(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 109816541 A
(43)申请公布日 2019.05.28

(21)申请号 201910066422.1

(22)申请日 2019.01.24

(71)申请人 易保互联医疗信息科技(北京)有限公司
地址 100027 北京市朝阳区新源里16号14层2座12B06

(72)发明人 金以东 李雪莉 任旻旻 王语莫 周大胜

(74)专利代理机构 北京科石知识产权代理有限公司 11595
代理人 唐玉刚

(51)Int.Cl.
G06Q 40/08(2012.01)
G06Q 30/00(2012.01)
G06Q 50/26(2012.01)

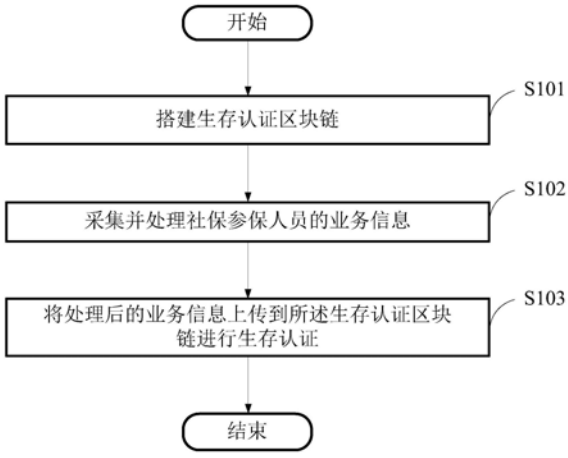
权利要求书3页 说明书8页 附图2页

(54)发明名称

基于区块链的多维数据生存认证方法、存储介质及设备

(57)摘要

本发明提供一种基于区块链的多维数据生存认证方法、存储介质及设备，其中，方法包括：搭建生存认证区块链；采集并处理社保参保人员的业务信息；将处理后的业务信息上传到所述生存认证区块链进行生存认证。本发明可以保证生存认证使用的业务信息的真实性，并且业务信息来源可以追溯，不可篡改；打破不同业务系统之间的信息壁垒，在保证数据安全的基础上，结合生存认证区块链上不同节点的数据进行生存认证，使得生存认证结果更加精确；可以提高办事效率，减轻社保机构的办事压力，最大程度使得“数据多跑路、参保人员少跑路”，生存认证在社保参保人员无感知的状态下完成。



CN 109816541 A

1.一种基于区块链的多维数据生存认证方法,其特征在于,该方法包括:

搭建生存认证区块链;

采集并处理社保参保人员的业务信息;

将处理后的业务信息上传到所述生存认证区块链进行生存认证。

2.根据权利要求1所述的基于区块链的多维数据生存认证方法,其特征在于,搭建生存认证区块链的步骤,具体包括:

制定上链需求表、共识算法和智能合约;

组建参保人员前端节点、服务机构节点和与所述服务机构节点对应的服务器节点,其中,所述服务机构节点包括多个人社服务节点和多个非人社服务节点,所述人社服务节点具有服务机构前端子节点,所述服务机构前端子节点用于选择生存认证时间段并批量录入参保人员编号,所述非人社服务节点用于存放所述非人社服务节点的满足所述上链需求表的业务信息,所述参保人员前端用于社保参保人员进行生物特征认证,所述服务器节点用于共识和记账;

分别为所述服务器节点分配互不相同的公钥和私钥;以及

所述人社服务节点与所述非人社服务节点之间交换公钥。

3.根据权利要求2所述的基于区块链的多维数据生存认证方法,其特征在于,采集并处理社保参保人员的业务信息的步骤,具体包括:

获取社保参保人员的授权信息,其中,所述授权信息允许所述服务机构节点基于该社保参保人员的业务信息对该社保参保人员进行生存认证;

利用所述人社服务节点的公钥对所述业务信息中包含的内容部分进行加密得到内容加密部分,其中,所述内容部分包括参保人员编号、业务办理时间、业务数据、业务类型和机构编码;

利用所述非人社服务节点的公钥对所述非人社服务节点的公钥和所述业务信息中包含的机构编码进行加密得到确权加密部分;

利用拜占庭容错共识机制对所述内容加密部分和所述确权加密部分进行共识。

4.根据权利要求3所述的基于区块链的多维数据生存认证方法,其特征在于,将处理后的业务信息上传到所述生存认证区块链进行生存认证的步骤,具体包括:

将共识后的所述内容加密部分和所述确权加密部分上传至所述生存认证区块链;

利用所述人社服务节点的私钥解密所述内容加密部分得到所述机构编码;

根据所述机构编码查找对应的所述非人社服务节点的公钥;

利用查找到的所述非人社服务节点的公钥加密所述机构编码和查找到的所述非人社服务节点的公钥得到确权数据;

比对所述确权加密部分和所述确权数据确定所述内容加密部分是否来自对应的所述非人社服务节点;

如果所述内容加密部分来自对应的所述非人社服务节点,对所述内容加密部分进行生存认证,否则生存认证失败。

5.根据权利要求4所述的基于区块链的多维数据生存认证方法,其特征在于,利用所述人社服务节点的私钥解密所述内容加密部分得到所述机构编码的步骤之前,还包括:

