调研背景

随着互联网，特别是移动互联网的发展，数字出版已经形成较为完整的产业链，给网络作家等相关参与方带来可观的收入。

但另一方面，侵权盗版制约着数字出版的进一步发展，各参与方都深受其害。特别是作者等内容生产商一直处于弱势地位，缺少相应的话语权和主导权，创作积极性倍受打击。面对这些问题，国家非常重视，各种政策和扶持计划频出，重拳解决版权保护难题，但是限于技术手段，很难从根本上解决。同时传统的版权保护手段非常有限。

在此背景下，区块链技术的诞生为解决版权保护带来了新的希望，其自身的分布式存储，无法篡改，可追溯等特性可以应用解决版权保护中所遇到的痛点。本次调研旨在调查目前市面上所使用区块链实现存证，版权保护相关的技术方案。为后期可能存在开发探路。

现存痛点

* **痛点之一，“版权归属”问题。**

虽然“版权自作品创作完成之时起自动产生”（依据《著作权法》的定义），但版权于何时、何地产生，由谁持有，却依然需要“被证明”。如何证明自己创作的作品，其版权是属于自己的？版权登记制度成为一个可行的方式。每一位创作者将已完成的作品提交至各地版权保护中心完成登记，实现版权信息在公信力机关的备案，这就让创作者的作品的版权归属有了依据。但复杂的流程与冗长的周期，不免让传统的版权保护方式在面对当今多样化的传播渠道和高时效性的传播手段时，显得力不从心。不少盗用者便借着创作者对版权保护流程的抵触与消极对待，肆无忌惮地侵占创作者的利益，而真正的创作者却在应对侵权时显得被动乏力。从近些年来层出不穷的版权纠纷案例来看，导致绝大多数创作者走向“侵权不期而遇，维权不了了之”的境地的主要原因可归结为：一是创作者的版权保护意识薄弱而让恶人有了可乘之机；二是缺乏一个即时、有效的版权确权平台。

* **痛点之二，当前版权保护的形式问题。**

作品的雏形、草稿，尚处于未完成状态，算不上是完整的“作品”。然而，这些素材依然具有相当高的价值，其创作理念已经能够充分反映终稿的形态。但大量创作者却忽视了对这些材料的保护，为日后遭遇侵权时无法提供有效的创作证据埋下了隐患。

* **痛点之三，如何与科技进步接轨的问题。**

随着信息的数字化、网络化程度不断加深，版权制品的载体逐步由传统的纸质稿件、实物作品转变为各种类型的数字化文档。互联网传播，作为当前版权制品的重要传播途径之一，所占比例也逐年攀升。以数字化设备创作、生产数字化作品，并且使用互联网进行发布与传播，这一方式已经脱离了传统“登记制度”的适用范畴，需要有新的方式进行补充、完善。而且，数字化作品传播速度快，可复制程度高，进一步增大了创作者的维权难度。

传统解决方案

* 公众认知确认法

　　该方法是指以公众的认知程度作为确定作者的依据。依法享有著作权的作品只要有署名，在没有相反证据证明的情况下，该署名人即推定为该作品的作者，即使该署名为笔名。只要公众根据署名可以毫无疑问地确定作者的身份，那么该署名就可以作为确认作者的依据。

* 推定代理法

　　该方法是指当网络上的作品没有署名或公众不能毫无疑问地确认笔名是谁时，将发表该作品的网站视为该作品的作者的代理人，由该网站代理作者行使署名权以外的著作权。当作者公开其身份并证实其为作者时，网站的代理权终止，网站向真正的作者交付因作品产生的利益。

* 网络注册号和密码验证法

　　该方法是利用网络注册号和密码验证的方式证明网络作品的作者身份。一般来说用户在网上发表文章、登陆各种论坛或聊天室时都要输入注册号和密码，如果他能够顺利地登陆，并能修改密码、上载文件、删除文件，在无相反证据证明的情况下，基本上可以确定他就是作者。

