

주요정보 요약

Summary of Whitepaper



본 문서는 거래지원 가상자산 백서의 주요 내용을 한글로 설명한 주요정보 요약입니다.

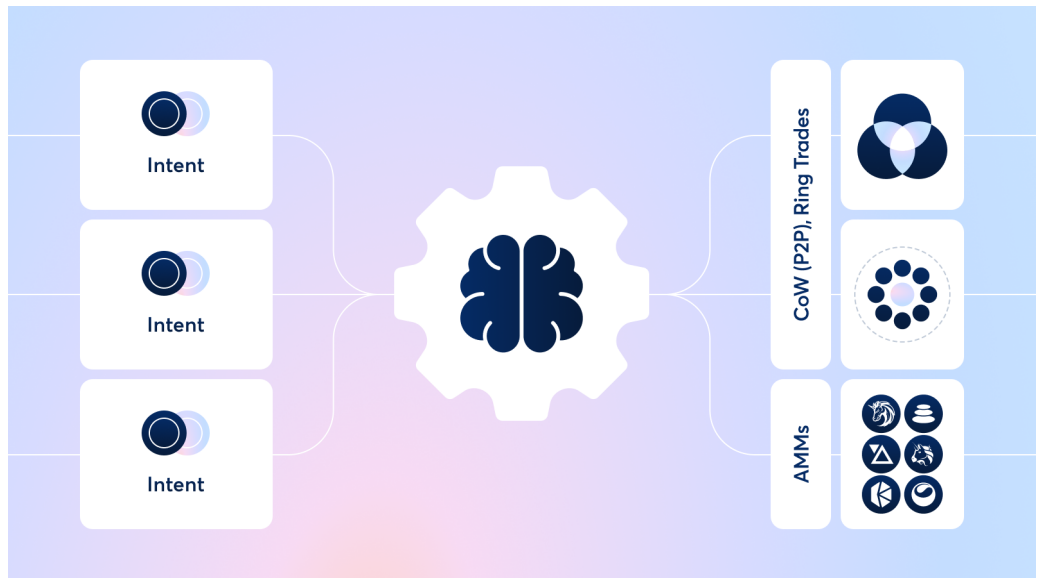
코인원은 거래지원 가상자산의 주요정보 요약을 주기적으로 점검하여 가능한 한 최신 정보를 제공할 예정입니다.

기본 정보

가상자산 카테고리	유틸리티
거래지원 네트워크	Ethereum
홈페이지	https://cow.fi/
참고문헌 (백서, Docs 등)	https://docs.cow.fi/

1. 프로젝트 정보

CoW Protocol이란? CoW Protocol은 솔버(Solver)라고 불리는 제3자에게 의존하여, Ethereum 및 EVM 호환 체인에서 거래를 실행하기 위한 조건을 명시한 거래 의향(Intent)에 대해 최적의 실행 경로를 찾습니다. 사용자의 거래 의향이 처음 접수되면, 프로토콜은 이를 다른 거래 의향들과 함께 하나의 배치(Batch)로 묶습니다. 그런 다음, 솔버는 다음과 같은 방식으로 거래를 처리합니다.



1. CoW(Coincidence of Wants)를 우선 탐색: 솔버는 동일한 배치 내에서 서로 상쇄될 수 있는 거래 의향을 찾아, 온체인 유동성보다 더 나은 가격을 제시할 수 있는지 확인합니다.
2. CoW를 찾지 못할 경우: 솔버는 온체인 및 오프체인에 존재하는 모든 유동성을 검색하여, 배치된 거래 의향 세트에 대해 가능한 최고의 가격을 제공합니다.

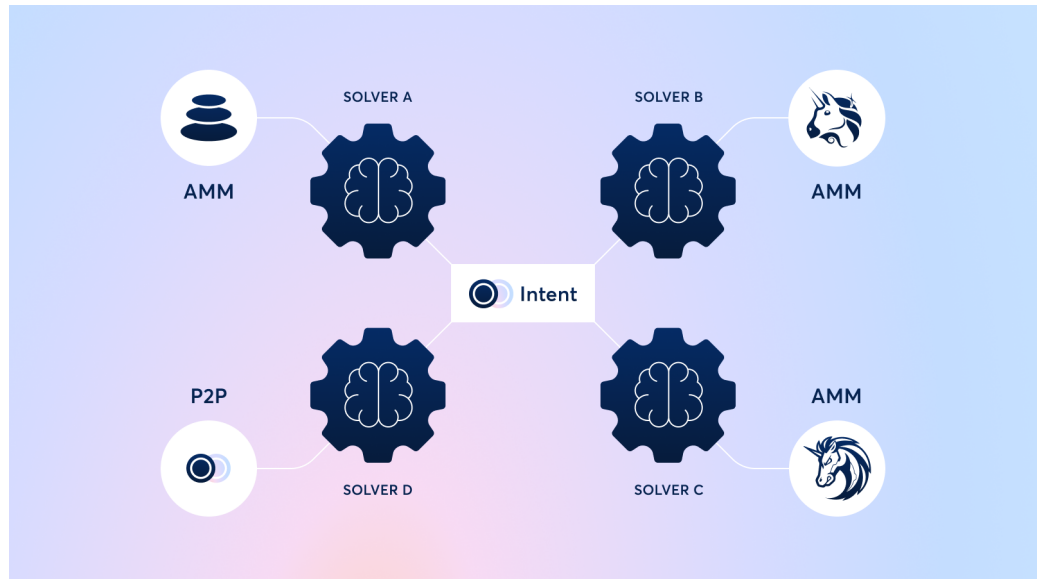
활용되는 유동성 원천

- AMM
예) Uniswap, Sushiswap, Balancer, Curve 등
- DEX 어그리게이터 (DEX Aggregator)
예) 1inch, Paraswap, Matcha 등
- 프라이빗 마켓 메이커 (Private Market Makers)

