



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2025-0059838
(43) 공개일자 2025년05월07일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) G06F 16/182 (2019.01)
H04L 9/00 (2022.01)
(52) CPC특허분류
H04L 9/3236 (2013.01)
G06F 16/182 (2019.01)
(21) 출원번호 10-2023-0143830
(22) 출원일자 2023년10월25일
심사청구일자 2023년10월25일

(71) 출원인
계명대학교 산학협력단
대구광역시 달서구 달구벌대로 1095, 계명대학교
산학협력관 201호(신당동)
(72) 발명자
박세진
대구광역시 동구 팔공로 260 (봉무동, 협성휴포레
이시아폴리스)
김진범
대구광역시 달서구 성서로72안길 16 (이곡동) 스
마트하우스2 303호
(74) 대리인
윤귀상

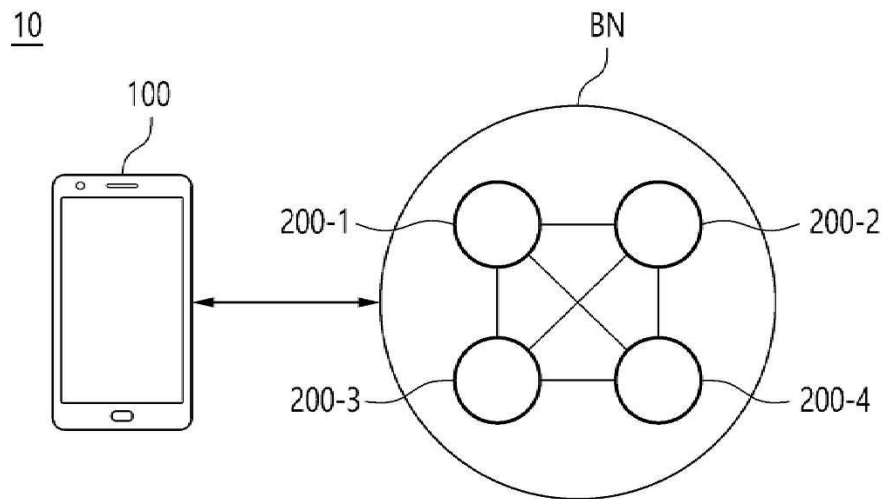
전체 청구항 수 : 총 11 항

(54) 발명의 명칭 외부 스토리지 활용을 위한 블록체인 네트워크 기반의 데이터 신뢰성 검증 방법, 이를 수행하는 기록매체 및 시스템

(57) 요약

본 발명은 외부 스토리지 활용을 위한 블록체인 네트워크 기반의 데이터 신뢰성 검증 방법에 관한 것으로, 클라이언트 노드가, 데이터를 상기 외부 스토리지에 저장하기 위한 저장 요청 트랜잭션을 생성하는 단계; 상기 클라이언트 노드가 상기 저장 요청 트랜잭션을 상기 블록체인 네트워크에 전송하는 단계; 상기 블록체인 네트워크에 참여하는 적어도 하나 이상의 검증 노드가, 상기 저장 요청 트랜잭션을 수신하면 상기 데이터를 검증하고, 검증한 결과를 블록에 추가하는 단계를 포함한다. 이를 통해 기존 외부 스토리지 방식과 달리 데이터의 저장 과정에서 검증 과정을 수행함으로써 데이터 활용 시 데이터 위변조 확인을 통해 오라클 문제를 해결할 수 있다.

대표도 - 도2



(52) CPC특허분류
H04L 9/50 (2022.05)

명세서

청구범위

청구항 1

외부 스토리지 활용을 위한 블록체인 네트워크 기반의 데이터 신뢰성 검증 방법은,
클라이언트 노드가, 데이터를 상기 외부 스토리지에 저장하기 위한 저장 요청 트랜잭션을 생성하는 단계;
상기 클라이언트 노드가 상기 저장 요청 트랜잭션을 상기 블록체인 네트워크에 전송하는 단계; 및
상기 블록체인 네트워크에 참여하는 적어도 하나 이상의 검증 노드가, 상기 저장 요청 트랜잭션을 수신하면 상기 데이터를 검증하고, 검증한 결과를 블록에 추가하는 단계를 포함하는, 데이터 신뢰성 검증 방법.

청구항 2

제1항에 있어서,
상기 저장 요청 트랜잭션은,
상기 데이터가 저장되는 외부 스토리지의 주소 정보 및 상기 데이터를 해시화한 원본 해시값을 포함하는, 데이터 신뢰성 검증 방법.

청구항 3

제2항에 있어서,
상기 검증한 결과를 블록에 추가하는 단계는,
상기 검증 노드가, 상기 주소 정보를 통해 상기 외부 스토리지로부터 상기 데이터를 수신하고 상기 저장 요청 트랜잭션에 포함된 상기 원본 해시값을 수신하는 단계; 및
상기 검증 노드가, 상기 수신한 데이터를 해시화하여 대조 해시값을 생성하는 단계를 포함하는, 데이터 신뢰성 검증 방법.

