(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108416578 A
(43)申请公布日 2018.08.17

(21)申请号 201810210284.5

(22)申请日 2018.03.14

(71)申请人 郑杰骞
地址 311100 浙江省杭州市余杭区西溪润景大厦2-425

(72)发明人 郑杰骞

(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
代理人 蒋冬梅 栗若木

(51)Int.Cl.
G06Q 20/06(2012.01)
G06Q 20/38(2012.01)

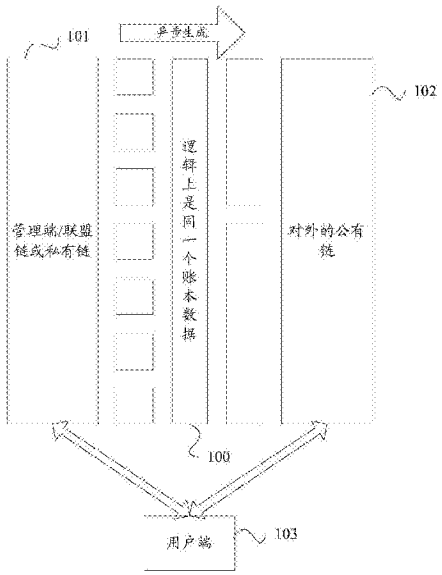
权利要求书2页 说明书10页 附图2页

(54)发明名称

一种区块链系统及数据处理方法

(57)摘要

本申请公开了一种区块链系统及数据处理方法；上述区块链系统，至少包括：管理端以及对外系统；其中，管理端的联盟链或私有链与对外系统使用逻辑相同的账本数据。本申请能够提供具有管理端背书的区块链系统，从而确保用户资产安全和数据隐私安全。



CN 108416578 A

1.一种区块链系统，其特征在于，至少包括：

管理端、对外系统；

其中，所述管理端的联盟链或私有链与所述对外系统使用逻辑相同的账本数据。

2.根据权利要求1所述的系统，其特征在于，所述对外系统包括对外的公有链或联盟链。

3.根据权利要求1所述的系统，其特征在于，所述对外系统上的每个区块数据由所述管理端的联盟链或私有链的多个区块数据顺序组成。

4.根据权利要求1所述的系统，其特征在于，在所述管理端的联盟链或私有链上获取到的任一账户的状态与在所述对外系统上获取到的所述账户的状态是一致的。

5.根据权利要求1所述的系统，其特征在于，所述系统还包括：用户端，适于通过交易标识，在所述账本数据上检索相关的交易数据。

6.根据权利要求5所述的系统，其特征在于，所述用户端的钱包适于自动验证在所述管理端的联盟链或私有链上获取到的账户的状态与在所述对外系统上获取到的所述账户的状态是否一致。

7.根据权利要求5所述的系统，其特征在于，所述交易标识包括发送标识和接收标识，所述发送标识由所述用户端上次发送交易的nonce值和加密密钥确定，所述接收标识由所述用户端上次接收交易的nonce值和加密密钥确定；其中，所述用户端的加密密钥由所述管理端颁发，交易的nonce值是一个随机数值。

8.根据权利要求5所述的系统，其特征在于，所述用户端的交易数据形成一个发送链条和一个有兄弟节点的接收链条。

9.根据权利要求5所述的系统，其特征在于，所述管理端，适于在接收到所述用户端提交的交易数据并验证通过后，对所述交易数据添加背书签名，并更新状态树。

10.根据权利要求5所述的系统，其特征在于，所述用户端，还适于在所述区块链系统中建立托管合约，并通过合约标识，在所述对外系统上检索相关的合约数据。

11.根据权利要求5所述的系统，其特征在于，所述系统还包括以下至少之一：

监管端，适于监管所述管理端发行的背书token，以及在所述管理端的授权下，监管所述交易数据以及账户信息；

第三方，适于在所述用户端的授权下，查验所述交易数据及账户信息。

12.根据权利要求1所述的系统，其特征在于，所述至少两个区块链系统通过所述管理端建立秘密通道进行数据流转，其中，所述任一区块链系统中的token总量保持不变。

13.一种数据处理方法，其特征在于，应用于区块链系统，所述区块链系统至少包括用户端和管理端；或者，所述区块链系统至少包括用户端、管理端以及对外系统，其中，所述管理端的联盟链或私有链与所述对外系统使用逻辑相同的账本数据；所述方法包括：

所述用户端根据上次交易的nonce值以及所述管理端颁发的加密密钥，确定交易标识；

所述用户端通过所述交易标识，在所述账本数据上检索相关的交易数据。

14.根据权利要求13所述的方法，其特征在于，所述交易标识包括发送标识和接收标识，所述发送标识由所述用户端上次发送交易的nonce值和所述加密密钥确定，所述接收标识由所述用户端上次接收交易的nonce值和所述加密密钥确定；其中，所述nonce值为随机数据。

