**中国大学生服务外包创新创业大赛**

**项目详细方案**

**作品名称： 基于区块链的艺术品数字资产确权流通系统**

**电子邮箱：** [**741026400@qq.com**](mailto:741026400@qq.com)

**提交日期： 2022.04.17**

# 摘要

近年来，随着计算机的普及和网络技术的进步，数字艺术品的交易越来越流行，而与之不匹配的是传统的交易系统仍存在着严重的确权问题。此外，艺术品在交易的流通过程中，来源难以确定，真实性难以鉴定，交易容易被抵赖等问题也亟待解决。同时，数字艺术品因为其易复制易传播等特点，导致作者对艺术品的版权维护和溯源变得更加困难，而且艺术品的内容合规性也难以保证。针对以上问题，本项目设计并实现了基于区块链和NFT技术的数字资产确权流通系统，同时通过均值Hash算法实现了内容级的版权保护，并通过第三方审核保证艺术品内容的合规性。旨在填补传统交易系统的不足，为艺术品交易提供一个便捷可信的平台以促进艺术品交易的良性发展。

本系统包含用户服务网站、区块链和数据库三个模块。针对艺术品的确权问题，首先本系统利用区块链技术，实现用户身份与区块链账户地址的绑定关系。然后当用户上传艺术品时，系统通过hash算法实现对艺术品的唯一标识。最后调用部署于区块链上的智能合约，生成包含艺术品唯一标识符与用户账户地址的NFT并上传至区块链，通过对NFT的查询，即可确定艺术品当前拥有者的账户地址，而账户地址可以唯一确定某一用户的真实身份，进而实现艺术品的确权流通；针对艺术品溯源，真实性鉴定，交易抵赖等问题，本系统利用区块链和数据库技术，将每次交易信息保存在数据库中，通过对艺术品id的查询，即可得到其历史交易信息，进而解决了上述问题。此外，系统会为每次交易生成并保存交易Hash，可以通过交易Hash在区块链上查询交易信息，进一步保证了交易的不可抵赖；针对版权问题，本系统采取均值Hash算法，通过计算艺术品哈希指纹的海明距离来量化艺术品间的相似度，实现了高效准确的查重，进而实现有效的版权保护。同时，本系统通过第三方审核保证了艺术品内容的合规性。

不同于传统的艺术品交易系统，本系统的核心在于将传统电商模式与区块链和NFT等技术相结合，解决了传统交易市场艺术品中艺术品交易难以确权流通的问题。除此以外，本系统还提出并建立了数据库+区块链的双库模式，在实现艺术品交易确权流通的同时还提高了交易的效率；采用均值hash算法对艺术品进行查重，在保证效率和精度的基础上，有效实现了艺术品的版权保护；引入第三方人工审核部分，对艺术品的内容进行审核，有效保证了艺术品内容级的合规性；内置钱包账户，为用户省略了复杂的区块链钱包注册和使用等步骤，降低了人们参与艺术品交易的门槛。简而言之，本系统在一定程度上填补了传统交易系统的不足，可以作为一个便捷可信的平台应用到艺术品交易中去，促进艺术品交易的良性发展。

**关键字：NFT；区块链；确权流通**

目录

[摘要 2](#_Toc101099154)

[第一章 项目概述 5](#_Toc101099155)

[1.1 项目背景 5](#_Toc101099156)

[1.2 系统介绍及特色描述 5](#_Toc101099157)

[1.2.1基于区块链技术实现艺术品确权流通 6](#_Toc101099158)

[1.2.2基于Hash算法的版权保护 6](#_Toc101099159)

[1.2.3基于第三方审核的内容级合规性保证 6](#_Toc101099160)

[1.2.4基于系统内置钱包账户的便捷交易 6](#_Toc101099161)

[1.3相关知识 7](#_Toc101099162)

[1.3.1NFT 8](#_Toc101099163)

[1.3.2 区块链 8](#_Toc101099164)

[1.3.3 智能合约 8](#_Toc101099165)

[1.3.4均值Hash技术 8](#_Toc101099166)

[第二章 确权交易系统分析及设计 7](#_Toc101099167)

[2.1整体方案设计 7](#_Toc101099168)

[2.1.1 业务需求说明 7](#_Toc101099169)

[2.1.2 总体模型 7](#_Toc101099170)

[2.2系统功能实现 9](#_Toc101099171)

[2.2.1系统功能总述 9](#_Toc101099172)

[2.2.2 web服务器模块 10](#_Toc101099173)

[2.2.3数据库模块 11](#_Toc101099174)

[2.2.4区块链模块 11](#_Toc101099175)

[2.3系统流程设计 12](#_Toc101099176)

[2.3.1用户信息管理流程 12](#_Toc101099177)

[2.3.2艺术品上传流程 13](#_Toc101099178)

[2.3.3艺术品上架流程 14](#_Toc101099179)

[2.3.4艺术品购买流程 15](#_Toc101099180)

[2.4 数据库设计 15](#_Toc101099181)

[2.4.1 功能需求 15](#_Toc101099182)

[2.4.2 安全性与完整性需求 15](#_Toc101099183)

[2.4.3 概念结构设计 16](#_Toc101099184)

[2.4.4 逻辑结构设计 16](#_Toc101099185)

[2.4.5数据库实现系统功能说明 19](#_Toc101099186)

[第三章 技术架构 21](#_Toc101099187)

[3.1基于NFT实现的艺术品数字资产确权机制 21](#_Toc101099188)

[3.1.1NFT数据结构的实现 21](#_Toc101099189)

[3.1.2资产确权的实现原理 21](#_Toc101099190)

[3.2基于区块链实现的交易安全性机制 22](#_Toc101099191)

[3.2.1 共识机制 22](#_Toc101099192)

[3.2.2 智能合约 23](#_Toc101099193)

[3.3基于均值hash算法的版权保护机制 23](#_Toc101099194)

[3.3.1均值Hash介绍 23](#_Toc101099195)

[3.3.2图像匹配算法 24](#_Toc101099196)

[3.3.3均值hash实现的版权保护 24](#_Toc101099197)

[3.4双库管理 25](#_Toc101099198)

[3.4.1实现方案 25](#_Toc101099199)

[3.4.2主要优势 25](#_Toc101099200)

[第四章 作品测试与分析 27](#_Toc101099201)

[4.1 测试环境搭建 27](#_Toc101099202)

[4.1.1测试设备 27](#_Toc101099203)

[4.1.2平台配置 27](#_Toc101099204)

[4.2 功能测试 28](#_Toc101099205)

[4.2.1用户信息管理测试方案 28](#_Toc101099206)

[4.2.2创作管理测试方案 30](#_Toc101099207)

[4.2.3购买流程测试方案 34](#_Toc101099208)

[4.3结果分析 37](#_Toc101099209)

[4.3.1可行性分析 37](#_Toc101099210)

[4.3.2安全性分析 37](#_Toc101099211)

[第五章 实践应用 38](#_Toc101099212)

[5.1 产业前景 38](#_Toc101099213)

[5.2 可行性分析 38](#_Toc101099214)

[5.2.1市场可行性 38](#_Toc101099215)

[5.2.2技术可行性 38](#_Toc101099216)

[5.2.3资源可行性 39](#_Toc101099217)

[5.3 应用环境与应用对象 39](#_Toc101099218)

[5.4业务模式 39](#_Toc101099219)

[第六章 总结 41](#_Toc101099220)

[文献引用 42](#_Toc101099221)

# 第一章 项目概述

## 1.1 项目背景

进入新世纪以来，全球传统艺术品市场传承有序，迎来了几十年的高速发展。但在繁荣背后及高速发展放缓后，大量问题暴露无遗。例如艺术品的真实性难以鉴别、艺术交易的安全性得不到保障，艺术品的来源难以追寻等等。

传统艺术品交易市场的典型特征就是模糊与非公开性，这使得收藏家在鉴定和购买艺术品时往往需要花费大量的时间和精力。当收藏家们之间试图要交易艺术品时，他们就不得不向一位中间人披露藏品的信息。然而，作为第三方的介绍人通常来说，不仅很有可能会向买方收取高昂的中介费用，而且还有可能外泄有价值的信息。并且传统艺术品交易原本是一个封闭、地域性明显、且低频次的商业活动，很容易受到地域，语言等物质限制，不利于艺术品在全球市场中的流转。‎而艺术品又讲究流通性，若是缺乏流通性，市场规模与收藏群体总量的基本盘即会变小。以及在传统市场中，每次交易都是一锤子买卖。内容创作者只能获得第一次交易的部分或全部收益。在传统艺术品市场，无论是买家还是卖家，进入门槛都相当高，也在一定程度上限制了艺术品流转。而NFT艺术作品对于艺术承载形允许高标准的自由形式，可以是一段视频，可以是一幅画，甚至可以是一段话，这就使得艺术作品在内容上得到灵活的呈现。

随着区块链的兴起与快速发展，链上世界的数字资产引发了学术界和产业界的广泛关注。与现实物理世界中的同质化资产和非同质化资产相对应，链上的数字资产也分为同质化数字资产和非同质化数字资产，其中最常见的同质化数字资产包括比特币、以太币等“虚拟货币”，而非同质化数字资产包括游戏项目、数字艺术品等非同质化通证。NFT使得联通现实物理世界和虚拟网络世界成为可能，已成为智能经济中心的核心要素。

NFT数字作品交易平台的出现，将有力解决传统艺术品交易的问题。在NFT数字作品交易平台，只存在买卖双方，有效解决传统艺术品市场的中介过多问题。同时，NFT采用了区块链底层技术，而区块链是按照时间顺序对系统中的每笔交易记录进行链式排列，也就是说每项记录都按照规律排列、彼此关联。每件NFT作品是可追溯的，还会打上时间戳等特性，总之，想篡改NFT上的数字作品，付出代价要远大于传统艺术品。并且NFT的出现，为所有数字内容创作者提供更公平的支付机制。 在这种公平的环境下 ，创作者可以轻松地将他们的作品货币化，有效简化流程并增加透明度，还可消除传统市场中存在的摩擦，跨越不同币种带来的鸿沟，这让艺术品在全球市场几乎0成本流转成为现实。在NFT中，每次当数字艺术被转售，原作者都能收到每笔NFT销售的一定比例。 因此，来自原始销售下游发生的所有经济活动的创作者和艺术家， 通过这种方式，作者获得了永久收益。NFT在具体布局上，始终秉承着让人人都能在区块链上自由创作的价值导向。

## 1.2 系统介绍及特色描述

基于区块链的艺术品数字资产确权流通系统，将有力解决传统艺术品交易中存在的问题。本系统的主要功能包括1.针对艺术品的操作功能；2.用户使用网站需要的基础功能；3.其他网站管理功能。系统架构主要包括四个部分：1.用于实现用户交互的网站服务器；2.管理数据信息的后台数据库；3.记录NFT和其交易信息的区块链4.存放艺术品完整信息的web资源服务器。

系统实现了以下四个主要内容：①艺术品的确权流通。本系统通过将艺术品数字化的标识和其创作者身份ID以及后续的拥有者身份ID上传到区块链上进行绑定生成NFT,实现艺术品的确权流通。②有效的版权保护。本系统通过图像hash算法对每一份艺术品生成唯一的标识符，有效避免了可能产生的侵权问题。③内容级的审查机制。本系统添加了艺术品后台审核功能，可以避免系统作品出现内容上的问题。④简洁的交易手续。本系统通过为每一个用户账户设置一个钱包，在交易时进行只需要通过钱包转账，极大地方便了国内用户参与NFT艺术品交易。

### 1.2.1基于区块链技术实现艺术品确权流通

传统艺术市场上版权不易管理，原因主要在于不易确权和历史交易信息不易追溯，艺术品创作者经常因为疲于维权而任由盗版横行。针对此问题，本系统设置了身份绑定与根据艺术品信息铸造NFT功能。身份绑定即在用户注册时，系统将用户提供的身份标识UID（User ID）和注册时的区块链上的账户CA(Chain accountant)绑定。铸造NFT功能即在用户进行上传艺术品时，将UID和其作品的唯一标识AID(Art ID)发送到区块链上共同生成NFT。利用NFT的不可分割性和独有唯一性，和区块链上数据的不可篡改性和可追溯性，使艺术品的交易公开透明，进而实现艺术品的确权流通。

### 1.2.2基于Hash算法的版权保护

在用户上传作品时，我们采用唯一性较强的hash算法得到艺术品的唯一标识AID，同时通过鲁棒性较强的hash算法生成艺术品的AIDP。AID作为艺术品的唯一标识，当系统检测到数据库中新上传艺术品的AID已经存在时，即存在相同艺术品时，直接返回给创作者审核不通过的结果。而AIDP则用于相似性检验，我们认为相同或相似AIDP则代表该艺术品在一定程度上存在抄袭或恶意修改已有艺术品的行为。当系统检测到拥有相同或相似AIDP的艺术品时，就会将这些艺术品发送到后台审核，经由人工审核，审核通过后才予以上传。从而实现了艺术品的版权保护。

### 1.2.3基于第三方审核的内容级合规性保证

不同于传统的NFT交易系统，用户在创作完艺术品后即可直接发布，本系统的用户在创作完艺术后需要通过第三方审核人员对其具体内容进行审查。对于不合规的艺术品，系统会拒绝用户的上传请求，不为其作品生成NFT。

### 1.2.4基于系统内置钱包账户的便捷交易

传统nft交易系统交易货币使用虚拟货币，但是虚拟货币在国内不合法，而且其价值极不稳定等，难以实现保值；同时虚拟货币的购买过程尤其是在国内十分繁琐。因此本系统在用户支付层面绕过虚拟货币，使用在系统内置的钱包账户作为支付手段。以简洁的方式完成交易，极大地方便了国内用户参与NFT艺术品交易。同时，真实货币交易的方式让用户不必担心虚拟货币价值波动的问题。

## 1.3相关知识

### 1.3.1NFT

本平台使用NFT在区块链的技术支持下作为数字艺术品、活动门票等数字商品的链上权利凭证。其中每个NFT都映射着特定区块链上的唯一序列号，不可篡改、不可分割，也不能互相替代。每一个NFT都代表特定数字艺术品或其限量发售的单个复制品，记录着其不可篡改的链上权利。NFT与虚拟货币等同质化代币存在本质不同，有数字商品的实际价值做支撑，也不具备支付功能等任何货币属性。

本系统中，数字艺术作品的拥有人可以将艺术品的版权信息存储在区块链中，在共识机制下，通过算力竞争获得计算权的节点链接到区块链上，完成版权登记。通过时间戳和NFT中的版权信息成为数字艺术的版权标识，整个登记过程便捷可追溯，无须外界认证机构的确认。除此以外，结合区块链技术，NFT艺术作品在整个生命周期内都可以实现其数字版权的可追溯性。进而实现艺术品的确权流通。

