(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109804374 A
(43)申请公布日 2019.05.24

(21)申请号 201780062404.5

(22)申请日 2017.08.15

(30)优先权数据
62/410,557 2016.10.20 US
15/458,807 2017.03.14 US

(85)PCT国际申请进入国家阶段日
2019.04.09

(86)PCT国际申请的申请数据
PCT/US2017/046906 2017.08.15

(87)PCT国际申请的公布数据
WO2018/075129 EN 2018.04.26

(71)申请人 索尼公司
地址 日本东京都
申请人 索尼图片娱乐公司

(72)发明人 E·迪赫尔

(74)专利代理机构 中国国际贸易促进委员会专利商标事务所 11038
代理人 郑宗玉

(51)Int.Cl.
G06F 21/10(2006.01)

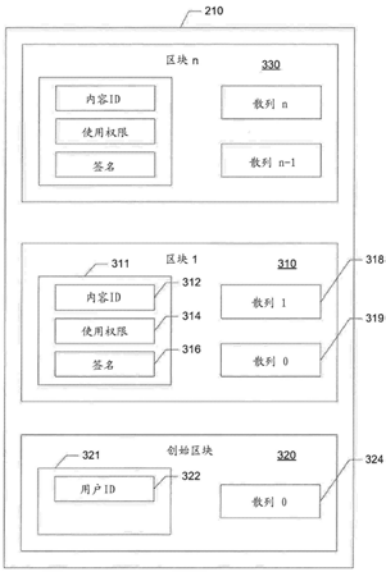
权利要求书1页 说明书7页 附图9页

(54)发明名称

基于区块链的数字权限管理

(57)摘要

生成存储用户的权限的权限区块链，包括：从用户接收登记请求和公钥；验证用户具有与公钥对应的私钥；使用公钥生成用户标识符；以及生成并向用户传递具有包括用户标识符的创始区块的权限区块链。



CN 109804374 A

1.一种用于生成存储用户的权限的权限区块链的方法,所述方法包括:

从用户接收登记请求和公钥;

验证用户具有与公钥对应的私钥;

使用公钥生成用户标识符;以及

生成并向用户传递具有包括用户标识符的创始区块的权限区块链。

2.如权限要求1所述的方法,还包括

在公钥已经被注册时,请求不同的公钥。

3.如权限要求1所述的方法,还包括

更新包括具有内容的内容标识符和相关联的使用权限的新区块的权限区块链。

4.如权限要求3所述的方法,还包括

从内容提供者接收用户已获取具有内容标识符的内容的信息。

5.如权限要求3所述的方法,其中所述相关联的使用权限包括

被许可的语言和字幕语言的列表。

6.一种用于生成存储用户的权限的权限区块链的系统,所述系统包括:

注册机构,被配置为从用户接收登记请求和公钥,所述注册机构还被配置为验证用户具有与所述公钥对应的私钥、使用所述公钥生成用户标识符,以及生成并向用户传递具有包括用户标识符的创始区块的权限区块链。

7.如权限要求6所述的系统,还包括

内容提供者,被配置为向注册机构通知用户已经获取内容。

8.如权限要求7所述的系统,其中所述注册机构还被配置为接收具有内容的内容标识符和相关联的使用权限的新区块并利用该区块来更新权限区块链。

9.如权限要求8所述的系统,其中所述内容提供者还被配置为对与更新后的权限区块链中的内容标识符对应的内容进行加扰,并生成内容的加扰版本。

10.一种使用存储用户的权限的权限区块链进行数字权限管理的方法,所述方法包括:

接收包括内容标识符、加扰的实质和加密的控制字的受保护内容;

接收权限区块链和用户的凭证;

在权限区块链中搜索包含受保护内容的内容标识符的第一区块;

当第一区块中的签名和使用权限被确定为有效时,对加密的控制字进行解密;以及

使用解密的控制字解扰加扰的实质。

11.如权限要求10所述的方法,还包括:

执行权限区块链的完整性检查以确定权限区块链尚未被破坏或篡改。

12.如权限要求10所述的方法,其中所述权限区块链包括具有用户的用户标识符的创始区块。

13.如权限要求10所述的方法,还包括

确定第一区块的签名和使用权限是否有效。

14.一种用于生成存储用户的权限的权限区块链以消费内容项的方法,所述方法包括:

从用户接收登记请求和公钥,并验证用户具有与所述公钥对应的私钥;

使用所述公钥生成包括用户的用户标识符的创始区块;以及

生成并添加具有内容项的内容标识符和相关联的使用权限的新区块。

基于区块链的数字权限管理

[0001] 对相关申请的交叉引用

[0002] 本申请依据35 U.S.C.§119(e)要求于2016年10月20日提交的标题为“Blockchain-Based DRM”未决定的美国临时专利申请No.62/410,557的优先权。以上引用的申请的公开内容通过引用并入本文。

技术领域

[0003] 本公开涉及数字权限管理(DRM),更具体而言,涉及使用区块链来实现DRM。

背景技术

[0004] 为了相互操作性,许多当前DRM解决方案通常需要由供应商或一组供应商管理的权限柜(locker)或其它公共存储装置。但是,这些常规的解决方案可能不是非常可靠并且取决于一个唯一的故障点。如果权限柜提供者或系统停止运营或以其它方式倒闭,则用户丢失所有获取的内容。

[0005] 当今的许多可相互操作的解决方案是基于共同的体系架构的,该体系架构将一条内容的使用权限存储到专用于一个用户和一个特定平台的许可中。例如,权限柜和管理的一个常见解决方案是UltraViolet™。

发明内容

[0006] 本公开提供了使用权限区块链来实现可相互操作的数字权限管理(DRM)。

[0007] 在一个实现中,公开了一种用于生成存储用户的权限的权限区块链的方法。该方法包括:从用户接收登记请求和公钥;验证用户具有与公钥对应的私钥;使用公钥生成用户标识符;以及生成并向用户传递具有包括用户标识符的创始(genesis)区块的权限区块链。

[0008] 在另一个实现中,公开了一种用于生成存储用户的权限的权限区块链的系统。该系统包括:注册机构,被配置为从用户接收登记请求和公钥,该注册机构还被配置为验证用户具有与公钥对应的私钥、使用公钥生成用户标识符,以及生成并向用户传递具有包括用户标识符的创始区块的权限区块链。

[0009] 在又一个实现中,公开了一种使用存储用户的权限的权限区块链来执行数字权限管理的方法。该方法包括:接收包括内容标识符、加扰的实质(essence)和加密的控制字的受保护内容;接收权限区块链和用户的凭证;在权限区块链中搜索包含受保护内容的内容标识符的第一区块;当第一区块中的签名和使用权限被确定为有效时,对加密的控制字进行解密;以及使用解密的控制字解扰加扰的实质。

[0010] 在还有的实现中,公开了一种用于生成存储用户的权限以消费内容项的权限区块链的方法。该方法包括:从用户接收登记请求和公钥并验证用户具有与公钥对应的私钥;使用公钥生成包括用户的用户标识符的创始区块;以及生成并添加具有内容项的内容标识符和相关联的使用权限的新区块。

[0011] 根据本描述,其它特征和优点应该是显而易见的,本描述通过示例的方式图示了

本公开的各方面。

附图说明

[0012] 本公开关于其结构和操作的细节可以通过研究附图来部分地收集,附图中类似的附图标记表示类似的部分,并且其中:

[0013] 图1是包括n个区块和创始区块的区块链的框图;

