

카우프로토콜(CoW Protocol)

해당 번역본은 이용자가 디지털자산 관련 정보를 편리하게 확인할 수 있도록
단순 참고용으로 번역된 것이며, 투자 권유를 목적으로 하지 않습니다.
그 내용이 정확하지 않을 수 있으므로 정확한 정보 습득을 위해서는
원문을 참고하시거나 원문 작성 주체 측에 문의하시기 바랍니다.
두나무는 해당 번역본 내용의 진실성 및 정확성을 보장하지 않고,
제공된 정보에 의한 투자 결과에 대하여 어떠한 책임도 지지 않으며,
투자 손실은 투자자에게 귀속됩니다.

CoW DAO

CoW DAO는 이더리움에서 가장 사용자 보호적인 제품을 혁신하는 것을 목표로 하고 있다.

현재 CoW DAO의 세 가지 주요 제품은 [CoW Protocol](#), [MEV Blocker](#), 그리고 [CoW AMM](#)이다. CoW DAO는 이를 개발 및 마케팅 자원으로 지원하며, [CoW Grants Program](#), [CoW Protocol Explorer](#), 그리고 [CoW Swap 프런트엔드](#)를 포함한다.

CoW Protocol이란?

CoW Protocol은 가격 발견 메커니즘으로 공정한 조합적 배치 경매([fair combinatorial batch auctions](#))를 활용하는 완전한 퍼미션리스(무허가형) 거래 프로토콜이다. CoW Protocol은 이러한 공정한 조합적 경매를 통해 [Coincidence of Wants \(CoWs\)](#)를 통한 유동성을 극대화하고, 필요할 경우 모든 온체인 유동성을 활용한다.

MEV Blocker란?

MEV Blocker는 프론트러닝(front-running)과 샌드위치(sandwich) 같은 MEV(Maximal Extractable Value) 공격으로부터 사용자 트랜잭션을 보호하도록 설계된 RPC 엔드포인트다. MEV의 위험으로부터 사용자를 보호하는 것 외에도, MEV Blocker는 서처(searcher)와 빌더(builder) 간의 오더 플로우 경매를 활용하여 사용자가 백러닝(backrunning)으로부터 리베이트를 받을 수 있도록 한다.

CoW AMM이란?

CoW AMM은 [LVR](#) 형태의 가격 착취로부터 LP(유동성 공급자)를 보호하기 위해 처음부터 새롭게 설계된 새로운 유형의 AMM이다. 유동성 공급자는 자신의 토큰이 수익을 창출하길 기대하지만, 대부분의 유동성 풀은 가격 지연(stale price)을 고려하면 실제로는 수익성이 없다. 차익거래자(arbitrageur)는 이러한 지연된 가격을 이용해 LP에게 손실을 입힌다. CoW AMM은 이러한 LVR 문제를 근본적으로 해결하며, Balancer와 Uniswap의 기준 풀보다 더 높은 성과를 입증한 유동성 풀을 제공한다.

거버넌스(Governance)

CoW DAO는 커뮤니티의 것이며, 커뮤니티에 의해, 커뮤니티를 위해 운영된다. CoW DAO는 커뮤니티가 프로토콜의 방향을 완전히 통제할 수 있도록 [탈중앙화된 거버넌스 모델](#)을 사용한다.

등록되지 않음 ×

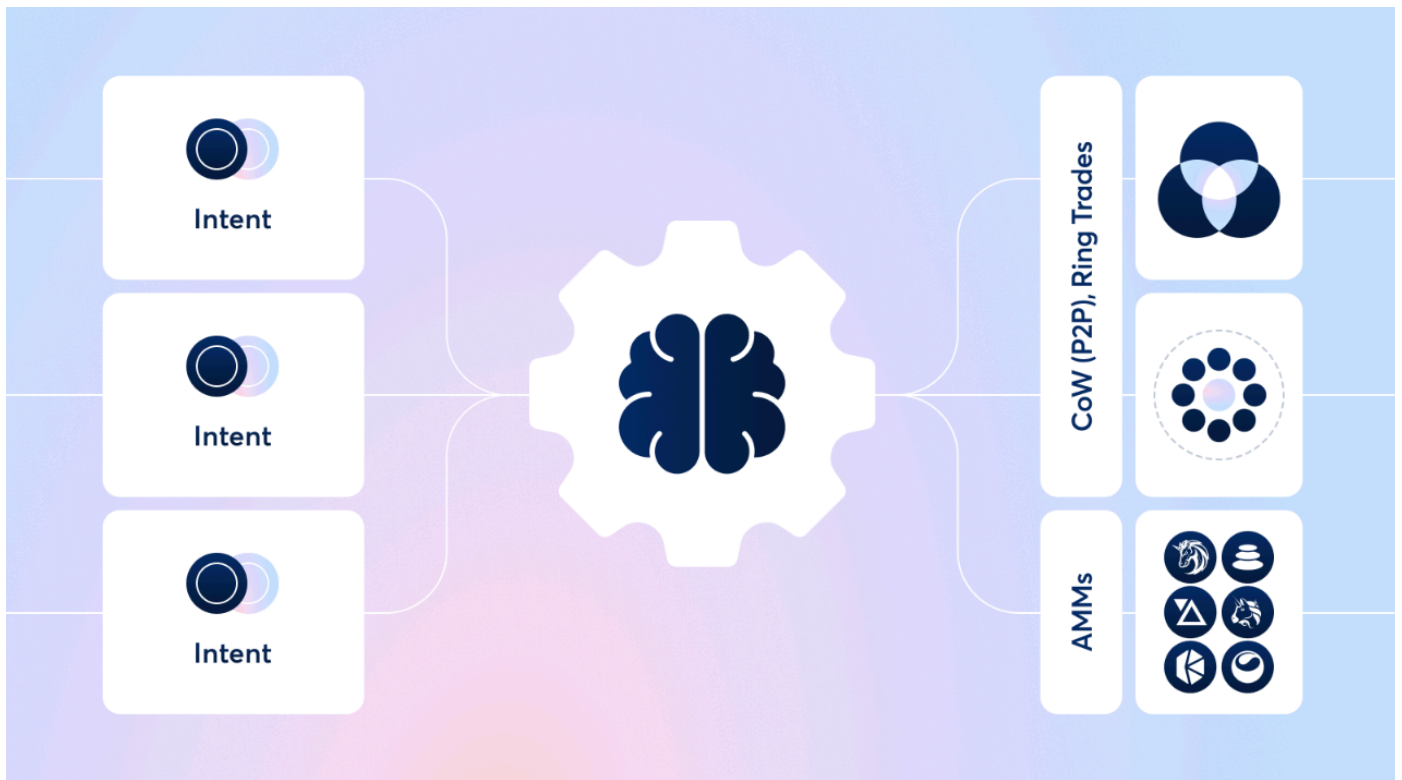
CoW DAO 문서 활용법 (How to use CoW DAO's documentation)

CoW DAO의 문서는 “Concepts”, “Tutorials”, “Technical Reference”의 구조를 따른다. 예를 들어 사용자가 배우고자 하는 것이 있을 때 다음과 같이 접근할 수 있다:

- 무엇인지 알고 싶을 때 (예: 배치 경매) → [Concepts](#) 참조
- 어떻게 하는지 알고 싶을 때 (예: 주문 생성) → [Tutorials](#) 참조
- 기술적 정보를 알고 싶을 때 (예: SDK, API 등) → [Technical Reference](#) 참조

CoW Protocol

CoW Protocol은 거래 의도(trade intents)와 공정한 조합적 배치 경매(fair combinatorial batch auctions)를 활용하여 암호화 자산 거래 시 더 나은 가격을 제공하는 메타 DEX 집계 프로토콜(meta-DEX aggregation protocol)이다.



이 프로토콜은 솔버(solvers)라 불리는 제3자에 의존해 거래 의도의 최적 실행 경로를 찾는다. 거래 의도는 이더리움 및 EVM 호환 체인에서 트랜잭션 실행 조건을 지정하는 서명된 메시지다.

사용자의 거래 의도가 처음 접수되면, 프로토콜은 이를 다른 의도들과 함께 배치(batch)로 묶는다. 거래 의도를 실행할 때, 솔버는 먼저 현재 배치 내에서 Coincidence of Wants (CoW)를 찾아 온체인 유동성보다 더 나은 가격을 제시할 수 있는지 확인한다. CoW가 없을 경우, 솔버는 모든 온체인 및 오프체인 유동성을 탐색해 배치 내 거래 의도 집합에 대한 최적의 가격을 찾는다.

유동성 출처는 다음과 같다:

- AMMs (예: Uniswap, Sushiswap, Balancer, Curve 등)
- DEX 집계기 (예: 1inch, Paraswap, Matcha 등)
- 개인 마켓 메이커

솔버가 접근할 수 있는 폭넓은 유동성 덕분에 CoW Protocol은 메타 DEX 집계기, 즉 “집계기의 집계기(agggregator of aggregators)”로 기능한다.

CoW Protocol이 사용하는 개념에 대해 더 알고 싶다면 [Concepts](#)를 참고하라.

CoW Protocol 또는 CoW Swap 사용법은 [Tutorials](#)에서 확인할 수 있다.

기술적 세부 사항은 [Technical Reference](#)에서 확인할 수 있다.

개념 (Concepts)

소개 (Introduction)

의도 (Intents)

Uniswap이나 SushiSwap처럼 *온체인에서 직접 실행되는 원시 트랜잭션(raw transaction)* 을 서명하여 주문을 제출하는 대신, CoW Protocol 사용자는 “*거래 의도(intent to trade)*” *메시지* 를 서명하여 주문을 제출한다. 이 메시지는 거래하고자 하는 자산과 수량 등의 파라미터를 지정하며, 솔버가 사용자를 대신해 해당 자산과 수량으로 거래를 실행할 수 있도록 한다.

의도 기반 거래에는 여러 가지 [금융적](#), [기술적](#) 이점이 있다.

의도의 금융적 이점 (Financial Benefits of Intents)

사용자가 온체인에서 직접 거래를 실행할 경우, 실행 경로는 고정되며, 트레이더는 AMM이나 집계기가 제공하는 가격($\pm$ 슬리피지)을 그대로 받는다.

의도 기반 구조 덕분에, CoW Protocol은 최적의 실행 경로를 찾는 역할을 [솔버](#)라 불리는 전문 제3자에게 위임한다. 솔버는 사용 가능한 모든 온체인 유동성을 탐색할 뿐 아니라, 다음과 같은 다양한 방식으로 추가적인 가격 개선을 제공한다:

- [Coincidence of Wants](#): 동일한 토큰 페어에 대해 반대 방향의 매수/매도 의도를 가진 두 명 이상의 사용자를 직접 P2P(피어 투 피어) 방식으로 매칭한다. 이 최적화는 배치 경매를 통해 가능하며, 유동성 공급자(LP) 수수료를 피하고 외부 스마트 계약 호출이 필요 없어 가스 비용도 절감된다.
- 개인 마켓 메이커 유동성: 많은 솔버는 CEX 재고, 개인 마켓 메이커 통합, 혹은 자체 유동성을 통해 오프체인 유동성에 접근할 수 있다. 이를 통해 솔버는 특정 시점의 온체인 AMM보다 더 나은 가격으로 거래를 체결할 수 있다.
- [MEV 보호](#): CoW Protocol에서는 사용자가 MEV 봇에 노출되지 않는다. 대신 솔버가 사용자를 대신해 거래를 결제하며, 모든 MEV 리스크를 부담한다. 또한 솔버는 모든 주문을 동일한 배치 내에서 균일한 결제 가격으로 제출하기 때문에, 거래 순서를 재배열하여 이익을 얻는 것이 불가능하다. (MEV 착취의 근본 원인 제거)

의도의 기술적 이점 (Technical Benefits of Intents)

CoW Protocol의 의도 기반 구조는 여러 기술적 이점을 제공한다:

- [솔버](#)가 특정 지침과 온체인 조건에 따라 다양한 트랜잭션(단순 거래뿐 아니라)을 실행할 수 있도록 한다. 이는 [CoW Hooks](#) 및 [Programmatic Orders](#)와 같은 기능을 가능하게 한다.
- 온체인에서 거래가 체결되는 방식에 대한 추가 규칙을 설정할 수 있다. 예를 들어, 거래가 [EBBO](#) (Ethereum Best Bid and Offer)에서 체결되도록 보장하고, 동일 배치 내 동일 토큰 페어 거래는 동일한 가격으로 결제되도록 보장한다.
- 사용자가 체인 네이티브 토큰(예: ETH)을 보유하지 않아도 [판매 토큰\(sell token\)](#)으로 가스 요금을 지불할 수 있다.
- 실패한 트랜잭션에 대한 수수료를 제거한다.

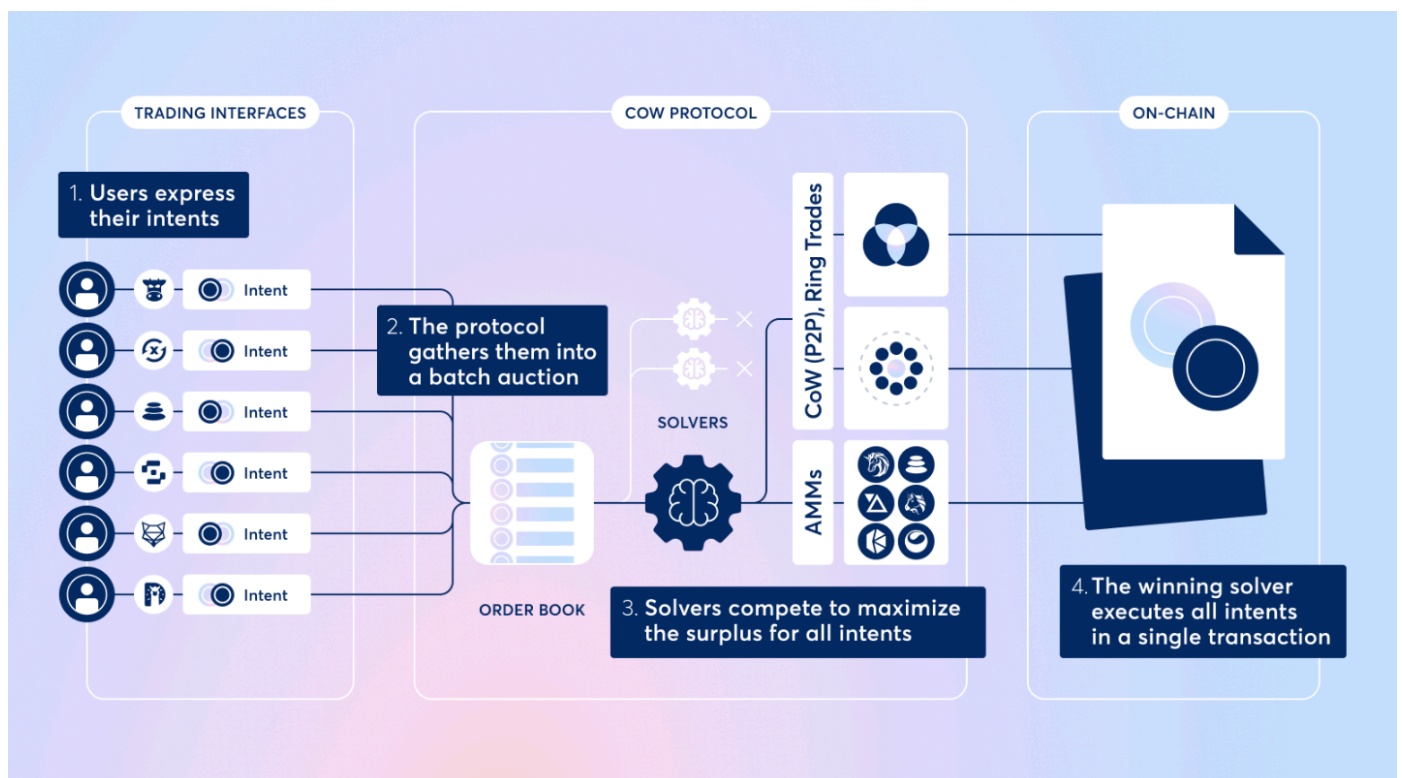
- 사용자가 여러 주문을 동시에 제출할 수 있다.
- 프로토콜이 주문을 배치 단위로 결제할 수 있게 하여 Coincidence of Wants와 가스 절약에서 오는 효율성을 창출한다.

동작 원리 (How it works)

주문의 흐름 (Flow of an order)

실행 가능한 온체인 트랜잭션을 생성하는 대신, CoW Protocol 사용자는 서명된 거래 의도(intent to trade) 메시지로 주문을 제출한다. 이는 솔버가 온체인에 커밋하기 전에 주문 배치에 대한 최적의 실행 경로를 찾을 수 있게 한다.

이제 CoW Protocol을 통해 주문이 흐르는 과정을 살펴보면서 지금까지의 핵심 개념을 모두 연결해 보자.



CoW Protocol에서 하나의 주문은 4개의 주요 단계를 거친다:

1. 사용자는 거래하고자 하는 자산과 수량 등 파라미터를 지정하는 메시지에 서명함으로써 거래 의도를 표현한다.
2. 프로토콜은 여러 사용자의 의도를 공정한 조합적 배치 경매로 모은다.
3. 솔버는 해당 배치에 대한 결제 방안을 제안할 수 있는 제한된 시간을 갖는다. 배치에 대해 가장 많은 잉여(surplus)를 생성할 수 있는 솔버가 승자로 선언된다.
4. 승리한 솔버는 사용자를 대신해 배치 트랜잭션을 온체인에 제출한다.

승리한 솔버가 배치의 주문을 온체인에서 실행하면, 사용자는 자신의 토큰을 수령한다.

배치 경매에서 솔버 간의 경쟁은 사용자(트레이더, DAO, 스마트 컨트랙트, 봇 포함)가 항상 거래에 대해 최적의 가격을 받도록 보장한다.

까다로운 일을 솔버가 처리하기 때문에, 사용자는 최적의 유동성 풀을 찾거나, 적절한 가스 가격을 설정하거나, 최적의 슬리피지 허용치를 고르는 문제를 걱정할 필요가 없다. 솔버는 또한 MEV 회피에 능숙하므로, 사용자는 프런트러닝과 샌드위치 공격을 통해 가격을 악용하는 MEV 봇으로부터 자신의 주문이 보호된다는 점을 안심할 수 있다.

욕구의 일치 (Coincidence of Wants)

CoW (Coincidence of Wants): 서로 상대가 필요로 하는 자산을 각각 보유한 두 당사자가 동등한 물물교환 방식으로 자산을 직접 교환하는 경제적 현상.

CoW Protocol의 배칭 메커니즘 덕분에, 동일한 자산을 거래하는 경우 사용자들은 피어 투 피어 방식으로 스왑을 수행할 수 있다.

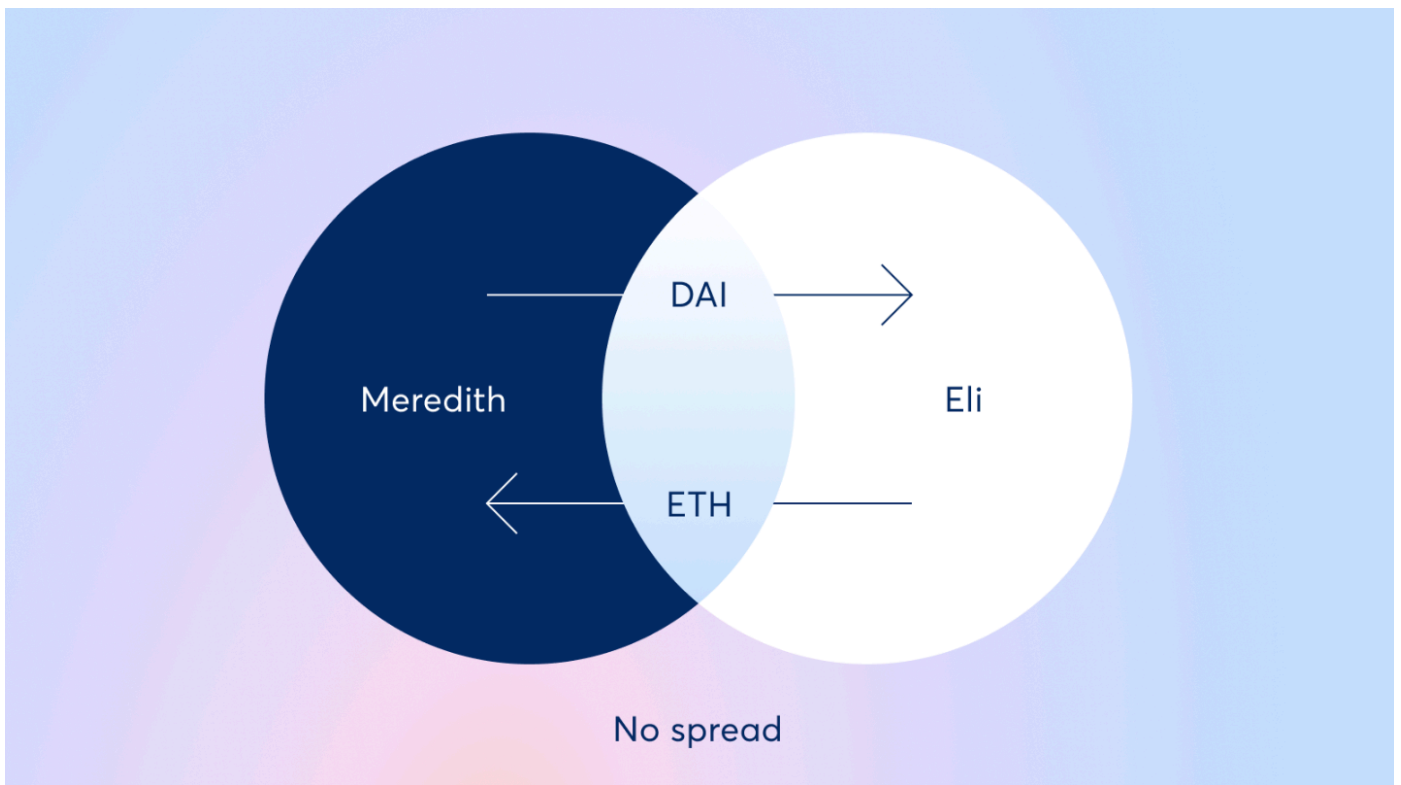
예를 들어, 한 배치에서 한 트레이더가 2,000 USD 상당의 DAI를 0.5 ETH로 매도하려 하고 같은 배치의 다른 트레이더가 0.5 ETH를 2,000 USD DAI로 매도하려 한다면, CoW Protocol의 솔버는 두 트레이더를 매칭하여 온체인 유동성에 의존하지 않고 자산을 교환할 수 있게 한다 — 이로써 유동성 공급자 수수료를 피할 수 있다.

CoW는 사용자가 유동성 공급자(LP) 수수료를 우회하도록 해 주며, 주문이 CoW Protocol의 스마트 컨트랙트와만 상호 작용하므로 가스 비용도 줄여 준다.

