한국은행 THE BANK OF KOREA

금융결제 업무정보

금융결제국
디지털화폐동향분석반, 기술반
2023. 1. 5.

지급결제 측면에서 본 암호자산 거래소 운영 구조 및 시사점

- CP-AMM 알고리즘 기반의 탈중앙 거래소(DEX)를 중심으로 -

□ **(현황)** 현재 주요 암호자산 거래소는 **중앙화 거래소**(CEX) 방식으로 운영되고 있으나, 최근 **탈중앙금융**(DeFi)의 일종인 **자동시장조성자**(AMM) 방식의 **탈중앙 거래소**(DEX)에 대한 관심이 증대

○ CEX는 **주식시장**과 달리, 각 거래소가 ① **시장조성 기능**뿐 아니라 ② 암호자산의 **예·수탁**과 **대금의 청산·결제**도 자체 수행함에 따라, **투명성**이 낮고 **횡령·해킹** 등 **이용자 피해**가 지속 발생

○ **DEX 모델**의 경우, **이용자**가 **개인 지갑**의 암호자산을 **스마트계약**으로 구현된 AMM과 ① **직접 거래**할 뿐 아니라 ② **거래유동성 공급**에도 참여할 수 있어 **투명성**이 높고 **탈중앙화 철학**에도 더 잘 부합하는 측면이 있음

□ **(전망)** 최근 FTX 사태 등으로 인해 **CEX**에 대한 **신뢰**가 낮아진 상황에서 **암호자산 시장** 내 **DEX의 비중이 더욱 확대**될 수 있겠으나, **CEX를 전면 대체**하기는 어려울 것으로 예상됨

○ **DEX**의 경우 ① **대고객 서비스** 등의 측면에서 **편의성**과 **접근성**이 낮고, ② 스마트계약의 **오류** 등에 따른 **이용자 피해**가 발생해 왔으며, ③ **규제 적용**이 쉽지 않아 **탈세, 자금세탁** 등에 악용되는 한계가 있음

○ 반면, **CEX**는 ① **규제**가 **강화**되고 ② **별도 예탁 및 결제 인프라**가 갖춰지는 경우, **리스크**가 점차 **분산**되고 **고객 자금 전용** 등의 문제가 발생할 소지도 축소될 수 있을 것으로 예상

□ **(시사점)** **지급결제 인프라** 측면에서, 향후 **AMM 알고리즘**은 ① **CBDC**를 활용한 **국가간 송금** 등에서의 **외환 유동성 공급 메커니즘**, ② **부동산, 저작권 등 토큰화된 자산**(tokenized assets) 거래에서의 **시장조성 메커니즘** 등으로 다양하게 활용될 여지

○ 동시에, **거시경제적 영향** 측면에서, 규제 적용이 쉽지 않은 **DEX**를 통해 미 달러화 및 원화 기반 **스테이블코인**의 **교환거래**가 가능할 수 있다는 점에서 향후 이를 이용한 **자본유출입**에도 대비할 필요

작성자 : 장하주(02-750-6516), 이기태(6656) 과장, 박준영(6641) 조사역, bokcbdc@bok.or.kr

Ⅰ 조사 배경

□ 글로벌 3위 암호자산 거래소인 **FTX**가 **고객자금 유용** 의혹에 이어 **파산보호**를 신청(11.11일)하고, 최근 세계 최대 거래소인 **바이낸스**도 대규모 **자금이탈**이 발생하면서 **암호자산 생태계 전반**에 대한 **부정적 시각**이 팽배

○ 암호자산 부문에 대한 **신뢰**가 크게 하락하고, 2022년 들어 **테라/루나** 사태, **암호자산 대출업체**(3AC, Celsius 등) **부실화** 등으로 촉발된 **암호자산 가격 하락세**가 더욱 심화

○ **암호자산 업계**에서는 **준비자산 보유증명***(proof of reserves) 방식 도입 등을 통해 **투명성**을 높이려는 노력이 이어지고 있는 가운데, **이용자 보호** 차원에서 거래소 등 **암호자산 취급업자**에 대한 **규율체계 도입 논의**도 가속화

* 암호학적 방법을 통해 거래소가 예치 및 보유중인 암호자산을 매도 또는 대출하지 않고 실제 보유하고 있음을 증명

□ 동시에 기존 거래소*와 달리 개인들이 암호자산을 예탁하지 않고 **직접 보유**하면서 다른 **암호자산**과 **교환**할 수 있는, 이른바 '**탈중앙 암호자산 거래소(DEX: Decentralized Exchange)**'에 대한 **관심**도 크게 **증대**

* 업계에서는 DEX와의 구분을 위해 기존 거래소를 **중앙화 거래소(CEX: Centralized Exchange)**로 지칭

○ **탈중앙 거래소**는 **이더리움 등**의 **암호자산**과 **NFT** 등 **디지털 자산 거래**에서 그 **비중**이 높아지고 있을 뿐 아니라,

자산의 **직접 보관(self-custody)**, 특정 금융기관이나 별도 인프라가 없더라도 **퍼블릭 블록체인**상에서 동작하는 **스마트계약** 기반의 **자동화된 시장조성**(AMM: Automated Market Maker) 등 관련 기술이 미래 **토큰화된 경제**에서 **지급결제 인프라**의 한 축으로 활용될 가능성도 있음

⇒ 향후 디지털 자산을 **제도적·기술적**으로 **뒷받침**하는 **지급결제 인프라 구축**의 관점에서 ❶ **탈중앙 거래소 등 암호자산 거래소의 운영 구조와 특징에 대**해 알아보고, ❷ 중앙은행 입장에서의 **정책적 시사점**을 도출

Ⅱ 암호자산 거래소 개황 및 탈중앙 거래소 현황

□ 현재 암호자산 거래소는 운영 구조에 따라, 크게 ❶ **중앙화 거래소**(CEX)와 ❷ **탈중앙 거래소**(DEX)로 구분

1. 중앙화 거래소

□ 암호자산 역사 초기부터 **법화**와 **암호자산** 간의 **교환**을 중개하는 **거래소**가 자연스럽게 등장

○ 개인간 직거래*시 ❶ **거래상대방**을 찾기 쉽지 않고, ❷ **가격 등 조건**에 합의하기도 쉽지 않으며, ❸ **대금결제** 등 리스크도 커 활발한 거래가 이루어지기 어렵기 때문

* 온라인 게시판 등을 통해 판매자가 수량과 가격을 제시하고, 희망하는 구매자가 있는 경우, 대면 또는 에스크로 서비스와 함께 비대면 거래를 지원하는 **통신판매중개업 형태**의 서비스가 가능(예: LocalBitcoins)

○ 특히 **다양한 암호자산**이 등장하고, **가격이 급변동**하면서 **시세 차익**을 목적으로 하는 **투기적 거래 수요**가 크게 증가함에 따라 전 세계적으로 **암호자산 거래소**들이 빠르게 성장

□ 현재 **바이낸스**(케이먼군도) **코인베이스**(미국), **업비트**(한국) 등 주요 거래소가 대부분 중앙화된 방식으로 운영되며, **송금업자** 등의 **인허가**를 받고 영업중임

○ 이용자가 다양한 **암호자산**과 **결제자산(예금, 스테이블코인 등)**을 거래소로 **입금**해 두고 **주식거래**와 유사하게 **집중화**된 **오더북***(order book) **방식**으로 **현물**(spot) 암호자산 및 암호자산을 기초자산으로 하는 **파생**(derivatives) 거래의 **체결** 및 **청산결제** 서비스를 제공