[0014] 图2是使用区块链的新DRM系统的一个实现中的组件和交互的框图;

[0015] 图3是权限区块链(RBC)的一个实现的框图;

[0016] 图4是受保护内容的一个实现的框图;

[0017] 图5是图示根据本公开的一个实现的使用区块链的数字权限管理操作的流程图;

[0018] 图6是图示根据本公开的一个实现的用于生成RBC的处理的流程图;

[0019] 图7是图示根据本公开的一个实现的用于获取给定内容并向RBC添加使用权限的处理的流程图;

[0020] 图8是图示根据本公开的一个实现的用于在内容提供者处打包内容的处理的流程图;以及

[0021] 图9是图示根据本公开的一个实现的用于消费内容的处理的流程图。

具体实施方式

[0022] 如上所述,许多当前的数字权限管理解决方案通常需要权限柜或其它公共存储装置,这取决于一个唯一的故障点。例如,如果权限柜提供者或系统停止运营或以其它方式倒闭,则用户丢失所有获取的内容。常规的解决方案将一条内容的使用权限存储到专用于一个用户和一个特定平台的许可中。

[0023] 本公开的某些实现提供了替代解决方案,该解决方案移除权限柜并提供了使用区块链的持久的可相互操作性的角度。在阅读这些描述之后,将明白如何在各种实现和应用中实现本公开。但是,虽然本文将描述本公开的各种实现,应该理解的是,这些实现仅以示例的方式呈现而非限制。由此,各种实现的详细描述不应该被解释为限制本公开的范围或广度。

[0024] 区块链数据结构是区块的有序列表。每个区块都安全地指向其前一个区块,直到区块链中的通常被称为“创始”区块的第一个区块。通过反向链接加密散列来保护区块及其序列的完整性。

[0025] 在一个实现中,执行软件应用和操作系统的若干计算机系统进行交互以管理对内容(诸如作为数据存储的视频内容)的访问。计算机系统使用权限区块链来管理访问。权限区块链包括存储用户的信息和内容项的数据的区块的有序序列。最开始,权限区块链包括存储用户信息的单个区块,即所谓的创始区块。当获取对内容项的使用权限时,将区块添加到权限区块链,其中每个新区块指示对一个或多个内容项的使用权限,并且包括对权限区块链中的前一个区块的引用。

[0026] 在一个示例中,用户已经向注册计算机系统注册了用户信息,并且注册系统已经向用户计算机系统提供了表示权限区块链的创始区块的数据。当用户从内容提供者或某个其它实体获取对内容项的权限时,用户系统将用户的权限区块链提供给内容提供者计算机

系统，并且内容提供者系统和注册系统更新用户的权限区块链以反映新权限，从而为添加针对新内容的新区块。内容提供者系统返回更新的权限区块链和表示内容项的对应的加密内容数据，并且用户系统存储接收到的数据。当用户获取附加的使用权限时，内容提供者系统和注册系统再次更新用户的权限区块链，从而添加针对新内容的新的区块。

[0027] 当用户想要访问内容数据时，用户系统将内容数据和权限区块链提供给DRM计算机系统。DRM系统验证权限区块链并确认该访问在权限区块链中的对应区块内授予的使用权限内。一旦经过验证和确认，DRM系统就解密或促进解密加密的内容数据，并且用户系统可以访问解密的内容。

[0028] 图1是包括n个区块110、120、130和创始区块140的区块链100的框图。在一个实现中，区块具有至少三个元素：存储注册数据和辅助数据的信息部分(例如，112)；前一个区块(创始区块不具有前一个区块)的加密散列(例如，114)；以及当前区块的加密散列(例如，116)。

[0029] 图2是使用区块链的新DRM系统200的一个实现中的组件和交互的框图。在传统DRM中，针对用户/设备加密的许可包含与一条内容或一组内容相关联的解扰密钥和使用权限。在新系统200中，该许可由RBC 210中保持由用户获取的所有使用权限的区块替代。该区块链210在保密性方面不受保护，而仅在完整性方面受到保护。图3是RBC 210的一种实现的框图。

[0030] 在图2和图3的所示实现中，DRM系统200包括RBC 210、内容提供者220、用户凭证230、注册机构240、受保护内容250和DRM代理260。在其它实现中，图2中所示的所有实体或对象/数据并非都是被需要或被使用的。

[0031] 用户凭证230对于用户是唯一的，并且加密地链接到RBC 210的用户ID(例如，图3的用户ID 322)。注册机构240将新区块添加到用户的RBC 210。内容提供者220将受保护内容250以及相关联的使用权限分发给用户。注册机构240将使用权限添加到用户的RBC 210。受保护内容250包含加扰内容(例如，加扰电影)。DRM代理260处理数字权限管理功能。在一个实现中，DRM代理260在用于消费/观看内容的用户设备中操作。DRM代理260接收受保护内容250和RBC 210。如果用户有权访问内容，则DRM代理260对受保护内容250进行解扰。

[0032] 在一个实现中，计算机系统的每个单元是分开的(例如，内容提供者220、注册机构240和DRM代理260)。在另一个实现中，计算机系统可以共存或被组合(例如，在相同服务器系统上操作的内容提供者220和注册机构240)，或者图中未示出的附加系统可以参与(例如，多个用户系统(诸如移动电话和/或平板电脑)，以及多个内容分发网络系统)。

[0033] 在图3所示的实现中，创始区块320的信息区块321至少保持用户ID 322。用户ID 322可以是匿名的，而RBC 210可能是公开的。用户ID 322不是保密的。创始区块320还包括其信息区块321的散列324。后续区块(例如，区块1(310))还包括当前区块的散列318和前一区块的散列319。

[0034] 后续区块(区块1(310)、…、区块n(330))的信息区块(例如，区块1的311)至少包括内容标识符(ID)(例如，区块1的312)、使用权限(例如，区块1的314)和数字签名(例如，区块1的316)。

[0035] 内容ID 312明确地识别一条内容或作品(work)。作品可以是内容的给定版本，或者它可以是内容本身而与格式无关。内容提供者220控制和定义内容ID 312。使用权限314

定义对于该作品用户已经被授权或获取的权限。格式可以或者是标准化的权限语言(诸如可扩展权限标记语言(XrML)或开放式数字权限语言(ODRL)、智能合约或者是任何专有格式。数字签名316由注册机构240颁发。签名316包含信息区块311。

[0036] 在一个实现中,RBC 210对于由用户ID 322识别的个体是唯一的。在另一个实现中,存在保持给定生态系统的所有用户的使用权限的全局RBC。在那种情况下,区块信息还将包含用户ID 322,并且创始区块320将是不同的(不专用于特定用户ID)。

[0037] 在一个示例实现中,区块链使用以下信息和格式:用户ID 322是当用户登记并创建创始区块320时由注册机构240提供的2048位数;内容ID(110)使用内容的娱乐标识符注册表(EIDR)标识符(参见例如,eidr.org);使用权限(例如,权限314)是列出许可的音频语言列表和许可的字幕列表的数据结构;并且所有散列(例如,散列318、319、324)在base64中进行SHA-512编码的。对于$block_n$,签名(例如,区块1的签名316)是$block_{n-1}$的三个字段内容ID(例如,312)、使用权限(例如,314)和散列(例如,319)的RSA 2048(Rivest、Shamir和Adelmana;公钥密码系统)。注册机构240使用其根签名私钥生成签名。对于创始区块,签名是字段用户ID(例如,322)的RSA 2048。区块的散列(例如,318、314)包含信息区块311和前一个区块的散列(例如,319)。创始区块320的散列324仅包含信息区块321。