솔버가 접근하는 이 광범위한 유동성 덕분에, CoW Protocol은 어그리게이터의 어그리게이터(Aggregator of aggregators)로 불립니다.

거래 의향(Intent)

Uniswap이나 SushiSwap 같은 프로토콜에서처럼 원시 트랜잭션을 직접 서명하여 온체인에서 즉시 실행하는 방식과 달리, CoW Protocol의 사용자들은 '거래 의향(intent to trade)' 메시지에 서명함으로써 주문을 제출합니다. 이 메시지에는 거래하고자 하는 자산과 수량 같은 주요 매개변수가 포함되어 있으며, 서명된 메시지를 바탕으로 솔버(solver)가 사용자를 대신해 거래를 실행할 수 있도록 합니다. 이러한 의향 기반 거래(intent-based trading) 방식은 재무적, 기술적으로 여러 가지 이점을 제공합니다.



거래 의향의 재무적 이점

사용자가 일반적인 온체인 거래를 실행하면, 그 실행 경로는 고정되며, 사용자는 해당 경로에서 발생하는 가격(미끄러짐 포함)을 그대로 받아들여야 합니다. 즉, 거래 플랫폼(AMM 또는 집계기)이 제시하는 가격 이상도 이하도 받을 수 없습니다.

반면, CoW Protocol의 의향 기반 구조에서는 최적의 실행 경로를 찾는 역할을 '솔버'라는 전문 제3자에게 위임합니다. 이 솔버들은 단순히 온체인 유동성만 스캔하는 것이 아니라, 여러 방식으로 더 나은 가격을 제시할 수 있습니다.

- CoW(Coincidence of Wants)

동일한 토큰 쌍에 대해 반대 방향(매수 ↔ 매도)의 거래 의향을 가진 두 명 이상의 사용자가 존재할 경우, 이를 직접 P2P 방식으로 매칭하는 최적화 기법입니다. 이는 배치 경매(batch auction) 구조를 통해 가능하며, LP 수수료를 피하고 외부 스마트 컨트랙트와의 상호작용을 줄여 가스비도 절감할 수 있습니다.

- 비공개 마켓메이커 유동성 활용

많은 솔버들은 중앙화 거래소(CEX)의 재고, 비공개 마켓메이커와의 통합, 또는 자체적인 오프체인 유동성 풀을 보유하고 있습니다. 이로 인해, 특정 거래의 경우 온체인 AMM보다 더 유리한 가격에 체결할 수 있습니다.

- MEV 보호

CoW Protocol에서 사용자는 MEV(최대 채굴자 이익) 봇의 공격에 노출되지 않습니다. 거래는 솔버가 대신 처리하며, 모든 MEV 리스크는 솔버가 감수합니다. 또한, 솔버는 모든 주문을 동일한 가격으로 배치 내 일괄 처리하므로, 거래 순서를 조작하여 이익을 취하는 MEV 기법이 원천적으로 불가능합니다.

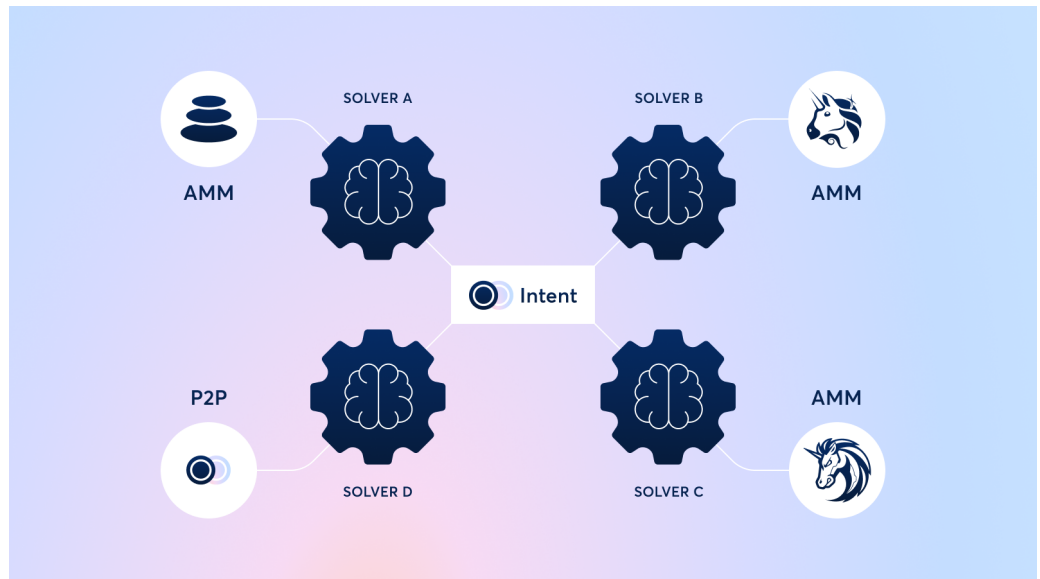
거래 의향의 기술적 이점

CoW Protocol의 의향 기반 아키텍처는 기술적으로도 다음과 같은 다양한 이점을 제공합니다.

