<2018> 1학기 인지과학@ 과학기술대학원>

권리보호 특허

2018-05-31

김태희 컴퓨터과학과

특허 개요

관련 출원에 대한 상호 참조

본 출원은 35 U.S.C. 2016 년 10 월 20 일자로 출원 된 "Blockchain-Based DRM"이라는 공동 계류중인 미국 임시 특허 출원 제 62 / 410,557 호의 §119 (e). 상기 인용 된 출원의 개시는 본원에 참고로 인용된다.

배경

본 발명은 DRM (digital rights management)에 관한 것으로, 특히 블록 체인 (blockchains)을 이용하여 DRM을 구현하는 것에 관한 것이다. 상호 운영 성을 위해 많은 현재 DRM 솔루션에는 일반적으로 공급 업체 또는 공급 업체 그룹이 관리하는 권한 보관함 또는 기타 공용 저장소가 필요하다.

그러나 이러한 기존 솔루션은 신뢰성이 높지 않고 고유 한 장애 지점에 의존합니다. 권한 보유자 공급자 또는 시스템이 업무를 중단하거나 실패하는 경우 사용자는 획득 한 모든 콘텐츠를 잃게된다. 따라서 블록체인을 이용하여 문제를 해결하고자 한다.

Fig.1 일반적인 블록체인의 구조

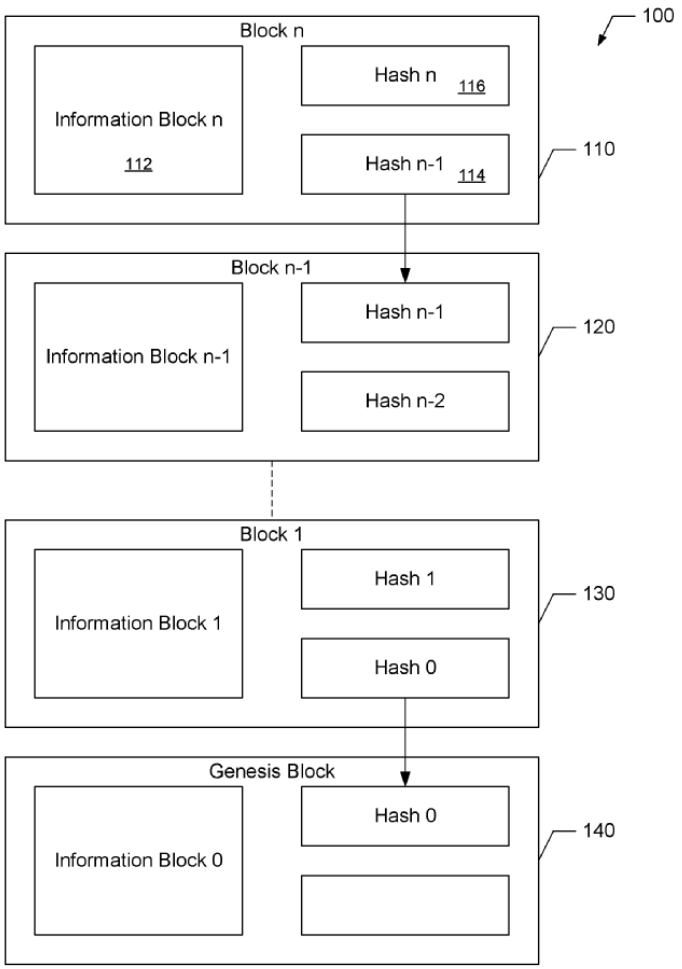


FIG. 1

블록은 적어도 3 개의 요소, 즉 등록 된 데이터를 저장하는 정보 , 현재 블록의 해시 이전 블록의 해시를 가지고 있다.

