토큰 신뢰도 결정방법

1. 엔티티 클러스터링(Entity Clustering): 여러 개의 다른 지갑 주소들을 하나의 동일한 주체로 묶어내는 온체인 기법
2. 자금 출처 동일성의 법칙 (The Golden Rule)
3. 분석 대상 지갑(A)을 블록 탐색기 (Etherscan 등)에서 찾는다
4. A의 첫번째 트랜잭션을 찾는다. 보통 외부에서 ETH을 소량 수혈받은 것임
5. 자금 출처 지갑(B) 을 클릭
6. B의 전체 거래 내역을 봄
7. B가 A뿐만 아니라 비슷한 시기에 C, D, E 등 다른 여러 지갑에도 똑같이 소량의 이더를 보냈다. 그러면 A, B, C, D, E… 은 하나의 엔티티
8. 심화 버전: 거래소 출금 패턴 🡪 하나의 주체가 CEX에서 여러 개인 지갑으로 동시출금하는 경우도 많음. 이 경우도 하나의 엔티티로 봐야 함
9. 자금 목적지 동일성의 법칙: 여러 지갑이 각자 활동을 마친 후 수익금이나 자산을 동일한 하나의 지갑으로 모음
10. 의심스러운 지갑 A, B, C의 활동을 추척
11. 이들이 특정 토큰을 매도하거나 이자를 받은 뒤 그 수익을 어디로 보내는지 확인
12. 만일 이들이 같은 마스터 지갑 D에 자금을 집결시키면 이들은 D의 통제를 받는 하나의 클러스터
13. 동일 행동 패턴 분석(Coordinated Action): 여러 지갑이 인간이라고 보기 힘든 수준으로 똑같은 행동을 동시에 할 때 하나의 클러스터로 의심

* 동시 매수/매도: 잘 알려지지 않은 특정토큰을 같은블록 or 몇 초 차이로 동시매매
* 동일 디앱활동: 새로운 디파이 프로토콜이 출시됐을때 여러 지갑이 동시에 같은 금액을 예치하거나 동일자산을 대출함
* 동일한 가스비 설정: 항상 똑같은 gwei를 사용하거나, 똑같은 고급 설정을 사용하는 등

1. Top Holders: 상위 지갑에 공급량이 얼마나 몰려 있는지 (시장집중률지수와 비슷? 허핀달지수 사용해볼까?)
2. TH10<=40
3. NHHI (정규화허핀달지수)

🡪 0에 가까우면 완전균등& 1에 가까우면 지갑 독점 🡪 정규화할 수 있어서 보다 객관적으로 집중도를 판단할 수 있을 것으로 보임.

1. 제외 대상:
2. **번(burn) 주소 / 소각 지갑**
   1. 이유: 영구 유통 불가.
   2. 규칙: 0x000…dead, 체인별 소각 패턴 전부 **완전 제외**.
3. **LP 락(유동성 잠금) 계약**
   1. 이유: 락 기간 중 실매도 불가.
   2. 규칙: TeamFinance/Unicrypt/투명한 타임락 계약으로 **락 기간 남은 물량은 제외**.
   3. 예외: 락 해제 직전(예: 7~14일 이내) 물량은 **민감도 체크**용으로 별도 표기.
4. **팀/어드바이저 베스팅 락(타임락)**
   1. 이유: 베스팅 이전에는 유통 불가.
   2. 규칙: **베스팅 미도래분 제외**, 이미 풀린 물량은 포함.
5. **거래소·커스터디(콜드/핫월렛)**
   1. 이유: ‘실제 소유자 다수의 **패스스루** 보관 지갑’이라 집중도 왜곡.
   2. 규칙: **원칙적 제외 또는 별도 버킷**. (가능하면 예치인 엔티티로 재배분, 불가 시 제외)
6. **브리지·라우터(跨체인 래핑)**
   1. 이유: 기술적 에스크로.
   2. 규칙: **브리지 컨트랙트 자체 제외**, 반대 체인의 랩드 토큰 쪽에서 보유자 집계.
7. **스테이킹/리워드 풀(스마트컨트랙트)**
   1. 이유: 컨트랙트 지갑이 점유자로 잡히면 집중도 과대평가.
   2. 규칙: **풀 주소 제외**하고, 가능하면 **언스테이킹 가정**으로 개별 스테이커로 분해(데이터 가능할 때). 불가 시 “Staking bucket”으로 별도 집계(점수화 때 패널티/보정).
8. **프로토콜 트레저리(거버넌스 멀티시그)**
   1. 이유: 즉시 매도 위험 낮음(정책적 의사결정 필요).
   2. 규칙: **멀티시그+타임락 확인되면 제외 또는 낮은 가중치**. (권한 느슨·무기한 현금화 가능이면 일부 포함)
9. **더스트/에어드롭 스팸**
   1. 이유: 지갑 수만 늘려 HHI를 인위적으로 낮춤.
   2. 규칙: **하한치 컷**(예: 유통의 0.01% 미만 또는 미화 $X 미만은 합산 버킷으로 처리).

