



(12) 发明专利申请

(10) 申请公布号 CN 111931237 A

(43) 申请公布日 2020. 11. 13

(21) 申请号 202010966889.4

(22) 申请日 2020.09.15

(71) 申请人 支付宝(杭州)信息技术有限公司  
地址 310000 浙江省杭州市西湖区西溪路  
556号8层B段801-11

(72) 发明人 黄佳 陈锡辉

(74) 专利代理机构 北京博思佳知识产权代理有  
限公司 11415  
代理人 周嗣勇

(51) Int. Cl.  
G06F 21/62 (2013.01)  
G06F 21/60 (2013.01)

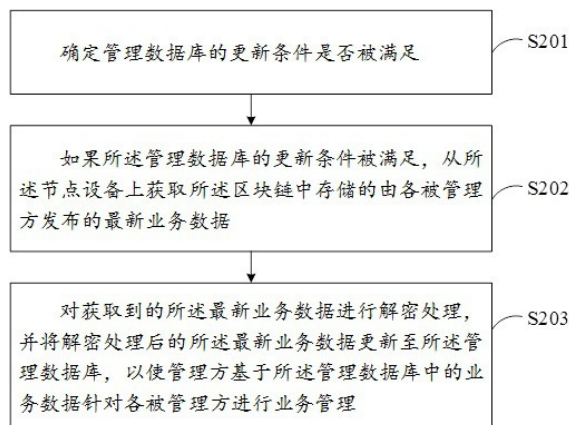
权利要求书3页 说明书10页 附图4页

(54) 发明名称

一种基于区块链的业务管理方法及装置

(57) 摘要

一种基于区块链的业务管理方法及装置,其中,所述方法应用于与区块链中的节点设备对接的管理服务节点;所述区块链存储了由各被管理方发布的业务数据;所述业务数据在被发布前经过了加密处理;所述方法包括:确定管理数据库的更新条件是否被满足;如果所述管理数据库的更新条件被满足,从所述节点设备上获取所述区块链中存储的由各被管理方发布的最新业务数据;对获取到的所述最新业务数据进行解密处理,并将解密处理后的所述最新业务数据更新至所述管理数据库,以使管理方基于所述管理数据库中的业务数据针对各被管理方进行业务管理。



1. 一种基于区块链的业务管理方法,应用于与区块链中的节点设备对接的管理服务节点;其中,所述区块链存储了由各被管理方发布的业务数据;所述业务数据在被发布前经过了加密处理;所述方法包括:

确定管理数据库的更新条件是否被满足;

如果所述管理数据库的更新条件被满足,从所述节点设备上获取所述区块链中存储的由各被管理方发布的最新业务数据;

对获取到的所述最新业务数据进行解密处理,并将解密处理后的所述最新业务数据更新至所述管理数据库,以使管理方基于所述管理数据库中的业务数据针对各被管理方进行业务管理。

2. 根据权利要求1所述的方法,所述最新业务数据包括:上一次针对所述管理数据库进行更新的时刻,与所述管理数据库满足更新条件的时刻之间,所述区块链中存储的新增业务数据;

所述管理数据库的更新条件,包括下列条件中的任意一者或者多者的组合:

当前时刻达到为所述管理数据库预设的更新时刻;

当前时刻与上一次针对所述管理数据库进行更新的时刻之间的时长间隔达到预设的时长间隔;

在上一次针对所述管理数据库进行更新之后,所述区块链中存储的新增业务数据的数据量达到预设的阈值;

所述新增业务数据中携带有指示立即对所述管理数据库进行更新的标识。

3. 根据权利要求1所述的方法,所述业务数据在被发布前由各被管理方基于与管理方协商出的对称密钥,进行了加密处理;

所述对获取到的所述最新业务数据进行解密处理,包括:

基于所述对称密钥对获取到的所述最新业务数据进行解密处理。

4. 根据权利要求1所述的方法,所述业务数据在被发布前由各被管理方基于与管理方对应的公钥,进行了加密处理;

对获取到的所述最新业务数据进行解密处理,包括:

基于与所述管理方对应的私钥,对获取到的所述最新业务数据进行解密处理。

5. 根据权利要求1所述的方法,还包括:

对所述管理数据库中存储的业务数据进行统计分析,得到与各被管理方对应的管理指标;

将所述管理指标通过预设的管理展示界面,向管理用户进行输出展示。

6. 根据权利要求1所述的方法,还包括:

接收各被管理方或者由所述各被管理方提供服务的用户发送的查询请求;

响应于所述查询请求,向所述各被管理方或者所述用户返回查询结果;其中,所述查询结果包括与所述各被管理方或者所述用户相关的业务数据;和/或,针对与所述各被管理方或者所述用户相关的业务数据进行统计分析得到的业务指标。

7. 根据权利要求1所述的方法,所述区块链为由多个被管理方作为联盟成员的联盟链。

8. 根据权利要求1所述的方法,所述被管理方为被管理的金融服务机构;所述业务数据为所述被管理的金融服务机构面向用户提供的金融服务相关的业务明细数据。

9. 一种基于区块链的业务管理装置,应用于与区块链中的节点设备对接的管理服务节点;其中,所述区块链存储了由各被管理方发布的业务数据;所述业务数据在被发布前经过了加密处理;所述装置包括:

确定模块,确定管理数据库的更新条件是否被满足;

获取模块,在所述管理数据库的更新条件被满足时,从所述节点设备上获取所述区块链中存储的由各被管理方发布的最新业务数据;