[0038] 图4是受保护内容250的一个实现的框图。受保护内容250至少包括内容ID 410、加扰的实质420和加密的控制字(加密的CW)430。内容ID 410识别作品。它与由RBC 210使用的内容ID相同。加扰的实质420是使用控制字(CW)对内容的明文实质(即,没有加扰的明文形式的内容)进行加扰的结果,控制字是由内容提供者220生成的随机数。在一个实现中,加扰算法是CBC模式下的AES 128位。即,加扰的实质=$AES_{(CW)}$(明文实质)。加密的CW 430是用对于DRM代理260已知的密钥(例如,使用秘密密钥、或公钥-私钥对)对CW(用于加扰这个实质)进行加密的结果。

[0039] 在一个实现中,DRM代理260具有用于加密CW的唯一128位DRM_KEY,并且加密使用高级加密标准(AES)。在一个实现中,CW是由随机数生成器生成的128位随机数(nonce)。即,加密的CW=$AES_{(DRM-KEY)}$(CW)。

[0040] 在一个实现中,内容提供者220可以使用若干DRM技术。在那种情况下,每个支持的DRM代理260通过DRM-ID来识别。受保护内容250的数据结构包含DRM-ID和对应的加密的CW 430对的列表。每个加密的CW 430是由对应DRM代理260的秘密DRM-KEY进行加密的CW。

[0041] 图5是图示根据本公开的一个实现的使用区块链的数字权限管理(DRM)操作的流程图500。在一个实现中,DRM操作在图2的DRM代理260内执行。

[0042] 在图5所示的实现中,在方框510处接收受保护内容250。在方框520处,请求并接收用户的凭证230和指向用户的RBC 210的指针。在方框530处,检查接收到的RBC 210的有效性。通过确定每个区块的散列(例如,图3中的区块1的散列318、319)和创始区块的散列(例如,图3中的创始区块的散列324)是否一致来检查RBC 210的有效性。对于每个非创始区块,检验验证计算出的该区块的散列等于散列318,并且计算出的前一个区块的散列等于散列319。对于创始区块,检验验证计算出的该区块的散列等于散列324。

[0043] 然后进行验证接收到的RBC 210实际上属于用户的确定。在一个实现中,在方框540处进行检查以确定RBC 210中的用户ID 322是否对应于接收到的用户凭证230。如果是这种情况,则可以确定在接收到的RBC中列出的所有使用权限(例如,图3中的RBC 210的区

块1中的权限314)与用户相关联。

[0044] 一旦确定接收到的RBC与用户相关联,则在方框550处搜索包含受保护内容的内容ID的RBC中的区块。然后,在方框560处,在对应的搜索到的区块中,检查信息区块的签名和使用权限。如果在方框570处确定使用权限是有效的,则在方框580处用秘密密钥(即DRM_KEY)对加密的CW 430进行解密,并取回明文CW。在方框590处,用明文CW对加扰的实质进行解扰。

[0045] 在图5所示的实现中,区块链DRM操作不使用集中式许可服务器或集中式权限柜。代替权限柜,使用RBC 210和注册机构240的关联。类似地,许可证服务器的角色由定义所需使用权限的RBC 210、保持加密的CW 430的受保护内容250和实施使用权限的DRM代理260之间共享。

[0046] 许多内容提供者可以共享相同的RBC。在一个实现中,用户具有一个RBC,并且每个内容提供者对该用户使用相同的RBC。在另一个实现中,用户可以具有多个RBC,其中一个RBC用于每个内容提供者,或者多个提供者可以共享或使用相同的RBC,或者内容提供者可以使用多个RBC。

[0047] 如果内容提供者220添加或改变其DRM技术,则它只需要利用用于新DRM代理260的新加密的CW 430重新发布受保护内容250的新版本。

[0048] 一个实现被设计为处理通过电子销售(E-sell through,EST)。用户获取观看给定语言(或一组语言)的内容并且具有以特定语言(或一组语言)的潜在字幕的许可权限。许可是永久性的(或至少在合理的年限内)并且独立于所观看的内容实例的质量。在一个这样的实现中,内容提供者220使用一个单个DRM。

[0049] 以下呈现使用RBC与系统交互的用户A的DRM操作的几个示例。

[0050] 为了创建RBC,用户A通过生成RSA 2048密钥对并联系注册机构240来执行用户登记。然后,注册机构240执行以下操作:请求用户A的公钥;验证该公钥是否已经被注册;如果密钥已经被注册,则请求用户A生成不同的密钥对;通过质询响应协议(challenge-response protocol)验证用户A是否具有对应的私钥;利用用户A的公钥创建用户ID 322;创建用于用户A的RBC 210的用户A的创始区块320;以及将创建的创始区块320传递给用户A。

[0051] 图6是图示根据本公开的一个实现的用于生成RBC的处理的流程图600。在图6所示的实现中,在方框610处,在注册机构处从用户接收登记请求。作为响应,在方框620处,注册机构请求来自用户的公钥,并在方框630处验证该公钥是否已经被注册。在方框640处,如果密钥已经被注册,则注册机构请求用户生成不同的密钥对。然后,注册机构在方框650处通过质询响应协议验证用户是否具有对应的私钥、在方框660处利用用户的公钥创建用户ID、在方框670处创建并向用户传递具有RBC的创始区块的权限区块链。

[0052] 为了获取给定内容并添加使用权限,执行以下操作:用户A将RBC提供给内容提供者220;内容提供者220向注册机构240通知用户A获取了内容;用户(或内容提供者220)向RBC 210提供所购买的内容的内容ID(例如,区块1的ID 312),以及相关联的使用权限(例如,区块1的ID 314)(诸如许可的语言和字幕语言的列表);注册机构240检查所提供的RBC的有效性/完整性(即,RBC没有受到损害或篡改);如果RBC 210有效,则注册机构240添加新区块,在新区块中具有所提供的数据和用于新区块和前一区块中的信息的散列(例如,图3

中的区块1的散列318、319)；以及注册机构240将RBC 210返回到内容提供者220，内容提供者220将RBC 210返回给用户A。

[0053] 图7是图示根据本公开的一个实现的用于获取给定内容并向RBC添加使用权限的处理的流程图700。在图7所示的实现中，在方框710处，当用户从内容提供者获取给定内容时，内容提供者在方框720处通知注册机构用户获取了内容。在方框730处，内容提供者向注册机构提供所购买的内容的内容ID和相关联的使用权限(诸如许可的语言和字幕语言的列表)。然后，在方框740处，注册机构检查所提供的RBC的完整性，并且如果RBC有效并且没有被破坏或篡改，则在方框750处添加具有所提供的数据和用于新区块和前一区块中的信息的散列的新区块。在方框760处，注册机构将RBC返回给用户。

[0054] 为了打包内容，在一个实现中，内容提供者220执行以下操作：在EIDR中注册内容的这个版本以接收内容ID(例如，区块1的312)；生成将成为CW的随机128位数字；通过用对应的DRM_KEY加密CW，计算用于每个支持的DRM的对应的加密的CW 430；利用CW加扰明文实质以生成加扰的实质420；以及将所有这些信息打包到受保护内容250中。在一个实现中，加扰使用计数器(CTR)模式下的AES。受保护内容250可以被自由分发，因为它是自我保护的。

