Journal of Computer Applications
计算机应用,2017,37(11):3281 -3287
ISSN 1001-9081
CODEN JYIIDU
2017-11-10
http://www.joca.cn

文章编号:1001-9081(2017)11-3281-07
DOI:10.11772/j.issn.1001-9081.2017.11.3281

# 基于区块链的数字作品 DCI 管控模型

李　悦,黄俊钦,王瑞锦*
(电子科技大学 计算机科学与工程学院,成都 611731)
(*通信作者电子邮箱 ruijinwang@uestc.edu.cn)

**摘　要**:针对互联网生态下数字知识产权面临的版权登记、盗版猖獗和版权纠纷等问题,提出了去信任的数字作品数字版权唯一标识符(DCI)管控模型。首先,构建了基于区块链去中心化理念的端到端体系架构,区块链取代传统关系数据库作为核心存储机制,通过创建交易、构造区块、区块的合法性验证与链接构建了数字作品区块链的交易信息存储机制,保证版权信息不可篡改性和可溯源性;其次,提出了基于智能合约的数字化发行和流通协议,设计了版权登记、查询、转让三类合约,通过自动执行预设指令的方式产生交易,保证模型透明高效与自动化运作。理论分析和仿真表明,在数字作品区块链网络中,伪造区块攻击的概率趋近于零,与传统的基于可信第三方版权认证机制相比,该模型具有更好的架构安全性。实验结果表明,该模型降低了数字版权登记的门槛,增强了版权认证的权威,具有更好的实时性和鲁棒性。

**关键词**:区块链;智能合约;数字作品;去中心化;版权管控
**中图分类号**:TP309.2　　**文献标志码**:A

# DCI control model of digital works based on blockchain

LI Yue, HUANG Junqin, WANG Ruijin*
(*University of Electronic Science and Technology of China, Chengdu Sichuan* 611731, *China*)

**Abstract:** In order to solve the problems of copyright registration, rampant piracy and copyright disputes faced by digital intellectual property under Internet ecology, a Digital Copyright Identifier (DCI) control model of digital works without trusted third party was proposed. Firstly, the Peer-to-Peer (P2P) architecture based on the concept of de-centralization of blockchain was constructed. The blockchain replaced the traditional database as the core of storage mechanism. Through the creation of transactions, construction of blocks, legitimacy validation and link of blocks a digital work blockchain transaction information storage structure was built, guaranteeing the copyright information not be tampered and traceable. Secondly, the digital distribution protocol based on smart contract was proposed, three types of contracts include copyright registration, inquiry and transfer were designed, and the transactions were generated by automatically executing the preset instructions to ensure the transparency and high efficiency of models. Theoretical analysis and simulation show that the probability of forged block attack is close to zero in the digital work blockchain network, compared with the traditional copyright authentication mechanism based on trusted third party, the model has better architectural security. The experimental results show that the model simplifies the threshold of digital copyright registration, enhances the authority of copyright certification and has better real-time and robustness.

**Key words:** blockchain; smart contract; digital works; decentralization; copyright control

## 0　引言

在“互联网+”的推动下,数字出版物(网络文学著作、图片、视频、网络文章等)呈爆炸式增长。2015 年我国数字出版领域的收入与 2014 年相比增长 30%,收入高达 4 403.85 亿元,数字出版领域的用户规模达到 17.235 7 亿人[1]。在数字出版产业高速发展的同时,也引发了一系列亟需解决的版权问题:首先,海量的数据导致版权登记困难无法保障作者的权益;其次,没有统一的数字版权管理平台导致数字版权资源分散,版权归属模糊。

目前,针对数字出版领域存在的问题,主要措施是进行相关法律体系建设和采用以数字水印为基础的数字版权管理(Digital Rights Management, DRM)技术[2]:前者无法从根本上解决数字版权存在的众多问题;后者的作用是防拷贝、防盗版,但是经过实践检验非但没有解决版权问题还导致了产业垄断和技术壁垒。周全[3]提出“嵌入式”版权服务组件的模式,通过基于可信第三方的模式管理各大数字作品出版平台进行统一的版权认证和记录。游福成等[4]提出基于数字水印和移动 Agent(Mobile Agent, MA)的数字版权保护机制,对数字出版物添加水印进行标记,通过数字水印认证版权。田园[5]基于现行对等网络(Peer-to-Peer, P2P)系统开放性导

**收稿日期**:2017-05-22;**修回日期**:2017-07-05。　**基金项目**:国家自然科学基金资助项目(61602096);中国博士后科学基金资助项目(2015M572464);四川省科技厅计划项目(2016ZC2575, 2015JY0178)。

**作者简介**:李悦(1997—),女,山西临县人,CCF 会员,主要研究方向:区块链、数字货币;　黄俊钦(1995—),男,福建莆田人,CCF 会员,主要研究方向:区块链、智能合约、网络通信;　王瑞锦(1980—),男,甘肃天水人,讲师,博士,CCF 会员,主要研究方向:信息系统安全、量子通信安全、云安全。

致的数字出版物盗版这一现象，提出基于哈希的分布式认证算法（Hash-based Decentralized Authentication，HDAP）和信誉值的反盗版机制，进而控制盗版产品的传播。