15.根据权利要求13所述的方法，其特征在于，所述用户端的交易数据形成一个发送链条和一个有兄弟节点的接收链条。

16.根据权利要求13所述的方法，其特征在于，所述方法还包括：所述用户端在所述区块链系统中建立托管合约，并通过合约标识，在所述对外系统上检索相关的合约数据。

一种区块链系统及数据处理方法

技术领域

[0001] 本申请涉及但不限于计算机数据处理技术领域，尤其涉及一种区块链系统及数据处理方法。

背景技术

[0002] 区块链技术也被称为分布式账本技术，是一种去中心化的分布式数据库技术，其特点是去中心化、公开透明、不可篡改、可信任。

[0003] 然而，当前的区块链系统，缺少管理者参与控制和管理，token的发行缺少相关背书，缺乏完善的监管以及隐私保护，导致安全性不足。

发明内容

[0004] 以下是对本文详细描述的主题的概述。本概述并非是为了限制权利要求的保护范围。

[0005] 本申请实施例提供一种区块链系统及数据处理方法，能够提供具有管理端背书的区块链系统，从而确保用户资产安全和数据隐私安全。

[0006] 第一方面，本申请实施例提供一种区块链系统，至少包括：管理端、对外系统；其中，所述管理端的联盟链或私有链与所述对外系统使用逻辑相同的账本数据。

[0007] 在示例性实施方式中，所述对外系统可以包括对外的公有链或联盟链。

[0008] 在示例性实施方式中，所述对外系统上的每个区块数据可以由所述管理端的联盟链或私有链的多个区块数据顺序组成。

[0009] 在示例性实施方式中，在所述管理端的联盟链或私有链上获取到的任一账户的状态与在所述对外系统上获取到的所述账户的状态可以是一致的。

[0010] 在示例性实施方式中，上述区块链系统还可以包括：用户端，适于通过交易标识，在所述账本数据上检索相关的交易数据。

[0011] 在示例性实施方式中，所述用户端的钱包可以适于自动验证在所述管理端的联盟链或私有链上获取到的账户的状态与在所述对外系统上获取到的所述账户的状态是否一致。

[0012] 在示例性实施方式中，所述交易标识可以包括发送标识和接收标识，所述发送标识可以由所述用户端上次发送交易的nonce值和加密密钥确定，所述接收标识可以由所述用户端上次接收交易的nonce值和加密密钥确定；其中，所述用户端的加密密钥由所述管理端颁发，交易的nonce值是一个随机数值。

[0013] 在示例性实施方式中，所述用户端的交易数据可以形成一个发送链条和一个有兄弟节点的接收链条。

[0014] 在示例性实施方式中，所述管理端可以适于在接收到所述用户端提交的交易数据并验证通过后，对所述交易数据添加背书签名，并更新状态树。

[0015] 在示例性实施方式中，所述用户端，还可以适于在所述区块链系统中建立托管合

约，并通过合约标识，在所述对外系统上检索相关的合约数据。

[0016] 在示例性实施方式中，上述区块链系统还可以包括以下至少之一：

[0017] 监管端，适于监管所述管理端发行的背书token，以及在所述管理端的授权下，监管所述交易数据以及账户信息；

[0018] 第三方，适于在所述用户端的授权下，查验所述交易数据及账户信息。

[0019] 在示例性实施方式中，所述至少两个区块链系统通过所述管理端建立秘密通道进行数据流转，其中，所述任一区块链系统中的token总量保持不变。

[0020] 第二方面，本申请实施例提供一种数据处理方法，应用于区块链系统，所述区块链系统至少包括用户端和管理端；或者，所述区块链系统至少包括用户端、管理端以及对外系统，其中，所述管理端的联盟链或私有链与所述对外系统使用逻辑相同的账本数据；所述方法包括：

[0021] 所述用户端根据上次交易的nonce值以及所述管理端颁发的加密密钥，确定交易标识；

[0022] 所述用户端通过所述交易标识，在所述账本数据上检索相关的交易数据。

[0023] 在示例性实施方式中，所述交易标识可以包括发送标识和接收标识，所述发送标识可以由所述用户端上次发送交易的nonce值和所述加密密钥确定，所述接收标识可以由所述用户端上次接收交易的nonce值和所述加密密钥确定；其中，所述nonce值为随机数据。

[0024] 在示例性实施方式中，所述用户端的交易数据可以形成一个发送链条和一个有兄弟节点的接收链条。

[0025] 在示例性实施方式中，上述方法还可以包括：所述用户端在所述区块链系统中建立托管合约，并通过合约标识，在所述对外系统上检索相关的合约数据。

[0026] 此外，本申请实施例还提供一种计算机可读介质，存储有数据处理程序，该数据处理程序被处理器执行时实现上述数据处理方法的步骤。

[0027] 在本申请实施例中，区块链系统至少包括管理端及对外系统，其中，管理端的联盟链或私有链与对外系统使用逻辑相同的账本数据。本申请实施例通过结合使用管理端的联盟链或私有链和对外系统，实现具有管理端背书的区块链系统，从而确保用户资产安全和数据隐私安全。

[0028] 在阅读并理解了附图和详细描述后，可以明白其他方面。

附图说明

[0029] 图1为本申请实施例提供的区块链系统的一种示意图；

[0030] 图2为本申请实施例提供的区块链系统的示例图；

[0031] 图3为本申请实施例提供的两个区块链系统之间的链间流转示意图；

[0032] 图4为本申请实施例提供的两个区块链系统的交互示意图；

[0033] 图5为本申请实施例提供的数据处理方法的流程图。

具体实施方式

[0034] 以下结合附图对本申请实施例进行详细说明，应当理解，以下所说明的实施例仅用于说明和解释本申请，并不用于限定本申请。

[0035] 需要说明的是，如果不冲突，本申请实施例以及实施例中的各个特征可以相互结合，均在本申请的保护范围之内。另外，虽然在流程图中示出了逻辑顺序，但是在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤。

[0036] 下面先对本申请涉及的概念进行说明。

[0037] token指区块链上的代币，也称为通证，但都与资产类相关。

[0038] 公有链指任何人都可以读取确认、参与共识的区块链，满足完全去中心化。本申请中，公有链上的区块数据由管理端的联盟链或私有链的数据组合而成，公有链的区块头数据和每个数据块内包含的管理端的数据块的数量由有公有链确定，并且公有链上的数据是不可逆的，任何人不能修改。

[0039] 私有链指写入权限在一个组织手里的数据链。本申请中，用户端提交的交易数据只包含用户端的认证签名，需要管理端进行验证并给出背书签名后，才能在管理端的联盟链或私有链上进行写入。