更新模块,对获取到的所述最新业务数据进行解密处理,并将解密处理后的所述最新业务数据更新至所述管理数据库,以使管理方基于所述管理数据库中的业务数据针对各被管理方进行业务管理。

10. 根据权利要求9所述的装置,所述最新业务数据包括:上一次针对所述管理数据库进行更新的时刻,与所述管理数据库满足更新条件的时刻之间,所述区块链中存储的新增业务数据;

所述管理数据库的更新条件,包括下列条件中的任意一者或者多者的组合:

当前时刻达到为所述管理数据库预设的更新时刻;

当前时刻与上一次针对所述管理数据库进行更新的时刻之间的时长间隔达到预设的时长间隔;

在上一次针对所述管理数据库进行更新之后,所述区块链中存储的新增业务数据的数据量达到预设的阈值;

所述新增业务数据中携带有指示立即对所述管理数据库进行更新的标识。

11. 根据权利要求9所述的装置,所述业务数据在被发布前由各被管理方基于与管理方协商出的对称密钥,进行了加密处理;

所述管理数据库更新模块,包括:

基于所述对称密钥对获取到的所述最新业务数据进行解密处理。

12. 根据权利要求9所述的装置,所述业务数据在被发布前由各被管理方基于与管理方对应的公钥,进行了加密处理;

所述管理数据库更新模块进一步:

基于与所述管理方对应的私钥,对获取到的所述最新业务数据进行解密处理。

13. 根据权利要求9所述的装置,还包括:

统计分析模块,对所述管理数据库中存储的业务数据进行统计分析,得到与各被管理方对应的管理指标;

管理指标展示模块,将所述管理指标通过预设的管理展示界面,向管理用户进行输出展示。

14. 根据权利要求9所述的装置,还包括:

查询请求接收模块,接收各被管理方或者由所述各被管理方提供服务的用户发送的查询请求;

查询结果返回模块,响应于所述查询请求,向所述各被管理方或者所述用户返回查询结果;其中,所述查询结果包括与所述各被管理方或者所述用户相关的业务数据;和/或,针对与所述各被管理方或者所述用户相关的业务数据进行统计分析得到的业务指标。

15. 根据权利要求9所述的装置,所述区块链为由多个被管理方作为联盟成员的联盟

链。

16. 根据权利要求9所述的装置,所述被管理方为被管理的金融服务机构;所述业务数据为所述被管理的金融服务机构面向用户提供的金融服务相关的业务明细数据。

17. 一种基于区块链的业务管理系统,包括:

若干被管理方,向区块链中发布经过加密处理的业务数据;

区块链,存储被管理方发布的经过加密处理的业务数据;

与所述区块链中的节点设备对接管理服务节点,在管理数据库的更新条件被满足时,从所述节点设备上获取所述区块链中存储的由各被管理方发布的最新业务数据,对获取到的所述最新业务数据进行解密处理,并将解密后的所述最新业务数据更新至所述管理数据库;

管理方,基于所述管理数据库中的业务数据针对各被管理方进行业务管理。

18. 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权利要求1~8任一所述的方法。

## 一种基于区块链的业务管理方法及装置

### 技术领域

[0001] 本说明书涉及计算机应用领域,尤其涉及一种基于区块链的业务管理方法及装置。

### 背景技术

[0002] 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。

### 发明内容

[0003] 本说明书公开了一种基于区块链的业务管理方法和装置。

[0004] 根据本说明书实施例的第一方面,公开了一种基于区块链的业务管理方法,应用于与区块链中的节点设备对接的管理服务节点;其中,所述区块链存储了由各被管理方发布的业务数据;所述业务数据在被发布前经过了加密处理;所述方法包括:

确定管理数据库的更新条件是否被满足;

如果所述管理数据库的更新条件被满足,从所述节点设备上获取所述区块链中存储的由各被管理方发布的最新业务数据;

对获取到的所述最新业务数据进行解密处理,并将解密处理后的所述最新业务数据更新至所述管理数据库,以使管理方基于所述管理数据库中的业务数据针对各被管理方进行业务管理。

[0005] 根据本说明书实施例的第二方面,公开了一种基于区块链的业务管理装置,应用于与区块链中的节点设备对接的管理服务节点;其中,所述区块链存储了由各被管理方发布的业务数据;所述业务数据在被发布前经过了加密处理;所述装置包括:

确定模块,确定管理数据库的更新条件是否被满足;

获取模块,在所述管理数据库的更新条件被满足时,从所述节点设备上获取所述区块链中存储的由各被管理方发布的最新业务数据;

更新模块,对获取到的所述最新业务数据进行解密处理,并将解密处理后的所述最新业务数据更新至所述管理数据库,以使管理方基于所述管理数据库中的业务数据针对各被管理方进行业务管理。

[0006] 根据本说明书实施例的第三方面,公开了一种基于区块链的业务管理系统,包括:

若干被管理方,向区块链中发布经过加密处理的业务数据;

区块链,存储被管理方发布的经过加密处理的业务数据;

与所述区块链中的节点设备对接管理服务节点,在管理数据库的更新条件被满足时,从所述节点设备上获取所述区块链中存储的由各被管理方发布的最新业务数据,对获取到的所述最新业务数据进行解密处理,并将解密后的所述最新业务数据更新至所述管理数据

库；

管理方，基于所述管理数据库中的业务数据针对各被管理方进行业务管理。

[0007] 以上技术方案中，一方面，被管理方的业务数据会被发布到区块链，再更新到管理数据库中，由于区块链不可抵赖、不可篡改的特性，因此相对于业务数据直接更新到中心化数据库的传统方案，管理方在进行业务管理时，获取的被管理方的业务数据更加真实可靠；

