KIPS Trans. Comp. and Comm. Sys.
Vol.11, No.11 pp.403~410
ISSN: 2287-5891 (Print), ISSN 2734-049X (Online)

https://doi.org/10.3745/KTCCS.2022.11.11.403

A Study on Non-Fungible Token Platform for Usability and Privacy Improvement

Kang Myung Joe† · Kim Mi Hui††

ABSTRACT

Non-Fungible Tokens (NFTs) created on the basis of blockchain have their own unique value, so they cannot be forged or exchanged with other tokens or coins. Using these characteristics, NFTs can be issued to digital assets such as images, videos, artworks, game characters, and items to claim ownership of digital assets among many users and objects in cyberspace, as well as proving the original. However, interest in NFTs exploded from the beginning of 2020, causing a lot of load on the blockchain network, and as a result, users are experiencing problems such as delays in computational processing or very large fees in the mining process. Additionally, all actions of users are stored in the blockchain, and digital assets are stored in a blockchain-based distributed file storage system, which may unnecessarily expose the personal information of users who do not want to identify themselves on the Internet. In this paper, we propose an NFT platform using cloud computing, access gate, conversion table, and cloud ID to improve usability and privacy problems that occur in existing system. For performance comparison between local and cloud systems, we measured the gas used for smart contract deployment and NFT-issued transaction. As a result, even though the cloud system used the same experimental environment and parameters, it saved about 3.75% of gas for smart contract deployment and about 4.6% for NFT-generated transaction, confirming that the cloud system can handle computations more efficiently than the local system.

Keywords : Non-Fungible Token, Blockchain, Cloud Computing, Usability and Privacy Improvement

사용성 및 프라이버시 개선을 위한 NFT 플랫폼 연구

강 명 조† · 김 미 희††

요 약

블록체인 기반으로 생성된 NFT는 자신만의 고유한 값을 지녀 위변조가 불가하며 다른 토큰이나 코인과 교환될 수 없다. 이러한 특성을 이용해 이미지나 비디오, 예술작품, 게임 캐릭터 및 아이템 등과 같은 디지털 자산에 NFT를 발행하여 사이버상에 존재하는 수많은 사용자와 객체들 사이에서 디지털 자산의 소유권을 주장할 수 있으며, 동시에 원본 증명도 가능하다. 하지만, 2020년 초기부터 NFT에 관한 관심이 폭발하여 블록체인 네트워크에 많은 부하를 일으켰고, 이에 따라 사용자들은 연산 처리가 늦어지거나 채굴 과정에 매우 큰 수수료가 발생하는 문제점을 겪고 있다. 또한, 사용자들의 모든 행위가 블록체인 장부에 저장되고 디지털 자산은 블록체인 기반 분산 파일 저장 시스템에 저장되어 자신의 신분을 밝히고 싶지 않은 사용자의 개인정보가 불필요하게 노출될 가능성이 있다. 본 논문에서는 클라우드 컴퓨팅과 접근 게이트, 변환 테이블, 클라우드 아이디 등을 활용한 NFT 플랫폼을 제안하여 기존 시스템에서 발생하는 사용성 문제와 프라이버시 문제를 개선할 수 있도록 한다. 로컬시스템과 클라우드 시스템의 성능 비교를 위해 스마트 계약 배포 및 NFT 발행 트랜잭션 연산 처리에 사용된 가스를 측정했다. 그 결과, 클라우드 시스템이 같은 실험 환경 및 파라미터를 사용했음에도 스마트 계약 배포에는 약 3.75%, NFT 생성 트랜잭션 처리에는 약 4.6%의 가스를 절약하는 결과를 도출했고, 이를 통해 클라우드 시스템이 로컬시스템보다 효율적으로 연산을 처리할 수 있음을 확인했다.

키워드 : NFT, 블록체인, 클라우드 컴퓨팅, 사용성 및 프라이버시 개선

1. 서 론

최근 블록체인의 발전에 따라 코인 및 토큰에 관심이 커졌고, 코로나19의 여파로 오프라인에서 할 수 있는 운동, 미팅, 모임 등의 활동보다 음악 감상, 게임 등 온라인에서 이루어질 수 있는 활동이 활발히 이루어졌다. 이러한 과정으로 사람들은 온라인에서 가치를 갖는 디지털 자산에 관심이 커졌고, 코인 및 토큰에 관한 관심과 디지털 자산에 관한 관심이 합쳐져 대체불가 토큰(NFT: Non-Fungible Token)도 주목받게 되었다. 대체불가 토큰은 블록체인 네트워크에서 사용하는 토큰의 일종으로, 단일 개체를 고유한 개체로 만들 수 있는 유일한 값을 지녀 다른 토큰들과 교환할 수 없고 위변조할 수 없는 특징을 가진다[1]. NFT를 음악, 비디오, 이미지와 같은

※ 이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2018R1A2B6009620).
※ 이 논문은 2022년 한국정보처리학회 ASK 2022에서 "개인정보 보호 및 성능 개선을 위한 NFT 플랫폼 연구"의 제목으로 발표된 논문을 확장한 것임.
† 준 회 원 : 한경대학교 컴퓨터응용수학부 석사과정
†† 종신회원 : 한경대학교 컴퓨터응용수학부 컴퓨터시스템연구소 교수
Manuscript Received : August 1, 2022
Accepted : September 4, 2022
* Corresponding Author : Kim Mi Hui(mhkim@hknu.ac.kr)

