Hyperindex

1. DEX
2. Institution(기관)의 역할: 유동성 풀을 공급해주는 역할을 한다. 우리에게 index 발행을 요구하고, 발행을 위한 자금을 대주고 차익거래를 실현하는 역할이다.
3. AMM xy=k 방식으로 지정가없이 시장가로 거래가 체결되게 하는 시스템
4. 풀의 개념: 스마트컨트랙트 안에 잠겨 있는 토큰들의 모음. 풀 안의 자산을 통해 swap이 이루어진다. CEX 오더북 없이 거래가 가능하다. 그리고 AMM을 운영한다.

예를 들어 이더/테더 풀이라고 하면 테더는 스테이블이라서 고정이고, 이더수량X테더수량=총유동성 식이 성립하는데, 이더수량이 적어지면 가격이 높아짐.

1. 하이브리드 DEX를 사용하면 매도호가보다 낮은 가격에서는 시장가, 같은 가격에서는 매도호가, 그 수량이 끝나면 다시 시장가를 적용함으로써 슬리피지를 최소화할 수 있고, 오프체인 주문을 활용해 빠른 거래체결이 가능하다. 하지만 오프체인에 대한 보안상의 문제가 발생한다는 단점이 존재한다.
2. DEX의 경우 블록체인네트워크를 사용하기 때문에 사용자는 네트워크에 가스비를 내야 함.
3. About Token and Coin(CEX like Binance)
4. Order Book : 피파에서 매수랑 매도 칸이랑 같은거임. 매수호가>=매도호가일 경우 거래체결 블록체인에 기록되지 않고 DB에 기록됨.
5. 체인에 기록되는 거는 only 입출금 트랜잭션 뿐이다.
6. DEX의 경우 스마트컨트랙트 풀만 만들 수 있다면, 누구나 코인이나 토큰을 상장할 수 있다.
7. CEX 사용자는 가스비+수수료를 내는 DEX 사용자와 달리 수수료만 지불하면 된다.
8. What is Token
9. 다른 블록체인 위에서 발행된 가상화폐
10. 같은 이름의 토큰이 여러 네트워크에서 발행될 수 있음. 예를 들면 테더는 이더리움이나 BNB네트워크 위에서 발행되고 있음.
11. 토큰은 네이티브코인 블록체인 위에 거래기록이 저장됨. -> 가스비 지불(네이티브코인형태)
12. 발행원리: 퍼블릭 블록체인 위에 스마트컨트랙트 코드를 올리고 mint 함수 실행
13. 블록체인과 비트코인
14. 개요: 2008 리먼브라더스로 중앙집권형 거래시스템에 대한 불신이 생김 -> P2P 거래 수요
15. 비트코인: 신뢰할 수 있는 제 3자 없이 P2P거래를 가능하게 함
16. 블록체인
17. 블록: 거래내역이 적힌 장부 한 장 -> 암호화되어 시간순으로 연결된 게 블록체인임

블록은 정보를 가지고 있는 헤더와 블록의 내용을 가지고 있는 바디로 구성됨.

헤더: 블록의 요약, 주소표. 블록 자체의 정보와 다음 블록을 잇는 역할

바디: 실제 트랙잭션 데이터

1. 합의알고리즘 중 작업증명(PoW): 블록을 연결하기 위한 암호풀이 과정을 말함. 채굴이라고 함

새로운 블록을 생성해서 연결하기 위해선 해시값 <= 목표값. 이를 만족하는 값을 찾으면

채굴 성공. 해시값은 다음 블록에 연동됨.

거래내역을 위조하려면 연결되어있는 모든 블록의 암호값을 찾아내고 이를 타 채굴자보다 빠르고 길게 블록을 연결해야 하기 때문임. 이를 위해서는 전체 컴퓨팅자원 중 51% 이상이 필요해 사실상 거래기록의 위조가 불가능하다.

채굴을 한 사람에게는 그에 대한 보상으로 비트코인을 받고, 이것이 비트코인이 발행되는 원리임. (제네시스블록 채굴에 대한 보상은 경제적가치가 없음)