### 1.3.2 区块链

区块链是一种分布式数据库，起源于中本聪在2008年阐述的构架理念中提出的比特币，但是经过13年的发展，它早已脱离比特币独立存在。区块链是一种以链表的形式按照时间顺序将区块通过哈希运算组成的链式结构，其中区块由交易记录组成，区块详细介绍如图所示:

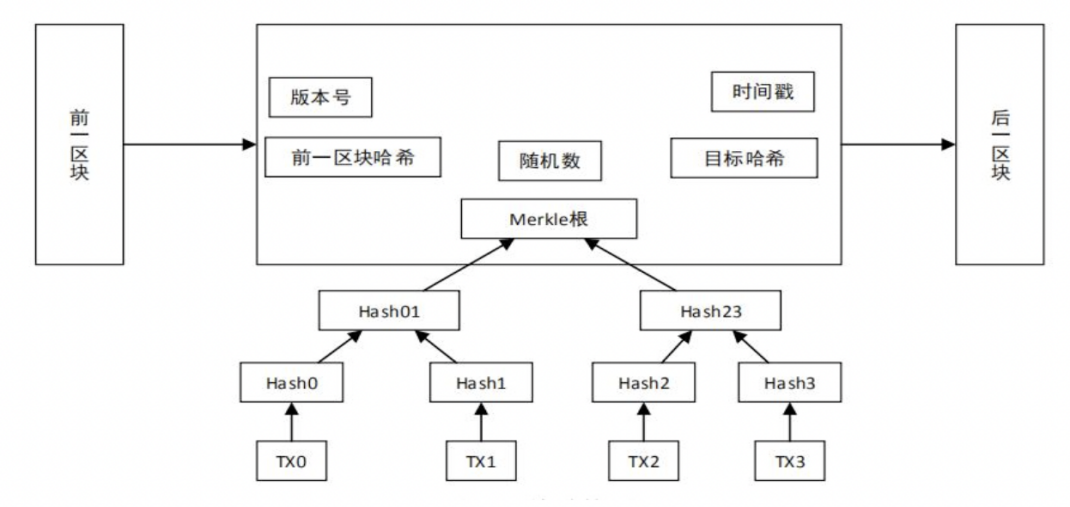


图 1-1 区块结构图

区块链中每一个区块都包含块头和块体两个部分，如上图 所示，块头包含版本号、前一个区块的哈希值、时间戳、一次性随机数和 Merkle 根哈希值，块体是二叉树形式存储的交易数据，交易数据经过多次哈希运算组合后即形成 Merkle 根哈希值。前一个区块哈希值是对前一个区块进行哈希运算的结果，用于连接前一个区块，可以防止对区块进行篡改;时间戳为区块链增加时间维度，是确定相邻区块之间继承关系的时间标签，可以用来保证区块的有序性并防止对区块进行篡改等行为;一次性随机数是一个随机哈希序列的值，是完成工作量的证明，目标值越小寻找随机数的难度就越大;Merkle根哈希值用来检测交易数据是否被篡改，是一种校验数据的验证保险。区块链是一个去中心化的分布式共享账本，具有如下几个特点:

（1） 去中心化:区块链的基本功能，意味着区块链网络中的节点都可以进行记账，数据可以进行分布式存储,不再需要依赖集中式的第三方平台,网络中的某个节点出现故障也不会影响系统的运行，网络中的全部节点共同维护一个账本数据库。

（2）公开透明:区块链中交易对所有节点都是公开透明的，网络中的任意节点可以查询交易信息，这就是区块链可以得到信任的原因，并且可以使用区块链技术创建自己想要的应用程序，实现特定的业务逻辑。

（3）不可篡改:由于区块中保留了前一区块的哈希值，所以区块链中的交易信息一旦被记录到区块中就不会被改变,区块中的任何记录都会被永久的保留，除非有人可以同时操控 51%以上的节点,否则单个节点无法对记录进行更改。

（4）全程留痕，可追溯:区块链记录了每笔交易的输入和输出，并且交易记录对所有节点都是透明的，所以交易信息在区块链中全程留痕，可追溯。

公有链是完全去中心化的区块链，对所有用户完全开放，任何节点都可以访问公有链网络，参与竞争实现共识，进行交易以及共同维护公有链;私有链是一个完全中心化的区块链，只对组织中的节点开放，系统中的节点需要进行授权认证;联盟链是介于公有链和私有链之间的一种部分去中心化的区块链，通常由多个机构共同管理，用于多个联盟成员跨机构进行数据交换，最典型的代表是 Hyperledger Fabric。超级账本 Hyperledger 是由 Linux 基金会主导的开源项目，带有可插入各种功能模块的区块链实施方案。Fabric 是超级账本中一个顶级项目，支持拜占庭容错算法等新的共识机制，引入了权限管理，支持可插拔和可扩展功能。联盟链中使用的共识算法主要是实用拜占庭容错算法(PBFT)，拜占庭错误表示的是由攻击者入侵导致的软件错误或者未知原因的硬件错误，拜占庭容错算法是指在发生该错误的时候保证系统正常运行的容忍算法。实用拜占庭容错算法可以实现当网络中的恶意节点不超过总结点的1/3时，保证网络的安全性。

### 1.3.3 智能合约

智能合约的概念于1995年由 Nick Szabo首次提出，是用户定义的程序，它指定交易的规则，一旦调用则自动强制执行，并且智能合约在每个区块链节点中执行并相互验证，因此计算结果是绝对可信的，所以它可以用来实现人类自动化交互的工具。并且智能合约是以交易的形式被创建和调用的，合约会在网络中的所有节点中执行，因此任何一个节点出现故障都不影响合约的执行。Fabric中智能合约又称为链码，一般是由开发人员使用编程语言(Go，Java 和 node.js 等)编写的不可篡改并自动执行的应用程序代码，是连接客户端与Fabric区块链数据库的重要组件。链码可分为系统链码和用户链码，其中系统链码负责Fabric节点自身的处理逻辑，包括交易背书、系统配置、校验等工作，在 peer 节点启动时会自动完成注册和部署；用户链码由用户编写，负责执行自定义处理逻辑，部署在Fabric的网络节点当中，可以独立的运行在受保护的 Docker 容器中，与相应peer节点通过发送ChaincodeMessage消息进行交互通信。

在NFT相关领域，智能合约是存放在区块链中的一些程序，使网络能够存储 NFT 交易中指示的信息，控制着这些称为 NFT 的数字资产。因此，智能合约是NFT运作的核心。在本平台中，部署智能合约后的交易流程相较于其他传统交易平台有以下优点：

（1）实现交易的低成本与高效性

在艺术品数字资产交易的过程中，NFT的上传与修改均基于智能合约的内容。而智能合约本质上是一串代码，当条件满足时，智能合约将被调用并自动完成交易所导致的NFT的修改等操作，这个过程无需任何人工干预。因此采用智能合约技术参与交易过程，低成本并高效地实现了交易的正常进行。

（2）实现交易过程的可靠性

在NFT技术中，智能合约被写在区块链中。相比传统的存放在计算机中的智能合约，由于区块链本身所具有的不可篡改和高可靠性，使得存放在区块链中的智能合约不能被修改，从而具有了更高的可靠性。与此同时由于智能合约本质上为代码，因此我们也无需担心当条件满足时合约不执行的情况，系统无需干预，便会在条件满足时自动调用智能合约对NFT进行上传和修改。因此通过基于区块链的智能合约，在交易过程中，用户不再需要去相信签订合约的对方，只需要相信系统完成交易的整个操作，实现了革命性的“去信任化”。

### 1.3.4均值Hash技术

均值hash技术主要利用图片的低频成分, 通过缩小图片去除图片的高频成分, 保留低频信息, 并使用图像灰度方法化去除图像色彩来进一步去除高频成分。在此基础上, 计算灰度图的像素平均值。遍历灰度图每一像素, 将其与像素均值做比较, 若大于均值, 则记下1;否则, 记下0, 得到二进制串即为图像Hash值, 也称为图像指纹。具体算法描述如下。

步骤1:将图片缩小到n×n, 共n2个像素;

步骤2:将n×n图片转换为灰度图, 记为Ga;

步骤3:计算灰度图Ga的像素平均值, 记为pavg;

步骤4:遍历Ga中每一个像素pi, 并将pi与pavg进行比较, 若pi≥pavg, 则记下1, 否则记下0, 得到n2个比特的二进制串即为图片a Hash值, 记为Ha;

步骤5:计算两张图片哈希值的海明距离, 距离越小图片越相似, 距离越大图片差异性越大。

将均值hash技术应用到本系统中，与其他交易系统相比，能有效提高本系统的查重精度和查重效率。使系统在保证效率和精度的基础上，有效的实现艺术品的产权保护。

# 第二章 确权交易系统分析及设计

## 2.1整体方案设计

### 2.1.1 业务需求说明

（1）艺术品上传及预览，支持图片、视频、音频及文档等文件；

（2）NFT铸造，为每一份独一无二的数字艺术品生成一个NFT,并支持NFT上链；

（3）后台审核数字艺术品，实现对内容级上的审核和产权保护；

（4）NFT上架及NFT展示浏览；

（5）NFT交易，实现交易透明且可溯源；

（6）用户身份绑定，实现现实世界身份与区块链账户一一对应关系；

（7）系统管理。包括用户账户管理、艺术品NFT管理，订单管理，系统配置等功能。

### 2.1.2 总体模型

基于区块链的艺术品数字资产确权流通系统总体分为三个部分，用户服务、数据库和区块链。用户服务部分分为用户前端和管理后台。

用户与用户服务部分直接交互，用户服务部分完成与数据库和区块链的交互操作，从而实现整体艺术品系统功能。

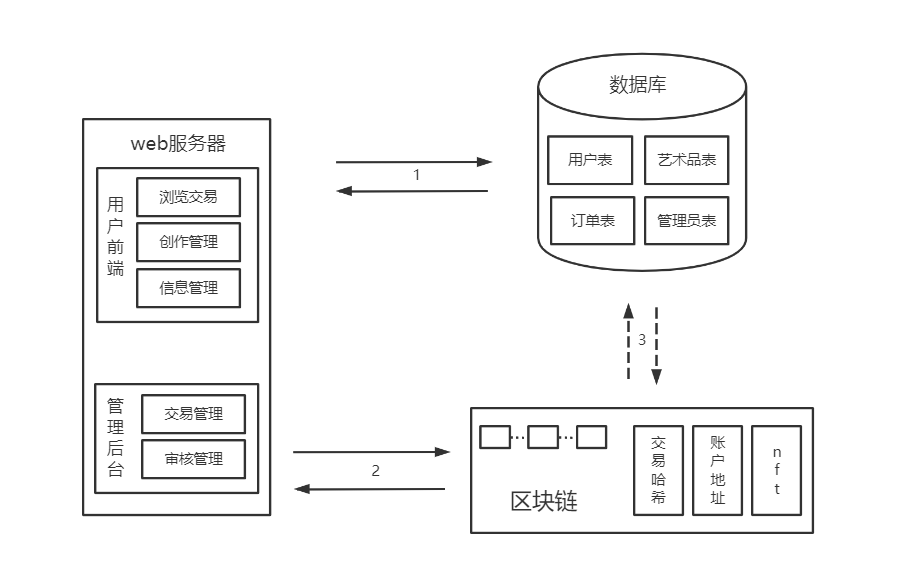


图 2-1 系统功能模块整体划分

系统重点功能大致分为三个功能模块：浏览交易模块、创作管理模块、信息管理模块。

#### 2.1.2.1在浏览交易模块中流程

（1）用户发起购买请求并完成支付，用户服务部分将购买者和拥有者区块链上的账户地址以及该艺术品的唯一标识一起发送到到区块链上。

（2）区块链通过拥有者的账户地址调用智能合约实现NFT的修改，并将交易的hash地址返还给用户服务部分。

（3）用户服务部分进行相关数据库操作。

#### 2.1.2.2在创作管理模块中流程

（1）用户上传作品，用户服务部分根据作品生成唯一标识和作为查重参考的has值，所有信息暂存数据库。

（2）后台调取数据库中未审核艺术品进行审核，审核不通过的结果返回用户服务审核通过后的艺术品传给区块链部分进行上链创作。

（3）审核通过的艺术品写入数据库。

#### 2.1.2.3在信息管理模块中流程

（1）注册时用户提交表单信息后，系统将用户密码上传到区块链上。

（2）区块链在网站拥有的节点下面新建一个账号，并将该账号的地址发送给用户服务部分。

（3）用户服务部分进行数据库操作。

## 2.2系统功能实现

### 2.2.1系统功能总述

系统总体功能图2-1.

