BlockChain and NFT/NFT

[NFT] NFT 기술 소개

Dbswnstjd 2022. 2. 24. 14:05

NFT 는

Non-Fungible-Token 으로 대체 불가능 토큰 이라고 한다. 그렇다면 여기서 Token 은 무엇을 말하는 것일까 ?

Token 이란 ?

- **프로그래밍 언어에서의 토큰**

문법적으로 더 이상 나눌 수 없는 기본적인 언어 요소를 말하는데, 예를 들어 하나의 키워드나 연산자 또는 구두점 등이 토큰이 될 수 있다.

- **네트워크에서의 토큰**

토큰링 네트워크를 따라 돌아다니는 일련의 특별한 비트열이다. 컴퓨터들은 네트워크를 따라 순환하는 토큰을 자신이 잡았을 때만 네트워크에 메시지를 보낼 수 있다. 각 네트워크에는 오직 단 한개의 토큰만이 존재함으로써, 두 개 이상의 컴퓨터가 동시에 메시지를 전송할 가능성을 사전에 차단한다.

- **보안 시스템에서의 토큰**

크레딧 카드 크기의 작은 장치를 말하는데, 계속해서 변화하는 ID 코드를 표시해준다. 사용자가 처음에 암호를 입력하면, 카드는 네트워크에 접속할 수 있는 ID를 그때그때 표시해준다. 보통, 매 5분마다 ID가 변경된다.

하지만 찾아본 결과 NFT에서의 토큰은 이와 같은 토큰과는 달리 특수한 유형의 암호화 토큰이며 상호 교환이 불가능한 특징을 가지고 있다고 한다.

> **NFT에서의 Token**

- 특수한 유형의 암호화 토큰
- 상호 교환이 불가능

NFT의 프로토콜

프로토콜

NFT Protocol

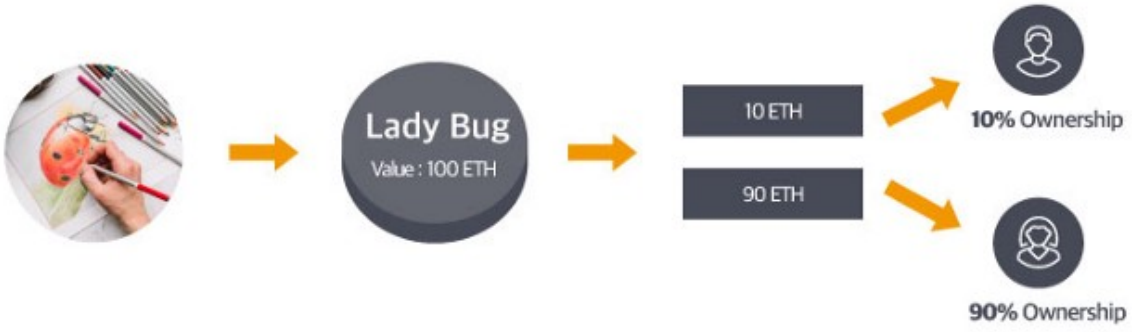
[ERC-20 이란?]

먼저, ERC는 'Ethereum Request for Comment'로, 이더리움 네트워크에서 토큰을 만들 때 따라야하는 프로토콜을 의미한다. 그리고 많은 프로토콜 중에서 20번째 프로토콜이 ERC-20이다. 그리고 ERC-20 프로토콜에 맞추어 생산된 암호화폐가 ERC-20 토큰인 것이다. 이더리움 네트워크에서 생성된 대부분의 토큰들은 ERC-20을 기반으로 생성되었다. 이러한 암호화폐들은 native Ethereum curreny(ETH)랑 교환이 가능하며 ERC-20 기반의 다른 화폐들과도 교환이 가능하다. 게다가 토큰들은 My Ether Wallet(MEW)와 같이 ERC-20 토큰을 지원하는 Wallet들을 사용하여 자유롭게 보내질 수 있다.

ERC-20의 토큰의 핵심적인 특성은 **동등한 가치로 구매, 판매, 교환**한다는 것이다. ERC-20 토큰의 가장 중요한 특성은 **누가 토큰을 가지고 있는지 상관없이 동일한 가치를 지닌다는 것**이다. 따라서 이것은 우리가 일상 생활에서 사용하는 화폐와 같다. 예를 들어 10000원짜리 공책은 누가 소지해도 동일하게 10000원이므로 이더리움의 관점에서 ERC-20 토큰이라고 볼 수 있다.
만약 아래의 그림과 같이 James와 Rachel이 A 토큰을 1개씩 들고 있으면, 두개는 동일한 가치를 지니기 때문에 동일한 가치로 교환을 할 수 있다. 만약 Rachel이 A토큰을 ETH와 1대1로 교환하였다면, James도 동일한 비율로 1ETH를 지불하여 1A토큰을 구매할 수 있다.

[ERC-721 이란?]