另一方面，由于管理方能够接触到的业务数据仅为最新的业务数据，而不是区块链上的全部业务数据，相对于相关技术方案而言，管理数据库存储的隐私数据量更小，因此数据泄露可能产生的危害更低；而且，由于业务数据在发布至区块链前经过了加密处理，因此即使不法分子从区块链上获取到加密后的业务数据，也无法从中获取到隐私数据，提高了业务管理流程的安全性。

## 附图说明

[0008] 此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本说明书的实施例，并与说明书文本一同用于解释原理。

[0009] 图1是本说明书所述基于区块链的业务管理系统的一结构示例图；

图2是本说明书所述基于区块链的业务管理方法的一流程示例图；

图3是本说明书所述管理展示界面的一示例图；

图4是本说明书所述查询结果的一示例图；

图5是本说明书所述基于区块链的业务管理装置的一结构示例图；

图6是本说明书所述用于业务管理的计算机设备的一结构示例图。

## 具体实施方式

[0010] 为了使本技术领域的人员更好地理解本说明书一个或多个实施例中的技术方案，下面将结合本说明书一个或多个实施例中的附图，对本说明书一个或多个实施例中的技术方案进行清楚、完整地描述。显然，所描述的实施例仅仅是一部分实施例，而不是全部的实施例。基于本说明书一个或多个实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都应当属于本说明书保护的范围。

[0011] 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、本说明书的一些方面相一致的系统和方法的例子。

[0012] 在本说明书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。在本说明书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。

[0013] 应当理解，尽管在本说明书可能采用术语第一、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”。

[0014] 区块链一般被划分为三种类型:公有链(Public Blockchain),私有链(Private Blockchain)和联盟链(Consortium Blockchain)。此外,还可以有上述多种类型的结合,比如私有链+联盟链、联盟链+公有链等。

[0015] 其中,去中心化程度最高的是公有链。公有链以比特币、以太坊为代表,加入公有链的参与者(也可称为区块链中的节点)可以读取链上的数据记录、参与交易、以及竞争新区块的记账权等。而且,各节点可自由加入或者退出网络,并进行相关操作。

[0016] 私有链则相反,该网络的写入权限由某个组织或者机构控制,数据读取权限受组织规定。简单来说,私有链可以为一个弱中心化系统,其对节点具有严格限制且节点数量较少。这种类型的区块链更适用于特定机构内部使用。

[0017] 联盟链则是介于公有链以及私有链之间的区块链,可实现“部分去中心化”。联盟链中各个节点通常有与之相对应的实体机构或者组织;节点通过授权加入网络并组成利益相关联盟,共同维护区块链运行。

[0018] 基于区块链的基本特性,区块链通常是由若干个区块构成。在这些区块中分别记录有与该区块的创建时刻对应的时间戳,所有的区块严格按照区块中记录的时间戳,构成一条在时间上有序的数据链条。

[0019] 对于物理世界产生的真实数据,可以将其构建成区块链所支持的标准的交易(transaction)格式,然后发布至区块链,由区块链中的节点设备对收到的交易进行共识处理,并在达成共识后,由区块链中作为记账节点的节点设备,将这笔交易打包进区块,在区块链中进行持久化存证。

[0020] 随着电子商务的发展,为了保证行业的稳定发展,管理方需要通过获取行业内各公司、机构等业务个体的业务信息,来进一步完成风险预警等管理任务。

[0021] 以监管机构对互联网金融业的监管为例,在地方金融机构开展的融资、借贷等金融业务中,可能出现多头借贷的情况,由于单个借款人的偿还能力较为有限,因此向多方借贷意味着借款人很可能正在借新还旧,其现金流存在较严重的问题,故而存在较为严重的信用和欺诈风险,如果对单个借款人放款的多个金融机构之间没有足够的信息互通,就需要监管方及时给出风险预警。

[0022] 在相关技术中,人们可以通过维护一个中心化的管理数据库的方式,将地方金融机构等行业内业务个体作为被管理方,并把被管理方的业务数据汇集到上述管理数据库中,从而方便管理方从该管理数据库中获知被管理方的运营状态,并及时发现被管理方业务中可能存在的风险,进而保证行业的稳定发展。

[0023] 然而,上述解决方案中存在两个主要问题,其一是,部分行业内业务个体出于自身业务和经营考虑,上报的业务数据存在造假、虚报、瞒报的现象,对于过往的数据也可能进行抵赖,造成传统的管理数据库中的数据往往不够真实可靠;其二是,管理方作为数据中心节点,管理数据库中业务数据的存储、处理、转发都需要管理方的许可,由于业务数据中包含巨量的个人金融数据等隐私信息,全部存储在管理单位中,存在较高的隐私数据泄露的风险。

[0024] 基于此,本申请提出了一种由被管理方向区块链中发布自身的业务数据,并由与区块链对接的管理服务节点从区块链中获取最新业务数据,以更新管理数据库的技术方

案。

[0025] 在实现中,管理服务节点只需从区块链中获取的最新业务数据,无需全部的历史业务数据,即可对管理数据库完成更新;

此外,被管理方在发布自身的业务数据时,可以对业务数据进行加密处理,管理服务节点需要使用这部分业务数据时再进行解密处理,以保证区块链上存储的业务数据不会造成隐私数据泄露。

[0026] 在以上技术方案中,一方面,被管理方的业务数据会被发布到区块链,再更新到管理数据库中,由于区块链不可抵赖、不可篡改的特性,因此相对于业务数据直接更新到中心化数据库的传统方案,管理方在进行业务管理时,获取的被管理方的业务数据更加真实可靠;