上述的解决方案均是基于可信第三方实现版权管理，不能做到版权信息的绝对权威；同时，提出的技术具有局限性并不适用于全部类型的数字出版物；再者，上述方案的实现成本高，不能做到技术的真正普及。近日，在“2017 中国版权保护中心（Copyright Protection Center of China，CPCC）中国版权服务年会”上举办的第七届数字版权唯一标识符（Digital Copyright Identifier，DCI）体系论坛中[6]，以“建构我国互联网版权基础设施”为主线，结合供给侧结构性改革、当下热点和未来发展方向，提出了集成区块链技术构建 DCI 体系为互联网版权基础设施的战略措施。

区块链是以比特币为例的各类新型加密数据货币的技术基础，是去中心化各节点共同维护的分布式账本[7-8]。目前区块链技术仅仅在金融领域被广泛使用。随着区块链 2.0 时代[9-12]的到来，本文将区块链技术引入数字版权领域，提出基于区块链的去中心化数字作品 DCI 管控模型，可为互联网数字出版物提供版权登记、版权查询、版权交易和保护的全链条一体化管控服务。设计了基于区块链的端到端体系架构，用区块链取代传统关系数据库进行信息存储，其中，区块由网络中矿工构造、链接，网络中的历史交易信息将永久保存在区块链中，使得版权记录和转移过程有绝对的溯源性和权威性。建立智能合约[10]自动化执行预设指令的机制，构建无需信任第三方的版权登记、版权查证、版权交易模式。区块链和智能合约共同打造一个可信权威、高效透明的数字出版物 DCI 管控平台，解决了现行数字出版物存在的一系列问题。

## 1 模型技术基础

本模型实现核心技术包括区块链技术和智能合约技术。

### 1.1 区块链技术

数据区块从整体结构上划分为区块头和区块体两部分[13]。其信息类型包括三大类：区块构造相关信息收集 $H$，区块产生对应的交易信息 $T$ 和区块中包含的其他区块的信息 $U$，区块 $B$ 的形式化定义如式(1)：

$$B = (B_H, B_T, B_U) \tag{1}$$

区块链网络中的矿工节点将一段时间内接收到的交易数据和合约代码封装到一个带有时间戳的版权区块中，版权区块链网络中其他节点对区块进行有效性验证，按照时间顺序进行哈希链接，产生最新的区块链，并在各个节点同步[13]。时间的不可逆转性致使历史区块数据无法修改和删除，保证数字作品 DCI 信息的不可否认性和可溯源性。

区块链不同于传统数据库的增、删、改、查，区块数据只能增加而不能修改或删除，但这并不是指系统中定义的某个字段的值不能被修改。区块其实记录的是交易的数据，它会记录下这个字段被修改的过程，而这一记录是不可修改的。这样就体现出了与传统数据库的差异性，传统数据库对某一字段的值并不会保留有历史修改记录，而区块链能够将某一字段从初始化到每一次的修改都完整地记录下来，从而保证了它的可溯源性。

### 1.2 智能合约

1995 年密码学家尼克萨博首次提出智能合约，将其定义为一系列计算机化的协议[14]，是一组预设条件对应的程序化规则，自动化运作不被干扰。每一份智能合约拥有数字作品区块链网络对应的合约账户。

数字作品区块链网络中的交易包括两大类：创建智能合约与通过已部署智能合约接口产生消息调用。其中，创建智能合约的过程就是将预设规则以代码的形式封装在区块中，对若干条件下对应的触发事件进行设定，经过数字作品区块链网络节点的验证进行链接同步。数字作品区块链网络实时监控已部署合约，动态检查外部数据源情况来判断是否满足合约预设的条件，若满足条件则触发矿工节点执行特定的智能合约，调用接口触发执行[15]。区块链的特性保证了智能合约从创建到执行不受任何影响准确执行。

## 2 模型实现方案

本章从模型的架构和相关协议设计出发，详细描述模型的实现方案。

### 2.1 模型架构设计

本模型设计了去中心化的数字作品区块链网络体系架构。模型架构设计如图 1 所示。

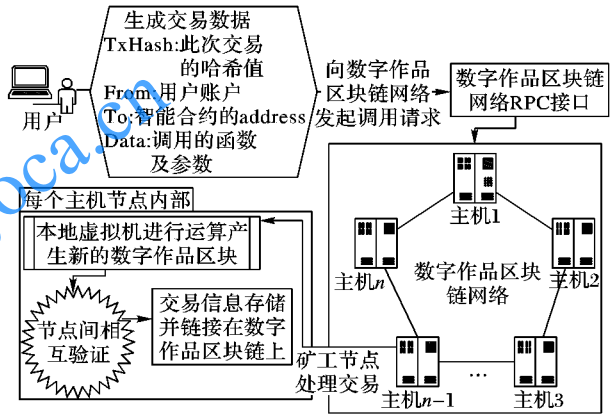


图 1 数字作品 DCI 管控模型架构设计

Fig. 1 Architecture design for digital works DCI control model

模型架构包括客户端和数字作品区块链网络中的矿工节点两部分：

1）用户使用客户端发起交易。用户在客户端的操作数据会生成一笔交易数据，由客户端将这笔数据通过区块链网络的远程过程调用协议（Remote Procedure Call protocol，RPC）接口，发送到数字作品区块链网络中，调用已部署的智能合约来完成版权登记、查询或转让功能。

智能合约在该模型中作为逻辑层，接收三种类型的请求：版权登记请求，记为 $T_\alpha$；版权转让请求，记为 $T_\beta$；版权查询请求，记为 $T_\gamma$。例如，一名网络文学作家使用客户端登记自己的原创文章版权，则客户端会向区块链网络发起一个 $T_\gamma$ 请求。通过调用部署在数字作品区块链上的智能合约，将自己的版权信息写入新的区块并链接到区块链上。因为区块链上存储的数据具有不可篡改的特性，而且每一笔交易都包含时间戳，所以能够为数字化版权的归属提供权威的证明，避免出现数字知识产权这类的版权纠纷问题。