CoW는 전부 또는 부분일 수 있다. 부분 CoW의 경우, 배치 내 거래 중 하나만이 반대 유동성으로 완전히 체결되며, 나머지를 채우기 위해 솔버가 추가 유동성을 조달해야 한다.

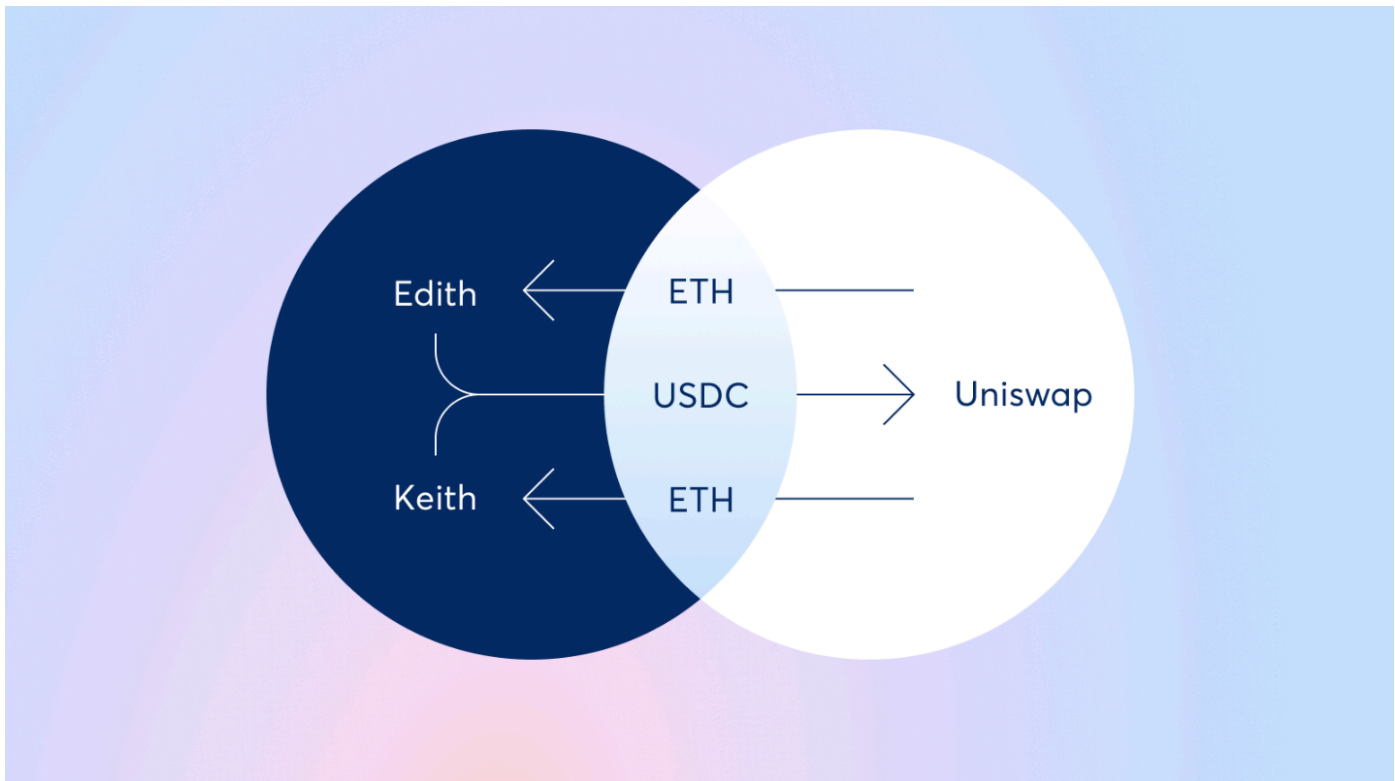
CoW의 유형 (Types of CoWs)

단순 (Simple)



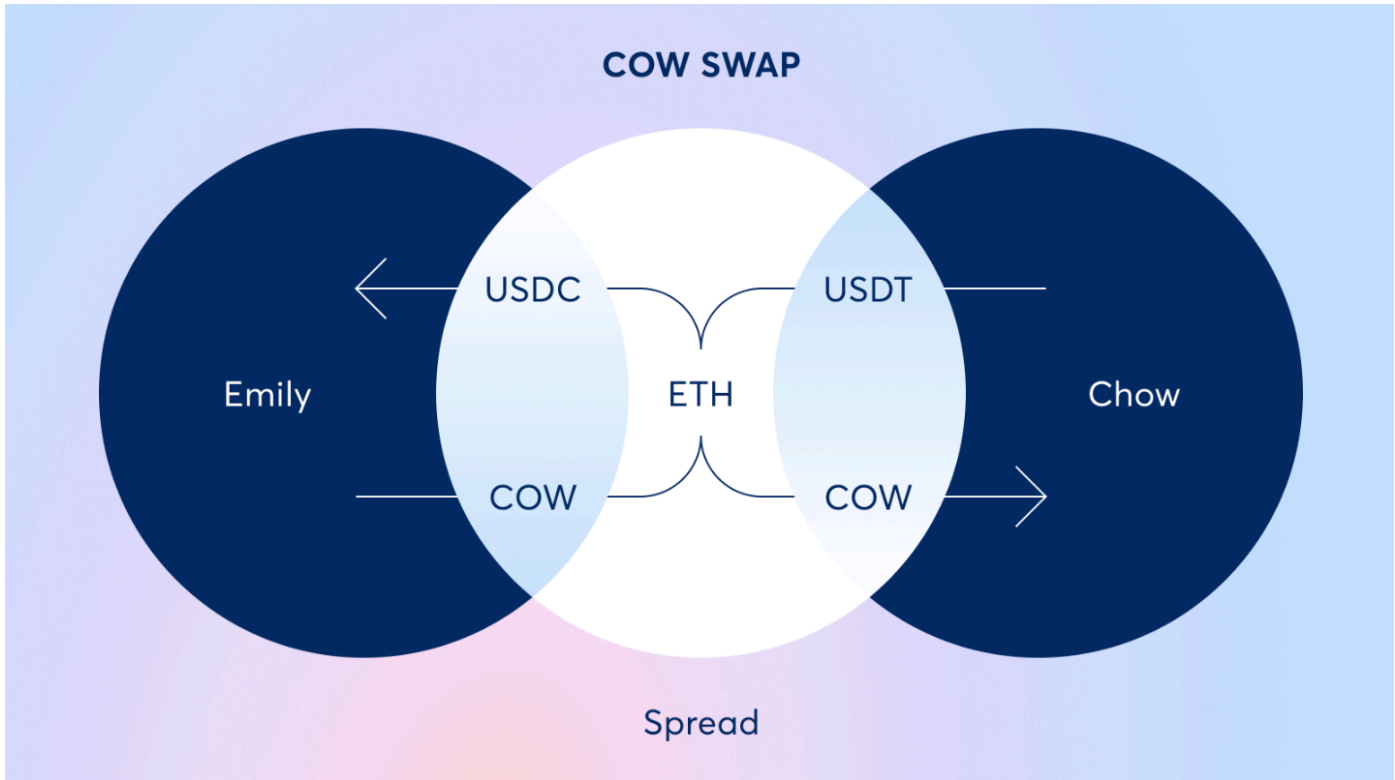
단순 CoW는 두 트레이더가 서로가 매수하려는 것을 각각 매도하는 경우를 의미한다. 이들은 AMM 유동성 풀과 상호작용하는 대신 서로 자산을 교환한다. 단순 CoW는 각 트레이더가 상대가 필요로 하는 정확한 수량을 거래하는 완전한 형태일 수도 있고, 두 트레이더가 반대 자산을 거래하지만 오직 한쪽만 CoW를 통해 전체 유동성을 충족할 수 있는 부분 형태일 수도 있다. 후자의 경우, 거래의 나머지 부분은 온체인으로 넘어가 최종 체결을 완료한다.

배칭 (Batching)



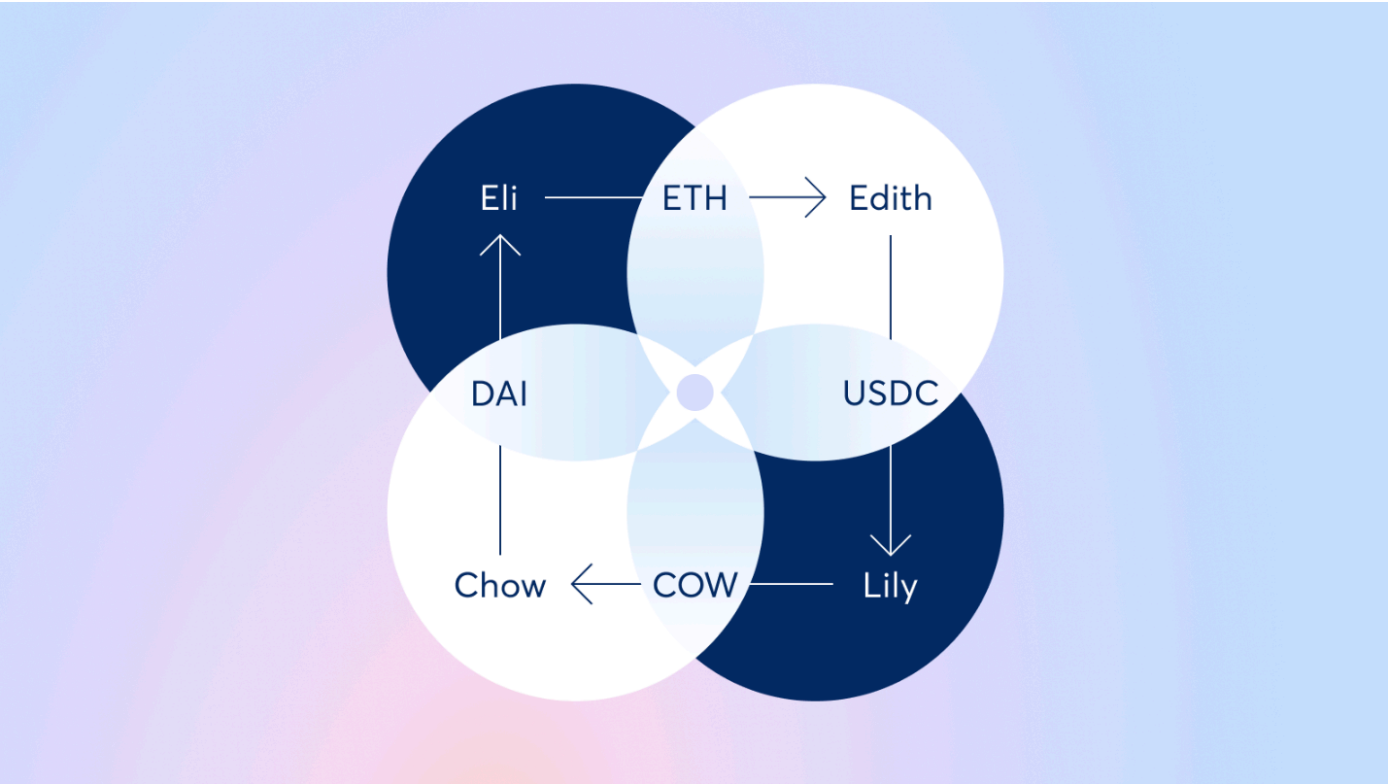
종종 하나의 배치 경매에는 동일한 거래를 수행하려는 서로 다른 사용자들의 여러 의도가 포함된다. 솔버는 이들의 거래를 개별적으로 하나씩 보내는 대신, 모든 의도를 하나로 배치하여 온체인에서 단일 거래로 실행할 수 있다. 배치 CoW는 온체인으로 진행되지만, 이 최적화는 사용자가 AMM 스마트 컨트랙트와 상호작용하는 횟수를 줄여 가스 비용을 절감한다.

중간 (Intermediate)



중간 CoW는 피어 투 피어로 정산될 수 있는 “중간” 거래가 존재할 때 발생한다. 예를 들어, 한 당사자가 CRV를 USDT로 교환하고 다른 당사자가 USDT를 COW로 교환하려는 경우, 중간에 “ETH” 거래가 필요할 수 있다. 첫 번째 트레이더는 CRV→ETH→USDT로, 두 번째 트레이더는 USDT→ETH→COW로 이동해야 할 수 있다. 이 예시에서, 첫 번째 트레이더의 ETH→USDT 거래와 두 번째 트레이더의 USDT→ETH 거래는 CoW로서 피어 투 피어로 체결될 수 있다.

다차원(링) (Multidimensional (Ring))

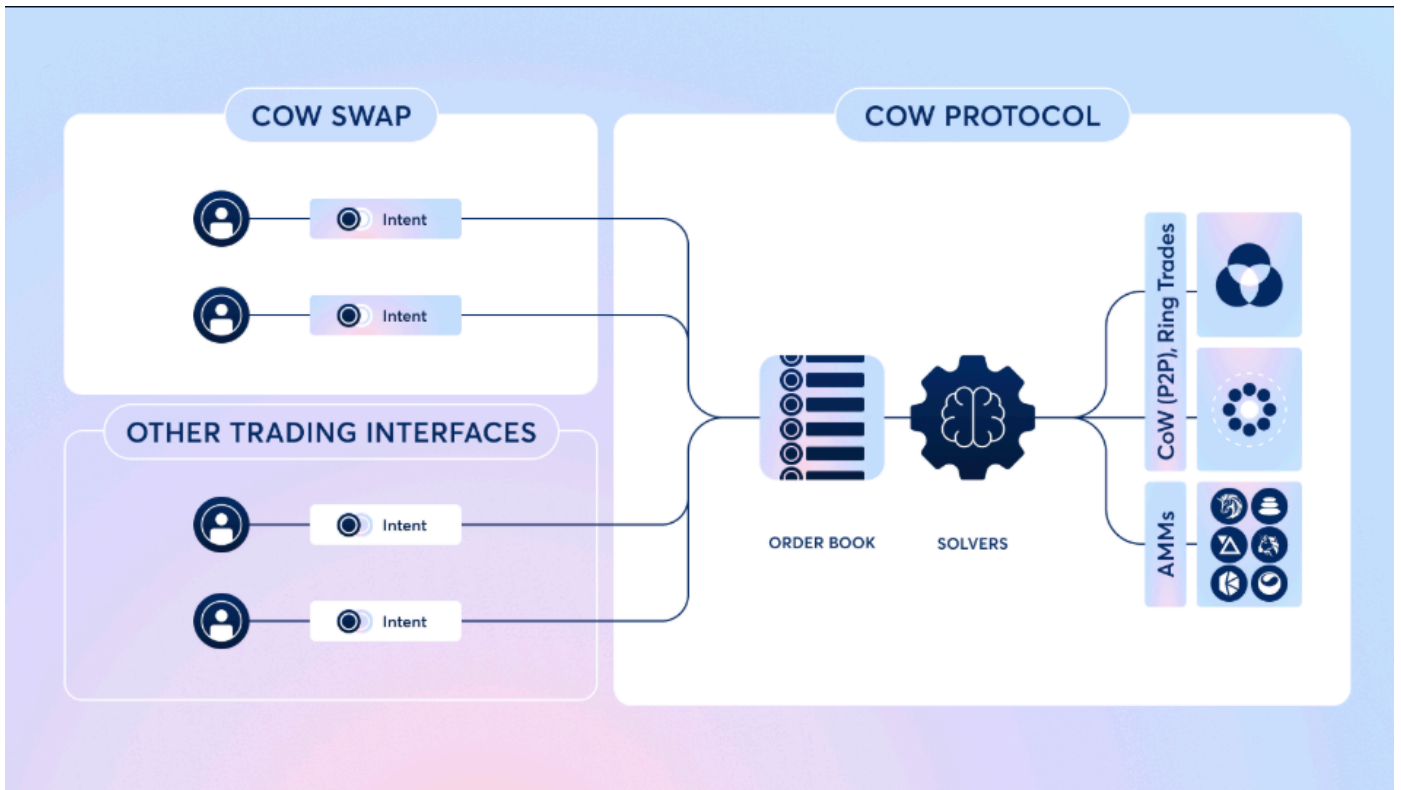


다차원 CoW는 세 명 이상의 사용자가 참여하며 각자의 거래 사이에서 유동성을 공유한다. 일반적으로 여러 자산이 포함되며, 오프체인 유동성 활용을 극대화하기 위해 솔버가 각 사용자에서 다음 사용자로 이어지는 최적 경로를 찾아야 한다.

일부 주문은 전부 CoW를 통해 체결되지만, 많은 주문은 피어 투 피어로 부분만 체결된다. 후자의 경우, 솔버는 주문을 완료하기 위해 필요한 나머지 유동성을 조달하기 위해 자동으로 온체인으로 이동한다.

CoW Protocol 대 CoW Swap (CoW Protocol vs. CoW Swap)

두 가지는 상호 연결되어 있지만, CoW Protocol과 CoW Swap 사이에는 중요한 차이가 있다.



CoW 프로토콜 (CoW Protocol)

CoW Protocol은 의도와 공정한 조합적 배치 경매를 활용하여 최적의 가격을 찾고 Maximal Extractable Value(MEV)로부터 주문을 보호하는 거래 프로토콜이다.

프로토콜은 주문을 배치로 묶고, 솔버라 불리는 제3자 간 경쟁에 의존하여 주어진 배치의 모든 주문에 대해 최적의 실행 가격을 찾는다.

솔버는 사용 가능한 모든 온체인 유동성을 검색하고, 주문 체결을 위해 오프체인의 사설 재고까지 활용한다. 배치 내 두 주문이 반대 자산을 교환하는 경우, 솔버는 이를 피어 투 피어 욕구의 일치(Coincidence of Wants, CoW) 거래로 매칭한다.

솔루션을 찾으면, 솔버들은 주문 배치의 결제 권한을 얻기 위해 경쟁한다. 프로토콜은 솔버 경쟁을 수행하고, 트레이더의 이익을 극대화할 수 있는 솔버를 각 주문 배치의 “승자”로 선택한다. 솔버는 일반적으로 온체인 및 오프체인 유동성 출처의 최적 조합, 가장 효율적인 CoW, 가장 효율적인 기술적 실행, 혹은 이들의 조합을 통해 경쟁에서 승리한다.

CoW 스왑 (CoW Swap)

CoW Swap은 CoW Protocol 위에 구축된 최초의 거래 인터페이스였으며, 현재 사용자가 CoW Protocol로 거래하는 가장 대중적인 방식이다.

Balancer와 같은 기타 거래 앱 및 dApp도 거래 인터페이스에 CoW Protocol을 네이티브로 통합했으며, 숙련된 트레이더는 종종 프로토콜을 통해 직접 거래를 제출한다.

CoW Swap의 UI에는 다음과 같은 고유한 기능이 포함된다:

- 지갑 히스토리
- 사용자 토큰 잔액
- 게임

- 전설적인 “Moo” 사운드
- 포춘 쿠키

CoW Swap은 [Rabby](#), [MetaMask](#), [Trust Wallet](#), [Safe](#), [Trezor](#), [Ledger](#), 그리고 [WalletConnect v2](#)를 지원하는 모든 지갑과 함께 동작한다.

주문 유형 (Order types)

시장가 주문 (Market orders)

시장가 주문은 가능한 한 빨리 현재 시장 가격으로 토큰을 매수 또는 매도하는 주문을 의미한다.

이는 본질적으로 지정가 가격이 현재 시장 가격에 가깝거나 그 이하인 지정가 주문에 해당한다.

사용자가 CoW Protocol에서 시장가 주문을 제출할 때, 해당 시점에 솔버가 찾을 수 있는 최적 가격을 받는 데 동의하는 것이다. 시장가 주문은 전량 체결 또는 취소(fill or kill) 방식이며(부분 체결 가능과 대비됨), 이는 솔버가 주문 전량에 대한 유동성을 찾거나 충분한 유동성이 확보될 때까지 주문 실행을 대기해야 함을 의미한다.

다른 거래소와 마찬가지로, 사용자는 변동성 시장에서도 실행을 보장하기 위해 가격이 일정 비율만큼 변동하는 것을 허용하는 슬리피지 허용치를 지정해야 한다.

Note

다른 DEX와 달리, 너의 슬리피지 허용치는 MEV 봇에 의해 추출될 수 없다(cf. [MEV 보호](#)). 솔버가 네 주문이 포함된 배치 경매 내에서 최적화를 찾을 수 있다면, 더 나은 가격을 받을 수도 있다.

시작하기 (Getting started)

시장가 주문을 만들고 싶다면? [시장가 주문 튜토리얼](#)을 확인하라.

지정가 주문 (Limit orders)

지정가 주문은 특정 만료일 전에 지정된 가격으로 토큰을 매수 또는 매도하는 주문이다.

자산의 시장 가격이 만료일 전에 어느 시점에서든 목표 가격과 일치하면, 주문이 실행된다. 그렇지 않으면 만료된다. 지정가 주문은 시간 민감도가 낮고 가격 민감도가 높은 거래에 이상적이다.

CoW Protocol의 지정가 주문 처리 방식 (How CoW Protocol Does Limit Orders)

CoW Protocol의 [의도 기반 거래 모델](#) 덕분에, 지정가 주문은 다른 DEX의 대응 방식 대비 몇 가지 큰 장점을 갖는다:

- 가스 없는 주문 관리: 트레이더는 가스 비용을 지불하지 않고 지정가 주문을 생성, 수정, 취소할 수 있다.
- 동시 주문: 트레이더는 동일한 암호화폐 잔고로 여러 미체결 주문을 동시에 제출할 수 있으며, 사용자 지갑에 자금이 있는 한 CoW Protocol이 이를 자동으로 체결한다.
- 주문 잉여: 모든 CoW Protocol 주문에서 트레이더는 실행 시점에 결정된 가격을 받는다. 지정가 주문의 경우, 시장 가격이 지정가보다 유리해지면 사용자는 그 우상향 이익을 전부 얻는다(다른 거래소는 자산의 실제 시장 가격과 관계없이 지정가에서 주문을 실행할 것이다). 추가로, 솔버가 더 나은 실행 경로를 찾아 생성하는 모든 가격 개선(예: [욕구의 일치\(CoW\)](#) 발견)은 트레이더의 몫이다.

CoW Protocol의 지정가 주문은 프로토콜의 의도 기반 실행과 공정한 조합적 배치 경매 아키텍처 덕분에 다른 DEX보다 더 유연하며 더 나은 가격을 제공한다.

시작하기 (Getting started)

지정가 주문을 제출하고 싶다면? 지정가 주문 튜토리얼을 확인하라. 또한 블로그의 지정가 주문 글도 읽어볼 수 있다.

TWAP 주문 (TWAP orders)

시간가중평균가격(Time-Weighted Average Price, TWAP) 주문은 CoW Protocol에서 제공하는 고급 주문 유형으로, 대규모 주문을 여러 개의 작은 조각으로 분할한다. TWAP 주문은 가격 영향력을 최소화하면서 대규모 거래를 실행하기에 이상적이다.

TWAP 주문의 작동 방식 (How TWAP Orders Work)

TWAP 주문은 대규모 주문을 일정한 간격으로 거래되는 일련의 일반 지정가 주문으로 분할한다. TWAP 주문을 설정할 때 사용자는 거래를 몇 개의 부분으로 나눌지, 그리고 주문의 총 지속 시간(시간, 일, 주, 심지어 월 단위까지 가능)을 지정한다.

