JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 26 No. 3, pp. 59-67, March 2021
https://doi.org/10.9708/jksci.2021.26.03.059

A Survey of Decentralized Finance(DeFi) based on Blockchain

Junsang Kim*, Seyong Kim*

*Deputy director, Ministry of National Defense, Seoul, Korea
*Lt. Col., Ministry of National Defense, Seoul, Korea

[Abstract]

Blockchain technology began in 2008 when an unidentified person named Satoshi Nakamoto proposed a cryptocurrency called Bitcoin. Satoshi Nakamoto had distrust of the existing financial system and wanted to implement a financial system that is robust against hacking or mannipulation without a middleman such as a bank through blockchain technology. Satoshi proposed a blockchain as a technology to prevent the creation of the bitcoin and forging of transactions, and through this, the functions of issuance, transaction, and verification of currency were implemented.

Since then, Ethereum, a cryptocurrency that can implement the smart contract on the blockchain, has been developed, allowing financial products that require complex contracts such as deposits, loans, insurance, and derivatives to be brought into the area of cryptocurrency. In addition, it is expanding the possibility of substituting products provided by financial institutions through combination with real assets. These applications are defined as Decentralized Finance (DeFi).

This paper was prepared to understand the overall technical understanding of DeFi and to introduce the services currently in operation. First, the technologies and ecosystems that implement the overall DeFi are explained, and then the representative DeFi services are categorized by feature and described.

▸ **Key words**: Blockchain, Bitcoin, Decentralized Finance, DeFi, Smart Contract

[요 약]

블록체인 기술은 2008년 나카모토 사토시라는 신원미상의 인물이 비트코인이라는 암호화폐를 제안하면서 시작되었다. 나카모토 사토시는 기존의 금융 시스템에 대한 불신을 가지고 있었고 은행과 같은 중개자 없이도 해킹이나 변조에 견고한 금융시스템을 블록체인 기술을 통해 구현하고자 했다. 사토시는 비트코인의 생성과, 거래의 위조를 방지하기 위한 기술로 블록체인을 제안하였고 이를 통해 화폐의 발행과 거래, 그리고 검증의 기능을 구현하였다.

이후 스마트 계약을 블록체인 상에서 구현할 수 있는 암호화폐인 이더리움이 개발되면서 예금, 대출, 보험, 파생상품 등 복잡한 계약이 필요한 금융상품을 암호화폐의 영역으로 끌어들일 수 있게 되었다. 또한 실물자산과 결합을 통해 금융 기관이 제공했던 상품을 대체할 수 있는 가능성도 확대해 나가고 있다. 이러한 애플리케이션들을 Decentralized Finance(DeFi)라고 정의한다.

본 논문은 전반적인 DeFi의 기술적 이해와 현재 운영되고 있는 어플리케이션의 소개를 위하여 작성되었다. 먼저 전반적인 DeFi를 구현하는 기술들과 생태계에 대해서 설명한 후 대표적인 DeFi 애플리케이션들을 특징별로 분류하여 설명한다.

▸ **주제어**: 블록체인, 비트코인, 탈중앙화 금융, 디파이, 스마트 계약

• First Author: Junsang Kim, Corresponding Author: Seyong Kim
*Junsang Kim (kjspbe@mnd.go.kr), Ministry of National Defense
*Seyong Kim (threedragon@mnd.go.kr), Ministry of National Defense
• Received: 2020. 12. 22, Revised: 2021. 01. 28, Accepted: 2021. 01. 28.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

블록체인 기술은 2008년 나카모토 사토시라는 신원미상의 인물이 비트코인(Bitcoin, BTC)이라는 암호화폐를 제안하면서 시작되었다[1]. 2008년은 미국의 서브프라임 모기지 사태가 발생했던 해로 현재 금융 시스템의 기반인 은행에 대한 불신이 팽배했던 시기이다. 나카모토 사토시 또한 기존의 은행 시스템에 대한 불신을 가지고 있었기 때문에 은행 없이도 해킹이나 변조에 견고한 금융시스템을 비트코인을 통해 구현하고자 했다. 비트코인은 은행 없이도 비트코인 사용자들의 참여를 통한 중앙 시스템의 역할을 10년이 넘은 지금까지 문제 없이 수행하고 있다. 사토시는 비트코인의 생성과 거래의 위조를 방지하기 위한 기술로 블록체인을 소개하였으며 현재는 암호화폐 분야 뿐만 아니라 데이터 위변조 방지가 필요한 많은 분야에 널리 사용되고 있다.

블록체인 기술의 활성화와 더불어 사토시가 원했던 은행이라는 중개자를 대체하기 위한 시도들이 암호화폐 업계에서는 지속적으로 이루어지고 있다. 비트코인 네트워크는 화폐의 생성과 거래, 그리고 검증의 기능만 가지고 있다. 시중 은행이 제공하는 예금, 대출, 보험, 파생상품 등 금융계약이 필요한 서비스들은 비트코인 상에서는 구현이 불가능했다. 하지만 스마트 계약을 블록체인 상에서 구현할 수 있는 암호화폐인 이더리움(Ethereum, ETH)이 개발되면서 중개자 없는 금융상품, 탈중앙화 금융(Decentralized Finance, DeFi)의 구현이 가능해졌다[2-3].

