(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112347188 B
(45)授权公告日 2024.07.30

(21)申请号 202011114782.3

(22)申请日 2020.10.16

(65)同一申请的已公布的文献号
申请公布号 CN 112347188 A

(43)申请公布日 2021.02.09

(73)专利权人 零氪科技(北京)有限公司
地址 100089 北京市海淀区海淀大街8号A座11层B区
专利权人 零氪信息技术(北京)有限公司

(72)发明人 于斌

(74)专利代理机构 北京知果之信知识产权代理有限公司 11541
专利代理师 卜荣丽

(51)Int.Cl.
G06F 16/27(2019.01)
G06F 21/32(2013.01)
G06F 21/60(2013.01)
G06F 21/62(2013.01)

(56)对比文件
CN 111274592 A,2020.06.12
CN 111552955 A,2020.08.18
CN 111651791 A,2020.09.11

审查员 刘雅敏

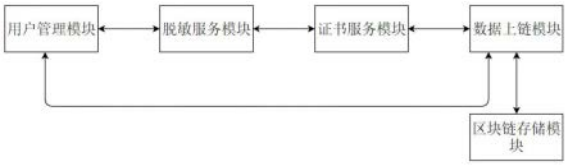
权利要求书3页 说明书6页 附图4页

(54)发明名称

一种基于私有链的授权及访问审计系统及方法

(57)摘要

本申请公开了一种基于私有链的授权及访问审计系统及方法。所述系统包括:用户管理模块、脱敏服务模块、证书服务模块、数据上链模块以及区块链存储模块;所述方法包括:用户授信过程以及授信验证过程。本申请通过区块链技术对于用户信息机进行存储,并且个人信息结合脱敏技术让用户隐私信息不直接参与用户认证数据过程,减少隐私泄露风险,同时引入IPFS存储相关记录及用户证书,私有链已索引方式对完成文件实体的指向,解决了传统授权认证模式下的数据可能被篡改及伪造的问题。



CN 112347188 B

1.一种基于私有链的授权及访问审计系统,其特征在于,包括:用户管理模块、脱敏服务模块、证书服务模块、数据上链模块以及区块链存储模块;

所述用户管理模块、脱敏服务模块、证书服务模块、数据上链模块以及区块链存储模块依次顺序连接,所述用户管理模块与所述数据上链模块相连接;

所述用户管理模块,用来接收新用户授权请求,获取新用户提交生物特征信息以及用户注册信息;

所述脱敏服务模块,用来接收新用户授权请求,根据预设定敏感字段,抽取所述生物特征信息以及用户注册信息中的敏感字段,并通过加密方式转换为密文;同时由脱敏服务模块为该用户随机生成唯一的用户ID,合并所述用户ID以及特征信息密文生成用户特征码;

所述证书服务模块,用来接收新用户授权请求及用户特征码后,签发用户证书,生成公钥以及对应私钥,通过证书对所述用户特征码二次加密,用于传输;将加密后数据及对应公钥提交到上链模块;

所述数据上链模块,用来将接收到新用户授权数据加密后及对应公钥保存到区块链内;

所述区块链存储模块,用来保存从数据上链模块中传递过来的数据;

所述数据上链模块返回上链成功信息到证书服务模块;

证书服务模块返回用户私钥及用户ID到脱敏服务模块;

脱敏服务模块通过证书服务模块返回的用户ID在本地系统中查询到相关特征码,并与证书服务模块返回的私钥在本模块内进行组装成为JSON格式的数据结构体;返回授权信息到所述用户管理模块;

用户管理模块收到用户私钥、用户ID保存到管理数据库,返回用户ID、私钥及用户特征码并进行USB-KEY烧录,用户管理模块提交用户ID及烧录情况、时间戳信息到数据上链模块;

数据上链模块将用户ID及烧录情况、时间戳保存至区块链模块;

所述用户管理模块还包括:用来接收用户登录信息,将用于认证的验证数据传递给所述数据上链模块,并且接收返回验证结果;所述用户登录信息包括:用户ID、密码以及本地USB-KEY数据;

所述数据上链模块还包括:接收用户所述用于认证的验证数据,根据区块链存储模块传递过来的加密数据信息进行对比,返回验证结果给所述用户管理模块,提交用户验证情况记录给所述区块链模块;

根据区块链存储模块传递过来的加密数据信息进行对比,包括:

判断用户ID及烧录写入设备ID是否正确,确认正确后对比用户特征码,返回验证结果到所述用户管理模块,提交用户验证情况记录给所述区块链模块;若用户ID、特征码、烧录写入设备ID任意一项不匹配则直接返回认证失败;

所述区块链存储模块,还包括:根据用户提交的验证数据获取加密数据信息,将获取到的加密数据信息发送到所述数据上链模块,接收所述上链模块提交的用户验证情况记录;

所述区块链存储模块存储方式为IPFS,用户证书及用户审计记录存入IPFS,并生成相关存储对象的hash值,私有链构建后区块链内每个区块保存相关存储对象的hash值,所述相关存储对象的hash值作为索引进行使用,在每个区块中的相关存储对象的hash值与IPFS

中每个节点值一一对应;

所述私有链构建过程如下:

针对区块链存储模块中的节点A~节点N创建区块,并进行初始化;

对每个节点进行配置;