청구항 4

제3항에 있어서,
상기 데이터를 검증하는 것은,
상기 검증 노드가 상기 대조 해시값과 상기 원본 해시값 간의 일치 여부를 검증하여 상기 데이터의 신뢰성을 검증하는 것인, 데이터 신뢰성 검증 방법.

청구항 5

제4항에 있어서,
상기 검증한 결과를 블록에 추가하는 단계에서는,
상기 검증 노드가 상기 대조 해시값과 상기 원본 해시값이 일치하면, 상기 저장 요청 트랜잭션을 합의 알고리즘을 통해 합의하는 단계를 더 포함하는, 데이터 신뢰성 검증 방법.

청구항 6

제1항에 따른 상기 데이터 신뢰성 검증 방법을 수행하기 위한 컴퓨터 프로그램이 기록된 컴퓨터로 판독 가능한 기록 매체.

청구항 7

외부 스토리지 활용을 위한 블록체인 네트워크 기반의 데이터 신뢰성 검증 시스템에 있어서,

데이터를 상기 외부 스토리지에 저장하기 위한 저장 요청 트랜잭션을 생성하고, 상기 저장 요청 트랜잭션을 상기 블록체인 네트워크에 전송하는 클라이언트 노드; 및

상기 블록체인 네트워크에 참여하는 검증 노드로서, 상기 저장 요청 트랜잭션을 수신하면 상기 데이터를 검증하고, 검증한 결과를 블록에 추가하는 적어도 하나 이상의 상기 검증 노드를 포함하는, 데이터 신뢰성 검증 시스템.

청구항 8

제7항에 있어서,

상기 저장 요청 트랜잭션은,

상기 데이터가 저장되는 외부 스토리지의 주소 정보 및 상기 데이터를 해시화한 원본 해시값을 포함하는, 데이터 신뢰성 검증 시스템.

청구항 9

제8항에 있어서,

상기 적어도 하나 이상의 검증 노드는,

상기 주소 정보를 통해 상기 외부 스토리지로부터 상기 데이터를 수신하고, 상기 저장 요청 트랜잭션에 포함된 상기 원본 해시값을 수신하고, 상기 수신한 데이터를 해시화하여 대조 해시값을 생성하는, 데이터 신뢰성 검증 시스템.

청구항 10

제9항에 있어서,

상기 적어도 하나 이상의 검증 노드는,

상기 대조 해시값과 상기 원본 해시값 간의 일치 여부를 검증하여 상기 데이터의 신뢰성을 검증하는, 데이터 신뢰성 검증 시스템.

청구항 11

제10항에 있어서,

상기 적어도 하나 이상의 검증 노드는,

상기 대조 해시값과 상기 원본 해시값이 일치하면, 상기 저장 요청 트랜잭션을 합의 알고리즘을 통해 합의하여 상기 저장 요청 트랜잭션을 블록에 추가하는, 데이터 신뢰성 검증 시스템.

발명의 설명

기술 분야

[0001] 본 발명은 스토리지 데이터에 대한 신뢰문제를 해결할 수 있는 외부 스토리지 활용을 위한 블록체인 네트워크 기반의 데이터 신뢰성 검증 방법, 이를 수행하는 기록매체 및 시스템에 관한 것이다.

배경 기술

[0002] 종래의 블록체인 기술은 블록체인의 대중화로 거래량이 늘어났으며, 이를 처리하기 위한 대용량 스토리지와 높은 트랜잭션(Transaction) 처리 속도가 요구되고 있다.

[0003] 이를 해결하기 위해 종래의 블록체인 확장 기술에서는 외부 저장소에 저장하는 방식을 사용함으로써 트랜잭션 처리 속도의 향상과 같은 긍정적인 측면을 누렸다.

[0004] 하지만 신뢰성이 보장되는 체인 내부 데이터와 달리, 체인 외부 데이터는 신뢰성을 확보할 수 없기 때문에 '외부 데이터의 위변조 방지 불가'와 같은 신뢰성 보장 불가 문제인 오라클 문제가 발생한다는 문제가 있다. 다시 말해 오라클 문제는 블록체인 자체는 안전하지만 블록체인 외부에서 수신되는 데이터의 신뢰성을 검증할 수 없

음으로 인한 문제이다.

[0005] 예컨대 NFT(Non-Fungible Token)를 발행하기 위한 원본 이미지를 외부 스토리지에 업로드하고 접근가능한 주소 값을 저장할 때 블록체인에 데이터가 기록되면 기록된 데이터의 위변조는 불가능하다. 하지만 실제 NFT를 구매하고, 주소값에 접근한 경우, 원본 이미지와는 다른 이미지가거나 원본 이미지가 없다는 문제가 발생하여 데이터의 신뢰성이 저하된다.