DeFi는 은행이라는 중개자가 없는 금융 생태계를 지향한다. 거래와 계약은 중개자 없이 스마트계약으로 블록체인에 기록되어 위변조가 불가능하며 예금, 대출, 이자 지급 등의 업무가 코드에 설계된 대로 수행된다[4-6].

본 논문은 전반적인 DeFi를 구현하는 기술들과 어플리케이션에 대한 이해를 돕기 위해 작성되었다. 또한 대표적인 DeFi 애플리케이션들을 소개하고 특징과 목적에 따라 분류한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 블록체인 기반의 DeFi를 구현하는 배경 기술에 대해서 설명한다. 그리고 3장에서는 DeFi의 생태계를 구성하는 어플리케이션들에 대해서 설명하고 4장에서는 대표적인 DeFi 애플리케이션들을 특징별로 분류하여 소개한다. 그리고 5장에서는 결론을 맺는다.

II. Background Technology

1. Bitcoin & Blockchain

블록체인은 수많은 노드가 인터넷 기반의 P2P 네트워크로 연결되어 거래를 기록하고 처리하는 '분장 원장 시스템'을 의미한다[7]. 일반적으로 금융 거래는 은행이라는 신뢰성있는 중개자(middleman)가 기록하고 보증하는 역할을 하지만 블록체인은 중개자 없이 사용자들이 원장을 공동으로 기록하고 관리하여 원장의 신뢰성을 보증한다. 어떠한 거래기록이 발생하면 모든 사용자의 원장에 동기화되어 기록되기 때문에 조작이 불가능하다.

비트코인은 블록체인 기술을 이용하여 구현된 최초의 암호화폐로 은행과 같은 중개자가 없이 모든 사용자가 참여하여 화폐발행과 송·수금 기록 및 검증의 역할을 할 수 있도록 설계된 시스템이다. 비트코인은 이러한 역할을 수행한 노드들에게 보상금으로 주어지는 형태로 발행되며 반감기 및 최대 발행량이 미리 정해져 있다.

비트코인 네트워크의 블록체인은 구조상 Fig 1.과 같이 블록으로 이루어진 연결 리스트이다. 새로 생성되는 블록의 해시는 직전 블록의 해시를 포함하여 생성되기 때문에 특정 블록을 임의로 수정하면 연결된 블록과 해시값이 일치하지 않게 되어 조작된 블록임이 드러나게 된다. 이러한 블록은 10분에 하나씩 생성되어 비트코인 네트워크에 참여한 모든 노드들에게 분배되고 검증된다. 그래서 특정 노드의 블록이 조작되어도 51% 이상의 노드들을 해킹하지 않는 이상 기록한 데이터를 조작할 수 없다. 현재 비트코인의 노드는 전 세계에 10000개가 넘는다.

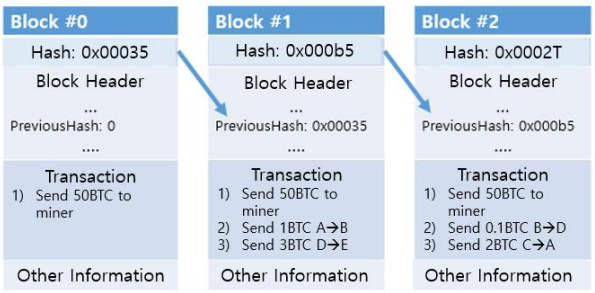

Fig. 1. Blockchain Architecture[7]

블록체인 기술은 단지 비트코인과 같은 암호화폐에만 한정되지는 않는다. 조작 방지 및 검증이 필요한 다양한 산업에서 사용되고 있고 활용 범위도 점점 넓어지고 있다.

2. Ethreum & Smart Contract

이더리움은 2015년 비탈릭 부테린(Vitalik Buterin)이 개발한 블록체인 기술 기반의 스마트 계약을 지원하는 분산 응용 어플리케이션 플랫폼이다[2]. 비트코인이 화폐거래 트랜잭션만을 블록체인에 기록할 수 있었다면 이더리움은 다양한 형태의 계약을 블록체인에 기록할 수 있다.

스마트 계약은 계약을 프로그래밍하여 블록체인에 탑재할 수 있는 기술로 중개자 없이 특정 요건에 도달했을 경우 자동으로 프로그래밍 된 계약이 실행이 된다. 암호자산을 맡겼을 때 자동으로 이자가 지급되게 한다던지, 특정 암호화폐를 보내면 다른 암호화폐를 교환하는 등 다양한 금융 거래를 스마트계약으로 구현할 수 있다. 스마트계약은 은행과 같은 신뢰성 있는 중개자가 없지만 블록체인의 특성상 조작이 불가능하고 많은 노드들에 의해 영구히 기록되기 때문에 모든 계약의 보증이 가능하다. 그 외 스마트 계약을 지원하는 블록체인 네트워크는 이오스(EOS)[8], 트론(TRON)[9] 등이 있다.

3. Decentralized Application(DApp)

우리가 흔히 사용하는 배달 앱이나 예약 앱의 경우 특정 회사의 시스템을 이용하여 운영된다. 신뢰성이 있는 3자가 개인과 업체를 연결해주며 수수료나 운영 정책은 해당 회사가 정한다. 모든 데이터도 해당 회사가 독점 보유하게 된다. 블록체인 업계에서는 이를 중앙화된 어플리케이션(Centralized Application)이라고 한다. 이와 반대되는 개념이 탈중앙화된 어플리케이션(Decentralized Application, DApp)이며 블록체인 기반의 스마트 계약을 이용하여 운영된다. DApp에서 운영되는 주요 데이터들은 특정 회사의 서버에 기록되는 것이 아니라 블록체인에 기록되어 영구히 보존되며 모든 이들이 열람할 수 있다. 앞으로 설명할 각종 DeFi 애플리케이션들도 DApp의 일종으로 대부분의 서비스들이 탈중앙화된 형태로 운영된다.