CoW Protocol의 TWAP 주문에는 여러 입력값이 필요하다:

- 자산(Assets): 일반 스왑과 마찬가지로, 교환하려는 자산을 지정한다.
- 가격 보호(Price Protection): CoW Protocol의 TWAP 주문의 고유한 기능 중 하나로, 주문에 대해 사용자가 수용 가능한 최소 시장 가격을 지정할 수 있다. 매수하려는 자산의 가격이 지정한 임계값 아래로 떨어지면, 그 부분의 TWAP 주문은 가격이 다시 회복될 때까지 실행되지 않는다.
- 분할 개수(Number of Parts): 대규모 주문을 몇 개의 부분으로 나눌지 지정한다.
- 총 지속 시간(Total Duration): 주문의 모든 부분이 실행되어야 하는 총 시간을 지정한다.

장점 (Benefits)

TWAP 주문은 특히 대규모 주문의 경우 여러 가지 장점을 제공한다:

- 낮은 슬리피지: 대규모 주문을 작은 조각으로 나누면, 각 조각마다 전체 주문보다 작은 슬리피지 허용치를 설정할 수 있다.
- 낮은 가격 영향: 슬리피지와 마찬가지로, 주문을 여러 조각으로 나누면 유동성 수요를 시간에 분산시켜 가격 충격을 줄인다.
- 주문 잉여의 100% 사용자 귀속: CoW Swap에서는 모든 주문 잉여가 사용자에게 전달된다. 욕구의 일치 (Coincidence of Wants)나 솔버가 찾은 기타 가격 개선 덕분에 주문이 견적보다 좋은 가격으로 실행되면, 그 초과 이익은 사용자에게 전달된다.
- 시장 변동 완화: 트레이더에게 시간가중평균가격을 제공함으로써 TWAP 주문은 시장 변동성을 완화한다.
- 맞춤형 주문 매개변수: 사용자는 TWAP 주문을 몇 개의 부분으로 나눌지 선택하고, 실행 기간을 조정하며, 시장 변동으로 인한 불리한 가격에서의 실행을 방지하는 “가격 보호” 기능을 활성화할 수 있다.

TWAP 주문 요건 (TWAP Requirements)

CoW Protocol을 통해 TWAP 주문을 제출하려면 몇 가지 요건이 있다:

- 이더리움 메인넷에서의 거래는 최소 \$1,000이어야 한다. (Gnosis 체인, Arbitrum One, Base에서는 최소 5)
- 사용자는 업그레이드된 폴백 핸들러를 갖춘 Safe 지갑을 보유해야 한다.

시작하기 (Getting started)

TWAP 주문을 제출하고 싶다면 [TWAP 주문 튜토리얼](#)을 확인하라. 또한 [블로그의 TWAP 관련 글](#)도 읽어볼 수 있다.

프로그래밍 주문 (Programmatic orders)

일반 지갑 외에도 CoW Protocol은 ERC-1271을 구현하는 스마트 컨트랙트 지갑을 지원한다. 이를 통해 사용자는 특정 조건에 따라 실행되는 프로그래머블 파라미터를 가진 주문을 스마트 컨트랙트를 통해 제출할 수 있다.

이러한 주문 유형을 “프로그래밍 주문(programmatic orders)”이라 부르며, 이를 위한 프레임워크를 Programmatic Order Framework라는 이름으로 개발했다.

프로그래밍 주문 생성 및 사용 (Creating & Using Programmatic Orders)

CoW Protocol의 Programmatic Order Framework는 특정 온체인 조건(예: 자산 가격, 지갑 잔고, 경과 시간 등)이 충족될 때 실행되는 조건부 주문을 쉽게 생성할 수 있도록 한다.

이 프레임워크는 CoW Protocol을 통해 주문을 생성하는 데 필요한 모든 보일러플레이트 코드를 처리하므로, 사용자는 주문 로직 코딩에만 집중하면 된다. 또한 프로그래밍 주문 의도는 단일 트랜잭션으로 그룹 단위로 생성, 업데이트, 삭제할 수 있다.

Programmatic Order Framework 덕분에 사용자는 복잡한 거래 전략에서 고급 주문 유형, 포트폴리오 관리, DAO 운영 등 다양한 작업을 몇 줄의 코드로 자동화할 수 있다.

프로그래밍 주문의 활용 사례 (Example Use-Cases of Programmatic Orders)

- 고급 주문 유형: 프로그래밍 주문의 조건부 특성 덕분에 스탑로스(stop-loss), 특정 시간 이후 실행(good-after-time), 익절(take-profit) 등 복잡한 주문 유형을 구현할 수 있다. 실제로 CoW Protocol의 [TWAP 주문](#)은 Programmatic Order Framework 위에 구축되어 있다.
- 지갑 자동화: 다양한 규모의 지갑은 Programmatic Order Framework를 통해 반복적 작업을 자동화할 수 있다. DAO는 급여 지급, 금고 다변화, 수수료 징수 등을 자동화할 수 있고, 개인은 포트폴리오 리밸런싱, 이자 농사, 헤징 전략 등을 자동화할 수 있다.
- 프로토콜 통합: Programmatic Order Framework를 통해 프로토콜은 모든 트랜잭션 유형에 맞춤형 기능을 추가할 수 있다. 예를 들어, DAO 도구 기업은 플러그 앤 플레이 제품을 구축할 수 있고, DeFi 프로토콜은 이 프레임워크를 활용해 대출 청산 등 프로토콜 수준의 반복 트랜잭션을 지원할 수 있다.

시작하기 (Getting started)

Programmatic Order Framework로 개발을 시작하려면 [기술 문서](#)를 확인하라. 또한 [블로그의 프로그래밍 주문 관련 글](#)도 참고할 수 있다.

밀크맨 주문 (Milkman orders)

Milkman은 [CoW DAO Grants 프로그램](#)을 통해 [Yearn Finance](#)와 CoW Protocol이 공동으로 개발한 주문 제출 메커니즘이다.

이 컨트랙트는 사용자가 고정된 가격을 지정하는 대신 가격 피드를 주문에 활용할 수 있게 한다. 이는 주문이 장기적으로도 공정한 시장 가격에서 실행될 수 있음을 의미하며, Milkman은 DAO나 거버넌스 기반 거래에서 인기가 높다.

CoW Hooks는 사용자가 이더리움 상의 임의의 동작(또는 동작 집합)을 CoW Protocol의 주문과 결합할 수 있도록 하며, 슬롯을 활용하여 일련의 동작을 함께 순차적으로 실행한다.

Hooks는 전체 시퀀스를 단일 트랜잭션으로 실행한다. CoW Protocol 모델에 충실하게, 사용자는 트랜잭션 시퀀스가 성공할 때에만 판매 토큰(sell token)으로 가스 비용을 지불한다. 내부적으로 CoW Hooks는 주문에 부착되어 주문 전(pre-hook) 및/또는 후(post-hook)에 실행되는 임의의 이더리움 “호출(call)”이다. 개발자 및 숙련된 트레이더는 코드를 사용하여 스왑 전에(pre-hook) 또는 스왑 후에(post-hook) 특정 작업을 수행하는 의도를 정의할 수 있다.

프리 훅 (Pre-Hooks)

이들은 스왑 전에 실행되는 동작으로, 주문을 “준비(set up)”하기 위해 사용된다. 예시는 다음과 같다:

- 거래 직전에 토큰 언스테이킹
- 매도 직전 에어드랍 수령
- 토큰 승인 서명을 통해 승인과 거래를 하나의 배치된 동작으로 결합

포스트 훅 (Post-Hooks)

이들은 스왑 이후에 실행되어 거래 수익을 활용한다. 예시는 다음과 같다:

- 자금의 L2 브리징
- 자금 스테이킹

시작하기 (Getting started)

CoW Hook 작성 시작을 위해 기술 문서를 참고하라. 또한 블로그의 CoW Hooks 글이나 이 튜토리얼 영상, 이 영상에서도 더 알아볼 수 있다.

담보로 부채 상환하기 (Repay debt with collateral using flash loans)

플래시 론의 주요 활용 사례 중 하나는 담보를 사용해 부채를 상환하는 것이다. 플래시 론을 통해 사용자는 사전에 유동성을 보유하지 않고도 부채 포지션을 종료하거나 축소할 수 있다.

사용자가 대출 상환에 필요한 자산을 미리 보유할 필요 없이, 플래시 론을 통해 필요한 자금을 일시적으로 빌리고, 그 자금으로 부채를 상환하며, 잠금된 담보를 즉시 회수할 수 있다. 담보를 수령한 후에는 이를 스왑하거나 청산하여 빌린 금액을 상환함으로써, 동일한 트랜잭션 내에서 대출을 완결시킬 수 있다.

이 접근법은 사용자가 미리 자산을 매도하거나 외부 유동성을 확보할 필요를 없애며, 부채 포지션을 관리하는 매우 유연하고 효율적인 방법을 제공한다.

담보로 부채를 상환하는 방법 (How to pay back a debt with collateral)

이는 다음과 같은 조건을 가진 매수 주문을 통해 달성할 수 있다:

- 매수 토큰(buy token): 상환해야 하는 플래시 론 자산
- 매수 금액(buy amount): 플래시 론을 상환하는 데 필요한 정확한 금액 (거래가 완료될 만큼 충분해야 하며, 부족할 경우 트랜잭션이 되돌려진다!)
- 매도 토큰(sell token): 담보로 사용되는 자산
- 매도 금액(sell amount): 전체 담보 금액

주문의 수신자는 항상 결제(settlement) 컨트랙트여야 하며, 이를 통해 프로토콜이 사용자를 대신해 상환을 처리할 수 있다.

부채 상환 방식은 대출자(lender)의 컨트랙트 조건에 따라 달라진다. 일부 대출자는 제3자가 담보 토큰을 대출 풀에서 트레이더 주소로 이전하는 것을 허용하지만, 그렇지 않은 경우도 있다.

대출자가 제3자의 담보 이전을 허용하는 경우 (Lender allows a third-party to initiate the transfer of collateral tokens)

이 경우 사용자는 플래시 론으로 빌린 토큰을 사용해 부채를 상환하는 [CoWSHed](#)을 배포하는 프리 혹은 서명할 수 있다. CoWSHed는 사용자가 소유한 ERC-1967 프록시로, 결정적 주소(deterministic address)에 배포된다. 이러한 결정적 배포를 통해 사용자는 pre/post-hook이 있는 cowswap 주문의 수신자로 프록시 주소를 설정할 수 있다. 사용자는 pre/post-hook에 대해 EIP-712 메시지에 서명하며, 해당 서명은 검증된다. 사용자 서명 혹은 사용자의 프록시에서 실행된다. 이를 통해 사용자는 다음과 같은 권한 있는 동작을 안전하게 수행할 수 있다:

- 프록시에서 다른 주소로 자산 전송
- 프록시를 사용하여 Maker CDP나 AAVE 부채 포지션의 담보 추가 또는 부채 상환

CoWSHed를 생성하기 위해 사용자는 CoWSHed SDK를 사용할 수 있다.

기본 사용자 주문은 필요한 플래시 론 상환에만 사용된다. 상환이 CoWSHed를 통해 처리되므로, 사용자는 EOA(외부 소유 계정)나 컨트랙트(예: SAFE 지갑)일 수 있다.

대출자가 제3자의 담보 이전을 허용하지 않는 경우 (Lender does not allow a third-party to initiate the transfer of collateral tokens)

대출자가 제3자가 대출 풀에서 트레이더 주소로 담보 토큰을 이전하는 것을 허용하지 않는다면, 절차는 더 복잡해진다. 이 경우 상환은 소유자의 계정에서 직접 이루어져야 하며, 소유자는 단순 EOA가 아닌 스마트 컨트랙트(예: SAFE 지갑)여야 한다. 이렇게 하면 사용자가 SAFE 서명을 통해 함수 호출을 승인할 수 있으며, 제3자가 실행할 수 있는 담보 토큰 인출 혹은 생성할 수 있다. 담보 소유자가 EOA인 경우에는 이 방법이 불가능하다.

또한 상환은 항상 담보 토큰 자체를 매도하는 방식으로 이루어지지 않을 수 있다. 일부 프로토콜에서는 토큰의 이자 발생 버전을 매도하도록 허용한다. 예를 들어, 담보가 aUSDC(즉, Aave에 예치되어 이자를 받는 USDC)를 나타내는 경우, USDC를 직접 인출하고 매도하는 대신 aUSDC를 매도하는 것이 더 원활한 상환 과정을 보장한다. 이러한 트레이드오프를 이해하면, 대출 프로토콜의 구체적인 요구사항에 따라 올바른 접근 방식을 결정할 수 있다.

플래시 론 (Flash loans)

플래시 론이란? (What is a flash loan?)

플래시 론은 블록체인의 단일 트랜잭션 내에서 대출과 상환이 원자적으로(atomic) 이루어지는 독특한 형태의 대출이다.

플래시 론을 통해 누구나 담보 없이 자산을 대출받을 수 있으며, 트랜잭션 종료 전까지 상환이 완료되어야 한다. 상환되지 않으면 전체 트랜잭션이 되돌려져, 대출은 자동으로 취소된다.

플래시 론은 [EIP-3156](#)에 표준화되어 있지만, 모든 제공자가 이 EIP를 준수하는 것은 아니다. 많은 자금을 보유한 스마트 컨트랙트들은 사용자에게 플래시 론을 통해 자산을 빌릴 수 있는 기능을 제공한다:

프로토콜 (Protocol)	수수료율 (Fee Percentage)	ERC-3156 준수 여부	문서 링크 (Documentation Link)
Aave V3	0.5%*	No	Aave Flash Loans
Uniswap (FlashSwap)	스왑 수수료	No	Uniswap V3 Overview
Balancer V3	0%	No	Balancer Flash Loans
MakerDAO	0%	Yes	MakerDAO DSS Flash
Euler	0%	Yes (via adapter)	Euler Flash Loans

- 이 수수료는 비활성화될 수도 있다.

주요 특징 (Key features)

- 무담보(Uncollateralized): 플래시 론은 동일한 트랜잭션 내에서 상환되도록 설계되었기 때문에 전통적인 대출과 달리 담보가 필요하지 않다.
- 상환 실패 시 트랜잭션 되돌림: 대출이 완전히 상환되지 않으면, 대출과 자금 사용을 포함한 전체 트랜잭션이 원래 상태로 되돌아가 대출자가 손해를 입지 않는다.
- 즉시 실행(Instantaneous): 플래시 론은 즉시 실행되고 결제된다. 일반적으로 차익거래, 담보 교체, 유동성 제공에 사용된다.
- 자금 활용: 사용자는 동일한 트랜잭션 블록 내에서 프리/포스트 훅을 활용하여 빌린 자금으로 다양한 작업(예: 차익거래, 부채 리파이낸싱, 포지션 청산 등)을 수행할 수 있다.

시작하기 (Getting started)

플래시 론 주문을 생성하고 싶다면 플래시 론 튜토리얼을 참고하라.

플래시 론 주문 명시 방법 (How to specify an order with flash loan)

플래시 론은 `appData` 메타데이터에 선택적 객체로 인코딩된다. 이 정보는 솔버에게 힌트를 제공하지만, 솔버는 보다 최적화된 실행을 위해 다른 접근 방식을 선택할 수 있다.

주문을 생성할 때는 플래시 론의 가스 오버헤드를 슬리피지 허용치에 포함시켜야 한다.

```
{
  "flashloan": {
    "lender": "0x1111111111111111111111111111111111111111",
    "borrower": "0x2222222222222222222222222222222222222222",
    "token": "0xdAC17F958D2ee523a2206206994597C13D831ec7",
    "amount": "1000000"
  }
}
```

- lender: 자금을 빌릴 때 사용할 수 있는 컨트랙트. 예를 들어, [ERC-3156](#)을 준수하는 모든 대출자 컨트랙트에는

0x60744434d6339a6B27d73d9Eda62b6F66a0a04FA, AAVE에는
0x87870Bca3F3fD6353C3F4ce8392D69350b4fA4E2.

- borrower (optional): 빌린 토큰을 수령할 주체. 값이 제공되지 않으면, 주문 소유자의 주소가 borrower로 사용된다.
- token: 대출이 필요한 토큰.
- amount: 대출이 필요한 토큰의 아톰 개수(예: 1 WETH는 10^{18}).

대출 프로토콜이 CoW Protocol과 호환되는 방법 (How a lender protocol can be compatible with CoW Protocol)

대출자가 ERC-3156을 지원한다면 추가적인 스마트 컨트랙트 작업은 필요 없다.

대출 프로토콜이 transferFrom을 통해 borrower의 직접 상황에 의존한다면, 대출 프로토콜은 [Aave Borrower](#) 또는 [ERC-3156 wrapper](#)에 있는 borrower 기능을 구현할 수 있다.

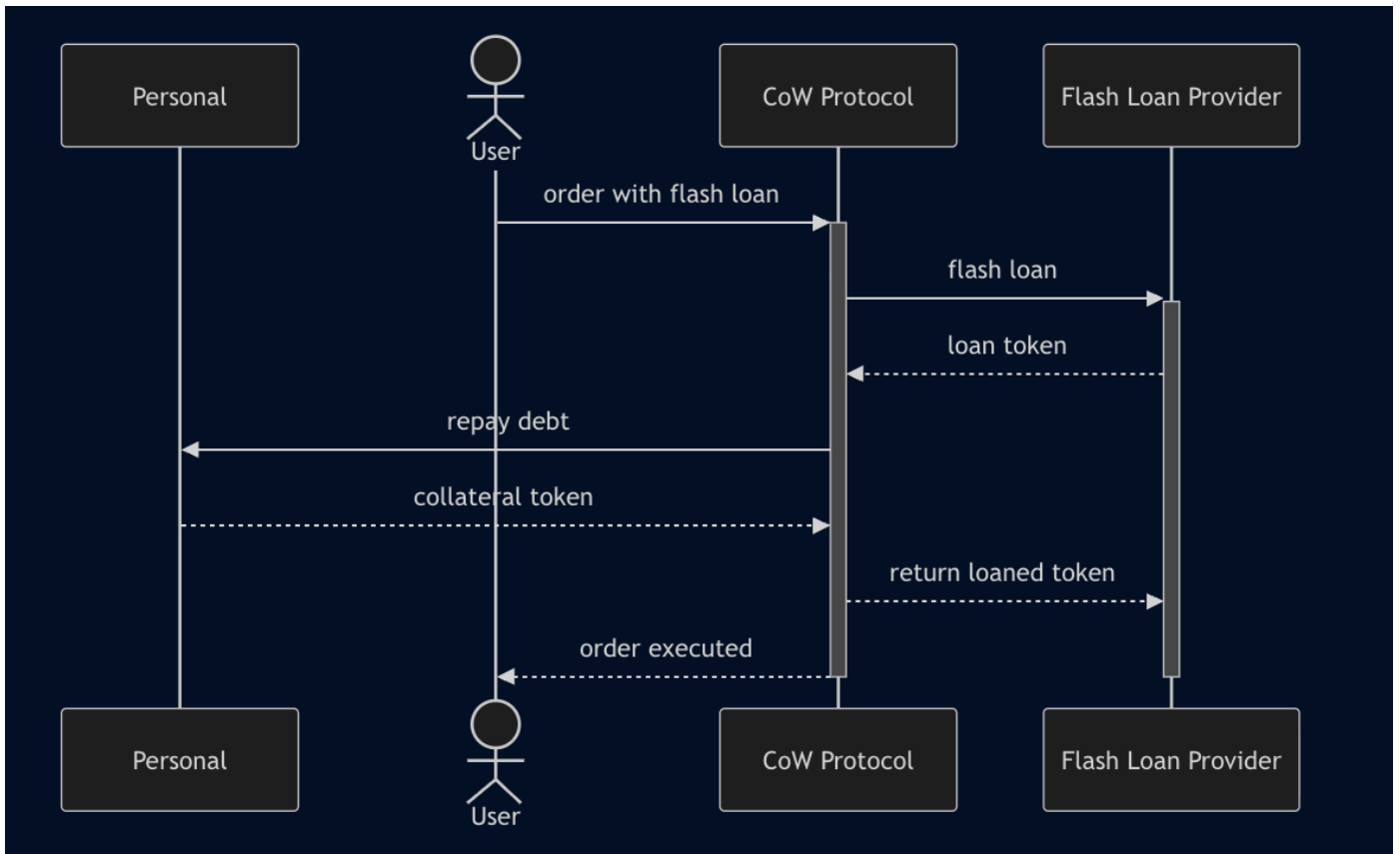
작동 방식 (How does it work?)

플래시 론은 일반적으로 다음 단계로 진행된다:

1. 사용자에게 자금을 선지급한다.
2. 사용자가 대출 자금으로 연산을 실행할 수 있도록 하는 함수를 호출한다.
3. 자금을 대출자에게 반환한다.
4. 잔액 상환되었는지 검증한다.

어떤 단계라도 실패하면 전체 트랜잭션이 되돌려져, 어떤 자금도 이동하지 않는다. 이는 담보가 없어도 플래시 론을 무위험하게 만든다.

사용자는 주문 실행이 끝날 때 결제(settlement) 컨트랙트가 대출자에게 상환하기에 충분한 자금을 보유하도록 보장해야 한다. 예를 들어, 사용자는 프리 혹에서 대출된 토큰을 활용하는 연산(예: 담보를 사용한 부채 상환)을 정의할 수 있다. 그 다음, 사용자 주문 내에서 상환에 필요한 대출 토큰을 얻기 위한 스왑을 수행할 수 있다.



플래시 론 사용 사례 (Flash loans Use Cases)

플래시 론은 다양한 시나리오에서 유용하다. 예를 들어:

- **담보로 미지급 부채 상환:** 플래시 론의 핵심 사용 사례는 담보로 부채를 상환하는 능력이다. 플래시 론을 통해 사용자는 선제적 유동성 없이도 부채 포지션을 종료하거나 축소할 수 있다.
- **레버리지 포지션의 청산 방지:** 트레이더의 담보 가치가 청산 임계값에 근접하면, 플래시 론을 사용해 일시적으로 유동성을 주입하고 부채 일부를 상환하거나 자금을 이동시켜 건전한 담보 비율을 유지할 수 있다. 이러한 선제적 조정은 강제 청산을 방지하고 잠재적 손실을 최소화한다.

이점 (Benefits)

모든 의도 거래 (Trade any intent)

CoW Protocol은 사용자가 이더리움 및 EVM 호환 체인에서 어떤 유형의 거래 의도라도 표현할 수 있도록 하며, 솔버를 활용해 가장 최적의 경로로 트랜잭션을 실행한다.

프로토콜은 표준 시장가 및 지정가 주문은 물론, TWAP 같은 고급 주문 유형을 포함한 임의의 주문 로직을 지원한다. ERC-1271 덕분에 스마트 컨트랙트도 의도를 제출할 수 있으며, 이는 Programmatic Order Framework와 Milkman 같은 컨트랙트를 가능하게 한다.