[0006] 도 1은 종래의 외부 저장소에 데이터를 저장하는 과정을 설명하기 위한 개략도이다. 도 1에 도시된 바와 같이 종래에는 데이터를 저장하는 과정에서 단순히 IPFS(Inter Planetary File System)와 같은 외부 분산 스토리지를 활용할 뿐, 저장되는 데이터에 대한 검증과정이 별도로 존재하지 않는다. 이에 외부 분산 스토리지에 저장된 데이터가 유효하다고 믿고 쓰는 것에 불과할 뿐이다.

[0007] 따라서 외부 데이터의 위변조 방지를 위해 블록체인의 합의 과정에서 체인 내외부 데이터의 일관성을 검증하여 이를 트랜잭션으로 기록하여 신뢰성을 높이는 외부 스토리지 데이터의 검증을 위한 방법이 요구되고 있다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 한국공개특허공보 제10-2007-0106095호

발명의 내용

해결하려는 과제

[0009] 본 발명은 상기와 같은 문제를 해결하기 위해 안출된 것으로, 본 발명의 목적은 데이터의 저장 과정에서 검증을 미수행하는 기존 외부 스토리지 방식과 달리 데이터의 저장 과정에서 검증 과정을 수행함으로써 데이터 활용 시 데이터 위변조 확인을 통해 오라클 문제를 해결할 수 있는, 외부 스토리지 활용을 위한 블록체인 네트워크 기반의 데이터 신뢰성 검증 방법, 이를 수행하는 기록매체 및 시스템을 제공하는 것이다.

과제의 해결 수단

[0010] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 데이터 신뢰성 검증 방법은, 외부 스토리지 활용을 위한 블록체인 네트워크 기반의 데이터 신뢰성 검증 방법으로, 클라이언트 노드가, 데이터를 상기 외부 스토리지에 저장하기 위한 저장 요청 트랜잭션을 생성하는 단계; 상기 클라이언트 노드가 상기 저장 요청 트랜잭션을 상기 블록체인 네트워크에 전송하는 단계; 및 상기 블록체인 네트워크에 참여하는 적어도 하나 이상의 검증 노드가, 상기 저장 요청 트랜잭션을 수신하면 상기 데이터를 검증하고, 검증한 결과를 블록에 추가하는 단계를 포함한다.

[0011] 그리고 상기 저장 요청 트랜잭션은, 상기 데이터가 저장되는 외부 스토리지의 주소 정보 및 상기 데이터를 해시화한 원본 해시값을 포함할 수 있다.

[0012] 또한 상기 검증한 결과를 블록에 추가하는 단계는, 상기 검증 노드가, 상기 주소 정보를 통해 상기 외부 스토리지로부터 상기 데이터를 수신하고 저장 요청 트랜잭션에 포함된 상기 원본 해시값을 수신하는 단계; 및 상기 검증 노드가, 상기 수신한 데이터를 해시화하여 대조 해시값을 생성하는 단계를 포함할 수 있다.

[0013] 그리고 상기 데이터를 검증하는 것은, 상기 검증 노드가 상기 대조 해시값과 상기 원본 해시값 간의 일치 여부를 검증하여 상기 데이터의 신뢰성을 검증하는 것일 수 있다.

[0014] 또한 상기 검증한 결과를 블록에 추가하는 단계에서는, 상기 검증 노드가 상기 대조 해시값과 상기 원본 해시값이 일치하면, 상기 저장 요청 트랜잭션을 합의 알고리즘을 통해 합의하는 단계를 더 포함할 수 있다.

[0015] 한편 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 기록매체는 본 발명의 일 실시예에 따른 상기 데이터 신뢰성 검증 방법을 수행하기 위한 컴퓨터 프로그램이 기록된 컴퓨터로 판독 가능한 기록 매체이다.

[0016] 한편 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 데이터 신뢰성 검증 시스템은, 외부 스토리지 활용을 위한 블록체인 네트워크 기반의 데이터 신뢰성 검증 시스템으로, 데이터를 상기 외부 스토리지에 저장하기

위한 저장 요청 트랜잭션을 생성하고, 상기 저장 요청 트랜잭션을 상기 블록체인 네트워크에 전송하는 클라이언트 노드; 및 상기 블록체인 네트워크에 참여하는 검증 노드로서, 상기 저장 요청 트랜잭션을 수신하면 상기 데이터를 검증하고, 검증한 결과를 블록에 추가하는 적어도 하나 이상의 상기 검증 노드를 포함한다.

[0017] 그리고 상기 저장 요청 트랜잭션은, 상기 데이터가 저장되는 외부 스토리지의 주소 정보 및 상기 데이터를 해시화한 원본 해시값을 포함할 수 있다.

[0018] 또한 상기 적어도 하나 이상의 검증 노드는, 상기 주소 정보를 통해 상기 외부 스토리지로부터 상기 데이터를 수신하고, 상기 저장 요청 트랜잭션에 포함된 상기 원본 해시값을 수신하고, 상기 수신한 데이터를 해시화하여 대조 해시값을 생성할 수 있다.

[0019] 그리고 상기 적어도 하나 이상의 검증 노드는, 상기 대조 해시값과 상기 원본 해시값 간의 일치 여부를 검증하여 상기 데이터의 신뢰성을 검증할 수 있다.

