



(12) 发明专利

(10) 授权公告号 CN 110278462 B

(45) 授权公告日 2021.07.09

(21) 申请号 201910534554.2

H04N 21/4627 (2011.01)

(22) 申请日 2019.06.20

H04N 21/63 (2011.01)

(65) 同一申请的已公布的文献号

申请公布号 CN 110278462 A

(56) 对比文件

CN 108683705 A, 2018.10.19

CN 109389500 A, 2019.02.26

(43) 申请公布日 2019.09.24

CN 109493017 A, 2019.03.19

(73) 专利权人 北京工业大学

CN 107563905 A, 2018.01.09

地址 100124 北京市朝阳区平乐园100号

CN 109215751 A, 2019.01.15

(72) 发明人 张延华 陈冰容 杨睿哲 杨硕鹏

CN 109462588 A, 2019.03.12

王倩雯 姚勇锋

US 2017249482 A1, 2017.08.31

KR 101780636 B1, 2017.09.21

(74) 专利代理机构 北京思海天达知识产权代理

US 2018300382 A1, 2018.10.18

有限公司 11203

US 2018005186 A1, 2018.01.04

代理人 刘萍

苏雄业. 基于区块链的大数据共享模型与关键机制研究与实现.《中国优秀硕士学位论文全文数据库(电子期刊)》.2019, (第5期),

(51) Int. Cl.

H04N 21/254 (2011.01)

H04N 21/258 (2011.01)

H04N 21/266 (2011.01)

审查员 张睿君

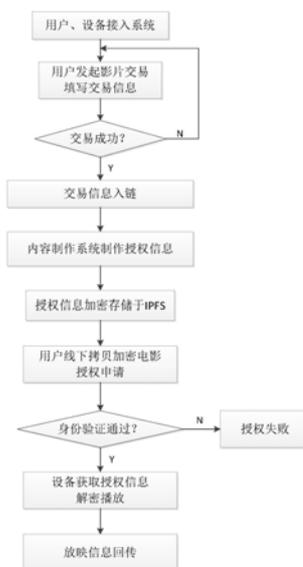
权利要求书1页 说明书3页 附图4页

(54) 发明名称

一种基于区块链的流动放映授权管理方法

(57) 摘要

一种基于区块链的流动放映授权管理方法, 涉及区块链技术领域、数字电影版权保护领域、数据安全领域。通过区块链技术和IPFS技术协同完成授权信息的加密分布式存储以及在节点上的授权处理。具体包括通过获取并上传授权信息, 加密后存储到区块链IPFS存储系统中; 用户设备分别接入区块链网络, 形成用户交互网络和设备轻节点网络。用户节点提出授权申请后, 通过身份认证以及设备认证进行授权信息的授权操作。认证成功后, 设备轻节点可获取授权信息进行相应的解密处理。该方法利用区块链和IPFS的存储模型, 改善区块链的容量存储问题, 提高区块链的可扩展性。



1. 一种基于区块链的流动放映授权管理方法,其特征在于包括以下步骤:

步骤1:打开windows的命令程序,开启以太坊环境;在以太坊区块链上新建账户并解锁,另开一个命令程序,执行truffle.cmd compile对合约进行编译,然后执行truffle.cmd migrate将合约部署在以太坊区块链上;

步骤2:打开另一个windows的命令程序,在Node.js环境下运行授权信息数据获取接口脚本和数据存储查询接口脚本;授权信息数据获取接口将开启监听等待授权信息的上传;

步骤3:通过授权信息获取接口获取授权信息,并将授权信息加密后分布式存于IPFS中;

步骤3.1:用户使用WebApp的方式输入用户ID、密码,并选择用户类型后发起注册请求;WebApp验证提交的信息后根据输入的密码生成用户公钥和私钥以及区块链地址,同时向区块链节点请求调用用户注册合约完成用户注册请求,并广播至各区块链节点,到达并记录后用户注册完成;

步骤3.2:设备生产商使用WebApp登录,填写设备信息进行设备注册,WebApp验证提交的设备信息后根据输入的设备唯一序列号生成设备公钥和私钥以及区块链地址,同时向区块链节点调用设备注册合约完成设备注册请求,并广播至各区块链节点,到达并记录后设备注册完成;