* 电子备案法

　　该办法是笔者在著作权备案制度上的一种想法和建议。根据我国现行的《著作权法》的规定，任何依法可以取得著作权的作品一旦完成，作者即依法享有著作权。但在多人对同一作品均主张权利，而且提供的电子原稿又无法确认作品完成时间的情况下，正确判断最先完成作品的作者是很难的。因此，笔者建议，政府主管部门或著作权集体管理组织或第三方中介机构单独或结合组成一个网络作品的备案机构，对完成的网络作品进行电子备案。在作者完成网络作品后，作者可以选择在该电子备案机构，对其享有该作品享有著作权这一事实进行备案，该备案机构在核实备案人的身份资料后给予备案。 该备案并非产生著作权的必要条件，但该备案的证明效力高于一般的证据效力，在只有电子文档作为作品原稿的情况下，该备案效力高于其他任何电子文档的证明效力，最先备案的作者就为该作品的作者。

　　尽管根据我国现行的《著作权法》的规定，该备案证明不可能作为著作权的权利凭证，但该凭证可以作为著作权的一个重要权利证明，一方面可以增加著作权交易的安全性，另一方面，随着该备案方法的不断被认知，备案作品不断增加，也会促使真正的作者在完成作品的第一时间就进行备案，这样该备案证明最终可以成为判断谁最先完成作品的最有效证明。

传统解决方案的局限

* 不够精确，容易出错。
* 基于中心化的网站，容易遭受攻击；另外，中心化的网站，一般都可以人为操纵，没有严格可信的可追溯性，给调查取证带来严重问题；
* 最为人熟知的“著作权登记”，因其费用高、费时长，也无法满足网络时代作品“产量多、传播快”的特点

区块链在版权保护方面的特点

* 分布存储：区块链处于P2P网络之中，无论什么公链、私链，还是联盟链，都要采取分布式存储，使用一种机制保证区块链的同步和统一;
* 公开透明：每个节点都有一个区块链副本，区块链本身没有加密，数据可以任意检索和查询，甚至可以修改（改了也没用）;
* 无法篡改：这是加密技术的巧妙应用，每一区块都会记录前一区块的信息，并实现验证，确保无法篡改。这里的无法篡改不是不能改，而是局部修改的数据，无法通过验证，要想通过验证，必须修改整个区块链，这在理论上可行，操作上不可行;
* 方便追溯：区块链是公开的，从任一区块都可以向前追溯，直到第一个区块，并通过区块查到与之关联的全部交易

区块链所能解决的版权相关痛点

* 记录所有环节。在所有涉及版权的使用和交易环节，区块链都可以记录下使用和交易痕迹，并且可以看到并追溯它们的全过程，直至最源头的版权痕迹。
* 去中心化。它打破了现在的从单点进入数据中心去进行版权确权的模式。区块链技术可以实现多节点进入，而且所有节点都能看到完整的版权使用和交易过程。
* 绝对安全可信。区块链所记录的版权追溯全过程，是不可逆且不可篡改的。版权资产有了全过程追溯的确权保障。

