

一种区块链存证方法、装置和计算机设备

技术领域

[01] 本说明书涉及数据处理技术领域，尤其涉及一种区块链存证方法、装置和计算机设备。

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 发明内容

[03] 本说明书提供了一种区块链存证方法，应用于包括计算存证节点设备的区块链系统；所述计算存证节点设备中部署有至少一种计算逻辑；所述方法包括：

[04] 所述计算存证节点设备接收计算调用申请，所述计算调用申请包括对目标业务事件数据的查询索引；

15 [05] 基于目标业务事件数据的查询索引，获取目标业务事件数据；

[06] 运行所述计算调用申请对应的计算逻辑，基于所述目标业务事件数据进行计算，以获得计算结果；

[07] 向所述区块链发送存证交易，以使所述存证交易被所述区块链的节点共识验证后收录于所述区块链的分布式数据库，其中，所述存证交易包括基于所述计算结果生成的第一存证信息。

20

[08] 在又一示出的实施方式中，所述存证交易还包括基于所述目标业务事件数据生成的第二存证信息。

[09] 在又一示出的实施方式中，所述第二存证信息包括所述目标业务事件数据的哈希摘要。

25 [10] 在又一示出的实施方式中，所述计算节点分别与第一数据终端和第二数据终端通信

连接, 所述第二数据终端用以接收用户的数据计算申请, 所述第一数据终端存储有业务事件数据;

[11] 所述计算存证节点设备接收计算调用申请, 包括:

[12] 所述计算存证节点设备接收所述第二数据终端发送的计算调用申请, 所述计算调用

5 申请基于用户的数据计算申请而生成;

[13] 所述基于目标业务事件数据的查询索引, 获取目标业务事件数据, 包括:

[14] 基于目标业务事件数据的查询索引, 从所述第一数据终端获取目标业务事件数据。

[15] 在又一示出的实施方式中, 所述计算存证节点设备与所述第一数据终端通过本地通信方式连接, 所述计算节点与所述第二数据终端通过外部通信方式连接。

10 [16] 在又一示出的实施方式中, 所述计算逻辑由所述第二数据终端通过所述外部通信方式传输至所述计算存证节点设备进行部署。

[17] 在又一示出的实施方式中, 所述计算逻辑由所述第二数据终端通过所述外部通信方式加密传输至所述计算存证节点设备进行加密部署;

15 [18] 所述基于所述目标业务事件数据进行计算, 包括基于所述目标业务事件数据进行加密计算;

[19] 所述计算结果为加密状态的计算结果。

[20] 在又一示出的实施方式中, 所述第二数据终端为所述区块链的节点设备; 所述存证交易还包括基于所述第一数据终端的身份标识而生成的第三存证信息。

20 [21] 在又一示出的实施方式中, 所述存证交易还包括基于发送所述计算调用申请的第二数据终端的身份标识而生成的第四存证信息。

[22] 在又一示出的实施方式中, 所述方法为保险理赔存证方法; 所述计算存证节点设备为理赔计算存证节点设备, 所述计算逻辑为理赔计算逻辑; 所述计算调用申请为理赔计算调用申请; 所述存证交易为理赔存证交易。

25 [23] 在又一示出的实施方式中, 所述方法为保险理赔存证方法; 所述计算存证节点设备为理赔计算存证节点设备, 所述计算逻辑为理赔计算逻辑; 所述计算调用申请为理赔计算调用申请; 所述存证交易为理赔存证交易; 所述第一数据终端为存储理赔基于的业务事件数据的业务数据方终端; 所述第二数据终端为接收用户理赔申请的理赔服务方终端。

[24]在又一示出的实施方式中，所述区块链为联盟链。

[25]相应地，本说明书还提供了一种区块链的存证装置，应用于包括计算存证节点设备的区块链系统；所述计算存证节点设备中部署有至少一种计算逻辑；所述装置包括：

5 [26]接收单元，接收计算调用申请，所述计算调用申请包括对目标业务事件数据的查询索引；

[27]获取单元，基于目标业务事件数据的查询索引，获取目标业务事件数据；

[28]计算单元，运行所述计算调用申请对应的计算逻辑，基于所述业务事件数据进行计算，以获得计算结果；

10 [29]存证单元，向所述区块链发送存证交易，以使所述存证交易被所述区块链的节点共识验证后收录于所述区块链的分布式数据库，其中，所述存证交易包括基于所述计算结果生成的第一存证信息。

[30]在又一示出的实施方式中，所述存证交易还包括基于所述目标业务事件数据生成的第二存证信息。

15 [31]在又一示出的实施方式中，所述第二存证信息包括所述目标业务事件数据的哈希摘要。

[32]在又一示出的实施方式中，所述计算节点分别与第一数据终端和第二数据终端通信连接，所述第二数据终端用以接收用户的数据计算申请，所述第一数据终端存储有业务事件数据；

