



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2019년06월07일
(11) 등록번호 10-1986482
(24) 등록일자 2019년05월31일

(51) 국제특허분류(Int. Cl.)
G06Q 50/18 (2012.01) G06Q 20/12 (2012.01)
H04L 29/08 (2006.01)
(52) CPC특허분류
G06Q 50/18 (2013.01)
G06Q 20/1235 (2013.01)
(21) 출원번호 10-2017-0169992
(22) 출원일자 2017년12월12일
심사청구일자 2017년12월12일
(56) 선행기술조사문헌
KR101628005 B1*
KR1020170129866 A*
JP2004532439 A*
KR1020090113310 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 디지캡
서울특별시 강서구 마곡중앙8로7길 11(마곡동, 디앤씨 캠퍼스)
상명대학교 천안산학협력단
충청남도 천안시 동남구 상명대길 31, 상명대학교내 (안서동)
(72) 발명자
고병수
경기도 수원시 권선구 금곡로 46, 505동 802호(금곡동, 수원호매실휴먼시아5단지아파트)
신수홍
서울특별시 강서구 마곡중앙5로1길 21, N403호(마곡동)
이중혁
충청남도 천안시 서북구 북일로 21, 104동 1503(두정동, e편한세상 두정3차)
(74) 대리인
특허법인 신지

전체 청구항 수 : 총 11 항

심사관 : 송원선

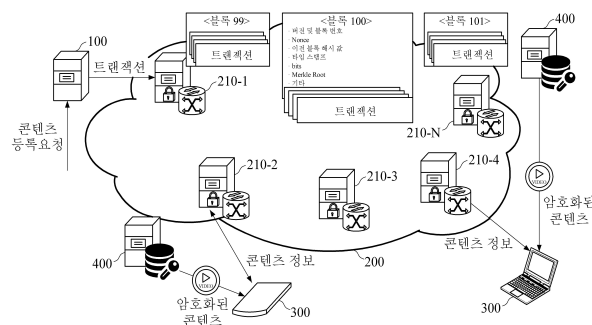
(54) 발명의 명칭 콘텐츠 정보 저장 및 관리를 위한 콘텐츠 블록체인

(57) 요약

블록체인 기반의 DRM 서비스 시스템에 관한 기술이 개시된다. 일 실시 예에 따른 DRM 서비스 시스템은 콘텐츠 등록 에이전트와, 블록체인 네트워크와, 사용자 에이전트를 포함한다.

콘텐츠 등록 에이전트는 서비스 제공자의 디지털 콘텐츠 등록 요청에 따라 표준 콘텐츠 식별자와 사용자 콘텐츠와 콘텐츠 속성과 콘텐츠 저작권 정보를 포함하는 트랜잭션을 생성하여 블록체인에 등록 요청하고, 블록체인 네트워크의 복수의 참여 노드는 합의 알고리즘에 따라 콘텐츠 등록 에이전트로부터 수신한 트랜잭션으로 블록을 생성하고 블록체인에 추가하며, 사용자 에이전트는 DRM 콘텐츠를 이용하기 위해 블록체인 네트워크에 연결하여 콘텐츠 정보를 획득한다.

대표도



(52) CPC특허분류

H04L 67/1065 (2013.01)

H04L 67/1097 (2013.01)

명세서

청구범위

청구항 1

블록체인을 기반으로 하는 DRM 서비스 시스템에 있어서,

서비스 제공자의 디지털 콘텐츠 등록 요청에 따라 콘텐츠 정보를 포함하는 트랜잭션을 생성하고, 생성된 트랜잭션을 블록체인 네트워크에 참여한 노드들로 전송하는 콘텐츠 등록 에이전트;

로컬 저장소에 블록체인을 저장하고, 콘텐츠 등록 에이전트로부터 트랜잭션들을 수신하여, 합의 알고리즘에 따라 블록을 생성하여 로컬 저장소의 블록체인에 추가하고 생성된 블록을 다른 노드로 전송하거나, 다른 노드가 생성한 블록을 검증하여 로컬 저장소의 블록체인에 추가하는 복수의 노드들을 포함하는 블록체인 네트워크; 및

블록체인 네트워크에 연결하여 콘텐츠 정보를 획득하는 사용자 에이전트;

를 포함하되,

콘텐츠 정보는 표준 콘텐츠 식별자와 사용자 콘텐츠 식별자와 콘텐츠 속성과 콘텐츠 저작권 정보를 포함하고,

사용자 에이전트는 콘텐츠의 식별자인 표준 콘텐츠 식별자 또는 사용자 콘텐츠 식별자로 블록체인에서 콘텐츠의 위치 정보를 검색하여 획득하는 블록체인 기반의 DRM 서비스 시스템.

청구항 2

제 1 항에 있어서,

DRM 서비스 제공에 필요한 사용자 정보와 디바이스 정보를 포함하는 서비스 정보를 저장하는 DRM 서버; 및

DRM 정책에 따라 패키징된 콘텐츠를 배포하는 콘텐츠 서버;

를 더 포함하는 블록체인 기반의 DRM 서비스 시스템.

청구항 3

삭제

청구항 4

제 1 항에 있어서,

표준 콘텐츠 식별자는 국제 표준 연속 간행물 번호(ISSN)와 디지털 객체 식별자(DOI)와 국제 표준 음악 작품 코드(ISWC)와 국제 표준 음악 번호(ISMN)와 국가 디지털 콘텐츠 식별체계(UCI) 중 어느 하나인 블록체인 기반의 DRM 서비스 시스템.

청구항 5

제 1 항에 있어서,

콘텐츠 속성은 콘텐츠의 메타데이터로 콘텐츠의 종류와 콘텐츠의 포맷과 콘텐츠의 크기와 콘텐츠 데이터의 해쉬 값과 콘텐츠의 위치 정보를 포함하는 블록체인 기반의 DRM 서비스 시스템.

청구항 6

제 1 항에 있어서,

트랜잭션은 콘텐츠를 구매한 사용자 정보와 콘텐츠 암호키와 라이선스 정보를 더 포함하는 블록체인 기반의 DRM 서비스 시스템.

청구항 7

삭제

청구항 8

제 1 항에 있어서,

사용자 에이전트는 콘텐츠의 식별자인 표준 콘텐츠 식별자 또는 사용자 콘텐츠 식별자로 블록체인에서 콘텐츠의 저작권 정보를 검색하여 획득하는 블록체인 기반의 DRM 서비스 시스템.