另一方面,由于管理方能够接触到的业务数据仅为最新的业务数据,而不是区块链上的全部业务数据,相对于相关技术方案而言,管理数据库存储的隐私数据量更小,因此数据泄露可能产生的危害更低;而且,由于业务数据在发布至区块链前经过了加密处理,因此即使不法分子从区块链上获取到加密后的业务数据,也无法从中获取到隐私数据,提高了业务管理流程的安全性。

[0027] 下面通过具体实施例并结合具体的应用场景对本说明书进行描述。

[0028] 请参见图1,图1为本说明书所述基于区块链的业务管理系统的一结构示例图;如图1所示,该基于区块链的业务管理系统可以包括若干被管理方、区块链、管理服务节点以及管理数据库,其中区块链与被管理方以及管理服务节点相连接,管理数据库可以连接到管理服务节点。

[0029] 其中,若干被管理方可以向区块链中发布经过加密处理的业务数据;

区块链可以将被管理方发布的经过加密处理的业务数据存储起来;

与上述区块链中的节点设备对接管理服务节点则可以在管理数据库的更新条件被满足时,从所述节点设备上获取所述区块链中存储的由各被管理方发布的最新业务数据,并对获取到的所述最新业务数据进行解密处理,再将解密后的所述最新业务数据更新至所述管理数据库;

管理方则可以基于所述管理数据库中的业务数据针对各被管理方进行业务管理。

[0030] 若将上述业务管理系统应用于对互联网金融业的监管情景下,那么上述被管理方可以是受监管的若干地方金融机构,上述管理方则可以是执行监管的监管机构,上述管理服务节点与管理数据库则分别可以是上述监管活动中使用的监管服务节点和监管数据库。可以理解的是,对互联网金融业的监管仅是上述方案的一个示例场景,本领域技术人员可以根据具体需求,将上述管理系统应用到其他行业中,本说明书无需进行具体限定。

[0031] 下面本说明书将从上述基于区块链的业务管理系统中,管理服务节点的角度,详细描述本说明书公开的基于区块链的业务管理方法。

[0032] 请参考图2,图2本说明书所述基于区块链的业务管理方法的一流程示例图,该方法可以应用于与区块链中的节点设备对接的管理服务节点;其中,上述区块链存储了由各被管理方发布的业务数据;上述业务数据在被发布前经过了加密处理;上述方法执行以下步骤:

S201,确定管理数据库的更新条件是否被满足;

S202,如果所述管理数据库的更新条件被满足,从所述节点设备上获取所述区块链中存储的由各被管理方发布的最新业务数据;

S203,对获取到的所述最新业务数据进行解密处理,并将解密处理后的所述最新业务数据更新至所述管理数据库,以使管理方基于所述管理数据库中的业务数据针对各被管理方进行业务管理。

[0033] 上述被管理方可以包括任意需要被管理的业务机构,与之对应的,上述业务数据的具体类型,以及管理方,也可以随被管理方的具体选择而发生变化;可以理解的是,虽然上述示例以地方金融机构为例,但显然其他行业、其他领域也可以应用本说明书所公开的业务管理方法,对被管理方实施管理;例如,某地的电子产业发达,整条产业链中可能包括材料冶炼企业、零部件制造企业、加工组装企业,也可以应用上述业务管理方法,利用各个企业的业务信息,由行业协会或者有关部门对上述企业进行的管理,从而及时发现原材料短缺、生产过剩乃至部分企业违规或者失信等风险。

[0034] 在示出的一种实施方式中,上述被管理方可以是被管理的金融服务机构;对应的业务数据即可以为被管理的金融服务机构面向用户提供的金融服务相关的业务明细数据,对应的管理方可以是当地的金融管理部门;举例而言,某地有若干家银行被管理,各家银行都提供金融贷款服务,那么包含借款人、借款时间、借款数额等信息的业务明细数据,即可作为各家银行用以提交管理系统的业务数据。

[0035] 上述区块链包括私有链、联盟链、公有链等任意形式的区块链,由于不同形式的区块链通常具有不同的特性,例如私有链的运算性能通常会高于公有链,但可信度则不及公有链,本领域技术人员可以根据具体需求,自行权衡利弊,选择具体使用的区块链形式,本说明书无需进行详细限定。

[0036] 在示出的一种实施方式中,上述区块链可以包括联盟链,其中,上述若干被管理方可以作为该联盟链的联盟成员。被管理方作为联盟成员,一方面可以方便其向联盟链中发布自身的业务信息,另一方面,也可以增强联盟链的可信度,通过一定的共识机制保证联盟链的顺利运行。

[0037] 上述管理服务节点,可以是一个逻辑节点,也可以是一个物理节点;具体而言,其可以是一个与区块链的节点设备对接的一个独立的节点设备(比如服务器),也可以是区块链的节点设备上搭载的一个服务程序,还可以是分别实现多个功能的多个服务程序组成的程序组;无论采用何种配置方式,都可以视为图1中管理服务节点与区块链的相连接的一种具体实现,对此本说明书无需进行具体限定,本领域技术人员可以根据具体需求自行参考相关技术,完成具体设计。

[0038] 在本说明书中,上述管理服务节点可以通过多种方式确定管理数据库的更新条件是否被满足;具体而言,可以采用周期性定时检查管理数据库的更新条件是否被满足的方案,也可以采用基于管理数据库内容的触发机制,本领域技术人员可以自行选择具体的实现方式,本说明书无需进行具体限定。