[33]所述接收单元：

20 [34]所述计算存证节点设备接收所述第二数据终端发送的计算调用申请，所述计算调用申请基于用户的数据计算申请而生成；

[35]所述获取单元：

[36]基于目标业务事件数据的查询索引，从所述第一数据终端获取目标业务事件数据。

25 [37]在又一示出的实施方式中，所述计算存证节点设备与所述第一数据终端通过本地通信方式连接，所述计算节点与所述第二数据终端通过外部通信方式连接。

[38]在又一示出的实施方式中，所述计算逻辑由所述第二数据终端通过所述外部通信方式传输至所述计算存证节点设备进行部署。

[39]在又一示出的实施方式中，所述计算逻辑由所述第二数据终端通过所述外部通信方式加密传输至所述计算存证节点设备进行加密部署；

[40]所述计算单元：基于所述目标业务事件数据进行加密计算；

[41]所述计算结果为加密状态的计算结果。

- 5 [42]在又一示出的实施方式中，所述第二数据终端为所述区块链的节点设备；所述存证交易还包括基于所述第一数据终端的身份标识而生成的第三存证信息。

[43]在又一示出的实施方式中，所述存证交易还包括基于发送所述计算调用申请的所述第二数据终端的身份标识而生成的第四存证信息。

- 10 [44]在又一示出的实施方式中，所述装置为保险理赔存证装置；所述计算存证节点设备为理赔计算存证节点设备，所述计算逻辑为理赔计算逻辑；所述计算调用申请为理赔计算调用申请；所述存证交易为理赔存证交易。

- [45]在又一示出的实施方式中，所述装置为保险理赔存证方法；所述计算存证节点设备为理赔计算存证节点设备，所述计算逻辑为理赔计算逻辑；所述计算调用申请为理赔计算调用申请；所述存证交易为理赔存证交易；所述第一数据终端为存储理赔基于的业务事件数据的业务数据方终端；所述第二数据终端为接收用户理赔申请的理赔服务方终端。
- 15

[46]在又一示出的实施方式中，所述区块链为联盟链。

[47]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，执行上述区块链的存证方法所述的步骤。

20 附图说明

[48]图1为本说明书所提供的一实施例所示的区块链的存证方法的流程图；

[49]图2为本说明书所提供的一实施例所示的应用于保险理赔场景中的区块链的存证方法的流程图；

- [50]图3为本说明书所提供的一实施例提供的一种保险理赔系统中的理赔计算存证节点设备执行的基于区块链的理赔存证方法的示意图；
- 25

[51]图4为本说明书所提供的一实施例所示的区块链的存证装置的示意图；

[52]图5为运行本说明书所提供的区块链的存证装置实施例的一种硬件结构图。

具体实施方式

[53]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。

- 5 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。

- [54]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。
- 10

[55]图1是一示例性实施例提供的一种计算存证节点设备执行的区块链的存证方法的流程图，应用于包括计算存证节点设备的区块链系统。

- [56]本发明所述的区块链，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所法比拟的保证数据安全、防攻击篡改的特性。由此可知，在本发明所提供的实施例中，被收录至区块链的分布式数据库中的数据不会被攻击或篡改，从而保证了存证数据的真实与公正性。
- 15
- 20

- [57]本发明所述的计算存证节点设备是指执行数据计算及存证的设备终端；上述执行计算及存证的设备终端可通过遵循相应节点协议、运行节点协议程序的安装来加入该区块链，作为该区块链的节点设备。本领域的技术人员通常将具有区块链分布式数据库的数据全备份的终端设备称为节点（或节点设备），将具有区块链分布式数据库的部分备份数据（如仅有区块头的数据）的终端设备称为客户端等，在本发明提供的各实施例中所述的节点设备不限于上述的节点或客户端，只要直接或间接连入上述区块链、且可发送和获取区块链的分布式数据库的数据的任何终端均可称为本发明所述的节点
- 25

设备。

[58]如图 1 所示, 本实施例所述的区块链存证方法包括:

[59]步骤 102, 所述计算存证节点设备接收计算调用申请, 所述计算调用申请包括对目标业务事件数据的查询索引;

5 [60]步骤 104, 基于目标业务事件数据的查询索引, 获取目标业务事件数据;

[61]步骤 106, 运行所述计算调用申请对应的计算逻辑, 基于所述目标业务事件数据进行计算, 以获得计算结果;

[62]步骤 108, 向所述区块链发送存证交易, 以使所述存证交易被所述区块链的节点共识验证后收录于所述区块链的分布式数据库, 其中, 所述存证交易包括基于所述计算结果生成的第一存证信息。
10

[63]基于本实施例所述的区块链存证方法, 计算存证节点基于计算调用申请包含的对业务事件数据的查询索引获取到相应的目标业务事件数据; 并通过运行该计算调用申请对应的计算逻辑, 计算获得到相应的计算结果。通过将计算结果上传于上述区块链, 基于区块链的防篡改机制完成对计算结果的存证。区块链上的其他节点可从上述区块链上获取到存证交易, 对计算结果进行进一步地应用逻辑。
15