정리: **Free-float(실제로 유통 가능한 물량)** = 총발행 − (소각 + 락/베스팅 + 브리지/라우터 + 스테이킹풀 + 트레저리(조건부) + CEX 보관(조건부)).

1. 보정해야 할 것들:
2. Entity resolution: 같은 주체의 다지갑을 하나의 엔티티로 합산
3. 공식 정리
4. **지갑 I 점유율**

7. 결론: NHHI로 score 계산하고 난 뒤에 TH10 및 다른 보정사항들 참고하여 최종 score 계산해서 판단하면 될 것 같다는 생각.
8. Dev Holdings: 개발자들이 가지고 있는 토큰 지분 🡪 비율이 과도하게 높으면 중앙화 + 덤핑&러그풀위험 존재

가중치 20퍼정도? 러그풀때문에

1. 범위: Deployer/팀 멀티시그, 베스팅/에스크로 계약
2. Deployer: 토큰

* 컨트랙트를 배포한 지갑.
* 블록 탐색기(Etherscan 등) **Contract Creator / Deployer** 항목에 표시.

1. 팀 멀티시그 (Team Multisig) -> 공식 문서 확인은 자동화 어려움. 블록체인 탐색기 활용

* 여러 명이 공동 서명해야 쓰는 다중서명 지갑(예: 3/5 Gnosis Safe).
* 한 사람이 임의로 자금/권한을 못 움직임 → 거버넌스 안전장치.
* 지갑 타입이 Safe(Gnosis) 등으로 표시, 설정에서 threshold(예: 3 of 5) 확인.

1. 트레저리 지갑 (Treasury)

* 프로젝트 자금·준비금 보관 지갑(운영·개발·MM 비용 등).
* 대량 물량 보유. 규율 없이 매도하면 가격충격.
* 팀 문서/공지 라벨, 멀티시그로 운영되는지, 지출 패턴(급여/마케팅/유동성 지원) 확인.

1. 마케팅 지갑 (Marketing)

* 마케팅·커뮤니티 보상·인플루언서 지급에 쓰는 지갑.
* 단기 대량 출금 빈번 → 단기 매도 압력 신호.
* 트랜잭션 메모/라벨, 다수 소액 전송 패턴, CEX 입금 잦음.

1. 베스팅 계약 (Vesting Contract)

* 팀/어드바이저 물량을 일정 기간 잠금·차등 해제하는 컨트랙트.
* 언락 스케줄이 곧 잠재 매도 시계.
* 컨트랙트 코드/이벤트에 release, vest, cliff, unlock 등 함수·로그. TeamFinance/Unicrypt/커스텀 베스팅 주소.

1. 에스크로 / 타임락 (Escrow / Timelock)

* 자산·권한을 시간 지연 후에만 이동/변경 가능하게 묶는 장치.
* 갑작스런 rug·권한 남용을 막음(예: 변경 공지 후 24–48h 지연).
* TimelockController 같은 컨트랙트, minDelay 파라미터 확인.

1. 권한 지갑 (Privileged / Admin Roles)

* 컨트랙트 내 특권(Role) 를 가진 지갑/컨트랙트.
* 주요 권한:

1. 민트(발행량 증가), 블랙리스트, 세금변경(transfer fee), 일시정지(pause), 업그레이드(proxy admin / upgrader),
2. (v4) Hook 소유/업그레이드(거래 수수료·화이트리스트·거래제한 로직 가능).