청구항 9

콘텐츠 등록 에이전트와, 다수의 노드들이 참여하는 블록체인 네트워크와, 사용자 에이전트와, 콘텐츠 서버와, 사용자 단말을 포함하는 블록체인 기반의 DRM 시스템의 DRM 서비스 제공 방법에 있어서,

콘텐츠 등록 에이전트가 서비스 제공자의 디지털 콘텐츠의 등록 요청에 따라 콘텐츠 정보를 포함하는 트랜잭션을 생성하는 단계;

콘텐츠 등록 에이전트가 생성된 트랜잭션을 블록체인 네트워크에 참여한 노드들로 전송하는 단계;

블록체인 네트워크에 참여한 노드들이 콘텐츠 등록 에이전트로부터 트랜잭션들을 수신하고 합의 알고리즘에 따라 블록을 생성하는 노드를 결정하는 단계;

결정된 노드가 블록을 생성하고 로컬 저장소의 블록체인에 추가하는 단계;

블록을 생성한 노드가 다른 블록체인 네트워크에 참여한 다른 노드로 생성된 블록을 전송하는 단계; 및

블록을 수신한 노드가 블록을 검증하여 로컬 저장소의 블록체인에 추가하는 단계;

를 포함하되,

콘텐츠 정보는 표준 콘텐츠 식별자와 사용자 콘텐츠 식별자와 콘텐츠 속성과 콘텐츠 저작권 정보를 포함하고,

상기 방법은

사용자 단말이 사용자 에이전트를 통해 콘텐츠의 식별자인 표준 콘텐츠 식별자 또는 사용자 콘텐츠 식별자로 블록체인에서 콘텐츠의 위치 정보를 검색하여 획득하는 단계;와 사용자 단말이 블록체인 검색으로 획득한 콘텐츠의 위치 정보로 콘텐츠 서버로부터 콘텐츠를 다운로드하는 단계;를 더 포함하는 블록체인 기반의 DRM 서비스 제공방법.

청구항 10

삭제

청구항 11

제 9 항에 있어서,

표준 콘텐츠 식별자는 국제 표준 연속 간행물 번호(ISSN)와 디지털 객체 식별자(DOI)와 국제 표준 음악 작품 코드(ISWC)와 국제 표준 음악 번호(ISMN)와 국가 디지털 콘텐츠 식별체계(UCI) 중 어느 하나인 블록체인 기반의 DRM 서비스 제공 방법.

청구항 12

제 9 항에 있어서,

콘텐츠 속성은 콘텐츠의 메타데이터로 콘텐츠의 종류와 콘텐츠의 포맷과 콘텐츠의 크기와 콘텐츠 데이터의 해쉬 값과 콘텐츠의 위치 정보를 포함하는 블록체인 기반의 DRM 서비스 제공 방법.

청구항 13

제 9 항에 있어서,

트랜잭션은 콘텐츠를 구매한 사용자 정보와 콘텐츠 암호키와 라이선스 정보를 더 포함하는 블록체인 기반의 DRM 서비스 제공방법.

청구항 14

삭제

청구항 15

제 9 항에 있어서,

사용자 단말이 사용자 에이전트를 통해 콘텐츠의 식별자인 표준 콘텐츠 식별자 또는 사용자 콘텐츠 식별자로 블록체인에서 콘텐츠의 저작권 정보를 검색하여 획득하는 단계;

를 더 포함하는 블록체인 기반의 DRM 서비스 제공방법.

발명의 설명

기술 분야

[0001] DRM 시스템에 관한 것으로, 특히 블록체인에 기반하여 콘텐츠 정보를 저장하고 관리하는 DRM 시스템에 대한 발명이 개시된다.

배경 기술

[0002] 디지털 저작권 관리(Digital Rights Management, 이하 DRM)는 디지털화되어 정보통신망을 통하여 손쉽게 배포될 수 있는 콘텐츠의 불법적이고 무제한적인 복제를 방지하고 적법한 사용자만이 디지털 콘텐츠를 사용할 수 있도록 관리하는 기술이다.

[0003] DRM은 콘텐츠의 생성에서 유통, 관리까지를 일괄적으로 관리하는 기술로 콘텐츠의 패키징, 콘텐츠의 배포, 콘텐츠 사용에 대한 과금, 콘텐츠의 모니터링, 콘텐츠의 개인화 등을 포함하는 종합적인 디지털 저작권 관리 시스템을 구성하는 기술이다.

[0004] DRM 시스템은 일반적으로 콘텐츠 관리를 위한 콘텐츠 정보와 라이선스 정보 등이 중앙의 서버에만 저장되어 다양한 사용자 단말들이 DRM 콘텐츠를 액세스할 때 사용자 단말과 서버간 많은 통신 부하가 걸리는 문제가 발생된다.

[0005] 블록체인은 각종 데이터를 중앙 서버 한곳에 저장하지 않고 네트워크에 참여한 노드들에 분산해서 처리하는 기술을 말한다. 가상 화폐를 비롯해 부동산, 토지, 주민등록 등 공공시스템까지 폭넓게 채택 활용되고 있다. 거래 기록이 블록이라는 단위로 정리돼 시간별로 이어지는 특징이 있고, 각 블록에는 앞의 블록과 뒤의 블록과 연결되는 연결 정보가 포함돼 있어 과거 블록의 내용을 조작하는 것이 어렵다.

[0006] 또한, 블록체인은 분산형 원장 구조이며, 그 블록체인 네트워크에 참가한 모든 사람이 모든 거래 기록을 기록한 원장을 소유하기 때문에 거래의 투명성이 높은 특징이 있다. 또한 거래 기록을 관리하는 거대한 중앙 시스템을 필요로 하지 않는다.

발명의 내용

해결하려는 과제

- [0007] 제안된 발명은 중앙 시스템에 통신 부하가 많이 발생하지 않도록 분산 원장 구조의 블록체인 기술을 DRM 시스템에 적용하는 방법을 제공함에 그 목적이 있다.
- [0008] 또한, 제안된 발명은 저작권 보호 시스템에서 디지털 콘텐츠 식별을 위한 표준적인 식별자를 적용하는 방법을 제공하는 것에 그 목적이 있다.