[64]可选的, 上述存证交易还可包括基于目标业务事件数据生成的第二存证信息, 用以协助区块链上的其他节点基于上述第二存证信息对上述计算结果进行审核校验。上述第二存证信息可包括上述目标业务事件数据的哈希摘要。

[65]可选的, 所述计算节点设备分别与第一数据终端和第二数据终端通信连接, 所述第二数据终端用以接收用户的数据计算申请, 所述第一数据终端存储有业务事件数据; 所述计算存证节点设备接收所述第二数据终端发送的计算调用申请, 所述计算调用申请基于用户的数据计算申请而生成; 上述计算节点基于目标业务事件数据的查询索引, 从所述第一数据终端获取目标业务事件数据。
20

[66]在又一示出的实施方式中, 为防止上述第一数据终端的数据发生未授权的泄露风险, 所述计算存证节点设备与所述第一数据终端通过本地通信方式连接, 所述计算节点与所述第二数据终端通过外部通信方式连接。
25

[67]在又一示出的实施方式中, 上述计算节点设备部署的计算逻辑由所述第二数据终端通过所述外部通信方式传输至所述计算存证节点设备进行部署。

[68]可选的, 所述计算逻辑由所述第二数据终端通过所述外部通信方式加密传输至所述计算存证节点设备进行加密部署, 以保护第二数据终端的计算逻辑不被获知; 所述基于所述目标业务事件数据进行计算, 包括基于所述目标业务事件数据进行加密计算; 所述计算结果为加密状态的计算结果。

- 5 [69]在又一示出的实施方式中, 所述第二数据终端为所述区块链的节点设备; 所述存证交易还包括基于所述第一数据终端的身份标识而生成的第三存证信息, 以协助区块链的其他节点设备在获取到上述存证交易后, 对为上述计算结果提供数据支持的第一数据终端进行数据贡献统计计算。

- [70]在又一示出的实施方式中, 所述存证交易还包括基于发送所述计算调用申请的第二数据终端的身份标识而生成的第四存证信息, 对为调用上述计算存证节点进行计算及存证的第二数据终端进行数据贡献统计。
- 10

- [71]以下, 以保险理赔场景为例, 详细阐述本说明书提供的区块链的存证方法。在该场景中, 上述区块链的存证方法为保险理赔存证方法; 上述计算存证节点设备为理赔计算存证节点设备, 上述计算逻辑为理赔计算逻辑; 上述计算调用申请为理赔计算调用申请;
- 15 所述存证交易为理赔存证交易。

- [72]本实施例所述的理赔计算存证节点设备是指在保险理赔中基于可理赔的业务事件数据执行理赔计算的设备终端; 上述执行理赔计算的设备终端可通过遵循相应节点协议、运行节点协议程序的安装来加入作该区块链, 作为该区块链的节点设备。本领域的技术人员通常将具有区块链分布式数据库的数据全备份的终端设备称为节点(或节点设备),
- 20 将具有区块链分布式数据库的部分备份数据(如仅有区块头的数据)的终端设备称为客户端等, 在本说明书提供的各实施例中所述的节点设备不限于上述的节点或客户端, 只要直接或间接连入上述区块链、且可发送和获取区块链的分布式数据库的数据的任何终端均可称为本实施例所述的节点设备。

[73]如图2所示, 本实施例所述的保险理赔方法包括:

- 25 [74]步骤202, 所述理赔计算存证节点设备接收理赔计算调用申请, 所述理赔计算调用申请包括对目标业务事件数据的查询索引。

[75]本实施例所述的理赔计算调用申请是对该理赔计算存证节点设备可执行的理赔计算操作进行申请的数据信息, 该理赔计算调用申请既可以由上述理赔计算存证节点设备的用户直接向上述理赔计算存证节点设备内输入, 也可以由其他终端设备发送至上述理赔

计算存证节点设备。上述由其他终端设备发送至上述理赔计算存证节点设备的具体方式，既可以是点对点发送接收，也可以是其他终端设备将上述理赔计算调用申请发送至区块链的分布式数据库中，由上述理赔计算存证节点设备从上述区块链中获取接收，在本说明书中不作限定。

- 5 [76]本实施例所述的业务事件数据为被保险的用户或其他个体所发生的可用于理赔的具体事件数据，例如用户的就医记录（包括费用收据、病例记录、检查单记录等）、被保险车辆的维修记录等，在保险理赔计算中应基于业务事件数据进行计算。

- [77]在目前的商业保险理赔过程中，参保人必须带齐所有报单、保险理赔所依据的业务事件数据（如医疗收录、病人病例等）到保险公司提交申请，或者手工拍照后通过保险
10 公司 APP 将资料上传给理赔平台并发起理赔申请，整个过程效率低、程序繁琐，需要等待多天才能获得理赔。纸质单据难保管，易丢失，而且当需要在多家保险机构报销时，过程更加繁琐。同时，对于保险公司，由于参保人自己提供相关就诊材料，存在伪造材料的可能性，不仅加大了对理赔材料审核的难度，也带来了一定的骗保风险。

