(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 109934005 A
(43)申请公布日 2019.06.25

(21)申请号 201910195879.2

(22)申请日 2019.03.15

(71)申请人 北京物资学院
地址 101149 北京市通州区富河大街321号北京物资学院信息学院

(72)发明人 丁毅 孙伽宁 华芳 林惠 曹婷婷 李洁

(74)专利代理机构 北京华仲龙腾专利代理事务所(普通合伙) 11548
代理人 李静

(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/62(2013.01)
G06F 21/64(2013.01)
G06Q 50/20(2012.01)

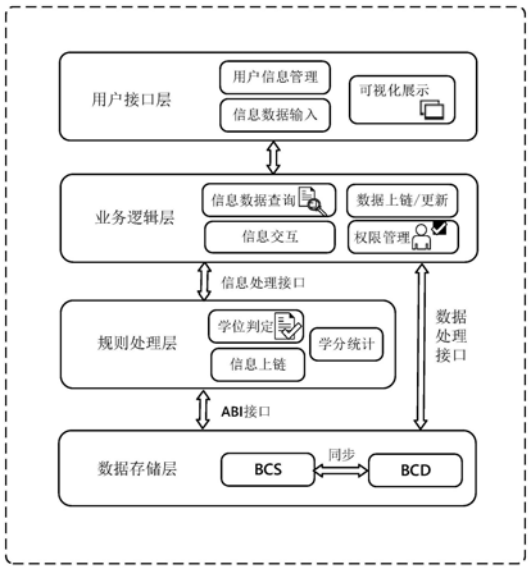
权利要求书3页 说明书7页 附图3页

(54)发明名称

一种基于区块链的学位认证系统及认证方法

(57)摘要

本发明提供了一种基于区块链的学位认证系统,包括:数据存储层,用于数据的存储;规则处理层,实现区块链智能合约相关操作,包括学位判定模块、学分统计模块以及信息上链模块;业务逻辑层,通过业务规则接收、处理、分发用户上传的数据,保证系统正常运行,包括信息数据查询模块、信息交互模块、数据上链/更新模块以及权限管理模块;用户接口层,位于系统的最上层,为用户提供信息的录入、查询、展示,包括用户信息管理模块、信息数据录入模块和可视化展示模块。还提供了相应的学位认证方法,不使用中心数据库和第三方机构背书,不过分依赖第三方机构,克服由于高校内部学位认证人工处理或简单信息化方法缺乏有效保障机制带来的问题。



CN 109934005 A

1.一种基于区块链的学位认证系统,其特征在于包括:

数据存储层,用于数据的存储;

规则处理层,用于实现区块链智能合约相关操作,所述规则处理层包括学位判定模块、学分统计模块以及信息上链模块;

业务逻辑层,通过业务规则接收、处理、分发用户上传的数据,保证系统正常运行,所述业务逻辑层包括信息数据查询模块、信息交互模块、数据上链/更新模块以及权限管理模块;

用户接口层,位于所述基于区块链的学位认证系统的最上层,用于为用户提供信息的录入、查询、展示,所述用户接口层包括用户信息管理模块、信息数据录入模块和可视化展示模块。

2.根据权利要求1所述的一种基于区块链的学位认证系统,其特征在于:所述数据存储层采用两种数据存储方式并行的机制进行数据存储,所述两种数据存储方式分别是:区块链系统以及区块链数据库,所述区块链系统采用符合区块链基本特征的链式结构,利用分布式节点的共识算法来生成和更新数据,利用密码学加密的方式来保证数据传输和访问的安全,利用由自动化脚本代码组成的智能合约来执行业务逻辑并操作数据,所述区块链数据库是采用分布式数据库和区块链技术的结合体,所述数据存储层将数据分别存储在区块链系统和区块链数据库内,对于数据量较大、不参与学位认证的非核心数据,通过专用接口上传到区块链数据库中,即直接通过相关驱动存储于区块链数据库中;对于学位认证中所需的核心数据,通过规则处理层中的信息上链模块,上传到区块链系统中,所述区块链系统和区块链数据库上的数据通过同步接口随时进行信息交互,确保数据同步运行,达到一致性要求,各部分存储数据不会产生矛盾或冲突;当查询相关数据时使用基于相关驱动的接口进行查询,所述业务逻辑层通过封装好消息格式的远程调用服务发送请求实现与智能合约的交互。

3.根据权利要求1所述的一种基于区块链的学位认证系统,其特征在于:所述学位判定模块根据各学校、专业的特点,以及国家对学位授予的相关法律法规,定制不同的学位认证条件,并记载在图灵完备的学位授予条例规则中,将学位认证结果进行有限共享,被授权的用人单位、高校、监管机构能够进行学生学业及学位信息的全部或部分查询,所述学生学业及学位信息从链上获取,保证数据安全有效,所述认证条件使用智能合约机制实现,在区块链系统上执行,所述智能合约机制遵守区块链基本规则,即所述智能合约一旦部署成功,将无法进行更改;所述学分统计模块根据高校不同专业的培养方案,制定相应的学分修习制度,包括公共基础课、必修课、选修课不同类别课程的统计规则,需要分门别类的进行计算,并提供统计结果的调用方法,方便所述学位判定模块进行调用;所述信息上链模块用于将各功能模块处理结果上传到所述区块链系统,同时保证链上只存储核心信息。

4.根据权利要求1所述的一种基于区块链的学位认证系统,其特征在于:所述信息数据查询模块处理用人单位、高校对学生成绩信息、学位授予情况的查询请求,调用信息交互模块存取数据,并返回用户接口层;所述信息交互模块用于处理数据请求,首先将请求进行分类,根据数据种类不同,通过数据上链/更新模块分别调取区块链系统和区块链数据库的数据,加工成所需信息后发给信息数据查询模块进行下一步处理;所述数据上链/更新模块根据收到的指令调用数据处理接口或应用程序接口,与所述规则处理层和所述数据存储层进

