JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 24, No. 7, pp. 1529-1536, Jul. 2023

Check for updates

NFT 데이터 파일 무결성 검사를 위한 해시알고리즘 활용

송 효 준[1] · 정 송 헌[2] · 김 경 백[3*]
[1]전남대학교 정보보안협동과정 석사
[2]전남대학교 정보보안협동과정 석사과정
[3*]전남대학교 인공지능융합학과 교수

Utilizing Hash Algorithms for NFT Data File Integrity Checks

Hyojun Song[1] · Songheon Jeong[2] · Kyungbaek Kim[3*]

[1]Master, Department of Information Securitynts, Chonnam University, Gwangju 61186, Korea
[2]Master's Course, Department of Information Securitynts, Chonnam University, Gwangju 61186, Korea
[3*]Professor, Department of Artificial Intelligence Converence Chonnam University, Gwangju 61186, Korea

[요 약]

Non Fungible Token(NFT) 시장 확대로 여러 NFT 취약점 사례들이 나타나고 있다. NFT의 경우 스마트계약만 블록체인에 저장하고 실제 미디어 데이터는 외부에 저장한다. 이로 인해 블록체인의 중요한 기능인 무결성이 외부 미디어 데이터에 적용되지 않는다. 외부 저장소로 InterPlanetary File System(IPFS)를 사용하지만, 데이터를 불러올 때 적절한 파일이 없거나 잘못된 파일을 불러오는 경우가 있다. 발급된 NFT가 가리키는 미디어 데이터 주소가 공격자에 의해 변조될 여지가 있다. 이에 해시 알고리즘을 사용하여 무결성을 보장하고 파일 위변조를 감지하는 방안을 제시한다. 해시 알고리즘을 이용해 미디어 데이터 정보를 스마트계약에 저장함으로써 해시값의 무결성을 보장한다. 사용자가 데이터를 불러올 때 무결성을 다시 확인한다. 이 방식은 비용 효과적으로 미디어 데이터의 무결성과 진위를 검증할 수 있게 한다.

[Abstract]

As the Non Fungible Token(NFT) market expands, several cases of NFT vulnerabilities are appearing. In the case of NFT, only the smart contract is stored on the blockchain, and the actual media data are stored externally. This prevents integrity, an important feature of blockchain, from being applied to external media data. InterPlanetary File System(IPFS) is used as an external storage, but there are cases where there is no appropriate file or the wrong file is loaded when loading data. There is room for an attacker to tamper with the media data address indicated by the issued NFT. Therefore, we propose a method that uses a hash algorithm to ensure integrity and detect file forgery. The integrity of the hash value is guaranteed by storing media data information in a smart contract using a hash algorithm. Integrity is re-checked when the user retrieves data. This method makes it possible to verify the integrity and authenticity of media data in a cost-effective way.

색인어 : 블록체인, NFT, NFT 데이터 파일, 스마트계약, 해시
Keyword : Blockchain, Non Fungible Token, NFT Data Files, Smart Contracts, Hash

http://dx.doi.org/10.9728/dcs.2023.24.7.1529

Received 07 June 2023; **Revised** 22 June 2023
Accepted 06 July 2023

***Corresponding Author; Kyungbaek Kim**

Tel: +82 062-530-3438
E-mail: kyungbaekkim@jnu.ac.kr

Ⅰ. 서 론

현재 블록체인 기술은 백서에 따른 비트코인 이후로 단순한 암호화폐 넘어 4차 산업혁명의 핵심 기술로 각광받고 있다. 블록체인의 가장 큰 특징은 중개 기관에 데이터 의존하지 않고 직접 검증, 승인, 합의로 데이터를 관리하는 탈중앙성이다. 탈중앙성으로 모든 기록을 누구나 볼 수 있고 참여자가 내부 이상을 감시할 수 있다[1].

이러한 블록체인에서 디지털 자산 소유권 증명을 위해 NFT가 만들어졌다. NFT는 대체 불가능한 토큰으로 블록체인에 기록되어 추적 용이하고 소유권 증명에 적합하다. 각 NFT가 대체 불가능하므로 유일성을 입증할 수 있다. NFT는 디지털 자산 소유권 증명에 주로 사용된다.

2021년 1월 NFT 최대 마켓인 오픈시에서 프론트엔드 취약점을 이용해 시장 가치의 11%에 해당하는 가격에 NFT를 훔쳐 19만 달러 차익을 얻었다. 2021년 2월 같은 마켓에서 와이번 프로토콜의 유연성을 악용해 중요 정보가 없는 계약서에 서명을 받은 뒤 자신에게 유리한 정보를 추가하며 NFT를 훔쳤다[2].

시장 확대로 외부, 내부 취약점을 이용한 다양한 공격이 나타나고 있다. NFT 사고에 비해 대응 방안은 제한적이다. NFT 사고는 블록체인 네트워크 하드포크나 롤백 등으로 대응한다. 따라서 사고 예방이 중요하다. 현재 NFT 사고는 대부분 외부 요인에 의한 피싱이나 스마트계약 취약점이다. NFT는 블록체인 네트워크 자원 절감을 위해 디지털 콘텐츠를 직접 저장하지 않고 URL을 NFT 데이터에 담는다.

본 논문에서는 NFT 내 이미지 위변조 공격 과정을 설명하고 두 가지 NFT에서 테스트하며 해시 알고리즘으로 무결성 테스트를 진행한다. 해시 알고리즘은 미디어 데이터를 고유한 번호로 변형시켜 스마트계약에 저장함으로써 해시값 무결성을 보장한다. 사용자가 데이터를 불러올 때 무결성을 다시 확인한다. 이는 비용 효과적으로 미디어 데이터 무결성과 진위를 검증할 수 있게 한다.