[0055] 图8是图示根据本公开的一个实现的用于在内容提供者处打包内容的处理的流程图800。在图8所示的实现中，在方框810处，内容提供者在EIDR中注册内容的当前版本以接收内容ID。然后，在方框820处，内容提供者生成将成为控制字(CW)的随机数，并且在方框830处，通过利用对应的秘密密钥(DRM_KEY)加密CW，计算用于每个支持的DRM的对应的加密的CW。在方框840处，内容提供者还利用CW对明文实质进行加扰以生成加扰的实质，并将所有信息打包到受保护内容中。

[0056] 为了消费内容(例如，观看受保护内容)，DRM代理260执行以下操作：从用户A接收RBC 210和受保护内容250；验证RBC 210的有效性；提取用户ID 322；使用质询响应协议验证用户A是否具有与用户ID 322对应的私钥；检查受保护内容250的内容ID(例如，区块1的312)是否存在于用户A的RBC 210中；如果内容ID存在于用户A的RBC 210中，则验证用户权限(例如，区块1的314)是否列出用户A请求的语言和字幕语言；如果使用权限经过验证，则利用其秘密密钥DRM_KEY对加密的CW 430进行解密并取回明文CW；以及解扰具有CW的加扰的实质420并将其发送给用户A以供消费。

[0057] 在另一个实现中，相同的RBC 210可用于若干独立的内容提供者220。每个内容提供者220可以使用其自己的DRM代理260或与其它提供者共享DRM代理260。

[0058] 图9是图示根据本公开的一个实现的用于消费内容的处理的流程图900。在图9所示的实现中，在方框910处，由DRM代理接收RBC和受保护内容，并且在方框920处验证RBC的有效性。然后在方框930处，从RBC提取用户ID，并且在方框940处，DRM代理使用质询响应协议验证用户是否具有与用户ID对应的私钥。在方框950处，检查受保护内容的内容ID以确定它是否存在于RBC中。然后，在方框960处，如果内容ID存在于RBC中，则DRM代理验证使用权限是否列出用户请求的语言和字幕语言。如果使用权限经验证，则在方框970处DRM代理利用秘密密钥对加密的CW进行解密并取回明文CW。在方框980处，对加扰的实质进行解扰并将其与CW一起发送给用户以供消费。

[0059] 其它变化和实现也是可能的。例如，内容数据可以是用于各种类型的内容或其它数据，诸如电影、电视、视频、音乐、音频、游戏、科学数据、医疗数据等。可以使用各种DRM和

加密算法。用户标识和权限的关联可以以不同的方式处理，诸如一个用户在不同设备上具有相同或不同的权限、用户共享权限(例如，家庭账户或主要/从属账户)、临时共享权限(例如，借出、演示模型)。因此，本文讨论的具体示例不是新技术范围内的唯一实现。

[0060] 一个实现包括一个或多个可编程处理器并且对应的计算机系统组件存储和执行计算机指令，诸如以提供表示区块链和内容的数据的创建、存储、修改和传输，以及信息的管理，以控制加密、解密和访问表示内容的数据。

[0061] 提供所公开实现的以上描述是为了使本领域的任何技术人员能够制作或使用本发明。对于本领域技术人员来说，对这些实现的各种修改是显而易见的，并且在不脱离本公开的精神或范围的情况下，本文描述的一般原理可以应用于其它实现。因此，本技术不限于上述具体示例。因此，应该理解的是，本文呈现的描述和附图表示本公开的目前可能的实现，因此代表本公开广泛预期的主题。还应该理解的是，本公开的范围完全涵盖对于本领域技术人员而言可能变得显而易见的其它实现，并且本公开的范围因此仅由所附权限要求限制。

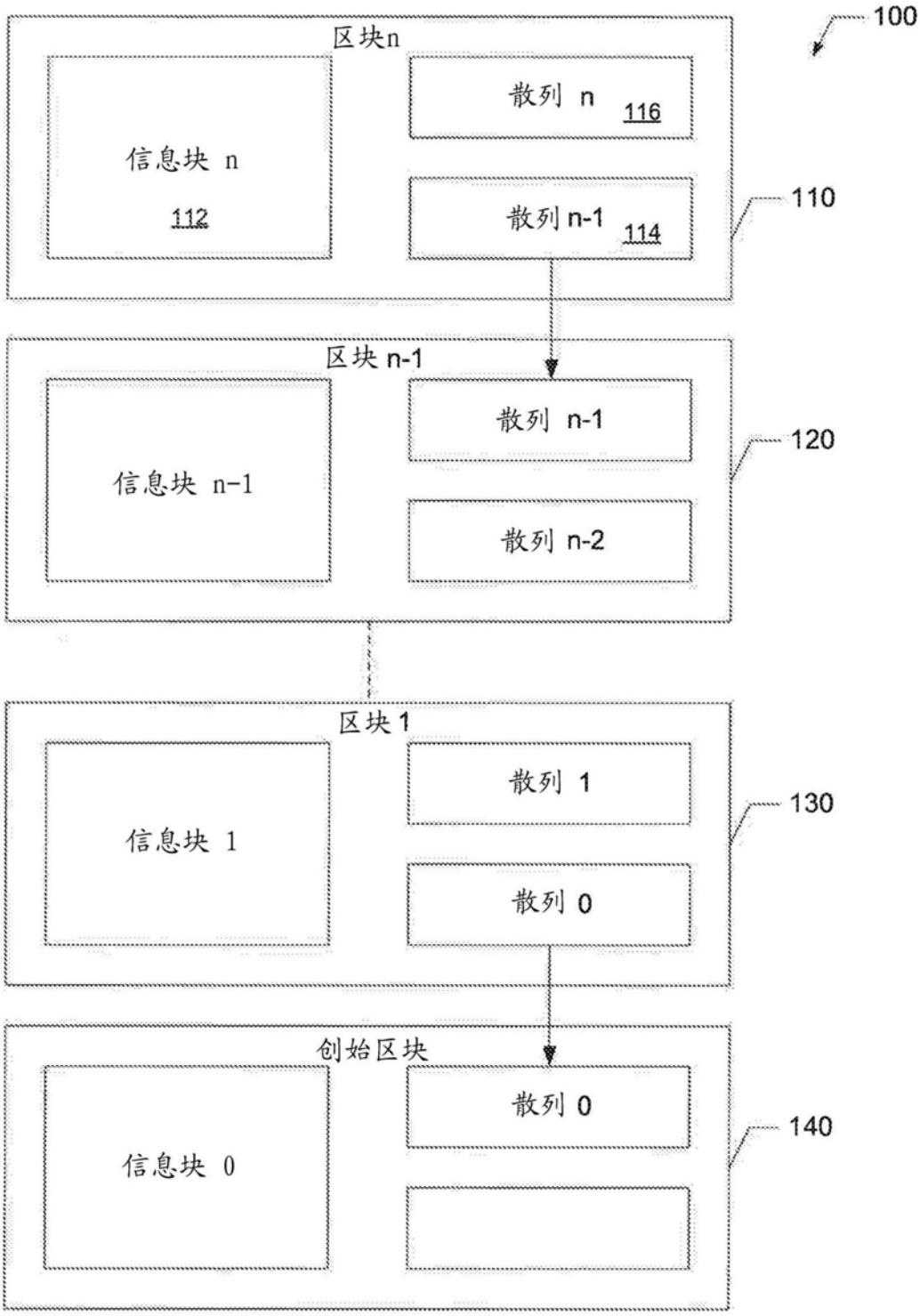

100
区块n
信息块 n
112
散列 n
116
散列 n-1
114
110
区块 n-1
信息块 n-1
散列 n-1
散列 n-2
120
区块 1
信息块 1
散列 1
散列 0
130
创始区块
信息块 0
散列 0
140