디지털 미디어 자산에 발행할 경우 해당 미디어 시장에서의 가치가 암호화폐로서 인정되어 디지털 자산의 원본을 인증함과 동시에 블록체인 네트워크에서 자유롭게 사고팔 수 있다. 또한, NFT는 소유주가 변경될 때마다 전자서명을 갱신하여 지금까지 해당 NFT를 소유하고 있던 모든 사용자를 확인할 수 있고, 공연 표나 예술품과 같이 위조가 쉬운 항목들에 대해 원본 증명을 쉽게 할 수 있다[2]. 이러한 특징을 가진 NFT의 가치는 게임 속 아이템 및 캐릭터, 그림이나 음악과 같은 예술, TV 프로그램이나 스포츠 경기의 하이라이트 비디오 유형 등에서 더 큰 가치를 인정받아 한화 약 1,000원에 매매되는 NFT부터, 약 1억~30억에 거래되는 NFT도 존재한다. 국내의 예로, 간송미술관에서 국보 70호인 훈민정음해례본을 100개의 NFT로 나누어 개당 1억 원에 판매하였고, 방송사 MBC에서 시청자들이 재밌어하고 좋아하는 부분만 따로 편집한 영상 클립에 NFT를 발행하여 MBC Archive에서 판매하고 있다. 해외의 예로, 가장 오래된 NFT 프로젝트 중 하나인 크립토펑크는 픽셀로 나타낸 캐릭터 집합 10,000개에 대해 서로 다른 NFT를 발행했다. 발행 초기에는 사람들의 많은 관심을 받지 못했으나, 해외 유명인들과 기업이 구매하여 사람들이 하나의 예술품으로써 취급해 현재까지 가장 높은 가격에 판매된 토큰은 약 140억 원이다. 다른 예시로, 비슷한 이름의 크립토키티는 자신만의 개별화된 가상 고양이 캐릭터를 수집하고 다른 고양이와 교배시켜 새로운 고양이를 번식시키는 게임으로, 출시 당시 이더리움 네트워크에 엄청난 부하를 일으켰다. 게임 속 고양이들은 전부 NFT로 취급되며 사람들에게 인기가 많은 유전형질을 가지고 태어난 고양이의 경우 약 14만~17만 달러의 가치를 갖는다[3-5].

이처럼 NFT 시장 규모가 확대됨에 따라, NFT 생성과 관련된 연산, NFT 매매 과정에서의 연산, 디지털 자산 및 메타데이터 저장과 관련된 연산 등이 폭발적으로 증가하여 연산 처리 속도가 감소하고 채굴 과정의 수수료가 커져 네트워크 참여자들이 불편함을 겪고 있다. 또한, 네트워크 참여자 중 자신의 지갑 주소와 디지털 자산 소유 정보 등 여타 개인정보를 공개하고 싶지 않은 사람이 있는 경우, 현재 NFT 플랫폼에서는 파일 저장을 주로 분산 파일 저장 시스템(IPFS: InterPlanetary File System)을 사용하기 때문에 이를 해결하기는 쉽지 않다[6,7]. 이러한 문제점을 개선하기 위해 본 논문은 클라우드 컴퓨팅을 이용해 블록체인 네트워크를 서비스로 제공하는 BaaS(Blockchain as a Service)를 이용한 NFT 시스템[8]을 상세 설계하여 기존보다 개선된 NFT 플랫폼을 제안하고, 로컬시스템과 클라우드 시스템을 구현하여 성능을 비교한다.

서론에 이어 2장 배경지식에서는 제안시스템의 이해를 위한 기본 개념을 소개하며, 3장 제안시스템에서는 본 논문에서 제안한 클라우드 컴퓨팅을 이용한 NFT 플랫폼을 소개한다. 4장 실험 결과 및 분석에서는 클라우드 컴퓨팅을 이용한 블록체인 네트워크와 기존 블록체인 네트워크의 성능을 비교하기 위해 진행한 실험의 방법과 결과를 설명하며, 마지막 5장 결론에서는 클라우드 컴퓨팅을 이용한 NFT 플랫폼의 의의를 제시하고, 제안시스템의 향후 연구 방향 및 보완점 등을 서술한다.

2. 배경 지식

2.1 대체불가 토큰

이더리움 블록체인의 스마트 계약으로 파생되는 대체불가 토큰, NFT는 블록체인의 투명성, 신뢰성과 같은 특성을 바탕으로 생성되며, 토큰마다 고윳값을 지녀 다른 토큰 및 코인들과 호환되지 않아 위변조가 불가하다. 이러한 특성을 이용해 디지털 자산에 NFT를 발행할 경우, 해당 디지털 자산이 원본임을 증명할 수 있어 이미지, 비디오, 게임 아이템 및 캐릭터, 공연 표, 예술작품 등의 소유권 보장 및 원본 증명에 사용된다. 블록체인 네트워크에서 NFT를 발행한 디지털 자산 저장 및 처리를 진행하려면, 매우 큰 연산과 채굴 비용이 발생하기 때문에 디지털 자산의 핵심 정보인 메타데이터를 추출하여 블록체인 네트워크에 저장하고, 디지털 자산은 IPFS를 통해 저장한다[1]. Fig. 1은 NFT를 발행한 디지털 자산의 메타데이터 예시를 나타낸다. 메타데이터는 키와 값의 짝으로 구성된 JSON(Javascript Object Notation) 형식을 이용해 작성하며, 디지털 자산의 이름, 유형, 저장 위치, 설명 등을 포함한다. Fig. 1의 메타데이터 예시에서는 화가 반 고흐의 별이 빛나는 밤이라는 그림을 예로 들어 작성했다.