Fig. 2 블록체인을 사용하는 DRM 시스템의 상호작용

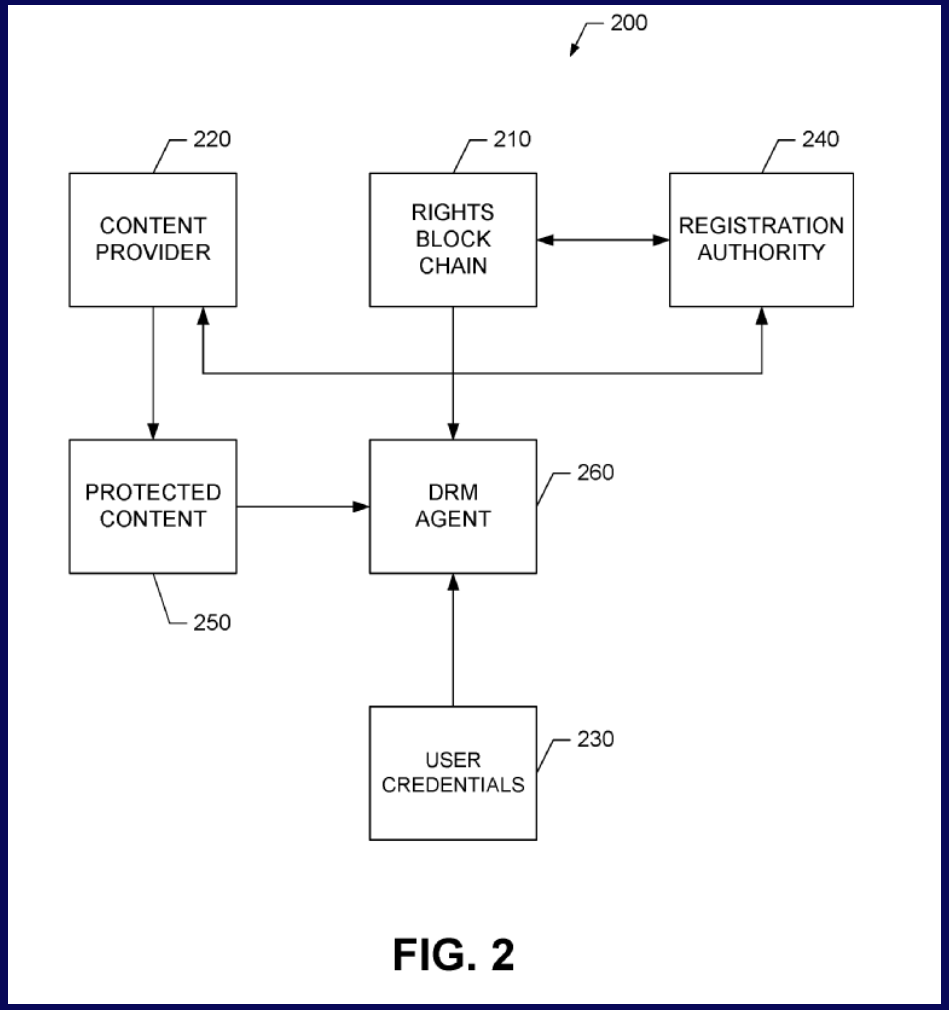


FIG. 2

Fig. 2는 블록 체인을 이용하는 새로운 DRM 시스템 (200)에서의 컴포넌트 및 상호 작용의 블록도이다.

새로운 시스템 (200)에서, 라이센스는 사용자에 의해 획득 된 모든 사용 권리를 보유하는 RBC (210) 내의 블록으로 대체된다.

이 블록 체인 (210)은 기밀성이 보호되지 않지만, 오직 무결성이 보장된다.

DRM 시스템 (200)은 RBC (210), 컨텐츠 제공자 (220), 사용자 증명서 (230), 등록 기관 (240), 보호 컨텐츠 (250) 및 DRM 에이전트 (260)를 포함한다.

