北京郵電大學
Beijing University of Posts and Telecommunications

数字内容安全

第五章 数字版权管理

网络空间安全学院

本章内容

- 5.1 数字版权管理概述
- 5.2 权限控制模型
- 5.3 权利描述语言
- 5.4 现有DRM系统
- 5.5 数字版权保护新趋势

讨论问题：如何保护数字版权？

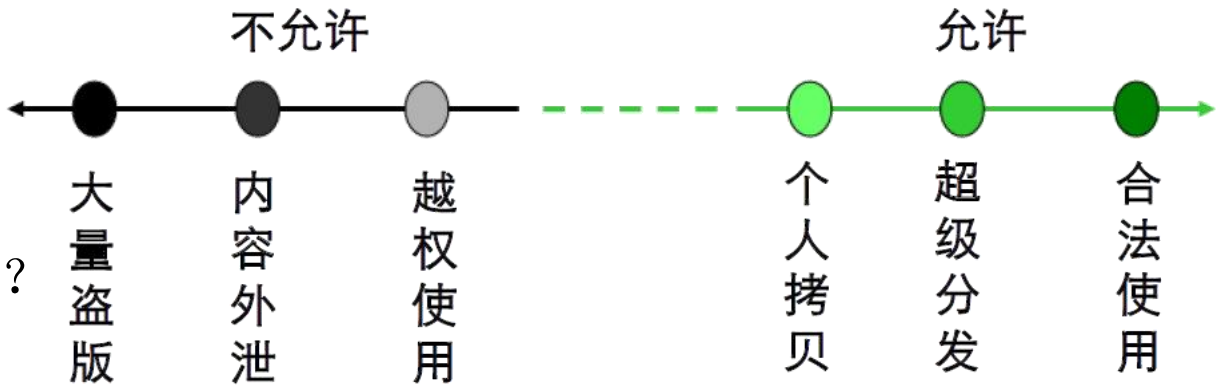
- 数字水印是否能够解决？
  - 一经破解，则由于网络上传播快速，马上失效。
  - 即使商品过了版权的保护年限，DRM仍然限制使用。
- 数字版权管理的限制包括哪些？
  - 必须在指定电脑或播放机才能播放
  - 必须在特定的日期前才能播放
  - 播放的次数
  - 传输到播放机的次数
  - 烧录到光碟的次数
  - 以上限制的混合

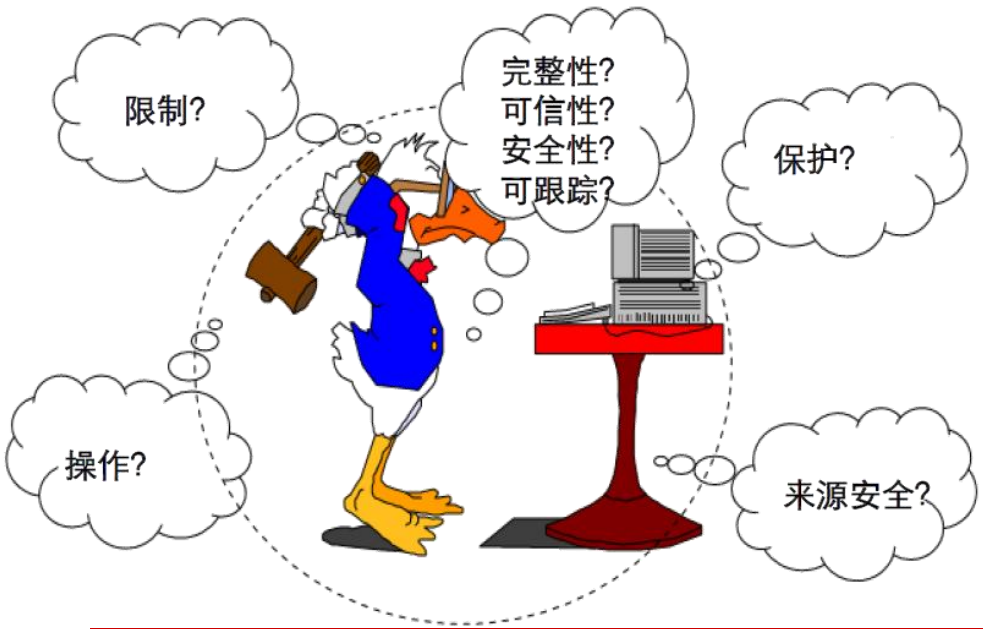
数字版权的“非技术公理”

- 媒体版权权属证明不是技术问题，或者说不能从根本上依靠技术解决，例如：
  - 对于公开发行的内容来说，数字水印是绕了弯路的办法，证明靠水印，可是非版权拥有者也叠加水印的情况下，只有出示未加水印的原始内容才能说明权属
  - 密码技术保护内容是本末倒置：内容拥有者和合法消费者支付密码技术设施等额外费用，盗版者透过模拟漏洞不用额外成本而消费内容
- 直接的办法是内容一旦创建，就有公认的中立机构注册登记，还需要数字版权管理的支持
  - 2006年3月，法国议会下院通过一系列版权法修订案，其中一条要求DRM系统之间必须能够互操作，从而使得消费者能够在不同设备上播放内容并能够复制个人拷贝。
  - 2006年6月，此法案几经争议、修改，由法国议会上院批准通过。
  - 这个法案标志着DRM领域讨论多时的互操作问题已经从技术层面上升到社会层面，互操作已经成为DRM技术研究和产品开发面临的最重要的问题之一。

数字版权管理

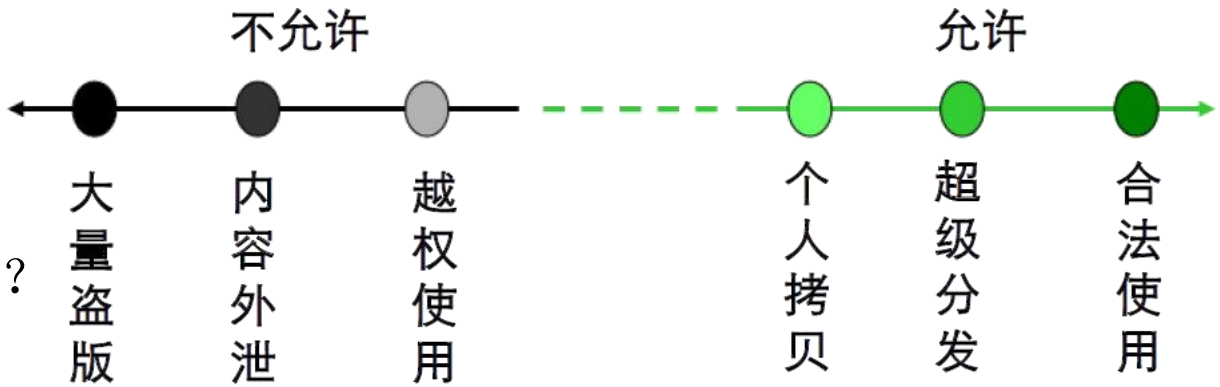
- 数字权利是什么？
- DRM是什么？
- DRM解决什么问题？

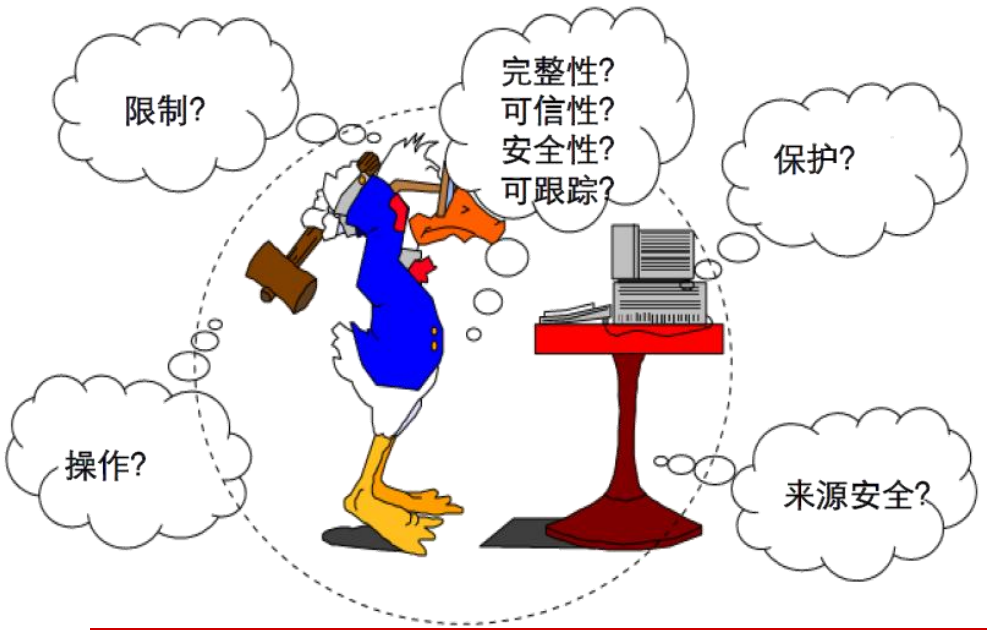




数字版权管理

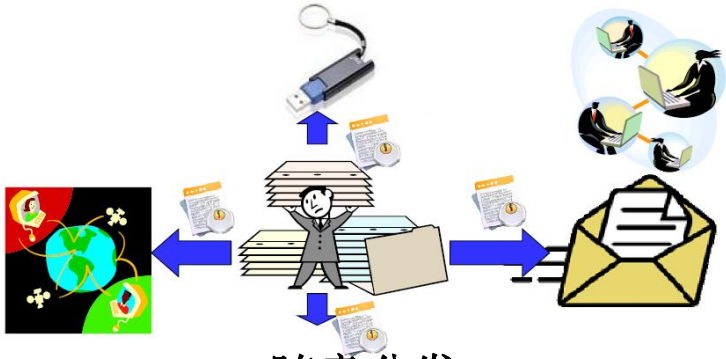
- 数字权利是什么？
- DRM是什么？
- DRM解决什么问题？



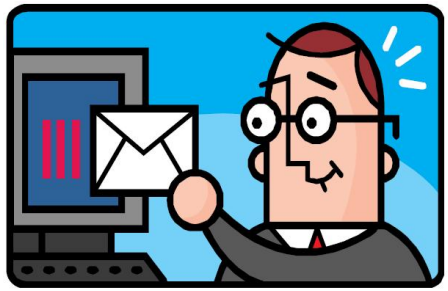


数字版权管理DRM解决的问题

- DRM解决什么问题？



随意分发

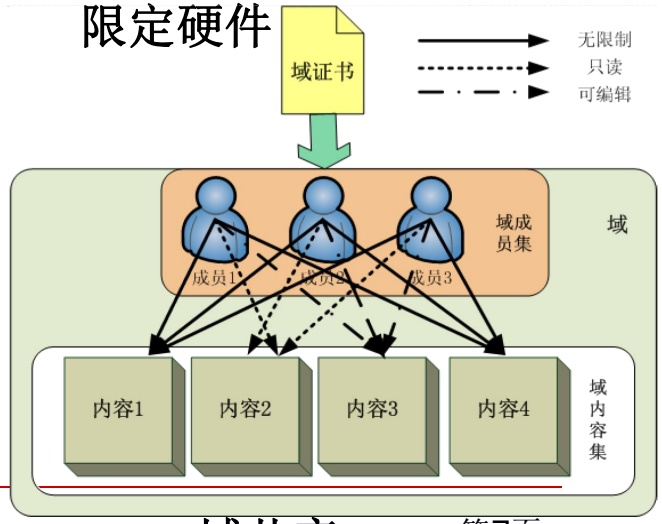


授权设备

非授权设备

多设备共享

限定硬件



域共享

数字版权管理DRM的例子

5.1数字版权管理概述

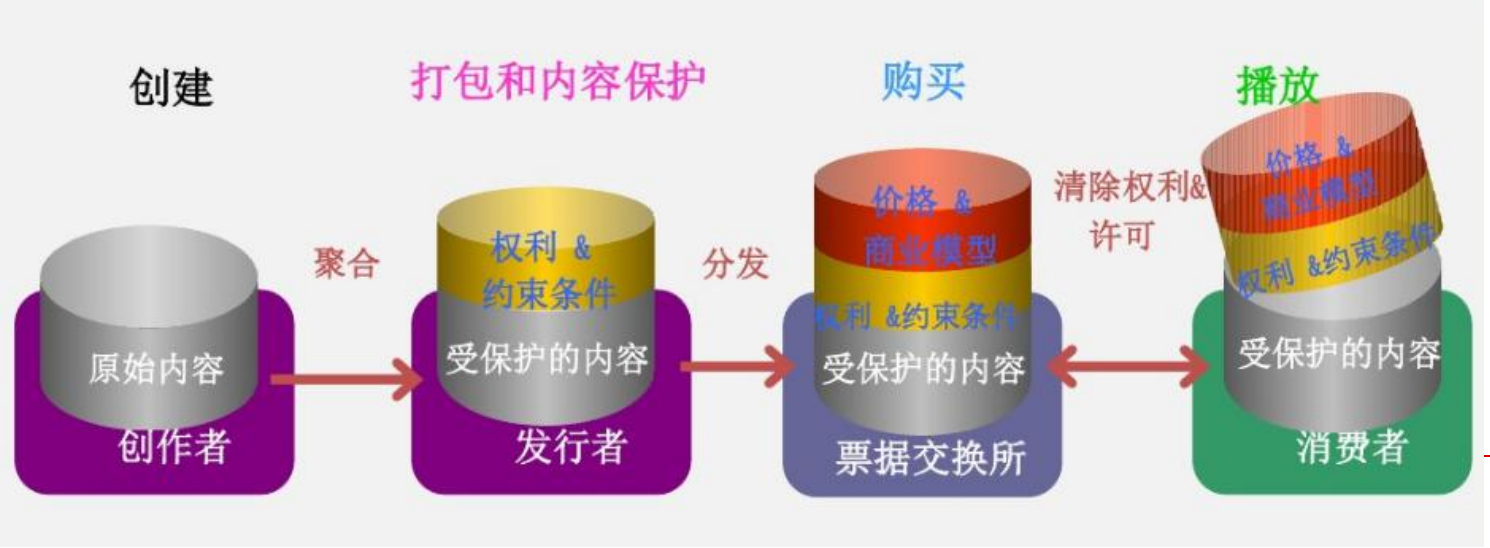
- 数字版权管理，即所谓的DRM（Digital Rights Management），也称数字版权保护，就是采取信息安全技术手段在内的系统解决方案，在保证合法的、具有权限的用户对数字信息（如数字图像、音频 、视频等）正常使用的同时，保护数字信息创作者和拥有者的版权，根据版权信息使其获得合法收益 ，在版权受到侵害时能够鉴别数字信息的版权归属及版权信息的真伪，并确定盗版数字作品的来源。
- DRM是对数字媒体进行版权管理的系统性方法。按W3C组织的建议，DRM涉及数字内容使用权限的描述、认证、交易、保护、监测、跟踪，以及对使用权拥有者之间关系的管理
  - 第一代DRM侧重于对内容加密，限制非法复制和传播，确保只有付费用户能够使用
  - 第二代DRM在第一代的基础上，在权限管理方面有了较大的拓展，发展非常蓬勃，索尼PS游戏机，以及苹果iPhone的热销，更多的用户开始在这些设备上下载和播放电影电视节目，带动了市场对DRM的需求