DApp은 이더리움 등의 기존 블록체인 플랫폼 위에서 동작하기 때문에 별도의 블록체인 네트워크를 개발 및 운영하지 않더라도 탈중앙화된 어플리케이션을 쉽게 구현할 수 있다. DApp 또한 거래와 보상을 위해 자체 암호화폐(토큰)를 발행할 수 있는데 이더리움 플랫폼의 경우 ERC-20, ERC-721라는 토큰의 표준을 제공한다.

III. DeFi Ecosystem

DeFi 애플리케이션을 이용하기 위해서는 우선 개인 암호화폐 지갑이 있어야 된다. 지갑은 암호화폐의 통장과 같은 역할을 한다. 모든 거래내역은 지갑의 주소를 기반으로 블록체인에 기록된다. 암호화폐의 큰 변동성은 금융 상품으로 활용하기에 어려운 측면이 있었는데 이를 보완하고 실물자산과 연계하여 가치를 보존할 수 있는 코인을 스테이블 코인이라고 한다. 안정화된 자산인 스테이블 코인으로 인해 더욱 다양한 DeFi 상품들을 사용할 수 있게 되었다.

본인의 지갑에 보유한 암호화폐를 다른 암호화폐나 스테이블 코인으로 바꾸기 위해서 거래소가 필요한데 이를 가능하게 해주는 어플리케이션이 바로 탈중앙화 거래소(DEX)이다. 만약 중앙화된 거래소에서 교환하려면 거래소 지갑에 보내고 거래를 마친 후에 다시 개인 지갑으로 전송해야 되는 문제가 발생한다. 탈중앙화 거래소는 교환할 코인의 유동성이 부족하거나 교환할 금액이 매우 클 경우 손실이 발생하는데, 이를 분산하여 최적의 거래조건을 만들어내는 어플리케이션을 DEX Aggregator라고 한다. 이러한 요소들은 DeFi 생태계의 일원으로 DeFi 애플리케이션을 가능하게 하는 기반이 된다.

1. Crypto Wallet

암호화폐에 투자하기 위해서 대부분 바이낸스나 업비트와 같은 중앙화된 거래소에 법정화폐를 입금하여 암호화폐를 구매한다. 그렇게 구매한 암호화폐는 개인의 소유이고 언제든지 출금과 거래가 가능지만 실제로는 거래소의 지갑에 보관되어 있는 자산이다. 그래서 DeFi와 같이 스마트계약을 통한 탈중앙화 애플리케이션을 사용하기 위해서는 개인 지갑의 주소로 암호화폐를 옮겨놓아야 한다.

가장 널리 쓰이는 개인 지갑은 메타마스크(metamask)이다. 이러한 소프트웨어 지갑은 거래 시 필요한 개인키를 잘 보관해야 하는데 지갑이 설치된 컴퓨터나 스마트폰 해킹으로 유출되는 경우가 종종 발생된다. 해커가 개인키를 확보하면 해당 지갑의 암호화폐를 모두 출금할 수 있다.

하드웨어 지갑은 개인키를 가지고 있는 하드웨어장치로 거래를 해당 하드웨어에서 직접 승인해야 개인키를 이용한 거래가 성립된다. 개인키가 직접 노출되지 않기 때문에 하드웨어 지갑은 소프트웨어 지갑에 비해 안전하다고 볼 수 있다. 유일한 해킹방법은 해커들이 하드웨어 지갑을 직접 훔치는 방법 밖에 없는데 하드웨어 지갑을 통해 **개인키를** 전송할 때 비밀번호를 입력하거나 지문을 인식하도록 되어 있기 때문에 해킹이 거의 불가능하다고 볼 수 있다.

2. Stable Coin

일반적인 암호화폐는 기본적으로 법정화폐보다 가격변동성이 높은 특징을 가지고 있다. 이러한 가격 변동성은

Table 1. Classification of Stable Coins (MarketCap reference : coinmarketcap.com, '20. 12.13.)

Name	Code	Catogory	Issuer	MarketCap (USD)	Pegged currency	Network
Tether	USDT	Fiat-Collateralized	Tether	19844M	US Doller	BTC, ETH, TRON, EOS
Tether Gold	XAUT	Materials-Collateralized	Tether	N/A	Gold	ETH
USD Coin	USDC	Fiat-Collateralized	Centre	3214M	US Doller	ETH
Dai	DAI	Crypto-Collateralized	MakerDAO	1097M	US Doller	ETH, Binance Chain
Binance USD	BUSD	Fiat-Collateralized	Binance	435M	US Doller	ETH, Binance Chain
TrueUSD	TUSD	Fiat-Collateralized	TrustToken	284M	US Doller	ETH, Binance Chain
TrueGBP	TGBP	Fiat-Collateralized	TrustToken	N/A	UK Pound	ETH
Paxos Standard	PAX	Fiat-Collateralized	Paxos Trust	244M	US Doller	ETH, Binance Chain
Paxos Gold	PAXG	Materials-Collateralized	Paxos Trust	77M	Gold	ETH, Binance Chain
sUSD	SUSD	Non-Collateralized	Synthetix	22M	US Doller	ETH
TerraUSD	UST	Non-Collateralized	Terra	23M	US Doller	Terra Mainnet
TerraKRW	KRT	Non-Collateralized	Terra	78M	Korea Won	Terra Mainnet