1. Cross chain messaging: 서로 다른 블록체인 네트워크가 데이터나 명령을 주고받을 수 있게 하는 기술
2. LP토큰: DEX에 유동성을 제공한 자에게 주어지는 지분 증서. 이를 반환하면 그 비율만큼 풀 안의 자산을 돌려주고, 거래 수수료 수익도 받을 수 있음. 🡪 소각됐다면 러그풀 위험이 상대적으로 낮다고 판단할 수 있음
3. Staking: 네이티브 코인이나 토큰을 네트워크나 프로토콜에 예치해서 그 대가로 보상을 받는 행위. 네이티브 스테이킹, 유동성 스테이킹, 거버넌스 스테이킹, 이자형 스테이킹 등이 있음. 하지만 락업(예치기가 중 자금인출불가), 가격변동리스크, 스마트컨트랙트 리스크(해킹이나 버그로 자산손실 가능) 등 위험 존재.
4. 러그풀 위험: 개발팀이나 발행자가 투자자 자금을 들고 잠적하거나 유동성을 빼서 프로젝트를 붕괴시키는 행위.
5. 종류
6. 유동성 인출형: DEX 유동성 풀에서 팀이 LP토큰을 전부 빼서 토큰 거래불가 상태로 만듦 🡪 토큰가격 폭락
7. 스마트컨트랙트 조작형: 발행자가 무제한 민팅, 전송 제한, 숏 불가 등 사기요소를 스마트컨트랙트에 넣음
8. 프로젝트 포기형: 초기 판매 후 갑자기 사라짐.
9. 예방 방법
10. LP Lock 여부 확인: vesting
11. 스마트컨트랙트 감사(Audit) 결과 확인
12. 팀 신원(KYC) 공개 여부
13. 토큰의 Owner 권한 범위 확인 (mint, burn, tax 조작 가능 여부)
14. 과도한 유인에 주의
15. TAM, SAM, SOM
16. TAM(Total Adressable Market): 기업이 목표로 하는 전체 시장 규모. 이론적으로 가장 큰 시장.
17. SAM (Serviceable Adressable Market): 유효 시장 규모 . TAM 중에서 실제로 우리 비즈니스가 제공 가능한 시장. 그중 우리가 도달할 수 있는 현실적 시장.
18. SOM (Serviceable Obtainable Market): 수익 시장 규모 . SAM 중에서 실제로 우리가 차지할 수 있는 시장 (점유율로 생각하면 편함)
19. EVM(Ethereum Virtual Machine) 이더리움 블록체인의 두뇌

* 이더리움 네트워크에서 스마트컨트랙트를 실행하고 트랜잭션을 처리하는 추상적인 컴퓨팅 환경
* 개발자가 작성한 코드를 EVM 바이트코드로 바꿔서 실행함
* 스마트컨트랙트를 실행, 네트워크 전체의 일관성 보장, 가스 계산
* 블록체인이 세계적으로 공유된 컴퓨터라고 하면 EVM=CPU, 스마트 컨트랙트=프로그램, 가스=전기세 임

1. SQL(Structured Query Langauge): 구조적 질의 언어

* 관계형 데이터베이스 (RDBMS)에서 데이터를 조회, 삽입, 수정, 삭제하는 표준 언어
* 대부분의 DB에서 사용됨
* Select, Insert, Update, Delete 등

1. 타임스탬프: 거래나 블록이 발생한 정확한 시각을 기록한 정보

* 거래소/마켓 타임스탬프: 거래소에서 매수 매도 체결된 시점 기록
* 주문 데이터도 다 타임스탬프 단위로 묶임.

1. 개별 트랜잭션: 스마트컨트랙트 함수를 호출한 결과 🡪 트랜잭션 해시로 조회 가능
2. 기본 함수들 (ERC-20)

* Transfer: 단순 송금
* Approve: 내가 가진 토큰을 다른 컨트랙트가 대신 쓸 수 있도록 권한을 줌

1. 유동성 관련

* addLiquidity: 내가 가진 두 개의 토큰을 풀에 넣어 유동성을 공급 🡪 LP토큰 받음
* removeLiquidity: LP 토큰을 반환하고 원래 넣었던 토큰과 수수료 수익을 돌려받음
* swapExactTokensForTokens: 지정한 양의 토큰을 다른 토큰으로 교환

1. 예치/대출

* deposit: 특정 자산을 프로토콜에 예치 🡪 상응하는 예치 증서를 받음
* withdraw: 예치했던 자산을 인출
* borrow: 담보를 맡긴 후 다른 자산을 빌림
* repay: 빌린 자산을 갚음

1. 스테이킹

* stake: 토큰을 스테이킹 계약에 예치, 보상을 받을 권리 획득
* unstake: 스테이킹했던 토큰을 회수
* claimRewads():쌓여있던 보상 토큰을 수령

1. 그외

* mint: 새로운 토큰 발행
* burn: 토큰 소각
* Yv6gfILatR0CI9696g1elvPkgEWjAZ0K

1. TVL(Total Value Locked): 특정 디파이 프로젝트의 스마트 컨트랙트에 사용자들이 예치하고 묶어둔(Locked) 모든 디지털 자산의 총 가치를 미국 달러로 환산한 금액= 예치된 자산의 개수X현재 가격