Fig. 3 권리블록체인(RBC)의 예시

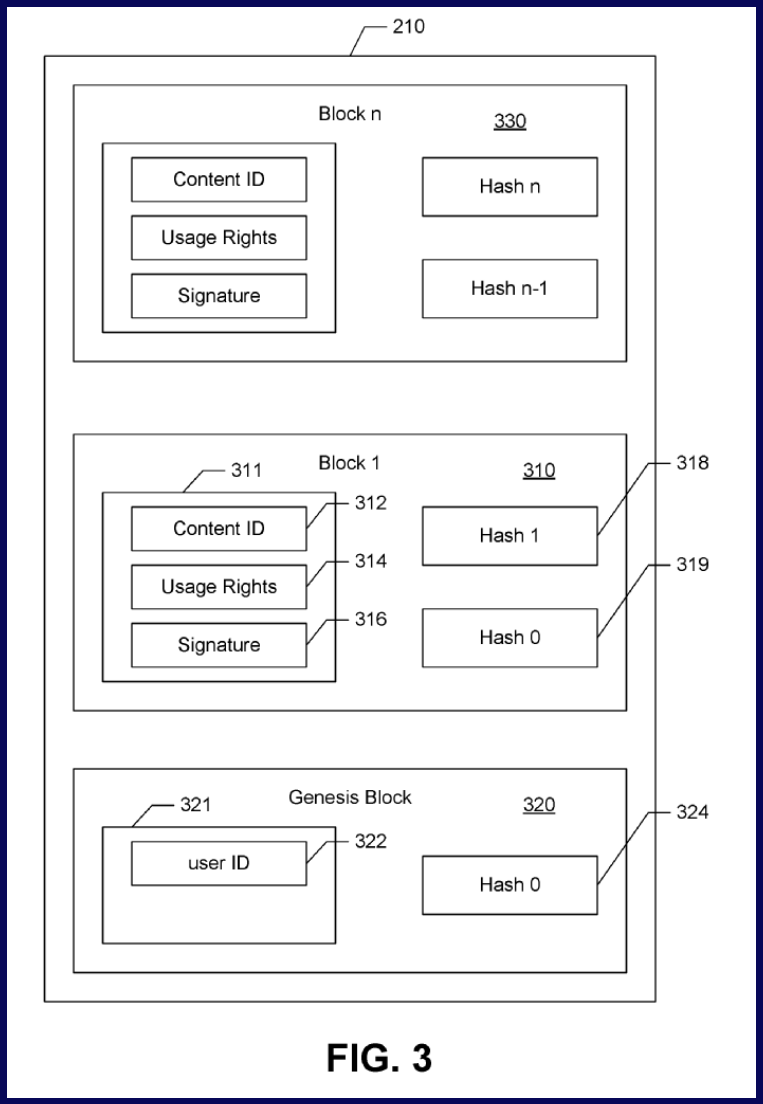


FIG. 3

제네시스 블록 (320)의 정보 블록 (321)은 적어도 사용자 ID (322)를 보유한다. 사용자 ID (322)는 RBC (210)가 공개 일 수 있기 때문에 익명 일 수 있다.

후속 블록들의 정보 블록 (예를 들어, 블록 1에 대한 311)은 적어도 콘텐츠 식별자 (ID) (예를 들어, 블록 1에 대한 312) 사용 권한 (예 : 블록 1의 314) 및 디지털 서명 (예 : 블록 1의 316).

사용 권한 (314)은 사용자가이 저작물에 대해 권리를 갖거나 획득 한 권리를 정의한다. 형식은 XrML (eXtensible Rights Markup Language) 또는 ODRL (Open Digital Rights Language)과 같은 표준화된 권한 언어, 스마트 계약 또는 독점적 형식 일 수 있습니다. 디지털 서명 (316)은 등록 기관 (240)에 의해 발행된다. 서명 (316)은 (311)의 정보 블록이다.

Fig. 4 보호된 내용(250)의 예시

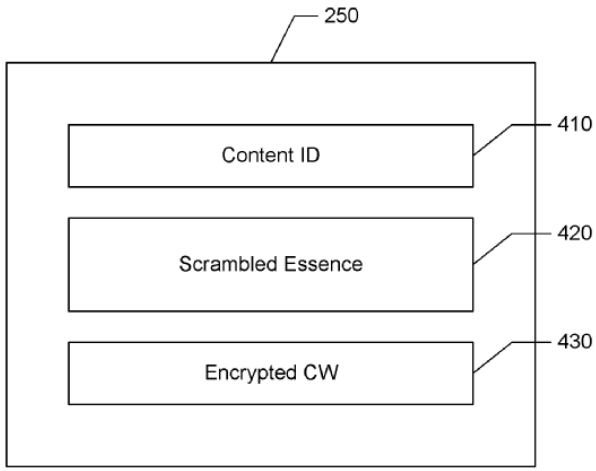


FIG. 4

Fig. 4 보호 컨텐트 (250)는 적어도 컨텐트 ID (410), 스크램블링 된 에센스 (420) 및 암호화 된 제어 워드 (암호화 된 CW) (430)를 포함한다.

컨텐트 ID (410)는 작업을 식별한다. RBC (210)에 의해 사용되는 것과 동일하다. 스크램블링 된 에센스 (420)는 제어 워드 (CW)를 사용하여 콘텐츠의 명확한 본질 (즉, 스크램블링없이 명확한 형태의 콘텐츠)을 스크램블링 한 결과이다.

스크램블링 알고리즘은 CBC 모드에서 AES 128 비트이다. 그것은 스크램블 에센스 = AES = 암호화 된 CW (430)는 (예를 들어, 비밀 키 또는 공개 키 – 비밀 키 쌍을 사용하여) DRM 에이전트 (260)에 알려진 키로 CW (이 본질을 스크램블링하는데 사용되는)를 암호화 한 결과이다.