Ⅱ. 배경 및 관련 연구

2-1 NFT산업의 확대

가상화폐 담당 애널리스트 기관에서 발표한 2021년 1분기 가상화폐 동향 보고에 따르면 NFT 거래량이 2020년 12월 930만 달러에서 2021년 3월 2억 2600만 달러로 약 26배 증가했다. NFT 산업은 가파른 성장세를 이어가고 있다. NFT는 디지털 아이템에 고유 가치를 부여하고, 해당 디지털 아이템에 대한 소유권과 저작권을 나타내준다. 이러한 특성으로 NFT는 디지털 아트, 가상 세계 아이템, 스포츠 카드 등 다양한 분야에서 주목받고 있다.

신종 코로나바이러스 감염증(COVID-19) 사태로 실제 경매나 오프라인 이벤트 등이 축소되면서 온라인으로 진행되는 디지털 아트 경매나 가상 세계 내 아이템 거래 등이 활성화되고 있어 2020년 NFT 거래량이 크게 증가하였고, 이러한 성장세가 2021년에도 이어지고 있는 것으로 나타났다. 또한, 가상세계, e스포츠, 디지털 아트 등 기존 영역에서 NFT 활용 사례가 나타나고 있고 음악, 영화, 출판 등 기존 산업 영역에서도 NFT 기술을 도입하여 수익 창출 모델을 변화시키는 추세로 가고 있다.

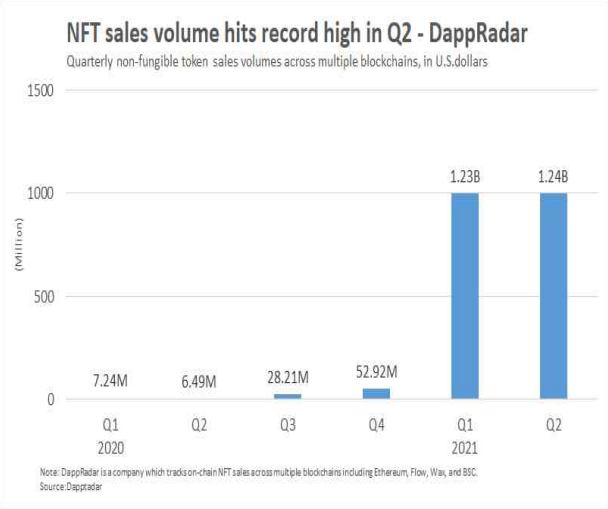

그림 1. DappRadar 2021년 상반기 NFT 거래량 보고서
Fig. 1. DappRadar H1 2021 NFT volume report

2-2 NFC의 특징

NFT(Non Fugible Token)는 대체 불가 토큰으로 기존 블록체인의 탈중앙화 점과 조작 불가능한 특징을 이용하여 디지털 자산의 소유권을 증명하고 암호화폐와 다르게 NFT 각각의 고유한 특성과 정보를 가지고 있다. 이 때문에 디지털 자산의 소유권을 증명하고 희소성을 부여한다[3]. 이러한 NFT의 특징으로는 독립성, 영속성 등이 있다.

표 1. 이더리움 NFT 데이터와 일반데이터의 차이[4]
Table 1. Measuring overhead based on capacity [4]

NFT data	General Data
NFTs are digitally unique, and no two identical NFTs can exist.	Copies of files such as .mp3 or .jpg are identical to the original
All NFTs must have an owner, which is a public record and can be easily verified by anyone	Ownership records are stored on servers managed by the institution and certified by the institution
Content creators can sell their work anywhere and have access to a global marketplace.	Creators depend on the infrastructure and distribution of the platform they use, and have terms of use and geographic restrictions.

2-3 NFT의 스마트 컨트랙트

NFT는 스마트 컨트랙트, 메타데이터, 미디어 데이터의 3가지로 구성된다[5].

1. 스마트 컨트랙트는 소유권 확인, 양도, 로열티 처리 등의 실제 거래 계약 조항을 Solidity 언어로 작성한다. 또한, 그림의 정보가 포함된 메타데이터 주소를 포함한다.
2. 메타데이터는 그림의 정보와 그림이 포함된 주소를 담고 있다.
3. 미디어 데이터에는 NFT를 통해 유일하게 정보를 저장한 디지털 미디어가 포함되어 있다.

블록체인 네트워크 내에서 스마트 컨트랙트가 동작하지만 NFT의 메타데이터나 미디어 데이터의 경우 블록체인 외부에 저장한다. 블록체인 내에 저장할 경우, 높은 수수료와 제한된 블록 데이터 크기로 인한 블록체인 제약으로 인해 원본 데이터를 별도로 저장하는 게 일반적이다. 이러한 구조로 인하여 블록체인 내에서 보호되는 스마트 컨트랙트와 달리 실제로 중요한 미디어 데이터 소유권을 나타내는 NFT 메타데이터는 블록체인 외부의 일반 DB 서버에 저장하기 때문에 블록체인과 동일한 무결성을 보장받기 어렵다. NFT는 블록체인 기술의 장점을 활용하면서도 블록체인의 제약으로 인한 한계를 극복하기 위해 블록체인 내부와 외부에 데이터를 별도로 저장하고 있다. 스마트 컨트랙트를 통해 거래의 안정성과 보안을 보장하면서, 메타데이터와 미디어 데이터는 블록체인 외부 별도 서버에 저장함으로써 블록체인의 제약을 해결하고 있는 구조이다.