数字版权管理概述

- DRM是内容安全的一种具体应用，即对数字内容使用权限的确认、封装、分发、控制、追踪的机制。
  - 权限确认即用户对感兴趣的内容提出使用权限的需求，服务器对其资格和要求验证的过程；
  - 权限封装即对赋予用户的使用权限及相关信息的加密或保护的过程；
  - 权限分发即将封装好的权限对象安全交付给用户的过程
  - 权限控制即内在的权限内容的具体生成和外在的权限内容的具体实施；
  - 盗版追踪即保证版权拥有者的合法权利，并对盗版者予以打击。数字内容盗版追踪主要靠数字水印技术或者一些网络追踪来实现。

数字版权管理概述

- DRM为数字内容产品创作—发行—消费的价值链中的各个环节都带来了实际的利益。
  - 对于消费者来说可以获得更多所需要的数字信息；
  - 对发行者而言，利用发行资源（如网络带宽）、增加消费数量，从而获得收益。
  - 创作者和版权拥有者的数字作品可以从保护中获得应有的收益。



数字版权管理概述

- DRM的基本特征

数字版权管理概述

- DRM的分类
  - 根据保护的数字内容，可以分为针对电子书的DRM系统（例如方正Apabi DRM），针对多媒体的DRM，针对数字电视的DRM系统（例如AVS DRM）等。
  - 根据有无使用特殊的硬件，可以分为基于硬件的DRM系统（例如iPod DRM）和纯软件的DRM系统
  - 根据采用的安全技术，可以分为基于密码技术的DRM系统和基于数字水印技术的DRM系统，以及两者结合的DRM系统。

数字版权管理概述

- DRM源于数字化商业活动中对版权保护的需求，对其功能上的需求包括权限控制、版权认证、内容认证、盗版追踪、操作跟踪等内容。

数字版权管理概述

- 权限控制 ： 对版权保护的最基本的要求就是权限控制。
- 权限控制包括两个方面：
  - 具有权限的合法用户能够正常使用数字内容，无权限的用户将被部分或完全禁止对数字内容的访问，比如只可以浏览内容摘要等；
  - 不同的权限具有不同的对数字内容的访问使用能力，版权保护系统应能区分不同的权限，并根据权限的不同控制用户对数字内容的访问。
- 拷贝控制、播放控制、处理能力控制、有效期限制都属于权限控制的范畴。

数字版权管理概述

- 拷贝控制对用户将数字内容在相同或不同设备上复制副本的操作进行限制；
- 播放控制主要对数字内容的播放次数、时间、对象进行限制。
- 处理能力控制是指对用户实施到数字内容上的旋转、剪辑、缩放、添加内容等操作的限制。
- 用户获得的权限往往是通过统一的格式即权力描述语言进行表 述的，被描述的权限可能作为权限证书的一部分（如PMI， Privilege Management Infrastructure，授权管理基础设施）， 也可能直接形成特殊的权限对象与受保护的数字内容一起或分别传递给授权用户（如SDMI）。
- 权限控制的实现方式有很多种比如有第三方参与的身份认证、PMI权限证书、内容加密、安全容器等。

数字版权管理概述

- 版权认证属于数字内容版权保护的基本功能，它也包括两部分内容，即：
  - 所有者鉴别，即验证数字内容的版权归属，即所有者是谁；
  - 所有权验证，即当多个人声称拥有数字内容的版权时，能够 验证数字内容的真正作者，为解决版权纠纷提供依据。
- 申请出版权认证的可能是数字内容制作、分发、使用全过程中的任何实体。
- 版权认证的方法有解密权限描述中的版权信息、提取版权水印、媒体桥技术等。版权信息应具有唯一性、 可验证性的特点。

数字版权管理概述

- 内容认证 ，也称为内容完整性认证，主要是对数字内容自生成以来是否发生过变化做出判断。这种变化可能是全局的也可能是局部的。
- 通常的内容认证方法是采用数字签名技术或信息摘要。
- 签名作为数字内容的辅助数据和内容一同传输、保存，容易丢失。可选的方法是采用水印技术，将签名作为脆弱水印嵌入到 数字内容中，内容的改变同样将导致签名不匹配。
- 内容认证属于版权保护的高级功能，往往被司法机关或对内容 修改敏感的应用使用。

数字版权管理概述

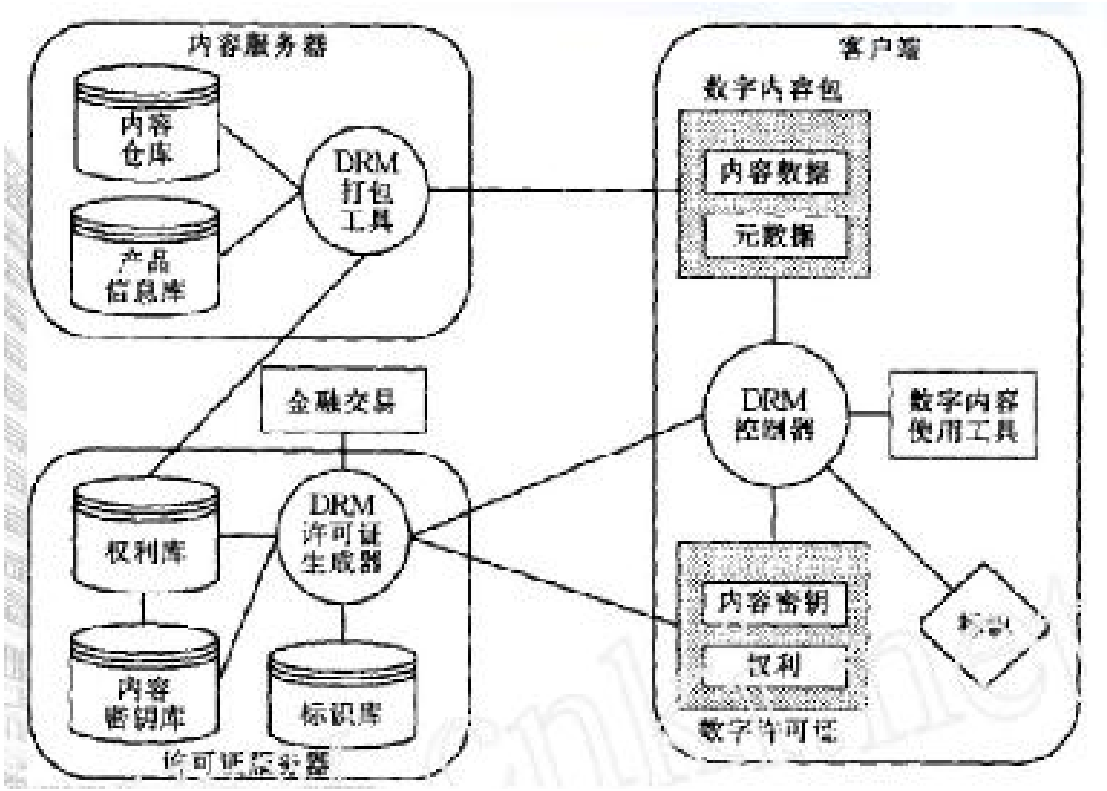
- 操作跟踪也属于版权保护的高级功能。数字内容被加入到版权保护系统中后，被传播和使用，在这期间，数字内容可能会被有意、无意的修改，通过操作跟踪可以确定数字作品所经历的修改，进一步有可能恢复出最初的数字内容
- 实现操作跟踪的简单方法就是在封闭的数字内容使用环境中建立修改日志，记录数字内容被修改所采取的操作。这种方式对 服务器来说是有用的，但对用户终端来说却没有意义，因为将侵犯个人隐私，而且任何人也不会报告自己对数字内容的处理 。

数字版权管理概述

- 盗版追踪是指确定数字内容盗版的来源，即第一个把受保护的 数字内容泄露出去的用户或实体，这个实体可能是数字作品的 制作者本身，也可能是销售者、运营商，或者是终端用户。
- 比如在DiVX增强播放器中就存在盗版追踪技术，它在播放的影片中添加了播放器唯一的水印，通过检测盗版影片中的水印即可判断它的来源。此外，在影片拷贝分发中也可以采用类似的原理，来控制盗版的发生。
- 盗版追踪主要通过数字水印技术来完成，同时为了实现主动的追踪，还应建立网络监控手段，通过追踪代理或网络警察来及时发现存在的盗版，防止复制。

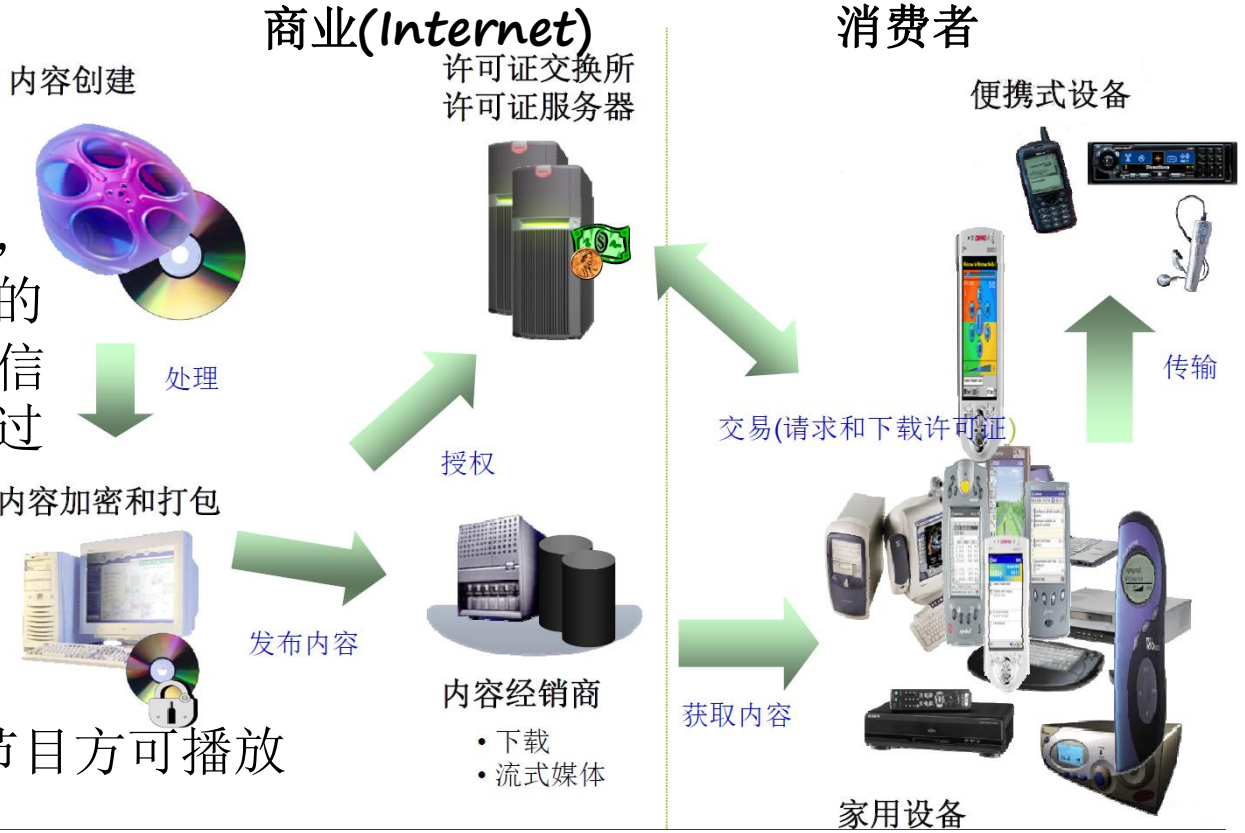
数字版权管理概述

- 数字内容提供者通过内容封装机制将其媒体内容为DRM媒体格式，同时也向授权中心注册其内容，并由用户申请获得对DRM媒体内容的使用权限。
- 其中的关键问题在于权限如何描述和管理。



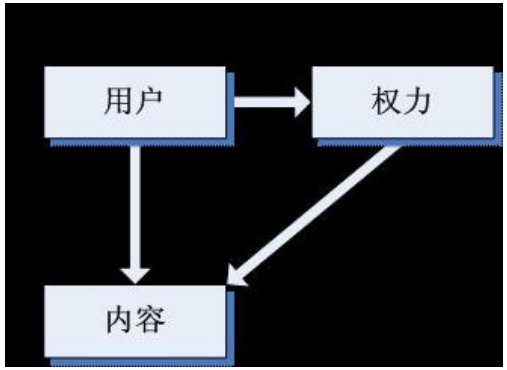
数字版权管理概述

- DRM技术的基本工作原理
- 首先建立数字节目授权中心。编码压缩后的数字节目内容，可以利用密钥（Key）进行加密保护（Lock），加密的数字节目头部存放着KeyID和节目授权中心的URL
- 用户在点播时，根据节目头部的KeyID和URL信息，就可以通过数字节目授权中心的验证授权后送出相关的密钥解密（unLock），节目方可播放