[0020] 또한 상기 적어도 하나 이상의 검증 노드는, 상기 대조 해시값과 상기 원본 해시값이 일치하면, 상기 저장 요청 트랜잭션을 합의 알고리즘을 통해 합의하여 상기 저장 요청 트랜잭션을 블록에 추가할 수 있다.

발명의 효과

[0021] 상술한 본 발명의 일 측면에 따르면, 외부 스토리지 활용을 위한 블록체인 네트워크 기반의 데이터 신뢰성 검증 방법, 이를 수행하는 기록매체 및 시스템을 제공함으로써, 기존 외부 스토리지 방식과 달리 데이터의 저장 과정에서 검증 과정을 수행함으로써 데이터 활용 시 데이터 위변조 확인을 통해 오라클 문제를 해결할 수 있다.

도면의 간단한 설명

[0022] 도 1은 종래의 외부 저장소에 데이터를 저장하는 과정을 설명하기 위한 개략도,

도 2는 본 발명의 일 실시예에 따른 데이터 신뢰성 검증 시스템의 구성을 설명하기 위한 도면,

도 3은 본 발명의 일 실시예에 따른 데이터 신뢰성 검증 시스템을 구체적으로 설명하기 위한 도면, 그리고,

도 4는 본 발명의 일 실시예에 따른 데이터 신뢰성 검증 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0023] 후술하는 본 발명에 대한 상세한 설명은, 본 발명이 실시될 수 있는 특정 실시예를 예시로서 도시하는 첨부 도면을 참조한다. 이들 실시예는 당업자가 본 발명을 실시할 수 있기에 충분하도록 상세히 설명된다. 본 발명의 다양한 실시예는 서로 다르지만 상호 배타적일 필요는 없음이 이해되어야 한다. 예를 들어, 여기에 기재되어 있는 특정 형상, 구조 및 특성은 일 실시예와 관련하여 본 발명의 정신 및 범위를 벗어나지 않으면서 다른 실시예로 구현될 수 있다. 또한, 각각의 개시된 실시예 내의 개별 구성요소의 위치 또는 배치는 본 발명의 정신 및 범위를 벗어나지 않으면서 변경될 수 있음이 이해되어야 한다. 따라서, 후술하는 상세한 설명은 한정적인 의미로서 취하려는 것이 아니며, 본 발명의 범위는, 적절하게 설명된다면, 그 청구항들이 주장하는 것과 균등한 모든 범위와 더불어 첨부된 청구항에 의해서만 한정된다. 도면에서 유사한 참조부호는 여러 측면에 걸쳐서 동일하거나 유사한 기능을 지칭한다.

[0024] 본 발명에 따른 구성요소들은 물리적인 구분이 아니라 기능적인 구분에 의해서 정의되는 구성요소들으로써 각각이 수행하는 기능들에 의해서 정의될 수 있다. 각각의 구성요소들은 하드웨어 또는 각각의 기능을 수행하는 프로그램 코드 및 프로세싱 유닛으로 구현될 수 있을 것이며, 두 개 이상의 구성요소의 기능이 하나의 구성요소에 포함되어 구현될 수도 있을 것이다. 따라서 이하의 실시예에서 구성요소에 부여되는 명칭은 각각의 구성요소를 물리적으로 구분하기 위한 것이 아니라 각각의 구성요소가 수행되는 대표적인 기능을 암시하기 위해서 부여된 것이며, 구성요소의 명칭에 의해서 본 발명의 기술적 사상이 한정되지 않는 것임에 유의하여야 한다.

[0025] 이하에서는 도면들을 참조하여 본 발명의 바람직한 실시예들을 보다 상세하게 설명하기로 한다.

[0026] 도 2는 본 발명의 일 실시예에 따른 데이터 신뢰성 검증 시스템(10)의 구성을 설명하기 위한 도면이다.

[0027] 본 발명의 데이터 신뢰성 검증 시스템(10, 이하 시스템)은 블록체인에서 외부 스토리지를 활용하여 데이터를 저장하는 과정에서 저장하는 데이터에 대한 검증 과정을 수행하지 않는 기존 외부 스토리지 방식을 해결하기 위해 마련된다.