- [78]鉴于以上的理赔现状，在本实施例所述的保险理赔方法中，理赔用户无需自己准备
15 业务事件数据材料，而由理赔计算存证节点设备向业务事件数据的存储终端请求获取。上述理赔计算调用申请可包括对目标业务事件数据的查询索引，以方便获取到目标业务事件数据的原文。例如上述目标业务事件数据为用户张三于 2018 年 11 月 20 日在医院 A 的就医记录数据，则上述用户理赔计算调用申请所包括的对目标业务事件数据的查询索引可以为张三的就诊身份信息（姓名或身份证号码或医疗卡号码）及就诊日期信息等。
20 上述查询索引的具体形式和内容可依据理赔计算存证节点设备或业务事件数据的存储终端对业务事件数据的存储方式而具体设置，在本说明书中不作限定。

[79]步骤 204，基于目标业务事件数据的查询索引，获取目标业务事件数据。

- [80]如上所述，上述理赔计算存证节点设备可基于理赔计算调用申请中包含的对目标业务事件数据的查询索引，从业务事件数据的存储终端获取相应的目标业务事件数据。值
25 得注意的是，上述理赔计算存证节点设备与上述业务事件数据的存储终端既可以是同一终端设备，也可以是不同的终端设备，在本实施例中不做限定。

[81]步骤 206，运行所述理赔计算调用申请对应的理赔计算逻辑，基于所述业务事件数据进行理赔计算，以获得理赔结果。

[82]由于保险理赔通常可基于不同类别、不同保险级别的保险产品提供多种不同类别、

- 不同级别的理赔服务，因此理赔计算节点中可针对多种不同的保险产品或理赔申请，部署不同的理赔计算逻辑。在具体实施时，所述理赔计算调用申请还可包括与所述多种理赔计算逻辑中的至少一种理赔计算逻辑对应的逻辑标识；理赔计算存证节点设备可基于所述逻辑标识获取所述理赔计算调用申请对应的至少一种理赔计算逻辑；进而运行所述
- 5 至少一种理赔计算逻辑，基于所述目标业务事件数据进行理赔计算，以获得至少一个理赔结果。

[83]步骤 208，向所述区块链发送理赔存证交易，以使所述理赔存证交易被所述区块链的节点共识验证后收录于所述区块链的分布式数据库，其中，所述理赔存证交易包括基于所述理赔结果生成的第一存证信息。

- 10 [84]在理赔节点计算获取到理赔结果后，可将上述理赔结果发送到区块链的分布式数据库中进行存证。区块链中的其他节点，可以从区块链的分布式数据库中获取到该理赔结果，以进行相应的理赔结果执行、或理赔结果审计等操作。

- [85]在本说明书中所描述的交易（transaction），是指各方用户通过区块链的节点设备端创建，并需要最终发布至区块链的分布式数据库中的一笔数据。其中，区块链中的交易，
- 15 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，交易可以是用户在区块链中发布的一笔与价值转移无关的、具有业务意图的业务（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）消息或者业务请求。本说
- 20 明书的上述实施例所述的理赔存证交易，即是上述理赔计算存证节点设备发送的，包括基于计算而得的理赔结果而生成的第一存证信息的数据消息，用以为理赔计算节点的理赔结果进行存储。

- [86]将上述理赔存证交易收录到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交易规则而具体设定。在一示出的实施例中，将所述理赔存证交易
- 25 上传到所述区块链的分布式数据库中，包括：

[87]所述区块链中具有记账权限的节点将所述理赔存证交易加入到候选区块；

[88]从所述具有记账权限的节点中确定满足所述区块链共识机制的共识记账节点；

[89]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；

[90]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。上述验证包括但不限于对交易的格式、合法性等方面的验证。

[91]在上述的实施例，具有记账权限的节点是指具有生成候选区块权限的节点。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中确定共识记账节点，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。

[92]PoS 或 DPoS 共识机制与 PoW 类似，均属于公有区块链中确认共识记账节点所常选用的共识算法。在又一示出的实施例中，为降低交易或数据的确认时间、提高交易吞吐量、满足对安全和性能的需求，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。用以处理用户的理赔申请的保险理赔机构方、关于保险及理赔行为的监督机构（如保监会等政府机构）可作为所述联盟链的成员节点设备，并可作为该联盟链的预选的节点，参与区块的记账。联盟链的共识过程也由该预选的节点控制，当网络上有超过设定比例（如 2/3）的节点确认一个区块，该区块记录的交易或数据将得到全网确认。

[93]联盟链通常多采用权益证明或 PBFT、RAFT 等共识算法。PBFT 算法可作为本说明书所提供的联盟链的共识算法的一种优选的实施方式，是由于采用该种算法共识的效率较高，可满足高频交易量的需求，例如在本实施例中理赔计算存证节点设备会频繁接收到理赔计算调用申请，相应地，基于上述理赔计算调用申请而计算出的理赔结果会非常频繁地被向区块链发送。PBFT 算法共识的时延很低，基本达到实时处理的要求，能快速实时地在区块链的新生区块中收录上述理赔存证交易；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，因此具有良好的可使用性。