최근 사이버상에 있는 디지털 자산에 관심을 많이 가지면서 NFT 시장은 2020년 초반기부터 급성장해 현재 약 400억 달러 이상의 시장 규모를 달성했고, 앞으로도 꾸준히 성장할 기세를 보인다. 많은 NFT의 경우 이더리움 네트워크의 ERC-721(ERC: Ethereum Request for Comment) 토큰 기반으로 생성되는데, NFT에 관한 관심 및 연산이 폭발적으로 증가함에 따라 네트워크에 많은 부하가 발생하여 연산이 처리되지 못하고 쌓여있거나 느리게 처리되었고, 연산을 처리하기 위해 채굴에 드는 비용이 증가했다. 이를 완화하기 위한 노력으로 Flow[9], WAX[10]와 같은 플랫폼이 등장했다.

2.2 클라우드 컴퓨팅

클라우드 컴퓨팅은 서비스의 범위에 따라 서비스형 인프라(IaaS: Infrastructure as a Service), 서비스형 플랫폼(PaaS: Platform as a Service), 서비스형 소프트웨어(SaaS: Software as a Service)로 나눌 수 있다. IaaS는 스토리지, 운영 체제, 네트워크, 메모리 등 하드웨어 컴퓨팅 자원을 인터

```
{
    “name”: “The Starry Night”,
    “image”: “http://gohhexample/picture/starrynight.png”,
    “description”: “Vincent Willem van Gogh’s Drawing”
}
```

Fig. 1. Example of NFT Metadata[8]

넷으로 제공하는 서비스를 뜻한다. PaaS는 사용자가 자신이 작성한 소프트웨어나 서비스를 배포할 수 있는 환경 및 플랫폼을 제공하는 서비스로서 사전 정의된 운영 체제 및 응용프로그램 구성을 제공한다. SaaS는 응용프로그램이나 소프트웨어를 클라이언트의 컴퓨터에 설치하는 대신 인터넷으로 해당 서비스를 제공하는 서비스로서 소프트웨어 관리나 유지보수, 업데이트 작업도 클라우드 사업자 측에서 모두 진행한다. 클라우드 사업자의 규모와 형태, 목표에 따라 인프라 서비스, 플랫폼 서비스, 소프트웨어 서비스 모두 제공하기도 하고, 사용자가 원하는 유형의 서비스만 제공하기도 한다. 클라우드 컴퓨팅을 사용하면 사용자가 인프라부터 소프트웨어까지 구축하거나 관리할 필요가 없어 비용이 감소하고, 서비스로 제공하는 모든 컴퓨팅 자원이나 네트워크 유형 등의 변경이 필요할 때 신속한 조정이 가능하도록 설계하여 유연성을 제공한다. 또한, 클라우드에서 처리되는 데이터를 암호화하고, 강력한 접근 제어를 수행하여 높은 보안성을 제공한다[11].

1) BaaS (Blockchain as a Service)

BaaS는 클라우드를 이용한 서비스형 블록체인으로서 인프라나 플랫폼, 소프트웨어를 제공하는 개념을 넘어 인터넷을 통해 블록체인을 제공하는 기술을 말한다. BaaS의 종류는 크게 두 가지로, BPaaS(Blockchain Platform as a Service)와 BSaaS(Blockchain Software as a Service)가 있으며, 실제로 BaaS를 사용하는 사용자는 두 가지를 동시에 사용하는 경우가 많다. BaaS를 사용할 경우 비용 감소, 유연성 및 확장성 확보, 보안성 제공과 같은 기존 클라우드 컴퓨팅의 이점들을 누리는 블록체인 네트워크를 사용할 수 있다. 또한, 개발 과정의 많은 부분을 생략할 수 있어 비용 및 개발 기간이 감소하며, 블록체인 네트워크 노드의 신뢰성도 보장할 수 있다[12].

BaaS를 제공하는 회사는 대표적으로 Alibaba, IBM, Microsoft, Amazon 등이 있으며, 이미 대규모 클라우드 컴퓨팅 서비스를 운영하는 회사다. Fig. 2는 계층적 구조를 가진 Alibaba, IBM, Microsoft의 BaaS 구조를 나타낸다. Alibaba는 컨테이너화된 애플리케이션과 서비스를 관리하기 위한 오픈소스 플랫폼인 쿠버네티스[13]를 기반으로 설계되었으며 인프라 계층, 클라우드 자원 계층, 플랫폼 서비스 계층, 응용프로그램 계층의 4계층으로 이루어진 BaaS를 운영중이다. IBM은 하이퍼레저 블록체인 기반의 탑, 미들 계층을 IBM 클라우드 위에서 운영하며, 주로 IoT 장치를 지원하기 위한 목적으로 사용된다. Microsoft는 자사의 클라우드 플랫폼인 Azure 기반으로 구축한 블록체인 서비스를 제공하며 기반 플랫폼 계층, 미들웨어 계층, 솔루션 계층으로 이루어진 3계층의 아키텍처를 사용한다. Amazon은 다른 BaaS 서비스와 달리 계층화된 아키텍처가 아닌 요소 기반 플랫폼을 사용하며, 구성원들을 네트워크에 추가할 때 투표 프로세스를 진행하는 특징이 있다[14].