启动节点A,将其他节点链接至节点A;

成功链接完成私有链构建。

2.如权利要求1所述的基于私有链的授权及访问审计系统,其特征在于,所述生物特征信息包括:指静脉、面部特征。

3.如权利要求1所述的基于私有链的授权及访问审计系统,其特征在于,所述用户注册信息包括:姓名、手机号、所属医院、所属病区、所属科室。

4.如权利要求1所述的基于私有链的授权及访问审计系统,其特征在于,所述初始化包括:部署ipfs执行文件、生成点对点密钥、创建数据目录、创建IPFS节点。

5.如权利要求1所述的基于私有链的授权及访问审计系统,其特征在于,所述配置包括:导入节点id、配置跨域资源共享。

6.一种基于私有链的授权及访问审计方法,其特征在于,采用如权利要求1-5任一项所述的基于私有链的授权及访问审计系统实现,包括:包括用户授信过程以及授信验证过程:

所述用户授信过程步骤如下:

用户管理模块收到新用户授权请求,获取新用户提交生物特征信息以及用户注册信息,并提交到脱敏服务模块;

脱敏服务模块接收新用户授权请求,根据预设定敏感字段,抽取所述生物特征信息以及用户注册信息中的敏感字段,并通过加密方式转换为密文;同时由脱敏服务模块为该用户随机生成唯一的用户ID,合并所述用户ID以及特征信息密文生成用户特征码;

证书服务模块接收新用户授权请求及用户特征码后,签发用户证书,生成公钥以及对应私钥,通过证书对所述用户特征码二次加密,用于传输;将加密后数据及对应公钥提交到上链模块;

所述数据上链模块,将接收到新用户授权数据加密后及对应公钥保存到区块链内;

数据上链模块返回上链成功信息到证书服务模块;

证书服务模块返回用户私钥及用户ID到脱敏服务模块;

脱敏服务模块通过证书服务模块返回的用户ID在本地系统中查询到相关特征码,并与证书服务模块返回的私钥在本模块内进行组装成为JSON格式的数据结构体;返回授权信息到所述用户管理模块;

用户管理模块收到用户私钥、用户ID保存到管理数据库,返回用户ID、私钥及用户特征码并进行USB-KEY烧录,用户管理模块提交用户ID及烧录情况、时间戳信息到数据上链模块;

数据上链模块将用户ID及烧录情况、时间戳保存至区块链模块。

7.如权利要求6所述的基于私有链的授权及访问审计方法,其特征在于,所述授信验证过程步骤如下:

用户管理模块接收用户登录信息,验证登录信息是否正确,若不正确则直接反馈登录验证失败,若验证通过,则获取用户提交的USB-KEY内相关内容,将用于认证的验证数据传

递给所述数据上链模块,并且接收返回验证结果;

所述用于认证的验证数据为私钥加密后数据;

数据上链模块接收用户所述用于认证的验证数据;

区块链存储模块根据用户提交的验证数据获取加密数据信息,将获取到的加密数据信息发送到所述数据上链模块;

数据上链模块根据区块链存储模块传递过来的加密数据信息进行对比,若对比结果正确,则返回验证结果到所述用户管理模块,提交用户验证情况记录给所述区块链模块;若对比结果不正确则直接返回认证失败;

区块链存储模块接收所述上链模块提交的用户验证情况记录。

一种基于私有链的授权及访问审计系统及方法

技术领域

[0001] 本申请涉及区块链技术领域,具体而言,涉及一种基于私有链的授权及访问审计系统及方法。

背景技术

[0002] 目前,随着医疗与大数据的结合逐渐紧密,对于系统及数据的访问变得更加重要。对于授权、访问、审计都提出了越来越高的要求。当前常见的医院内部信息系统的认证及授权方式通常为传统方式,即账号密码或基于生物技术的相关信息进行数字化后作为登录标记进行使用。而由于传统数据库的防篡改性具有一定缺陷,用户账号生成过程中的隐私问题及传统授权认证模式下的数据可能被篡改及伪造。

[0003] 针对相关技术中用户账号生成过程中的隐私问题及传统授权认证模式下的数据可能被篡改及伪造的问题,目前尚未提出有效的解决方案。

发明内容

[0004] 本申请的主要目的在于提供一种基于私有链的授权及访问审计系统及方法,以解决相关技术中用户账号生成过程中的隐私问题及传统授权认证模式下的数据可能被篡改及伪造的问题。

[0005] 为了实现上述目的,第一方面,本申请提供了一种基于私有链的授权及访问审计系统,包括:用户管理模块、脱敏服务模块、证书服务模块、数据上链模块以及区块链存储模块;

[0006] 所述用户管理模块、脱敏服务模块、证书服务模块、数据上链模块以及区块链存储模块依次顺序连接,所述用户管理模块与所述数据上链模块相连接;

[0007] 所述用户管理模块,用来接收新用户授权请求,获取新用户提交生物特征信息以及用户注册信息,并根据返回授权信息进行USB-KEY烧录;

[0008] 所述脱敏服务模块,用来接收新用户授权请求,根据预设定敏感字段,抽取所述生物特征信息以及用户注册信息中的敏感字段,并通过加密方式转换为密文。同时由脱敏服务模块为该用户随机生成唯一的用户ID,合并所述用户ID以及特征信息密文生成用户特征码;

