새로운 금융 형태로서 DeFi의 가능성 점검

자본시장연구원
연구위원 권민경

스마트계약의 이해

- 스마트계약(smart contract)
  - 1994년 닉 재보(Nick Szabo)가 처음 고안한 개념으로 2013년 비탈릭 부테린 (Vitalik Buterin)이 이더리움을 통해 블록체인 네트워크에 첫 적용
  - 계약의 조항들이 전산으로 프로그래밍 되어 자동으로 실행되는 것 (Szabo, 1994)

(2008년) 비트코인
블록체인

(2013년) 이더리움
스마트계약

자료: ledger.com에서 그림 일부 발췌

스마트계약의 이해

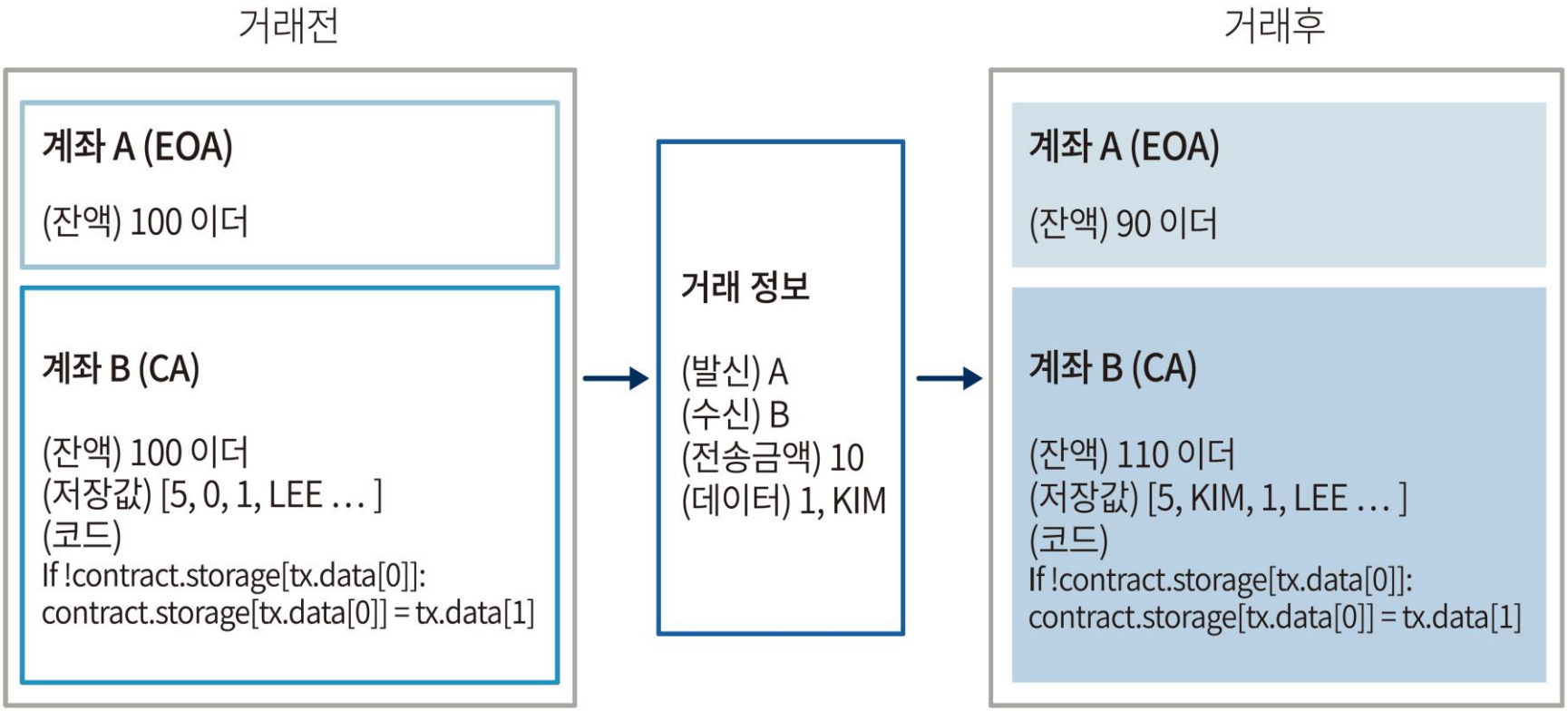
- '계좌(account)' 개념의 확장
  - 사용자 보유계좌 (Externally Owned Account, EOA)
    - 사용자들이 이더(Ether)를 보유하는 일반적인 계좌
  - 계약계좌 (Contract Account, CA)
    - 프로그래밍 코드와 저장소(storage)를 포함
- '거래(transaction)' 개념의 확장
  - 거래 유형이 늘어나고 항목에 '데이터'가 새롭게 추가