그렇다면 위에서 설명한 ERC-20와 Non-Fungible Token(NFT)인 ERC-721의 차이점은 무엇일까?
ERC-20은 대체가능하지만 **ERC-721은 대체불가능하다는 것**이다. 즉, ERC-721은 이더리움 네트워크에서 대체 불가능하다는 NFT의 개념이 도입된 토큰이다.
예를 들어 만약 우리가 무당벌레를 그리고, 이 그림을 '무당벌레 그림'이라고 하자. 여기서 그린다는 것은 '무당벌레 그림'과 같은 하나의 작품을 만드는 것이 되는 것이다. 이렇게 하나의 작품을 만드는 과정이 ERC-721 토큰을 만드는 과정에 해당하는 것이고, '무당벌레 그림'은 다른 무당벌레를 그린 그림들과 대체가 불가능하며 가치가 다르므로 ERC-721 기반의 NFT에 해댕하는 것이다.



NFT의 또 다른 특징은 **토큰에 대한 소유권이 나뉘어 질 수 있다는 것**이다. 즉, 부분적인 소유권이 허용되며 교환될 수 있다.

예를 들어 '무당벌레 그림'의 소유권은 James가 100ETH 모두 가질 수 있고, Rachel이 90ETH를 주고 구매한다면 James와 Rachel이 소유권을 각각 10%, 90%씩 나누어 가질수도 있다.
NFT에 대한 판매와 구매는 온라인 시장에 제한되어 있지 않다. 핸드폰과 같은 제품들 역시 ERC-721 토큰의 개념이 도입될 수 있고, 제품에 대한 소유권은 온라인으로 거래될 수 있다. 음악 산업에서 음악의 소유권이 여러 사람들에게 나누어지며, 그 소유권을 바탕으로 수익이 나누어지고 있다. 위의 예시들처럼 ERC-721 기반의 토큰을 활용할 수 있는 방안이 많이 있다.
현재는 ERC-1155를 사용하여 토큰 개발이 많이 이루어 지고 있다고 한다.

이와 같이 ERC-721을 통해 발행된 NFT 토큰은 그 존재 자체가 유일무이하다. 왜냐하면 고유의 해시값을 가지고 있기 때문이다.

[ERC-1155 이란?]

- ERC-20과 ERC-721의 장점을 혼합하여 두 토큰이 연동하여 거래할 수 있도록 설계된 프로토콜
- 하나의 트랜잭션을 이용하여 한 명 이상의 수신자에게 두 개 이상의 토큰을 보낼 수 있는 멀티 전송(Multi-transfers)이 가능

NFT의 저장 방식

[IPFS]

ipfs(InterPlanetary File System)이란 프로토콜이며, 분산 파일 시스템에서 데이터를 공유하고 저장하기 위한 peer-to-peer 네트워크이다. IPFS는 모든 컴퓨팅 기기를 연결하는 글로벌 네임스페이스에서 각 파일을 식별하기 위해 content-addressing 을 사용한다.

[IPFS Example]

만약 NFT를 조사하기 위해 아래와 같은 주소를 입력한다고 가정하면

```
https://en.wikipedia.org/wiki/NFT
```

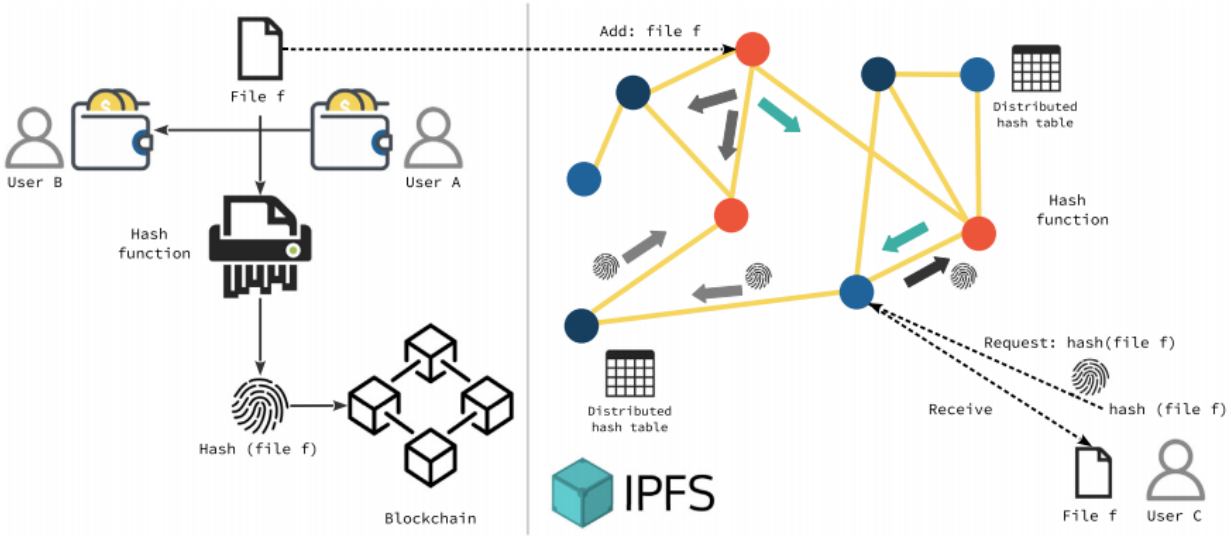
URL을 입력하게 되면 컴퓨터는 해당 국가(또는 지구 어딘가)에 있는 위키피디아의 서버에 요청을 보내 해당 페이지를 가져오게 된다.

