

# 基于区块链的数字版权交易系统

李莉, 周斯琴, 刘芹, 何德彪

(武汉大学国家网络安全学院, 湖北 武汉 430072)

**摘要:** 在当前数字化、网络化时代中, 数字版权交易需求越来越大, 传统的中心化版权保护系统存在注册成本高、作品受理时间长、容易遭受破坏者的篡改等问题。区块链技术作为一个以 P2P 网络为基础, 以密码技术为核心的去中心化网络结构, 能够在网络上以纯数学方法建立信任关系, 无需依托中间平台就能够缓解上述问题。借助区块链技术的自我监管、可追溯、去中心化的特性, 结合数字版权交易场景, 设计了一个基于联盟链的数字版权交易系统模型, 利用当前 IBM 提供的最新联盟链技术, 做了版权注册和版权交易的实现, 能够保证版权信息不可篡改性和可溯源性。最后, 测试了链码部署安装时间。结果表明, 系统安装简单, 维护成本低。相比传统的基于可信第三方版权认证机制, 基于区块链的数字版权交易系统注册时间短, 无需注册费, 具有更好的架构安全性和可扩展性。

**关键词:** 数字版权交易; 区块链; 超级账本; 系统设计与实现

**中图分类号:** TP309.7

**文献标识码:** A

**doi:** 10.11959/j.issn.2096-109x.2018060

## Blockchain-based digital copyright trading system

LI Li, ZHOU Siqin, LIU Qin, HE Debiao

School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China

**Abstract:** In the current era of digitalization and networking, the demand for digital copyright transactions is increasing. The traditional centralized copyright protection system has series of problems such as high registration costs, long work acceptance times, and being vulnerable to tampering by saboteurs. Blockchain as a decentralized network structure and based on P2P network and cryptographic technology, which can establish trust relationship on the network by pure mathematics. Without relying on the middle platform, blockchain technology can naturally alleviate the above problems. With the help of self-regulatory, traceable and decentralized features of blockchain technology and digital copyright trading scenarios, a digital copyright trading system model was designed. The new system is based on the advanced permissioned blockchain provided by IBM. The implementation of copyright registration and copyright transaction can ensure the integrity and tamper-resistant of the information. Finally, the installation time of chain code deployment was tested. The results show that the system is simple to install and has low maintenance costs. Compared with the traditional trusted third party copyright authentication mechanism, the blockchain-based digital rights trading system has a short registration time, no registration fee, and better architecture security and scalability.

**Key words:** digital rights trading, blockchain, superbooks, system design and implementation

收稿日期: 2018-06-10; 修回日期: 2018-07-01

通信作者: 何德彪, hedeiao@163.com

基金项目: 国家重点研发计划基金资助项目 (No.2017YFB0802500); 国家自然科学基金资助项目 (No.61402339, No.61572370)

**Foundation Items:** The National Key Research and Development Program of China (No.2017YFB0802500), The National Natural Science Foundation of China (No.61402339, No.61572370)

## 1 引言

数字版权保护技术是基于密码学技术和相关法律法规来保障数字作品的合理使用以及创作者权益的一项技术，它需要确保数字内容从出版到使用整个流通过程中的安全性，对数字内容的原创者、所有者和使用者都应该授予不同的使用权力以及使用控制，确保内容的合理使用，以及权力转移的公开透明。但是，当前的数字版权保护系统注册成本高，申请过程复杂，而且花费时间长<sup>[1-2]</sup>。由于这些原因，在数字化网络时代中，很多数字作品创作者不愿意申请数字版权保护，使大量碎片化的数字作品难以得到版权保护。这就导致网络作品容易遭到篡改和盗用，原创者利益大大受损。而基于中心化的权威机构授权管理方式也增加了现实经济和社会活动的信任成本和会计成本。这些问题都使现有的版权保护系统难以满足当前数字版权贸易需求<sup>[3-4]</sup>。作为“信任互联网”的底层架构，区块链是由节点参与的分布式开放账本<sup>[5-6]</sup>，基于一种新型的去中心化协议，能安全地存储交易信息和其他数据（债权、股权和数字资产）。联盟链<sup>[7]</sup>是对特定组织团体开放的区块链系统，与公有链不同，联盟链的共识过程是由预先选择的一系列节点所掌控，这种共识方式加快了交易的确认时间。因此，可以在这类的区块链系统上构建自己的数字版权交易系统，一些权威管理机构充当系统中的部分管理节点，在普通用户发起上传自己数字作品唯一标识符（DCI, digital copyright identifier）<sup>[8]</sup>的交易时，这些管理节点对这笔交易进行验证，只有通过一定数量节点的同意，这笔交易才能上链，链上的版权数据库才会增加一条新的数字版权记录。这种“部分去中心化”的管理方式相比传统的数字版权系统，更加安全、高效。

