密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2018, 5(5): 568–578

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

区块链技术专刊

基于区块链技术的高校成绩管理系统*

孙韵秋, 王启春

南京师范大学计算机科学与技术学院, 南京 210046
通信作者: 孙韵秋, E-mail: yunqiu_sun@163.com

摘 要: 成绩管理对于高校管理而言具有十分重大的意义. 可以帮助学校更好的整理、统计、分析学生的学习情况. 因此, 成绩管理系统中信息的真实性和安全性尤为重要. 目前的成绩管理系统大多采用中心化的管理方式, 依赖于管理员通过 SQL Server、Oracle 等大型中心化数据库来进行数据管理, 中心化平台往往会带来信息的泄露和篡改等问题. 随着区块链技术的兴起, 其具有的去中心化、去信任化的特性逐渐引起人们的关注. 本文利用去中心化的区块链技术, 为成绩管理系统提出一个安全、防篡改的管理系统. 我们利用 P2P 网络和区块链技术为系统提供一个安全稳定的运行环境, 将学生成绩进行 Hash, 利用时间戳服务 OriginStamp 的 API 将 Hash 后的结果嵌入区块链中, 区块链中的数据受到整个网络的管理和监控, 防止随意篡改和破坏. 同时为用户和底层数据提供交互界面, 完成成绩上传、修改以及查询功能. 该方案可以有效的保证成绩管理系统中数据的真实性、有效性, 对学校管理学生信息、制定教学任务等有着重大的影响.

关键词: 区块链; 成绩管理; 信息安全
中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000266

中文引用格式: 孙韵秋, 王启春. 基于区块链技术的高校成绩管理系统[J]. 密码学报, 2018, 5(5): 568–578.
英文引用格式: SUN Y Q, WANG Q C. University score management system based on blockchain technology[J]. Journal of Cryptologic Research, 2018, 5(5): 568–578.

University Score Management System Based on Blockchain Technology

SUN Yun-Qiu, WANG Qi-Chun

School of Computer Science and Technology, Nanjing Normal University, Nanjing 210046, China
Corresponding author: SUN Yun-Qiu, E-mail: yunqiu_sun@163.com

Abstract: Grade management is of great significance for university management. It helps schools to better organize, count, and analyze students' learning. Therefore, the authenticity and security of information in the management system is particularly important. Most of the current score management systems use centralized management methods, relying on administrators to manage data through centralized databases such as SQL Server, Oracle, which have the risk about information leakage and tampering. With the rise of blockchain technology, the decentralized and distrusted features

* 基金项目: 国家自然科学基金 (61572189)
Foundation: National Natural Science Foundation of China (61572189)
收稿日期: 2018-07-16 定稿日期: 2018-09-30

have attracted much attention. By using decentralized blockchain technology to proposes a secure and tamper-proof management system for score management. We use P2P network and blockchain to provide a safe and stable operating environment for the system, The students' grades are hashed, and the results of the hash are embedded in a blockchain using the timestamp service OriginStamp's API. The data in the blockchain is managed and monitored by the entire network to prevent illegal tampering and destruction. We provide interactive interfaces for users and the underlying data to complete the uploading, modifying and query functions. The proposed system can effectively provide the authenticity and validity of data in the score management system, and has a significant impact on the management of student information in schools and the formulation of teaching tasks.

Key words: blockchain; score management; information security

1 引言

成绩管理系统已经是各大高校用于学生成绩管理的标准工具, 通过成绩管理系统, 学校可以更好的保存学生的信息, 对学生的成绩进行分析, 进而对学校以后教学发展的方向、教师教学成果的评估等提出有依据的参考. 目前的成绩管理系统多为基于中心化管理的平台, 虽然简化了信息处理的流程, 使得成绩管理更加高效, 同时也伴随着潜在的安全威胁. 中心化的服务器面临着以下几个风险: 一是单点故障的风险, 一旦中央服务器出现问题, 整个系统就会停止运行, 甚至对已保存的数据造成破坏. 二是单点突破的风险, 如果管理服务器的管理员账户被攻击, 攻击者则可以在不被发现的情况下修改数据, 或者破坏模型. 甚至, 由于管理员的不诚实行为, 就可能造成数据真实性和完整性的破坏. 三是 CS 架构面临共识/同步问题, 比如女巫攻击和拜占庭将军问题 [1].

除却外在的风险, 还存在某些极端的情况, 在成绩已经被提交的情况下, 学生通过不正当的方式, 向老师提出修改成绩的申请, 这对于其他同学而言, 是非常不公平的行为, 并且对学校学风造成不良影响. 比如, 学生为了申请较好的学校继续深造或者为了进入更好的公司工作, 通过不正当手段, 请求教师或者学校成绩系统管理员为自己修改原本较低的成绩.

针对上述风险, 我们提出了一个可行的解决方案, 即在成绩管理系统中采用区块链技术. 区块链技术是在多方无需互信的环境下, 通过密码学技术让系统中所有参与方协作, 来共同维护可靠数据日志的方式, 区块链具有分布式、去中心化和安全可信的特点 [2]. 我们可用该技术来设计成绩管理系统, 提高系统安全性.

2 背景

目前国内高校使用的成绩管理系统多采用 B/S 架构, 前端以 Visual Studio 为开发工具, 以 Web 窗口为交互界面, 后台数据库使用 SQL Server 数据库, 对数据进行存储. 这样的系统具有中心化的特点, 数据库的管理权限集中在少部分管理员手中, 管理员可以进行增删改查, 而普通用户只有访问的权限.