2）矿工节点处理交易。矿工节点网络中的主机节点接收到用户发起的交易请求数据后，通过数字作品区块链网络的共识机制，在本地进行运算产生新的数字作品区块，该区块

会在矿工节点之间传播,当超过半数节点确认了该区块的有效性后,此次的版权信息才会被写入到区块链存储。

如图 2 所示,新的区块在经过验证其合法性之后,通过记录父块哈希链接到数字作品区块链上。智能合约作为运行在区块链上的自动执行代码,不受干预地执行版权登记、查询、转让等操作,保证了整个流程的公开透明,让版权信息更具权威性。

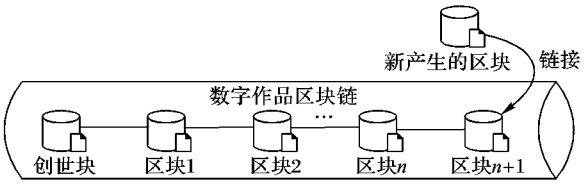


图 2　区块链接机制

Fig. 2　Blocklink mechanism

## 2.2　基于区块链的交易信息存储机制

数字作品区块链网络是由加入的各个节点共同构建的端到端的分布式网络。DCI 信息存储的核心是数字作品区块链,由网络中的全部节点共同维护。假设网络中有 A,B,C,D4 个节点,交易信息以及合约代码的存储机制如图 3 所示。

1)创建交易。

数字作品区块链网络中的客户端调用 RPC 接口发起交易。网络中的交易包括两大类:其一是在特定的条件下部署一份智能合约 $S$,其二是通过已部署的合约产生消息调用,交易 $T$ 的序列化表示如式(2):

$$T=\begin{cases}RLP(T_n,T_t,T_s,T_c), & T_t=\varnothing\\ RLP(T_n,T_t,T_d,T_s), & \text{其他}\end{cases}\tag{2}$$

其中:$RLP$ 为递归长度前缀编码,将交易序列化表示;$T_t$ 表示交易接收方的账户地址,当其为空时,代表交易类型为创建合约;$T_c$ 代表新合约的代码的字节数组;$T_n$ 代表合约的创建者发起的总交易数;$T_s$ 为交易发起方对交易信息签名。

当 $T_t$ 表示交易接收方的账户地址不为空时,表明交易的类型是通过已部署的智能合约产生消息调用,$T_t$ 为 20 个字节的地址哈希值,$T_d$ 为调用智能合约接口数据的字节数组。

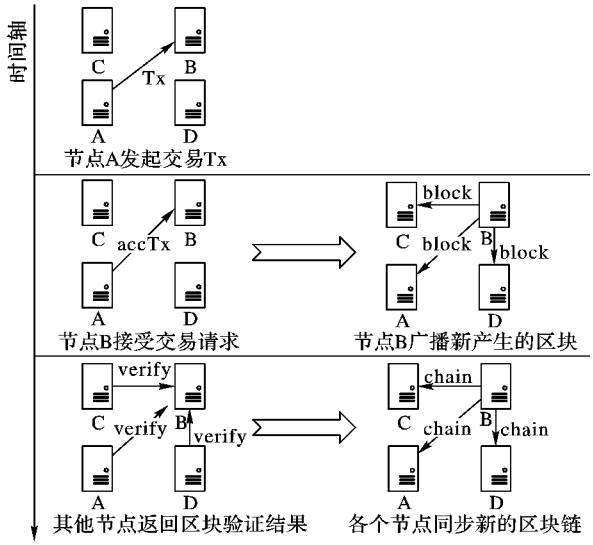


图 3　交易信息存储机制

Fig. 3　Transaction information storage mechanism

2)构造区块。

数字作品区块链网络中的矿工构造区块分为同步区块链、构造新区块 $B_n$($B_n$ 指不含 *nonce* 的区块 $B$)和挖矿产生完整区块 $B$ 三大步骤,详细流程如图 4 所示。