行信息交互，并将底层返回的数据进行打包，发回其他模块；所述权限管理模块用于管理高校管理者、教师、学生、用人单位、第三方监管机构各角色的权限，并整合数据安全机制，保证数据使用、存储过程安全可控。

5.根据权利要求1所述的一种基于区块链的学位认证系统，其特征在于：所述用户信息管理模块提供用户信息的采集、修改、添加、删除操作，并协助其他各层完成新加入节点用户的授权；所述信息数据录入模块提供高校管理者导入学生个人信息、课程信息、培养方案以及考核成绩重要信息数据的录入功能；所述可视化展示模块根据系统中存在的大量数据，进行数据整合和统计，最终以统计图或表的形式进行展示，供用人单位、高校管理人员、学生以及第三方监管机构查询和参考。

6.根据权利要求1所述的一种基于区块链的学位认证系统，其特征在于：所述区块链系统采用特定共识机制和区块链运行环境的结合，所述特定共识机制包括共识引擎和通用的应用接口，采用加入拜占庭容错机制的PoS(Proof of Stake，权益证明)算法；所述区块链运行环境提供使用虚拟机的环境，执行特定语言编写的智能合约。

7.根据权利要求1所述的一种基于区块链的学位认证系统，其特征在于：所述基于区块链的学位认证系统对完成注册并授权的高校将分配唯一ID，所述ID包括一对表示账户地址的公钥和用于签名的私钥，高校在上传学生信息、成绩、培养方案、学位证书编码数据至区块链数据库和区块链系统中时，使用自己的私钥对数据进行签名并发起交易，当满足共识机制所要求的节点个数对该消息进行确认后，数据才能上传成功。

8.一种使用权利要求1-7任一所述的学位认证系统进行的基于区块链的学位认证方法，其特征在于包括以下步骤：

步骤1：各高校完成注册，被联盟区块链系统通过共识授权，加入基于联盟区块链的学位认证系统并获取一对公钥和私钥；

步骤2：学生开学报道，高校管理员负责将学生信息导入系统；

步骤3：高校在系统内公示学生培养方案和学分修习规则；

步骤4：培养方案公示结束后，高校将该培养方案写入智能合约，部署至区块链，智能合约生效；

步骤5：学生根据培养方案参加课程的学习和考试，获得考核成绩；

步骤6：高校负责人将学生成绩导入系统，学生可以登录系统进行查询，如有异议，需在管理员或系统指定和/或调整的时间内提交修改成绩的申请，公示期满，系统自动将成绩上传至区块链数据库中进行保存；

步骤7：智能合约根据上传的数据，自动执行判定规则判定学生是否通过该阶段学习，可以进入下一阶段的学习；

步骤8：学生完成所有阶段的学习后，智能合约自动判定学生是否取得学位证书，并对取得的学位证书通过调用一种针对非同质通证的标准接口生成该证书独一无二的证明编号，所述编号和最终授予的纸质证书编号进行绑定。

9.根据权利要求8所述的认证方法，其特征在于：所述步骤8中所述非同质通证的接口使用可基于相关标准提供，从而定义不同学生的学位证书，在区块链系统上存储，保证学位证书的唯一性、不可篡改性，每个所述非同质通证具有唯一的通证编号，和学校颁发的有效学位证书编号进行绑定，当高校确认学生完成所有阶段的学习后，智能合约自动判定学生

是否取得学位，并对取得的学位证书通过调用所述非同质通证的标准接口生成所述学位证书独一无二的证明编号；授权的用人单位或学校使用证书编号或者非同质通证编号查询学生的学位授予信息以及在读期间的所有成绩信息。

10.根据权利要求8所述的认证方法，其特征在于所述方法还包括：

步骤9：学生求职时将学位证书交与用人单位，用人单位将证书编号输入系统即可查询该学位证书真伪以及证书获取过程中所产生的关键数据，完成学位信息溯源，包括四六级成绩、过程性考核结果以及专业课考试成绩，学生可以通过系统查看自到校报道开始至获取资质的所有相关的重要数据，所有数据传输和存储过程中使用加密算法。

一种基于区块链的学位认证系统及认证方法

技术领域

[0001] 本发明涉及计算机技术领域，特别涉及一种基于区块链的学位认证系统及认证方法。

背景技术

[0002] 学位证书是为了证明学生专业知识以及技术水平，并由相关部门授予的证书，学生获得学位意味着其受教育程度和学术水平达到规定的要求。学位是目前社会衡量个人能力的重要标准之一，对于个人的求职与继续深造都会产生重要的影响。

[0003] 区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块链具有去中介化、开放性、自治性、信息很难篡改等特点。一旦信息经过验证并添加至区块链，就会永久的存储起来，单个节点对数据的修改无效。从区块链2.0时代开始，智能合约的价值被真正发挥出来。智能合约是一种旨在以信息化方式传播、验证或执行合同的计算机协议。智能合约允许在没有第三方的情况下进行可信交易，这些交易可追踪且不可逆转。

[0004] 利用区块链和智能合约理论探索学位认证规则，可有效追踪学位授予流程。由于获得学位过程的数据真实不可篡改、规则执行过程安全可靠、规则执行结果可信，有效减少社会上伪造学位的现象，督促学校提高教学效果，加强学位质量，促使优良学风的发展。然而，如何利用区块链技术解决实际问题，目前现有技术还没有提出一套实际有效的学位认证系统及认证方法。