Fig. 5 DRM 동작을 나타내는 흐름도

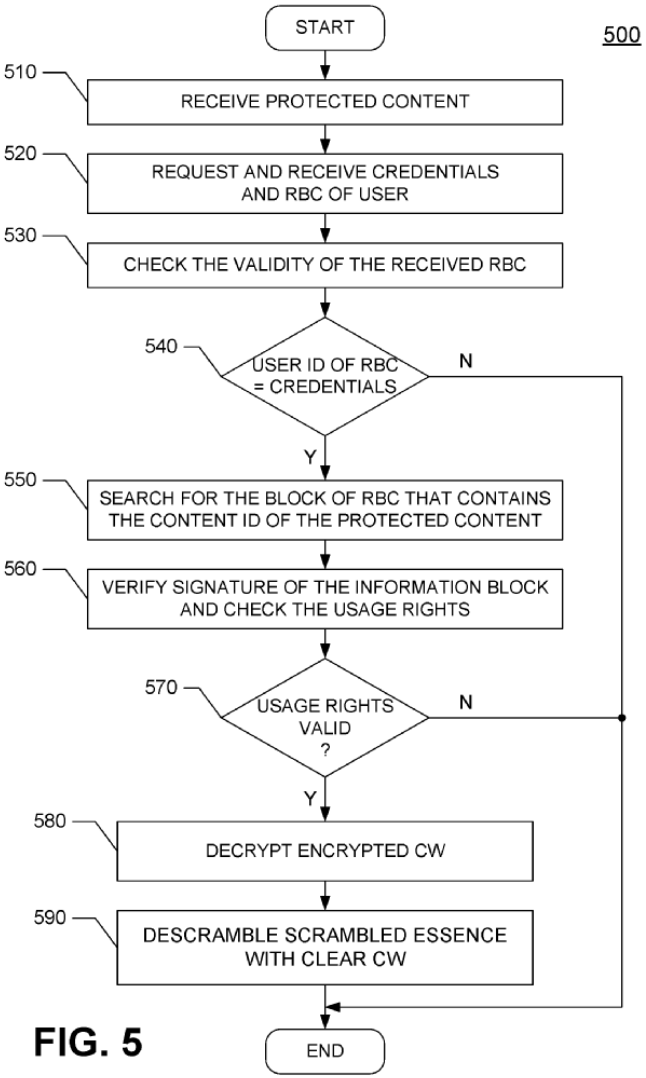


FIG. 5

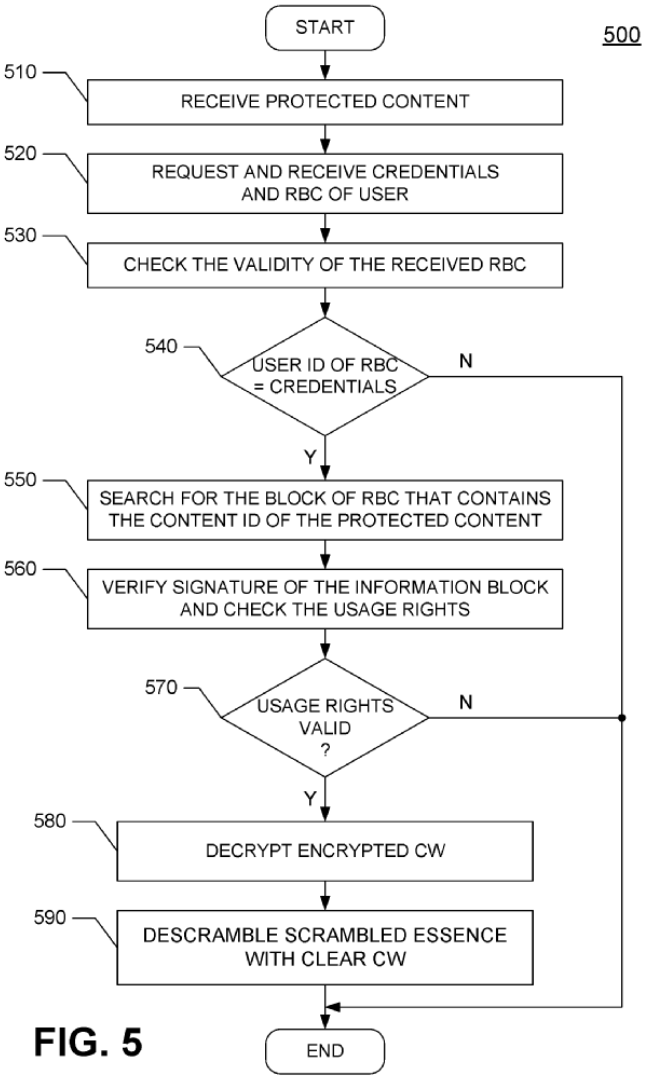
Fig.5 는 블록 체인을 사용하는 디지털 권리 관리 (DRM) 동작을 나타내는 흐름도 (500)이다.

DRM 동작은 Fig.1의 DRM 에이전트 (260) 내에서 수행된다. 블록 (530)에서, 수신 된 RBC (210)의 유효성이 검사된다

사용자 인증과정

그 다음, 수신 된 RBC (210)가 실제로 사용자에 속하는지를 검증하기 위한 결정이 이루어진다. 블록 (540)에서, RBC (210) 내의 사용자 ID (322)가 수신 된 사용자 증명서 (230)에 대응하는지 여부를 결정하기 위한 검사가 이루어진다.

Fig. 5 DRM 동작을 나타내는 흐름도 2



역암호화 과정

일단 수신 된 RBC가 사용자와 관련된다고 결정되면, 블록 (550)에서 보호 컨텐트에 대한 컨텐트 ID를 포함하는 RBC 내의 블록이 검색된다.

그 다음, 대응하는 검색 블록에서, 정보 블록의 서명 및 블록 (570)에서 사용 권한이 유효하다고 결정되면,

블록 (580)에서 암호화 된 CW (430)는 비밀 키 (즉, DRM_KEY)로 해독되고, 클리어 CW는 검색된다.