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

스마트계약의 이해

이더리움 네트워크에서의 거래 예시

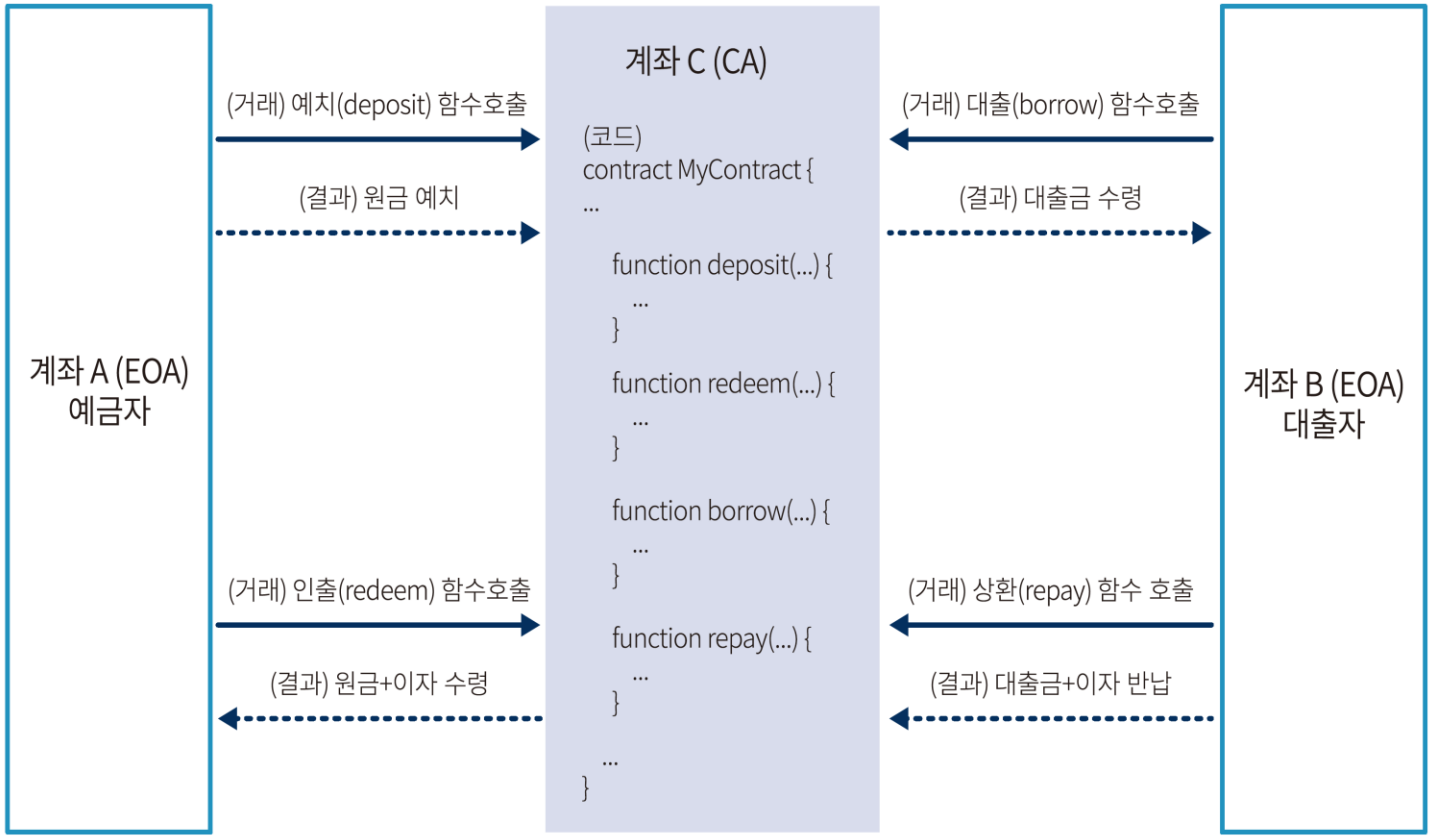


주 : 이더리움 백서 상의 도표를 단순화하여 재작성함

스마트계약의 이해

- 예금 및 대출 서비스 예시
  - 사용자는 은행에 가서 계약서를 작성하는 대신,
    본인의 EOA에서 CA로 거래를 전송하면서 필요한 함수를 호출

