# 2022年全国大学生信息安全竞赛安徽省赛

# 信息安全作品赛道

# 作品报告

作品名称：基于区块链的文件著作保护系统

# 填写说明

1.所有参赛项目必须为一个基本完整的设计。作品报告书旨在能够清晰准确地阐述（或图示）该参赛队的参赛项目（或方案）。

2.作品报告采用A4纸撰写。除标题外，所有内容必需为宋体、五号字、1.5倍行距。

3.作品报告中各项目模板文字部分仅供参考，作品报告书撰写完毕后，请删除所有模板文字。(本页不删除)

4.作品报告模板里已经列的内容仅供参考，作者可以在此基础上增加内容或对文档结构进行微调。

5.网评采用双盲评审，因此请勿在该文档中出现任何有关学校、队伍、个人等的信息，否则按作弊论处。

6．如果能通过网评参加决赛，请在决赛之前对作品进行完善，并对作品报告完善后再在竞赛系统中上传。具体时间要求请参考组委会发布的通知。

# 摘要

针对当前著作权保护时等级成本过高和登记证明效力低等问题，提出了一种基于区块链的文件著作保护系统。首先，用户上传一份文件由本地服务器接收到后，使用共识算法pow生成区块，区块包含当前区块的哈希值，前一个区块的哈希值以及生成区块的时间戳，引入Hash算法对用户数据进行单向数据Hash加密，通过与时间戳结合，构建不可篡改的区块链数据，然后再将得到的哈希值通过Gossip协议广播给每一位用户，并运用redis分布式数据库储存起来。且在查询用户文件的过程中，通过上传文件的hash值，运用字典树查询方式以方便用户查找。

关键词：著作权保护；区块链；共识算法；Gossip协议；分布式数据库；字典树查询方式

目录

[2022年全国大学生信息安全竞赛安徽省赛 1](#_Toc120905245)

[信息安全作品赛道 1](#_Toc120905246)

[作品报告 1](#_Toc120905247)

[填写说明 2](#_Toc120905248)

[摘要 3](#_Toc120905249)

[基于区块链的文件著作保护系统 5](#_Toc120905250)

[第一章作品概述 5](#_Toc120905251)

[1.1背景介绍 5](#_Toc120905252)

[1.1.1当前著作权保护制度的不足 5](#_Toc120905253)

[1.1.2当今应对知识产权的方法 6](#_Toc120905254)

[1.1.3区块链技术对著作权的必要性 6](#_Toc120905255)

[第二章作品设计 8](#_Toc120905256)

[2.1系统概述 8](#_Toc120905257)

[2.1.1系统功能 8](#_Toc120905258)

[2.2技术原理 8](#_Toc120905259)

[2.2.1区块链运用 8](#_Toc120905260)

[2.2.2分布式存储 9](#_Toc120905261)

[2.2.3字典树查询技术原理 9](#_Toc120905262)

[2.2.4Gossip协议 9](#_Toc120905263)

[第三章作品测试与分析 10](#_Toc120905264)

[3.1测试环境 10](#_Toc120905265)

[3.2实验数据 11](#_Toc120905266)

[3.3服务端客户端的开启和区块链的构建 13](#_Toc120905267)

[3.4基于字典树索引和普通索引算法间的性能测试 15](#_Toc120905268)

[第四章创新性说明 16](#_Toc120905269)

[4.1实现了大数据时代的个人著作信息保护 16](#_Toc120905270)

[4.2使用共识算法pow 16](#_Toc120905271)

[4.3基于字典树的数据库检索方式 17](#_Toc120905272)

[第五章总结 18](#_Toc120905273)

[5.1作品技术难点 18](#_Toc120905274)

[5.1.1基于字典树的数据库检索方式 18](#_Toc120905275)

[5.1.2区块链的实现 19](#_Toc120905276)

[5.1.3共识算法的实现 20](#_Toc120905277)

[5.2作品应用前景 20](#_Toc120905278)

[参考文献 0](#_Toc120905279)

# 基于区块链的文件著作保护系统

# 第一章作品概述

## 1.1背景介绍

### 1.1.1当前著作权保护制度的不足

1.著作权等级成本过高

著作权登记成本主要包括两个方面，一是以作品作者角度出发而产生登记成本，二是以行政机关角度出发而产生的登记管理成本。

（1）作者成本

从作品作者角度出发，著作权登记的成本主要为登记的费用成本以及登记所耗费的时间成本。在登记费用成本上，虽然在“互联网+”时代著作权登记的渠道越来越多，但是登记的费用标准参差不齐。以原创文字作品为例，根据《中国版权保护中心著作权自愿登记收费标准》与《使用文字作品支付报酬办法》的规定，可以得到不同字数下原创文字作品的登记费用及基本稿酬。作者的登记成本除了登记费用成本之外，还有登记时间成本。现阶段我国的作品著作权登记流程仍然过于繁杂，需要经历注册、在线填报、受理申请、受理通知、审查、发证六个流程。我国作品著作权登记的周期约为30个工作日，如此漫长的登记周期与现代快节奏的出版模式不相兼容。举例来说，对出版商而言，由于较长的登记周期与较短的出版周期间存在矛盾，导致经济效益滞后，从而使按件计费的出版商难以负担高昂的登记费用。

