이슈보고서 21-24

ISSUE
REPORT

스마트계약에 기반한 DeFi의 활용 가능성

권민경

자본시장연구원
Korea Capital Market Institute

스마트계약에 기반한 DeFi의 활용 가능성

저자 권민경*

DeFi는 블록체인 네트워크상에서 은행, 증권사 등 중앙화된 중개인을 거치지 않고 스마트계약을 통해 구현된 탈중앙화 금융서비스를 의미한다. DeFi를 이해하기 위해서는 먼저 기반기술인 블록체인과 스마트계약의 이해가 선행되어야 한다. 우선 블록체인은 2008년 비트코인의 개발로 처음 탄생하여 현재는 이미 많은 분야에 도입되어 활용되고 있다. 한편, 스마트계약은 1994년 닉 재보에 의해 처음 고안되었으며 2013년 이더리움의 개발로 블록체인에 적용되면서 본격적으로 활용되기 시작하였다. 이더리움은 프로그래밍 코드를 내포한 형태의 '계좌'와 데이터를 주고받을수 있는 '거래'의 개념을 새롭게 도입함으로써 스마트계약을 구현하였으며 궁극적으로 중앙화된 중개인 없이도 거래 상대방에 대한 신뢰 부족 문제를 해결하였다. DeFi는 이러한 기술들을 바탕으로 하여 2017년 본격적으로 시작되었으며 최근 2년 동안 가파른 성장 추세를 보이고 있다.

DeFi는 기존 금융시스템과 근본적으로 다르다. 예를 들면 물리적 실체 없이 블록체인 네트워크상에서 운영되기 때문에 서비스 제공자는 직원을 고용하거나 전산 설비를 갖추지 않고도 프로그래밍 코드를 개발 · 배포하는 것만으로 금융서비스를 구현할 수 있으며, 사용자는 기존 중앙화된 중개인에게 지급하였던 막대한 비용을 절감할 수 있다. 그러나 다른 한편으로 DeFi에는 여전히 풀어야 할 숙제가 많다. DeFi의 안정성과 영속성에 대해 많은 이들이 아직 우려를 표하고 있으며, 실제로도 DeFi는 가상자산 투자를 보조하는 역할 외 금융의 다른 중요한 기능들을 거의 수행하지 못하고 있다. 결국 DeFi는 중앙화된 중개인의 역할이 중요하지 않은 비교적 간단한 영역에서 사용자에게 새로운 옵션을 제공하는 정도의 제한적 역할을 당분간 수행할 전망이다. 향후 그 영역을 확장하는 과정에서 다양한 기술적 도전과 시장 불확실성에 맞닥뜨리게 될 것이며 새로운 금융 형태로서의 가능성을 시험받게 될 것이다.

---

* 본고의 견해와 주장은 필자 개인의 것이며, 자본시장연구원의 공식적인 견해가 아님을 밝힙니다.
펀드연금실 연구위원 권민경 (mkkwon@kcmi.re.kr)

Ⅰ. 논의 배경

최근 DeFi라는 용어가 새롭게 등장하여 주목을 받고 있다. DeFi는 탈중앙화된 금융(Decentralized Finance)의 약자로 블록체인 네트워크상에서 은행, 증권사, 보험사 등 중앙화(centralized)된 중개인을 거치지 않고 스마트계약(smart contract)을 통해 구현된 탈중앙화 금융서비스를 의미한다. 넓은 의미에서 핀테크의 일종으로 볼 수 있지만, 일각에서는 DeFi를 기존 핀테크 서비스들과 차별화된 새로운 개념으로 소개하기도 한다. 다시 말해, 기존 핀테크 서비스들이 전통적인 금융산업과 비교하여 새로운 서비스를 창출하기보다는 IT기술을 이용해 이미 존재하는 서비스의 고객 경험 및 접근성을 제고하는 데 초점을 맞춘 반면, DeFi는 중앙화된 중개인에 대한 의존을 없앰으로써 전에 없던 완전히 새로운 형태의 서비스를 제공할 수 있다는 주장이다.

DeFi에 대해 논의하기 위해서는 우선 기반기술인 블록체인과 스마트계약의 개념을 이해하는 것이 필요하다. 블록체인의 원리에 대해서는 권민경 · 조성훈(2018)을 비롯한 각종 문헌과 언론에서 이미 많이 다루었으니 본고에서는 생략하도록 한다. 그러나 스마트계약은 아직 많은 이들에게 생소하여 익숙한 개념이 아니기 때문에 그 원리를 간단히 소개하겠다. 그다음에는 본격적으로 DeFi의 개념 및 현황을 살펴보고 예시를 통해 세부적인 알고리즘을 설명한다. 마지막으로 기존 금융서비스와 비교하여 DeFi가 지니는 차별성은 무엇인지, 그리고 어떠한 한계를 가지는지 각각 살펴보고 궁극적으로 새로운 형태의 금융으로서 DeFi의 가능성을 진단하도록 한다.

Ⅱ. 스마트계약의 이해

블록체인 기술은 사토시 나카모토(Satoshi Nakamoto)라는 가명의 프로그래머가 2008년 비트코인을 개발하면서 처음으로 탄생하였다. 이후 비트코인과 유사한 형태를 지닌 다양한 블록체인 네트워크들이 출현했으나, 그중에서 가장 돋보였던 것은 2013년 비탈릭 부테린(Vitalik Buterin)이 개발한 이더리움이다. 기존의 비트코인이 가치의 저장과 전달이라는 전자화폐의 기능을 주로 추구하였다면, 이더리움은 여기에 더해 스마트계약 기능을 탑재하여 블록체인 기술의 전반적인 활용도를 크게 향상시켰다. 비탈릭 부테린의 이러한 시도는 블록체인

기술의 진일보에 크게 기여한 것으로 널리 인정받고 있으며 이더리움과 같이 스마트계약을 탑재한 네트워크를 통상 블록체인 2세대라고 부르며 기존의 네트워크들과 구분하고 있다.[01]

사실 스마트계약은 블록체인이 개발되기 전에 이미 존재했던 개념으로 1994년에 닉 재보(Nick Szabo)가 처음 고안한 것으로 알려져 있다. Szabo(1994)에 따르면 스마트계약은 '계약의 조항들이 전산으로 프로그래밍 되어 자동으로 실행되는 것'을 의미한다.[02] 사전에 작성된 프로그래밍 코드가 기계적으로 계약을 검증하고 실행하기 때문에 별도의 중앙화된 중개인을 필요로 하지 않는다는 점이 스마트계약의 가장 큰 강점이다. 스마트계약이 현실에서 효과적으로 구현될 수 있다면 그동안 중개인에 크게 의존했던 여러 산업에서 커다란 파급을 일으킬 것이며 특히 가능성이 큰 대표적인 분야가 바로 금융이다. 대부분의 금융 거래에서 계약 상대방에 대한 신뢰 부족 문제로 인해 금융기관이 중개인 역할을 주로 맡아왔는데, 스마트계약을 활용하면 금융기관의 중개 없이도 거래가 가능해지기 때문이다.

그러면 이제부터 이더리움의 사례를 통해 스마트계약의 원리를 살펴보도록 하자. 우선 우리가 익숙한 기존의 금융시스템을 떠올려보자. 우리는 통상 금융서비스를 받기 위해 본인 명의의 '계좌(account)'를 개설하고 다른 계좌와 '거래(transaction)'를 수행한다. 예를 들면 본인 계좌 A에서 타인 계좌 B로 100만원을 이체 거래할 것을 금융기관에 요청할 수 있다. 이처럼 이더리움 네트워크에서도 '계좌'와 '거래'의 개념이 존재하며 이들은 스마트계약 기능 구현에 있어 핵심 역할을 수행한다. 단, 새로운 유형의 '계좌'와 '거래'가 추가로 도입되었다는 점에서 기존 금융시스템과 차이를 보인다.

이더리움 네트워크에서 계좌의 유형은 크게 두 가지로 구분된다. 하나는 사용자들이 이더(Ether)[03]를 보유하고 있는 일반적인 계좌이며 이를 사용자 보유계좌(Externally Owned Account: EOA)라고 부른다. 또 다른 하나는 스마트계약 기능을 위해 특별히 고안된 것으로 이더뿐 아니라 프로그래밍 코드 및 저장소(storage)를 포함하고 있다. 이를 계약계좌(Contract Account: CA)라 칭한다. 이처럼 계좌의 유형이 두가지로 늘어남에 따라 계좌 간 거래의 유형은 <표 II-1>에서와 같이 총 네 가지로 구분할 수 있다. 'EOA→EOA', 'EOA→CA', 'CA→EOA', 'CA→CA'가 바로 그것이다.