- [0028] 구체적으로 본 시스템(10)은 블록체인 네트워크(BN)에서 외부 스토리지를 도입할 때 외부 스토리지에 데이터를 저장하는 경우, 해당 데이터의 저장 요청에 대한 합의 시점에 데이터를 검증하고 이를 트랜잭션(Transaction)으로 기록함으로써 오라클 문제를 해결하기 위해 마련된다.
- [0029] 이때 시스템(10)은 블록체인 네트워크(BN)에 연결되는 복수개의 노드에서 생성되는 트랜잭션을 사전에 설정되는 주기 또는 조건에 따라 블록으로 생성하여 각각의 노드에 저장되는 체인에 연결하는 블록체인 기법에 기반할 수 있다.
- [0030] 여기서 노드는 무선 또는 유선으로 블록체인 네트워크(BN)에 연결되는 장치를 의미할 수 있으며, 이동성을 갖거나 고정될 수 있다. 여기서 장치는, 서버(server) 또는 엔진(engine) 형태일 수 있으며, 디바이스(device), 기구(apparatus), 단말 terminal), UE(user equipment), MS(mobile station), 무선기기(wireless device), 휴대기기(handheld device) 등 다른 용어로 불릴 수 있다. 그리고 장치는 운영체제(Operation System; OS), 즉 시스템을 기반으로 다양한 소프트웨어를 실행하거나 제작할 수 있다. 여기서 운영체제는 소프트웨어가 장치의 하드웨어를 사용할 수 있도록 하기 위한 시스템 프로그램으로서, 안드로이드 OS, iOS, 윈도우 모바일 OS, 바다 OS, 심비안 OS, 블랙베리 OS 등 모바일 컴퓨터 운영체제 및 윈도우 계열, 리눅스 계열, 유닉스 계열, MAC, AIX, HP-UX 등 컴퓨터 운영체제를 모두 포함할 수 있다.
- [0031] 또한 블록체인 네트워크(BN)는 분산원장을 의미할 수 있다.
- [0032] 따라서 블록체인 네트워크(BN)는 복수개의 노드에서 생성되는 트랜잭션을 수집하여 블록에 추가 또는 블록을 생성할 수 있으며 이와 관련하여 블록체인 네트워크(BN)는 복수개의 서버 중에서 사전에 설정되는 조건에 따라 선출되는 임의의 대표 노드가 임의의 서버에서 생성되는 트랜잭션을 수집하여 블록을 생성하도록 마련될 수도 있다.
- [0033] 이때 블록체인 네트워크(BN)가 블록을 생성하는 것은 블록체인 네트워크(BN)에 연결된 복수의 노드 중 대표 노드로 선출된 노드가 복수개의 노드로부터 전달받는 트랜잭션에 따라 블록을 생성하는 것일 수 있다.
- [0034] 한편 블록체인 네트워크(BN)에서 생성되는 블록은 이전에 생성된 블록의 정보와 복수개의 노드로부터 전달받은 트랜잭션을 포함하도록 생성될 수 있으며, 블록을 생성한 노드는 생성된 블록을 블록체인 네트워크(BN)에 연결된 복수개의 노드에 전달할 수 있다.
- [0035] 여기에서, 블록은 이전에 생성된 블록의 정보를 해시 함수를 이용하여 암호화된 상태로 포함시킬 수 있다.
- [0036] 그리고 복수의 노드는 공지된 합의 알고리즘을 이용해 전달받은 블록을 검증할 수 있으며, 검증이 완료된 블록은 이전에 생성된 블록에 연결될 수 있다.
- [0037] 이를 위해 본 실시예에 따른 블록체인 네트워크에 기반한 시스템(10)은 클라이언트 노드(100) 및 검증 노드(200)를 포함할 수 있다.
- [0038] 그리고 클라이언트 노드(100) 및 검증 노드(200)는 블록체인 네트워크(BN)에 기반한 데이터 신뢰성 검증 방법을 수행하기 위한 소프트웨어(어플리케이션)가(이) 설치되어 실행될 수 있다.
- [0039] 클라이언트 노드(100)는 데이터를 외부 스토리지에 저장하기 위한 저장 요청 트랜잭션을 생성할 수 있다.
- [0040] 그리고 클라이언트 노드(100)는 생성한 저장 요청 트랜잭션을 블록체인 네트워크(BN)에 전송할 수 있다.
- [0041] 저장 요청 트랜잭션은, 데이터가 저장되는 외부 스토리지의 주소 정보 및 데이터를 해시화한 원본 해시값을 포함할 수 있다.
- [0042] 여기서 데이터라 함은 클라이언트 노드(100)가 외부 스토리지에 NFT(Non-Fungible Token) 발행 데이터 또는 거래 등과 같은 특정 트랜잭션과 관련된 데이터를 의미할 수 있다.
- [0043] 그리고 클라이언트 노드(100)는 예컨대 SHA-256과 같은 해시 함수를 통해 데이터를 해시화하여 원본 해시값을 생성할 수 있다.
- [0044] 한편 검증 노드(200)는 블록체인 네트워크(BN)에 참여하는 적어도 하나 이상의 노드로서, 저장 요청 트랜잭션을 수신하면 해당 데이터를 검증하고, 검증한 결과를 블록에 추가할 수 있다.
- [0045] 본 실시예에 따른 검증 노드(200)는, 블록체인 네트워크(BN)에 전파된 저장 요청 트랜잭션을 수신하면, 저장 요청 트랜잭션에 포함되는 데이터가 기록된 주소 정보를 이용해 외부 스토리지로부터 데이터를 수신하고, 저장 요

청 트랜잭션에 포함된 원본 해시값을 수신할 수 있다.