图1

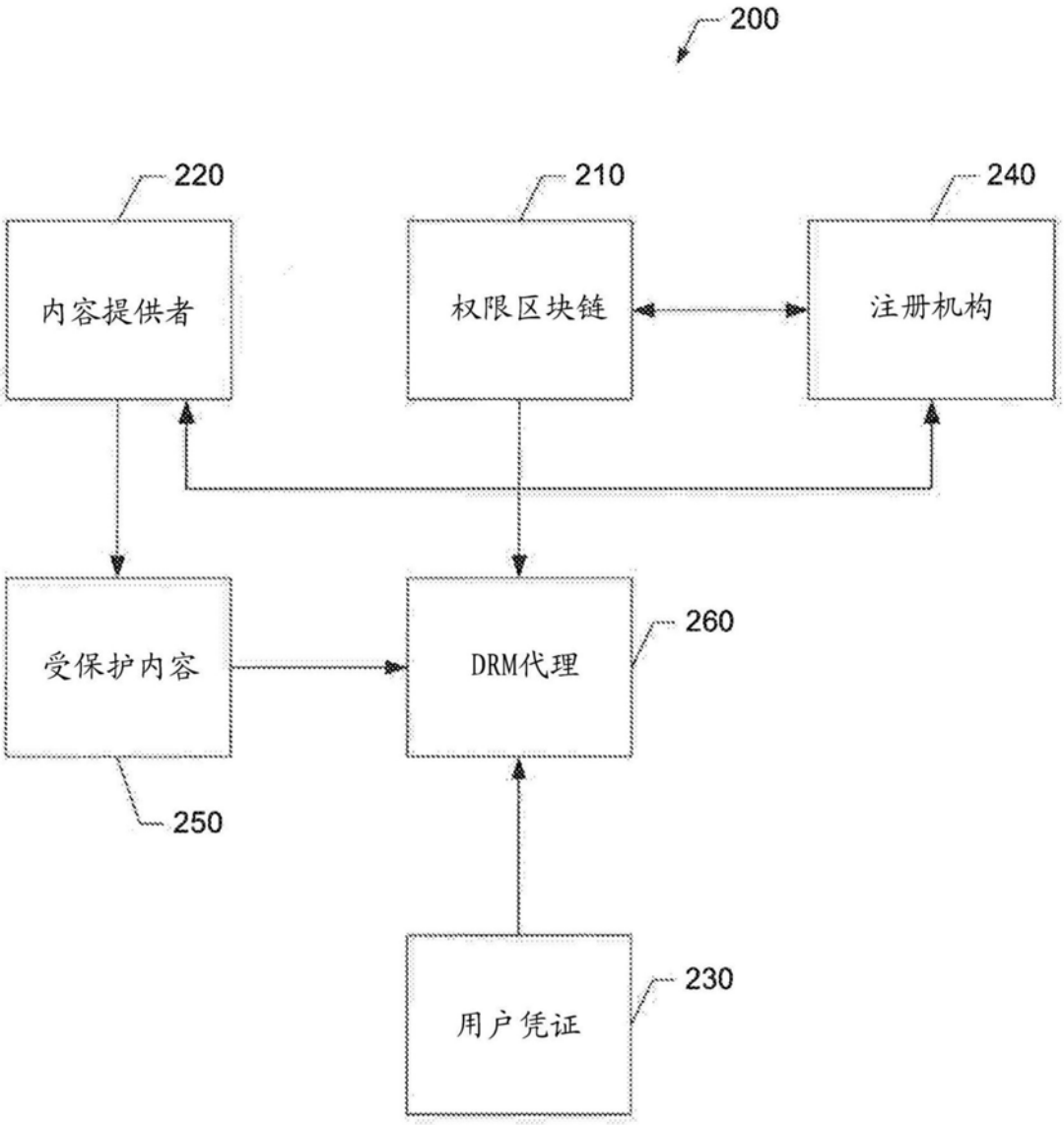


图2

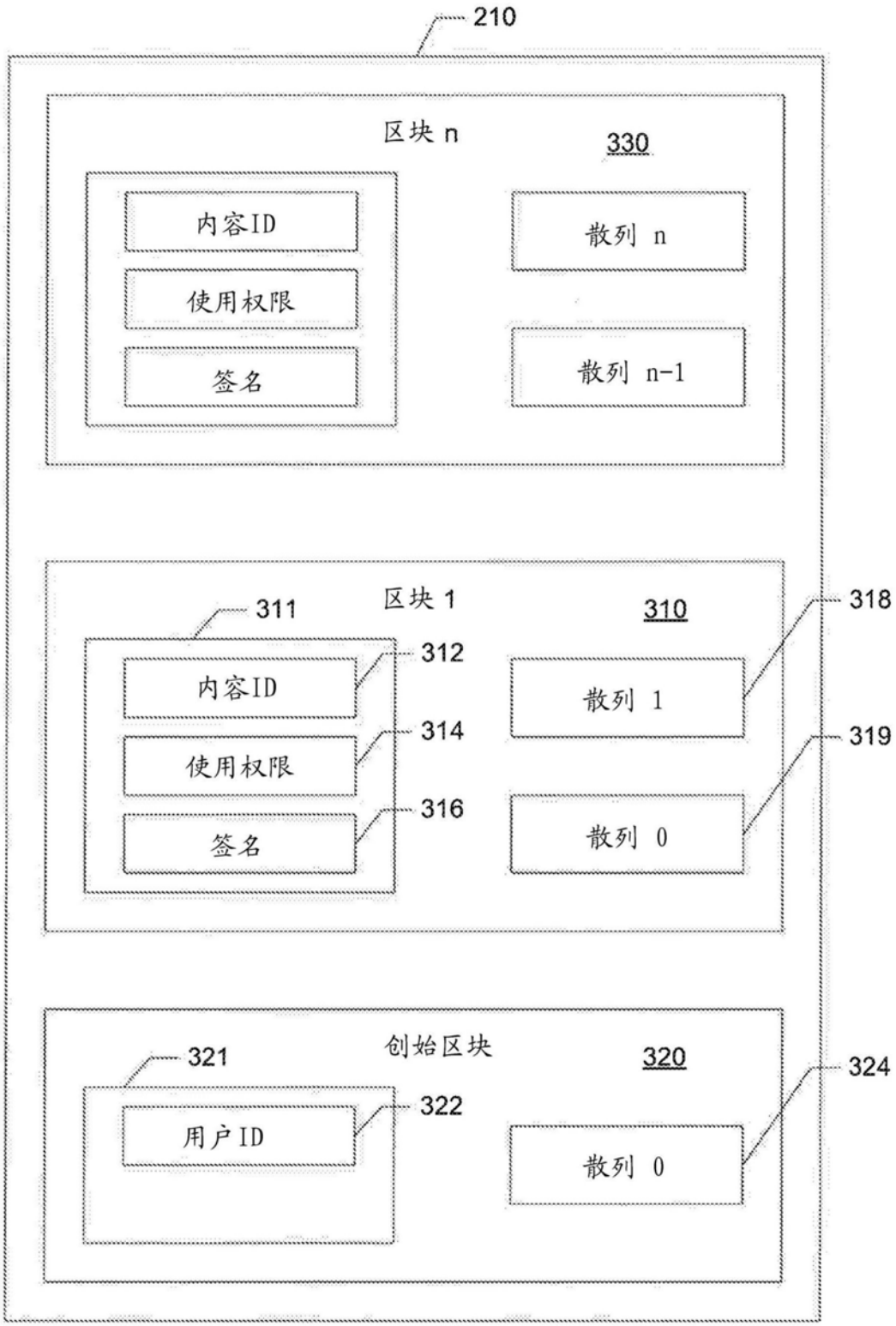

210
区块 n
330
内容ID
使用权限
签名
散列 n
散列 n-1
区块 1
311
310
312
314
316
318
319
内容ID
使用权限
签名
散列 1
散列 0
创始区块
321
320
322
324
用户 ID
散列 0

