(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0110670
(43) 공개일자 2018년10월10일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 9/3239 (2013.01)
H04L 9/0891 (2013.01)
(21) 출원번호 10-2018-7022860
(22) 출원일자(국제) 2017년02월07일
심사청구일자 없음
(85) 번역문제출일자 2018년08월08일
(86) 국제출원번호 PCT/AU2017/050096
(87) 국제공개번호 WO 2017/136879
국제공개일자 2017년08월17일
(30) 우선권주장
2016900405 2016년02월08일 오스트레일리아(AU)

(71) 출원인
몰로니 린제이
오스트레일리아, 뉴 사우스 웨일즈 2000, 시드니, 요크 스트리트 65, 엘11, 씨/- 페이턴텍 페이턴트 어토니
스콧 가이
오스트레일리아, 뉴 사우스 웨일즈 2000, 시드니, 요크 스트리트 65, 엘11, 씨/- 페이턴텍 페이턴트 어토니
(72) 발명자
몰로니 린제이
오스트레일리아, 뉴 사우스 웨일즈 2000, 시드니, 요크 스트리트 65, 엘11, 씨/- 페이턴텍 페이턴트 어토니
스콧 가이
오스트레일리아, 뉴 사우스 웨일즈 2000, 시드니, 요크 스트리트 65, 엘11, 씨/- 페이턴텍 페이턴트 어토니
(74) 대리인
강명구

전체 청구항 수 : 총 30 항

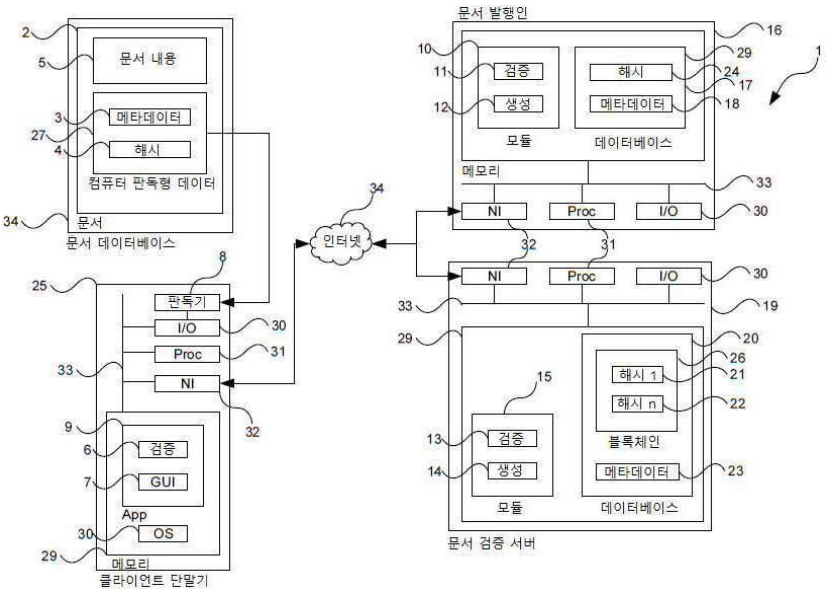
(54) 발명의 명칭 **문서 정보의 진본성을 검증하기 위한 시스템 및 방법**

(57) 요 약

등록된 훈련 기관에 의해 발행되는 코스의 수료 문서의 정보의 진본성을 검증하는 것, 여행 문서의 검증 및 진본성 검증을 필요로 하는 그 밖의 다른 민감한 문서, 예컨대 법률 회사, 회계 회사, 정부 기관 등에 의해 발행된 문서의 진본성을 검증하기 위한 시스템 및 방법이 제공된다. 상기 방법은 문서로부터 문서 내용 메타데이터를 수

(뒷면에 계속)

대 표 도



신하는 단계, 문서 내용 메타데이터를 이용해 메타 데이터 해시를 생성하는 단계, 메타데이터 해시를 포함하는 블록체인 트랜잭션을 생성하는 단계, 및 메타데이터 해시를 인코딩하는 컴퓨터 판독형 데이터를 생성하는 단계, 컴퓨터 판독형 데이터로 문서를 업데이트하는 단계를 포함하는 검증 레코드 생성 스테이지와, 문서를 수신하는 단계, 컴퓨터 판독형 데이터로부터 메타데이터 해시를 추출하는 단계, 및 블록체인의 블록체인 트랜잭션 내에서 메타데이터 해시를 식별하여 문서 메타데이터의 진본성을 검증하는 단계를 포함하는 문서 검증 스테이지를 포함할 수 있다.

(52) CPC특허분류

H04L 9/3247 (2013.01)

H04L 2209/38 (2013.01)

명 세 서

청구범위

청구항 1

문서 정보 진본성 검증을 위한 방법으로서, 상기 방법은

문서 내용 메타데이터를 문서로부터 수신하는 단계,

문서 내용 메타데이터를 이용해 메타데이터 해시를 생성하는 단계,

메타데이터 해시를 포함하는 블록체인 트랜잭션을 생성하는 단계,

메타데이터 해시를 인코딩하는 컴퓨터 판독형 데이터를 생성하는 단계, 및

컴퓨터 판독형 데이터로 문서를 업데이트하는 단계

를 포함하는 검증 레코드 생성 스테이지, 및

문서를 수신하는 단계,

컴퓨터 판독형 데이터로부터 메타데이터 해시를 추출하는 단계, 및

블록체인의 블록체인 트랜잭션 내 메타데이터 해시를 식별하여 문서 메타데이터의 진본성을 검증하는 단계

를 포함하는 문서 검증 스테이지

를 포함하는, 문서 정보 진본성 검증을 위한 방법.

청구항 2

제1항에 있어서, 상기 컴퓨터 판독형 데이터는 바코드인, 문서 정보 진본성 검증을 위한 방법.

청구항 3

제2항에 있어서, 상기 바코드는 2차원 바코드인, 문서 정보 진본성 검증을 위한 방법.

청구항 4

제1항에 있어서, 검증 레코드 스테이지는 문서 검증 서버와 연관된 개인 키로 문서를 서명하는 단계를 더 포함하는, 문서 정보 진본성 검증을 위한 방법.

청구항 5

제1항에 있어서, 문서 내용 메타데이터를 저장하는 단계를 더 포함하여, 문서 검증 스테이지가 문서 내용 메타데이터를 불러오는 단계 및 문서 내용 메타데이터를 디스플레이하는 단계를 더 포함하도록 하는, 문서 정보 진본성 검증을 위한 방법.

청구항 6

제5항에 있어서, 문서 내용 메타데이터를 저장하는 단계는 메타데이터를 컴퓨터 판독형 데이터 내에 인코딩하는 단계를 포함하는, 문서 정보 진본성 검증을 위한 방법.

청구항 7

제5항에 있어서, 문서 내용 메타데이터를 저장하는 단계는 메타데이터를 블록체인 트랜잭션 내에 인코딩하는 단계를 포함하는, 문서 정보 진본성 검증을 위한 방법.

청구항 8

제1항에 있어서, 검증 레코드 생성 스테이지는 문서로부터의 문서 내용 메타데이터의 식별을 더 포함하는, 문서

정보 진본성 검증을 위한 방법.

청구항 9

제8항에 있어서, 문서 내용 메타데이터의 식별은 광학 문자 인식을 포함하는, 문서 정보 진본성 검증을 위한 방법.

청구항 10

제9항에 있어서, 문서 내용 메타데이터의 식별은 광학 문자 인식을 이용해 추출되는 텍스트에 대한 검색 문자열 질의를 수행하는 단계를 포함하는, 문서 정보 진본성 검증을 위한 방법.

청구항 11

제9항에 있어서, 문서 내용 메타데이터의 식별은 문서의 적어도 하나의 사용자 정의 영역 내에 텍스트를 고립시키는 단계를 포함하는, 문서 정보 진본성 검증을 위한 방법.

청구항 12

제1항에 있어서,

문서에 대한 업데이트된 문서 내용 메타데이터를 수신하는 단계,

업데이트된 문서 메타데이터를 이용해 새로운 메타데이터 해시를 생성하는 단계,

새로운 메타데이터 해시를 포함하는 추가 블록체인 트랜잭션을 생성하는 단계

를 포함하는 문서 콘텐츠 업데이팅 스테이지를 더 포함하는, 문서 정보 진본성 검증을 위한 방법.

청구항 13

제12항에 있어서, 문서 검증 스테이지는

문서와 연관된 둘 이상의 블록체인 트랜잭션을 식별하는 단계를 포함하는, 문서 정보 진본성 검증을 위한 방법.

청구항 14

제13항에 있어서, 문서 검증 스테이지는 문서 내용 메타데이터가 업데이트된 문서 내용 메타데이터로 대체됨을 식별하는 단계를 더 포함하는, 문서 정보 진본성 검증을 위한 방법.

청구항 15

제14항에 있어서, 문서의 어느 부분이 대체되었는지를 식별하는 단계를 더 포함하는, 문서 정보 진본성 검증을 위한 방법.

청구항 16

제1항에 있어서,

철회 블록체인 트랜잭션을 생성하는 단계를 포함하는 문서 검증 철회 스테이지를 더 포함하여, 문서 검증 스테이지 동안, 방법은

블록체인 트랜잭션에 시간상 다음인 철회 블록체인 트랜잭션이 문서 정보의 진본성의 검증에 실패하는 것을 식별하는 단계를 더 포함하는, 문서 정보 진본성 검증을 위한 방법.

청구항 17

제1항에 있어서, 블록체인 트랜잭션이 유효성 주기를 더 특정하며, 문서 검증 스테이지 동안, 상기 방법은 유효성 주기가 만료된 경우 문서의 검증을 실패하는 단계를 더 포함하는, 문서 정보 진본성 검증을 위한 방법.

청구항 18

제17항에 있어서,

추가 유효성 주기를 포함하는 유효성 주기 갱신 블록체인 트랜잭션을 생성하는 단계를 더 포함하며, 문서 검증 스테이지 동안, 문서의 유효성을 결정할 때 추가 유효성 주기가 사용되는, 문서 정보 진본성 검증을 위한 방법.

청구항 19

문서 정보 진본성 검증을 위한 시스템으로서, 상기 시스템은

문서 정보 검증 서버 - 상기 문서 정보 검증 서버는

해시 블록체인, 및 단방향 해시 블록체인과 관련하여 저장되는 문서 메타데이터 테이블을 포함하는 데이터베이스,

문서 생성 모듈 및 문서 검증 모듈을 포함하는 소프트웨어 모듈을 포함함 - ,

문서 정보 검증 서버와 동작 가능하게 통신하는 클라이언트 단말기 - 상기 클라이언트 단말기는 컴퓨터 판독형 데이터 판독기, 상기 컴퓨터 판독형 데이터 판독기와 동작 가능하게 통신하며 문서 정보 검증 모듈을 포함하는 소프트웨어 애플리케이션을 포함함 -

를 포함하며, 사용될 때 상기 시스템은

문서 정보 검증 서버의 문서 생성 모듈,

상기 문서와 관련하여 문서 메타데이터를 수신하는 단계,

해싱 알고리즘을 이용해 문서 메타데이터로부터 단방향 해시를 수신 또는 생성하는 단계,

단방향 해시에 대해 단방향 해시 블록체인에 엔트리를 생성하는 단계,

문서 메타데이터 및 단방향 해시 중 적어도 하나를 포함하는 컴퓨터 판독형 데이터를 생성하는 단계, 및

컴퓨터 판독형 데이터를 문서 생성 모듈로 전송하는 단계

를 포함하는 검증 레코드 생성 스테이지, 및

클라이언트 단말기의 문서 정보 검증 모듈이 문서로부터 컴퓨터 판독형 데이터를 수신하는 단계,

클라이언트 단말기 및 문서 정보 검증 서버가 문서 메타데이터 및 컴퓨터 판독형 데이터로부터의 단방향 해시 중 적어도 하나를 식별하는 단계 - 문서 메타데이터만 수신하는 경우, 단방향 해싱 알고리즘을 이용해 단방향 해시를 생성함 - , 및

단방향 해시를 해시 단방향 해시를 위한 블록체인 내 엔트리와 비교함으로써 문서 정보 검증 서버의 문서 정보 검증 모듈이 문서를 검증하는 단계

를 포함하는 문서 정보 검증 스테이지를 위해 구성되는, 시스템.

청구항 20

제19항에 있어서, 상기 시스템은 문서 정보 검증 서버와 동작 가능하게 통신하는 문서 발행자 서버를 더 포함하는, 시스템.

청구항 21

제20항에 있어서, 문서 정보 검증 서버는 문서 발행자 서버로부터 문서 메타데이터를 수신하도록 구성되는, 시스템.

청구항 22

제20항에 있어서, 문서 정보 검증 스테이지는 클라이언트 단말기 및 문서 정보 검증 서버 중 적어도 하나가 문서의 추가 검증을 위해 단방향 해시 및 문서 메타데이터 중 적어도 하나를 문서 발행자로 전송하는 단계를 더 포함하는, 시스템.

청구항 23

제22항에 있어서, 상기 문서 발행자 서버는 해시 및 메타데이터 데이터 중 적어도 하나를 포함하는 데이터베이스를 포함하며, 추가 검증은 해시 및 문서 발행자 서버 데이터베이스 내 메타데이터 데이터 중 적어도 하나를 교차-참조하는 것을 포함하는, 시스템.

청구항 24

제19항에 있어서, 문서 정보 검증 서버의 문서 정보 검증 모듈은 검증 결과를 클라이언트 단말기로 전송하도록 더 구성되는, 시스템.

청구항 25

제24항에 있어서, 클라이언트 단말기 소프트웨어 애플리케이션은 그래픽 사용자 인터페이스를 생성하도록 더 구성되며, 그래픽 사용자 인터페이스는 검증 결과를 디스플레이하도록 구성되는, 시스템.

청구항 26

제25항에 있어서, 그래픽 사용자 인터페이스는 적어도 문서 메타데이터의 서브세트를 디스플레이하도록 더 구성되는, 시스템.

청구항 27

제19항에 있어서, 상기 시스템은 복수의 문서 정보 검증 서버를 포함하고, 블록체인은 복수의 문서 정보 검증 서버에 걸쳐 분산된 분산 블록체인인, 시스템.

청구항 28

제19항에 있어서, 컴퓨터 판독형 데이터를 생성하는 단계는 광학 컴퓨터 판독형 데이터를 생성하는 단계를 포함하는, 시스템.

청구항 29

제28항에 있어서, 상기 컴퓨터 판독형 데이터는 2D 바코드인, 시스템.

청구항 30

제19항에 있어서, 컴퓨터 판독형 데이터를 문서로 삽입하는 것을 더 포함하는, 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 문서 정보 진본성(authenticity) 검증과 관련되며, 구체적으로 시스템 및 방법과 관련되며, 특히 그러나 비제한적으로, 등록된 훈련 기관에 의해 발행된 코스 수료 확인 문서의 정보 진본성을 검증하는 것, 여행 문서의 검증 및 그 밖의 다른 진본선 검증을 요하는 민감한 문서, 가령, 법률 회사, 회계 회사, 정부 기관 등이 발행한 문서의 검증을 포함하는 문서 정보 진본성 검증을 위한 시스템 및 방법과 관련된다.

[0002] 또한 본 명세서에 기재된 진본성 검증 기법은 상이한 문서 매체, 가령, 하드카피(즉, 종이, 스마트 카드 여행 문서) 및 소프트카피(즉, 전자 포맷, 가령, 문서 레포지토리에 저장되는 것을 포함해 PDF 포맷)에 대해 널리 적용될 수 있다.

배 경 기 술

[0003] 문서 진본성 검증은 예를 들어, 법적 문서, 개인 신원 문서, 인정 문서, 접속 문서 등에 포함된 정보의 진본성의 검증에 적용되기에 바람직하다.

[0004] 이들 문서의 문제점은 예를 들어 여기에 담긴 정보가 수정될 수 있다는 것인데, 가령, 인정이 잘못 주장되거나, 문서가 위조되는 등이 있다.