2-4 NFT의 스마트 컨트랙트 작동 방식

스마트 컨트랙트는 일반 계약과 달리 제3자 보증 기관을 포함하지 않고 이루어지는 디지털 계약이다. 스마트 컨트랙트는 계약 조건을 코딩하여 자동으로 실행된다. NFT도 스마트 컨트랙트를 사용하여 작동한다. NFT 스마트 컨트랙트의 주요 역할은 NFT 계약을 통해 영구 식별 데이터를 제공하는 것이다. 스마트 컨트랙트는 소유자와 구매자의 계약 조건이 충족되면 자동으로 실행된다.

스마트 컨트랙트의 특징으로 자율성, 투명성, 비용 절감, 확장성 등이 있다. 자율성은 기존 거래에서 보증 기관을 통한 복잡한 절차가 필요했으나 스마트 컨트랙트는 중립적이고 자동화된다. 투명성은 블록체인의 스마트 컨트랙트 내용을 누구나 확인할 수 있고, 성사된 계약은 모든 노드에서 복제된다. 비용 절감은 전체 비용과 중개 비용이 제거된다. 확장성은 어디에서나 사용할 수 있다.

스마트 컨트랙트의 단점은 합의된 요구사항을 모두 반영하는 스마트 컨트랙트를 작성하기 어렵고, 위반사항이 있어도 발견하기 어려운 점이다. 또한, 한번 업로드된 스마트 컨트랙트는 거의 수정할 수 없다. 수정 시 새 트랜잭션과 기존 트랜잭션이 충돌할 수 있다. 스마트 컨트랙트는 블록체인의 특성을 활용하여 보증 기관 없이 자동화된 디지털 계약을 실행한다. NFT에서의 스마트 컨트랙트 또한 소유자의 증명 내용과 외부에 연결된 메타 데이터의 주소를 가지고 있어 증명하는 역할을 가지고 있다.

2-5 NFT 스마트 컨트랙트 종류와 상태변환 원리

NFT 발행 과정에서 사용되는 기본 스마트 컨트랙트는 블록체인 네트워크에 따라 다르게 작성된다. 그러나 NFT가 가진 고유한 상태 변환 원리는 모두 동일하다. 일반적인 FT(fungible token)의 경우 A에서 B로 2만큼 가치를 이전하면 A의 가치가 2만큼 줄어들고 B의 가치가 2만큼 증가한다. 그러나 NFT는 각 토큰이 고유한 가치를 가지므로 A에서 B로 소유권을 이전하더라도 해당 NFT의 가치가 B의 지갑에 추가되고 기존 NFT들도 그대로 남아있다. NFT는 대체 불가능한 성격으로 인해 개별 토큰을 유일한 가치를 가진다. 이러한 NFT의 특성으로 인해 소유권 이전 시에도 개별 NFT의 가치는 변하지 않는다. FT와 달리 NFT의 가치는 개별 토큰 단위로 존재하므로 지갑 간 이전이나 거래에서 개별 NFT의 가치가 합쳐지거나 사라지지 않는다.

2-6 NFT의 유통과정

NFT 토큰의 트랜잭션 내역은 클레이튼 블록체인 네트워크 탐색기 Klaytnscope를 통해 확인할 수 있다. 특정 트랜잭션을 선택하여 토큰 URL을 확인하면 NFT가 포함된 JSON 파일에 접속할 수 있다. JSON 파일에서 이미지 URL을 열면 NFT 이미지에 접근할 수 있다. NFT 발행 과정은 다음과 같다[6].

1. 그림 파일을 개인 서버나 IPFS[7]에 업로드하여 URL 생성
2. 그림 파일 정보를 담은 JSON 파일 작성 및 서버 업로드로 URL 생성
3. 생성된 URL을 KIP-17 클레이튼 NFT 표준 스마트 컨트랙트 코드에 맞게 작성
4. 완성된 스마트 컨트랙트를 클레이튼 블록체인에 배포하여 N로써 유통이 완료된다.

2-7 NFT 데이터의 저장 방식

NFT의 경우 블록체인에 용량이 크고 중요한 미디어 데이터나 메타데이터를 직접 저장할 경우 비용이 비례하게 증가한다. 따라서 NFT의 데이터는 주로 블록체인 외부에 저장된다. NFT 데이터를 저장하는 주된 방식에는 중앙 집중식 스토리지, IPFS, Arweave 등이 있다.

1. 중앙 집중식 스토리지: NFT 작성자의 개인 서버를 사용한다. 서버 유지가 중단되면 데이터와 NFT 링크가 사라지고 NFT 가치가 훼손된다.
2. IPFS: P2P 파일 저장 네트워크로, 컴퓨터 네트워크의 노드에 파일을 업로드하고 해시를 사용하여 식별한다. 요청 시 해당 노드에서 파일을 제공한다. 지속성이 보장되지 않고, 데이터 유지를 위해 노드가 직접 데이터를 고정하고 1개 이상의 노드가 유지해야 한다.
3 Arweave: 지속성이 보장되는 분산형 파일 스토리지 네트워크다. 사용자는 200년 저장 비용을 일시불로 지급한다. 데이터 스토리지 가격 하락을 기반으로 비용을 추정한다. 새 데이터 블록은 이전 블록과 연결된다.