发明内容

[0005] 为了解决这些问题，本发明提供了一种基于区块链的学位认证系统及认证方法。传统认证系统及认证方法使用中心数据库和第三方机构背书，过分依赖第三方机构来完成真伪查询。而高校内部学位认证，通常使用人工处理或者简单的信息化方法，缺乏有效的保障机制。本发明使用区块链上的智能合约将学位授予规则代码化，放置于区块链之上，基本去除了人为干涉的可能性。

[0006] 本发明的目的在于提供一种基于区块链的学位认证系统，包括：

[0007] 数据存储层，用于数据的存储；

[0008] 规则处理层，用于实现区块链智能合约相关操作，所述规则处理层包括学位判定模块、学分统计模块以及信息上链模块；

[0009] 业务逻辑层，通过业务规则接收、处理、分发用户上传的数据，保证系统正常运行，所述业务逻辑层包括信息数据查询模块、信息交互模块、数据上链/ 更新模块以及权限管理模块；

[0010] 用户接口层，位于所述基于区块链的学位认证系统的最上层，用于为用户提供信息的录入、查询、展示，所述用户接口层包括用户信息管理模块、信息数据录入模块和可视化展示模块。

[0011] 优选的，所述数据存储层采用两种数据存储方式并行的机制进行数据存储，所述两种数据存储方式分别是：区块链系统以及区块链数据库，所述区块链系统采用符合区块链基本特征的链式结构，利用分布式节点的共识算法来生成和更新数据，利用密码学加密的方式来保证数据传输和访问的安全，利用由自动化脚本代码组成的智能合约来执行业务逻辑并操作数据，所述区块链数据库是采用分布式数据库和区块链技术的结合体，所述数据存储层将数据分别存储在区块链系统和区块链数据库内，对于数据量较大、不参与学位认证的非核心数据，通过专用接口上传到区块链数据库中，即直接通过相关驱动存储于区块链数据库中；对于学位认证中所需的核心数据，通过规则处理层中的信息上链模块，上传到区块链系统中，所述区块链系统和区块链数据库上的数据通过同步接口随时进行信息交互，确保数据同步运行，达到一致性要求，各部分存储数据不会产生矛盾或冲突；当查询相关数据时使用基于相关驱动的接口进行查询，所述业务逻辑层通过封装好消息格式的远程调用服务，例如JSON-RPC--JSONRemote Protocol Call，基于JSON消息格式的远程调用服务，发送请求实现与智能合约的交互。

[0012] 优选的，所述学位判定模块根据各学校、专业的特点，以及国家对学位授予的相关法律法规，定制不同的学位认证条件，并记载在图灵完备的学位授予条例规则中，将学位认证结果进行有限共享，被授权的用人单位、高校、监管机构能够进行学生学业及学位信息的全部或部分查询，所述学生学业及学位信息从链上获取，保证数据安全有效，所述认证条件使用智能合约机制实现，在区块链系统上执行，所述智能合约机制遵守区块链基本规则，即所述智能合约一旦部署成功，将无法进行更改；所述学分统计模块根据高校不同专业的培养方案，制定相应的学分修习制度，包括公共基础课、必修课、选修课不同类别课程的统计规则，需要分门别类的进行计算，并提供统计结果的调用方法，方便所述学位判定模块进行调用；所述信息上链模块用于将各功能模块处理结果上传到所述区块链系统，同时保证链上只存储核心信息。

[0013] 优选的，所述信息数据查询模块处理用人单位、高校对学生成绩信息、学位授予情况的查询请求，调用信息交互模块存取数据，并返回用户接口层；所述信息交互模块用于处理数据请求，首先将请求进行分类，根据数据种类不同，通过数据上链/更新模块分别调取区块链系统和区块链数据库的数据，加工成所需信息后发给信息数据查询模块进行下一步处理；所述数据上链/更新模块根据收到的指令调用数据处理接口或应用程序接口，与所述规则处理层和所述数据存储层进行信息交互，并将底层返回的数据进行打包，发回其他模块；所述权限管理模块用于管理高校管理者、教师、学生、用人单位、第三方监管机构各角色的权限，并整合数据安全机制，保证数据使用、存储过程安全可控。

[0014] 优选的，所述用户信息管理模块提供用户信息的采集、修改、添加、删除操作，并协助其他各层完成新加入节点用户的授权；所述信息数据录入模块提供高校管理者导入学生个人信息、课程信息、培养方案以及考核成绩重要信息数据的录入功能；所述可视化展示模块根据系统中存在的大量数据，进行数据整合和统计，最终以统计图或表的形式进行展示，供用人单位、高校管理人员、学生以及第三方监管机构查询和参考。

[0015] 优选的，所述区块链系统采用特定共识机制和区块链运行环境的结合，所述特定共识机制包括共识引擎和通用的应用接口，采用加入BFT(Byzantine Fault Tolerance，拜占庭容错)机制的PoS(Proof of Stake，权益证明)算法；所述区块链运行环境提供使用虚

拟机的环境,(如EVM,Ethereum Virtual Machine,以太坊虚拟机),执行特定语言(如Solidity)编写的智能合约。

[0016] 优选的,所述基于区块链的学位认证系统对完成注册并授权的高校将分配唯一ID,所述ID包括一对表示账户地址的公钥和用于签名的私钥,高校在上传学生信息、成绩、培养方案、学位证书编码等数据至区块链数据库和区块链系统中时,使用自己的私钥对数据进行签名并发起交易,当满足共识机制所要求的节点个数对该消息进行确认后,数据才能上传成功。

[0017] 本发明的目的还在于提供一种基于区块链的学位认证方法,包括以下步骤:

[0018] 步骤1:各高校完成注册,被联盟区块链系统通过共识授权,加入基于联盟区块链的学位认证系统并获取一对公钥和私钥;

[0019] 步骤2:学生开学报道,高校管理员负责将学生信息导入系统;

[0020] 步骤3:高校在系统内公示学生培养方案和学分修习规则;

[0021] 步骤4:培养方案公示结束后,高校将该培养方案写入智能合约,部署至区块链,智能合约生效;

[0022] 步骤5:学生根据培养方案参加课程的学习和考试,获得考核成绩;

[0023] 步骤6:高校负责人将学生成绩导入系统,学生可以登录系统进行查询,如有异议,需在管理员或系统指定和/或调整的时间内提交修改成绩的申请,公示期满,系统自动将成绩上传至区块链数据库中进行保存;

[0024] 步骤7:智能合约根据上传的数据,自动执行判定规则判定学生是否通过该阶段学习,可以进入下一阶段的学习;

[0025] 步骤8:学生完成所有阶段的学习后,智能合约自动判定学生是否取得学位证书,并对取得的学位证书通过调用一种针对非同质通证的标准接口生成该证书独一无二的证明编号,所述编号和最终授予的纸质证书编号进行绑定;

[0026] 优选的,所述步骤8中所述非同质通证的接口使用可基于相关标准(比如 ERC721)提供,从而定义不同学生的学位证书,在区块链系统上存储,保证学位证书的唯一性、不可篡改性,每个所述非同质通证具有唯一的通证编号,和学校颁发的有效学位证书编号进行绑定,当高校确认学生完成所有阶段的学习后,智能合约自动判定学生是否取得学位,并对取得的学位证书通过调用所述非同质通证的标准接口生成所述学位证书独一无二的证明编号;授权的用人单位或学校使用证书编号或者非同质通证编号查询学生的学位授予信息以及在读期间的所有成绩信息。

[0027] 优选的,所述方法还包括:

[0028] 步骤9:学生求职时将学位证书交与用人单位,用人单位将证书编号输入系统即可查询该学位证书真伪以及证书获取过程中所产生的关键数据,完成学位信息溯源,包括四六级成绩、过程性考核结果以及专业课考试成绩,学生可以通过系统查看自到校报道开始至获取资质的所有相关的重要数据,所有数据传输和存储过程中使用加密算法。

[0029] 本发明的有益效果:

[0030] 所提供的基于区块链的学位认证方法和实现系统有别于传统认证方法使用中心数据库和第三方机构背书,保证真伪查询,过分依赖第三方机构,而且克服了由于高校内部学位认证,通常使用人工处理或者简单的信息化方法,缺乏有效的保障机制所带来的问题,

本发明使用区块链上的智能合约将学位授予规则代码化，放置于区块链之上，基本去除了人为干涉的可能性。

[0031] 根据下文结合附图对本发明具体实施例的详细描述，本领域技术人员将会更加明了本发明的上述以及其他目的、优点和特征。

附图说明

[0032] 后文将参照附图以示例性而非限制性的方式详细描述本发明的一些具体实施例。附图中相同的附图标记标示了相同或类似的部件或部分。本领域技术人员应该理解，这些附图未必是按比例绘制的。本发明的目标及特征考虑到如下结合附图的描述将更加明显，附图中：

[0033] 图1为根据本发明实施例的基于区块链的学位认证系统的架构图；

[0034] 图2为根据本发明实施例的基于区块链的学位认证实现的一个实例架构图；

[0035] 图3为根据本发明实施例的基于区块链的学位认证方法的流程图。

具体实施方式

[0036] 为了使得本发明能够针对其发明要点更加明显易懂，下面将结合附图和实例对本发明作进一步的说明。在下面的描述中阐述了很多细节和具体实例，提供这些实例是为了能够更透彻地理解本发明，并且能够将本发明完整形象地传达给本领域的技术人员。虽然本发明能够以很多不同于此描述的其它方式实施，但是本领域技术人员可以在不违背本发明内涵的情况下做相应的推广，因此本发明不受下面公开的具体实例及具体附图所限制。

[0037] 本发明的系统架构如图1所示，分为数据存储层、规则处理层、业务逻辑层和用户接口层。

[0038] 一、数据存储层，主要负责数据的存储。本系统存在两种数据存储方式，分别是：

[0039] 1、区块链系统(Blockchain System,简称BCS)，这就是符合区块链基本特征的链式结构，利用分布式节点的共识算法来生成和更新数据，利用密码学加密的方式来保证数据传输和访问的安全，利用由自动化脚本代码组成的智能合约来执行业务逻辑并操作数据。搭建在区块链系统上的应用具有强的不可篡改、分布式共识等特性，智能合约的部署和使用保证了代码执行无法受到人工干预，提高系统安全性和可信度。

[0040] 2、区块链数据库(Blockchain Database,简称BCD)，具备分布式数据库和区块链两方面技术特征的结合体，具有高吞吐量、低延时、大容量、易于查询等传统数据库优点，又具有去中心化、数据不可篡改等区块链特有的优势。

[0041] 本学位认证系统在实际运行中，需要在线处理大量事务，尤其在期末考试之后，每个节点需要及时响应万名学生百万条数据信息存储、查询，如果联盟链中加入较多的学校，则需同时处理的数据量倍增。此外，每年毕业季用人单位和各高校会集中发起学位认证、查询认证结果的请求。

[0042] 由于以上原因，本系统对延迟性具有较高的要求，依靠单一的区块链系统无法满足这一实际需求，因此本发明创新性地实施了将数据分别存储在区块链数据库BCD和区块链系统BCS上的解决方案。