하지만, NFT 페이지를 다른 방식으로 가져올 수 있는데 이는 IPFS에 저장된 위키피디아 미러(mirror)가 존재하기에 이것을 사용이 가능하다. 만약 IPFS를 사용한다면 컴퓨터는 NFT 페이지

를 아래와 같이 요청한다.

```
/ipfs/QmXoypizjW3WknFiJnKLwHCnL72vedxjQkDDP1mXWo6uco/wiki/Aardvark.html
```

그리고 IPFS는 해당 페이지가 위치가 아닌 컨텐츠를 기반으로 정보를 찾을 수 있다.(Content-addressing)
NFT 페이지의 IPFS 버전은 URL 중간에 포함된 숫자와 문자로 나타나게 된다. 그리고 그 요청을 위키피디아의 서버에 요청하는 것이 아니라, 전세계에 퍼져 있는 수많은 컴퓨터들에 NFT 검색 페이지를 공유해줄 것을 요청한다. 따라서 해당 페이지정보를 가지고 있는 누구에게서로부터 얻을 수 있다.
그리고 IPFS를 사용할 때, 해당 컴퓨터는 다른 누구로부터 파일들을 다운받는 것과 동시에 파일들을 나누어 주는 역할을 하게 된다. 해당 컴퓨터에서 몇 블록 떨어진 누군가가 똑같은 페이지를 요청한다면 그 페이지를 나누어 줄 수 있다.



IPFS

[IPFS의 주요 특징]

- **분산화(Decentralization)**

IPFS는 하나의 기관이 중심이 되어 관리하는 중앙화 시스템이 아닌 분산된 환경의 여러 장소로부터 파일을 다운로드 받을 수 있도록 한다. 또한 중앙 서버가 아닌 탈중앙화 시스템이기 때문에 데이터의 조작이나 변조가 불가능 하다.
IPFS의 파일은 다양한 장소로부터 전달되기에 기관, states 등이 특정 정보를 막기 위해 검열하는 것을 매우 어렵게 한다. 이러한 IPFS의 특성은 정보에 대해 자유로운 접근을 향상 시킨다.
마지막으로 요청하는 컴퓨터가 외지에 있거나 연결되지 않은 상황에서 웹을 빠르게 만들 수 있다. 매우 멀리 떨어진 어떤 장소로부터 해당 파일을 받는 대신 주변의 가까운 다른 노드로부터 빠르게 파일을 받을 수 있다.

특히 이는 로컬에서는 서로 잘 연결되어 있짐나 외부와는 연결이 잘 되지 않을때 더욱 효과가 좋다고 할 수 있다.
이러한 특징으로 IPFS는 (범지구적 파일 시스템) 이라는 이름을 따오게 되었다고 한다.

- **컨텐츠 어드레싱(Content Addressing)**

```
/ipfs/QmXoypizjW3WknFiJnKLwHCnL72vedxjQkDDP1mXWo6uco/wiki/NFT.html
```

위의 URL에서 ipfs이후의 문자열은 content identifier으로 IPFS가 여러 장소로부터 컨텐츠를 가져오는 키가 된다.
IPFS에서는 위치 기반의 표기 대신 하나의 파일을 '해당 파일에 무엇이 들어 있는지'를 통해 나타낸다. 위에서 살펴본 content identifier는 해당 주소를 가진 컨텐츠의 cryptographic hash 값이다. 원본 컨텐츠에 비해 짧아 보이지만 해당 hash 값은 기원한 컨텐츠에 따라 unique한 값을 가지게 된다. 또한 이러한 hash는 컨텐츠와 hash가 매칭되지 않으며 다른 컨텐츠를 전달하는 것을 막는다.

IPFS에서 하나의 파일에 대한 주소는 컨텐츠 자체로부터 생성되기 때문에 IPFS의 링크는 변하지 않는다.

- **참여(Participation)**

IPFS에는 많은 기술들이 적용되었지만, 기본적인 아이디어는 사람들과 컴퓨터가 어떻게 의사소통하는지를 변경한 부분에 존재한다.

현재 www는 소유권과 접근을 기반으로 구축되었기에 사람들은 파일들을 저장한 서버에 요청을 보내고 이에 따라 접근을 허용하면 응답이 오게 되는데 IPFS 소지와 참여에 기반해서 많은 사람들이 각각 다른 파일들은 가지고(소유)있고 그것들을 사용할 수 있도록 참여하고 공유하게 된다.

이것은 IPFS는 사람들이 적극적으로 참여할 떄 잘 작동된다는 것이다.

출처