- 단순 거래 외에도 다양한 유형의 트랜잭션 실행 가능
특정 조건과 체인 상의 상황에 따라 다양한 유형의 트랜잭션을 실행할 수 있도록 함으로써, CoW Hooks나 Programmatic Orders 같은 고급 기능을 지원합니다.
- 거래 체결 방식에 대한 추가 규칙 설정 가능
예를 들어, 거래가 EBBO(Ethereum Best Bid and Offer, 이더리움 체인 상 최적 매수/매도 호가) 기준으로 체결되도록 보장하거나, 동일 배치 내 동일 토큰 쌍은 동일 가격으로 일괄 체결하는 등의 조건을 설정할 수 있습니다.
- 체인 네이티브 토큰(예: ETH)을 보유하지 않아도 트랜잭션 수수료 지불 가능
사용자는 판매하려는 토큰으로 가스비를 낼 수 있어, 별도로 체인 네이티브 토큰을 보유하지 않아도 됩니다.
- 실패한 거래에 대한 수수료 없음
거래가 실패하더라도 수수료가 부과되지 않으며, 사용자는 손해를 보지 않습니다.
- 여러 주문을 한 번에 제출 가능
사용자는 복수의 거래 의향을 동시에 제출할 수 있어 복잡한 거래 전략도 수월하게 실행할 수 있습니다.
- 배치 경매 구조 구현 가능
이는 곧 배치 체결 방식이 제공하는 다양한 혜택(가스비 절감, MEV 방지, 더 나은 가격 발견 등)을 프로토콜 전반에서 활용할 수 있게 합니다.

솔버(Solver)

CoW Protocol은 주문 매칭에 있어 '개방형 솔버 경쟁(Open Solver Competition)' 메커니즘을 활용하여 최적의 가격을 실현합니다.



솔버란?

솔버는 사용자를 대신해 거래를 실행하는 담보(bonded)를 제공한 제3자이며, 이는 의향 기반 위임 실행 모델(intent-based delegated execution model)을 통해 이루어집니다. 사용자가 거래 의향(intent)을 제출하면, 프로토콜은 이를 다른 사용자들의 의향과 함께 하나의 배치(batch)로 묶어 경매(batch auction)를 구성합니다. 일정 시간이 지나 해당 배치가 "주문 접수 종료(closed for orders)" 상태에 도달하면, 프로토콜은 솔버 간의 경쟁(competition)을 시작합니다. 이때 솔버들은 배치 내 의향들을 어떻게 체결할지에 대한 자신만의 솔루션을 제출합니다.

가장 우수한 솔루션을 제출한 솔버, 즉 사용자 주문에 가장 많은 잉여가치(surplus)를 제공하는 솔루션을 제시한 솔버가 해당 배치의 거래를 실행할 수 있는 권한을 획득하게 됩니다.

솔버는 이러한 배치 정산(settlement)을 수행한 대가로 COW 토큰으로 보상을 받으며, 이는 더 나은 가격을 제시하고 거래 체결권을 확보하기 위한 경쟁 유인을 형성합니다.

솔버의 작동 방식

- 솔버는 사용자가 미리 승인한 ERC-20 승인 권한(approvals)을 통해, 금고 릴레이어(vault relayer) 계약을 통해 사용자의 토큰을 이동시킬 수 있습니다.
- 정산 계약(settlement contract)은 사용자의 거래 의향에 대한 서명(signature)을 검증하며, 사용자가 설정한 리밋 가격(limit price)과 수량(quantity)에 따라 정확히 거래가 실행되도록 보장합니다.

솔버가 되기 위한 자격

기본적인 DeFi 지식과 최적화 알고리즘을 구현할 수 있는 코딩 능력만 있다면, 누구나 솔버를 개발하고 참여할 수 있습니다.

배치 경매 (Batch Auction)

CoW Protocol은 거래 의향(intent)을 오프체인에서 수집·집계한 뒤, 이를 그룹으로 묶어 일괄 처리합니다. 이러한 그룹을 '배치(batch)'라고 부릅니다. 이후 해당 배치에 포함된

주문들을 체결할 권한은 경쟁을 통해 경매 방식으로 솔버에게 할당되며, 가장 많은 사용자 잉여가치(surplus)를 제공하는 솔버가 낙찰자가 됩니다.