[0009] 所述证书服务模块,用来接收新用户授权请求及用户特征码后,签发用户证书,生成公钥以及对应私钥,通过证书对所述用户特征码二次加密,用于传输;将加密后数据及对应公钥提交到上链模块;

[0010] 所述数据上链模块,用来将接收到新用户授权数据加密后及对应公钥保存到区块链内;

[0011] 所述用户管理模块还包括:用来接收用户登录信息,将用于认证的验证数据传递给所述数据上链模块,并且接收返回验证结果。

[0012] 区块链存储模块根据用户提交的验证数据获取加密数据信息,将获取到的加密数

据信息,发送到所述数据上链模块;

[0013] 所述加密数据信息包括:用户ID、特征码、烧录写入设备ID。

[0014] 数据上链模块根据区块链存储模块传递过来的加密数据信息进行对比,先判断用户ID及烧录写入设备ID是否正确,确认正确后对比用户特征码,返回验证结果到所述用户管理模块,提交用户验证情况记录给所述区块链模块。若用户ID、特征码、烧录写入设备ID任意一项不匹配则直接返回认证失败;

[0015] 所述区块链存储模块存储方式为IPFS(InterPlanetary File System,星际文件系统。一种点对点的分布式超媒体分发协议,可通过不同节点分布存储的方式对存储进行扩容,获取相关数据也由多节点获取),用户证书及用户审计记录存入IPFS,并生成相关存储对象的hash值,私有链构建后区块链内每个区块保存相关存储对象的hash值,所述相关存储对象的hash值作为索引进行使用,在每个区块中的相关存储对象的hash值与IPFS中每个节点值一一对应。

[0016] 所述私有链构建过程如下:

[0017] 针对区块链存储模块中的节点A～节点N创建区块,并进行初始化,包括:部署ipfs执行文件、生成点对点密钥、创建数据目录、创建IPFS节点;

[0018] 对每个节点进行配置,包括:导入节点id、配置跨域资源共享;

[0019] 启动节点A,将其他节点链接至节点A;

[0020] 所述初始化包括:部署ipfs执行文件、生成点对点密钥、创建数据目录、创建IPFS节点。

[0021] 所述配置包括:导入节点id、配置跨域资源共享。

[0022] 第二方面,本申请还提供了一种基于私有链的授权及访问审计方法,采用所述的基于私有链的授权及访问审计系统实现,包括用户授信过程以及授信验证过程:

[0023] 所述用户授信过程步骤如下:

[0024] 用户管理模块收到新用户授权请求,获取新用户提交生物特征信息以及用户注册信息,并提交到脱敏服务模块;

[0025] 所述脱敏服务模块,接收新用户授权请求,根据预设定敏感字段,抽取所述生物特征信息以及用户注册信息中的敏感字段,并通过加密方式转换为密文。同时由脱敏服务模块为该用户随机生成唯一的用户ID,合并所述用户ID以及特征信息密文生成用户特征码;

[0026] 所述证书服务模块,接收新用户授权请求及用户特征码后,签发用户证书,生成公钥以及对应私钥,通过证书对所述用户特征码二次加密用于传输;将加密后数据及对应公钥提交到上链模块;

[0027] 所述数据上链模块,将接收到新用户授权数据加密后及对应公钥保存到区块链内;

[0028] 数据上链模块返回上链成功信息到证书服务模块;

[0029] 证书服务模块返回用户私钥及用户ID到脱敏服务模块;

[0030] 脱敏服务模块通过证书服务模块返回的用户ID在本地系统中查询到相关特征码,并与证书服务模块返回的私钥在本模块内进行组装成为JSON格式的数据结构体;返回授权信息到所述用户管理模块;

[0031] 用户管理模块收到用户私钥、用户ID保存到管理数据库,返回用户ID、私钥及用户

特征码并进行USB-KEY烧录,用户管理模块提交用户ID及烧录情况、时间戳信息到数据上链模块;所述烧录情况包含烧录是否成功、烧录写入设备ID、烧录设备ID;

[0032] 数据上链模块将用户ID及烧录情况、时间戳保存至区块链模块。所述时间戳包括烧录时间戳、上传时间戳。

[0033] 所述授信验证过程步骤如下:

[0034] 用户管理模块接收用户登录信息,验证登录信息是否正确,若验证通过,则获取用户提交的USB-KEY内相关内容,将用于认证的验证数据传递给所述数据上链模块,并且接收返回验证结果。

[0035] 所述用户登录信息包括:用户ID、密码以及本地USB-KEY数据;

[0036] 所述用于认证的验证数据为私钥加密后数据;

[0037] 所述USB-KEY内相关内容包括用户ID、用户私钥;

[0038] 数据上链模块接收用户所述用于认证的验证数据;

[0039] 区块链存储模块根据用户提交的验证数据获取加密数据信息,将获取到的加密数据信息发送到所述数据上链模块;所述加密数据信息包括用户ID、特征码、烧录写入设备ID。

[0040] 数据上链模块根据区块链存储模块传递过来的加密数据信息进行对比,,若对比结果正确,则返回验证结果到所述用户管理模块,提交用户验证情况记录给所述区块链模块;若对比结果不正确则直接返回认证失败;

[0041] 区块链存储模块接收所述上链模块提交的用户验证情况记录。

[0042] 有益技术效果:

[0043] 本申请通过区块链技术对于用户信息机进行存储,并且个人信息结合脱敏技术让用户隐私信息不直接参与用户认证数据过程,减少隐私泄露风险,同时引入IPFS存储相关记录及用户证书,私有链已索引方式对完成文件实体的指向。

[0044] 用户信息通过脱敏方式提取特征码,并将特征码及用户id进行关联,关联后使用证书加密方式对用户信息进行加密,加密后的hash存入私有链。

[0045] 用户敏感信息通过脱敏服务进行脱敏,只保留特征码,不会使用任何用户信息实体,例:指静脉、指纹、面部特征等。

[0046] 用户证书及用户审计记录存入IPFS,并生成相关hash,私有链内保存hash索引,实现用户访问数据的不可篡改的审计需求。

附图说明

[0047] 构成本申请的一部分的附图用来提供对本申请的进一步理解,使得本申请的其它特征、目的和优点变得更明显。本申请的示意性实施例附图及其说明用于解释本申请,并不构成对本申请的不当限定。在附图中:

[0048] 图1是根据本申请实施例提供的一种基于私有链的授权及访问审计系统原理框图;

[0049] 图2是根据本申请实施例提供的区块链存储模块存储方式示意图;

[0050] 图3是根据本申请实施例提供的私有链构建过程示意图;

[0051] 图4是根据本申请实施例提供的用户授信过程时序图;

[0052] 图5是根据本申请实施例提供的授信验证过程时序图。

具体实施方式

[0053] 为了使本技术领域的人员更好地理解本申请方案,下面将结合本申请实施例中的附图,对本申请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本申请一部分的实施例,而不是全部的实施例。基于本申请中的实施例,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,都应当属于本申请保护的范围。

[0054] 需要说明的是,本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象,而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换,以便这里描述的本申请的实施例。此外,术语“包括”和“具有”以及他们的任何变形,意图在于覆盖不排他的包含,例如,包含了一系列步骤或单元的过程、方法、系统、产品或设备不必限于清楚地列出的那些步骤或单元,而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0055] 在本申请中,术语“上”、“下”、“左”、“右”、“前”、“后”、“顶”、“底”、“内”、“外”、“中”、“竖直”、“水平”、“横向”、“纵向”等指示的方位或位置关系为基于附图所示的方位或位置关系。这些术语主要是为了更好地描述本申请及其实施例,并非用于限定所指示的装置、元件或组成部分必须具有特定方位,或以特定方位进行构造和操作。

[0056] 并且,上述部分术语除了可以用于表示方位或位置关系以外,还可能用于表示其他含义,例如术语“上”在某些情况下也可能用于表示某种依附关系或连接关系。对于本领域普通技术人员而言,可以根据具体情况理解这些术语在本申请中的具体含义。

[0057] 另外,术语“多个”的含义应为两个以及两个以上。

[0058] 需要说明的是,在不冲突的情况下,本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

[0059] 第一方面,本申请提供了一种基于私有链的授权及访问审计系统,如图1所示,包括:用户管理模块、脱敏服务模块、证书服务模块、数据上链模块以及区块链存储模块;

[0060] 所述用户管理模块、脱敏服务模块、证书服务模块、数据上链模块以及区块链存储模块依次顺序连接,所述用户管理模块与所述数据上链模块相连接;

[0061] 所述用户管理模块,用来接收新用户授权请求,获取新用户提交生物特征信息以及用户注册信息,并根据返回授权信息进行USB-KEY烧录;

[0062] 所述脱敏服务模块,接收新用户授权请求,根据预设定敏感字段,抽取所述生物特征信息以及用户注册信息中的敏感字段,并通过加密方式转换为密文。同时由脱敏服务模块为该用户随机生成唯一的用户ID,合并所述用户ID以及特征信息密文生成用户特征码;

[0063] 所述证书服务模块,接收新用户授权请求及用户特征码后,签发用户证书,生成公钥以及对应私钥,通过证书对所述用户特征码二次加密用于传输;将加密后数据及对应公钥提交到上链模块;

[0064] 所述数据上链模块,将接收到新用户授权数据加密后及对应公钥保存到区块链内;

[0065] 所述用户管理模块还包括:用来接收用户登录信息,将用于认证的验证数据传递

给所述数据上链模块,并且接收返回验证结果。

[0066] 区块链存储模块根据用户提交的验证数据获取加密数据信息,将获取到的加密数据信息发送到所述数据上链模块;所述加密数据信息包括:用户ID、特征码、烧录写入设备ID。

[0067] 数据上链模块根据区块链存储模块传递过来的加密数据信息进行对比,先判断用户ID及烧录写入设备ID是否正确,确认正确后对比用户特征码,返回验证结果到所述用户管理模块,提交用户验证情况记录给所述区块链模块。若用户ID、特征码、烧录写入设备ID任意一项不匹配则直接返回认证失败;

[0068] 所述区块链存储模块存储方式为IPFS(InterPlanetary File System,星际文件系统。一种点对点的分布式超媒体分发协议,可通过不同节点分布存储的方式对存储进行扩容,获取相关数据也由多节点获取),用户证书及用户审计记录存入IPFS,并生成相关存储对象的hash值,私有链构建后区块链内每个区块保存相关存储对象的hash值,所述相关存储对象的hash值作为索引进行使用,在每个区块中的相关存储对象的hash值与IPFS中每个节点值一一对应。