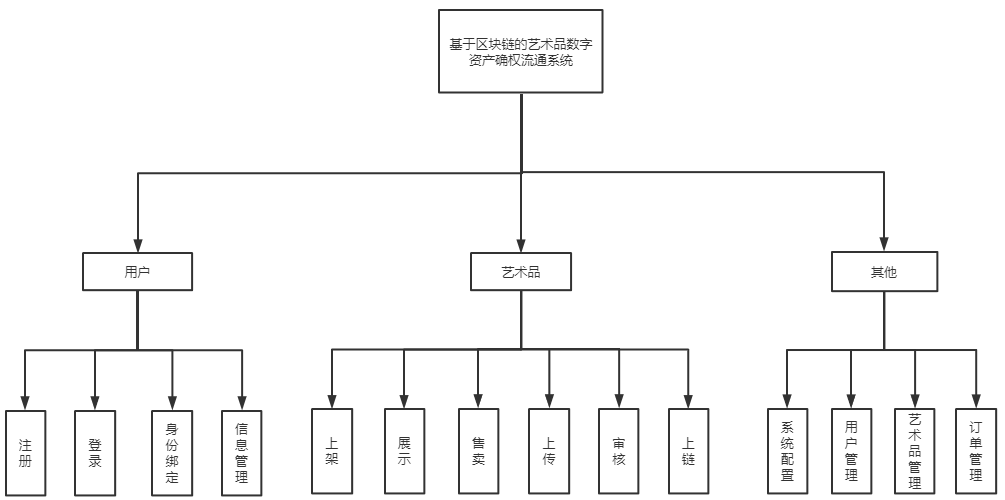


图2-2系统总体功能图

本系统主要功能分为三大类：针对艺术品的操作功能、用户使用网站需要的基础功能，以及其他网站管理功能。

针对艺术品的操作功能有：支持图片、视频、音频及文档等格式的艺术品上传、人工对艺术品进行审核、铸造NFT、NFT上链、上架艺术品、展示艺术品和售卖艺术品。

用户使用网站的基础功能有：注册、登录、将现实身份与区块链账户，网站账户绑定、以及基础信息管理。

其他网站管理功能包括：系统配置、订单管理、用户管理以及艺术品管理。

各模块完成功能如下：

### 2.2.2 web服务器模块

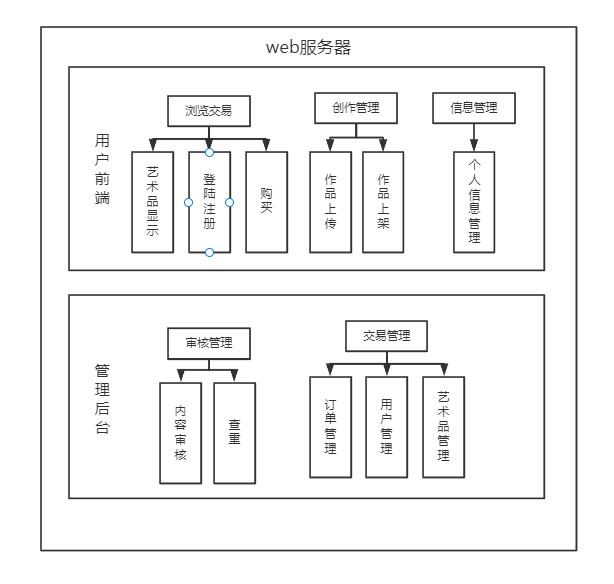


图2-3web服务器模块

* 1. 艺术品显示：采用分页的形式显示商品缩略图。可以按不同的标签显示不同类别的商品。用户点击艺术品后显示详情信息，包含图片、售价、作者、简述，以及该艺术品交易历史等。
  2. 登陆注册：为用户提供登陆注册服务，并将用户填写的个人信息传给数据库。
  3. 个人信息管理：提供用户自主管理个人信息功能。可以修改用户头像、密码，绑定银行卡等，还可以查看历史记录，收藏的艺术品与所有订单信息。
  4. 购买功能：用户在商品详情页点击购买后确认订单信息，然后提交订单，最后支付。待用户完成支付后系统自动调用数据库与区块链模块完成数据更新与信息保存。
  5. 作品上传：用户可将艺术品上传，图片、视频、音频及文档等格式。接收到用户上传的艺术品后，系统为其生成唯一哈希与查重哈希，随后将基本信息存入数据库，待后台审核。
  6. 作品上架：用户可选择将作品上架。接收到用户的上架请求后，系统将改变数据库中艺术品表的状态，使其能在商城显示。
  7. 作品审核：系统为管理员显示所有待审核作品与相关的具有相似内容的艺术品，等待管理员审核。接收到审核操作后，系统调用区块链模块与数据库模块进行后续操作。
  8. 网站管理：网站管理包括订单管理、用户管理和艺术品管理。后台管理员可以查看并管理网站所有用户基本信息、所有艺术品基本信息和所有历史订单信息

### 2.2.3数据库模块

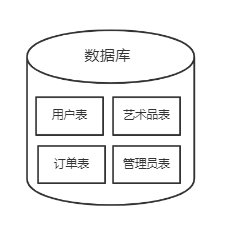


图2-4数据库模块

数据库模块主要完成网站所有数据存储功能。维护的表有：存储所有用户信息的用户表；存储所有艺术品信息的艺术品表；存储所有订单信息的订单表；存储所有管理员信息的管理员表。

### 2.2.4区块链模块

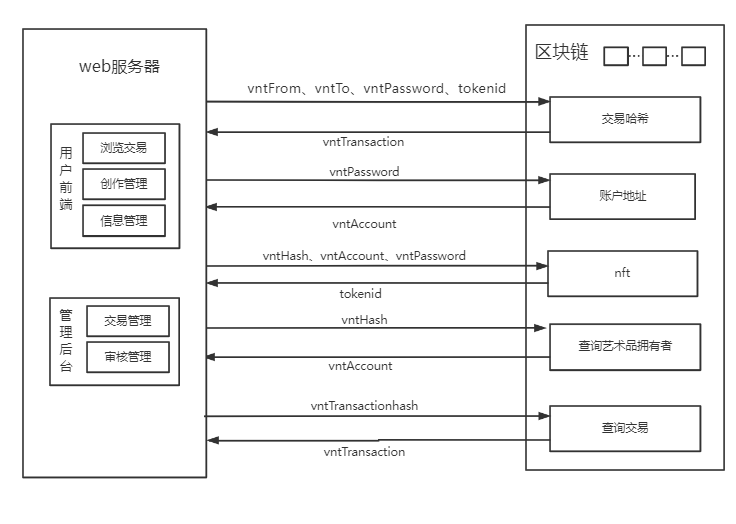


图2-5区块链模块

区块链模块主要功能分为：

1. 账户地址模块：当有新用户注册时，账户地址模块收到web服务器传来的参数，即用户密码，随后在区块链上为该用户注册一个区块链账户，并将区块链账户地址返回到web服务器
2. 交易哈希模块：当用户发起一笔交易时，交易哈希模块收到web服务器传来的卖方、买方的信息以及艺术品信息作为参数，随后将该订单信息打包上链，向web服务器返回交易哈希。
3. 上链模块：当艺术品审核通过后，web服务器将该艺术品的AID和作者在区块链上的账户地址以及账户密码一起传给区块链，区块链调用上链模块为改艺术品上链，并返回该艺术品的NFT。
4. 查询交易模块：用户可以选择根据交易哈希查询每一次交易记录。当web服务器发出查询请求，传入需要查询的交易哈希后，查询交易模块就会返回交易对象。
5. 查询艺术品拥有者：艺术品的历史拥有者都会在区块链上永久保留，用户可以查询某件艺术品的当前拥有者。当web服务器发出查询请求，传入需要查询的艺术品AID后，查询交易模块就会返回艺术品拥有者的当前区块链账户。

## 2.3系统流程设计

### 2.3.1用户信息管理流程

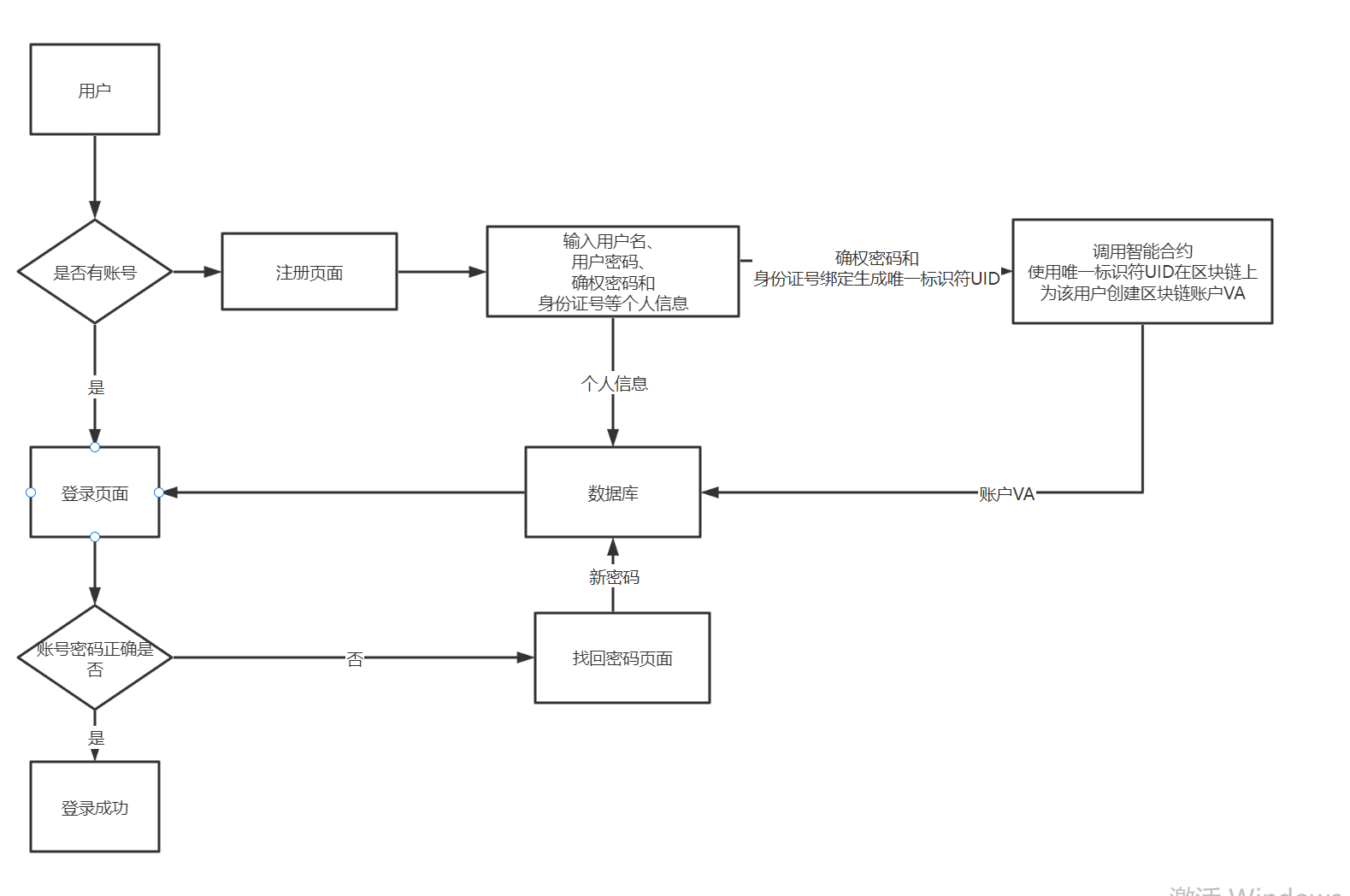


图 2-6用户信息管理流程图

（1）用户进入界面后，若没有账号，进入注册页面注册；若已有账号，则进入登陆页面或选择找回密码。

（2）进入注册页面，①用户输入用户名、用户密码、确权密码和身份证号等个人信息。②系统将用户输入的确权密码和身份证号绑定生成用户的唯一标识符UID（User ID），并调用智能合约使用唯一标识符UID在区块链上为该用户创建区块链账户VA(Vnt Account), 通过UID实现用户和VA的绑定，并将该账户返回到网站中。③网站将用户除确权密码外的个人信息和区块链账户VA一起存入数据库中。④注册成功，进入登录界面。

（3）进入登录页面，用户输入用户名和用户密码，若验证通过，则进入网站首页若验证失败，则退回到登录页面。

（4）进入找回密码页，通过绑定的邮箱验证后，修改得到新的用户密码，再由系统存入数据库中，返回登录页面。

### 2.3.2艺术品上传流程

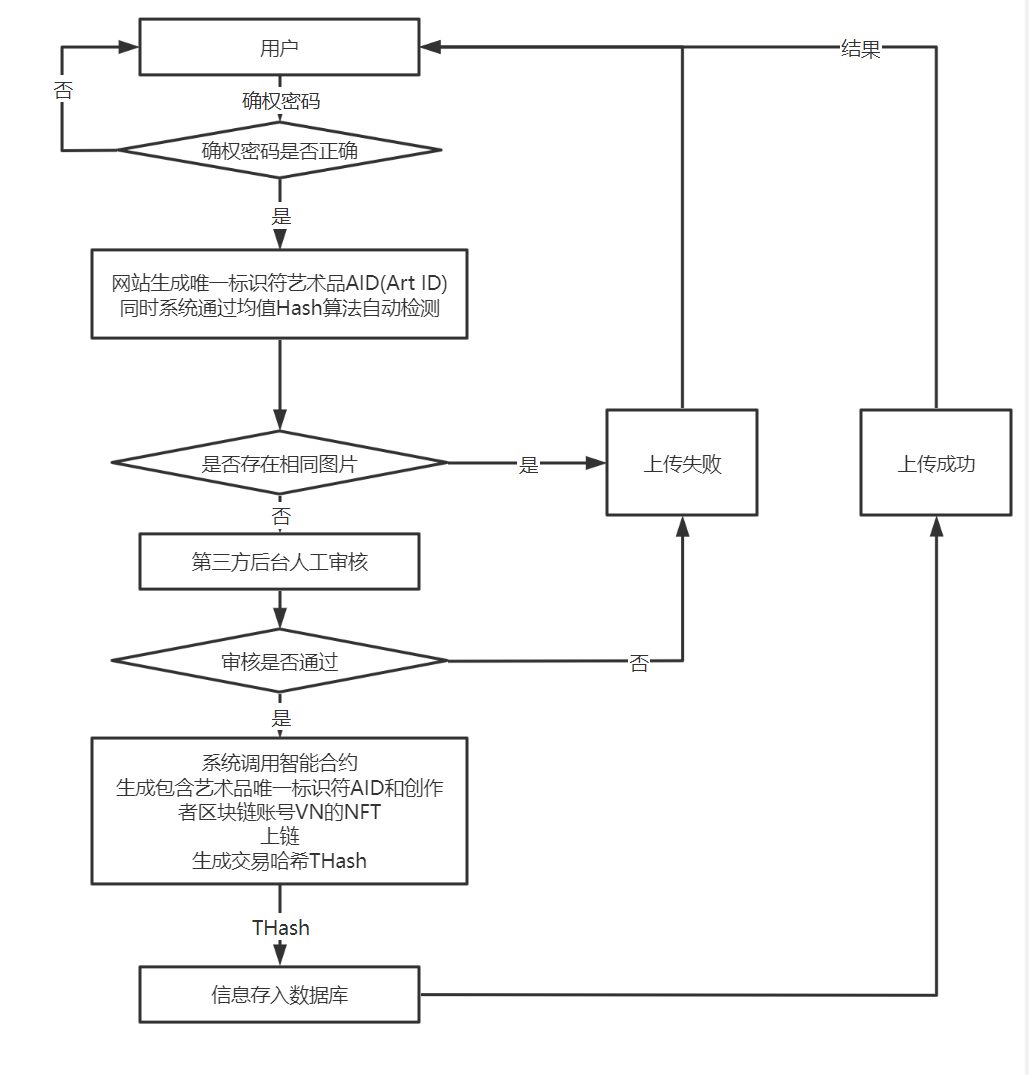


图 2-7 艺术品上传流程图

（1）创作者在输入艺术品信息后，输入确权密码开始上传艺术品。

（2）网站为艺术品生成唯一标识符AID(Art ID)，同时通过均值hash算法对艺术品的内容进行查重。

（3）如果存在完全相同的艺术品，网站通知创作者上传失败；不存在则交给第三方由后台管理人员。对相似度较高的艺术品，将相似的艺术品一起交由第三方进行二次查重。

（4）第三方审核检测艺术品内容是否违规，同时对相似的艺术品进行审核。审核结束后将结果返回给网站。

（5）若审核结果未通过，通知创作者上传失败；若审核通过，网站调用智能合约通过用户输入的确权密码在该用户的区块链账号VN下，生成包含艺术品唯一标识符AID和创作者区块链账号VN的NFT，并上链，同时将生成的交易哈希THash(Transaction Hash)返回到网站。网站将艺术品的信息和THash一起存储到数据库中。