---

01 혹자는 여기에서 더 나아가 비트코인·이더리움 등 기존 블록체인 네트워크들이 겪고 있는 확장성(scalability), 상호운용성(interoperability) 문제 등을 해결하기 위해 새롭게 등장한 Cardano, Polkadot 등을 블록체인 3세대로 칭하기도 한다.

02 원문의 표현은 "a computerized transaction protocol that executes the terms of a contract"다.

03 이더리움의 거래 단위를 이더라 부른다.

<표 Ⅱ-1> 거래유형 구분

	From EOA (사용자의 거래 지시)	From CA (② 또는 ④에서 프로그래밍 코드 실행 결과로 인한 거래)
To EOA (단순 이체)	① EOA→EOA	③ CA→EOA
To CA (프로그래밍 코드 실행)	② EOA→CA	④ CA→CA

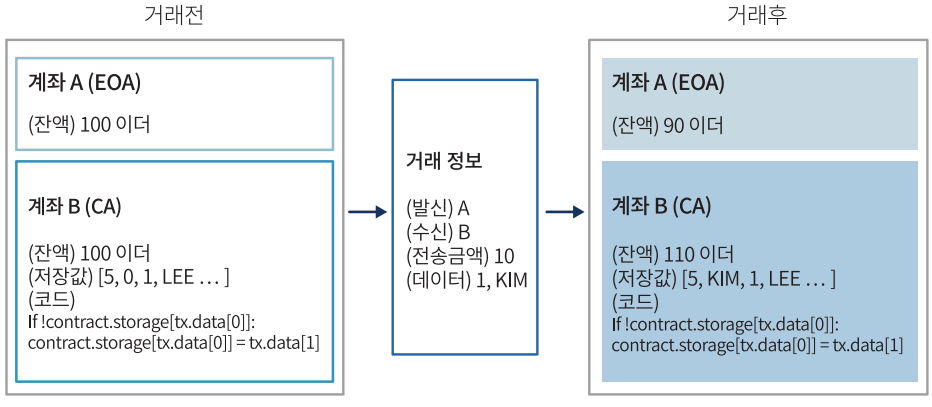
첫 번째 거래유형인 EOA→EOA는 기존의 금융시스템에서 일상적으로 나타나는 거래와 같은 방식으로 작동한다. 예를 들면 어떠한 사용자가 본인 계좌 A에서 타인 계좌 B로 10이더를 단순 이체하는 식이다. 이와 달리 두 번째 거래유형인 EOA→CA는 스마트계약과 직접 관련이 있는데, 사용자가 CA에 담겨 있는 프로그래밍 코드를 실행시키는 작용을 한다. 코드 실행의 결과로 CA 내 저장값이 업데이트될 수 있으며, 경우에 따라서는 CA가 새로운 거래를 추가로 일으켜 세 번째 유형(CA→EOA) 또는 네 번째 유형(CA→CA)의 거래를 생성하기도 한다.[04] 만약 EOA→CA의 거래가 새로운 CA→CA의 거래를 추가로 생성할 경우 새로운 거래의 수신계좌인 CA에 담겨 있는 프로그래밍 코드가 연달아 실행되며 이는 또다시 새로운 CA→EOA 또는 CA→CA 거래를 연쇄적으로 발생시킬 수 있다.

이더리움 네트워크에서 거래 정보가 포함하는 항목(item) 또한 기존 금융시스템의 그것과 조금 다르다. 기존 금융시스템에서 거래 정보의 핵심 항목은 '발신계좌', '수신계좌', '전송금액'이지만, 이더리움 네트워크에서는 여기에 더해 '데이터'라는 항목이 새롭게 추가된다. 앞에서 본 것처럼 거래가 단순히 이더의 전송뿐 아니라 CA가 내포한 프로그래밍 코드를 작동시키는 역할 또한 수행하기 때문에, '데이터' 항목을 추가함으로써 이를 프로그래밍 코드의 입력값(input)으로 활용할 수 있도록 설계한 것이다.[05] <그림 Ⅱ-1>의 예시를 살펴보면 거래의 결과로 계좌 B의 코드가 실행되며 이때 거래 정보에 포함된 '데이터'를 활용하여 저장값이 업데이트되는 모습을 확인할 수 있다.

04 모든 스마트계약의 실행은 EOA→CA의 거래로부터 시작된다. 즉, CA는 독자적으로 새로운 거래를 생성하지 못하며 CA→EOA 또는 CA→CA의 거래는 반드시 EOA→CA 거래의 결과로서만 발생할 수 있다.

05 사실 '데이터' 외에도 이더리움의 거래 정보에 포함된 추가 항목들은 더욱 많다. 그러나 스마트계약의 핵심 개념만 쉽고 간결하게 설명하고자 하는 본고의 목적에 따라 자세한 언급은 생략한다.

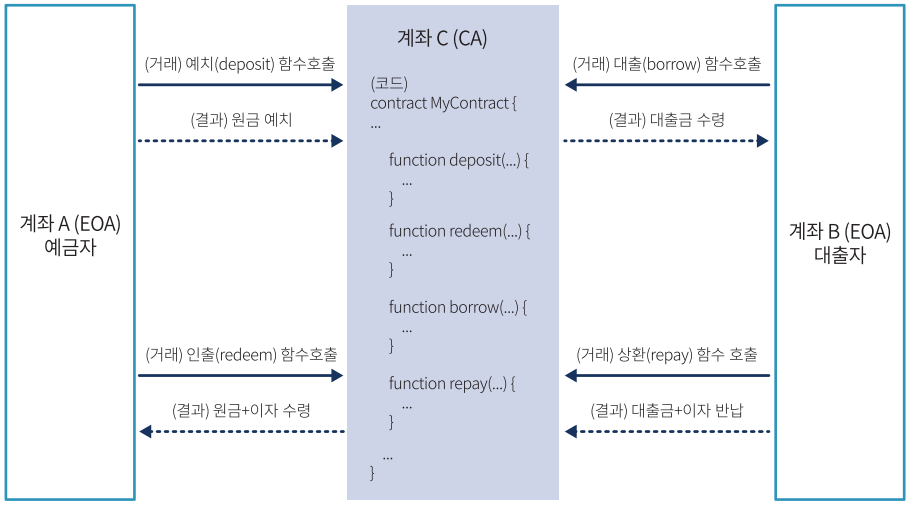
<그림 Ⅱ-1> 이더리움 네트워크에서의 거래 예시



주: 이더리움 백서 상의 도표를 단순화하여 재작성함

그렇다면 스마트계약 기능을 활용하여 어떻게 금융서비스를 구현할 수 있을까? 은행의 예금-대출 서비스를 예시로 들어보자. 예금 서비스의 핵심 기능은 크게 '예치'와 '인출'로 구분할 수 있다. 사용자는 '예치'를 통해 돈을 맡겨두었다가 '인출'을 통해 그동안의 이자와 함께 원금을 수령한다. 한편, 대출 서비스의 핵심 기능은 '대출'과 '상환'이다. 사용자는 '대출'을 통해 돈을 빌렸다가 '상환'을 통해 그동안의 이자와 함께 원금을 갚는다. 스마트계약에서는 개발자들이 '예치', '인출', '대출', '상환' 함수(function)를 각각 프로그래밍 코드로 작성한 다음 이를 담은 CA를 생성하는 방식으로 서비스가 구현된다. 그리고 사용자들은 본인의 EOA에서 해당 CA로의 거래를 요청하면서 본인에게 필요한 함수를 호출(call)함으로써 해당 서비스를 이용할 수 있다.

<그림 Ⅱ-2> 스마트계약 기능 예시 – 예금 및 대출 서비스 구조



'예치', '인출', '대출', '상환' 등 각 함수 안에는 <표 Ⅱ-2>에서 보듯 서비스가 원활하게 작동할 수 있도록 하는 세부 알고리즘들이 탑재된다. 예를 들어 '대출' 함수가 호출되었을 경우 CA는 사전에 정한 공식에 따라 사용자의 대출한도를 산정하고 만약 대출이 가능하다면 사용자 EOA로의 거래를 생성하여 대출금액을 전송해야 한다. 또한 CA 저장소에 개별 사용자의 잔고와 CA 내 총 잔고를 업데이트하고, 대출금액이 늘어난 상황을 반영하여 미리 정한 공식에 따라 이자율을 재산정할 필요가 있다. 이러한 세부 알고리즘들은 개발자들에 의해 각 함수 안에 프로그래밍 코드 형태로 작성되어 CA가 생성될 때 함께 저장된다.