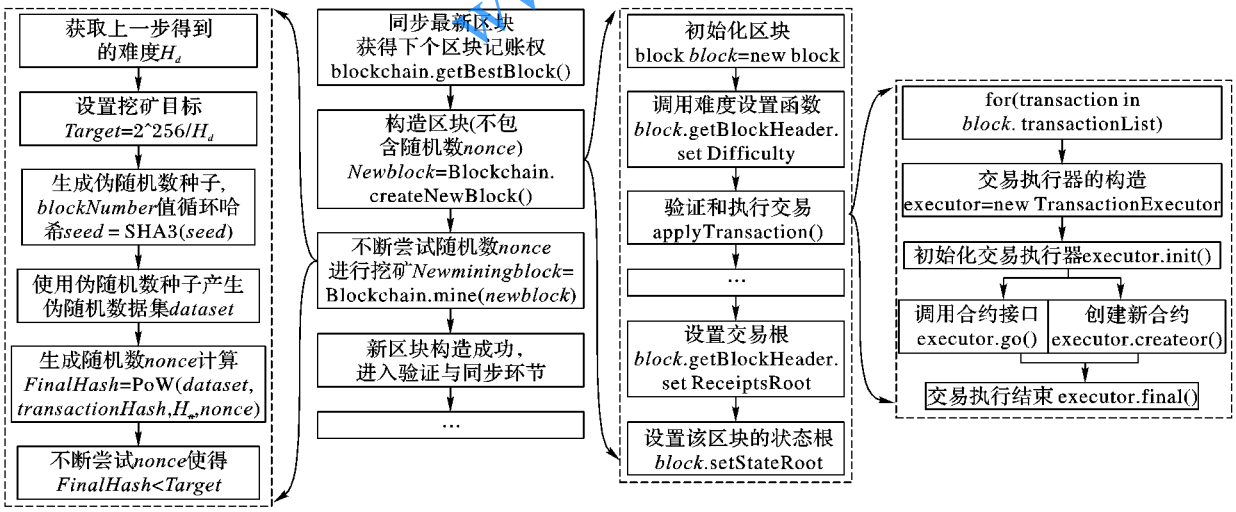


图 4　数字作品区块链网络矿工构造区块流程

Fig. 4　Produce of constrution blocks by miners in digital work blockchain network

1)构造新区块 $B_n$。

数字作品区块链网络中的矿工通过同步最新区块链获得下一个区块的记账权,对一段时间内网络中未确认的交易进行收集 $T=\{T_1,T_2,\cdots,T_n\}$。调用数字作品区块难度值设置函数得到新区块头的难度值 $H_d$,用于设定下一步的挖矿目标 $Target$。在交易执行和验证阶段,对收集到的交易进行验证包括交易签名的合法性和账户的合法性,验证通过的交易将被执行。交易执行完成返回设定区块交易根,即通过 trie 前缀树(Merkle Patricia Tree, MPT)编码的返回值。此外,根据数字作品区块所包含信息进行信息的计算和收集,数字作品区块信息详见图 5。由此,构造出不包含随机数的数字作品区块 $B_n$。

2)挖矿算法执行构建区块 $B$。

根据 $B_n$ 的区块头难度值 $H_d$,定义该区块的难度系数为 $Target$,$Target=2^{256}/H_d$,生成随机数 $nonce$ 值,输入 PoW 函数计算得到 $FinalHash$,若其小于 $Target$,则挖矿成功。该过程形式化描述为式(3):

$$F \leqslant \frac{2^{256}}{H_d} \&\& F = \mathrm{PoW}(H_*, Tx, nonce, dataset) \tag{3}$$

其中：$F$ 表示符合条件的 $FinalHash$，PoW 为工作量证明函数，$H_n$ 为 $B_n$ 的区块头，$nonce$ 为随机实验值，$dataset$ 为该区块的伪随机种子产生的数据集，详细产生流程见图 4。$Tx$ 为数字作品区块 $B$ 中确认交易的哈希值。通过不断尝试 $nonce$ 的机制保证矿工的工作量，抵制分布式拒绝服务（Distributed Denial of Service，DDoS）攻击。成功构造的区块信息如图 5 所示。

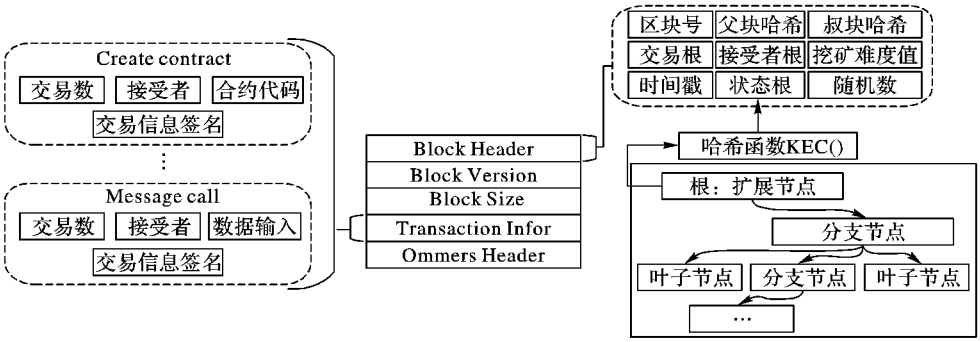


图 5 数字作品区块链网络区块信息

Fig. 5 Block information in digital works blockchain network

3）区块的合法性验证与链接。

矿工在构造出新的数字作品区块后，在网络广播该区块，其他节点对区块进行合法性验证，若该区块合法即同步新区块到数字作品区块链上，该过程的详细描述如图 6 所示。

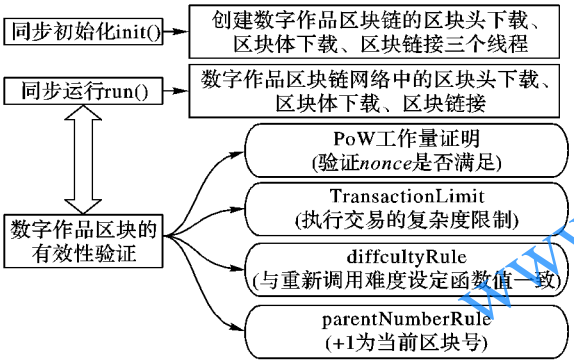


图 6 数字作品区块同步

Fig. 6 Synchronization of digital work blocks

如图 6 所示，数字作品区块的同步分为两大阶段：初始化和运行。在运行阶段，对同步的数字作品区块进行一些验证，包括：交易验证、区块头验证和工作量证明验证。图 6 展示常规的验证项。