실생활에서 암호화폐 사용에 큰 걸림돌이 되어왔다. 실제로 제도권 은행을 통하는 것보다 암호화폐를 이용하여 송금하는 것이 수수료 측면이나 송금 속도 측면에서 훨씬 유리하지만 송금 전후의 가격 변동에 따라 손해를 볼 수 있다는 단점이 있다. 비트코인은 중개자를 통하지 않고도 금융거래가 가능한 혁신적인 플랫폼이었지만 이러한 높은 가격 변동성으로 인해 실생활에서의 사용이 한정적일 수 밖에 없었다. 암호화폐를 기반으로 하는 금융상품 또한 가격변동성이 높은 경우 리스크와 불확실성이 증가하기 때문에 출시 및 운용이 어려울 수 밖에 없다.

스테이블 코인은 가격 변동성이 거의 없는 암호화폐로 이러한 문제를 해결하기 위하여 고안되었다. 대부분의 스테이블 코인은 1달러의 가치를 가지고 있기 때문에 보유한 암호화폐를 스테이블 코인으로 교환하거나 담보로 스테이블 코인을 빌려서 암호화폐의 가치를 실물 경제로 이동시켜 사용할 수 있다. 스테이블 코인은 가치의 보존을 위해 담보를 두고 발행하는 등 다양한 방법을 사용하는데 이러한 특성에 따라 다음과 같이 4가지 종류로 분류하고 Table 1에 정리하였다.

2.1. Fiat-Collateralized Stable Coin

법정화폐 담보 스테이블 코인(Fiat-Collateralized Stable Coin)은 코인을 발행한 회사에서 동일한 가치만큼의 법정화폐를 예치하여 사용자가 원할 때 언제든지 법정화폐로 교환할 수 있도록 운영하는 방식이다. 대부분 미국 달러에 연동되어 있는 스테이블 코인이 유통되고 있으며 유로나 원화에 연동된 스테이블 코인도 존재한다. 대표적인 법정화폐 담보방식으로는 스테이블 코인 시총 1위인 Tether(USDT)[10]가 있으며 2위인 Binance USD(BUSD)[11], 3위인 USD Coin(USDC)[12], 4위인 TrueUSD(TUSD)[13]가 있다. 이와 같이 시총 상위권 스테이블 코인은 대부분 법정화폐 담보방식으로 발행되고 있다.

법정화폐 담보 방식은 결국 운영사라는 중개자가 포함될 수밖에 없는 구조를 가지고 있기 때문에 중앙화 이슈에 따른 취약성이 존재한다. 대부분의 스테이블 코인은 정기 회계감사 등의 방법을 통해 발행한 코인만큼의 담보를 적절하게 유지하고 있는지 검증하고 있지만 일부는 이러한 과정이 불분명하여 논란이 된 경우가 존재한다.

2.2 Crypto-Collateralized Stable Coin

암호화폐 담보 스테이블 코인(Crypto-Collateralized Stable Coin)은 사용자가 기존 암호화폐를 담보로 스테이블 코인을 발행하는 방식으로 암호화폐의 가격 변동성 문제로 인해 실제 암호화폐의 가치보다 작은 가치의 스테이블 코인을 발생할 수 있다. 그리고 담보로 맡긴 암호화폐의 가치가 급락할 경우 담보물을 자동으로 청산하여 스테이블 코인의 가치를 유지한다. 대표적인 암호화폐 담보방식의 스테이블코인은 MakerDAO에서 발행하는 DAI[14]이다. 그 외에도 Bitshare에서 발행하는 bitUSD[15]등이 있으며 대부분 미국 달러의 가격에 연동되어 있다. 암호화폐 담보 방식은 중개자의 개입이 없이 스마트 계약으로 발행, 소각, 청산이 이루어지기 때문에 모든 과정이 투명하다는 장점이 있는 반면 담보된 암호화폐의 급격한 가치변화로 인해 담보물이 청산되어 손해를 입을 수 있다는 단점 또한 존재한다.

2.3 Non-Collateralized Stable Coin

무담보형 스테이블 코인(Non-Collateralized Stable Coin)은 실물자산과 연동되지 않지만 코인의 유통량을 코인의 가격 변동에 따라 늘리거나 줄여서 가격 안정성을 유지한다. 화폐의 수요-공급의 법칙을 이용하여 코인의 가격이 상승했을 때 추가발행하여 가치를 줄이고 가격이 하락하면 매수하여 소각하는 방식으로 가치를 조정한다. 이 방

식은 국가가 금리나 통화량을 조절하여 화폐의 가치를 유지하는 정책과 유사하다. 다만 이러한 과정이 중개자의 개입 없이 자동화된 알고리즘에 의해서 수행된다는 점에서 차이가 존재한다. 하지만 회사의 운영문제나 해킹 등으로 해당 스테이블 코인의 신뢰성이 한번에 추락할 경우 담보가 없기 때문에 사용자들이 손실을 입을 가능성도 존재한다. 대표적인 무담보 방식의 스테이블 코인은 TerraUSD[16], sUSD[17]등이 있다. 대부분 미국 달러에 연동되어 있으며 TerraKRW[16]와 같이 원화에 연동된 스테이블 코인도 발행되고 있다.