通过所述人社服务节点的服务机构前端子节点选择生存认证时间段并批量录入参保

人员编号；

将所述人社服务节点的公钥和机构编码写入所述智能合约；

所述人社服务节点将所述人社服务节点的公钥和机构编码上传至所述生存认证区块链；

比对所述智能合约中的所述人社服务节点的公钥和机构编码，以及所述人社服务节点上传的所述人社服务节点的公钥和机构编码，确认是否是所述人社服务节点发起的生存认证。

6.根据权利要求5所述的基于区块链的多维数据生存认证方法，其特征在于，对所述内容加密部分进行生存认证的步骤，具体包括：

比对解密所述内容加密部分得到的参保人员编号与批量录入的参保人员编号，确认解密所述内容加密部分得到的所述业务数据为欲做生存认证的社保参保人员的交易数据；

确认所述业务数据中是否包含有社保参保人员的死亡记录数据；

如果包含有社保参保人员的死亡记录数据，直接认定所述参保人员编号对应的社保参保人员的生存状态为死亡；

如果没有包含有社保参保人员的死亡记录数据，利用生存认证公式和解密所述内容加密部分得到的业务办理时间确定所述参保人员编号对应的社保参保人员的生存状态；

如果确定所述参保人员编号对应的社保参保人员的生存状态为生存，则将该社保参保人员的生存状态上传至所述生存认证区块链；

如果无法确定所述参保人员编号对应的社保参保人员的生存状态为生存，则向所述非人社服务节点推送无法确定该社保参保人员的生存状态的通知，要求该社保参保人员到所述参保人员前端节点做生物特征认证。

7.根据权利要求6所述的基于区块链的多维数据生存认证方法，其特征在于，所述生存认证公式Y_N具体为：

$$Y_N=\sum_{i=1}^{N}\frac{e^{CX_i}-e^{-CX_i}}{(e^{CX_i}+e^{-CX_i})CX_i}\cdot\omega_i$$

其中，公式中i为进行生存认证使用的业务信息的序数；N为业务信息的总条目数；e为自然常数；X_i为生成第i条业务信息距离生存认证的时间；C为时间权重函数的参数，取值为20/M，其中，以天作为时间段时，M取365，以月为时间段时，M取12，以年为时间段时，M取1；ω_i为社保参保人员办理业务的权重，包括强生存权重、中生存权重和弱生存权重；$\frac{e^{CX_i}-e^{-CX_i}}{(e^{CX_i}+e^{-CX_i})CX_i}$为时间权重函数。

8.根据权利要求2所述的基于区块链的多维数据生存认证方法，其特征在于，所述非人社服务节点包括医疗服务机构节点、公安服务机构节点、银行服务机构节点和民政服务机构节点。

9.一种存储介质，其特征在于，所述存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现权利要求1至8中任意一项所述方法的步骤。

10.一种计算机设备，其特征在于，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现权利要求1至8中

任意一项所述方法的步骤。

基于区块链的多维数据生存认证方法、存储介质及设备

技术领域

[0001] 本发明涉及区块链技术领域，尤其涉及一种基于区块链的社保参保人员生存认证方法，具体来说就是一种基于区块链的多维数据生存认证方法、存储介质及设备。

背景技术

[0002] 生存认证是证明退休人员是否健在，是否符合领取退休养老待遇条件的一道程序，退休社保参保人员能否通过生存认证是能否领取基本养老金的关键。为了保证养老保险基金的安全，防范和打击不法分子欺诈、冒领养老保险基金，生存认证是必要的。

[0003] 现有技术中，凡是从社保基金领取养老金的企、事业退休人员及生活补助人员，每年都要进行一次领取养老金资格的生存认证工作。逾期没有参加生存认证的人员，将暂停发放其基本养老金，待其通过生存认证后给予补发。

[0004] 为了方便市民，堵住冒领养老金的黑洞，目前的生存认证方法采用“土洋结合”方式，主要包括以下方式：1.现场认证：又称“集中认证”，对参保人进行面对面认证，认证地点为社保经办机构；2.照相认证：属地开通“异地认证”的地区，异地居住的离退休人员，每年照相后寄回社保经办机构，照相人持当年某月的月历或持当月发行的报纸(杂志)，以证明本人键在，有的社保机构还制定退休人员每年用不同动作拍照；3.社区认证：加强与社区服务组织的联系，委托社区服务组织派工作人员上门慰问，了解生存认证状况；4.上门认证：对高龄、行动不便的离退休人员，由社保经办机构派工作人员上门慰问，了解其生存情况；5.户籍认证：请公安部门协助提供离退休人员的生存情况和异地安置情况；6.信函认证：对异地安置离退休人员每年通过慰问信或公函等信函邮寄形式，确认生存状况；7.委托认证：在养老金发放中，借助邮政的网点多，投递员走村串巷的优势，委托邮局代发养老金并负责了解和掌握退休人员生存情况；8.视频认证：通过社交即时通讯工具，开展离退休人员远程视频认证；9.指纹认证：利用人体指纹的不可重复性，利用养老金发放指纹识别系统来防范死亡家属冒领养老金；10.刷脸认证：采用“人脸识别”技术。

[0005] 但是，现有生存认证存在以下问题：仍然存在不同的办事地点需要跑多次、需要千里奔波等生存认证难的现象；认证方式仅仅局限于人力资源与社会保障服务机构的生存认证数据，没有充分运用其他生存认证数据(如医疗机构的看诊数据、民政的结婚登记数据等)进行认证；如果不法分子假造生存认证数据，冒领养老保险基金时无法追责。