其中，数字作品区块链接的形式化表述如式（4）所示：

$$\alpha_{t+1} = \zeta(\cdots\gamma(\gamma(\alpha_t, T_0), T_1)\cdots) \tag{4}$$

其中：$t+1$ 产生的新区块 $B$，确认的交易包括 $\{T_1, T_2, \cdots, T_n\}$，$\zeta$ 表示经区块 $B$ 链接的数字作品区块链状态转换函数，$\gamma$ 表示单个有效交易引起的数字作品区块链的状态转变函数，$\alpha_t$ 表示 $t$ 时刻的数字作品区块链状态，$\alpha_{t+1}$ 表示添加新区块 $B$ 后的数字作品区块链状态。经过链接，交易才被真正确认并永久记录到数字作品区块链上，此时其他节点同步新区块获得记账权。

4）交易信息存储机制实现。

通过以上三个步骤，存储的整体实现流程如下：

协议 1 版权信息存储协议。

Input: A set $N$ of Nodes in the network, the new block $M$
Input: The copyright blockchain, $B\{b_0, b_1, \cdots, b_n\}$
Input: $T_{end}$, the end of create block phase
1) procedure STORE($N$, $M$, $B$, $T_{end}$)
2) $P = \{T_1, T_2, \cdots, T_n\}$
3) createBlockhader $H()$ without $nonce$ and $mixhash$
4) if $time < T_{end}$ then
5) foreach $nonce$ do
6) if $nonce <= 2^{256}/H_d$ && $mixhash = H(mixhash)$ then
7) if ($nonce$, $mixhash$) = PoW() then
8) foreach $n \in N$ do
9) verify($M$)
10) if $M$ = True then
11) $B'$ = AddBlock($B$, $M$)
12) foreach $n \in N$ do
13) distributeBlockchain($B'$, $n$)
14) else updateTime()
15) end procedure

## 2.3 基于智能合约的版权管控协议

本文模型设计了以智能合约为驱动的版权管控协议，该协议主要由版权登记合约（Copyright Registration Contract，CRC）、版权查询合约（Copyright Inquiry Contract，CIC）、版权转让合约（Copyright Transfer Contract，CTC）三个部分构成。

1）版权登记合约。版权登记合约用于用户登记自己的数字知识产权。用户在注册账户的时候会同时在区块链上部署一份 CRC 合约，通过构造函数初始化合约拥有者。在用户调用 CRC 合约时，该合约会预先检测交易发起方的信息 $msg$，若合约的调用者不是该份合约的拥有者，则无法向区块链上写入自己的数字知识产权；若成功登记新的数字作品之后，CRC 合约会返回由文件特征值提取的 Hash 值作为该数字作品的 DCI。

该合约设计如下：

协议 2 版权登记合约。

Input: $tx$, the object of transaction
Output: if error, throw exception else return DCI
1) procedure register($tx$)
2) if msg. sender = $owner$ then
3) $tx$ = new Transaction ();
4) $tx$. name = $tx$. name;
5) $tx$. time = now;
6) $tx$. content = $tx$. content;
7) $hash$ = generateDCI();
8) writeToBlock($tx$);
9) return $hash$;
10) end if
11) end procedure

2)版权查询合约。版权查询合约为用户提供权限管理途径以及其他用户对该数字作品版权的查询等操作。作品拥有者通过调用 CIC 合约管理用户授权列表,只有处于列表中的用户才有查看作品的权限。授权列表 *Authorized List* 中存放被授权用户的公钥 *Puk*,当其他用户调用合约查询某一数字作品时,CIC 合约会先检查该用户是否有权限访问(即该用户的公钥是否存在于授权列表中),若存在,被查询的数字作品数据会先经过查询用户的公钥 *Puk* 加密后再返回给用户,用户使用自己的私钥 *Prk* 解密即可获取到版权信息,确保了在传输过程中的数字作品不会被他人截获。

该合约设计如下:

协议 3　版权查询协议。

```
Input: tx, the object of transaction
Output: dataSet, encrypted with Puk
1)  List [ ] authorized;
2)  procedure query(tx)
3)    if msg. sender in authorized = True then
4)      Puk = authorized[ msg. sender] . puk;
5)      data = encrypt( dataset, Puk) ;
6)      return data;
7)    end if
8)  end procedure
```

3)版权转让合约。版权转让合约可以让用户之间交易自己数字作品的版权,为版权的管控更具灵活性。当两方协商好交易的数字作品后,版权的购买方发起版权转让请求,版权拥有者收到请求后,调用 CTC 合约的版权转让协议触发转让事件。若版权拥有者同意此次交易,CTC 合约将不受干预的进行版权转移并且调用 transfer 函数执行转账操作;若版权拥有者不同意则直接从交易队列中弹出该笔交易即可。

该合约设计如下:

协议 4　版权转让合约。

```
Input: tx, the object of transaction
1)  procedure receiveTx(tx)
2)    if msg. sender = owner then
3)      if tx. operation == True then
4)        transfer( tx. to, tx. from)
5)        digitalWork = getCIC( tx. hash) ;
6)        removeFrom( owner, digitalWork) ;
7)        linkTo( tx. buyer, digitalWork) ;
8)      end if
9)      pop( tx) ;
10)   end if
11) end procedure
```