因此，本文设计实现了一个基于联盟链的数字版权交易系统，该系统由多个节点进行管理，系统的身份准入机制可以将满足要求的其他节点加入系统，多用户的权限分配使参与系统的不同用户拥有对链的不同操作权限。目前，系统能够安全地管理用户信息并提供基本的数字版权管理

和数字版权交易服务。当系统管理员通过初始化、实例化，安装合约到链上后，其他用户可以调用链上的合约来请求系统服务。为了实现系统的可扩展性和高安全性，本文采用了 Hyperledger 提供的联盟链系统<sup>[9]</sup>和 composer 框架<sup>[10]</sup>进行开发，完成了数字版权交易系统的后台业务代码，并提供简单的 Java Web 可视界面，用户可以登录 Java Web 客户端查看每次调用系统服务的历史交易记录。

## 2 区块链及 Fabric 简介

区块链概念起源于比特币系统<sup>[11]</sup>，它最初的学术定义为：由包含交易信息的区块从后向前有序连接起来的数据结构。区块链作为一个记录所有交易记录的公开账本，链上的每一个块里面都存有矿工们的最近交易记录，而且这些块以时间顺序依次链接起来。每一条区块链都完整地存储在由多个节点组成的分布式网络上，从而避免单点失效，或者中心数据库被攻击等问题。通过这个公开账本，区块链实现了其不需要一个中央权力机构或受信任的第三方来协调互动，验证交易或监管行为的特征。区块链网络中存储了完整的数据账本，包含曾经执行的所有交易，使历史上发生的交易信息都可以被网络中节点所访问，而一个节点只有超过全网 51% 的算力，才能更改区块链上的交易信息。实际上，这是很难做到的。

区块链的应用有很多，其中的典型应用是资产注册、存储和交易，包含金融、经济和货币等各个领域的有形资产和无形资产。使用区块链技术开辟了不同类型各个层次的行业应用功能，包括货币、市场、金融交易、物资等<sup>[12]</sup>。通过智能合约使用区块链编码的资产，可以称为智能资产<sup>[13-14]</sup>。本文以数字版权作为一种智能资产，将版权交易通过智能合约实现，并记录在公开账本中。

目前，根据权限管理将区块链分为 3 种形态：私有区块链、公共区块链和联盟区块链。相比前 2 种区块链，联盟链结合了公共区块链的“低信任”和私有区块链的“单一高度信任”，提供了一种混合的模式，能够适应市场上大多数的应用场

景。超级账本是由非营利组织 Linux 基金会成立的一项企业级区块链开发及应用的开源项目。Fabric 是最早加入超级账本中的顶级项目,项目在 GitHub 上,网址为 <https://github.com/hyperledger/fabric>。本文就是以该项目为技术依托,构建了企业级数字版权交易系统。Fabric 可以为其上的应用提供 gRPC API,以及封装 API 的 SDK 调用。应用可以通过 SDK 访问区块链网络中的多种资源,包括公开账本、交易、链码、事件和权限管理等。交易的执行逻辑通过链码承载,权限管理则负责整个过程中的访问控制。Fabric 大致分为 3 种不同的层级结构<sup>[15]</sup>:网络层;共识机制和权限管理;业务层。网络层面向系统管理人员。该模块实现了 P2P 网络,提供底层构建区块链网络的基本能力,包括不同角色的节点和服务。共识机制<sup>[16]</sup>和权限管理面向联盟和组织管理人员,实现共识和权限管理。业务层面向业务开发人员,支持业务应用的开发工作。本文主要是在业务层进行操作,实现业务链码,并将链码打包发布到 Fabric 网络的多个节点上。这里所说的节点与以太坊<sup>[17]</sup>有些不同。从功能上, Fabric 网络中的节点可以分为:背书节点、确认节点、排序节点。背书节点负责对来自客户端的交易提案进行检查和背书;确认节点检查交易请求,并执行交易;排序节点负责将接收到的交易排序并打包成区块,进行共识。