[0040] 联盟链指写入权限在多个组织手里的数据链。

[0041] eID(electronic Identity)为公安部公民网络身份识别系统，由公安部第三研究所建设，具有可信的实名认证方式。

[0042] 本申请实施例提供一种区块链系统，至少包括：管理端、对外系统；其中，管理端的联盟链或私有链与对外系统使用逻辑相同的账本数据。

[0043] 其中，对外系统可以包括：对外的公有链或联盟链。

[0044] 本实施方式中，对外系统(比如，对外的公有链)上的每个区块数据由管理端的联盟链或私有链的多个区块数据顺序组成。示例性地，公有链上的每个区块数据中包含的管理端的区块数据的数量和区块头数据由公有链确定。然而，本申请对此并不限定。

[0045] 在示例性实施方式中，公有链上只顺序记录管理端提交的数据，而管理端提交的数据是管理端的联盟链或私有链产生的区块数据，因此，公有链和管理端的联盟链或私有链使用的账本数据在逻辑上是同一个。本实施例提供的区块链系统可以看作是一个双层体系(即包括以下两层：管理端的联盟链或私有链、对外系统)。然而，本申请对此并不限定。在实际运用中，本实施例提供的区块链系统还可以扩展到多层体系，比如，在管理端进行体系扩展。

[0046] 本实施例中，在管理端的联盟链或私有链以及对外系统(比如，对外的公有链)上使用不同方式获取到的账户的状态是一致的。示例性地，管理端可以生成状态树，从而得到任一账户的状态；在公有链上，可以通过累计交易结果获知任一账户的状态；通过累计交易结果获知的账户的状态与管理端上得到的该账户的状态是一致的。如此，通过公有链可以实现账户的交易数据的不可更改性。其中，用户端的钱包可以自动验证在管理端的联盟链或私有链上获取到的账户的状态与在对外系统(比如，对外的公有链)上获取到的该账户的状态是否一致。

[0047] 本实施例中，用户端提交的数据需经过管理端背书签名，而所有的读取都以对外系统上的数据为准则，从而实现具有管理端背书的区块链系统。其中，管理端适于管理区块链系统，调整区块链系统中发行的token总量，并满足交易管理、实名制、有效监管、用户数据隐私保护等特点，并且通过结合对外系统的使用，使对外系统上的数据可信任不可更改。

[0048] 本实施例提供的区块链系统中，既有用户端的认证签名，又有管理端的背书签名，

还有对外系统的共识确认，所以对外系统上的数据是不可逆的，任何人不能修改。如此，既确保了用户资产安全和数据隐私，又能保证链上的token和交易是具有背书的。

[0049] 下面以对外系统包括对外的公有链为例，对本申请实施例提供的区块链系统进行说明。

[0050] 图1和图2为本申请实施例提供的区块链系统的示意图。如图1所示，本实施例提供的区块链系统，包括：管理端101、对外的公有链102以及用户端103。其中，管理端101的联盟链或私有链与公有链102使用逻辑相同的账本数据100。

[0051] 在本实施例中，管理端、用户端可以分别为包括一个或多个通信设备的系统。用户端的数目可以分别为多个。然而，本申请对此并不限定。

[0052] 在本实施例中，对外的公有链上的每个区块数据由管理端的联盟链或私有链的多个区块数据顺序组成。即管理端的联盟链或私有链与公有链的底层账本数据在逻辑上是同一个账本数据，账本的顺序也是依次关联的。如此，管理端可以通过公有链检查自身的数据状态，并可通过公有链恢复出完整的管理端的联盟链或私有链的数据。其中，管理端的联盟链或私有链与公有链使用的共识算法不同，所以各自产生区块数据的时间也不相同；管理端的联盟链或私有链使用共识时间更短的算法，以满足快速确认和高频交易需求，而公有链的共识时间更长，因此公有链相对管理端的联盟链或私有链是一个异步的过程。公有链上的每个区块数据包含的管理端产生的区块数据的数量也不固定，比如，在图1中，公有链上的一个区块数据可以包括管理端产生的三个或四个区块数据；因此不会影响管理端的联盟链或私有链的产生，从而满足管理端的高并发需求。

[0053] 在本实施例中，管理端生成的联盟链或私有链的数据可以全部对外公布，异步生成对外的公有链。公有链的数据块是由管理端的联盟链或私有链的多个连续的数据块组合而成的，仅添加公有链的区块头数据，由于区块头数据的占比很小，所以新增加的数据量也很小。而且，公有链使用的数据块都是经过管理端的联盟链或私有链打包后的区块数据，因此也有利于公有链的数据交换。

[0054] 在本实施例中，管理端的联盟链或私有链上的数据分为控制数据和交易数据两部分。控制数据主要是管理端用于管理和控制区块链系统而发布的信息数据的集合，可以包括用户、机构的注册和注销，token的发行，交易规则和密钥、证书等更新信息。除用户的身份信息为密文外，其余大部分数据都为明文，以方便有效监管，也能保护用户的身份隐私。交易数据是所有单笔交易的集合；交易规则由管理端在控制数据中发布，可以包括交易双方的身份标、交易数额、nonce值、时间戳、交易标识(ID)和附加信息等，还可以包括用户端的认证签名和管理端的背书签名；其中，每笔交易都需要经过管理端进行验证并给出背书签名后才能生效，以达到管理端对交易进行管理的目的。其中，交易的nonce值是一个随机数值；除时间戳、交易ID和签名值是明文外，其余数据都是密文，且用户端的认证签名是对交易双方的身份标识的明文和nonce值的明文及其它密文数据进行的签名，而管理端的背书签名是对用户端提交的整个交易数据的签名，所以对外部可以验证管理端的背书签名，但不能验证用户端的认证签名，并能防止暴力尝试交易双方的身份标识，保护交易双方身份隐私。

[0055] 在本实施例中，管理端的联盟链或私有链可以生成整个系统的状态树，从而得到每个账户的状态；而公有链上由于没有管理端的秘密共享子密钥，所以不能生成整个系统