중앙 집중식 스토리지의 경우 NFT의 가치를 해칠 위험이 있다. IPFS는 지속성이 보장되지 않고 수동으로 데이터 유지가 필요하다. Arweave는 지속적인 저장을 위한 일회성 비용 지급 모델을 제공한다. NFT 생태계 내 데이터 저장 방식은 NFT의 특성에 부합하고 지속 가능해야 한다. Arweave와 같이 장기적 데이터 보존을 보장하는 저장 기술을 기반으로 하는 방식이 NFT의 가치를 유지하는 데 더욱 적합할 것으로 보인다. 향후 NFT 시장의 성장에 따라 더욱 지속 가능하고 비용 효율적인 데이터 저장 기술이 요구된다.

2-8 NFT 주요 공격 기법

첫 번째로 ERC-721 기반 소스 코드 취약점을 이용한 공격이 있다. 이는 NFT를 추적하고 전송하는 기능을 담당하는 'setApprovalForAll'에 존재하는 취약점을 악용하여 NFT가 탈취되는 사고가 발생했다. 이러한 소스 코드가 유출될 경우 해커는 이용자 또는 NFT 서비스 마켓의 지갑 내 NFT 및 암호 자산을 쉽게 탈취할 수 있다. 이 때문에 스마트 컨트랙트의 취약점은 CVE 취약점 리포트를 통해 지속적으로 보고하고 관리한다. 또한 VeriSmart[8]와 같은 취약점 도구를 이용하여 탐지한다.

두 번째로 블록체인 오라클은 블록체인 네트워크와 외부 데이터를 연결하는 장치 또는 시스템이다. 오라클은 블록체인 네트워크가 외부 데이터에 접근하고, 외부 데이터가 블록체인 네트워크에 접근할 수 있도록 한다. 이로 인해 블록체인 네트워크는 외부 데이터를 활용하여 다양한 서비스를 제공할 수 있다[9].

세 번째로 사회 공학적 공격 기법이 사용된다. 공격자는 문자, 이메일, SNS 등을 이용하여 허위 사이트 주소를 이용자에게 전송하고, 이용자가 허위 사이트에 정보를 입력하도록 유도한다. 공격자는 이용자의 정보를 통해 NFT를 탈취한다. 또한, 공격자는 허위 플랫폼 또는 공격자 지갑으로 연결한 뒤, 정상적인 거래가 발생한 것처럼 위장하여 메시지를 전송한다. 이때 공격자는 이용자에게 개인키 서명을 유도하여 공격자에게 직접 자산을 이관한다[10].

마지막으로 NFT를 거래하는 서비스 플랫폼에 대한 공격들이 있다. 해커는 악의가 있는 NFT를 직접 수신자에게 보내고, 수신자가 해당 NFT를 확인하려고 할 때 해커는 공격 대상자의 NFT 권한을 얻어 지갑에 있는 NFT와 자산을 훔친다. 또한 이중 인증이 되지 않은 계정의 경우 해킹을 통해 가진 NFT를 해커의 지갑으로 옮기고 판매한다. NFT 마켓 사이트에서 직접 취약점을 악용하여 구매나 판매 가격을 조작하여 저렴한 가격에 NFT를 얻고 높은 가격에 다시 판매하는 공격이다. 해커가 악의가 있는 NFT를 받는 사람에게 직접 보내고 받는 사람이 그 NFT를 보려고 할 때 해커는 공격 대상자의 NFT 권한을 가져가 지갑에 있는 NFT와 자산을 훔친다[11].

Ⅲ. 분산 저장을 이용한 NFT 무결성 검사

3-1 해시 알고리즘을 이용한 NFT 데이터 무결성 검사

기존 유통되는 NFT는 대부분 최종 미디어 데이터를 바깥 서버에 저장한다. 그러므로 중간중간 메타데이터가 가리키는 미디어 데이터 URL이 바뀌면 NFT의 디지털 증명서 역할을 할 수 없다[12]. 일반적인 검사 방법으로 tripwire, Fcheck 등이 있지만 NFT는 소유권이 자주 바뀌기 때문에 일반적으로 데이터베이스를 관리하기 어렵다. 그래서 해시값을 직접 스마트 계약에 저장하고 데이터 무결성을 지키고 사용자가 데이터를 불러올 때 두 번 확인해 위변조를 검사하는 방법을 제안한다. 사용자가 NFT 미디어 데이터를 요청하면 블록체인 네트워크 안의 해시값과 바깥의 메타데이터 해시값을 각각 불러와 해시값을 비교하여 위변조를 확인한다. 제안한 NFT 미디어 데이터 로딩 시 해시를 사용한 무결성 검사 알고리즘은 다음과 같다.

1단계 : 처음 사용자가 미디어 데이터를 요청하면 스마트 계약의 getHash 함수로 해시값을 받아 변수에 저장한다.
2단계 : 스마트 계약 안에 메타데이터 주소로 가서 메타데이터의 description 값을 변수에 저장한다.
3단계 : 각 저장된 변수를 비교하여 무결성 검사를 진행하고, NFT 발행한다. 발행된 NFT는 오픈씨, 액시, 크립토펑크와 같은 NFT 거래소에 등록되어 판매된다. 사용자는 거래소에서 지갑을 등록하여 구매한다. 구매 시 거래소는 수수료를 받고, 제작자의 NFT 스마트 컨트랙트를 통해 NFT를 발급하여 사용자 지갑에 소유권을 입력한다. NFT 발행을 위해 그림 및 정보를 개인 서버나 IPFS에 업로드하고, URL과 스마트 컨트랙트를 생성한다. 배포된 NFT는 NFT 거래소를 통해 유통되고 이용자는 거래소에서 지갑을 연동하여 NFT를 구매하게 된다. 구매 시 거래소는 스마트 컨트랙트

를 통해 NFT를 발급하고 소유권을 지갑에 입력한다.