Fig. 3은 시스템의 개요를 나타낸다. 시스템의 엔티티는 사용자, 접근 게이트, 변환 테이블, NFT 네트워크, 디지털 자산 저장소가 있다. 사용자(Fig. 3. User)는 시스템을 직접 사용하는 엔티티로서 접근 게이트에 본인의 지갑 주소로 NFT 네트워크에 참여하여 자신이 가지고 있는 NFT를 팔거나, 다른 사람의 NFT를 구매한다. 접근 게이트(Fig. 3. Access Gate)는 시스템을 보호하기 위한 장치로서 사용자의 지갑 주소를 변환 테이블로 검증해 NFT 네트워크에 접속할 수 있도록 클라우드 계정을 넘겨준다. 클라우드 계정은 단순히 NFT 네트워크에서 사용하는 일종의 별칭 개념으로서 블록체인에서 익명성을 보장할 수 있도록 한다. 변환 테이블(Fig. 3. Conversion Table)은 사용자들의 지갑 주소와 클라우드 계정을 보관하며, 블랙리스트를 따로 관리해 네트워크에 악영향을 끼칠 수 있는 사람을 차단한다. NFT 네트워크(Fig. 3. NFT Network)는 다수의 사용자가 참여하는 NFT 플랫폼으로 사용하며, 사용자들이 사고파는 디지털 자산의 메타데이터를 저장소에 저장하거나, 내용을 변경하는 등의 연산을 수행한다. 디지털 자산 저장소(Fig. 3. Storage)는 사용자가 NFT를 발행하는 디지털 자산을 저장하는 곳이며, 어떤 자산이 누구의 소유인지를 나타낸다.

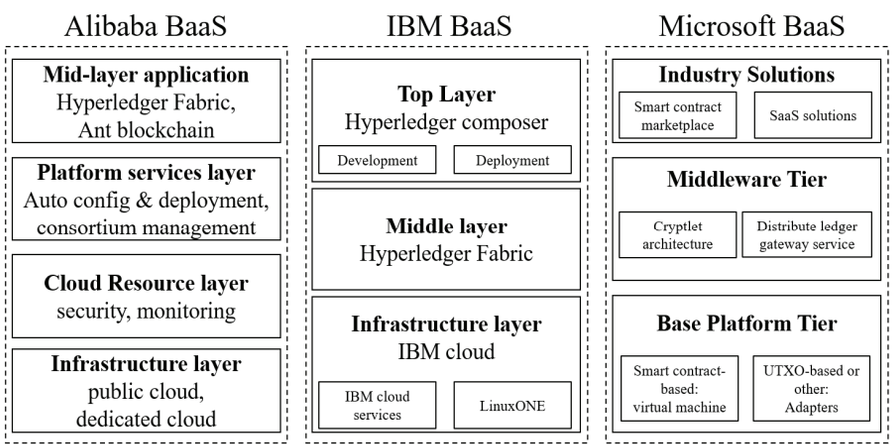

Fig. 2. BaaS Architectures of Alibaba, IBM, Microsoft[14]

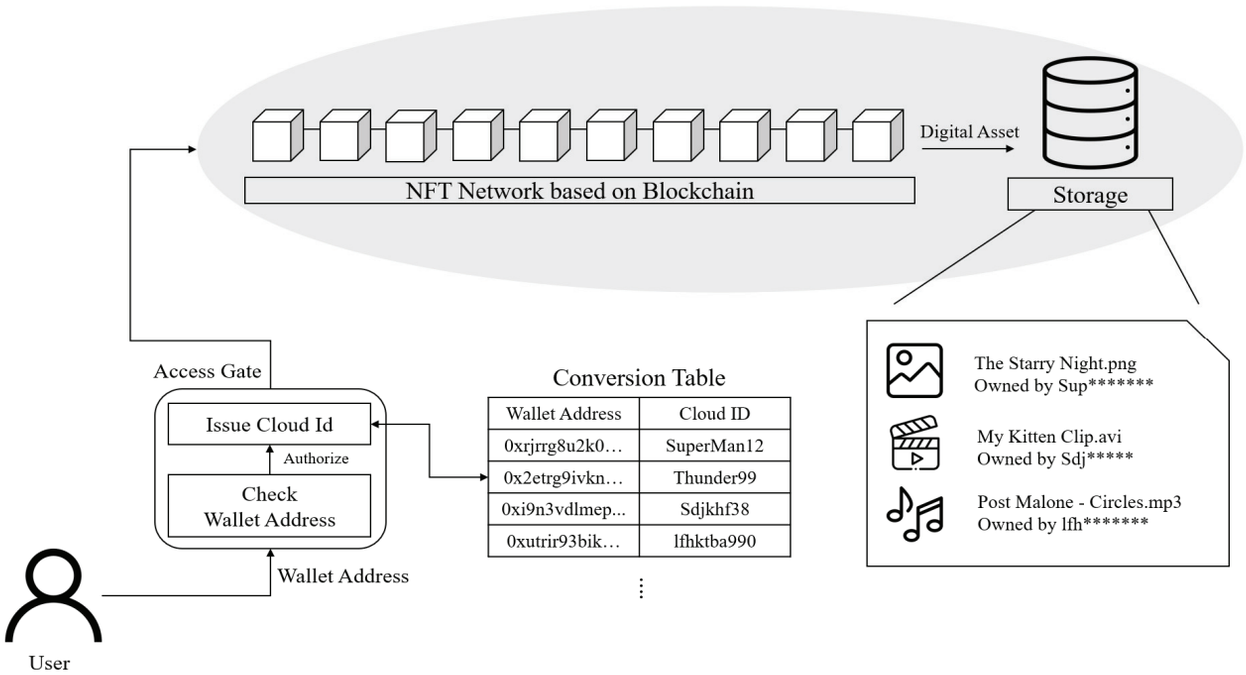

Fig. 3. Proposed System[8]

3. 제안시스템

3.1 블랙리스트 관리

변환 테이블에서 수행되는 블랙리스트 기법은 시스템에 비인가된 사용자를 접속하지 못하도록 하는 역할로 사용한다. 비 인가된 사용자는 불필요하거나 잘못된 행위를 통해 시스템에서 추방된 사람과 악의적으로 자원을 고갈시킨 경우, 유효하지 않은 지갑 주소의 경우 등에 블랙리스트만의 특정 문자로 시작하는 클라우드 계정을 부여해 관리한다.