的状态数据，但是由于管理端的联盟链或私有链与公有链的底层采用同一份账本数据，因此，在公有链上可以获取并累计账户余额，得到的账户余额与管理端的状态树中的账户余额的状态是一致的。

[0056] 换言之，针对同一份账本数据，对于管理端和用户端的使用方式是不一样的，管理端能生成系统的状态树，从而得知每个账户的状态，而用户端能得知自己的每笔交易的详细数据，通过累计交易结果得到的账户状态和管理端得到的状态是一致的，也就通过公有链实现了用户交易数据的不可更改性，并且管理端也不能伪造用户端的认证签名和更改交易数据，从而确保用户资产安全。

[0057] 在本实施例中，用户端的密钥可以分为签名密钥和加密密钥两类。其中，签名密钥是由用户端本地生成和管理使用的，使用不可导出的硬件作为载体，以确保密钥的安全使用。签名密钥通过CA(Certificate Authority，认证授权)机构颁发用户端的身份认证证书或使用eID机制，实现用户端的实名身份认证。加密密钥是用户端通过身份认证证书或eID在管理端注册后，由管理端颁发的，且由用户端的本地钱包存储使用。

[0058] 示例性地，加密密钥可以包括加法同态的标识密钥、秘密共享子密钥和对称加密密钥。比如，用户的身份信息可以使用对称加密密钥，采用对称加密算法进行加密存储；交易双方的身份标识等数据可以使用秘密共享算法，采用秘密共享子密钥进行加密存储；交易数额可以使用加法同态算法，采用加法同态的标识密钥进行加密存储。其中，对称加密指采用这种加密算法的双方使用同样的密钥进行加密和解密。秘密共享指秘密消息以适当的方式拆分为N份，只有M份协作才能恢复秘密消息。加法同态加密指消息通过公钥加密后，可在密文上进行加法的运算，运算输出使用私钥解密，其结果与使用加法处理未加密的原始数据得到的结果一致。

[0059] 在本实施例中，公有链上的数据对外只能验证联盟链或私有链打包的数据块的完整性和验证每笔交易的管理端的背书签名，并能查看管理端在控制数据中发布的明文信息和交易数据中的交易ID和时间戳信息，其它信息对外都是保密存储的。

[0060] 在本实施例中，用户端可以适于通过交易ID，在账本数据上检索相关的交易数据。即用户端可以通过交易ID，在管理端和对外的公有链中至少一项上检索相关的交易数据。其中，用户端的钱包是一个轻量级的钱包，并不需要完整的公有链数据；用户端的钱包可以从公有链上解密查看自己的账户信息以及与自己相关的交易数据，比如包括交易双方的身份标识、自己的交易数额，并能验证交易数据的认证签名和背书签名。而且，用户端的钱包在把所有与自己相关的交易数据解密后累计的余额信息，与从管理端查询的帐户余额密文解密后的信息是一致的。

[0061] 下面对用户端从公有链上检索相关的交易数据的方式进行说明。

[0062] 由于交易数据关联有发送者和接收者，因此，交易ID可以分为发送ID和接收ID两部分。其中，发送ID可以由用户端上次发送交易的nonce值和用户端的对称加密密钥通过单向不可逆函数产生，发送ID在系统中是唯一的；接收ID由用户端上次接收交易的nonce值和用户端的对称加密密钥通过单向不可逆函数产生，在系统中不同用户端的接收ID是唯一的，但因为存在并发交易，因此存在同一个用户端针对不同交易具有相同的接收ID。

[0063] 其中，用户端在向管理端注册时，由管理端生成一个随机的nonce值和初始接收ID，并使用用户端的对称加密密钥进行加密存储，并在管理端的状态树中记录。在交易时由

状态树中发送者的nonce值和用户端的对称加密密钥通过单向不可逆函数产生发送ID，连同状态树中接收者的接收ID组成交易ID。nonce值由管理端随机生成，并确保计算出的下一个发送ID和接收ID在系统中都是唯一的。管理端将nonce值与交易双方的身份标识通过秘密共享算法进行加密，并连同交易ID传输给用户端。当用户端提交交易数据后，管理端可以验证用户端的发送ID是否符合，并验证接收ID是否属于接收者，然后根据交易的nonce值更新状态树中发送者的nonce值，并查找交易数据中的接收ID是否与状态树中的接收ID相同，如果相同，则根据nonce值计算出的接收ID进行更新。由此可见，用户端的交易数据根据发送和接收各组成了一个链条，并且由于并发交易的原因，接收链条上存在同一时刻的兄弟节点。换言之，用户端的交易数据形成一个发送链条和一个有兄弟节点的接收链条。

[0064] 其中，用户端的钱包可以通过用户标识查找账户信息，解密注册时的nonce值和初始接收ID，就能计算出下一次的发送ID，分别在公有链上查询发送ID和接收ID，进而获取到所有与用户相关的发送交易和接收交易。由于用户端提交的交易数据中nonce值已知，也就确定了下一个发送ID，可以验证管理端传输给用户端的发送ID是否符合。而每个发送ID都已确认，也就防止了重放攻击。通过交易ID和nonce值，用户端的交易数据形成了一个发送链条和一个有兄弟节点的接收链条，并且可以在公有链上通过交易ID方便地检索用户端的交易数据，而对外部是不可得知的。用户端的钱包可以使用轮询或订阅方式从公有链上查询交易ID，保存与用户端相关的所有交易数据，就能分析用户端的账户状态，以便与管理端进行查询验证。