[0006] 综上所述，政府如何利用可以证明参保人生存的多方数据来做生存认证，如何解决“数据多跑路，群众少跑腿”，并通过高效、便捷的方法采集到真实信息，并通过信息披露防范假信息，做到数据可追溯、可追责、不可篡改成为了所属领域技术人员亟需解决的问题。

发明内容

[0007] 有鉴于此，本发明要解决的技术问题在于提供一种基于区块链的多维数据生存认证方法、存储介质及设备，解决了现有生存认证技术无法利用多维大数据交叉比对，社保参

保人员生存认证难，而且认证效率低下的问题。

[0008] 为了解决上述技术问题，本发明的具体实施方式提供一种基于区块链的多维数据生存认证方法，包括：搭建生存认证区块链；采集并处理社保参保人员的业务信息；将处理后的业务信息上传到所述生存认证区块链进行生存认证。

[0009] 本发明的具体实施方式还提供一种存储介质，所述存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现基于区块链的多维数据生存认证方法的步骤。

[0010] 本发明的具体实施方式还提供一种计算机设备，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现基于区块链的多维数据生存认证方法的步骤。

[0011] 根据本发明的上述具体实施方式可知，基于区块链的多维数据生存认证方法、存储介质及设备至少具有以下有益效果：建立了医疗机构、公安、银行、经办机构、民政等相关部门信息数据共享机制，打破各部门之间的信息壁垒，不需要社保参保人员跨部门确权，确保验证数据的真实、安全、可靠、可追溯，利用不同部门的多条业务信息进行生存认证，生存认证结果可靠性和准确性高；利用多维大数据进行交叉对比，不需要参保用户特意去进行生存认证，自动完成社保参保人员的生存认证，参保用户不会感知到生存认证的过程，最大程度地使得“数据多跑路，参保人少跑路”，解决异地社保参保人员生存认证困难的问题，认证过程简单、认证效率高，减轻经办机构的办事压力；生存认证区块链上节点提供的业务信息可以追溯，防篡改，解决了数据共享时可能出现的数据抵赖、数据篡改等问题。

[0012] 应了解的是，上述一般描述及以下具体实施方式仅为示例性及阐释性的，其并不能限制本发明所欲主张的范围。

附图说明

[0013] 下面的所附附图是本发明的说明书的一部分，其绘示了本发明的示例实施例，所附附图与说明书的描述一起用来说明本发明的原理。

[0014] 图1为本发明具体实施方式提供的一种基于区块链的多维数据生存认证方法的流程图。

[0015] 图2为本发明具体实施方式提供的一种搭建的参保人员生存认证区块链。

[0016] 图3为本发明具体实施方式提供的一种参保业务信息上链后的参保人员生存情况区块链。

[0017] 图4为本发明具体实施方式提供的一种时间权重函数图像。

具体实施方式

[0018] 为使本发明实施例的目的、技术方案和优点更加清楚明白，下面将以附图及详细叙述清楚说明本发明所揭示内容的精神，任何所属技术领域技术人员在了解本发明内容的实施例后，当可由本发明内容所教示的技术，加以改变及修饰，其并不脱离本发明内容的精神与范围。

[0019] 本发明的示意性实施例及其说明用于解释本发明，但并不作为对本发明的限定。另外，在附图及实施方式中所使用相同或类似标号的元件/构件是用来代表相同或类似部分。

[0020] 关于本文中所使用的“第一”、“第二”、…等，并非特别指称次序或顺位的意思，也非用以限定本发明，其仅为了区别以相同技术用语描述的元件或操作。

[0021] 关于本文中所使用的方向用语，例如：上、下、左、右、前或后等，仅是参考附图的方向。因此，使用的方向用语是用来说明并非用来限制本创作。

[0022] 关于本文中所使用的“包含”、“包括”、“具有”、“含有”等等，均为开放性的用语，即意指包含但不限于。

[0023] 关于本文中所使用的“及/或”，包括所述事物的任一或全部组合。

[0024] 关于本文中的“多个”包括“两个”及“两个以上”；关于本文中的“多组”包括“两组”及“两组以上”。

[0025] 关于本文中所使用的用语“大致”、“约”等，用以修饰任何可以微变化的数量或误差，但这些微变化或误差并不会改变其本质。一般而言，此类用语所修饰的微变化或误差的范围在部分实施例中可为20％，在部分实施例中可为10％，在部分实施例中可为5％或是其他数值。本领域技术人员应当了解，前述提及的数值可依实际需求而调整，并不以此为限。

[0026] 图1为本发明具体实施方式提供的一种基于区块链的多维数据生存认证方法的流程图，如图1所示，首先搭建生存认证区块链，然后采集社保参保人员的业务信息，并将处理后的业务信息上传到生存认证区块链做生存认证。

[0027] 该附图所示的具体实施方式中，基于区块链的多维数据生存认证方法包括：

[0028] S101：搭建生存认证区块链。本发明的实施例中，步骤S101具体包括：

[0029] 制定上链需求表、共识算法和智能合约。其中，上链需求表的全称为人社服务机构生存认证上链需求表，人社服务节点根据生存认证的需求制定人社服务机构生存认证上链需求表，并通过区块链公布给非人社服务节点，上链需求表对可以上生存认证区块链的业务类型做了明确规定。共识算法具体为拜占庭容错(PBFT)算法，即使区块链网络上存在故障服务器节点或者遭受破坏的服务器节点，共识算法也能保证正常运行的服务器节点之间形成共识。智能合约的目的主要包括：确定发起的生存认证的节点为人社服务节点；按照规定的生存认证时间段和目标参保人员进行认证；从区块链上抽取目标参保人员的业务信息进行多维数据痕迹生存认证；对已经通过生存认证的社保参保人员的业务信息进行记录，提高生存认证的验证速度。