마지막으로, 의도는 거래에만 국한되지 않는다. CoW Hooks는 사용자가 트레이드 이전 또는 이후에 솔버가 실행하길 원하는 임의의 EVM 호환 동작 집합을 지정할 수 있게 한다.

따라서 온체인 조건에 따라 실행되는 자동화된 거래 전략을 만들든, 브리지와 스왑을 단일 의도에 묶든, 단순히 시장가 주문 하나를 제출하든, CoW Protocol이 이를 지원한다.

MEV 보호 (MEV protection)

CoW Protocol의 주요 이점 중 하나는 모든 주문에 대한 포괄적 MEV 보호다.

MEV(최대 추출 가능 가치)는 이더리움에서 토큰 스왑과 기타 트랜잭션에 영향을 미치는 가격 착취 형태다. MEV 공격은 악의적 트레이더(보통 MEV 봇)가 사용자의 주문 앞뒤로 트랜잭션을 전략적으로 배치해, 사용자의 비용으로 자산 가격을 조작할 때 발생한다 — 이는 일반적으로 "샌드위치 공격"으로 알려져 있다. 지금까지 MEV는 일반 트레이더들에게 수십억 달러 규모의 손실을 야기했다.

MEV 공격은 대부분의 주요 거래소에서 발생한다. 그러나 CoW Protocol의 독특한 거래 모델은 다음 세 가지 방식으로 사용자를 MEV로부터 보호한다:

- **균일 결제 가격(Uniform Clearing Prices)**: 동일한 배치에서 동일한 토큰 페어(예: ETH-USDC)가 여러 번 거래되면, 동일 방향의 각 거래는 동일한 시장 가격으로 결제된다. 이 메커니즘은 “균일 지시 결제 가격”이라 불리며, 트랜잭션 순서를 무의미하게 만들어 MEV 봇이 재정렬로 이익을 추출할 수 없게 한다. 균일 지시 결제 가격은 동일 블록 내 동일한 지시 토큰 페어에 대해 일관된 가격을 확립해, 전통적 Uniswap 유동성 풀과 같은 CFMM 설계로 인해 발생하는 불일치를 해소한다.
- **위임된 거래 실행(Delegated Trade Execution)**: CoW Protocol에서는 솔버라 불리는 채권(stake)을 보유한 제3자가 사용자를 대신해 거래를 실행한다. 이는 사용자가 온체인에서 MEV에 직접 노출되지 않음을 의미한다 (솔버는 노출될 수 있다). 승리한 솔버는 사용자가 서명한 가격 이상을 제공해야 하므로, 잠재적 MEV 공격으로 인한 가격 위험은 솔버가 부담한다. 솔버는 전문 주체이므로, 각 거래에 대해 최적 슬리피지를 계산하고 가능할 때 P2P CoW나 개인 마켓 메이커를 통해 오프체인으로 유동성을 매칭해 MEV 리스크를 줄인다.
- **욕구의 일치(Coincidence of Wants)**: MEV 공격은 AMM의 동학을 이용한 가격 착취에 의존한다. 그러나 주문이 CoW를 통해 피어 투 피어로 매칭될 때는 온체인 유동성에 접근하지 않으므로, MEV로부터 보호된다.

CoW Protocol의 탁월한 MEV 보호에 대해 더 알아보려면 블로그 글을 참고하라.

가격 개선 (Price improvement)

MEV 보호 외에도, CoW Protocol의 또 다른 주요 이점은 가격 개선과 주문 잉여로 이어지는 최적의 가격 실행이다.

CoW Protocol의 모든 주문은 잉여를 포착할 수 있다. 이는 주문 제출 전 받은 견적과 실제 실행 가격 사이에 양의 차이가 있으면, 그 차액을 잉여로 수취한다는 의미다. CoW Protocol은 지정가 주문과 TWAP 주문에도 잉여를 제공한다.

주문이 유의미한 가격 잉여를 얻지 못하더라도, 솔버는 여전히 사용 가능한 모든 온체인 및 오프체인 유동성 전반에서 각 거래의 최적 실행 경로를 찾는다. CoW Protocol에서는 다음과 같은 이유로 다른 DEX나 DEX 집계기보다 더 나은 가격을 받을 수 있다:

- **효율적 주문 라우팅(Efficient Order Routing)**: 솔버는 주문이 실행되는 시점에 배치 내 거래에 최적의 레이트를 얻기 위해 사용 가능한 모든 온체인 유동성을 검색한다. 때로는 가격 충격을 줄이기 위해 거래를 여러 유동성 소스에 분할하기도 한다.
- **비공개 오프체인 유동성(Private Off-Chain Liquidity)**: 솔버는 온체인 유동성보다 더 좋은 가격을 제공하고 다른 DEX나 집계기에 인덱싱되지 않은 개인 마켓 메이커 유동성에 접근할 수 있다.
- **욕구의 일치(Coincidence of Wants)**: 피어 투 피어 욕구의 일치(CoWs)는 트레이더를 서로 매칭하여, 가스 비용이 적고 AMM의 유동성 공급자 수수료를 회피하므로 더 나은 가격을 제공한다. 주문 방향과 거래 페어가 같으면 CoW는 추가적인 가스 절감도 제공한다 — 개별 실행 대신 단일 주문으로 그룹화되기 때문이다.

추가 이점 (Additional benefits)

CoW Protocol의 의도 기반 거래 모델과 배칭을 가능하게 하는 경매 메커니즘은 임의 의도 표현, MEV 보호, 가격 개선 등 다양한 이점을 제공한다.

또한 모든 주문이 상속받는 CoW Protocol 고유의 추가 이점도 있다:

- 가스 없는 거래 (사용자는 판매 토큰으로 결제 수수료를 지불하며, 거래가 배치에 포함되면 결제 수수료가 가스비보다 낮을 수 있다)
- 실패 또는 취소된 주문에 대한 수수료 없음 (대부분의 거래소는 주문이 체결되지 않아도 가스비를 청구한다)
- Ethereum Best Bid Offer 이상에서의 주문 결제
- 동시에 여러 주문 제출 지원
- 모든 주문에 대한 슬리피지 보호

프로토콜의 아키텍처는 중요한 “수동적” 이점도 제공하며, 틈새 거래 사용 사례를 지원한다:

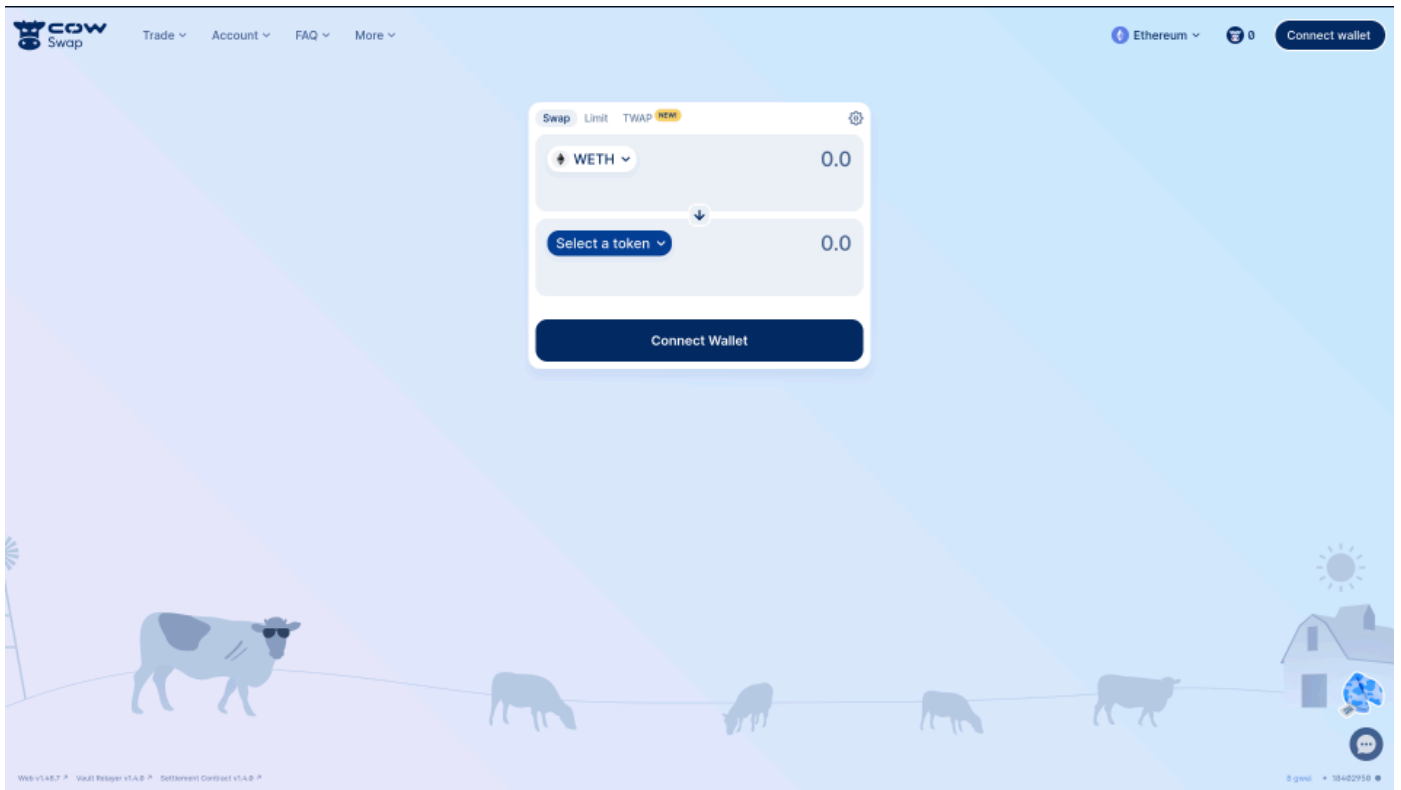
- 모든 온체인 AMM에 대한 익스포저는 솔버가 부담하므로 스마트 컨트랙트 리스크 최소화
- 솔버가 예치, 민팅, 스테이킹 같은 중간 단계를 추상화하므로 이국적 토큰에 직접 접근 가능
- 오프체인 주문의 빠른 결제 덕분에 개인 마켓 메이커로부터 더 촘촘한 스프레드
- 모든 거래가 거래소 컨트랙트로의 입금/출금 없이 사용자 계정에 직접 정산되므로 가스 효율 증가
- 트레이더가 컨트랙트를 승인하고 특정 토큰을 다른 토큰으로 매도하는 주문을 서명한 경우에만 자금 이체가 가능하므로 보안성 향상
- 서명된 주문의 지정가와 수량이 항상 충족됨을 보장
- 서명된 주문에는 만료일이 있으며 온체인에서 취소할 수 있어, 오래된 승인에 의존해 주문이 재실행되는 취약점을 방지
- 슬래싱 대상인 솔버만 배치 경매 결제를 실행할 수 있음
- 중앙 운영자나 CFMM 대신 주문 매칭을 위한 공개 경쟁이 이루어지는 공정하고 탈중앙화된 결제

튜토리얼 (Tutorials)

CoW 스왑 (CoW Swap)

CoW Swap은 CoW Protocol 위에 구축된 최초의 인터페이스로, CoW Protocol을 위한 사용자 인터페이스를 구축하려는 개발자에게 참조 구현(reference implementation)의 역할을 한다.

이 인터페이스는 일반적인 DeFi 사용자에게 매우 익숙하게 느껴질 수 있는데, 이는 Uniswap 인터페이스를 기반으로 만들어졌기 때문이다. 이를 통해 사용자는 친숙한 사용자 경험을 유지하면서도 CoW Protocol의 고유한 기능의 혜택을 누릴 수 있다.



지원 지갑 (Supported Wallets)

CoW Swap은 다음과 같은 다양한 지갑을 지원한다:

- [Rabby](#), [MetaMask](#), [Trust Wallet](#)과 같은 인젝티드(injected) 지갑. 일반적으로 [EIP-1193](#)을 구현한 모든 지갑.
- [Safe](#)와 같은 멀티시그 지갑. [Safe 앱](#) 또는 [WalletConnect\(iOS, Android, Web\)](#)를 통해 연결 가능.
- [WalletConnect v2](#)를 지원하는 대부분의 모바일 지갑.
- [Trezor](#) 같은 하드웨어 지갑 (직접 연결하거나 Rabby, Metamask 등의 인젝티드 지갑 통합을 통해 연결 가능).

[EIP-712](#) 또는 [ERC-1271](#) 서명을 지원하는 지갑을 개발했고, CoW Swap에서 지원받고 싶다면 [이슈 등록](#)을 하거나 [Discord](#)에서 문의할 수 있다.

또는 CoW Swap을 지갑 인터페이스에 직접 통합할 수도 있다. 통합 지원이 필요하다면 bd@cow.fi로 문의하라.

시장가 주문 (Market orders, swap)

스왑은 CoW Protocol의 핵심 기능이다! 이제 토큰을 스왑해보자.

지갑 연결 (Connect wallet)

[CoW Swap](#)에 접속하여 Web3 지갑을 연결한다.

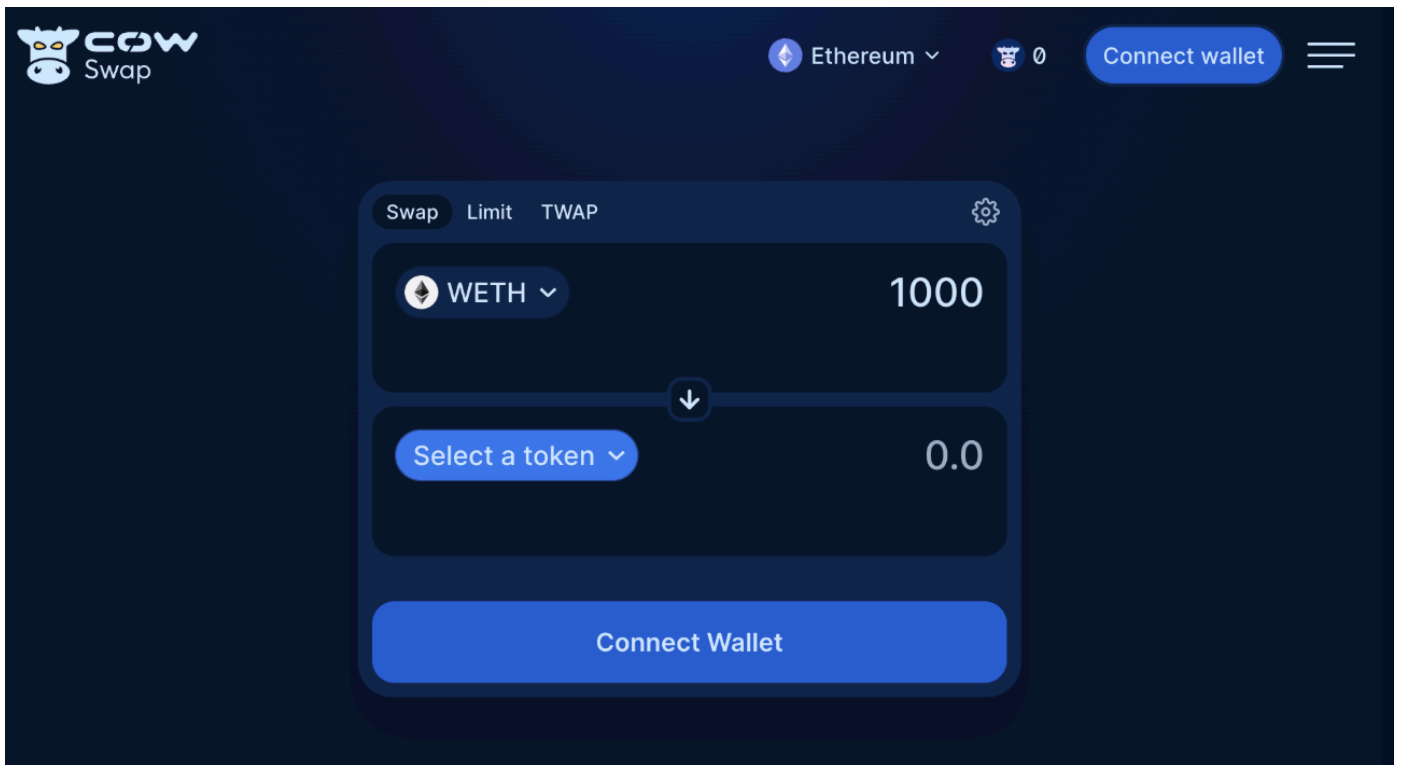
Note

아직 Web3 지갑이 없다면 손쉽게 만들 수 있다. 예시:

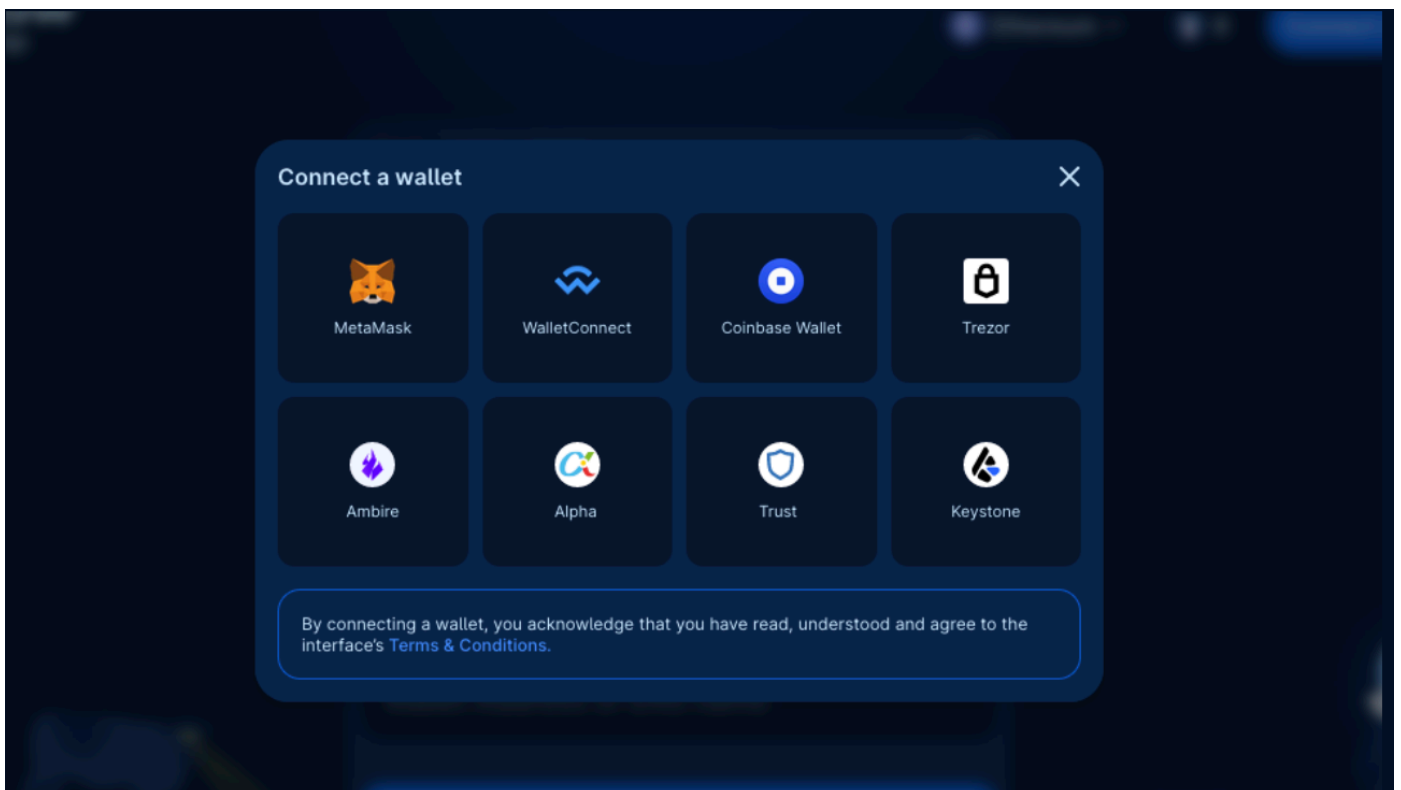
- [Rabby](#) 또는 [Metamask](#) 같은 브라우저 확장형 지갑
- [Trezor](#) 같은 하드웨어 지갑

- Safe 같은 스마트 컨트랙트 지갑

각 지갑의 장단점을 직접 조사하고, 자신에게 가장 적합한 지갑을 선택하라.



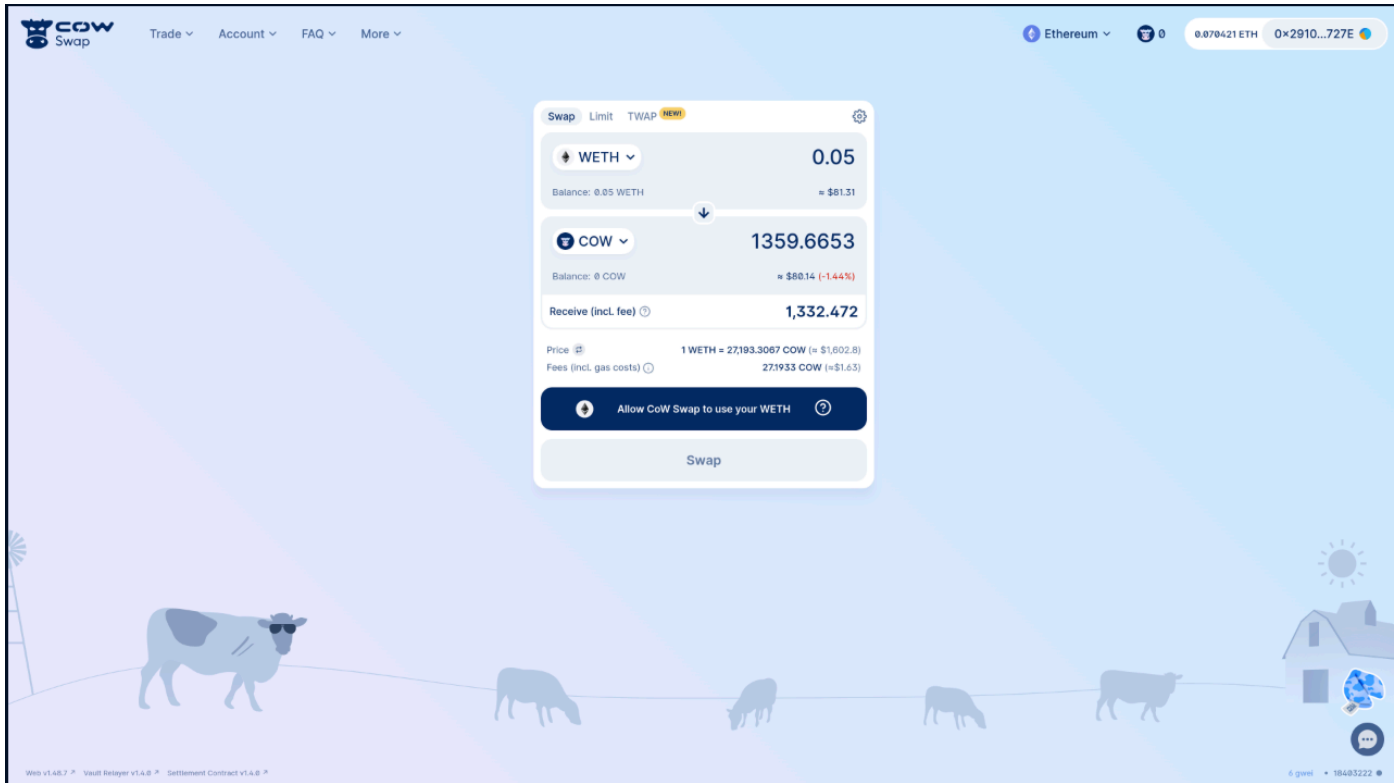
Connect wallet을 클릭한다.