4단계 : 무결성이 확인되면 이미지 URL로 최종적으로 사용자가 처음 요청한 NFT 이미지를 호출한다. 보통 경로에서 NFT 데이터는 블록체인 네트워크에서 스마트 계약을 통해 호출되면 정상 메타데이터를 거쳐 최종 NFT 데이터 파일에 도달하여 불러온다. 그렇지만 메타데이터가 악성코드에 걸리거나 다른 악성 링크로 주소가 바뀌었을 때 사용자는 악성코드를 호출하기 전까지 대처 방법이 없다. 그래서 기존의 무결성을 보장할 NFT 데이터를 해시 데이터로 바꾸어 각각 스마트 계약 안과 메타데이터에 분산 저장하여 호출 시 두 해시값을 비교하여 무결성 검사를 하면 악성코드 피해를 막을 수 있다.

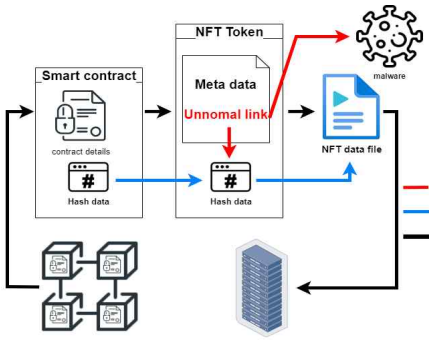

그림 2. 해시 분산 저장을 이용한 NFT 데이터 무결성 검사
Fig. 2. NFT data integrity checks using distributed hash storage

3-2 NFT 데이터 공격 시나리오 설정

일반적인 상황에서 소비자가 NFT를 구매하고 미디어 데이터를 불러올 때의 상황에서의 공격 과정을 설정하였다. 2.6에서 설명한 NFT 유통과정과 동일하게 Json 파일을 구성하고 이후 연결된 데이터를 이미지 서버에 업로드하였다. 소비자가 해당 NFT의 소유권을 얻게 되었을 때 공격자는 기존에 주소에 연결된 데이터를 경로만 일치하여 악성 데이터로 바꾸었다. 이때 사용자는 기존과 같이 해당 NFT 데이터에 접근하도록 하였다.

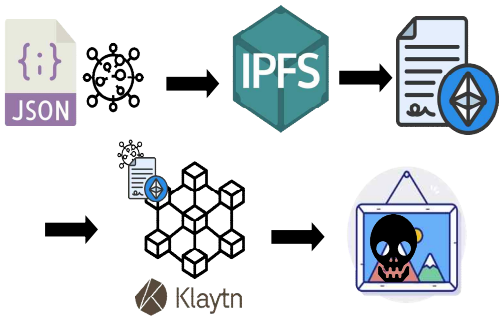

그림 3. NFT 데이터 공격 시나리오
Fig. 3. NFT data attack scenarios

3-3 NFT 스마트 컨트랙트 구성

스마트 계약 안에 getHash 함수를 사용하여 NFT에서 쓸 미디어 데이터의 해시값을 입력받는다. 그 데이터는 스마트 계약 안에 저장되기 때문에 모두가 볼 수 있고 가스를 사용하여 그 값을 변경할 수 있다. 함수를 불러와 기존에 들어있는 해시값을 확인할 수 있다. 이를 통해 기존 값이 변조되었는지 미디어 데이터에 접근하기 전에 우선 확인이 가능하다. 또한, 기존 무결성 검사가 필요로 했던 원본 DB값을 별도로 저장해야 했던 점이 있었지만, 스마트 계약을 통해 해시값을 저장하게 되면 블록체인 네트워크에 저장되어 DB 자체적으로 무결성을 보장받게 된다.

그림 4. 스마트 컨트랙트에 입력된 해시로드
Fig. 4. Hashload entered in the smart contract

3-4 NFT 메타 데이터 구성

보통 환경에서 메타데이터는 description, external_url, image, name, attributes 속성이 있다. 여기에서 description 속성으로 NFT 설명이나 여러 가지 특징 설명한다. image를 보면 실제 미디어 데이터 바깥 주소가 적혀 있다. 이를 통해 메타데이터는 연결된 이미지 정보 제공하고 더 나아가 이미지 자체 불러오는 데 쓰인다.

```
{
  "description": "Friendly OpenSea Creature that enjoys long swims in the ocean.",
  "external_url": "https://openseacreatures.io/3",
  "image": "https://storage.googleapis.com/opensea-prod.appspot.com/puffs/3.png",
  "name": "Dave Starbelly",
  "attributes": [ ... ]
}
```

그림 5. NFT json 파일 양식
Fig. 5. NFT json file form

Ⅳ. 실험 및 결과

4-1 실험 환경

블록체인 테스트 넷은 임시 네트워크로, 실제 블록체인 네

트워크를 테스트하기 위해 사용된다. 테스트 넷은 기능과 성능을 확인하거나 새로운 기능, 프로토콜, 애플리케이션을 실험하는 용도로 활용된다. 하지만 테스트 넷은 실제 블록체인 네트워크와 완전히 동일한 환경을 제공하지는 않기 때문에 노드 수나 처리되는 트랜잭션 수가 실제 환경과 동일하지 않을 수도 있다.