[0005] D1: US 2011/0161674 A1 (MING) 2011년 06월 30일은 문서에 대한 인증 정보가 문서 상에 인쇄되는 바코드로 인

코딩되는 자체-인증 문서를 생성하는 방법을 개시함으로써 이 문제를 해결하고자 한다. 해시(hash)가 인정 정보로부터 계산되고 서버로 전송되어 저장된다. 문서의 스캔된 카피가 인증될 때, 바코드가 판독되어 인증 정보를 추출할 수 있다. 타깃 해시가 추출된 인증 정보로부터 계산되고 검증을 위해 서버로 전송된다. 서버는 타깃 해시를 이전에 저장된 해시와 비교한다. 이들이 동일하지 않는 경우, 바코드는 변경되었던 것이다. 이들이 동일한 경우, 추출된 인증 정보가 사용되어 스캔된 카피를 인증할 수 있다. 문서 ID가 생성되고 서버로 전송될 수 있으며 서버에 의해 사용되어 저장된 해시를 인덱싱 또는 검색할 수 있다.

[0006] 그러나 D1은 서버가 오염될 수 있고 여기에 저장된 해시가 조작된 문서와 매칭되도록 수정될 수 있다.

[0007] 따라서 D1은 높은 보안 엄격성을 요하는 경우, 예컨대 탑승권, 개인 신원 문서 등에 사용되기에 적합하지 않다.

[0008] 따라서 본 발명은, 바람직한 실시예에서, 변경될 수 있는 방식으로 문서 검증 레코드를 저장하기 위해 분산 암호 기반 블록체인을 이용한다.

[0009] 이제, D2: "What is proof of existence?" [2016년 4월 20일에 인터넷에서 검색] <URL: https://web.archive.org/web/20151222163927/https://proofofexistence.com/about> 웨이백 머신(Wayback Machine)에 따라 2015년 12월 22일 개시 D2는 각자의 문서의 개별 암호 다이제스트를 블록체인에 저장함으로써 온라인 분산된 존재 증명을 저장하기 위한 블록체인을 개시한다.

[0010] D2는 전자 문서(가령, PDF)를 해싱하고 해시를 OP_RETURN 스크립트를 통해 특수 비트코인 트랜잭션으로 저장하는데, 이 트랜잭션은 해시를 인코딩/담는다. 이는 트랜잭션 출력을 provably unspendable로 마킹하고 적은 양의 데이터 이 경우, 문서의 해시에 D2의 트랜재션 모두를 식별하기 위한 마커를 더한 것이 삽입될 수 있도록 하는 비트코인 스크립팅 연산코드이다.

[0011] 그러나 D2는 문서 내 정보의 진본성을 검증하는 문제와 직접 관련되지 않고, 오히려 특정 시점에서 특정 문서가 특정 전자 포맷으로 존재함을 증명하는 것과 관련된다.

[0012] 따라서 D2는 문서가 조작되었는지 여부를 검출하는 데 사용될 수 없다.

[0013] 또한, D2는 전체 전자 문서를 해싱하고 따라서 하드카피 문서에 대해 사용될 수 없는데, 하드카피의 경우, D2의 시스템을 이용해 외양 일탈의 가벼운 인쇄, 스캐닝, 복사가 전체적으로 상이한 해시를 생성할 것이고 따라서 여기에 담긴 문서 정보가 검증될 수 없을 것이다.

[0014] 따라서 본 발명은, 바람직한 실시예에서, (D1의 문서 해시와 다른, 메타데이터 해시를 이용해 저장되는) 문서 내용 메타데이터를 검증의 토대로서 이용하고 따라서 하드카피 문서에 대해서도 사용될 수 있다.

[0015] 또한, D1 및 D2는 문서 정보가 문서가 검증 가능한 상태로 업데이트될 수 없다는 점에서 결함이 있다.

[0016] 예를 들어, D2를 이용해, 원본 문서에 대해 제1 비트코인 트랜잭션이 생성될 것이고, 상기 원본 문서가 업데이트된 경우 제1 비트코인 트랜잭션이 업데이트된 문서에 대해 생성될 것이다.

[0017] 그러나 D2를 이용할 때, 원본 문서가 대체되었음에도 불구하고 원본 문서와 변경된 문서 모두 유효한 것으로 나타날 것이다.

[0018] 반대로, 본 발명은 하나의 실시예에서 이러한 방식으로 문서 내용 필드를 업데이트하기 위한 목적으로 블록체인 업데이트 트랜잭션을 이용하고, 이러한 방식으로 문서 검증 스테이지 동안, 블록체인은 역 연대순으로 검사되어 문서 (또는 특정 문서 내용 정보 필드)가 대체되었는지 여부를 검출할 수 있다.

[0019] 덧붙여, D1과 D2 모두 검증이 지정 주기 동안 이뤄질 수 없다는 점에서 부족하다.

[0020] 반대로, 본 발명은 하나의 실시예에 따라 유효성 주기를 특정하는 블록체인 트랜잭션을 생성한다.

[0021] 또한 D1과 D2 모두 문서가 철회(revoke)될 수 없다는 점에서 결함이 있다.

[0022] 반대로, 본 발명은 하나의 실시예에 따라 철회-유형(revocation-type) 블록체인 트랜잭션을 이용해, 이전 검증 트랜잭션에 후속하는 철회-유형 트랜잭션에 의해 문서의 진본성의 철회가 검출될 수 있도록 한다.

[0023] 또한, D1과 D2는 시각적 비교를 위해 검증된 정보가 문서와 연계되어 디스플레이될 수 없다는 점에서 결함이 있다.

[0024] 반대로, 본 발명은 하나의 실시예에 따라, 메타데이터를 저장, 가령, 컴퓨터 판독형 데이터(즉, 2D 바코드)로

문서 자체 또는 블록체인 내에 저장하여, 나중에 정보가 추출되고 사용자에게 디스플레이될 수 있게 한다.

[0025] 임의의 선행 기술 정보가 본 명세서에 언급된 경우, 이러한 언급이 정보가 호주 또는 그 밖의 다른 나라에서 해당 분야의 일반적인 지식의 일부를 형성한다는 인정을 의미하는 것이 아님이 이해되어야 한다.

[0026] 따라서 상기의 내용을 고려하여, 하나의 실시예에 따라, 문서 정보 진본성 검증을 위한 방법이 제공되며, 상기 방법은 검증 레코드 생성 스테이지를 포함하며, 상기 스테이지는 문서로부터 문서 내용 메타데이터를 수신하는 것, 문서 내용 메타데이터를 이용해 메타데이터 해시를 생성하는 것, 메타데이터 해시를 포함하는 블록체인 트랜잭션을 생성하는 것, 및 메타데이터 해시를 인코딩하는 컴퓨터 판독형 데이터를 생성하는 것, 컴퓨터 판독형 데이터로 문서를 업데이트하는 것을 포함하며, 상기 방법은 문서 검증 스테이지를 포함하고, 상기 스테이지는 문서를 수신하는 것, 컴퓨터 판독형 데이터로부터 메타데이터 해시를 추출하는 것, 및 블록체인의 블록체인 트랜잭션 내 메타데이터 해시를 식별하여 문서 메타데이터의 진본성을 검증하는 것을 포함한다.

[0027] 알다시피, D1 또는 D2는 문서의 문서 정보에 대한 메타데이터 해시의 생성, 연관된 블록체인 트랜잭션의 생성 및 메타 윌 데이터 해시에 의한 컴퓨터 판독형 데이터(즉, 2D 바코드)의 업데이트를 개시하지 않는다.

[0028] 컴퓨터 판독형 데이터는 바코드일 수 있다.

[0029] 바코드는 2차원 바코드일 수 있다.

[0030] 검증 레코드 스테이지는 문서 검증 서버와 연관된 개인 키로 문서에 서명하는 단계를 더 포함할 수 있다.

[0031] 방법은 문서 내용 메타데이터를 저장하는 단계를 더 포함할 수 있으며, 문서 검증 스테이지는 문서 내용 메타데이터를 불러오는 단계 및 문서 내용 메타데이터를 디스플레이하는 단계를 더 포함할 수 있다.

[0032] 문서 내용 메타데이터를 저장하는 단계는 컴퓨터 판독형 데이터 내에 메타데이터를 인코딩하는 단계를 포함할 수 있다.

[0033] 문서 내용 메타데이터를 저장하는 단계는 블록체인 트랜잭션 내에 메타데이터를 인코딩하는 단계를 포함할 수 있다.

[0034] 검증 레코드 생성 스테이지는 문서로부터의 문서 내용 메타데이터의 식별을 더 포함할 수 있다.

[0035] 문서 내용 메타데이터의 식별은 광학 문자 인식을 포함할 수 있다.

[0036] 문서 내용 메타데이터의 식별은 광학 문자 인식을 이용해 추출된 텍스트에 대한 검색 문자열 질의를 수행하는 것을 포함할 수 있다.

[0037] 문서 내용 메타데이터의 식별은 문서의 적어도 하나의 사용자 정의된 영역 내 텍스트를 고립시키는 단계를 포함할 수 있다.

[0038] 상기 방법은 문서에 대한 업데이트된 문서 내용 메타데이터를 수신하는 단계, 업데이트된 문서 메타데이터를 이용해 새 메타데이터 해시를 생성하는 단계, 새 메타데이터 해시를 포함하는 추가 블록체인 트랜잭션을 생성하는 단계를 포함하는 문서 내용 업데이팅 스테이지를 더 포함할 수 있다.

[0039] 문서 검증 스테이지는 문서와 연관된 둘 이상의 블록체인 트랜잭션을 식별하는 단계를 포함할 수 있다.

[0040] 문서 검증 스테이지는 문서 내용 메타데이터가 업데이트된 문서 내용 메타데이터에 의해 대체될 수 있음을 식별하는 단계를 더 포함할 수 있다.

[0041] 상기 방법은 어느 문서가 대체될 수 있는지를 식별하는 단계를 더 포함할 수 있다.

[0042] 상기 방법은 철회 블록체인 트랜잭션을 생성하는 단계를 포함하는 문서 검증 철회 스테이지를 더 포함할 수 있으며, 문서 검증 스테이지 동안, 방법은 블록체인 트랜잭션에 시간상 다음인 철회 블록체인 트랜잭션이 문서 정보의 진본성의 검증에 실패하는 것을 식별하는 단계를 더 포함할 수 있다.

[0043] 블록체인 트랜잭션이 유효성 주기를 더 특정하며, 문서 검증 스테이지 동안, 상기 방법은 유효성 주기가 만료된 경우 문서의 검증을 실패하는 단계를 더 포함할 수 있다.

[0044] 상기 방법은 추가 유효성 주기를 포함하는 유효성 주기 갱신 블록체인 트랜잭션을 생성하는 단계를 더 포함할 수 있으며, 문서 검증 스테이지 동안, 문서의 유효성을 결정할 때 추가 유효성 주기가 사용될 수 있다.

[0045] 또 다른 양태에 따르면, 문서 정보 진본성 검증을 위한 시스템이 제공되며, 상기 시스템은 문서 정보 검증 서버

- 상기 문서 정보 검증 서버는 해시 블록체인, 및 단방향 해시 블록체인과 관련하여 저장되는 문서 메타데이터 테이블을 포함하는 데이터베이스, 문서 생성 모듈 및 문서 검증 모듈을 포함하는 소프트웨어 모듈을 포함함 - , 문서 정보 검증 서버와 동작 가능하게 통신하는 클라이언트 단말기 - 상기 클라이언트 단말기는 컴퓨터 판독형 데이터 판독기, 상기 컴퓨터 판독형 데이터 판독기와 동작 가능하게 통신하며 문서 정보 검증 모듈을 포함하는 소프트웨어 애플리케이션을 포함함 - 를 포함할 수 있으며, 사용될 때 상기 시스템은 문서 정보 검증 서버의 문서 생성 모듈, 상기 문서와 관련하여 문서 메타데이터를 수신하는 단계, 해싱 알고리즘을 이용해 문서 메타데이터로부터 단방향 해시를 수신 또는 생성하는 단계, 단방향 해시에 대해 단방향 해시 블록체인에 엔트리를 생성하는 단계, 문서 메타데이터 및 단방향 해시 중 적어도 하나를 포함하는 컴퓨터 판독형 데이터를 생성하는 단계, 및 컴퓨터 판독형 데이터를 문서 생성 모듈로 전송하는 단계를 포함하는 검증 레코드 생성 스테이지, 및 클라이언트 단말기의 문서 정보 검증 모듈이 문서로부터 컴퓨터 판독형 데이터를 수신하는 단계, 클라이언트 단말기 및 문서 정보 검증 서버가 문서 메타데이터 및 컴퓨터 판독형 데이터로부터의 단방향 해시 중 적어도 하나를 식별하는 단계 - 문서 메타데이터만 수신하는 경우, 단방향 해싱 알고리즘을 이용해 단방향 해시를 생성함 - , 및 단방향 해시를 해시 단방향 해시를 위한 블록체인 내 엔트리와 비교함으로써 문서 정보 검증 서버의 문서 정보 검증 모듈이 문서를 검증하는 단계를 포함하는 문서 정보 검증 스테이지를 위해 구성될 수 있다.

[0046] 상기 시스템은 문서 정보 검증 서버와 동작 가능하게 통신하는 문서 발행자 서버를 더 포함할 수 있다.

[0047] 문서 정보 검증 서버는 문서 발행자 서버로부터 문서 메타데이터를 수신하도록 구성될 수 있다.

[0048] 문서 정보 검증 스테이지는 클라이언트 단말기 및 문서 정보 검증 서버 중 적어도 하나가 문서의 추가 검증을 위해 단방향 해시 및 문서 메타데이터 중 적어도 하나를 문서 발행자로 전송하는 단계를 더 포함할 수 있다.

[0049] 상기 문서 발행자 서버는 해시 및 메타데이터 데이터 중 적어도 하나를 포함하는 데이터베이스를 포함하며, 추가 검증은 해시 및 문서 발행자 서버 데이터베이스 내 메타데이터 데이터 중 적어도 하나를 교차-참조하는 것을 포함할 수 있다.

[0050] 문서 정보 검증 서버의 문서 정보 검증 모듈은 검증 결과를 클라이언트 단말기로 전송하도록 더 구성될 수 있다.

[0051] 클라이언트 단말기 소프트웨어 애플리케이션은 그래픽 사용자 인터페이스를 생성하도록 더 구성되며, 그래픽 사용자 인터페이스는 검증 결과를 디스플레이하도록 구성될 수 있다.

[0052] 그래픽 사용자 인터페이스는 적어도 문서 메타데이터의 서브세트를 디스플레이하도록 더 구성될 수 있다.

[0053] 상기 시스템은 복수의 문서 정보 검증 서버를 포함할 수 있고, 블록체인은 복수의 문서 정보 검증 서버에 걸쳐 분산된 분산 블록체인일 수 있다.

[0054] 컴퓨터 판독형 데이터를 생성하는 단계는 광학 컴퓨터 판독형 데이터를 생성하는 단계를 포함할 수 있다.

[0055] 상기 컴퓨터 판독형 데이터는 2D 바코드일 수 있다.

[0056] 상기 시스템은 컴퓨터 판독형 데이터를 문서로 삽입하는 것을 더 포함할 수 있다.

[0057] 본 발명의 또 다른 양태가 또한 개시된다.

도면의 간단한 설명

[0058] 본 발명의 범위 내에 속할 수 있는 그 밖의 다른 임의의 형태에도 불구하고, 본 발명의 바람직한 실시예가 첨부된 도면을 참조하여, 단지 예시로서, 기재될 것이다.

도 1은 본 발명의 실시예에 따르는 문서 정보 진본성 검증을 위한 시스템을 도시한다.

도 2는 실시예에 따라 문서 정보 진본성 검증의 생성을 위한 예시적 방법을 도시한다.

도 3은 실시예에 따라 정식으로 생성된 문서 진본성 검증 레코드를 이용해 문서의 진본성을 검증하기 위한 예시적 방법을 도시한다.

도 4는 실시예에 따라 업데이트된 문서의 진본성을 검증할 수 있는, 문서 정보를 업데이트하기 위한 또 다른 방법을 도시한다.

도 5는 실시예에 따라 특정 문서의 진본성 레코드를 철회하기 위한 예시적 방법을 도시한다.