스마트계약 기능 예시 – 예금 및 대출 서비스 구조



스마트계약의 이해

- 각각의 함수 안에는 서비스가 원활하게 작동할 수 있도록 하는 세부 알고리즘들이 개발자들에 의해 프로그래밍 코드 형태로 탑재

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

스마트계약의 이해

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 EOS로부터 해당 CA로의 거래를 지시하여 원하는 함수를 호출

⇩

중앙화된 중개인 없는 금융서비스 제공

DeFi의 개념 및 현황

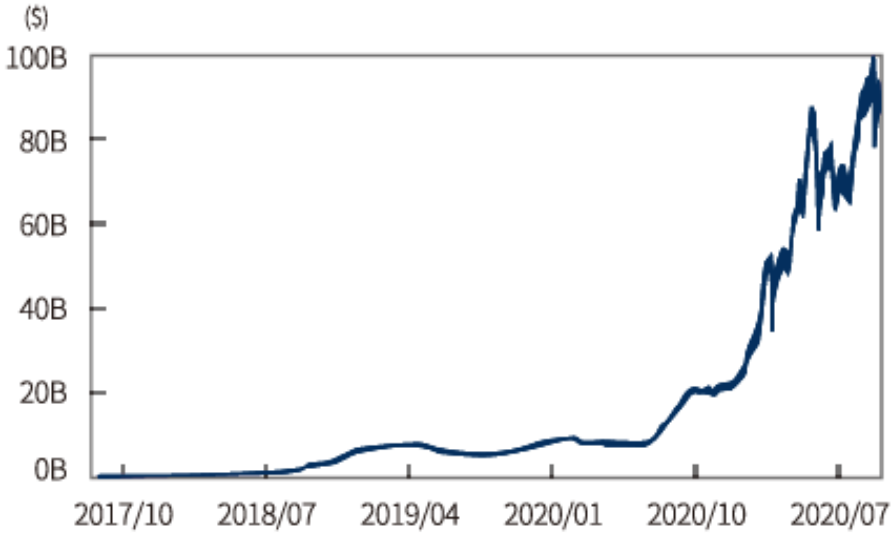
- Decentraliezed Finance(DeFi)의 개념 (이준호 외(2021) 참고)
  - 블록체인 네트워크상에서 은행, 증권사 등 중앙화된 중개인(central financial intermediaries)을 거치지 않고 스마트계약을 통해 구현된 탈중앙화 금융 서비스

- 현황
  - 2017년 MakerDAO가 이더리움 네트워크를 기반으로 스마트계약을 이용한 예금-대출 서비스를 성공적으로 출시하면서 본격 시작 (한국은행, 2021)
  - 대출(MakerDAO, Compound, Aave), 탈중앙화 거래소(Uniswap), 자산운용(yearn.finance), 파생상품(Synthetix), 보험(Nexus Mutual) 등의 분야가 대표적
  - 이더리움, BSC, Polygon, Polkadot 등이 DeFi의 네트워크 역할 수행

DeFi의 개념 및 현황

- DeFi에 예치되어 있는 글로벌 자산규모는 109조원 수준 (2021.10.6.PM 3:00기준, DEFIPULSE)
  - (비교) 국내은행의 원화 저축성예금 합계(1,504조원) 대비 7% 불과 (2021.6.30기준)
- 10여개 주요 DeFi의 토큰 가치총액은 33조원 수준 (2021.10.6.PM 4:00기준)
  - Uniswap(18.3조원), Aave(4.7조원), MakerDAO(2.9조원), Compound(2.0조원) 등
  - (비교) 국내 주요 은행 9개 사의 시가총액 합계(106조원) 대비 1/3에 불과
- 미미한 비중에도 불구하고 DeFi의 폭발적인 성장세는 주목할 만함
  - 예치금액은 2019년말 대비 11배가량 증가