* 거래소에서 시장의 모든 매수·매도 주문을 집중 기록하여 보여주는 전자 목록으로 자산별 매수·매도 주문을 실시간 취합하여 자체 원장인 오더북(order book)에 기록하고, 사전에 정해진 규칙(매칭 알고리즘)에 따라 조건에 부합하는 거래를 순차적으로 체결

2. 탈중앙 거래소

□ 탈중앙 거래소는 비교적 최근에야 등장한 **탈중앙금융(DeFi)**의 일종으로, 이용자들이 **퍼블릭 블록체인**상에서 동작하는 **스마트계약**을 통해 **한 쌍**의 **암호자산**을 **교환**할 수 있는 서비스를 제공

○ **유니스왑**(2018년)이 대표적인 탈중앙 거래소이며, 이외에 펜케익스왑(2020년), 커브(2020년) 등 유사 서비스가 출현

□ 현재 전체 암호자산 시장에서 **탈중앙 거래소**의 비중(현물 거래액 기준)은 20%에 못 미치는 수준이나 점유율이 지속 확대 중

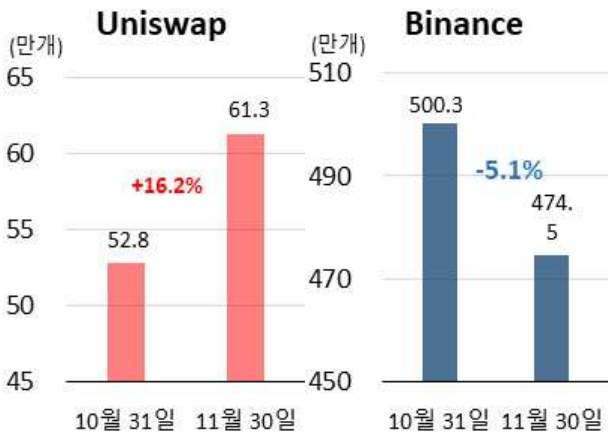
○ 최근에는 중앙화 거래소인 FTX의 파산을 계기로 탈중앙 거래소의 **암호자산 보유량** 및 **거래금액**이 **증가**하고, 중앙화 방식 주요 거래소 대비 **비중**도 **다시 상승**

주요 중앙화 및 탈중앙 암호자산 거래소(11월 현물 거래액 기준)

순위	중앙화 거래소			순위	탈중앙 거래소	
	거래소명	거래액($bn)	비고		거래소명	거래액($bn)
1	Binance	505.63		1	Uniswap (V3)	47.42
2	Coinbase	62.09	Fiat-only	2	Pencake Swap	8.65
3	OKX	40.86		3	Curve	8.88
4	Upbit	25.94	Fiat-only	4	Dodo	5.04
5	Kraken	23.91	Fiat-only	5	Balancer	3.82

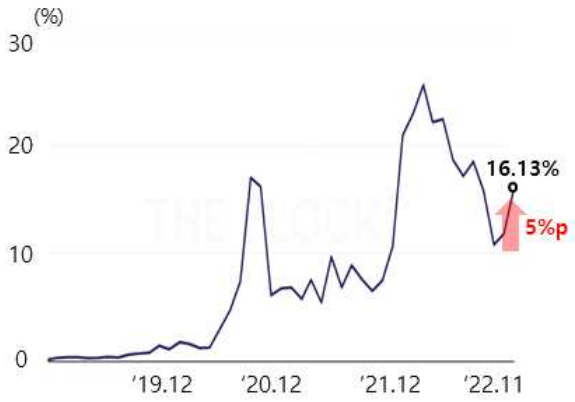
자료: The Block

주요 거래소[1](중앙 vs 탈중앙) 이더리움 보유량[2]



주: 1) Uniswap은 탈중앙 거래소 점유율 1위(10%), Binance는 중앙화 거래소 점유율 1위
2) 탈중앙 거래소의 경우 유동성 공급액을 의미(p11 참조)
출처: Uniswap, CryptoQuant

탈중앙 거래소 거래액 비중(vs 중앙화 거래소)



출처: The Block(2022.12월 발표 기준)

Ⅲ 중앙화 거래소(CEX) 구조 및 문제점

□ 현행 **주식 거래 및 청산결제 인프라**와 비교시,

현재 **CEX 모델**의 경우 ❶동일한 암호자산이 전세계 다수 거래소에 걸쳐 **거래**됨에 따라 **시장조성자** 역할 및 **재정거래** 가능성이 **제약**되는 등 **효율성**이 낮고, ❷개별 거래소가 **암호자산**의 **예·수탁**과 **대금의 청산·결제**를 자체 수행함에 따라 투명성이 낮고 **횡령·해킹** 등 **이용자 피해** 발생 우려도 큼

1. 주식 거래 및 청산결제 인프라: Benchmark

□ 현행 **주식 거래** 및 **청산결제 인프라**는 ❶**거래체결** 및 **시장조성** 기능을 **집중**하여 **효율성**을 높이는 동시에, ❷**증권의 예·수탁**과 ❸**대금**의 **예치** 및 **청산·결제** 기능을 **증권사**에서 **분리**하여 **안전성**을 제고

① 상장 및 시장조성

○ **(상장)** 국가별로 하나의 거래소만 있거나, 여러 거래소가 있는 경우에도 종목별로 **하나의 거래소**(예: 한국거래소)에만 **상장·거래**되며*, **상장 여부**는 개별 증권사가 아닌 거래소의 **심사**를 통해 **결정**

* 단, 은행 발행 DR(Depository Receipt)를 통해 해외 거래소에서 유통될 수 있음

○ **(시장조성)** **금융기관**이 **시장조성자**(market-maker)*로 참여하여 **거래 유동성**을 공급함

* 이용자 주문을 연결하는 방식만으로는 원활한 거래 체결이 어렵기 때문에 금융기관 등이 시장조성자(market maker)로 참가하여 시장에서 형성된 스프레드보다 좁은 호가를 제시하여 거래를 촉진하는 역할을 담당. 자세한 내용은 **<참고1>「전통적인 거래소에서 시장조성자의 역할」(p.16)** 참조