B/S 架构主要事务逻辑在服务器端 (Server) 实现, 形成三层 (3-tier) 结构. 这样使得客户端电脑负荷大大简化 (因此被称为瘦客户端), 减轻了系统维护和升级的支出成本, 降低了用户的总体成本 (TCO). BS 的主要特点是分布性强, 维护方便, 开发简单且共享性强. 但 B/S 架构对服务器要求过高, 数据传输速度慢, 软件的个性化特点明显降低, 难以实现传统模式下的特殊功能要求 [3].

同时, 中心化的系统也会带来一些安全性的问题, 如单点故障, 单点突破, 甚至中心节点不诚实等问题, 中心化系统示意图如图1 左所示. 因此, 我们提出利用区块链技术, 以去中心化的方式对高校成绩系统进行管理, 提高系统的安全性和可靠性.

中本聪首次提出了比特币 [4], 并且引入区块链技术, 相对于传统的中心化记账方式, 区块链技术采用一种去中心化的全分布式方式来记录数据. 去中心化系统具有如下特点:

(1) **分布式传输**

区块链的底层为 P2P 网络, 彼此互联的多台计算机都处于对等的地位, 没有中心化特殊节点和层

级结构, 以扁平式拓扑结构互相连通和交互. 各个计算机有相同的功能, 但无主从之分, 每一台计算机既是网络服务的请求者, 也是网络服务的提供者, 可以为其他计算机提供资源和服务等.

(2) 分布式记录

区块链让网络中的每一个节点都参与记账, 并且每个节点都有验证其他节点记录是否正确的权限, 当大多数节点判定某一节点提交的交易记录正确时, 数据才可以被写入区块中.

(3) 分布式存储

区块链构建了一个分布式结构的网络系统, 数据库中的数据都存放在区块链的网络节点之中, 根据节点存储数据量的区别, 分为全节点和轻量级节点. 全节点存储完整的区块链数据, 从创世区块直到最新产生的区块, 并且, 节点主动参与区块链的实时记账和校验, 动态的维护区块链数据 [5]. 轻量级节点只保存一部分区块链数据, 并且通过简易支付认证的方式从网络中其他对等节点获取相应数据完成数据校验. 去中心化系统示意图如图1 右所示.

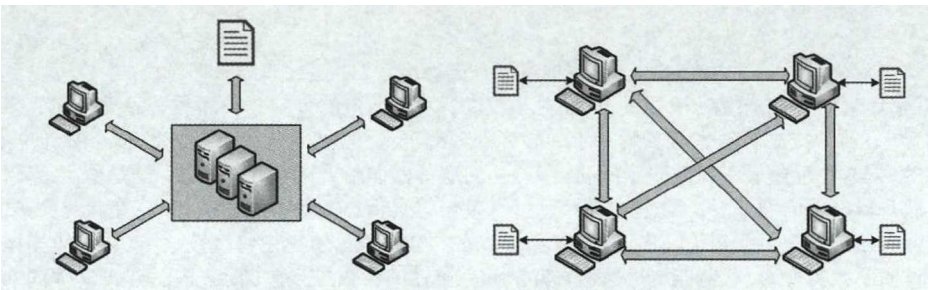


图 1 中心化系统和去中心化系统

Figure 1 Centralized system and decentralized system

3 关键技术

3.1 区块链简介

3.1.1 区块链的概念

具体来说, 区块链是一种按照时间顺序将数据区块以链条的方式组合成特定数据结构, 以密码学的方式保证的不可篡改和不可伪造的去中心化共享账本, 能够安全地存储简单的、有先后关系的以及能在系统中验证的数据 [6]. 如图2所示, 区块体中包括当前区块的交易数量以及经过验证的区块创建过程中生成的交易记录, 记录通过 Merkle 树的哈希过程生成唯一的 Merkle 根记入区块头.

3.1.2 共识机制

共识机制是分布式系统的核心, 在 P2P 系统中, 互相不信任的节点通过预设机制最终达到数据的一致性称为共识. 所谓 “共识机制”, 是通过特殊节点的投票, 在很短的时间内完成对交易的验证和确认; 对一笔交易, 如果利益不相干的若干个节点能够达成共识, 我们就可以认为全网对此也能够达成共识 [7].

区块链作为一种按时间顺序存储数据的数据结构, 可支持不同的共识机制. 共识机制是区块链技术的重要组件. 区块链共识机制的目标是使所有的诚实节点保存一致的区块链视图, 同时满足两个性质:

(1) 一致性. 所有诚实节点保存的区块链的前缀部分完全相同.

(2) 有效性. 由某诚实节点发布的信息终将被其他所有诚实节点记录在自己的区块链中.

目前, 广泛被认可的共识机制有三种, 分别是工作量证明机制 (proof of work, PoW), 权益证明机制 (proof of stake, PoS) 以及授权股份证明机制 (delegated proof of stake, DPoS), 下面将简要的介绍这三种共识机制.