DeFi의 예치 자산 규모 추이



자료: DEFIPULSE

새로운 금융 형태로서의 가능성

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

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

새로운 금융 형태로서의 가능성

블록체인과 스마트계약에 기인하는 DeFi의 차별성

언제 어디서든 누구나 간편하게 접근할 수 있음

- 365일 24시간 쉬지 않고 운영되며 업무 종료 시각이 따로 없음
- 인터넷만 접속할 수 있으면 누구든지 DeFi 서비스 이용 가능
  - 비금융계좌인구(약 17억명, 31%)에게 금융 혜택을 제공할 가능성 (한국은행, 2021)
- 별도의 가입절차나 KYC 등 인증 절차가 없으며 설명의무와 같은 판매규제 없음

금융 서비스 제공자의 진입요건을 현격히 낮춤

- 기존에는 서버, 저장장치, 보안설비 등 물리적 요건은 물론, 이에 대한 유지보수, 모니터링, 내부통제 체계를 갖추어야 하며, 인건비, 전기, 통신, 보험 등 비용 지속 부담
- 스마트계약 활용 시 서비스 내용을 프로그래밍 코드로 작성하고 이를 담은 CA를 생성하기만 하면 이후 서비스의 운영은 블록체인 네트워크가 전담하여 수행
- 공간, 시차, 언어, 규제, 자본금 등의 제약으로부터 자유로워 글로벌 서비스 구현 용이

중앙화된 중개인에게 지급하는 수수료 비용을 절감

- 기존 금융시스템을 운영하는 데 드는 인건비 · 시설비 · 임대료 등의 비용 절감
- 대신 사용자는 블록을 검증 · 생성하는 주체에게 네트워크 사용 대가를 지급

새로운 금융 형태로서의 가능성

- 개별 DeFi 간 상호 연결과 조합이 자유로움 (머니레고, Money Lego)
  - 기존 금융시스템에서는 금융회사 간 이해관계 문제로 인해 상호 협력이 잘 일어나지 않으며 이에 따라 금융서비스 간 시너지가 매우 제한적
  - DeFi 개발자가 별도의 동의를 구하지 않고서도 다른 DeFi 서비스의 프로그래밍 코드를 응용하거나 이들을 하위 도구로 활용하여 새로운 융합 서비스 구현 가능
  - 사용자는 여러 DeFi 서비스들이 마치 하나의 거대한 금융회사가 제공하는 서비스인 양 제약 없이 유기적으로 연동하여 활용하고 시너지를 누릴 수 있음

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

새로운 금융 형태로서의 가능성

블록체인과 스마트계약에 기인하는 DeFi의 한계점

블록체인 네트워크의 안정성 및 영속성에 대한 우려

- 탈중앙화 블록체인 네트워크에서 블록을 검증하고 생성하는 주체들 간의 합의 과정이 계속해서 별 탈 없이 지금처럼 유지될 수 있을까?
- 미래에 양자컴퓨터가 상용화되더라도 유지가 가능할까?
- 만약 합의과정이 변경되어야 한다면 그 위에 운영되고 있는 DeFi 서비스들은 연속성을 유지할 수 있을까?

블록체인 네트워크의 확장성 문제

- 2021년 5월 중 이더리움 사용자들이 거래 한 건당 네트워크에 지급한 평균 수수료는 21.7달러(중간값 9.2달러)를 기록하여 특히 소액 거래자에 큰 부담 야기 (Glassnode Studio 자료 참조)
- 이는 근본적으로 이더리움 네트워크가 이렇게 많은 거래를 원활하게 처리할 수 있을 정도의 충분한 확장성을 가지지 못했다는 사실에 기인

새로운 금융 형태로서의 가능성

- 프로그래밍 코드가 공개되어 있어 취약한 부분에 대한 해킹 공격이 용이
  - 개발자 커뮤니티 또는 전문 보안 기관에서 사전 검증 절차를 거치더라도 미처 발견하지 못한 취약점이 남아있을 수 있음
  - 해킹 사고 발생 시 DeFi에 예치된 가상자산이 대거 탈취될 수 있으며 해커들은 블록체인 네트워크의 익명성으로 인해 비교적 쉽게 은닉 가능

DeFi 관련 보안사고 목록

DeFi 이름	일시	탈취금액 (백만 달러)	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 : 2021년 10월 1일 기준으로 조회하였으며 탈취금액 순으로 상위 10건을 추출