（2）管理成本

著作权登记的管理成本主要为人工审核成本与信息管理成本。著作权登记实际上是为了实现其财产权利而构筑的“篱笆”，将财产权利从公共领域中隔离出来，从而确立财产权利的边界。构筑财产权利边界的行政成本看似不是施加在著作权作者的财产权上的成本，其实行政成本仍然通过税收转化为公共成本，造成社会的经济资源总价值减少，变相增加了该财产权的成本负担。现阶段我国著作权登记过程中，由于作品数量的众多，著作权登记的审查仍然是一项消耗社会资源的任务。

2.登记证明效力低

由于现行著作权登记主要采用形式审查而非实质审查模式，所以在大量著作权纠纷案件中，权利证书并不能作为决定著作权归属的决定性证据。当事人提供的各种文件均可以成为确定著作权归属的初步证据，例如合同、底稿、权利人申明、作品原件等。这与不动产纠纷案件中，产权证书具有一锤定音的证明力大不相同。

### 1.1.2当今应对知识产权的方法

在网络上发表作品的作者，一般都需要利用相关网站服务商提供的服务和平台，比如注册成为某论坛的用户、使用网站的邮箱、使用网站提供的个人主页或空间。因此，如果法院认为网络著作权人自行出具的电子资料可信度低，则可以对网络服务商进行取证，要求网络服务商提供能够证明该著作权人的相关信息，如用户名、注册信息、邮箱地址等。而当今网络上对著作权保护如目前较为流行的数字水印、电子签名等，它们虽有着标识自己作品的优势，但都缺乏一些证据效力

### 1.1.3区块链技术对著作权的必要性

1.“去中心化”以及降低登记成本

由于我国现有著作权登记模式是以中国版权保护中心为主，各地版权中心分散登记的模式，重复登记、登记系统重复建设等情况时有发生。加之各地登记机构人员较少，登记作品数量庞大，导致登记成本较高。而区块链的“去中心化”特征则能显著改善“中心化”登记的不足。首先，“去中心化”有效解决了登记数据的管理问题，因为登记数据不会因为一个节点的失灵而导致整个区块链数据毁损灭失，而且不会因为作品数量的增加而不断需要对登记系统进行升级维护；其次，对于著作权人来说，整个登记过程方便快捷，对于登记数据上链则通过汇聚各节点的算力来完成，节省了著作权人大量的登记时间成本，也不会因为登记时间而影响到著作权的财产效益。

2.时间戳与哈希值技术提高证据证明效力

在著作权纠纷案件中，著作权所有证明的证据是决定案件走向的关键因素。由于我国现行著作权登记采用形式审查而非实质审查，著作权登记证书只能作为著作权所有的初步证明。其次，由于互联网的公开性以及手机端、APP、自媒体的发展，导致作品一经上传就面临着极大的盗版风险。作品一旦被盗版后，会在短时间内形成庞大的复制品数量，极大增加了著作权所有人的证明难度。另外，现在许多作者在互联网使用笔名或匿名，使得这些作者在证明作品著作权归属时无法拿出决定性证据。例如“《见与不见》著作权纠纷案”中，原告谈笑靖于2007年5月15日使用扎西拉姆·多多的笔名在自己的博客日志中创作了《班扎古鲁白玛的沉默》这首小诗，却被《读者》杂志及其后的珠海出版社认为是仓央嘉措所写的一首《见与不见》情诗，在诉讼中，谈笑靖出示了大量证据证明博客归属、创作日期、维权邮件等证据才证明自己是这首诗的著作权所有者。

相对于数字水印与电子签名技术，区块链的优势在于其证据有力性，在同样的抄袭案例中，对于数字水印等技术，其没有充分证据标识作者，而区块链技术中的时间戳技术和哈希算法则可以解决证据证明力的问题。由于作品文件占用较大的存储空间，在区块链中将作品上传是不可能的，故文本、音乐、视频等作品将通过哈希函数转换为64位或者256位的哈希值，最终将这些数据容量极小的哈希值上传至区块链中。区块链的每个节点虽然都可以看到这些作品的哈希值，但无法通过计算机终端将哈希值转换为文本、音乐或者视频，这是一个不可逆的过程，这将有效降低互联网盗版的规模。此外，当哈希值上传至区块链中时，会在生成的新块的块头中加盖时间戳，以便每个区块按照时间顺序排列。由于哈希值与时间戳的不可逆性和不可篡改性，其作为证明著作权作者的证据具有很高的可信度。