도 6은 본 발명의 실시예에 따라 도 1의 문서를 검증할 때 시스템의 클라이언트 단말기에 의해 디스플레이되는 예시적 그래픽 사용자 인터페이스를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0059] 본 발명에 따르는 원리의 이해를 촉진시키기 위해, 지금부터 도면에 도시된 실시예에 대한 참조가 이뤄질 것이며, 이를 설명하기 위해 특정 기재가 사용될 것이다. 그럼에도 본 발명의 범위의 어떠한 제한도 의도되지 않음이 이해될 것이다. 해당 분야의 통상의 기술자에게 자명할 본 명세서에 나타난 본 발명의 특징부의 임의의 변경 및 추가 수정, 및 본 발명의 원리의 임의의 추가 적용이 본 발명의 범위 내에 있는 것으로 간주될 것이다.

[0060] 문서 정보 진본성 검증을 위한 시스템과 관련된 구조물, 시스템 및 관련 방법이 개시 및 기재되기 전에, 본 발명은 다소 변동될 수 있기에 본 명세서에 개시된 특정 구성, 프로세스 단계, 및 물질에 한정되지 않음이 이해되어야 한다. 또한 본 명세서에서 사용되는 용어는 특정 실시예를 설명하기 위한 목적만으로 사용되며, 본 발명의 범위는 청구항 및 이의 균등물에 의해서만 한정될 것이기 때문에, 한정으로 의도된 것이 아니다.

[0061] 본 발명의 주 사항을 기재하고 주장할 때, 다음의 용어가 이하에서 제공되는 정의에 따라 사용될 것이다.

[0062] 본 명세서 및 청구항에서 사용될 때, 문맥상 명확히 달리 나타내지 않는 한, 단수 형태는 복수의 지시어를 포함한다.

[0063] 본 명세서에서 사용될 때, 용어 "~를 포함(comprising, including, containing)", "~를 특징으로(characterised by)" 및 이들의 문법적 균등물은 추가적인 언급되지 않은 요소 또는 방법 단계들을 배제하지 않는 포괄적 용어 또는 개방형 용어다.

[0064] 다음의 설명에서 상이한 실시예에서의 유사하거나 동일한 도면 부호는 동일하거나 유사한 특징부를 지칭한다.

[0065] 문서 정보 진본성 검증을 위한 시스템 아키텍처

[0066] 다시 도 1을 참조하면, 문서 정보 진본성 검증을 위한 시스템(1)이 도시되어 있다.

[0067] 이하의 기재에서 명백해지겠지만, 시스템(1)은 문서 조작, 자격증명의 위조 등을 감소 또는 제거하기 위해, 문서, 가령, 종이 기반 및 전자 문서, 특히, 이러한 문서가 디스플레이하는 정보의 진본성을 검증하도록 구성된다.

[0068] 제공된 예시적 아키텍처에서, 시스템(1)은 문서 검증 서버(19)를 포함한다. 이하에서 더 상세히 설명될 바와 같이, 문서 검증 서버(19)는 본 명세서에 기재되는 다양한 계산 처리 작업을 수행하기 위한 다양한 소프트웨어 모듈로 구성된다.

[0069] 하나의 실시예에서, 문서 검증 서버(19)는 물리적(가령, 랙 장착형) 컴퓨터 서버의 형태를 취할 수 있지만, 대안 실시예에서, 관련 서버가 AWS(Amazon Web Services)에 의해 구현될 수 있는 것과 같은 가상화된 서버 인스턴스의 형태를 취할 수 있다.

[0070] 더 상세히 설명될 바와 같이, 실시예에서, 문서 검증 서버(19)는 블록체인 렛저(ledger)의 카피를 유지하고 따라서 본 명세서에 기재된 문서 검증 서버(19)의 프로세스가 복수의 서버(19) 간에 공유될 수 있다.

[0071] 더 구체적으로, 문서 검증 서버(19)는 디지털 데이터를 처리하기 위한 프로세서(31)를 포함한다. 시스템 버스(33)를 통해 프로세서는 메모리 디바이스(29)와 동작 가능하게 통신한다.

[0072] 메모리 디바이스(29)는 디지털 데이터, 가령, 컴퓨터 프로그램 코드를 저장하도록 구성된다. 이러한 방식으로, 동작 동안, 프로세서(31)는 메모리 디바이스(29) 내에 저장된 명령을 인출 및 실행할 수 있고 메모리 디바이스(29) 상에 이러한 실행의 데이터 결과를 저장한다.

[0073] 메모리(29)는 휘발성(RAM) 및 비휘발성(HDD) 저장장치의 조합의 형태를 취할 수 있다.

[0074] 설명 편의를 위해, 도 1에서 메모리(29)는 복수의 소프트웨어 모듈(15) 및 데이터베이스 신경(20) 내 연계된 데이터로 구성되는 것으로 도시된다.

[0075] 보다시피, 소프트웨어 모듈(15)은 이하에서 더 상세히 기재되는 방식으로 검증 모듈(13)에 의해 추후 검증될 수 있는 문서 검증 레코드를 생성하기 위한 생성 모듈(14)을 포함할 수 있다.

[0076] 덧붙여, 데이터베이스 내에 나타나는 데이터는 설명 편의를 위해 문서 메타데이터(23)를 포함하는 것으로 도시

되며, 블록체인이 사용되는 실시예에서, 블록체인 데이터(26)가 다양한 검증된 문서의 문서 메타데이터(23)를 나타내는 복수의 문서 해시(21, 22)를 포함한다.

[0077] 문서 검증 서버(19)는 다양한 컴퓨터 주변장치, 가령, 사용자 인터페이스 주변장치 등과 통신하기 위한 I/O 인터페이스(30)를 더 포함한다.

[0078] I/O 인터페이스(30)는 데이터 저장 주변장치, 가령, USB 저장 디바이스와 더 인터페이싱할 수 있다. 이러한 방식으로, 컴퓨터 프로그램 코드 모듈(15)은 컴퓨터 판독형 매체에 저장될 수 있으며, I/O 인터페이스(30)(또는 네트워크 인터페이스(32))를 통해 검증 서버(19)로 업로드되어, 본 명세서에 기재된 특정 계산 처리 작업을 수행하도록 문서 검증 서버(19)를 설정할 수 있다.

[0079] 문서 검증 서버(19)는 도시된 시스템(1)에서 인터넷(34)으로 도시된 컴퓨터 네트워크를 통해 데이터를 전송 및 수신하기 위한 네트워크 인터페이스(32)를 더 포함한다. 이러한 방식으로, 문서 검증 서버(19)는 도 1에 도시된 타 컴퓨팅 액터와 동작 가능하게 통신할 수 있다.

[0080] 이와 관련하여, 시스템(1)은, 실시예에서, 문서 발행자 서버(document issuer server)(16)를 더 포함할 수 있다. 일반적으로, 문서 발행자 서버(16)는 본 명세서에 기재된 방식으로 진본성 검증을 요하는 민감한 문서를 발행하는 사람, 개체, 조직, 기관 등에 의해 사용된다.

[0081] 이와 관련하여, 문서 발행자는 문서 메타데이터(16)를 저장하고, 문서를 컴파일 및 생성하며, 문서를 인터넷(34) 등을 통해 저장 및 포워딩하기 위해 문서 발행자 서버(16)를 이용할 수 있다.

[0082] 이와 관련하여, 유사하게 문서 발행자 서버(16)는 검증 모듈(11) 및 생성 모듈(12)을 갖는 소프트웨어 모듈(10)을 포함할 수 있다. 또한, 문서 발행자 서버(16)는 문서 메타데이터(18) 및 연관된 해시(24)를 더 저장할 수 있다.

[0083] 따라서 실시예에서, 가령, 조직이 문서 검증을 격리된 방식으로 수행하기 위해 문서 발행자 서버(16)를 이용하는 경우 문서 발행자 서버(16)는 모든 문서 진본성 검증 작업 및 데이터를 수행할 수 있다.

[0084] 대안 실시예에서, 문서 발행자(16)는 (가령, 구독 API를 기초로) 문서 검증 작업의 전부 또는 적어도 일부를 수행하기 위해 문서 검증 서버(19)를 이용할 수 있다.

[0085] 시스템(1)은 문서 발행자 서버(16) 및 문서 검증 서버(19) 중 적어도 하나와 인터넷(34)을 통해 동작 가능하게 통신하는 클라이언트 단말기(25)를 더 포함한다.

[0086] 일반적으로, 클라이언트 단말기(25)는 문서의 진본성을 나타내는 정보를 디스플레이하기 위해 사용될 수 있다.

[0087] 하나의 실시예에서, 클라이언트 단말기(25)는 문서의 진본성을 검증하도록 사용자에 의해 사용될 수 있는 개인 컴퓨터 디바이스, 가령, 노트북, 모바일 통신 디바이스(가령, 스마트 폰 디바이스, 가령, Apple iPhone 등)의 형태를 가질 수 있다.

[0088] 보다시피, 클라이언트 단말기(25)는 인터넷(34)을 통해 통신하기 위한 네트워크 인터페이스(32)를 더 포함할 수 있다.

[0089] 클라이언트 단말기(25)가 모바일 통신 디바이스(25)의 형태를 갖는 실시예에서, 네트워크 인터페이스(32)는 셀룰러 네트워크, 가령, 3-5G 셀룰러 데이터 네트워크를 통해 데이터를 전송 및 수신할 수 있다.

[0090] 마찬가지로 클라이언트 단말기(25)는 디지털 데이터를 처리하기 위한 프로세서(31) 및 시스템 버스(33)를 통해 프로세서(31)와 동작 가능하게 통신하는 메모리 디바이스(29)를 포함한다.

[0091] 클라이언트 단말기(25)의 메모리(29)는 운영 체제(30) 가령, Apple OS 또는 Android 운영 체제를 더 포함할 수 있다.

[0092] 또한, 클라이언트 단말기(25)는 도시된 실시예에서 컴퓨터 판독형 데이터 판독기(8)와 인터페이싱할 수 있는 I/O 인터페이스(30)를 더 포함할 수 있다. 이와 관련하여, 그리고 이하에서 상세히 기재될 바와 같이, 판독기(8)는 문서(2)로부터 검증을 위해 컴퓨터 판독형 데이터(27)를 판독하여, 문서의 진본성을 검증할 수 있다.

[0093] 클라이언트 단말기(25)가 모바일 통신 디바이스의 형태를 취하는 실시예에서, 판독기(8)는 클라이언트 단말기(25)의 이미지 캡처/카메라 디바이스의 형태를 가질 수 있으며 컴퓨터 판독형 데이터(27)는 2차원(2D)(가령, QR(Quick Response)) 바코드의 형태를 가질 수 있다. 따라서 문서(2)를 검증하기 위해, 사용자는 문서(2)가 품

고 있는 2D 바코드의 이미지를 캡처하여, 클라이언트 단말기(25)가 진본성을 검증할 수 있게 할 수 있다.

[0094] 실시예에서, (모바일 통신 디바이스의 형태를 취하는) 클라이언트 단말기(25)는 소프트웨어 애플리케이션 스토어, 가령, Apple App 스토어 등으로부터 클라이언트 단말기(25)에 의해 설치 및 실행을 위해 다운로드될 수 있는 다운로드된 소프트웨어 애플리케이션 "앱(app)"(9)을 이용해 설정될 수 있다.

[0095] 이와 관련하여, 소프트웨어 애플리케이션(9)은 검증 모듈(6) 및 그래픽 사용자 인터페이스 모듈(7)을 포함하는 다양한 서브 모듈/소프트웨어 모듈을 포함할 수 있다.

[0096] 도 1은 시스템(1)에 의해 검증되는 문서(2)를 포함하는 시스템(1)을 더 도시한다. 앞서 언급된 바와 같이, 문서(2)는 하드 카피 및 소프트 카피 문서의 형태를 가질 수 있다. 후자의 경우, 소프트 카피(전자, 가령, PDF 포맷) 문서는 문서 데이터베이스(34)에 저장될 수 있다. 이와 관련하여, 특정 문서가 URL 및 문서 ID 또는 그 밖의 다른 고유 식별자, 가령, 문서 해시를 이용해 검색될 수 있다.

[0097] 도시된 바와 같이, 문서(2)는 문서 내용(5)을 포함할 수 있다. 또한, 문서(2)는 앞서 언급된 바와 같이, 문서(2) 상에 포함 또는 인쇄된 2D 바코드의 형태를 가질 수 있는 컴퓨터 판독형 데이터(27)를 포함할 수 있다. 따라서 컴퓨터 판독형 데이터(27)가 클라이언트 단말기(25)(또는 인터넷(34)을 가로지르는 그 밖의 다른 컴퓨팅 액터)에 의해 판독되어 이의 진본성이 검증될 수 있다.

[0098] 실시예에서, 컴퓨터 판독형 데이터(27)는 특정 적용예에 따라 문서 ID, 문서 메타데이터 해시(4) 또는 문서 메타데이터(3) 또는 이들의 조합을 포함할 수 있다.

[0099] 도 1에 제공된 컴퓨터 아키텍처는 설명 목적을 갖는 예시에 불과하다.

[0100] 특히, 도 1에 제공되는 특정 아키텍처는 문서 검증 서버(19)가 구독 기반으로 사용되도록 배치되어 다양한 문서 발행자, 사용자 등이 문서를 검증하기 위해 문서 검증 서버(19)에 의해 노출된 웹 기능을 선택적으로 액세스할 수 있다.

[0101] 그러나 특정 아키텍처는 동일한 문서 진본성 검증 작업 및 기능을 여전히 수행하면서 본 명세서에 기재된 실시예의 범위 내에서 수정될 수 있다.

[0102] 문서 진본성 레코드 생성을 위한 예시적 방법(35)

[0103] 상기의 계산 아키텍처를 일반적으로 기재하였고, 이제 문서 진본성 검증을 위한 시스템(1)의 사용을 위한 다양한 예시적 방법, 가령, 도 3에 나타난 문서 진본성 레코드 생성 방법(35)이 제공될 것이다.

[0104] 방법(35)은 추후 검증 단계에서 사용될 수 있는 문서 진본성 레코드를 생성하기 위해 사용된다.

[0105] 방법(35)은 예시에 불과하고 모든 실시예에 어떠한 기술적 한정도 부가하지 않음이 이해되어야 한다.

[0106] 방법(35)의 단계(39)에서, 문서 내용이 획득된다.

[0107] 문서(2)가 물리적 문서인 경우, 문서는 스캐너를 이용해 스캔될 수 있으며 문서 내용이 광학 문자 인식(OCR)을 이용해 획득될 수 있다.

[0108] 또는, 문서(2)가 소프트 카피 문서인 경우, 문서 내용이 전자 파일 시스템 문서 자체로부터 판독되거나(가령, 다양한 문서 메타데이터 또는 문서 내용을 판독함으로써 - 이 경우 문서 내용이 OCR을 이용해 인식될 수도 있음), 적절한 데이터베이스, 가령, 문서 발행자 서버(16)의 데이터베이스(17)로부터 검색될 수 있다.

[0109] 일반적으로, 문서 내용은 중요한 문서 내용(본 명세서에서 메타데이터 해시, 가령, MD5, SHA256 해시 또는 그 밖의 다른 적절한 단방향 해시로 해싱하는 메타데이터라고 지칭됨)이며, 이 중요한 문서 내용의 후속 변경 또는 수정이 시스템(1)에 의해 검출될 수 있다. 또 다른 실시예에서, 문서의 임의의 변경이 검출될 수 있도록 전체 문서가 문서 해시로 해싱될 수 있다.

[0110] 또한 이하에서 더 상세히 기재될 바와 같이, 시스템(1)은 문서 내용/메타데이터의 업데이트, 또는 진본성 인정의 철회 위한 기능을 포함할 수 있다.

[0111] 단계(40)에서, 다양한 메타데이터가 식별될 수 있다. 앞서 언급된 바와 같이, 메타데이터는 문서 내에 담긴 중요 정보를 나타낸다.