[0065] 在示例性实施方式中，用户端还可以适于在区块链系统中建立托管合约，并通过合约标识，在对外系统上检索相关的合约数据。

[0066] 在本实施例中，公有链上的共识奖励是管理端记录公有链上要奖励的账户信息，等待比如6个公有链的区块数据确认后，在控制数据中明文发布奖励到相应的帐户中，并累计到账户余额密文中。即公有链上的共识奖励，会在后面的数据块中由管理端进行颁发，并通过共识奖励以保障公有链上只顺序记录管理端提交的数据，具体的奖励规则可由管理端自定。如此，用户端的钱包从公有链上查询的余额信息，还需要累计公有链上的共识奖励，才与管理端的帐户余额状态是一致的。而共识奖励是由明文颁发，所以通过用户标识就可在公有链上检索。为确保系统中的token总量是一定的，管理端可在发行token时，预留部分token不转移至发行机构的账户余额中，作为公有链上的共识奖励。

[0067] 在示例性实施方式中，如图2所示，本实施例的区块链系统还可以包括：监管端104以及第三方105；其中，监管端104，适于监管管理端101发行的背书token，以及在管理端101的授权下，监管交易数据以及账户信息；第三方105，适于在用户端103的授权下，监管交易数据及账户信息。

[0068] 在本示例中，为了有效监管管理端的行为，监管端可以提供自动监管和人为参与监管两部分功能。自动监管可在管理端的联盟链或私有链上，也可在公有链上。自动监管在启动时能获取管理端的秘密共享子密钥，所以能生成相应的系统状态树，能验证每笔交易的认证签名和背书签名，并根据每笔交易使用加法同态算法修改状态树中的帐户余额密文，并不泄漏相关的账户余额信息。为了能够验证每笔交易数额的有效性，管理端还需提供一个经过审核的黑盒验证模块，功能是输入交易双方的数额密文和标识，以及支付方的账户余额密文，在黑盒验证模块内解密数额并验证是否能满足，返回成功与否。自动监管的目

的在于验证所有的交易数额是否满足，确保系统中token的总量是一定的。而人为参与的监管一部分是通过监管管理端在控制数据中发布的明文数据，主要包括管理端发行的token背书，比如需要管理端具有相关资产抵押或保证金等证明并具有相关监管的签名才能发行相应背书的token；另一部分是需要监管系统中某些用户的账户信息，管理端可授权相应的用户端的加密密钥给监管端，监管端就能解密并查看对应用户的交易数据和账户信息。

[0069] 在本示例中，第三方需要查验用户端的账户信息时，用户端可以授权加密密钥给第三方，以便第三方在公有链上进行查验。

[0070] 在本实施例中，自动监管能验证交易数额的有效性，确保系统中token的总量是一定的。系统中token总量的变化需要管理端在控制数据中明文发行或移除相应数量的token，通过指定的发行机构，在其账户余额中增加或减少相应的数额密文，达到调整系统中token总量的目的，而这些信息都是明文公开的。链内的普通交易需要具有用户端的认证签名才能生效，而签名密钥是用户端本地管理不可导出的，并绑定了用户端的身份认证证书或使用eID机制，用户端可在公有链上验证与自己相关交易的认证签名，所以管理端并不能伪造更改用户端的认证签名和交易数据，从而确保用户资产安全。另外，针对多个具有管理端背书的区块链系统，用户端注册只需使用同一份身份认证证书或eID，方便了用户使用和更新。

[0071] 下面参照图3和图4，对多个具有管理端背书的区块链系统之间的数据流转进行说明。图3和图4分别为本申请实施例提供的两个区块链系统之间的链间流转示意图和交互示意图。在图3和图4中以两个具有管理端背书的区块链系统为例进行说明。

[0072] 在示例性实施方式中，至少两个区块链系统通过管理端建立秘密通道进行数据流转，其中，任一区块链系统中的token总量保持不变，相关合约数据在各自系统中存储。

[0073] 在本示例中，多个具有管理端背书的区块链系统之间数据流转是通过各个系统的管理端之间建立秘密通道实现的。如图3和图4所示，区块链系统SA和区块链系统SB之间通过各自的管理端建立秘密通道。其中，秘密通道上并不存储重要的数据，仅作为数据协商和触发合约的通道，具体的用户合约数据都在各个区块链系统上存储，因此，用户端可以在对应的公有链上查询相关的合约数据。相应的合约规则由各个管理端在控制数据中发布，并通过跨链合约ID，使不同系统间数据流转的合约数据关联起来，用户端的钱包就可以分析相关合约的执行情况。

[0074] 如图4所示，在多个区块链系统间进行数据流转时，需要交易双方在要流转的系统中进行注册。比如，用户A向区块链系统SA和SB的管理端进行注册，用户B向区块链系统SA和SB的管理端进行注册。由于交易双方的用户端并不知道交易的对方是谁，所以需要进行托管合约声明。其中，声明的托管合约可以包括托管的人、托管的数额密文、时间戳、nonce值、合约ID、附加信息和用户端的认证签名等，这里合约ID也可以使用上述的交易ID的规则，以方便用户端在公有链上检索。管理端验证用户端的托管合约并背书签名后，合约就生效了。管理端从用户端的账户余额中减去相应的数额密文到新建的合约余额中。托管的合约交易则不再需要用户端的认证签名，区块链系统的管理端之间经过协商和触发，生成相关的合约交易并背书签名即可。每个合约交易都要包含该托管合约的合约ID，用户端通过检索合约ID，就可以获取这个托管合约的所有相关交易，并且接收者通过合约交易中的接收ID，也能检索到该交易。如果合约余额中有剩余，用户端可以生成一个解除托管合约的操作，指定