# 第二章作品设计

## 2.1系统概述

### 2.1.1系统功能

本系统由五个部分组成（见下图1），核心部分是区块链技术的实现，pow共识算法的实现，RSA和AES加密算法的结合实现，字典树检索个人著作信息。本系统主要运用。python在pycharm（2022version）平台上进行开发。用户在客户端填写个人信息，并提交个人文件，服务端进行接受对客户的文件，个人信息，时间戳一起进行哈希加密放入数据库中进行存储，并以哈希值构建字典树结构方便后期进行查询。服务端收到的文件将会进行区块生成，每个区块都记录着一个文件著作的归属权，上面记载着上一个区块的哈希值，当前区块的哈希值，和生成区块的时间戳，能够证明某个用户的文件著作归属权。当用户的文件著作已经在区块链登记过后想要进行查询可以通过生成区块时的区块哈希值进行字典树查找。

## 2.2技术原理

### 2.2.1区块链运用

用户创作了一篇文章，并将相应的数字文件上传到某一个区块链版权登记系统中，这个系统会登记申请人信息及存证内容摘要，同时为你的数字文件生成一个全网唯一标识的哈希码（这种标识与文件的每一个字节相关从而无法被伪造），之后将这些信息记录到某一个区块链中进行全网节点的同步，并为你生成一份独特的区块链版权证书，这时相应的版权登记及存证工作便初步完成了。具体实现为用户上传一份文件由本地服务器接收到后，使用共识算法pow生成区块，区块包含当前区块的哈希值，前一个区块的哈希值以及生成区块的时间戳，为防止区块链的区块数据被篡改，引入Hash算法对用户数据进行单向数据Hash加密，生成固定长度的字符串，通过与时间戳结合，构建不可篡改的区块链数据。具体结构见图2-1

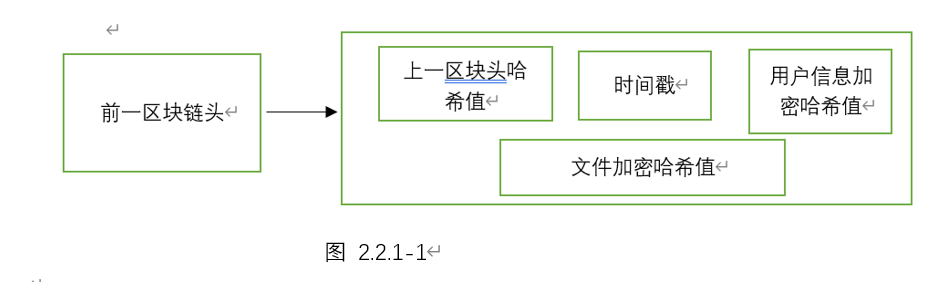


图2-1

### 2.2.2分布式存储

每个节点都保存有完整的数据库拷贝，全网节点的权利和义务均等，系统中的数据由全网中的节点采用点对点传输，共同存储、更新和维护[8]；因此，与传统中心化的网络相比，不存在单个中心被攻击，整个网络数据都被破坏的缺点。而解决存储时分布式一致性问题的方式是工作量证明，既共识机制。

共识机制本质是基于可靠性高的节点对区块进行验证的算法，选取PoW共识机制算法。PoW算法可以为整个系统节约大量的算力，并提高运算效率，同时使区块生成的时间大幅度减少。PoW共识算法主要是通过计算难度值来决定谁来出块。PoW的工作量是指方程式求解，谁先解出来，谁就有权利出块。方程式是通过前一个区块的哈希值和随机值nonce来计算下一个区块的哈希值，谁先找到nonce，谁就能最先计算出下一个区块的哈希值，这种方式之所以被称为计算难度值是因为方程式没有固定解法，只能不断的尝试，这种解方程式的方式称为哈希碰撞，是概率事件，碰撞的次数越多，方程式求解的难度就会越大。分布式存储结构见下图2-2