기존 금융시스템에서 은행마다 또는 개별 상품마다 금리 산정 방식과 서비스 방식이 각각 상이하듯 실제 스마트계약을 적용하여 구현된 예금-대출 서비스들도 '예치', '인출', '대출', '상환' 등 기본적인 함수의 형태는 같지만 그 안에 탑재되는 세부 알고리즘들은 모두 제각각이다. 예를 들면 대출자의 대출한도 및 이자율을 결정하는 공식은 서비스마다 완전히 상이할 수 있다. 이러한 알고리즘들은 사전에 결정되어 CA의 프로그래밍 코드에 포함되어 있으며 누구에게나 투명하게 공개되어 있다. 따라서 은행에서 상품 가입 전 계약조건 및 약관을 검토하듯 사용자들은 스마트계약을 활용한 서비스의 세부 알고리즘을 미리 파악한 다음 본인의 참여 여부를 결정할 수 있다.[06]

<표 Ⅱ-2> 스마트계약 기능 예시 – 예금 및 대출 서비스의 세부 알고리즘

함수명	기능	세부 알고리즘
deposit( )	예치	① 개별 사용자 잔고 및 총 잔고 업데이트 ② 이자율 재산정
redeem( )	인출	① 인출 한도 산정 및 인출 가능 여부 체크 ② 예금금리를 복리로 계산하여 이자 금액 산출 ③ 원금 및 이자를 EOA로 전송 ④ 개별 사용자 잔고 및 총 잔고 업데이트 ⑤ 이자율 재산정
borrow( )	대출	① 대출한도 산정 및 대출 가능 여부 체크 ② 대출금을 EOA로 전송 ③ 개별 사용자 잔고 및 총 잔고 업데이트 ④ 이자율 재산정
repay( )	상환	① 대출금리를 복리로 계산하여 이자 금액 산출 ② 개별 사용자 잔고 및 총 잔고 업데이트 ③ 이자율 재산정

06 프로그래밍 코드에 익숙지 않은 사용자들을 위해 스마트계약을 활용한 서비스 대부분은 웹사이트 등을 통해 일상적인 언어로 그들의 알고리즘을 설명하고 있다.

다시 정리하면 스마트계약에서 개발자와 사용자의 역할은 <표 II-3>과 같다. 개발자들은 새로운 서비스를 구상하여 개별 함수들과 그 안에 담길 세부 알고리즘들을 프로그래밍 코드로 작성하고 이를 담은 CA를 이더리움 네트워크상에 생성한다. 사용자들은 개별 CA들의 세부 알고리즘을 검토하여 본인에게 가장 적합한 서비스를 결정한 다음 본인의 EOA로부터 해당 CA로의 거래를 지시하여 서비스받고자 하는 함수를 호출한다. 이 두 가지 역할이 모두 수행되면 비로소 블록체인 네트워크상에서 스마트계약을 활용한 서비스가 작동하게 된다.

<표 II-3> 스마트계약에서 개발자와 사용자의 역할

개발자		CA		사용자
① 새로운 서비스를 구상 ② 서비스의 세부 알고리즘을 프로그래밍 코드로 작성 ③ 이를 담은 CA를 블록체인 네트워크상에 생성	⇨	사전에 정해진 알고리즘을 그대로 이행 (autonomous agency)	⇦	① 개별 CA들의 세부 알고리즘을 검토하여 본인에게 적합한 서비스 선택 ② 본인의 EOA로부터 해당 CA로의 거래를 지시하여 원하는 함수를 호출

이제 중앙화된 중개인이 있는 전통적인 금융시스템과 스마트계약을 활용한 새로운 금융시스템을 서로 비교해보자. 전통적인 금융서비스는 금융기관이 고객과 사전에 합의한 조항들을 앞으로도 온전히 이행할 것이라는 믿음을 전제로 작동한다. 만약 고객에게 그러한 신뢰를 줄 수 없다면 해당 금융기관은 영업할 수 없을 것이다. 따라서 금융기관은 철저한 위험관리와 충분한 자금 조달을 통해 재정 건전성을 확보하고 인력과 설비 등에 대규모로 투자하여 평판을 높이는 등 고객 신뢰를 유지하기 위해 필사적으로 노력한다. 반면, 스마트계약에서는 블록체인 네트워크가 유지되는 한 프로그래밍 코드로 이루어진 알고리즘이 사전에 정해진 대로 한 치의 오차 없이 이행되기 때문에 신뢰의 문제가 발생하지 않는다. 설령 서비스 제공자가 대규모 자본, 다수의 직원과 사무실, 고도화된 전산 설비 등을 갖추지 않았더라도 네트워크가 정상적으로 작동한다면 사용자는 스마트계약을 통해 항상 정해진 서비스를 받게 될 것이다. 스마트계약은 신뢰 문제를 해결함으로써 중앙화된 중개인의 필요성을 제거하였으며 대신 프로그래밍 코드를 담고 있는 CA가 이와 유사한 역할을 수행한다. CA가 자율 중개인(autonomous agency)이라고 불리는 이유가 바로 여기에 있다.

III. DeFi의 현황 및 작동방식

DeFi는 2017년 MakerDAO가 이더리움 네트워크를 기반으로 스마트계약을 이용한 예금-대출 서비스를 성공적으로 출시하면서 본격 시작되었다.[07] 이후 Compound, Aave 등도 두각을 드러내며 예금-대출 분야에서 대표적인 DeFi 서비스로 자리를 잡았으며, 탈중앙화 거래소(Decentralized Exchange: DEX) 분야에서는 Uniswap, 자산운용 분야에서는 yearn.finance, 파생상품 분야에서는 Synthetix, 보험 분야에서는 Nexus Mutual 등이 안착하면서 DeFi의 영역이 점차 확장되고 있다. 이들은 주로 이더리움 네트워크를 기반으로 서비스를 제공하여 왔으나 최근에는 Binance Smart Chain, Polygon, Polkadot 등 다른 블록체인 네트워크로도 저변을 넓혀 나가고 있다.

DeFi의 현황을 보여주는 객관적이면서 공신력 있는 통계는 아직 존재하지 않는다. DeFi의 정의와 분류, 지표, 집계방식 등이 통일되지 않고 모두 제각각이기 때문이다. 그럼에도 불구하고 다음의 자료들을 통해 대략적인 윤곽은 살펴볼 수 있다. 우선 DEFI PULSE에 따르면 DeFi에 예치된 총 자산규모는 현재 109조원 수준이다.[08] 글로벌 DeFi의 예치금액 합계가 국내은행의 원화 저축성예금 합계(1,504조원)[09]에 비해 7% 수준이라는 사실에 비추어볼 때 기존 금융시스템에 비하면 아직 그 규모가 극히 미미하다는 사실을 확인할 수 있다. DeFi의 현황을 살펴볼 수 있는 또 다른 지표로 개별 DeFi들이 자체적으로 발행하고 있는 토큰의 가치총액을 꼽을 수 있다. 이들 토큰은 해당 DeFi의 사용자가 많아지고 거래량이 늘어날수록 가치 상승의 수혜를 입을 수 있다는 측면에서 은행 등 금융기관의 주식과 유사한 성격을 가진다. CoinMarketCap에 따르면 Uniswap(18.3조원), Aave(4.7조원), MakerDAO(2.9조원), Compound(2.0조원) 등 예치금액 상위 10여 개의 토큰 가치총액은 33조원 수준을 나타내고 있다. 반면, 카카오뱅크(27.6조원), KB금융(22.5조원), 신한지주(20.3조원) 등 국내 주요 은행 9개 사의 시가총액 합계는 106조원을 기록하여 주요 DeFi 토큰 가치총액의 3배를 상회하였다.[10] 글로벌 대표 DeFi들의 가치총액이 국내은행 시가총액에도 크게 미치지 못한다는 점은 이들의 규모가 기존 금융시스템이 비해 아직 미미하다는 점을 다시 한번 보여준다.

07 한국은행(2021) 참조

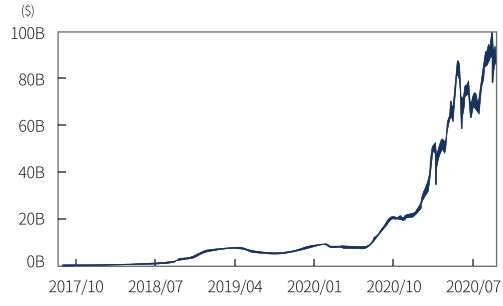
08 DEFI PULSE는 개별 DeFi들로부터 주기적으로 예치금액을 보고받아 이를 웹사이트에 공개하고 있다. 여기에서 '예치금액'은 개별 DeFi의 CA에 보관된 가상자산들을 해당 시점의 달러 가치로 합산한 값이다. 본문의 값은 2021년 10월 6일 15시를 기준으로 집계되었다.