2.4 Materials-Collateralized Stable Coin

기본적으로 법정화폐 담보 방식과 유사한 방식이지만, 법정 화폐가 아닌 원자재에 연동되는 구조를 가지고 있다. 현재 출시되어 있는 원자재 담보 스테이블 코인(Materials-Collateralized Stable Coin)은 현재 금을 담보로 발행되는 Tether Gold(XAUT)[10], Paxos Gold(PAXG)[18]가 있다. 해당 코인들은 1온스의 금 가격으로 고정되어 있으며 발행량만큼의 금이 담보로 보관되어 있다.

향후 Tether사는 원유 등의 다른 원자재와 연동된 스테이블 코인을 출시할 예정이다. 원자재 기반의 담보 방식은 아직 시작단계이지만 향후 다양한 실물 자산들이 블록체인 영역으로 연결되어 중개자 없이 거래될 것으로 예상된다.

3. Decentralized Exchange(DEX)

탈중앙화 거래소는 암호화폐의 거래가 가능한 플랫폼이다. 바이낸스나 업비트 등의 중앙화된 거래소는 모든 사용자가 거래소의 지갑에 입금하여 거래소의 통제에 따라 암호화폐를 거래하는 형식인 반면 탈중앙화 거래소는 개인의 지갑을 이용하여 직접 거래하는 형식으로 운영된다. 오직 지갑의 주소로 거래하기 때문에 중앙화된 거래소처럼 가입 절차나 개인정보의 제공이 필요없다.

초기의 탈중앙화 거래소는 사용자가 오더북에 판매/구매 주문조건을 등록하고 또 다른 교환을 원하는 사용자가 교환을 수락하면 개인 지갑 대 지갑의 스마트 계약을 통해 거래가 이루어지는 형식이었다. 금액이나 거래량 조건이 맞아야 된다는 제약사항 때문에 활성화되지 못하였지만 자동화된 마켓 메이킹(Automated Market Making, AMM) 기술이 개발되면서 이러한 단점이 보완되었다.

최초로 AMM을 구현한 탈중앙화 거래소인 유니스왑(Uniswap)[19]은 이더리움 재단의 투자를 받아 2년간의 개발과정을 거쳐 개발되었다. AMM은 유동성 공급자를 통해 유동성 풀을 만들고 미리 구현되어 있는 스마트 계약에 의해 결정된 가격으로 거래를 가능하게 한다.

우선 유동성 공급자는 2개의 토큰 쌍을 유동성 풀에 예치를 하여 거래의 기반을 만든다. 예를 들어 유동성 공급자가 만약 동일한 금액의 USDT와 이더리움 쌍으로 유동성 풀을 만들면 교환을 원하는 사용자들은 이 유동성 풀을 이용하여 USDT와 이더리움을 자동화된 가격에 따라 거래 가능하게 된다. 만약 USDT를 이더리움으로 교환한다고 가정하면 교환 후에는 유동성 풀의 USDT가 증가하고 이더리움은 감소하게 된다. 그러면 AMM에 의하여 이더리움의 가격이 증가하고 결국 동일한 금액이 맞추어지게 된다. 토큰의 교환으로 인해 이더리움의 가격이 상승한 경우 일반 거래소나 다른 탈중앙화된 거래소와 가격 차이가 나는 경우가 발생한다. 이러한 경우 장외에 있던 이더리움의 보유자들은 다른 거래소보다 더 비싼 가격에 이더리움을 판매하기 위해 유입되기 때문에 결국 시장가에 근접한 가격이 형성되게 된다.

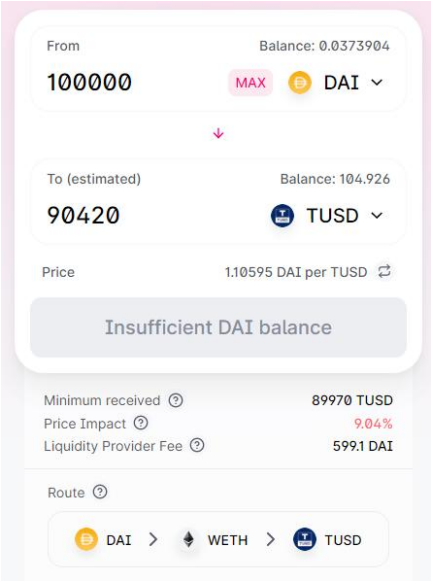

Fig. 2. Uniswap Exchange Example[19]

만약 교환을 원하는 토큰 쌍이 없다면 여러 토큰 쌍을조합하여 거래가 가능하다. Fig 2에는 유니스왑에서 DAI를 TUSD로 교환할 때 해당 토큰 쌍의 유동성 풀이 없어서 이더리움-DAI 풀과 이더리움-TUSD 풀을 조합하여 교환되는 중간과정을 보여준다.