[0039] 在本说明书中,上述管理服务节点在确定管理数据库的更新条件被满足后,可以从区块链中获取由各被管理方发布的最新业务数据;例如,假设被管理方每放出10笔贷款,就会向区块链中存入一次当前的业务数据,那么上述管理服务节点可以仅获取其中最新的业务数据,就足以令管理数据库中的数据更新至最新状态;可以理解的是,即使相邻两次更

新中某被管理方的业务数据并没有更新,管理服务节点也可以进行重复获取,以确保数据的完整性。

[0040] 在示出的一种实施方式中,上述管理服务节点可以通过增量更新的方式完成对于上述管理数据库的更新;具体而言,增量更新的方式中,新增业务数据可以视为间接指示被管理方当前业务状态的数据,上述管理服务节点可以只获取上一次针对管理数据库进行更新后,到当前时刻之间,上述区块链中存储的新增业务数据,由于节省了对于未发生变化的状态的获取动作,因此可以提高获取最新业务数据的效率。

[0041] 在示出的一种实施方式中,上述管理数据库的更新条件可以从下列条件中任选一者或者多者的组合:

达到为该管理数据库预设的更新时刻;例如预设3月9日0点进行更新;

距离上一次针对该管理数据库进行更新的时刻的时长间隔,达到预设的时长间隔;例如每隔3小时进行一次更新;

在上一次针对该管理数据库进行更新之后,该区块链中存储的新增业务数据的数据量达到预设的阈值;例如区块高度每增高2即进行一次更新;

该新增业务数据中携带有指示立即对该管理数据库进行更新的标识;等等。可以理解的是,当采用多个条件的组合作为上述管理数据的更新条件时,多个条件彼此之间可以是“或”的关系,任意一者被满足即视为管理数据的更新条件被满足,也可以使“且”的关系,必须所有的条件均被满足才可视为管理数据的更新条件被满足;本领域技术人员也可以根据具体需求自行确定逻辑组合关系,本说明书不作进一步限定。

[0042] 在本说明书中,上述被管理方在将各自的业务数据发布至上述区块链前,可以对业务数据进行加密处理,而上述管理服务节点在从区块链中获取被加密的业务数据后,则可以对应地完成解密处理,再将解密后的业务数据用于对上述管理数据库的更新。

[0043] 可以理解的是,由于区块链本身需要大量的计算,因此在具体实现时,也可以仅在上述在区块链中存储加密后业务数据的哈希值,并将加密后业务数据存储到相对应的另一数据库中,需要对区块链中存储的业务数据进行读写的操作则实际对应于对上述另一数据库的读写,以及对区块链中对应哈希值的校验;如此设计,可以兼顾可靠性与效率,避免巨量数据写入区块链造成的性能损失。

[0044] 在示出的一种实施方式中,上述业务数据在被发布前,由各被管理方基于与管理方协商出的对称密钥进行了加密处理;对应的,上述管理服务节点可以基于上述对称密钥,对获取到的上述最新业务数据进行解密处理。可以理解的是,管理服务节点本质上被管理方所控制,因此被管理方与管理方协商出的对称密钥可以由该管理服务节点持有并使用;另外,一个被管理方可以根据需求协商出多个对称密钥,多个被管理方也可以经过协商后共用同一个对称密钥;

举例而言,银行A与管理方协商后,可以约定3个对称密钥A1、A2和A3,而银行B、银行C与管理方协商后,可以约定1个共用的对称密钥B1,银行D与管理方协商后,可以约定1个专用的对称密钥D1……等等;因此,本说明书无需对上述加解密机制的具体实现方式进行详细限定,本领域技术人员可以根据具体情况自行选择并设计实现。

[0045] 在示出的一种实施方式中,上述业务数据在被发布前,由各被管理方基于与管理方对应的公钥进行了加密处理;相对应的,上述管理服务节点也可以在从区块链中获取被

加密的业务数据后,使用与管理方对应的私钥进行解密处理;相对于使用对称加密的方案,使用非对称加密方案可以令所有的被管理方均使用同样的公钥进行加密,从而省略与每一个被管理方单独进行对称密钥协商的过程,只需管理服务节点保证其持有的、与管理方对应的私钥不被泄露,就能够保证加密机制的生效。

[0046] 在本说明书中,管理方可以根据上述管理数据库中的业务数据,对被管理方进行业务管理;具体而言,管理方既可以获知整个行业的业务水平,也可以具体地获知某个被管理方的业务细节,具体管理方式以及风险预警等算法,本领域技术人员可以根据具体需求和实际应用情况进行开发设计,本说明书不作进一步限定。

[0047] 在本说明书中,在上述步骤之外,还可以将管理数据库中存储的业务数据进行进一步处理和展示,便于管理方更加直观地获知统计结果;具体的实现过程,本领域技术人员可以根据具体的需求以及相关技术文献完成具体设计,本说明书无需进行具体的限定。

[0048] 在示出的一种实施方式中,上述管理服务节点还可以对所述管理数据库中存储的业务数据进行统计分析,得到与各被管理方对应的管理指标;并进一步将所述管理指标通过预设的管理展示界面,向管理用户进行输出展示;以对地方金融机构的管理为例,地方金融机构上报的业务数据中可以包含诸多贷款业务的业务记录,那么,进行统计分析后,即可得到各个地方金融机构的放款总额、逾期预期等管理指标,并将得到的管理指标通过预设的管理展示界面(例如管理信息网页)进行输出展示。

[0049] 请参见图3,图3是本说明书所述管理展示界面的一示例图在该图中以被管理对象为地方金融机构为例,通过图形化的方式直观地向管理用户展示了统计分析得到的融资担保总额、融资担保余额、月度贷款余额等等诸多管理指标。采用此方案,可以使管理方对于管理数据库中的业务数据进行更细致、有效的应用,从而更高效地完成管理任务。