(1) 工作量证明机制 (PoW)

工作量证明机制由中本聪在设计比特币系统时提出, 通过引入分布式节点的算力竞争来保证数据

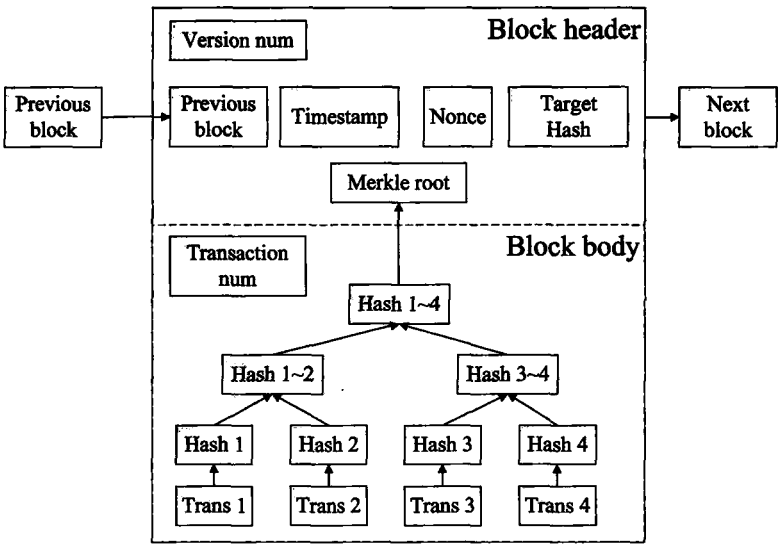


图 2 区块链结构示意图

Figure 2 Blockchain structure diagram

一致性和共识的安全性. 在比特币系统中, 各节点 (即矿工) 基于各自的计算机算力相互竞争来共同解决一个求解复杂但验证容易的 SHA-256 数学难题, 最快解决该难题的节点将获得区块的记账权和系统自动生成的比特币奖励 [8]. 这里的数学难题是指根据系统当前设置的难度值, 通过搜索求解一个合适的随机数 (nonce) 使得区块头中各元数据的双 SHA-256 哈希值小于等于目标哈希值, 公式如式 (1) 所示:

$$\text{SHA256(SHA256(BlockHeader))} \leqslant \text{Target} \tag{1}$$

由此可见, PoW 共识机制通过强大的算力保证整个系统的安全性和不可篡改性, 攻击者若想对数据进行篡改, 必须伪造一条超过主链长度的伪造链, 即从被攻击块开始, 重新计算该块以及该块之后的所有区块的双 SHA-256 难题, 这是非常困难的. 但是, PoW 共识机制还存在着显著的缺陷, 当系统中不诚实节点比例大于 50% 时, 此时交易就非常容易被伪造, 攻击者攻击成功. 同时, 该共识算法所需要的强大算力会造成极大的电力浪费, 并且确认时间过长, 不适合小额交易 [9].

(2) 权益证明机制 (PoS)

PoS 共识机制旨在解决 PoW 共识算法资源浪费和安全缺陷等问题, PoS 本质上是由系统中具有最高权益者获得区块记账权, 权益由币龄体现, 币龄是特定数目的币与其最后一次交易的时间长度的乘积, 拥有的币龄越高, 相对的挖矿难度也就越低 [10].

(3) 授权股份证明机制 (DPoS)

DPoS 共识机制的基本思路类似于 "董事会决策", 即系统中每个股东节点可以将其持有的股份权益作为选票授予一个代表, 获得票数最多且愿意成为代表的前 101 个节点将进入 "董事会", 按照既定的时间表轮流对交易进行打包结算并且签署 (生产) 一个新的区块, 每个区块被签署前, 必须先验证前一个区块已经被受信任的代表节点签署 [10].

与 PoW 和 PoS 不同, DPoS 共识机制中每个节点都能够自主决定其新人的授权节点并且由这些节点轮流记账生成新区块, 因而大幅度减少了参与验证和记账的节点数量, 可以实现快速共识验证.

3.1.3 OriginStamp

时间戳是一个能表示一份数据在某个特定时间之前已经存在的、完整的、可验证的数据, 通常是一个字符序列, 唯一标识某个时刻的时间.

OriginStamp 是一个基于 Web 的可信时间戳服务, 它使用分散的比特币区块链来存储任何数字内容的匿名防篡改时间戳. OriginStamp 允许用户对文件、电子邮件或纯文本进行散列处理, 然后将创建的散列存储在比特币块链中, 并检索和验证已提交给块链的时间戳. OriginStamp 免费且易于使用, 因此允许任何人 (例如学生、研究人员、作者、记者或艺术家) 在给定时间点证明他们是某些信息的创始人. OriginStamp 的常见用例包括证明:

(1) 合同已签署或任务在某一日期之前已完成.

(2) 在某个日期之前已经记录了照片或视频.

(3) 一个专利的想法在某个日期之前已经存在, 例如在签署 NDA 之前.

为了克服依赖于 TSA 的传统模式的缺点, 我们的设计采用一种分布式的时间戳服务, 即 OriginStamp, 当用户通过浏览器提交文件或纯文本时, 客户端 Java 脚本会散列数据. 为了降低运营成本, 服务器收集提交的哈希值, 连接哈希值, 并生成单个聚合哈希值. 通过执行额外的散列和编码操作, 聚合散列被转换为区块链地址. 通过执行交易, 交易的汇总散列和时间戳被永久地嵌入到分布式区块链中. 比特币货币将交易存储为 Merkle 树的叶节点. 当计算节点成功找到一个数字 (随机数) 时, 事务就形成一个块, 该数字在插入到块中时会导致块的散列符合一定的复杂性标准. 在其他信息中, 块包含 Merkle 树的根和前一个块的哈希, 从而形成一个区块链 [11].

这个概念与已建立的时间戳协议相比具有以下优点:

(1) 包含时间戳过程的分散式密码完整性验证;

(2) 向为分散式流程做出贡献的计算节点提供激励政策;

(3) 无需设置专门的硬件或软件;

(4) 运营成本低, 能够提供免费服务.