[94]在又一示出的实施例中，上述理赔存证交易还包括基于目标业务事件数据而生成的第二存证信息。理赔计算节点将上述理赔结果相关的目标业务事件数据存证于区块链中，方便区块链上的其他节点如保险公司方节点设备、保险监督机构方节点设备对本实施例所述的理赔计算节点所执行的理赔方法进行真实有效性审核或管理。

[95]由于上述目标业务事件数据通常涉及被理赔用户的一些隐私信息，如身份信息、个人健康或财产信息等，为进一步保护被理赔用户的隐私不被无关方获知，上述理赔存证交易中所包含的第二存证信息可包括所述目标业务事件数据的哈希摘要。这样在区块链上的其他节点如保险公司方节点设备、保险监督机构方节点设备对本实施例所述的理赔计算存证节点设备所执行的理赔方法进行真实有效性审核或管理时，可以从上述理赔计

算存证节点设备（或业务事件数据的存储终端）获取上述目标业务事件数据的原文，通过将上述原文的哈希值与区块链上存证的目标业务事件数据的哈希值进行比对，即可获知上述原文是否为理赔计算存证节点设备计算所述理赔结果时所基于的目标业务事件数据。

- 5 [96]进一步地，本说明书以包括业务数据方终端、理赔服务方终端和理赔计算存证节点设备的保险理赔系统为例，详细地阐述本说明书所提供的保险理赔方法。在本实施例中，所述理赔计算存证节点设备分别与所述业务数据方终端和所述理赔服务方终端通信连接，所述连接包括但不限于本地连接、外部连接等方式。

- 10 [97]本实施例所述的理赔服务方终端为可与用户进行理赔服务的交互，接收用户的理赔申请、或向用户提供理赔结果、或对用户执行理赔结果的终端设备，具体可包括各家独立的保险公司的服务器、或多个保险公司统一设置的理赔服务平台机构对应的服务器等。

- [98]本实施例所述的业务数据方终端为存储有理赔所基于的业务事件数据的终端设备。例如，当用户的理赔申请为医疗保险理赔申请时，相应的业务数据方终端为存储有用户医疗事件数据的终端设备，具体如综合性医院、专科性诊所、个性化医疗服务（如基因检测、身体检查）公司等机构的数据服务器；当用户的理赔申请为车辆保险理赔申请时，
- 15 相应的业务事件数据方终端为存储有车辆维修、美容、改装等记录的终端设备。随着保险业务的发展，越来越多的事物或事物的状态被纳入到保险或理赔的范围中来，相应的业务数据存储终端均可属于本实施例所述的业务数据方终端。

- [99]在又一示出的实施方式中，上述理赔计算存证节点设备与所述业务数据方终端通过
- 20 所述本地通信方式连接，上述理赔计算存证节点设备与所述理赔服务终端通过外部通信方式连接，亦即，上述理赔计算存证节点设备被配置在上述业务数据方终端的本地。上述本地通信方式包括但不限于有线连接通信、终端内数据总线连接通信、专用总线连接通信、局域网通信；上述外部通信方式包括但不限于外部网络通信等。

- [100] 通过将上述理赔计算存证节点设备配置在上述业务数据方终端的本地，使得业
- 25 务数据方终端的管理机构可以监控或取证上述理赔计算节点的输出数据，防止理赔计算节点将其获取的业务事件数据进行未授权的传输，有效保证业务事件数据的使用安全，防止业务事件数据产生未授权的输出后而可能产生数据安全风险。

[101] 理赔计算存证节点设备内部署的理赔计算逻辑通常是基于用户购买或用户作为受益人的保险产品合约所规定的理赔规则而制定的，因此，上述理赔计算逻辑的制定或

部署方通常为保险理赔服务机构对应的终端设备，或本实施例所述的理赔服务方终端。

[102] 当上述理赔计算存证节点设备需被本地配置于上述业务数据方终端进行理赔逻辑计算时，则既可以由上述理赔服务方终端在保险理赔服务机构的本地（及上述理赔服务方终端的本地）依据用户对应的保险理赔规则部署上述理赔计算节点内的理赔计算逻辑，并在部署完后将上述理赔计算存证节点设备移动至上述业务数据方终端的本地，与上述业务数据方终端以上述本地通信方式进行连接；也可以由上述理赔服务方终端通过外部通信方式将上述理赔计算逻辑传输至所述理赔计算节点内进行部署安装。