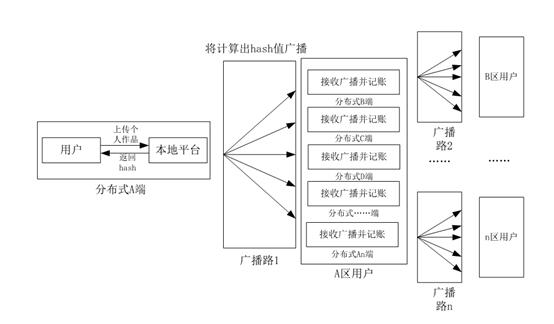


图2-2

### 2.2.3字典树查询技术原理

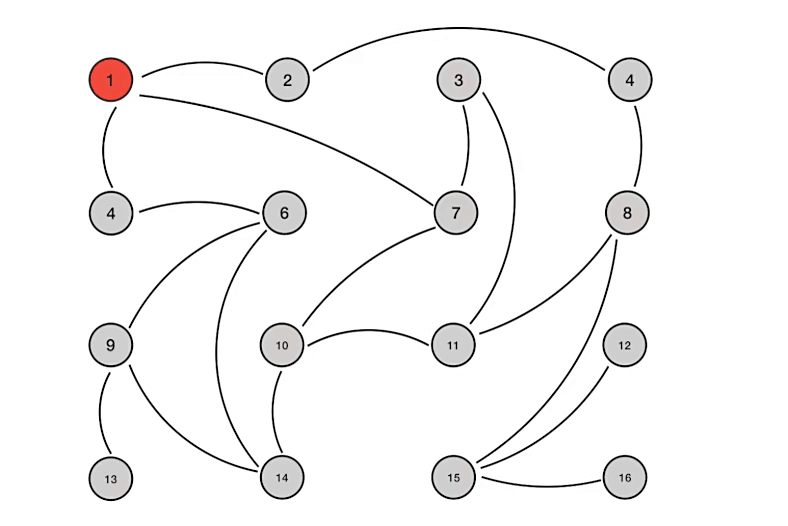
Trie树，是一种树形结构，是一种哈希树的变种。典型应用是用于统计，排序和保存大量的字符串（但不仅限于字符串），所以经常被搜索引擎系统用于文本词频统计。使用用户生成的哈希值构建trie树，方便日后用户对于文件版权的查找。

### 2.2.4Gossip协议

Gossip 过程是由种子节点发起，当一个种子节点有状态需要更新到网络中的其他节点时，它会随机的选择周围几个节点散播消息，收到消息的节点也会重复该过程，直至最终网络中所有的节点都收到了消息。这个过程可能需要一定的时间，由于不能保证某个时刻所有节点都收到消息，但是理论上最终所有节点都会收到消息，因此它是一个最终一致性协议。如果用数学解释该理论，那就是，若每个人平均认识260人，其六度就是260↑6 =1,188,137,600,000。消除一些节点重复，那也几乎覆盖了整个地球人口若干多倍，这也是Gossip协议的雏形。

Gossip协议基本思想就是：一个节点想要分享一些信息给网络中的其他的一些节点。于是，它周期性的随机选择一些节点，并把信息传递给这些节点。这些收到信息的节点接下来会做同样的事情，即把这些信息传递给其他一些随机选择的节点。一般而言，信息会周期性的传递给N个目标节点，而不只是一个。这个N被称为fanout（这个单词的本意是扇出）。

Gossip协议的主要用途就是信息传播和扩散：即把一些发生的事件传播到全世界。它们也被用于数据库复制，信息扩散，集群成员身份确认，故障探测等。



# 第三章作品测试与分析

本项目针对区块链个人著作信息保护的实现两个不同版本，一个是基于普通索引检索的数据库，一种是基于字典树的数据库检索

## 3.1测试环境

|  |  |
| --- | --- |
| 项目 | 配置参数 |
| 操作系统 | WindowsFeatureExperiencePack120.2212.4180.0 |
| CPU | Intel(R)Core(TM)i7-10510UCPU@1.80GHz2.30GHz |
| 内存 | 8.00GBRAM |
| 磁盘 | 200G |
| 网络连接 | 以太网 |

## 3.2实验数据

实验中使用的用户数据是我们使用python随机生成的，数据中包含用户的个人信息和其所拥有著作的文件。(图3-1)其中10个用户的数量级，总文件大小11.2KB，100个用户的数量级，总文件大小为133KB，1000个用户的数量级，总文件大小为1.37MB，10000个用户的数量级，总文件大小为13.7MB，100000个用户的数量级，总文件大小为137MB,人物信息与文件信息如下图(图3-2，3-3)

|  |  |
| --- | --- |
| 用户数 | 文件集大小 |
| 10 | 11.2KB |
| 100 | 133KB |
| 1000 | 1.37MB |
| 10000 | 13.7MB |
| 100000 | 137MB |