[0112] 예를 들어, 수료 확인 문서의 경우, 메타데이터는 발행 조직의 이름, 수료자의 이름 및 자격의 이름을 나타낼 수 있다. 또 다른 예를 들어, 탑승권의 경우, 메타데이터는 승객의 이름, 항공기 번호, 탑승 게이트, 여권

번호, 도착지 등을 나타낼 수 있다.

[0113] 실시예에서, 시스템(1)은 중요 메타데이터의 변조가 시스템(1)에 의해 검출될 수 있도록 메타데이터의 메타데이터 해시(4)를 생성하도록 구성된다. 또한, 메타데이터는 해싱되지 않은 포맷(평문 또는 암호화된 포맷)으로 유지되어 검증 동안 클라이언트 단말기(25)에 의한 후속 디스플레이를 가능하게 할 수 있다.

[0114] 단계(40)에서의 (특정 중요 문서 정보를 나타내는) 메타데이터의 사용이 하드 카피 문서의 경우 유용할 수 있는데 여기서 디스플레이되는 중요 정보가 검증을 위해 격리될 수 있다. 이러한 식으로, 문서의 진본성을 검증하기 위한 기능에 영향을 주지 않으면서, 문서는 또 다른 방식으로, 가령, 복사 및 스캐닝 수차를 포함시키는 방식, 차이 나는 레터헤드(letterhead) 상에 인쇄하는 방식 등으로 수정될 수 있다.

[0115] 그러나 앞서 언급된 바와 같이, 실시예에서, 특히, 전자 문서의 경우, 전자 데이터 파일의 전체 내용이 해싱되는 것을 대신하여 메타데이터는 문서로부터 반드시 격리될 필요는 없다. 특히, 이 실시예에서, 메타데이터를 해싱하는 것과 반대로, 전자 문서 파일이 해시, 가령, MD5, SHA256 해시 등일 수 있다. 실시예에서, 개별 메타데이터 해시 및 문서 해시가 사용되어 문서 또는 문서 내 민감한 메타데이터의 변형이 독립적으로 검출될 수 있다.

[0116] 실시예에서, 사용되는 메타데이터가 사용자에 의해 특정될 수 있다. 예를 들어, 문서 발행자 데이터베이스(29)로부터 사용되는 특정 메타데이터가 사용자에 의해 특정된다.

[0117] 메타데이터가 문서 자체로부터 추출되는 대안 실시예에서, 시스템(1)이 적절한 메타데이터를 추출(가령, OCR을 이용)할 수 있도록 검색 문자열 필터가 특정될 수 있다.

[0118] 예를 들어, 수료 확인 문서의 경우, 조직, 수료자, 및 자격의 이름만 검증 목적으로 메타데이터로서 유지되도록 특정되어, 그 밖의 다른 문서 내용이 문서의 메타데이터의 진본성을 검증하는 기능에 영향을 미치지 않은 채 수정될 수 있다.

[0119] 따라서, 다양한 검색 문자열이 사용되어 시스템(1)이 이들 메타데이터 필드를 추출할 수 있다.

[0120] 또 다른 실시예에서, (문서 내 문서 메타데이터의 위치를 나타내는) 문서 영역/사각형이 특정되어 시스템이 특정된 영역에서의 텍스트만 추출할 수 있다.

[0121] 단계(41)에서, 문서 ID가 획득 또는 생성될 수 있다. 바람직한 실시예에서, 문서 ID는 전역 고유(globally unique)(GUID)해서, 문서 ID 충돌을 방지 또는 실질적으로 없앨 수 있다.

[0122] 문서 ID는 검증을 위해 문서를 고유하게 식별하도록 사용될 수 있다. 예를 들어, 문서 ID는 문서 ID를 포함하는 URL을 이용하는 문서 데이터베이스(34)로부터 문서를 검색하는 데 사용될 수 있다. 또한 문서 ID는 문서를 철회하기 위해 문서를 업데이트하는 데 사용될 수 있다.

[0123] 실시예에서, 문서 ID는 시스템(1)에 의해 생성될 수 있다. 그러나 대안 실시예에서, 문서 ID 1은 문서 발행자, 가령, 수료 확인 문서를 발행하는 등록된 훈련 조직에 의해 순차적인 숫자로 제공될 수 있다.

[0124] 실시예에서, 문서 ID는 메타데이터 해시 또는 문서 해시의 일부로서 해싱되어, 문서 ID의 조작을 방지할 수 있다.

[0125] 그러나 특정 실시예에서, 문서 ID가 반드시 요구되지는 않는다. 예를 들어, 하드 카피 문서가 메타데이터의 해시를 나타내는 2D 바코드를 포함할 수 있으며, 상기 메타데이터는 문서에 의해 디스플레이되는 정보를 나타낸다. 따라서 반드시 문서 ID를 사용할 필요 없이 2D 바코드는 스캔되어 문서 내용을 검증할 수 있다.

[0126] 또 다른 실시예에서, 문서 파일 또는 메타데이터로부터 생성된 해시가 고유 문서 ID로서 역할 할 수 있다.

[0127] 단계(42)에서, 해시(4)가 생성된다. 바람직하게는, 해시는 단방향 해시, 가령, MD5, SHA256 등이다. 해시는 많을 수 있는 양의 정보를 작은 크기로 감소시키는 기능을 제공하지만, 중요한 것은 내용의 하나의 문자의 조작도 해시에 크게 영향을 미친다는 것이다.

[0128] 바람직한 실시예에서, 해시(4)는 메타 데이터 해시이며, 메타 데이터(중요 문서 정보)가 이 중요 문서 정보의 차후 변경을 검출할 수 있도록 해싱될 수 있다. 그러나 앞서 역시 언급된 바와 같이, 또 다른 실시예에서, 해시(4)는 전자 문서 파일의 문서 해시일 수 있다.

[0129] 그 밖의 다른 정보, 가령, 문서 ID가 해시(4) 내에서 해싱될 수 있다.

[0130] 실시예에서, 상기 정보의 조합이 해싱되어 해시(4)를 형성할 수 있다.

[0131] 바람직한 실시예에서, 시스템(1)은 해시(4)를 저장하기 위한 목적으로 블록체인을 이용해, 문서를 검증하는 변경 불가능하며 분산되고 신뢰되는 렛저(ledger)를 제공할 수 있다.

[0132] 특히, 도 1에 도시된 바와 같이, 문서 검증 서버(19)가 블록체인 렛저(26)의 카피를, 다른 문서 검증 서버(19)와 동기화될 수 있는 데이터베이스(20) 내에 저장할 수 있다.

[0133] 따라서 단계(43)에서 해시가 블록체인 트랜잭션에 추가되며, 그 후 블록체인 트랜잭션이 마이닝되고 블록체인 내 블록에 추가된다. 해시가 블록체인에 추가될 수 있는 다른 방식이 있는데, 가령, 비트코인 스크립팅 연산코드 내 비트코인 블록체인이 사용된다. 대안 실시예에서, 커스텀화된 블록체인이 적절한 데이터 필드를 포함하고 사용될 수 있다.

[0134] 따라서 문서를 검증할 때, 블록체인이 검사되어, (2D 바코드(27)로부터 스캔되거나 그때 그때 계산될 수 있는) 해시(4)가 블록체인 내에 있는지 여부를 확인할 수 있다.

[0135] 실시예에서, 전체 블록체인에서 해시가 검색될 수 있지만, 바람직한 한 실시예에서, 해시 발견 프로세스를 가속화하기 위해 개별 해시 인덱스가 사용될 수 있다.

[0136] 모든 실시예가 반드시 블록체인을 이용하는 것은 아님을 알아야 한다. 예를 들어, 문서 발행자 서버(16)가 공유 렛저의 사용 없이 문서의 독립된 검증을 가능하게 하기 위해 문서 메타데이터(18)(또는 문서 내용) 및 연관 문서 해시(24) 또는 문서 ID를 유지할 수 있다. 시스템(1)이 메타데이터(18)의 카피(가령, 사용자에 의한 시각적 비교를 위해 검증 프로세스 동안 메타데이터의 디스플레이를 가능하게 하기 위함)를 유지하고 (비록 블록체인을 이용해 피할 수 있는 데이터베이스(17) 조작에 대한 보안이 없을지라도) 메타데이터의 조작을 검출할 수 있도록 연관된 해시를 유지한다.

[0137] 단계(44)에서, 그 후 검증을 위해 문서와 함께 사용될 수 있는 컴퓨터 판독형 데이터는 생성될 수 있다.

[0138] 단계(46)에서, 컴퓨터 판독형 데이터가 가시적으로 또는 비가시적으로 문서에 삽입된다.

[0139] 앞서 언급된 하나의 실시예에서, 컴퓨터 판독형 데이터(27)가 문서 해시, 문서 ID 및 문서 메타데이터 중 하나 이상을 포함하는 2D 바코드의 형태를 가질 수 있다.

[0140] 바람직한 실시예에서, 컴퓨터 판독형 데이터(27)가 문서의 인쇄, 스캐닝 및 복사를 가능하게 하도록 가시적이다.

[0141] 예를 들어, 문서는 컴퓨터 판독형 데이터(27)를 가시적으로 디스플레이하도록 수정될 수 있는데, 가령, PDF 문서가 문서의 하단 우측에서 2D 바코드의 이미지를 포함하도록 수정된다. 이러한 방식으로, 추후 전자 문서 또는 이의 인쇄물을 검증할 때, 사용자는 스마트폰(25)의 카메라 디바이스를 이용해 2D 바코드의 이미지를 캡처하여 문서의 내용 또는 메타데이터를 검증할 수 있다.

[0142] 대안 실시예에서, 전자 형태로 단독으로 존재하는 전자 문서의 경우 컴퓨터 판독형 데이터(27)가 반드시 육안에 가시적일 필요는 없으며 예를 들어 문서의 메타데이터에 포함될 수 있다. 이러한 방식으로, 문서를 디스플레이할 때, 문서 디스플레이 소프트웨어가, 배경에서, 연관 메타데이터를 검사할 수 있으며 문서가 검증되었는지 여부에 대한 지시를 디스플레이할 수 있다.

[0143] 예를 들어, PDF 문서 메타데이터가 (앞서 언급된 바와 같이, 문서 메타데이터, 문서 ID 및 문서 해시 중 하나 이상을 포함할 수 있는) 컴퓨터 판독형 데이터(27)를 포함하도록 PDF 문서가 업데이트될 수 있다. 따라서 PDF 애플리케이션, 가령, Adobe Acrobat reader 내에 디스플레이될 때, PDF 소프트웨어는 컴퓨터 판독형 데이터(27)를 자동으로 검사하고 문서가 검증되었는지 여부에 대한 지시를 디스플레이할 수 있다.

[0144] 대안 실시예에서, 가령, 여행 문서 등에서 사용될 때, RFID가 사용될 수 있다.

[0145] 단계(46)에서, 문서가 전자 문서의 형태를 취하고, 문서는 디지털 서명되어 포함되거나 삽입된 컴퓨터 판독형 데이터의 조작 또는 변형을 방지할 수 있다.

[0146] 하나의 실시예에서, 다른 이들이 문서 검증 서버(19)가 연관된 공개 키를 이용해 문서를 서명했음을 차후 검증할 수 있도록 문서 검증 서버(19)는 개인 키를 이용해 문서를 서명할 수 있다.

[0147] 문서 진본성 검증을 위한 예시적 방법(36)

[0148] 도 2를 참조하여, 문서 진본성 검증을 위한 예시적 방법(36)이 존재한다. 이하의 설명으로부터 자명하겠지만, 연관된 컴퓨터 판독형 데이터(27)를 이용해 문서의 진본성을 검증하기 위해 방법(36)이 사용된다.

[0149] 방법(36)은 단계(47)에서 시작하며, 여기서 문서가 획득된다. 예를 들어, 물리적 문서가 수중에 획득될 수 있거나, 전자 문서가 파일 시스템으로부터 불러와 지거나 URL로부터 다운로드 등이 될 수 있다.

[0150] 단계(48)에서 문서와 연관된 컴퓨터 판독형 데이터가 스캔 또는 판독된다.

[0151] 2D 바코드의 형태로 된 컴퓨터 판독형 데이터(27)를 포함하는 물리적 문서의 경우, 바코드가 클라이언트 단말기(25)의 판독기(8)를 이용해 판독될 수 있다.

[0152] 전자 문서의 경우, 컴퓨터 판독형 데이터(27)가 문서 디스플레이 소프트웨어(가령 Adobe Acrobat)에 의해 불러와 질 수 있다.

[0153] 단계(49)에서, 해시가 컴퓨터 판독형 데이터(27)로부터 추출될 수 있다.

[0154] 컴퓨터 판독형 데이터가 문서 ID를 포함하는 경우, 문서 ID가 또한 컴퓨터 판독형 데이터로부터 불러와 져서, 문서를 불러오기 위해 사용되는 또는 문서와 연관된 문서 ID와 비교될 수 있다.

[0155] 단계(50)에서, 시스템(1)은 블록체인을 이용하며, 상기 블록체인에서 해시를 포함하는 트랜잭션을 포함하는 블록 및 실시예에서 연관된 문서 ID가 검사될 수 있다.

[0156] 블록체인 내에서 매칭되는 트랜잭션이 발견되는 경우 단계(51)에서 문서가 진본임을 가리키는 검증이 사용자에게 디스플레이될 수 있다.

[0157] 덧붙여, 단계(52)에서 메타데이터가 컴퓨터 판독형 데이터로부터 추출되고 클라이언트 단말기(25)에 의해 디스플레이되어, 사용자가 컴퓨터 판독형 데이터로부터 추출된 메타데이터를 문서 상에 디스플레이되는 메타데이터에 비교할 수 있게 한다.

[0158] 또 다른 특정 실시예에서, 메타데이터(23)가 검증 동안 블록체인(26)으로부터 불러와 질 수 있어서, 메타데이터(23)를 2D 바코드(27) 자체 내에 저장할 필요가 없게 하도록 메타데이터(23)가 블록체인(26) 자체 내에 저장될 수 있다.

[0159] 문서 메타데이터를 업데이트하기 위한 예시적 방법(37)

[0160] 도 4를 참조하면, 문서 메타데이터를 업데이트하기 위한 예시적 방법(37)이 도시된다.

[0161] 구체적으로, 실시예에서, 문서 메타데이터를 업데이트하기 위한 필요성이 발생할 수 있다.

[0162] 예를 들어, 탑승권의 경우, 게이트 변경이 발생할 수 있다. 또 다른 예를 들면, 수료 확인의 경우, 수료자의 이름이 결혼 전 성(maiden name)에서 변경될 수 있다.

[0163] 따라서 문서의 진본성을 검증하기 위한 기능을 유지할 수 있으면서 특정 문서 필드의 업데이트를 가능하게 하는 방법(37)이 사용될 수 있다.

[0164] 따라서 단계(52)에서, 업데이트될 문서에 대한 문서 ID(또는 그 밖의 다른 고유 식별자, 가령, 문서 또는 메타데이터 해시)가 생성 또는 획득될 수 있다.

[0165] 단계(54)에서, 업데이트된 메타데이터(또는 문서 내용)가 수신된다. 예를 들어, 업데이트된 메타데이터가 새로운 성(surname)을 포함할 수 있다.

[0166] 단계(55)에서 업데이트된 메타데이터(또는 업데이트된 문서 내용)가 해싱된다.

[0167] 이제, 단계(56)에서, 새로운 해시가 추가 트랜잭션을 이용해 블록체인에 추가된다.

[0168] 단계(57 - 59)에서, 문서는 새 컴퓨터 판독형 데이터(27)를 포함하도록 수정될 수 있다. 그러나 특히 이미 확산된 문서에 대해 2D 바코드(27)의 업데이트가 반드시 일어날 필요는 없다.

[0169] 따라서 차후 문서를 검증할 때, 블록체인 트랜잭션이 역 연대순으로 검사될 수 있으며, 여기서, 가장 최신 검증 트랜잭션이 현재 검증 트랜잭션으로 사용된다.

[0170] 또는, 해시가 더 최신 블록체인 트랜잭션이 존재하는 블록체인 트랜잭션과 연관된 문서로부터 추출되는 경우, 클라이언트 단말기(25)는 사용자에게 문서 메타데이터/내용에 데이터가 없고 문서는 대체되었음을 알릴 수

있다.