과제의 해결 수단

- [0009] 과제를 해결하기 위한 제안된 발명의 일 양상에 따르면, 블록체인을 기반으로 하는 DRM 서비스 시스템은 콘텐츠 등록 에이전트와, 블록체인 네트워크와, 사용자 에이전트를 포함한다.
- [0010] 콘텐츠 등록 에이전트는 서비스 제공자의 디지털 콘텐츠 등록 요청에 따라 표준 콘텐츠 식별자와 사용자 콘텐츠와 콘텐츠 속성과 콘텐츠 저작권 정보를 포함하는 트랜잭션을 생성하여 블록체인에 등록 요청한다.
- [0011] 블록체인 네트워크의 복수의 참여 노드는 합의 알고리즘에 따라 콘텐츠 등록 에이전트로부터 수신한 트랜잭션으로 블록을 생성하고 블록체인에 추가한다.
- [0012] 사용자 에이전트는 DRM 콘텐츠를 이용하기 위해 블록체인 네트워크에 연결하여 콘텐츠 정보를 획득한다.
- [0013] 과제를 해결하기 위한 제안된 발명의 또 다른 양상에 따르면, 블록체인을 기반으로 하는 DRM 서비스 시스템은 DRM 서버와, 콘텐츠 서버를 더 포함할 수 있다.
- [0014] DRM 서버는 DRM 서비스 제공에 필요하나 블록체인에 저장되지 않은 제2 콘텐츠 정보를 저장할 수 있다.
- [0015] 콘텐츠 서버는 DRM 정책 즉, DRM 종류에 따라 패키징된 콘텐츠를 저장하고 있으며 이용 권한을 가진 사용자 단말의 요청에 따라 콘텐츠를 배포할 수 있다.
- [0016] 과제를 해결하기 위한 제안된 발명의 일 양상에 따르면, 블록체인 기반의 DRM 시스템의 DRM 서비스 제공방법은 콘텐츠 등록 에이전트가 트랜잭션을 생성하는 단계와 생성된 트랜잭션을 블록체인 네트워크 상의 노드들에 전송하는 단계와, 블록체인 네트워크에 참여한 노드들이 합의 알고리즘에 따라 블록을 생성하는 노드를 선정하는 단계와 선정된 노드가 블록을 생성하고 로컬 저장소의 블록체인에 추가하는 단계와 생성된 블록을 다른 노드로 전송하는 단계와 수신된 블록을 검증하여 로컬 저장소의 블록체인에 추가하는 단계를 포함한다.

발명의 효과

- [0017] 제안된 발명에 따른 블록체인 기반의 DRM 서비스 시스템은 분산 원장 구조인 블록체인을 사용하여 중앙 시스템으로의 통신 부하 집중을 방지하여 네트워크의 효율성을 증대할 수 있다.
- [0018] 또한, 제안된 발명에 따른 블록체인 기반의 DRM 서비스 시스템은 블록체인에 콘텐츠 및 저작권 정보를 저장하여 다른 저작권 보호 기술에서도 활용이 가능한 방법을 제공할 수 있다.
- [0019] 또한, 제안된 발명에 따른 블록체인 기반의 DRM 서비스 시스템은 사용자가 구매한 콘텐츠에 대한 라이선스를 라이선스 발급 서버로부터 발급받아 블록체인에 저장하면 콘텐츠 액세스마다 다시 발급받을 필요 없이 블록체인으로부터 기 발급된 라이선스를 획득하는 방법을 제공할 수 있다.

도면의 간단한 설명

- [0020] 도 1은 일 실시 예에 따른 블록체인 기반의 DRM 서비스 시스템의 서비스 개념을 나타내는 도면이다.
- 도 2는 또 다른 실시 예에 따른 사용자 단말이 블록체인에 저장된 콘텐츠 라이선스를 획득하는 개념을 나타내는 도면이다.
- 도 3은 또 다른 실시 예에 따른 DRM 시스템이 블록체인 기반으로 서비스 제공하는 절차를 나타내는 절차도이다.

발명을 실시하기 위한 구체적인 내용

- [0021] 전술한, 그리고 추가적인 양상들은 첨부된 도면을 참조하여 설명하는 실시예들을 통해 구체화된다. 각 실시예

들의 구성 요소들은 다른 언급이나 상호간에 모순이 없는 한 실시예 내에서 다양한 조합이 가능한 것으로 이해된다. 블록도의 각 블록은 어느 경우에 있어서 물리적인 부품을 표현할 수 있으나 또다른 경우에 있어서 하나의 물리적인 부품의 기능의 일부 혹은 복수의 물리적인 부품에 걸친 기능의 논리적인 표현일 수 있다. 때로는 블록 혹은 그 일부의 실체는 프로그램 명령어들의 집합(set)일 수 있다. 이러한 블록들은 전부 혹은 일부가 하드웨어, 소프트웨어 혹은 이들의 결합에 의해 구현될 수 있다.

- [0022] 도 1은 일 실시예에 따른 블록체인 기반의 DRM 서비스 시스템의 서비스 개념을 나타내는 도면이다. 발명의 일 실시예에 따르면, 블록체인 기반의 DRM 서비스 시스템은 콘텐츠 등록 에이전트(100)와, 블록체인 네트워크(200)와, 사용자 에이전트(300)를 포함한다.
- [0023] 콘텐츠 등록 에이전트(100)는 서비스 제공자의 디지털 콘텐츠 등록 요청에 따라 콘텐츠 정보를 포함하는 트랜잭션을 생성하고, 생성된 트랜잭션을 블록체인 네트워크(200)에 참여한 노드들로 전송한다.
- [0024] 서비스 제공자는 이미지, 음성, 음향 및 영상 특히, UHD, IPTV, VOD 서비스를 제공하는 사업자로 디지털 콘텐츠를 DRM 시스템에 등록하여 제공한다.
- [0025] 따라서, 서비스 제공자는 콘텐츠 등록 에이전트(100)를 통해 디지털 콘텐츠 등록을 요청한다. 콘텐츠 등록 에이전트(100)가 생성하는 트랜잭션은 블록체인에 연결될 블록의 바디에 포함되는 일종의 거래 기록이다.
- [0026] 콘텐츠 등록 에이전트(100)는 생성된 트랜잭션을 블록체인 네트워크(200)의 노드들에게 전송한다. 즉, 새로운 트랜잭션이 발생했음을 블록체인 네트워크(200)의 모든 노드들에게 알린다. 블록체인 네트워크(200)에 참여한 모든 노드들이 동일한 거래 기록 즉, 트랜잭션을 보유하여야 하기 때문에 모든 노드들을 대상으로 브로드캐스팅한다. 발명의 양상에 따라서는 콘텐츠 등록 에이전트(100)는 특정 노드에만 생성된 트랜잭션을 전송하고, P2P(Peer to Peer) 네트워크 시스템인 블록체인 네트워크(200)에서 각 노드들이 서로 트랜잭션을 송수신해 버킷 릴레이와 같은 방식으로 데이터를 확산시킬 수 있다.
- [0027] 콘텐츠 등록 에이전트(100)는 서버로 구성되며 해당 서버의 프로세서에서 실행되는 명령어 세트로 구성되는 서버 프로그램 형태의 소프트웨어를 포함하는 개념이다.
- [0028] 블록체인 네트워크(200)는 로컬 저장소에 블록체인을 저장하고, 콘텐츠 등록 에이전트(100)로부터 트랜잭션들을 수신하여, 합의 알고리즘에 따라 블록을 생성하여 로컬 저장소의 블록체인에 추가하고 생성된 블록을 다른 노드로 전송하거나, 다른 노드가 생성한 블록을 검증하여 로컬 저장소의 블록체인에 추가하는 복수의 노드들을 포함한다.
- [0029] 블록체인 네트워크(200)는 발명의 양상에 따라서는 공개형과, 컨소시엄형과, 비공개형으로 구분될 수 있다.
- [0030] 공개형 블록체인은 운영주체와 참여자간 신뢰관계가 없다. 블록체인은 누구나 접근 가능하도록 공개되어 있으며, 트랜잭션을 발생시키고 전송시키는 권한도 제한이 없다. 블록체인 네트워크(200)에 참여자의 제한이 없으므로 블록을 생성하고 확인할 수 있는 권한 즉, 합의 알고리즘에 참여할 수 있는 권한도 누구에게나 있다. 합의 알고리즘은 일반적으로 작업 증명(Proof of Work, PoW) 또는 지분 증명(Proof of Stake, PoS)가 사용된다. 익명성을 보장하므로 블록체인 노드(210)에 대한 아이디 관리를 하지 않는다.
- [0031] 컨소시엄형 블록체인은 콘텐츠 사업자 및 저작권자 등으로 구성된 컨소시엄 멤버가 운영주체가 되며 참여자인 컨소시엄 멤버들간 신뢰관계가 있다. 블록체인 접근은 컨소시엄 멤버들에게만 권한이 주어지며 트랜잭션을 생성하고 전송하는 권한도 컨소시엄 멤버들에게만 있고 블록을 생성하고 확인할 수 있는 권한 즉, 합의 알고리즘에 참여할 수 있는 권한도 컨소시엄 멤버들에게만 있다. 합의 알고리즘으로 위임된 지분 증명(Delegated PoS, DPoS), PBFT(Practical Byzantine Fault Tolerance)가 사용된다. 인증 및 접근 제어를 위해 블록체인 노드(210)에 대하여 아이디 관리를 수행한다.
- [0032] 비공개형 블록체인은 콘텐츠 사업자 즉, 특정 운영주체가 존재하며 블록체인 접근 권한은 운영자에 의해 판단된다. 트랜잭션을 생성하고 전송하는 권한은 운영 주체 또는 특정 멤버가 가질 수 있으며 합의 알고리즘에 참여할 수 있는 권한은 운영 주체에만 있다. 합의 알고리즘으로 DPoS와 PBFT와 PoA(Proof of Authority)가 사용된다. 인증 및 접근 제어를 위해 블록체인 노드(210)에 대하여 아이디 관리를 수행하고 어떤 노드가 언제 어떤 블록체인에 데이터를 요청했는지를 기록한다.
- [0033] 블록체인 네트워크(200)는 운영하는 방식에 따라 공개형 블록체인과 컨소시엄형 블록체인과 비공개형 블록체인 중 하나의 아키텍처로 구성될 수 있으나 콘텐츠 정보와 라이선스 데이터와 콘텐츠 암호키 등이 트랜잭션에 포함