09 은행연합회에서 2021년 6월말을 기준으로 집계한 값이다.

10 토큰의 가치총액은 2021년 10월 6일 16시를 기준으로, 주식의 시가총액은 같은 날 종가를 기준으로 작성되었다.

그럼에도 불구하고 DeFi의 폭발적인 성장세는 주목할 만하다. <그림 III-1>에서 보듯 DeFi의 예치금액 합계는 2019년말과 비교하여 최근 21개월 동안 11배가량 증가하였다. 2020년말과 비교해서도 최근 9개월 동안 4배가량 급증하였다. 물론 해당 기간 동안 이더리움을 비롯한 주요 가상자산의 달러 환산 가치가 크게 늘어난 것이 동 결과에 상당한 영향을 미쳤을 가능성을 배제하기는 어렵다. 그럼에도 불구하고 여전히 DeFi의 성장세를 무시하기는 어렵다는 평가가 일반적이다. 일례로 DEFI PULSE에서는 가상자산 중 유일하게 이더리움에 대해서 예치자산의 달러 환산 가치가 아닌 수량 정보를 공개하고 있는데 이를 살펴보면 2019년말과 비교하여 현재 이더리움의 예치 수량이 12배가량 늘었고, 2020년말과 비교하여도 1.6배 정도 늘었다.

<그림 III-1> DeFi의 예치자산 규모 추이



자료: DEFI PULSE

다음으로 DeFi 서비스의 작동방식을 실제 사례를 통해 파악해보자. 여기에서는 예금-대출 서비스 분야의 대표 DeFi 중 하나인 Compound를 예시로 들겠다. 앞서 <그림 II-2>에서 기존 은행의 예금-대출 서비스를 스마트계약으로 구현하는 방법을 간단히 묘사하였지만, 이는 반드시 존재해야 하는 최소한의 기능만을 제시한 것이며 실제 DeFi들은 이보다 더욱 많은 기능을 필요로 한다. 그 이유는 다음과 같다. 첫째, 현재 DeFi들은 대부분 신용대출이 아닌 담보대출의 형태로 서비스가 이루어지고 있어 담보의 설정, 관리, 청산 등의 기능을 추가로 필요로 한다. 중앙화된 중개인이 없는 DeFi에서는 신용대출을 구현하기가 매우 까다로우므로 <그림 II-2>와 같이 단순한 기능만 갖춘 DeFi 서비스는 아직 존재하지 않는다. 둘째, DeFi가 작동하기 위해서는 사용자 참여를 유도하는 인센티브 체계가 대부분 필요하므로 해당 기능을 추가로 구현해야 한다. 이를테면 담보대출의 경우 기존 은행에서는 담보비율 하락 시 대출자에게 새로운 담보를 요청하거나 여의치 않으면 은행 스스로 기존 담보를 시장에 판매하여 대출을 변제할 수 있다. 그러나 DeFi에서는 사용자의 거래요청이 없으면 DeFi가 스스로 이러한 역할을 수행할 수가 없다. II 장에서 설명한 대로 CA의 프로그래밍 코드가 작동하려면 일단 사용자의 EOA로부터 CA로의

거래가 선행되어야 하기 때문이다. 즉, 담보비율 하락 시에도 DeFi가 스스로 담보물을 청산할 수 없으므로 외부 사용자로 하여금 담보를 대신 청산하도록 유도할 필요가 있으며 이를 위해 청산자에게 인센티브를 제공하는 기능을 구현해야 한다.

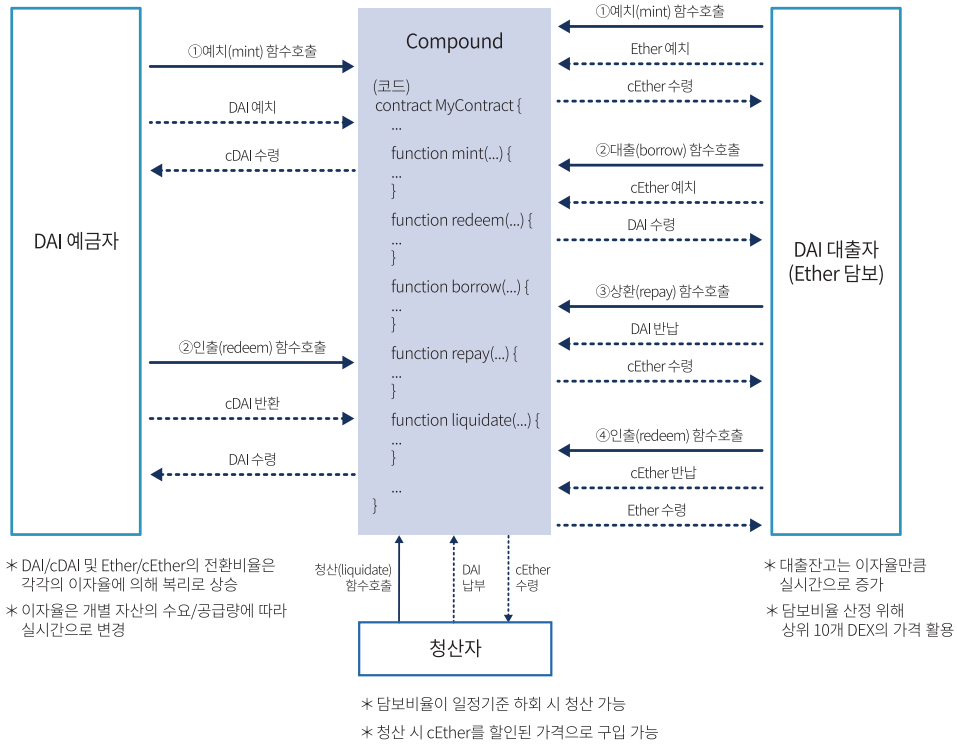
사용자가 Compound에서 스테이블 코인(stable coin)[11]의 일종인 DAI에 대해 예금-대출 서비스를 받을 때 실제로 서비스가 작동하는 방식을 <그림 III-2>에서 확인할 수 있다. 우선 예금자의 경우 예치(mint) 함수를 통해 DAI를 예치할 수 있으며 이때 Compound로부터 동일한 가치만큼의 cDAI를 수령한다. 이후 인출(redeem) 함수를 통해 cDAI를 다시 반환할 수 있으며 그 대가로 DAI를 다시 수령하게 된다. 여기에서 cDAI는 Compound에서 자체적으로 발행하는 토큰으로 일종의 예치증서라고 볼 수 있다. cDAI의 가치는 Compound에서 DAI에 책정한 실시간 이자율만큼 복리로 상승한다.[12] 예를 들어 1 cDAI = 0.1 DAI일 때 100 DAI를 예치하면 1,000 cDAI를 수령할 수 있는데, 만약 1년 뒤에 1 cDAI = 0.105 DAI로 변하였다면 1,000 cDAI를 반납할 시 그 대가로 105 DAI를 수령할 수 있다. cDAI의 가격 상승분만큼 예금자는 이자 수익(5 DAI)을 얻을 수 있는 것이다. 한편, 대출자의 경우 우선 예치 함수를 통해 담보로 맡길 자산을 예치해야 한다. 예를 들어 Ether를 담보자산으로 맡기고자 한다면 먼저 예치 함수를 통해 Ether를 예치하고 cEther를 수령해야 한다. 그다음 대출(borrow) 함수를 호출하여 cEther를 담보로 맡기고 DAI를 빌릴 수 있다. 추후 상환(repay) 함수를 통해 DAI를 이자와 함께 모두 반납하면 담보로 맡겼던 cEther를 돌려받을 수 있다. 마지막으로 인출 함수를 통해 cEther를 반납하면 Ether를 그동안의 이자와 함께 수령하게 된다.