- [0046] 그리고 검증 노드(200)는 수신한 데이터를 해시화하여 대조 해시값을 생성할 수 있다.
- [0047] 또한 검증 노드(200)는 생성한 대조 해시값과 저장 요청 트랜잭션에 포함되는 원본 해시값을 비교하여 일치 여부를 검증함으로써 데이터의 신뢰성을 검증할 수 있다.
- [0048] 그리고 검증 노드(200)는, 대조 해시값과 원본 해시값이 일치하면, 저장 요청 트랜잭션을 합의 알고리즘을 통해 합의하여 저장 요청 트랜잭션을 블록에 추가할 수 있다.
- [0049] 이를 통해 본 실시예에 따른 시스템(10)은 외부 스토리지에 저장되는 데이터가 블록체인에 기록되는 시점에 검증을 수행함으로써, 데이터에 대한 신뢰성을 검증하여 오라클 문제를 해결할 수 있다.
- [0050] 구체적으로 이하에서는 클라이언트 노드(100)가 NFT를 발행하는 발행자인 경우를 예시적 사항으로 설명하기로 한다.
- [0051] NFT를 발행하기 위한 원본 이미지를 외부 스토리지에 업로드하면, 클라이언트 노드(100)는 해당 원본 이미지가 저장된 외부 스토리지에 접근 가능한 주소 값인 해시값과, 원본 이미지 즉 데이터를 해시값으로 변환하여 원본 해시값을 생성할 수 있다.
- [0052] 그리고 클라이언트 노드(100)는 이를 저장 요청 트랜잭션에 포함시켜 블록체인 네트워크(BN)에 전파하여 등록요청할 수 있다.
- [0053] 외부 스토리지를 활용하는 종래의 경우에는 주소정보만이 포함되도록 하지만, 본 발명의 시스템(10)은 주소정보와 함께 데이터, 즉 이미지와 같은 콘텐츠의 해시 정보가 저장 요청 트랜잭션에 함께 저장된다.
- [0054] 따라서 블록체인의 합의 과정에서 해당 콘텐츠가 믿을 수 있는지를 검증하는 과정이므로, 합의하는 과정 내에서 실제 클라이언트 노드(100)가 요청한 위치, 즉 주소에 검증 노드(200)가 접근하여 원본 콘텐츠를 다운로드 받을 수 있다.
- [0055] 그리고나서 검증 노드(200)가 다운로드한 원본 콘텐츠에 대한 해시화하여 대조 해시값을 생성하고, 원본 콘텐츠의 해시값인 원본 해시 값을 비교하여 검증할 수 있다.
- [0056] 이를 통해 본 실시예에 따른 외부 스토리지에 저장 및 기록된 콘텐츠가 블록체인에 기록되는 시점에 검증을 수행함으로써 오라클 문제를 해결할 수 있다.
- [0057] 도 3은 본 발명의 일 실시예에 따른 데이터 신뢰성 검증 시스템(10)을 구체적으로 설명하기 위한 도면이다.
- [0058] 도 3에 도시된 바와 같이 클라이언트 노드(100)와 적어도 하나 이상의 검증 노드(200), 즉 블록체인 네트워크(BN)에 참여하는 모든 노드는 API(Application Program Interface)로서 오프체인 데이터 검증 모듈(Off-Chain Data Verify Module)을 포함하도록 마련될 수 있다.
- [0059] 그리고 블록체인 네트워크(BN)에서의 블록 구조(Block Structure in BN)는 도 3에 도시된 바와 같이 데이터 리스트(Data List)와 데이터 저장 타임 스탬프(Data Store Time Stamp)를 포함할 수 있다.
- [0060] 클라이언트 노드(100)가 외부 스토리지에 데이터를 저장하기 위해 저장 요청 트랜잭션을 발생시키면, 오프체인 데이터 검증 모듈(Off-Chain Data Verify Module)에 포함되는 데이터 스토리지(Data Storage)는 전달받은 데이터를 해시화하여 외부 스토리지에 저장시킬 수 있다.
- [0061] 도 3에 도시된 해시값(Hash Value)는 데이터 리스트를 SHA-256 함수를 통해 해시화한 값으로 원본 해시값을 의미할 수 있다.
- [0062] 그리고 검증 노드(200)는 오프체인 데이터 검증 모듈(Off-Chain Data Verify Module)에 포함되는 데이터 검증 기능(Data Verify Function)을 통해 외부 스토리지에 저장된 데이터가 실제 저장하고자 한 데이터인지를 해시값 대조를 통해 비교한 후 결과를 도출할 수 있다.
- [0063] 그리고 오프체인 데이터 검증 모듈(Off-Chain Data Verify Module)은 유효 노드 리스트(Validator Node List)를 포함할 수 있다.
- [0064] 이후 해시값을 대조한 결과를 통해 적어도 하나 이상의 검증 노드(200)가 합의를 이뤄 해당 데이터를 신뢰할 수 있는 경우에는 이를 해당 블록에 추가할 수 있다.