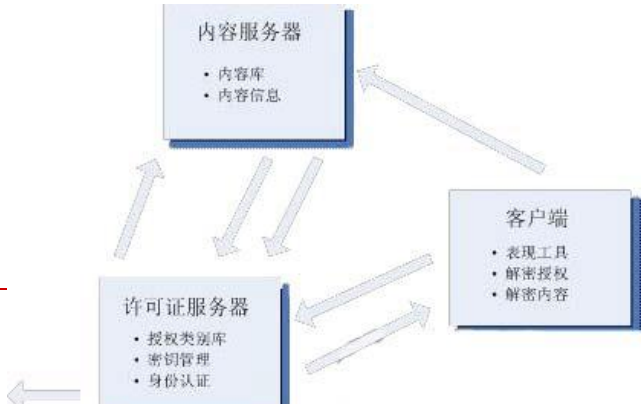
数字版权管理概述

- 用户、授权和内容是DRM系统的三个基本要素。
  - 用户是内容的创建者和使用者，用户可以是出版商、电影制作商、唱片公司、企业或消费者个人
  - 内容系指一切可以通过网络传播的数字内容的集合
  - 授权系指加载于内容之上并授给用户的许可、约束和义务
    - 许可是对用户操作内容方式的授权，比如针对用户的读写、打印、屏幕复制等权限
    - 约束是对许可的限制，比如用户只能在自己的电脑上操作等
    - 义务是对用户的要求，比如用户必须提供相关资料、承担法律义务等



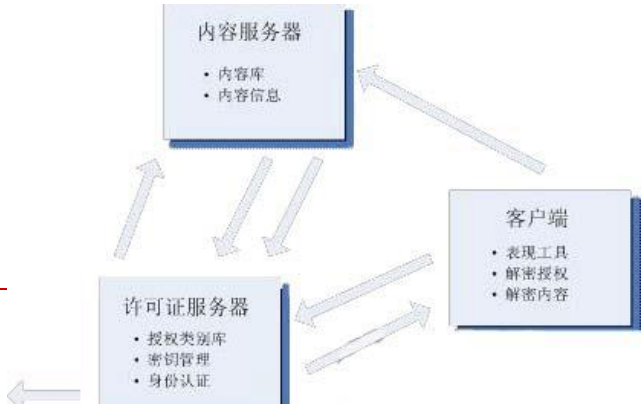
数字版权管理概述

- DRM系统运作：
  - DRM系统还可包括授权策略定义和管理、授权协议管理、风险管理等功能
    - 目前DRM系统多采用XrML语言来描述授权。XrML语言与XML语言的元素与属性一致，专门用于描述数字内容属性
    - 符合XrML规范的授权许可作为附加，随数字内容一起分发，即可在线下载，也可离线分发
  - DRM系统由内容服务器、授权服务器和客户端三部分组成
    - 内容服务器不仅存储数字内容，还存放关于数字内容的信息，比如数字内容的目录、数字内容的简介、说明、价格等信息。
    - 许可证服务器负责管理与授权类别相关的XrML文档、生成并管理密钥、识别和认证用户身份。
    - 客户端需要有支持DRM的数字内容表现工具（比如播放器、阅读器等），承担解密XrML格式的授权代码并对加密的数字内容进行解密



数字版权管理概述

- DRM系统的运作，从用户查找数字内容到按授权使用，大致有九步
  - 1. 用户从客户端访问内容服务器，查询内容情况，确定自己需要的内容
  - 2. 用户从客户端向许可证服务器发出请求，提出自己所需要的内容并申请所需的使用授权，通常会要求用户填写在线表格
  - 3. 许可证服务器请求内容服务器核查用户请求的内容是否可用
  - 4. 许可证服务器检证用户身份，比如需要将用户的权限请求与用户权限数据库核对
  - 5. 内容服务器将用户需要的内容从内容库取出，发到许可证服务器
  - 6. 在商业性DRM系统里，需要与银行相联，完成转帐、信用卡支付等必要的财务过程
  - 7. 许可证服务器将数字内容和授权代码合并加密，生成向用户下载的数据包
  - 8. 将数据包发给用户
  - 9. 客户端解密授权代码和数字内容，表现工具按代码展现数字内容

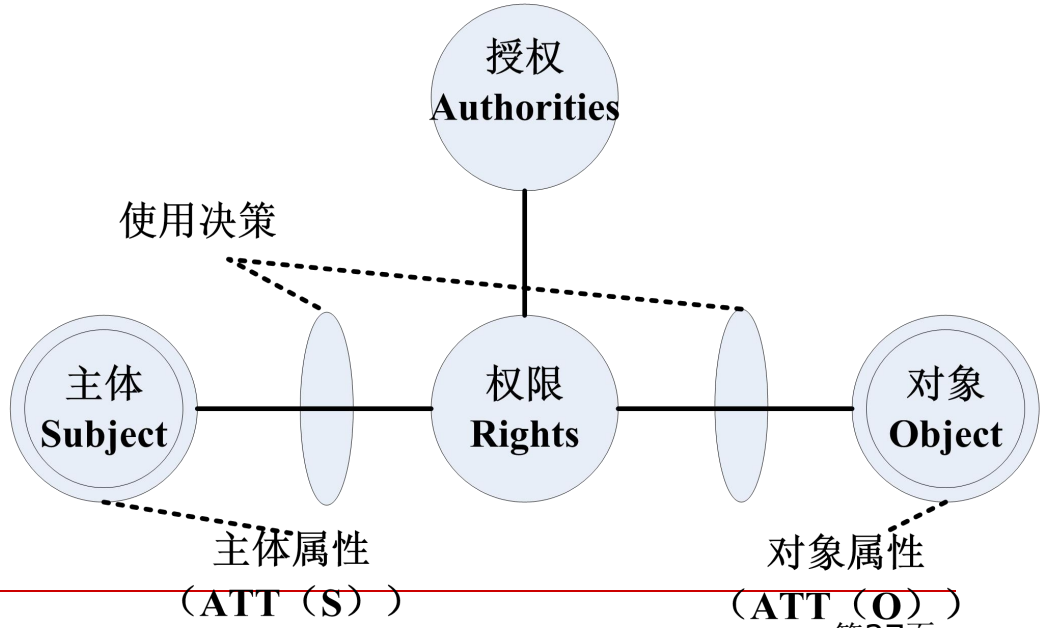


5.2权限控制模型

- 权限控制源于传统的访问控制，又与之有所不同
- 传统的访问控制是通过某种途径显式地允许或限制主体对客体访问能力及范围的一种方法。
- 访问控制的核心是授权策略，主要策略有：
  - 自主访问控制
  - 强制访问控制
  - 基于角色的访问控制

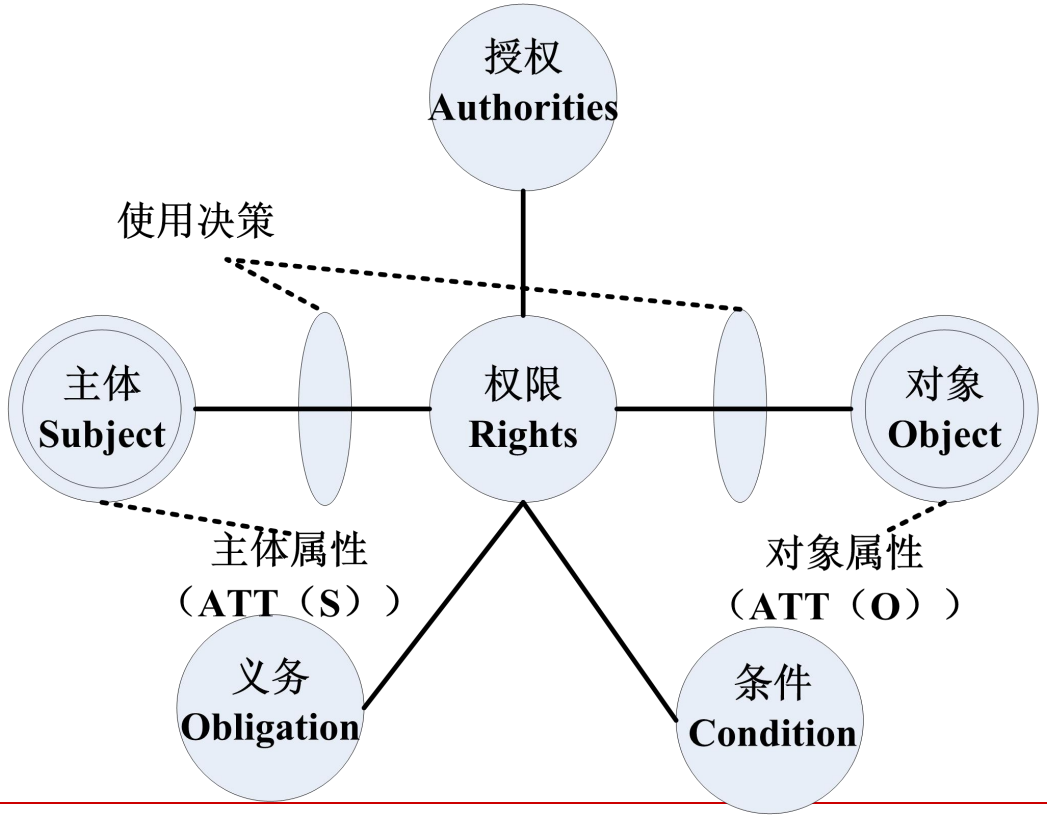
5.2权限控制模型

- 传统的访问控制模型都是基于主体-客体的安全模型，存在如下缺陷：
  - 权限是静态的
  - 权限分配只能在执行任务之前
  - 处在封闭环境中



5.2权限控制模型

- 使用控制模型：UCON模型，ABC(Authorities, oBligation, Condition)模型



5.2权限控制模型

- 使用控制模型：UCON模型，ABC模型
- 授权
- 义务
- 条件
- 连续性：在整个资源的使用过程中对访问请求进行实时监控
- 可变性：有些属性会因为主体的行为而被修改
  - 不变属性：由管理员进行修改，如用户的工作组
  - 可变属性：在系统运行过程中改变

5.2权限控制模型

- UCON模型，ABC模型
  - 主体
    - 主体（S）是可以对客体拥有某些使用权限的主动实体，包括用户组（用户所在的组织）、用户、计算机终端、手持终端、应用服务程序等。
    - 消费者主体（Consumer Subject，CS）
    - 生产者主体（Provider Subject，PS）
    - 审计主体（Identifiee Subject，IS）
  - 客体
    - 客体（Object）是按权限集合的规定接受主体访问的被动的实体。客体可以是文本（例如.doc、.pdf、.ps）、语音（例如.mp3、.wav）、视频（例如JPEG、DVD、MPEG）、可执行文件（例如游戏）等数字作品，也可以是网络上的硬件设备，无线通信中的终端等。
    - 原始客体和派生客体

5.2权限控制模型

- UCON模型，ABC模型
  - 权限
    - 权限（R）是主体可以对客体拥有和实施的权限集，包括允许主体访问客体的使用功能集。
    - 消费权限（CR），生产权限（PR）和审计权限（IR）。
  - 授权（A）
    - 授权是基于主、客体的属性和所请求的权限（如读或写权限）并依据权限规则集进行的权限判断操作。
    - 可以在访问之前或是访问过程中进行授权判断的操作

5.2权限控制模型

- UCON模型，ABC模型
  - 义务
    - 义务（O）是强制要求主体必须在访问之前或访问过程中执行的功能性谓词。
  - 条件
    - 条件（C）是环境的或面向系统的决策因素。
    - 评估当前环境或系统的状态，检查是否满足了相应请求。

5.2权限控制模型

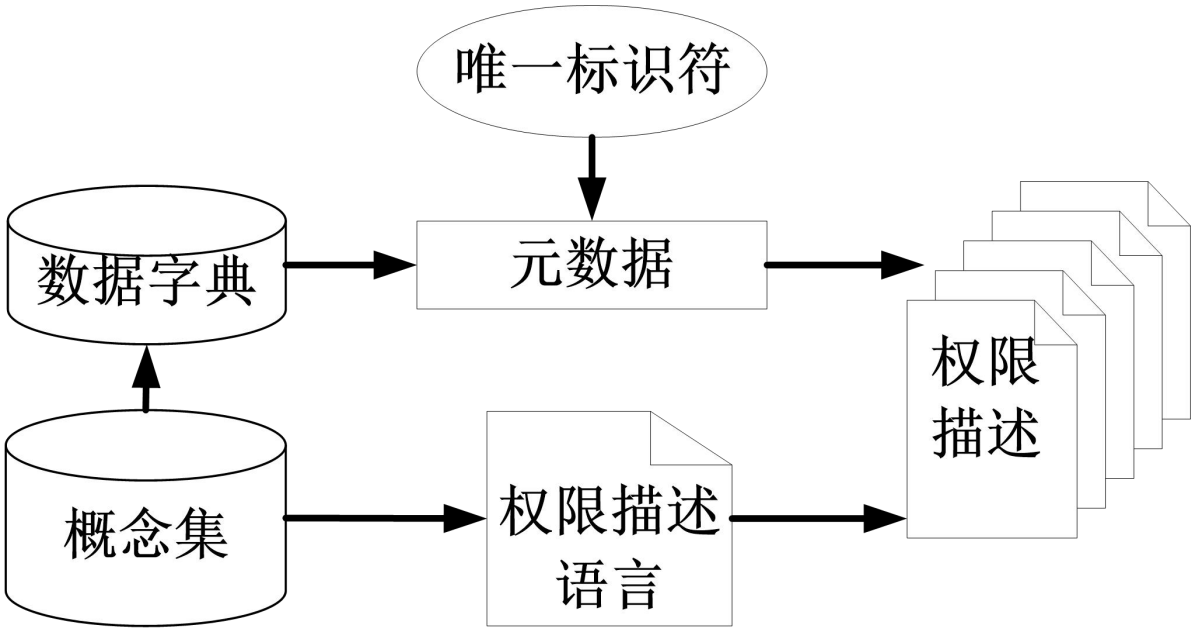
- 横坐标，属性可变性
- 纵坐标，使用前/后授权(preA/onA)赋予、使用前/后义务(preB/onB)赋予、使用前/后环境条件(preC/onC)赋予

