부동산 소유권 NFT 와 분할 판매 및 거래 시스템 설계

김영근 [1], 김성환 [1], Hyo Jung Song[2]
서울시립대학교 컴퓨터과학과 [1], San Francisco State Univ[2].
miso07@uos.ac.kr, swkim7@uos.ac.kr, hjsong@sfsu.edu

NFT Tokenization of Real Estate and Divisible FT Trading with Asset Portfolio Management

Young-Gun Kim[1], Seong-Whan Kim[1], Hyo Jung Song[2]
Dept. of Computer Science, University of Seoul[1], San Francisco State University[2]

요 약

대체 불가능 토큰 (NFT, non-fungible token)은 고유하고 더 이상 분할할 수 없는 특성을 가지고 있다. NFT 는 디지털 콘텐츠에 대한 소유권을 증명해 주지만 현재 1) 소유권 증명 이상의 유틸리티가 명확하지 않고, 2) 토큰이지만 유동성이 거의 없으며, 3) 가격이 예측 불가능하다. 특히, 부동산의 경우 가격이 매우 높은 특징으로 인하여 투자 진입장벽이 매우 높다. NFT 분할을 하면 유동성의 증가, 그리고 접근성 증가에 따른 커뮤니티 볼륨의 증가를 기대해 볼 수 있다. 이러한 특성을 활용하여 기존에 투자하기 어려웠던 부동산을 다양한 기술을 활용하여 쉽게 투자를 할 수 있게 된다. 또한, Black Litterman 모델을 활용하여 보다 여러 종류의 NFT 들에 대한 최적 포트폴리오를 구성할 수 있는 알고리즘을 설계하고 구현하였다.

1. 서론

블록체인 (blockchain)이란 분산 원장 기술을 통해 기록된 데이터에 대한 비밀성과 투명성, 보안성을 제공하는 기술이다 [1]. 최근 블록체인을 활용한 NFT 가 ICO, 거래소 토큰, 디파이 (DeFi, decentralized finance) 등으로 발전하고 있다. NFT 는 디지털 파일에 대한 소유권의 확인과 양도, 로열티 지급 등에 관한 정보가 코딩 되어 있는 프로그램인 'NFT 스마트계약' 이 블록체인에 직접 저장되면서 발행되는 토큰으로, 다른 토큰과의 1: 1 교환이나 대체가 불가능하며 각 토큰은 모두 각자의 가치를 가진다. 블록체인의 기술적 특성상 한번 발행하면 위변조나 복제를 할 수 없고, 소유권과 거래 내역을 비가역적으로 증명할 수 있기 때문에 실물 및 가상 자산의 디지털 원본 증명서 또는 소유권 보증서로 활용된다 [2]. 본 논문에서는 oracle 기반으로 부동산 기초 자산의 실제 가격을 가져오고, 가격이 정해진 NFT 토큰을 다시 FT (fungible token)으로 분할 거래하는 시스템을 설계하고 구현하였다.

2. 관련 연구

블록체인이란 다수의 거래내역을 묶어 블록을 구성하고, 해시를 이용하여 여러 블록들을 체인처럼 연결한 뒤, 다수의 사람들이 복사하여 분산 저장하는 알고리즘이다. 블록체인 기술을 이용하면 데이터의 위변조가 불가능하여 권위 있는 중개기관이 없더라도 신뢰할 수 있는 안전한 거래와 데이터 처리를 할 수 있다. NFT (ERC-721 표준)는 토큰마다 고유한 값 (hash)을 가지고 있어 다른 토큰으로 대체가 불가능하다. 무형의 디지털 자산을 NFT 화한다면 무형의 디지털 자산의 소유권을 보장받을 수 있다. 대부분의 유틸리티 토큰의 경우 FT (ERC-20 표준)로 각 토큰들이 동일한 단위로 교환되고 대체될 수 있다. 가상자산 (cryptocurrency)은 암호화폐라고도 불리는데, 분산 장부 (distributed ledger)에서 공개키 암호화를 통해 안전하게 전송하고, 해시 함수를 이용해 쉽게 소유권을 증명해 낼 수 있기 때문이다. 일반적으로 암호화폐는 블록체인이나 DAG (directed acyclic graph)를 기반으로 한 분산 원장 (distributed ledger) 위에서 동작한다. 가상자산은 (1) 플랫폼 토큰 (platform coin): 다양한 서비스와 토큰에서 사용하는 공통된 기능을 모아서 제공하는 플랫폼에 사용되는 암호화폐이다. 플랫폼 코인 위에 다양한 서비스에서 사용하기 위한 탈중앙 분산형 응용 프로그램인 디앱 (DApp)을 만들 수 있다. 대표적인 플랫폼 코인에는 이더리움, 이오스, 카르다노, 트론, 아이콘, 루니버스, 클레이튼, 티티씨 등이 있다. (2) 증권형 토큰 (security token): 주식, 채권, 부동산 등 실물자산을 블록체인 기반의 암호화폐에 페깅 (고정)한 디지털 자산을 말한다. 증권형 암호화폐 또