배치 경매의 주요 이점

1. MEV(최대 채굴자 이익) 방지

배치 경매에서는 UCP(Uniform Clearing Prices, 균일 정산 가격)라는 개념을 적용합니다. 이는 하나의 자산이 동일한 배치 내 여러 주문에서 등장할 경우, 해당 자산은 일괄적으로 동일한 가격으로 정산된다는 의미입니다. 이러한 구조 덕분에 트랜잭션의 순서가 블록 내에서 무의미해지며, MEV 봇이 거래 순서를 조작하여 이익을 추출하는 것이 불가능해집니다.

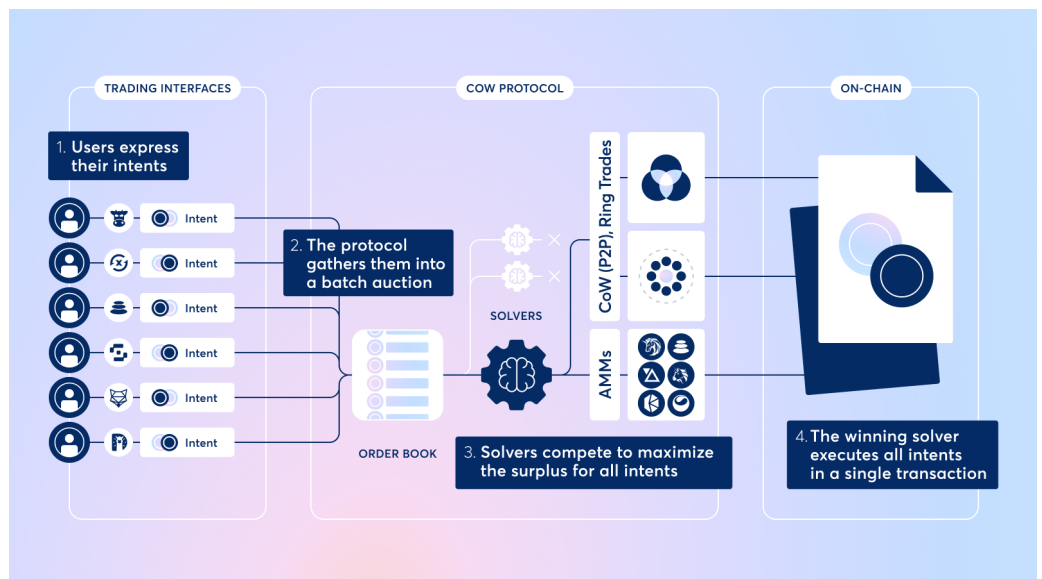
2. CoW(Coincidence of Wants) 최적화

배치 내 여러 사용자가 동일한 자산을 서로 반대 방향으로 거래하려는 경우, 온체인 유동성을 거치지 않고 직접 P2P 방식으로 스왑이 이루어질 수 있는 기회가 발생합니다. 이러한 직접 매칭 기법은 CoW 메커니즘의 핵심이며, 배치 경매 구조 없이는 실현될 수 없습니다.

3. EBBO(Ethereum Best Bid Offer) 보장

CoW Protocol은 사용자의 거래가 최소한 온체인 AMM에서 직접 거래할 때 받을 수 있는 가격(Ethereum Best Bid Offer, EBBO)과 같거나 더 좋은 조건으로 정산되도록 보장합니다. 이는 사용자 보호를 위한 중요한 기준이며, 배치 경매 구조 덕분에 시스템적으로 강제될 수 있습니다.

주문 처리 절차



거래 의향 제출

사용자는 거래하고자 하는 자산과 수량, 기타 조건을 포함한 메시지에 서명함으로써 자신의 거래 의향을 제출합니다.

배치 경매 구성

프로토콜은 여러 사용자의 거래 의향을 하나의 배치(batch)로 모아 배치 경매(batch auction)를 시작합니다.

솔버 경쟁 및 낙찰자 선정

솔버들은 제한된 시간 동안 해당 배치에 대한 정산(settlement) 방안을 제안할 수 있습니다. 이때 사용자들에게 가장 많은 잉여가치(surplus)를 제공하는 솔버가 승자로 선정됩니다.

온체인 정산 및 토큰 수령

선정된 솔버는 사용자를 대신하여 해당 배치를 온체인에서 실행합니다. 이후 사용자들은 각자의 지갑으로 거래 결과 토큰을 수령하게 됩니다.

사용자에게 유리한 구조

배치 경매에서의 솔버 간 경쟁은, 트레이더, DAO, 스마트 컨트랙트, 거래 봇 등 모든 사용자가 항상 최상의 가격에 거래할 수 있도록 보장합니다.

또한, 복잡한 유동성 탐색, 가스비 설정, 슬리피지 한도 조정 등을 사용자 대신 솔버가 수행하기 때문에, 사용자는 기술적 디테일에 신경 쓸 필요가 없습니다. 솔버는 MEV 회피 전략의 전문가이기도 하여, 사용자는 프론트러닝이나 샌드위치 공격과 같은 MEV 봇의 가격 착취로부터도 보호받을 수 있습니다.

CoW (Coincidence of Wants): 원하는 것이 일치하는 순간

CoW (Coincidence of Wants): 두 당사자가 서로가 필요로 하는 자산을 보유하고 있을 때, 이를 직접 교환하는 경제적 현상으로, 동등한 물물교환 형태입니다.