（6）网站通知创作者上传成功。

### 2.3.3艺术品上架流程

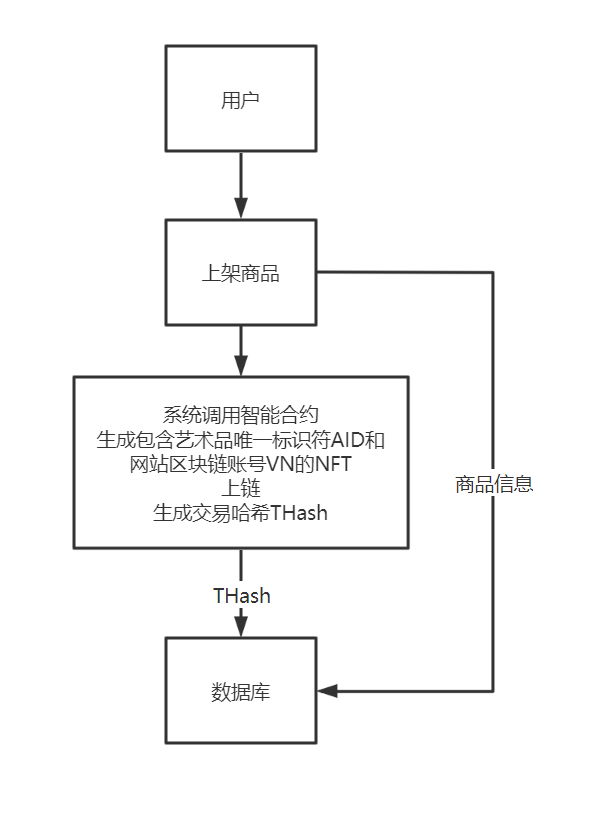


图 2-8艺术品上架流程图

（1）用户选择上架商品

（2）网站调用智能合约生成包含艺术品唯一标识符AID和网站区块链账号VN的NFT，并上链，同时将生成的交易哈希THash(Transaction Hash)返回到网站。

（3）网站将得到的THash存储到数据库中，同时更新数据库中艺术品的信息。

（4）网站通知用户上架成功。

### 2.3.4艺术品购买流程

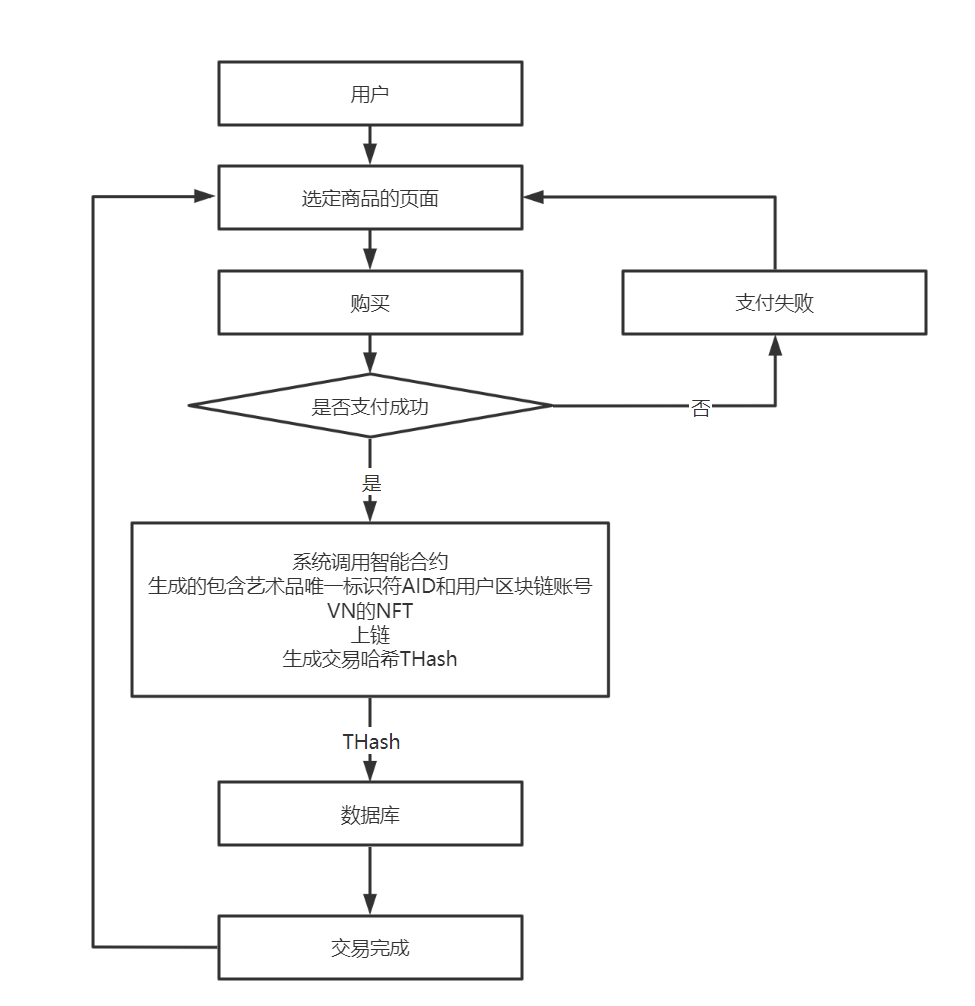


图 2-9艺术品购买流程

（1）用户选定商品后进行支付。

（2）支付失败，则返回购买界面；支付成功，网站调用智能合约生成包含艺术品唯一标识符AID和用户区块链账号VN的NFT，并上链，同时将生成的交易哈希THash(Transaction Hash)返回到网站。

（3）网站将得到的THash存储到数据库中，同时更新数据库中艺术品的信息。

（4）网站通知用户购买成功。

## 2.4 数据库设计

### 2.4.1 功能需求

能够进行数据库的数据定义、数据操纵、数据控制等处理功能。具体功能包括：对于所有艺术品信息、用户信息和订单信息的添加、插入、删除、更新、查询，对网站信息的更新与查询，对管理员信息查询的功能

### 2.4.2 安全性与完整性需求

作为数字资产确权系统中所有信息的保存系统，应做好数据库的安全性与完整性设计，需要防止非授权用户对数据库的恶意存取和破坏、数据库中重要或敏感的数据被泄露等问题。具体要求包含：系统根据管理员标识鉴定管理员身份，合法管理员才准许进入数据库系统进行操作；数据库管理系统进行存取控制，只允许管理员执行合法操作；重要数据以密码形式存储到数据库中。

### 2.4.3 概念结构设计

本系统一共有4个实体，包括：用户、管理员、艺术品、订单。根据需求分析得到它们的关系如下：

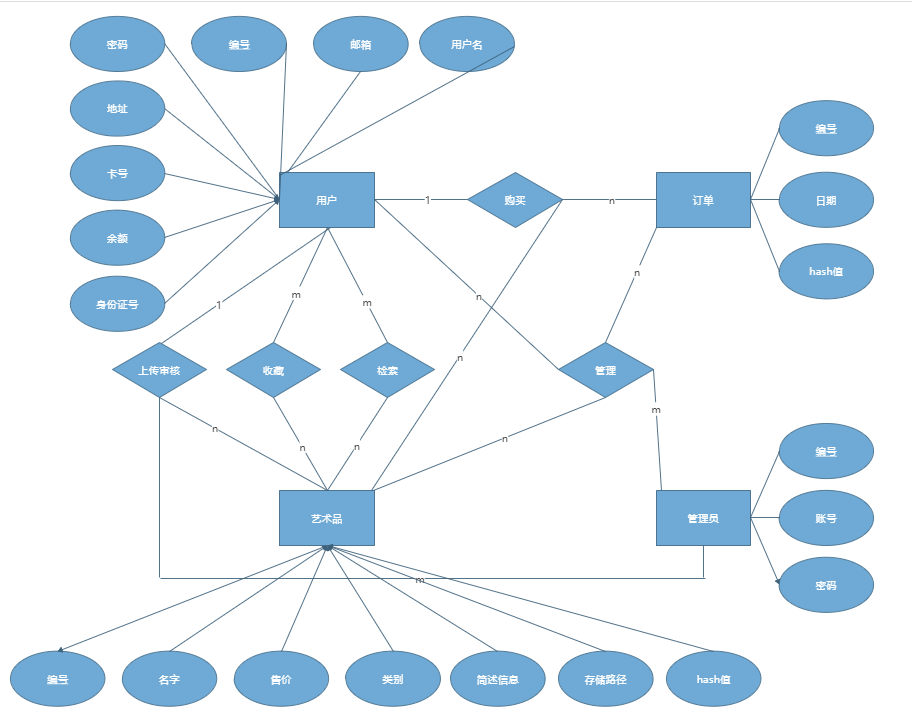


图 2-10 ER图

用户可以浏览、检索、收藏艺术品，为多对多的关系；可以上传艺术品和购买艺术品，且为一对多的关系。管理员可以管理商品、订单、用户，是一对多的关系；管理员还可以审核艺术品，是一对多的关系。

### 2.4.4 逻辑结构设计

本系统的数据库共包括4张表，分别为用户表User\_table，艺术品表Nft\_table，订单表Order\_table，管理者表Admin\_table。各个表设计如下：

#### 2.4.4.1用户表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段 | 字段名 | 类型 | 宽度 | 说明 |
| User\_id | 用户编号 | Int | 10 | 主键 |
| User\_name | 用户名称 | Varchar | 20 | 用户的名称 |
| User\_card | 用户银行卡 | Int | 19 | 用户绑定的银行卡号 |
| User\_pict | 用户头像存储路径 | Varchar | 128 | 用户头像的存储路径 |
| User\_money | 用户余额 | Float | 10 | 用户钱包的余额 |
| User\_password | 用户密码 | Varchar | 20 | 密文存储 |
| User\_email | 用户邮箱 | Varchar | 20 | 用户的邮箱 |
| User\_idertity | 用户身份证号 | char | 18 | 用户的身份证号 |
| User\_addr | 用户账户地址 | char | 64 | 区块链返回的账户地址 |

用户表使用场景如下：

1. 用户登录。后端程序调用用户名与用户密码进行比较，比较通过后登录成功。
2. 用户注册。后端程序为新用户生成一个元组存入用户表。
3. 用户个人信息管理。用户更改信息，后端程序更改相应元组中的属性。
4. 用户交易。用户使用网站钱包交易，当用户充值或者购买、售卖艺术品后，用户表属性钱包中的数额相应改变。
5. 后台管理。管理员管理用户时，系统会调用用户表在后台显示。

#### 2.4.4.2艺术品表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段 | 字段名 | 类型 | 宽度 | 说明 |
| Nft\_id | 艺术品编号 | Int | 10 | 主键 |
| Nft\_hash | 艺术品哈希值 | varchar | 20 | 唯一标识符 |
| Nft\_name | 艺术品名称 | Varchar | 20 | 艺术品的名称 |
| Nft\_descri | 艺术品描述 | Varchar | 255 | 艺术品的描述 |
| Nft\_price | 价格 | float | 10 | 艺术品的价格 |
| Nft\_writer\_id | 作者ID | Int | 10 | 艺术品的创作者 |
| Nft\_owner\_id | 当前拥有者 | Int | 10 | 艺术品当前的拥有者 |
| Nft\_check | 艺术品审核状态 | Int | 1 | 艺术品的审核状态 |
| Nft\_sta | 艺术品上下架状态 | Int | 1 | 艺术品的上下架状态 |
| Nft\_loc | 艺术品存储路径 | Varchar | 128 | 艺术品的存储路径 |
| Nft\_class | 艺术品类型 | Int | 1 | 艺术品的类型 |
| Nft\_fingerprint | 艺术品指纹 | Varchar | 280 | 用于查重的AIDP |

艺术品表使用场景如下：

1. 用户浏览。当用户进入商城后，系统会调用艺术品表以显示艺术品。
2. 用户搜索。当用户输入关键字进行搜索时，系统会检索艺术品表中名称和类别属性，按相关性高低在前端显示。
3. 用户交易。用户成功购买艺术品后，该艺术品的当前拥有者属性改变。
4. 用户上传。当一件新艺术品上传时，艺术品基础信息写入表中，并且系统检索现有艺术品的AID与AIDP，并与新艺术品的AID和AIDP进行比对。若存在相同的AID，则删除该艺术品的元组；若不存在系统将所有AIDP相近的艺术品与新艺术品一起交由后台审核。
5. 艺术品上链。艺术品上链后将艺术品哈希值存入表中。
6. 后台审核。后台审核时，系统会调用所有未审核的艺术品在后台显示。审核后，该艺术品的审核状态会相应改变。
7. 用户上架。用户选择上架后艺术品上架属性值改变，属性值表示为“已上架”的艺术品才会在商城展示。
8. 后台管理。管理员管理艺术品时，系统会调用艺术品表在后台显示。

#### 2.4.4.3订单表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段 | 字段名 | 类型 | 宽度 | 说明 |
| Order\_id | 订单编号 | Int | 10 | 主键 |
| Order\_hash | 订单哈希 | Varchar | 128 | 区块链返回的交易哈希 |
| Order\_nft\_id | 购买艺术品 | Int | 10 | 购买的艺术品的编号 |
| Order\_sell\_id | 卖方 | Varchar | 10 | 卖方编号 |
| Order\_buy\_id | 买方 | Varchar | 10 | 买方编号 |
| Order\_date | 购买日期 | Date |  | 购买的日期 |
| Order\_price | 购买价格 | Float | 10 | 交易完成的价格 |
| Order\_sta | 订单状态 | Int | 1 | 上链状态 |

订单表应用场景如下：

1. 用户交易。当用户交易完成后，系统会生成新的订单信息存入表中。
2. 用户查询。用户查询订单时，系统会检索订单表中相应的数据显示。
3. 订单上链。订单上链后将交易哈希存入表中。
4. 后台管理。管理员管理订单时，系统会调用订单表在后台显示。

#### 2.4.4.4管理员表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段 | 字段名 | 类型 | 宽度 | 说明 |
| Admin\_id | 管理员编号 | Int | 10 | 主键 |
| Admin\_account | 管理员账户 | Varchar | 20 | 管理员登录用的账号 |
| Admin\_password | 管理员密码 | Varchar | 20 | 密文存储 |

管理员表即当管理员登录时，后端程序调用管理员账户与密码进行比较，比较通过后登录成功。

### 2.4.5数据库实现系统功能说明

#### 2.4.5.1登录、注册

新用户注册填写用户名、密码、邮箱、身份证等个人信息，验证通过后注册成功。所有用户信息以及从系统返回的该用户的区块链账号地址一并存入数据库中的用户表。登陆时用户填写用户名及密码，与用户表中信息核实后登录成功。

#### 2.4.5.2浏览商品

用户进入商城，系统默认调用艺术品表的第一页艺术品在前台显示。随后用户选择页数或者类别，系统调用艺术品表中相应的艺术品进行显示。用户在搜索框搜索关键字，后台在艺术品表中选择艺术品名或类别名相近的进行展示。

#### 2.4.5.3购买

用户点击具体的艺术品完成购买后，系统将购买时间、买方id、卖方id和艺术品id存入订单表，并标注上链状态为未上链。待该订单信息存入区块链后，系统将区块链哈希值存入订单表。