16 种基本 ABC 模型矩阵

	0（不可改变）	1（使用前更新）	2（使用中更新）	3（使用后更新）
preA	Y	Y	N	Y
onA	Y	Y	Y	Y
preB	Y	Y	N	Y
onB	Y	Y	Y	Y
preC	Y	N	N	N
onC	Y	N	N	N

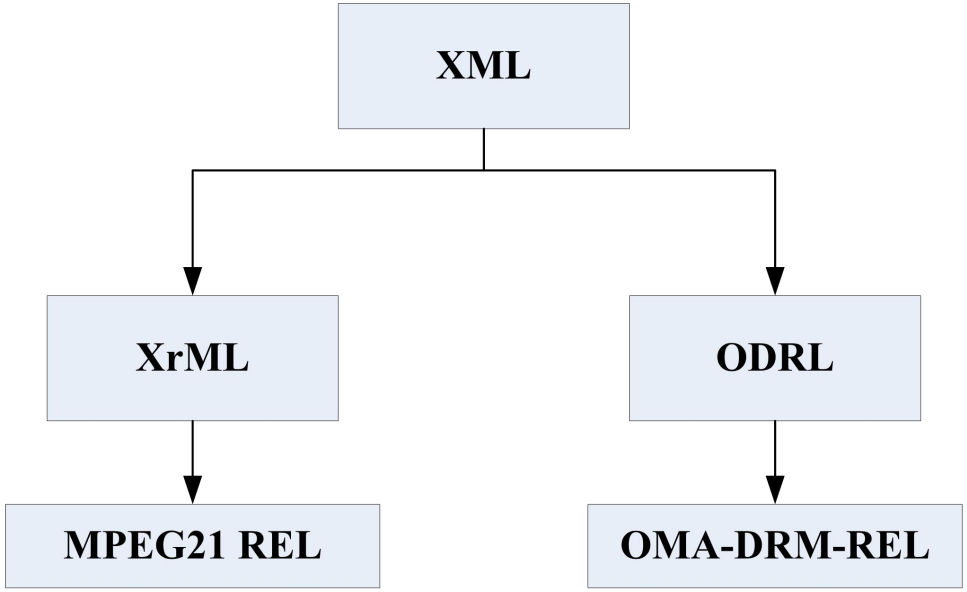
5.3权利描述语言（REL）

- REL体系结构



5.3权利描述语言（REL）

- REL体系结构

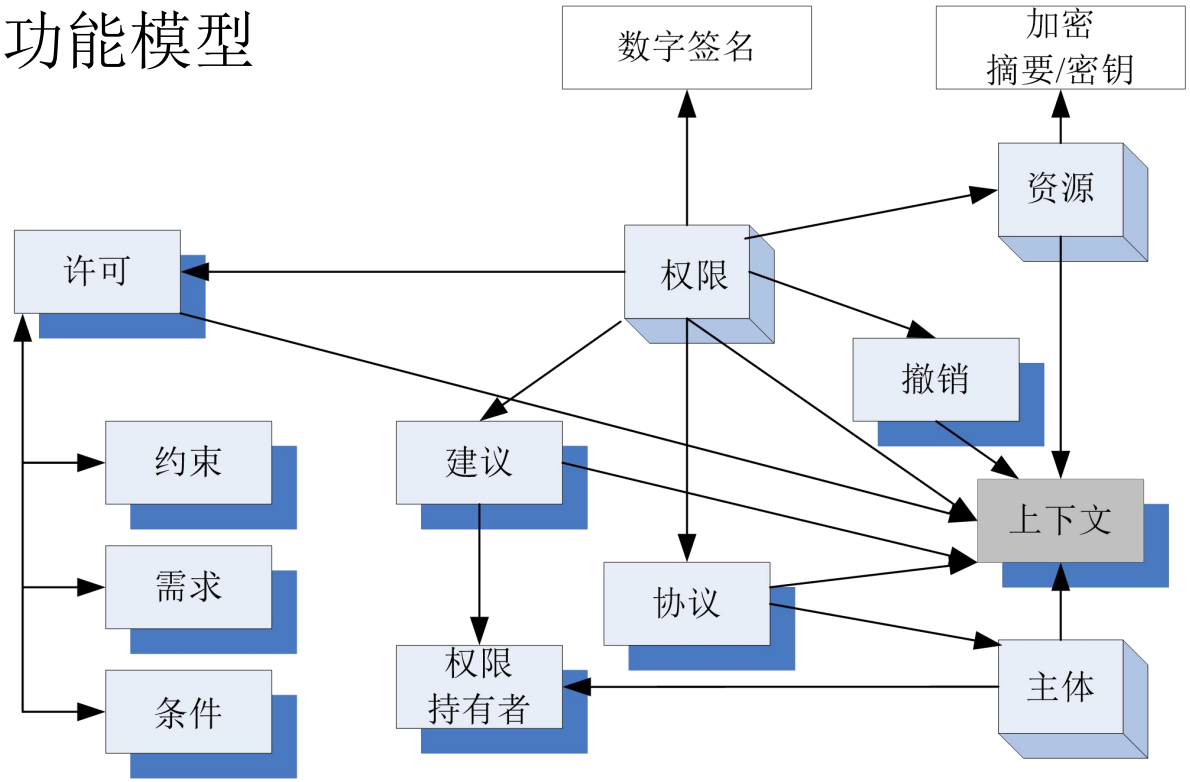


5.3权利描述语言（REL）

- ODRL（OMA-DRM-REL ）
  - 权限表达模型
  - 权限数据字典
  - XML Schema

5.3权利描述语言（REL）

- ODRL（OMA-DRM-REL ）
  - 功能模型



5.3权利描述语言（REL）

- ODRL（OMA-DRM-REL ）
  - 功能模型
    - 资源：可以是任何实物和数字内容
    - 权限：包括许可，许可包括约束、需求和条件。
      - 许可是被允许对资源进行的一些使用或操作，如播放一段视频
      - 约束是对许可的限制，如最多播放5次
      - 需求是为了执行某个许可而必须承担的义务，如付费
      - 条件是指明例外情况
    - 主体：包括终端和权限持有者，通常是消费者。

5.3权利描述语言（REL）

- ODRL（OMA-DRM-REL ）
  - 功能模型
    - 建议是指权限持有者对其拥有的资源的某个确定权限的一些建议，针对资源不同的商业模式可以创造不同的建议来满足需要。
    - 协议就是主体对某个资源权限的建议到许可的中间过渡，但这并不意味着建议一定要出现在协议之前。
    - 上下文具有十分重要的唯一标识实体功能

5.3权利描述语言（REL）

- ODRL（OMA-DRM-REL ）
  - 功能模型

例 9.1 功能模型的 XML 语法

```
<rights>
    <context>.
        <uid>...</uid>
    </context>
    <offer>
        <asset>...</asset>
        <permission>
            <permission-type>
                <requirement>...</requirement>
                <constraint>...</constraint>
            </permission-type>
            <condition>...</condition>
        </permission>
        <party>
            <context>...</context>
            <rightsholder>...</rightsholder>
        </party>
    </offer>
    <agreement>
        <context>...</context>
        <party>...</party>
        <permission>...</permission>
        <asset> ... </asset>
    </agreement>
</rights>
```

5.3权利描述语言（REL）

- ODRL（OMA-DRM-REL ）
  - 许可模型
    - 使用（Usage）是指对资源的一类使用或消费方法。具体实现包括显示（Display）、打印（Print）、播放（Play）、执行（Execute）等。
    - 重用（Reuse）指重用资源的一类操作。具体实现有修改（Modify）、引用（Extract）、注释（Annotate）、聚合（Aggregate）等。
    - 传递（Transfer）指资源权限传递的过程集。具体实现有销售（Sell）、出借（Lend）、给予（Give）、出租（Lease）等。
    - 资源管理（Asset Management）指数字资源管理操作集。具体实现有移动（Move）、复制（Duplicate）、删除（Delete）、核实（Verify）、备份（Backup）、恢复（Restore）、保存（Save）、安装（Install）、卸载（Uninstall）等。
    - 排他性”（Exclusivity）

5.3权利描述语言（REL）

- ODRL（OMA-DRM-REL ）
  - 约束模型
    - 用户（User）指用于限定用户的一类约束。具体实现是单个（Individual）和群（Group）。
    - 设备（Device）指用于限定使用的物理设备或系统的一类约束。具体实现为CPU、网络（Network）、屏幕（Screen）、内存（Memory）、打印机（Printer）、软件（Software）、硬件（Hardware）等。
    - 范围（Bounds）:指用于限定使用数量和范围的一类约束。具体实现为数量（Count）、范围（Range）、空间（Spatial）等。
    - 时间（Temporal）指限制使用时间的一类约束。具体实现为日期（Date Time）、累计时间（Accumulated）、间隔（Interval）等。
    - 外观（Aspect）指限定资源特征和表现形式的一类约束。具体实现包括格式（Format）、质量（Quality）、单位（Unit）、水印（Watermark）等。
    - 目标（Target）指限制使用资源的地点和方法的一类约束。具体实例为目的（Purpose）、行业（Industry）、等。
    - 权限（Rights）指用于授权转移许可和使能下游许可规范的一些约束。具体实现为转移许可（Transfer Permission）。

5.3权利描述语言（REL）

- ODRL（OMA-DRM-REL ）
  - 需求模型
    - 费用（Fee）指使用付费需求。具体实现包括预付（PrePay）、后付（PostPay）一次一付（PerUse）等。
    - 交互（Interaction）指用户交互需求。具体实现为注册（Register）等。
    - 使用（Usage）指使用资源的需求。具体实现为归属（Attribution）、追踪（Tracked）等。

5.3权利描述语言（REL）

- ODRL（OMA-DRM-REL ）
  - 条件模型

例 6.2 条件模型的 XML 语法

```
<permission>
    <sell/>
    <play>
        <condition>
            <constraint>
                <software>…</software>
            <constraint/>
        </condition>
    </play>
</permission>
```

```
<condition>
    <constraint>
        <spatial>
            <context>
                <uid>iso3166:AU</uid>
            </context>
        </spatial>
    <constraint/>
</condition>
```

5.3权利描述语言（REL）

- ODRL（OMA-DRM-REL ）
  - 权限持有者模型
    - 只有一个抽象实体——版税（Royalty），其具体实现为：百分比（Percentage）和定值（Fixed Amount），分别指主体为每次交易所承担的付费占整个交易的比例和付费的具体值，即权限持有者能够获得的利益。

5.3权利描述语言（REL）

- ODRL（OMA-DRM-REL ）
  - 权限持有者模型

例 6.3 权限持有者模型 XML 语法

```
<party>
    <context> ... </context>
    <rightsholder>
        <percentage>90</percentage>
    </rightsholder>
</party>
<party>
    <context> ... </context>
    <rightsholder>
        <percentage>10</percentage>
    </rightsholder>
</party>
```

5.3权利描述语言（REL）

- ODRL（OMA-DRM-REL ）
  - 上下文模型
    - 十个实体的聚合。包括实体的唯一标识符UID、名称——实体名称、角色、备注、版本、日期、事件、物理位置、数字位置、外部引用、交易和服务。

5.3权利描述语言（REL）

- ODRL（OMA-DRM-REL ）
  - 建议和协议实体模型
    - 建议实体和协议实体都由资源、权限持有者、许可和上下文等四个实体的组合来表达。二者不同之处在于协议由多个主体参与。

5.3权利描述语言（REL）

- ODRL（OMA-DRM-REL ）
  - 撤销模型
    - 撤销实体表示对建议或协议的撤销，它只包含一个上下文实体，用上下文实体来标识被撤销的建议或协议。

5.3权利描述语言（REL）

- ODRL（OMA-DRM-REL ）
  - 安全模型
    - ODRL支持W3C规定的XML数字签名和加密技术。

5.3权利描述语言（REL）

- XrML语言
  - 微软（Microsoft）和施乐（Xerox）合作的ContentGuard公司

例 6.4 一位密钥持有者可以在 2007 年 5 月 30 日之前阅读给定 URL 上的一本电子书

```
<license>
    <grant>
        <keyHolder>
            <info>
                <dsig:KeyValue>
                    <dsig:RSAKeyValue>
                        <dsig:Modulus>Fa7wo6NYfmvGqy4ACSWcNmuQfbejSZx7aCib
                        kYswUeTCrmS0h27GJrA15SS7TYZzSfaS0xR9lZdUEF0ThO4w=
```

5.3权利描述语言（REL）

- XrML语言

```
                    </dsig:Modulus>
                    <dsig:Exponent>AQABAA==</dsig:Exponent>
                </dsig:RSAKeyValue>
            </dsig:KeyValue>
        </info>
    </keyHolder>
    <cx:read/>
    <cx:digitalWork>
        <cx:locator>
            <nonSecureIndirectURI="http://www.contentguard.com/sampleBook.spd"/>
        </cx:locator>
    </cx:digitalWork>
    <validityInterval>
        <notAfter>2007-05-30T23:59:59</notAfter>
    </validityInterval>
</grant>
</license>
```