CoW Protocol의 배치 메커니즘 덕분에, 사용자는 동일한 자산을 거래할 경우 피어 투 피어 방식의 스왑을 수행할 수 있습니다.

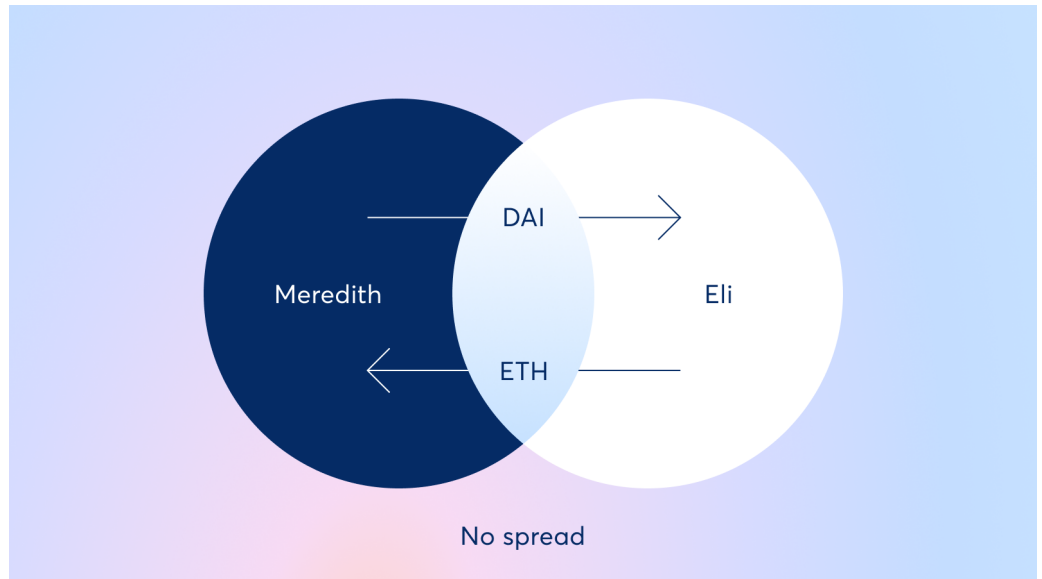
예를 들어, 하나의 배치에서 한 트레이더가 2,000달러 상당의 DAI를 0.5 ETH로 교환하려 하고, 같은 배치 내 다른 트레이더가 0.5 ETH를 2,000달러의 DAI로 교환하려고 할 경우, CoW Protocol의 솔버가 두 트레이더를 매칭시켜 온체인 유동성에 접근하지 않고 자산을 교환할 수 있도록 합니다. 이는 유동성 공급자 수수료를 피할 수 있게 해줍니다.

CoW는 사용자가 유동성 공급자(LP) 수수료를 피할 수 있게 해줄 뿐만 아니라, 주문이 CoW Protocol의 스마트 컨트랙트와만 상호작용하기 때문에 가스 수수료도 절감됩니다.

CoW는 완전하거나 부분적일 수 있습니다. 부분적인 CoW에서는, 배치 내 하나의 거래만이 반대 유동성을 통해 완전히 충족되며, 솔버는 나머지 거래의 유동성을 확보하기

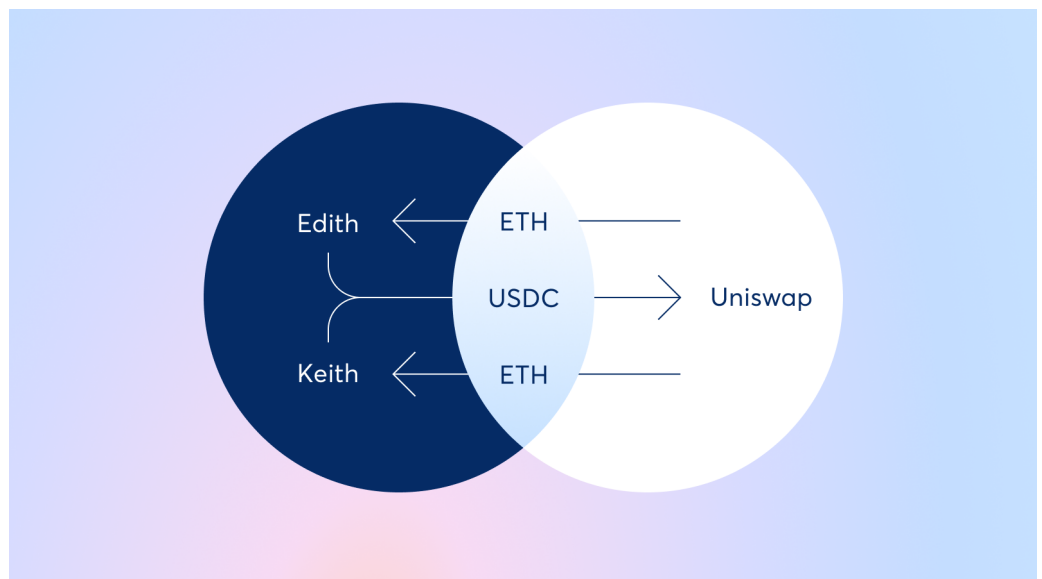
위해 온체인 유동성에 접근해야 합니다.