Fig. 4는 블랙리스트를 적용한 변환 테이블의 예를 보인다. 시스템에서 정상적인 활동을 할 수 있는 지갑 주소는 위에 4개(즉, No. 1-4)의 계정으로 보이며, 각 지갑 주소에 할당된 클라우드 계정은 'SuperMan12'(Fig. 4. No. 1), 'Thunder99'(Fig. 4. No. 2), 'Sdjkf38'(Fig. 4. No. 3), 'lfhktba990'(Fig. 4. No. 4)으로 나타냈다. 시스템에 접근할 수 없는 블랙리스트의 경우 아래 3개의 계정(즉, No. 151-153)으로 보이며, 각 지갑 주소에 할당된 클라우드 계정은 블랙리스트임을 나타내는 'Bl-'이 붙은 형식으로 나타냈다(Fig. 4. No. 151-153). 변환 테이블은 접근 게이트에서 사용자의 지갑 주소를 받아 사용자를 인증하며, 사용자가 클라우드 계정을 소유하지 않은 경우, 사용자에게 따로 입력받거나, 무작위 클라우드 계정을 만들어 네트워크에 접속할 수 있도록 한다.

Fig. 5는 사용자가 NFT 네트워크에 접속하는 과정을 나타낸다. 사용자가 접근 게이트에 자신의 지갑 주소를 이용해 접속을 요청한다(Fig. 5.1). 사용자의 접속 요청을 받은 접근 게이트는 변환 테이블에 사용자의 지갑 주소가 있는지 질의한다(Fig. 5.2). 변환 테이블은 접근 게이트로부터 받은 사용자의 지갑 주소를 검색하고, 클라우드 계정이 존재할 경우 클라우드 계정을 넘겨준다(Fig. 5.3). 만약 클라우드 계정이 존재하지 않은 지갑 주소인 경우, 클라우드 계정을 만들어주는 함수를 통해 새로운 클라우드 계정을 할당받아 넘겨주고 테이블에 저장한다(Fig. 5. opt no wallet address). 변환 테이블로부터 클라우드 계정을 넘겨받은 접근 게이트는 클라우드 계정이 블랙리스트를 뜻하는 글자로 시작할 경우, 사용자에게 접근 불가 메시지를 반환하며(Fig. 5. opt blacklist) 정상 클라우드 계정인 경우, 접근 허용 메시지와 함께 클라우드 계정을 부여하여 사용자가 네트워크에 접속할 수 있도록 한다.

Conversion Table

No.	Wallet Address	Cloud ID
1	0xrjrrg8u2k0…	SuperMan12
2	0x2etrg9ivkn…	Thunder99
3	0xi9n3vdlmep...	Sdjkhf38
4	0xutrir93bik…	lfhktba990
⋮		
151	0xocqefn4u1z…	Bl-43753659
152	0xku8npsrd1h…	Bl-24089135
153	0xbj13yxl9xw...	Bl-60431982

Fig. 4. Example of Conversion Table[8]