앞서 언급한 대로 일반적인 은행과 달리 Compound에는 예금자와 대출자 외에도 청산자 역할이 별도로 존재한다. 청산자는 담보비율이 일정 수준 이하로 하락한 대출에 대해 담보물을 할인된 가격에 취득할 기회를 얻는다. <그림 III-2>의 경우 청산자는 청산(liquidate) 함수를 통해 대출자를 대신하여 DAI를 변제하고 그 대가로 담보물인 cEther를 저렴하게 취득할 수 있다. 이더리움 네트워크상에서 어떠한 사용자라도 청산자가 될 수 있으므로 대출자의 담보비율 하락 시 사용자들은 경쟁적으로 청산 절차를 통해 수익을 올리고자 할 것이다. 이처럼 Compound는 스스로 수행할 수 없는 청산 기능을 외부의 사용자들이 대신 수행하게끔 인센티브 시스템을 구축하여 운영하고 있다.

11 특정 법화(fiat money)와 동일한 가치를 갖도록 설계된 코인을 의미한다.

12 정확히 표현하면 Compound의 자체 알고리즘에 따라 DAI/cDAI의 전환비율이 실시간 이자율을 반영하여 지속 상승한다.

<그림 III-2> Compound 예금-대출 서비스의 구현 사례



주: Leshner & Hayes(2019)의 내용을 그림으로 정리

예금-대출 서비스의 이자율은 개별 자산의 수요-공급량에 따라 실시간으로 변화하며 이를 결정하는 공식은 사전에 프로그래밍 코드로 작성되어 Compound 알고리즘에 포함되어 있다. 그리고 동 알고리즘은 Compound의 서비스가 중단되지 않고 지속해서 운영되는 데 있어 핵심 역할을 수행한다. 만약 DAI의 예금이 늘고 대출이 줄어든다면 알고리즘에 의해 이자율은 곧장 하락할 것이고, 반대로 예금이 줄고 대출이 늘어난다면 이자율은 상승할 것이다. 실시간으로 변하는 이자율은 예금자와 대출자의 행동에 즉각 영향을 미치므로 해당 자산의 예대율(loan-deposit ratio)을 일정하게 유지하는 데 도움을 준다. 만약 DAI의 예금 인출이 크게 늘어 잔고가 급격히 줄어드는 상황이 발생하더라도 알고리즘에 따라 이자율이 급등할 것이며 기존의 대출자들은 높아진 이자 부담을 피하고자 서둘러 대출을 갚으려 할 것이다.[13] 이러한 과정을 통해 궁극적으로 DAI 잔고는 다시 회복되고 이후에는 이자율 또한 다시 정상화될 가능성이 크다.

13 Compound를 비롯하여 통상 DeFi에는 예금자와 대출자 모두 정해진 약정기한이 없으므로 이들은 언제든 원하는 시기에 예치금을 인출하거나 대출금을 상환할 수 있다. 예를 들어 원래 2%였던 이자율이 10%로 급등한다면 대출자들은 이전보다 원금 상환 일정을 앞당기려 할 것이다.

이상에서 살펴보았듯 개별 DeFi들은 기존의 중앙화된 중개인의 역할 없이도 금융서비스를 온전히 구현하기 위해서 상당한 노력을 기울이고 있다. 특히, 기존 금융시스템에서는 존재하지 않았던 새로운 알고리즘들을 계속해서 고안해나가고 있으며 이는 예금-대출 외에도 탈중앙화 거래소, 자산운용, 파생상품, 보험 등 DeFi의 다른 분야에서도 공통으로 나타나는 현상이다. 현재의 초기 단계에서 DeFi 알고리즘들은 중앙화된 중개인의 역할을 대체하기 위해 어쩔 수 없이 도입된 측면이 크며, 냉정하게 평가하였을 때 이들이 기존 금융시스템과 비교하여 그다지 효율적이지는 않아 보이는 것이 사실이다. 그러나 개발자 커뮤니티를 중심으로 현재 발생하는 문제들을 해결하기 위해 활발한 논의들이 이루어지고 있으며 실제로도 창의적인 아이디어들이 새롭게 등장하고 속속 채택되면서 단점을 신속하게 보완해나가고 있다.

IV. 새로운 금융 형태로서의 가능성

이번 장에서는 DeFi가 기존 금융시스템과 비교하여 어떠한 차별성을 지니고 있는지 그리고 DeFi의 한계점은 무엇인지에 대해 각각 살펴보자 한다. 우선 블록체인과 스마트계약 등 기반기술로부터 유래하는 DeFi의 특징을 논의하고, 다음으로 현재 운영 중인 주요 DeFi 알고리즘의 공통된 특징을 살펴볼 것이다. 전자는 기반기술에 종속되어 개별 DeFi들이 쉽게 바꿀 수 없는 태생적 특징이고[14], 후자는 앞으로의 상황에 따라 개별 DeFi들이 비교적 쉽게 개선해나갈 수 있는 경험적 특징이라고 볼 수 있다. 이러한 분석을 통해 최종적으로는 새로운 금융 형태로서 DeFi의 가능성을 진단해 보고자 한다.

1. 기반기술에 기인하는 DeFi의 특징

블록체인과 스마트계약 등 기반기술로부터 유래하는 DeFi의 차별성은 다음과 같다. 첫째, 블록체인 네트워크상에서 일어나는 모든 거래가 그러하듯 DeFi 역시 언제 어디서든 누구나 간편하게 접근할 수 있다는 장점을 가진다. 블록체인 네트워크는 365일 24시간 쉬지 않고 운영되며 기존 금융기관과는 다르게 업무 종료 시각이 따로 존재하지 않는다. 또한 인터넷만 접속할 수 있으면 누구든지 DeFi 서비스를 이용할 수 있다. 특히 기존 금융시스템에 대해 국민

14 물론 블록체인과 스마트계약 등 기반기술 자체도 계속 진화하기 때문에 앞으로 변화할 가능성이 전혀 없는 것은 아니다.

상당수의 접근성이 떨어지는 일부 개발도상국의 경우 DeFi가 그 대안으로 역할을 수행할 수 있다는 주장도 있다.[15] 그리고 대부분의 DeFi 서비스는 별도의 가입 절차가 필요 없다. 현재 DeFi에는 Know-Your-Customer(KYC) 등 별도의 인증 절차가 없으며 설명의무와 같이 판매와 관련된 규제 등이 적용되지 않아 기존 금융시스템과 비교하여 사용자 관점에서 서비스 활용이 간편하다.[16]

둘째, 스마트계약은 금융서비스 제공자의 진입요건을 현격히 낮춘다. 기존에는 금융서비스 제공자가 되기 위해 상당한 수준의 물적 · 인적 요이 필요하였다. 예를 들어 은행을 설립하기 위해서는 서버, 저장장치, 보안설비 등 물리적 요건을 충족해야 함은 물론이고 이에 대한 유지보수, 모니터링, 내부통제 체계를 갖추어야 하며, 인건비와 전기, 통신, 보험의 비용 등을 지속해서 부담해야 한다. 그러나 DeFi는 이러한 것들을 전혀 요구하지 않는다. 서비스 내용을 프로그래밍 코드로 작성하고 이를 담은 CA를 생성하기만 하면 이후 서비스의 운영은 블록체인 네트워크가 전담하여 수행한다. 물리적인 설비도 필요 없고 유지비용도 전혀 들지 않는다. DeFi는 또한 공간, 시차, 언어, 규제, 자본금 등의 제약으로부터 자유로워 글로벌 서비스 구현에도 훨씬 용이하다.

셋째, 스마트계약의 활용은 사용자가 기존 중앙화된 중개인에게 지급하는 비용을 크게 절감하는 효과를 낳는다. 기존의 중앙화된 중개인은 다수의 사무실 또는 지점을 운영하고 설비를 유지하며 인력을 고용하기 위해 많은 비용을 지출하고 있다. 그리고 이를 충당하기 위해 고객에게 상당한 비용을 청구한다. 그러나 스마트계약을 활용하면 중앙화된 중개인 없이도 금융서비스가 가능하므로 DeFi 사용자는 이러한 비용을 전혀 부담할 필요가 없다. 대신 사용자는 블록체인 네트워크상에서 블록을 검증 · 생성하는 주체에게 네트워크 사용 대가를 지급하면 되는데 소액 거래를 제외하고 일반적인 거래의 경우 사용자의 비용 부담은 기존 금융시스템 대비 현격히 작은 편이다.[17]

넷째, 스마트계약은 오픈소스(open source)[18]를 기반으로 하고 있어 개별 DeFi 간 상호 연결과 조합이 자유롭다. 기존 금융시스템에서는 금융회사 간 이해관계로 인하여 상호 협력이 잘 일어나지

15 한국은행(2021)에 따르면 전세계에서 금융 혜택을 받지 못하는 비금융계좌인구는 2019년 기준 약 17억명에 달한다고 한다.