는 시큐리티 토큰이라고도 한다. 일반적으로 주식과 비슷한 개념으로 사용자는 보유한 증권형 토큰의 개수에 따라 토큰 발행사가 창출한 이윤의 일부를 배당금으로 받거나 발행사의 경영권의 일부를 가질 수 있다. 세종텔레콤의 '비브릭 (BBRIC)'이 국내 증권형토큰의 첫 사례이다. (3) 유틸리티 토큰 (utility token): 독립적인 블록체인이 존재하지 않으며, 특정 플랫폼 블록체인상의 스마트 컨트랙트로 생성·관리되는 암호화폐를 의미한다. 일반적으로 플랫폼 코인 위에서 작동하는 디앱 (DApp) 방식으로 개발한다. (4) 거버넌스 토큰 (governance token): 블록체인 생태계 유지를 위한 투표에 사용한다. 탈중앙화 운영되는 디파이 특성상 이용자들은 거버넌스 토큰을 이용해 시스템 개선안, 운영방안 등에 의사를 표시한다.

DeFi 는 탈중앙화된 분산 금융을 말한다. DeFi 의 주요 응용으로는 (1) credit/lending: 신원 확인 절차 후, 암호화폐를 담보로 일정 금액을 대출받는 방식이다. Capital Pool (CP) 모델과 P2P 모델이 존재한다. CP 모델은 서비스 운영 주체가 담보를 받고 대출을 해주는 형식이며, P2P 모델은 특정 운영 주체 없이 대출받고자 하는 사람과 해주고자 하는 사람을 연결해주는 형식이다. MakerDAO, Compound, Aave 등이 있다. (2) DEX (decentralized exchange): 중앙화된 암호화폐 거래소 (CeX: centralized exchange)는 상장 수수료, 자의적인 입출금 통제, 거래소 해킹 등의 문제점이 있고, 이를 해결하기 위해 거래소 인터페이스만 제공하고 그 외 부분은 블록체인 네트워크를 활용하는 탈중앙화 거래소가 등장했다. UNISWAP, Binance DEX 등이 있다. (3) 파생 거래 (derivatives, 마진 거래): 마진 거래는 코인 공매수, 공매도 계약을 통한 마진 (증거금) 거래에 레버리지를 통해 수익을 극대화하는 투자수단이다. Yield Protocol, dYdX, Synthetix 등이 있다. (4) Tokenization: 블록체인 비즈니스를 위한 재화 및 서비스 교환수단의 용도로 암호화폐를 발행하던 과거와 달리 실물자산을 토큰화하는 추세가 늘어나면서 이를 대신해주는 서비스들이 등장했다. Set Protocol, wBTC 등이 있다. (5) 이자농사 (yield farming): 이자 농사란 수익을 얻기 위해 암호화폐를 예치하고 (플랫폼에 유동성을 제공), 이에 대한 보상으로 이자를 받는다. 이는 전통적인 명목화폐 예금 방식과 유사하다. 일반적으로 계좌에 예치된 돈은 은행의 유동성 공급에 사용된다. 은행은 고객에게 대출 및 자금을 제공하는데 유동성 풀을 활용한다. 이자농사는 동일한 개념으로 은행이 아닌 대출 플랫폼에 유동성을 공급하는 것이다.

블록체인 네트워크와 스마트계약 그 자체는 외부 네트워크의 데이터 흐름을 반영하지 못한다. 따라서 블록체인 네트워크는 인터넷 접속이 안 되는 컴퓨터와 유사하다고 볼 수 있다. 그러나 블록체인 네트워크 및 스마트 컨트랙트가 본격적으로 활성화되기 위해서는 외부 네트워크 (실세계)와 연결되는 것이 필수적이다. 오라클은 블록체인 네트워크 (on-chain)와 외부 네트워크 (off-chain)를 잇는 교량 역할을 하는 미들웨어 인프라를 의미한다. 데이터 제공자, 웹 API, 엔터 프라이즈 백엔드, 클라우드 제공자, IoT 기기, 결제 시스템 등이 블록체인 네트 워크와 연결될 수 있는 외부 네트워크의 예이다.