[0030] 组建参保人员前端节点、服务机构节点和与所述服务机构节点对应的服务器节点，其中，所述服务机构节点包括多个人社服务节点和多个非人社服务节点，参保人员前端节点可以为服务机构节点中的设备，也可以为人社服务节点中的设备，每个人社服务节点都具有一个服务机构前端子节点，所述服务机构前端子节点用于选择对多条业务信息进行生存认证的时间段，还用于批量录入参保人员编号，多条业务信息来自不同的服务机构节点；所述非人社服务节点用于存放所述非人社服务节点的满足所述上链需求表的社保参保人员的业务信息，所述参保人员前端用于社保参保人员生物特征认证，所述服务器节点用于共识和记账。所述非人社服务节点包括多个医疗服务节点、多个公安服务节点、多个银行服务节点和多个民政服务节点等。

[0031] 分别为所述服务器节点分配互不相同的公钥和私钥。

[0032] 所述人社服务节点与所述非人社服务节点之间交换公钥。此时，医疗服务机构节点拥有：医疗服务机构公钥(MPUK)、医疗服务机构私钥(MPRK)、人社服务机构公钥(RPUK)；

银行服务节点拥有:银行服务机构公钥(BPUK)、银行服务机构私钥(BPRK)、人社服务机构公钥(RPUK);民政服务节点拥有:民政服务机构公钥(CPUK)、民政服务机构私钥(CPRK)、人社服务机构公钥(RPUK);公安服务节点拥有:公安服务机构公钥(PPUK)、公安服务机构私钥(PPRK)、人社服务机构公钥(RPUK);人社服务节点拥有:人社服务机构公钥(RPUK)、人社服务机构私钥(RPRK)、公安服务机构公钥(PPUK)、民政服务机构公钥(CPUK)、银行服务机构公钥(BPUK)、医疗服务机构公钥(MPUK)。

[0033] S102:采集并处理社保参保人员的业务信息。本发明的实施例中,步骤S102具体包括:

[0034] 获取社保参保人员的授权信息,其中,所述授权信息允许所述服务机构节点基于该社保参保人员的业务信息对该社保参保人员进行生存认证。本发明的具体实施例中,获取社保参保人员的授权信息之后,所述非人社服务节点还可以对所述业务信息进行筛选处理,筛选出满足所述上链需求表的业务信息,摈弃与生存认证无关的业务信息,从而减少后续步骤的数据处理量。经社保参保人员授权后,非人社服务节点才能对业务信息进行筛选处理,保护社保参保人员的隐私及数据自主权;上链需求表明确规定哪些业务信息对生存认证有价值,由人社服务节点制定并公布(例如:社保参保人员去在xxx医院进行体检,该业务信息对生存认证有意义,在上链需求表中服务机构为医疗服务机构,服务类型编号为MA001,业务详细名称为在xxx医院进行体检),各非人社服务节点将社保参保人员办理的业务信息(服务机构采集到的业务信息)与上链需求表中的业务详细名称进行对比筛选出对生存认证有意义的业务信息,进行上链请求,摈弃与生存认证无关的业务信息(例如:社保参保人员通过ATM机取款,因为取款时只需要输入密码,并不会认证是否是持卡本人在取款,该业务信息对生存认证没有意义,可以过滤掉)。

[0035] 利用所述人社服务节点的公钥对所述业务信息中包含的内容部分进行加密得到内容加密部分,其中,所述内容部分包括参保人员编号、业务办理时间、业务数据、业务类型和机构编码。其中,业务类型便于非人社服务节点对业务信息进行筛选处理。

[0036] 利用所述非人社服务节点的公钥对所述非人社服务节点的公钥和所述业务信息中包含的机构编码进行加密得到确权加密部分。其中,确权加密部分便于人社服务节点确权。

[0037] 利用拜占庭容错共识机制对所述内容加密部分和所述确权加密部分进行共识。

[0038] S103:将处理后的业务信息上传到所述生存认证区块链进行生存认证。本发明的实施例中,步骤S103具体包括:

[0039] 将共识后的所述内容加密部分和所述确权加密部分上传至所述生存认证区块链。

[0040] 通过所述人社服务节点的服务机构前端子节点选择生存认证时间段并批量录入参保人员编号。其中,参保人员编号可以为参保人员身份证号码。

[0041] 将所述人社服务节点的公钥和机构编码写入所述智能合约。其中,将所述人社服务节点的公钥和机构编码写入所述智能合约后,写入的公钥和机构编码无法修改或删除。

[0042] 所述人社服务节点将所述人社服务节点的公钥和机构编码上传至所述生存认证区块链。

[0043] 比对所述智能合约中的所述人社服务节点的公钥和机构编码,以及所述人社服务节点上传的所述人社服务节点的公钥和机构编码,确认是否是所述人社服务节点发起的生