16 물론 이에 따른 부작용으로 자금세탁, 탈세 등의 위법행위 및 소비자 보호 관련 다양한 문제들이 발생할 수 있으며 각국 정부에서는 이에 대한 대응책을 고심하고 있다.

17 네트워크 이용 비용은 거래금액이 아닌 네트워크 이용량에 비례하여 책정되기 때문에 소액 거래의 경우 다소 불리한 측면이 있다.

18 오픈소스란 개발자가 소프트웨어를 개발 및 배포할 때 해당 소프트웨어가 어떻게 작동하는지 누구나 알 수 있도록 소스 코드나 설계도 등을 공개하는 것을 의미한다.

않았으며 이에 따라 금융서비스 간 시너지가 매우 제한적이었다. 그러나 DeFi에서는 통상 프로그래밍코드 및 저장 데이터가 투명하게 공개되어 있어, 새로운 서비스의 개발자는 별도의 동의를 구하지 않고서도 다른 DeFi 서비스의 프로그래밍 코드를 응용하여 사용할 수 있으며 더 나아가 이들을 하위 도구로 사용하여 새로운 융합 서비스를 구현하는 것도 가능하다. 머니 레고(Money Lego)라고 불리는 이러한 특징은 레고블록을 쌓듯 다수의 DeFi 서비스들을 자유롭게 연결하고 조합함으로써 전체 DeFi의 영역이 점점 거대화되고 확장되는 것을 의미한다. 예를 들면 1inch라는 DeFi 서비스는 Uniswap, Sushiswap 등 주요 탈중앙화 거래소의 가상자산 가격을 각각 추출하고 이를 비교하여 사용자가 현시점에서 가장 좋은 가격으로 가상자산을 매매할 수 있도록 돕는다. 또한 yearn.finance는 Compound, Aave 등 예금-대출 서비스를 제공하는 주요DeFi들의 이자율을 비교하여 가장 금리가 높은 DeFi 서비스에 사용자의 가상자산을 예치하며, 한 번 예치한 후에도 DeFi들의 금리가 변동하면 실시간으로 최고 금리를 제공하는 곳을 찾아자동으로 가상자산을 옮겨 예치하는 서비스를 제공한다. 또 다른 사례로 DAI는 원래 MakerDAO의 예금-대출 서비스 수단으로 고안된 토큰이지만, 현재는 Compound, Aave 등 다수의 DeFi들이 이를 자체 서비스의 핵심 자산으로 활용하고 있다. 이러한 머니 레고 효과로 인해 사용자들은 여러 DeFi 서비스들이 마치 하나의 거대한 금융회사가 제공하는 서비스인 양 제약 없이 유기적으로 연동하여 활용하고 시너지를 누릴 수 있게 된다.

<표 IV-1> DeFi 간 융합 서비스 사례

활용 주체	활용 대상	융합 서비스 사례
1inch	Uniswap, Sushiswap등	주요 DeFi 거래소의 가격을 비교하여 가장 좋은 가격으로 거래
yearn. finance	Compound, Aave 등	가장 금리가 높은 DeFi를 추출하여 그곳에 자산을 예치하며, 한 번 예치한 후에도 금리 순위가 바뀌면 최고 금리가 있는 곳을 찾아 자동으로 자산을 이체
Compound, Aave 등	MakerDAO (DAI)	DAI는 원래 MakerDAO의 서비스 수단으로 고안되었으나 현재는 다수의 DeFi들이 이를 서비스의 핵심 자산으로 활용

지금까지 DeFi가 태생적으로 가지는 긍정적인 측면을 살펴보았는데 이번에는 반대로 블록체인과 스마트계약에 기인하는 DeFi의 한계점을 살펴보자. 가장 먼저 짚어야 할 사실은 블록체인 네트워크의 안정성 및 영속성에 대한 우려가 여전히 존재한다는 것이다. 탈중앙화 블록체인 네트워크에서 블록을 검증하고 생성하는 주체들 간의 합의 과정이 계속해서 별 탈 없이 지금처럼 유지될 수 있을지에 대해 우리는 아직 명확한 답을 가지고 있지 않다. 예를 들어 미래에

양자컴퓨터의 개발이 완료되어 널리 상용화되더라도 현재의 합의 과정이 계속해서 유지될 수 있을까?[19] 만약 환경이 변화하고 이에 맞추어 블록체인의 합의 과정이 지금과 다르게 변경되어야 한다면 그 위에 운영되고 있는 DeFi 서비스들은 연속성을 유지할 수 있을까? 이러한 우려 속에서 사용자들이 과연 본인 자산의 큰 비중을 기존 금융시스템이 아닌 DeFi에 안심하고 맡길 수 있을지에 대해서 여전히 의구심이 들 수밖에 없다.

둘째, DeFi가 기반으로 하는 블록체인 네트워크의 확장성 문제다. 현재 가장 많은 개별 DeFi들이 활용하고 있는 블록체인 네트워크는 단연 이더리움이다. Glassnode Studio에 따르면 2021년 7월 중 이더리움 사용자들이 거래 한 건당 네트워크에 지급한 평균 수수료는 5.3달러(중간값 2.3달러) 수준이었으며, 사상 최고가를 경신했던 2021년 5월에는 평균 21.7달러(중간값 9.2달러)를 기록하기도 하였다. 소액으로 DeFi 서비스를 이용하려는 사용자에게 이렇게 높은 수수료 수준은 큰 부담이 아닐 수 없다. 그러나 이더리움의 네트워크 수수료가 원래부터 이렇게 높았던 것이 아니다. 2020년 7월까지만 해도 월평균 수수료가 1달러를 넘은 적은 단 한 차례에 불과하였으며 그마저도 2달러를 넘지 않았다.[20] 최근의 수수료 급등 현상은 일차적으로 DeFi 활성화에 따른 사용자들의 거래 수요 폭증이 영향을 미쳤으며, 보다 근본적으로는 이더리움 네트워크가 이렇게 많은 거래를 원활하게 처리할 수 있을 정도로 충분한 확장성을 지니지 못했다는 사실에 기인한다. 다만, 그동안 블록체인 네트워크의 확장성 문제를 해결하기 위해 다양한 시도가 이루어졌으며 그 중 일부는 이미 상당한 진척을 보이고 있으므로 조만간 긍정적인 결과를 나타낼 것으로 기대된다.

셋째, 가상자산 가격의 높은 변동성 문제다. 현재 DeFi는 가상자산만을 그 대상으로 취급하고 있으므로 DeFi 서비스의 안정성은 가상자산의 가격 변동에 큰 영향을 받는다. 예를 들어, 이더리움의 가격이 급락하는 경우를 생각해보자. Compound와 같이 담보대출 서비스를 진행하는 DeFi에서 이더리움의 담보가치가 크게 떨어지고 이를 담보로 한 대출들이 단기간에 대거 청산될 위험에 놓이게 될 것이다. 담보물의 청산은 또다시 이더리움 가격의 추가 하락을 야기하고 이는 곧 또 다른 이더리움 담보물의 청산 가능성을 의미한다. 이러한 연쇄 작용은 가상자산 시장 및 DeFi 서비스의 안정성을 동시에 위협하는 요인으로 작용한다. 또한 현재 DeFi 사용자 대부분이 가상자산 투자자로 이루어져 있어 가상자산 시장이 붕괴되면 DeFi 서비스의 수요층이 대거 이탈할 가능성 또한 존재한다.

---

19 양자컴퓨터는 기존 컴퓨터보다 연산 능력이 월등히 뛰어나 향후 블록체인에 적용된 현재의 암호화 기술을 무력화할 가능성이 존재한다. 따라서 상당수 전문가들은 양자컴퓨터가 상용화되면 이에 맞게 블록체인 네트워크에서도 양자컴퓨터에 맞설 수 있는 새로운 암호화 표준을 채택해야 할 것이라고 주장한다.

20 가상자산 투기 열풍이 절정에 달했던 2018년 1월에 월평균 수수료 1.9달러를 기록한 적이 있다.