블록 (590)에서, 스크램블링 된 에센스는 클리어 CW로 디스크램블된다.

Fig. 6 RBC를 생성하는 프로세스 흐름도

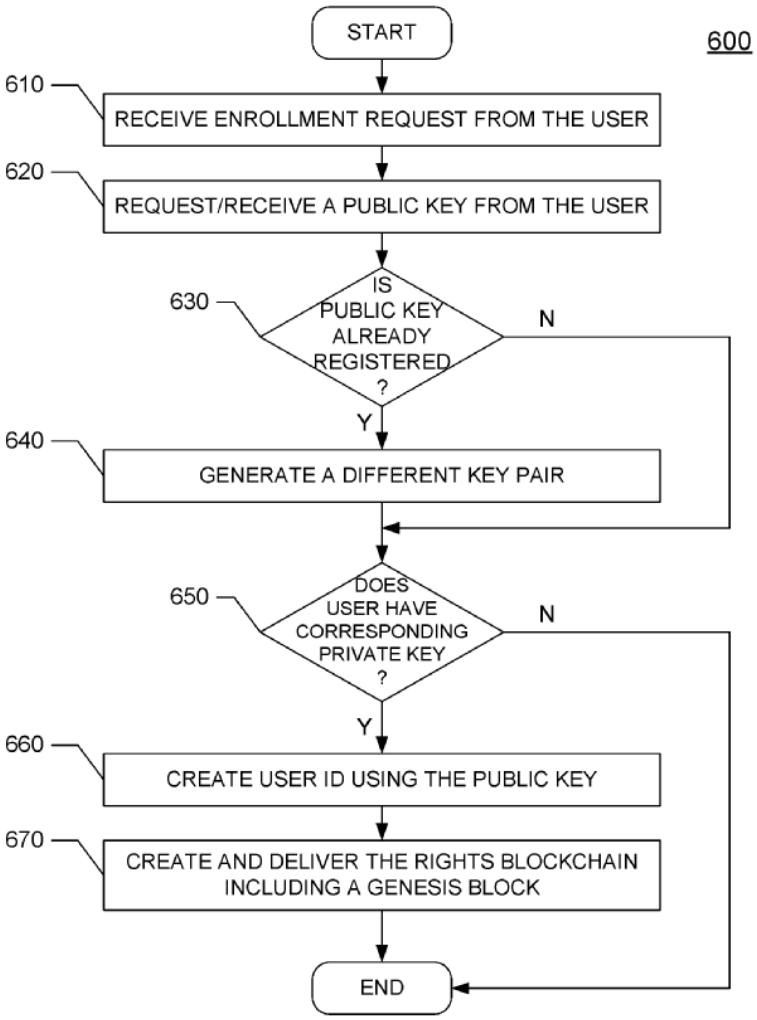


FIG. 6

Fig. 6은 RBC를 생성하는 프로세스를 나타내는 흐름도 (600)이다.

등록 기관은 블록 (620)에서 사용자로부터 공개 키를 요청하고, 블록 (630)에서 이 공개 키가 이미 존재하는지 여부를 검증한다.

블록 (640)에서, 등록 기관은 키가 이미 등록 된 경우 다른 키 쌍을 생성하도록 사용자에게 요청한다.

등록 기관은 블록 (650)에서 사용자가 챌린지 – 응답 프로토콜을 통해 대응하는 개인 키를 갖는지 여부를 검증하고,

블록 (660)에서 사용자의 공개 키로 사용자 ID를 생성하고, 블록 (660) RBC를 사용자에게 전송한다 (블록 670).