Simple CoW



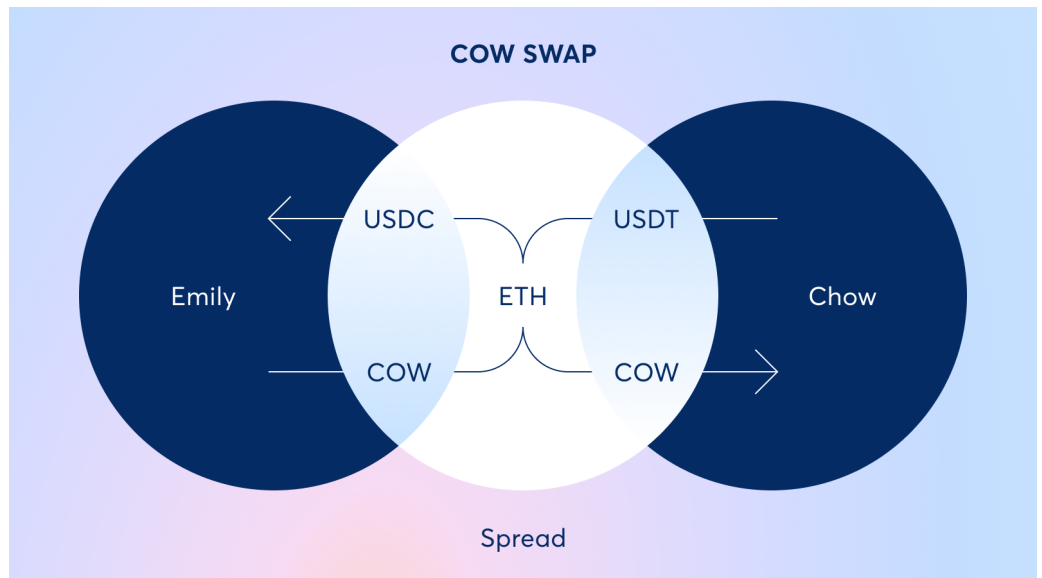
Simple CoW는 두 명의 트레이더가 서로 상대방이 구매하고자 하는 자산을 판매하는 경우입니다. 이들은 AMM 유동성 풀과 상호작용하는 대신, 서로 직접 자산을 교환합니다. Simple CoW는 각 트레이더가 상대방이 필요로 하는 정확한 금액을 거래하는 완전한 형태일 수도 있고, 반대 자산을 거래하되 한쪽만 전체 유동성이 CoW로 충족되는 부분적인 형태일 수도 있습니다. 후자의 경우, 거래의 나머지 부분은 온체인에서 마무리됩니다.

Batching CoW



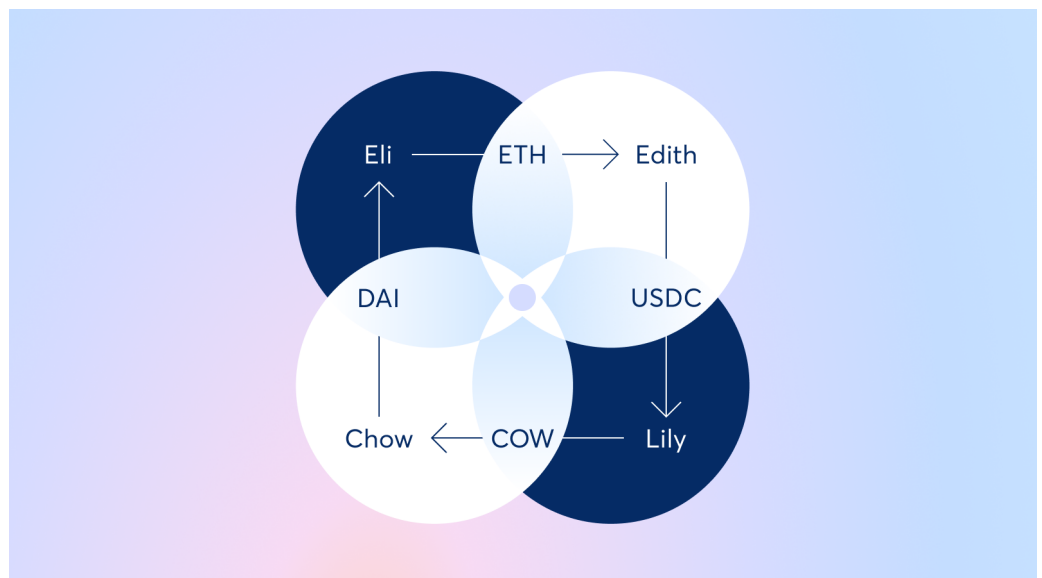
배치 경매에는 종종 동일한 거래를 수행하고자 하는 여러 사용자의 의향이 포함됩니다. 이들이 각각 개별적으로 거래를 보내는 대신, 솔버는 모든 의향을 하나로 배치하여 단일 거래로 온체인에서 실행할 수 있습니다. Batching CoW는 온체인에서 실행되지만, 사용자의 거래가 AMM 스마트 컨트랙트와 상호작용하는 횟수를 줄이기 때문에 가스 수수료를 절감할 수 있습니다.