② 예탁

○ 고객이 보유한 주식은 거래 증권사가 아니라 **특정 전자등록기관**(예: 한국예탁결제원)에 **집중 기록·관리**됨*

* 단, 소유권은 계좌관리기관(예: 증권사)이 투자자별로 기록·관리하는 고객계좌를 통해 법적 효력을 인정

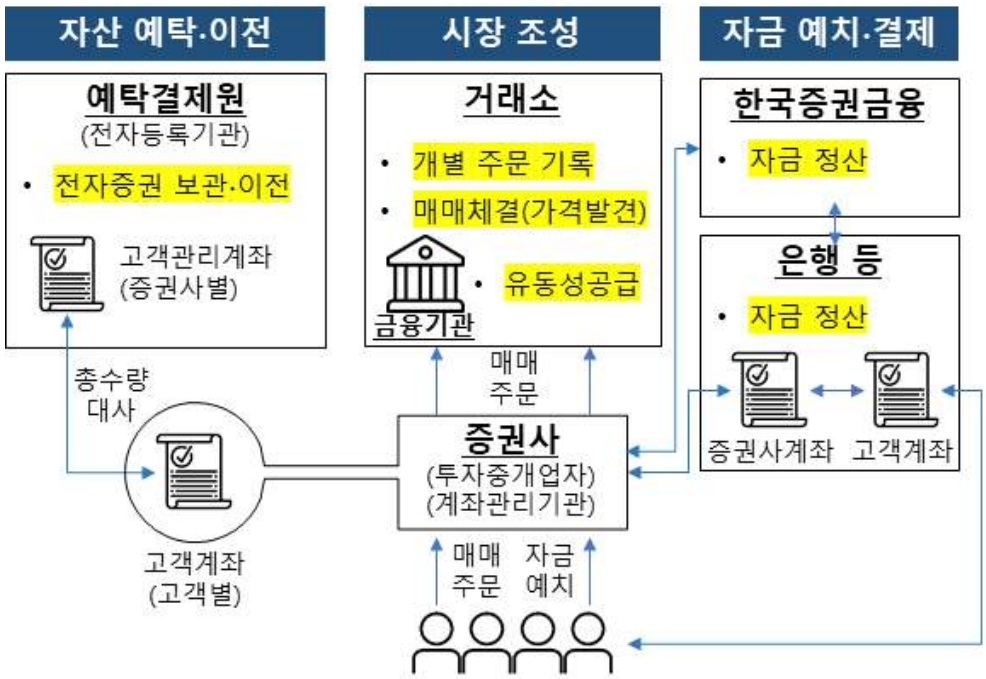
③ 청산결제

○ 주식 거래대금의 청산결제를 위한 **투자자 예탁금**도 개별 증권사가 아닌 **금융기관 등***(예: 한국증권금융)에 외부 예치됨

* 미국, 일본 등은 다수 신탁회사 또는 은행 신탁계정을 이용하는 분산예치방식을 사용

○ **거래소**는 **청산 기능**만 수행하고, 실제 **최종적인 자금의 결제**는 **예탁원**이 **한국은행**의 **대금결제계좌**를 통해 완결

주식 거래 및 청산결제 인프라



2. 중앙화 거래소(CEX) 특징 및 문제점

□ 중앙화 거래소는 **매매거래**를 **중개**하는 **플랫폼 역할**을 담당하는데, ❶**거래체결**은 물론 ❷**암호자산**의 **예·수탁**과 ❸**대금의 청산·결제**에 이르기까지 모든 기능을 **중앙화된 방식**으로 **자체 처리**

① 자체 상장 및 시장조성 미비

○ **(상장)** 각 거래소는 자체적으로 개별 암호자산의 취급(상장) 여부를 결정*하는데, 이 과정에서의 불투명성으로 인해 **선행매매**(front-running) 등 **시세조작**과 **투자유인 사기**(rug pull)에 취약**

* 일본의 경우 상장 심사를 생략할 수 있는 18개 암호자산 리스트(Green list)를 제공하고 있으며 이외 암호자산 상장은 거래소협회(JVCEA) 및 금융청(FSA)의 허가가 요구됨

** 글로벌 2위 거래소인 코인베이스 직원이 NFT의 상장과 관련하여 내부 정보를 이용하여 이익을 편취한 혐의로 기소된 바 있음(2022.8월)

- 또한 동일한 암호자산의 전 세계 여러 거래소에서 개별적으로 거래됨에 따라 취급 종목은 물론 가격도 거래소별로 상이하고, 특히 가격이 **급변동**하는 시기에는 **가격 격차**도 크게 **확대**되는 현상이 빈발*

  * 글로벌 시장에서 국내 거래소의 거래 비중이 높았던 2017년~2018년중 국내 거래소의 암호자산(BTC)이 해외 거래소 대비 최대 63% 높은 가격에 거래되는 현상('김치 프리미엄')이 발생하였으며, 최근에도 21%('21.5월), 8.6%('22.5월) 등 가격 격차 확대 현상이 지속적으로 발생

○ **(시장조성)** 전 세계 다수 거래소에서 **분산**되어 있는 암호자산 시장의 특성상 **거래 유동성**이 **부족**하다는 점에서 **시장조성**의 **필요성**이 더 큼에도 불구하고, **금융기관**들의 **참여**가 **미진**하고, **개인들**의 **참여**도 **제약**이 큼

- **무위험 차익거래** 등을 통해 거래소 간 **가격격차**를 **해소**할 수 있는 여지가 있지만,

  ❶ **금융기관**의 경우 **규제 및 평판 리스크**와 **분리 수탁** 등 **인프라 구축 미비**로 참여를 **기피**하는 가운데, ❷ **개인들**의 참여도 **본인확인(KYC) 및 자금세탁(AML) 규제**, **외국환거래** 규제 등으로 **제약**

② 분리 예탁 미비

○ 고객이 보유한 암호자산은 **개별 거래소의 지갑**에 **보관**된다는 점에서, 실제 고객은 **암호자산 자체**가 아니라 **암호자산에 대한 청구권**(claim)만 보유

- 개인 지갑 또는 타 거래소 지갑으로 인출해 줄 것을 요청하는 경우에만 요청한 지갑 주소로 **암호자산의 이전**이 이루어짐

○ 2014년 **Mt. GOX** 해킹 및 파산 이래 최근의 **FTX** 사태에 이르기까지 **해킹**, **횡령**, **무단 전용** 등에 따른 **대규모 이용자 피해**가 지속적으로 발생

- 해킹에 대비하여 **콜드월렛**에 암호자산을 보관하고, **내부통제** 강화, **외부감사**, **준비자산 보유증명**(proof of reserves) 등 투명성 강화 노력이 이루어짐

- 암호자산 커뮤니티 일각에서는 암호자산을 직접 소유하지 않고 예탁하는 CEX 모델이 애당초 **탈중앙화 철학***과도 부합하지 않는다는 비판도 제기

  * 비트코인 지지자들은 암호자산을 개인 지갑에 직접 보관(self-custody)해야 한다고 주장해 왔음("Not your keys, not your coin")

③ 청산결제 자체 수행

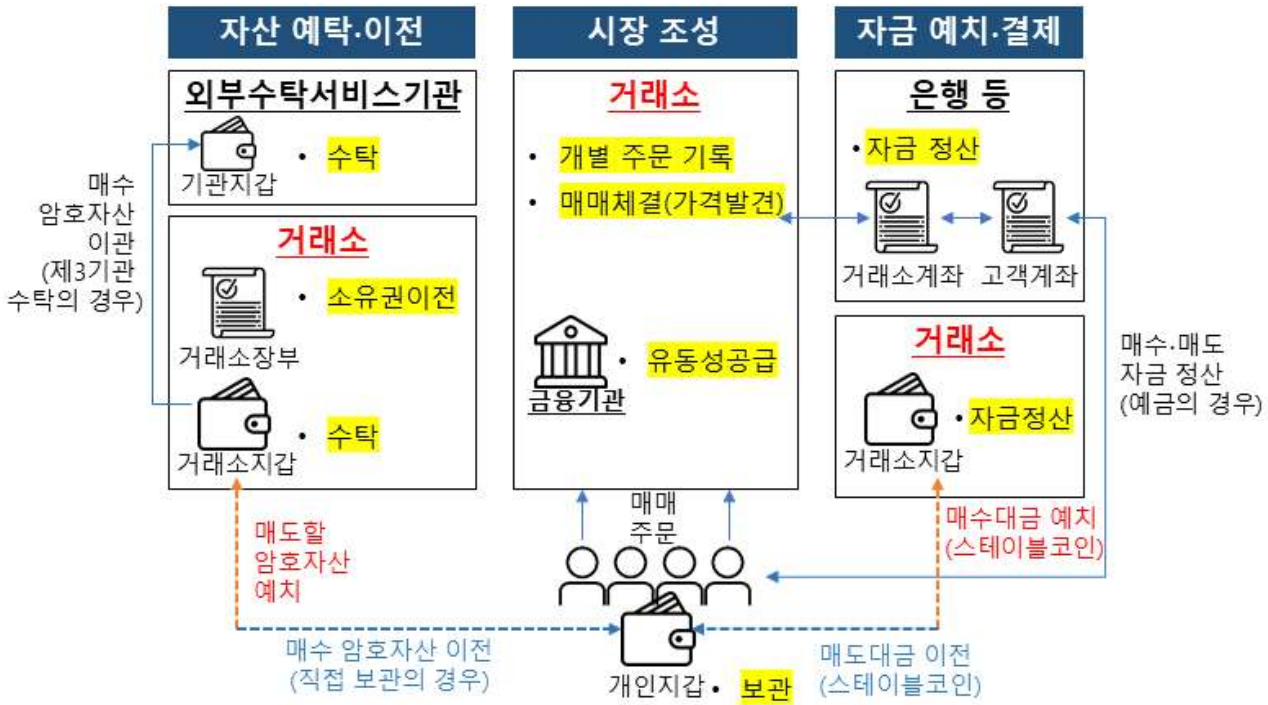
○ 은행 예금의 경우 이용자가 **거래소 은행계좌**로 **예금**을 **입금**하면 거래소는 이용자별 잔액을 **별도 장부**에 기록하고, 암호자산 **매수·매도 거래**가 **체결**되면 이를 반영하여 **자체 장부상 이용자별 잔액**을 **증감**