사용 가능한 지갑 중 하나를 선택한다.

토큰 선택 (Select tokens)

예를 들어 0.05 WETH를 COW로 스왑한다고 가정하자.



CoW Swap에서 처음으로 스왑을 수행할 때, vault relayer 컨트랙트가 네 토큰(여기서는 WETH)을 사용할 수 있도록 승인해야 한다. 이 컨트랙트가 사용자의 지갑에서 WETH를 가져와 settlement 컨트랙트로 전달하여 거래를 조정하기 때문이다.

두 컨트랙트 모두 감사를 거쳤고, 전투 검증(battle-tested)을 마친 비업그레이드형(non-upgradeable) 컨트랙트다.

또한 settlement 컨트랙트만이 vault relayer에게 자금을 가져오도록 요청할 수 있으며, 다음 두 가지 조건이 모두 검증된 경우에만 가능하다:

1. 주문이 사용자의 서명으로 이루어졌음
2. 사용자가 설정한 최소 실행 가격 이상을 받을 것임

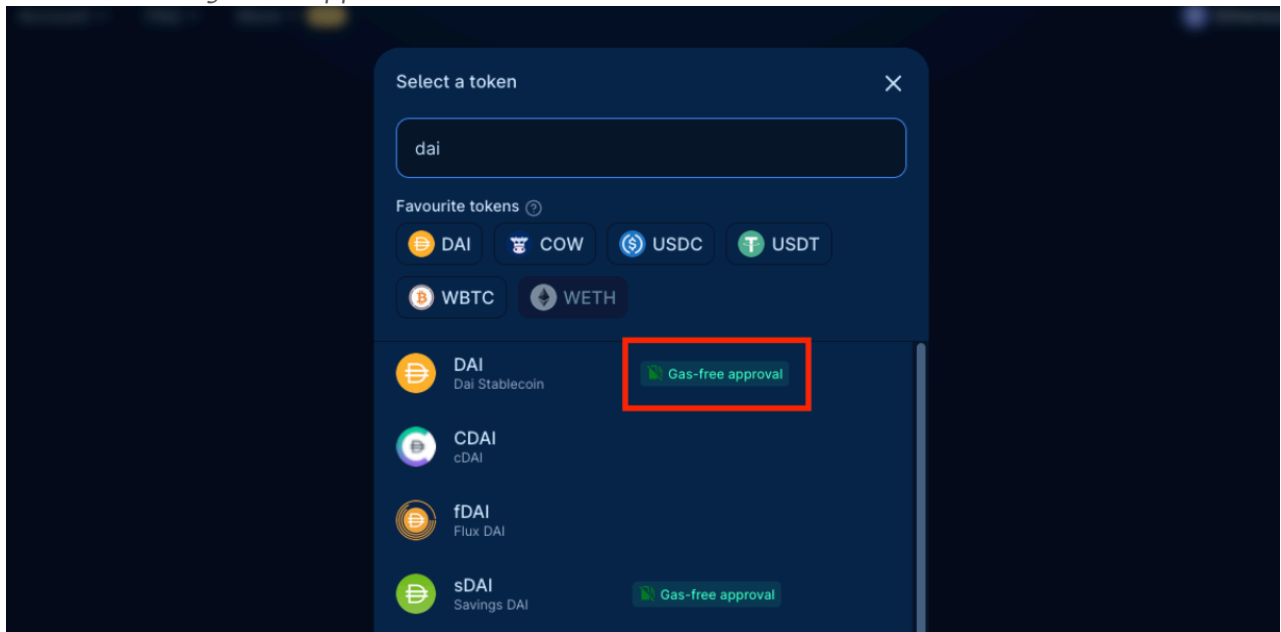
판매 토큰 승인 (Approve sell token)

Tip

USDC, DAI, COW 등 일부 토큰은 가스 없는 승인(gasless approval)을 지원한다. 이는 온체인 트랜잭션에 필요한 초기 가스 없이 vault relayer 컨트랙트가 토큰 사용을 승인받을 수 있다는 뜻이다. 가스비를 절약할 수 있는 좋은 방법이다.

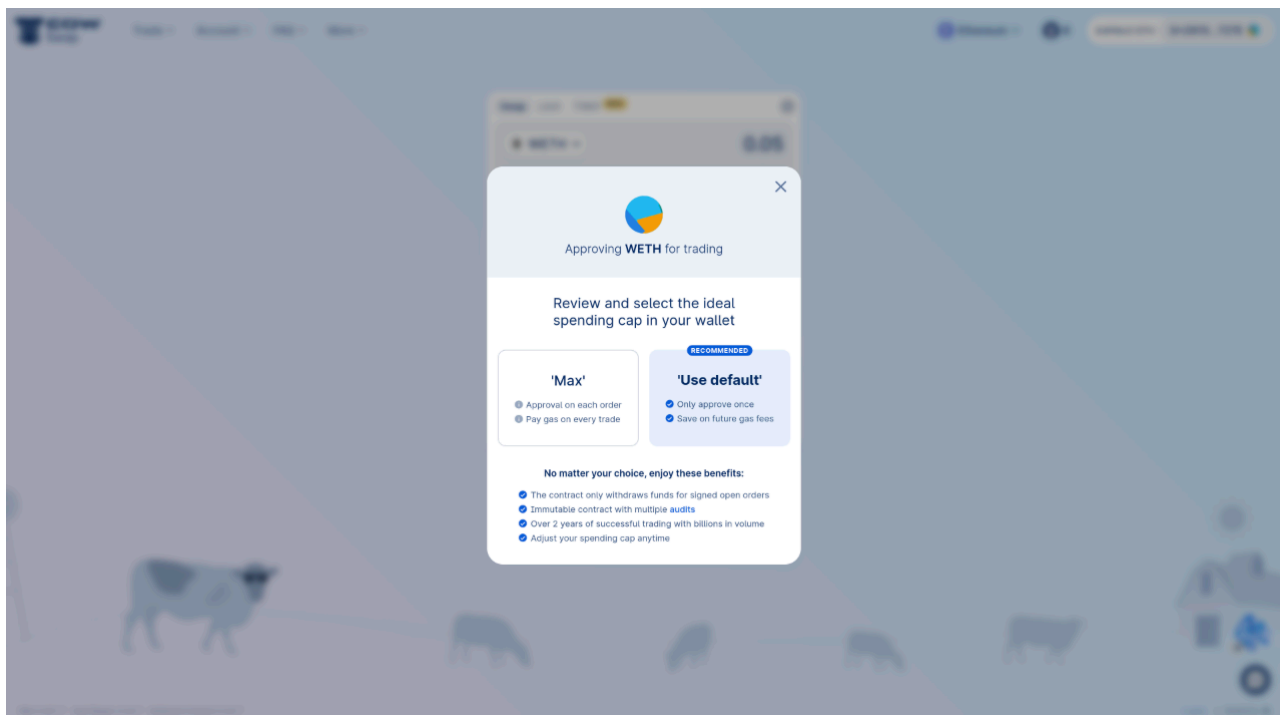
CoW Swap은 토큰이 가스 없는 승인을 지원하는지 자동으로 감지하고, 프로세스를 안내한다.

토큰을 선택할 때 *gasless approval* 표시가 있는지 확인하라.



Note

가스 없는 승인 토큰의 거래는 Swap과 Limit 주문에서 지원되며, 스마트 컨트랙트 지갑에서는 지원되지 않는다.



기본적으로 CoW Swap은 판매 토큰에 대해 vault relay에 “무제한(unlimited)” 허용량(allowance)을 부여하도록 요청한다.

이 방식의 장점은 다음과 같다:

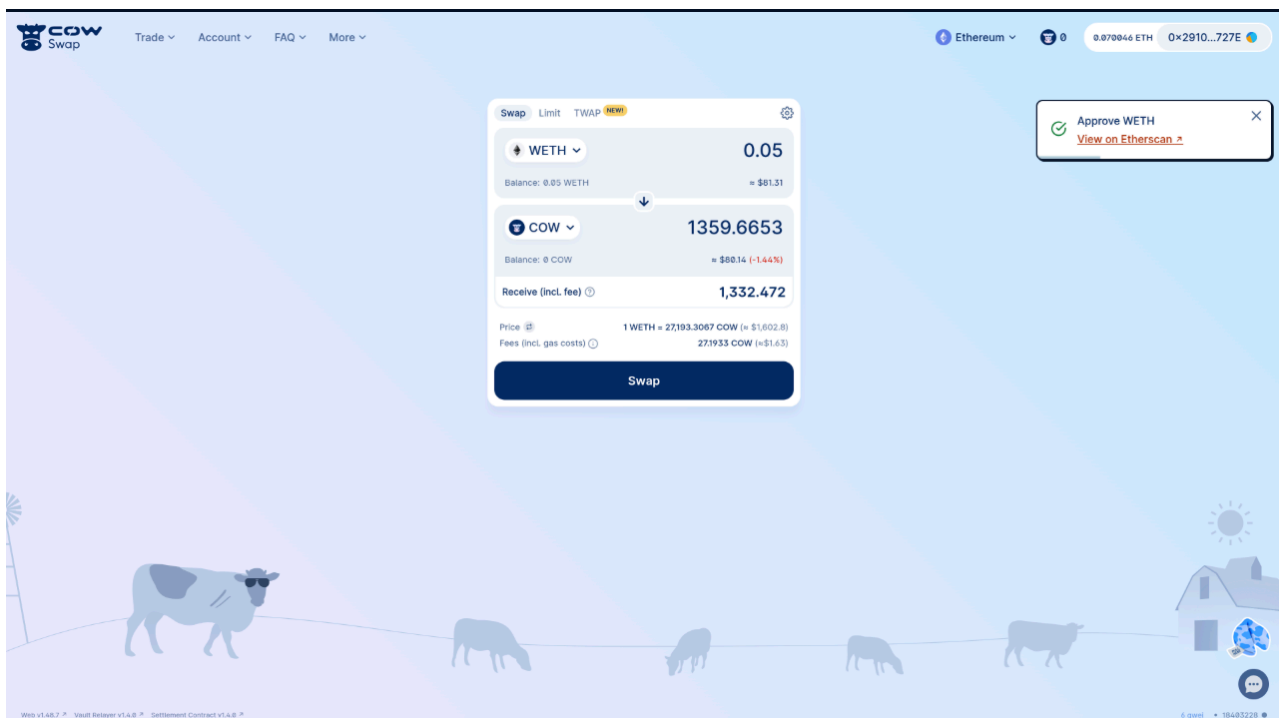
- 거래할 때마다 승인할 필요가 없다.
- 가스비를 절약할 수 있다.

Caution

승인 트랜잭션에 서명할 때는 주의해야 한다. spender 주소가 올바른지(이 경우 GPv2VaultRelayer의 주소) 반드시 확인하라.

의심스러운 경우 트랜잭션에 서명하지 말라. 승인 내역을 검토하려면 revoke.cash를 사용할 수 있다.

approve 트랜잭션이 확인되면, 스왑을 진행할 수 있다.



Tip

Safe 앱으로 CoW Swap을 실행할 때, 승인과 주문 생성 트랜잭션을 하나의 Safe 트랜잭션으로 결합할 수 있다.

SwapLimitTWAP

COW

715.045537673912...

Balance: 715.0455 COW

≈ \$173.51

WXDAI

172.0549

Balance: 91.5826 WXDAI

≈ \$171.95 (-0.9%)

Receive (incl. fee)

172.0546

Price

1 COW = 0.240621 WXDAI (≈ \$0.24)

Fees

0.00034 WXDAI (≈ \$ < 0.01)

Token approval bundling

For your convenience, token approval and order placement will be bundled into a single transaction, streamlining your experience!

Approve COW and Swap

Confirm transaction

Gnosis Chain

CoW Swap

Nonce # 257

Interact with: gno:0x...

Approve access to

This allows contracts to spend the selected amounts of your asset balance.

Token

COW

Unlimited (not recommended)

Spender

gno:0x...

All actions

Expand all | Collapse all

<> 1 approve

<> 2 setPreSignature

Transaction details

multiSend

Transaction status

Create

Confirmed (0 of 1)

Execute

스왑 확인 (Confirm swap)

스왑할 준비가 되면 “Swap” 버튼을 클릭한다.

스왑을 확인하라는 메시지가 표시된다. 이때 건적, 슬리피지 허용치 등 스왑의 세부 정보를 검토할 수 있다.

세부 정보가 만족스럽다면 “Confirm Swap” 을 클릭하고 주문에 서명하라.

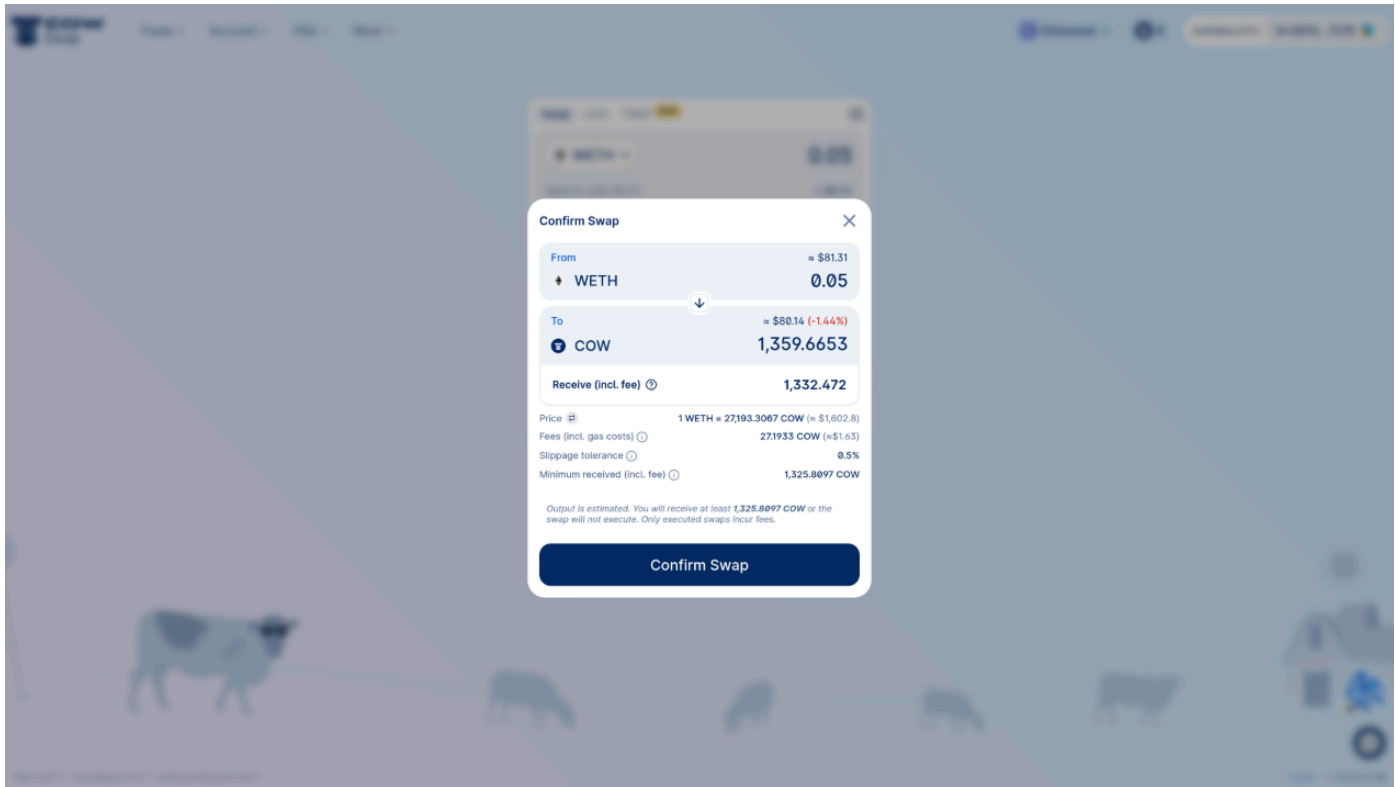
Warning

수신자 주소(receiver address)가 올바른지 반드시 확인하라. 가짜 CoW Swap 웹사이트는 종종 이 매개변수를 자신들의 주소로 바꾼다.

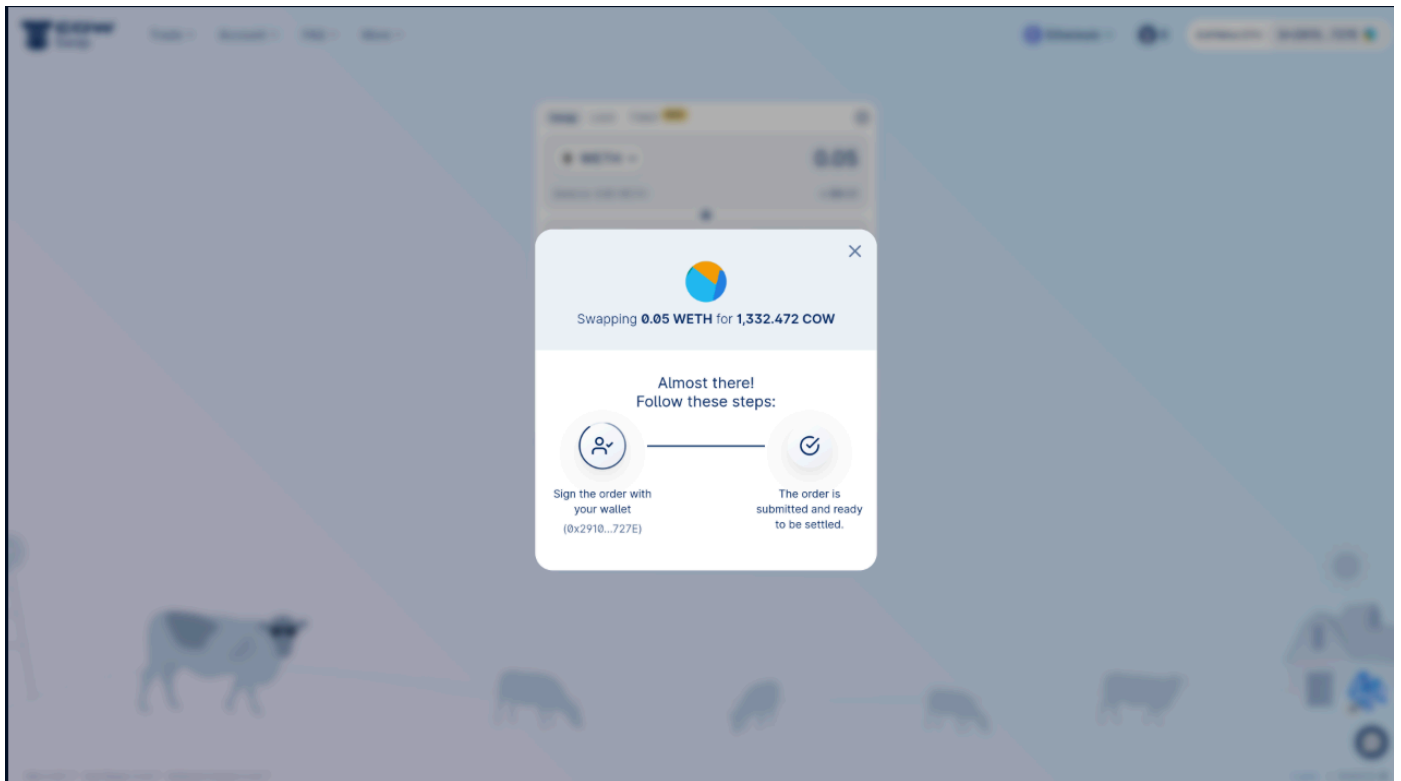
이 값은 0x0...0 또는 주문 서명자의 주소로 설정되어야 하며, 이는 토큰이 주문 서명자 주소로 전송됨을 의미한다. 사용자 지정 수신자를 설정한 경우, 해당 주소가 올바른지 반드시 검증하라.

인터페이스는 receiver address가 서명자 주소와 다를 경우 경고를 표시해야 한다.

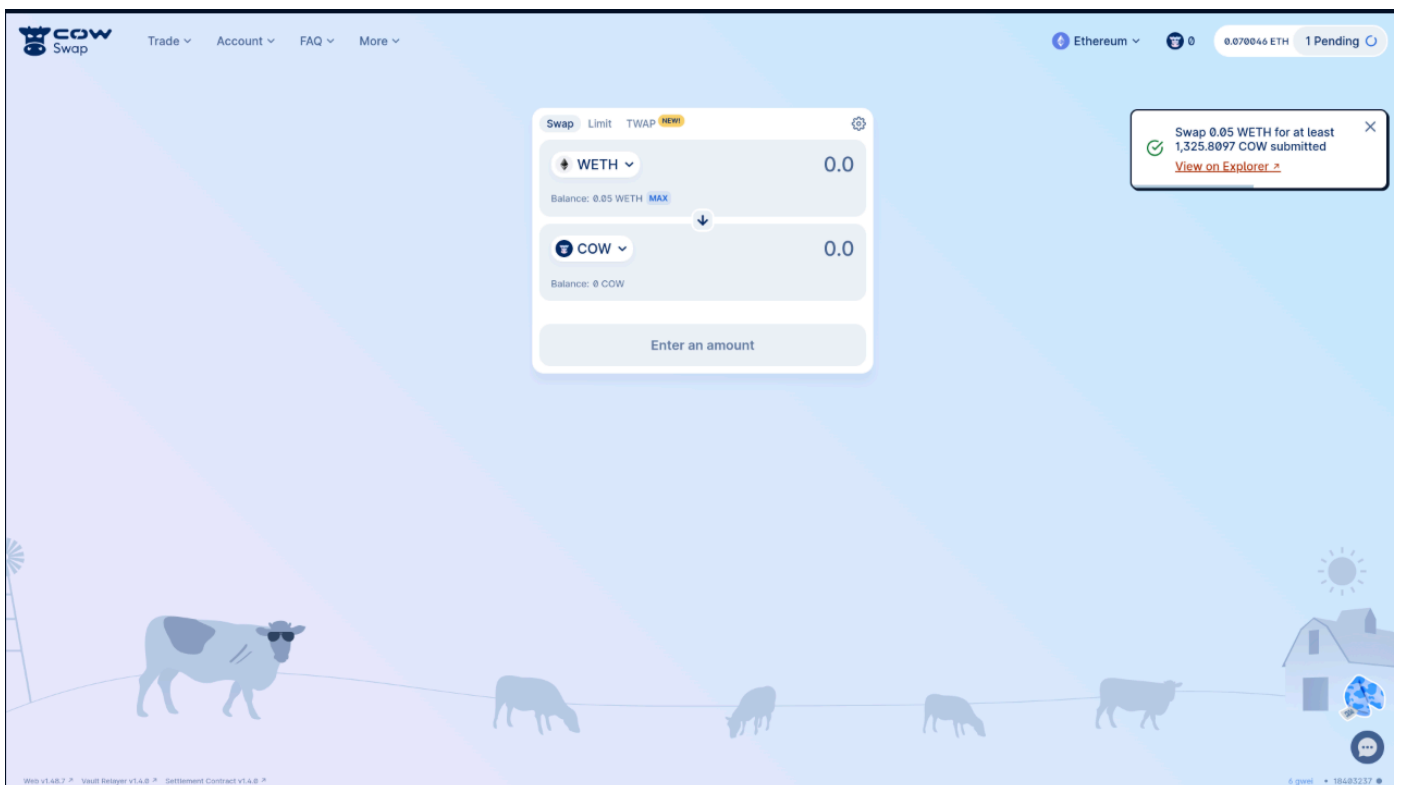
주문에 서명할 때는 주의하라. 주문과 관련된 모든 파라미터는 최종적이며, 서명 및 제출 후에는 변경할 수 없다. 실수했다면 주문을 취소하고 새 주문을 생성해야 한다.