总之,以 Fabric 为技术依托的联盟链可以做到很好的节点间的连接,只需要极少的成本就能维持运行,提供迅速的交易处理和低廉的交易费用,有很好的扩展性(但是扩展性随着节点增加又会下降),数据可以有一定的隐私。

### 3 数字版权保护系统设计与实现

#### 3.1 系统结构

基于区块链的数字版权保护系统是在区块链网络上建立的数字版权保护系统,它具有去中心化、数字内容安全存储,交易记录可追溯,防篡改等优点。因此,本文设计了一种新的基于区块链的数字版权交易系统,它的总体架构如图 1 所示。

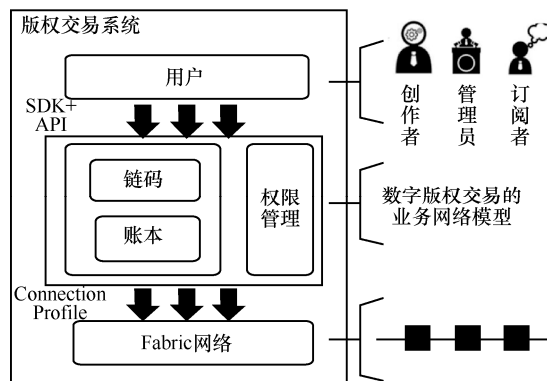


图 1 版权交易系统结构

从功能类型上,系统大体分为 3 层结构。最上层是用户层,负责提供用户管理服务接口以及版权管理服务接口,如用户注册、用户登入管理、个人信息修改、密钥管理、版权登记接口、版权查询接口、版权交易接口、版权注销接口。中间层是数字版权交易的业务模型层,这部分是由开发人员进行设计实现,其中链码(即智能合约)定义了数字版权交易系统的数据结构和功能函数,账本则记载了用户的每次交易。用户在用户层通过 API+SDK 调用业务模型中的链码,从而完成相应的业务功能。由于每次交易都被记载在账本中,版权的交易信息可以在链上进行追溯。最下层是 Fabric 网络层,这一层与中间层通过 Connection Profile 这个文本文件进行连接,这个连接文件定义了节点信息,节点通信端口,便于将本文所设计的业务模型安装到不同用户的节点上,从而形成去中心化通信网络。

该系统所针对的用户主要分为 3 类用户:创作者、管理员和订阅者。

1) 创作者,即数字作品的原创作者。他可以将自己申请到的数字版权的 DCI 码填入表单,随后调用 Fabric 提供的 SDK 和远程 API 来操作链码,将数字作品的信息(数字作品名称、DCI、著作人、作品类型、创作时间)存入区块链上,并可以通过函数接口进行修改 DCI。

2) 管理员,即权威管理机构,可以对创作者和订阅者的账号进行管理,同时发布新的合约到链上,或者废除链上旧的合约。

3) 订阅者作为最普通的大众用户,能够订阅链上的某个数字作品,在订阅者调用远程 API,执

行订阅链码, 就可以获取链上数字作品的阅读权。

链码是超级账本中所用到的一个专业术语, 它可以被称为合约代码, 被用来实现系统的主要逻辑。链码最初是由管理人员在系统初始阶段部署到各个节点上的。当链码成功地在节点上初始化、实例化、安装这3个过程后, 用户通过登录客户端软件, 利用业务模型提供的远程 API 函数调用链码。每个节点都设有客户端软件。账本记录了每次链码调用的日志, 有增减链上用户的交易记录, 有版权转移的交易记录, 有作品订阅的交易记录等, 维护这些交易记录就是维护记账的过程。