- 이용자가 충전금을 자신의 예금 계좌로 인출해 줄 것을 요청하면 거래소는 자신의 은행 계좌에서 요청한 계좌로 자금을 이체

○ 한편, 은행 계좌 발급의 어려움 등으로 인해 암호자산 거래시 법화(예금)가 아닌 **비트코인**, **스테이블코인** 등을 **결제자산**으로 하여 여타 암호자산을 매매하는 거래(BTC마켓, USDT마켓)가 발달해 왔는데, 이 경우에도 해당 암호자산은 **거래소 지갑**에 **예탁**됨

  * 국내에서도 은행과 실명계좌 계약을 맺지 않은 일부 중소형 거래소들은 BTC마켓 서비스를 제공중

중앙화 거래소(CEX) 기본 구조



Ⅳ 탈중앙 거래소(DEX) 운영 구조 및 평가

□ **DEX 모델**의 경우 **이용자**가 암호자산을 **직접 보유**한다는 점에서 **탈중앙화**의 원칙에 더 잘 부합하는 측면이 있으나,

❶ **대고객서비스** 등의 측면에서 **편의성**과 **접근성**이 낮고, ❷ **시세조작**, **해킹** 등의 발생 가능성도 배제하기 어려우며, ❸ **규제 적용**이 어려워 **이용자 피해**가 발생하거나 **자금세탁** 등의 창구로 기능할 위험도 상존

1. 탈중앙 거래소 기본 구조

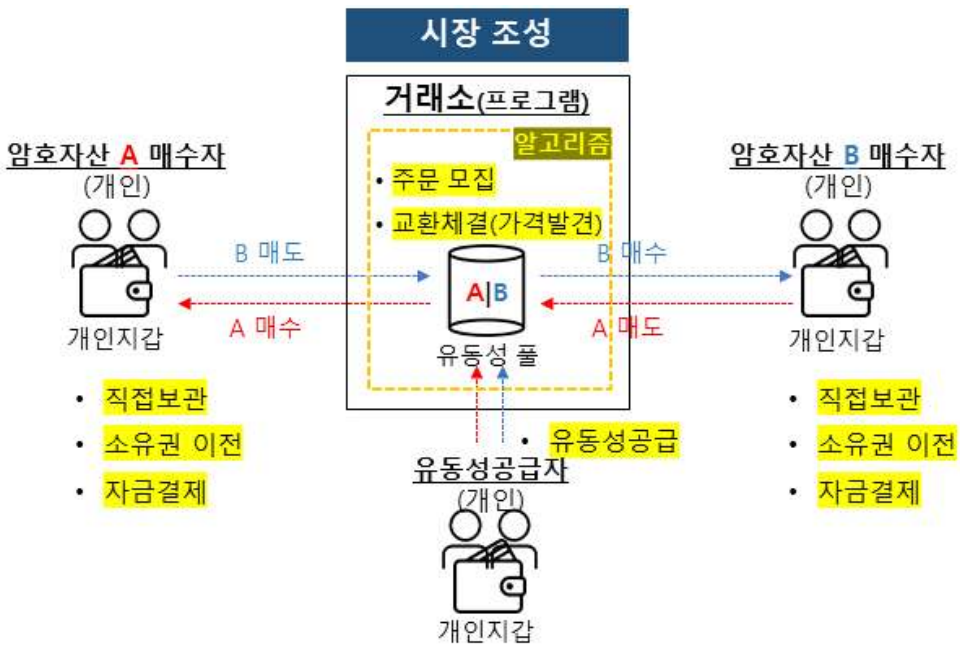
□ 중앙화 거래소를 대신하여 **수탁** 및 **결제**를 **개인**이 **직접 수행**하면서 암호자산을 **거래**하는 **방안**이 일찍부터 논의되어 왔으며,

현재 **탈중앙 거래소**(DEX)는 **CP-AMM**(Constant Product Automatic Market Maker) 알고리즘 방식으로 운영됨

○ **(예탁 및 결제)** 이용자가 자신의 **개인 지갑**에 보관중인 암호자산을 **거래소 지갑**을 거치지 **않고 직접 교환**

○ **(시장조성)** 오더북을 대신하여 **퍼블릭 블록체인**에서 동작하는 **스마트계약**으로 구현된 유동성풀(liquidity pool)이 **거래 상대방** 역할을 수행

탈중앙 거래소(DEX)의 개념



2. AMM 도입 배경 및 작동 원리

(도입 배경)

□ 현재 **퍼블릭 블록체인** 자체의 **거래처리량 및 속도***로는 **스마트계약**을 통해 **다량의 주문**을 **오더북** 방식으로 **실시간**으로 기록·처리하는 것이 불가능

* 이더리움의 경우 블록 생성 시간에 따라 최소 10초의 처리시간이 소요

○ **오더북 방식**을 **적용**하려고 했던 **초기 탈중앙 거래소**(IDEX, EtherDelta 등)는 **느린 거래처리 속도** 등으로 인해 대중화에 실패

□ 동시에 원활한 거래 체결을 위해 필요한 **시장조성자**(market maker) 기능을 어떻게 **탈중앙화된 방식**으로 구현할 수 있는지에 대한 문제 해결 필요성도 부각

○ **금융기관**(헤지펀드 등)에 의존하지 않고 **개별 이용자들**이 **시장조성자**로 **자발적으로 참여**할 수 있는 **탈중앙화 방식**의 **거래 유동성 공급 메커니즘**을 구현할 필요

□ 2016년 **비탈릭 부테린(Vitalik Buterin)**이 예측 시장(prediction market)에 착안한 **알고리즘을 사용**하여 탈중앙화 시장조성 방안을 **최초로 제안***하였으며, 이를 계기로 **AMM** 방식의 알고리즘 기반 탈중앙 거래소가 등장

* Vitalik Buterin, "Let's run on-chain decentralized exchanges the way we run prediction markets", (Reddit 포스트, 2016.10월)

(작동 원리*)

* 자세한 내용은 「**<참고2> CP-AMM 알고리즘**」**(p.17)** 참조

□ **(매매거래)** 이용자는 **유동성풀**이 제시하는 **암호자산 교환비율(상대가격)**에 따라 언제든 두 암호자산을 **교환(매매)**할 수 있음