이 단계에서 지갑이 주문 서명을 요청한다. 서명 인터페이스는 사용하는 지갑에 따라 다르다.



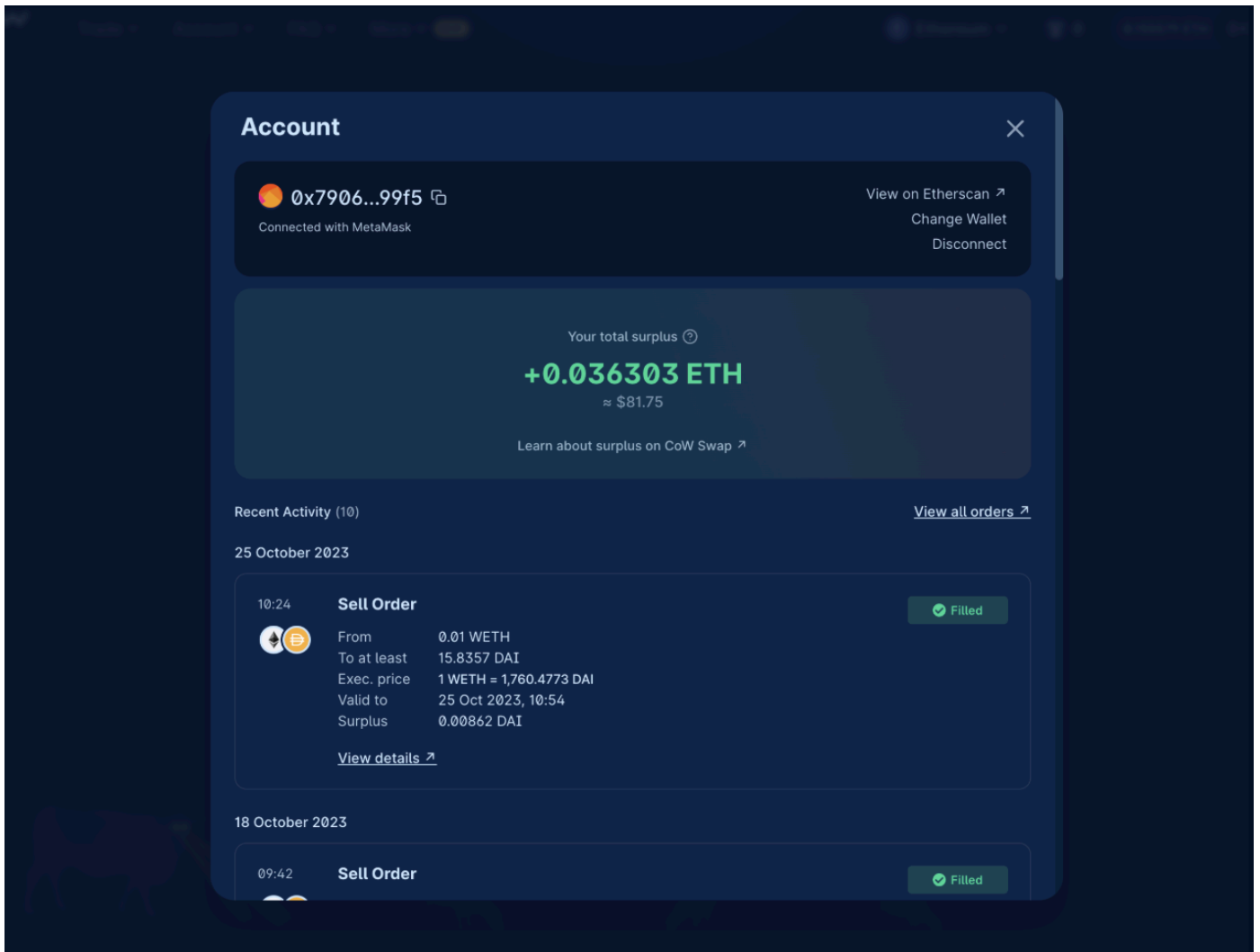
주문이 서명되면 CoW Protocol로 전송되어 실행 준비가 완료된다. 🎉



주문 추적 (Track your order)

주문은 오더북에 등록되어 실행 대기 상태가 된다.

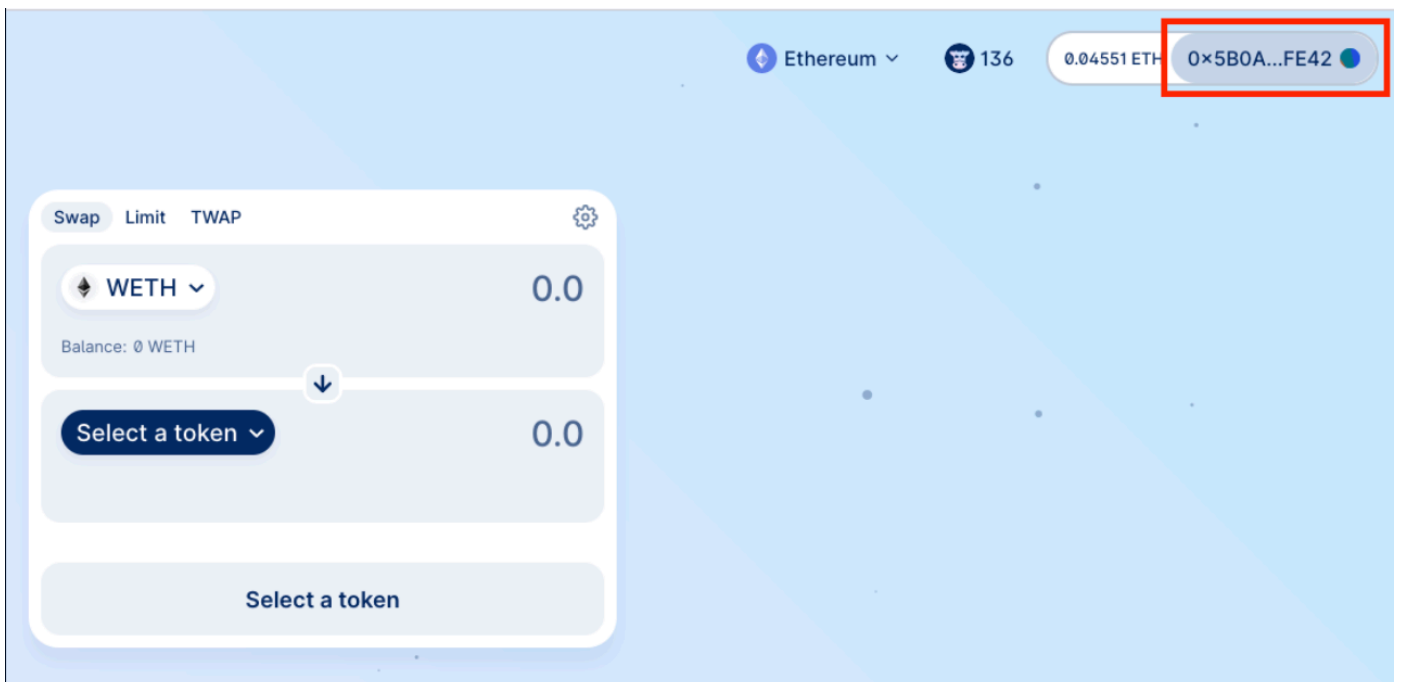
- CoW Swap은 주문이 실행되면 팝업 메시지로 자동 알림을 표시한다.
- 오른쪽 상단의 연결된 지갑 주소를 클릭하면 최근 내역에서 주문 상태를 확인할 수 있다.
- [CoW Explorer](#)에서 주문을 조회할 수도 있다.



주문 취소 (Cancel your order)

마음이 바뀌었는가? 문제없다! CoW Swap에서는 가스 없이(gasless) 주문을 손쉽게 취소할 수 있다.

먼저 오른쪽 상단의 주소를 클릭해 활동 패널을 연다.



목록에서 보류 중인 주문을 찾아 Cancel order를 클릭한다.

Recent Activity (9)

[View all orders ↗](#)

December 22, 2023

4:11 p.m. **Sell Order**



From135.2536 COW

To at least0.006414 ETH

Limit price1 ETH = 10,799.3096 COW

Valid toDec 22, 2023, 4:41 p.m.

Open

Cancel order

[View details ↗](#)



 Order Status: Looking for a [Coincidence of Wants \(CoW\)](#) ↗



CoW Swap can save you gas costs and get a better price if another trader takes the opposite side of your trade.

취소를 확인하고, 원하는 취소 방식을 선택한다: 오프체인(off-chain)(기본) 또는 온체인(on-chain).

오프체인 취소는 무료이며 트랜잭션이 필요하지 않다. 그러나 취소 요청이 처리되기 전에 주문이 매칭될 위험이 존재한다.

Note

취소는 즉시 이루어지지 않으며, 취소가 처리되기 전에 주문이 체결될 수 있다.

오프체인 취소를 진행하려면 아래와 같이 Request cancellation을 클릭한다.

No. 29 / 110

Cancel order 0x02130e



Are you sure you want to cancel order **0x02130e**?

Swap 135.2536 COW for at least 0.004763 ETH

This is an **off-chain →** cancellation [-less]

Off-chain cancellations require a signature and are free.

Keep in mind a solver might already have included the order in a solution even if this cancellation is successful.

Read more in the [FAQ](#).

Request cancellation

API를 신뢰해 주문을 취소하고 싶지 않다면, 온체인(on-chain) 트랜잭션을 통해 주문을 직접 취소할 수 있다. 이 경우 수수료가 발생한다. off-chain을 클릭해 취소 유형을 on-chain으로 전환하라.

Note

온체인 취소의 경우에도, 취소 트랜잭션이 블록에 포함되기 전에 주문이 매칭될 수 있는 위험이 존재한다. 우선순위가 수수료를 높게 설정하고 빠르게 서명하라.

지갑에서 트랜잭션을 확인하면 완료된다!

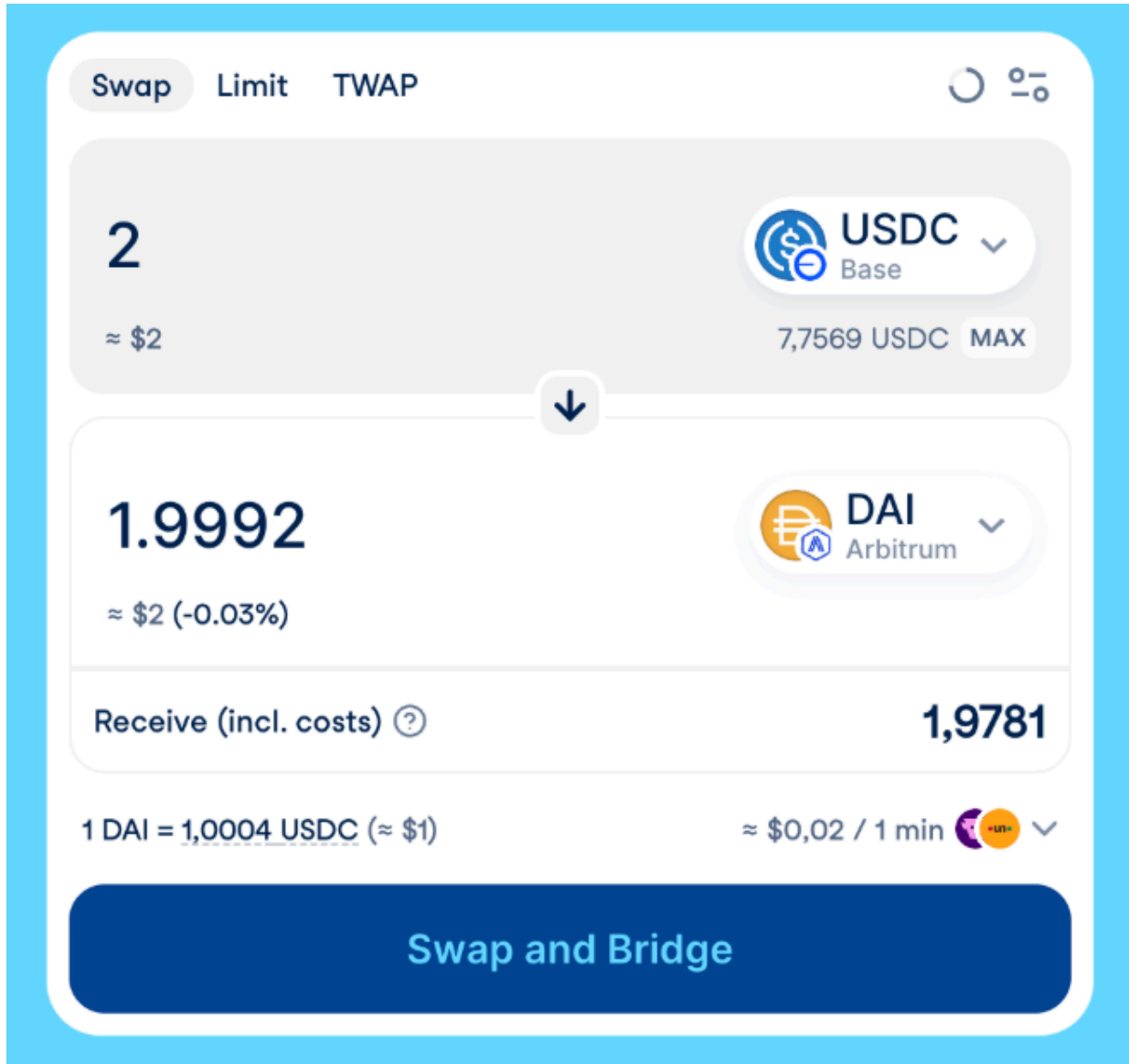
각주 (Footnotes)

1. 오프체인(off-chain) 취소만 수수료가 들지 않는다.
온체인(on-chain) 취소는 이름 그대로 일반 네트워크 트랜잭션이 필요하다.

크로스체인 스왑 (Cross-chain swaps)

swap.cow.fi의 크로스체인 스왑 기능을 사용하면 하나의 네트워크에서 토큰을 스왑하고 다른 네트워크에서 다른 토큰을 수령할 수 있으며 — 이 모든 과정을 하나의 매끄러운 트랜잭션으로 처리할 수 있다.

이 가이드는 트레이드 설정부터 익스플로러에서 추적하는 것까지 단계별로 설명한다.



Note

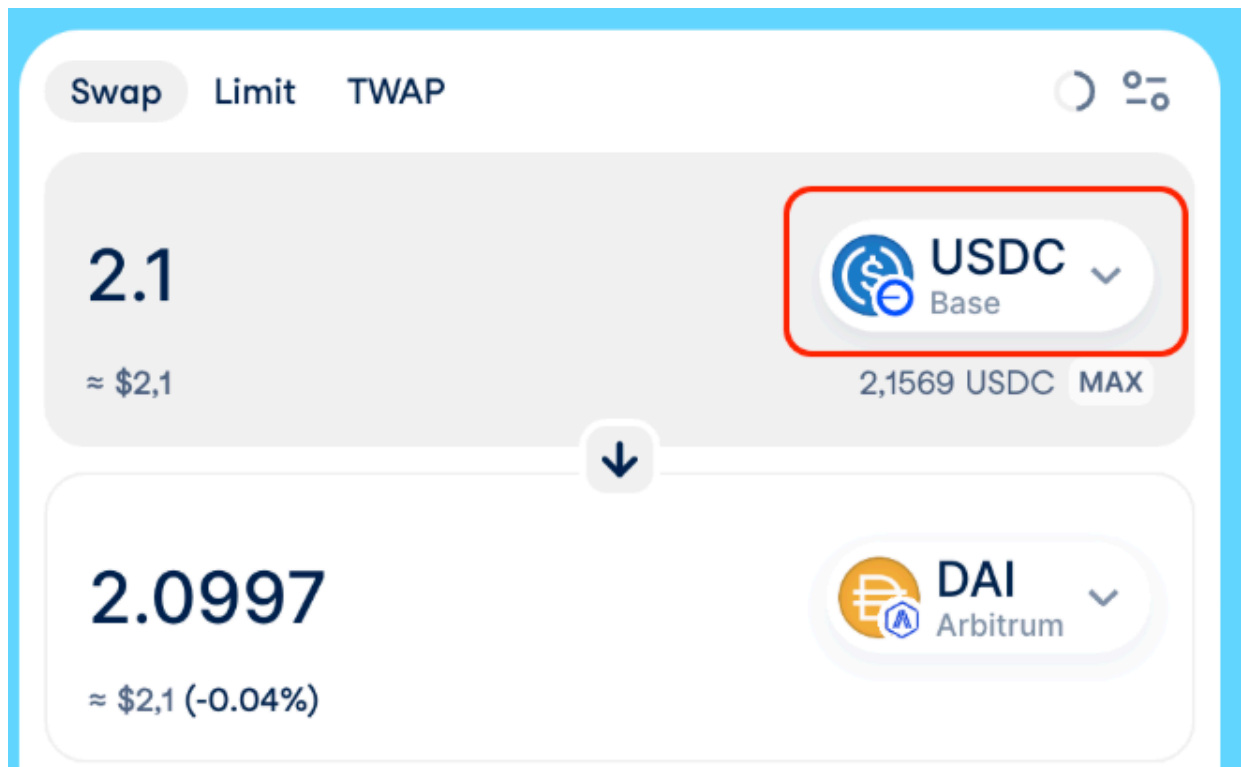
현재 크로스체인 스왑 기능은 스왑 주문으로 제한되며 스마트 컨트랙트 지갑에서는 사용 불가하다. 해당 기능들은 향후 제공될 예정이다.

1. 서로 다른 네트워크 자산으로 스왑 설정하기 (Setting up a Swap with Different Network Assets)

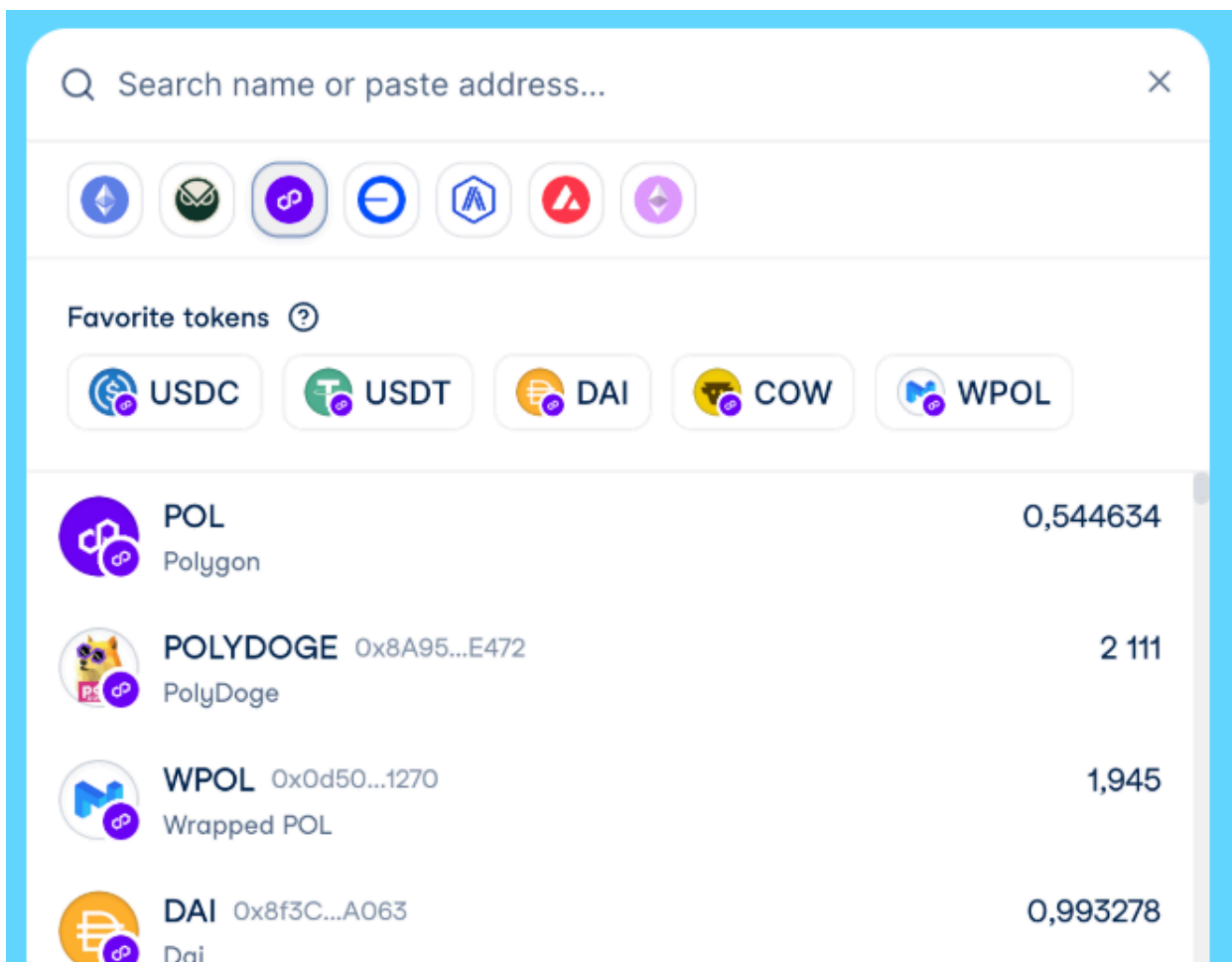
크로스체인 스왑을 사용할 때는 일반 스왑과 동일하게 거래할 토큰을 선택하는 것부터 시작하되, 목적지 체인을 다르게 선택하는 옵션이 추가된다.