OriginStamp 的工作模式如下:

(1) 通过电子邮件或直接上传提交您的内容. 您可以使用纯文本或任何文件格式, 例如: pdf、doc、png、音频或视频文件. 如果使用直接上载选项, 则文件在浏览器中被散列化, 只有散列被传输到 OriginStamp 服务器.

(2) OriginStamp 收集所有提交的哈希指纹, 并每天创建一个新的聚合哈希. 使用 Base 58 编码, 然后使用汇总的散列值创建一个新的比特币地址, 并将最小可能数量的比特币 (0.000 055 BTC) 传输到该地址. 该交易确保散列现在永久嵌入比特币网络的分散区块链中. 区块链中的交易发生后, 不可能更改此散列的时间戳.

(3) 现在, 世界上所有可以访问互联网的人都可以通过使用区块链浏览器 (例如 blockchain.info) 或通过检查区块链本身的副本来轻松验证 OriginStamp 中的可信时间戳.

4 系统设计

由于现有的成绩管理系统的局限性, 本文提出一种基于区块链技术的在线成绩管理系统, 利用区块链技术保证高校成绩系统中的数据完整性. 同时我们通过去中心化的时间戳服务 OriginStamp, 生成可信时间戳, 防止数据被篡改.

4.1 系统总体架构设计

本文设计的系统采用分层架构, 我们把系统分成两个层次: 应用交互层和区块链层, 如图3所示.

上层的应用交互层为用户和系统交互提供了友好的界面, 完成用户和区块链之间的数据转换, 将教师提交的成绩数据封装为虚拟资产和交易, 提交给节点校验后, 存储到区块链上. 同时, 学生还可以提出成绩查询请求, 利用区块链查询接口获取数据, 并且以直观的方式在浏览器上向用户呈现.

底层的区块链层包括两部分, 一部分是 P2P 网络, 组成了区块链网络, 维护系统的正常运行, 并且处理网络中的交易, 生成区块并且进行验证, 这些节点还提供数据查询的功能. 另一部分是区块链, 整个系统中维护一条区块链, 从创世区块到最新的区块, 包含整个系统中所有已验证的交易数据.

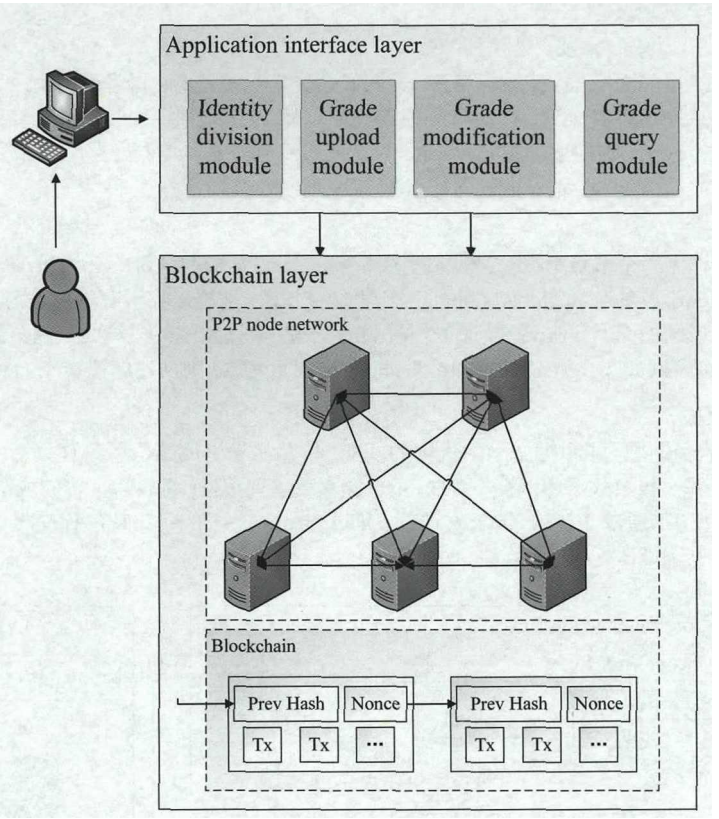


图 3 系统总体架构图

Figure 3 System architecture

4.2 系统详细设计

4.2.1 角色注册模块

(1) 学生身份

系统为学生提供了注册的界面, 学生打开系统进行注册, 选择学生角色, 输入姓名、学号、学院等相关信息, 并且点击密钥生成按钮, 系统利用密钥生成器生成公私钥对, 学生自己保存其私钥, 公钥提交给学校. 注册完成之后, 根据学生的注册信息, 创建虚拟资产 stu, 并且把虚拟资产 stu 提交给学校. 学生注册流程图如图4所示.

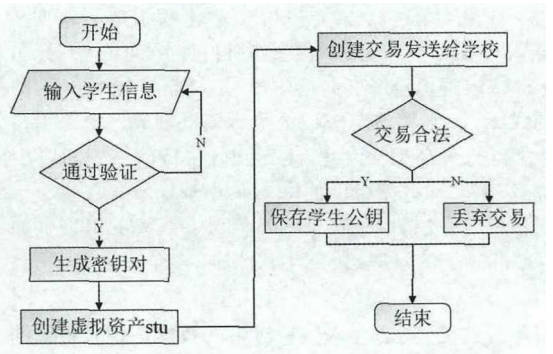


图 4 学生注册流程图

Figure 4 Student registration flow chart

(2) 教师身份

教师进入注册界面后, 选择教师身份, 输入姓名、工号等信息, 利用密钥生成器生成公私密钥对, 公钥应记录在册并且公开. 教师将成绩整理好以后, 创建虚拟资产 grade, 将该交易提交给学校. 如果要修改成绩, 则创建虚拟资产 alt, 并且把该交易发送给学校. 若收到 agree 交易, 则重新上传修改后的成绩. 若收到 reject 交易, 则不做修改.