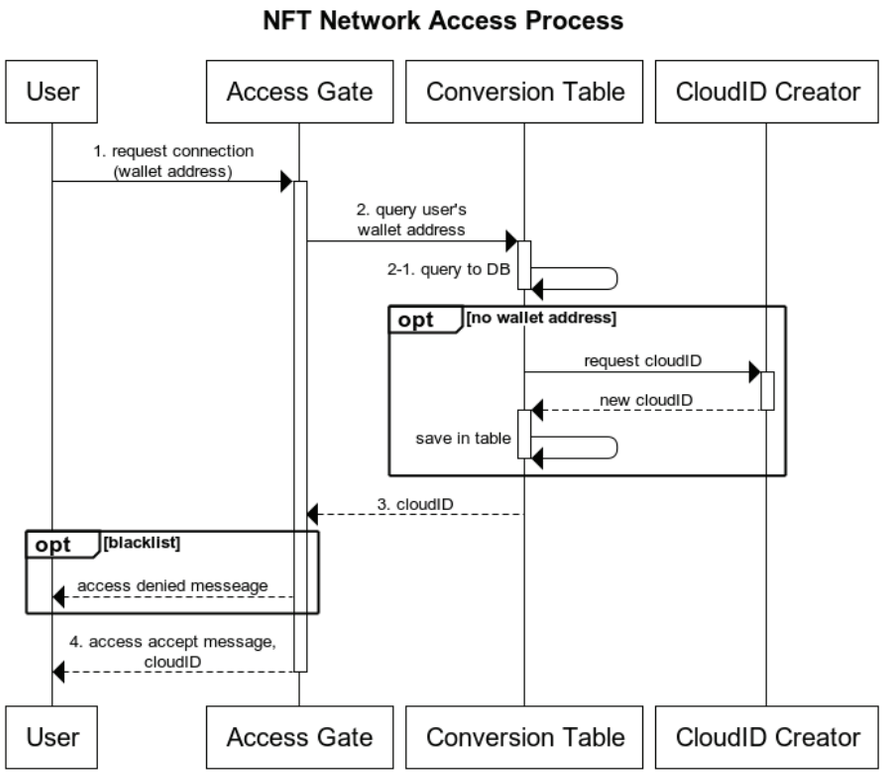

Fig. 5. Sequence of NFT Network Access Process

3.2 사용성 개선

현재 많은 NFT 플랫폼에서 높은 수수료와 트랜잭션 지연 등의 문제를 겪고 있다. NFT를 생성하거나 매매하는데 필요한 많은 연산 과정이 네트워크에 부하를 일으켜 발생한다. 제안시스템의 경우, 클라우드 시스템을 사용함으로써 어떠한 종류의 블록체인 기반으로도 네트워크를 구축할 수 있으며, 클라우드의 자원으로 생성한 네트워크이기 때문에 합의 알고리즘의 변경, 네트워크 유형 변경 등이 자유로워 확장성을 확보하고 수수료와 지연 시간 등을 최소화할 수 있다. 또한, 이러한 일련의 과정은 클라우드 서비스의 로그 서비스를 이용하여 기존 네트워크보다 유연하게 관리할 수 있으며, 디지털 자산의 저장 역시 클라우드 서비스 내의 저장소에서 이루어져 안전하게 보관할 수 있다. 인터넷으로 서비스를 제공하는 클라우드 서비스는 인터넷에 있는 모든 사용자가 예비 사용자가 될 수 있으며, 프라이빗 네트워크와 퍼블릭 네트워크의 장점을 합친 하이브리드 네트워크를 구축할 수 있다. 본 논문에서 제안하는 기법의 클라우드 컴퓨팅 서비스 주체는 신뢰할 수 있는 성능과 책임 추적성, 로그 관리 등의 기능을 제공하는 곳이어야 한다. 대표적인 예로, 해외의 Amazon, Microsoft, IBM 등이 있고 국내의 경우 두나무, KT 등의 기업이 있다.

3.3 프라이버시 보호

NFT가 사이버상에서 가치를 인정받아 가상화폐의 개념으로 사용되는 만큼, 대중에게 많이 알려진 부자나 연예인, 정치인, 유명인 등도 취미 등으로 사용한다. 이런 경우, 허세나 자기 과시를 위해 직접 자신을 밝히는 인물도 있지만, 그와 반대로 대중들에게 알려지고 싶지 않은 인물도 존재한다. 해당 개념은 NFT와 관련된 수행 내용을 외부에 알리고 싶지 않은 일반인에게도 적용된다. 본 논문에서는 접근 게이트와 변환 테이블에서 다루는 클라우드 계정을 통해 공개 네트워크에서 개인의 신상을 추적할 수 있을 만한 정보를 공개하지 않는다. 즉, 네트워크에 참여한 사용자들은 표면적인 클라우드 계정을 사용하여 거래나 NFT 등록 등의 과정을 통해 상호작용하며, 클라우드 계정과 지갑 주소의 변환 과정과 같이 개인정보가 드러날 수 있는 상호작용의 실질적인 연산 부분은 사용자들이 볼 수 없는 클라우드 내에서 처리하여 프라이버시를 보호할 수 있도록 한다.

4. 실험 결과 및 분석

4.1 실험 환경 및 설계

본 논문에서는 로컬시스템 환경과 클라우드 시스템 환경의 가스 사용량 비교를 위해 geth와 web3, nodejs, etherjs 등으로 이더리움 기반 사설 블록체인 네트워크를 구축했고, 이더리움 블록체인에서 사용하는 튜링 완전 언어 솔리디티와 NFT의 표준으로 사용되고 있는 오픈제플린 ERC-721 라이브러리를 이용해 NFT 발행을 위한 스마트 계약과 트랜잭션

을 작성했다. 작성한 스마트 계약은 솔리디티 컴파일러를 통해 배포에 사용되는 ABI(Application Binary Interface)와 bin(binary)의 형식으로 변환하여 배포 파일을 작성했으며, 배포 및 트랜잭션 처리에 필요한 채굴에는 3개의 스레드를 사용해 진행했다. 두 시스템의 연산력 차이를 비교하기 위해 블록체인 초기 설정에 사용한 제네시스 블록에서 난이도를 '0x1000'으로 설정하여, 채굴 과정이 너무 쉽지 않도록 조정했다[15-20].

4.2 실험 결과 및 분석

이더리움 블록체인에서 사용하는 가스는 채굴에 연산력을 사용하는 데 발생하는 값으로, 스마트 계약 배포 및 트랜잭션 연산 처리 등으로부터 발생하며 연산의 크기가 클수록 더 많이 발생한다. 일반적으로 스마트 계약 배포에 발생하는 가스가 계약 속 트랜잭션 발행에 발생하는 가스보다 매우 크고 만약 가스가 모두 소진될 경우, 추가적인 트랜잭션 발행이 불가해 시스템이 정상적으로 운영되지 않을 수 있다.

본 논문에서는 로컬시스템과 클라우드 시스템의 스마트 계약 배포와 NFT 발행 트랜잭션 처리 과정에서 사용되는 가스 사용량을 비교했다. Fig. 6은 로컬시스템과 클라우드 시스템의 NFT 스마트 계약 배포 과정의 가스 사용량을 비교했다. Fig. 7은 로컬시스템과 클라우드 시스템의 NFT 발행 트랜잭션 처리 과정의 가스 사용량을 비교했다. 스마트 계약 배포 및 트랜잭션 처리 과정에 사용되는 가스는 코드나 파라미터가 변경되지 않으면 오차가 거의 없는 가스를 사용하지만, 두 실험은 평균 10회의 수행을 통해 측정했다. NFT를 발행한 디지털 자산은 PNG 확장자를 가진 이미지이며, 네트워크의 임의의 계정을 소유주로 설정했다.