테스트 넷은 블록체인 네트워크의 종류에 따라서도 달라진다. 본 실험에서는 이더리움 블록체인 테스트 넷으로 구성하였다. 이더리움 블록체인과 동일한 환경을 제공한다. 해당 실험에서는 블록 생성 속도와 노드 생성을 제한하였지만 일반적인 환경과 같은 요소를 조정하였다. 또한, 블록체인 테스트 넷 환경 구성에서는 로컬 테스트 넷, 정적 테스트 넷, 동적 테스트 넷이 있는데 해당 실험에서는 실제 NFT를 제작하고 사용자가 사용하기 전까지 데이터를 관리하고 데이터의 전체적인 흐름을 관찰하기 위해 로컬 구조 테스트 넷을 활용했다.

1) 실험 환경 구성

블록체인 네트워크에서 사용자 NFT 미디어 데이터 불러올 때 전체 구조도다. 스마트 계약 만들어 직접 블록체인 네트워크로 배포 진행하고, 데이터 저장되는 DB 서버는 라즈베리 써서 SFTP 서버로 구축했다. 가나슈로 4개 블록 로컬 네트워크 구성했다. 첫 번째 블록 제네시스 블록이고 나머지 블록 랜덤하게 만들어 연결했다.

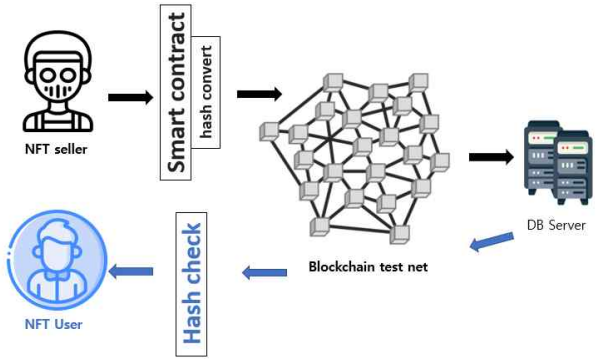

그림 6. NFT 데이터 로드 전체 구성도
Fig. 6. NFT data load overall block diagram

2) 테스트 파일 셋 선택

NFT 거래소 오픈씨[13]에서 지원하는 NFT 형식 중에서 가장 많이 사용되는 형식인 gif, jpg, png, svg, mp4, mp3, wav, ogg을 미디어 데이터로 사용했다. 각 파일 형식당 여러 해시값 테스트를 진행했다. 또한, NFT의 특성상 다양한 용량을 테스트하기 위해 100KB부터 1GB까지의 다양한 용량의 더미 파일을 제작하여 무결성 테스트를 진행했다. 일반적으로 실제 유통되는 NFT 미디어 데이터를 가져와 비교 테스트를 하기 위해 거래소에서 TOP10위 안에 드는 NFT 중에서 무작위로 선정하여 데이터 셋에 추가했다.

3) 클레이튼 KIP-17 환경 설정

테스트넷 사용부터 배포 및 계약 실행까지 한 번에 사용이 가능한 Remix IDE를 통하여 환경을 구축하고 KIP-17을 제작 및 배포하였다. 이때의 미디어 데이터 부분도 외부 ftp 서버를 통하여 저장하였다. 일반적인 환경 설정과 다르게 IDE의 경우 블록체인 네트워크 속 블록들 또한 자동으로 생성하여 기초적인 클레이튼[14] NFT 환경 구성이 가능하다.

4-2 실험 결과 분석

1) 일반적인 호출방식

해시 비교 없이 일반적인 상황에서 기존 미디어 데이터 파일이 악성 파일로 주소가 바뀌었을 때 필터링 없이 직접 호출했을 경우, 바깥 저장소에 저장되어 있던 악성 파일이 메타데이터 URL로 호출되고 다시 그 데이터에서 스마트 계약으로 url_call 함수로 입력받게 된다. 최종 사용자는 바뀐 악성 파일을 설치하게 된다. 이 결과로 NFT가 스마트 계약에 블록체인 무결성을 보장받지만, 바깥 저장소에 연결된 미디어 데이터는 무결성을 보장받지 못하고 이런 악성코드 공격에 취약하다는 것을 증명했다.

2) 해시 알고리즘의 비교를 통한 호출

미디어 데이터 불러오기 전 메타데이터 해시 정보 먼저 불러와 블록체인에 담긴 스마트 계약과 해시 비교해 미디어 데이터 위변조된 것인지 판단할 수 있었다. NFT에서 주로 쓰는 파일 확장자에 대해 해시로 호출했을 때 기존 시간과 차이가 거의 없었다. 동일용량 경우 오차 범위 내 차이 보여주고 약간 용량 차이 때문에 생기는 것으로 나타났다.