步骤3.3:利用步骤3中获取的授权信息进行影片授权信息的上传;用户使用WebApp上传信息并使用用户的公钥对上传请求进行签名,然后将授权信息用设备公钥进行加密后存入IPFS中并获取IPFS返回的哈希值,同时向区块链节点请求调用数据存储合约,区块链节点接收到请求首先验证用户的签名,通过后执行智能合约,并将哈希值、信息类型进行全网广播,达成共识后将智能合约执行结果写入区块链中,最后提示用户信息上传成功;

步骤4:信息查询:用户发起查询请求进行签名后WebApp提取查询信息类别,然后向区块链节点请求调用数据查询合约输入用户ID和信息类别,区块链节点验证用户的签名后执行数据查询智能合约,然后继续调用查询访问权限合约,区块链节点智能合约根据用户信息及查询信息判断是否具有查询权限,若有权限则相应的区块链放映机轻节点调用区块链查询接口获取查询信息的哈希值,然后根据哈希值获取IPFS节点存储的加密信息;

步骤5:区块链放映机轻节点将会将信息回传作为交易请求调用信息回传智能合约将交易请求发送至区块链服务器;区块链服务器接收并广播交易,在各个区块链节点达成共识后记入区块链账本并向用户返回信息回传结果。

2. 根据权利要求1所述的方法,其特征在于:将区块链IPFS存储模型应用于授权信息的存储以及授权信息的查询获取。

## 一种基于区块链的流动放映授权管理方法

### 技术领域

[0001] 本发明涉及区块链技术领域、数字电影版权保护领域、数据安全领域,特别是用于电影流动放映系统的授权管理方法。

### 背景技术

[0002] 近年来,农村数字电影流动放映成为我国农村一项重大文化扶贫工程。但现有流动放映授权管理基于传统集中式数据库技术,采用中心化管理模式,授权信息通过互联网传输到院线授权接收站。随着互联网的迅猛发展,放映授权管理的效率和安全问题日益突出,存在人为篡改数据、非法授权等问题。因此,建立一个安全可靠的流动放映授权管理平台迫在眉睫。

[0003] 随着比特币的兴起,作为它的底层技术的区块链受到业界专业人士的广泛关注。区块链是一种透明化的不可篡改的分布式加密账本,拥有去中心化、公开透明、不可篡改等特点,智能合约是在去中心化的区块链平台——以太坊上运行的程序,完全按照程序运行,杜绝了了停机、中心化操控、欺诈和第三方干涉的可能性。使用以太坊运行智能合约的主要优点是方便智能合约彼此交互,而且不需要担心整合共识协议等事情,只需编写应用所需逻辑即可。

[0004] 区块链由于其链式特性,随着交易的不断产生,区块不断增多。IPFS(星际文文件系统)是一个对等的分布式文件系统。它提供了一个高吞吐量、按内容寻址的块存储模型,以及与内容相关的超链接。因此,将区块链与IPFS结合可有效解决区块链的容量存储问题。

[0005] 区块链技术以其分布式结构和共识机制为数据存储和授权提供可信性保证。将区块链和IPFS技术运用到授权管理中,可增加授权管理的安全性,提高授权数据信息的可靠性。以太坊智能合约的运用可使身份认证、授权管理智能化,从而很好地提高授权认证效率。

### 发明内容

[0006] 针对上述现有系统采用技术存在的不足,本发明提供一种基于区块链的流动放映授权管理方法,用于解决流动放映中授权信息的安全存储和合法授权分发问题,实现授权请求者的有效身份认证和授权信息的分发。从而确保用户和设备身份的真实性和合法性,防止用户对资源进行非授权访问;保证数字影片的密钥等机密数据不被泄露给非授权实体;防止数据被未经授权的增删、篡改或替代;同时提供用户操作行为的审计记录,以便必要时提供审查和追责,防止操作者事后否认操作行为的发生。

[0007] 针对上述问题,本发明采用以下技术方案:

[0008] 实现方法流程图如图1所示:将流动放映中涉及的各类用户接入到区块链网络作为P2P用户节点,分布式存储的区块链会在每个用户节点产生信息备份,以此形成用户交互的可信任信息网络。设备为放映设备,放映设备内嵌区块链轻量级节点模块,也可以参与到区块链网络中进行信息交互。结合WebApp完成用户和设备的注册,用户完成影片交易后,内

容制作系统制作加密影片并根据相应的信息生成授权信息。授权信息通过基于区块链的IPFS存储模型进行加密分布式存储,用户在获取授权信息时需进行相应的身份认证被证明为授权用户才可获取授权信息。验证通过后,授权信息将会发送到对应区块链放映机轻节点进行授权放映。区块链轻节点放映完成后会自动上传放映信息至区块链系统。

[0009] 本发明采用区块链和IPFS的存储模型,如图2所示。该模型核心是每个矿工检查接收到的事务,将有效事务放入交易池中,并存储在IPFS中,同时返回事务的IPFS哈希值。当计算下一个区块时,每个矿工将验证过的IPFS哈希打包到新的区块中并计算merkle根和区块哈希。区块链和IPFS结合的存储系统用于存储授权信息,该系统核心是以太坊作为区块链平台,IPFS用于分布式存储加密授权信息。

[0010] 本发明为用户和设备提供了身份认证、为影片提供了授权保护。本发明将以太坊作为区块链平台,应用智能合约,以truffle作为开发框架搭建用于授权认证的区块链。通过授权信息数据接口获取授权信息,通过智能合约输入参数编码将获得的相应影片授权信息写入区块链交易,分布式存储于IPFS中。最后在用户节点通过身份验证查询获取授权信息,实现影片的授权认证。

[0011] 有益效果

[0012] 本方法可行性高,可靠性强,解决了传统授权管理方法依赖于中心化数据库的安全信任问题,提高了授权管理的安全性。运用基于区块链的IPFS存储模型解决了传统区块链的存储容量问题,提高了区块链的可扩展性。

## 附图说明

[0013] 图1是基于区块链的流动放映授权管理系统流程图

[0014] 图2是基于区块链和IPFS的存储模型

[0015] 图3是授权信息上传流程图

[0016] 图4是授权信息查询流程图

## 具体实施方式

[0017] 本发明提供一种基于区块链和IPFS的授权信息管理方法,系统流程图如图3所示。具体包括以下步骤:

[0018] 步骤1:打开windows的命令程序,开启以太坊环境。在以太坊区块链上新建账户并解锁,另开一个命令程序,执行truffle.cmd compile对合约进行编译,然后执行truffle.cmd migrate将合约部署在以太坊区块链上。

[0019] 步骤2:打开另一个windows的命令程序,在Node.js环境下运行授权信息数据获取接口脚本和数据存储查询接口脚本。授权信息数据获取接口将开启监听等待授权信息的上传。

[0020] 步骤3:通过授权信息获取接口获取授权信息,并将授权信息加密后分布式存于IPFS中。

[0021] 步骤3.1:用户使用WebApp等方式输入用户ID、密码,并选择用户类型后发起注册请求。WebApp验证提交的信息后根据输入的密码生成用户公钥和私钥以及区块链地址,同时向区块链节点请求调用用户注册合约完成用户注册请求,并广播至各块链节点,达成共

并记帐后用户注册完成。

[0022] 步骤3.2:设备生产商使用WebApp登录,填写设备信息进行设备注册,WebApp验证提交的设备信息后根据输入的设备唯一序列号生成设备公钥和私钥以及区块链地址,同时向区块链节点调用设备注册合约完成设备注册请求,并广播至各区块链节点,达成共并记帐后设备注册完成。

[0023] 步骤3.3:利用步骤3中获取的授权信息进行影片授权信息的上传,流程如图3所示。用户使用WebApp上传信息并使用用户的公钥对上传请求进行签名,然后将授权信息用设备公钥进行加密后存入IPFS中并获取IPFS返回的哈希值,同时向区块链节点请求调用数据存储合约,区块链节点接收到请求首先验证用户的签名,通过后执行智能合约,并将哈希值、信息类型进行全网广播,达成共识后将智能合约执行结果写入区块链中,最后提示用户信息上传成功。