Fig. 7 주어진 내용을 획득하고 RBC에 사용권한 추가

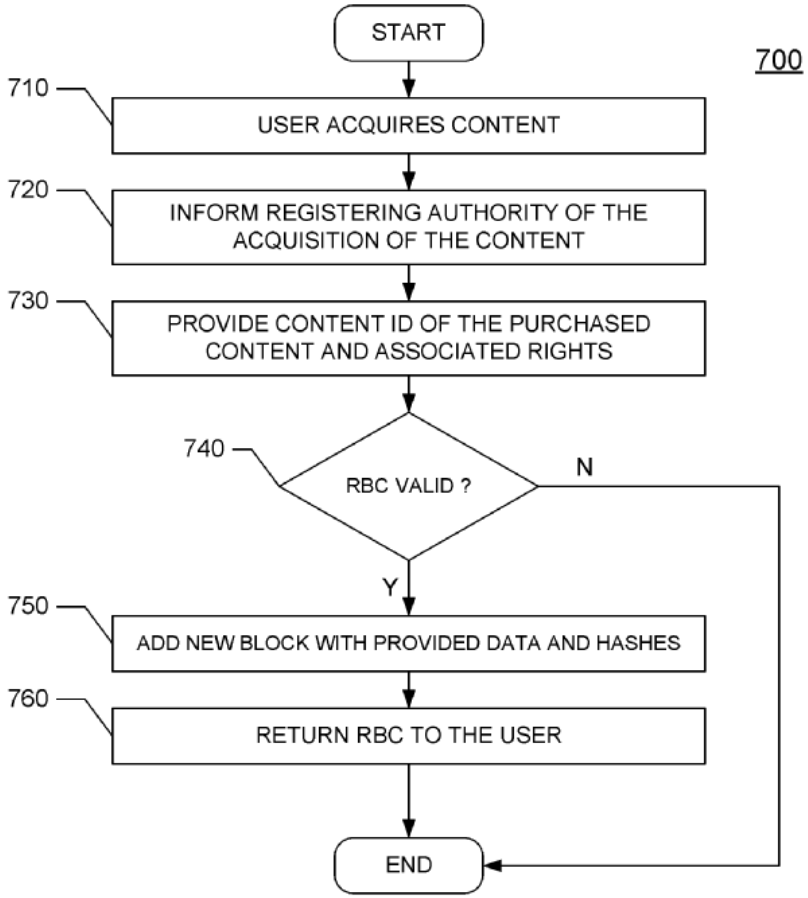


FIG. 7

Fig. 7은 주어진 컨텐츠를 획득하고 RBC에 사용 권한을 추가하는 프로세스를 나타내는 흐름도 (700)이다.

블록 (710)에서 사용자가 콘텐츠 제공자로부터 주어진 콘텐츠를 획득하면, 콘텐츠 제공자는 블록 (720)에서 사용자가 콘텐츠를 획득한 것을 등록 기관에 알린다.

콘텐츠 제공자는 구매된 콘텐츠의 콘텐츠 ID 및 블록 (730)에서 인가된 언어 및 자막 언어의 목록과 같은 관련 사용 권한을 등록 기관에 제공한다.

등록 기관은 블록 (740)에서 제공된 RBC의 무결성을 검사하고, RBC가 유효하고 그렇지 않은 경우, 블록 (750)에서 새로운 블록 및 선행 블록에 정보를 해싱하여 블록 (750)에서 제공한다.

Fig. 8 내용 제공자가 패키징 하는 프로세스

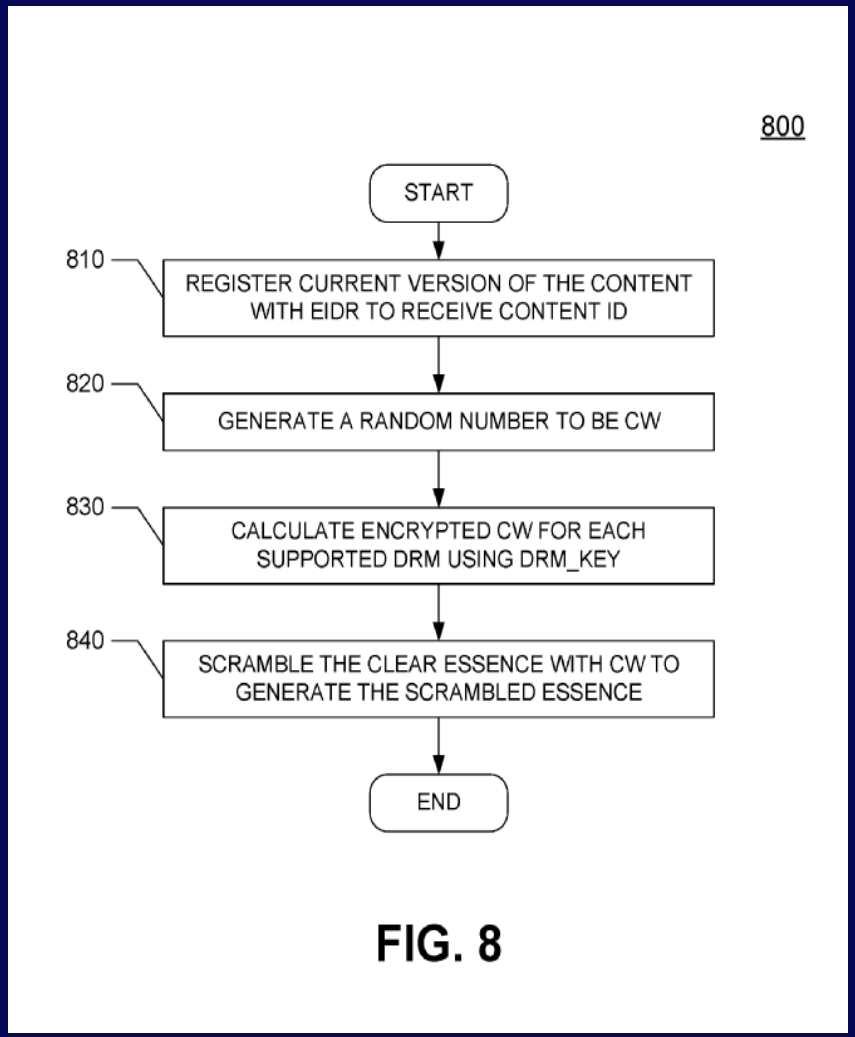


FIG. 8

Fig. 8은 콘텐츠 제공자에서 콘텐츠를 패키징하기 위한 프로세스를 나타내는 흐름도 (800)이다.