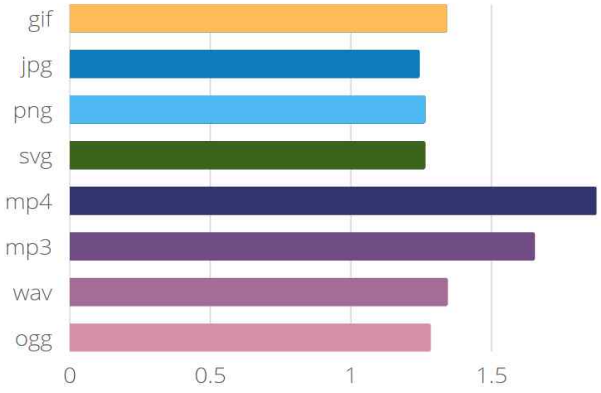

그림 7. 파일 확장자에 따른 전송속도(bps)
Fig. 7. Transfer speed (bps) based on file extension

3) 해시 종류에 따른 성능 평가

Hashlib에서 쓰는 대표적인 해시인 BLAKE2b[15], MD5[16], SHAKE, SHA3[17]를 썼다. 같은 조건으로 테스트해 속도와 용량 측정했다. 테스트 세트는 동일한 용량 데이터 파일 썼다. 알고리즘별 오버헤드만 측정했다. BLAKE2b

해시 알고리즘이 변환 속도에서 높은 성능 보여주고 용량도 64비트라 스마트 계약 안에 등록돼 블록체인 네트워크 올라갔을 때 수수료 부담 가장 적은 것으로 나타났다.

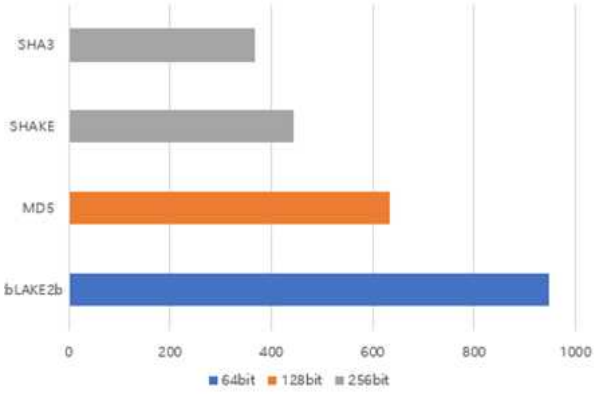

그림 8. 해시 jpg 전송시 알고리즘별 속도(MiBps)
Fig. 8. Speed per algorithm when sending hashed jpgs (MiBps)

4) NFT 데이터 용량에 따른 성능 변화

NFT는 NFT 제작자에 따라 다양한 크기의 NFT가 만들어진다. 이에 대응하기 위해 여러 크기의 NFT 데이터를 해시 MD5 알고리즘으로 테스트했다. 대부분 기존 0.1MB, 1MB에서는 2~40 Mibps로 매우 빠른 속도로 처리됐다. NFT 최대 거래소 오픈씨에서 판매 중인 TOP10 파일 용량 평균 1.6mb로 일반적인 NFT 상황에서 오버헤드 없어 사용자 불편 없다. 그 중 10mb 이하일 때 앞선 알고리즘별 데이터 속도와 비교하면 blake2b에서 약간 앞선 차이 보였다. 하지만 100mb 넘어가며 md5 알고리즘이 안정적으로 오버헤드 가장 적게 증가한 것에 비해 나머지 알고리즘들은 큰 폭으로 증가했다. 이를 통해 평균적으로 blake2b 쓰는 게 적절하고 용량 클수록 md5 쓰는 게 안정적이다.

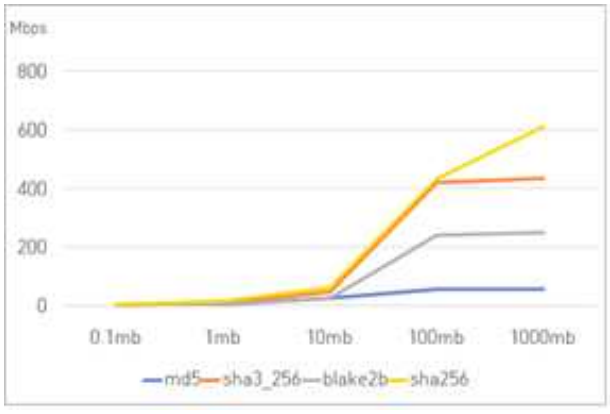

그림 9. 용량에 따른 오버헤드 측정
Fig. 9. Measuring overhead based on capacity

V. 결 론

이 논문에서는 NFT 시장에서 발생할 수 있는 데이터 위변조 문제를 해결하기 위해, 블록체인과 해시 알고리즘을 활용한 방법을 제안하고 있다. 구체적으로, 미디어 데이터 불러오기 전 메타데이터 해시 정보를 먼저 불러와 블록체인에 담긴 스마트 계약과 해시 비교해 미디어 데이터 위변조 여부를 판단하고 있다. 이를 통해 NFT에서 주로 쓰고 있는 파일 확장자에 대해 해시로 호출했을 때 기존 시간과 차이가 거의 없다는 것을 검증하고 있다.

따라서, 이 논문에서 제안한 방법은 블록체인과 해시 알고리즘을 활용하여 NFT 시장에서 발생할 수 있는 데이터 위변조 문제를 해결하는 데 효과적이며, BLAKE2b 해시 알고리즘이 가장 적합한 알고리즘이라는 것을 검증하고 있다. 최근 예술 작품이나 게임 아이템 등의 유니크한 데이터 검증 보관에 대한 수요가 증가함에 따라, 이 기술은 디지털 자산의 소유권을 보장하고, 위 변조 방지하는 데 활용될 것으로 기대된다[18].

감사의 글

본 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임. (IITP-2022-0-01203) 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 지역지능화혁신인재양성사업의 연구결과로 수행되었음 (IITP-2023-RS-2022-00156287)

참고문헌

[1] R. C. Park and Y. S. Lee, “An Overview of Blockchain Technology: Concepts, Consensus, Standardization, and Security Threats,” *Journal of the Institute of Convergence Signal Processing*, Vol. 20, No. 4, pp. 218-225, December 2019.