[0043] 数据上传过程中分为两种情况，对于数据量较大、不参与学位认证的非核心数据，

通过专用接口上传到区块链数据库BCD，实现数据的快速存取，保证数据无法篡改。

[0044] 对于成绩、学分等学位认证中所需核心数据，将通过规则处理层中的信息上链模块，上传到区块链系统BCS中，该数据可追溯，不可修改，能够保证学位认证的整个过程准确迅速。

[0045] 区块链数据库BCD和区块链系统BCS上的数据通过同步接口可以随时进行信息交互，确保数据同步运行，达到一致性要求，各部分存储数据不会产生矛盾或冲突；当查询相关数据时使用基于相关驱动的接口进行查询，业务逻辑层通过封装好的消息格式的远程调用服务，例如JSON-RPC，发送请求实现与智能合约的交互。二、规则处理层，主要是实现区块链智能合约相关操作。规则处理层包括学位判定、学分统计、信息上链三大功能模块。

[0046] 1、学位判定模块能够根据各学校、专业的特点，以及国家对学位授予的相关法律法规，定制不同的学位认证条件，并记载在图灵完备的学位授予条例规则中，认证过程快速准确，自动执行，无法人为干预。可以将学位认证结果进行有限共享，被授权的用人单位、高校、监管机构能够进行学生学业及学位信息的全部或部分查询。关键信息从链上获取，保证数据安全有效。上述认证规则可以使用不同机制实现，比如使用智能合约机制，在区块链系统上执行，目前主流的系统有以太坊和超级账本。智能合约遵守区块链基本规则，即一旦部署成功，将无法进行更改。

[0047] 2、学分统计模块根据高校不同专业的培养方案，制定相应的学分修习制度，一般包括公共基础课、必修课、选修课等不同类别课程的统计规则，需要分门别类的进行计算，并提供统计结果的调用方法，方便学位判定模块进行调用。

[0048] 3、信息上链模块负责将各功能模块处理结果上传区块链系统BCS，保证链上只存储核心信息，能够完成系统对学位认证结果不可更改、可追溯的要求，又不影响系统的低延迟性能。

[0049] 三、业务逻辑层，主要通过业务规则接收、处理、分发用户上传的数据，保证系统正常运行。业务逻辑层包括信息数据查询、信息交互、数据上链/更新、权限管理各模块。

[0050] 1、信息数据查询模块处理用人单位、高校对学生成绩信息、学位授予情况的查询请求，调用信息交互模块存取数据，并返回用户接口层。

[0051] 2、信息交互模块主要负责处理数据请求，首先将请求进行分类，根据数据种类不同，通过数据上链/更新模块分别调取区块链系统BCS和区块链数据库 BCD的数据，加工成所需信息后发给信息数据查询模块进行下一步处理。

[0052] 3、数据上链/更新模块根据收到的指令调用数据处理接口或应用程序接口，与规则处理层和数据存储层进行信息交互，并将底层返回的数据进行打包，发回其他模块。

[0053] 4、权限管理模块负责管理高校管理者、教师、学生、用人单位、第三方监管机构等各角色的权限，并整合了数据安全机制，共同保证数据使用、存储过程安全可控，有效避免因系统原因造成数据盗用、滥用、泄露等恶性事件的发生。

[0054] 四、用户接口层，系统的最上层，提供给用户进行信息的录入、查询、展示等，分为用户信息管理模块、信息数据录入模块、可视化展示模块三部分功能。

[0055] 1、用户信息管理模块提供了用户信息的采集、修改、添加、删除等操作，并可协助其他各层完成新加入节点用户的授权。

[0056] 2、信息数据录入模块可以提供高校管理者导入学生个人信息、课程信息，以及培

养方案、考核成绩等重要信息数据的录入功能。

[0057] 3、可视化展示模块根据系统中存在的大量数据，进行数据整合和统计，最终以统计图或表的形式进行展示，供用人单位、高校管理人员、学生以及第三方监管机构查询和参考。

[0058] 在上述实施过程中，本基于区块链的学位认证系统对完成注册并授权的高校将分配唯一ID，该ID包括一对表示账户地址的公钥和用于签名的私钥。高校在上传学生信息、成绩、培养方案、学位证书编码等数据至区块链数据库BCD 和区块链系统BCS中时，需要用自己的私钥对数据进行签名并发起交易，当满足共识机制所要求的节点个数对该消息进行确认后，数据才能上传成功。数据签名既保证了数据的真实可靠又使提供数据的责任人可以被追溯，一旦数据出现问题，可以找到责任人并对其进行追责。同时数据需要通过多数节点确认才可上链，数据无法篡改。共识机制、非对称加密技术可以有效减少传统中心第三方管理员为了某种利益篡改以及伪造数据的可能性。

[0059] 当高校确认学生完成所有阶段的学习后，智能合约自动判定学生是否取得学位，并对取得的学位证书通过调用一种针对非同质通证的标准接口生成该证书独一无二的证明编号。由于取得的证明编号非同质，所以独一无二，不可更改。整个学位证书的获得过程公开透明，数据真实可靠，伪造的学位证书编号无法通过系统查验。通证是一种加密的数字资产，在区块链中可以将非标准化的商品及服务进行通证化映射，从而保证所绑定物品的唯一性，在本例中，利用非同质通证标准接口可以生成唯一的学位证书编号，方便进行学位获取过程的溯源、查询以及学位证书的防伪。

[0060] 图2为基于区块链的学位认证方法具体实现的一个实例的架构图。如图2 所示，是本系统具体实施的一个方案，业务逻辑层可以由Java编写的业务逻辑代码组成，区块链系统BCS可以由基于HyperledgerBurrow和tendermint的区块链环境实现，区块链数据库BCD可以使用BigchainDB区块链数据库进行部署。