存认证。

[0044] 利用所述人社服务节点的私钥解密所述内容加密部分得到所述机构编码。其中，利用所述人社服务节点的私钥解密所述内容加密部分能够得到参保人员编号、业务办理时间、业务数据、业务类型和机构编码。

[0045] 根据所述机构编码查找对应的所述非人社服务节点的公钥。

[0046] 利用查找到的所述非人社服务节点的公钥加密所述机构编码和查找到的所述非人社服务节点的公钥得到确权数据。

[0047] 比对所述确权加密部分和所述确权数据确定所述内容加密部分是否来自对应的所述非人社服务节点。

[0048] 如果所述内容加密部分来自对应的所述非人社服务节点，对所述内容加密部分进行生存认证，否则生存认证失败。

[0049] 本发明的具体实施例中，对所述内容加密部分进行生存认证的步骤，具体包括：比对解密所述内容加密部分得到的参保人员编号与批量录入的参保人员编号，确认解密所述内容加密部分得到的所述业务数据为欲做生存认证的社保参保人员的交易数据；确认所述业务数据中是否包含有社保参保人员的死亡记录数据；如果包含有社保参保人员的死亡记录数据，直接认定所述参保人员编号对应的社保参保人员的生存状态为死亡；如果没有包含有社保参保人员的死亡记录数据，利用生存认证公式和解密所述内容加密部分得到的业务办理时间确定所述参保人员编号对应的社保参保人员的生存状态；如果确定所述参保人员编号对应的社保参保人员的生存状态为生存，则将该社保参保人员的生存状态上传至所述生存认证区块链；如果无法确定所述参保人员编号对应的社保参保人员的生存状态为生存，则向所述非人社服务节点推送无法确定该社保参保人员的生存状态的通知，要求该社保参保人员到所述参保人员前端节点做生物特征认证。其中，参保人员前端节点可以为人社服务节点的子节点。对于已经通过生存认证的社保参保人员，该社保参保人员的交易数据存储在生存认证区块链中专门的存储空间内，并对该社保参保人员的交易数据的位置进行记录(数组形式记录)，以便提高生存认证的速度。

[0050] 社保参保人员到所述参保人员前端节点做生物特征认证主要包括以下几种情况：

[0051] 参保人员前端节点设计注册功能，注册流程中嵌入实名认证功能，注册人输入的身份证号和姓名调取公安的相关接口，根据身份证姓名和身份证号码核对是否一致，实时联网核查；参保人员前端节点设计绑定社保卡功能，通过调取社保核心库接口保证实名认证的注册人员是参加了社会保险的参保人员，并确定了参保人员的参保类型；通过调第三方活体认证接口(国民或者face++等)，证明当前参保人员是活体；通过调取人社局社保卡发卡中心照片库中的照片和当前进行生存认证的参保人员照片进行比对，证明当前验证的参保人是本人。

[0052] 其中，所述生存认证公式Y_N具体为：

[0053] $$Y_N=\sum_{i=1}^{N}\frac{e^{CX_i}-e^{-CX_i}}{(e^{CX_i}+e^{-CX_i})CX_i}\cdot\omega_i$$

[0054] 其中，公式中i为进行生存认证使用的业务信息的序数；N为业务信息的总条目数；e为自然常数；X_i为生成第i条业务信息距离生存认证的时间；C为时间权重函数的参数，取值为20/M，以天作为时间段时，M取365，以月为时间段时，M取12，以年为时间段时，M取1；ω_i

为社保参保人员办理业务的权重，包括强生存权重、中生存权重和弱生存权重，例如，参保人员在两天之内在民政机构办理了婚姻登记，因为婚姻登记需要本人携带户口本到民政局现场办理，所以该业务信息标记为强生存权重；参保人员通过ATM机取款，因为取款时只需要输入密码，并不会核验取款人是否为持卡人本人，所以该业务信息标记为弱生存权重；$\frac{e^{CX_i}-e^{-CX_i}}{(e^{CX_i}+e^{-CX_i})CX_i}$为时间权重函数，时间权重函数如图4所示，假如时间段为月(M取12时)，并且参保人员所做的业务在规定时间段内，时间离现在越近，结果越大，距离现在时间越远，结果越小，当超过一年是，结果小于0.05，视为0。

[0055] 假设T为预设的时间遍历，为服务机构前端子节点选择的时间，当$X_N>T$或者遍历到区块链头节点，如果加和的结果Y_N还未超过D(D为认定该参保人员生存的阈值，根据实际情况由人社服务节点给出)，将停止结果的相加，向各非人社服务节点推送无法确定该社保参保人员生死，要求社保参保人员使用参保人员前端节点做生物特征认证的通知，当加和结果Y_N大于D，认定社保参保人员生存。

[0056] 本发明的具体实施方式提供一种存储介质，所述存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现基于区块链的多维数据生存认证方法的步骤：

[0057] S101：搭建生存认证区块链。

[0058] S102：采集并处理社保参保人员的业务信息。

[0059] S103：将处理后的业务信息上传到所述生存认证区块链进行生存认证。

[0060] 本发明的具体实施方式还提供一种计算机设备，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述处理器执行所述计算机程序时实现基于区块链的多维数据生存认证方法的步骤：