자료: rekt.news

새로운 금융 형태로서의 가능성

- 가상자산 가격의 높은 변동성
  - DeFi는 가상자산만을 그 대상으로 취급하고 있으며 따라서 DeFi 서비스의 안정성은 가상자산의 가격 변동에 큰 영향을 받음
  - 예를 들면 이더리움 가격 급락 시 이를 담보로 한 대출이 단기간에 대거 청산될 수 있으며 이는 또다시 이더리움의 추가적인 가격 하락 및 또 다른 담보물 청산을 야기
  - 또한 DeFi 사용자 대부분이 가상자산 투자자로 이루어져 있어 가상자산 시장이 붕괴되면 DeFi 서비스의 수요층이 대거 이탈하여 서비스 안정성이 저해될 수 있음

- 사용자 보호 측면에서 매우 취약
  - DeFi에는 고객센터가 없으므로 민원을 제기하고 거래를 무효로 하는 것이 불가능
  - 사용자가 비밀번호를 잃어버리거나 갑자기 사망하여 계정에 접속할 수 없는 경우 DeFi에 예치된 자산을 되찾는 일 또한 매우 어려우며 지갑 해킹 사례도 빈번하게 발생
  - 미국 SEC는 향후 문제의 발생 소지가 다분하므로 사용자 피해 예방을 위해 DeFi에 대한 규제가 필요하다는 태도를 계속해서 견지하고 있어 향후 규제 강화 가능성이 존재

새로운 금융 형태로서의 가능성

개별 알고리즘에 기인하는 DeFi의 차별성

통상 약정기한을 설정하지 않으며 차별 없는 서비스 제공

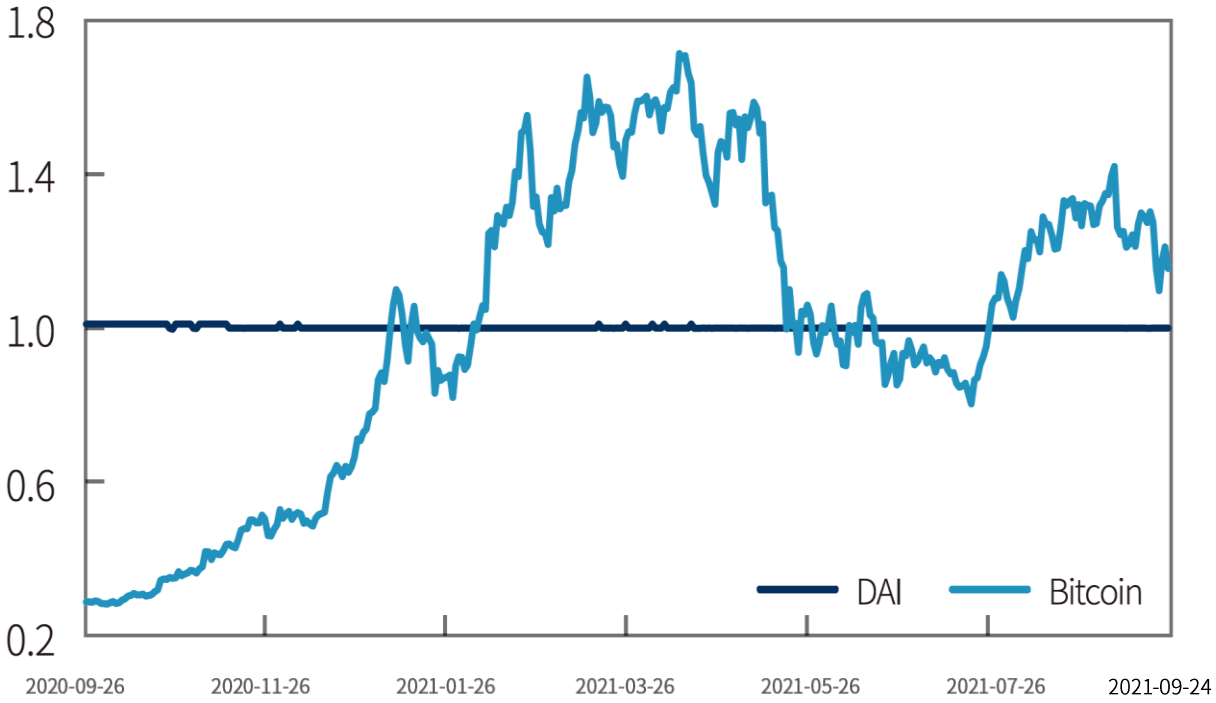
- 언제든 원하는 시기에 인출하거나 상환할 수 있으며 거의 실시간으로 이자 발생
- 기존 금융 서비스는 고액 거래에 대해 우대 조건을 적용하는 경우가 많으나 DeFi에서는 소액이든 고액이든 동일한 가격으로 서비스를 받을 수 있음