[0050] 在本说明书中,还可以将包含更加丰富的业务信息的区块链为基础,开发功能更加完善的应用;具体而言,上述管理数据库中仅包含最新业务数据,但区块链中则包含了所有的历史业务数据,因此可以提供历史数据的查询类服务。

[0051] 在示出的一种实施方式中,上述管理服务节点可以接收查询请求,并响应于该查询请求,返回所需要的业务数据;具体而言,上述查询请求可以来自于被管理方,也可以来自于由被管理方提供服务的用户;返回的业务数据可以是原始的业务数据,也可以是对这些业务数据进行进一步统计分析后得到的业务指标,或者两者兼有。

[0052] 举例而言,某银行的客户可以向上述管理服务节点发送查询请求,以查询自己的信用报告;某银行也可以向上述管理服务节点发送查询请求,以查询向自己借款的某企业是否存在经营风险等等。

[0053] 请参见图4,图4为本说明书所述查询结果的一示例图。该图展示了查询入口为小程序的实现效果,用户张三通过“个人借贷信息查询”小程序,可以查询到自己过往借贷的金额、逾期等信息;在图4所示的示例中,上述信息可以通过卡片的方式进行展示,如果界面无法容纳所有卡片,还可以对卡片进行滚动显示。

[0054] 可以理解的是,图4中展示的仅是一可行的实现方式的示例,上述功能中涉及的诸如网络通信、接口开发、数据处理、界面设计等技术,本领域技术人员可以参考相关技术文献,根据上述功能需求,结合具体实施环境进一步完成开发实现,例如,上述查询的入口,可以是传统的手机或PC客户端,也可以是查询网页或者是小程序等等;上述多个卡片在界面

中的布置方式,还可以是层叠方式,或者基于缩略图的并列排布等等;本说明书对具体的实现方式不作进一步限定。

[0055] 上述内容即为本说明书针对所述基于区块链的业务管理方法的全部实施例。本说明书还提供了对应的基于区块链的业务管理装置的实施例如下:

本说明书提出一种基于区块链的业务管理装置,应用于与区块链中的节点设备对接的管理服务节点;其中,上述区块链存储了由各被管理方发布的业务数据;上述业务数据在被发布前经过了加密处理;

请参见图5,图5为上述基于区块链的业务管理装置的一结构示例图,该装置包括:

确定模块501,确定管理数据库的更新条件是否被满足;

获取模块502,在所述管理数据库的更新条件被满足时,从所述节点设备上获取所述区块链中存储的由各被管理方发布的最新业务数据;

更新模块503,对获取到的所述最新业务数据进行解密处理,并将解密处理后的所述最新业务数据更新至所述管理数据库,以使管理方基于所述管理数据库中的业务数据针对各被管理方进行业务管理。

[0056] 在示出的一种实施方式中,上述被管理方可以是被管理的金融服务机构;对应的业务数据即可以为被管理的金融服务机构面向用户提供的金融服务相关的业务明细数据,对应的管理方可以是当地的金融管理部门。

[0057] 在示出的一种实施方式中,上述区块链可以包括联盟链,其中,上述若干被管理方可以作为该联盟链的联盟成员。

[0058] 在示出的一种实施方式中,上述管理服务节点可以通过增量更新的方式完成对于上述管理数据库的更新;具体而言,增量更新的方式中,新增业务数据可以视为间接指示被管理方当前业务状态的数据,上述管理服务节点可以只获取上一次针对管理数据库进行更新后,到当前时刻之间,上述区块链中存储的新增业务数据,由于节省了对于未发生变化的状态的获取动作,因此可以提高获取最新业务数据的效率。

[0059] 在示出的一种实施方式中,上述管理数据库的更新条件可以从下列条件中任选一者或者多者的组合:

达到为该管理数据库预设的更新时刻;例如预设3月9日0点进行更新;

距离上一次针对该管理数据库进行更新的时刻的时长间隔,达到预设的时长间隔;例如每隔3小时进行一次更新;

在上一次针对该管理数据库进行更新之后,该区块链中存储的新增业务数据的数据量达到预设的阈值;例如区块高度每增高2即进行一次更新;

该新增业务数据中携带有指示立即对该管理数据库进行更新的标识;等等。可以理解的是,当采用多个条件的组合作为上述管理数据的更新条件时,多个条件彼此之间可以是“或”的关系,任意一者被满足即视为管理数据的更新条件被满足,也可以使“且”的关系,必须所有的条件均被满足才可视为管理数据的更新条件被满足;本领域技术人员也可以根据具体需求自行确定逻辑组合关系,本说明书不作进一步限定。

[0060] 在示出的一种实施方式中,上述业务数据在被发布前,由各被管理方基于与管理方协商出的对称密钥进行了加密处理;对应的,上述管理服务节点可以基于上述对称密钥,对获取到的上述最新业务数据进行解密处理。

[0061] 在示出的一种实施方式中,上述业务数据在被发布前,由各被管理方基于与管理方对应的公钥进行了加密处理;相对应的,上述管理服务节点也可以在从区块链中获取被加密的业务数据后,使用与管理方对应的私钥进行解密处理。

[0062] 在示出的一种实施方式中,上述管理服务节点还可以对所述管理数据库中存储的业务数据进行统计分析,得到与各被管理方对应的管理指标;并进一步将所述管理指标通过预设的管理展示界面,向管理用户进行输出展示。