평균분산모형 (mean-variance optimization, MVO)은 분산투자를 통한 위험감소 효과를 토대로 주어진 위험 수준 하에서 최대의 기대수익을 얻을 수 있는 최적의 포트폴리오를 도출하는 이론이다. Black-Litterman Model (BL)은 MVO 의 입력 변수의 불안정성을 극복하는 모델로 시장포트폴리오 (market portfolio)로부터 균형기대수익률을 도출하여, 자산이 균형 있게 배분되는 최적의 포트폴리오가 되도록 만든 이론이다. 다음과 같은 순서로 계산한다.

1. 각 자산의 시가총액 비율을 이용하여 균형기대수익률을 구한다. $\Pi = \mu + \xi_{\Pi} = \lambda \Sigma W_{mkt}$
2. 투자자의 시장전망과 전망 확신도를 행렬식으로 표현한다. $Q = P * \mu + \xi_Q, \quad \Omega = P \tau \Sigma P^T$
3. Black-Litterman Formula 에 적용하여 기대수익률을 도출한다. $\mu_{BL} = [\lambda \Sigma]^{-1} [\tau \Sigma)^{-1} + P' \Omega^{-1} P]^{-1} [\tau \Sigma)^{-1} \Pi + P' \Omega^{-1} Q]$
4. 최적 투자비율을 결정

3. 부동산 NFT Tokenization and FT Trading 설계

부동산 자산을 ERC-721 을 이용하여 NFT 를 생성한다. 생성된 NFT 를 금고에 저장하고 (LOCK) 저장된 NFT 를 가지고 ERC-20 을 이용하여 FT 를 생성한다. 생성된 FT 를 각각의 구매자가 구매하여 각각의 금액으로 매매를 할 수 있도록 한다. 예를 들어 부동산 자산 ABC 가 있다고 할 때 자산을 NFT nABC (ERC-721)로 모델링 한다. 한 개의 NFT 로 생성된 nABC 를 NFT Vault 에 저장 (LOCK)을 하고, nABC 를 지정한 갯수의 FT fABC (ERC-20)들로 분할한다.

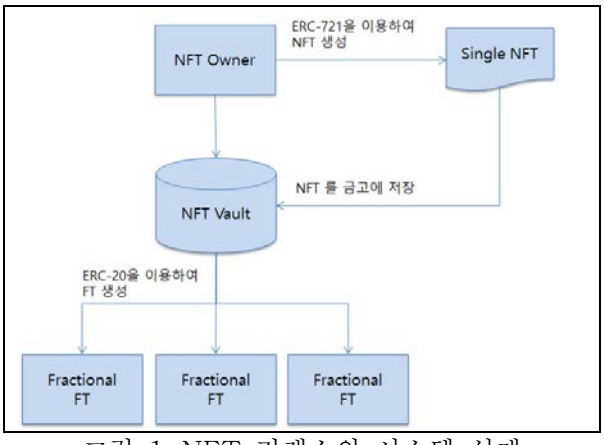

그림 1. NFT 거래소의 시스템 설계

해당 부동산 자산의 가격을 실시간으로 가져오기 위해서 공공데이터 포털에서 Open API 를 활용하여 해당지역의 부동산 자산가격을 실시간으로 가져오고 해당 지역의 평균값을 적용한다. 예를 들어 부동산 자산을 NFT (ERC-721)로 모델링 한 nABC 의 가격

을 Open API 를 이용하여 실시간으로 평균 가격을 반영한다. 이때 파라미터로는 주소 정보와 해당 가격을 가져오기 위한 연월 정보가 필요하다.