#### 2.4.5.4创作

当创作者上传所创作的艺术品时，首先系统为该艺术品生成唯一标识符和用于查重的哈希值，将所有信息存入艺术品表。然后在艺术品表中检索，标记具有相似哈希值的艺术品。后台审核时将该艺术品和相似艺术品一并显示。审核未通过标记为通过状态，审核通过后则标记为通过状态。

#### 2.4.5.5管理

管理员在后台管理系统中增加、删除、改写、查询以改变数据库中各表状态，实现管理功能。

# 第三章 技术架构

## 3.1基于NFT实现的艺术品数字资产确权机制

### 3.1.1NFT数据结构的实现

针对艺术品传统交易市场确权难的问题，本系统使用NFT技术来解决。在智能合约中，系统定义了若干状态变量来存储NFT。通过使用vntlib库中的mapping数据结构，系统将艺术品唯一标识AID与区块链账号VA以键值对的形式作为智能合约中的状态变量存储到链上中，其中艺术品唯一标志作为KEY，拥有这个艺术品的区块链账号等其余有关这个艺术品的信息作为value。在合约中，通过艺术品唯一标志,系统就可以得到艺术品所有者等其余NFT中的信息，由此实现了NFT具有的不可分割性和唯一性，并将艺术品拥有者和艺术品进行绑定，从而可以确定艺术品的拥有者。

### 3.1.2资产确权的实现原理

在维特链中，状态变量只能通过调用智能合约进行修改，账户调用能够修改状态变量的合约方法会产生一笔交易。这笔交易会被广播至网络中的所有节点，并被矿工节点打包成区块，上传至链上。因此，本系统通过在智能合约中对能够修改NFT的账户进行限制，保证了NFT只能被其拥有者等少部分有权限的账户修改，相比使用传统数据库存储，确保了NFT安全性。最后，NFT是高度透明的，与NFT相关的每笔交易都可以被完全回溯。通过调用智能合约，系统可以通过艺术品AID查询到拥有它的区块链账户，从而实现了艺术品所有者确权的问题。

#### 3.1.2.1NFT铸币

在合约中NFT的铸币是通过upload方法实现的。方法的主要内容分为两步：第一，对NFT进行查重，当发现艺术品的AID与当前所有的NFT的AID相同时，说明艺术品被重复上传，程序会对这种情况进行报错，这保证了NFT的唯一性和每个NFT拥有者的唯一性。第二，NFT的铸造，当发现艺术品未被上传过，合约在存储NFT的mapping状态变量中追加一个键值对，将艺术品AID作为键值对的key，将方法的调用者作为value，并对其余相关结构进行修改，实现NFT的铸造。该方法在作品没有被重复铸币的情况下可以被任何区块链账户进行调用。

#### 3.1.2.2 NFT的转让

在合约中，NFT仅被允许由两类账户修改，分别为NFT所有者账户和被NFT所有者授予转让权的账户。NFT所有者可以通过transfer方法实现NFT的转让，transfer方法的函数声明如下

|  |
| --- |
| MUTABLE void transfer(address to,//交易中的买方，即转让目标  uint256 tokenId)//被转让的艺术品AID |

该函数限制了能够调用的账户必须是被转让的NFT的所有者，方法在实现NFT的修改之前会先确认被交易的NFT已存在，之后调用vntlib库中的GetSender()获取函数调用者，并通过调用合约中的ownerOf方法查询当前该NFT的拥有者，当两者相同时该方法才会被正常实行。由于在区块链中交易在发起前不会被篡改，因此这种方法可以保障NFT只能由其所有者进行修改，保证了艺术品确权的安全性和正确性。

在合约中，NFT所有者可以调用approve方法将NFT的转让权授予其他账户，此时NFT的所有者没有被改变，但被授权的账户也可以对NFT进行修改，实现NFT的转让。approve方法的声明如下

|  |
| --- |
| void approve(address to,//转让目标账户  uint256 tokenId)//被转让的艺术品AID |

合约中为NFT定义了如下数据结构记录了NFT转让权的所有者：

|  |
| --- |
| KEY mapping(address  , mapping (uint256，address)) allowed; |

## 3.2基于区块链实现的交易安全性机制

为了实现交易的安全性和可追溯性，防止交易被抵赖，系统借助了VNT所提供的区块链技术。由于区块链中的交易必须经过发起账户通过密钥进行签名，确认交易信息无误后才能被发起，交易无法被冒名发起或是被恶意修改。因此区块链中的交易将完全遵循发起人的意志，具有极高的安全性。由于区块链具有不可篡改，透明性等特征，调用智能合约产生修改NFT产生的交易会永久存放在区块链上并能够被任何人通过交易哈希查询。系统可以通过保留交易哈希进行NFT历史所有者的追溯，以此保证交易不可被抵赖和可追溯。

### 3.2.1 共识机制

共识机制是区块链技术的核心，它维系着系统正常运转，共识机制是区块链系统在分布式环境下保持各节点分布式账本统一性、共识性和一致性而建立的协议、算法以及规则的统称。 可以说，有分布式结构存在就需要达成共识，全网节点达成一致、确定记账节点的方式，认定一个记录是否有效，平衡耗费的资源与产出，都是共识机制需要解决的问题。

本系统所使用的维特链采用一种全新的 Vortex 共识算法，称为 Vortex 共识机制，可达到 10000+TPS；并融入了保证金、高安全、终局性、激 励机制等设计。Vortex 具有交易吞吐量高、具备终局性、安全性高、传输效率高、激励机制有效、出块速度块等主要技术特征。

### 3.2.2 智能合约

维特链的智能合约基于 WebAssembly（WASM）语言编写，支持将成熟的高级语言(如 C 语言)开发的智能合约编译成 WASM 格式的二进制代码运行。WASM 语言具有性能高效、存储成本低、多语言支持等优点。

在 WASM 的优势基础之上，VNT Chain 自主研发了 WAVM 虚拟机。WAVM 是一个 Web Assembly 语言的执行机，继承了 WASM 的所有优点，并进一步 在以下四个方面对 WASM 进行了优化：

1) 改造原生 WASM 中多线程、浮点数、异常处理等导致计算非确定性的设计，确保计算的确定性；

2) 增加燃料(Gas)机制，解决了智能合约中的停机问题；

3) 提供沙箱运行环境，实现资源隔离，保障系统的安全性；

4) 实现了链上标准指令集，且易于扩展。

## 3.3基于均值hash算法的版权保护机制

为实现对艺术品的查重，本系统通过对输入的图片首先进行系列处理得出该图片的Hash指纹。通过计算不同图片hash指纹间的海明距离来量化相似度。并设置了查重阈值，当计算的出的最大相似度超过阈值时，系统判定存在相似图片，交由第三方人工审核查重。

### 3.3.1均值Hash介绍

均值Hash特征描述方法利用图像的低频信息,生成一个二值化序列,相对于LBP等特征描述方式,均值Hash带有更加丰富的结构信息。在图像检索中,图像均值Hash因计算量小,速度快,占有举足轻重的地位。算法根据其二值化序列计算图像间的相似度。

系统参考了pHash检索算法的思路。即先将图像映射成较短的编码序列,即哈希指纹,用来表示其内容特征。然后通过计算图片间的哈希指纹的海明距离来判断两张图片间的相似度。从而实现图片间相似度的量化。

### 3.3.2图像匹配算法

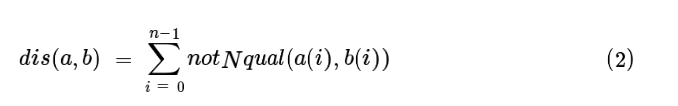
图像是一个定义在二维平面上的信号,它包括低频信号和高频信号。图像信号的幅值对应像素的灰度,因此图像频率则反映了图像的像素灰度在空间中的变化情况。高频信号是信幅值变换强烈的地方,如图像的轮廓(边缘),它描述了图像的细节;低频信号则是对图像亮度的综合度量。

算法定义如下:



其中:PH是感知哈希函数,I是目标图像。感知哈希值有诸多形式,如实数向量和复杂的数据结构等,但通常情况下,感知哈希值是一个二值化序列。

在信息论中,字符串a、b的海明距离定义如下:



它表示两个字符串对应位置的不同字符的个数,哈希指纹可以用字符串表示。相应地,可以用任何两个长度相同的哈希指纹间的距离来度量其相似度。

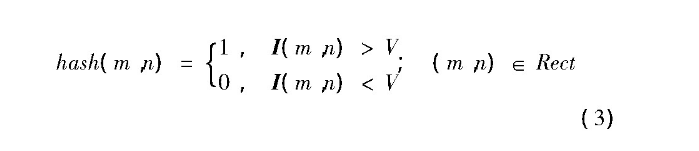
基于以上分析，可以将均值Hash图像匹配算法步骤归纳如下:

(1)图像预处理。确定目标尺寸,过滤高频信息,通常将图像缩小到8×8的尺寸,即保留64个像素。

(2)图像简化。将图像进行灰度变换,同时计算64个像素点的灰度平均值。

(3)灰度二值化。将像素的灰度与平均值进行比较,如灰度大于平均值,则取值为1;反之为0。

(4)计算Hash值。将上述结果拼接在一起就构成一个64位的二值化序列。局部均值Hash与图像的像素点的灰度平均值有关,其特征提取公式如下:



其中:Rect表示目标图像,V表示目标图像像素平均值。

### 3.3.3均值hash实现的版权保护

为实现对艺术品的查重，本系统通过导入BufferedImage包对输入的图片首先进行预处理，在计算完艺术品大小后，对其高频信息进行过滤，压缩处理为8\*8的尺寸。之后对图像进行灰度变换并计算得出平均值。然后根据得出的平均值计算每个像素点的取值，最后通过hash(m,n)函数计算得出该图片的hash指纹。

为了提高查重效率，本系统将艺术品的hash指纹存储在数据库中。当有新的艺术品上传时，本系统会自动根据算法计算其hash指纹，然后与数据库中已有的艺术品的hash指纹进行比较。本系统通过计算不同图片hash指纹间的海明距离来量化相似度，并将阈值设置为0.9。当计算的出的最大相似度超过阈值时，系统判定存在相似图片，交由第三方人工审核。

均值Hash特征描述方法利用图像的低频信息,生成一个二值化序列,带有丰富的结构信息。在图像检索中,具有计算量小,速度快等优点。能有效提高本系统的查重精度和查重效率。同时，为了防止误判，本系统还引入了第三方平台对相似图片进行人工审核。总的来说，基于均值Hash算法，本系统在保证效率和精度的基础上，有效实现了艺术品的产权保护。

## 3.4双库管理

### 3.4.1实现方案

本系统的数据存储采用了区块链和传统数据库相结合的“双库”管理模式。传统数据库中的信息作为区块链中信息的备份与补充，而区块链中的数据作为传统数据库中数据的保证。区块链上存储的信息主要有NFT，交易对象等关键信息。而传统数据库中的信息主要有以下两类：

（1）有关用户、艺术品和交易的详细信息

系统将账户信息，艺术品详细信息，艺术品状态信息，交易详细信息等与系统相关的详细信息存放在数据库中传统的数据库中。为每个系统中每个实体的状态提供详尽的记录，这部分信息不像区块链上的信息一样重要，但提高了整个系统功能的丰富性。

（2）有关确权的关键信息

这部分信息的主要内容为交易哈希等，交易对象的具体内容存放在区块链上。而区块链上查找信息不如传统数据库方便快捷，并且在区块链上存储的交易无法按照一种更为清晰的方式进行组织。因此我们将交易哈希存放在传统数据库中，通过对交易哈希根据用户或NFT等信息进行组织，可以更加清晰和高效地通过维特链提供的API，对交易地详细内容进行查询，实现交易的可追溯性。同时交易对象存放在区块链上，借助区块链的不可篡改的性质实现了交易的不可抵赖。

### 3.4.2主要优势

通过双库管理，我们使得整个系统的功能更加丰富与高效。双库管理的优势如下：

（1）防止存储资源的浪费

在本系统中，艺术品的主要形式有图片、视频和音频。在区块链中，每个全节点都具有链上所有信息的备份。因此将艺术品完整的存放在链上是不现实的，会造成存储资源的大量浪费。本系统通过仅将艺术品的唯一哈希存放在NFT中，实现了NFT与对应艺术品的映射关系，保证了NFT的唯一性，节省了空间资源。

（2）高效性

本系统利用了传统数据库所具有的易于查询的特点。将链上关键信息（如交易哈希）存放在数据库中，使这些用户经常需要获取的信息被有组织的存放。同时这些信息可以作为链上信息的索引，调用区块链的API，我们可以高效的获得其详细地信息，由此保障了系统功能的高效性。

（3）安全性

区块链具有不可篡改，透明性等性质。相比之下，传统数据库容易受到不法分子的攻击，造成关键信息的丢失或被篡改，无法对其中的信息提供安全性的保障。因此我们例如NFT，交易记录等将与确权相关的详细信息存放在区块链中，而传统数据库中相关部分的内容则作为链上内容的备份和补充，通过区块链上的内容，可以验证传统数据库中的内容的安全性。

# 第四章 作品测试与分析

## 4.1 测试环境搭建

### 4.1.1测试设备

作品的硬件环境为：区块链网络部署于阿里云存储服务器，区块链中有四个节点，分别部署于四台虚拟空间服务器中，WEB前端部署于一台电脑。

仿真实验的软件环境为：MySQL为 5.5.62 版本，区块链版本为0.6.4，Ubuntu版本为 16.04，Spring-boot版本为2.6.4，Vue版本为4.5.15，本文所使用的实验数据范围为 1MB–512MB。

### 4.1.2平台配置

根据平台方案设计，需要搭建包含四个节点的本地测试链来测试该平台的详细功能。

首先使用下面命令分别创建四个节点的账户

gvnt account new --datadir nodeX (X=0,1,2,3)

然后生成节点p2p地址。其中地址包含了IP和端口号，我们在启动节点的时候需要指定节点间通信的端口号，节点0到节点4分别分配端口号：12340，12341，12342，12343，并使用如下命令启动节点，获取p2p地址

gvnt --datadir nodeX --port 12340 console (X=0,1,2,3)

将四个节点的账户和p2p地址分别粘贴到dpos.json后，使用下面命令初始化每个节点

gvnt init dpos.json --datadir node0 (X=0,1,2,3)

而后启动bootnode节点，将节点0作为初始见证人节点，则当其他节点与该节点建立连接后，就会和剩余节点建立连接。当每个节点下都会有3个节点，说明测试网络已经搭建起来。

一張含有 文字 的圖片

自動產生的描述

图4-1 测试网络

## 4.2 功能测试

### 4.2.1用户信息管理测试方案

|  |  |
| --- | --- |
| 测试内容 | 用户信息管理 |
| 测试目标 | 首先验证用户注册后，区块链可以生成账户地址，同时数据库可以正确存储信息。然后验证用户可以正常登录到系统之中。 |
| 测试方案 | 注册一个新用户，首先查看区块链生成的账户地址，然后查看数据库中是否正确存储的用户信息。该过程的验证可以对比区块链中的账户地址与数据库中存储的账户地址是否一致，符合则说明数据库成功存储区块链生成的账户地址。最后通过登录，查看登录是否成功即可验证是否注册成功 |