유니스왑과 같이 규모가 큰 거래소의 경우 대부분의 토큰들이 이더리움과 한 쌍으로 유동성이 공급되어 있기 때문에 해당하는 토큰 쌍이 없는 경우에도 대부분 이더리움 풀을 경유해서 거래가 가능하다. 각 거래에는 Fig 2와 같이 수수료(Liqudity Provider Fee)가 일정부분 부과되는데 이 수수료는 유동성 공급자들에게 지급되어 암호자산

Fig. 3. DEX Aggregator(1inch) Example[20]

보유자들이 유동성 풀에 참여하도록 유도한다. 유동성 풀은 크면 클수록 유리한데, 더 큰 금액의 거래를 지원할 수 있기 때문이다. 유동성 풀이 작은데 큰 금액의 거래가 요청되면 풀의 유동성 변동이 커지고 AMM의 알고리즘에 따라 가격이 조정되면서 시중가와 차이가 벌어지게 된다.

Fig. 2의 Price Impact는 이러한 차이를 나타내는 지표이다. DAI와 TUSD는 스테이블 코인으로 가치가 동일하게 1달러인데 수수료인 599.1DAI를 고려해도 Price Impact가 9.04나 되기 때문에 9% 가량의 가격 차이가 나게 된다. 그러므로 Price Impact가 높은 경우 해당 유동성 풀이 작아서 손해가 크게 되므로 다른 거래소나 중앙형 거래소를 이용하는 것을 고려해야 된다. 이러한 부분은 후술할 Dex Aggregator를 이용하여 어느정도 보완할 수 있다.

4. DEX Aggregator

DEX Aggregator는 탈중앙화 거래소의 유동성 정보를 모아 가장 효율적인 방식으로 거래를 할 수 있는 서비스를 제공한다. 소액의 암호화폐를 교환할 때는 가장 좋은 조건의 DEX를 추천해준다. 하지만 큰 금액의 암호화폐를 거래할 경우 여러 유동성 풀을 조합하여 추천한다. 단일 유동성 풀을 이용하여 큰 금액의 암호화폐를 교환 할 경우 시세 대비 가격 괴리가 매우 높게 형성되기 때문에 교환 효율이 떨어지기 때문이다.

Fig. 3은 대표적인 DEX Aggregator인 1inch[20]에서 대량의 이더리움을 TUSD로 교환할 때 Uniswap, Balancer[21] 등 총 8개의 풀에 분산하여 교환하는 경로를 나타내고 있다. 이렇게 어려 개의 풀과 경로로 암호화폐를 교환하게 되면 시세와의 가격 괴리는 줄게 되지만 거래에 따른 수수료(Gas fee)는 상당히 증가하게 된다. DEX Aggreator은 수수료 부분까지 감안하여 최적의 조건을 검출한다. 현재 1inch외에도 Matcha[22], DEX.AG[23] 등의 DEX Aggreator가 서비스 되고 있다.

5. Pegged Token

비트코인은 전체 암호화폐 시총의 60% 이상을 차지하고 있다. 하지만 대부분의 DeFi 애플리케이션은 이더리움 네트워크 기반의 스마트 계약으로 동작하기 때문에 보유하고 있는 비트코인을 직접적으로 DeFi 애플리케이션에 사용하는 것이 불가능하다. Wrapped BTC(WBTC)[24]는 비트코인을 담보로 이더리움 기반의 ERC-20 토큰을 생성한다. 해당 토큰은 수탁받은 비트코인의 개수만큼 생성되며 정확히 비트코인 가격과 일치한다. 해당 토큰은 이더리움 기반의 스마트 계약에 연동되어 각종 DeFi 애플리케이션에 사용이 가능하다.

6. Governance Token

DeFi 애플리케이션 등 DApp의 기여자들에게 보상으로 주어지는 토큰으로 보유 시 해당 DApp의 각종 의사결정에 투표지분을 확보할 수 있다. 이러한 거버넌스 토큰들이 가치를 인정받게 되면서 거래소에서 높은 가격에 거래되기 시작했다. 여러 DeFi 애플리케이션에서 암호자산을 수탁하거나 유동성을 공급할 경우 보너스로 지급했기 때문에 투자자 입장에서는 비교적 고수익이 얻을 수 있다. 거버넌스 토큰을 지급한 최초의 DeFi 애플리케이션은 Compound[25]이며 이로 인해 DeFi 이용자와 수탁금액이 대폭 확대되는 계기가 되었다.

IV. Type of DeFi Application

DeFi는 금융기관이라는 중개자 없이 블록체인에 기록되어 실행되는 스마트 계약을 통해서 서비스되는 탈중앙화된 금융상품을 의미한다.

DeFi 어플리케이션은 예금, 대출, 펀드, 보험 등 일반 금융기관에서 판매되는 금융 상품과 유사한 속성을 가지고 있다. 다만 자산 수탁의 경우 그 형태에 따라서 스테이

킹, 랜딩, 유동성 마이닝으로 분류된다. 또한 지원하는 블록체인 네트워크에 따라서 사용 가능한 암호화폐의 종류가 다르게 되는데 현재는 이더리움 네트워크 기반의 애플리케이션이 대부분을 차지한다. 트론이나 이오스 블록체인 네트워크 기반의 DeFi도 출시되였으나 아직 TVL은 미미한 상황이다. 아래의 Table 2는 각 DeFi 어플리케이션의 카테고리와, 발생하는 거버넌스 토큰, 그리고 지원하는 블록체인 네트워크를 정리한 표이다.