소스 토큰 선택기 (Source Token Selector)

소스 토큰 선택기를 연다:

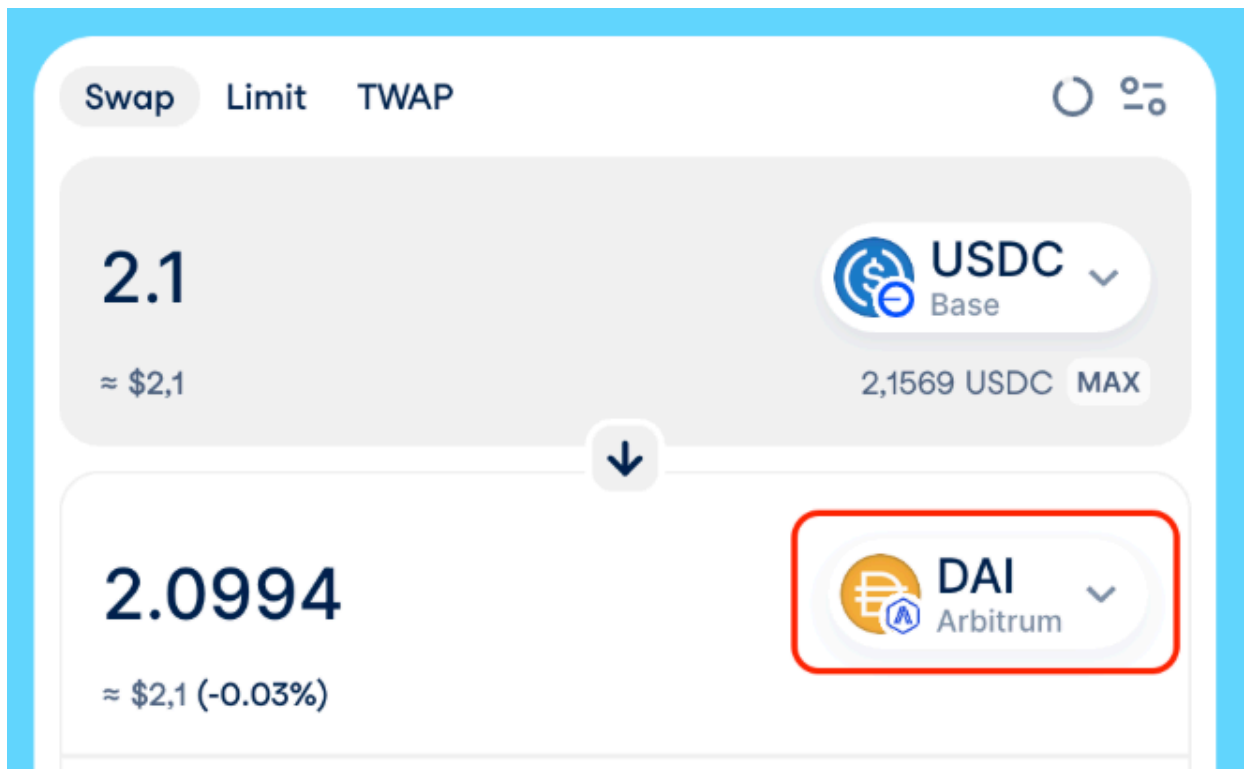


판매할 네트워크와 토큰을 선택한다:



목적지 토큰 선택기 (Destination Token Selector)

소스 토큰 선택기와 유사하게 선택기를 열고, 구매하려는 네트워크와 토큰을 선택한다.



Tip

사용 가능한 목적지 네트워크 목록은 선택한 소스 토큰에 따라 달라진다.

목적지 네트워크가 소스 토큰의 네트워크와 다르면:

- 해당 체인에 대해 브리지 제공자가 지원하는 토큰만 표시된다.

목적지 네트워크가 소스 네트워크와 같다면:

- 토큰 리스트의 일반 토큰 목록이 표시된다.

Note

토큰은 서로 달라야 한다. 동일 토큰을 두 네트워크 간에 브리지하는 기능은 아직 지원되지 않는다. 이 기능은 향후 제공될 예정이다.

2. 크로스체인 스왑 생성하기 (Creating a Cross-chain swap)

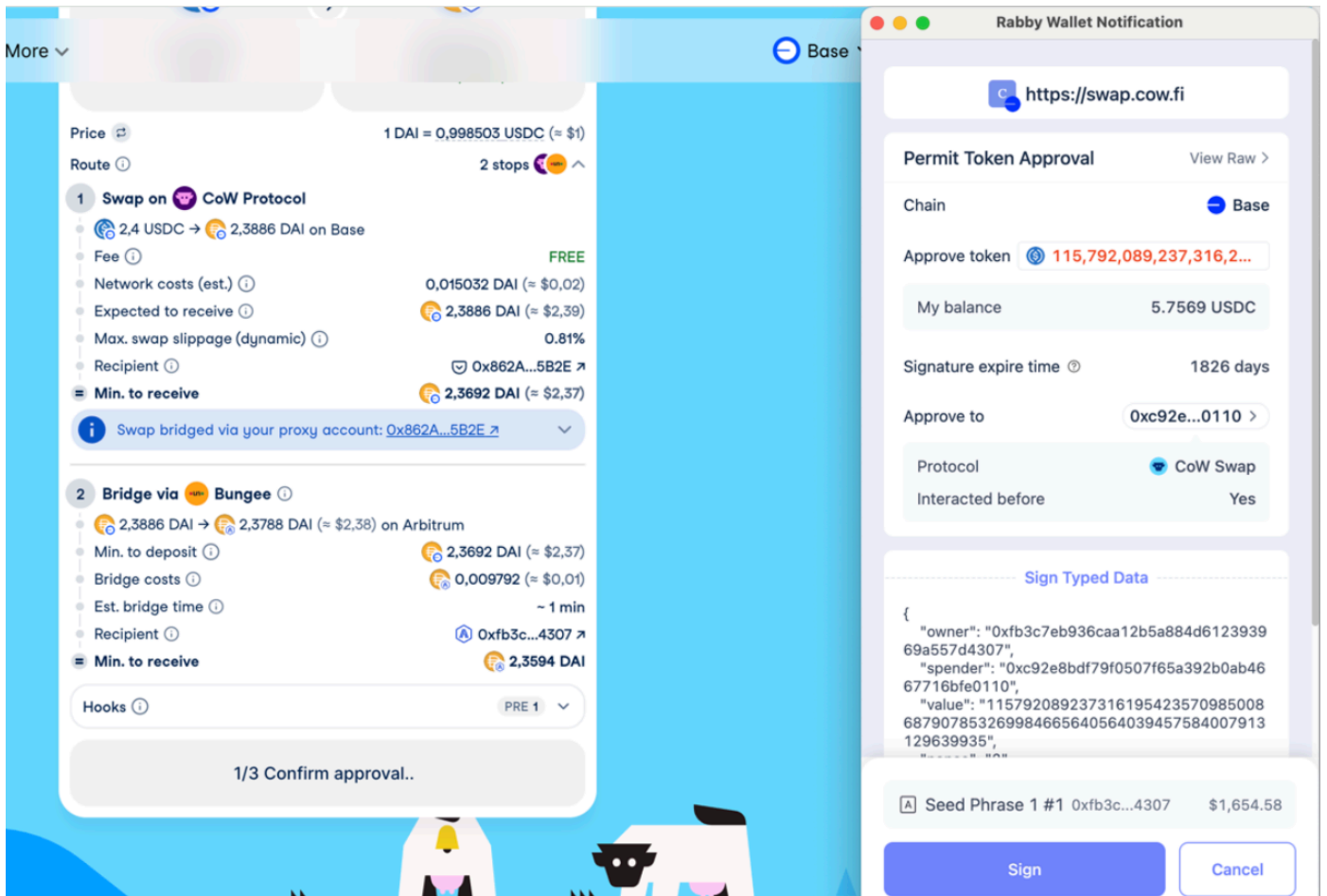
토큰과 네트워크를 설정했으면 주문 생성을 진행할 수 있다.

토큰 승인 (Token Approval)

해당 토큰을 CoW Swap에서 처음 판매한다면 승인이 필요하다. 이는 거래에 CoW Protocol이 토큰을 사용할 수 있도록 허용하는 표준 ERC-20 승인 절차다.

승인은 다음 방법으로 진행될 수 있다:

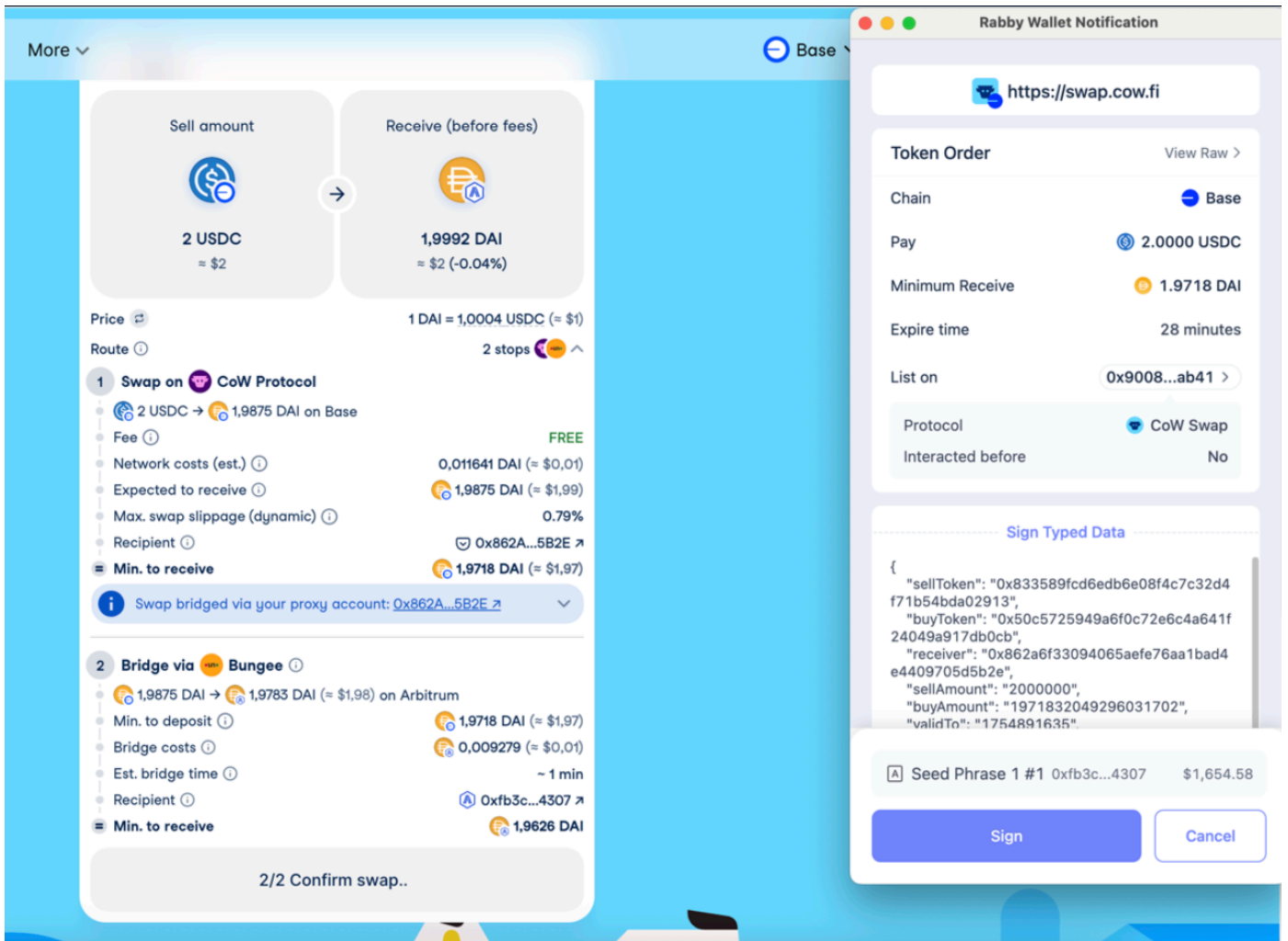
- 일반 ERC-20 허용량(allowance) 트랜잭션
- EIP-2612 서명(토큰이 지원하는 경우)



서명 단계 (Signing Steps)

1. 브리지 제공자에 대한 포스트 혹은 호출에 서명한다.
 - 포스트 혹은 호출에는 Account Proxy에서 중간 토큰 승인을 위한 호출이 포함될 수 있으며, 이를 통해 해당 토큰을 예치 스마트 컨트랙트로 전송할 수 있다.
 - 포스트 혹은 호출에는 항상 브리지 제공자의 스마트 컨트랙트 호출이 포함되며, 스왑된 금액을 예치 스마트 컨트랙트로 전송한다.
2. 주문에 서명한다:
 - 오프체인 주문에 서명한다(ERC-20 토큰 매도).
 - 트랜잭션에 서명한다(네이티브 토큰, 예: ETH 매도).

[illegible]



Note

중간 토큰(Intermediate token) — 스왑 결과로 소스 체인에서 수령하여 이후 브리지 제공자에게 예치하는 통화다. 일반적으로 목적지 체인의 통화와 동일하지만, 소스 블록체인 상에서 발행된 버전이다.

Note

매도할 토큰에 대해 승인된 퍼밋이 없다면, 프로세스는 퍼밋 서명부터 시작해 총 세 번의 서명 단계가 포함된다.

3. 커스텀 수신자 사용 (Using a Custom Recipient)

기본적으로 연결된 지갑 주소가 목적지 체인에서의 수신자로 설정된다. 다른 주소로 자금을 보내고 싶다면:

1. 설정에서 Custom recipient를 활성화한다(일반 스왑과 동일한 위치).
2. 수신자 주소를 입력한다.
3. 참고: 여기서는 ENS 이름을 지원하지 않는다 — 전체 지갑 주소를 사용해야 한다.

Swap Limit TWAP

2.1
≈ \$8 967,17

WETH Base
0,002273 WETH MAX

↓

8968.927
≈ \$8 967,41 (0%)

USDT Polygon

Receive (incl. costs) ⓘ 8 954,617

↓

Recipient
0x0000 ⓘ

1 USDT = 0,000234 WETH (≈ \$1) ≈ \$14,31 / 1 min ⓘ

Enter a valid recipient

4. 견적 미리보기 (Previewing Your Quote)

스왑 폼에서 예상 스왑 및 브리징 내역을 자세히 볼 수 있다:

- Swap Min. to receive: 모든 스왑 비용과 슬리피지 허용치를 반영한 최종 수령 예상 금액.
- Expected deposit amount: 스왑 단계의 “Expected to receive” 금액과 동일하다.
- Bridge cost: 전송 처리에 대해 브리지 제공자가 부과하는 수수료.
- Estimated bridging time: 브리지 제공자로부터 직접 가져오는 예상 소요 시간(네트워크 및 제공자에 따라 다름).

- Bridge Min. to receive: (Swap min. to receive) – (Bridge provider cost)로 계산된다.

1
Swap on

CoW Protocol

- 2 USDC → 1,9873 DAI on Base
- Fee ⓘ FREE
- Network costs (est.) ⓘ 0,011921 DAI (≈ \$0,01)
- Expected to receive ⓘ  1,9873 DAI (≈ \$1,99)
- Max. swap slippage (dynamic) ⓘ 0.8%
- Recipient ⓘ  0x862A...5B2E ↗
- = Min. to receive  1,9714 DAI (≈ \$1,97)

 Swap bridged via your proxy account: [0x862A...5B2E ↗](#)

2
Bridge via

Bungee ⓘ

-  1,9873 DAI →  1,978 DAI (≈ \$1,98) on Arbitrum
- Min. to deposit ⓘ  1,9714 DAI (≈ \$1,97)
- Bridge costs ⓘ  0,009278 (≈ \$0,01)
- Est. bridge time ⓘ ~ 1 min
- Recipient ⓘ  0xfb3c...4307 ↗
- = Min. to receive  1,9621 DAI

Swap and Bridge

5. Account Proxy 이해하기 (Understanding the Account Proxy)

Account Proxy(CoW Shed로도 알려짐)는 CoW Hooks와 같은 고급 기능을 지원하는 헬퍼 컨트랙트다.

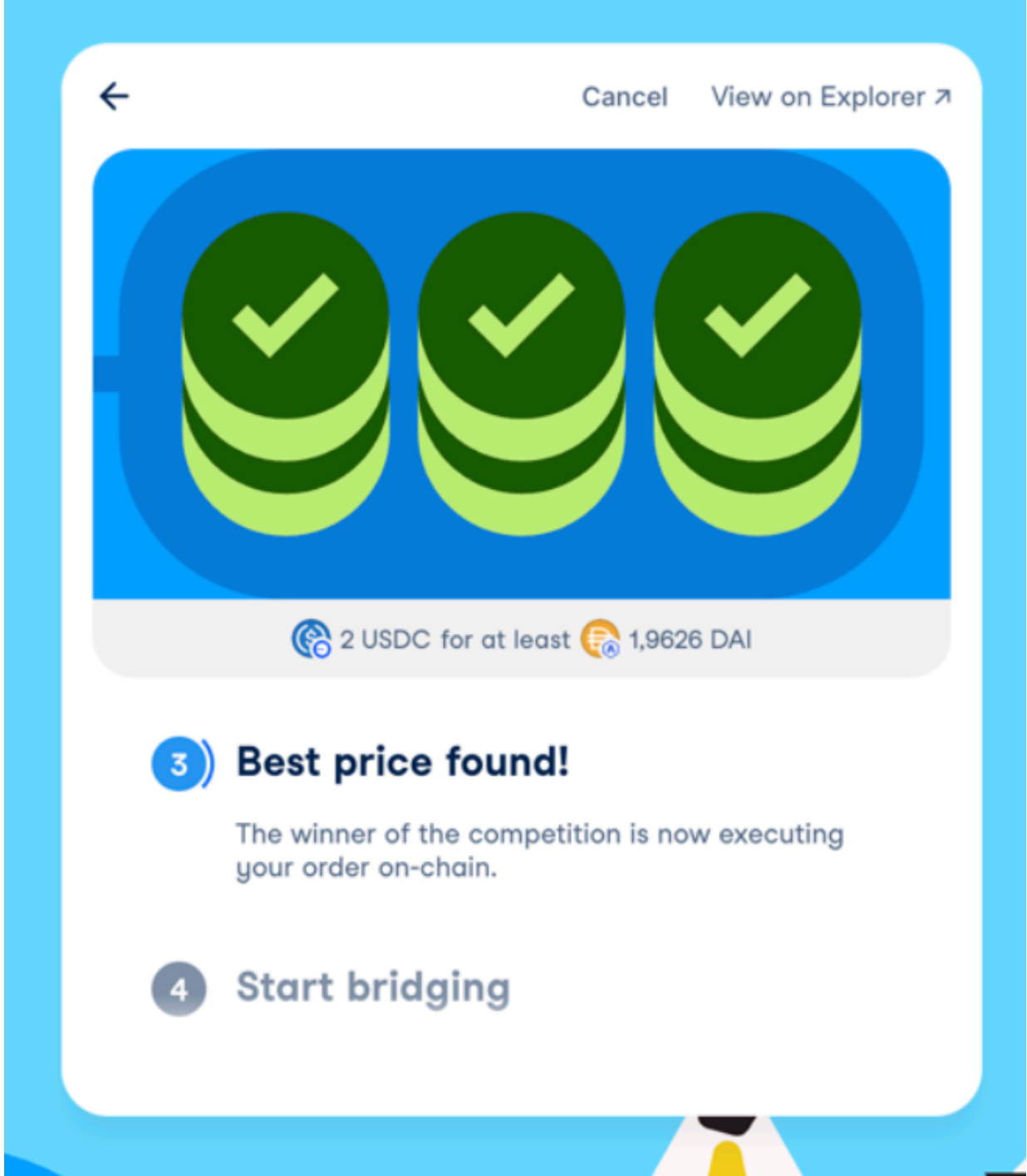
- CoW Hooks는 주문 결제 전후에 솔버가 추가 이더리움 호출을 실행할 수 있게 한다.
- 자금은 안전하다: 실행 중 문제가 발생하면 자산은 개인 프록시 계정으로 전송된다. 언제든지 지갑으로 인출할 수 있다.

자세한 내용은 Account Proxy 페이지에서 확인할 수 있다.

6. 브리징 실행 방식 (How Bridging Execution Works)

1. 브리지 단계는 스왑이 성공한 이후에만 시작된다.

! [Bridging initiation screen showing confirmation and status checks]



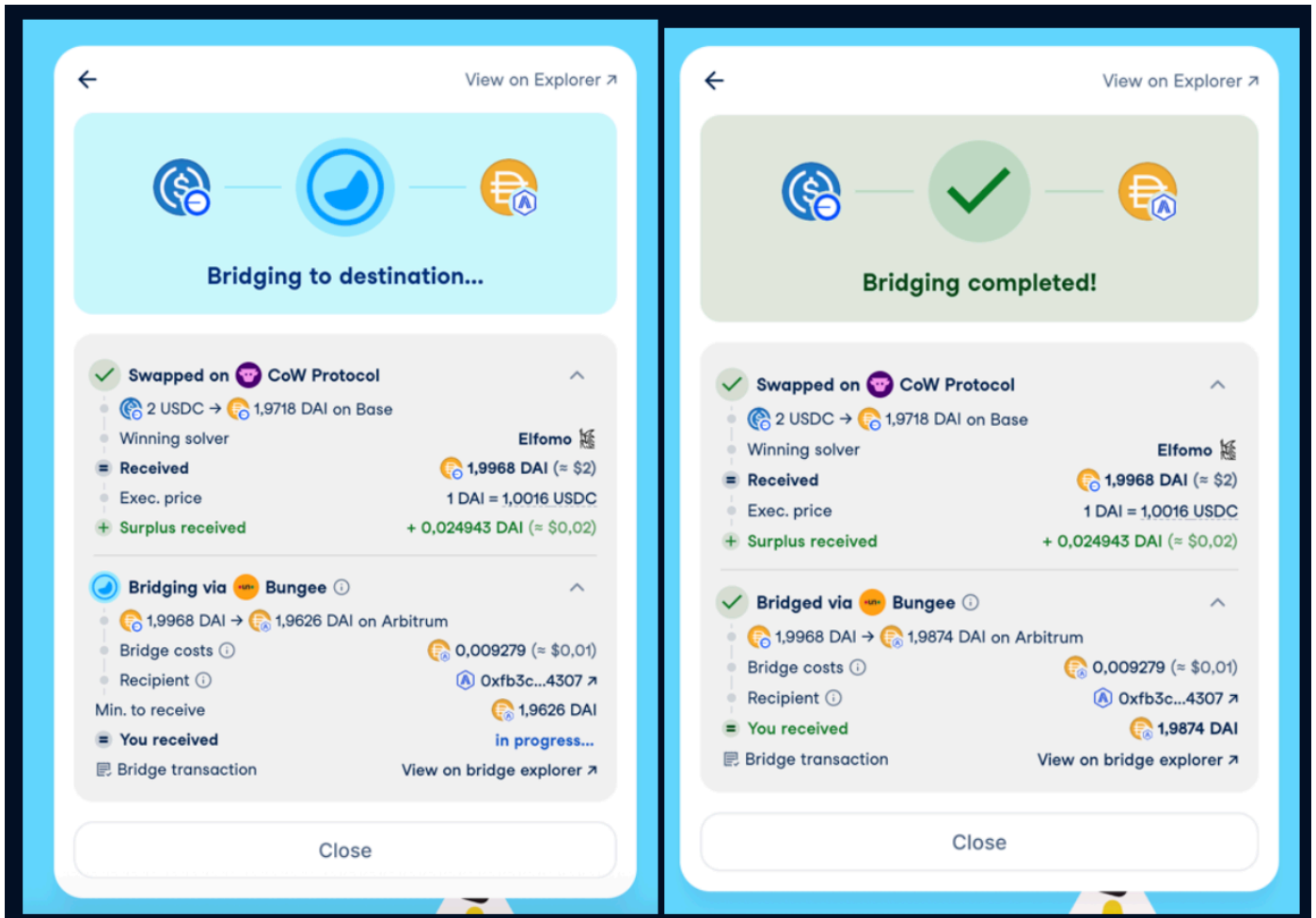
Note

주문이 만료되거나, 취소되거나, 실패하면 브리징은 시작되지 않으며 — 자금은 지갑에 그대로 남는다.