[0063] 在示出的一种实施方式中,上述管理服务节点可以接收查询请求,并响应于该查询请求,返回所需要的业务数据;具体而言,上述查询请求可以来自于被管理方,也可以来自于由被管理方提供服务的用户;返回的业务数据可以是原始的业务数据,也可以是对这些业务数据进行进一步统计分析后得到的业务指标,或者两者兼有。

[0064] 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前述的基于区块链的业务管理方法。

[0065] 图6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,该设备可以包括:处理器1010、存储器1020、输入/输出接口1030、通信接口1040和总线1050。其中处理器1010、存储器1020、输入/输出接口1030和通信接口1040通过总线1050实现彼此之间在设备内部的通信连接。

[0066] 处理器1010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。

[0067] 存储器1020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1020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1020中,并由处理器1010来调用执行。

[0068] 输入/输出接口1030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。

[0069] 通信接口1040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。

[0070] 总线1050包括一通路,在设备的各个组件(例如处理器1010、存储器1020、输入/输出接口1030和通信接口1040)之间传输信息。

[0071] 需要说明的是,尽管上述设备仅示出了处理器1010、存储器1020、输入/输出接口1030、通信接口1040以及总线1050,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。

[0072] 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前述的基于区块链的业务管理方法。

[0073] 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。

[0074] 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。

[0075] 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。

[0076] 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,对于装置实施例而言,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。