技术方案

1. 纯hash,去存储方案：

代表：Originstamp: http://originstamp.org/home

* 实现方案

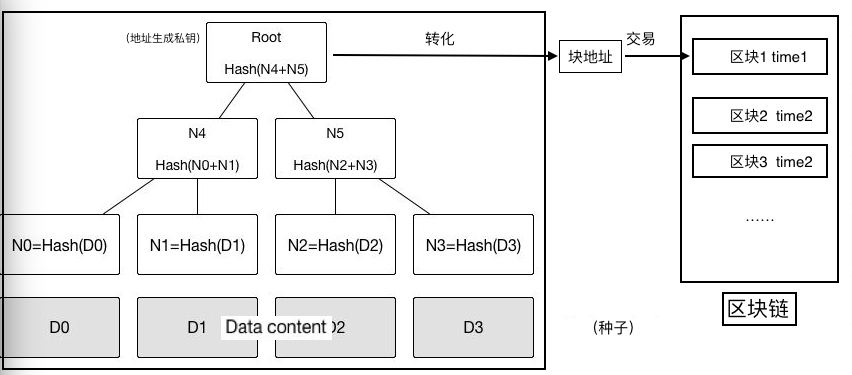
1、将需要存证源文件进行hash,将hash值传到服务器。

2、服务器批量统计步骤1中的hash值，生成默克尔树。

3、获取默克尔树的根hash,将其作为比特币块地址生成的私钥

4、生成块地址，进行交易，生成块。

原理图：



* 验证过程

1、写入块成功后，返回给用户一个种子（步骤2中的默克尔树）

2、对自己的源文件进行hash,查看hash值是否在种子中。

3、获取种子中的根hash，作为块地址生成私钥，生成块地址。

4、在区块链浏览器中根据步骤3中生成的块地址查询交易，获取交易时间，从而实现验证

* 缺陷

用户（或者托管服务器）要保存好源文件且不能进行修改变动。因为校验需要对源文件进行hash操作。一旦丢失，那么将难以进行校验。

1. 借助Factom系统

代表：保全网



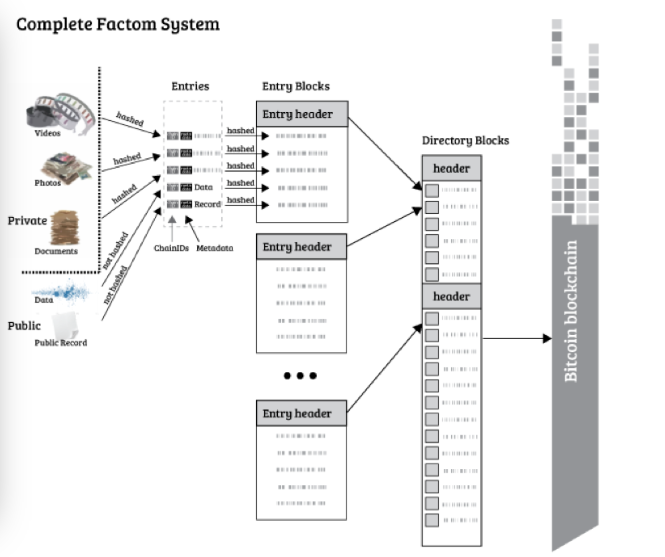
* factom系统特点

Factom是用一种去中心化的方式来收集，打包，安全保护数据，并把数据锚定到比特币的区块链上。

* factom系统原理

首先将一段时间内上传的数据都纳入到Merkle Hash tree（间接或者直接）；然后每隔10min中Root Hash加入到OP\_RETRUN交易中，锚定到bitcoin区块链。

* 原理图



* factom系统完整流程

1.APP的运营者先去Factom上买Factoids，然后将Factoids兑换成Entry Credit

2.APP将数据提交到Factom Servers，加入该APP对应的Entry Chain

3.将 当前周期内上传 Entry 打包成 EntryBlocks（白皮书上显示 1min钟生成一个块）；

4.将 当前周期内生成的EntryBlocks 打包成 Directory Blocks；

5.间隔一段时间（白皮书显示是10min，正好是比特币生成区块的平均时间）将未锚定的Diretory Blocks加入到一个Merkle tree中（按照白皮书说法应该是10块）；