用户注册界面如图4-2，需要填写用户名，身份证号码，用于艺术品上传和上架时的确权密码，用于网站账号绑定的个人邮箱和邮箱验证码，最后是用于网站登录的网站账号密码。输入完毕后，点击注册，可以看到注册成功的提示，并自动跳转到登录页面。



图4-2 注册界面

登录前我们先查看区块链和数据库中的信息，如图4-3所示。可以看到，数据库中的信息，和注册时表单的填写信息一致，并且区块链上的账户地址User\_addr和数据库中也一致，这里区块链上的password是确权密码和用户身份证连接组成的。初步说明了注册功能的可行性。



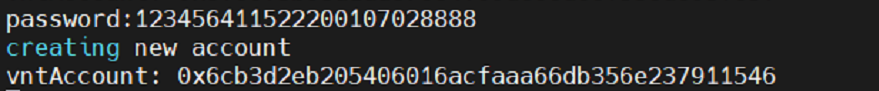


图4-3 数据库和区块链注册信息

登录过程如图4-4所示，首先输入用户名和密码，然后输入验证码，阅读并同意左下角的用户协议。然后点击用户登录按钮。



图4-4 登录界面

可以看到，使用刚注册的账号成功的登录到了网站，如图4-5所示，并来到商城页面。验证了登录功能，同时进一步证明了注册功能的可行性。

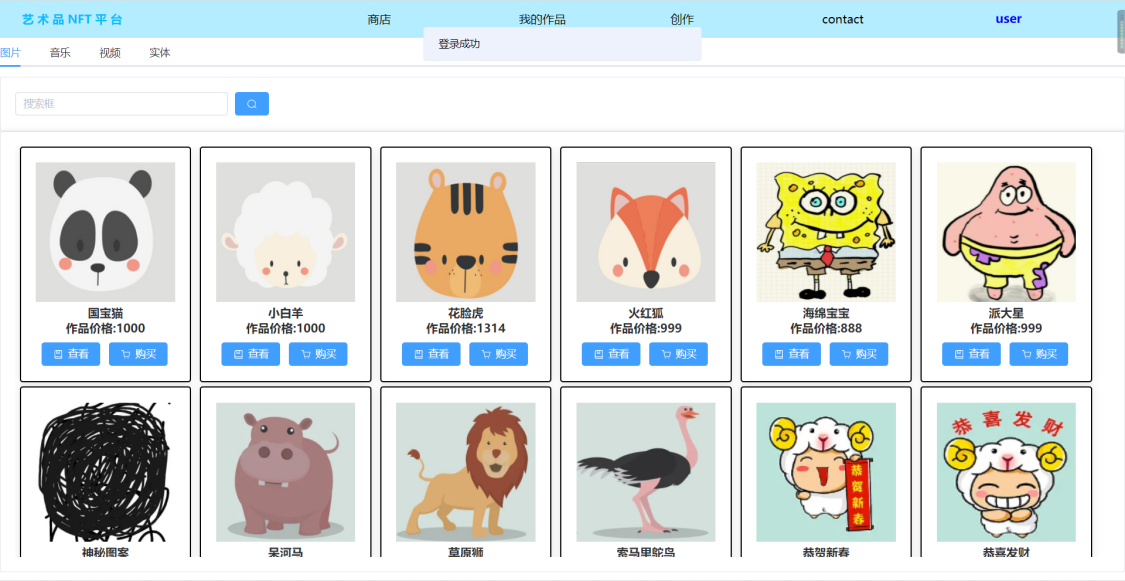


图4-5 登录成功界面

### 4.2.2创作管理测试方案

|  |  |
| --- | --- |
| 测试内容 | 创作管理 |
| 测试目标 | 验证用户能够上传作品。上传作品成功后能够上架其作品，并被其他用户浏览信息。 |
| 测试方案 | 首先，用户在后台上传自己的艺术品。然后可以查看系统自动生成该艺术品的ID，以及系统自动查重结果和第三方审核结果。通过后，可以正确生成THash并存在数据库中。根据该THash查询区块链，可以查到包含艺术品ID和用户ID的NFT。最后，用户上架该艺术品后，其他用户可以在网站浏览该艺术品。 |

首先我们在用户账号user下上传一幅“虎.jpg”的作品，如图4-6和4-7所示，点击创建后，输入确权密码后点击确认。



图4-6 艺术品创作界面

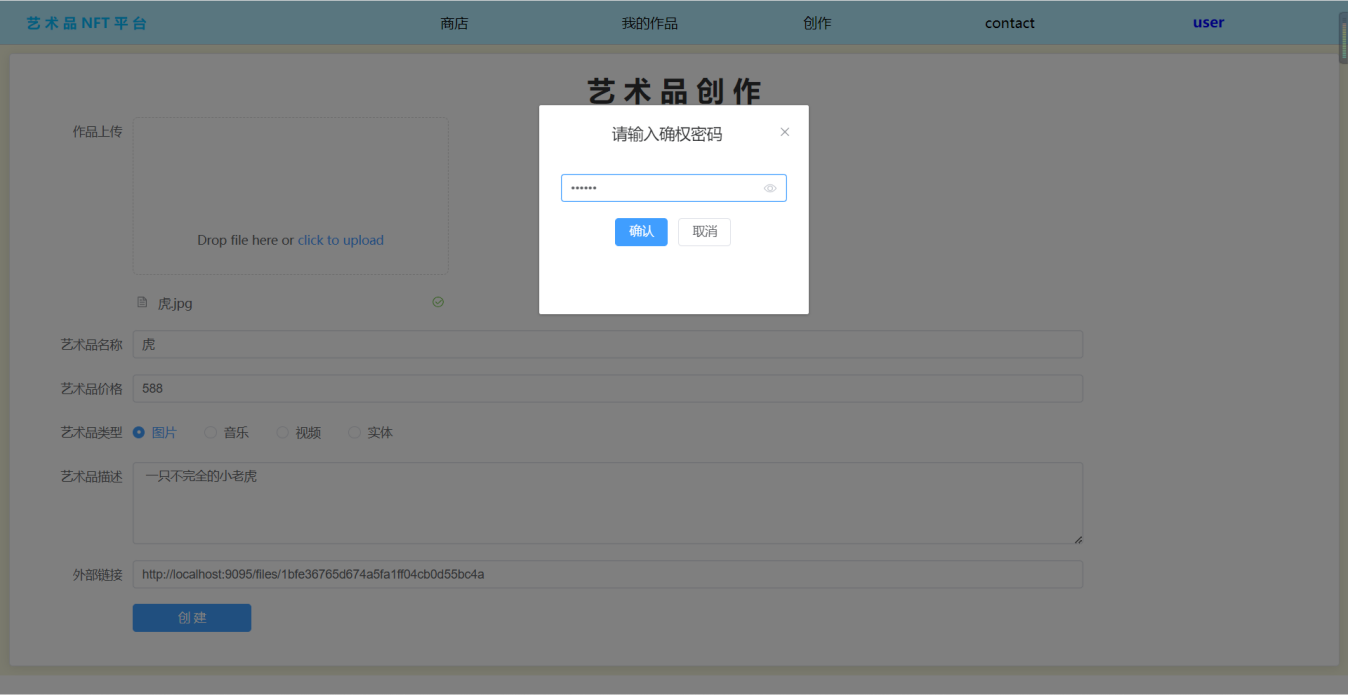


图4-7 确权密码输入界面

可以看到，上传成功，区块链上生成了THash并作为确权凭证，如图4-8所示。用户自己需要保存好该凭证用以证明自己对作品的所有权，如图4-9所示。同时在区块链后端可以查看到NFT信息已经上链，如图4-10。为了验证确权凭证，我们在区块链上通过该确权凭证进行查询，查询结果如图4-11所示，可以看到，根据确权凭证我们可以查到艺术品唯一标识和作者标识以及交易时间。

