据。由于密钥分配方也可作为其他更高级密钥分配方的密钥接收方，亦即，该密钥分配方的派生密钥是由其他更高级密钥分配方的派生密钥派生而来的，由此可依据区块链运营业务所涉及的用户业务关系（如监督与被监督关系、数据共享关系、数据不能共享关系等），建立起相应的派生密钥树，从而既保证了业务数据在具有不同业务数据权限类型的用户之间的隔离，也保证了业务数据可被高级业务数据权限类型的用户监督；既保证了业务数据的安全隐私性，又保证了业务数据的可被监管性。

[66] 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公共交通数据处理装置。该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 5 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。

[67] 图 4 所示为一种基于区块链的业务数据加密装置 40，应用于包括密钥分配方节点设备和密钥接收方节点设备的区块链，包括：

[68] 获取单元 402，所述密钥接收方节点设备获取所述密钥分配方节点设备分配的第一派生密钥，所述第一派生密钥由所述密钥分配方的派生密钥基于所述密钥接收方的业务数据权限类型而派生生成，所述派生密钥可解密被所述第一派生密钥加密的业务数据；

[69] 加密单元 404，基于所述第一派生密钥对业务数据进行加密以获得加密业务数据；

[70] 发送单元 406，向所述区块链发送所述加密业务数据，以使所述加密业务数据被所

述区块链共识验证后收录于所述区块链的分布式数据库。

[71] 在又一示出的实施方式中，所述密钥分配方的派生密钥和所述密钥接收方的第一派生密钥均为对称加密密钥；所述获取单元 402：

[72] 所述密钥接收方节点设备从所述区块链的分布式数据库中获取被加密的第一派生密钥，所述第一派生密钥被基于所述密钥接收方的用户公钥加密；

[73] 基于所述密钥接收方的用户私钥解密上述被加密的第一派生密钥，以获取所述第一派生密钥。

[74] 在又一示出的实施方式中，所述密钥分配方的派生密钥和所述密钥接收方的第一派生密钥均为非对称加密密钥对，所述第一派生密钥包括第一派生公钥和第一派生私钥；

10 [75] 所述获取单元 402：

[76] 从所述区块链的分布式数据库中获取所述第一派生公钥和被所述密钥接收方的用户公钥加密的第一派生私钥。

[77] 在又一示出的实施方式中，所述发送单元 406：

[78] 向所述区块链发送对所述第一派生私钥的请求交易，其中，所述请求交易被所述密钥接收方的用户私钥加密，以使所述密钥分配方节点设备在基于所述密钥接收方的用户公钥对所述请求交易验证通过后，向所述区块链发送被所述密钥接收方的用户公钥加密的第一派生私钥。

[79] 在又一示出的实施方式中，所述第一派生密钥是由所述密钥分配方的派生密钥基于所述密钥接收方的业务数据查看权限类型进行 KDF 计算而派生生成的密钥。

20 [80] 在又一示出的实施方式中，所述加密单元 404：

[81] 使用所述第一派生密钥对所述业务数据进行加密以获得第一加密业务数据；

[82] 所述加密业务数据包括所述第一加密业务数据。

[83] 在又一示出的实施方式中，所述加密单元 404：

[84] 使用所述第一派生公钥对所述业务数据进行加密以获得第一加密业务数据；

25 [85] 所述加密业务数据包括所述第一加密业务数据。

[86] 在又一示出的实施方式中，所述加密单元 404：

[87] 使用第三加密密钥对所述业务数据进行加密以获得第二加密业务数据；

- [88] 使用所述第一派生密钥对所述第三加密密钥对应的第三解密密钥进行加密以获得第三加密密钥数据;
- [89] 所述加密业务数据包括第二加密业务数据和第三加密密钥数据。
- [90] 在又一示出的实施方式中, 所述加密单元 404:
- 5 [91] 使用第三加密密钥对所述业务数据进行加密以获得第二加密业务数据;
- [92] 使用所述第一派生公钥对所述第三加密密钥对应的第三解密密钥进行加密以获得第三加密密钥数据;
- [93] 所述加密业务数据包括第二加密业务数据和第三加密密钥数据。
- [94] 在又一示出的实施方式中, 所述的装置 40 还包括:
- 10 [95] 存储单元 408, 将所述第一派生密钥与所述业务数据权限类型的标识对应保存于所述密钥接收方的本地数据库中。
- [96] 在又一示出的实施方式中, 所述发送单元 406:
- [97] 向所述区块链发送所述加密业务数据和所述业务数据权限类型的标识。
- [98] 上述装置中各个单元和模块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。
- 15 [99] 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。
- 20 [100] 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数据加密方法的各个步骤。对基于区块链的数据加密方法的各个步骤的详细描述请参见之前的内容,
- 25 不再重复。
- [101] 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。