[0061] S101：搭建生存认证区块链。

[0062] S102：采集并处理社保参保人员的业务信息。

[0063] S103：将处理后的业务信息上传到所述生存认证区块链进行生存认证。

[0064] 图2为本发明具体实施方式提供的一种搭建的参保人员生存认证区块链，如图2所示，服务机构节点包括多个医疗服务节点、多个公安服务节点、多个银行服务节点、多个人社服务节点和多个民政服务节点。其中，医疗服务节点、公安服务节点、银行服务节点和民政服务节点为非人社服务节点。服务机构节点与服务器节点一一对应，服务器节点可以为服务机构节点的子节点。智能合约是生存认证区块链上所有节点达成的合约。每个人社服务节点具有服务机构前端子节点，所述服务机构前端子节点用于选择生存认证时间段并批量录入参保人员编号。非人社服务节点用于存放所述非人社服务节点的满足所述上链需求表的业务信息；参保人员前端节点用于社保参保人员生物特征认证；所述服务器节点用于共识和记账，提升系统安全，解决系统容错。

[0065] 人社服务节点建设人社服务机构生存认证上链需求表，人社服务节点根据生存认证的业务需求，制定人社服务机构生存认证上链需求表并公布给非人社服务节点。表中对可以上生存认证区块链的办理业务类型做明确规定：

[0066] 服务机构名称：该业务来源的服务机构。

[0067] 业务类型编号：服务机构英文大写字母缩写+编号(例如MA001)。

[0068] 业务详细名称：办业务的详细名称，用来给上链的数据详细内容做简要的归纳。

[0069] 制作该表是为了对需要上区块链的社保参保人员的多维业务信息的详细业务名称和内容进行规定，具体哪些业务对生存认证有价值由人社服务机构制定并公布(例如:社保参保人员去在xxx医院进行体检，该业务信息对生存认证有意义，在表中服务机构为医疗服务机构，服务类型编号为MA001，业务详细名称为在xxx医院进行体检)，各服务机构将参保人在机构办理的业务信息(服务机构采集到的业务信息)与表中的业务详细名称进行对比筛选出对生存认证有意义的业务信息，进行上链请求，摈弃了与生存认证无关的机构业务信息上链。

[0070] 下述表1为人社服务机构生存认证上链需求表的样表，如表1所示。

[0071] 表1

[0072]

ID	服务机构名称	业务类型编号	业务详细名称
1	医疗服务机构	MA001	在某医院进行体检
2		MA002	在某医院进行抽血化验
3	人社服务机构	HRA001	在人社中心信息窗口办理社保卡
4		HRA002	在人社中心经办窗口办理社保卡挂失

[0073] 图3为本发明具体实施方式提供的一种参保业务信息上链后的参保人员生存情况区块链，使用拜占庭容错(PBFT)共识机制进行共识，业务信息上社保参保人员生存认证区块链，生存认证区块链上的业务信息如图3所示，众所周知，区块链包括公有链、私有链和联盟链，生存认证区块链可以为联盟链的一种。

[0074] 本发明具体实施例提供一种基于区块链的多维数据生存认证方法、存储介质及设备，建立了医疗机构、公安、银行、经办机构、民政等相关部门信息数据共享机制，不需要社保参保人员跨部门确权，确保验证数据的真实、安全、可靠、可追溯，生存认证结果可靠性高;利用多维大数据进行交叉对比，不需要参保用户特意去进行生存认证，自动完成社保参保人员的生存认证，参保用户不会感知到生存认证的过程，解决异地社保参保人员生存认证困难的问题，认证过程简单、认证效率高，减轻经办机构的办事压力;解决了数据共享时可能出现的数据抵赖、数据篡改等问题。

[0075] 上述的本发明实施例可在各种硬件、软件编码或两者组合中进行实施。例如，本发明的实施例也可为在数据信号处理器(Digital Signal Processor,DSP)中执行上述方法的程序代码。本发明也可涉及计算机处理器、数字信号处理器、微处理器或现场可编程门阵列(Field Programmable Gate Array,FPGA)执行的多种功能。可根据本发明配置上述处理器执行特定任务，其通过执行定义了本发明揭示的特定方法的机器可读软件代码或固件代码来完成。可将软件代码或固件代码发展为不同的程序语言与不同的格式或形式。也可为不同的目标平台编译软件代码。然而，根据本发明执行任务的软件代码与其他类型配置代码的不同代码样式、类型与语言不脱离本发明的精神与范围。