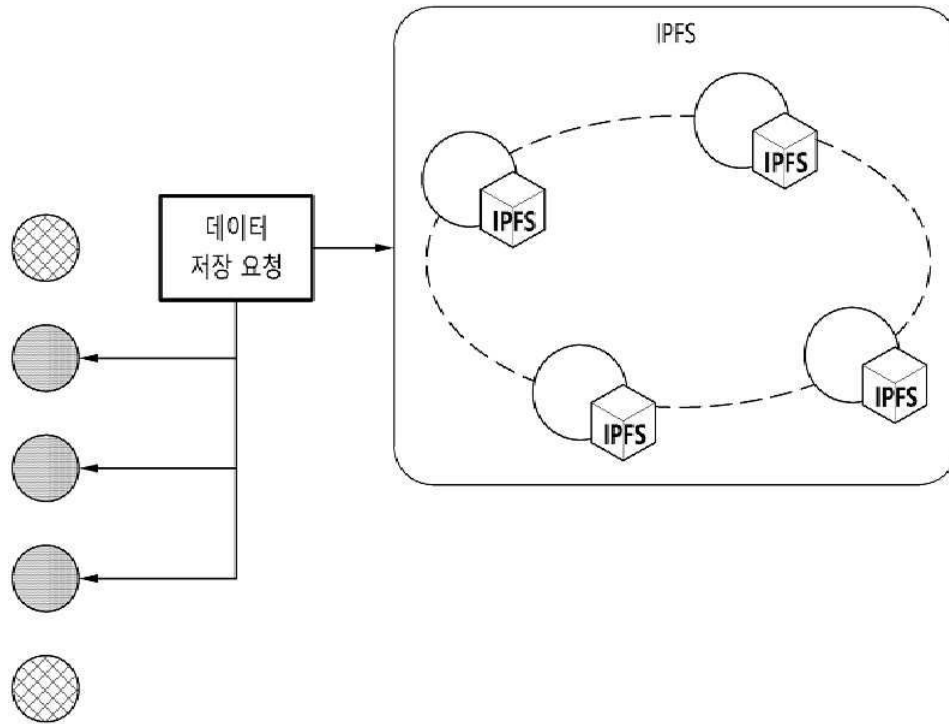
- [0065] 따라서 변조 가능성이 있는 외부 스토리지를 사용하더라도, 외부 스토리지에 저장되는 데이터의 해시 값은 변조 불가능한 블록체인에 저장하기 때문에 저장되는 시점에는 해당 데이터가 유효함을 보장할 수 있다.
- [0066] 이를 통해 종래에는 데이터가 변조되더라도 이를 알 수 있는 방법이 없지만, 본 발명에 따른 데이터 신뢰성 검증 시스템(10)은 해시 값이 블록체인에 기록되어 데이터를 읽는 시점에 변조 여부를 정확하게 알 수 있다.
- [0068] 한편 도 4는 본 발명의 일 실시예에 따른 데이터 신뢰성 검증 방법을 설명하기 위한 흐름도로써, 본 발명의 일 실시예에 따른 데이터 신뢰성 검증 방법은 도 2 및 도 3에 도시된 데이터 신뢰성 검증 시스템(10)과 실질적으로 동일한 구성 상에서 진행되므로, 도 2 및 도 3의 데이터 신뢰성 검증 시스템(10)과 동일한 구성요소에 대해 동일한 도면 부호를 부여하고, 반복되는 설명은 생략하기로 한다.
- [0069] 먼저 클라이언트 노드(100)가, 데이터를 외부 스토리지에 저장하기 위한 저장 요청 트랜잭션을 생성할 수 있다(S110).
- [0070] 그리고 클라이언트 노드(100)가 저장 요청 트랜잭션을 블록체인 네트워크(BN)에 전송할 수 있다(S120).
- [0071] 이후 블록체인 네트워크(BN)에 참여하는 적어도 하나 이상의 검증 노드가, 저장 요청 트랜잭션을 수신하면 데이터를 검증할 수 있다(S130).
- [0072] 이때 저장 요청 트랜잭션은, 데이터가 저장되는 외부 스토리지의 주소 정보 및 상기 데이터를 해시화한 원본 해시값 중 적어도 하나를 포함할 수 있다.
- [0073] 그리고나서 블록체인 네트워크(BN)에 참여하는 적어도 하나 이상의 검증 노드가, 검증한 결과를 블록에 추가할 수 있다(S140).
- [0074] 이러한 검증한 결과를 블록에 추가하는 단계(S140)는, 검증 노드(200)가 주소 정보를 통해 외부 스토리지로부터 데이터를 수신하고 저장 요청 트랜잭션에 포함된 원본 해시값을 수신하는 단계를 포함할 수 있다.
- [0075] 그리고 검증한 결과를 블록에 추가하는 단계(S140)는, 검증 노드(200)가 수신한 데이터를 해시화하여 대조 해시값을 생성하는 단계를 포함할 수 있다.
- [0076] 그리고 검증한 결과를 블록에 추가하는 단계(S140)에서 데이터를 검증하는 것은, 검증 노드(200)가 대조 해시값과 원본 해시값 간의 일치 여부를 검증하는 것일 수 있다.
- [0077] 또한 검증한 결과를 블록에 추가하는 단계(S140)에서는, 검증 노드(200)가 대조 해시값과 원본 해시값이 일치하면, 저장 요청 트랜잭션을 합의 알고리즘을 통해 합의하는 단계를 더 포함할 수 있다.
- [0078] 이와 같은 본 발명의 데이터 신뢰성 검증 방법은 다양한 컴퓨터 구성요소를 통하여 수행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다.
- [0079] 상기 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수도 있다.
- [0080] 컴퓨터 판독 가능한 기록 매체의 예에는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD 와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다.
- [0081] 프로그램 명령어의 예에는, 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 상기 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.
- [0083] 이상에서는 본 발명의 다양한 실시예에 대하여 도시하고 설명하였지만, 본 발명은 상술한 특정의 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형실시들은 본 발명의 기술적 사상이나 전망으로부터 개별적으로 이해되어져서는 안될 것이다.