(3) 学校身份

学校也是作为一个节点存在, 是交易的主体身份之一, 学校的身份不必注册, 在系统安装时候就已经直接生成学校的公私密钥对, 并且公开学校的公钥. 学校接收所有学生信息的交易 stu 和教师上传学生成绩的交易 grade, 验证审核收到的交易. 若收到修改成绩的交易, 经审核后, 若同意修改, 则创建虚拟资产 agree, 并返回给教师. 若不同意修改, 则创建虚拟资产 reject, 并发送给教师.

4.2.2 成绩上传模块

系统前端为教师提供登陆和提交学生成绩的功能, 教师将学生成绩信息整理好后, 上传至系统中, 系统前端将成绩提交并上传至数据库, 客户端的 Java 脚本会散列数据, 将教师上传的成绩通过哈希函数 (如 SHA-256) 生成比特串, 通过 POST 请求发送给 OriginStamp API, 将比特串提交至 OriginStamp 服务器, 获取可信时间戳, 如图5所示.

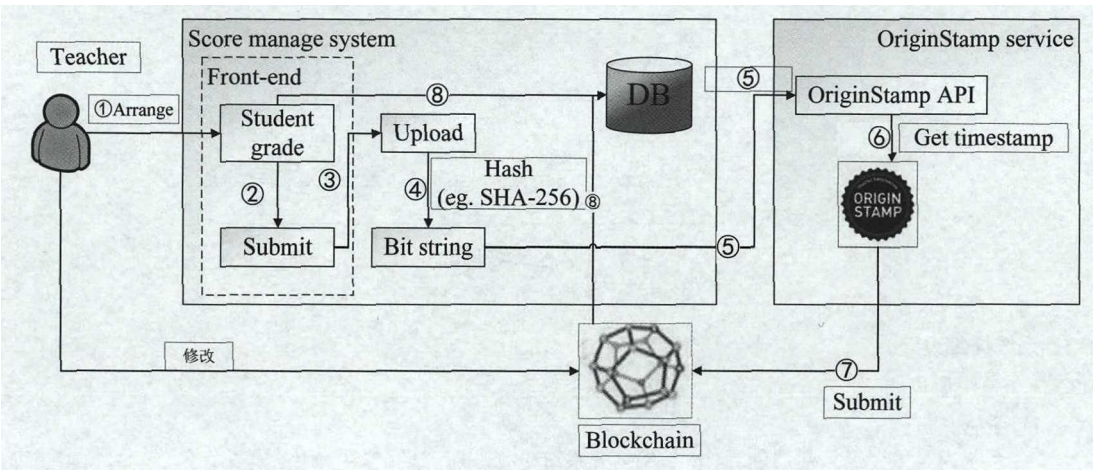


图 5 成绩管理系统

Figure 5 Grade management system

系统为学生提供友好的可视化界面, 学生在注册界面提交自己的个人信息时, 通过点击界面上密钥生成按钮, 系统调用 KeyPairGenerator 类提供实例化和生成密钥对的方法, 即 KeyPairGenerator.getInstance ("SHA-256"). 学生即可在界面上查看到自己的公私密钥对, 并将密钥对保存下来. 学生完成注册后, 创建虚拟资产 stu, 将该虚拟资产交易给学校, 这样学校便可获得学生的公钥信息.

当教师提交多个学生的成绩时, 则将多个成绩的哈希值聚合成一个总哈希值, 通过额外的哈希及编码技术, 将聚合散列值转换为全新的聚合 Hash 值, 提交到区块链网络中, 成绩和可信时间戳共同存入数据库中, 确认交易的时间戳和它们编码的数据可以使用 OriginStamp 网站验证, 该服务专门存储哪些哈希包含在哪个交易中. 此信息允许使用区块链验证任何哈希值. 因此, 数据和时间戳就可以保持可验证. 聚合哈希值主要作用是提高成绩存储和提交的效率, 降低运营成本. 多个成绩提交示意图如图6所示.

4.2.3 成绩修改模块

区块链中的信息具有不可篡改性, 所有存入区块链中的数据都是多备份的, 即使网络中的部分节点被攻破, 数据依然很难被篡改. 因此, 成绩的修改不能像传统数据库 (如 SQL Server, Oracle) 中一样, 直接对成绩这一字段中的数据进行修改. 区块链中采取的方式是将之前记录的成绩标记为无效, 并且把修改后的新的成绩提交, 通过校验后, 存入区块链之中.

当教师提出修改申请时, 则创建虚拟资产 alt, 并且把该交易发送给学校. 申请则被提交至区块链, 此时区块链中的节点运行共识协议, 判断修改申请是否合法, 如果合法, 若同意修改, 则创建 agree 虚拟资产, 并返回给教师. 否则, 就驳回修改申请, 创建虚拟资产 reject, 并发送给教师.

如果教师收到 agree 交易, 则重新上传修改后的成绩, 区块链重新审核新提交的成绩, 若通过验证, 则在原先记录上把这条记录标记为无效, 并且将哈希指针指向更新后的新的交易所在的区块, 若是查找相应信息, 当查找到原先记录时, 首先检查该记录是否有效, 若有效即可得到正确数据, 若改数据已经被标记为无效数据, 则根据该区块所指向的新区块, 根据相应的哈希值, 找到更新后的数据.