[0171] 실시예에서, 검증 결과가 문서가 대체되었음을 가리킬 수 있다. 그러나 또 다른 실시예에서 검증 결과가 어느 문서 내용 메타데이터가 대체되었는지를 가르킬 수 있다.

[0172] 예를 들어, 제1 블록체인 검증 트랜잭션을 만들 때, 문서 ID 및 원본 메타데이터 해시가 블록체인 내에 저장될 수 있다.

[0173] 그 후, 문서 메타데이터로의 업데이트를 수신할 때, 새 블록체인 트랜잭션이 문서 ID 및 (업데이트된 메타데이터를 나타내는) 새 메타데이터 해시를 포함하는 블록체인 내에 생성될 수 있다.

[0174] 따라서 문서의 차후 검증 동안, 컴퓨터 판독형 데이터(27)는 클라이언트 단말기(25)에 의해 판독되어 문서 ID 및 메타데이터 해시를 추출할 수 있다.

[0175] 그 후, 블록체인에서 문서 ID와 연관된 블록체인 트랜잭션이 검색될 수 있다.

[0176] 그러나 시스템(1)이 둘 이상의 트랜잭션을 식별하는 경우, 시스템(1)은 불러와 진 해시를 둘 이상의 트랜잭션에 비교하여 특정 트랜잭션이 현재 트랜잭션인지 또는 대체되었는지를 식별할 수 있다.

[0177] 문서 진본성 철회를 위한 예시적 방법(38)

[0178] 이제 도 5를 참조하여, 문서 진본성 철회를 위한 예시적 방법(38)이 도시된다.

[0179] 특히, 문서를 철회할 필요가 발생할 수 있다. 예를 들면, 수료 확인증을 수신한 사람이 자격을 부정하게 획득했다고 차후 발견될 수 있고 따라서 수료 확인증이 철회될 필요가 있다.

[0180] 블록체인 기술이 사용되는 경우, 블록체인으로부터 트랜잭션을 삭제하는 것이 가능하지 않다.

[0181] 따라서 방법(38)은 문서를 철회하기 위해 블록체인에 추가되는 철회 트랜잭션을 이용한다.

[0182] 구체적으로, 방법(38)은 단계(60)에서 시작하며 여기서 문서 ID(또는 그 밖의 다른 고유 식별자, 가령 문서 또는 메타데이터 해시)에 의해 식별되는 특정 문서에 대한 철회 요청이 수신된다.

[0183] 단계(61)에서, 철회 트랜잭션이 블록체인에 추가된다. 철회 트랜잭션이 트랜잭션 유형(비트코인 스크립팅 연산코드에 다시 저장될 수 있는 철회 트랜잭션 유형) 및 문서 ID에 의해 식별된다.

[0184] 따라서 추후의 검증 동안, 단계(62)에서 컴퓨터 판독형 데이터가 문서 및 문서 ID에 대해 수신되고 문서 해시가 이로부터 추출된다.

[0185] 단계(63)에서, 블록체인에서 매칭되는 문서 ID 또는 해시가 검색된다.

[0186] 그러나 블록체인 내에서 식별되는 임의의 검증 트랜잭션에 대해, 단계(63)에서, 시스템(1)은 문서 ID 또는 해시와 연관된 블록체인 내에서 다음 철회 트랜잭션을 식별하고 따라서 단계(64)에서 검증이 실패한다.

[0187] 유한 진본성 검증 주기

[0188] 실시예에서, 문서는 유한 진본성을 가질 수 있다. 여기서 예를 들면, 운전 면허증의 경우처럼 문서가 12달 동안만 유효할 수 있다.

[0189] 따라서 블록체인 내에 저장된 검증 트랜잭션이 (비트코인 스크립팅 연산코드에 다시 저장될 수 있는) 유효성 주기를 특정할 수 있다. 따라서 검증 동안, 시스템(1)은 검증 트랜잭션의 엔트리 날짜를 검사할 수 있고 현재 날짜가 유효성 주기를 초과하는 경우 검증에 실패한다.

[0190] 예를 들어, 시스템(1)이 블록체인 내에서 12달을 초과한 트랜잭션을 식별하지만 반면 검증 트랜잭션이 검증이 12달의 주기 동안 유효하다고 특정하며 시스템(1)이 문서와 연관된 어떠한 추가적인 시간상 다음 검증 트랜잭션도 식별할 수 없는 경우, 검증에 실패한다.

[0191] 이와 관련하여, 시간상 다음 블록체인 검증 트랜잭션의 추가를 통해 유효성 주기가 갱신될 수 있다.

[0192] 등록된 훈련 조직(RTO, registered training organisation)에 의해 발행된 수료 확인 문서의 검증을 위한 시스템(1) 아키텍처의 예시적 사용

[0193] 앞서 시스템(1) 아키텍처 및 연관된 방법이 기재되었으며, 이제 등록된 훈련 조직(RTO)에 의해 발행된 수료 확인 문서의 검증을 위해 사용되는 시스템(1)의 예시적 사용이 기재될 것이다.

[0194] 보다시피, 문서 발행자(RTO) 서버(16)는 복수의 소프트웨어 모듈(10)을 포함한다.

[0195] 본 명세서에 기재된 실시예에서, 소프트웨어 모듈(10)은 차후 검증을 위해 문서 레코드를 생성하기 위해 검증 레코드 생성 모듈(12)을 포함할 수 있다.

[0196] 또한 보다시피, 문서 정보 검증 서버(19)가 검증 레코드 생성 모듈(14)을 포함하는 복수의 소프트웨어 모듈(16) 자체를 포함할 수 있다.

[0197] 또한, 문서 발행자(RTO) 서버(16)의 소프트웨어 모듈(10)이 문서의 차후 검증을 위한 검증 모듈(11)을 더 포함할 수 있다.

[0198] 마찬가지로, 문서 정보 검증 서버(19)의 소프트웨어 모듈(15)이 문서를 검증하기 위한 검증 모듈(13)을 포함하며 이는 이하에서 더 상세히 기재될 것이다.

[0199] 앞서 언급된 바와 같이, 문서 발행자(RTO) 서버(16)와 문서 정보 검증 서버(19)의 기능가 단일 서버에 의해 구현되는 경우, 이러한 검증 및 생성 기능이 동일한 모듈에 의해 구현될 수 있다.

[0200] 이 예시적 실시예에서, James Smith라는 이름의 사람이 특정 RTO의 코스를 성공적으로 수료한다.

[0201] 코스를 수료한 후, 수료 확인 또는 코스의 세부사항이 RTO에 의해 기록된다.

[0202] 특히, 보다시피, 문서 발행자(RTO) 서버(16)가 데이터베이스(17)를 포함한다.

[0203] 또한 데이터베이스(17)는 James Smith가 수료한 코스와 관련된 다양한 정보 필드를 저장하도록 구성된 메타데이터(18) 또는 그 밖의 다른 유형의 구조화된 데이터를 포함할 수 있다.

[0204] 따라서, 다음의 정보가 데이터베이스(17)에 기록(record)될 수 있다:

[0205] a. 이름: James Smith

[0206] b. 발행일: 2007년 7월 7일

[0207] c. 문서 번호: 0007/07/2007

[0208] d. 발행 RTO: Allwest Training service

[0209] e. 국가 공급자 번호: 51925

[0210] f. 증명서의 유형: 수료 확인/코스

[0211] g. 서명인: Bob Cooper

[0212] h. 서명인 직급: 최고 경영자

[0213] 이제, 검증 레코드 생성 스테이지 동안, 상기 메타데이터의 해시가 생성된다. 하나의 실시예에서, 메타데이터는 예컨대 다음을 포함하는 문자열로 연결(concatenate)된다:

[0214] a. James Smith|19051983|M|007 007 007|0007/07/2007|Allwest Training service|51925|07072007|수료 확인|운반 트럭 조작 교육|Bob Cooper|최고 경영자

[0215] 그 후, 단방향 해시 알고리즘, 가령, MD5, SHA256 또는 그 밖의 다른 해시 알고리즘을 이용해 연결된 문자열이 해싱된다. 예를 들어 이러한 해시는 다음의 해시를 생성할 수 있다:

[0216] a. 25908e49524e4828190dae3d79b894eec7ec3e4843c8bca6ef9f384c679167bc

[0217] 그 후, 메타데이터 해시가 차후 문서 정보 검증을 위해 사용되도록 저장된다.

[0218] 구체적으로, 보다시피, 문서 정보 검증 서버(19)는 정보, 가령, 해시 데이터를 저장하기 위한 데이터베이스(20)를 포함한다.

[0219] 따라서 상기의 메타데이터 해시는 데이터베이스(20)에 삽입된다. 이러한 삽입은 가령, 주기 간격으로, 또는 요청이 있을 때 등, 문서 발행자(RTO) 서버(16)의 데이터베이스(17)로부터 메타데이터(또는 메타데이터 해시)를 수신하는 문서 정보 검증 서버(19)를 포함할 수 있다.

[0220] 본 명세서에 기재된 해싱 알고리즘이 본 명세서에 기재된 실시예의 범위 내에서 임의의 컴퓨팅 액터에 의해 수행될 수 있다. 다시 말하면, 예를 들어 문서 발행자(RTO) 서버(16) 또는 문서 정보 검증 서버(19)가 해싱을 수

행할 수 있다.

[0221] 바람직한 실시예에서, 데이터베이스(20)로의 부정한 해싱 엔트리의 삽입으로부터 사기(fraud)가 발생하는 것을 막기 위해, 각각의 해시 엔트리가 데이터베이스(20) 내 다른 해시 엔트리에 따라 검증 가능하도록 시스템(1)은 분산 공개 렛져 블록체인(26)을 구현할 수 있다.

[0222] 본 명세서에 기재된 실시예에서, 단일 문서 정보 검증 서버(19)에 의해 검증이 수행된다. 그러나 블록체인(26)이 복수의 서버(19)에 걸쳐 분산된 분산 블록체인일 수 있음을 알아야 한다.

[0223] 본 명세서에 기재된 실시예의 범위 내에서 임의의 분산 암호 기반 블록체인이 사용될 수 있음을 알아야 하며, 예를 들어 비트코인, 이더리움, 라이트코인 블록체인 등에서 사용되는 것 또는 이들과 유사한 것이 있다.

[0224] 이들 실시예에서, 각각의 RTO(16)("문서 정보 발행자") 및 문서 검증 서버(19)에 비트코인 지갑 주소일 수 있는 "발행자 주소"가 할당될 수 있다. 커패시터, 비트코인 블록체인 내 트랜잭션이 각자의 문서 발행자 서버(16) 또는 문서 검증 서버(19)와 고유하게 연관될 수 있다.

[0225] 실시예에서, 메타데이터가 문서 정보 검증 서버(19)의 데이터베이스(20) 내에 역시 저장될 수 있다. 이러한 방식으로, 해시(또는 문서 ID)를 가질 때, 메타데이터가 검색(look up)될 수 있다.

[0226] 이 실시예에서, 해시가 기본 키(primary key)로서 역할 할 수 있다. 그러나 문서 정보 검증 목적으로 해시만 포함하도록 데이터베이스(20)가 반드시 메타데이터(23)를 포함할 필요는 없음을 알아야 한다.

[0227] 이제, 해시와 메타데이터 중 적어도 하나를 포함하는 컴퓨터 판독형 데이터가 생성된다. 컴퓨터 판독형 데이터의 생성이 문서, 가령, 문서 및 여기에 저장된 문서 메타데이터의 진본성을 검증하기 위해 클라이언트 단말기(25)에 의해 차후 판독될 수 있는 종이-기반 또는 전자 문서(즉, PDF)인 수료 증명서로의 컴퓨터 판독형 데이터의 삽입을 가능하게 할 것이다.

[0228] 바람직한 실시예에서, 컴퓨터 판독형 데이터가 2D 바코드로 구현된다. 예를 들어, 2D 바코드 컴퓨터 판독형 데이터를 생성할 때, 다음의 포맷이 데이터 인코딩을 위해 사용될 수 있다:

[0229] a. [키_해시] || [이름] || [생년월일 DD/MM/YYYY] || [성별] || [DL 번호] || [문서 번호] || [발행 RTO] || [국가 제공자 코드 번호] || [발행일 DD/MM/YYYY] || [증명서의 유형] || [자격증의 유형] || [서명인] || [서명인 직위]

[0230] 이는 적절한 알고리즘을 이용해 다음의 2D 바코드로 생성될 수 있다:

[0231] 

[0232] 컴퓨터 판독형 데이터를 생성하면, 그 후 컴퓨터 판독형 데이터가 문서로 삽입 또는 문서 상에 인쇄된다.

[0233] 도 1에서 보다시피, James Smith가 수료한 코스에 대한 수료 증명서인 문서(2)가 도시되어 있다. 이 구체적 실시예에서, 문서(2)는 문서 발행자(RTO) 서버(16)에 의해 PDF 문서로 발행된다. 따라서 James Smith가 전자 PDF 문서(2)를 다양한 취업 목적으로 자신의 자격의 증거로서 이용할 수 있다.

[0234] 보다시피, 문서는 보통의 인간 판독 가능한 정보, 가령, 적어도 상기에서 기재된 메타데이터의 서브셋을 포함할 수 있는 문서 내용(5)을 포함할 수 있다. 그러나 앞서 언급된 바와 같이, 선행 기술에서 문서는 전자적으로 또는 물리적으로 편집되어 부정한 정보를 나타낼 수 있다.

[0235] 따라서 문서는, 컴퓨터 판독형 데이터(27)를 더 포함함으로써, 클라이언트 단말기(25)를 이용하여 검증될 수 있다. 보다시피, 문서(2)에 담긴 컴퓨터 판독형 데이터(27)는 메타데이터(3), 메타데이터 또는 문서 해시(4) 및 문서 ID 중 적어도 하나를 포함할 수 있다.

[0236] 실시예에서, 메타데이터(3)는 컴퓨터 판독형 데이터(27) 내에 인코딩되어, 검증을 위해 해시가 메타데이터로부터 계산될 수 있다. 또 다른 실시예에서, 해시(4)만 컴퓨터 판독형 데이터(27) 내에 인코딩되어, 메타데이터가 문서 정보 검증 서버(19)의 데이터베이스(20) 또는 문서 발행자(RTO) 서버(16)의 데이터베이스(17) 또는 블록체인으로부터 불러와 질 수 있다.

[0237] 보다시피, 클라이언트 단말기(25)는 본 명세서에 기재된 특징 및 기능을 구현하도록 구성된 소프트웨어 애플리케이션(9)을 포함한다. 앞서 언급된 바와 같이, 실시예에서, 클라이언트 단말기(25)는 모바일 통신 디바이스, 가령, 스마트폰 디바이스 등이다. 본 명세서에서, 클라이언트 단말기(25)는 실시예에서 모바일 폰 카메라의 형태를 가질 수 있는 판독기(8)를 포함할 수 있다.

[0238] 사용 중에, 클라이언트 단말기(25)의 동작이 클라이언트 단말기(25)에 의해 실행될 소프트웨어 애플리케이션(9)을, 가령, 소프트웨어 애플리케이션 스토어, 가령, Apple iTunes store 등으로부터 다운로드할 수 있다.

[0239] 보다시피, 소프트웨어 애플리케이션(9)은 클라이언트 단말기에 의해 구현되는 문서 정보 검증을 위한 기능을 구현하도록 구성된 검증 모듈(6) 및 사용자에게 다양한 정보를 디스플레이하기 위한 디스플레이를 위한 그래픽 사용자 인터페이스를 표시하기 위한 그래픽 사용자 인터페이스(GUI) 모듈을 포함할 수 있다.

[0240] 따라서 문서의 진본성을 검증하기 위해, 클라이언트 단말기 사용자는 판독기(8)를 이용해 문서 상에 제공되는 2D 바코드 컴퓨터 판독형 데이터(27)를 스캔할 것이다. 문서(2)로부터 컴퓨터 판독형 데이터를 수신하면, 클라이언트 단말기(25) 및 문서 정보 검증 서버(19) 중 적어도 하나가 메타데이터(3) 및 해시(4) 중 적어도 하나를 식별하도록 구성된다.