下面, 以发布一个版权转移交易为例, 介绍本系统的交易流程。

1) 数字作品创作者登录系统客户端, 进行身份注册, 获取注册证书 (Ecrt) 和交易证书 (Tcrt)。随后, 用户才能利用客户端发起交易。

2) 用户成功登录客户端, 创建一笔版权转移的交易提案 (Proposal), 并将这笔交易提案发送到各个背书节点。

3) 背书节点执行版权转移链码, 并将提案结果返回给客户端。

4) 客户端收集到足够的背书支持后, 将交易提交到排序节点, 交易内容包括提案结果。

5) 排序节点将排完序的交易封装到区块中, 区块随后被发送给各个验证节点。

6) 验证节点定期地从排序后的交易区块结构

中, 对交易进行落盘前的最终检查 (包括交易消息结构、签名完整性、是否重复、读写集合版本是否匹配等)。检查通过后, 执行合法的交易所, 将结果写入账本, 同时构造新的区块, 更新区块中元数据块, 记录交易是否合法等信息。

发布版权订阅交易类似上述流程, 在此不赘述。

以上对该系统的架构和功能进行了详细介绍。相较于其他版权管理系统, 基于区块链的数字版权交易系统有如下优点: ①创作者将自己的数字版权信息存储在区块链上, 保障了创作者对于创作作品的拥有权; ②创作者能根据自己的定价, 将自己的数字作品版权转移给其他用户, 从而获得经济利益, 数字作品版权的转移是调用区块链上的版权转移链码实现的, 在整个 Fabric 网络上透明的、可监控的, 版权的转移不会存在争议; ③给链上的数字作品提供订阅接口, 普通用户可以支付小额费用给原创者, 从而获得数字作品的阅读权。

### 3.2 业务模型描述

本节从用户、资产和交易这3个模块介绍数字版权交易系统的业务模型。

#### 1) 用户

用户分为普通用户、管理员、创作者 (即最初的数字资产所有者)。其属性结构分别设计为如下元组所示:  $User=\{Uid, userName, email, balance, PK, SK, bookList\}$ ,  $Admin=\{Uid, userName, email, PK, SK\}$ ,  $Author=\{Uid, userName, email,$

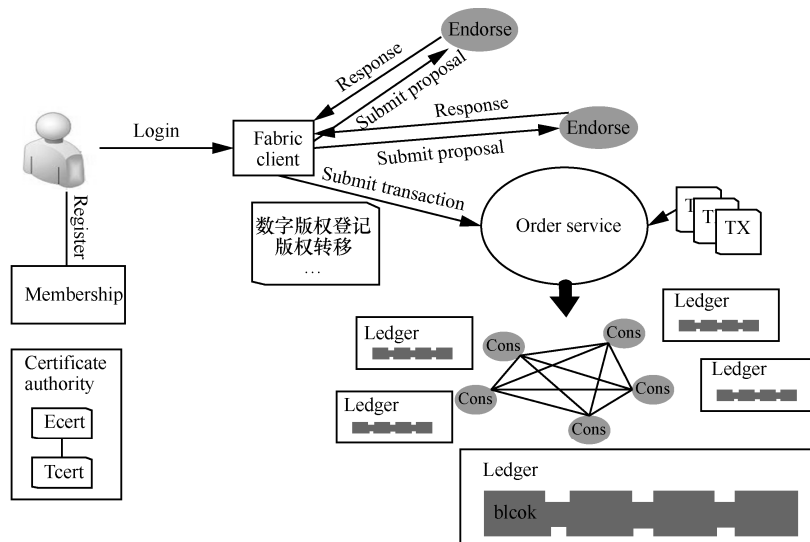


图2 基于 Fabric 应用的交易流程

$PK, SK, myBookList\}$ 。定义 *Person* 是用户基类, 普通用户和管理员用户属于 *User* 这一类, 创作者属于 *Owner* 这一类, *PK* 是用户的公钥, *SK* 是用户的私钥, *balance* 是用户钱包余额, *bookList* 记录用户订阅的所有书籍信息, *myBookList* 记录用户创作的所有书籍信息。私钥被用来对数字版权交易做签名, 进而在版权交易中, 确保交易信息的完整性和正确性。正如前文所说, 数字作品创作者可以通过转让版权或者提供数字作品, 从而获得经济利益, 因此当发生这 2 种交易时, 创作者的余额会增加, 消费者的余额会减少。