如图 7 展示了合约的基本结构和映射关系。

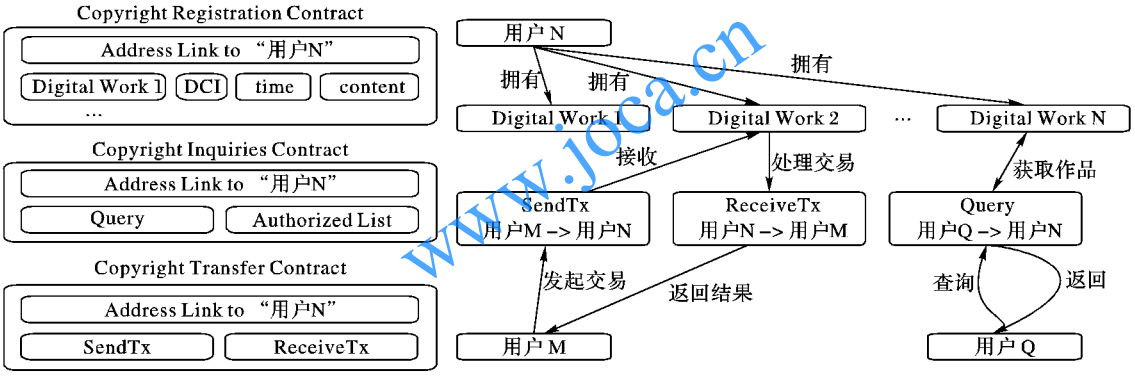




图 7　合约的结构和映射关系

Fig. 7　Structure and mapping relationship of contracts

## 3　模型安全性实验与分析

本章从数字作品区块构造安全性、模型架构安全性和模型性能三方面对模型整体的安全性进行实验与分析。

### 3.1　伪造区块攻击控制

数字作品区块链网络中的节点总是会维护最长的主链,若存在攻击者想要制造伪造区块,试图撤回某些操作,那么他必须做到比诚实节点更快地制造出代替性区块,让分支超过主链长度成为新的主链[17]。如图 6 所示,当分支链的长度超过主链,那么原主链上分叉后的区块将作为无效区块处理,那么攻击者的目的就达成了。

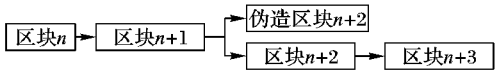


图 8　伪造区块攻击示意图

Fig. 8　Diagram of forged block attack

假定诚实节点制造出下一节点的概率为 $\mu$,攻击者制造出下一节点的概率为 $\nu$,攻击者能够弥补 $z$ 个区块差距的概率为 $\nu_z$。那么,可以得到:

$$\nu_z = \begin{cases} 1, & \mu \leqslant \nu \\ (\nu/\mu)^z, & \nu < \mu \end{cases} \tag{5}$$

假设 $\nu < \mu$,攻击者攻击成功的概率 $P$ 随着区块差距 $z$ 增长呈指数下降。

假设诚实区块将耗费平均预期时间以产生一个区块,那么攻击者的潜在进展就是一个泊松分布,分布的期望值为:

$$\lambda = z\frac{\mu}{\nu} \tag{6}$$

当此情形,为了计算攻击者追赶上的概率,本文将攻击者取得进展区块数量的泊松分布的概率密度,乘以在该数量下攻击者依然能够追赶上的概率。

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (\mu/\nu)^{(z-k)}, & k \leqslant z \\ 1, & k > z \end{cases} \tag{7}$$

通过对 $\nu = 0.1$ 和 $\nu = 0.3$ 两种概率进行仿真实验,可以得到伪造区块攻击概率 $P$ 和攻击者与主链区块差距 $z$ 之间的关系,如表 1 所示。

根据表 1 的仿真数据绘制折线图,从图 9 可以直观地看出,在 $z$ 的数值大于 5 时,$P$ 无限接近于零。

表 1 伪造区块攻击仿真实验数据集

Tab. 1 Data set of forged block attack simulation experiment

| $\nu=0.1$ | | $\nu=0.3$ | |
|---|---|---|---|
| 攻击者与主链区块差距 $z$ | 伪造区块攻击概率 $P$ | 攻击者与主链区块差距 $z$ | 伪造区块攻击概率 $P$ |
| 0 | 1.000 000 | 0 | 1.000 000 |
| 1 | 0.204 587 | 5 | 0.177 352 |
| 2 | 0.050 978 | 10 | 0.041 660 |
| 3 | 0.013 172 | 15 | 0.010 101 |
| 4 | 0.003 455 | 20 | 0.002 480 |
| 5 | 0.000 914 | 25 | 0.000 613 |
| 6 | 0.000 243 | 30 | 0.000 152 |
| 7 | 0.000 065 | 35 | 0.000 038 |
| 8 | 0.000 017 | 40 | 0.000 009 |
| 9 | 0.000 005 | 45 | 0.000 002 |
| 10 | 0.000 001 | 50 | 0.000 001 |

若要使 $\mu < \nu$，则要求攻击者能提供的算力必须能超过整个区块链网络。但由于区块链网络中拥有大量的节点，其算力十分巨大，所以这种情况的概率几乎为零。

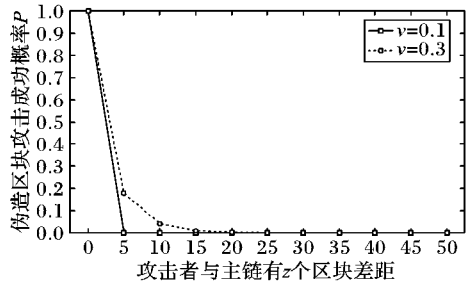


图 9 伪造区块成功概率趋势

Fig. 9 Probability of successful probability of forged blocks

综上分析可知，数字作品区块链网络对于抵抗伪造区块攻击的有很好的鲁棒性。

### 3.2 架构安全性分析

现行的系统几乎都是以中心服务器为核心的体系架构，传统的关系数据库导致数据存放过于集中化，数据的安全性依赖于中心服务器安全性，多数数据的泄露均是由于黑客对服务器的攻击，例如 DDoS 攻击、SQL（Structured Query Language）注入攻击、CC（Challenge Collapsar）攻击等[16]。