○ 교환비율은 유동성풀 내 두 **암호자산**의 **개수의 곱**(product)이 교환 전후 일정한 **상수**(constant)를 유지하도록 결정

<예시>

- 현재 유동성풀에 이더리움(A)이 100개, USDC(B)가 10,000개 있는 상황에서 이용자가 이더리움 2개를 팔아 USDC를 구매하는 경우
- DEX는 교환 전후의 두 자산 개수의 곱이 변하지 않도록* A 1개와 교환되는 B 개수를 196개(10,000-9,804)로 계산

  * [교환전] 100(A) * 10,000(B) = [교환후] 102(A) * X(B) ⇒ X=9,804

○ CP-AMM은 단순한 수식을 통해 실제 **시장**에서 **가격발견**(price finding) 과정에서 나타나는 **패턴***을 **근사**하여 구현한 것으로, 타 거래소에서 형성된 **가격**과 **유동성풀 가격** 간에는 **괴리**가 발생할 수 있음

* ❶ 매매 거래는 가격의 변동을 초래(예: 자산 매입시 해당 자산 가격이 상승),
❷ 개별 거래 규모가 클수록 가격 변동 확대(예: 대량 매도시 큰 폭의 가격 하락),
❸ 유동성이 풍부할수록 매매로 촉발되는 가격 변동이 축소

– 다만, 가격 격차는 동일 암호자산이 여러 거래소에서 매매되는 특성상 중앙화 거래소에서도 발생하며, **재정거래**(arbitrage)를 통해 조정됨

□ **(유동성 공급)** 특정 금융기관이 아니더라도 누구나 AMM에 원하는 만큼의 **유동성을 공급**하고, 그 대가로 **거래수수료 수익**을 얻을 수 있음

○ 유동성 공급에 참여하고자 하는 이용자들은 **기존 풀 내 비율과 동일한 비율***로 **한 쌍의 암호자산**을 **제공**(대여)

* 가령 A 100개, B 10,000개로 구성된 유동성풀에 유동성을 공급하는 경우, 1:100의 비율로 A와 B를 제공(예: A 0.01개, B 1개)

○ 이용자는 자신이 공급한 **유동성에 비례**하여 유동성풀 내에 있는 **암호자산에 대한 지분을 증명**하는 **풀 토큰**(Pool token)을 **수령**하며*,

반납시 해당 토큰을 **소각**하며, ❶ **지분율**에 따라 풀 내 **암호자산**과 ❷ 보유기간 중 누적된 **거래 수수료**(암호자산)가 지급됨

* 풀 토큰은 유동성풀에 있는 암호자산들에 대한 청구권으로 거래소의 가치와 연동된 자산이 아니며, 이와 별도로 DEX의 운영(governance)을 결정하고 수수료도 일부 수취하는 거래소 토큰을 발행·유통하는 경우가 많음. 자세한 내용은 「**<참고3> 테라-루나 교환관계와 풀토큰의 차이점」(p.20)** 참조

3. 평가 및 한계

□ **(평가)** **탈중앙 거래소**는 **스마트계약 기능**을 이용하여 **중개기관** 없이도 **이용자**가 자신이 개인지갑에 직접 보유(self-custody)한 **암호자산**을 **탈중앙화**된 방식으로 **거래**할 수 있는 가능성을 제시

○ 특히, **FTX 사태** 등에서와 같은 **운영 업체**의 **고객 자산 무단 이용**이나 **횡령** 등에 따른 이용자 피해 발생 가능성이 원천적으로 차단

□ **(한계)** 그러나 탈중앙 거래소는 ❶ **대고객서비스** 등의 측면에서 **편의성**과 **접근성**이 낮고, ❷ **탈중앙화**를 표방하더라도 이를 완벽히 **구현**하기가 어려우며, ❸ **규제 적용**이 어려워 **이용자 피해**가 발생하거나 **자금세탁** 등의 창구로 악용될 위험도 상존

① **(편의성)** 탈중앙 거래소(DEX)는 중앙화 거래소(CEX)와 같은 수준의 **대고객서비스**를 제공하기 어렵다는 점에서, 암호자산에 익숙한 일부 계층을 넘어 일반인들에게 **광범위하게 확산**되는데는 **한계**가 있음

- 특히, 이용자가 **직접 보관**(self-custody)중인 암호자산의 **개인키**를 **분실**하는 경우 이를 복원하는 것이 불가능

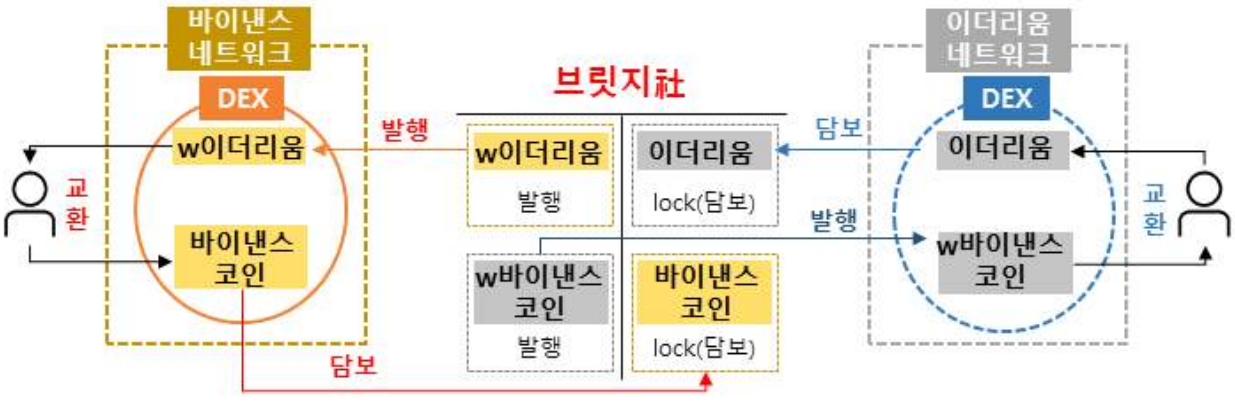
② **(불완전한 탈중앙화)** 탈중앙화를 표방하더라도 **거버넌스 구조**가 사실상 중앙화되어 있는 경우, 위기시 **유동성풀**에 있는 **자산**의 **안전성**을 보장하기 어려울 수 있음

- 상당수 블록체인 메인넷의 경우 프로토콜 의사결정 권한이 개발자와 소수 투자자 등에 집중되어 있는 사례가 많음

- 또한 스마트계약을 통한 암호자산 간의 **교환**은 **동일한 블록체인 네트워크 상에서만 가능**하기 때문에 **서로 다른 블록체인 네트워크**에 기반한 암호자산간 거래에는 **중개기관의 개입**이 불가피한데,

  해당 **중개기관**의 **건전성**이 **악화**될 경우 담보자산이 있음에도 발행된 암호자산 가격이 하락하는 등 **리스크**가 **그대로 고객에게 전이**될 위험

* 브릿지社로 불리는 기관이 자신의 책임하에 암호자산 교환을 중개하는데, 하나의 블록체인 네트워크상 암호자산을 자신의 지갑에 담보로 묶어두고(wrap), 다른 네트워크에 해당 자산의 시장가격을 추종하는 새로운 암호자산을 발행하는 방식



③ **(규제 사각지대)** 탈중앙 거래소는 분산화된 거버넌스를 갖는 **소프트웨어 프로토콜**이라는 점에서 **현행 업자(거래소) 중심**의 **암호자산 규제 체계**를 그대로 적용하기 **어려울** 수 있음