될 수 있으므로 단일 콘텐츠 사업자가 운영하는 경우에는 비공개형 블록체인을 적용하는 것이 바람직하다.

- [0034] 블록체인 네트워크(200)에 참여하는 노드는 복수로 구성되며, 시스템을 운용하는 규모에 따라 적절한 노드 수를 결정하여 시스템을 구성할 수 있다. 즉, 노드 수는 운용 규모에 따라 달라질 수 있으며 추후 운용 규모가 확장됨에 따라 노드를 추가할 수 있다.
- [0035] 블록체인 노드(210)는 자신의 로컬 저장소에 블록체인을 저장한다. 블록체인은 분산 원장 구조이므로 모든 노드는 동일한 블록체인을 저장한다. 로컬 저장소는 데이터를 저장할 수 있는 물리적 매체로 하드 디스크 또는 낸드 플래시 메모리와 이를 제어하는 컨트롤러로 구성된 대용량 저장장치인 SSD(Solid State Drive) 일 수 있다.
- [0036] 콘텐츠 등록 에이전트(100)로부터 트랜잭션을 수신한 노드는 트랜잭션을 검증하고 일정시간 동안 수신된 트랜잭션들을 모아 블록을 생성한다. 발명의 양상에 따라서는 노드는 다른 노드를 통해 트랜잭션을 수신할 수 있으며 수신한 트랜잭션을 검증하고 일정시간 동안 수신된 트랜잭션들을 모아 블록을 생성할 수 있다.
- [0037] 블록은 블록체인의 원소로서 개념적으로는 다수의 트랜잭션의 묶음을 의미하며 블록 헤더와 트랜잭션과 기타 정보로 구성된다. 발명의 일 양상에 따른 블록 헤더는 version, previousblockhash, merklehash, time, bits, nonce로 구성된다. version은 소프트웨어/프로토콜 버전이고, previousblockhash는 블록체인에서 바로 앞 블록의 블록 해쉬값이고, merklehash는 개별 트랜잭션의 해쉬값 구성되는 해쉬 트리의 루트에 해당하는 해쉬값이며 time은 블록이 생성된 시간이고 bits는 난이도 조절용 수치이며 nonce는 PoW 합의 알고리즘의 해답에 해당하는 값으로 PoW 이외의 합의 알고리즘에서는 사용되지 않는다.
- [0038] 블록 해쉬값은 블록의 식별자 역할을 하는 값으로 블록 헤더를 SHA256 해쉬 함수를 2회 적용해서 계산되는 값이다.
- [0039] 블록은 블록체인의 합의 알고리즘에 따라 결정된 노드가 생성한다. 예를 들어, 합의 알고리즘이 PoW인 경우에는 가장 빨리 해답을 찾은 노드가 생성 노드로 결정되고, 합의 알고리즘이 PoS인 경우에는 가장 많은 지분을 증명한 노드가 생성 노드로 결정되며, PBFT는 프라이머리 노드가 모든 참가자에게 요청을 보내고 그 요청에 대한 결과를 집계하여 블록을 확정하므로 프라이머리 노드가 생성 노드로 결정된다.
- [0040] 블록을 생성한 노드는 자신의 로컬 저장소에 저장된 블록체인에 생성된 블록을 추가하여 연결하고, 다른 노드들에 생성된 블록을 전송한다.
- [0041] 블록을 수신한 노드들은 수신한 블록을 검증하고 자신의 로컬 저장소에 저장된 블록체인에 생성된 블록을 추가하여 연결한다.
- [0042] 사용자 에이전트(300)는 블록체인 네트워크(200)에 연결하여 콘텐츠 정보를 획득한다. 발명의 일 양상에 따르면, 사용자 에이전트(300)는 사용자 단말에서 실행되는 프로그램 명령어 세트일 수 있다. 다만 이에 한정되는 것은 아니며 발명의 또 다른 양상에 따르면, 서버에 실행되는 사용자 에이전트(300) 기능을 수행하는 서버 프로그램을 포함하는 서버일 수 있다.
- [0043] 블록체인의 아키텍처에 따라서는 사용자 에이전트(300)가 블록체인에 접근하여 데이터를 획득할 수 있도록 운영자가 접근 권한을 할당 해주어야 한다.
- [0044] 사용자 에이전트(300)는 사용자 단말이 DRM 서비스를 이용할 때 중앙 시스템에만 통신 부하를 발생시키지 않고 블록체인에 저장된 콘텐츠 정보를 획득하도록 하여 중앙 시스템으로 집중되는 트래픽을 분산시킬 수 있다.
- [0045] 발명의 또 다른 실시 예에 따르면, 블록체인 기반의 DRM 서비스 시스템은 콘텐츠 등록 에이전트(100)와, 블록체인 네트워크(200)와, 사용자 에이전트(300)를 포함하고 DRM 서버와 콘텐츠 서버(400)를 더 포함할 수 있다.
- [0046] DRM 서버는 DRM 서비스 제공에 필요한 사용자 정보와 디바이스 정보를 포함하는 서비스 정보를 저장한다. DRM 서버는 블록체인에 저장되는 콘텐츠 정보 등을 제외한 DRM 서비스에 필요한 나머지 정보들을 저장하고 있어 블록체인이 모든 정보를 저장하지 않도록 하고 있다.
- [0047] 콘텐츠 서버(400)는 실제 콘텐츠 미디어가 저장되는 서버로, DRM 정책 즉, DRM 방식에 따라 암호화되고 패키징된 콘텐츠를 저장한다. 콘텐츠 서버(400)는 저장된 콘텐츠를 사용자 단말의 배포 요청에 따라 배포한다. 배포되는 콘텐츠는 암호화된 콘텐츠로 사용자가 암호키를 보유하여야 복호화 후 콘텐츠를 재생 또는 확인할 수 있다.
- [0048] 발명의 일 실시 예에 따르면, 블록체인 기반의 DRM 서비스 시스템의 트랜잭션에 포함되는 콘텐츠 정보는 표준 콘텐츠 식별자와 사용자 콘텐츠 식별자와 콘텐츠 속성과 콘텐츠 저작권 정보를 포함한다.