Intermediate CoW



Intermediate CoW는 피어 투 피어 방식으로 정산될 수 있는 ‘중간’ 거래가 있을 때 발생합니다. 예를 들어, 한 사용자가 CRV를 USDT로 교환하고, 다른 사용자가 USDT를 COW로 교환하려고 할 경우, 중간 단계로 “ETH” 거래가 필요할 수 있습니다. 첫 번째 트레이더는 $CRV \rightarrow ETH \rightarrow USDT$ 로 이동해야 하고, 두 번째 트레이더는 $USDT \rightarrow ETH \rightarrow COW$ 로 이동해야 할 수 있습니다. 이 예시에서, 첫 번째 트레이더의 $ETH \rightarrow USDT$ 거래와 두 번째 트레이더의 $USDT \rightarrow ETH$ 거래는 피어 투 피어 방식으로 CoW를 통해 정산될 수 있습니다.

Multidimensional CoW

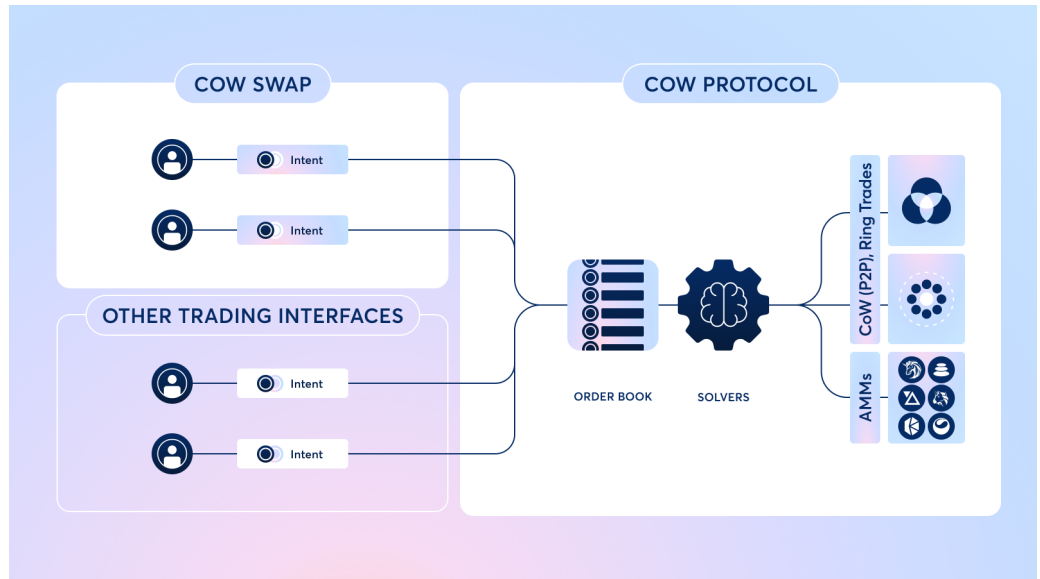


Multidimensional CoW는 세 명 이상의 사용자가 참여하며, 각자의 거래 간 유동성을 공유합니다. 일반적으로 여러 자산이 포함되며, 오프체인 유동성 활용을 극대화하기 위해 솔버가 사용자 간 최적의 경로를 찾는 데 의존합니다.

일부 주문은 CoW를 통해 전부 체결되지만, 많은 경우에는 일부만 피어 투 피어 방식으로 체결됩니다. 이러한 경우, 솔버는 거래를 완전히 체결하기 위해 자동으로 온체인에서 나머지 유동성을 확보합니다.

CoW Swap

CoW Swap은 CoW Protocol 위에 구축된 최초의 거래 인터페이스이며, 현재 사용자들이 CoW Protocol을 이용한 거래를 수행하는 가장 인기 있는 방법입니다. Balancer와 같은 기타 거래 앱 및 dApp들도 자체 거래 인터페이스에 CoW Protocol을 네이티브로 통합하고 있으며, 고급 사용자들은 CoW Protocol과 직접적으로 상호작용하여 거래를 수행하기도 합니다.



CoW Swap 인터페이스의 주요 특징

CoW Swap의 UI는 다음과 같은 독특한 기능들을 포함하고 있습니다.

- 지갑 거래 내역(Wallet history) : 사용자의 과거 거래 기록을 확인할 수 있습니다.
- 토큰 잔액 표시(User token balances) : 보유 중인 자산의 잔고를 직관적으로 확인할 수 있습니다.
- 게임 요소(Games) : 사용자 참여도를 높이기 위한 가벼운 게임 콘텐츠가 탑재되어 있습니다.
- 전설의 “Moo” 사운드 : 거래 체결 시 재생되는 재미 요소로, CoW Swap의 시그니처 중 하나입니다.
- 포춘 쿠키(Fortune cookies) : 사용자 경험을 유쾌하게 만들어주는 작은 운세 메시지 요소입니다.

지갑 호환성

CoW Swap은 다음과 같은 다양한 지갑들과 호환됩니다.