- 기존 중앙화 거래소에 적용되는 **KYC/AML 규제** 적용이 쉽지 않다는 점에서, **프라이버시**와 **익명성**이 보장되는 장점이 있으나 **범죄**나 **자금세탁** 등의 창구로 악용될 여지*

  * 다만 DEX를 통한 거래 내역은 블록체인상에 모두 기록 및 공개됨

- 중앙화 거래소와 달리 소프트웨어 **취약점** 등에 따른 **해킹** 등으로 **이용자 피해**가 발생하더라도 이를 **배상**할 **주체**도 특정하기 어려움

  * 탈중앙화된 네트워크를 기반으로 하더라도 코드에 오류가 있는 경우 해킹이 가능 (예: Osmosis 거래소 유동성풀 해킹 2022.6월)

- 중앙화 거래소 대비, ❶ 신규 암호자산 상장이 용이하고, ❷ 시세조종 행위 등의 감시가 미흡하며, ❸ 거래 유동성도 크지 않은 점에서, **선행매매**(front-running) 등 **시세조작**과 **투자유인 사기**(rug pull)에 더 취약할 수 있음

4. 전망

□ 최근 FTX 사태 등을 통해 중앙화 거래소에 대한 신뢰가 낮아진 상황에서 장기적으로 **암호자산 시장**에서 **탈중앙 거래소**의 비중이 점차 확대될 가능성

○ **탈중앙 거래소**가 짧은 시간 동안 **빠르게 발전**해 왔고, 특히 **스테이블코인** 등이 확산되는 경우 중앙화 거래소가 수행해 온 **예금**과의 **온/오프 램프 기능***의 중요성이 점차 축소

* 명목화폐를 암호자산으로 전환하는 과정을 on-ramp, 반대의 경우를 off-ramp라고 함

○ 다만 **퍼블릭 블록체인**상 **소프트웨어 프로토콜**로 운영되는 탈중앙 거래소는 **편의성**과 **안전성** 측면에서의 한계가 뚜렷하고, 그 비중이 확대될수록 **정책당국**의 **견제**도 커질 것이라는 점에서 기존 **중앙화 거래소**를 전면 대체하기는 쉽지 않을 전망

- 반면 **중앙화 거래소**들의 경우 **규제**가 **강화**되고 **예탁 및 결제 인프라**가 갖춰짐에 따라 **리스크**가 **점차 분산**되고 **고객 자금 전용** 등의 문제가 발생할 소지도 줄어들 것으로 기대됨

V 당행 디지털 화폐 관련 업무에의 시사점

1. CBDC의 국가간 지급결제

□ 향후 AMM 알고리즘은 암호자산 거래를 넘어 CBDC를 활용한 국가간 지급 프로젝트에 외국환거래 유동성 공급 메커니즘으로 적용될 가능성

○ BIS 혁신허브(스위스, 싱가포르, 유로시스템 센터)에서는 AMM이 향후 암호자산 생태계의 핵심 요소가 될 수 있다고 평가하고,

다수의 이종 통화 CBDC를 연계하여 국가간 지급결제에 활용시 원활한 유동성 공급 메커니즘으로 AMM의 적용 가능성을 연구하는 공동 프로젝트*(Project Mariana)를 진행할 예정(2022.10월)

* CP-AMM를 활용한 JP Morgan, MAS, BdF의 공동 프로젝트(Liquidity Management in a Multi-Currency Corridor Network, 2021.11)에 기반

○ 한편, 금년중 당행 참가 예정인 Dunbar 프로젝트에서도 외환 유동성 공급을 자동화하는 방식*으로 AMM을 적용하는 방안을 고려 중

* 이외에 ① 참가자 간 직접 거래(OTC), ② 플랫폼 참가자 중 시장조성자를 지정, ③ 플랫폼 외 외환시장과 연계(oracle) 등을 고려

2. 디지털 자산 보관 및 결제 인프라

□ 향후 AMM 등의 스마트계약 기술은 미래 디지털 경제를 뒷받침하는 지급결제 인프라의 한 축으로 자리잡을 가능성

○ 향후 암호자산과 NFT 뿐 아니라 증권, 부동산, 미술품, 저작권 등 다양한 자산이 토큰화(tokenization)되어 유통될 가능성이 증대

○ 개인이 직접 보관(self-custody)하는 토큰 자산에 대한 대안적 거래 및 시장조성 메커니즘으로서 AMM 기반의 스마트계약을 활용하는 방안을 고려*

* 미술품 등 토큰을 ❶ 현행 증권예탁제도와 유사하게 예탁결제원 등 기존 기관 활용 또는 신설 등을 통해 일원화하여 관리하는 방안, ❷ 현재 부동산 투자 플랫폼과 같이 발행 주관사가 집중 관리하는 방안을 고려할 수 있겠으나, ❸ AMM 등 스마트계약을 활용시 별도 예탁 없이도 결제가 가능할 수 있음

- AMM 활용시 발행사나 특정 금융기관에 의존하지 않고도 토큰 보유자가 자발적으로 거래 유동성 공급에 참여하고 수수료 수익을 얻을 수 있어, 2차 시장의 거래 유동성 공급을 늘리고 투명성도 제고할 수 있음

3. 스테이블코인의 거시경제적 영향 확대

□ 향후 탈중앙 거래소는 **달러화 스테이블코인**이 **유출입**하는 **경로**가 될 가능성이 있으므로, 이에 따른 **거시경제적 영향**에 **유의**할 필요

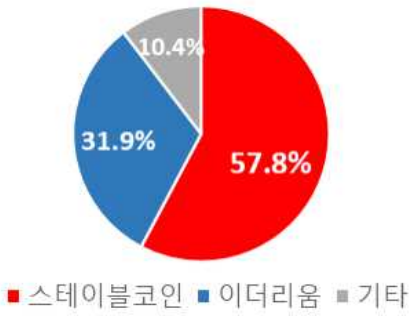
○ 아직 국내 암호자산 거래소들은 암호자산 거래시 스테이블코인을 취급하지 않고 있으나, 탈중앙 거래소들의 경우 주요 **스테이블코인을 결제 자산**으로 활용하며 특히 **달러화 스테이블코인**이 큰 비중을 차지

Uniswap 상위 7개 유동성풀[1)]

유동성풀 페어	규모(백만달러)
1) DAI/USDC	437.7
2) USDC/ETH	369.8
3) wBTC/ETH	252.7
4) USDC/USDT	111.6
5) FRAX/USDC	105.1
6) USDC/USDM	101.7
7) ETH/USDT	60.0

주: 1) 파란색=스테이블 코인
출처: Uniswap(2022.12.7.)

Uniswap 유동성풀 상위 10개 토큰의 종류



출처: Uniswap(2022.12.7.)