图3

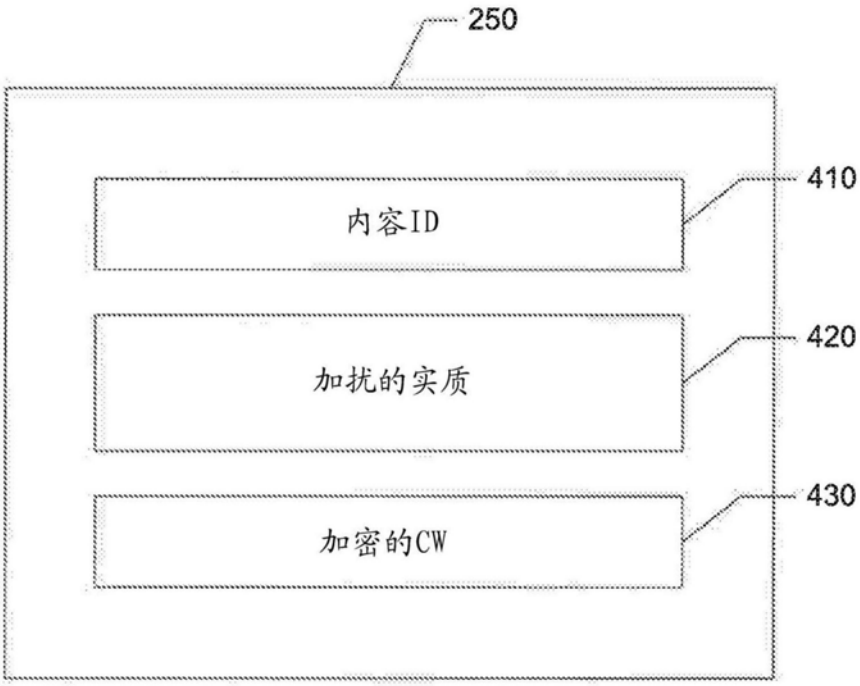


图4

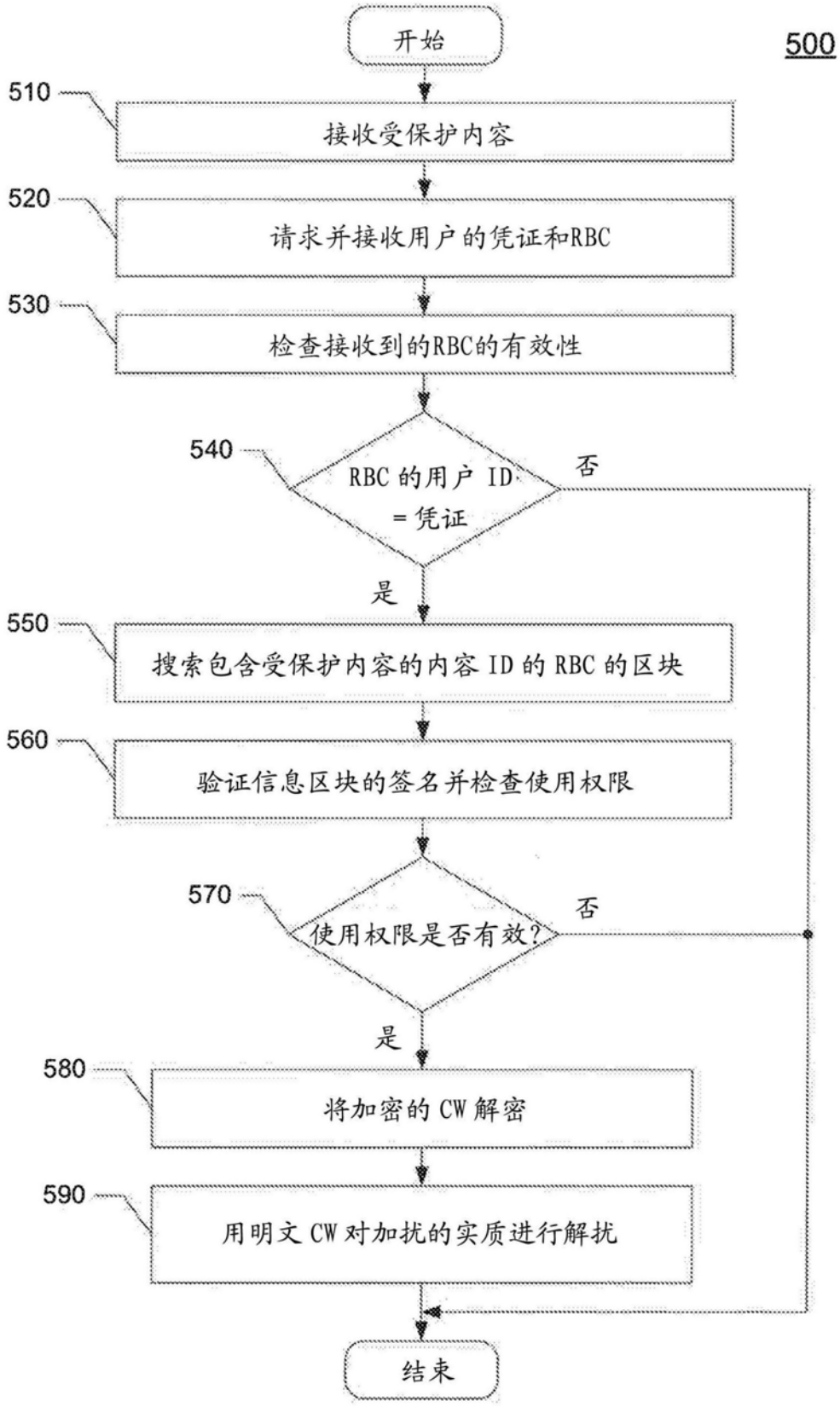

开始
500
510
接收受保护内容
520
请求并接收用户的凭证和RBC
530
检查接收到的RBC的有效性
540
RBC 的用户 ID = 凭证
否
是
550
搜索包含受保护内容的内容 ID 的 RBC 的区块
560
验证信息区块的签名并检查使用权限
570
使用权限是否有效?
否
是
580
将加密的 CW 解密
590
用明文 CW 对加扰的实质进行解扰
结束