[0061] 本方案所述区块链系统可以采用Tendermint共识机制以及 HyperledgerBurrow区块链运行环境，它们的结合解决了传统单一区块链环境 (如比特币、以太坊等)高延迟性的问题，能够缩短达到共识所需要的时间。Tendermint包括共识引擎和通用的应用接口，采用了加入BFT(Byzantine Fault Tolerance，拜占庭容错)机制的PoS(Proof of Stake，权益证明)算法，与传统共识机制相比，共识过程更加简便、迅速。Hyperledger Burrow区块链环境提供了使用虚拟机的环境，本实施例中采用EVM(Ethereum Virtual Machine，以太坊虚拟机)虚拟机，能够执行特定语言的智能合约，例如本实施例中基于 Solidity编写，可行性强。

[0062] 无需参与智能合约计算的数据，可直接通过本实施例中的BigchainDB JavaDriver存储于BigchainDB中，当查询BigchainDB中的数据时可使用 BigchainDB JavaDriver进行查询。业务逻辑层通过封装好的JSON-RPC(JSON Remote Protocol Call，基于JSON消息格式的远程调用服务)发送请求实现与合约层的交互。本示例所述能够充分满足高吞吐量、低延迟、数据无法篡改等要求。BigchainDB符合区块链数据库的特点，继承了现代分布式数据库的特性，具有海量数据存储、亚秒级响应延迟、百万次每秒的吞吐量、高效的查询和权限管理等优势。同时，又兼具去中心化、不可篡改等区块链特有的核心优势。

[0063] 图3为基于区块链的学位认证方法流程图。如图3所示，本系统的具体实施方案可以包括以下步骤：

[0064] 步骤1：各高校完成注册，被联盟区块链系统通过共识授权，加入该基于联盟区块链的学位认证系统并获取一对公钥和私钥。

[0065] 步骤2：学生开学报道，高校管理员负责将学生信息导入系统。

[0066] 步骤3：高校在系统内公示学生培养方案和学分修习规则。

[0067] 步骤4：培养方案公示结束后，高校通过一定方式将该培养方案写入智能合约，部署至区块链，智能合约生效。

[0068] 步骤5：学生根据培养方案参加课程的学习和考试，获得考核成绩。

[0069] 步骤6：高校负责人将学生成绩导入系统，学生可以登录系统进行查询，如有异议，需在15个工作日(该时间可由管理员进行指定和调整)内提交修改成绩的申请。公示期满，系统自动将成绩上传至区块链数据库BigchainDB中进行保存。

[0070] 步骤7：智能合约根据上传的数据，自动执行判定规则判定学生是否通过该阶段学习，可以进入下一阶段的学习。

[0071] 步骤8：学生完成所有阶段的学习后，智能合约自动判定学生是否取得学位证书，并对取得的学位证书通过调用一种针对非同质通证的标准接口生成该证书独一无二的证明编号。该编号可以和最终授予的纸质证书编号进行绑定。

[0072] 本发明可以使用基于ERC721标准提供的非同质通证接口来定义不同学生的学位证书，在区块链系统上存储，保证学位证书的唯一性、不可篡改性。每个通证具有唯一的通证编号，可以和学校颁发的有效学位证书编号进行绑定，授权的用人单位或学校可以使用证书编号或者非同质通证编号查询学生的学位授予信息以及在读期间的所有成绩信息。与传统中心化监管机构提供的查询网站不同，这些数据分布式存储在区块链各节点中，数据的增加、删除、修改、查看等所有操作均可溯源，有效避免了中心数据库难以解决的单点攻击、数据篡改等问题。

[0073] 步骤9：学生求职时将学位证书交与用人单位，用人单位将证书编号输入系统即可查询该学位证书真伪以及证书获取过程中所产生的关键数据，完成学位信息溯源，如四六级成绩、过程性考核结果以及专业课考试成绩等，方便各数据使用单位更好地安排学生职位，监管机构掌握高校教学情况并加强管理。此外，学生也可以通过系统查看自到校报道开始至获取资质的所有相关的重要数据。所有数据传输和存储过程中使用了加密算法，有效保护了数据的真实性与学生个人信息的隐私。

[0074] 本实施例所提供的基于区块链的学位认证系统及认证方法有别于传统认证方法使用中心数据库和第三方机构背书，避免过分依赖第三方机构来完成真伪查询的现象，而且克服了由于高校内部学位认证，通常使用人工处理或者简单的信息化方法，缺乏有效的保障机制带来的问题，本实施例使用区块链上的智能合约将学位授予规则代码化，放置于区块链系统之上，基本去除了人为干涉的可能性。

[0075] 虽然本发明已经参考特定的说明性实施例进行了描述，但是不会受到这些实施例的限定而仅仅受到附加权利要求的限定。本领域技术人员应当理解可以在不偏离本发明的保护范围和精神的情况下对本发明的实施例能够进行改动和修改。