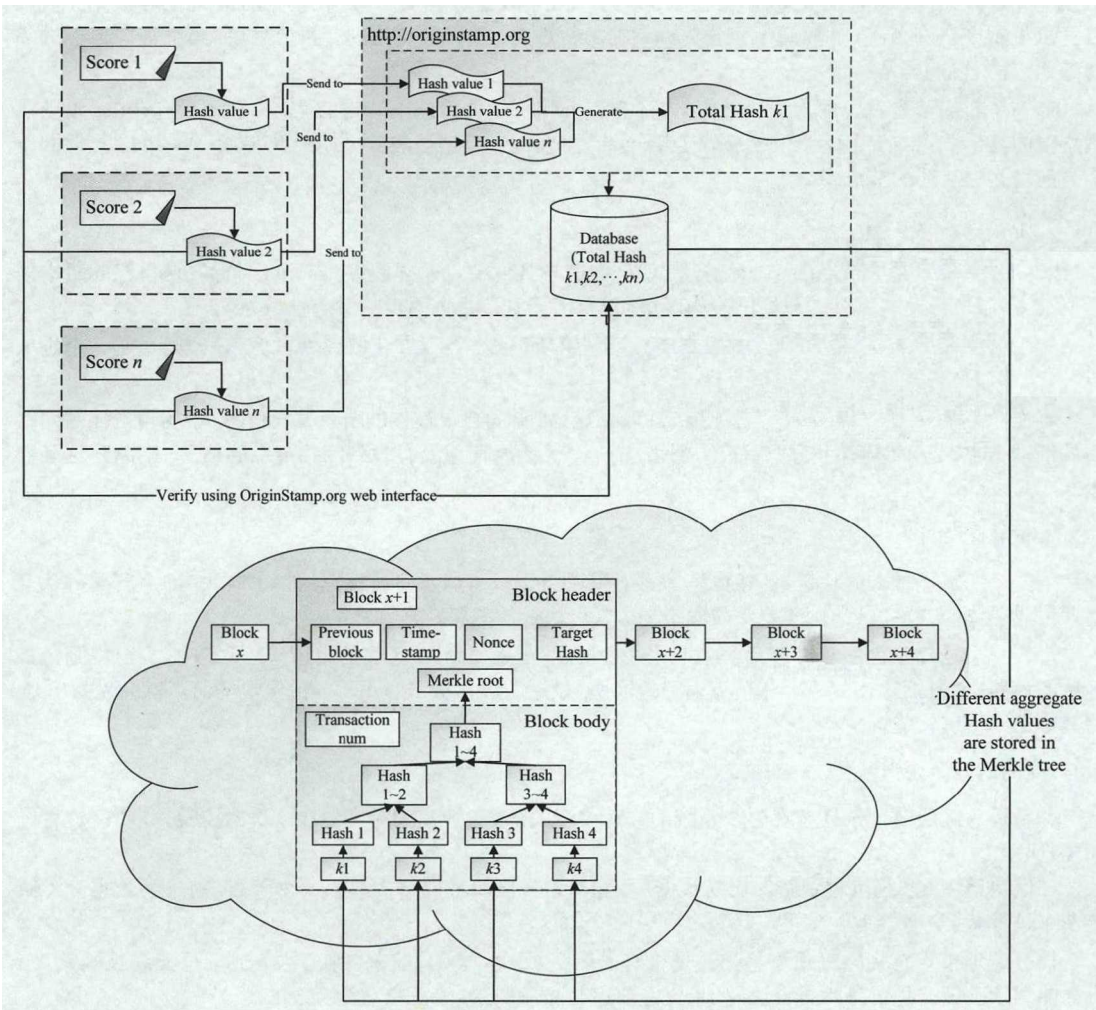


图 6 提交多个成绩示例图

Figure 6 Submit multiple sample examples

4.2.4 成绩查询模块

本文设计的基于区块链的成绩管理系统方便学生查询成绩, 用户可以使用浏览器通过 HTTP 请求来查询交易的数据, 系统中设计的数据查询接口可以方便的查询交易的数据、区块的数据、节点信息以及区块状态等信息.

对学生成绩的查询是以学生的公钥为查询条件的, 如果学生的账户没有收到来自学校的交易, 说明目前还没有录入的成绩. 如果教师已经成功提交成绩, 并且通过区块链验证, 则可以查找到学生的成绩.

4.3 P2P 网络设计

区块链的节点网络是一个 P2P 网络, 区块链网络中所有节点共同维护系统中交易和数据, 本文中区块链的网络节点由教师组成, 每个教师在网络中在网络中作为对等节点互相监督互相协作.

4.3.1 新节点加入

对于节点的初始化, 我们采取与比特币一致的方式, 即使用 DNS 的方式来查询其他节点, DNS 一般是硬编码到代码里的, 这些 DNS 服务器就会提供比特币节点的 IP 地址列表, 从而新节点就可以找到其他节点建立连接通道. 新节点与邻居节点建立连接后, 还需要进行全网广播, 让整个网络知道该节点的存在. 以泛洪机制向全网节点广播, 该节点首先向邻居节点广播, 邻居节点收到广播消息后, 再继续向自己的邻居节点广播, 以此类推.

当一个新的节点需要加入区块链网络时, 首先会随机地向系统中写定的 DNS 节点发起请求, 以获取网络中的其他节点. 若得不到回应, 新节点会不断发起请求, 直到被响应, 并且相应节点会向新节点返回一个当前网络中活动的节点 IP.