1) NFT 스마트 계약 배포 과정의 가스 사용량 비교

Fig. 6은 제안시스템에서 사용자가 디지털 자산에 NFT를 발행하고자 할 때, 첫 단계인 스마트 계약 배포에 사용되는 가스 사용량 측정의 결과를 나타낸다. 왼쪽 막대는 로컬시스템을 나타내며, 2,627,983 만큼의 가스를 사용했다. 오른쪽 막대는 클라우드 시스템을 나타내며, 2,529,674 만큼의 가스를 사용했다. 스마트 계약의 코드와 블록체인 네트워크의 구성, 채굴에 사용한 스레드 수, 파라미터 등 같은 실험 환경에서 클라우드 시스템이 약 3.75% 정도의 가스를 적게 사용함을 확인했다. 이는 클라우드를 구성하고 있는 시스템의 연산장치가 로컬시스템을 구성하고 있는 연산장치보다 성능이 뛰어난 부분에서 도출되었다. 즉, 더 적은 연산으로 채굴에 성공했음을 의미하고, 더 적은 연산은 더 짧은 시간을 사용해 채굴에 성공했다고 해석할 수 있다.

2) NFT 발행 트랜잭션 처리 과정의 가스 사용량 비교

Fig. 7은 제안시스템에서 Fig. 6의 스마트 계약이 배포된 후, 디지털 자산에 NFT를 발행하는 트랜잭션이 처리되기 위한 가스 사용량 측정의 결과를 나타낸다. Fig. 6의 구성과 같이, 왼쪽 막대는 로컬시스템을 나타내며 오른쪽 막대는 클라우드 시스템을 나타낸다. 로컬시스템은 NFT 발행을 위한 트랜잭션 처리에 182,916의 가스를, 클라우드 시스템은 174,511의 가스를 사용했다. 이는 Fig. 6에서 나타내고 있는 스마트 계약 배포 과정의 가스 사용량과 비슷하게 클라우드 시스템이 약 4.6% 정도 적은 가스를 사용했다.

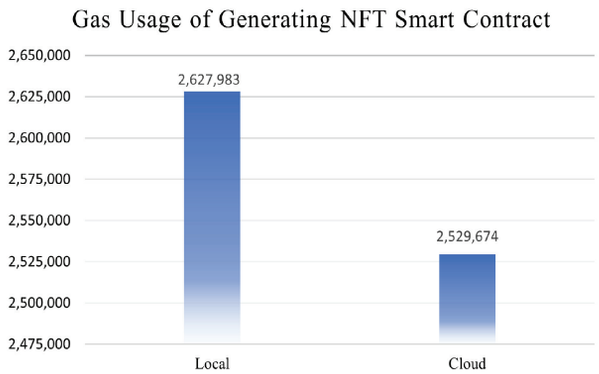

Fig. 6. Gas Usage of Generating NFT Smart Contract

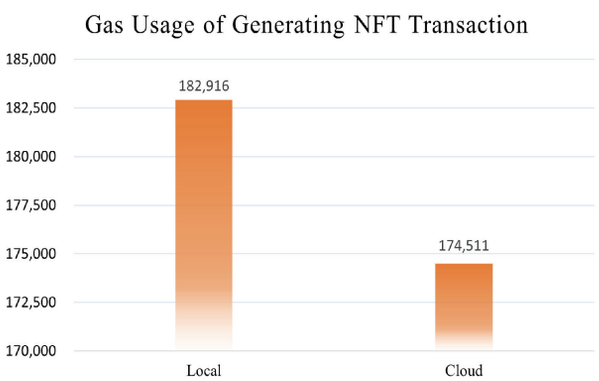

Fig. 7. Gas Usage of Generating NFT Transaction

실험 환경 중 로컬, 클라우드의 차이만 있을 뿐, 모든 환경 구성과 파라미터가 같음에도 클라우드 시스템을 구성하고 있는 연산장치의 연산 능력이 강력해 적은 가스를 사용한 결과가 도출되었다.

3) 채굴 성능 향상

사설 네트워크에서 연산을 처리하기 위한 채굴에 사용하는 명령어인 'miner.start()'은 채굴에 사용할 스레드의 수를 파라미터로 사용한다. 만약 파라미터를 기재하지 않으면, 기본으로 'miner.start(1)'의 명령어가 적용되어 1개의 스레드로 채굴을 진행한다. 본 논문에서 진행한 실험에서는 로컬시스템의 성능 한계치를 고려해 클라우드 시스템과 로컬시스템에서 3개의 스레드를 이용해 채굴을 진행했다. 그러나, 클라우드 시스템의 경우 강력한 연산 능력을 갖춘 하드웨어의 구축

과 업그레이드에 걸리는 시간, 비용 등의 측면에서 로컬시스템보다 뛰어나기에, 스레드를 적게는 16개, 많게는 32개 이상까지도 사용할 수 있다. 스레드의 특성상 스레드 A개를 사용하는 시스템과 A보다 큰 B개를 사용하는 시스템이 있으면, B를 사용하는 시스템은 A개의 스레드를 사용하는 시스템보다 B/A 배의 성능을 확보할 수 있다. 이러한 부분에서 클라우드 시스템이 로컬시스템보다 강점을 가질 수 있다.

5. 결 론

그림, 이미지, 비디오, 게임 캐릭터 및 아이템과 같은 디지털 자산을 하나의 투자 수단이나, 개인 소장품, 취미로 여기는 사람들이 늘어나면서 NFT는 하나의 블록체인 시장의 전문 분야로 자리 잡았다. 하지만, 2020년부터 관심이 폭발적으로 증가하며 블록체인 네트워크에 NFT와 관련된 연산이 급격하게 많아졌고, 이는 채굴 수수료 비용의 증가와 연산 처리 효율 감소의 원인이 되었다. 또한, 유명인, 부자, 프라이버시를 중요하게 여기는 일반인 등의 경우 NFT를 발행하고 매매하는 과정에서 본인의 신분이 외부로 노출되는 것을 원하지 않지만, 디지털 자산의 저장 매체로 IPFS를 사용함으로써 디지털 자산의 위치와 정보가 모두에게 공개된다.