[0069] 所述私有链构建过程如下,如图3所示:

[0070] 针对区块链存储模块中的节点A～节点N创建区块,并进行初始化,所述初始化包括:部署ipfs执行文件、生成点对点密钥、创建数据目录、创建IPFS节点;

[0071] 对每个节点进行配置,所述配置包括:导入节点id、配置跨域资源共享;

[0072] 启动节点A,将其他节点链接至节点A;

[0073] 第二方面,本申请还提供了一种基于私有链的授权及访问审计方法,采用所述的基于私有链的授权及访问审计系统实现,包括用户授信过程以及授信验证过程:

[0074] 所述用户授信过程步骤如下,如图4所示:

[0075] 步骤S11:用户管理模块收到新用户授权请求,获取新用户提交生物特征信息以及用户注册信息,并提交到脱敏服务模块;

[0076] 步骤S12:所述脱敏服务模块,接收新用户授权请求,根据预设定敏感字段,抽取所述生物特征信息以及用户注册信息中的敏感字段,并通过加密方式转换为密文。同时由脱敏服务模块为该用户随机生成唯一的用户ID,合并所述用户ID以及特征信息密文生成用户特征码;

[0077] 步骤S13:所述证书服务模块,接收新用户授权请求及用户特征码后,签发用户证书,生成公钥以及对应私钥,通过证书对所述用户特征码二次加密用于传输;将加密后数据及对应公钥提交到上链模块;

[0078] 步骤S14:所述数据上链模块,将接收到新用户授权数据加密后及对应公钥保存到区块链内;

[0079] 步骤S15:数据上链模块返回上链成功信息到证书服务模块;

[0080] 步骤S16:证书服务模块返回用户私钥及用户ID到脱敏服务模块;

[0081] 步骤S17:脱敏服务模块通过证书服务模块返回的用户ID在本地系统中查询到相关特征码,并与证书服务模块返回的私钥在本模块内进行组装成为JSON格式的数据结构体;返回授权信息到所述用户管理模块;

[0082] 步骤S18:用户管理模块收到用户私钥、用户ID保存到管理数据库,返回用户ID、私

钥及用户特征码并进行USB-KEY烧录,用户管理模块提交用户ID及烧录情况、时间戳信息到数据上链模块;所述烧录情况包括烧录是否成功、烧录写入设备ID、烧录设备ID。

[0083] 步骤S19:数据上链模块将用户ID及烧录情况、时间戳保存至区块链模块。所述时间戳包括烧录时间戳、上传时间戳。

[0084] 所述授信验证过程步骤如下,如图5所示:

[0085] 步骤S21:用户管理模块接收用户登录信息,验证登录信息是否正确,若不正确则直接反馈登录验证失败,若验证通过,则获取用户提交的USB-KEY内相关内容,将用于认证的验证数据传递给所述数据上链模块,并且接收返回验证结果。

[0086] 所述用户登录信息包括:用户ID、密码以及本地USB-KEY数据;

[0087] 所述用于认证的验证数据为私钥加密后数据;

[0088] 所述USB-KEY内相关内容包括:用户ID、用户私钥;

[0089] 步骤S22:数据上链模块接收用户所述用于认证的验证数据;

[0090] 步骤S23:区块链存储模块根据用户提交的验证数据获取加密数据信息,将获取到的加密数据信息发送到所述数据上链模块;所述加密数据信息包括用户ID、特征码、烧录写入设备ID。

[0091] 步骤S24:数据上链模块根据区块链存储模块传递过来的加密数据信息进行对比,先判断用户ID及烧录写入设备ID是否正确,确认正确后对比用户特征码,返回验证结果到所述用户管理模块,提交用户验证情况记录给所述区块链模块。若用户ID、特征码、烧录写入设备ID任意一项不匹配则直接返回认证失败;

[0092] 步骤S25:区块链存储模块接收所述上链模块提交的用户验证情况记录。

[0093] 以上所述仅为本申请的优选实施例而已,并不用于限制本申请,对于本领域的技术人员来说,本申请可以有各种更改和变化。凡在本申请的精神和原则之内,所作的任何修改、等同替换、改进等,均应包含在本申请的保护范围之内。