4.3.2 节点连接

新节点接收到其他节点的 IP 地址后, 就会尝试与其他节点建立连接, 向连接目标发送自己的版本信息, 包括节点自身的版本号、已经同步的区块, 以及用于确认是否同步的系统时间等.

目标节点接收到后, 会把自己的版本信息返回给新节点, 当双方获取到版本信息后, 则发送一个确认信息, 此时连接建立.

当连接确认以后, 需要定时维护连接, 每隔 30 分钟会向自己连接的节点发送信息, 证明自己还是网络中的活动节点, 这个时间间隔成为保活周期. 若三个保活周期都没有收到连接节点的信息, 则断开这条连接.

4.3.3 区块初始化

当一个新节点加入区块链网络时, 其本地存储的链上只有用于身份标识的创世区块, 节点若想确认交易并生成区块的完整节点, 则需要下载网络中最长区块链的完整数据.

当新节点连接上区块链网络后, 随机向网络中的节点发出同步区块的申请, 重复多次, 直至得到全部区块的内容, 并且通过比较网络中节点返回的区块, 发送与大多数节点不一样的区块的节点就会显露出来, 将其标记为不可信节点.

4.4 交易写入区块链

交易写入区块链这一环节在整个系统的设计中至关重要, 涉及到对交易和区块的校验和审核, 流程图如图7所示.

在区块链中, 系统接收到新的交易数据后, 随机地在区块链网络中寻找一个节点, 将交易数据分配给该节点进行验证.

被分配地节点首先要确认这笔交易是否有前序交易, 若有前序交易, 则必须等到前序交易被确认, 节点才能继续验证交易自身是否合法. 如果没有前序交易, 则直接验证交易是否合法.

接着节点验证交易自身的合法性, 若交易合法 [7], 则生成新区块, 并把新区块在全网广播, java.net 包中提供了 MulticastSocket 类, 其 send 方法可以将数据以广播的方式发送给网络中的所有主机, 等待全网投票. 如果这个交易不合法, 则直接丢弃.

当交易打包进区块全网投票, 每个投票节点列表中需包含投票节点的公钥, 投票结果, 投票时间点的时间戳, 以及产生该投票的节点提供的签名信息, 节点签名由 Signature 类实现, 签名前调用 initSign 和 update 方法初始化签名并更新数据, 执行 sign 方法即可获取签名字节数组签名, 校验前同样需要初始化和更新数据, 调用 verify 方法验证签名, 返回校验结果. 若同意的票数超过全网节点的 50%, 则把该区块标记为合法区块. 若区块不合法, 就把这个区块标记为不合法, 并且提取区块中的合法交易, 重新认证并打包进入新的区块.

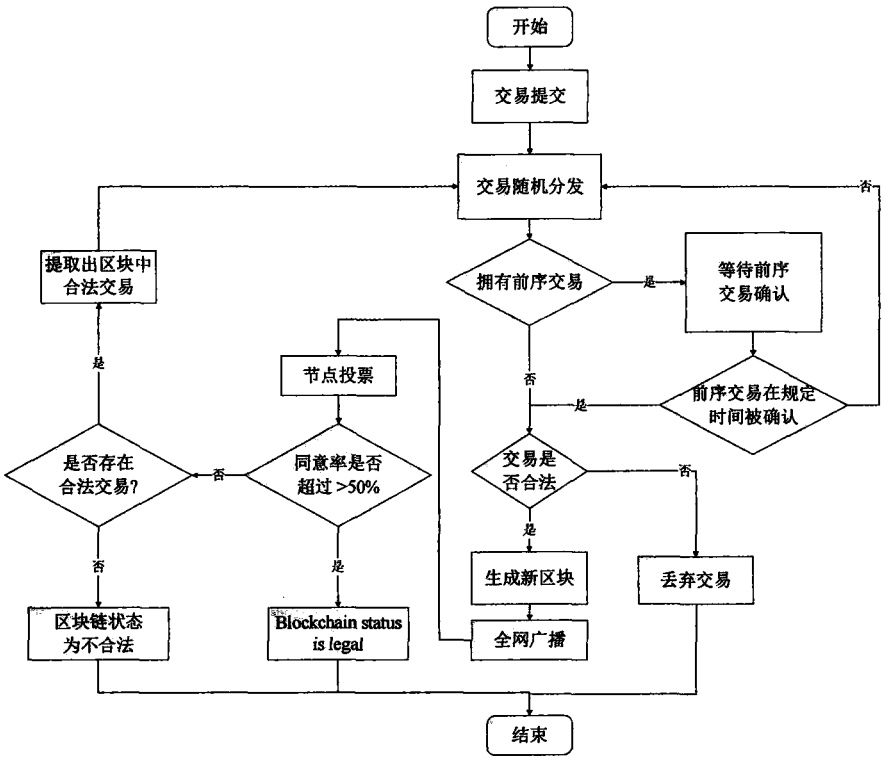


图 7 交易写入流程图

Figure 7 Transaction write flow chart

5 系统性能分析

系统性能分析主要考虑系统功能在运行过程中能够达到指标, 对于一个完备的系统而言, 性能需求分析十分重要.

5.1 易用性指标分析

基于区块链技术的高效管理平台的设计目的在于提高高校成绩管理的效率, 该系统贴近实际的应用流程, 对于学生而言, 与中心化系统的操作大同小异, 符合他们的操作习惯. 高校师生都具有一定的计算机操作水平, 使用起来没有困难, 满足系统易用性要求.