* 한 번에 토큰 경제를 바꿀 수 있어 리스크 큼.
* Read Contract의 owner/roles, ProxyAdmin 주소, UUPS/Transparent Proxy 존재, v4 Hook 소유자.

1. 초기 LP 제공 지갑 (Initial LP Provider)

* DEX 풀(HYPE/USDC 등)에 초기 유동성 넣은 지갑(받은 LP 토큰의 소유자).
* LP 토큰이 락/소각되지 않으면 언제든 유동성 빼서 가격 붕괴(rug) 가능.
* DEX 트랜잭션에서 Add Liquidity 첫 기록, LP 토큰 보유/이동 내역, LP 락/소각(0xdead) 여부.

정리: 위 사항들, 즉 **“팀이 통제하거나 경제적 이해가 있는 물량/권한”** 을 한데 묶어 **실제 매도 가능성·권한남용 가능성**을 평가하려는 것임. 이때, 온체인 데이터만으로 확인하기 어려운 정보는 프로젝트의 공식 문서, 트위터 등 오프체인 데이터를 통해 교차검증하는 것이 필요함.

1. 산식: Dev Holdings 점수와 위험도 스코어링을 n:m 비율로 합산하여 최종 점수를 산정함
2. Dev Holdings: 1)에서 나열한 것들로 개발자 비율을 계산함
3. Dev Risk Score: 개발자 비율이 폭탄의 크기라면, 이는 폭탄의 잠금장치가 얼마나 잘 작동되는지를 판단하는 점수임.

* 치명적 리스크: mint, upgrade 등 핵심 권한이 개인 지갑 (EOA)에 있음 +50

Pause, blacklist, 세금 변경 등 부가 권한이 개인 지갑에 있음 +20

초기 LP 토큰이 락업/소각되지 않고 개인 지갑 (EOA)에 있음 +40

* 보유 물량 리스크: 락업되지 않은 팀 관련 총 보유량이 유통량의 20% 초과 +20

락업되지 않은 팀 관련 총 보유량이 유통량의 5%~20% +10

* 위험 완화 장치: 팀/어드바이저 물량이 1년 이상 장기 베스팅됨 90%이상 -20, 70~89% -15, 40~69% -5, 40%미만 +5

주요 권한 및 기능 변경에 24시간 이상 타임락이 적용됨 -15

Treasury 등 주요 자산을 다중서명 지갑으로 관리함 -10

초기 LP토큰이 1년 이상 장기 락업 또는 소각됨. -10

1. Snipers holdings: 런칭 직후 자동 봇으로 빠르게 매수한 지갑. 초기 유동성 빨아먹고 덤핑할 가능성 높음

왜? 스나이퍼들은 대부분 런칭직후 유동성이 풀리자마자 초단위로 매수해서 일반투자자보다 훨씬 낮은 가격에 매수. 그러면 가격이 좀만 올라도 이득이니까 곧바로 매도할 동기가 있음. 그래서 많은 스나이퍼가 동시 매도하게 되면 시장충격이 발생. => 출시 과정이 공정했는가? 에 대한 대답이 될 수 있음.

1. 범위
2. 유동성 공급과 동시에 매수 발생

* 0번 블록 혹은 첫 블록에서의 매수: Transaction Block or 다음 블록에서 매수거래
* 매수 시간: 유동성 공급 트랜잭션과 매수 트랜잭션의 Timestamp 차이가 수 초 이내일 경우

1. 비정상적으로 높은 가스비

* 네트워크의 평균 가스비보다 수십수백배 높은 가스비를 사용한 매수 거래. (거래가 먼저 처리되도록 하기 위해 높은 가스비를 지출함.)