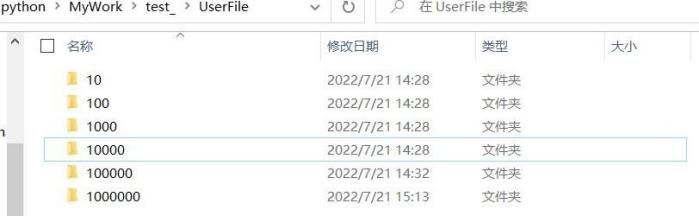


图3-1

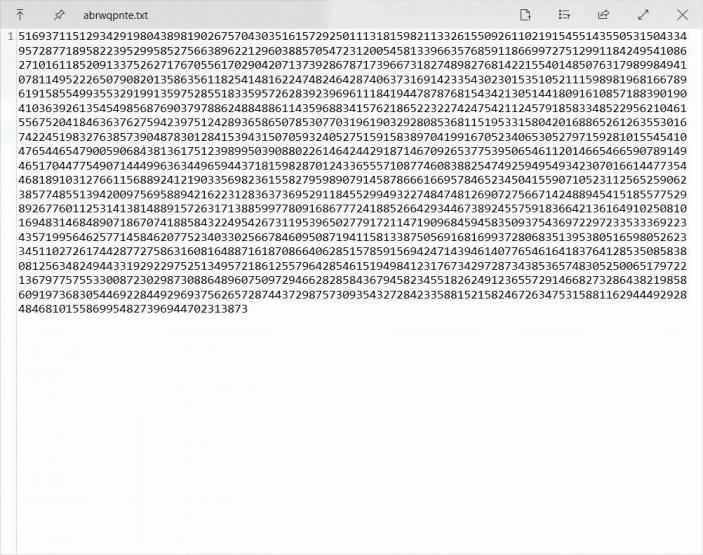


图3-2用户文件内容

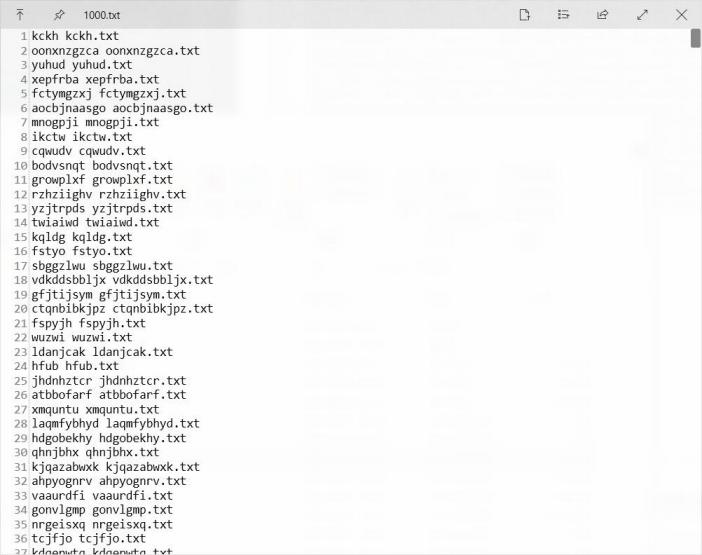


图3-3用户文件信息

## 3.3服务端客户端的开启和区块链的构建

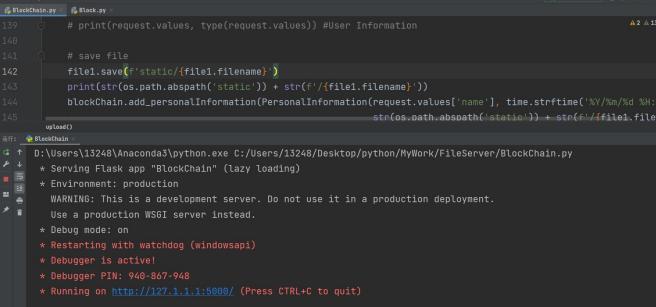
首先打开pycharm使用flask模拟服务端,使用电脑中的http://127.1.1.1:5000/端口充当服务器，供客户们获取区块链信息，和上传区块链。

图3-3-1服务器界面

在运行testfile.py程序模拟用户上传区块,每个用户上传完区块都能获得代 表自己文件著作唯一的 hash 值来确定自己的著作所有权，在通过testinformation.py验证的时候也是通过该hash值来查询个人信息



图3-3-2上传区块界面

下图是端口网页中每位用户的区块链显示结果



客户端上传的文件都会存储在服务器文件中的static/目录下，上传文件的端口为http://127.1.1.1:5000/upload/如下图

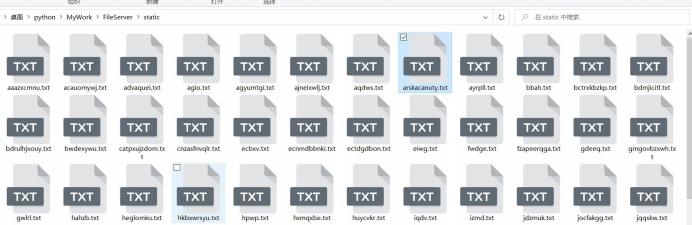


图3-3-3区块链显示结果

## 3.4基于字典树索引和普通索引算法间的性能测试

|  |  |  |  |
| --- | --- | --- | --- |
| 用户数 | 总文件大小 | 字典树查找 | 普通查找 |
| 10 | 11.2KB | 0.026343100000000064s | 0.02816810000000003s |
| 100 | 133KB | 0.2951456s | 0.3109219s |
| 1000 | 1.37MB | 3.1406598000000017s | 3.178538599999996s |
| 10000 | 13.7MB | 36.468672000000026s | 47.787770300000034s |
| 100000 | 137MB | 1412.4293027000003s | 2547.3840185999998s |