[0076] 以上所述仅为本发明示意性的具体实施方式，在不脱离本发明的构思和原则的前

提下,任何本领域的技术人员所做出的等同变化与修改,均应属于本发明保护的范围。

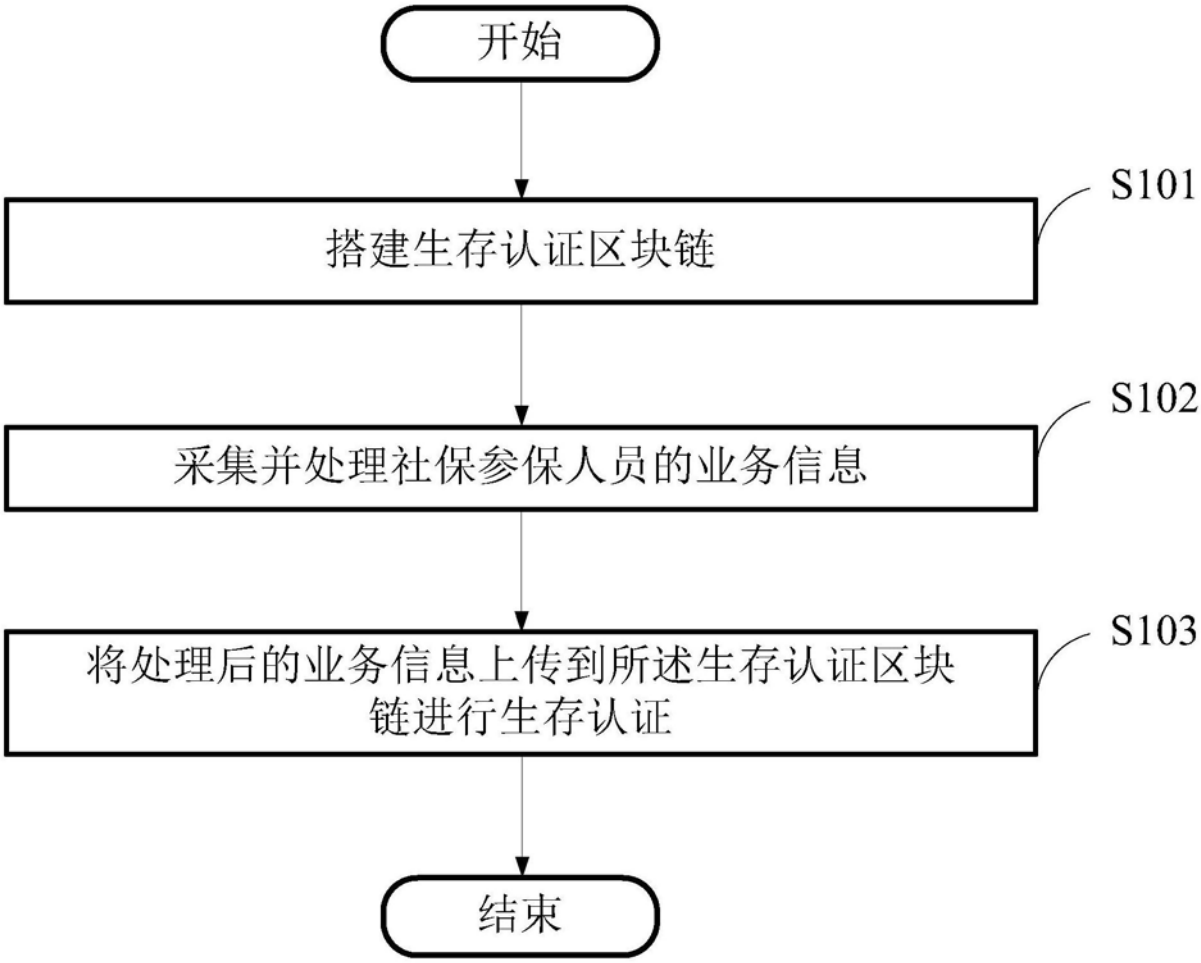

开始
S101
搭建生存认证区块链
S102
采集并处理社保参保人员的业务信息
S103
将处理后的业务信息上传到所述生存认证区块链进行生存认证
结束

图1

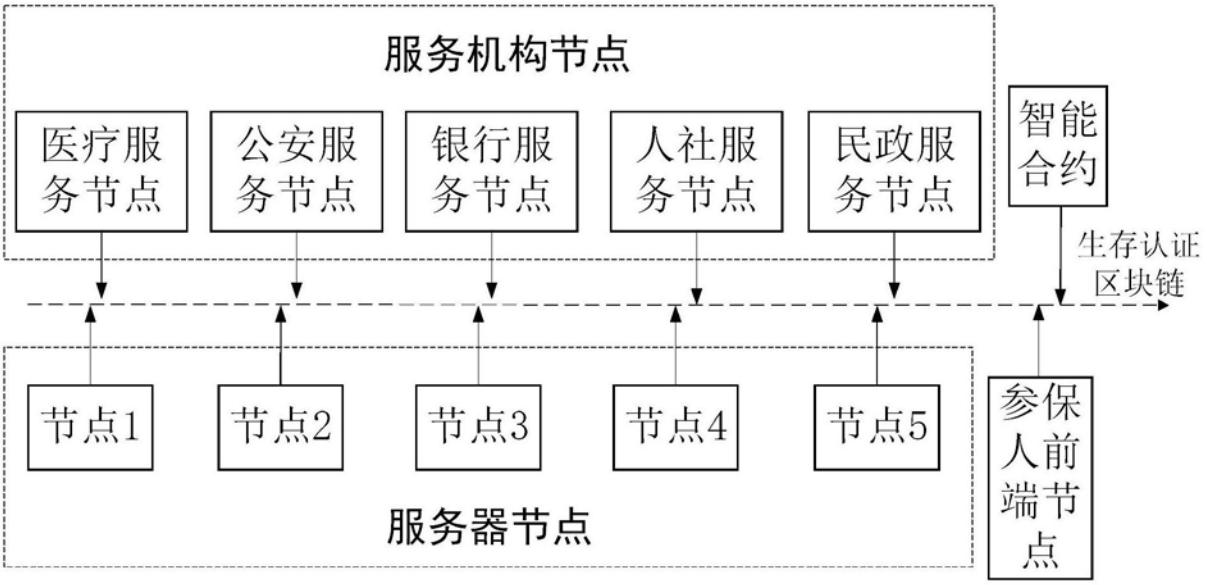

服务机构节点
医疗服务节点
公安服务节点
银行服务节点
人社服务节点
民政服务节点
智能合约
生存认证区块链
节点1
节点2
节点3
节点4
节点5
服务器节点
参保人前端节点