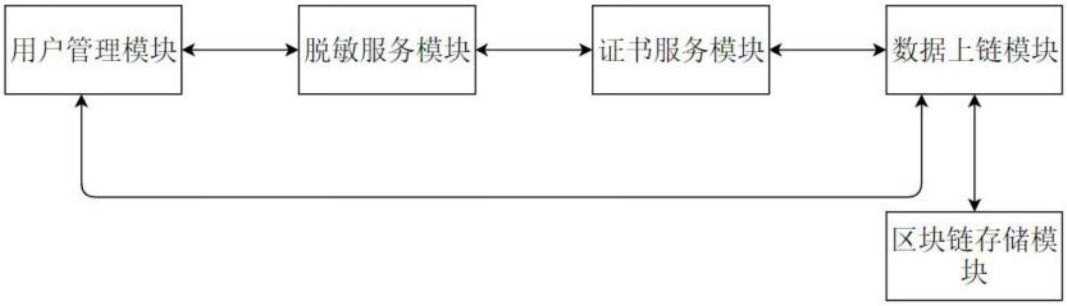

用户管理模块
脱敏服务模块
证书服务模块
数据上链模块
区块链存储模块

图1

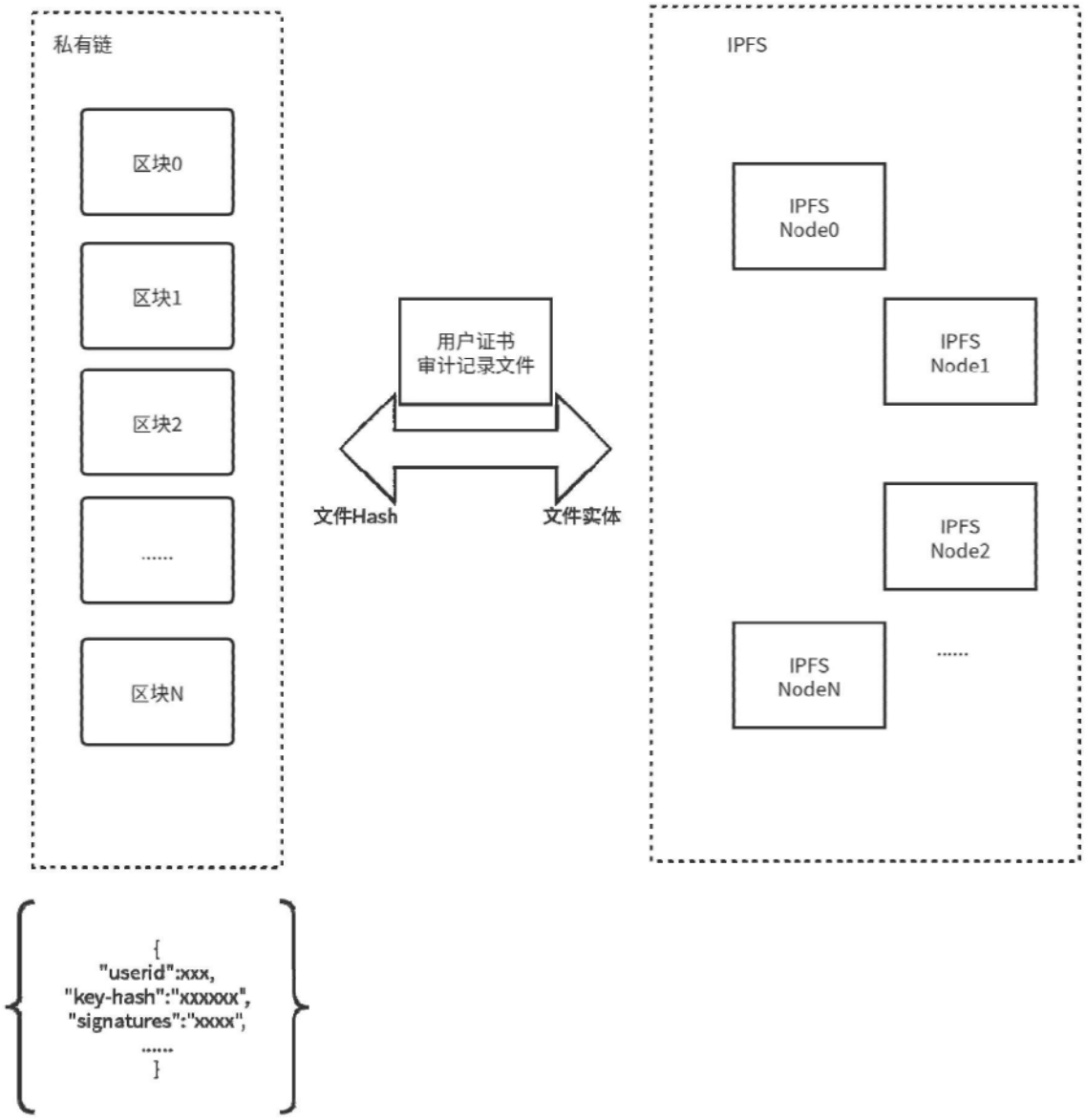

私有链
区块0
区块1
区块2
.....
区块N
用户证书
审计记录文件
文件Hash
文件实体
IPFS
IPFS Node0
IPFS Node1
IPFS Node2
IPFS NodeN
.....
{
"userid":xxx,
"key-hash":"xxxxxx",
"signatures":"xxxx",
.....
}