- [0049] 표준 콘텐츠 식별자와 사용자 콘텐츠 식별자는 선택적으로 사용될 수 있으며 사용자 에이전트(300)가 콘텐츠를 검색할 때 사용하는 콘텐츠 아이디로 사용된다.
- [0050] 표준 콘텐츠 식별자는 국제 표준 연속 간행물 번호(ISSN)와 디지털 객체 식별자(DOI)와 국제 표준 음악 작품 코드(ISWC)와 국제 표준 음악 번호(ISMN)와 국가 디지털 콘텐츠 식별체계(UCI) 중 어느 하나를 사용한다.
- [0051] ISSN(International Standard Serial Number)은 전 세계에서 생산되는 각종 연속 간행물의 식별을 위하여 국제적으로 표준화된 방법에 따라 부여하는 고유번호이다. ISSN은 연속간행물을 단순하고 유일하게 식별할 목적으로 고안되었다. 정기간행물을 유일하게 구별하여 등록하기 위해 UNESCO와 ICSU-AB의 작업에 의하여 만들어졌다. ISSN은 각 정기간행물의 유일한 식별자인 ISSN과 각 간행물에 붙여지는 유일한 이름인 key-title로 구성되며 ISO 3297의 국제표준으로 등록된 번호이다.
- [0052] DOI(Digital Object Identifier)는 인터넷 주소가 변경되더라도 사용자가 그 문서의 새로운 주소로 다시 찾아갈 수 있도록, 웹 파일이나 인터넷 문서에 영구적으로 부여된 식별자. 즉 서적에 매겨진 국제 표준 도서 번호(ISBN)와 같이 모든 디지털 객체에 부여되는 고유 식별 번호다. DOI에는 디지털 콘텐츠 소유, 제공자를 비롯하여 데이터에 관한 각종 정보가 입력되어 있어 디지털 콘텐츠의 주소나 위치가 바뀌어도 쉽게 찾을 수 있고, 저작자 보호와 콘텐츠의 유통 경로를 자동 추적하여 불법 복제를 막을 수 있도록 도와주는 식별자이다.
- [0053] ISWC(International Standard Musical Work Code)는 2001년 ISO TC46(문헌정보기술분과) SC9에서 표준코드로 제정한 국제시청각자료관리번호(ISO 15707)로서 추상적인 음악 작품 또는 문학 작품을 관리하기 위한 번호 체계로 초기에는 국제저작권관리단체연맹(CISAC)과 녹음권협회국제사무국(BIEM)이 음악 작품의 관리를 위해 제안되었다. 이후 문학작품에도 활용되었으며 1996년부터 CISAC에 의해 관리되고 있는 코드이다.
- [0054] ISMN(International Standard Music Number)은 국제 표준화 기구(ISO)가 악보에 부여하는 식별자이다. ISO 표준 번호는 ISO 10957이다.
- [0055] UCI(Universal Content Identifier)는 식별 가능한 자원의 효율적인 유통과 활용을 위하여 개별 자원에 유일하고 영구한 코드를 부여하고 이를 관리해주는 체계 또는 상이한 체계간의 연계표준으로 사용되는 식별자이다. UCI는 식별체계 구성요소인 구문구조, 메타데이터, 운영시스템, 운영절차 네 가지 요소가 서로 유기적으로 결합된 체계이며 URN(Uniform Resource Name)을 기반으로 디지털콘텐츠 유통 인프라 구축 및 활성화를 목표로 2000년에 한국전산원(NCA)에서 개발되었고 전반적인 UCI 운영을 담당하는 총괄기구, 디지털콘텐츠에 대한 식별정보를 등록받고 UCI를 부여하는 등록관리기관(RA), 그리고 자원에 대한 식별정보를 등록하는 등록자로 구성되며 현재 한국저작권위원회에서 UCI 식별체계의 총괄기구를 담당하고 있다.
- [0056] 사용자 콘텐츠 식별자는 콘텐츠 정보를 등록하는 사용자가 자신만의 콘텐츠 식별자로 각 콘텐츠를 구분하기 위해 임의로 정의한 콘텐츠 식별자이다.
- [0057] 콘텐츠 속성은 콘텐츠의 메타데이터로 콘텐츠의 종류와 콘텐츠의 포맷과 콘텐츠의 크기와 콘텐츠 데이터의 해쉬값과 콘텐츠의 위치 정보 즉, 콘텐츠 링크 정보를 포함한다.
- [0058] 콘텐츠 데이터의 해쉬값은 콘텐츠의 변조 여부를 확인하는 용도로 사용되며 콘텐츠의 위치 정보는 실제 콘텐츠 다운로드할 수 있는 주소이다.
- [0059] 도 2는 또 다른 실시 예에 따른 사용자 단말이 블록체인에 저장된 콘텐츠 라이선스를 획득하는 개념을 나타내는 도면이다. 발명의 또 다른 실시 예에 따른 블록체인 기반의 DRM 서비스 시스템의 트랜잭션은 콘텐츠 정보를 포함하고 사용자 정보와 콘텐츠 암호키와 라이선스 정보를 더 포함할 수 있다.
- [0060] 트랜잭션이 콘텐츠를 구매한 사용자 정보를 더 포함함으로써 사용자가 자신의 단말기로 단말기에 설치된 DRM 소프트웨어가 콘텐츠를 재생하려고 할 때 중앙 시스템에 액세스할 필요 없이 블록체인에서 콘텐츠 구매 여부를 확인할 수 있게 되어 중앙 시스템에 집중될 수 있는 트래픽을 분산하는 효과가 발생한다.
- [0061] 또한 트랜잭션이 콘텐츠를 복호화할 수 있는 콘텐츠 암호키를 더 포함함으로써 사용자가 중앙 시스템에 액세스하여 암호키를 획득하지 않고 블록체인을 통해 획득할 수 있게 되어 중앙 시스템에 집중될 수 있는 트래픽을 분산하는 효과가 발생한다.
- [0062] 또한 트랜잭션이 라이선스 정보를 매번 라이선스 발급 서버로부터 라이선스를 발급 받지 않더라도 블록체인으로부터 라이선스 정보를 획득하여 라이선스를 확인할 수 있다.
- [0063] 도 2를 참조하여 설명하면, 셋톱 박스 또는 노트북 등의 사용자 단말을 통해 시청할 콘텐츠에 대한 라이선스인