[103] 由于理赔服务方通常可基于不同类别、不同保险级别的保险产品提供多种不同类别、不同级别的理赔服务，理赔服务方可能经常增加理赔计算逻辑的种类，或每隔设定的时间对已有的理赔计算逻辑进行更新或修改；而且本实施例所述的理赔计算存证节点设备还可以与多个理赔服务方连接以提供理赔计算服务；本领域的技术人员熟知，相比于在理赔服务方终端本地配置理赔计算逻辑并移动安装上述理赔计算节点的方式，通过外部通信方式在上述理赔计算节点内传输部署理赔计算逻辑，可以灵活地配置、增加或更新理赔计算逻辑。

[104] 而且，由于依据用户对应的保险理赔规则而生成的理赔计算逻辑通常与保险理赔服务方的业务机密或商业秘密相关，上述理赔计算逻辑还可以由所述理赔服务方终端通过上述外部通信方式加密传输至所述理赔计算节点进行加密部署；这样即使理赔计算节点位于上述业务数据方终端的本地，业务数据方也不能获知上述理赔计算逻辑的具体规则设置等机密内容，从而保护了保险理赔方的商业秘密；而且，当理赔计算存证节点设备与多个理赔服务方终端连接时，将相应理赔服务方提供的理赔计算逻辑进行加密，有效地隔离了不同理赔服务方的商业秘密。

[105] 图2示意了本实施例所述的理赔计算存证节点设备所执行的保险理赔方法步骤。本实施例所述的理赔计算节点可以与多个理赔服务方终端和多个业务数据方终端连接，为不同的保险理赔机构提供理赔计算服务；相应地，上述理赔计算存证节点设备部署有多种理赔计算逻辑。上述理赔计算存证节点设备作为区块链的节点设备，与区块链网络连接。本实施例并不限定上述业务数据方终端或理赔服务方终端是否与区块链网络连接。

[106] 如图3所示，上述理赔计算存证节点设备执行以下步骤：

[107] 步骤301，接收所述理赔服务方终端发送的理赔计算调用申请，所述理赔计算调用申请基于用户的理赔申请而生成。

- [108] 本实施例所述的理赔服务方终端通过与用户交互，获取到用户理赔申请。由于本实施例所提供的理赔服务方法无需用户提供理赔所基于的业务事件数据，上述用户理赔申请及基于用户理赔申请生成的理赔计算调用申请可包括获取目标业务事件数据的查询索引，所述目标业务事件数据即用户理赔所基于的业务事件数据，例如上述目标业务事件数据为用户张三于2018年11月20日在医院A的就医记录数据，则上述用户理赔计算调用申请所包括的对目标业务事件数据的查询索引张三的就诊身份信息（姓名或身份证号码或医疗卡号码）及就诊日期信息等。上述查询索引的具体形式和内容可依据理赔计算节点或业务数据方终端对业务事件数据的存储方式而具体设置，在本说明书中不作限定。
- 10 [109] 由于在本实施例中所说理赔计算节点部署有多种理赔计算逻辑，上述用户理赔计算调用申请还包括与上述多种理赔计算逻辑中的至少一种理赔计算逻辑对应的逻辑标识，以方便理赔计算节点选取对应的理赔计算逻辑进行计算。
- [110] 步骤302，基于目标业务事件数据的查询索引，从所述业务数据方终端获取目标业务事件数据。
- 15 [111] 上述理赔计算存证节点设备从上述业务数据方终端获取目标业务事件数据的具体方式可以有多种，例如上述理赔计算节点可以将上述用户理赔计算调用申请所包括的对目标业务事件数据的查询索引发送至上述业务数据方终端，上述业务数据方终端在查询获取到上述目标业务事件数据后，而将其发送至上述理赔计算存证节点设备。
- [112] 在又一种示出的实施方式中，上述业务数据方终端为保证自身终端存储的所有业务事件数据及其他数据的安全，可以向相应的理赔服务方进行数据授权，基于上述本地通信方式将被授权的业务事件数据集合传输至上述理赔计算节点，以方便理赔计算节点在理赔计算时可以从上述被授权的业务事件数据集合中直接获取目标业务事件数据。对业务事件数据的具体的授权规则，可以依据业务数据方和理赔服务方的约定而具体设定，例如，理赔服务方终端可以将被保险的用户名单发送给业务数据方，业务数据方终端基于上述被保险的用户名单整理上述被保险的用户对应的业务事件数据集合。
- 20 [113] 在又一种示出的实施方式中，上述业务数据方终端向理赔服务方进行数据授权可以通过向所述理赔计算存证节点设备发送被授权的业务事件数据对应的数据索引表的形式来实现。理赔计算存证节点设备在接收到上述理赔计算调用申请后，基于上述理赔计算调用申请包括的对目标业务事件数据的查询索引在上述被授权的业务事件数据索引表中进行检索，如果能够在上述数据索引表中检索查询到上述查询索引或上述查询
- 25
- 30

索引指向的数据对象，即表明上述目标业务事件数据为业务数据方终端授权的业务事件数据，则上述理赔服务方再基于所述查询索引，从业务数据方终端存储的所述被授权的业务事件数据集合中获取所述目标业务事件数据。本实施方式所提供的上述理赔计算存证节点设备从上述业务数据方终端获取目标业务事件数据的实现方式，省去了理赔计算