图2

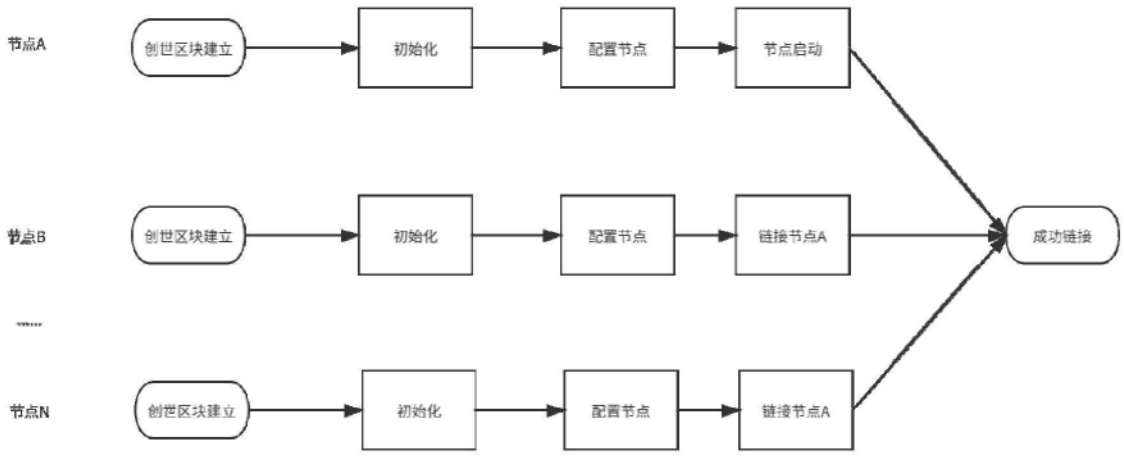

节点A
创世区块建立
初始化
配置节点
节点启动
节点B
创世区块建立
初始化
配置节点
链接节点A
成功链接
.....
节点N
创世区块建立
初始化
配置节点
链接节点A