相关托管合约的合约ID，经过管理端背书签名后，移除合约并累计合约的余额到账户余额中，完成托管合约的解除。

[0075] 在本示例中，在多个具有管理端背书的区块链系统之间进行的合约交易，合约中需要包含秘密通道中的跨链合约ID。用户端的钱包通过前文的交易ID规则获取到用户相关的托管合约，然后可以在公有链上检索所有和该托管合约关联的合约交易，通过合约交易中的跨链合约ID，就可以在对应流转的另一个公有链上检索包含该跨链合约ID相关的合约交易。解密可以查看相关的合约交易内容，包括时间戳、交易数额、合约信息等内容，并能验证管理端的背书签名，但只能查看对应的托管合约ID，而不能查看托管合约的身份标识。用户端的钱包获取到相关的托管合约信息和分别在两个系统的流转合约交易信息后，就可以分析相关合约的执行情况。

[0076] 在本示例中，在多个具有管理端背书的区块链系统之间，交易双方用户端的合约交易并不会影响各自系统中token总量的变化，只是双方系统内不同用户token流转的过程。并且也可通过自动监管验证交易数额的有效性，确保系统中token的总量是一定的。而在多个具有管理端背书的区块链系统之间，管理端相互建立了相关的秘密通道后，就可以实现用户数据在系统间的流转，并且流转的数据都在相应的公有链上记录并可查询验证，也方便进行监管。

[0077] 由此可知，在多个具有管理端背书的区块链系统之间通过管理端间建立秘密通道进行数据流转，秘密通道上并不存储重要数据，仅作为数据协商和触发合约的通道，相关的合约交易数据都在各自系统的数据链上存储，用户可在公有链上查询相关的交易数据。并且链间数据流转能保持各自系统中token总量的不变，也方便管理端对发行token的管理和监管。

[0078] 图5为本申请实施例提供的数据处理方法的流程图。本实施例提供的数据处理方法，应用于区块链系统，区块链系统至少包括用户端和管理端；或者，区块链系统至少包括用户端、管理端以及对外系统，其中，管理端的联盟链或私有链与对外系统使用逻辑相同的账本数据。

[0079] 如图5所示，本实施例提供的数据处理方法包括：

[0080] S501、用户端根据上次交易的nonce值以及管理端颁发的加密密钥，确定交易标识；

[0081] S502、用户端通过交易标识，在账本数据上检索相关的交易数据。

[0082] 在本实施例提供的数据处理方法应用于至少包括用户端和管理端的区块链系统时，用户端可以通过交易标识，在管理端使用的账本数据上检索相关的交易数据。在本实施例提供的数据处理方法应用于至少包括用户端、管理端和对外系统的区块链系统时，由于管理端的联盟链或私有链与对外系统使用逻辑相同的账本数据，则用户端可以执行以下至少一项：通过交易标识，在管理端上检索相关的交易数据；通过交易标识，在对外系统上检索相关的交易数据。

[0083] 示例性地，交易标识可以包括发送标识和接收标识，发送标识由用户端上次发送交易的nonce值和加密密钥确定，接收标识由用户端上次接收交易的nonce值和加密密钥确定；其中，nonce值为随机数值。

[0084] 示例性地，用户端的交易数据可以形成一个发送链条和一个有兄弟节点的接收链

条。其中，通过交易标识可以使交易数据形成一个发送链条和一个有兄弟节点的接收链条。

[0085] 示例性地，本实施例的方法还可以包括：用户端在区块链系统中建立托管合约，并通过合约标识，在对外系统上检索相关的合约数据。

[0086] 关于本实施例提供的数据处理方法的相关说明可以参照上述区块链系统的描述，故于此不再赘述。

[0087] 此外，本申请实施例还提供一种数据处理装置，应用于用户端，包括：

[0088] 确定模块，适于根据上次交易的nonce值以及管理端颁发的加密密钥，确定交易标识；

[0089] 检索模块，适于通过交易标识，在账本数据上检索相关的交易数据。

[0090] 其中，管理端的联盟链或私有链与对外系统(比如，对外的公有链)使用逻辑相同的账本数据。

[0091] 关于本实施例提供的数据处理装置的相关说明可以参照上述数据处理方法的描述，故于此不再赘述。

[0092] 此外，本申请实施例还提供一种通信设备，包括：存储器与处理器，存储器适于存储数据处理程序，该数据处理程序被处理器执行时实现图5对应实施例提供的数据处理方法的步骤。

[0093] 其中，处理器可以包括但不限于微处理器(MCU，Microcontroller Unit)或可编程逻辑器件(FPGA，Field Programmable Gate Array)等的处理装置。存储器可用于存储应用软件的软件程序以及模块，如本实施例中的数据处理方法对应的程序指令或模块，处理器通过运行存储在存储器内的软件程序以及模块，从而执行各种功能应用以及数据处理，即实现上述的数据处理方法。存储器可包括高速随机存储器，还可包括非易失性存储器，如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中，存储器可包括相对于处理器远程设置的存储器，这些远程存储器可以通过网络连接至上述通信设备。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

[0094] 示例性地，上述通信设备还可以包括通信单元；通信单元可以经由一个网络接收或者发送数据。在一个实例中，通信单元可以为射频(RadioFrequency，简称为RF)模块，其用于通过无线方式与互联网进行通信。

[0095] 此外，本申请实施例还提供一种计算机可读介质，存储有数据处理程序，该数据处理程序被处理器执行时实现上述数据处理方法的步骤。

[0096] 本领域普通技术人员可以理解，上文中所公开方法中的全部或某些步骤、系统、装置中的功能模块或单元可以被实施为软件、固件、硬件及其适当的组合。在硬件实施方式中，在以上描述中提及的功能模块或单元之间的划分不一定对应于物理组件的划分；例如，一个物理组件可以具有多个功能，或者一个功能或步骤可以由若干物理组件合作执行。某些组件或所有组件可以被实施为由处理器，如数字信号处理器或微处理器执行的软件，或者被实施为硬件，或者被实施为集成电路，如专用集成电路。这样的软件可以分布在计算机可读介质上，计算机可读介质可以包括计算机存储介质(或非暂时性介质)和通信介质(或暂时性介质)。如本领域普通技术人员公知的，术语计算机存储介质包括在用于存储信息(诸如计算机可读指令、数据结构、程序模块或其他数据)的任何方法或技术中实施的易失性和非易失性、可移除和不可移除介质。计算机存储介质包括但不限于RAM、ROM、EEPROM、闪