[0077] 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。

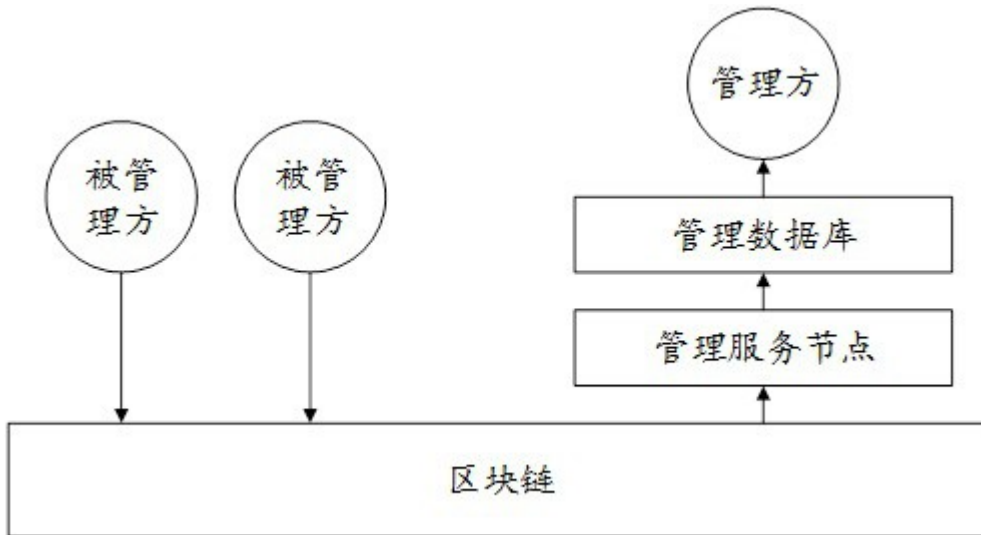


图1

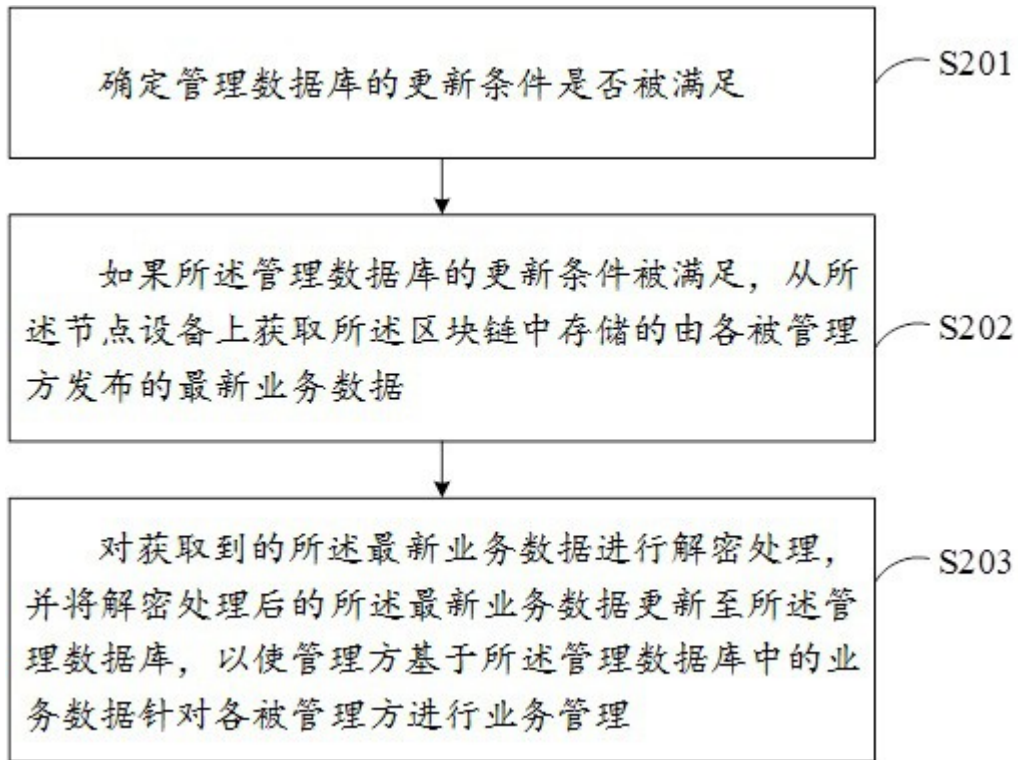


图2

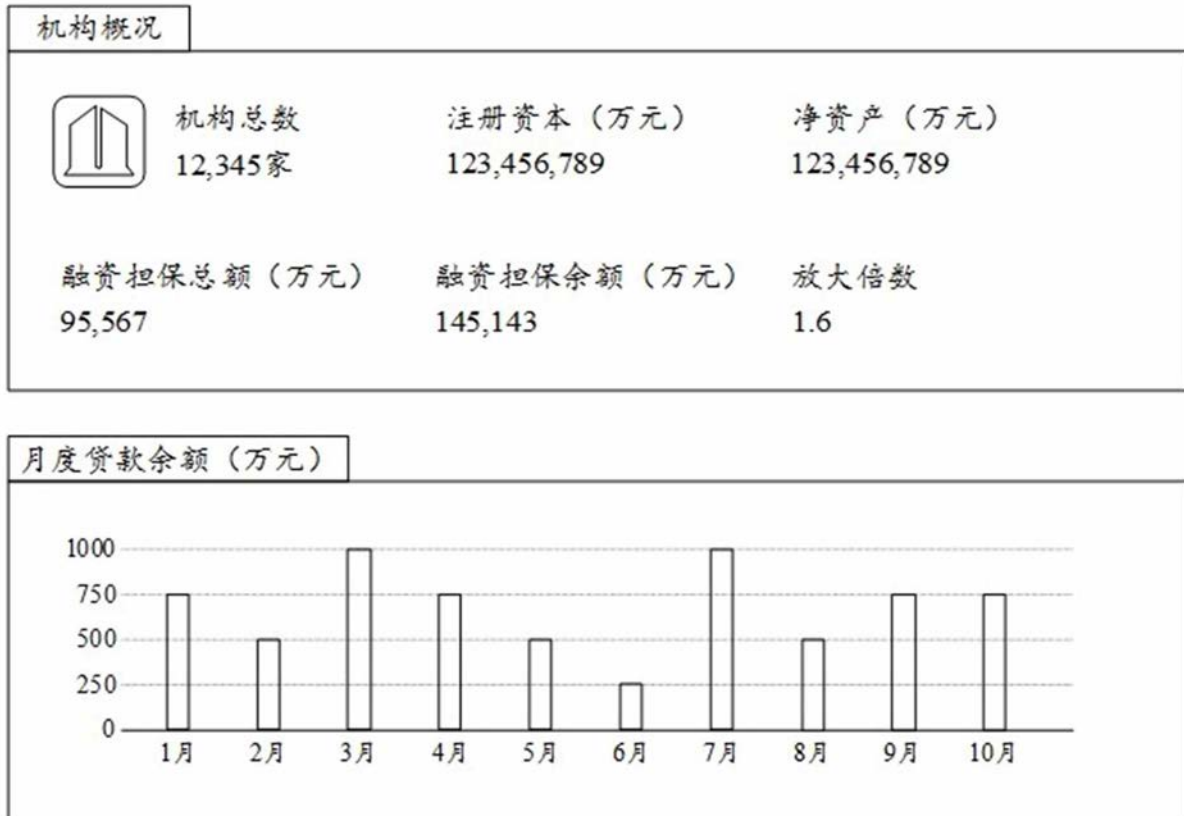


图3



图4

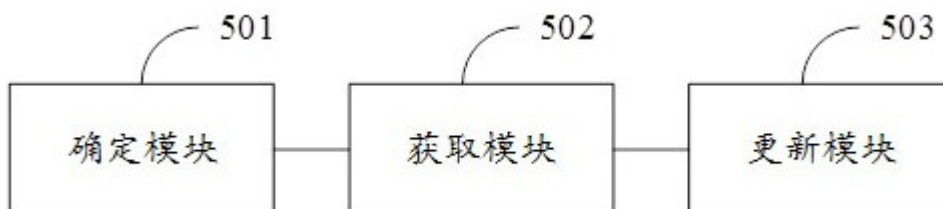


图5

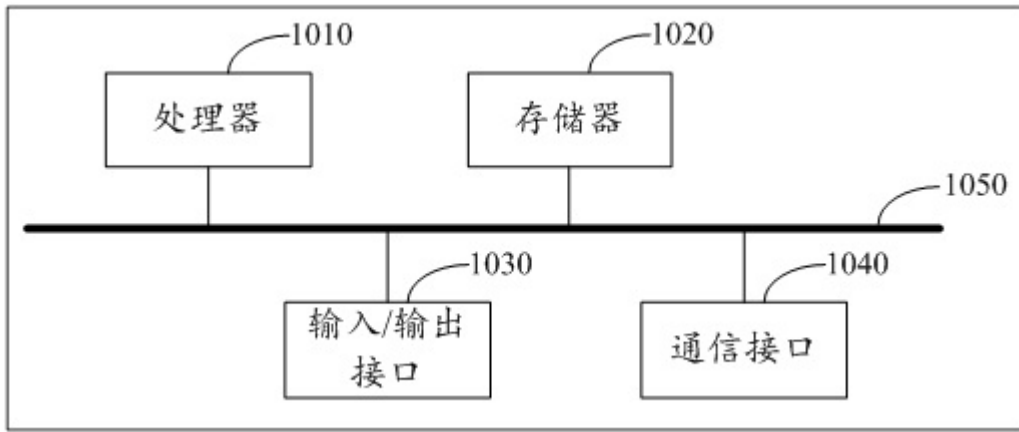


图6