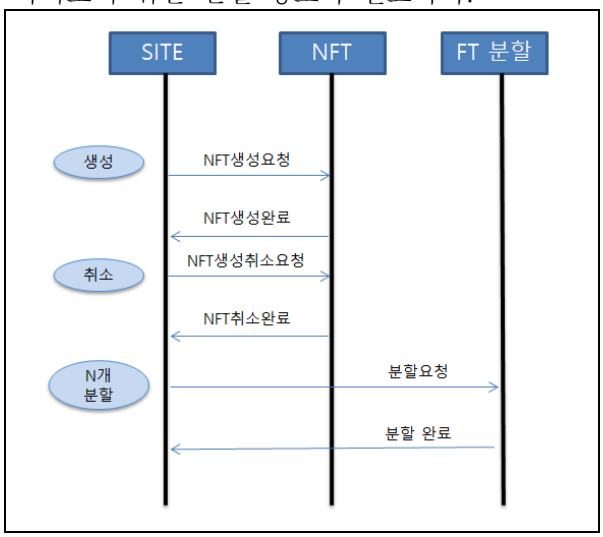

그림 2. 부동산 자산을 NFT 로 만들고 FT 로 분할

4. 구현

전체적인 시스템 구성은 그림 3 과 같다. 클라이언트에서 web3.js 라이브러리를 이용하여 NFT Smart Contract 와 연동하여 이더리움 네트워크와 통신한다. web3.js 는 이더리움과 상호 작용하는 자바스크립트 라이브러리다. 일반적으로 분산 앱 (dapps)에서 거래 전송, 스마트 계약 상호 작용, 블록 데이터 읽기 및 기타 다양한 이벤트를 지원한다. Smart Contract 내부에서는 부동산 가격을 가져올 수 없기 때문에 외부 데이터를 가져오기 위해 ORACLE (Open API)를 활용하였다. ORACLE 을 활용하기 위하여 Flask 를 이용하여 사용자 정의 웹 서버를 만들었다. Flask 는 사용자의 요청이 들어올 때마다 동적으로 HTML 코드를 만들어내는 파이썬 기반의 웹 서버이다. Flask Server 에서는 ORACLE 를 활용한 부동산 자산의 가격을 가져오고 또한 BOOT Server 을 이용하여 구매자가 NFT 를 구매할 때 Black Litterman 를 이용하여 효과적인 포트폴리오 구성을 할 수 있도록 한다.

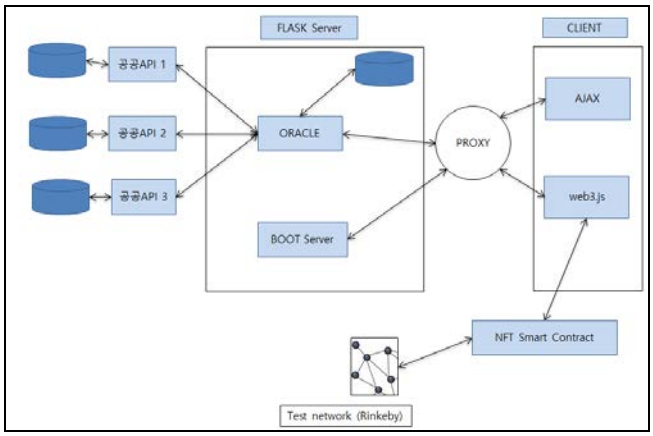

그림 3. NFT 거래소의 전체 시스템 구조

그림 4 와 같이, 생성된 NFT 를 NFT 마켓에서 확인하고, 상세 화면에서 분할된 내용에서 판매개수를 지정하여 구매한다. 또한 NFT 평가 메뉴에서 자산 가격 조회와 Black-Litterman 평가를 이용하여 내가 보유하고 있는 NFT 의 평가 Black-Litterman 를 하여 현재 보유하고 있는 나의 자산이 합리적인지를 평가할 수 있다.

5. 결론

본 논문에서는 분할 NFT 를 만들고 합리적인 매매를 하는 기법을 제안한다. Smart Contract 내부에서는 부동산 가격을 가져올 수 없기 때문에 외부 데이터를 가져오기 위해, Open API 기반의 oracle 를 활용하였다. 또한, 부동산 소유권을 ERC-721 을 활용하여 NFT 를 만들었고 생성된 NFT 에 높은 유동성과 이익 창출 등을 위해서 FT 로 분할하여, 스마트 계약 기반의 거래를 할 수 있도록 하였다. 그리고 구매자가 구매할 때 Black Litterman 모델을 적용하여 효과적인 포트폴리오를 구성하는 것을 제안하였다.

그림 4. NFT 분할, 구매, 및 자산포트폴리오 최적화

참고문헌

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, Whitepaper, 2008.

[2] 권혁준, 임민수, 김협. (2021).NFT 의 거래 가능성 및 확장성에 대한 고찰 -대체거래소 연계를 중심으로-.지급결제학회지,13 (1),257-272.

[3] Black Litterman 모델: https://m.blog.naver.com/koieam7673/221913595878