6.将root hash 锚定到Bitcoin中

* 鉴权流程

在锚定之前，将原始文件及文件的hash都进行了存储，当写入区块链后，交易信息和公钥将被返回，并同样被存储于数据库中。这样能够方便的对文件进行分类和查询。

1. IPFS+以太坊

* IPFS介绍

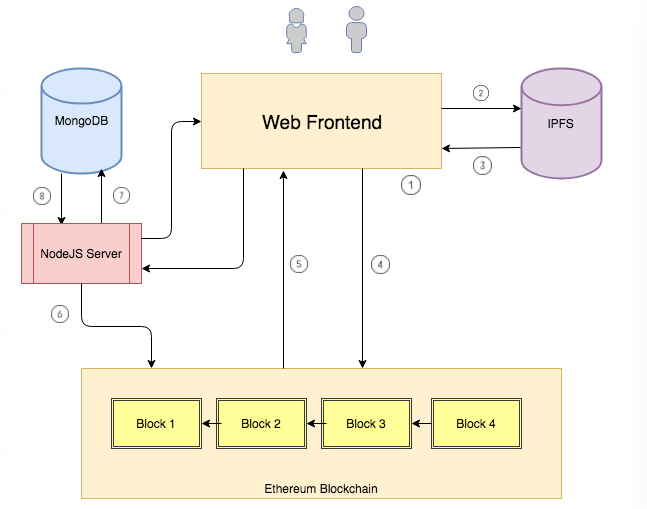
星际文件系统(InterPlanetary File System)，本质上是一种内容可寻址、版本化、点对点超媒体的分布式存储、传输协议，目标是补充乃至取代过去20年里使用的超文本媒体传输协议（HTTP），希望构建更快、更安全、更自由开放的互联网时代。

Ipfs最核心的技术是p2p，原来是中心化的服务器在分发内容，现在我们想要下载某一个内容，可以直接建立一个连接，也可以跟其他人连接，迅雷也是这种模式，它是一个虚拟的p2p中心网络。

* 实现方案

将存储到ipfs，将图片hash存储到Ethereum区块链，取数据时先从区块链读取文件hash，再通过hash从ipfs读取数据，解决了区块链大数据存储成本高昂的问题。

* 实例方案



(**1**)前端使用一个HTML表单来采集用户输入的商品细节，例如起拍价、商品图片、描述信息等。（此处商品类比需要版权保护的产物）

(**2**)(**3**) 前端将商品图片和介绍文本上传到IPFS，并返回所上传内容对应的链接（哈希）。

(**4**)(**5**) 然后，web前端（也可后端进行操作）会调用电商合约将商品信息和IPFS链接存储到链上。当合约成功地将商品存入区块链后， 就会触发一个事件，该事件中包含了商品所有的信息。

(**6**)(**7**)(**8**) NodeJS服务器监听区块链事件，当事件被电商合约触发时，服务器读取事件内容并将商品信息插入到 MongoDB数据库中。

相关资料

IPFS+以太坊：

* 以太坊将数据写入到区块：

<https://yq.aliyun.com/articles/477873>

<http://www.blockchainbrother.com/article/2006>

* IPFS搭建区块链服务：

<http://www.8btc.com/ipfs-qtum>

* 搭建自己的ipfs私有网网络：

<https://blog.csdn.net/oscube/article/details/80598790>

* IPFS初体验(环境搭建,私有网络环境搭建,API演示)：

<https://blog.csdn.net/wen942467928/article/details/79377402>

* 以太坊+IPFS简单案例：

<http://liyuechun.org/2017/11/25/ipfs-upload-image/>

factom相关：

* Factom开源地址：

<https://blog.csdn.net/elwingao/article/details/52679475>

<https://github.com/FactomProject/factomd>

* Factom API:

<https://docs.factom.com/api>

* Factom白皮书：

http://www.8btc.com/factom-white-paper

* Factom白皮书：

<https://blog.csdn.net/u011015260/article/details/51471281>

* Factom基本原理及组织架构：

<https://www.cnblogs.com/cnblogs-wangzhipeng/p/8270075.html>

* Factom时间戳锚定到比特币

<http://baijiahao.baidu.com/s?id=1602799302413353992&wfr=spider&for=pc>

* 关于OP\_RETURN

<https://segmentfault.com/a/1190000013614471>

<https://blockchain.info/tx/b17a027a8f7ae0db4ddbaa58927d0f254e97fce63b7e57e8e50957d3dad2e66e>

纯hash相关：

* 默克尔树

<https://blog.csdn.net/weixin_37504041/article/details/80474636>

* 比特币秘钥生成

<https://bbs.huaweicloud.com/blogs/7e4a3da5177211e89fc57ca23e93a89f>