컨텐트 제공자는 블록 (810)에서 컨텐츠 ID를 수신하기 위해 컨텐츠의 현재 버전을 등록한다.

컨텐츠 제공자는 블록 (820)에서 제어워드 (CW)가 될 난수를 생성하고, 블록 (830)에서 대응하는 비밀 키 (DRM_KEY)로 CW를 암호화함으로써 각각의 지원되는 DRM에 대응하는 암호화된 CW를 생성한다.

또한, 콘텐츠 제공자는 블록 (840)에서 클리어본에 CW를 스크램블하여 스크램블링된 에센스를 생성하고, 보호된 콘텐츠로 콘텐트를 소비한다.

Fig. 9 내용을 소비하는 프로세스 흐름도

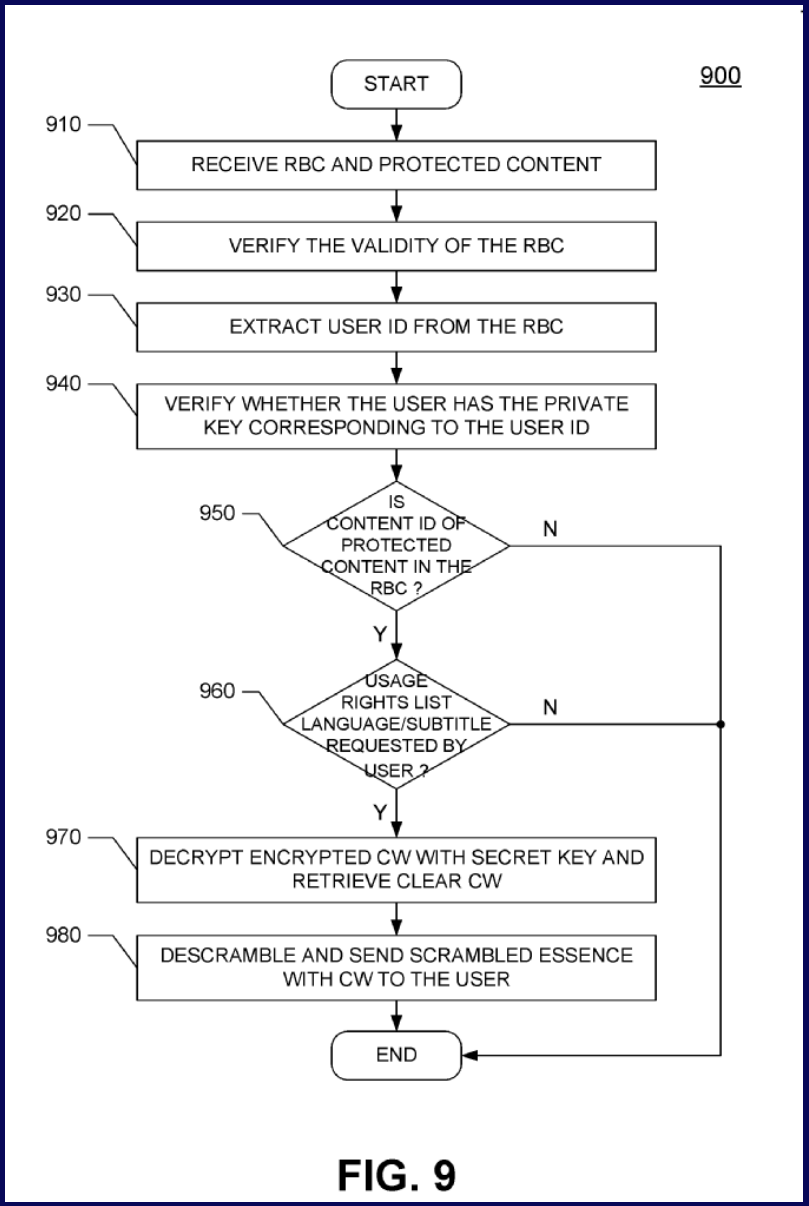


FIG. 9

Fig. 9 는 콘텐츠를 소비하는 프로세스를 나타내는 흐름도 (900)이다.

블럭 (920)에서 RBC 및 보호 컨텐츠가 DRM 에이전트에 의해 수신되고 RBC의 유효성이 검증된다.