* 유동성 공급: 덱스에서 자산을 맡기는것도 TVL에 포함됨
* 스테이킹: 네트워크의 안정성을 위해 자신의 코인을 맡기고 이자를 받음
* 랜딩(Lending): 다른 사람이 자산을 빌려갈 수 있도록 내 자산을 담보로 맡기고 이자를 받는 행위
* 높을수록 신뢰도와 인기가 높고, 유동성 수준이 높다.
* 신규발행 밈코인이 상장된 LP의 TVL은 코인의 초기 자본금이자 신뢰도를 의미함.
* DEX의 TVL: 유니스왑(ETH)이나 레이디움(SOL)같은 덱스 자체 TVL은 그 플랫폼의 안정성과 신뢰성을 나타냄
* 높은 이자율(APY)로 사용자를 유인해 단기간에 TVL을 부풀리는 프로젝트도 있음

1. 소스코드(Source Code): python, java 등에 프로그래밍언어를 사용해서 컴퓨터에게 시킬 일을 적어놓은 명령서

- 토큰 컨트랙트의 소스코드를 확인하는 것은 깜깜이 투자를 피하고, 숨겨진 위험을 찾아내며, 프로젝트의 신뢰도를 직접 검증하기 위한 필수적인 과정

- 이더스캔(Etherscan) 같은 블록체인 탐색기에 올라온 소스코드가 실제로 블록체인에 배포된 프로그램(바이트코드)과 100% 동일하다는 것을 공식적으로 인증받는 절차

1. 팀 멀티시그: M of N 방식으로, 공동성명이 있어야 코인이 전송되는 지갑. ‘
2. Base / Polygon / Arbitrum / Optimism : 이더리움을 더 빠르고 싸게 쓰게 해주는 확장 네트워크
3. EOA와 컨트랙트 계정

* EOA (Externally Owned Account): 개인 지갑 🡪 우리가 흔히 쓰는 메타마스크 같은 개인 지갑 🡪 개인 키가 있어야만 제어할 수 있음. 주인이 사람임
* 컨트랙트 계정: 코드로 작동하는 로봇 지갑 🡪 스마트 컨트랙트가 배포되면 생기는 계정 🡪 개인키가 없고 미리 짜인 코드 규칙에 따라서만 작동. 주인이 코드임.

1. Proxy, ProxyAdmin, Owner

* Proxy: 스마트 컨트랙트를 업그레이드 할 수 있게 해주는 기술. 바꿀 수 없는 블록체인의 특성 때문에 로직을 수정해야 할 때를 대비해 사용.
* ProxyAdmin/ Owner: 프록시 권한을 가진 관리자. EOA일 수도 있고 멀티시그(팀)일 수도 있음. 이것이 누구에게 있느냐가 보안의 핵심.

1. eth\_getCode: EVM에 내리는 명령어. 특정 주소에 혹시 코드가 저장되어 있는지 확인하는 역할

* 결과가 0x (비어 있음) 🡪 코드가 없네? 🡪 EOA
* 결과가 0x…. (긴 코드) 🡪 코드가 있네? 🡪 컨트랙트 계정

1. 트레저리(Treasury): 프로젝트가 보유한 공식적인 자금 = 프로젝트의 금고. 발행한 자체 토큰, 투자금으로 받은 스테이블 코인, 이더리움 등이 들어있음.

* 풀을 만들 때 보통 트레저리에 있는 자금을 사용하는데, 이때 LP를 소각하면 투입한 트레저리의 자산을 영원히 회수할 수 없게 된다. 그렇기에 러그풀 위험이 확 줄어들게 되는 것임. 🡪 소각하면 텔그에 알리고 그럼.

1. 브리지/라우터 (Bridge/Router) : 다른 블록체인으로 이사 가려고 잠시 환승센터에 맡겨둔 물량

* ETH 체인의 토큰을 BNB 체인으로 옮기는 것이 예시. 서로 다른 블록체인 간에 자산을 이동시켜주는 서비스 (브리지)에 예치된 토큰. 이동이 완료되기 전까지는 특정 주소에 묶여있어서 거래 불가.

1. 거래소 커스터디/ 프로토콜 트레저리: 회사 금고나 거래소의 대형 창고에 보관된 물량

* 거래소 커스터디: 바이낸스, 업비트 같은 대형 거래소가 고객 자산을 보관하기 위해 가진 지갑(핫월렛/콜드월렛)의 물량
* 프로토콜 트레저리: 위에서 설명함.

1. 컨트랙트 배포자(Deployer): 스마트 컨트랙트를 블록체인에 처음 올린 사람(주소). 절대 바꿀 수 없음.
2. Verified 소스 / ABI

* Verified 소스: 프로젝트 팀이 블록체인 탐색기에 공개한 인증된 소스 코드. 실행되고 있는 코드와 100% 일치함을 보장하는 공개된 설계도.
* ABI (Application Binary Interface): 컨트랙트와 소통하기 위한 사용 설명서. 어떤 함수를 가지고 있는지 목록을 알려줌.

1. EIP-1967 슬롯: 업그레이드 가능한 프록시 컨트랙트를 위한 표준화된 보관함 주소.

* 정해진 위치(슬롯)에 실제 로직 컨트랙트의 주소와 관리자 주소를 저장한다.