RO(Right Object)를 라이선스 발급 서버인 RI(Right Issuer) Server로부터 발급받고 사용자 단말을 통해 콘텐츠를 복호화 후 재생한다. 사용자가 이후 자신이 보유한 다른 단말기를 통해 동일한 콘텐츠를 재생하는 경우 기 발급된 라이선스 정보를 라이선스 발급 서버에 액세스할 필요 없이 블록체인에서 획득하여 동일한 콘텐츠를 재생할 수 있다. 발명의 또 다른 양상에 따르면, 콘텐츠의 재생 시간, 재생 회수를 더 포함하는 트랜잭션을 생성하여 블록체인에 추가하여 관리할 수 있다.

[0064] 발명의 또 다른 실시 예에 따른 블록체인 기반의 DRM 서비스 시스템의 사용자 에이전트(300)는 사용자 단말의 요청에 따라 콘텐츠의 식별자인 표준 콘텐츠 식별자 또는 사용자 콘텐츠 식별자로 블록체인에서 콘텐츠의 위치 정보를 검색하여 획득할 수 있다. 일 예로, 콘텐츠 A의 식별자를 ID-A라고 하면, 사용자 에이전트(300)는 블록체인에서 ID-A로 검색하여 콘텐츠 A의 실제 위치를 획득할 수 있다.

[0065] 발명의 또 다른 실시 예에 따른 블록체인 기반의 DRM 서비스 시스템의 사용자 에이전트(300)는 사용자 단말의 요청에 따라 콘텐츠의 식별자인 표준 콘텐츠 식별자 또는 사용자 콘텐츠 식별자로 블록체인에서 콘텐츠의 저작권 정보를 검색하여 획득할 수 있다. 일 예로, 콘텐츠 B의 식별자를 ID-B라고 하면, 사용자 에이전트(300)는 블록체인에서 ID-B로 검색하여 콘텐츠 B에 대한 저작권 정보를 획득할 수 있다.

[0066] 도 3은 또 다른 실시 예에 따른 DRM 시스템이 블록체인 기반으로 서비스 제공하는 절차를 나타내는 절차도이다. 발명의 또 다른 실시 예에 따르면, 콘텐츠 등록 에이전트(100)와, 다수의 노드들이 참여하는 블록체인 네트워크(200)와, 사용자 에이전트(300)와, 콘텐츠 서버(400)를 포함하는 DRM 시스템의 블록체인 기반의 DRM 서비스 제공 방법은 콘텐츠 등록 에이전트(100)가 서비스 제공자의 디지털 콘텐츠의 등록 요청에 따라 콘텐츠 정보를 포함하는 트랜잭션을 생성하는 단계와, 콘텐츠 등록 에이전트(100)가 생성된 트랜잭션을 블록체인 네트워크(200)에 참여한 노드들로 전송하는 단계와, 블록체인 네트워크(200)에 참여한 노드들이 콘텐츠 등록 에이전트(100)로부터 트랜잭션들을 수신하고 합의 알고리즘에 따라 블록을 생성하는 노드를 결정하는 단계와, 결정된 노드가 블록을 생성하고 로컬 저장소의 블록체인에 추가하는 단계와, 블록을 생성한 노드가 다른 블록체인 네트워크(200)에 참여한 다른 노드로 생성된 블록을 전송하는 단계와, 블록을 수신한 노드가 블록을 검증하여 로컬 저장소의 블록체인에 추가하는 단계를 포함한다.

[0067] 콘텐츠 등록 에이전트(100)가 서비스 제공자의 디지털 콘텐츠의 등록 요청에 따라 콘텐츠 정보를 포함하는 트랜잭션을 생성하는 단계의 서비스 제공자는 이미지, 음성, 음향 및 영상 특히, UHD, IPTV, VOD 서비스를 제공하는 사업자로 디지털 콘텐츠를 DRM 시스템에 등록하여 제공한다.

[0068] 콘텐츠 등록 에이전트(100)가 생성된 트랜잭션을 블록체인 네트워크(200)에 참여한 노드들로 전송하는 단계는 새로운 트랜잭션이 발생했음을 블록체인 네트워크(200)의 모든 노드들에게 알리기 위한 것이다. 블록체인 네트워크(200)에 참여한 모든 노드들이 동일한 거래 기록 즉, 트랜잭션을 보유하여야 하기 때문에 모든 노드들을 대상으로 브로드캐스팅한다. 발명의 양상에 따라서는 콘텐츠 등록 에이전트(100)는 특정 노드에만 생성된 트랜잭션을 전송하고, P2P 네트워크 시스템인 블록체인 네트워크(200)에서 각 노드들이 서로 트랜잭션을 송수신해 버킷 릴레이와 같은 방식으로 데이터를 확산시킬 수 있다.

[0069] 블록체인 네트워크(200)에 참여한 노드들이 콘텐츠 등록 에이전트(100)로부터 트랜잭션들을 수신하고 합의 알고리즘에 따라 블록을 생성하는 노드를 결정하는 단계에서 결정되는 노드는 합의 알고리즘에 따라 결정되는 방식이 다르다. 예를 들어, 합의 알고리즘이 PoW인 경우에는 가장 빨리 해답을 찾은 노드가 생성 노드로 결정되고, 합의 알고리즘이 PoS인 경우에는 가장 많은 지분을 증명한 노드가 생성 노드로 결정되며, PBFT는 프라이머리 노드가 모든 참가자에게 요청을 보내고 그 요청에 대한 결과를 집계하여 블록을 확정하므로 프라이머리 노드가 생성 노드로 결정된다.