[0241] 바람직한 실시예에서, 클라이언트 단말기(25)의 GUI(7)가 메타데이터를 디스플레이할 수 있도록 메타데이터(3)가 컴퓨터 판독형 데이터(27) 내에 인코딩된다.

[0242] 추가 바람직한 실시예에서, 해시(4)와 메타데이터(3) 모두가 컴퓨터 판독형 데이터(27) 내에 인코딩되어, 클라이언트 단말기(25)가 인코딩된 메타데이터(3)를 이용하는 해싱 알고리즘을 이용해 해시를 생성하여, 인코딩된 해시(4)가 메타데이터(3)와 매칭됨을 적어도 검증할 수 있다. 실시예에서, 사설 해시 알고리즘이 사용되어 사기범들이 공지된 해싱 알고리즘을 이용해 해시를 부정하게 생성 및 인코딩하지 못하게 할 수 있다.

[0243] 또한, 클라이언트 단말기(25)가, 데이터 네트워크, 가령, 인터넷을 통해, 문서 정보 검증 서버(19)와 동작 가능하게 통신함으로써, 메타데이터(3) 및 해시(4) 중 적어도 하나를 검증을 위해 문서 정보 검증 서버(19)로 전송할 수 있다.

[0244] 문서 정보 검증 서버(19)는 클라이언트 단말기(25)로부터 수신된(또는 클라이언트 단말기(25)에 의해 판독된 메타데이터(3)로부터 계산된) 해시를 블록체인(26) 내에 저장된 해시 값에 비교하도록 구성된다.

[0245] 매칭됨이 발견되면, 문서 정보 검증 서버(19)가 문서 정보가 진본임을 검증하는 검증 결과를 클라이언트 단말기(25)로 다시 전송할 수 있다.

[0246] 또는, 어떠한 매칭도 발견되지 않는 경우, 검증 서버(19)가 문서 정보가 부정하거나 조작됐을 수 있음을 가리키는 비-검증 결과(non-verification result)를 클라이언트 단말기(25)로 전송하도록 구성된다.

[0247] 어느 경우라도, GUI(7)는 검증 결과를 클라이언트 단말기 사용자에게 디스프레이하도록 구성된다. 또한, GUI(7)는 연관된 메타데이터를 디스플레이할 수 있다.

[0248] 예를 들어, 도 6을 참조할 때, GUI(7)에 의해 디스플레이되는 예시적 인터페이스(28)가 도시되며, 여기서 문서가 검증된다. 보다시피, 인터페이스(28)는 다양한 메타데이터 및 문서 정보가 진본이라는 확인을 포함한다.

[0249] 실시예에서, 시스템(1)은 추가 검증을 구현하도록 구성되며, 여기서 (레코드가 업데이트 또는 철회된 경우) RTO 서버 데이터베이스(17)에 보유되는 레코드가 추가로 교차-참조된다. 특히, 교차-참조는 해시 및 메타데이터 중 적어도 하나를 이용해 수행될 수 있다. 보다시피, 실시예에서, 문서 발행자(RTO) 서버(16)의 데이터베이스(17)가 메타데이터(19)와 관련하여 해시 값(24)을 저장하도록 구성될 수 있다. 앞서 언급된 바와 같이, 이러한 해시 값(24)은 문서 정보 검증 서버(19)로부터 수신되거나 문서 발행자(RTO) 서버(16) 자체에 의해 계산될 수 있다. 앞서 언급된 바와 같이, 실시예에서, 데이터베이스(17)는 해시 값(24)을 반드시 포함할 필요는 없으며, 여기서 메타 데이터(18)는 교차-참조된다.

[0250] 메타데이터(18)가 교차-참조될 때, 클라이언트 단말기(25) 및 문서 정보 검증 서버(19) 중 적어도 하나가 문서 발행자(RTO) 서버(16)의 검증 모듈(11)로 데이터베이스(17) 내 저장된 데이터를 검증하기 위한 추가 질의를 전

송할 수 있다. 예를 들어, 클라이언트 단말기(25)는 RTO 서버(16)로 문서 번호를 전송하여, 문서 번호가 진짜임을 검증할 수 있다. 또 다른 교차-참조가 본 명세서에 기재된 실시예의 범위 내에서 이뤄질 수 있다.

[0251] 하드 카피 문서를 위한 시스템(1)의 예시적 사용

[0252] 하드 카피 문서를 위한 시스템(1)의 사용이 지금부터 기재될 것이다.

[0253] 구체적으로, 앞서 언급된 바와 같이, 하드 카피 문서의 문제가 시간에 따라 변하는 문서의 외관, 가령, 복사 수차에 의해 발생하는 것 등을 포함할 수 있다.

[0254] 따라서 이 예시적 사용에서, 외관의 변화에도 불구하고 하드 카피 문서를 검증할 수 있는 시스템(1)이 기재될 것이다.

[0255] 특히, 이 예시에서, 하드 카피 문서가 판매자, 구매자 및 증인에 의해 부서(countersign)된 매매 계약서이다. 하드 카피 문서는 번지수(lot number)로 판매, 식별되는 부동 자산을 더 특정한다.

[0256] 따라서 문서 검증 레코드를 생성하기 위해, 설명된 계약서가 스캐너를 이용해 스캔될 수 있고 그 후 시스템(1)이 문서의 OCR 인식을 수행하여, 매매 계약서로부터 관련 메타데이터를 식별할 수 있다. 이 예시에서, 관련 메타데이터는 판매자 및 구매자의 이름 및 번지수이다.

[0257] 따라서 시스템(1)은 문서로부터 이러한 메타데이터를 추출하도록 구성된다. 예를 들어, OCR을 이용해, 시스템(1)은 문자열 매칭 등을 이용하여 데이터로부터 이들 필드를 추출하도록 구성될 수 있다.

[0258] 대안적으로, 문서의 이미지 스캔이 클라이언트 단말기(25) 상에 디스플레이되어, 변호사가 가령 마우스를 이용해 연관된 텍스트 주위에 사각형을 드래그함으로써 검증될 메타데이터를 구분할 수 있다.

[0259] 덧붙여, 변호사에 의해 파일 시스템에 의해 생성된 문서 ID인 문서 ID가 특정될 수 있다.

[0260] 관련 메타데이터를 획득한 후, 시스템(1)은 메타데이터(및 실시예에서 문서 ID)를 해싱하고 블록체인 내에 검증 트랜잭션을 생성한다.

[0261] 덧붙여, 시스템(1)은 매매 계약서 상에 인쇄될 2D 바코드의 형태로 컴퓨터 판독형 데이터를 생성한다.

[0262] 2D 바코드는 메타데이터 해시(4), 문서 ID 및 메타데이터를 포함한다.

[0263] 그 후 매매 계약서가 복사되고 복사본이 공인중계사(conveyancer)에게 전송된다.

[0264] 그러나 복사 과정에서 약간의 시각적 수차가 발생한다.

[0265] 그럼에도, 매매 계약서를 검증하기 위해, 공인중계사가 공인중계사의 모바일 통신 디바이스(25)의 카메라를 이용해 문서의 이미지를 캡처한다.

[0266] 모바일 통신 디바이스(25)는 2D 바코드를 식별하고 메타데이터 해시 문서 ID 및 메타데이터를 2D 바코드로부터 추출하는 애플리케이션(9)을 포함한다.

[0267] 그 후 모바일 통신 디바이스(25)가 인터넷(34)을 통해 문서 검증 서버(19)로 검증 요청을 전송한다. 검증 요청은 해시를 포함하지만, 실시예에서 문서 ID를 더 포함할 수 있다.

[0268] 그 후 문서 검증 서버(19)가 블록체인의 검증 트랜잭션을 통해 검색하고 생성된 이전 검증 트랜잭션을 식별한다.

[0269] 그 후 문서 검증 서버(19)는 모바일 통신 디바이스(25)에 검증 응답을 전송하여, 모바일 통신 디바이스(25)가 검증 레코드가 존재한다는 지시를 디스플레이 할 수 있다.

[0270] 이제 하나의 실시예에서, 공인중계사의 모바일 통신 디바이스(25)가 2D 바코드로부터 추출된 메타데이터를 디스플레이할 수 있다. 따라서 공인중계사는 모바일 통신 디바이스(25)에 의해 디스플레이될 때 당사자의 이름 및 번지수를 문서 상에서 시각적으로 검사함으로써 이들의 일관성(consistency)을 보장할 수 있다.

[0271] 클라이언트 단말기(25)가 (바코드 내에서의 메타데이터의 조작을 방지하기 위해) 2D 바코드 내에 저장되는 메타데이터를 재-해싱(rehash)하여 생성된 해시가 2D 바코드의 해시와 매칭되는지 여부를 확인할 수 있다.

[0272] 또한, 초기 검증 트랜잭션 동안, 메타데이터가 또한 블록체인 내에 저장되어 메타데이터가 문서 검증 서버(19)로부터 디스플레이되기 위해 클라이언트 단말기(25)로 전송될 수 있다.

[0273] 대안적 실시예에서, 공인중계사에 의한 시각적 비교를 위해 메타데이터를 디스플레이하는 것과 반대로, 모바일 통신 디바이스가 (복사 수차에도 불구하고) 광학 문자 인식을 수행하여 문서로부터 텍스트를 판독하고 인식된 텍스트가 메타데이터와 매칭되는지 여부를 확인할 수 있다.

[0274] 예를 들어, 2D 바코드 또는 블록체인 내에 저장된 메타데이터의 경우, 클라이언트 단말기(25)가 OCR 텍스트를 검색하여, 이러한 메타데이터를 식별할 수 있다. 식별되지 않는 경우, 가령, 스캔된 문서가 동일한 번지수를 포함하지 않는 경우, 검증에 실패한다.

[0275] 실시예에서, 관련 메타데이터가 경계 내에서 구분지어지는데, 가령, 앞서 기재된 실시예에서, 변호사가 검증될 스크린 상에 디스플레이되는 메타데이터 위에 사각형을 그린다. 예를 들어, 번지수가 페이지의 중앙 상부에 위치하고 당사자들의 이름이 문서의 하단 좌측 우 모서리에 위치할 수 있다.

[0276] 따라서 검증 동안, 모바일 통신 디바이스(25)가 구분된 경계 내의 텍스트 만을 인식하고, 그 후 이들 구분된 경계부로부터 추출된 텍스트를 메타데이터에 비교하도록 구성된다. 카메라를 이용할 때, 모바일 통신 디바이스(25)는 배향을 위해 페이지 모서리를 식별하여 구분된 경계를 정확히 위치시킬 수 있다.

[0277] 탑승권의 검증을 위한 시스템(1) 아키텍처의 예시적 사용

[0278] 지금부터 탑승권의 검증을 위한 시스템의 예시적 사용이 기재될 것이다.

[0279] 구체적으로, 기존 탑승권 시스템에는 탑승권에 인쇄된 데이터가 조작될 수 있다는 문제가 존재한다. 또한, 데이터베이스 엔트리가 조작된 인쇄와 매칭되도록 수정되어, 체크인 동안 탑승 직원이 수정된 데이터베이스 엔트리와 매칭되도록 조작된 탑승권을 알아차리지 못할 수 있다.

[0280] 따라서 이 실시예에서, 탑승권을 초기에 인쇄할 때, 승객 레코드 컴퓨팅 시스템이 관련 메타데이터를 문서 검증 서버(19)로 전송한다.

[0281] 이 실시예에서, 관련 메타데이터는 탑승권 ID, 승객의 이름, 및 출발 게이트를 포함할 수 있다.

[0282] 문서 검증 서버(19)는 메타데이터를 해싱할 수 있고 블록체인 내 엔트리를 생성하며 탑승권 상에 인쇄되도록 2D 바코드를 승객 레코드 컴퓨팅 시스템으로 전송할 수 있다.

[0283] 이제, 출발 전에, 비행 스케줄 변경이 게이트 번호의 업데이트를 야기할 수 있다. 따라서 승객 레코드 컴퓨팅 시스템이 모든 영향 받는 승객을 식별하며, 이들 식별된 영향 받는 승객에 대해, 업데이트 통지를 문서 검증 서버(19)로 전송한다.

[0284] 예를 들어, 각각의 탑승권에 대해, 승객 레코드 컴퓨팅 시스템은 탑승권 ID 및 업데이트된 게이트 번호를 전송할 수 있다.

[0285] 각각의 업데이트에 대해, 문서 검증 서버(19)는 블록체인 내 새로운 엔트리를 생성한다.

[0286] 이제 체크인 동안, 탑승권의 2D 바코드가 스캔되고 탑승권 ID 및 메타데이터(승객 이름 및 게이트 번호)가 바코드로부터 추출된다. 하단에, 이러한 정보가 또한 탑승권 인쇄물로부터 OCR을 통해 불러와 질 수 있다.

[0287] 그 후 이러한 추출된 메타데이터가 검증을 위해 문서 검증 서버로 전송될 수 있다.

[0288] 실시예에서 탑승 게이트 컴퓨터가 블록체인의 카피를 유지하여 인터넷을 통한 문서 검증 서버(19)로의 시간 소모적인 질의를 피할 수 있다.

[0289] 승객을 또 다른 이름으로 대체하려는 시도가 있었다고 가정하면, 탑승권이 조작되었을 수 있어서 탑승권 상에 인쇄된 이름 및 승객 레코드 컴퓨팅 시스템 데이터베이스 내 연관된 엔트리를 변경할 수 있다. 2D 바코드 내에 저장된 메타데이터가 추가로 수정될 수 있다.

[0290] 그러나 이러한 이름 수정의 경우, 문서 검증 서버(19)가 블록체인 내에 저장된 해시에 대해 새로운 이름의 해시를 매칭하는 데 실패할 것이기 때문에 문서 검증 서버(19)에 의한 검증이 실패할 것이다.

[0291] 이제, 업데이트된 게이트 번호에 대해, 탑승권이 오래된 게이트 번호를 여전히 나타낼 수 있다.

[0292] 따라서, 2D 바코드 내에 인코딩되는 해시가 (오래된 게이트 번호를 여전히 나타내기 때문에) 오래됐을 것이다(obsolete).

[0293] 그러나 체크인에서, 승객 체킹 컴퓨터에 의해 문서 검증 서버(19)로 새로운 게이트 번호가 전송될 수 있으며,

이때, 문서 검증 서버(19)가 새로운 게이트 번호를 갖는 탑승권 ID와 관련된 또 다른 검증 트랜잭션을 식별하고 따라서 탑승권의 검증을 통과할 수 있다. 이와 관련하여, 블록체인 내 게이트 업데이팅 트랜잭션과 매칭되지 않는 그 밖의 다른 임의의 게이트 번호에 대해 검증이 실패할 것이다.

[0294] 해석

[0295] 무선(Wireless):

[0296] 본 발명은 다른 네트워크 표준에 따르고 그 밖의 다른 애플리케이션, 가령, 다른 WLAN 표준 및 그 밖의 다른 무선 표준을 위한 디바이스를 이용해 구현될 수 있다. 수용될 수 있는 애플리케이션은 IEEE 802.11 무선 LAN 및 링크, 및 무선 이더넷을 포함한다.

[0297] 본 명세서의 맥락에서, 용어 "무선" 및 이의 파생어는 비-고체 매체를 통해 변조된 전자기 복사의 사용을 통해 데이터를 통신할 수 있는 회로, 디바이스, 시스템, 방법, 기법, 통신 채널 등을 설명하는 데 사용될 수 있다. 일부 실시예에서 그렇지 않을 수 있지만, 용어가 연관된 디바이스가 어떠한 와이어도 포함하지 않음을 의미하는 것이 아니다. 본 명세서의 맥락에서, 용어 "유선(wired)" 및 이의 파생어는 고체 매체를 통해 변조된 전자기 복사를 사용하여 데이터를 통신할 수 있는 회로, 디바이스, 시스템, 방법, 기법, 통신 채널 등을 설명하는 데 사용될 수 있다. 용어는 연관된 디바이스가 전기적으로 전도성 와이어에 의해 연결됨을 의미하는 것은 아니다.