[102] 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、网络接口和内存。

[103] 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。

[104] 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。

[105] 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。

[106] 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。

[107] 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、一种基于区块链的业务数据加密方法，应用于包括密钥分配方节点设备和密钥接收方节点设备的区块链，包括：

5 所述密钥接收方节点设备获取所述密钥分配方节点设备分配的第一派生密钥，所述第一派生密钥由所述密钥分配方的派生密钥基于所述密钥接收方的业务数据权限类型而派生生成，所述派生密钥可解密被所述第一派生密钥加密的业务数据；

基于所述第一派生密钥对业务数据进行加密以获得加密业务数据；

向所述区块链发送所述加密业务数据，以使所述加密业务数据被所述区块链共识验证后收录于所述区块链的分布式数据库。

10 2、根据权利要求 1 所述的方法，所述密钥分配方的派生密钥和所述密钥接收方的第一派生密钥均为对称加密密钥；所述密钥接收方节点设备获取所述密钥分配方节点设备分配的第一派生密钥，包括：

所述密钥接收方节点设备从所述区块链的分布式数据库中获取被加密的第一派生密钥，所述第一派生密钥被基于所述密钥接收方的用户公钥加密；

15 基于所述密钥接收方的用户私钥解密上述被加密的第一派生密钥，以获取所述第一派生密钥。

3、根据权利要求 1 所述的方法，所述密钥分配方的派生密钥和所述密钥接收方的第一派生密钥均为非对称加密密钥对，所述第一派生密钥包括第一派生公钥和第一派生私钥；

20 所述密钥接收方节点设备获取所述密钥分配方节点设备分配的第一派生密钥，包括：

所述密钥接收方节点设备从所述区块链的分布式数据库中获取所述第一派生公钥和被所述密钥接收方的用户公钥加密的第一派生私钥。

4、根据权利要求 3 所述的方法，还包括：

25 向所述区块链发送对所述第一派生私钥的请求交易，其中，所述请求交易被所述密钥接收方的用户私钥加密，以使所述密钥分配方节点设备在基于所述密钥接收方的用户公钥对所述请求交易验证通过后，向所述区块链发送被所述密钥接收方的用户公钥加密的第一派生私钥。

5、根据权利要求 1 所述的方法，所述第一派生密钥是由所述密钥分配方的派生密钥基于所述密钥接收方的业务数据查看权限类型进行 KDF 计算而派生生成的密钥。

30 6、根据权利要求 2 所述的方法，所述基于所述第一派生密钥对业务数据进行加密以获得加密业务数据，包括：

使用所述第一派生密钥对所述业务数据进行加密以获得第一加密业务数据;

所述加密业务数据包括所述第一加密业务数据。

7、根据权利要求 3 所述的方法,所述基于所述第一派生密钥对业务数据进行加密以获得加密业务数据,包括:

5 使用所述第一派生公钥对所述业务数据进行加密以获得第一加密业务数据;

所述加密业务数据包括所述第一加密业务数据。

8、根据权利要求 2 所述的方法,所述基于所述第一派生密钥对业务数据进行加密以获得加密业务数据,包括:

使用第三加密密钥对所述业务数据进行加密以获得第二加密业务数据;

10 使用所述第一派生密钥对所述第三加密密钥对应的第三解密密钥进行加密以获得第三加密密钥数据;

所述加密业务数据包括第二加密业务数据和第三加密密钥数据。

9、根据权利要求 3 所述的方法,所述基于所述第一派生密钥对业务数据进行加密以获得加密业务数据,包括:

15 使用第三加密密钥对所述业务数据进行加密以获得第二加密业务数据;