알고리즘이 자동으로 수요-공급량을 조절

- 사전에 정해진 수식에 따라 수요(공급)가 많으면 가격을 상승(하락)
- 수요-공급량을 적절한 수준으로 통제함으로써 서비스의 지속 가능성을 확보
  - 특정 자산 고갈 시에도 뱅크런이 발생하기 보다는 '이자율 상승 → 대출자산의 상환 또는 담보자산의 청산 증가' 과정을 통해 잔고 회복 가능성 높음
- 이러한 원리는 일부 스테이블 코인에도 유사하게 적용되어 특정 가상자산의 가치를 법화에 연동하는 데 활용되기도 함
  - 실제 DAI 가격은 가상자산 시장의 높은 변동성에도 불구하고 목표가(1 USD)에 매우 근접한 수준 유지

새로운 금융 형태로서의 가능성

DAI와 비트코인 가격 추이



주 : 두 개의 시계열을 각각의 평균값으로 나누어 높낮이를 평준화함
자료: CoinMarketCap

새로운 금융 형태로서의 가능성

개별 알고리즘에 기인하는 DeFi의 한계점

가격 및 금리 변동 위험에 크게 노출

- 대출자의 경우 급격한 이자율 상승으로 예상치 못했던 큰 이자를 갑자기 부담하게 되거나 담보비율 하락으로 대출 자체가 청산될 수 있음
- 개별 DeFi의 가격 및 금리 산정 방식이 개발자에 의해 자의적으로 결정되며 서비스마다 모두 제각각이라는 점에서도 사용자들의 혼동과 불만을 야기

비정상적 상황에서도 수요-공급 조절 기능이 잘 작동할 수 있을지에 대한 우려

- 만약 수요-공급량 통제가 불가능한 상황이 오면 이를 전제로 구현된 다수의 DeFi 서비스들이 일시에 붕괴될 수 있음
- 예를 들어 알고리즘에 의해 작동되는 스테이블 코인 DAI의 가격이 1달러를 크게 벗어나 폭락한다면 어떠한 일이 발생할 것인가?

DeFi 운영 주체에 대한 위험

- 탈중앙화된 서비스를 표방하지만 아직 완벽하게 탈중앙화되어 있지 않음
- 만약 운영 주체가 자금난 등으로 부도 상황에 놓인다면 해당 DeFi 알고리즘의 유지보수가 중단되면서 서비스가 제대로 작동하지 않을 위험 존재

새로운 금융 형태로서의 가능성

종합

- DeFi는 기존 금융시스템과 근본적으로 다르며 큰 차별성을 지님
  - 물리적인 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 활용
  - 향후 블록체인 네트워크가 진화하고 실물 자산의 디지털화가 가속화되면서 DeFi의 기능과 영역은 지금보다 더욱 확대될 것

- 그러나 기존 금융시스템의 대체재로 활용하기에는 아직 부족한 점이 많은 것도 사실
  - 현재 가상자산 투자를 보조하는 역할 외 금융의 다른 기능들을 거의 수행하지 못하고 있으며, 특히 기존 금융시스템의 신용 창출 기능을 구현하기가 까다롭다는 점도 걸림돌로 작용
  - 무엇보다 우선 블록체인 네트워크와 그 위에 생성된 가상자산, DeFi 알고리즘의 안정성과 영속성에 대한 철저한 검증이 필요

- 기존 금융시스템을 급격히 대체하기보다는 중앙화된 중개인의 역할이 중요하지 않은 비교적 간단한 영역에서 새로운 옵션을 제공하는 제한적 역할을 당분간 수행할 전망
  - 비교적 간단한 가상자산의 예금 및 담보대출 분야에서부터 시작하여, 향후 디지털화된 실물 자산으로 저변을 확장하고, 점차 자산운용 서비스로 영역을 넓힐 것으로 기대
  - 그 과정에서 다양한 기술적 도전과 시장 불확실성에 맞닥뜨리게 될 것이며 새로운 금융 형태로서의 가능성을 시험받게 될 것임