## 2) 资产

本系统中资产就是数字版权作品, 其属性结构设计为如下元组。

$DigitalWork = \{dci, name, category, createTime, description, content, owner\}$ ,  $Book = \{dci, name, category, createTime, description, content, owner, price, subscribePrice, subscribers\}$ 。

*dci* 是数字作品唯一标识符, *name* 是数字版权作品名字, *category* 是作品分类, *createTime* 是创建时间, *description* 是数字作品简要描述, *content* 是部分内容信息, *owner* 是作品所有者, *price* 是版权转移价格, *subscribePrice* 是订阅作品需支付的价格, *subscribers* 是该作品订阅的所有用户集合。

## 3) 交易

在区块链系统中, 用户每次对智能合约 (或者链码) 的调用, 都称为交易。用户通过调用 *composer-rest-serve* 提供的函数接口可以对合约进行调用, 从而执行相应的操作。版权注册、版权转移, 数字内容订阅交易的主要代码如表 1-表 3 所示。

表 1 数字版权注册主要代码

版权注册主要代码

```
前提: 链码初始化, 安装到链上, 用户利用客户端调用函数名,
传入打包好的新 Work 结构

function onRegisterOfWork(Work) {
    var newWork=work;
    return getAssetRegistry('org.whu.dci.management.Work')
        .then(function(){
            return getAssetRegistry('org.whu.dci.management.Book')); //
            在账本中记录新的 work , 更新账本
        }
    }
```

表 2 版权转让主要代码

版权转让主要代码

```
前提: 链码初始化, 安装到链上, 用户利用客户端调用函数名,
传入打包好的新 Work 结构

function onChangeOwnerOfWork(ChangeOwnerOfWork) {
    var newOwner=ChangeOwnerOfWork.newOwner; //获取版权
    转让的被转让方
    var oldOwner=ChangeOwnerOfWork.book.owner; //获取版权
    转让的转让方

    ChangeOwnerOfWork.book.owner=newOwner;
    var price=ChangeOwnerOfWork.book.price; //获取转让合约
    中用户确定的转让价格
    newOwner.balance=newOwner.balance-price; //从被转让方的
    钱包中扣除转让费
    oldOwner.balance=oldOwner.balance+price; //在转让方的钱
    包中增加转让费

    UpdateUserRegister(); //更新账本中用户信息和该数字版
    权信息
    UpdateDciRegister();
    return 1;
}
```

表 3 数字内容订阅主要代码

数字内容订阅主要代码

```
前提: 链码初始化, 安装到链上, 用户利用客户端调用函数名,
传入打包好的新 Work 结构

function onSubscribeWork(SubscribeWork) {
    var subscriber=SubscribeWork.subscriber;
    var author=SubscribeWork.book.owner;
    var subscribePrice=SubscribeWork.book.subscribePrice;

    subscriber.bookList.push(SubscribeWork.book); // '书架'上 新
    增一个数字作品
    author.balance+=subscribePrice; //author 账户钱包数额增加,
    subscriber.balance-=subscribePrice; //订阅者钱包数额减少

    UpdateUserRegister(); //更新账本中用户信息和该数字版
    权信息
    UpdateDciRegister();
    return 1;
}
```

## 3.3 系统实现

为了将数据的修改以及用户的管理权放在部分用户手中, 选择 IBM 提供的 fabric1.0 联盟链项目作为开发平台, 进而构建自己的数字版权保护系统。根据官方 Fabric 给出的节点部署方案, 在各个节点上安装 docker 以及 docker compose 工具, 下载相应的 docker 镜像和 Fabric 源码, 编译生成 Cryptogen 程序, 利用该程序和相关 crypto-config.yaml 配置文件生成公私钥和证书。