图5

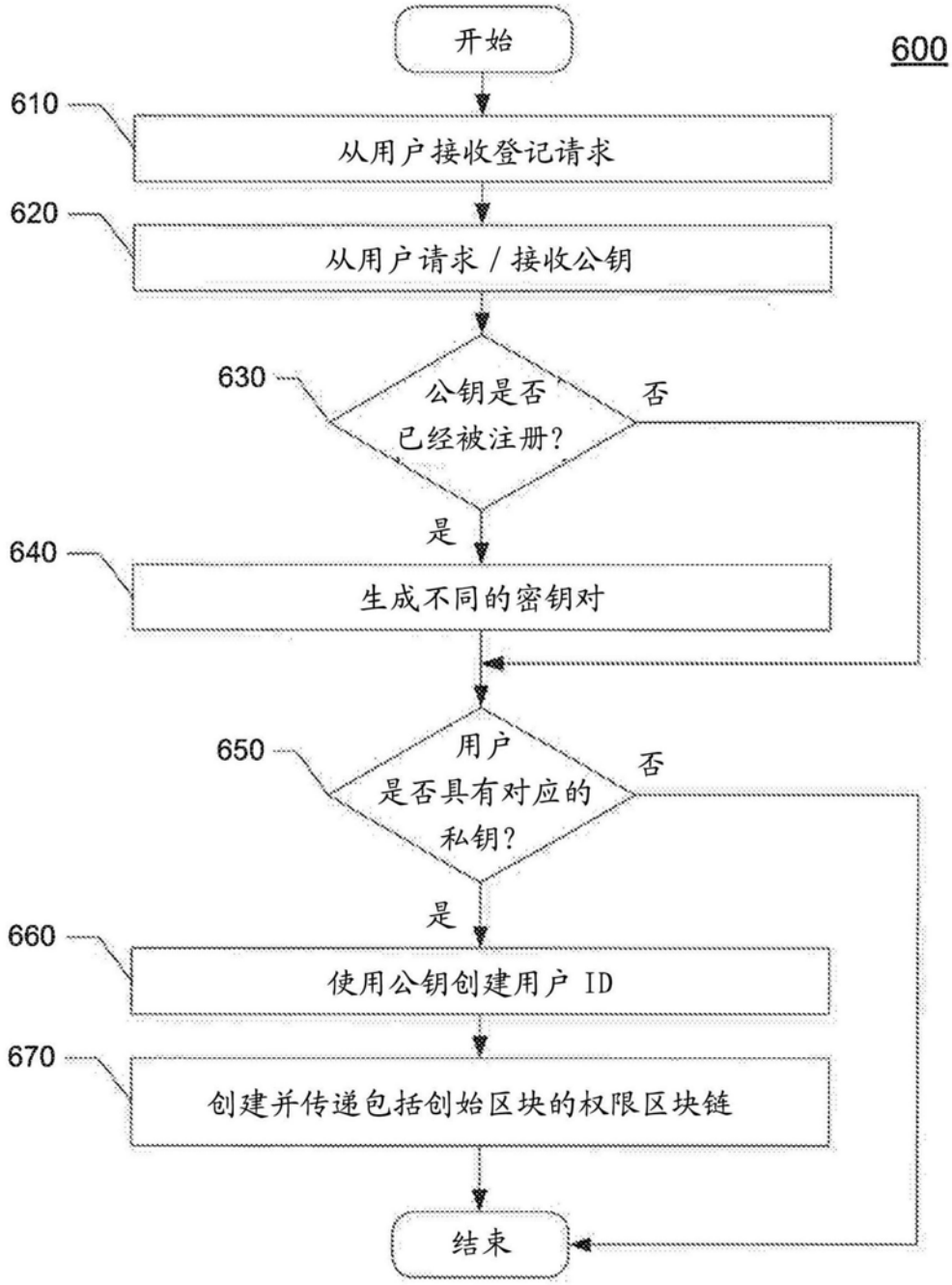

开始
600
610
从用户接收登记请求
620
从用户请求 / 接收公钥
630
公钥是否已经被注册?
否
是
640
生成不同的密钥对
650
用户是否具有对应的私钥?
否
是
660
使用公钥创建用户 ID
670
创建并传递包括创始区块的权限区块链
结束

图6

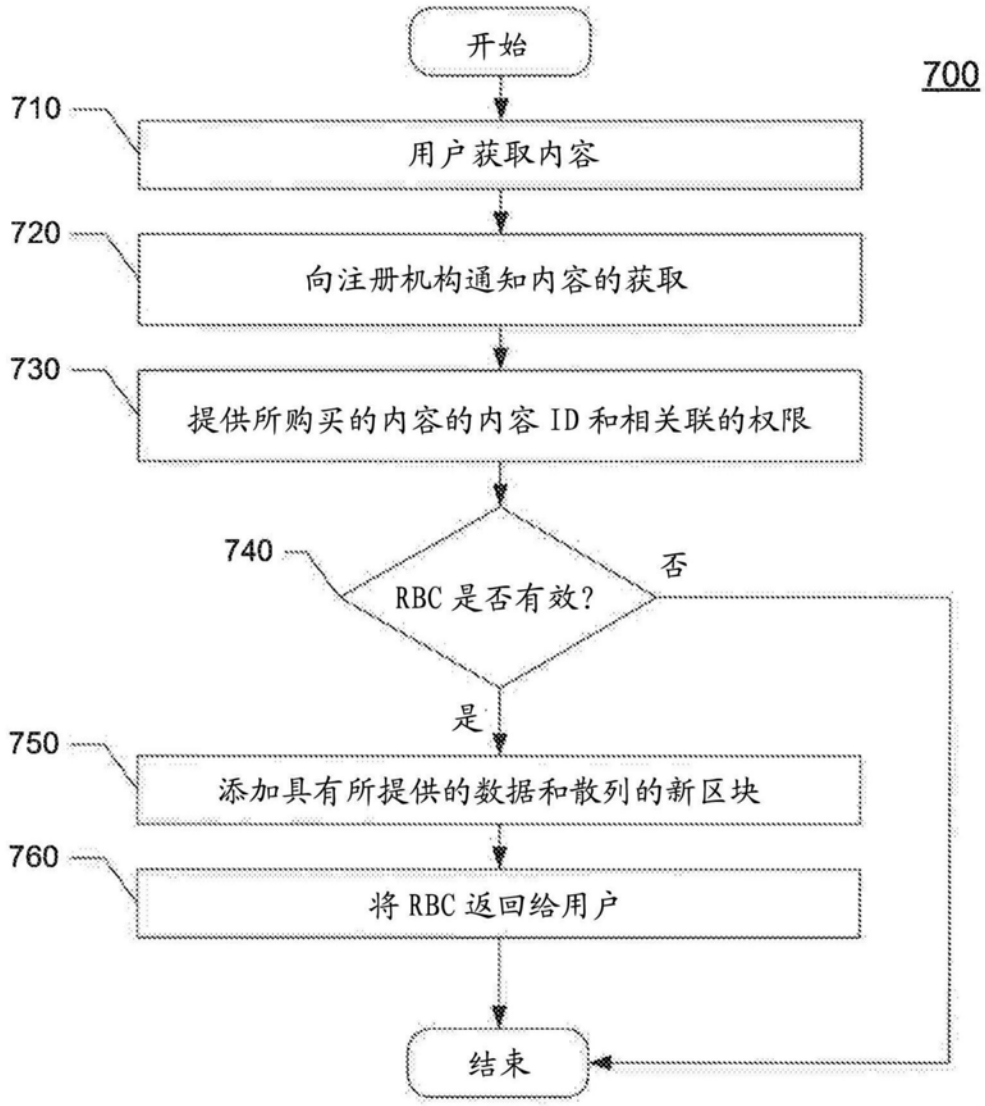

开始
700
710
用户获取内容
720
向注册机构通知内容的获取
730
提供所购买的内容的内容 ID 和相关联的权限
740
RBC 是否有效?
否
是
750
添加具有所提供的数据和散列的新区块
760
将 RBC 返回给用户
结束