- Rabby
- MetaMask
- Trust Wallet

- Safe (Gnosis Safe)
- Trezor
- Ledger
- WalletConnect v2를 지원하는 모든 지갑

2. 토큰 이코노미

가상자산 소개

CoW Protocol의 핵심에는 COW 토큰이 있으며, 이는 CoW Protocol 생태계 내에서 거버넌스 토큰으로 기능합니다.

COW 토큰 보유자는 프로토콜의 개발 방향과 진화 과정을 이끄는 의사결정 과정에 직접 참여할 수 있는 권한을 가집니다.

즉, 프로토콜의 중요한 변경 사항에 대한 제안과 투표에 참여함으로써, 생태계의 거버넌스에 기여하게 됩니다.

CoW Protocol의 거버넌스 프레임워크는 다음을 목표로 설계되어 있습니다.

- 사용자, 개발자, 지지자 간의 인센티브 정렬
- 탈중앙화되고 커뮤니티 중심적인 운영 구조 형성
- 지속 가능한 생태계 발전을 위한 참여 기반 시스템 구축

이러한 구조 덕분에 COW 토큰은 단순한 유틸리티를 넘어, 프로토콜의 방향성을 형성하는 핵심 수단으로 자리 잡고 있습니다.

발행량 및 유통량계획

COW 토큰은 CoW Protocol의 장기적인 지속 가능성과 자율성을 뒷받침하기 위해 설계된 거버넌스 토큰입니다. 최대 연간 인플레이션율은 3%로 제한됩니다. 어떤 형태의 토큰 공급 증가도 최소 365일에 한 번만 가능하도록 설정되어 있습니다. 이러한 신중한 인플레이션 설계는 무분별한 발행으로 인한 희석 효과(dilution)를 방지하고, 공급 증가가 반드시 필요한 경우에만 신중하게 시행되도록 만듭니다. 인플레이션 관련 조치는 오직 CoW DAO에 의해만 결정될 수 있습니다. 즉, COW 토큰 보유자는 직접적으로 프로토콜의 인플레이션 정책에 참여할 수 있으며, 이는 토큰 경제에 대한 커뮤니티의 실질적 통제권을 보장합니다. 현재까지 어떠한 인플레이션 조치도 시행된 적이 없으며, COW 토큰의 총 공급량은 10억(1,000,000,000) 개로 유지되고 있습니다. COW 토큰의 초기 분배는 균형 잡히고 지속 가능한 생태계를 구축하기 위해 정밀하게 설계되어 실행되었습니다.

초기 발행된 10억 개의 COW 토큰은 다음과 같이 배분되었습니다.

- CoW DAO 금고(Treasury) : 44.4%
이 큰 비율은 커뮤니티가 프로토콜의 지속적인 개발과 유지에서 중심적인 역할을 담당하고 있음을 강조합니다.
- 팀(Team) : 15%
CoW Protocol을 구축하고 지금도 계속 발전시키고 있는 팀 구성원들에게 보상하기 위한 몫입니다.
- GnosisDAO : 10%
CoW Protocol 프로젝트에서의 파트너십 및 협력 관계를 인정하는 차원에서 배분되었습니다.
- CoWmunity 에어드랍 : 10%
초기 사용자 및 기여자들에게 감사를 표하고 이들의 참여를 유지하기 위해 제공되었습니다.
- CoWmunity 투자(CoWmunity Investment): 10%
초기 사용자가 프로토콜에 재정적 기여를 하는 대신 더 많은 지분을 확보할 수 있는 옵션으로, 이는 커뮤니티의 참여 확대 및 장기적인 커밋먼트 유도를 목표로 합니다.
- CoW 자문(CoW Advisory): 0.6%
프로토콜에 전략적 자문과 전문성을 제공한 이들에 대한 보상입니다.
- 투자 라운드(Investment Round): 10%
프로토콜의 성장과 확장을 위한 필수 자금 조달 목적입니다.

자문, 팀, 투자자, GnosisDAO, CoWmunity 투자 등 특정 이해관계자에게 배분된 COW 토큰은 'vCOW' 형태로 지급되며, 배포 시점을 기준으로 4년에 걸쳐 선형적으로 베스팅(잠금 해제)됩니다. 이러한 베스팅 메커니즘은 이해당사자와 프로토콜의 성공 사이에 장기적인 이해관계 정렬을 유도하며, vCOW 토큰은 완전히 베스팅되기 전까지는 양도할 수 없습니다. 이는 토큰 보유자의 이익이 CoW Protocol의 건전성과 번영에 긴밀히 연동되도록 하기 위한 장치입니다.

3. 참고자료

<https://docs.cow.fi/>

위험고지 안내 Disclaimer

본 문서에 기재된 정보는 당사(코인원)가 본 가상자산 심사 시점에 접근 가능한 정보 채널을 통하여 확인한 것으로, 정확하지 않거나 투자시점에는 변경 또는 유효하지 않을 수 있습니다.

가상자산 발행자가 공시한 내용 및 백서를 통해 정확한 정보를 확인하신 후 투자하시기 바랍니다.

가상자산은 법정화폐가 아니므로 특정 주체가 가치를 보장하지 않습니다.