而本文模型采用去中心化的架构模式使得区块信息由网络中的节点共同维护，即使黑客控制了区块链网络中的有限个节点，也不会影响该系统模型的正常运作；而且区块链中的数据信息经过了私钥加密，进而保证了数据的机密性。如图 10 所示，如果黑客对区块信息进行篡改，由于区块头验证非法，被攻击节点会被其他诚实节点排斥。这样的机制抵制了所有针对传统数据存储模式的攻击。

### 3.3 模型性能实验分析

本节采用的实验环境为 6 个节点，满足拜占庭一致性算法的要求。随着区块包含交易的数量增加，计算区块所花费的时间也越来越多。

对模型性能的要求，即对模型处理交易的速度的要求，本文定义计算处理交易速度的方式如下：

$$\text{平均交易速度} = \sum_{i=1}^{n} t_i \Big/ \sum_{i=1}^{n} s_i \tag{8}$$

$$\text{峰值交易速度} = \max(t_i/s_i) \tag{9}$$

其中：$n$ 为已打包交易的区块数，$t_i$ 为第 $i$ 个区块计算所消耗的时间，$s_i$ 为第 $i$ 个区块所包含的交易数。根据实验得到的区块处理交易速度与包含交易数的关系，如图 11 所示。可以算出该模型每秒平均交易数为 1 536.8，峰值交易速度为每秒 2 152.4，吞吐量已经足够支撑现有平台的运作。

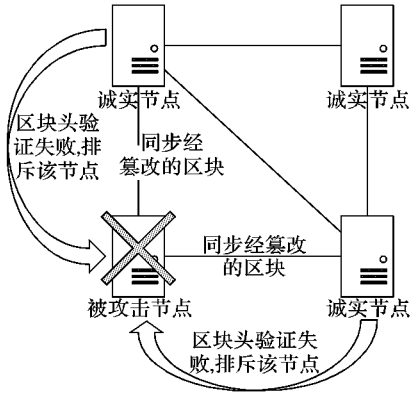


图 10 节点攻击安全性示意图

Fig. 10 Node attack security diagram

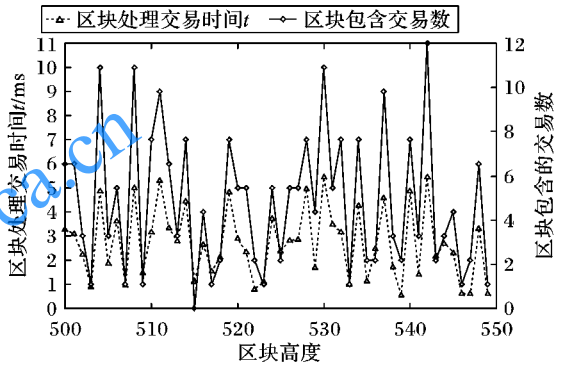


图 11 数字作品区块链网络交易吞吐量

Fig. 11 Transaction throughput of digital work blockchain network

综上实验可知，该模型具有较好的性能，可以满足现有平台的需求。

## 4 结语

本文采用了区块链技术和智能合约，设计了一种去信任的数字作品 DCI 管控模型。该模型设计了基于区块链的版权信息存储协议，保证了版权信息不可篡改；基于智能合约的版权管控协议，自动化执行且不可干预的机制保证了模型运作高效透明。本模型为互联网数字化作品提供版权登记、版权查询、版权交易和保护的全链条一体化去中心化管控服务，为现行数字版权存在的一系列问题提供了行之有效的解决方案，具有广阔的应用前景。最后，仿真与分析表明，该模型在保证版权信息权威的同时安全性高。

但是，区块链技术公开透明的特性是一把双刃剑，它在保证系统透明运作的同时，可能会不经意泄露用户的一些个人信息。下一步将采用动态交易签名技术，例如环签名技术，与区块链技术相结合，在利用好区块链技术不可篡改、公开透明等特性的同时，保护好用户的个人隐私信息。

**参考文献**（References）

[1] 魏玉山. 2015—2016 中国数字出版产业年度报告[J]. 印刷杂志, 2016(8):8-12.（WEI Y S. 2015—2016 China digital publishing industry annual report [J]. Print Magazine, 2016(8): 8-