图3-4中对比了字典树查询方式和线性查询方式每次插叙所花费的时间开销，从图中可以看出在数据越大的情况下，字典树的查询的优势就越明显，虽然字典树在建树的时间花费\*\*O(n\*log(n))的复杂度，Trie树的平均高度h为len，所以Trie树的查询复杂度为O(h)=O(len)。好比一棵二叉平衡树的高度为logN，则其查询，插入的平均时间复杂度亦为O(logN)，在越大的数据直线这种查询方式的速度优势就越明显，可以在图中看到在用户数据达到1e5时字典树的平均每次查询只需要0.015s,而线性查询要0.025s，接近字典树查询的一倍。

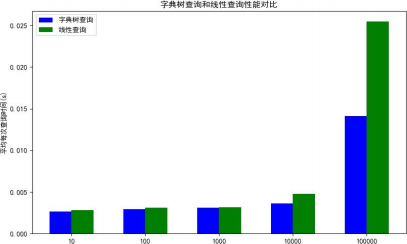


图3-4线性和字典树查询性能对比

# 第四章创新性说明

本作品创新性的提出了“基于字典树的数据库检索方式”，旨在大数据时代实现个人著作信息的保护，并且使用了共识算法使每个节点都可共享相同的数据副本，利用查询效率快的字典树搜索相关信息,并且还使用了拜占庭BFT算法，为了防止分布式系统造成的故障，而采用这种算法。

## 4.1实现了大数据时代的个人著作信息保护

“大数据”时代的概念最早由世界的著名的咨询公司麦肯锡提出。麦肯锡说：“数据已渗透到今天的每个行业和业务功能领域，并已成为重要的生产要素。随着新一轮的生产力增长和消费者盈余浪潮的到来，海量数据的挖掘和使用预示着“大数据”已经存在于物理学，生物学，环境生态学等领域以及军事，金融，通信等行业，但是由于近年来互联网的发展，信息产业的发展才引起了人们的关注。而在大数据时代下的个人著作信息保护愈来愈收到重视，网络环境纷杂，一个最简单有效的方法就是基于区块链技术，实现作品上链存证确权，上传作品进行存证操作即可出具版权存证电子证书，为版权保护提供技术支持。每一位个体在搜索引擎上的任何一次搜索形成的数据都会被记录下来，这些数据在不断积累、汇集的过程中，逐渐成了“大数据”。大数据的定义很多学者已经给出，但表述各不相同。综合来看，大数据就是数据量大、数据类型多的数据集合，同时传统的数据处理技术及IT技术无法对该数据集进行采集、获取、处理等操作。用户最能切身感受到的大数据表现相关。

## 4.2使用共识算法pow

共识机制是区块链的核心基石，是区块链系统安全性的重要保障。区块链是一个去中心化的系统，共识机制通过数学的方式，让分散在全球各地成千上万的节点就区块的创建达成一致的意见。共识机制中还包含了促使区块链系统有效运转的激励机制，是区块链建立信任的基础。Proof-of-Work简称PoW，即为工作量证明通过计算一个hash值，通过是否是正确Hash值之后，就会判断文件是否被篡改，也就确保了整个系统的安全

共识算法pow最大的优点可归纳为:

◼算法简单，容易实现，节点可自由进入，去中心化程度高。

◼破坏系统需要投入极大的成本，安全性极高。

◼区块生产者的选择通过节点求解哈希函数实现，提案的产生、验证到共识的最终达成过程是一个纯数学问题，节点间无需交换额外的信息即可达成共识，整个过程不需要人性的参与。

◼为了保证去中心化程度，区块的确认时间难以缩短。

◼没有最终性，需要检查点机制来弥补最终性，但随着确认次数的增加，达成共识的可能性也呈指数级地增长。

## 4.3基于字典树的数据库检索方式

字典树又称单词查找树，Trie树，是一种树形结构，是一种哈希树的变种。典型应用是用于统计，排序和保存大量的字符串(但不仅限于字符串)，所以经常被搜索引擎系统用于文本词频统计。它的优点是：利用字符串的公共前缀来减少查询时间，最大限度地减少无谓的字符串比较，查询效率比哈希树高。

正因如此，在数据库检索过程中，我们通过查询效率极快的字典树快速的搜索到我们需要的信息，在进行著作信息保护时，需保护的信息将第一时间搜索出来，然后对其进行后续处理。

我们的构建步骤大概是这样的：

1、维护字符串集合(即字典)。

2、向字符串集合中插入字符串(即建树)。

3、查询字符串集合中是否有某个字符串(即查询)。

4、统计字符串在集合中出现的个数(即统计)。

5、将字符串集合按字典序排序(即字典序排序)。

6、求集合内两个字符串的LCP(LongestCommonPrefix，最长公共前缀)(即求最长公共前缀)。

查询操作和刚刚的思路大同小异，因为我们已经有了一个“虚拟全树”，那么我们还是按深度向下迭代，对于需要查询的字符串的当前字符，如果这个对应的字符指针为空，就说明不含这个单词直接跳出即可，当我们都迭代完成之后，直接返回即可。