存或其他存储器技术、CD-ROM、数字多功能盘(DVD)或其他光盘存储、磁盒、磁带、磁盘存储或其他磁存储装置、或者可以用于存储期望的信息并且可以被计算机访问的任何其他的介质。此外，本领域普通技术人员公知的是，通信介质通常包含计算机可读指令、数据结构、程序模块或者诸如载波或其他传输机制之类的调制数据信号中的其他数据，并且可包括任何信息递送介质。

[0097] 以上显示和描述了本申请的基本原理和主要特征和本申请的优点。本申请不受上述实施例的限制，上述实施例和说明书中描述的只是说明本申请的原理，在不脱离本申请精神和范围的前提下，本申请还会有各种变化和改进，这些变化和改进都落入要求保护的本申请范围内。

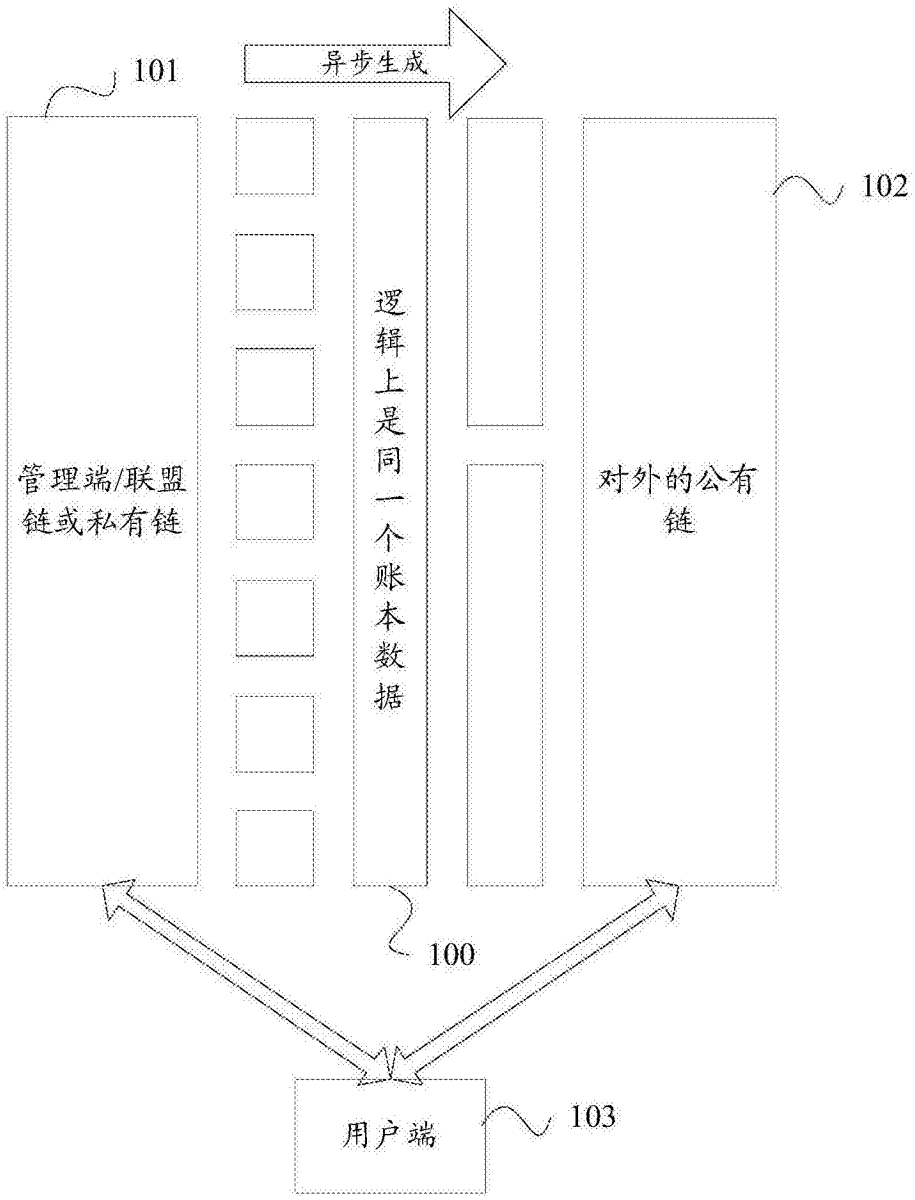

101
异步生成
102
逻辑上是同一个账本数据
管理端/联盟链或私有链
对外的公有链
100
用户端
103

图1

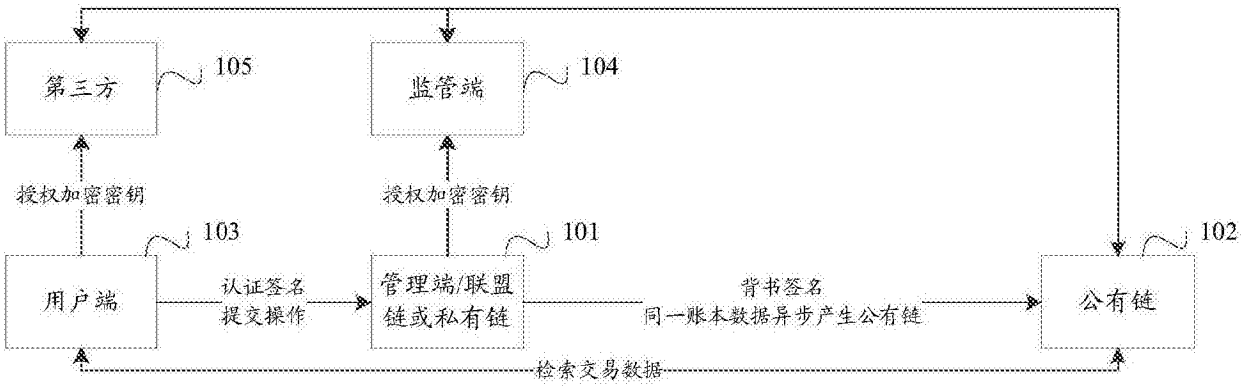

第三方
105
监管端
104
授权加密密钥
授权加密密钥
103
101
102
用户端
认证签名
提交操作
管理端/联盟链或私有链
背书签名
同一账本数据异步产生公有链
公有链
检索交易数据