1. 정형화되고 반복적인 매수 패턴:

* 동일한 매수금액: 신규토큰에 대해서 항상 비슷한금액으로 매수시도
* 다수의 신규토큰에 대한 초기 매수

1. 보조지표들

* 새로운 지갑(Fresh Wallet) 사용: 추적을 피하기 위해 사용
* 토큰 발행자와의 연관성
* 빠른 매도 패턴: 단기차익 실현 목표이기 때문에

1. 산식:

* Sniper Holdings Ratio X 100 = f(snipers) 로 정의한다.
* Σ Sniper Holdings= 스나이퍼로 분류된 모든 지갑들이 보유한 ‘토큰의 총량’

스나이퍼 지갑 A가 100,000개의 토큰을 보유

스나이퍼 지갑 B가 50,000개의 토큰을 보유

스나이퍼 지갑 C가 30,000개의 토큰을 보유

* 이 경우, Σ Sniper Holdings= 100,000 + 50,000 + 30,000 = 180,000

1. Sniper Holdings 판단 기준 : Scoring Model

* 1)에서 나열한 각 요소에 가중치를 두어 점수를 매김
* 예) (1)은 50점, (2)은 20점, (3)은 10점, (4)은 5점으로 하고, 임계(Threshold)를 설정(예:70점) 🡪 임계 이상이면 스나이퍼로 분류한다.
* Machine Learning Scoring Model: 데이터 라벨링 🡺 모델 훈련 🡺 자동 가중치 산정
* 자동 가중치 산정: 여러 데이터셋을 보고 학습하면서 AI가 스스로 각 요소의 중요도를 계산해낸다. 🡪 Scoring은 머신러닝이 가능한 환경에서 이루어짐. (대안: 전문가의 휴리스틱)
* 역치 설정: Scoring 모델이 완성된 후에 설정.

1. 총 가중치: 10~15퍼
2. Insiders (내부자 지갑): 프로젝트 팀원, 투자사(VC), 고래(Whale) 등 일반 대중에게 공개되지 않은 정보를 이용해 부당 이익을 취할 가능성이 있는 내부자.
3. 범위
4. 정보 공개 전. 사전 매집 활동

* 공지 직전 대규모 매수량: 특정 이벤트 수 시간 or 수일 전에 갑자기 대규모 토큰매수
* 신규 고래지갑의 등장: 고래가 새로 나타나 특정 토큰만 대량으로 매집하는 경우
* 자금 출처 분석: 매집에 사용된 자금이 CEX나 내부자 지갑에서 출금했는지 파악

1. 팀/재단 물량의 ‘비정상적 이동’

* 거래소 입금량: 팀 또는 재단의 공식 지갑에서 대규모 물량이 CEX로 입금되는지 확인 🡪 현금화를 위한 매도 압력으로 작용할 수 있음.
* 락업 해제 직후의 움직임: 락업기간 끝나자마자 물량 분산
* 지갑 분산 패턴: 추적을 피하기 위해 하나의 팀 지갑에서 여러 개의 새로운 지갑으로 토큰을 쪼개서 보냄

1. VC 및 초기 투자자의 매도 패턴

* 베스팅 물량 수령 후 즉시 매도: 베스팅 물량을 지급받자마자 거래소로 보내거나 덱스에서 매도하는 패턴 추적. 🡪 햬당 투자자가 프로젝트의 장기적 가치에 대해 비관적이라는 신호
* 평균 보유 기간 (Average Hold Time): 비정상적으로 짧다면 단기 차익 실현에만 관심이 있다는 뜻
* 초기 투자자 그룹의 동시 움직임: 이들이 동시에 토큰을 매도하는 움직이는 사전 교감된 행동일 가능성이 있다.

1. 산식

* **x 100 = f(Insiders**) 로 정의
* = 내부자 지갑에 있는 토큰의 총량

1. Insiders 판단 기준: Insider Risk Score

* 사전 매집 (Front-Running) 지수=X100 : (1)을 측정하는 산식

특정 지갑 그룹: 공지 직전에 생성, 거래내역 없다가 해당토큰 대량매수, 과거에도 다른 토큰 상장직전 매집 이력 있는 지갑

N시간: 주요 공지 전 12시간에서 72시간

X100: 이 비율이 높을수록 팀의 현금화(매도) 의지가 강하다고 해석할 수 있음.

N일: 보통 7일 또는 30일을 기준으로 측정

* 매도 압력 지수=X100 : 초기 투자자들이 프로젝트를 얼마나 장기적으로 보고 있는지를 측정하는 산식

VC 지갑 그룹: 주요 VC나 초기 투자자들의 지갑 주소는 대부분 알려져 있어 그룹으로 묶어 추적

N일: 보통 30일 기준으로 측정

텍스트, 스크린샷, 디스플레이, 소프트웨어이(가) 표시된 사진

AI 생성 콘텐츠는 정확하지 않을 수 있습니다.