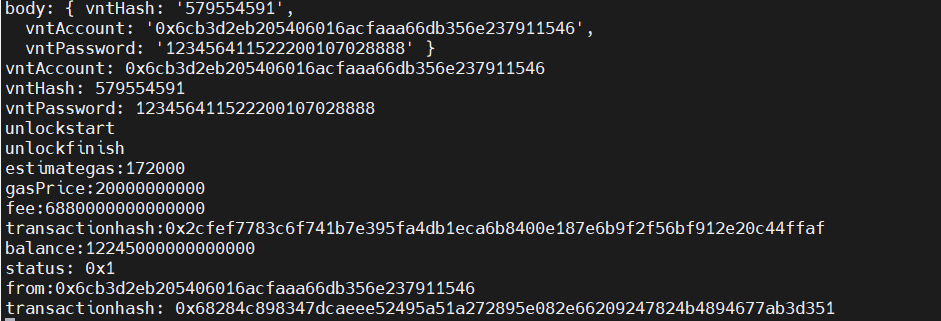


图4-8 上传生成的交易Hash

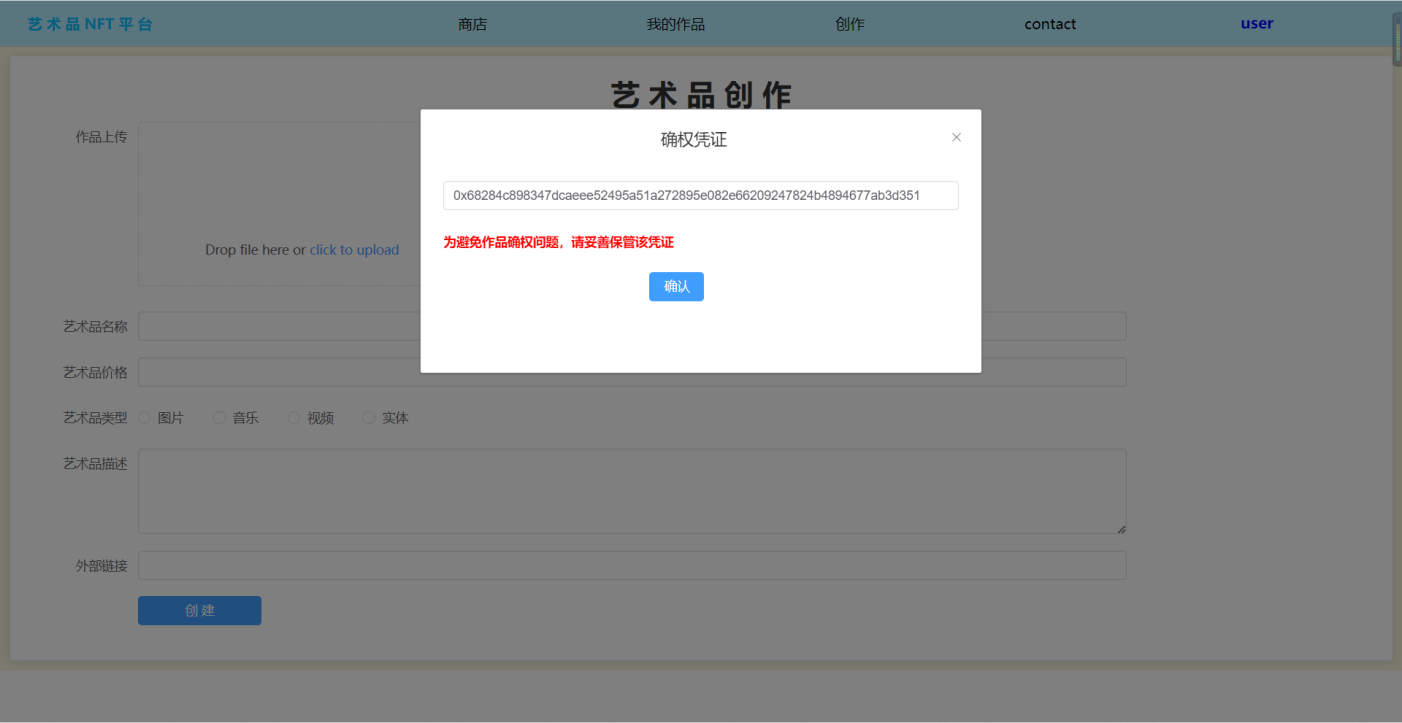


图4-9 获取确权凭证界面

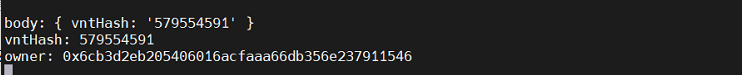


图4-10 NFT信息

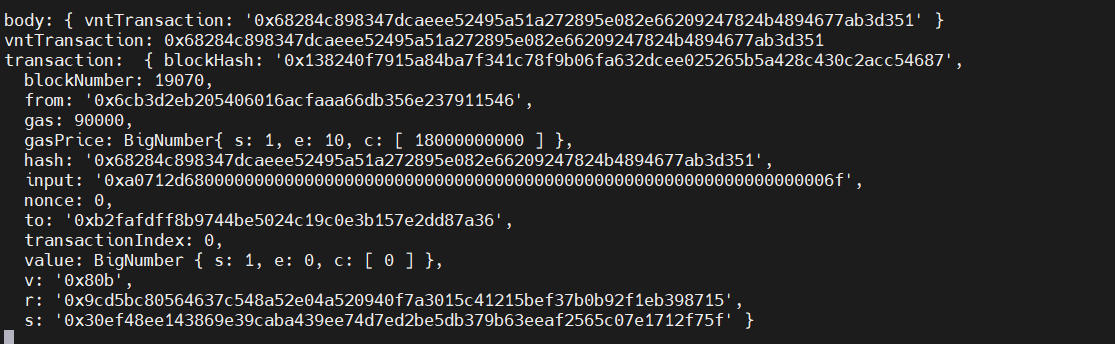


图4-11 确权凭证的查询信息

然后我们可以在“我的作品”里进行查看，如图4-12所示，可以看到作品的详细信息，包括系统为其生成的艺术品唯一标识作品hash。现在是等待审核的状态。



图4-12 我的作品界面

接着，我们在后台对其进行人工审核，如图4-13所示。

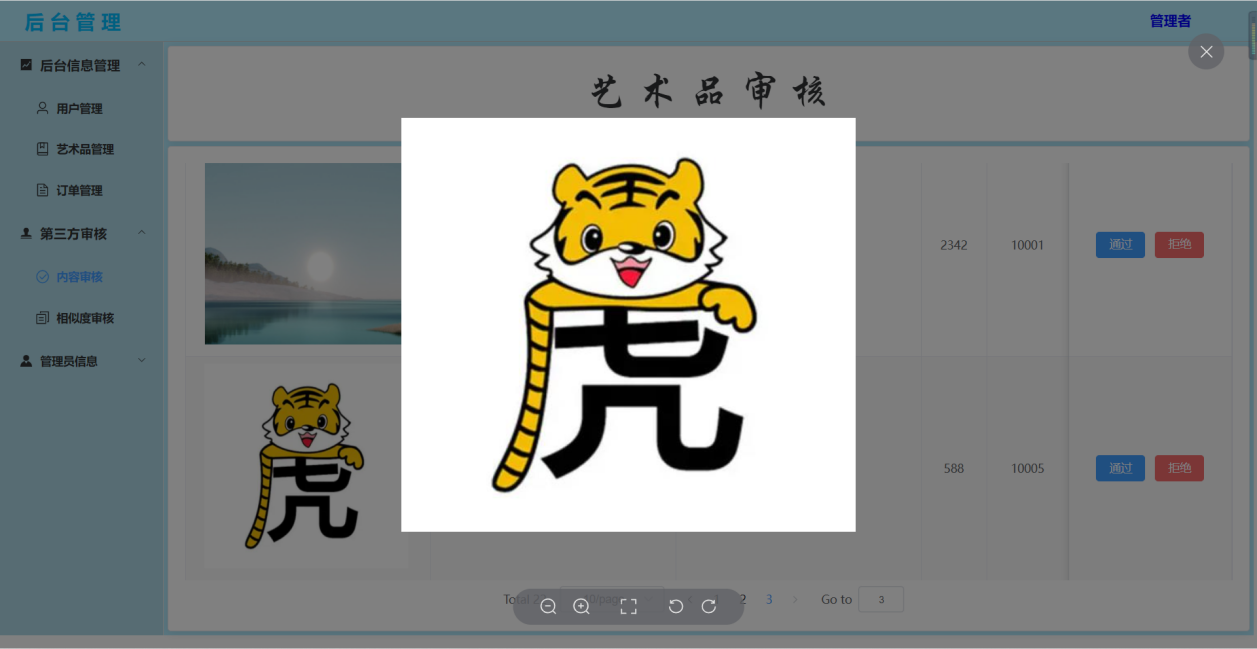


图4-13 艺术品审核界面

审核通过后返回用户“我的作品”界面下进行查看，如图4-14所示。



图4-14 审核通过界面

可以看到，已通过审核，这时我们可以对作品进行上架和修改信息操作（这里不在赘述）。点击上架，输入确权密码后，即可实现上架操作。然后我们可以在商城查看我们的作品。如图4-15所示，，我们再切换为用户user2进行查看，也能看到user上传的作品“虎.jpg”,如图4-16所示，证明可以实现上架。至此创作管理测试成功完成。

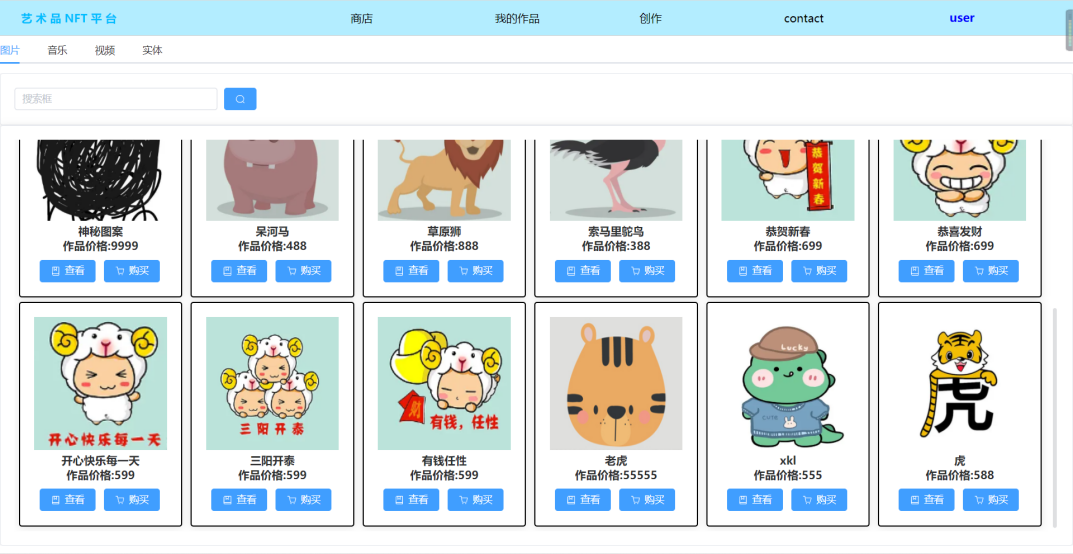


图4-15 作者查看界面

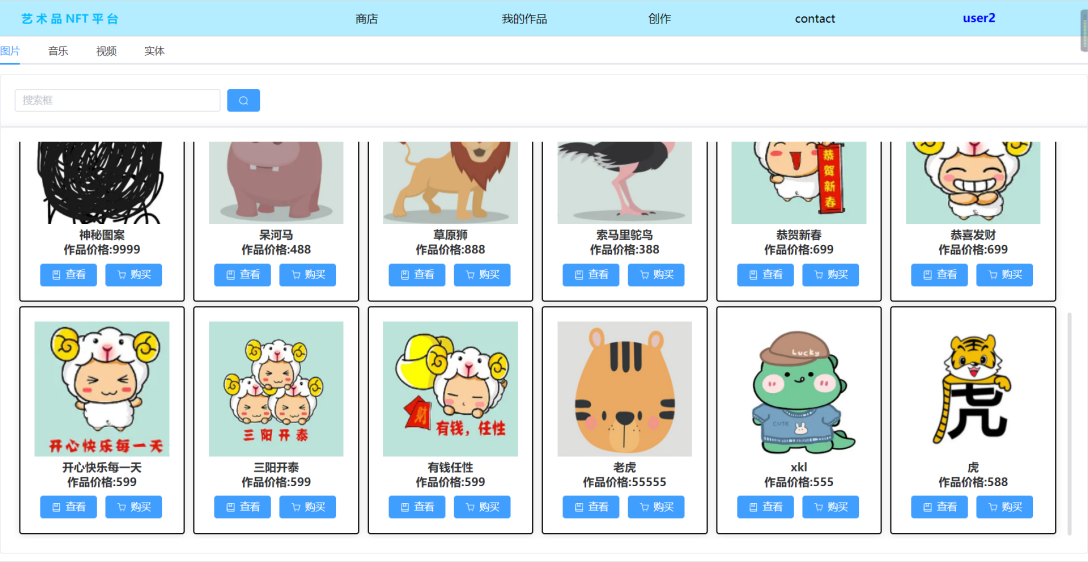


图4-16 其他用户查看界面

### 4.2.3购买流程测试方案

|  |  |
| --- | --- |
| 测试内容 | 购买流程 |
| 测试目标 | 验证买方可以浏览艺术品信息，在付款完成后，数据库中存有该笔交易的信息。通过其中存储的THash值可以在区块链上查询该NFT。 |
| 测试方案 | 首先，买方查看到自己心仪的艺术品，然后完成付款。之后，网站调用智能合约生成该笔交易的NFT上传到区块链中。再将该交易的THash存在数据库中。通过数据库里的信息即可查看该笔NFT，验证该艺术品的拥有者。 |