图3

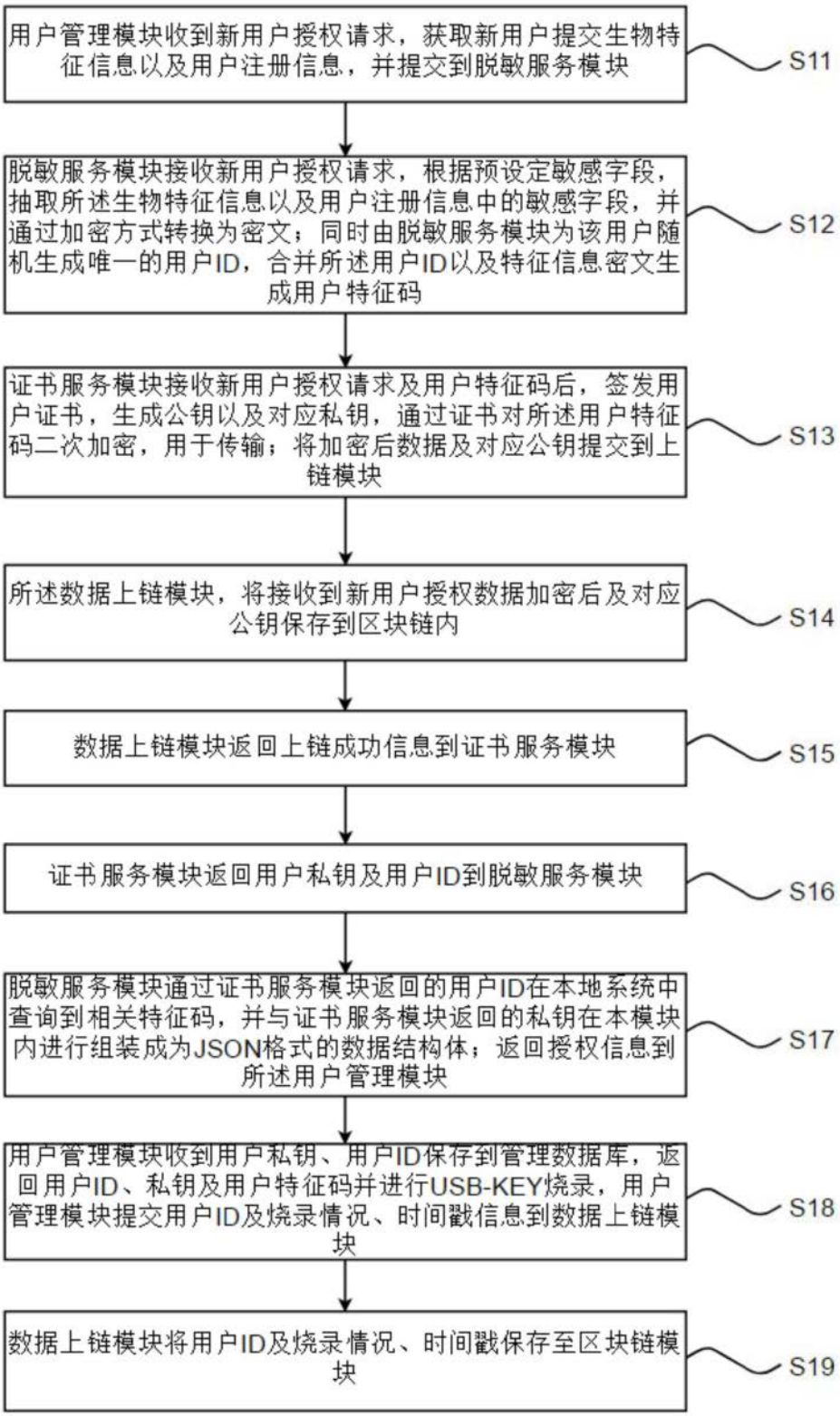

用户管理模块收到新用户授权请求，获取新用户提交生物特征信息以及用户注册信息，并提交到脱敏服务模块
S11
脱敏服务模块接收新用户授权请求，根据预设定敏感字段，抽取所述生物特征信息以及用户注册信息中的敏感字段，并通过加密方式转换为密文；同时由脱敏服务模块为该用户随机生成唯一的用户ID，合并所述用户ID以及特征信息密文生成用户特征码
S12
证书服务模块接收新用户授权请求及用户特征码后，签发用户证书，生成公钥以及对应私钥，通过证书对所述用户特征码二次加密，用于传输；将加密后数据及对应公钥提交到上链模块
S13
所述数据上链模块，将接收到新用户授权数据加密后及对应公钥保存到区块链内
S14
数据上链模块返回上链成功信息到证书服务模块
S15
证书服务模块返回用户私钥及用户ID到脱敏服务模块
S16
脱敏服务模块通过证书服务模块返回的用户ID在本地系统中查询到相关特征码，并与证书服务模块返回的私钥在本模块内进行组装成为JSON格式的数据结构体；返回授权信息到所述用户管理模块
S17
用户管理模块收到用户私钥、用户ID保存到管理数据库，返回用户ID、私钥及用户特征码并进行USB-KEY烧录，用户管理模块提交用户ID及烧录情况、时间戳信息到数据上链模块
S18
数据上链模块将用户ID及烧录情况、时间戳保存至区块链模块
S19

图4

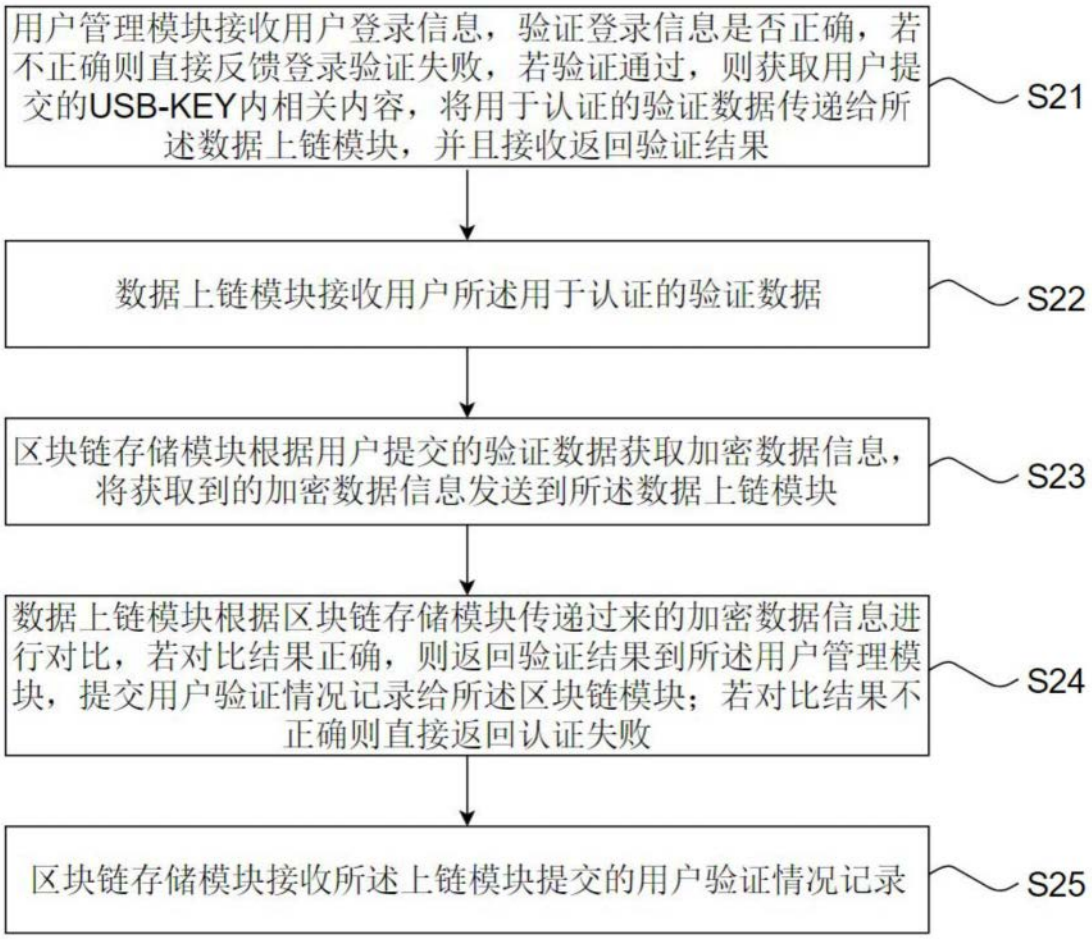

用户管理模块接收用户登录信息，验证登录信息是否正确，若不正确则直接反馈登录验证失败，若验证通过，则获取用户提交的USB-KEY内相关内容，将用于认证的验证数据传递给所述数据上链模块，并且接收返回验证结果
S21
数据上链模块接收用户所述用于认证的验证数据
S22
区块链存储模块根据用户提交的验证数据获取加密数据信息，将获取到的加密数据信息发送到所述数据上链模块
S23
数据上链模块根据区块链存储模块传递过来的加密数据信息进行对比，若对比结果正确，则返回验证结果到所述用户管理模块，提交用户验证情况记录给所述区块链模块；若对比结果不正确则直接返回认证失败
S24
区块链存储模块接收所述上链模块提交的用户验证情况记录
S25

图5