○ 향후 **규제**가 **정비**되고 **원화 스테이블코인**이 **발행**되는 등 스테이블코인 이용이 확산되는 경우 규제* 적용이 어려운 **탈중앙 거래소**를 통한 **달러화 스테이블코인** 국내 유출입이 증가할 가능성

* 일본 금융청은 자금결제법 개정(2022.6월), 동법 가이드라인 발표(2022.12월)를 통해 스테이블코인 규제를 구체화하면서 해외 발행 스테이블코인 송금을 허용하되 한도 등을 제한할 방침

□ 탈중앙 거래소를 통한 **달러화 스테이블코인 유출입 동향** 및 이 과정에서 형성될 수 있는 **이중 환율** 등을 효과적으로 **모니터링**하기 위한 방안을 마련할 필요

<참고1>

전통적인 거래소에서 시장조성자의 역할

□ 중앙화 거래소에서 **시장조성자**는 유동성 공급의무가 있는 종목(시장조성 대상종목)에 대해 **매수·매도 양방향 호가**를 제출함으로써 **스프레드**를 특정 수준 이내로 **유지**할 **의무***를 지며, 주로 **대형 금융기관**이 담당

* 동 방식을 **호가주도형**(quote-driven)이라 부르며 미국, 영국, 독일 등의 주요 주식거래소는 호가주도형 혹은 혼합형 방식을 따름

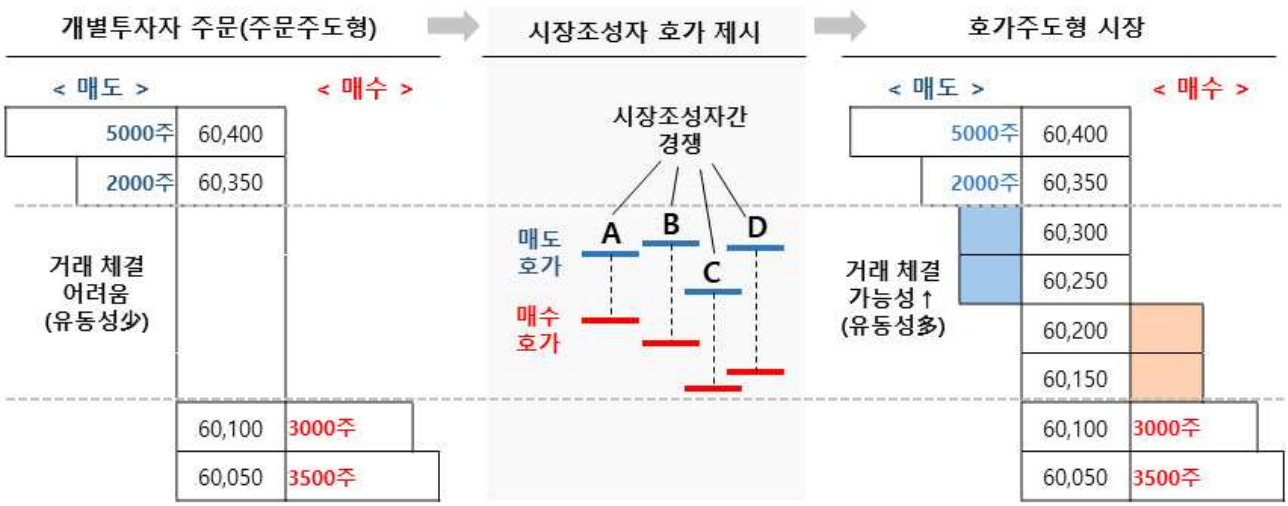
- ㅇ 양방향 거래가 모두 체결될 경우 스프레드를 수익으로 수취하고, 한쪽 거래만 체결된 경우 **다른 시장**에서 **반대 매매를 수행**(예: 공매도, 파생시장 활용)

- ㅇ 시장조성자는 '(bid-ask 스프레드) X 거래량'을 수익으로 확보하며, 안전한 무위험 포지션 구축을 위해서는 현물(spot) 시장과 연계된 파생상품 시장 등이 필요

□ 시장조성자는 유동성 공급을 통해 거래소의 가격발견(price finding)을 촉진할 뿐만 아니라, **일시적인 가격 급변동을 완화**(가격연속성 제고)하고 **거래 비용을 줄여**주는(스프레드 축소) 등 **순기능**을 수행

- ㅇ 다만, 일부 시장조성자는 스프레드가 아닌 시세조종을 통한 자본이득 추구한다는 의혹도 제기됨

시장조성자의 시장조성 과정



<참고2>

CP-AMM 알고리즘

□ **(개요)** 현재 대부분(약 80%)의 탈중앙 거래소가 CP-AMM(Constant Product Automated Market Maker) 알고리즘을 사용하고 있음

○ CP-AMM 알고리즘 : $\mathbf{Q_{암호자산1}}$ **X** $\mathbf{Q_{암호자산2}}$ **= C** (Constant)

— ($Q_{암호자산1}$, $Q_{암호자산2}$)는 당시 시가에 따라 유동성풀(liquidity pool) 내의 두 자산의 가치가 동일하도록 하는 암호자산 수량이며, 이의 곱으로 C가 결정됨

► (예) 이용자가 「암호자산1 & 암호자산2」 풀을 만들고자 하는 경우,

$$P_{암호자산1} \text{ X } \mathbf{Q_{암호자산1}} = P_{암호자산2} \text{ X } \mathbf{Q_{암호자산2}}$$

가 되도록 하는 한 쌍의 ($Q_{암호자산1}$, $Q_{암호자산2}$)를 제공(스마트계약)하여 최초의 유동성풀을 생성하고 C를 결정*

* 기존에 존재하던 풀에 **유동성**이 **추가**되거나 **회수**될 때는 **C가 변화**

— **암호자산1의 상대가격**은 $\mathbf{Q_{암호자산2}} \div \mathbf{Q_{암호자산1}}$가 되며, 동 조건하에 거래자가 **암호자산1**을 **매수**하는 경우 매수자는 **C를 고정시키는 수량**의 **암호자산2**를 대가로 풀에 **지불** ($\mathbf{Q_{암호자산1}} \downarrow$ X $\mathbf{Q_{암호자산2}} \uparrow$ = **C 고정**)

□ **(예시)** (P_{ETH}, P_{USDC}) = ($100, $1)일 때 이용자가 ($Q_{ETH}$, Q_{USDC}) = (100, 10,000) 유동성풀을 만든 경우

(최초)	ETH	USDC	c
시장가격(P)	$100	$1	-
풀내수량(Q)	100	10,000	1,000,000
거래소 가격 (교환 수량)	100USDC (=$100)	0.01ETH (=$1)	-
자산 가치	$10,000	$10,000	$20,000(=합계)

* ETH: 이더리움, USDC: USD Coin (스테이블코인)

① **(매매거래와 slippage*)** 매수 수량이 많을수록 당초 가격보다 높은 매수가를 지불

* 주문 가격과 실제 체결 가격 간 차이로 유동성 대비 거래량이 크면 언제나 발생하며, 주식 시장 등에서는 이를 계산하는 것이 복잡한 반면, AMM은 거래 규모에 따라 단순하게 계산됨

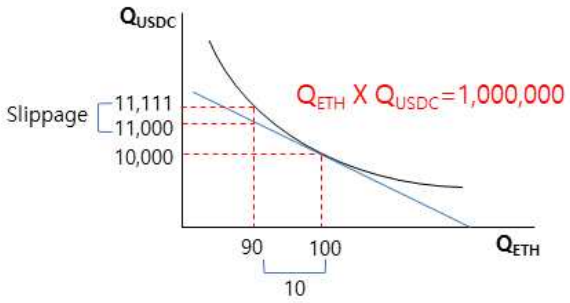
► 최초 상태에서 ETH 10개를 매수하는 경우,

→ t=0에서의 당초 가격 = 10개 X 100 USDC = 1,000 USDC = **$1,000**

→ 매수 실행시 CP-AMM에 의한 실제 지불가격 = 1,111 USDC = **$1,111**

* CP-AMM 알고리즘: (100-10) X (10,000+**1,111**) = 1,000,000

→ $111의 slippage 발생



— 유동성(pool size)이 풍부할수록 slippage가 작아지고, 소수 투자자의 시세조종 가능성이 줄어듦

▸ 최초 상태에서 신규 유동성 공급자가 (Q_{ETH}, Q_{USDC}) = (25, 2500) 만큼을 추가 공급하고, 이후 ETH 10개 매수가 일어나는 경우