5 存证节点设备存储被授权的业务事件数据所需的存储容量需求，且使得业务数据方终端对业务事件数据有着更灵活的可操作性。

[114] 当然，由于本实施例中的理赔计算存证节点设备可以为多个理赔服务方终端提供理赔计算服务，理赔计算存证节点设备可将不同理赔服务方终端被授权的不同的业务事件数据作出数据隔离，也可将不同理赔服务方终端被授权的相同的业务事件数据作出

10 数据共享，具体方式在此不再赘述。

[115] 步骤 303，运行所述理赔计算调用申请对应的理赔计算逻辑，基于所述业务事件数据进行理赔计算，以获得理赔结果。

[116] 在一示出的实施方式中，当上述理赔计算逻辑是由所述理赔服务方终端通过所述外部通信方式加密传输至所述理赔计算存证节点设备而加密部署的时，所述理赔计算

15 为基于所述目标业务事件数据和被加密的理赔计算逻辑而进行的加密计算；相应地，所述理赔结果为加密状态的理赔结果。在本实施方式中，虽然理赔计算存证节点设备被本地部署于业务数据方终端，业务数据方终端由于不能解密上述理赔计算逻辑，也不能解密上述理赔计算的理赔结果，从而既保证了业务数据方终端的业务事件数据的安全性，又保证了理赔计算过程的隐私性和安全性。

20 [117] 在本实施例中，所述理赔计算存证节点设备部署有多种理赔计算逻辑时，本领域的技术人员易知，所述用户理赔计算调用申请还应包括与所述多种理赔计算逻辑中的至少一种理赔计算逻辑对应的逻辑标识；相应地，基于所述逻辑标识获取所述用户理赔计算调用申请对应的至少一种理赔计算逻辑；运行与所述至少一种理赔计算逻辑，基于所述目标业务事件数据进行理赔计算，以获得至少一个理赔计算的结果。上述实施例尤其适用于同一用户参保了多项保险产品，且该多项保险可基于同一目标业务事件数据进行多次理赔的情景中

25

[118] 步骤 304，向所述区块链发送理赔存证交易，以使所述理赔存证交易被所述区块链的节点共识验证后收录于所述区块链的分布式数据库，其中，所述理赔存证交易包括基于所述理赔结果生成的第一存证信息。

[119] 由于本实施例并不限定上述理赔服务方终端是否为上述区块链的节点设备，因此上述理赔服务方终端既可以通过与上述理赔计算存证节点设备通过点对点的通信而获得上述理赔结果，也可以作为上述区块链的节点设备，从区块链上获取上述理赔存证交易，而获得上述理赔结果。本领域的技术人员应知，通过区块链获得上述理赔结果的方式，基于区块链的防篡改机制，更能保证上述理赔结果的真实性。

[120] 当上述理赔计算节点运行的上述理赔计算调用申请对应的理赔计算逻辑是由所述理赔服务方终端通过外部通信方式加密传输至所述理赔计算节点进行加密部署时，所述理赔结果也为基于所述目标业务事件数据和被加密的理赔计算逻辑而进行的加密计算所得的加密状态的理赔结果。上述理赔服务方在获取到加密状态的理赔结果后，可对该理赔结果进行解密，并将解密后的理赔结果发送至用户端的设备终端。

[121] 上述各实施例所述的理赔结果，可包括理赔方案的具体执行内容（包括是否理赔、理赔金额度、理赔金的支付期限等）的告知书、或向用户直接支付理赔金的支付指令等内容。相应地，理赔服务方终端在获取到上述理赔结果后，可以将理赔方案的具体执行内容的告知书发送至用户端设备终端，或直接向用户（或其他保险理赔受益人）的账户转移理赔金。

[122] 保险理赔机构通常会对其执行的理赔结果进行阶段性审核或管理，因此在本说明书提供的又一实施例中，上述理赔计算存证节点设备除存证上述理赔结果（或基于上述理赔结果生成的第一存证信息）外，还可存证支持作出上述理赔结果的目标业务事件数据，或是，基于上述目标业务事件数据生成的第二存证信息。该第二存证信息可以包括上述目标业务事件数据的哈希摘要，这样，既为支持上述理赔结果的目标业务事件数据进行存证，又不会泄露用户及业务数据方的数据隐私。在保险理赔机构进行理赔审计管理时，可以抽样要求上述业务数据方提供原始业务事件数据，并将原始业务事件数据与区块链上存证的哈希数据摘要进行比对，以鉴证上述原始业务事件数据是否为理赔计算时所基于的目标业务事件数据。

[123] 在图 3 所示的保险理赔系统中，同一理赔服务方可以与多家业务数据方进行数据授权合作服务，例如，同一保险公司在保险理赔时可以认定多家医疗机构提供的用户就医记录，因此，该保险公司可以上述多家医疗机构进行数据授权合作，以基于上述多家医疗机构授权的用户就医记录，使理赔计算存证节点设备实施本说明书各实施例所提供的保险理赔方法。在此情况下，理赔计算存证节点设备向区块链发送的理赔存证交易还可包括基于所述业务数据方终端的身份标识而生成的第三存证信息；这样，在理赔服