넷째, DeFi의 프로그래밍 코드가 모두에게 투명하게 공개되어 있어 만약 취약성이 존재하면 해킹 공격으로 인해 큰 피해가 발생할 수 있다. DeFi는 일반적인 기업 서버에서 제공하는 기존 서비스들과는 달리 해커들이 프로그래밍 코드를 분석하여 버그를 찾아내는 데 한결 용이하다. 사용자들의 관심을 많이 받는 주요 DeFi들은 통상 개발자 커뮤니티 또는 전문 보안 기관에서 사전에 검증하는 절차를 거치지만 설령 그렇다 하더라도 미처 발견하지 못한 취약점이 남아있을 수 있다. 특히 신규 서비스를 개시하거나 기존의 서비스를 업그레이드할 때에 더욱 그러하다. 더욱이 사용자들의 관심이 비교적 덜한 DeFi들의 경우 해커에 의해 취약점이 발견될 가능성은 이보다 훨씬 높다. 만약 해킹 사고가 발생하면 DeFi에 예치된 가상자산이 대거 탈취될 수 있으며 블록체인 네트워크의 익명성으로 인해 해커들은 탈취한 가상자산을 비교적 쉽게 유용하거나 은닉할 수 있다. 설령 공격에 실패하더라도 일반적인 기업 서버를 해킹하는 것과 비교하여 해커들의 법적 처벌 가능성도 훨씬 낮은 편이다. DeFi에서 발생한 주요 보안사고 사례를 <표 IV-2>에 정리하였는데 단 10건에서 해커들의 탈취금액이 총 9억 8천달러에 달할 정도로 피해 규모가 큰 편이다.

<표 IV-2> DeFi 관련 보안사고 목록

(단위: 백만달러)

DeFi 이름	일시	탈취금액	보안감사 업체명
Poly Network	2021. 8. 10	611	없음
EasyFi	2021. 4. 19	59	없음
Uranium Finance	2021. 4. 28	57	없음
PancakeBunny	2021. 5. 19	45	없음
Kucoin	2020. 9. 29	45	내부 감사
Alpha Finance	2021. 2. 13	38	Quantstamp, Peckshield
Vee Finance	2021. 9. 21	34	Slowmist, Certik
Meerkat Finance	2021. 5. 4	32	없음
Spartan Protocol	2021. 5. 2	31	Certik
StableMagnet	2021. 6. 23	27	Techrate

주 : 1) 보안감사란 전문 보안 기관에서 사전에 프로그래밍 코드를 분석하여 취약성이 없는지 여부를 조사하는 것을 의미
2) 2021년 10월 1일 기준으로 조회하였으며 탈취금액 순으로 상위 10건을 추출

자료: rekt.news

다섯째, 현재 DeFi는 사용자 보호 측면에서 매우 취약하며, 따라서 향후 각국의 규제로 인해 성장 속도가 위축될 가능성이 있다. 기존 금융회사와 달리 DeFi에는 고객센터가 없으므로 서비스를 이용하는 중 불합리한 결과가 예상치 못하게 발생하였더라도 사용자가 이에 대해 민원을 제기하고 이를 무효로 하는 것이 거의 불가능하다. 또한 사용자가 비밀번호를 잊어버리거나 갑자기 사망하여 계정에 접속할 수 없는 경우 DeFi에 예치된 자산을 되찾는 일 또한 매우 어렵다. 해커가 사용자의 가상자산 계정의 비밀번호를 알아내고 이를 통해 DeFi에 예치된 자산을 인출하여도 한번 상황이 벌어지고 난 뒤에 사용자가 복원할 방법은 거의 없다. 사용자 보호 문제와 관련하여 미국 SEC와 CFTC 등 규제당국에서는 DeFi에 대한 규제 필요성을 이미 수차례 언급하였으며 실질적인 규제 방안을 검토 중인 것으로 알려져 있어[21] 향후 미국을 비롯한 각국의 규제가 강화될 가능성이 존재한다.

<표 IV-3> 기반기술에 기인하는 DeFi의 특징

차별성	한계점
1. 사용자의 접근성 확대 2. 금융서비스 제공자의 진입요건 완화 3. 중개 비용 절감 4. 상호 연결과 조합이 자유로움	1. 블록체인 네트워크의 안정성 및 영속성에 대한 우려 2. 블록체인 네트워크의 확장성 문제 3. 가상자산 가격의 높은 변동성 문제 4. 해킹 공격으로 인한 피해 5. 사용자 보호 측면에서 매우 취약하며 향후 규제 대상이 될 가능성 존재

2. 개별 알고리즘에 기인하는 DeFi의 특징

현재 활용되고 있는 주요 DeFi 서비스들은 알고리즘상 다음의 차별성을 공통으로 가지고 있다. 첫째, 통상 약정기한을 설정하지 않으며 사용자에게 차별 없이 동일한 서비스를 제공한다. 예를 들어 예금-대출 서비스의 경우 사용자는 언제든 원하는 시기에 자산을 인출하거나 상환할 수 있다. 또한 이자를 만기에 한꺼번에 지급하는 대신 네트워크상에서 새로운 블록이 생성될 때마다 거의 실시간으로 이자가 쌓이게 된다. 이더리움 네트워크의 경우 블록 생성에 약 15초가 소요되므로 예금자는 예금을 맡긴 다음 15초만 지나도 그 시간만큼의 이자를 얻을 수 있는 것이다.[22] 통상 최소 수개월에서 수년의 만기를 채워야 하는 기존 금융서비스들과는 차별화된 점이다. 또한 기존

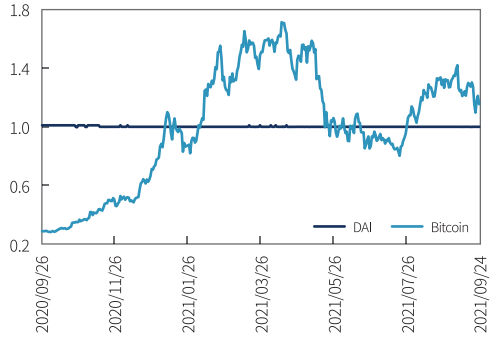
21 King & Spalding(2021) 참고

22 단, 이자가 자동으로 사용자의 계좌에 이체되는 것은 아니며, CA 안에 보관되어 있다가 사용자가 인출 함수를 호출하면 비로소 이체가 이루어진다.

금융기관들은 서비스에 드는 실질 비용 수준을 고려하여 고액 거래에 대해 우대 조건을 적용하는 경향이 있으나, DeFi는 사용자의 거에 따른 비용 부담이 전혀 없으므로 그러한 고려 없이 고액이든 소액이든 상관없이 모든 거래에 대해 동일한 조건으로 서비스를 제공한다.[23]

둘째, DeFi는 알고리즘을 통해 자동으로 수요-공급량을 조절하여 서비스의 지속가능성을 확보한다. 만약 특정 자산에 대한 수요가 많으면 사전에 정해진 수식에 따라 실시간으로 가격을 상승시키고 반대로 공급이 많으면 가격을 하락시켜 수요-공급량을 적절한 수준으로 통제한다. 이는 DeFi 서비스의 지속가능성을 확보하는 데 있어 핵심 수단이 된다. 자세한 내용은 앞에서 Compound의 사례를 들어 설명하였으므로 여기에서는 생략한다. 한편, 이러한 원리는 일부 스테이블 코인에서도 유사하게 적용되어 특정 가상자산의 가치를 법화에 연동하는 데 활용되기도 한다. 예를 들어 예금-대출 서비스 분야에서 대표 DeFi 중 하나인 MakerDAO는 DAI라는 자체 토큰을 발행하는데, 이 토큰은 담보물 없이 순수하게 알고리즘에 의해 가치가 1달러로 고정되도록 설계되었다. 만약 DAI의 시장가격이 1달러를 초과하면 발행량이 늘고 1달러를 밑돌면 소각량이 늘어나는 식이다. 실제로 DAI의 가치는 가상자산 시장의 높은 변동성에도 불구하고 <그림 IV-1>에서 보듯 별다른 변화 없이 1달러 수준을 유지하고 있다. 이는 알고리즘의 수요-공급량 조절 기능이 현실에서 매우 강력하게 작동한다는 사실을 보여준다.

<그림 IV-1> DAI와 비트코인의 가격 추이



주 : 두 개의 시계열을 각각의 평균값으로 나누어 높낮이를 평준화함

자료: CoinMarketCap

한편, 현재 운영 중인 주요 DeFi 서비스의 알고리즘들은 공통으로 다음의 한계점을 지니고 있기도 하다. 첫째, 사용자들이 가격 및 금리 변동 위험에 크게 노출되어 있다. 예를 들어, 예금-대출 서비스의 경우 약정기한이 없는 대신 이자율이 실시간으로 변하기 때문에 사용자들은 이자율 변동 위험에 크게 노출된다. 특히 대출자들은 급격한 이자율 상승으로 인해 예상치 못했던 큰 이자를 갑자기 부담하게 되거나 담보비율이 순식간에 하락하여 의도치 않게 대출 자체가 청산되는 상황에 맞닥트릴 수 있다. 또한 개별 DeFi의 가격 및 금리 산정 방식이 개발자에 의해 지나치게 자의적으로 결정되며 서비스마다 모두 제각각이라는 점에서도 사용자들이 혼동과 불만을 호소할 수 있다.