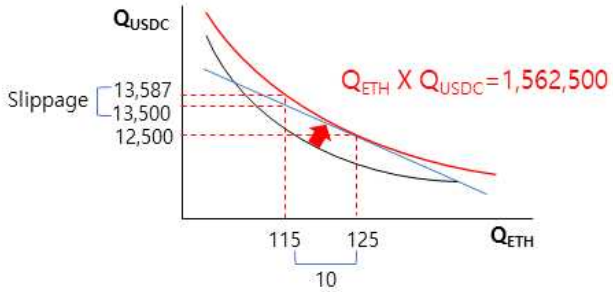
→ C가 바뀜 (1,000,000 -> 1,562,500 = 125 X 12,500)

→ 당초 가격 = 10개 X 100 USDC = 1,000 USDC = **$1,000**

→ 매수 실행시 CP-AMM에 의한 실제 지불가격 = 1,087 USDC = **$1,087**

* CP-AMM 알고리즘: (125-10) X (12,500+**1,087**) = 1,562,500

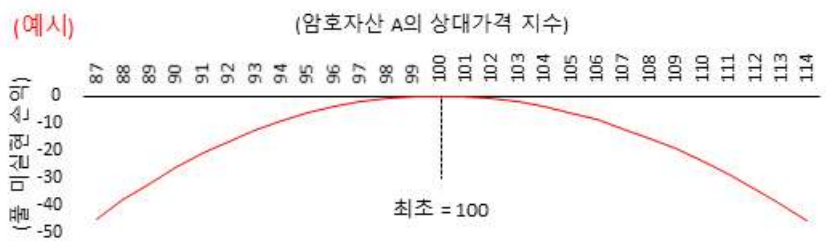
→ $87의 slippage 발생



② **(재정거래 과정 및 유동성 공급자의 손익)** 시장가격과 풀 가격 간의 괴리가 발생할 경우 재정거래 목적의 매매 거래가 이루어지고, 이 경우 유동성 공급자에게는 비영구적 손실*(=Impermenant loss or Divergence loss)이 발생

* 암호자산을 보유하는 대신 유동성풀에 공급함으로써 유동성풀 잔여 암호자산의 상대 수량이 변함에 따라 발생하는 미실현 손실

— 유동성풀은 재정거래를 받아줄 때마다 상대가격이 높은 암호자산의 수량은 줄어들고 상대가격이 낮은 자산의 수량은 늘어나기 때문



— 다만, 알고리즘에 의해 매수량이 증가할수록 매수 가격이 상승하므로 재정거래 가능 수량에는 제한이 있어 비영구적 손실 규모가 제한

► 최초 상태에서 ETH의 외부 거래소 등 가격이 $120으로 상승한 경우

→ 탈중앙 거래소의 가격은 $100(=USDC 100개)이므로 ETH를 매수하여 무위험수익을 올리려는 재정거래 유인이 발생

→ 다만, CP-AMM에 의해 매수 수량이 9개를 초과할경우 $120보다 비싼 값을 지불해야 하므로 9개까지만 거래가 발생

* i) [Constant 조건] (100-A) X (10,000+B) = 1,000,000
ii) [가격 조건] (10,000+B) ÷ (100-A) = 120을 풀면,
A=9, B=954이므로, ETH는 최대 9개를 매수할 수 있으며 대가로 USDC 954개를 지불 (소수점 이하 반올림, A=8.71, B=954.46)

ETH 재정거래시 투자자 이익

	기대 손익	실제 손익	slippage
수익	9개 X $120 = $1,080	9개 X $120 = $1,080	-
비용	9개 X $100 = $900	954개 X $1 = $954	
이익	$180	**$126**	$54

유동성 공급자(100% 소유 가정)**의 비영구적 손실**

	(가정) 풀에 투자하지 않고 보유하고 있었을 경우			(실제) 풀에 유동성을 공급한 경우			비영구적 손실
	ETH	USDC	합계	ETH	USDC	합계	
수량	100	10,000	-	91	10,954	-	-
가격	120	1		120	1		
가치	12,000	10,000	**22,000**	10,954	10,954	**21,909**	**-91**

— 유동성 공급자는 시가가 최초 공급 당시 가격수준에서 벗어날 때마다 미실현 손실에 노출되나, CP-AMM에 의해 손실 규모가 제한되고 거래 수수료를 통해 이를 만회 가능

<참고3>

테라-루나 교환관계와 풀 토큰(pool token)의 차이

□ 스테이블코인인 테라의 가치를 유지하는 알고리즘의 핵심은 언제나 $1 가치의 루나 토큰*과 테라를 교환할 수 있다는 데 있음

* 테라 에코시스템 활용 정도에 따라 수수료를 수취하고 가격이 변하는 거버넌스 토큰

① $1를 유지해야 하는 테라의 가치가 $1 밑으로 하락할 경우(침체기)

→ 테라를 프로그램에 지급하고 $1 상당의 루나를 받으려는 수요가 발생
→ 테라의 수 감소 → 테라 가격 $1 복귀
→ 루나 발행 증가로 가치 하락
(루나 토큰 가격의 상승을 주요 보상으로 하는 채굴자들의 손실)

② 테라의 가치가 $1 위로 상승할 경우(호황기)

→ $1 상당의 루나를 프로그램에 지급하고 테라를 받으려는 수요 발생
→ 테라의 수 증가 → 테라 가격 $1 복귀
→ 프로그램이 모집된 루나를 소각하여 루나 가격을 지지
(침체기 채굴자들의 손실을 보상)

□ 테라의 가치를 보장하는 역할을 하는 **루나 토큰이 전적으로 테라 생태계의 가치에 연동**되어 있어 사실상 자기가 자신을 보장

ㅇ 따라서 침체기에 채굴자들이 기회비용을 장기간 감당하기 어려우며*, 큰 규모의 외부 자금 유입과 인출에 대항하여 안정적인 가치를 유지하기 어려움

* 테라 가격 지속 하락 → 루나로의 교환 수요 증가
→ 발행량 증가로 루나 가치 하락
→ 채굴자의 수익성 및 채굴 유인 하락, 기회비용 증가 → 채굴자 이탈
→ 테라 네트워크 기능 하락 → 테라 유용성 하락
→ 테라 가격 하락

□ 반면 풀 토큰이 보장하는 것은 **거래소와 관계없는 토큰에 대한 청구권**이므로 거래소의 수익성 악화가 청구권의 가치에 영향을 미치지 않음

ㅇ 거래소와 관계없이 유동성풀에 공급한 두 종류의 암호자산 가격이 모두 하락할 때에만 풀토큰이 보장하는 청구권의 가치가 하락(비영구적손실 제외)

<참고문헌>

법무부·금융위원회 (2019),「전자증권제도 및 법령 주요 내용」

한국거래소 (2020),「시장조성자 제도개선 기본방향」

한국예탁결제원 (2020),「주식 전자등록 발행회사 업무 안내」

한국은행 (2014),「한국의 지급결제제도」

Altschuler, Samantha (2022),「SHOULD CENTRALIZED EXCHANGE REGULATIONS APPLY TO CRYPTOCURRENCY PROTOCOLS?」

FRB New York (2022),「Can Decentralized Finance Provide More Protection for Crypto Investors?」

Lehar, Alfred. and Parlour, Christine (2022),「Decentralized Exchanges」

___ (2022),「Systemic fragility in decentralized markets」, BIS Working Papers No 1062

O'Neill, Peter (2022),「Can Markets be Fully Automated? Evidence from an "Automated Market Maker"」