务方进行阶段性理赔结果审计或管理时，可以作为上述区块链的节点设备，从上述区块链的分布式数据库中获取为上述理赔结果而提供业务事件数据支持的业务数据方终端的身份，计算相应的业务数据方终端的数据贡献，进而可向上述业务数据方进行相应的贡献费用结算。

- 5 [124] 相似的，理赔计算存证节点设备向区块链发送的理赔存证交易还可包括基于发送所述理赔计算调用申请的理赔服务方的身份标识而生成的第四存证信息，以便于区块链上的节点设备，如理赔计算存证节点设备、或对保险理赔进行监管的行政机构等，统计分析、监督管理不同理赔服务方的保险理赔服务开展情况。

- 10 [125] 与上述流程实现对应，本说明书的实施例还提供了一种区块链的存证装置。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。

- 15 [126] 图 4 所示为一种区块链的存证装置，应用于包括计算存证节点设备的区块链系统；所述计算存证节点设备中部署有至少一种计算逻辑；所述装置 40 包括：

[127] 接收单元 402，接收计算调用申请，所述计算调用申请包括对目标业务事件数据的查询索引；

[128] 获取单元 404，基于目标业务事件数据的查询索引，获取目标业务事件数据；

- 20 [129] 计算单元 406，运行所述计算调用申请对应的计算逻辑，基于所述业务事件数据进行计算，以获得计算结果；

[130] 存证单元 408，向所述区块链发送存证交易，以使所述存证交易被所述区块链的节点共识验证后收录于所述区块链的分布式数据库，其中，所述存证交易包括基于所述计算结果生成的第一存证信息。

- 25 [131] 在又一示出的实施方式中，所述存证交易还包括基于所述目标业务事件数据生成的第二存证信息。

[132] 在又一示出的实施方式中，所述第二存证信息包括所述目标业务事件数据的哈希摘要。

- [133] 在又一示出的实施方式中，所述计算节点分别与第一数据终端和第二数据终端通信连接，所述第二数据终端用以接收用户的数据计算申请，所述第一数据终端存储有业务事件数据；
- [134] 所述接收单元 402:
- 5 [135] 所述计算存证节点设备接收所述第二数据终端发送的计算调用申请，所述计算调用申请基于用户的数据计算申请而生成；
- [136] 所述获取单元 404:
- [137] 基于目标业务事件数据的查询索引，从所述第一数据终端获取目标业务事件数据。
- 10 [138] 在又一示出的实施方式中，所述计算存证节点设备与所述第一数据终端通过本地通信方式连接，所述计算节点与所述第二数据终端通过外部通信方式连接。
- [139] 在又一示出的实施方式中，所述计算逻辑由所述第二数据终端通过所述外部通信方式传输至所述计算存证节点设备进行部署。
- [140] 在又一示出的实施方式中，所述计算逻辑由所述第二数据终端通过所述外部通信方式加密传输至所述计算存证节点设备进行加密部署；
- 15 [141] 所述计算单元 406: 基于所述目标业务事件数据进行加密计算；
- [142] 所述计算结果为加密状态的计算结果。
- [143] 在又一示出的实施方式中，所述第二数据终端为所述区块链的节点设备；所述存证交易还包括基于所述第一数据终端的身份标识而生成的第三存证信息。
- 20 [144] 在又一示出的实施方式中，所述存证交易还包括基于发送所述计算调用申请的第二数据终端的身份标识而生成的第四存证信息。
- [145] 在又一示出的实施方式中，所述装置为保险理赔存证装置；所述计算存证节点设备为理赔计算存证节点设备，所述计算逻辑为理赔计算逻辑；所述计算调用申请为理赔计算调用申请；所述存证交易为理赔存证交易。
- 25 [146] 在又一示出的实施方式中，所述装置为保险理赔存证方法；所述计算存证节点设备为理赔计算存证节点设备，所述计算逻辑为理赔计算逻辑；所述计算调用申请为理赔计算调用申请；所述存证交易为理赔存证交易；所述第一数据终端为存储理赔基于的业务事件数据的业务数据方终端；所述第二数据终端为接收用户理赔申请的理赔服务方

终端。

[147] 在又一示出的实施方式中，所述区块链为联盟链。

[148] 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。

- 5 [149] 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。

- 10 [150] 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、可穿戴设备或者这些设备中的任意几种设备的组合。

- 15 [151] 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理赔计算节点执行的基于区块链的保险理赔方法的各个步骤。对理赔计算节点执行的保险理赔方法的各个步骤的详细描述请参见之前的内容，不再重复。

- 20 [152] 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。

[153] 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。

- 25 [154] 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。

[155] 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。

[156] 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, 5 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。

[157] 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, 10 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。

[158] 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 15 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。