5.3权利描述语言（REL）

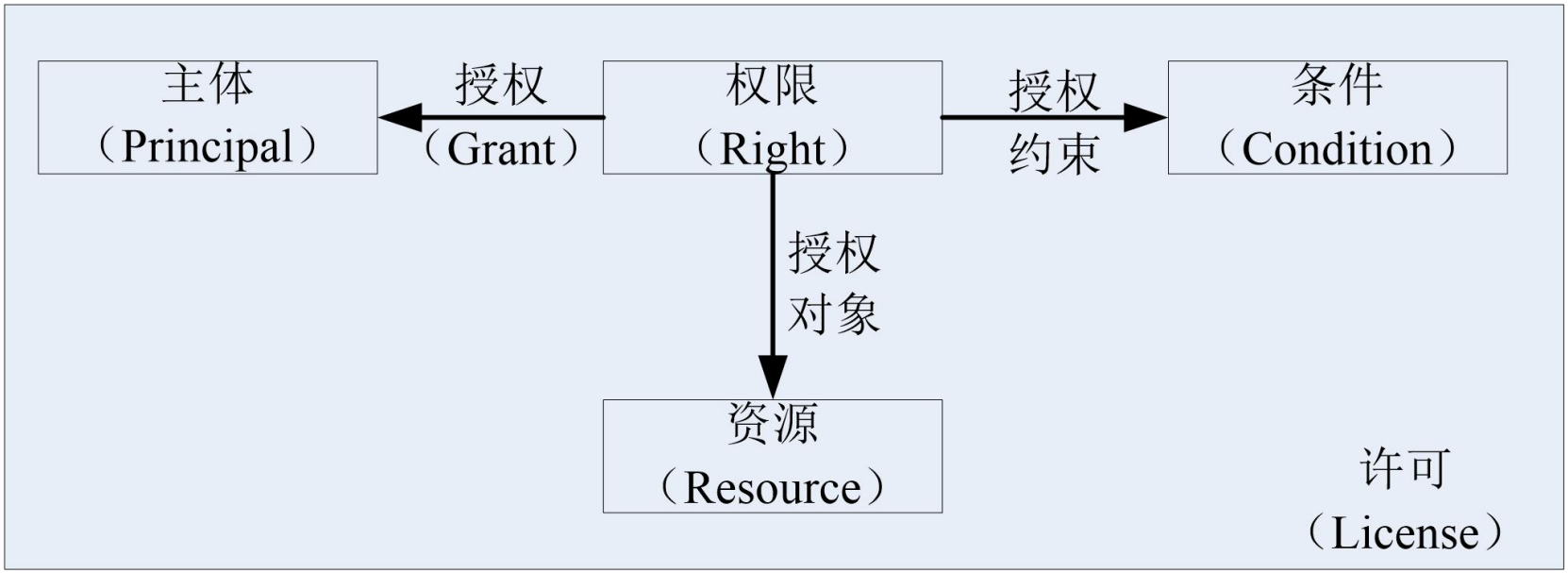
- XrML语言
  - 核心schema
    - 定义作为XrML v2.0核心语义的概念，特别是那些有关信任决策评估的概念，包括主体（principal）、权限（right）、资源（resource）、条件（condition）、授权（grant）和许可（license）等六种概念。其名称空间由前缀“r:”标识。
  - 标准扩展schema
    - 定义广泛应用于XrML v2.0使用场景但又不是XrML2.0核心语义的概念，包括六种核心概念的商业应用扩展概念。标准扩展模式的名称空间由前缀“sx:”标识。

5.3权利描述语言（REL）

- XrML语言
  - 特定内容扩展schema
    - 定义了特定的、与数字内容或作品（如图书、音乐、视频等）相关的权限管理概念，以“cx”为前缀。包括内容扩展权限、内容扩展资源和元数据、内容扩展条件和义务等。特定内容扩展模式的名称空间由前缀“cx:”标识。

5.3权利描述语言（REL）

- XrML语言



5.3权利描述语言（REL）

- XrML语言
  - 权限
  - 呈现权（Render Rights）包括：播放（play）、打印（print）、输出（export）。
  - 传送权（Transport Rights）包括：复制（copy）、转移（transfer）、借出（loan）。
  - 作品派生权（Derivative Work Rights）包括：编辑（edit）、摘录（extract）、嵌入（embed）。
  - 配置权（Configuration Rights）包括：安装（install）和卸载（uninstall）。
  - 文件管理权（File Management Rights）包括九种权利：读取（read）、写入（write）、执行（execute）、删除（delete）备份（backup）、恢复（restore）、验证（verify）、管理文件夹（manageFolder）、访问文件夹信息（accessFolderInfo）。

5.3权利描述语言（REL）

- XrML语言
  - 资源
  - 数字资源（digitalResource ）
  - 授权（grant）
  - 主体（principal）
  - 服务参考（serviceReference）
  - XML模式摘要(xmIPatternAbstract)
  - 可撤销的签名（sx:revocable）
  - 名称空间中的名称（sx:name）
  - 安全级别（cx:securityLevel）指主体的抽象安全级别
  - 数字作品（cx:digital Work）。

5.3权利描述语言（REL）

- XrML语言
  - 条件
  - 目的地（cx:destination）、助手（cx:helper）、播放器（cx:render）、来源（cx:source）、水印（cx:watermark）、现有权限（existsRight）、先决权限（prerequisiteRight）、撤销开始（revocationFreshness）、执行次数（sx:exerciseLimit）费用（sx:fee）、寻求认可（sx:seekApproval）、地域（sx:territory）、跟踪查询（sx:trackQuery）、跟踪报告（sx:trackReport）、有效时间间隔（validityInterval）、有效持续时间（sx:validityIntervalFloating）、有效累计时间（sx:validityTimeMtered）、有效时间周期（sx:validityTimePeriodic）。

5.4 现有DRM系统——电子书DRM

- Microsoft ：Digital Asset Server
  - 微软电子图书技术的DRM模型是一种非常紧密的集成， 不仅包括Digital Asset Server（简称DAS）和Microsoft Reader，而且包括微软的Passport用户标识和注册系统。
  - DAS可被服务提供者或电子图书零售商部署。
- Adobe：Adobe Content Server（ACS ）
  - 是一种保障eBook销售安全的易用集成系统。
  - 出版商可以利用Content Server的打包服务功能对可移 植文档格式（PDF）的电子书进行权限设置（打印次数、 阅读时限等），从而建立数字版权管理。

5.4 现有DRM系统——电子书DRM

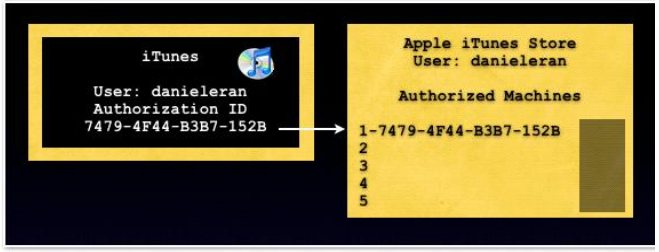
- 书生商业机密保护系统（SDP）
  - SDP是书生公司最新研制的文档管理应用系统，该产品 基于书生独有的国际领先的TESDI-DRM技术研制而成，同时支持在线式与离线式DRM应用模型，通过三重安全体系的保障，可严格防止电子文件被非法使用和非法扩散，即使对有权阅读的人也能够控制其复制、打印、摘录、传播等权限，从而可以在充分保证文档安全性的前提下提供最大程度的文档共享功能。
  - 书生商业机密保护系统攻克了防止有权接触信息的人扩 散该信息的世界级难题，提供了多达14种细粒度的管理 权限，是目前世界上最专业、最完善、最先进的文档管 理软件之一。

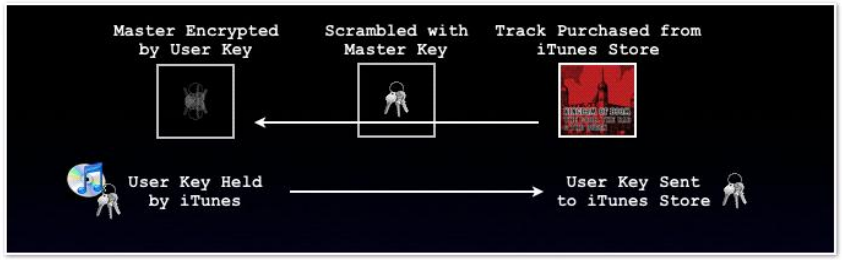
5.4 现有DRM系统——电子书DRM

- 方正：Apabi Right Server
  - Apabi Maker：将多种格式电子文档转化成eBook格式
  - Apabi Rights Server：用在出版社端服务器；
  - Apabi Retail Server：用在书店端服务器；
  - Apabi Reader：用来阅读电子图书，可以在网上买书， 读书，下载，建立自己的电子图书馆，实现分类管理。

5.4 现有DRM系统——多媒体DRM

- Apple：FairPlay
  - iTunes是迄今为止最成功的网上付费音乐下载项目，之前由苹果公司的“FairPlay”数字版权管理技术保护
  - 考虑到制作公司和电影工作室对他们的知识产权将被违法复制和销售的担心，FairPlay是苹果公司使用的数字产权管理(DRM)系统，用来加密iTunes上受产权保护的媒体文件
  - 在FairPlay下加密的媒体可以被同时传输到无限量的iPod上或者在五台授权计算机上
  - FairPlay的音轨也可以被刻录到一个音频CD达七次



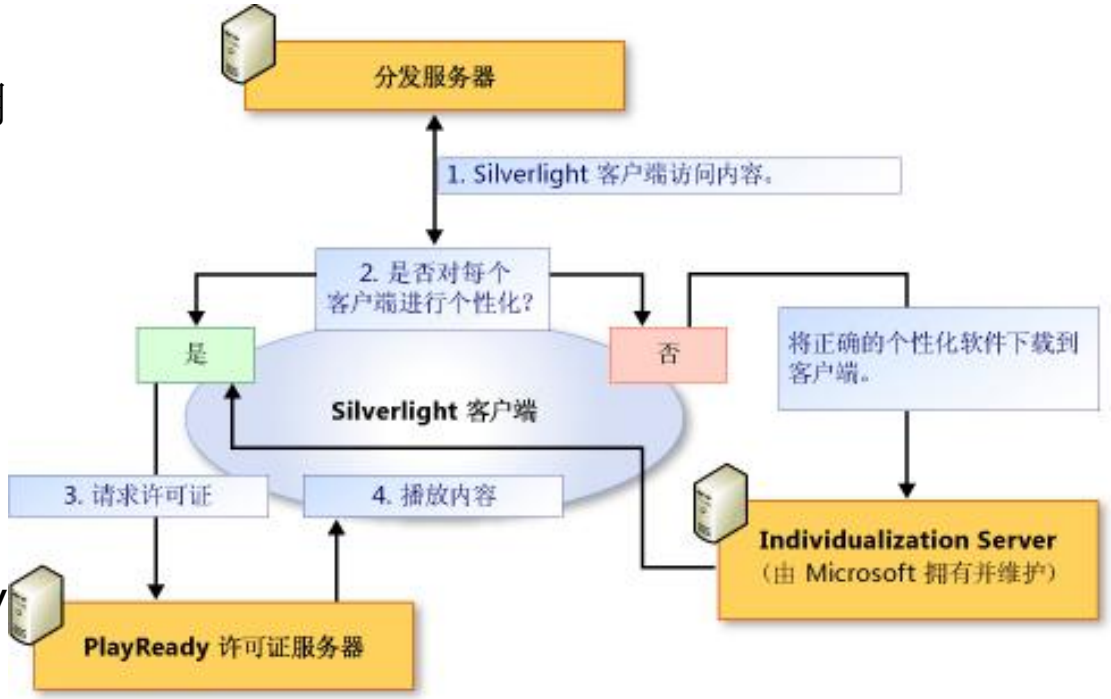


5.4 现有DRM系统——多媒体DRM

- Microsoft Windows Media DRM
  - 当消费者从网站下载到经过加密以后的媒体文件后，他 同时需要获取一个包含解密密钥的许可证来播放这个媒 体文件。
  - 内容的所有者可以方便地通过该系统来管理这些许可证 和密钥的分发
  - 网上的音乐零售网站可以在消费者购买音乐前提供对音 乐的预览。消费者在网站注册以后可以下载到完整的音 乐并且可以在电脑上播放两次。而当消费者第三次播放 该文件的时候，就会被引导到网站的销售页面，在这里 他可以付费进行音乐播放许可证的购买。

5.4 现有DRM系统——Silverlight

- Silverlight DRM
  - 微软Silverlight是一个跨浏览器、跨客户平台的技术，能够设计、开发和发布有多媒体体验与富交互应用的网络交互程序，能够开发出具有专业图形、音频和视频的Web应用程序，增强了用户体验。
  - PlayReady 增强了以Silverlight DRM来保护H.264 媒体的内容，脱机DRM可让具备PlayReady技术的现有Silver-light DRM 脱机工作。受保护的内容可以透过持续性的授权来提供，如此使用者可以立即脱机，并开始享用其内容



5.4 现有DRM系统——Silverlight

- Silverlight使用DRM过程
  - 1.Silverlight 客户端访问内容
    - 最终用户尝试在Silverlight 应用程序中播放某些存储在分发服务器上的受DRM保护的内容，Silverlight 客户端下载内容和标头
  - 2.对每个客户端进行个性化处理
    - 在Silverlight 请求许可证来解密内容之前，Silverlight 必须先确定最终用户的计算机上是否安装了适当的DRM 软件。这种软件称为个性化组件，是播放受保护内容所需的DRM 客户端组件。个性化组件软件使客户端计算机可以请求和使用DRM 许可证，并保护在解密过程中用到的敏感数据
    - 如果客户端上还没有适当的个性化组件软件，客户端将向Microsoft Individualization Service 请求该组件。获取个性化的组件软件的过程称为“个性化”
  - 3.Silverlight 请求许可证
    - 一旦客户端上存在有效的个性化组件软件，就可开始播放DRM了。在访问带有DRM 内容的页面时，Silverlight 客户端将联系PlayReady许可证服务器以获取许可证。如果许可证服务器批准该请求，则颁发许可证，客户端将使用该许可证来解密特定的媒体文件，之后，就可以播放内容了