这里生成 2 种证书：一种是给节点安全通信而准备的 TLS 证书；另一种是 CA 颁布的用于用户登录和权限控制的用户证书。随后，采用编译生成的 configtxgen 生成创世区块（如图 3(a)所示）以及 Channel 配置区块。再通过配置相关文件，即可启动 Fabric 容器（如图 3(b)所示），接着，完成创建 channel（如图 3(c)所示），各个 Peer 节点依次加入 Channel，更新锚节点（如图 3(d)所示）这一系列操作。这样，Fabric 网络就准备好了。接下来，将业务链码安装到 Fabric 网络中。

Fabric 链码支持 golang 和 JavaScript。为了提高程序的可扩展性，通过 fabric composer 进行开

发并建立系统的业务模型。随后，利用 composer-rest-server 可以生成业务模型的远程接口（如图 4 所示），用户可以通过这些函数接口访问交易记录、数字版权记录等。每当用户提交资产注册信息后，该交易记录后续会被其他节点打包成区块，并记录在链上，交易记录一旦上链，就无法被篡改。

## 4 系统的测试与分析

目前，系统的核心链码大约为 5 kB，通过在网络的各个节点上安装和实例化链码后，测试了单个节点链码的安装和实例化时间大约为 9 770 ms，链码的单次调用时间为 0.7~3 s。本地采用的开发

```
##### Generating Orderer Genesis block #####
#####
2018-06-26 21:32:46.810 CST [common/configtx/tool] main -> INFO 001 Loading configuration
2018-06-26 21:32:46.840 CST [common/configtx/tool] doOutputBlock -> INFO 002 Generating genesis block
2018-06-26 21:32:46.841 CST [common/configtx/tool] doOutputBlock -> INFO 003 Writing genesis block
```

(a) 生成创世区块

```
Creating network "net_byfn" with the default driver
Creating peer0.org1.example.com
Creating orderer.example.com
Creating peer0.org2.example.com
Creating peer1.org2.example.com
Creating peer1.org1.example.com
Creating cli
```

START

(b) 启动 Fabric 容器

```
### Generating channel configuration transaction 'channel.tx' ###
#####
2018-06-26 21:32:46.852 CST [common/configtx/tool] main -> INFO 001 Loading configuration
2018-06-26 21:32:46.855 CST [common/configtx/tool] doOutputChannelCreateTx -> INFO 002 Generating new channel configtx
2018-06-26 21:32:46.855 CST [common/configtx/tool] doOutputChannelCreateTx -> INFO 003 Writing new channel tx
===== Channel "mychannel" is created successfully =====
Having all peers join the channel...
```

(c) 创建 Channel

```
##### Generating anchor peer update for Org1MSP #####
#####
2018-06-26 21:32:46.867 CST [common/configtx/tool] main -> INFO 001 Loading configuration
2018-06-26 21:32:46.869 CST [common/configtx/tool] doOutputAnchorPeersUpdate -> INFO 002 Generating anchor peer update
2018-06-26 21:32:46.870 CST [common/configtx/tool] doOutputAnchorPeersUpdate -> INFO 003 Writing anchor peer update
```

(d) 更新锚节点

图 3 Fabric 应用环境部署

```
zsq@zsq-ThinkPad-X1-Carbon-5th:~/桌面/BND/12.24$ composer-rest-server
? Enter the name of the business network card to use: admin@tutorial-network
? Specify if you want namespaces in the generated REST API: never use namespaces

? Specify if you want to enable authentication for the REST API using Passport:
No
? Specify if you want to enable event publication over WebSockets: Yes
? Specify if you want to enable TLS security for the REST API: No

To restart the REST server using the same options, issue the following command:
composer-rest-server -c admin@tutorial-network -n never -w true

Discovering types from business network definition ...
Discovered types from business network definition
Generating schemas for all types in business network definition ...
Generated schemas for all types in business network definition
Adding schemas for all types to Loopback ...
Added schemas for all types to Loopback
Web server listening at: http://localhost:3000
Browse your REST API at http://localhost:3000/explorer
```