图2

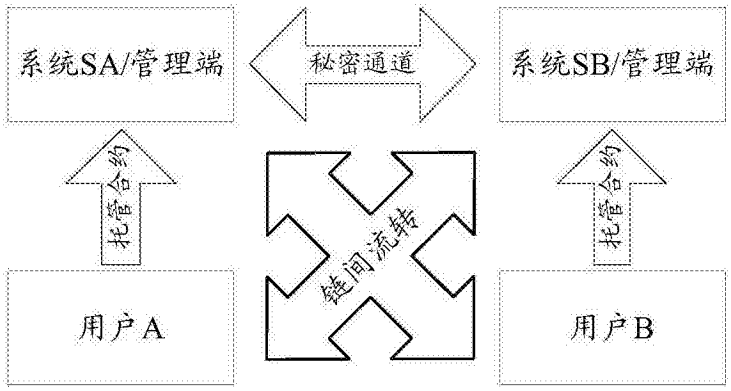

系统SA/管理端
秘密通道
系统SB/管理端
托管合约
链间流转
托管合约
用户A
用户B

图3

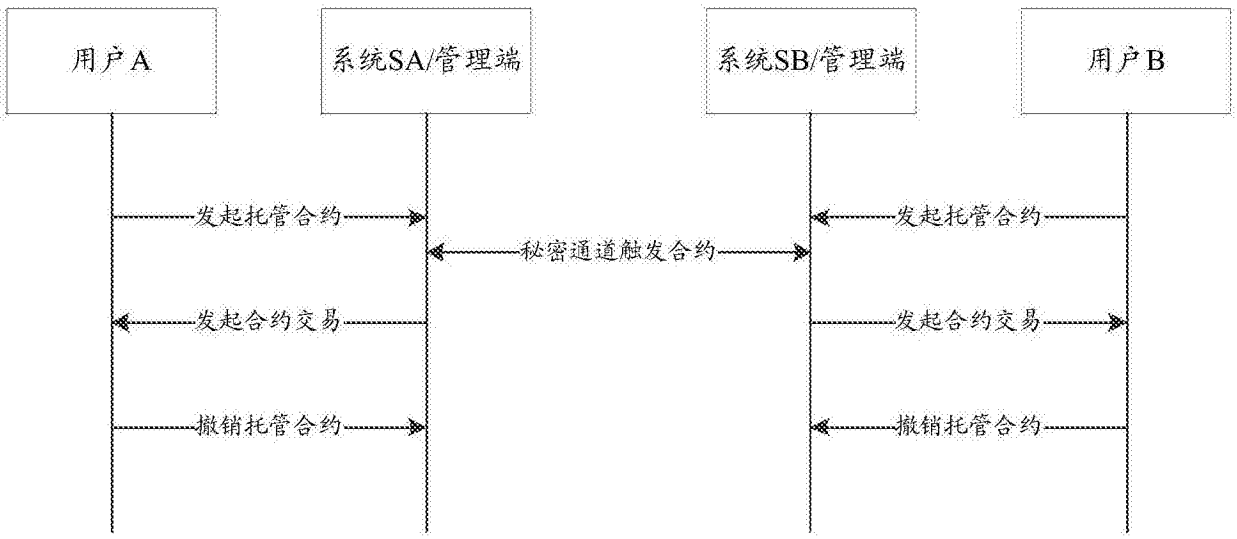

用户A
系统SA/管理端
系统SB/管理端
用户B
发起托管合约
秘密通道触发合约
发起托管合约
发起合约交易
发起合约交易
撤销托管合约
撤销托管合约

图4

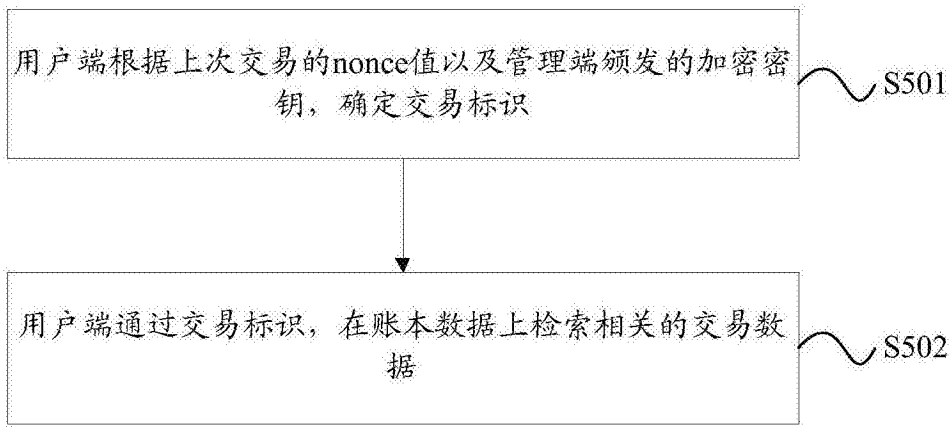

用户端根据上次交易的nonce值以及管理端颁发的加密密钥，确定交易标识
S501
用户端通过交易标识，在账本数据上检索相关的交易数据
S502

图5