12.)
[2] BLESSING L T M, CHAKRABARTI A. DRM, a Design Research Methodology[M]. London: Springer, 2009:4 - 10.
[3] 周全. "嵌入式"版权服务组件管理平台设计与实现[D]. 北京: 北方工业大学, 2015. (ZHOU Q. "Embedded" copyright service component management platform design and implementation [D]. Beijing: North China University of Technology, 2015.)
[4] 游福成, 郑良斌, 曾广平. 基于数字水印与移动 Agent 的数字版权保护系统设计[J]. 中南大学学报(自然科学版), 2007, 38(S1):1087 - 1091. (YOU F C, ZHENG L B, ZENG G P. Design of digital copyright protection system based on digital watermarking and mobile Agent [J]. Journal of Central South University (Natural Science Edition), 2007, 38(S1):1087 - 1091.
[5] 田园. P2P 内容分发网络的数字版权保护系统研究[D]. 北京: 北京邮电大学, 2012. (TIAN Y. P2P content distribution network digital copyright protection system research [D]. Beijing: Beijing University of Posts and Telecommunications, 2012.)
[6] 中华人民共和国国家版权局. DCI 体系将成互联网版权基础设施[EB/OL]. [2017-03-02]. http://www.ncac.gov.cn/chinacopyright/contents/4509/316473.html. (National Copyright Administration of the People's Republic of China. The DCI system will become an Internet copyright infrastructure[EB/OL]. [2017-03-02]. http://www.ncac.gov.cn/chinacopyright/contents/4509/ 316473.html.)
[7] GRINBERG R. Bitcoin: an innovative alternative digital currency [EB/OL]. [2017-03-01]. http://www.bitcointrading.com/pdf/bitcoinbyreubengrinberg.pdf.
[8] SASSON E B, CHIESA A, GARMAN C, et al. Zerocash: decentralized anonymous payments from bitcoin[C]// Proceedings of the 2014 IEEE Symposium on Security & Privacy. Piscataway, NJ: IEEE, 2014:459 - 474.
[9] SWAN M. Blockchain: Blueprint for a New Economy[M]. Sebastopol: O'Reilly Media, Inc., 2015: 20 - 37.
[10] PREE W. Blockchain : technology and applications [EB/OL]. [2017-03-02]. http://docplayer.net/42277669-Blockchain-technology-and-applications.html.
[11] ZHAO J L, FAN S, YAN J. Overview of business innovations and research opportunities in blockchain and introduction to the special issue[J]. Financial Innovation, 2016, 2(1): 28.
[12] NORTA A. Creation of smart-contracting collaborations for decentralized autonomous organizations[C]// Proceedings of the 14th International Conference on Business Informatics Research. Berlin: Springer International Publishing, 2015: 3 - 17.
[13] GARAY J A. Blockchain-based consensus[C]// Proceedings of the 19th International Conference on Principles of Distributed Systems. Dagstuhl: Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2016: 2 - 4.
[14] SZABO N. Formalizing and securing relationships on public networks[EB/OL]. [2016-11-20]. http://journals.uic.edu/ojs/index.php/fm/article/view/548/469.
[15] KOSBA A, MILLER A, SHI E, et al. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts[C]// Proceedings of the 2016 IEEE Symposium on Security and Privacy. Piscataway, NJ: IEEE, 2016:839 - 858.
[16] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system [EB/OL]. [2016-11-20]. http://www.infres.telecom-paristech.fr/people/urien/blockchain_urien_2017.pdf.
[17] SIMMONS C, ELLIS C, SHIVA S, et al. AVOIDIT: a cyber attack taxonomy[EB/OL]. [2016-11-20]. http://www.teraits.com/pitagoras/marcio/segapp/CyberAttackTaxonomy_IEEE_Mag.pdf.

This work is partially supported by the National Natural Science Foundation of China (61602096), the China Postdoctoral Science Foundation (2015M572464), the Science and Technology projects in Sichuan Province (2016ZC2575, 2015JY0178).

**LI Yue**, born in 1997. Her research interests include blockchain, digital currency.

**HUANG Junqin**, born in 1995. His research interests include blockchain, smart contract network, telecommunication.

**WANG Ruijin**, born in 1980. Ph. D., lecturer. His research interests include information system security, quantum communication security, cloud security.

(上接第 3280 页)

[7] WANG F, HUANG Z, YU H, et al. EESM-based fingerprint algorithm for WiFi indoor positioning system [C]// Proceedings of the 2013 IEEE International Conference on Communications in China. Piscataway, NJ: IEEE, 2013: 674 - 679.
[8] 林子. 用 Dundas 制作箱形图 Box Plot [EB/OL]. (2007-09-04) [2017-04-25]. http://www.cnblogs.com/linfuguo/archive/2007/09/04/878345.html. (LIN Z. Make box plot with Dundas [EB/OL]. (2007-09-04) [2017-04-25]. http://www.cnblogs.com/linfuguo/archive/2007/09/04/878345.html.)
[9] SAMIH E, JOAO P, FILIPE M. Removing useless APs and fingerprints from WiFi indoor positioning radio maps [C]// Proceedings of the 2013 International Conference on Indoor Positioning and Indoor Navigation. Piscataway, NJ: IEEE, 2013: 1 - 7.
[10] 原志强,赵春艳. 两种改进的模拟退火算法求解大值域约束满足问题[J]. 计算机应用研究,2017,34(12):1 - 9. (YUAN Z Q, ZHAO C Y. Two improved simulated annealing algorithms for solving constraint satisfaction problems with large domains [J]. Application Research of Computers, 2017, 34(12): 1 - 9.)
[11] DEVIJVER P A, KITTLER J. Pattern recognition: a statistical approach [J]. Image and Vision Computing, 1985, 3(2): 87 - 88.
[12] LI B, SALTER J, DEMPSTER A G, et al. Indoor positioning techniques based on wireless LAN [C]// Proceedings of the 2006 IEEE International Conference on Wireless Broadband and Ultra Wideband Communications. Piscataway, NJ: IEEE, 2006: 13 - 16.

**LI Xinchun**, born in 1963, senior engineer. His research interests include wireless sensor network, embedded system, digital image processing.

**HOU Yue**, born in 1992, M. S. candidate. Her research interest include wireless sensor network.