5.4 现有DRM系统——广播电视内容保护

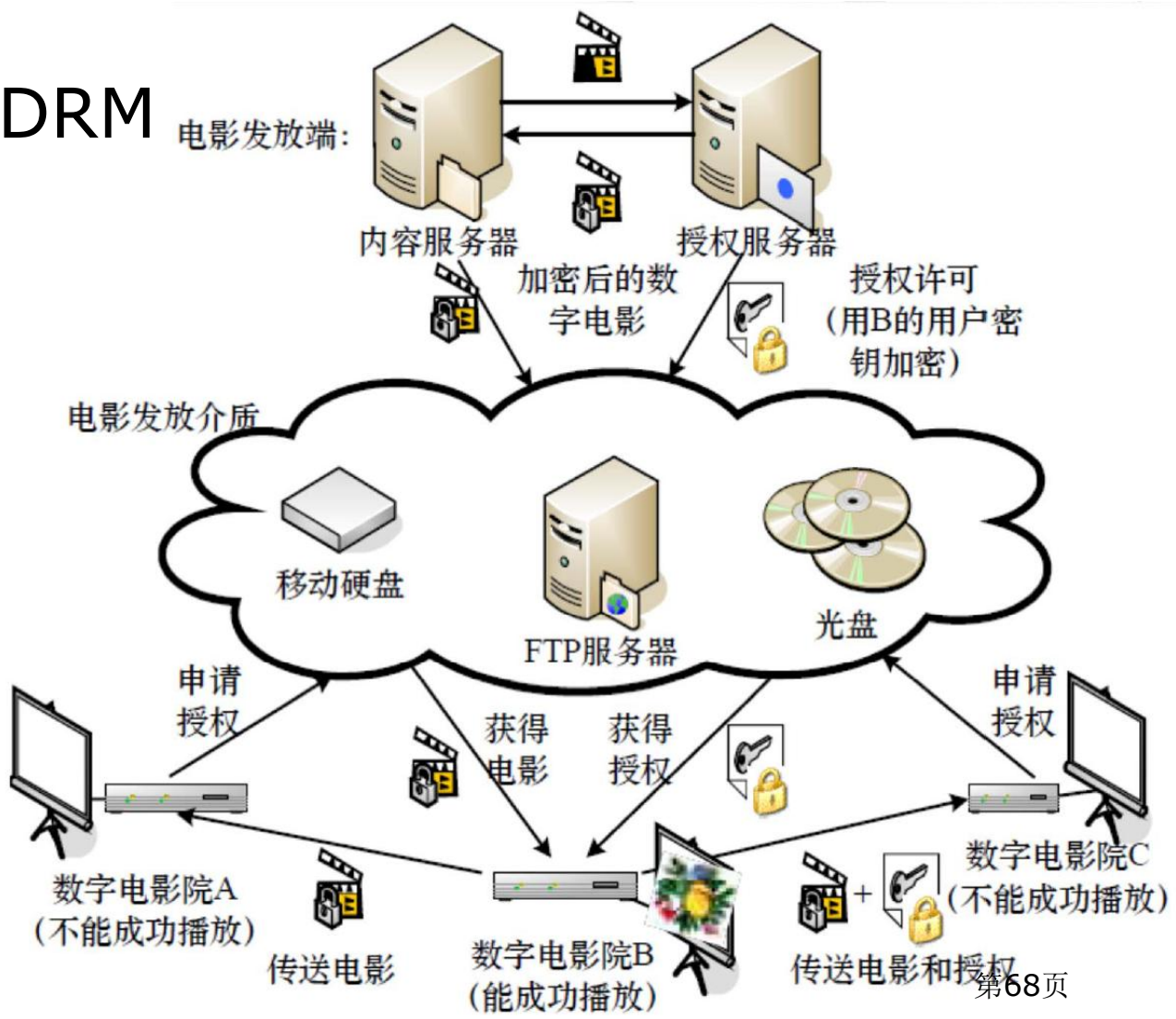
- 在广播及数字电视系统中，DRM技术主要用于数字内 容的制作管理和传输使用的各个环节上，其应用前景十分广阔。
- 国际上的相关标准包括HDCP（高带宽数字内容保护）、DTCP（数字传输内容保护）、CPRM（可录制媒体内容保护）、SDMI（安全数字音乐促进）以及CAs（条件接收系统）等。
- 我国数字电视产业联盟制订了UCPS（统一内容保护系统）标准，长虹、康佳、海信、西安电子科技大学等十几家生产单位、科研机构和高校于2004年联合成立了UCPS论坛以适应市场对数字音视频设备的商业化需求。

5.4 现有DRM系统——数字电影院

- 影院必须提供持久、安全的环境
  - 保护内容、数据的安全，并支持鉴证过程
  - 根据分销协议，依据商业规则解密和播放特定影片
  - 防止未被授权的进入、复制、编辑、或者特影片的播放
  - 提供有关安全的事件的记录
- 授权分离机制
  - 将加密后的数字电影与密钥、用户的权限和使用条件相分离的授权许可分发机制
  - 一部数字电影只被加密一次，通过电影发放介质发放给用户
  - 将解密数字电影的密钥和该用户的权限、使用条件合在一起，用版权描述语言(Right Expression Language, REL)描述后生成授权许可，对用户授权

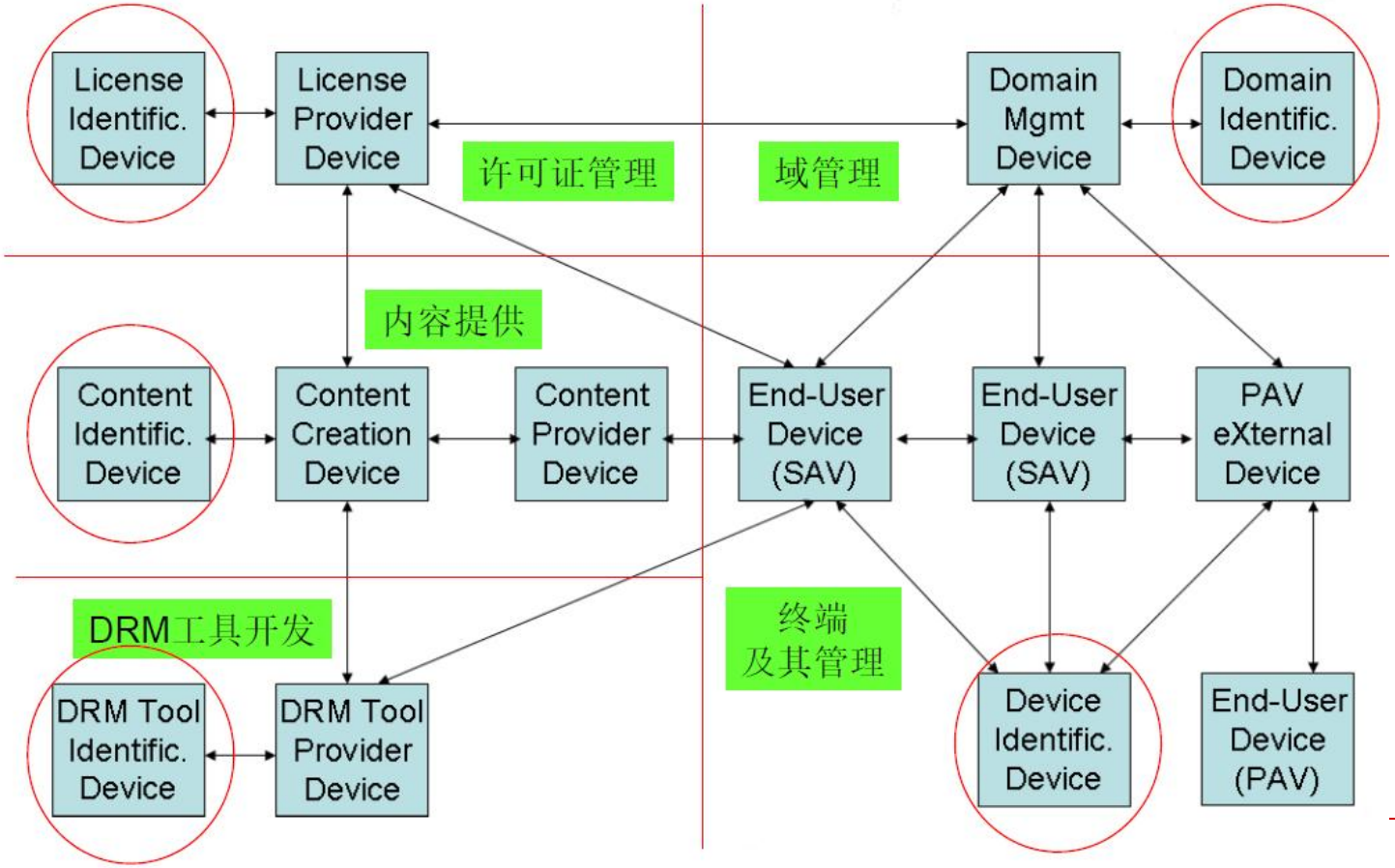
5.4 现有DRM系统——数字电影院

- 数字电影院DRM



5.4 现有DRM系统

- DRM产业链的主要角色



5.5 数字版权保护新趋势

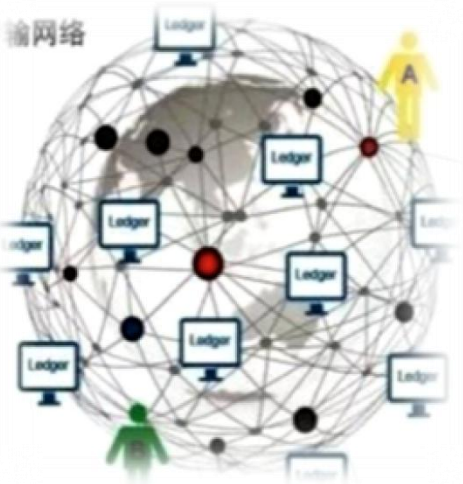
- DRM的现状
  - DRM系统能够做到
    - 对一般人来说，复制权利信息不可能，对专家来说也变得困难
    - 利用数字水印技术和指纹技术去识别内容和某些元数据
    - 整合元数据表和REL，它能管理内容入口
    - 在部分或全文中禁用播放和显式设备
  - DRM系统不能做到
    - 对于任意长的时间里阻止复制和文件共享
    - 混合公平利用
    - 完全准确复制法律合同条款
    - 彼此互动
    - 在本地网络工作
    - 确保艺术家（或任意另外供应链方）得到他们应得的专利版权

5.5 数字版权保护新技术

分类	技术方案	作用阶段	内容
第一类	区块链技术	版权传播前	基于区块链技术的不可篡改、防伪追溯等特性，实现版权存证、登记、溯源、侵权证据固化、透明化交易等功能，达到版权保护目的
	可信时间戳(DTS)	版权传播前	中国科学院国家授时中心联合信任时间戳服务中心签发的用于证明电子数据（电子文件）在一个时间点是已经存在的、完整的、可验证的，具备法律效力的电子凭证
	DCI保护体系	版权传播前	中国版权保护中心提出。主要逻辑是给数字作品版权赋予唯一的身份标示，即DCI 码。通过该DCI 码的查询和验证，即可证明版权归属，并能进行版权的网上监测、取证、维权等工作，达到版权保护的目的
	数字水印	版权传播前	将版权信息、标识信息、图像等信息以可见或者不可见的方式嵌入进视频、音频、图片、文本等载体图像之中，用于证明作品的来源，作为侵权起诉的证据；此外，通过对数字作品的水印进行检测、分析，实现对作品的完整性保护
第二类	数字版权管理DRM	版权传播中	数字版权管理系统颁发数字许可证，对数字内容在分发、传输和使用等各个环节进行控制，将版权控制版权的流转和使用限定在信息系统内。使得数字内容作品只能被授权用户,按照授权方式,在授权期限和范围内使用
第三类	数字DNA技术	版权传播后	通过大数据爬虫和图像检索技术发现疑似侵权作品，并与原创的、已经存证的数字内容作品DNA（数字特征或指纹）进行对比，如果数字特征信息的相似度超过阈值，则认为侵权