[0298] 프로세스:

[0299] 특정하게 달리 언급되지 않는 한, 다음의 설명으로부터 명백할 바와 같이, 명세서 전체에서 "프로세싱", "컴퓨팅", "계산", "결정", "분석" 등의 용어를 이용하는 것은 물리적, 가령, 전자, 양자로 표현되는 데이터를 물리적 양으로 유사하게 표현되는 다른 데이터로 조작 및/또는 변화하는 컴퓨터 또는 컴퓨팅 시스템 또는 유사한 전자 컴퓨팅 디바이스의 동작 및/또는 프로세스를 지칭함을 알아야 한다.

[0300] 프로세서:

[0301] 유사한 방식으로, 용어 "프로세서"는 가령, 레지스터 및/또는 메모리로부터 전자 데이터를 처리하여 전자 데이터를 그 밖의 다른 전자 데이터, 가령, 레지스터 및/또는 메모리에 저장될 수 있는 데이터로 변환하는 임의의 디바이스 또는 디바이스의 일부분을 지칭할 수 있다. "컴퓨터" 또는 "컴퓨팅 디바이스" 또는 "컴퓨팅 머신" 또는 "컴퓨팅 플랫폼"이 하나 이상의 프로세서를 포함할 수 있다.

[0302] 본 명세서에 기재되는 방법이, 하나의 실시예에서, 하나 이상의 프로세서에 의해 실행될 때 본 명세서에 기재된 방법들 중 적어도 하나를 실행하게 하는 명령 세트를 포함하는 컴퓨터-판독형(또는 기계-판독형) 코드를 수용하는 하나 이상의 프로세서에 의해 수행 가능하다. 발생될 동작을 특정하는 명령 세트를 (순차적으로 또는 그 밖의 다른 식으로) 실행할 수 있는 임의의 프로세서가 포함된다. 따라서 하나의 예시는 하나 이상의 프로세서를 포함하는 일반적인 프로세싱 시스템이다. 프로세싱 시스템은 메인 RAM 및/또는 정적 RAM 및/또는 ROM을 포함하는 메모리 서브시스템을 포함할 수 있다.

[0303] 컴퓨터-판독형 매체:

[0304] 또한, 컴퓨터-판독형 반송 매체는 컴퓨터 프로그램 프로덕트를 형성하거나 포함될 수 있다. 컴퓨터 프로그램 프로덕트가 컴퓨터 이용형 반송 매체 상에 저장될 수 있으며, 컴퓨터 프로그램 프로덕트는 프로세서로 하여금 본 명세서에 기재된 방법을 수행하게 하는 컴퓨터 판독형 프로그램 수단을 포함한다.

[0305] 네트워킹된 또는 복수의 프로세서:

[0306] 대안 실시예에서, 하나 이상의 프로세서가 독립형 디바이스로서 동작하거나 네트워킹된 배치로 또 다른 프로세서(들)에 연결, 가령, 네트워킹될 수 있으며, 하나 이상의 프로세서는 서버-클라이언트 네트워크 환경에서, 서버 또는 클라이언트 머신으로서 동작하거나 피어-투-피어 또는 분산 네트워크 환경에서 피어 머신으로서 동작할 수 있다. 하나 이상의 프로세서는 웹 기기, 네트워크 라우터, 스위치 또는 브릿지, 또는 기계가 취할 수 있는 동작을 특정하는 명령 세트를 (순차적으로 또는 그 밖의 다른 방식으로) 실행할 수 있는 임의의 기계를 형성할 수 있다.

[0307] 일부 도면이 단일 프로세서 및 컴퓨터 판독형 코드를 지니는 단일 메모리만 도시하고 있지만, 해당 분야의 통상의 기술자라면 앞서 기재된 구성요소들 중 다수가 포함되거나 본 발명의 양태를 모호하게 하지 않기 위해 명시적으로 도시되거나 기재되지 않음을 이해할 것이다. 예를 들어, 단 하나의 기계만 도시되었지만, "기계"는 본 발명의 방법들 중 임의의 하나 이상을 수행하기 위한 명령의 세트(또는 복수의 세트)를 개별적으로 또는 공동으

로 실행하는 기계의 임의의 집합을 포함하는 것으로 이해될 것이다.

[0308] 추가 실시예:

[0309] 따라서 본 명세서에 기재된 방법 각각의 실시예가 명령의 세트, 가령, 하나 이상의 프로세서 상에서 실행되기 위한 컴퓨터 프로그램을 지니는 컴퓨터 판독형 반송 매체의 형태이다. 따라서 해당 분야의 통상의 기술자에게 자명할 바와 같이, 본 발명의 실시예는 방법, 장치, 가령, 특수 장치, 데이터 처리 시스템 또는 컴퓨터 판독형 반송 매체 등의 장치로서 구현될 수 있다. 컴퓨터 판독형 반송 매체는 실행될 때 하나 이상의 프로세서로 하여금 프로세서 또는 프로세서들이 방법을 구현하게 하는 명령의 세트를 포함하는 컴퓨터 판독형 코드를 반송한다. 따라서 본 발명의 양태는 방법, 완전 하드웨어 실시예, 완전 소프트웨어 실시예, 또는 소프트웨어와 하드웨어 양태를 조합하는 실시예의 형태를 취할 수 있다. 덧붙여, 본 발명은 컴퓨터 판독형 프로그램 코드를 반송하는 반송 매체(가령, 컴퓨터 판독형 저장 매체 상의 컴퓨터 프로그램 프로덕트)의 형태를 취할 수 있다.

[0310] 반송 매체:

[0311] 소프트웨어는 네트워크 인터페이스 디바이스를 통해 네트워크를 통해 더 송신 또는 수신될 수 있다. 예시적 실시예에서 반송 매체는 단일 매체인 것으로 도시되지만, 용어 "반송 매체"는 하나 이상의 명령 세트를 저장하는 단일 매체 또는 복수의 매체(가령, 중앙집중형 또는 분산형 데이터베이스 및/또는 연관된 캐시 및 서버)를 포함하는 것으로 이해된다. 용어 "반송 매체"는 또한 하나 이상의 프로세서에 의해 실행되며, 하나 이상의 프로세서로 하여금 본 발명의 방법들 중 하나 이상을 수행하게 하는 명령 세트를 저장, 인코딩, 또는 반송할 수 있는 임의의 매체를 포함하는 것으로 이해된다. 반송 매체는 많은 형태, 비제한적 예를 들면, 비휘발성 매체, 휘발성 매체, 및 전송 매체를 포함할 수 있다.

[0312] 구현예:

[0313] 언급된 방법의 단계들은 저장장치에 저장된 명령(컴퓨터 판독형 코드)을 실행하는 프로세싱 시스템(즉, 컴퓨터)의 적절한 프로세서(또는 복수의 프로세서)에 의해 수행된다. 본 발명은 임의의 특정 구현예 또는 프로그램 기법에 한정되지 않으며 본 발명은 본 명세서에 기재된 기능을 구현하기 위한 임의의 적절한 기법을 이용해 구현될 수 있음이 이해되어야 한다. 본 발명은 임의의 특정 프로그래밍 언어 또는 운영 체제에 한정되지 않는다.

[0314] 방법 또는 기능을 수행하기 위한 수단

[0315] 또한, 실시예들 중 일부는 프로세서 디바이스, 컴퓨터 시스템, 또는 그 밖의 다른 기능을 수행하는 수단의 프로세서에 의해 구현될 수 있는 방법 또는 방법의 요소들의 조합으로 기재된다. 따라서 이러한 방법 또는 방법의 요소를 수행하기 위한 필수 명령을 갖는 프로세서가 방법 또는 방법의 요소를 수행하기 위한 수단을 형성한다. 또한, 장치 실시예의 본 명세서에 기재된 요소가 본 발명을 실행하기 위한 목적으로 요소에 의해 수행되는 기능을 수행하기 위한 수단의 예시이다.

[0316] 연결된(connected)

[0317] 마찬가지로, 용어 "연결된"은, 청구항에서 사용될 때, 직접 연결만으로 한정하는 것으로 해석되어서는 안 된다. 따라서 디바이스 A가 디바이스 B에 연결됨이라는 표현의 범위는 디바이스 A의 출력이 디바이스 B의 입력으로 직접 연결되는 디바이스 또는 시스템으로 한정되어서는 안 된다. A의 출력과 B의 입력 사이에 다른 디바이스 또는 수단을 포함하는 경로가 존재함을 의미한다. "연결된"은 둘 이상의 요소가 직접적인 물리적 또는 전기적 접촉으로, 또는 둘 이상의 요소가 서로 직접 접촉하지 않지만 서로 여전히 상호 동작하거나 상호작용함을 의미한다.

[0318] 실시예:

[0319] 본 명세서에서 "하나의 실시예" 또는 "실시예"는 본 실시예와 관련하여 설명 된 특정 특징, 구조 또는 특성이 본 발명의 적어도 하나의 실시예에 포함됨을 의미한다. 따라서, 본 명세서 전체에 걸쳐 다양한 곳에서 "하나의 실시예에서"또는 "실시예에서"라는 표현의 출현은 반드시 동일한 실시예를 지칭하는 것이 아니라, 동일한 실시예를 지칭할 수도 있다. 또한, 특정 특징들, 구조들 또는 특성들은 하나 이상의 실시예들에서 본 개시 내용으로부터 해당 분야의 통상의 기술자에게 명백한 바와 같이 임의의 적절한 방식으로 결합 될 수 있다.

[0320] 유사하게, 본 발명의 예시적인 실시예들의 상기 설명에서, 본 발명의 다양한 특징들은 본 발명을 간소화하고 본 발명의 실시예를 돕기 위해 단일의 실시예, 도면 또는 그 설명으로 함께 그룹화되는 경우가 있음을 알아야 한다. 그러나, 이 개시 방법은 청구된 발명이 각 청구항에 명시적으로 언급된 것보다 많은 특징을 요구한다는 의도를 반영하는 것으로 해석되어서는 안 된다. 오히려, 이하의 청구 범위가 반영하는 바와 같이, 진보적인 양

태는 단일한 실시 형태의 모든 특징보다 적다. 따라서, 특정 실시예에 대한 상세한 설명에 이어지는 청구항들은 본 발명의 개별 실시예로서 그 자체로 각 청구항이 기재된 특정 실시예에 대한 상세한 설명에 명백히 포함된다.

[0321] 또한, 본 명세서에 설명된 일부 실시예는 다른 실시예에 포함된 일부 특징을 포함하지만 다른 특징을 포함하지는 않지만, 다른 실시예의 특징의 조합은 본 발명의 범위 내에 있고 다른 실시예를 형성하는 것으로 이해될 것이다 예를 들어, 다음의 청구항들에서, 청구된 실시예들 중 임의의 것이 임의의 조합으로 사용될 수있다.

[0322] 다양한 목적어 사례

[0323] 본 명세서에 사용될 때, 달리 지정되지 않는 한, 공통 대상을 기술하기 위한 서수 형용사 "제 1", "제 2", "제 3" 등의 사용은 단지 유사한 대상의 상이한 경우가 참조되는 것을 나타내며, 그렇게 기술된 대상이 시간적, 공간적, 순위적 또는 다른 방식으로 주어진 순서로 존재해야 함을 의미하지는 않는다.

[0324] 특정 세부 사항

[0325] 본 명세서에 제공된 설명에서, 다수의 특정 세부 사항이 제공된다. 그러나, 본 발명의 실시예들은 이들 특정 세부 사항 없이도 실시될 수 있음이 이해되어야 한다. 한편, 잘 알려진 방법, 구조 및 기술이 설명의 이해를 모호하게 하지 않기 위해 상세하게 나타나지 않는다.

[0326] 용어

[0327] 도면에 도시 된 본 발명의 바람직한 실시예를 기술할 때, 명료성을 위해 특정 용어가 사용된다. 그러나 본 발명은 그렇게 선택된 특정 용어에 한정되도록 의도되지 않으며, 각각의 특정 용어는 유사한 기술적 목적을 달성하기 위해 유사한 방식으로 작동하는 모든 기술적 등가물을 포함하는 것으로 이해되어야 한다. "전방", "후방", "방사형", "주변부", "상향", "하향 형" 등과 같은 용어는 참조 점을 제공하는 편의상의 단어로 사용되며 용어를 제한하는 것으로 해석되어서는 안 된다.

[0328] 포함 및 포함(Comprising and Including)

[0329] 다음의 청구 범위 및 본 발명의 전술 한 설명에서, 명시적인 언어 또는 필요한 의미로 인해 문맥이 다른 것을 요구하는 경우를 제외하고, "포함하다(comprise)"이라는 단어 또는 "포함하다(comprises)" 또는 "포함하는(comprising)"과 같은 변형은 포괄적인 의미, 즉 명시된 특징의 존재를 특정하며 본 발명의 다양한 실시예에서의 다른 특징의 존재 또는 추가를 배제하지 않는다.

[0330] 본 명세서에서 사용될 때 포함하다(include)라는 용어 역시 개방형 용어이며, 이 용어 뒤에 따르는 요소/특징을 적어도 포함하며, 그 밖의 다른 것들을 배제하지 않음을 의미한다.

[0331] 본 명세서에 사용된 용어를 포함하는 것을 포함하는 모든 용어는 적어도 용어를 따르는 요소들 / 특징들을 포함하지만 다른 것들을 배제하지 않는 것을 의미하는 공개 용어이다. 따라서, 포함하다(including)는 포함하다(comprising)와 동의어이다.

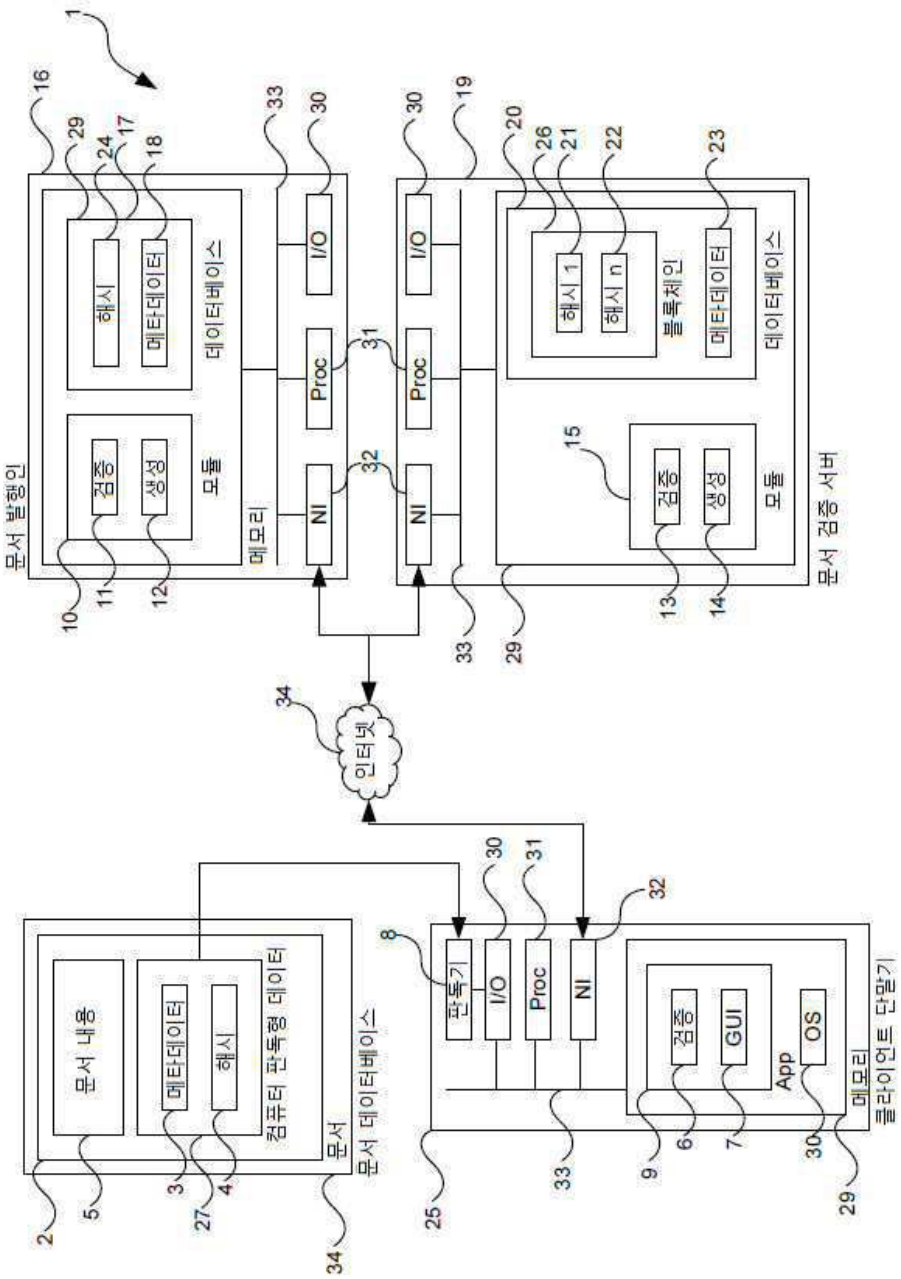
[0332] 발명의 범위

[0333] 따라서, 본 발명의 바람직한 실시예인 것으로 여겨지는 것을 설명하였지만, 해당 분야의 통상의 기술자라면 본 발명의 사상을 벗어나지 않는 또 다른 변형 예가 이루어질 수 있음을 알 것이며, 그러한 모든 변경 및 수정이 본 발명의 범위 내에 있음을 청구하기 위한 것이다. 예를 들어, 앞서 제공된 공식은 단지 사용될 수있는 절차를 대표하는 것에 불과하다. 기능이 블록도에 추가되거나 블록도로부터 삭제될 수 있으며 동작이 기능 블록들 간에 교환될 수 있다. 단계들은 본 발명의 범위 내에서 설명된 방법들에 추가되거나 삭제 될 수 있다.