23 비용은 DeFi가 아닌 사용자가 블록 생성 주체에게 지급한다. 만약 현재의 이더리움과 같이 네트워크 수수료가 높은 수준으로 계속 유지된다면 실질적으로는 고액 거래가 수익률 측면에서 사용자에게 더욱 유리할 것이다.

둘째, 알고리즘이 내포하고 있는 실시간 수요-공급량 조절 기능이 극단적인 상황에서도 잘 작동할 수 있을지에 대한 우려가 존재한다. 일반적인 상황에서는 알고리즘을 통해 수요-공급량을 통제하는 것이 가능하지만 이른바 블랙스완(Black Swan)이라 불리는 비정상적인 상황이 닥치더라도 이러한 기능이 여전히 잘 작동할지에 대해서는 의구심이 존재한다. 만약 알고리즘으로 수요-공급량을 통제할 수 없는 상황이 닥친다면 이를 전제로 구현된 다수의 DeFi 서비스들이 일시에 붕괴될 수 있다. 예를 들어 알고리즘에 의해 동작하는 스테이블 코인 DAI의 가격이 1달러를 크게 벗어나 폭락한다면 어떠한 일이 발생할 것인가? 이를 핵심 자산으로 취급하는 다수의 DeFi들이 즉각 치명적인 타격을 입을 것이다.

셋째, DeFi 운영 주체에 대한 위험이다. DeFi는 그 용어가 의미하듯 탈중앙화된 서비스를 표방하지만, 현재 작동 중인 대부분의 DeFi들은 아직 완벽하게 탈중앙화되어 있지 않다.CA 저장소 내 관리자 키(admin keys)를 만들어 보관함으로써 운영 주체가 소유한 특정 EOA로 하여금 해당 DeFi의 알고리즘을 유지보수하거나 업그레이드할 수 있는 권한을 부여하는 경우가 많으며, 해킹과 같이 예상치 못한 이벤트 발생 시 서비스를 일시적으로 중단시킬 수 있는 권한을 부여하기도 한다. 이에 따라 운영 주체가 자금난 등을 이유로 부도 상황에 놓인다면 해당 DeFi 알고리즘의 유지보수가 중단되면서 서비스가 제대로 작동하지 않을 수 있다.

넷째, 기존 중앙화된 중개인이 제공하는 정보생산 및 모니터링 기능을 구현하기가 까다롭다. 여기에서 '정보생산'은 금융기관이 차주의 대출 원리금 상환 가능성에 관한 정보를 획득하는 것을 의미하며, '모니터링'은 금융기관이 대출 이후 차주의 상환능력 유지 여부를 확인 및 감시하고 만기 시에 차주가 원리금을 상환하지 않고 파산한 경우 청산가치를 평가하는 기능을 뜻한다(강종구, 2005). 예를 들면, 기존 은행은 미래 성장능성이 높지만 담보 제공 여력이 부족해 금융시장을 통한 자금조달이 어려운 기업들을 선별하여 대출을 제공함으로써 정보 비대칭 문제를 완화하고 자금배분의 효율성을 높이는 순기능을 수행한다. 반면 DeFi는 아직까지 기술적 한계로 인해 이러한 기능을 거의 수행하지 못하고 있다. 향후 DeFi 알고리즘으로 이러한 정보생산 및 모니터링 기능을 구현하는 것이 과연 가능할지에 대해 아직 속단하기는 어려우나 적어도 당분간은 어려울 것으로 보인다.

<표 III-4> 개별 알고리즘에 기인하는 DeFi의 특징

차별성	한계점
1. 약정기한을 설정하지 않으며 사용자에게 차별 없이 동일한 서비스 제공 2. 알고리즘을 통해 자동으로 수요-공급량을 조절하여 서비스의 지속 가능성 확보	1. 가격 및 금리 변동 위험에 노출 2. 극단적인 상황에서 수요-공급량 조절 기능 상실에 대한 우려 3. DeFi 운영 주체에 대한 위험 4. 정보생산 및 모니터링 기능 구현 어려움

Ⅴ. 요약 및 시사점

DeFi는 분명히 기존 금융시스템과 근본적으로 다르며 큰 차별성을 지니고 있다. DeFi는 물리적 실체 없이 블록체인 네트워크상에서 운영되기 때문에 서비스 제공자는 프로그래밍 코드를 개발 · 배포하는 것만으로 금융서비스를 구현할 수 있으며, 사용자는 인터넷 접속만 가능하면 언제 어디서든 손쉽게 이를 활용할 수 있다. 중앙화된 중개인이 존재하지 않기 때문에 막대한 비용을 절감할 수 있고 중개인의 신용 위험을 걱정할 필요도 없다. 상호 연결 및 조합이 자유롭게 가능하여 DeFi 서비스 간 시너지 효과가 극대화된다는 장점도 가지고 있다. 향후 블록체인 네트워크가 더욱 진화하면 DeFi의 기능은 지금보다 더욱 고도화될 것이고, 실물 자산의 디지털화가 가속화되면서 DeFi가 취급하는 가상자산의 저변 또한 확대될 가능성이 크다.

다만, DeFi를 기존 금융시스템의 대체재로 활용하기에는 아직 부족한 점이 많은 것 또한 부인할 수 없는 사실이다. 현재까지 DeFi는 가상자산 투자를 보조하는 역할 외 금융의 다른 기능들을 거의 수행하지 못하고 있다. DeFi의 영역을 지금보다 더욱 확장하기 위해서는 무엇보다 먼저 블록체인 네트워크와 그 위에 생성된 가상자산, 그리고 DeFi 알고리즘의 안정성과 영속성에 대해 각각 전문적이고 철저한 검증이 필요할 것이다. 이들에 대한 우려가 모두 해소되지 않는다면 DeFi가 기존 금융시스템을 대체할 정도로 크게 성장하기는 어려울 것이다. 그 밖에도 중앙화된 중개인이 없는 DeFi에서 기존 금융시스템의 정보생산 및 모니터링 기능을 구현하기가 매우 까다롭다는 점도 걸림돌로 작용한다. 또한 전문적인 지식이 없는 일반인들도 원활하게 서비스를 받을 수 있도록 사용자 친화적인 인터페이스와 서비스 작동방식에 대한 직관적인 설명, 사용자 보호장치 등도 보완될 필요가 있다.

결국 DeFi는 앞으로 기존 금융시스템을 급격히 대체하기보다는 이와 공존하면서 일부 차별성을 지닌 영역에서 사용자에게 새로운 옵션을 제공하는 정도의 제한적 역할을 당분간 수행할 전망이다. 즉, DeFi에는 아직 해결해야 할 과제가 산적해 있어 단기간에 기존 금융시스템을 잠식할 정도로 크게 성장하기는 어렵다고 판단된다. 일단은 중앙화된 중개인의 역할이 중요하지 않은 비교적 간단한 영역, 특히 가상자산의 예금 및 담보대출 분야에서부터 시작하여, 향후 디지털화된 실물 자산으로 저변을 확장하고, 점차 자산운용 서비스로도 영역을 넓힐 것으로 예상한다. 그 과정에서 DeFi는 다양한 기술적 도전과 시장 불확실성에 맞닥뜨리게 될 것이며 새로운 금융 형태로서의 가능성을 시험받게 될 것이다.

참고문헌

강종구, 2005, 은행의 금융중개기능 약화 원인과 정책과제, 『경제분석』 11(3), 1-33.

권민경 · 조성훈, 2018, 『4차 산업혁명과 자본시장 - 인공지능과 블록체인 -』, 자본시장연구원 조사보고서 18-04.

한국은행, 2021, 디지털 혁신에 따른 금융부문 패러다임 전환 가능성, 『국제경제리뷰』 2021(16).

King&Spalding, 2021, *Decentralized Finance - Risks, Regulation, And The Road Ahead*, https://www.jdsupra.com/legalnews/decentralized-finance-risks-regulation-9351911.

Leshner, R., Hayes, G., 2019, *Compound: The Money Market Protocol*.

Szabo, N., 1994, *Smart Contracts*.

은행연합회	www.kfb.or.kr
이더리움	ethereum.org
DEFI PULSE	defipulse.com
Glassnode Studio	studio.glassnode.com
rekt	rekt.news