[0070] 도 3을 참조하여 다시 설명하면, 콘텐츠 등록 에이전트(100)가 콘텐츠 정보를 포함하는 거래 정보에 해당하는 트랜잭션을 생성하고(S1000), 생성한 트랜잭션을 블록체인 노드(210)로 전송한다(S1020). 이때 발명의 양상에 따라서는 특정 노드에만 생성된 트랜잭션을 전송하고, P2P 네트워크 시스템인 블록체인 네트워크(200)에서 각 노드들이 서로 트랜잭션을 송수신해 버킷 릴레이와 같은 방식으로 데이터를 확산시킬 수 있다. 블록체인 네트워크(200) 블록체인 노드(210)들이 합의 알고리즘에 따라 수신된 트랜잭션을 포함하는 블록을 생성하는 노드를 결정하고(S1040), 결정된 노드가 블록을 생성하고 자기의 로컬 저장소의 블록체인에 추가하여 연결한다(S1060). 블록을 생성한 노드가 블록체인 네트워크(200) 내의 다른 노드들에 생성된 블록을 전송하고(S1080), 블록을 수신한 노드는 수신한 블록을 검증하고 자기의 로컬 저장소의 블록체인에 추가하여 연결한다(S1100). 이렇게 함으로써 모든 블록체인 노드(210)들이 동일한 블록체인을 보유하게 된다.

- [0071] 발명의 또 다른 실시 예에 따르면, 블록체인 기반의 DRM 서비스 제공 방법의 트랜잭션에 포함되는 콘텐츠 정보는 표준 콘텐츠 식별자와 사용자 콘텐츠 식별자와 콘텐츠 속성과 콘텐츠 저작권 정보를 포함한다.
- [0072] 표준 콘텐츠 식별자와 사용자 콘텐츠 식별자는 선택적으로 사용될 수 있으며 사용자 에이전트(300)가 콘텐츠를 검색할 때 사용하는 콘텐츠 아이디로 사용된다.
- [0073] 표준 콘텐츠 식별자는 국제 표준 연속 간행물 번호(ISSN)와 디지털 객체 식별자(DOI)와 국제 표준 음악 작품 코드(ISWC)와 국제 표준 음악 번호(ISMN)와 국가 디지털 콘텐츠 식별체계(UCI) 중 어느 하나를 사용한다.
- [0074] ISSN은 전 세계에서 생산되는 각종 연속 간행물의 식별을 위하여 국제적으로 표준화된 방법에 따라 부여하는 고유번호이고, DOI는 인터넷 주소가 변경되더라도 사용자가 그 문서의 새로운 주소로 다시 찾아 갈 수 있도록, 웹 파일이나 인터넷 문서에 영구적으로 부여된 식별자로 모든 디지털 객체에 부여되는 고유 식별 번호이고, ISWC는 ISO TC46(문헌정보기술분과) SC9에서 표준코드로 제정한 국제시청각자료관리번호(ISO 15707)로서 추상적인 음악 작품 또는 문학 작품을 관리하기 위한 번호 체계이고, ISMN은 국제 표준화 기구(ISO)가 악보에 부여하는 식별자이며 UCI는 식별 가능한 자원의 효율적인 유통과 활용을 위하여 개별 자원에 유일하고 영구한 코드를 부여하고 이를 관리해주는 체계 또는 상이한 체계간의 연계표준으로 사용되는 식별자이다.
- [0075] 사용자 콘텐츠 식별자는 콘텐츠 정보를 등록하는 사용자가 자신만의 콘텐츠 식별자로 각 콘텐츠를 구분하기 위해 임의로 정의한 콘텐츠 식별자이다.
- [0076] 발명의 또 다른 실시 예에 따르면, 블록체인 기반의 DRM 서비스 제공 방법의 콘텐츠 정보에 포함되는 콘텐츠 속성은 콘텐츠의 메타데이터로 콘텐츠의 종류와 콘텐츠의 포맷과 콘텐츠의 크기와 콘텐츠 데이터의 해쉬값과 콘텐츠의 위치 정보 즉, 콘텐츠 링크 정보를 포함한다.
- [0077] 콘텐츠 데이터의 해쉬값은 콘텐츠의 변조 여부를 확인하는 용도로 사용되며 콘텐츠의 위치 정보는 실제 콘텐츠 다운로드할 수 있는 주소이다.
- [0078] 발명의 또 다른 실시 예에 따르면, 블록체인 기반의 DRM 서비스 제공 방법의 트랜잭션은 콘텐츠 정보를 포함하고 사용자 정보와 콘텐츠 암호키와 라이선스 정보를 더 포함할 수 있다.
- [0079] 트랜잭션이 콘텐츠를 구매한 사용자 정보를 더 포함함으로써 사용자가 자신의 단말기로 단말기에 설치된 DRM 소프트웨어가 콘텐츠를 재생하려고 할 때 중앙 시스템에 액세스할 필요 없이 블록체인에서 콘텐츠 구매 여부를 확인할 수 있게 되어 중앙 시스템에 집중될 수 있는 트래픽을 분산하는 효과가 발생한다.
- [0080] 또한 트랜잭션이 콘텐츠를 복호화할 수 있는 콘텐츠 암호키를 더 포함함으로써 사용자가 중앙 시스템에 액세스하여 암호키를 획득하지 않고 블록체인을 통해 획득할 수 있게 되어 중앙 시스템에 집중될 수 있는 트래픽을 분산하는 효과가 발생한다.
- [0081] 또한 트랜잭션이 라이선스 정보를 매번 라이선스 발급 서버로부터 라이선스를 발급 받지 않더라도 블록체인으로부터 라이선스 정보를 획득하여 라이선스를 확인할 수 있다.
- [0082] 발명의 또 다른 실시 예에 따르면, 블록체인 기반의 DRM 서비스 제공 방법은 사용자 단말이 사용자 에이전트(300)를 통해 콘텐츠의 식별자인 표준 콘텐츠 식별자 또는 사용자 콘텐츠 식별자로 블록체인에서 콘텐츠의 위치 정보를 검색하여 획득하는 단계와, 사용자 단말이 블록체인 검색으로 획득한 콘텐츠의 위치 정보로 콘텐츠 서버(400)로부터 콘텐츠를 다운로드하는 단계를 더 포함할 수 있다.
- [0083] 일 예로, 콘텐츠 A의 식별자를 ID-A라고 하면, 사용자 단말은 사용자 에이전트(300)를 통해 블록체인에서 ID-A로 검색하여 콘텐츠 A의 실제 위치를 획득할 수 있고 사용자 단말은 콘텐츠 A의 실제 위치로부터 콘텐츠를 다운로드 할 수 있다.
- [0084] 발명의 또 다른 실시 예에 따르면, 블록체인 기반의 DRM 서비스 제공 방법은 사용자 단말이 사용자 에이전트(300)를 통해 콘텐츠의 식별자인 표준 콘텐츠 식별자 또는 사용자 콘텐츠 식별자로 블록체인에서 콘텐츠의 저작권 정보를 검색하여 획득하는 단계를 더 포함할 수 있다.
- [0085] 일 예로, 콘텐츠 B의 식별자를 ID-B라고 하면, 사용자 에이전트(300)는 블록체인에서 ID-B로 검색하여 콘텐츠 B에 대한 저작권 정보를 획득할 수 있다.
- [0086] 이상에서 본 발명을 첨부된 도면을 참조하는 실시예들을 통해 설명하였지만 이에 한정되는 것은 아니며, 이들로 부터 당업자라면 자명하게 도출할 수 있는 다양한 변형예들을 포괄하도록 해석되어야 한다. 특허청구범위는 이