5.2 可扩展性指标分析

基于区块链的高校成绩管理平台的设计是以当前需求为目标的, 由于校园成绩管理可能有新的规定、内容扩充, 为适应系统变化, 系统需要具备良好的可扩展性. P2P 网络架构本身就具有良好的可扩展性, 即便日后增加新模块也不会对原有系统架构和功能模块造成太大的影响, 能够根据需求对系统的功能进行扩展.

5.3 健壮性指标分析

P2P 架构天生具有耐攻击、高容错的优点. 由于服务是分散在各个节点之间进行的, 部分节点或网络遭到破坏对其它部分的影响很小. P2P 网络一般在部分节点失效时能够自动调整整体拓扑, 保持其它节点的连通性. P2P 网络通常都是以自组织的方式建立起来的, 并允许节点自由地加入和离开 [12].

5.4 安全性指标分析

成绩管理系统中存储大量的学生成绩信息, 所以系统需要具备完善的安全机制. 本质上, 区块链技术是在信息不对称的情况下, 无需相互担保信任或第三方中介参与, 采用基于共识机制和加密算法的节点间普遍通过即为认可的信任机制. 共识机制和加密算法也是区块链保证数据安全, 不可篡改以及透明性的关键技术.

6 结论

本文提出利用去中心化的区块链技术, 为成绩管理系统提出一个安全、防篡改的管理系统, 解决了传统的 B/S 模式下的安全性问题. 本文采取的途径是教师通过系统将学生成绩提交, 系统将学生的成绩进行 Hash, 并且利用时间戳服务 OriginStamp 的 API 将 Hash 后的结果嵌入区块链中. P2P 网络和区块链技术为系统提供一个安全稳定的运行环境, 区块链中的数据受到整个网络的管理和监控, 可以有效地防止随意篡改和破坏.

对于利用区块链对数据进行保护还可以在其他方面得到应用, 如智能家居物联网设备的安全隐私问题等各方面. 在未来的工作中, 我们会更对区块链进行更加深入的研究, 将其应用在更多领域.

References

[1] LUU L, NARAYANAN V, ZHENG C, et al. A secure sharding protocol for open blockchains[C]. In: Proceedings of ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016: 17–30. [DOI: 10.1145/2976749.2978389]

[2] KARAME G. On the security and scalability of Bitcoin's blockchain[C]. In: Proceedings of ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016: 1861–1862. [DOI: 10.1145/2976749.2976756]

[3] TSAI W D, YU L, WANG R, et al. Blockchain application development techniques[J]. Journal of Software, 2017, 28(6): 1474–1487. [DOI:10.13328/j.cnki.jos.005232]
蔡维德, 郁莲, 王荣, 等. 基于区块链的应用系统开发方法研究 [J]. 软件学报, 2017, 28(6): 1474–1487. [DOI:10.13328/j.cnki.jos.005232]

[4] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. https://bitcoin.org/bitcoin.pdf. 2008.

[5] BÖHME R, CHRISTIN N, EDELMAN B, et al. Bitcoin: Economics, technology, and governance[J]. Journal of Economic Perspectives, 2015, 29(2): 213–238. [DOI: 10.1257/jep.29.2.213]

[6] PUTHAL D, MALIK N, MOHANTY S P, et al. The blockchain as a decentralized security framework [Future Directions][J]. IEEE Consumer Electronics Magazine, 2018, 7(2): 18–21. [DOI: 10.1109/MCE.2017.2776459]

[7] KRAFT D. Difficulty control for blockchain-based consensus systems[J]. Peer-to-Peer Networking and Applications, 2016, 9(2): 397–413. [DOI: 10.1007/s12083-015-0347-x]

[8] TSCHORSCH F, SCHEUERMANN B. Bitcoin and beyond: A technical survey on decentralized digital currencies[J]. IEEE Communications Surveys & Tutorials, 2016, 18(3): 2084–2123. [DOI: 10.1109/COMST.2016.2535718]

[9] YUAN Y, WANG F Y. Blockchain: The state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481—494. [DOI: 10.16383/j.aas.2016.c160158]
袁勇, 王飞跃. 区块链技术发展现状与展望 [J]. 自动化学报, 2016, 42(4): 481—494. [DOI: 10.16383/j.aas.2016.c160158]

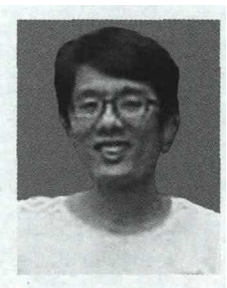
[10] KOSBA A, MILLER A, SHI E, et al. HAWK: The blockchain model of cryptography and privacy-preserving smart contracts[C]. In: Proceedings of 2016 IEEE Symposium on Security and Privacy (SP). IEEE, 2016: 839–858. [DOI: 10.1109/SP.2016.55]

[11] CHRISTIDIS K, DEVETSIKIOTIS M. Blockchains and smart contracts for the Internet of Things[J]. IEEE Access, 2016, 4: 2292–2303. [DOI: 10.1109/ACCESS.2016.2566339]

[12] FELD S, SCHÖNFELD M, WERNER M. Analyzing the deployment of Bitcoin's P2P network under an AS-level perspective[J]. Procedia Computer Science, 2014, 32: 1121–1126. [DOI: 10.1016/j.procs.2014.05.542]

作者信息

孙韵秋 (1995–), 江苏淮安人, 硕士生在读. 主要研究领域为区块链.
yunqiu_sun@163.com



王启春 (1980–), 江苏射阳人, 博士, 副教授. 主要研究领域为对称密码、布尔函数.
qcwang@fudan.edu.cn