# 第五章总结

[区块链](https://www.zhihu.com/search?q=%E5%8C%BA%E5%9D%97%E9%93%BE&search_source=Entity&hybrid_search_source=Entity&hybrid_search_extra=%7B%22sourceType%22%3A%22answer%22%2C%22sourceId%22%3A158086555%7D)版权之所以能保护原创，是因为它能解决目前原创环境下最迫切的痛点，它在现下的所有版权维权场景中都能适用，因而具有一定的法律效力。区块链的去中心化结构能解决一些中心化服务器面临的隐私泄露问题，每个区块记录着本区块的hash值和上一个区块的hash值，我们算出每一个文件的hash值，如果文件被篡改，那么对应的文件hash值就会被改变，通过文件hash值是否改变，就可以判断出此文件是否被修改，被何人何时修改。

本项目研究了文件著作保护系统的构建方法，我们通过在网上大量搜集相关文件著作保护的资料，以及其他与此相关的讨论，我们总结了一些经验，了解了当下的一些不足之处，并再次基础上改进、创新，增加了我们自己的想法并努力去实现了我们的想法。提出了基于区块链的文件著作保护系统方案，并设计了一套可应用在实践中的文件著作保护系统，此方案用python代码实现，在Flask框架测试通过，我们通过对图片加入噪声，进行裁剪，以及对密钥敏感性的测试等都成功的实现了，并且可以通过网页访问运行。证明了本次方案的有效性。

本项目的关键步骤如下：

1)基于区块链的去中心化；

2)基于字典树的数据库检索方式；

3)不可篡改性；

4)hash函数的应用；

5)Flask框架的搭建；

6)本项目系统在网页上的搭建和运行；

7)客户端界面和后端程序的实现。

## 5.1作品技术难点

### 5.1.1基于字典树的数据库检索方式

字典树也叫Trie树、前缀树。顾名思义，它是一种针对字符串进行维护的数据结构，类似于如下图这样一种结构。他有ABC，ABD，BA,BC,AB,这么多中数据可以存储，而我们的用户的个人信息就是用这种方式存储。我们通过字典树可以快速的查询出是哪一位用户，在什么时间，将文件上传到区块链中的。

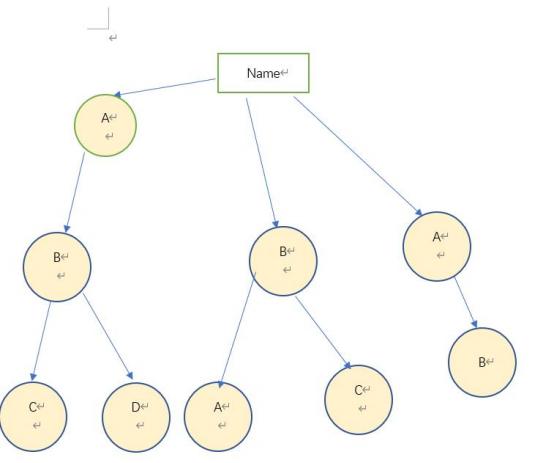


图5-1字典树检索方式

### 5.1.2区块链的实现

区块链最早出现在1991年，由一群研究人员用来给数字化文档打时间戳。以使得这些文档不能被篡改，看上去区块链技术就像一位公证人一样。我们也是用这种方法实现判断文件是否被篡改，我们每生成一个区块，我们都会给这个区块按照特定的hash算法，来得到一个hash值，一般来说，只要这个区块的index,previoushash,timestamp,data有改动，那么它所算出的hash值也会改变，所以当你想要篡改某个区块的数据时，你需要将后面所有的区块的previoushash都进行篡改。

首先我们定义区块，在一个区块中，存储着一个时间戳和一个(可选的)索引。为了保证整个区块链的完整性，每个区块有一个标记自己身份的哈希值，像莱特币，每个区块的哈希值都是由一个密码学算法根据区块的索引、时间戳、数据以及前一个区块的哈希值生成的。区块的数据可以是任何你想要的东西。

现在我们有自己的区块结构，我们需要开始把区块附加到实际的链条上。前面提到过，每个区块需要前面区块的信息，第一个区块，或者说创世区块，是一个特殊的区块，在许多情况下，这是通过手工或者一个唯一的逻辑添加上去的。它的数据值和previoushash参数是任意指定的。接下来我们需要一个函数来生成区块链里的后续区块，这个函数将链条中的前一个区块作为参数，为新的区块创建数据，并返回带有一个带有合适的数据的新区块。当新的区块哈希来自前面的区块的信息，伴随着新区块的加入，区块链的完整性也得以增强。如果我们不这么做的话，那么外界就很容易用他们的新区块来替换我们的链条里的区块，以达到“篡改历史”的目的。