图2

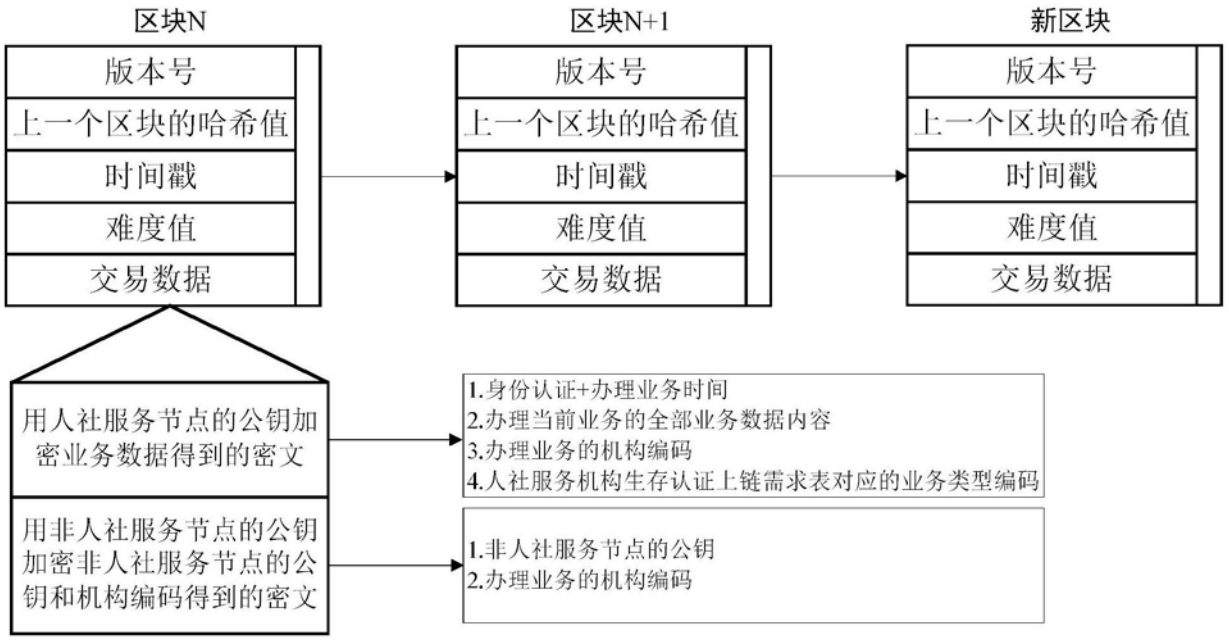

区块N
版本号
上一个区块的哈希值
时间戳
难度值
交易数据
区块N+1
版本号
上一个区块的哈希值
时间戳
难度值
交易数据
新区块
版本号
上一个区块的哈希值
时间戳
难度值
交易数据
用人社服务节点的公钥加密业务数据得到的密文
1.身份认证+办理业务时间
2.办理当前业务的全部业务数据内容
3.办理业务的机构编码
4.人社服务机构生存认证上链需求表对应的业务类型编码
用非人社服务节点的公钥加密非人社服务节点的公钥和机构编码得到的密文
1.非人社服务节点的公钥
2.办理业务的机构编码

图3

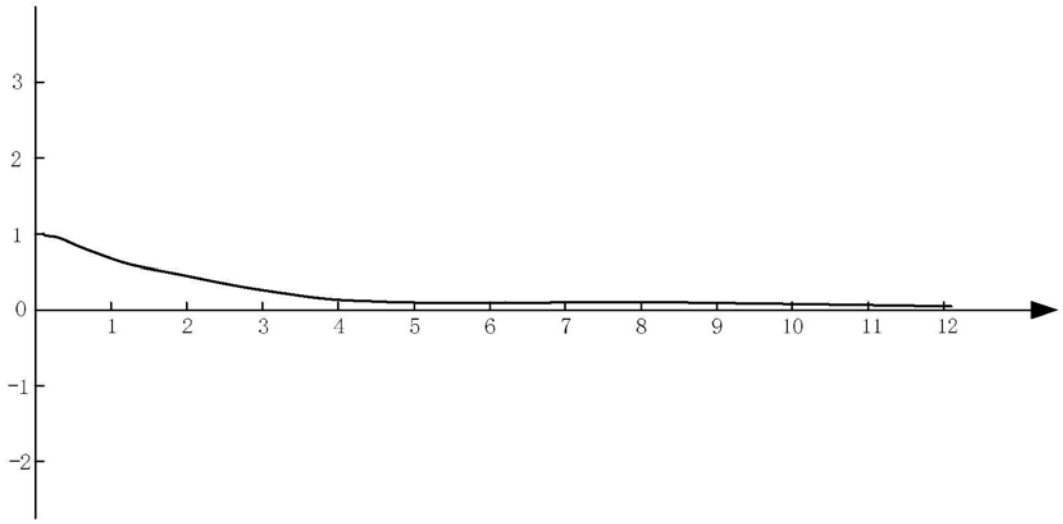

3
2
1
0
-1
-2
1
2
3
4
5
6
7
8
9
10
11
12

图4