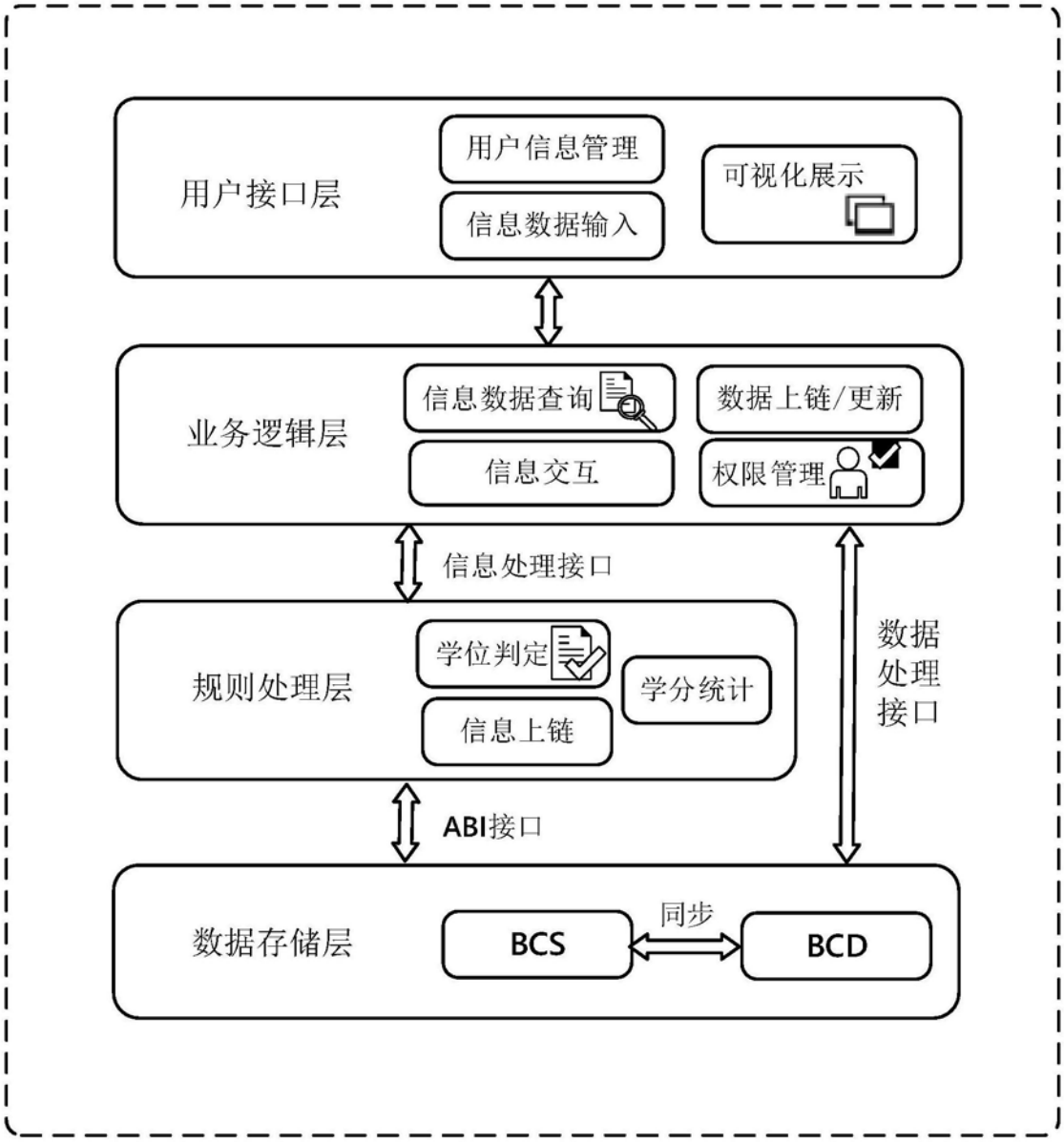

用户接口层
用户信息管理
信息数据输入
可视化展示
业务逻辑层
信息数据查询
数据上链/更新
信息交互
权限管理
信息处理接口
规则处理层
学位判定
学分统计
信息上链
数据处理接口
ABI接口
数据存储层
BCS
同步
BCD

图1

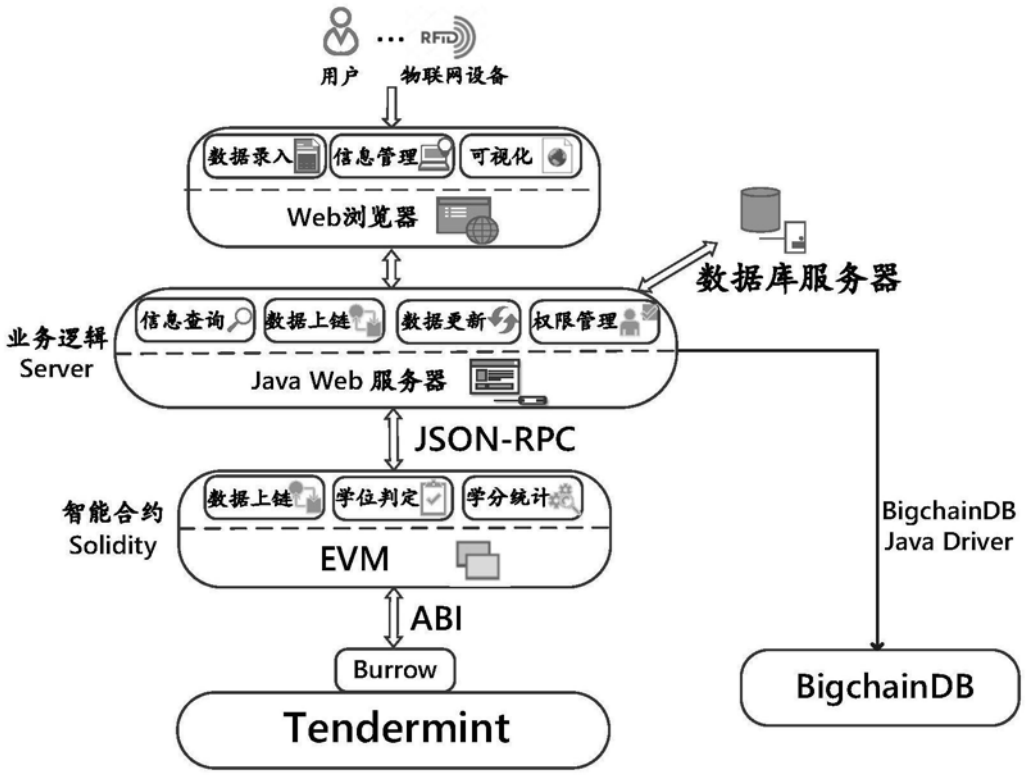

用户
物联网设备
RFID
数据录入
信息管理
可视化
Web浏览器
数据库服务器
业务逻辑
Server
信息查询
数据上链
数据更新
权限管理
Java Web 服务器
JSON-RPC
智能合约
Solidity
数据上链
学位判定
学分统计
EVM
ABI
Burrow
Tendermint
BigchainDB
Java Driver
BigchainDB