[2] ET News. World’s Largest NFT Exchange ‘OpenSea’ Phishing Accident…“Hundreds of NFTs Stolen” [Internet]. Available: https://www.etnews.com/20220221000220.

[3] Ethereum. NFT [Internet]. Available: https://ethereum.org/ko/nft/.

[4] 2e Consulting. It’s Not ‘Irreplaceable’, It’s a ‘Token’! Let’s Get It Right, Blockchain and NFT Technologies [Internet]. Available: https://www.2e.co.kr/news/articleView.html?idxno=302178.

[5] Klaytn Improvement Proposals. KIP 17: Non-Fungible Token Standard [Internet]. Available: https://kips.klaytn.foundation/KIPs/kip-17.

[6] JoCoding. How to Make Clayton-based NFTs [Internet].

Available: https://ttfent.notion.site/ttfent/NFT-JoCoding-06741e9e2cc448758099d818072367cb.

[7] LG CNS Blog. Distributed Web 'IPFS' Using Blockchain Technology Has Appeared! [Internet]. Available: https://www.lgcns.com/blog/it-trend/31193/.

[8] S. So, M. Lee, J. Park, H. Lee, and H. Oh, "VeriSmart: A Highly Precise Safety Verifier for Ethereum Smart Contracts," in *Proceedings of 2020 IEEE Symposium on Security and Privacy (SP)*, San Francisco: CA, pp. 1678-1694, May 2020. https://doi.org/10.1109/SP40000.2020.00032

[9] HashNetWiki. Oracle Problems [Internet]. Available: http://wiki.hash.kr/index.php/%EC%98%A4%EB%9D%BC%ED%81%B4_%EB%AC%B8%EC%A0%9C.

[10] KISA. [KISA Insight 2022 Vol.04] Metaverse and NFT, Cybersecurity Threat Outlook and Analysis [Internet]. Available: https://www.kisa.or.kr/20301/form?postSeq=12&lang_type=KO

[11] D. Das, P. Bose, N. Ruaro, C. Kruegel, and G. Vigna, "Understanding Security Issues in the NFT Ecosystem," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22)*, Los Angeles: CA, pp. 667-681, November 2022. https://doi.org/10.1145/3548606.3559342

[12] X. Yan, Y. Xu, B. Cui, S. Zhang, T. Guo, and C. Li, "Learning URL Embedding for Malicious Website Detection," *IEEE Transactions on Industrial Informatics*, Vol. 16, No. 10, pp. 6673-6681, October 2020. https://doi.org/10.1109/TII.2020.2977886

[13] OpenSea. NFT Marketplace [Internet]. Available: https://opensea.io/.

[14] Klaytn Api Service. What are the KCT, KIP-7, KIP-17? [Internet]. Available: https://support.klaytnapi.com/hc/en-us/articles/4403232605711-What-is-KCT-KIP-7-and-KIP-17.

[15] HashNetWiki. Blake2B [Internet]. Available: http://wiki.hash.kr/index.php/%EB%B8%94%EB%A0%88%EC%9D%B4%ED%81%AC2B.

[16] A. K. Kasgar, M. K. Dhariwal, N. Tantubay, and H. Malviya, "A Review Paper of Message Digest 5 (MD5)," *International Journal of Modern Engineering & Management Research*, Vol. 1, No. 4, pp. 29-35, December 2013.

[17] Vitis Security Library. SHA-3 Algorithms [Internet]. Available: https://xilinx.github.io/Vitis_Libraries/security/2019.2/guide_L1/internals/sha3.html.

[18] H. J. Song, NFT File Using Hash Password Integrity Verification and Forgery Detection, Master's Thesis, Chonnam National University, Gwangju, February 2023.

송효준(Hyojun Song)

2021년 : 조선대학교 (학사)
2023년 : 전남대학교 대학원 (석사)

2015년~2021년: 조선대학교 컴퓨터공학과
2021년~2023년: 전남대학교 정보보안협동과정 석사
※관심분야 : 블록체인, NFT, 클라우드컴퓨팅, 빅데이터, 인공지능 등

정송헌(Songheon Jeong)

2022년 : 광주대학교 (학사)
2023년 : 전남대학교 대학원 (석사과정)

2016년~2022년: 광주대학교 사이버보안경찰학과
2022년~현 재: 전남대학교 정보보안협동과정 석사과정
※관심분야 : 정보보호(Personal Information), 클라우드, 모빌리티, 블록체인 등

김경백(Kyungbeak Kim)

1999년 : 한국과학기술원 전기 및 전자공학과(학사)
2001년 : 한국과학기술원 전기 및 전자공학과(석사)
2007년 : 한국과학기술원 전기 및 전자공학과(박사)
2007년~2008년: Network and Distributed Systems Group, Dept. Computer Science, University of California Irvine
2008년~2012년: Information Systems Group, Dept. Computer Science, University of California Irvine
2012년~2016년: 전남대학교 전자컴퓨터공학과 조교수
2016년~2021년: 전남대학교 전자컴퓨터공학과 부교수
2021년~현 재: 전남대학교 소프트웨어공학과/인공지능학부 교수
※관심분야 : 지능형 분산시스템, SDN/NFV, 빅데이터 플랫폼, 인공지능, 블록체인, 클라우드 등