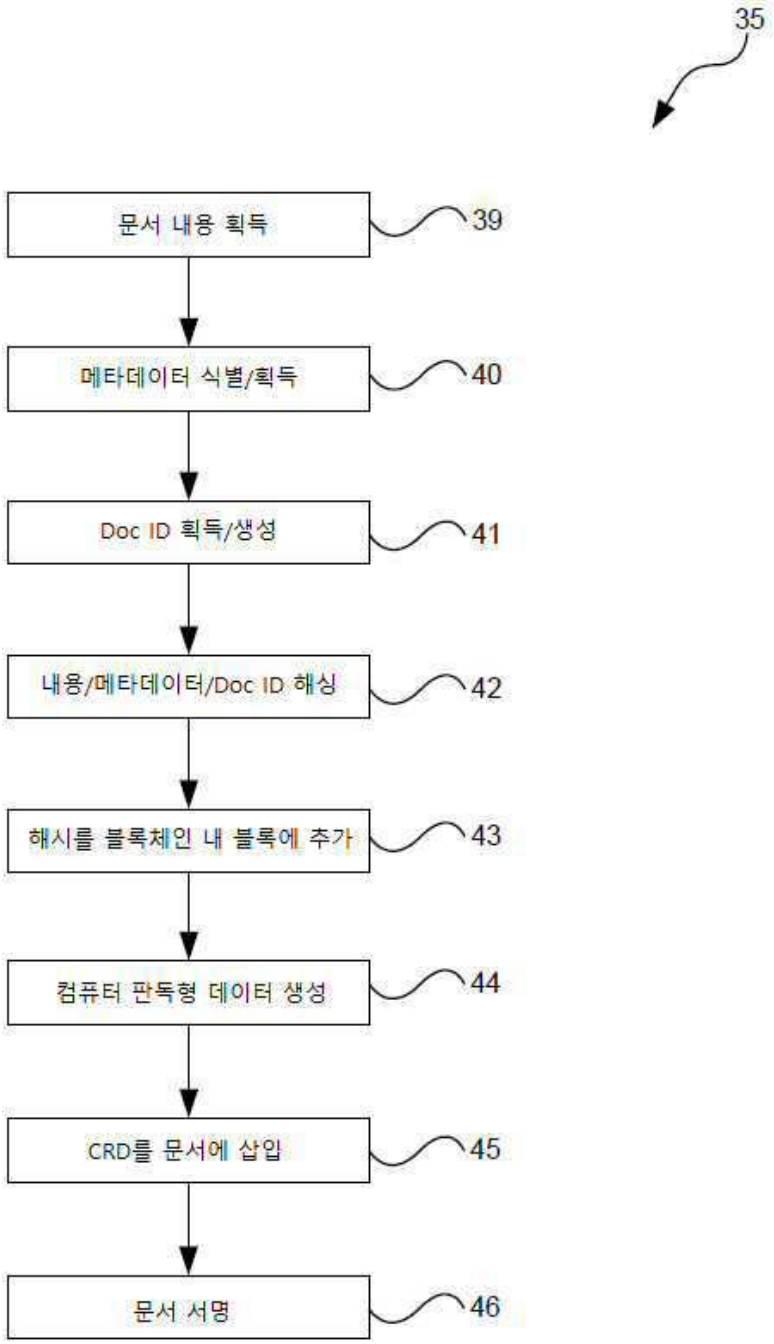
[0334] 비록 본 발명이 특정 예시를 참조하여 기술되었지만, 본 발명이 많은 다른 형태로 실시될 수 있다는 것은 해당 분야의 통상의 기술자에게 자명하다.

도면

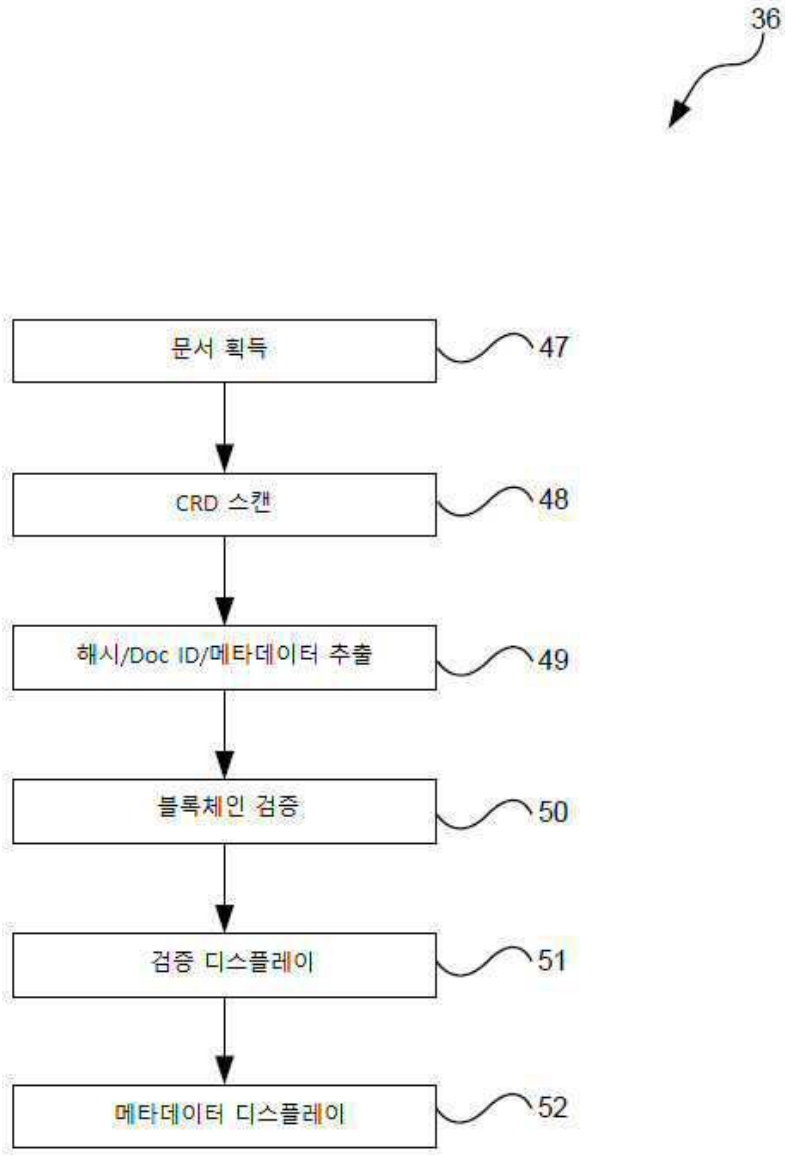
도면1


문서 발행인
데이터베이스
해시
메타데이터
모듈
검증
생성
메모리
I/O
Proc
NI
블록체인
해시 1
해시 n
문서 검증 서버
인터넷
컴퓨터 판독형 데이터
문서 내용
문서
문서 데이터베이스
판독기
GUI
App
OS
클라이언트 단말기

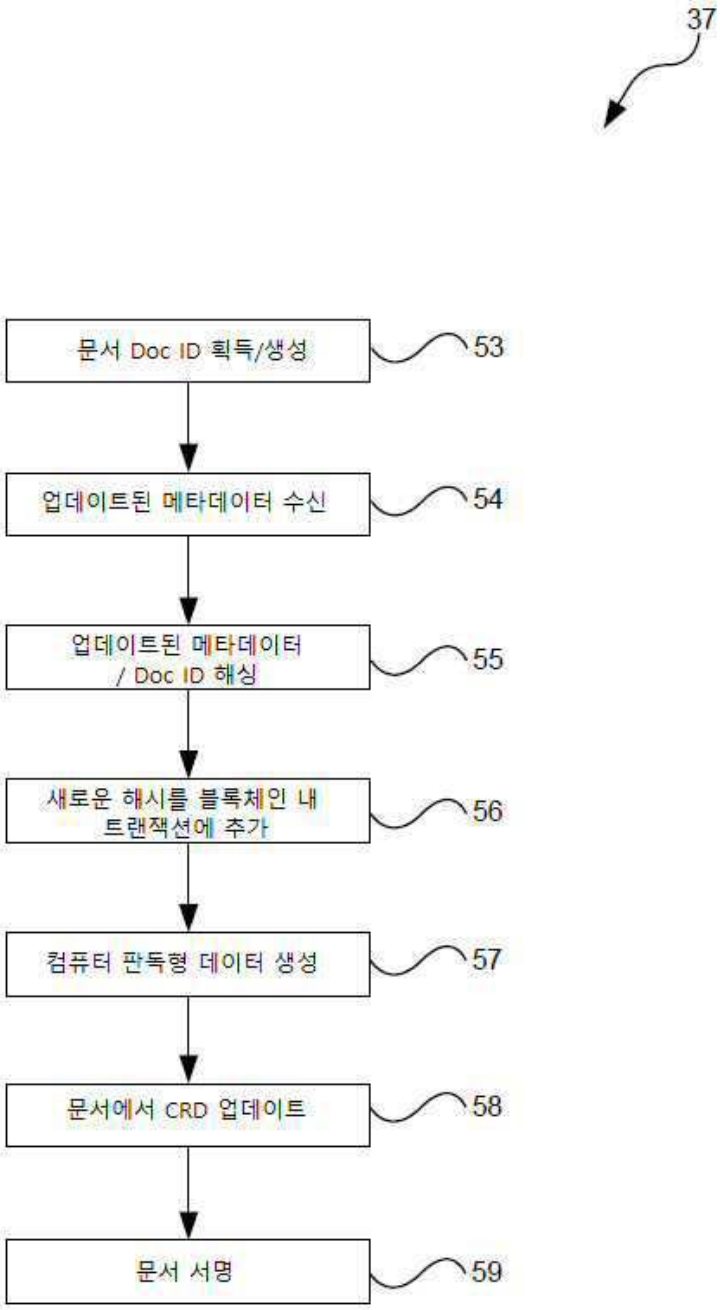
도면2


35
문서 내용 획득
39
메타데이터 식별/획득
40
Doc ID 획득/생성
41
내용/메타데이터/Doc ID 해싱
42
해시를 블록체인 내 블록에 추가
43
컴퓨터 판독형 데이터 생성
44
CRD를 문서에 삽입
45
문서 서명
46

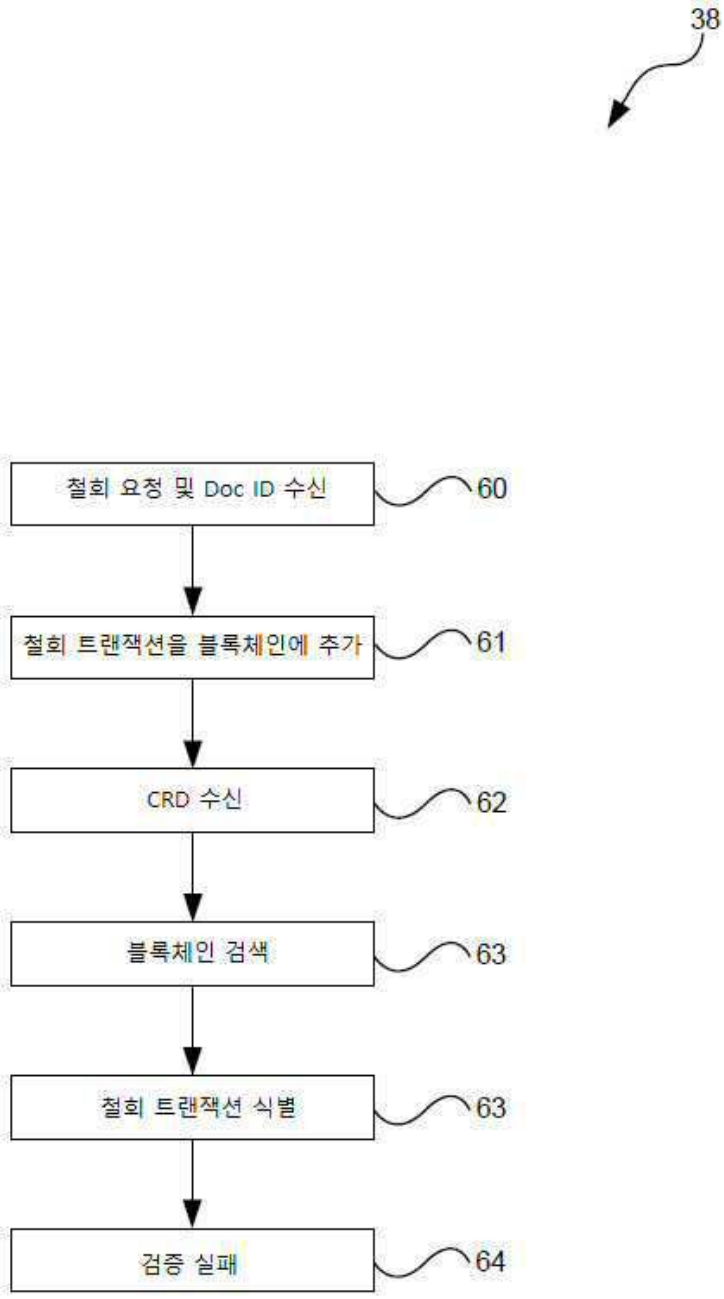
도면3


36
문서 획득
47
CRD 스캔
48
해시/Doc ID/메타데이터 추출
49
블록체인 검증
50
검증 디스플레이
51
메타데이터 디스플레이
52

도면4


37
문서 Doc ID 획득/생성
53
업데이트된 메타데이터 수신
54
업데이트된 메타데이터
/ Doc ID 해싱
55
새로운 해시를 블록체인 내
트랜잭션에 추가
56
컴퓨터 판독형 데이터 생성
57
문서에서 CRD 업데이트
58
문서 서명
59

도면5


38
철회 요청 및 Doc ID 수신
60
철회 트랜잭션을 블록체인에 추가
61
CRD 수신
62
블록체인 검색
63
철회 트랜잭션 식별
63
검증 실패
64

도면6


28
30% 5:30 PM
Document
Statement of Attainment
A Statement of Attainment is issued by a Registered Training Organisation when an individual has completed one or more accreditade units
ALLWEST
TRAINING SERVICE
ROBBAR PTY LTD
National Provider Code No 51925
This is a statement that
James Smith
has attained
RIIMPO311A
Conduct haul truck operation
Bob Cooper
Chief Executive Officer
Date 7th July 2007
Documet 0007/07/2007