[0024] 步骤4:信息查询流程如图4所示。用户可根据需要进行查询操作,用户发起查询请求进行签名后WebApp提取查询信息类别,然后可向区块链节点请求调用数据查询合约输入用户ID和信息类别,区块链节点验证用户的签名后执行数据查询智能合约,然后继续调用查询访问权限合约,区块链节点智能合约根据用户信息及查询信息判断是否具有查询权限,若有权限则相应的区块链放映机轻节点调用区块链查询接口获取查询信息的哈希值,然后根据哈希值获取IPFS节点存储的加密信息。

[0025] 步骤5:区块链放映机轻节点将会将信息回传作为交易请求调用信息回传智能合约将交易请求发送至区块链服务器。区块链服务器接收并广播交易,在各个区块链节点达成共识后记入区块链账本并向用户返回信息回传结果。

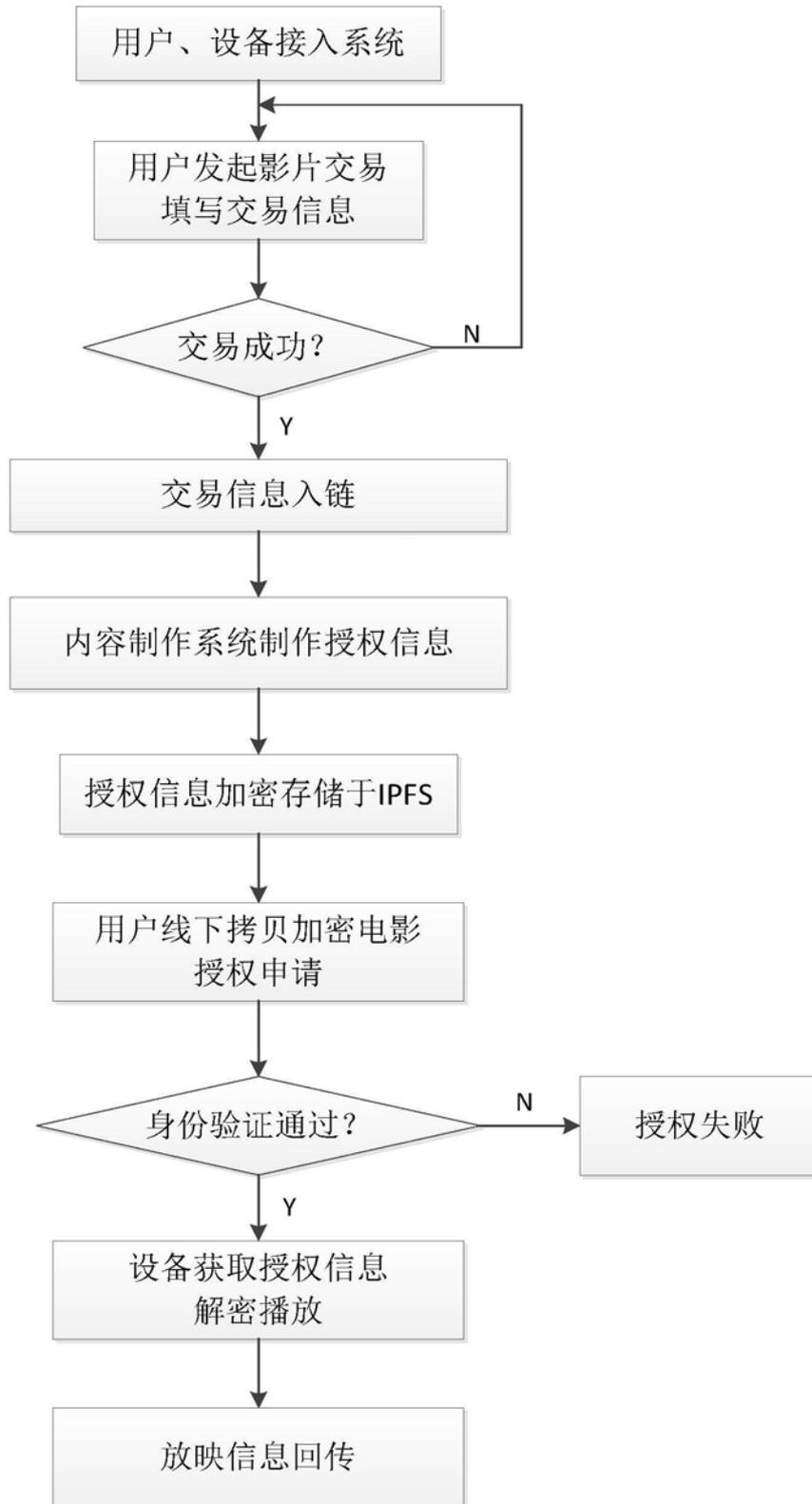


图1

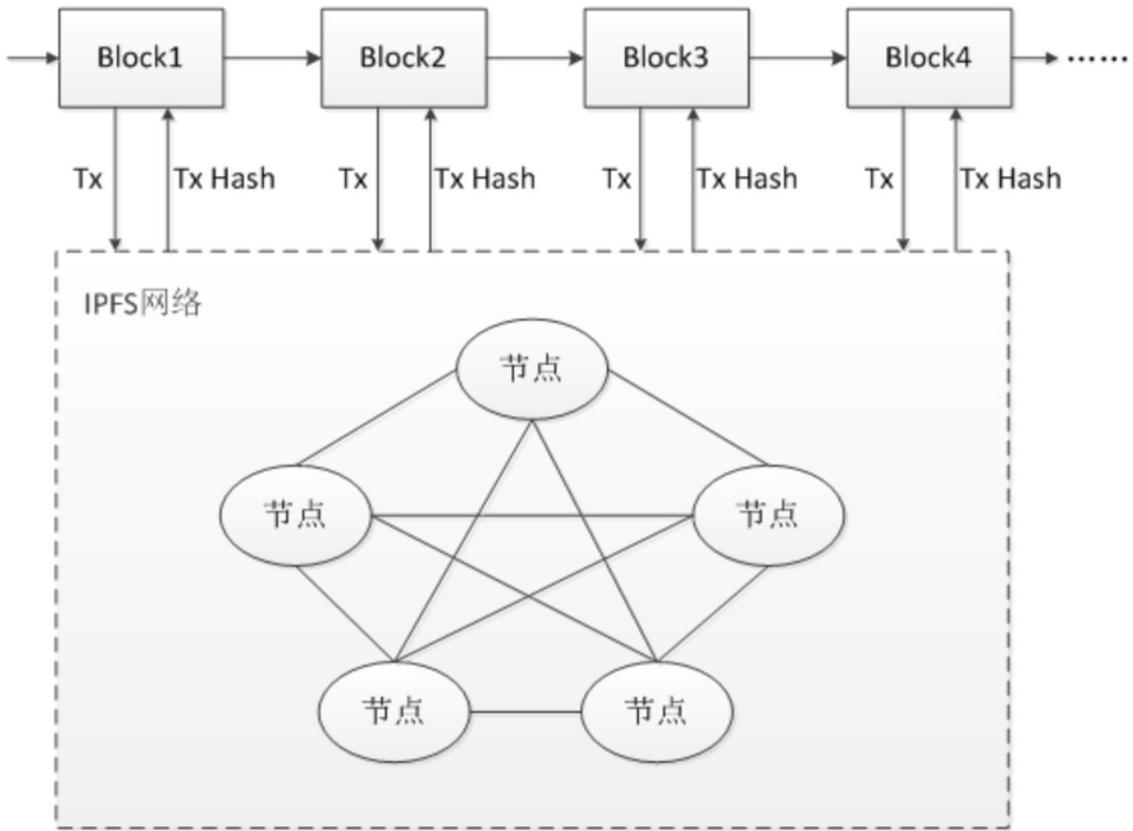


图2

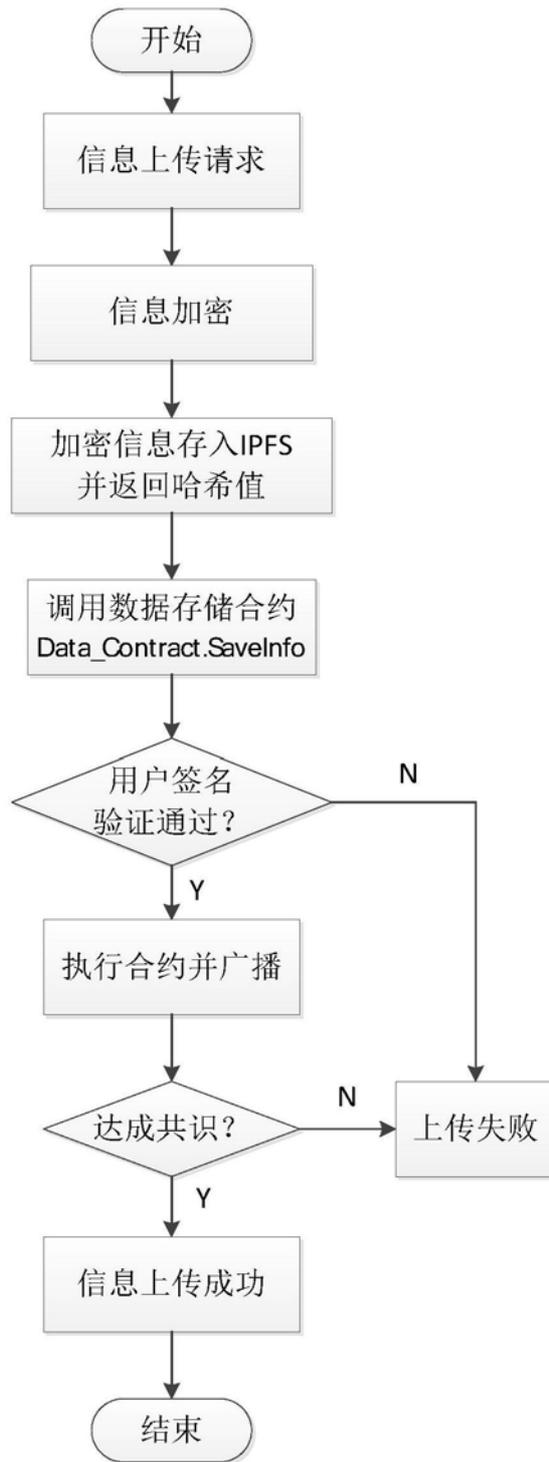


图3

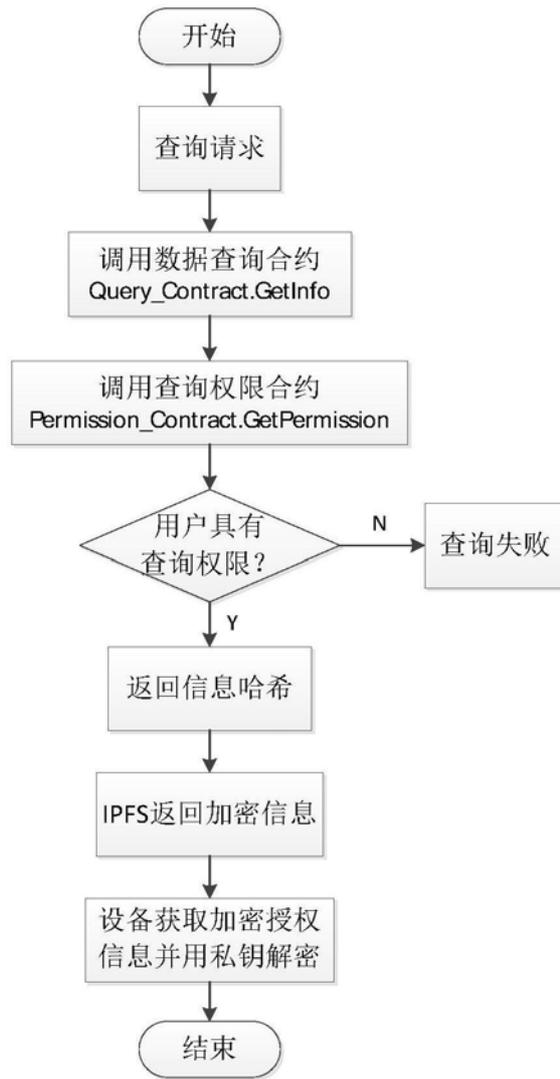


图4