80점 이상/79~60점/59~40점/40점 미만 으로 구분해서 평가

1. 스나이퍼와 인사이더 비교

| 구분 | 스나이퍼 탐지 | 인사이더 탐지 |
| --- | --- | --- |
| 문제의 성격 | 수많은 거래 속에서 미세한 패턴을 찾는 것 | 의미가 명확한 결정적 이벤트를 해석하는 것 |
| 데이터의 양 | 매우 많음 (수천~수만 건의 초기 거래) | 상대적으로 적음 (팀의 거래소 입금은 가끔 발생) |
| 신호의 명확성 | 낮음 (일반 거래와 섞여 있어 신호가 약함) | 매우 높음 ("팀 지갑 → 거래소"는 그 자체로 강력한 신호) |
| 적합한 모델 | 머신러닝 (인간이 찾기 힘든 복잡한 패턴 학습) | 휴리스틱 (신호가 명확해 전문가 규칙만으로도 충분히 강력함) |

* 하지만 실제 분석 플랫폼들은 휴리스틱과 머신러닝을 하이브리드 방식으로 채택해서 사용

1. Paid: 마케팅/인플루언서 유료 홍보 여부 🡪 실제 성과보다 홍보성 지출만 크면 스캠가능성 높음

보조지표이고 Binary라서 가중치 낮게하는 것이 좋을 듯

1. 전체 인덱스

*텍스트, 스크린샷, 폰트이(가) 표시된 사진

AI 생성 콘텐츠는 정확하지 않을 수 있습니다.*

1. 패널티 가중 법칙 – 회의 주제
2. 번외) 네트워크 상에서의 Bundlers: 사용자의 여러 트랜잭션을 하나의 묶음으로 만들어 블록체인에 효율적으로 제출해주는 전문 중개자. MEV 공격방지와 가스비 효율을 높이지만, 번들러의 점유율이 너무 높을 경우엔 탈중앙성에 위험 생김.
3. 번들러 식별: 어떤 주소(EOA)가 번들러 역할을 하고 있는지 찾아냄
4. 계정 추상화(EIP-4337) 번들러 식별: 모든 것이 ‘EntryPoint’ 스마트컨트랙트를 통해 이루어짐(쉬움)

* EntryPoint 컨트랙트 주소 확인: 대부분 체인에 단 하나의 공개된 컨트랙트가 있음
* handleOps 함수 호출 필터링: 온체인 데이터를 분석할 때, 이 EntryPoint 컨트랙트로 들어오는 모든 트랜잭션 중 handleOps라는 특정 함수를 호출하는 것들만 모두 필터링. 모든 번들링된 UserOperation은 반드시 이 함수를 통해 실행
* 호출자 (msg.sender) 식별: handleOps 함수를 호출한 주소 (msg.sender)가 바로 그 거래 묶음을 제출한 번들러임

1. MEV 번들러 식별 방법: 정해진 규칙 X. 블록 빌더에게 지불하는 팁을 찾아내는 것. (어려움)

* 알려진 '블록 빌더' 주소 목록 확보: 분석 플랫폼은 Flashbots, Beaver Builder 등 주요 블록 빌더들이 사용하는 이더리움 주소 목록을 이미 확보하고 있음.
* 블록 내 '팁' 거래 스캔: 블록에 포함된 트랜잭션들을 스캔하여, 위에서 확보한 블록 빌더의 주소로 직접 ETH를 송금하는 거래를 찾아냄. 이것이 바로 번들을 블록에 포함시켜준 대가로 지불하는 '팁' 또는 '뇌물(Bribe)'이다.
* '팁' 지불자 식별: 이 '팁'을 보낸 주소(from address)가 바로 'MEV 번들러'일 확률이 매우 높다.
* 패턴 검증: 하나의 주소가 여러 다른 블록 빌더에게 지속적으로 팁을 지불하고, 그 직전에 여러 개의 트랜잭션 묶음(Bundle)을 실행시키는 패턴이 반복적으로 관찰되면, 해당 주소를 'MEV 번들러'로 확신하고 라벨링.

1. 번들러 활동 추적-