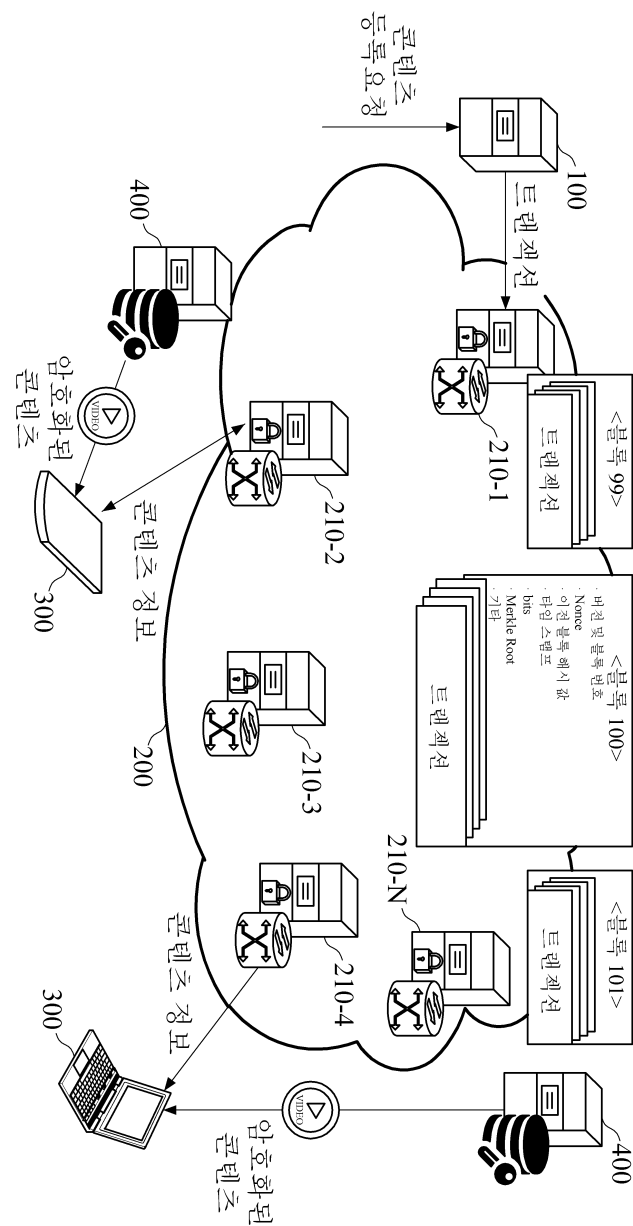
러한 변형예들을 포괄하도록 의도되었다.

부호의 설명

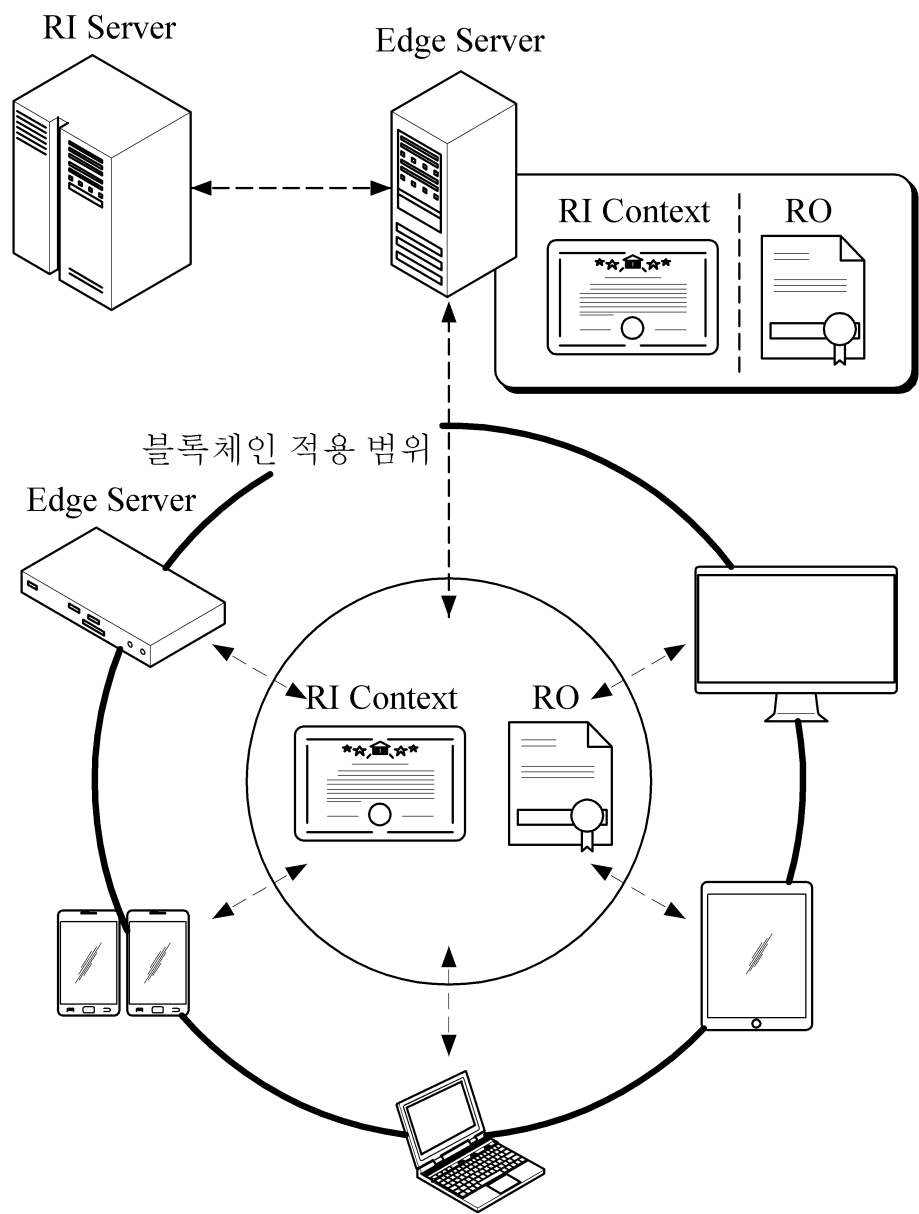
- 100 : 콘텐츠 등록 에이전트
- 200 : 블록체인 네트워크
- 210 : 블록체인 노드
- 300 : 사용자 에이전트
- 400 : 콘텐츠 서버

도면

도면1



도면2



도면3