본 논문에서는 기존 NFT 플랫폼의 사용성 문제와 프라이버시 보호 문제를 개선하기 위해 클라우드 컴퓨팅 기술과 접근 게이트 및 변환 테이블을 활용한 NFT 플랫폼을 제안했다. 시간이 지남에 따라 느린 연산 처리 속도 및 높은 가스 수수료와 같은 사용성 문제는 사용자의 및 복잡한 연산의 증가로 인해 점차 심화할 가능성이 크며 프라이버시 보호를 요구하는 사용자들이 많아질 경우, 모든 사용자의 다양한 요구를 충족하기는 쉽지 않다. 하지만, 클라우드 컴퓨팅의 연산 능력 및 자원을 이용한 블록체인 네트워크를 구성함으로써 사용성 문제를 완화할 수 있으며, 접근 게이트와 변환 테이블을 이용해 네트워크에 접근하기 전 익명화를 진행해 프라이버시를 보호할 수 있다. 또한, 클라우드 컴퓨팅을 통한 블록체인 구성이기에, 네트워크 구조 및 유형 변경, 개인정보 보호 및 암호화 적용 등에 있어 유연한 대처가 가능하다.

향후 연구에서는 클라우드 컴퓨팅을 활용한 블록체인 구성에 최적화된 합의 알고리즘이 무엇인지, 채굴을 담당하는 노드는 클라우드에서 어떻게 구현해야 할지를 연구하고, 프라이빗 블록체인과 퍼블릭 블록체인을 간편히 전환할 수 있는 하이브리드 블록체인 네트워크를 이용한 NFT 플랫폼을 고안한다. 또한, 제안시스템의 접근 게이트 및 변환 테이블에 사용한 블랙리스트 기법과 클라우드 계정을 통한 익명화를 발전시켜 프라이버시 보호를 철저히 수행할 수 있는 시스템을 연구하고, 디지털 자산의 이동 및 NFT 발행 과정에 적용할 수 있는 클라우드 컴퓨팅 암호화 기법을 도입하여 외부의 공격자로부터 데이터를 보호할 수 있도록 할 계획이다.

References

[1] Q. Wang, R. Li, Q. Wang, and S. Chen, "Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges (Tech ReportV2)," *arXiv:2105.07447v3* [cs.CR], 2021.

[2] R. Wajiha, I. Jaweria, E. Z. Hijab, and B. Narmeen, "NFTs: Applications and Challenges," *22nd International Arab Conference on Information Technology (ACIT)*, pp.1-7, 2021.

[3] Gansong Museum, Humminjeongeum Limited Edition NFT [Internet], https://kansong.org/hm-nft.

[4] Cryptopunks [Internet], https://www.lavalabs.com/cryptopunks.

[5] Cryptokitties, [Internet], https://www.cryptokitties.co.

[6] J. Y. Lee and G. S. Jo, "Understanding and utilizing the latest NFT technology," *Korea Institute of Information Technology Magazine*, Vol.19, No.1, pp.7-11, 2021.

[7] H. J. Kim, "Overseas cases and trends in NFT copyright-related industries," *Korea Copyright Protection Agency Global Issue Report*, pp.1-10, 2021.

[8] M. J. Kang, "A study on NFT platform to improve privacy and performance," *Proceedings of the Annual Spring Conference of Korea Information Processing Society Conference (KIPS) 2022*, Vol.29, No.1, pp.248-251, 2022.

[9] Flow [Internet], https://flow.com.

[10] WAX [Internet], https://on.wax.io/wax-io.

[11] P. Srivastava and R. Khan, "A review paper on cloud computing," *International Journals of Advanced Research in Computer Science and Software Engineering*, Vol.8, No.6, pp.17-20, 2018.

[12] H. J. Yu, "NIPA Issue Report(2020-06) Infrastructure of a Blockchain Powerhouse, Blockchain as a Service (BaaS)," National IT Industry Promotion Agency Issue Report, 2020.

[13] kubernetes [Internet], https://kubernetes.io.

[14] J. Song, P. Zhang, M. Alkubati, Y. Bao, and G, Yu, "Research advances on blockchain-as-a-service: Architectures, applications and challenges," *Digital Communications and Networks*, 2021.

[15] Geth [Internet], https://geth.ethereum.org.

[16] Web3 [Internet], https://web3js.readthedocs.io.

[17] Nodejs [Internet], https://nodejs.org.

[18] Etherjs [Internet], https://docs.ethers.io.

[19] Solidity [Internet], https://docs.soliditylang.org.

[20] Openzeppelin [Internet], https://openzeppelin.com.

강 명 조

https://orcid.org/0000-0002-0691-2970
e-mail : rkdaudwh13@hknu.ac.kr
2021년 한경대학교 컴퓨터응용수학부 (학사)
2022년 한경대학교 컴퓨터응용수학부 석사과정
관심분야 : 네트워크 보안, 블록체인, 머신 러닝

김 미 희

https://orcid.org/0000-0002-4896-7400
e-mail : mhkim@hknu.ac.kr
1997년 이화여자대학교 전자계산학과(학사)
1999년 이화여자대학교 컴퓨터학과(석사)
1999년 ~ 2003년 한국전자통신연구원 연구원
2007년 이화여자대학교 컴퓨터학과(박사)
2007년 ~ 2009년 이화여자대학교 컴퓨터학과 전임강사
2009년 ~ 2010년 노스캐롤라이나주립대학교 연구원
2011년 ~ 현 재 한경대학교 컴퓨터응용수학부 컴퓨터시스템연구소 교수
관심분야 : 네트워크 성능 분석 및 보안, 무선네트워크 보안, 침입대응, 크라우드센싱, 블록체인