图 4 生成业务模型的远程接口

环境为个人 PC 计算机, CPU 2.7 GHz, RAM 8 GB。操作系统为 ubuntu 16.04。

系统部署容易, 耗时短, 适合企业级应用。为了展示实验结果, 利用 angular JavaScript 构建 Java Web 客户端, 界面如图 5 所示。合法用户通过注册个人信息, 成功登录 Java Web 客户端进行资产注册、版权转移操作、数字内容订阅等操作。

如图 5 所示, 当数字作品创作者想要在本系统进行版权注册时, 创作者通过单击 add asset 按钮, 填入数字作品 dci, 数字作品名称、数字作品分类、描述、作品简介、选择作品所属人, 就可以发起数字版权注册的交易。当数字作品创作者想要转移数字版权时, 调用版权转移交易、输入新的版权所有者以及需要转移的数字版权(具体函数见业务模型章节)发起交易。随后, 系统调用智能合约, 按照预先设置的版权转移费, 从新版权所有者的余额中扣除版权费, 从创作者余额中增加版权费, 完成版权转移交易。除此之外, 利用版权注册时填入的相关信息, 其他用户可以订阅感兴趣的数字版权, 发起版权订阅交易。后续内容的传输, 由交易双方在其他内容分享平台完成。由于这部分不是本系统的研究重点, 在此不过多介绍。

## 5 结束语

当前, 数字版权保护方法都是集中登记式, 本质上是基于中心化由权威管理机构授权的版权管理机制。而区块链技术可以为数字版权提供一种不可更改的去中心化的版权登记形式。它以密码学为基础, 建立的信任关系能够给交易多方提

供安全保障。本文分析了当前数字版权保护的痛点, 并详细介绍了区块链技术。结合当前最新的联盟链技术和当前需求, 本文又设计了一种适合于企业应用的数字版权交易系统, 该系统实现了版权登记、版权转移的基本功能, 保护创作者的版权所有权, 减少了申请者的注册时间, 且无需数字版权注册费。相较于传统的数字版权保护方案, 本系统能够保证版权登记信息的不可篡改性, 以及版权交易的可追溯性, 可以安全、高效地满足用户需求。另外, 基于 composer 框架的开发, 使业务逻辑与 Fabric 系统的耦合性降低, 开发人员更专注于功能性模块的编码工作, 因此, 具有更好的可扩展性。未来在数字版权保护的道路上, 基于区块链的版权保护方案将是市场的一大需求。当然系统还有一些不完善的地方, 后续笔者也会对本系统进行进一步的改进。

## 参考文献:

- [1] 范科峰, 莫玮, 曹山, 等. 数字版权管理技术及应用研究进展[J]. 电子学报, 2007, 35(6):1139-1147.  
FAN K F, MO W, CAO S, et al. Progress in digital rights management technology and application[J]. Chinese Journal of Electronics, 2007, 35(6): 1139-1147.
- [2] 翟永兴. 我国数字出版的版权保护现状与对策研究[J]. 传播与版权, 2015(3):178-179.  
ZHAI Y X. Research on the status quo and countermeasures of copyright protection in digital publishing in China[J]. Communications and Copyright, 2015(3): 178-179.
- [3] 吴健, 高力, 朱静宁. 基于区块链技术的数字版权保护[J]. 广播电视信息, 2016(7):60-62.  
WU J, GAO L, ZHU J N. Digital copyright protection based on Blockchain technology[J]. Radio and TV Information, 2016(7): 60-62.
- [4] 安瑞, 何德彪, 张韵茹, 等. 基于区块链技术的防伪系统的设计