Table 2. List of DeFi Application

Name	Category	Govenence Token	Network
Ethereum 2.0	Staking	-	Ethereum
QTUM	Staking	-	QTUM
MakerDAO	**Lending**	MKR	Ethereum
Compound	**Lending**	COMP	Ethereum
Aave	**Lending**	AAVE	Ethereum
Uniswap	Liquidity Mining	UNI	Ethereum
SushiSwap	Liquidity Mining	SUSHI	Ethereum
Curve Finance	Liquidity Mining	CRV	Ethereum
Synthetix	Derivatives	-	Ethereum
Balancer	Liquidity Mining	BAL	Ethereum
Harvest Finance	Fund	FARM	Ethereum
yearn.finance	Fund	YFI	Ethereum
yinsure.finance	Insurance	YFI	Ethereum

1. Staking

퀀텀(QTUM)[26], 이더리움 2.0(출시예정) 등의 블록체인 네트워크는 PoS(Proof of Stake)라는 합의 알고리즘으로 운영된다. 해당 네트워크를 구성하는 노드는 본인의 지갑에 보유하고 있는 암호화폐를 일정부분 락업(Lock up)한 후에 해당 블록체인 네트워크의 블록 생성과 검증에 참여한다. 이를 대가로 암호화폐가 주어지는데 기술적으로 금융상품에 가깝지는 않지만 락업된 암호화폐에 이자가 주어지는 형태를 취하고 있기 때문에 DeFi의 한 분류에 포함된다고 볼 수 있다.

2. Lending

암호화폐를 맡기거나 빌릴 수 있는 예금/대출 서비스이다. 암호화폐를 맡기면 일정 부분 이자를 받을 수 있고 반대로 빌리게 되면 이자를 지급해야 된다. 대부분의 플랫폼에서 이자율은 정해진 알고리즘에 따라 수요에 따라 수시로 조정되지만 일부는 고정 이율을 제시하는 경우도 있다. 예금/대출 이자가 높은 암호화폐는 대출 수요가 높은 암호화폐이다, 해당 플랫폼은 지급하는 예금이자와 지급받은 대출이자의 차이를 이용하여 수익을 창출한다. 대부분의 플랫폼에서 대출 시 담보를 요구하며 담보의 50~80% 선까지 대출이 가능하다. 만약 담보로 맡긴 암호화폐가 가격이 떨어지거나 대출한 암호화폐의 가격이 급등하여 대출금액에 근접하게 되면 해당 담보는 스마트 계약에 따라 강제로 청산되게 된다.

랜딩 서비스를 지원하는 대표적인 DeFi 애플리케이션은 MakerDAO, Compound, Aave[27] 등이 있으며 이 세 개의 어플리케이션이 항상 TVL 상위 5위에 들 정도로 큰 규모의 자산이 수탁되어 있다.

3. Liquidity Mining

유동성 마이닝(Liquidity Mining)은 탈중앙화 거래소의 유동성 풀을 제공하여 수익을 얻는 것을 의미한다. 전체 수수료에서 제공한 토큰 쌍의 유동성의 비율만큼 수수료를 받기 때문에 많은 암호화폐를 예치할수록 많은 수수료를 획득할 수 있다. 일부 유동성 풀은 거버넌스 토큰을 함께 제공하여 수수료보다 더 큰 수익을 유동성 제공자에게 지급하기도 한다. 유동성 마이닝은 유동성 풀을 운영하는 탈중앙화 거래소에서는 모두 가능하다. 대표적인 탈중앙화 거래소에는 Uniswap이 있으며 Uniswap을 하드포크한 SushiSwap[28]를 비롯하여 Curve Finance[29], Balancer가 TVL 상위 10위권 안에 포진되어 있다.

4. Derivatives

DeFi 파생상품(Derivatives)은 블록체인 네트워크와 스마트 계약을 이용하여 기존 금융시장에 존재하는 파생상품들을 중개자 없이 거래할 수 있게 한다.

대표적인 파생상품 어플리케이션인 Synthetix[17]는 탈중앙화된 합성자산(synthetic asset) 투자 플랫폼이다. 합성자산은 전통 금융에서 만들어진 상품으로 현물을 보유하지 않고 가격만 추종하는 상품을 의미하는데 Synthetix는 이를 토큰화 하여 이더리움 블록체인 네트워크를 이용하여 거래할 수 있다. Synthetix에서는 암호화폐뿐만 아니라 법정 통화, 원자재, 니케이 지수 같은 인덱스를 추종하는 상품을 모두 거래할 수 있으며 향후 주식도 추가될 예정이다.

5. Fund

보유하고 있는 암호화폐를 맡기면 자동으로 가장 높은 수익을 제공하는 DeFi 애플리케이션에 투자하여 간편하게 수익을 낼 수 있는 서비스이다. DeFi 애플리케이션의 이자 수익은 수시로 변동되므로 투자 전략 또한 변동된다. 특정 DeFi 애플리케이션의 경우 거버넌스 토큰을 추가 수익을 지급하기도 하는데 특정 펀드 서비스에서는 이를 다시 맡긴 암호화폐로 교환하여 자동으로 재투자하기 때문에 투자자 입장에서는 굉장히 편리한 서비스이다. 자산 운용의

대가로 수수료를 부과한다. 가장 대표적인 어플리케이션은 yearn.finance[30]의 valut 서비스이며 후발주자로 Harvest Finance[31]가 급성장하고 있다.