부호의 설명

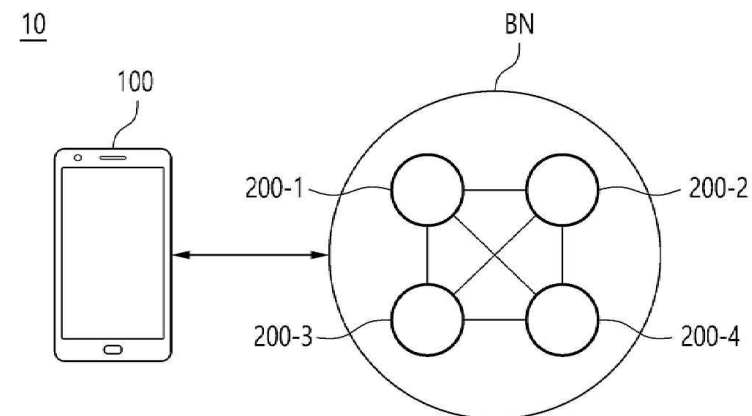
[0084] 10 : 데이터 신뢰성 검증 시스템 100 : 클라이언트 노드
200 : 검증 노드 BN : 블록체인 네트워크

도면

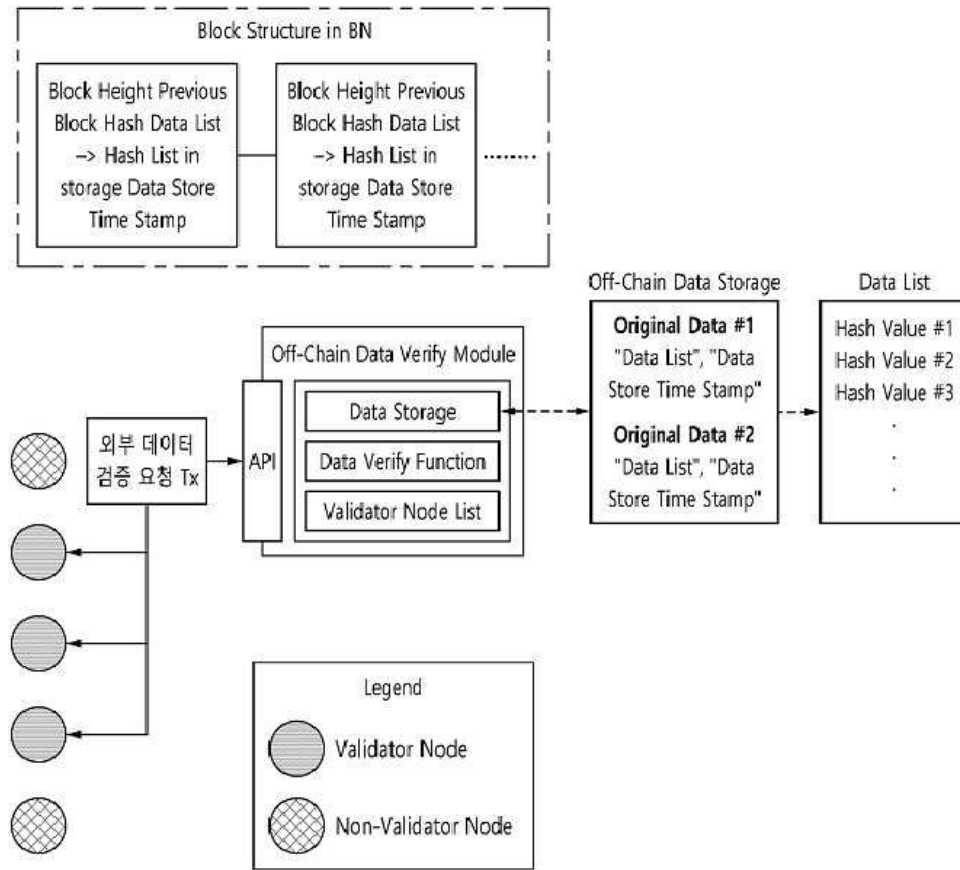
도면1



도면2



도면3



도면4