블럭 (930)에서 사용자 ID가 RBC로부터 추출되고 ,

DRM 에이전트 블록 (940)에서 챌린지 – 응답 프로토콜을 사용하여 사용자가 사용자 ID에 대응하는 개인 키를 가지고 있는지 여부를 검증한다.

Fig. 9 내용을 소비하는 프로세스 흐름도

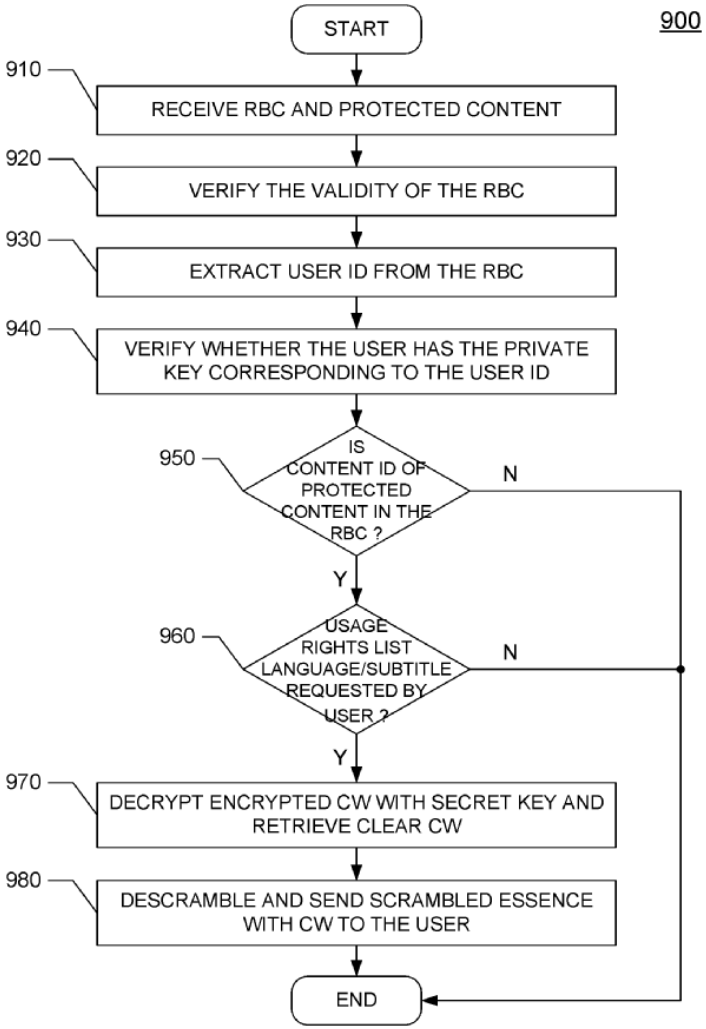


FIG. 9

블록 (950)에서, 보호된 콘텐츠의 콘텐츠 ID가 RBC에 존재하는지 여부를 결정하기 위해 검사한다.

그런 다음, 블록 (960)에서, DRM 에이전트는 RBC에 컨텐츠 ID가 존재하면 사용자가 요청한 언어 및 자막 언어를 사용 권한 목록에 나열하는지 여부를 확인한다. (700번 참조)

DRM 에이전트는 암호화 된 CW를 비밀키로 해독하고, 블록 (970)에서 사용 권한이 검증되는지를 알기 위해 클리어 CW를 검색한다.

스크램블링 된 에센스는 디 스크램블링되고 블록 (980)에서 소비를 위해 사용자에게 CW와 함께 전송된다.

마무리 정리

콘텐츠 데이터는 영화, 텔레비전, 비디오, 음악, 오디오, 게임, 과학 데이터, 의료 데이터 등과 같은 다양한 유형의 콘텐츠 또는 다른 데이터에 대한 것일 수 있다.

다양한 DRM 및 암호화 알고리즘이 사용될 수 있으며, 사용자 식별 및 권한 조합은 다른 장치에서 동일하거나 다른 권한을 가진 한 사용자, 권리를 공유하는 사용자 (예 : 가족 계좌 또는 기본 / 종속 계정), 권리의 임시 공유 (예 : 대여 , 데모 모델)의 추가 변형 및 구현도 가능하다.

개시된 구현들의 상기 설명은 임의의 당업자가 본 발명을 제조 또는 사용할 수 있도록 제공된다. 이러한 구현들에 대한 다양한 수정들이 당업자에게 쉽게 명백 할 것이며, 본 명세서에 설명 된 일반적인 원리들은 본 개시의 사상 또는 범위를 벗어나지 않고 다른 구현 예들에 적용될 수 있다. 따라서,이 기술은 상술한 특정 예에 한정되지 않는다

따라서, 본 명세서에 제공된 설명 및 도면은 본 개시의 현재 가능한 구현을 나타내므로 본 개시에 의해 광범위하게 고려되는 주제를 대표 함을 이해해야 한다.

Thank for your listening