图2

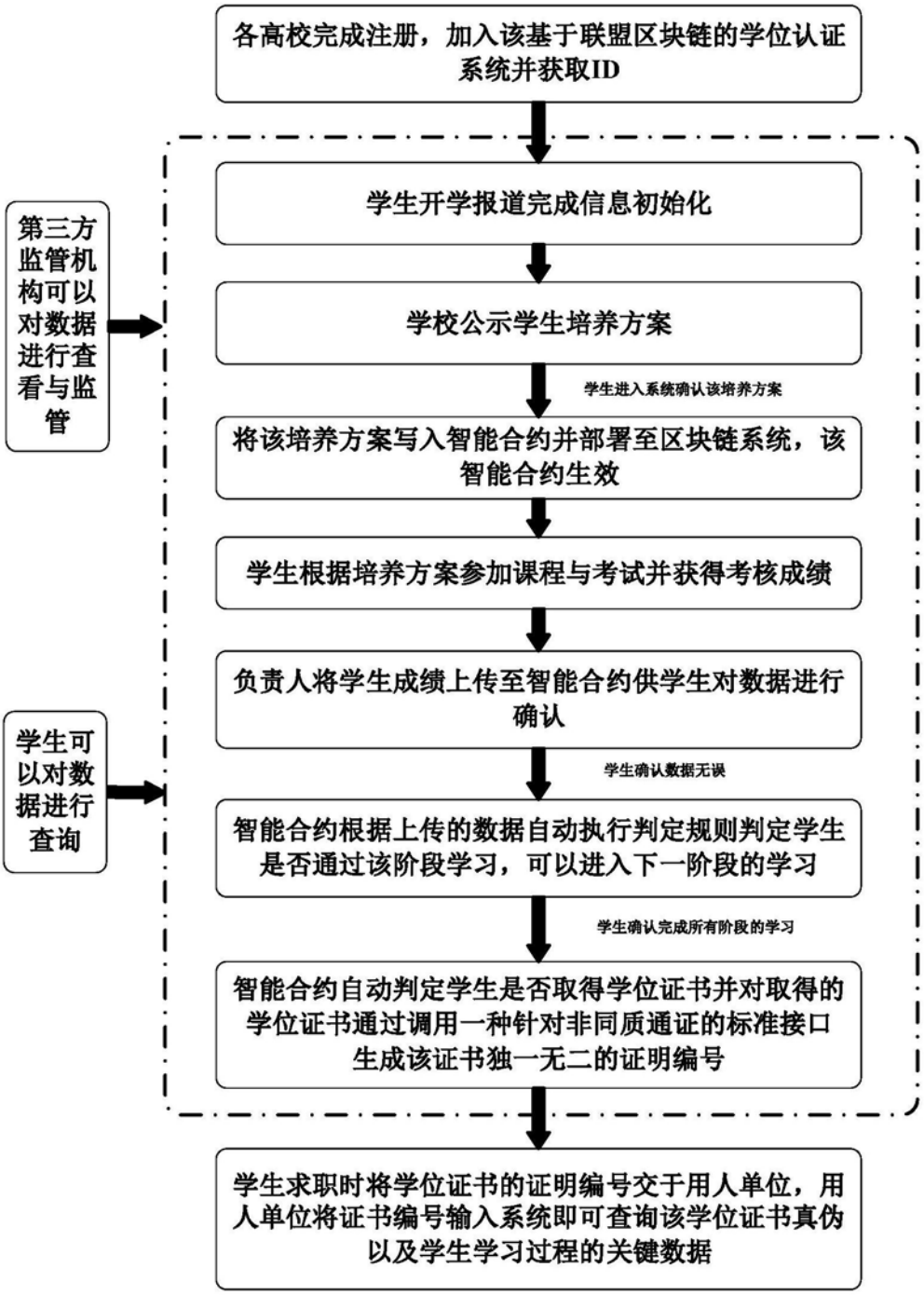

各高校完成注册，加入该基于联盟区块链的学位认证系统并获取ID
学生开学报道完成信息初始化
学校公示学生培养方案
学生进入系统确认该培养方案
将该培养方案写入智能合约并部署至区块链系统，该智能合约生效
学生根据培养方案参加课程与考试并获得考核成绩
负责人将学生成绩上传至智能合约供学生对数据进行确认
学生确认数据无误
智能合约根据上传的数据自动执行判定规则判定学生是否通过该阶段学习，可以进入下一阶段的学习
学生确认完成所有阶段的学习
智能合约自动判定学生是否取得学位证书并对取得的学位证书通过调用一种针对非同质通证的标准接口生成该证书独一无二的证明编号
学生求职时将学位证书的证明编号交于用人单位，用人单位将证书编号输入系统即可查询该学位证书真伪以及学生学习过程的关键数据
第三方监管机构可以对数据进行查看与监管
学生可以对数据进行查询

图3