使用所述第一派生公钥对所述第三加密密钥对应的第三解密密钥进行加密以获得第三加密密钥数据;

所述加密业务数据包括第二加密业务数据和第三加密密钥数据。

10、根据权利要求 1 所述的方法,还包括:

20 将所述第一派生密钥与所述业务数据权限类型的标识对应保存于所述密钥接收方的本地数据库中。

11、根据权利要求 10 所述的方法,所述向所述区块链发送所述加密业务数据,包括:

向所述区块链发送所述加密业务数据和所述业务数据权限类型的标识。

25 12、一种基于区块链的业务数据加密装置,应用于包括密钥分配方节点设备和密钥接收方节点设备的区块链,包括:

获取单元,所述密钥接收方节点设备获取所述密钥分配方节点设备分配的第一派生密钥,所述第一派生密钥由所述密钥分配方的派生密钥基于所述密钥接收方的业务数据权限类型而派生成,所述派生密钥可解密被所述第一派生密钥加密的业务数据;

30 加密单元,基于所述第一派生密钥对业务数据进行加密以获得加密业务数据;

发送单元,向所述区块链发送所述加密业务数据,以使所述加密业务数据被所述区

区块链共识验证后收录于所述区块链的分布式数据库。

13、根据权利要求 12 所述的装置，所述密钥分配方的派生密钥和所述密钥接收方的第一派生密钥均为对称加密密钥；所述获取单元：

所述密钥接收方节点设备从所述区块链的分布式数据库中获取被加密的第一派生
5 密钥，所述第一派生密钥被基于所述密钥接收方的用户公钥加密；

基于所述密钥接收方的用户私钥解密上述被加密的第一派生密钥，以获取所述第一派生密钥。

14、根据权利要求 12 所述的装置，所述密钥分配方的派生密钥和所述密钥接收方的第一派生密钥均为非对称加密密钥对，所述第一派生密钥包括第一派生公钥和第一派
10 生私钥；

所述获取单元：

从所述区块链的分布式数据库中获取所述第一派生公钥和被所述密钥接收方的用户公钥加密的第一派生私钥。

15、根据权利要求 14 所述的装置，所述发送单元：

15 向所述区块链发送对所述第一派生私钥的请求交易，其中，所述请求交易被所述密钥接收方的用户私钥加密，以使所述密钥分配方节点设备在基于所述密钥接收方的用户公钥对所述请求交易验证通过后，向所述区块链发送被所述密钥接收方的用户公钥加密的第一派生私钥。

16、根据权利要求 12 所述的装置，所述第一派生密钥是由所述密钥分配方的派生
20 密钥基于所述密钥接收方的业务数据查看权限类型进行 KDF 计算而派生生成的密钥。

17、根据权利要求 13 所述的装置，所述加密单元：

使用所述第一派生密钥对所述业务数据进行加密以获得第一加密业务数据；

所述加密业务数据包括所述第一加密业务数据。

18、根据权利要求 14 所述的装置，所述加密单元：

25 使用所述第一派生公钥对所述业务数据进行加密以获得第一加密业务数据；

所述加密业务数据包括所述第一加密业务数据。

19、根据权利要求 13 所述的装置，所述加密单元：

使用第三加密密钥对所述业务数据进行加密以获得第二加密业务数据；

使用所述第一派生密钥对所述第三加密密钥对应的第三解密密钥进行加密以获得
30 第三加密密钥数据；

所述加密业务数据包括第二加密业务数据和第三加密密钥数据。

20、根据权利要求 14 所述的装置，所述加密单元：

使用第三加密密钥对所述业务数据进行加密以获得第二加密业务数据；

使用所述第一派生公钥对所述第三加密密钥对应的第三解密密钥进行加密以获得第三加密密钥数据；

5 所述加密业务数据包括第二加密业务数据和第三加密密钥数据。

21、根据权利要求 12 所述的装置，还包括：

存储单元，将所述第一派生密钥与所述业务数据权限类型的标识对应保存于所述密钥接收方的本地数据库中。

22、根据权利要求 21 所述的装置，所述发送单元：

10 向所述区块链发送所述加密业务数据和所述业务数据权限类型的标识。

23、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 11 任意一项所述的方法。