### 5.1.3共识算法的实现

分布式系统是若干独立计算机的集合，这计算机对用户来说就像单个相关系统。那么我们需要时每个节点共享相同的数据副本，自然而然地也就解决了单点故障的问题。也就是每个块内都要存储所有的信息，互相牵制，相互联系，最终实现去中心化，在不同的情况下，所选择的中心不同，且每个块都可作为中心。每个块都有对应保存的hash值，同时也保存上一个块的hash值，这样以此类推，每一个块都与上一个块相互联系，从而使所有块被一张网链接起来。这样每个块都能和其他块形成联系，这样实现共识算法。这里我们采用拜占庭容错技术 (ByzantineFaultTolerance，BFT)是一类分布式计算领域的容错技术。拜占庭假设是对现实世界的模型化，由于硬件错误、网络拥塞或中断以及遭到恶意攻击等原因，计算机和网络可能出现不可预料的行为。拜占庭容错技术被设计用来处理这些异常行为，并满足所要解决的问题的规范要求。

## 5.2作品应用前景

现如今，知识产权已经成为经济全球化背景下的至高点，它能够使企业获得超额利润，已成为企业乃至国家竞争的焦点。企业研发新产品(此处指广义的产品，包括一切有形和无形的产品)必然会投入大量的人力、物力和财力，如果不对知识产权进行有效保护，那么竞争对手便会通过模仿、复制、反向工程、商业间谍等不正当手段低成本地获得知识产权，从而生产出新产品参与市场竞争。工业作为国民经济的主导，保护工业企业的知识产权问题显得尤为重要。

知识产权是权利人对所创作的智力劳动成果所享有的财产权利，其本质核心就是为了证明是谁在什么时间创作了什么样的劳动成果。但由于传统登记方式的局限性，一直存在确权难、盗版严重、公开性差等诸多问题。而区块链技术作为一种分布式账本技术，优势正是防篡改、不可逆，可靠性、可信任，去中心化、分布式、公开透明，一旦记录完成就会永远存在并且无法更改。也因此，区块链有望成为知识产权保护完美的解决方案。区块链技术目的之一是通过在数字文件和所有者身份信息上创建数字签名或者加密“Hash”，在原作与所有权信息之间建立不可磨灭的“联系”。

知识产权是整个行业面临的痛点

1.确权耗时长，时效性差，成本高

2.变现难，供需无法匹配

3.维权效率低，尤其是版权行业，举证、溯源异常困难。最为人熟知的“著作权登记”，费用高、耗时长，根本无法满足网络时代作品“产量多、传播快”的特点。

4.侵权现象严重，纠纷频发，侵蚀原创精神、行政保护力度较弱、举证困难、维权成本过高

而区块链特点(区块链没有管理员，它是彻底无中心的，数据不可篡改，去中心化，信息公开透明。)恰好解决了这些问题

如今许多侵权事件在社会上引起了舆论，例如中国知网侵权事件：中国知网未经[赵德馨](https://baike.baidu.com/item/%E8%B5%B5%E5%BE%B7%E9%A6%A8/2362356)教授本人同意，擅自转载其160多篇文章。以及前一段时间刘德华为奔驰代言的视频中对二十四节气中小满的解说词涉嫌抄袭事件。随着知识产权在大家的脑海中愈加深刻，所以保护文件著作对当今社会发展至关重要。而我们的方案就像是为每一个作品提供一个身份证，就像人们的身份证一样是独一无二的，很符合现在发展的主流。

# 参考文献

【1】基于区块链的隐私安全保护可行性分析-计算机网络论文-论文网

【2】区块链论文集/基于区块链的数据库内部攻击检测-汇智网

【3】区块链论文集/去中心化数据集市-汇智网

【4】https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf《Swirlds哈希图共识算法》

【5】区块链关键技术及其应用研究论文-经济论文-SCI论文网(scipaper.net)

【6】祝子丽.“区块链+会计”构筑产权保护防火墙[N].中国社会科学报，2019.4.12.

【7】基于区块链技术的数字知识产权保护方案研究\_民法论文\_笔耕文化传播 (bigengculture.com)

【8】陈鹏《区块链技术发展现状及面临的挑战》2019.10.30区块链技术发展与展望-知乎(zhihu.com)

【9】前瞻产业研究院《2021年中国区块链行业市场现状及发展前景分析未来市场规模有望达到万亿级别》

【10】黄建平,杨少杰,余建,陈浩.基于分布式区块链技术的供应链数据平台架构设计[J].电子设计工程,2022,30(17):45-49.

【11】刘新,胡翔瑜,徐刚,陈秀波.区块链数据保密查询的不经意传输方案[J].计算机工程:1-11.