图7

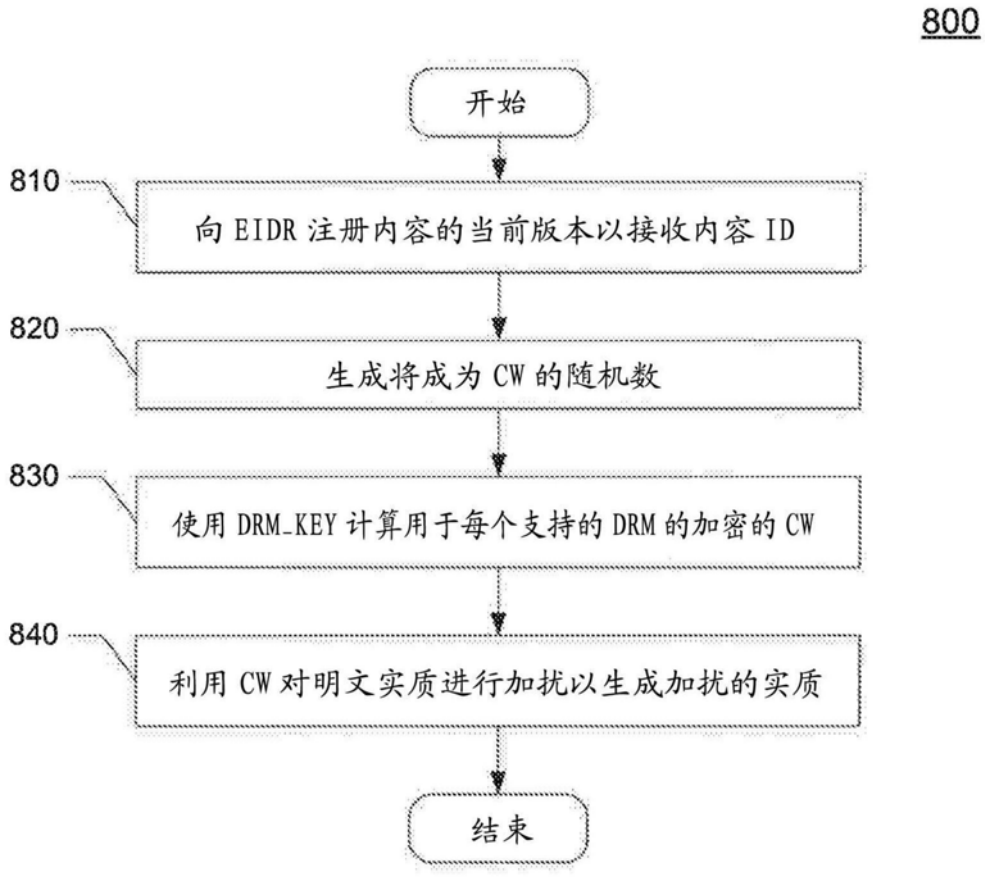

800
开始
810
向 EIDR 注册内容的当前版本以接收内容 ID
820
生成将成为 CW 的随机数
830
使用 DRM_KEY 计算用于每个支持的 DRM 的加密的 CW
840
利用 CW 对明文实质进行加扰以生成加扰的实质
结束

图8

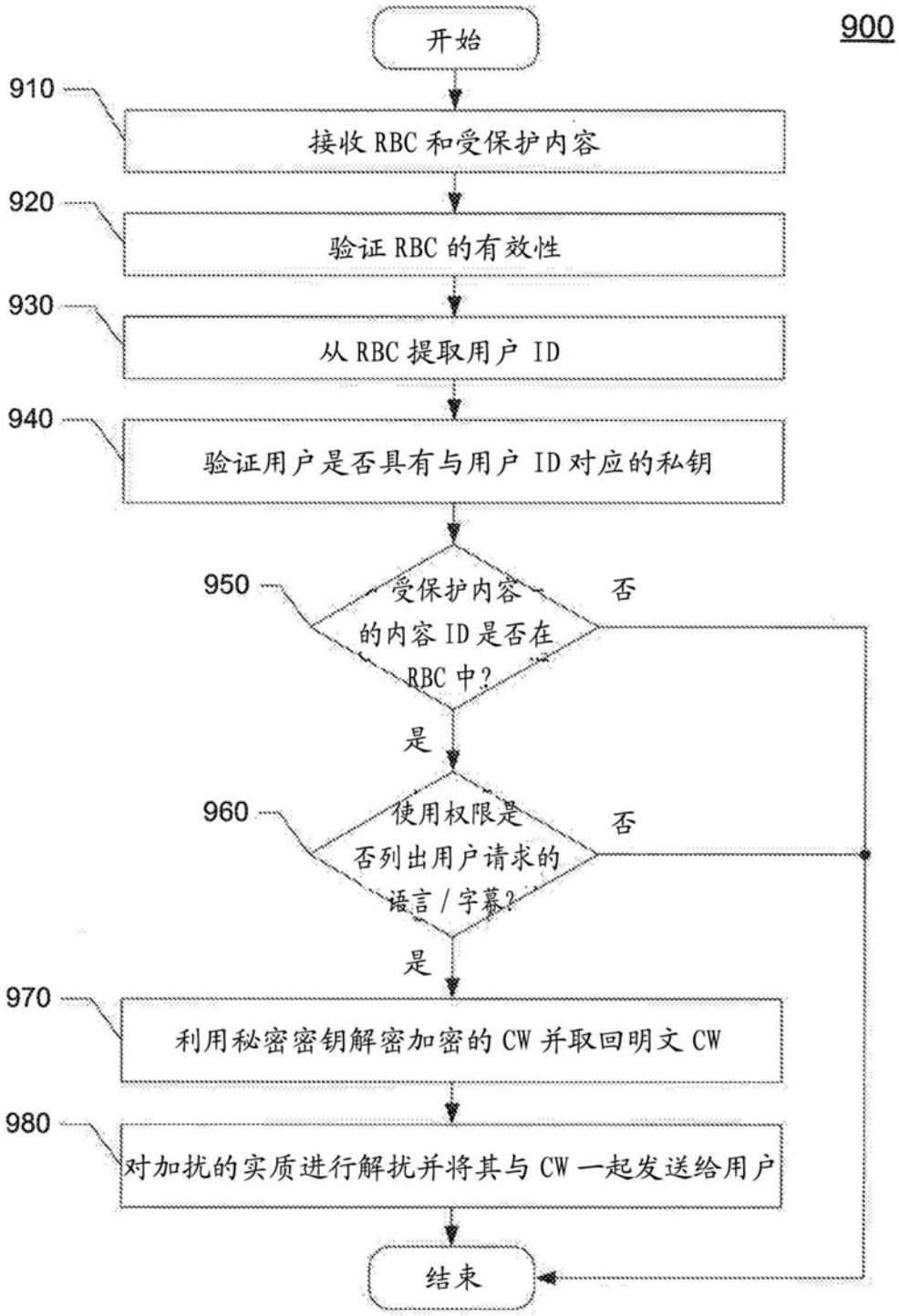

900
开始
910
接收 RBC 和受保护内容
920
验证 RBC 的有效性
930
从 RBC 提取用户 ID
940
验证用户是否具有与用户 ID 对应的私钥
950
受保护内容的内容 ID 是否在 RBC 中?
否
是
960
使用权限是否列出用户请求的语言 / 字幕?
否
是
970
利用秘密密钥解密加密的 CW 并取回明文 CW
980
对加扰的实质进行解扰并将其与 CW 一起发送给用户
结束

图9