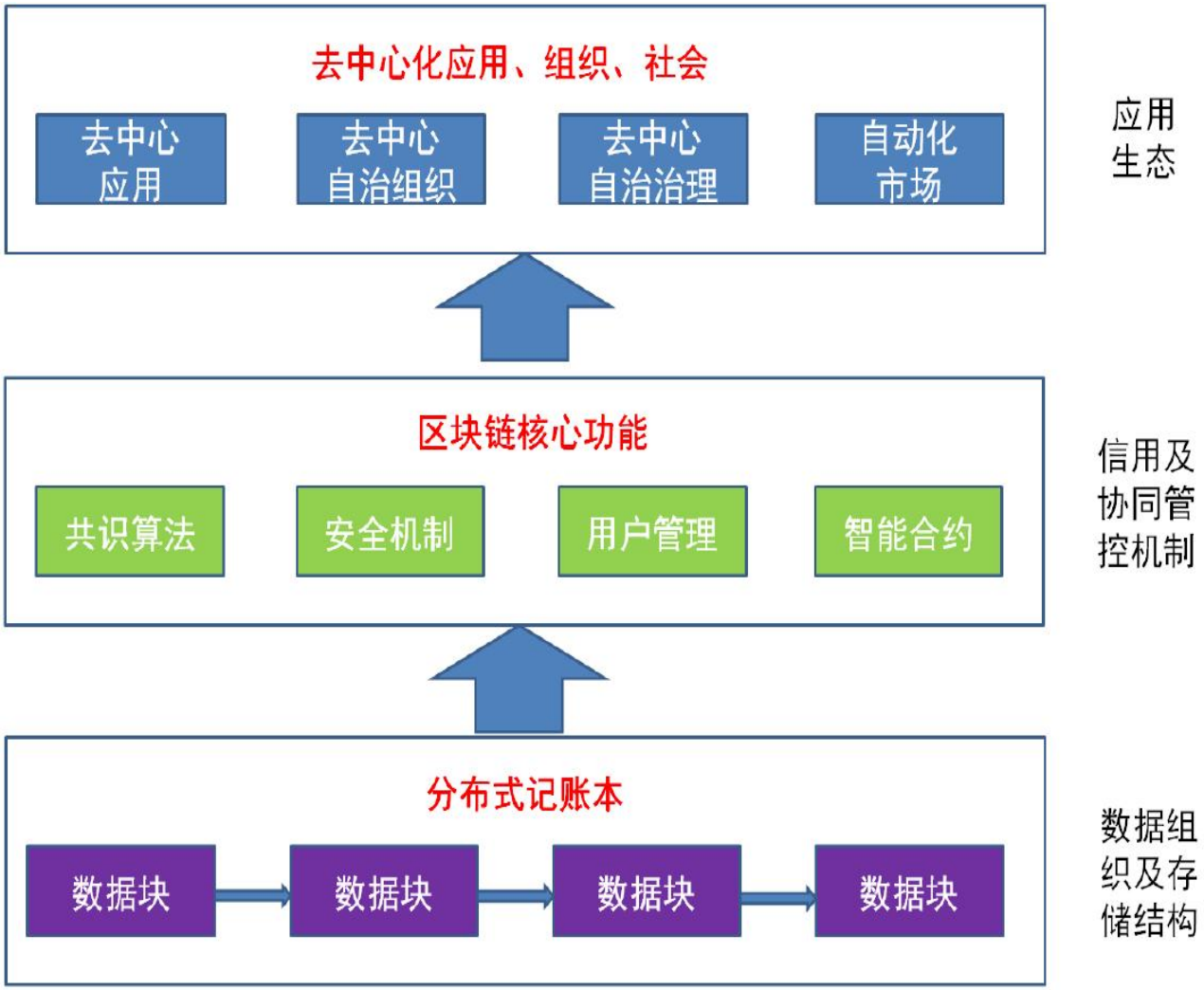
5.5 数字版权保护新趋势

- 数字版权行业存在的问题
  - 1.版权确权难
  - 2.侵犯监控难
  - 3.维权取证难
  - 4.版税结算难
- 引入区块链，为数字版权保护带来新机遇
  - 1.数据确权明确数据权益归属
  - 2.数据不可篡改、防伪和溯源
  - 3.智能合约保障交易安全公平
- 区块链(Blockchain)是一个分布式账本，一种通过去中心化、去信任的方式集体维护一个可靠数据库的技术方案
  - 核心是共识算法，建立去中心化的全球信用，也解决了价值传递的低成本和高效率问题



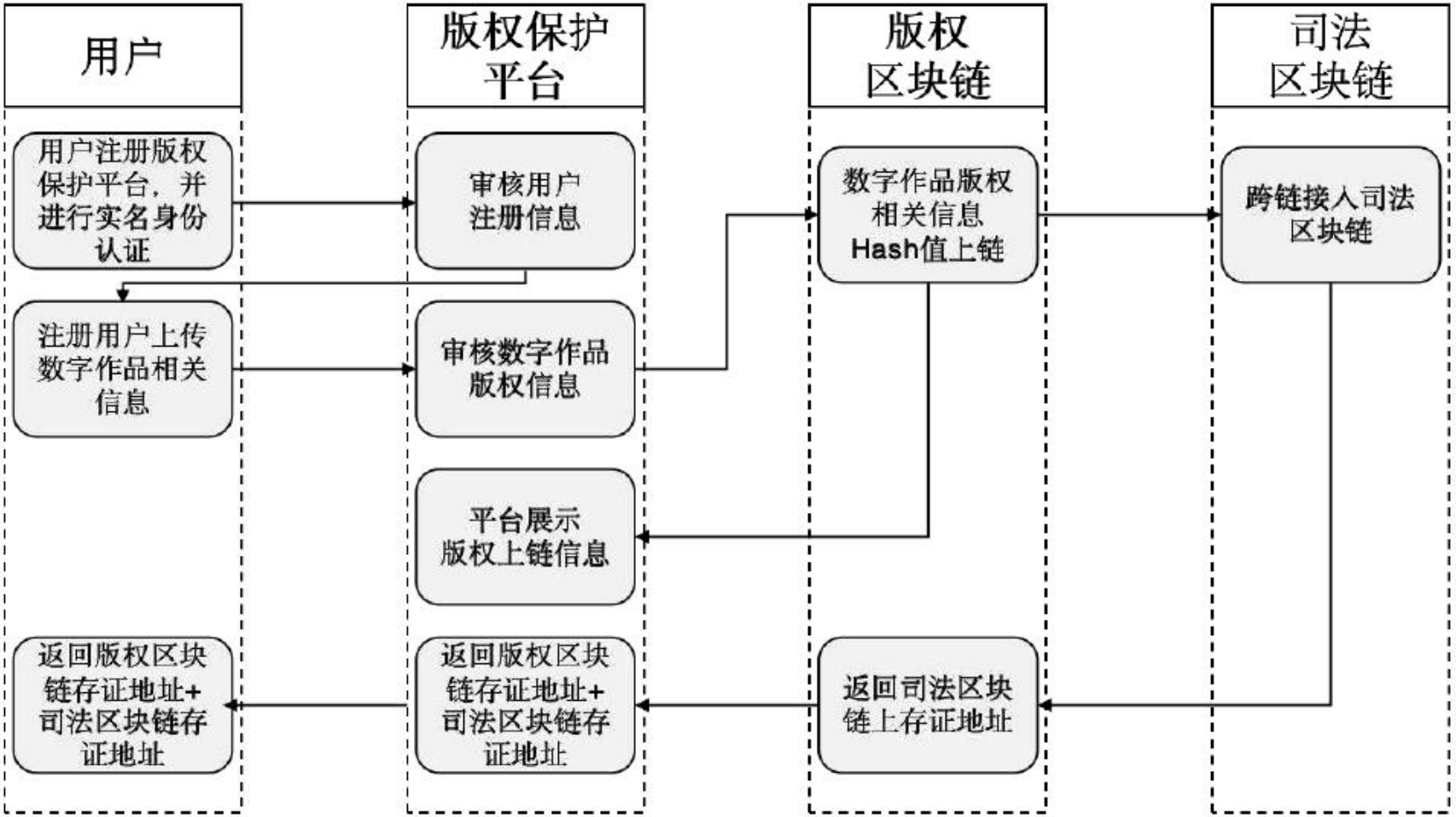
5.5 数字版权保护新趋势

- 区块链技术特点
- 分布式账本－系统中每个节点都能获得一份完整“账本”的拷贝
- 密码算法—可信真实的记录每笔交易
- 共识机制－POW等算法使得参与记账过程的去中心化信任
- 智能合约—实现交易的公平性