5. Insure

탈중앙화 보험은 yearn.finance에서 출시한 yinsure[32]가 유일하다. Aave, Balancer 등 11개의 DeFi 애플리케이션에서 발생한 재정적인 손실의 보상을 제공한다. 보험 기간과 금액을 입력하면 자동으로 보험료를 산출하며 보험료는 보험제공자에게 지급된다. 보험 이용자는 스마트 계약에 명시된 투표 등의 과정을 거쳐 보험금을 수령할 수 있다. 현재는 실험성이 강한 프로젝트이지만 향후 실물자산과 결합하여 더 발전가능한 DeFi 영역이 될 것으로 예상된다.

V. Conclusion

2020년부터 본격적으로 확대된 DeFi 생태계는 점점 금융기관을 닮아가고 있다. 정확히 금융기관 자체가 아닌 금융기관이 제공하는 기능과 판매하는 상품이 DeFi 생태계에도 나타나고 있다.

DeFi는 중개자 없이 금융상품을 거래할 수 있다는 측면에서 전통 금융시장의 파괴적 혁신을 주도할 도전자가 될 수 있다. 특히 DeFi는 자본통제가 심하거나 금융 시스템이 제대로 갖추어지지 않은 국가나 지역에서는 스마트폰과 인터넷만으로 예금, 송금, 대출, 결제, 보험 등의 금융 모두 가능한 혁신적인 기술이 될 수 있다.

하지만 암호화폐에 대한 각국의 규제정책 및 소비자 보호대책이 모호한 측면이 있으며 관련 기술의 복잡성으로 인해 일반인들이 이해와 접근이 어려운 한계점이 존재한다. 그리고 대부분의 DeFi 서비스가 이더리움 네트워크에 편중되어 있고 이로 인하여 높은 수수료(Gas Fee)가 발생되고 있어 소액으로는 투자가 불가능하다는 문제가 존재한다. 이러한 문제를 해결하기 위해서는 우선 각국의 암호화폐 관련 제도의 정비와 소비자를 위한 법률적 보호장치가 필요하다. 또한 기존 금융기관들의 서비스를 벤치마킹하여 일반인들이 이해와 접근이 쉬운 서비스들의 출시가 필요하다. 특히 수수료 문제 해결을 위해서는 현재의 이더리움 네트워크 외 확장성이 뛰어난 다른 블록체인 플랫폼을 기반으로 하는 서비스들의 확대가 요구된다.

REFERENCES

[1] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system," *https://bitcoin.org/bitcoin.pdf*

[2] Buterin, Vitalik. "A Next-Generation Smart Contract and Decentralized Application Platform-Ethereum Whitepaper“, 2014. *https://github.com/ethereum/wiki/wiki/White-Paper*

[3] Schär, Fabian. "Decentralized Finance: On Blockchain-and Smart Contract-based Financial Markets." Available at SSRN 3571335 (2020).

[4] Chen, Yan, and Cristiano Bellavitis. "Decentralized finance: Blockchain technology and the quest for an open financial system." Stevens Institute of Technology School of Business Research Paper (2019).

[5] Chen, Yan, and Cristiano Bellavitis. "Blockchain disruption and decentralized finance: The rise of decentralized business models." Journal of Business Venturing Insights 13 (2020): e00151.

[6] Zetzsche, Dirk A., Douglas W. Arner, and Ross P. Buckley. "Decentralized Finance." Journal of Financial Regulation 6.2 (2020): 172-203.

[7] Kim, Junsang. "A Survey of Cryptocurrencies based on Blockchain." Journal of The Korea Society of Computer and Information 24.2 (2019): 67-74.

[8] Tron, *https://tron.network*

[9] EOS. *https://eos.io*

[10] Tether, *https://tether.to/*

[11] Binance USD, *https://www.binance.com/en/busd*

[12] USD Coin, *https://www.centre.io/usdc*

[13] TrueUSD, TrueGold, *https://www.trusttoken.com/*

[14] MakeerDAO, DAI, *http://www.makerdao.com/*

[15] bitUSD, *http://bit.ly/BitShares_USD*

[16] TerraUSD, *TeraKRW, https://terra.money/*

[17] Synthetix, sUSD, *https://www.synthetix.io/*

[18] Paxos Gold, *https://www.paxos.com/paxgold/*

[19] Uniswap, *https://uniswap.org/*

[20] 1inch exchange, *https://1inch.exchange/*

[21] Balancer, *https://balancer.finance/*

[22] Matcha, *https://matcha.xyz/*

[23] DEX.AG, *https://dex.ag*

[24] Wrapped BTC, *https://wbtc.network/*

[25] Compound, *https://compound.finance/*

[26] QTUM, *https://qtum.org/*

[27] Aave, *https://aave.com/*

[28] Sushiswap, *https://sushiswap.org/*

[29] Curve Finance, *https://www.curve.fi/*

[30] yearn.finance, *https://yearn.finance/*

[31] Harvest Finance, *https://harvest.finance/*

[32] yinsure.finance, *https://yinsure.finance/*

Authors

Junsang Kim received the B.S., M.S. and Ph.D. degrees in Computer Science and Engineering from Hanyang University, Korea, in 2003, 2005 and 2017, respectively. Dr. Kim is currently a deputy director in the Ministry of National Defense, South Korea.
He is interested in blockchain, big data, and cloud computing.

Seyong Kim received the M.S degrees in Operation Analysis from Korea National Defense University, Korea, in 2009. Mr. Kim is currently a Lt. Col. in the Ministry of National Defense, South Korea.
He is interested in AI, big data, cloud computing, block-chain and M&S.