首先，我们以用户user2作为买方登录，首先user2（买方）购买user（卖方）的作品“虎.jpg”并完成付款，即可成功购买。如图4-所示和图4-所示

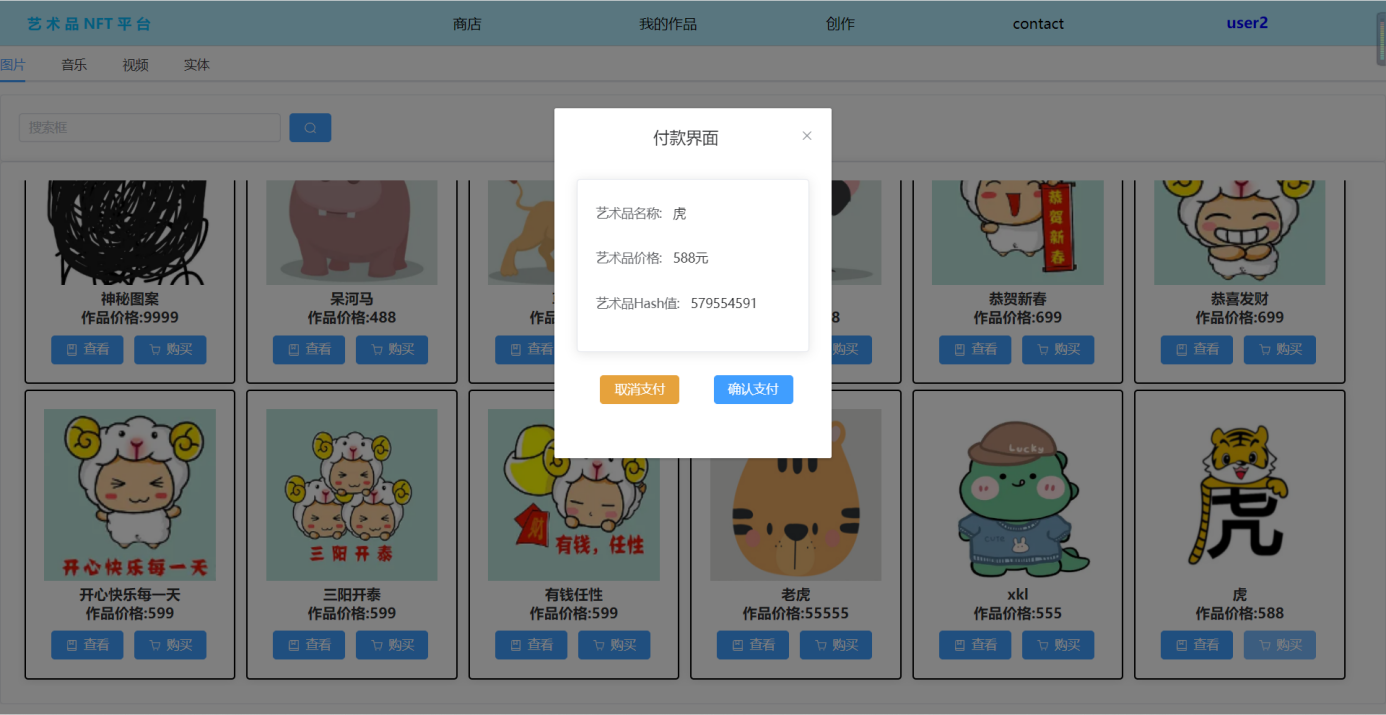


图4-17 付款界面

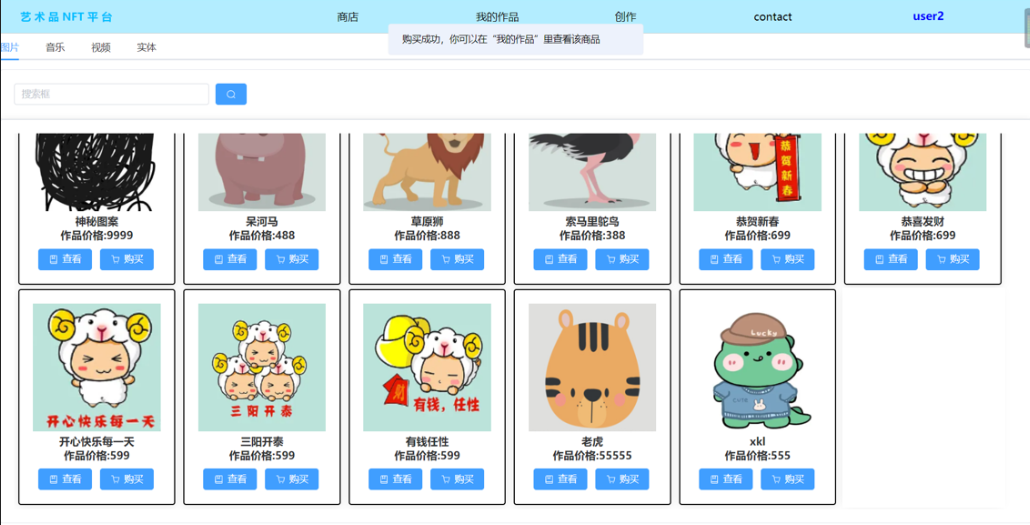


图4-18 购买成功界面

用户user2购买后，区块链上生成的交易哈希Thash和修改后的NFT如图4-19和图4-20所示。

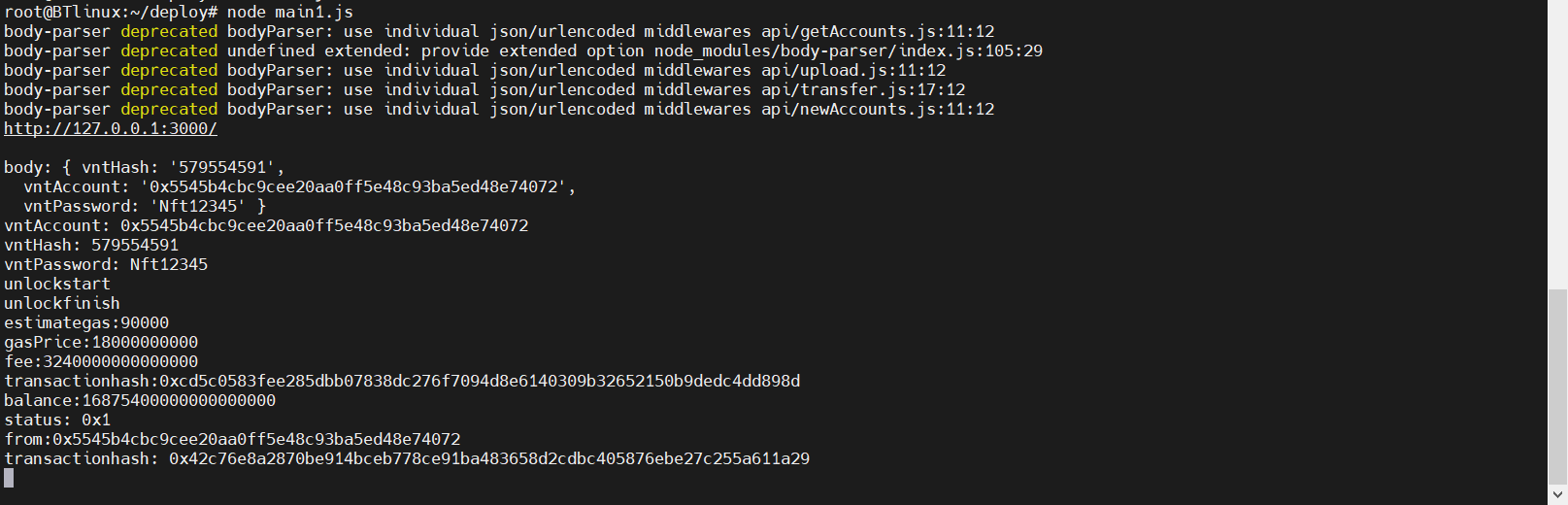


图4-19 购买生成的交易Hash



图4-20 购买完成后NFT信息

同时数据库中的订单也会保存此次交易记录，如图4-21所示。通过该Thash，我们可以查到此次交易的所有信息。

图4-21 订单信息

我们也可以根据Thash在区块链上查到交易信息，如图4-22所示。

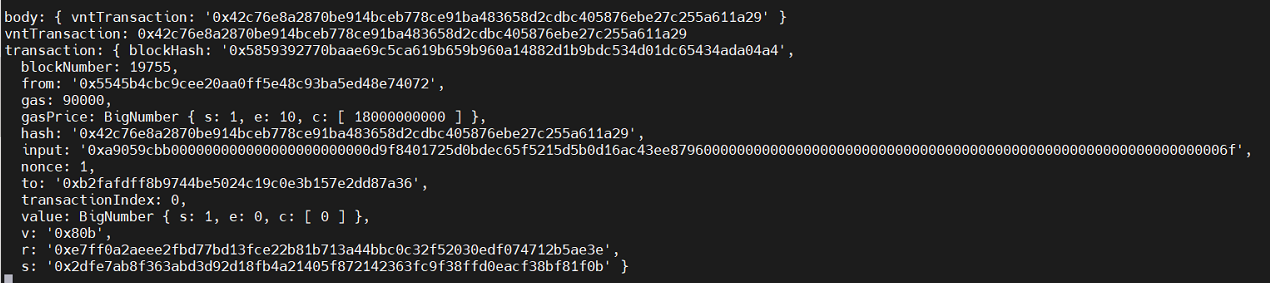


图4-22 交易Hash查询信息

## 4.3结果分析

### 4.3.1可行性分析

功能测试为用户信息管理、创作管理和购买流程三个方面进行了测试，展示了本作品基于区块链的艺术品数字资产确权流通系统的工作正常。在用户信息管理中，用户可以通过在前端网页注册账号，得到能在区块链网络中标识自己唯一身份的区块链账号，实现自己身份与区块链账号的绑定。在创作管理功能模块中，用户可以通过自己的账号，实现交易的上传和上架，在上传后，可以查询到数字艺术品对应的NFT已存在，且属于该用户；同时网站可以对用户作品进行审核，阻止不符合要求的艺术品上架。在购买模块，用户可以通过自己的账号购买已上架的艺术品，在购买后可以查询到链上的NFT已被修改，实现了数字艺术品的转让。由此可见，作品通过基于区块链的NFT技术，可以按照要求实现数字艺术品的上传、流通和确权。

### 4.3.2安全性分析

**交易安全性**

数字艺术品交易的本质是通过在区块链中发起交易，对NFT进行修改来实现的。当艺术品原拥有者将艺术品上架时，会调用智能合约使网站账户获取将NFT转让给买方的权力。当网站节点将NFT修改为买方所有时，会在区块链中产生一笔交易，这笔交易记录将存放在区块链上。根据区块链的不可篡改的性质，这笔交易是不可抵赖的。当这笔交易被打包产生区块后，会将交易哈希返回给网站和用户，网站会将交易哈希值存放在数据库中，而用户也将保存自己的交易哈希。通过交易哈希，任何人都可以查到这笔交易的具体内容，从而实现交易的可追溯性和不可抵赖性。

**确权安全性**

用户通过本作品进行注册时，需要输入自己的身份证号，由此可以将网站账户和现实中人的真实身份建立联系，从而保证账户一定被现实存在的人所有，使得平台所保障的数字艺术品确权是具有真实意义的。当有账户进行非法交易时，可以找到对应的负责人并实现对其责任的追究，从而对数字艺术品的所有权进行保护。保障账户的数字艺术品的所有权是由存储在区块链上的NFT来实现的，NFT必须通过账号发起在链上发起交易，按照智能合约的规定进行修改，而区块链使得NFT具有了不可被非法篡改，不会丢失的特征。任何人都可以通过调用智能合约的方式查询每个NFT的当前所有者。用户在向网站注册时创建了自己的区块链账户，使得用户可以在区块链上发起交易，从而能够为自己的数字艺术品铸造NFT。用户在区块链上的账号地址也将被用作用户在链上的唯一标识存在NFT中，实现对艺术品所有者身份的确认。用户将自己的艺术品上链和上架时都需要在区块链中发起一笔交易，此时用户需要输入自己的确权密码，系统将用户的确权密码和用户身份证号向结合形成用户的区块链账户密码并解锁用户的区块链账户，账户解锁后才可在区块链在发起交易。由此保证艺术品的上传、流通以及转让权的授予是在用户同意下所发起的，保证了用户的知情权。

# 第五章 实践应用

## 5.1 产业前景

本项目研究成果可以应用于艺术品交易领域，市场容量至少在200亿以上，拥有极为广阔的市场前景。特别是本项目研究的艺术品交易模式、系统与人工共同审核模块、图片唯一标识与查重标识生成算法均可以进行升级或功能扩展，推广应用到更多场景。

## 5.2 可行性分析

### 5.2.1市场可行性

从2021年2月开始， NFT开始爆炸式增长，每周交易量超过200万美元，截至到5月，在不到三个月的时间里，大型 NFT 项目的总市值增长高达2000%。国内的NFT商品交易平台并不多，因此艺术品交易平台有巨大的市场和发展潜力。

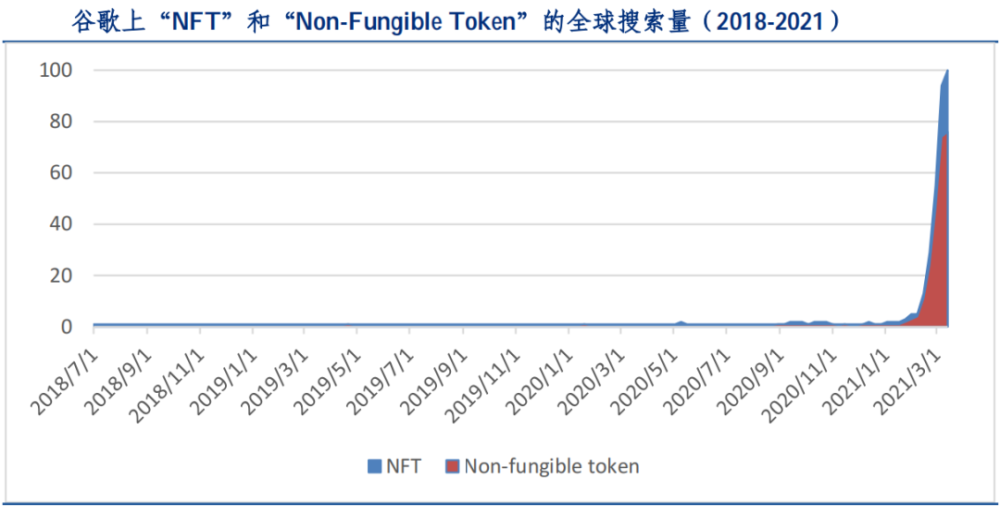


图 5-1 NFT搜索量

### 5.2.2技术可行性

从技术可行性方面，我们系统需要的技术有区块链、Spring Boot、数据库与哈希算法。结合团队成员能力分析，技术层面可以达到要求。

|  |  |  |  |
| --- | --- | --- | --- |
| 关键技术项 | 要求 | 现有水平 | 对照分析 |
| 区块链 | 熟练 | 了解 | 经过指导培训短期内可以达到要求 |
| Spring | 精通 | 熟练 | 可以满足要求 |
| 数据库 | 精通 | 熟练 | 可以满足要求 |
| Hash | 熟悉 | 了解 | 可以满足要求 |

### 5.2.3资源可行性

1. 人力资源

现项目人员构成为五人，共同进行研发，可以完成该项目。

1. 软件资源

服务器系统平台Windows10，区块链依托于云象。

1. 时间资源

目前项目产品开发进度已完成70%，预计剩余项目开发、研究与产品测试所需时间为两个月，时间充裕。

1. 社会可行性
   1. **法**律可行性

该产品没有侵权或者抄袭等违法情况，也没有被申请过专利。

* 1. 政策可行性

无国家政策限制，也无地方政府（或其它机构）的限制。

## 5.3 应用环境与应用对象

本系统应用对象是需要平台进行交易与需要产权保护的艺术家，以及有购买艺术品需求的消费者。

本系统应用环境为兼容ie8及其以上的谷歌浏览器，IE浏览器等双核浏览器。

## 5.4业务模式

系统业务模式采用CToC模式，即个人与个人之间的消费活动。

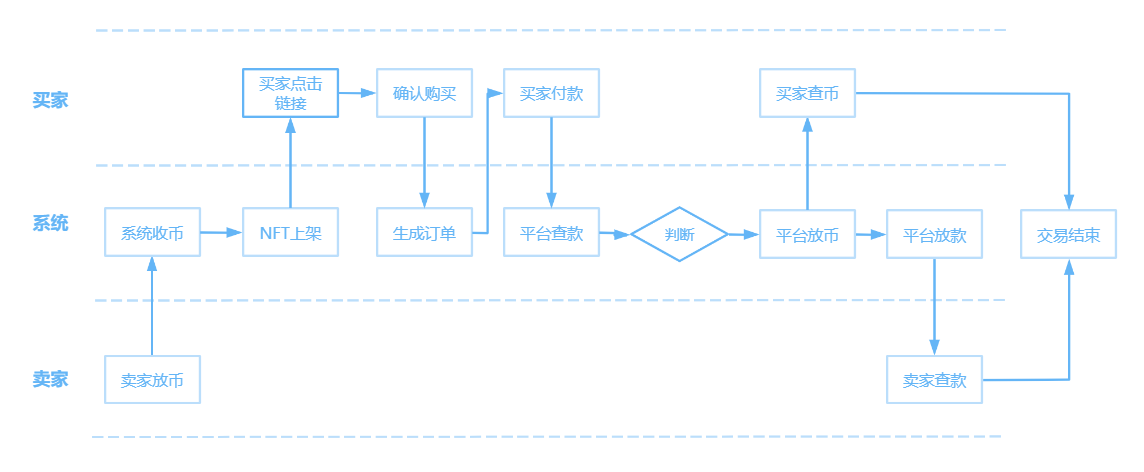


图 5-2 业务模式

买家与卖家通过系统进行交易。首先卖家上传艺术品，待艺术品审核通过成功铸币后，卖家可选择将艺术品上架。上架即将NFT所有权移交给系统。系统在商城展示该艺术品，若有买家选定该艺术品并确认购买，系统将生成订单，买家付款，系统确认收款后，平台将艺术品的所有权转移给买家，并放款给卖家，买家查币且卖家查款，确认无误后交易结束。

本系统的盈利主要通过会员费、交易提成、广告、搜索排名竞价四种方式，此外，也可以用过售卖系统的方式盈利。

网站向所有用户提供会员服务，充值成为会员即可享受升级服务；每完成一笔交易，网站收取艺术品售价的一小部分作为交易提成；第三方可选择向网站投放广告，广告位置可设于横幅、弹窗等位置；创作者可选择向网站支付一部分钱款来提高自己作品的搜索排名。

# 第六章 总结

本系统针对传统交易市场存在的问题提出了一种基于区块链和NFT技术的数字资产确权流通系统。利用基于区块链的NFT技术实现了艺术品的确权流通，并通过区块链存储管理NFT来保证NFT的权威性。同时本项目还通过均值Hash算法实现了艺术品内容级的版权保护，并设置了第三方审核机制来保证艺术品内容的合规性。

系统主要功能可分为两个部分，一是与用户交互的网站功能，网站功能针对不同用户，可再分为两类：针对购买以及创作艺术品的普通用户功能和针对进行艺术审查工作和网站维护管理的管理用户的功能。系统为普通用户提供登录、注册、展示商品、上传、购买商品等的功能；为管理用户提供登录、注册、审查等功能。二是与区块链以及数据库交互的信息存储功能。根据存储信息的性质和位置不同，信息存储也可分为两个部分，将艺术品的NFT以及交易记录等用于认证的信息存放在区块链中，增强权威性。而对艺术品的详细信息和用户信息等数据量较大的普通数据存放在数据库中，利用数据库存储大量数据时便于管理的优势比如数据组织结构化；数据冗余度比较小，易扩充；统一的数据控制等特点，提高平台数据存储以及管理的效率。

通过对系统核心流程中各个功能的测试，展示了本系统提出的基于区块链和NFT技术实现数字资产确权流通的方案各部分工作正常。系统测试包括注册登录，艺术品上传，艺术品上架和艺术品交易四个核心流程，说明了系统确权流通，版权保护和内容合规性保证等功能的可行性，同时通过在区块链上查询NFT和交易Hash等信息进一步验证了系统功能的安全性。测试结果表明基于区块链和NFT技术的数字资产确权流通系统能够实现确权流通，版权保护和内容合规性等功能。

总而言之，根据基于区块链的NFT技术，以及相关的智能合约等技术，本作品设计的实现方案为数字艺术品提供了一种资产确权流通的方案，实现了系统目的。

# 文献引用

[1]刘双舟,郭志伟.论非同质化代币对数字艺术版权管理与保护的影响[J].中国美术,2021,(04):29-32.

[2]曹傧,聂凯君,彭木根,周治中,张磊.无线网络中区块链共识算法的开销分析[J].北京邮电 大学学报,2020,43(06):140-146

[3]唐林川,邓思宇,吴彦学,温柳英.基于pHash分块局部探测的海量图像查重算法[J].计算机应用,2019,39(09):2789-2794.

[4]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(04):481-494.

[5]沈鑫,裴庆祺,刘雪峰.区块链技术综述[J].网络与信息安全学报,2016,2(11):11-20.

[6]何蒲,于戈,张岩峰,鲍玉斌.区块链技术与应用前瞻综述[J].计算机学,2017,44(04):1- 7+15.

[7]曹傧,聂凯君,彭木根,周治中,张磊.无线网络中区块链共识算法的开销分析[J].北京邮电 大学学报,2020,43(06):140-146.

[8]李康,孙毅,张珺,李军,周继华,李忠诚.零知识证明应用到区块链中的技术挑战[J].大数 据,2018,4(01):57-65

[9] LIU Y,ZHANG D,LU G,et al.A survey of content-based image retrieval with high-level semantics [J].Pattern Recognition,2007,40(1):262-282.

[10] AL-MANSOORI S,KUNHU A.Hybrid DWT-DCT-Hash function based digital image watermarking for copyright p and content authentication of DubaiSat-2 images [C]// Proceedings of the High-Performance Computing in Remote V.Bellingham,WA:SPIE,2014,9247:924707

[11] 宁星,蒋年德.基于LBP人脸识别算法的预处理研究[J].电子质量,2012(4):76-77.(NING X,JIANG N D.Pretreatment research for face recognition based on LBP [J].Electronic Quality,2012(4):76-77.)

[12] LIN K,YANG H-F,HSIAO J-H,et al.Deep learning of binary hash codes for fast image retrieval [C]// Proceedings 15 IEEE Conference on Computer Vision and Pattern Recognition Workshops.Piscataway,NJ:IEEE,2015:27-35

[13]（VNT Chain 分布式智能价值网络白皮书 v1.1）