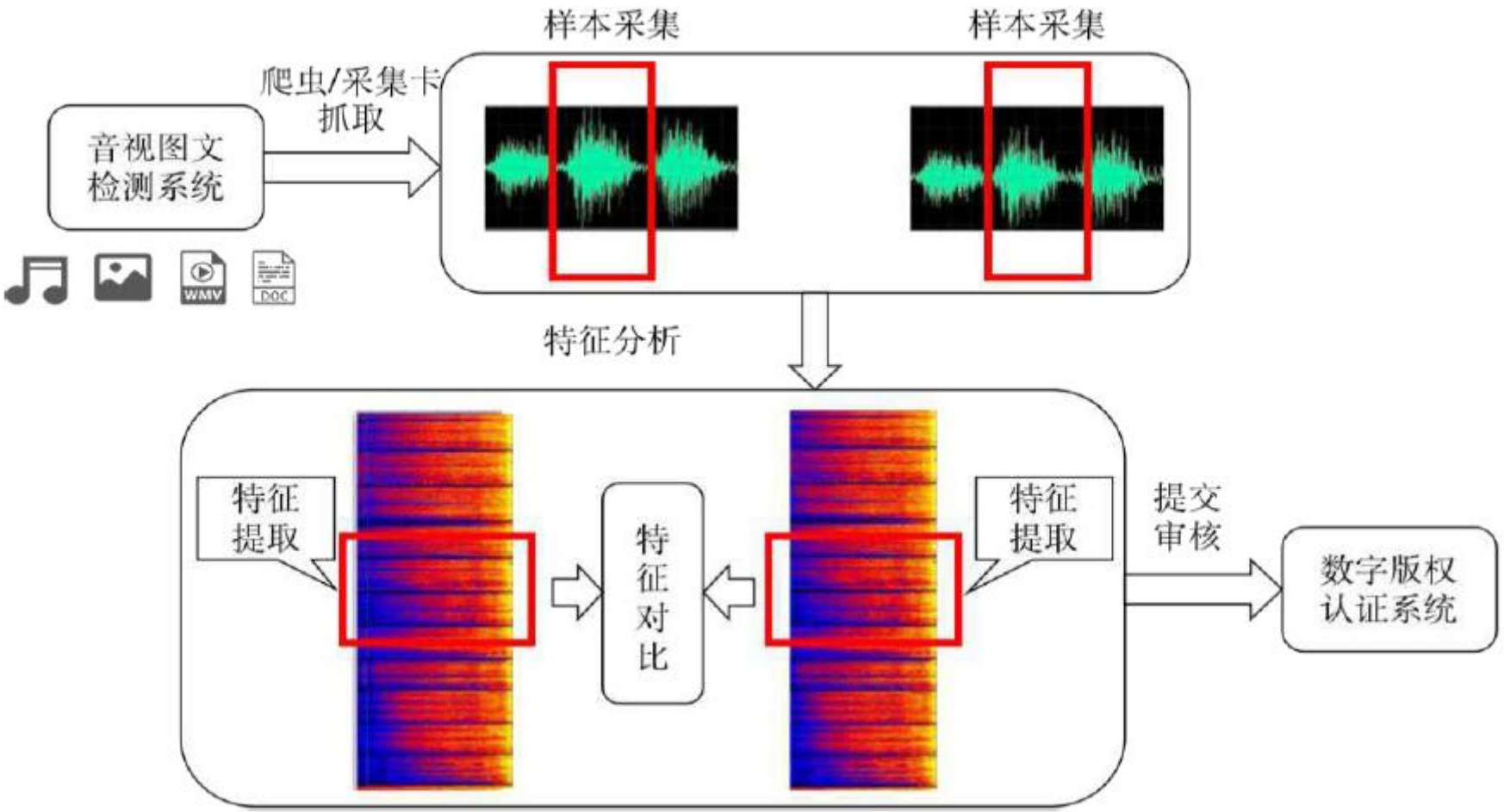
5.5 数字版权保护新趋势

- 基于区块链的版权存证



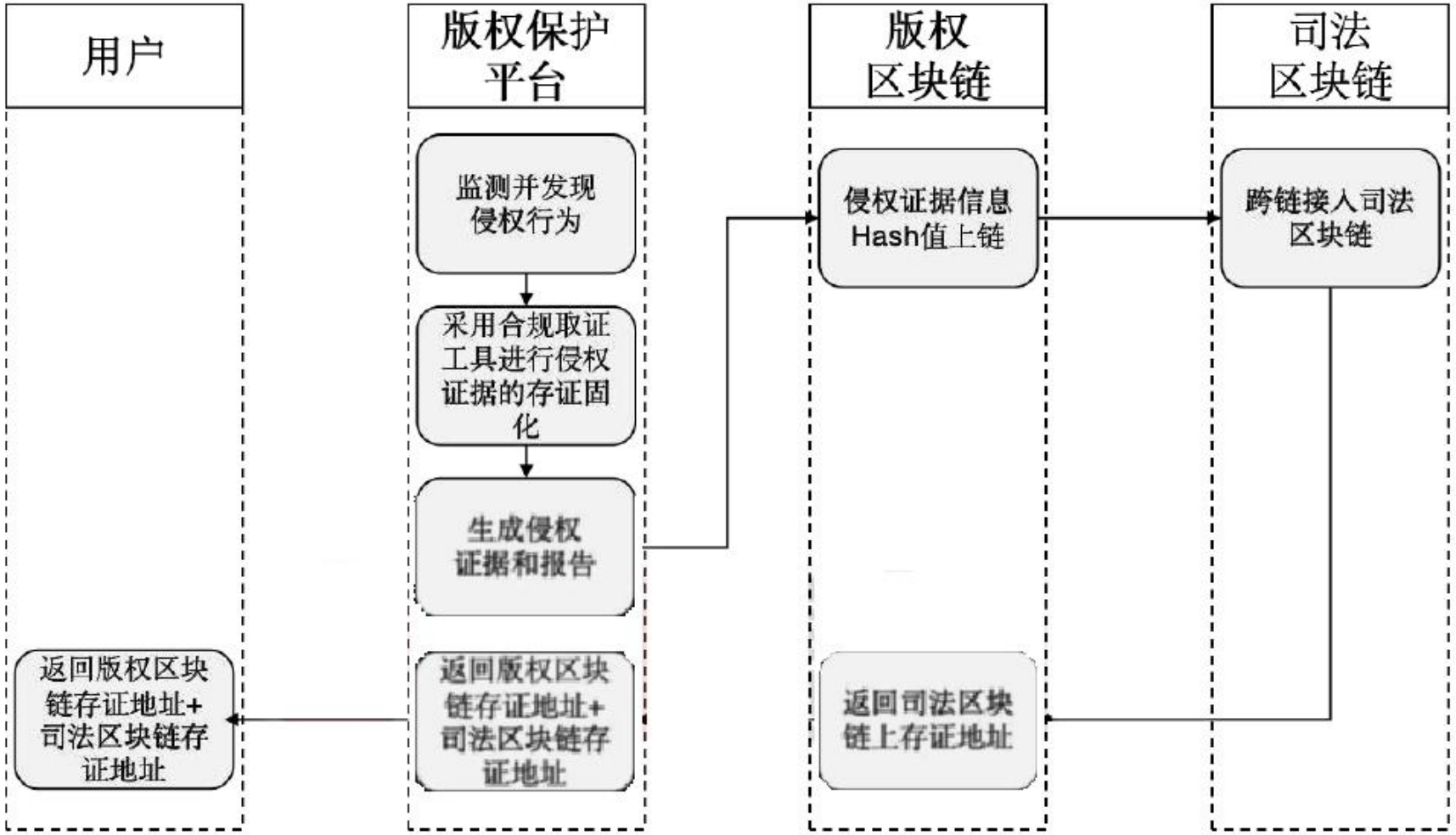
5.5 数字版权保护新趋势

- 侵权监测预警



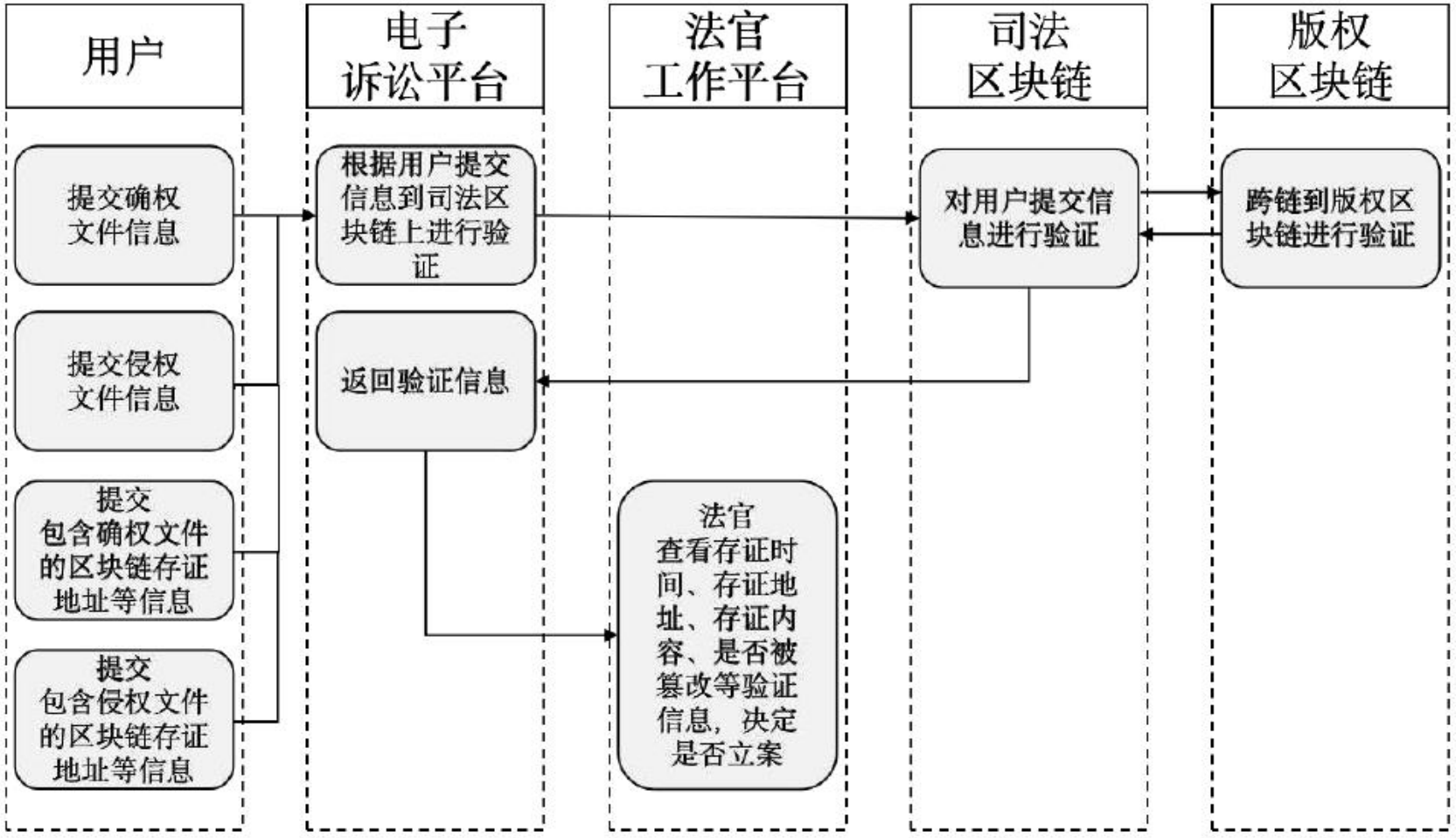
5.5 数字版权保护新趋势

- 侵权取证



5.5 数字版权保护新趋势

- 司法维权

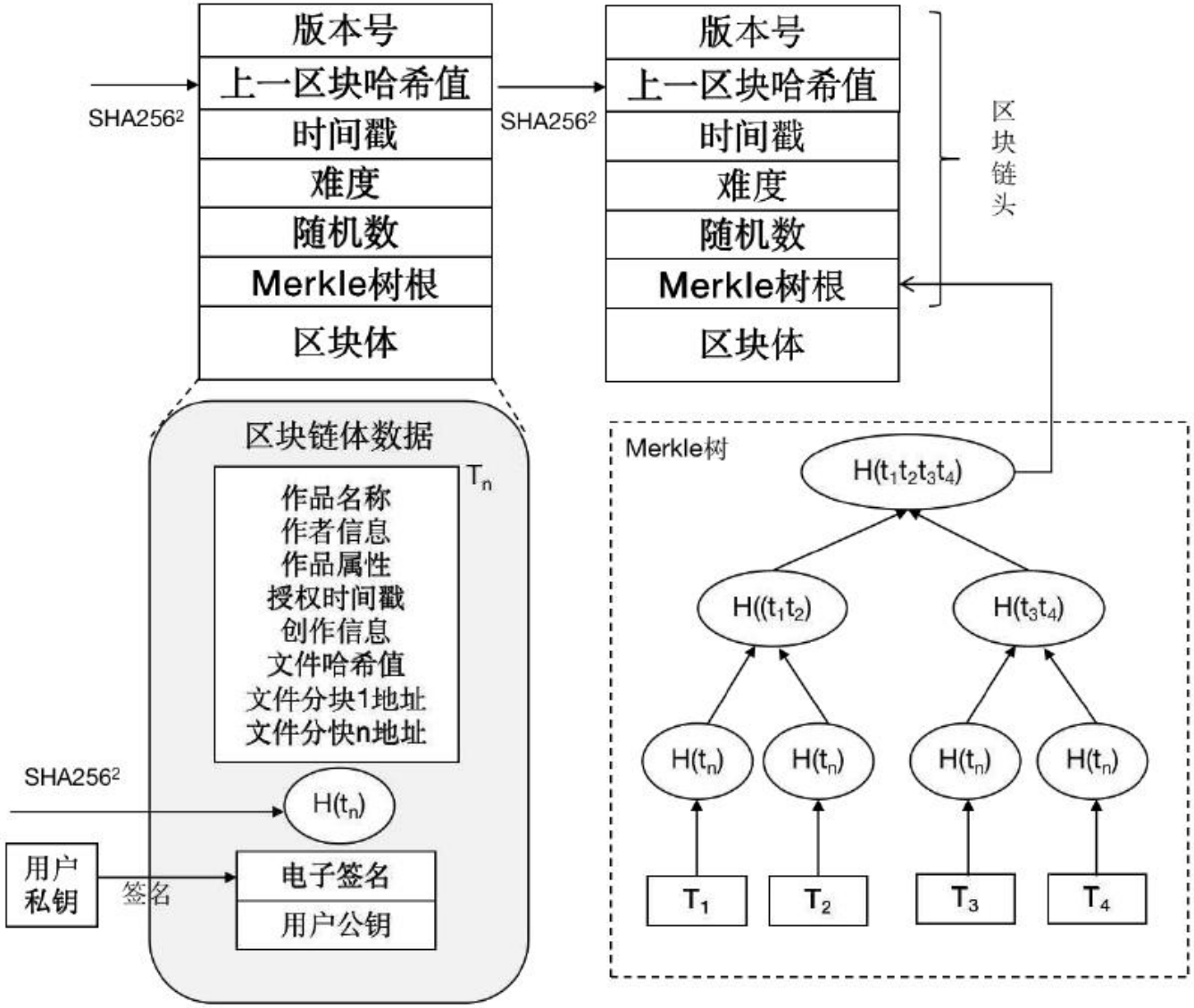


5.5 数字版权保护新趋势

- 通用的区块链数字版权平台技术整体架构

5.5 数字版权保护新趋势

- 数据上链与数据存储



5.5 数字版权保护新趋势

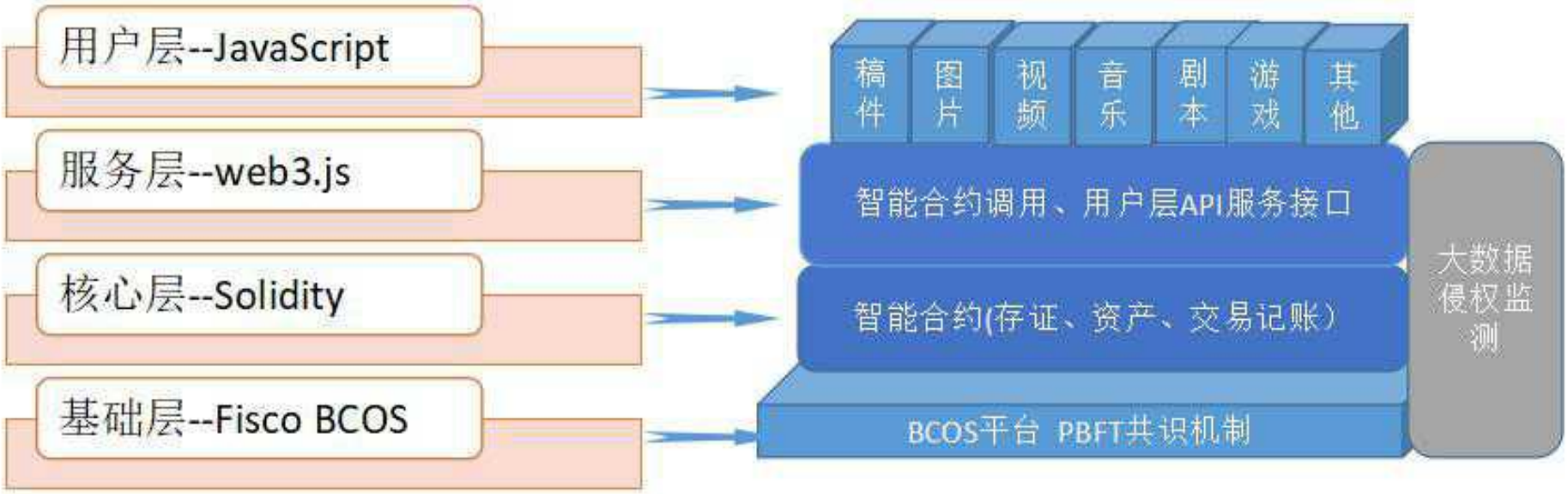
- 智能合约：
  - 可以实现没有第三方的情况下可信交易，有助于数字版权价值安全流转。在区块链数字版权交易系统中，业界尝试将智能合约设计成三类模式：内容预购模式、零售模式和分销商模式。
- 数字内容检索：
  - 数字版权侵权监测环节的重要技术。通过对数字内容特征提取，并进行相似度匹配，可以识别和检测数字内容是否被盗版侵权。数字内容检索的基本步骤主要包括特征提取、指纹生成和相似度匹配。
- 数字水印：
  - 通过在数字作品中嵌入具有唯一性的标识本水印，无论数字作品被传播至微博、微信等各类新媒体平台，都可通过该水印进行识别和追溯，一旦数字版权侵权监测平台发现侵权行为，便会立即取证存证。此外，从数字作品被创作、流转、消费全生命周期中，数字作品版权的每一次授权、转让，都能够被记录和追踪，不仅能优
- 隐私保护
  - 使用多重签名，可以将一段信息或数据用多个私钥签名，表示该项信息由多人共同背书、管理和支配。

5.5 数字版权保护新趋势

- 案例1：百度超级链版权解决方案

5.5 数字版权保护新趋势

- 案例2：版权家区块链版权保护解决方案



5.5 数字版权保护新趋势

- 区块链版权保护的挑战与趋势

区块链数字版权应用面临的挑战

- （一）行业跨界牵涉多部门，资源整合难度较大
- （二）区块链平台尚未互联互通，导致存在信息壁垒
- （三）区块链版权服务同质化，盈利模式较为单一
- （四）侵权手段方式渠道不断变化，版权保护技术面临挑战

区块链数字版权应用发展趋势

- （一）基于区块链的数字版权交易有望迎来更大发展空间
- （二）AI 大数据等技术将推动区块链数字版权服务得到快速发展
- （三）区块链数字版权激发优质内容产出，版权付费氛围有望形成

本章内容总结

5.1数字版权管理DRM概述

针对问题：随意分发、限定硬件、多设备共享(互操作)、域共享；**数字版权管理/数字版权保护概念（三大目标）**、DRM分类、DRM五大功能（权限控制、版权认证、盗版追踪、内容认证、操作跟踪）、**工作原理（内容服务器、许可证服务器、客户端三方架构）**

5.2权限控制模型

传统访问控制的缺陷、**UCON/ABC模型**、主体、客体、**权限**、**授权**、**义务**、**条件**、ABC模型矩阵

5.3权利描述语言

ODRL、XrML

5.4现有DRM系统

电子书DRM、多媒体DRM、广播电视DRM、数字电影DRM

5.5数字版权保护新趋势

区块链、可信时间戳、DCI保护体系、数字水印、DRM、数字DNA