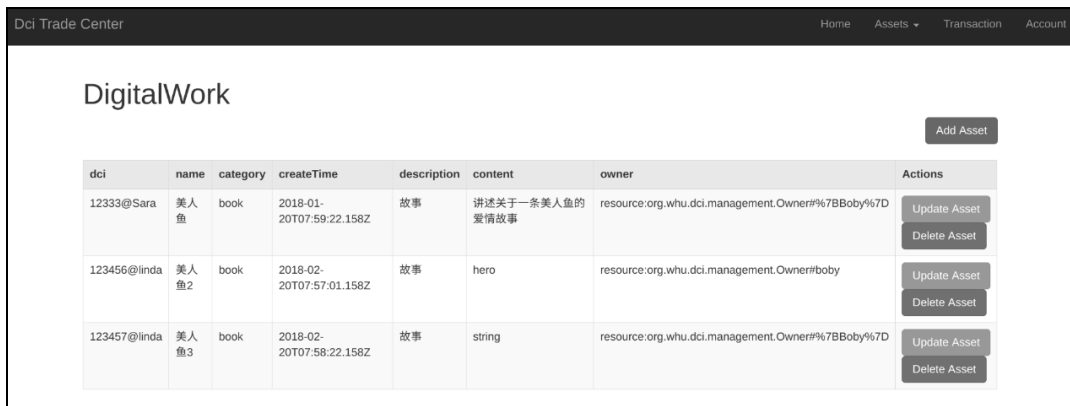


图 5 客户端界面

- 与实现[J]. 密码学报, 2017, 4(2):199-208.
- AN R, HE D B, ZHANG Y R, et al. Design and implementation of anti-counterfeiting system based on Blockchain technology[J]. CMD Journal, 2017, 4(2): 199-208.
- [5] 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.
- YUAN Y, WANG F Y. Current status and prospects of Blockchain technology development[J]. Journal of Automation, 2016, 42(4): 481-494.
- [6] DUBOVITSKAYA A, XU Z, RYU S, et al. Secure and trustable electronic medical records sharing using Blockchain[J]. arXiv preprint arXiv:1709.06528, 2017.
- [7] PETERS G W, PANAYI E. Understanding modern banking ledgers through Blockchain technologies: future of transaction processing and smart contracts on the internet of money[M]//Banking Beyond Banks and Money. Berlin: Springer. 2016: 239-278.
- [8] 吴洁明, 周倩, 许传祥, 等. DCI 体系下数字版权管理服务平台的设计[J]. 计算机应用与软件, 2014(4):62-65.
- WU J M, ZHOU Q, XU C X, et al. Design of digital rights management service platform under DCI system[J]. Journal of Computer Applications and Software, 2014(4):62-65.
- [9] VUKOLIĆ M. Rethinking permissioned blockchains[C]//ACM Workshop on Blockchain, Cryptocurrencies and Contracts. 2017: 3-7.
- [10] CACHIN C. Architecture of the hyperledger blockchain fabric[C]// Workshop on Distributed Cryptocurrencies and Consensus Ledgers. 2016.
- [11] DHILLON V, METCALF D, HOOPER M. The Hyperledger project[M]//Blockchain Enabled Applications. Berlin: Springer. 2017: 139-149.
- [12] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[J]. Consulted. 2008.
- [13] SWAN M. Blockchain: blueprint for a new economy[M]. O'Reilly Media, Inc. 2015.
- [14] PETERS G W, PANAYI E. Understanding modern banking ledgers through blockchain technologies: future of transaction processing and smart contracts on the internet of money[M]//Banking Beyond Banks and Money. Berlin: Springer. 2016: 239-278.
- [15] CACHIN C. Architecture of the hyperledger blockchain fabric[C]//Workshop on Distributed Cryptocurrencies and Consensus Ledgers. 2016.
- [16] BALIGA A. Understanding blockchain consensus models[R]. 2017.
- [17] WOOD G. Ethereum: a secure decentralised generalised transaction ledger[J]. Ethereum Project Yellow Paper, 2014, 151: 1-32.

#### [作者简介]



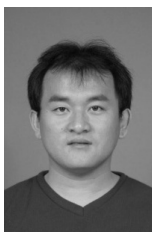
李莉 (1976-), 女, 安徽芜湖人, 博士, 武汉大学副教授、硕士生导师, 主要研究方向为物联网安全。



周斯琴 (1994-), 女, 湖北孝感人, 武汉大学硕士生, 主要研究方向为区块链技术。



刘芹 (1978-), 女, 湖北随州人, 博士, 武汉大学副教授、硕士生导师, 主要研究方向为物联网安全。



何德彪 (1980-), 男, 山东阳谷人, 博士, 武汉大学教授、博士生导师, 主要研究方向为密码算法的设计与实现。