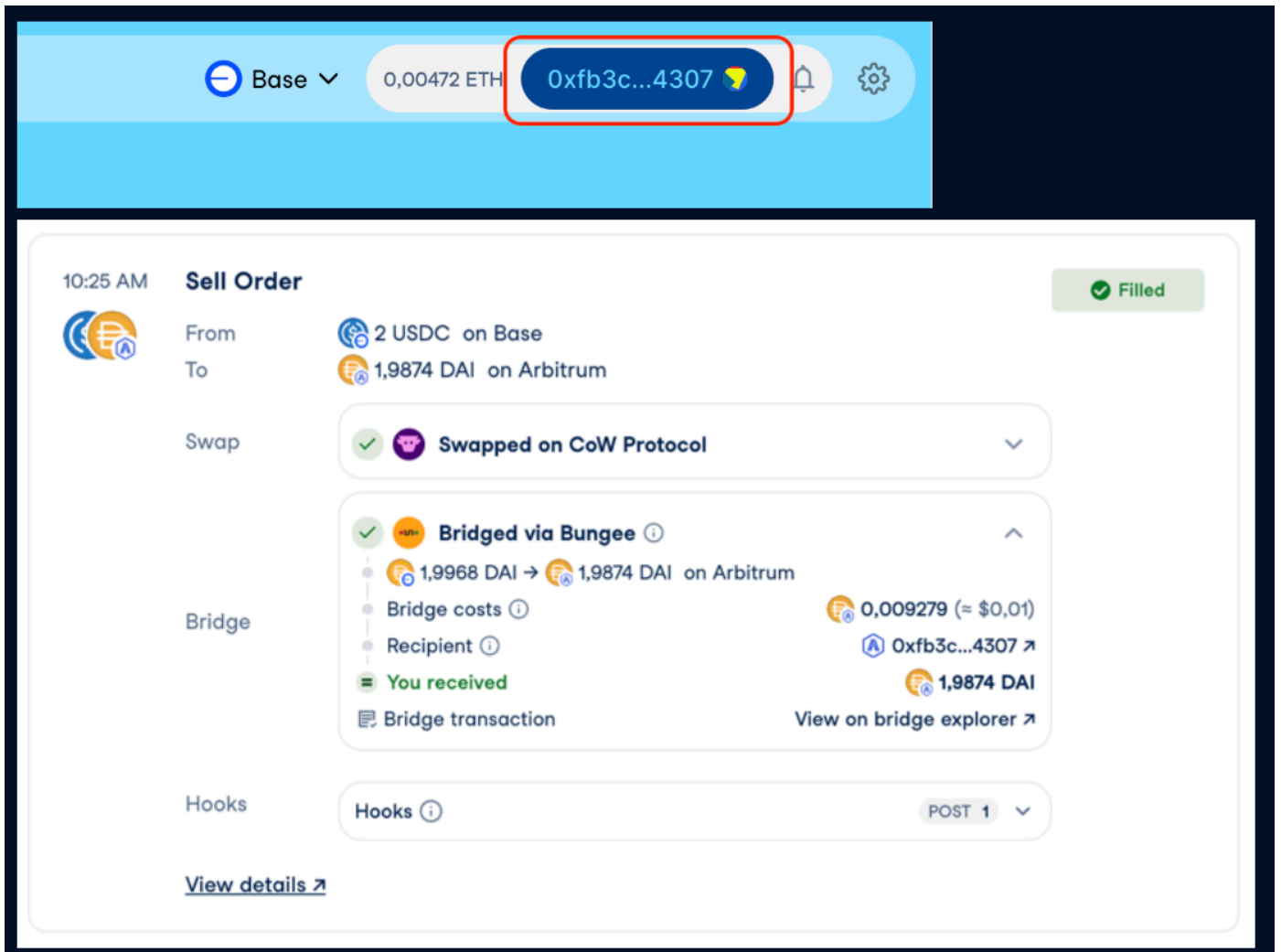
Note

스왑 단계 동안에만 주문을 소프트 취소할 수 있다. 스왑이 실행되고 Account Proxy가 브리지 예치를 제출한 이후에는 브리지 전송을 취소할 수 없다. 전송은 목적지 체인에서 완료되거나 제공자 정책에 따라 환불된다.

2. 스왑이 완료되면:
 - 주문 상태가 'Bridging in progress'로 변경된다.
 - 수령한 금액은 Account Proxy로 전송된다.
 - 그 후 브리지 제공자의 스마트 컨트랙트로 예치된다.
 - 이러한 단계는 한 번의 트랜잭션 내에서 수행된다.
3. 브리징이 완료되면, 목적지 체인에서의 최종 수령 금액과 함께 "Bridging completed!" 상태가 표시된다.
4. 주문 진행 상황을 추적할 수 있도록 브리지 제공자의 익스플로러 링크가 항상 제공된다.



5. 크로스체인 스왑 기록은 CoW Swap의 Account 모달에서 확인할 수 있다.



Note

Account 모달은 최근 10건의 주문만 표시한다. 전체 주문 내역은 [CoW Explorer](#)에서 확인하라.

7. 브리징 실패 시 – 환불 받기 (If Bridging Fails – Getting a Refund)

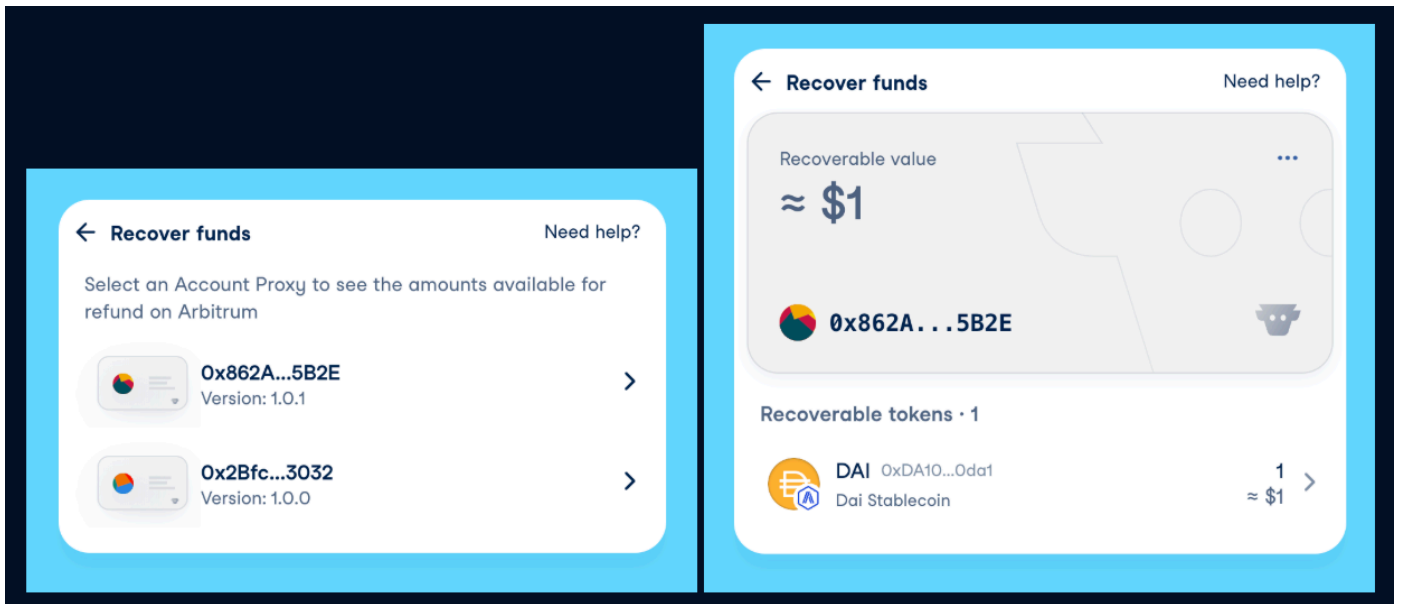
드물게 브리징 단계가 실패할 수 있다. 걱정할 필요 없다 — 자금은 안전하다.

대부분의 브리지 제공자는 예치가 완료되면 자금을 [Account Proxy](#)로 자동 환불한다.

만료 시간은 제공자에 따라 다르다. 예를 들어, Across 제공자는 예치가 완료되지 않은 경우 보통 약 3시간 후 환불한다.

환불이 Account Proxy에 도착하면:

1. [CoW Swap Account Proxy 페이지](#)를 연다.
2. Account Proxy 버전 목록에서 최신 버전을 선택한다(특별한 안내가 없는 한).
3. 필요한 Account Proxy 버전의 상세 정보를 연다.
4. 토큰을 선택하고 자금을 지갑으로 복구(recover)한다.



8. 익스플로러에서 주문 추적 (Tracking Your Orders in the Explorer)

explorer.cow.fi에서 모든 크로스체인 스왑을 확인할 수 있다.

- In Progress, Completed, Cancelled 등 모든 상태의 주문을 볼 수 있다.
- 결과를 필터링하고 각 트레이드의 전체 세부 정보를 확인할 수 있다.
- 각 크로스체인 스왑에는 Swap과 Bridge 두 개의 탭이 있어 트랜잭션의 두 부분을 쉽게 탐색할 수 있다.

BASE

Order details
0x1d4240318...

1. Swap	2. Bridge
FILLED	EXECUTED
Transaction Details View on bridge explorer	
Provider Bungee	
From 0x862a6f33094065aefe76aa1bad4e4409705d5b2e on Base	
To 0xfb3c7eb936caa12b5a884d612393969a557d4307 on Arbitrum	
Status EXECUTED	
Amounts From: 1.1924 Dai Stablecoin (DAI) Base To at least: 1.184 MakerDAO Arbitrum Bridged DAI Arbitrum (DAI) Arbitrum	
You received 1.184 MakerDAO Arbitrum Bridged DAI Arbitrum (DAI) Arbitrum	

지정가 주문 (Limit orders)

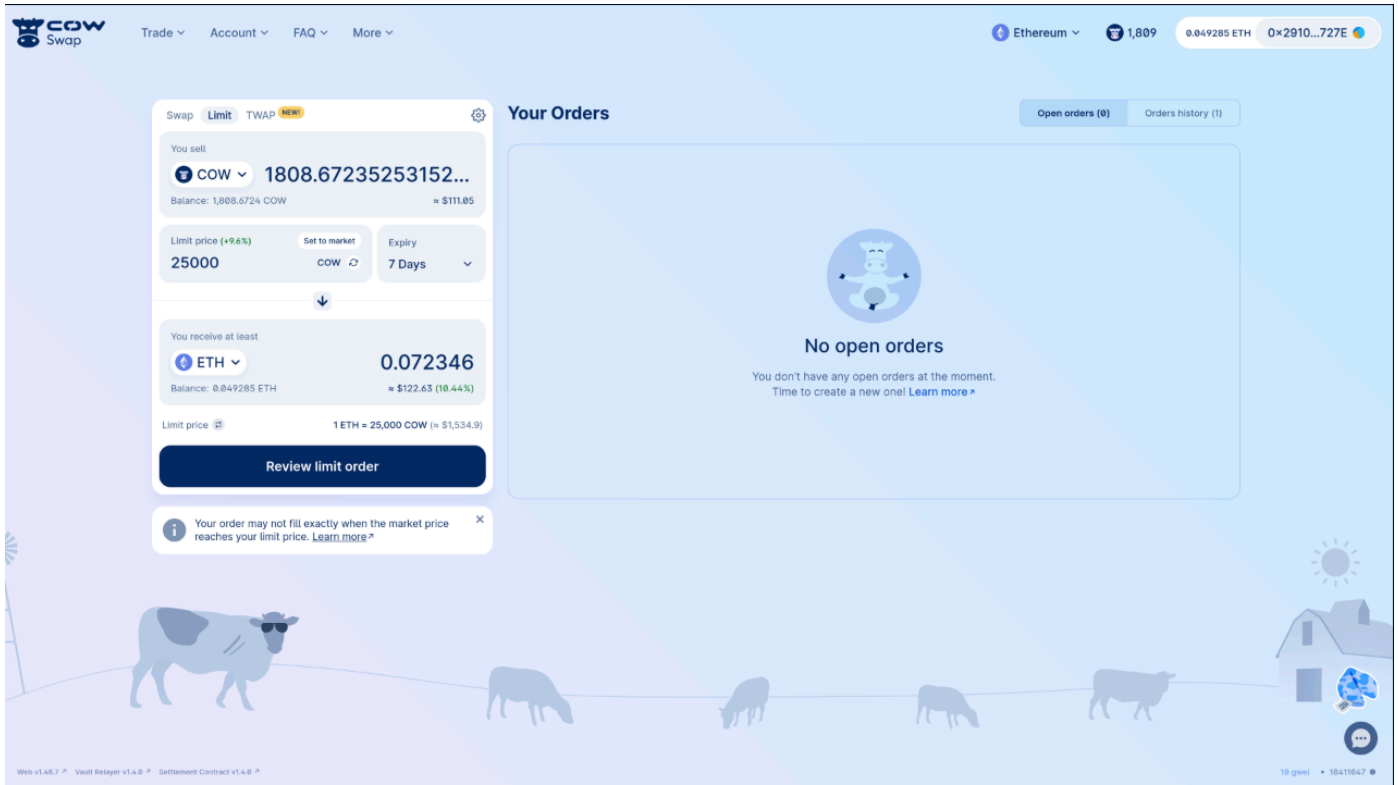
CoW Protocol은 사용자가 특정 가격 또는 그보다 더 좋은 가격으로 토큰을 매수하거나 매도할 수 있는 지정가 주문 (limit order)을 지원한다.

매수 지정가 주문은 트레이더가 토큰에 대해 지불할 의사가 있는 최대 가격을 지정할 수 있게 하며, 매도 지정가 주문은 토큰을 판매할 최소 가격을 지정할 수 있게 한다.

CoW Swap은 이러한 지정가 주문을 쉽게 설정할 수 있는 직관적인 인터페이스를 제공한다.

지정가 주문 생성 (Place a limit order)

예를 들어 COW를 판매하려 한다고 가정하자. 판매를 원하는 지정가와 지정가 주문의 유효 기간을 설정할 수 있다:

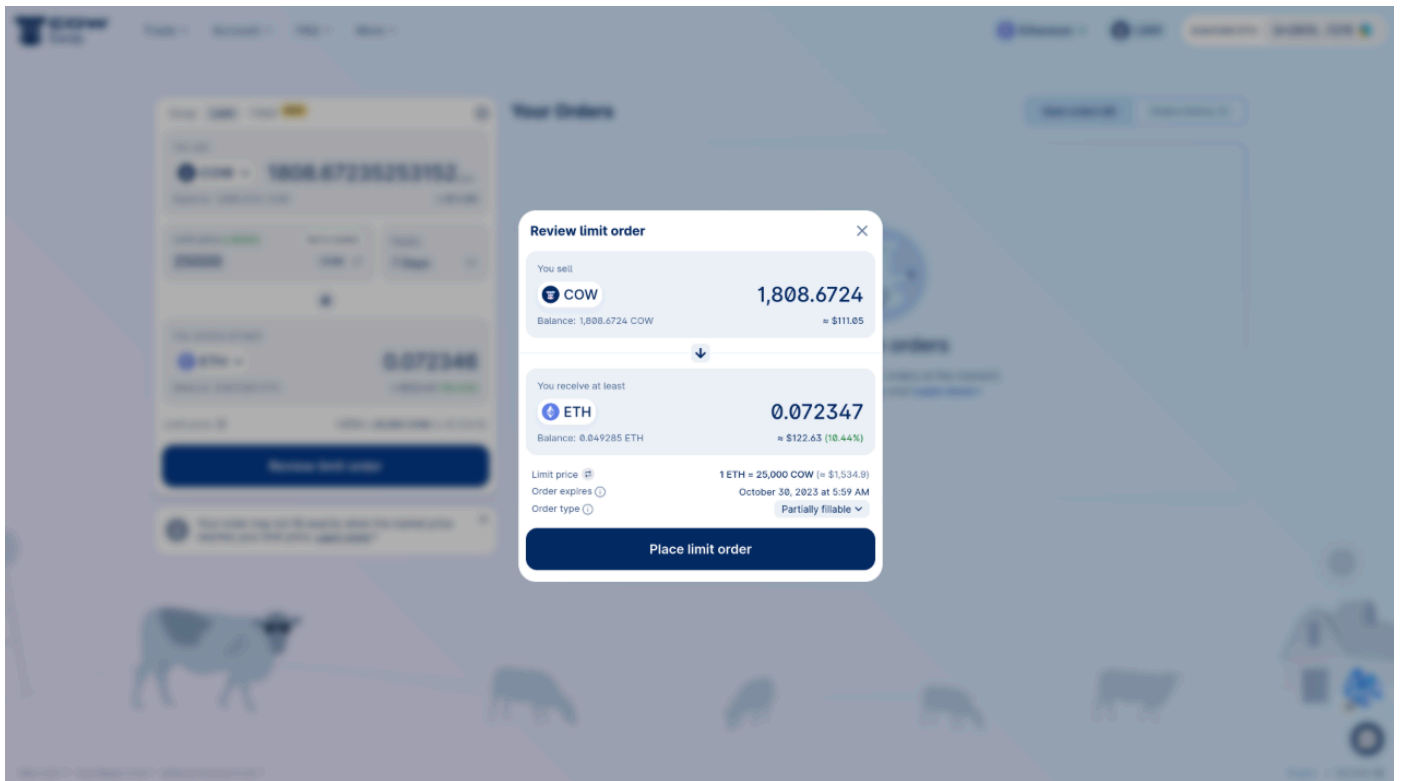


Info

CoW Protocol은 지정가 주문을 제출할 때 수수료를 부과하지 않는다. 대신 프로토콜은 지정가보다 더 나은 가격으로 주문을 실행하여 수수료를 충당한다.

CoW Protocol은 시장 가격이 지정가와 네트워크 수수료를 모두 충당할 수 있을 때까지 대기하므로, 실제로 주문이 시장 가격이 지정가에 도달하자마자 즉시 실행되지 않을 수 있다.

이 시점에서 CoW Swap은 지정가 주문을 검토하도록 요청한다:



Tip

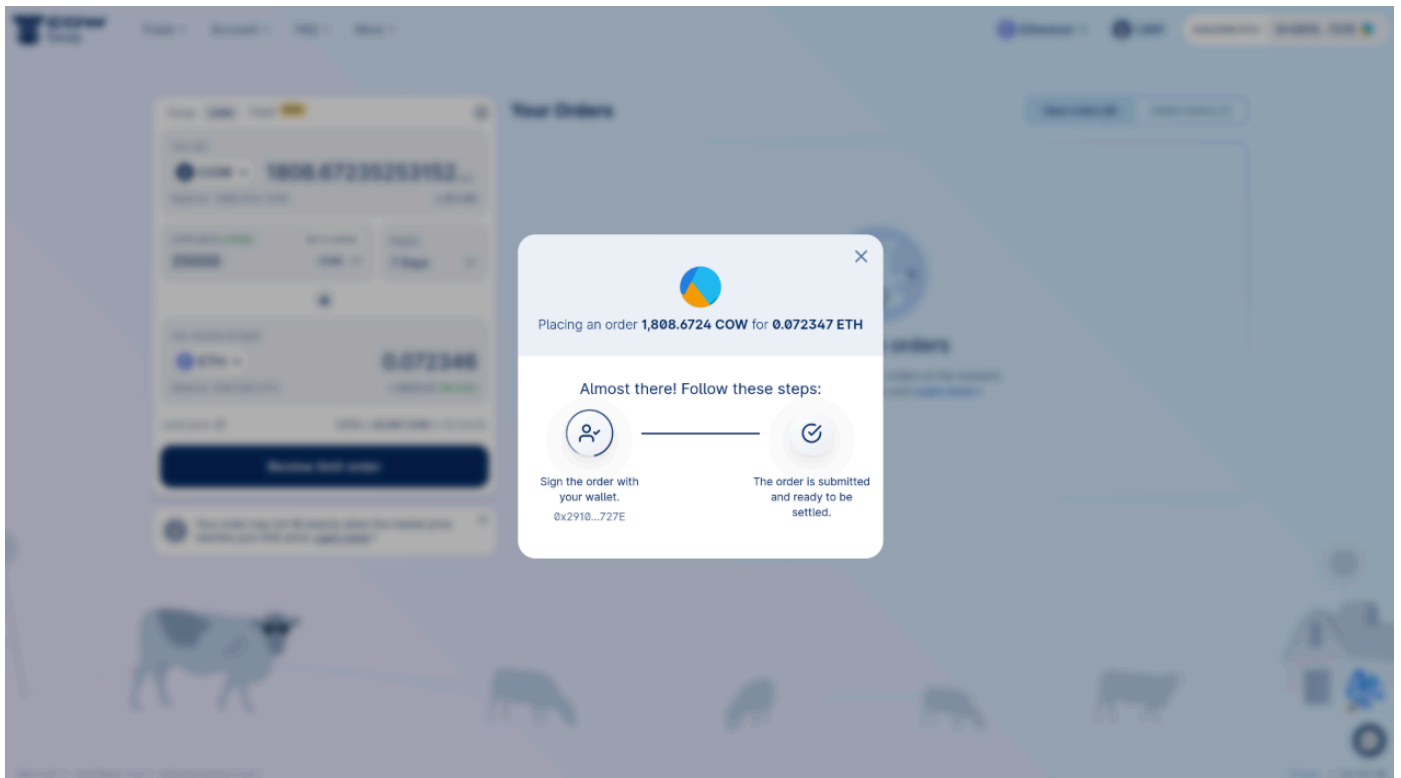
기본적으로 CoW Swap은 지정가 주문을 부분 체결 가능(partially fillable) 상태로 설정한다. 이는 유동성이 확보될 때 주문이 점진적으로 체결될 수 있도록 한다.

부분 체결 가능한 주문은 일반적으로 전량 체결 또는 취소(fill or kill) 주문보다 더 빠르게 완료되며, 더 나은 가격을 제공하는 경우가 많다. 따라서 지정가 주문의 기본 실행 메커니즘으로 사용된다.

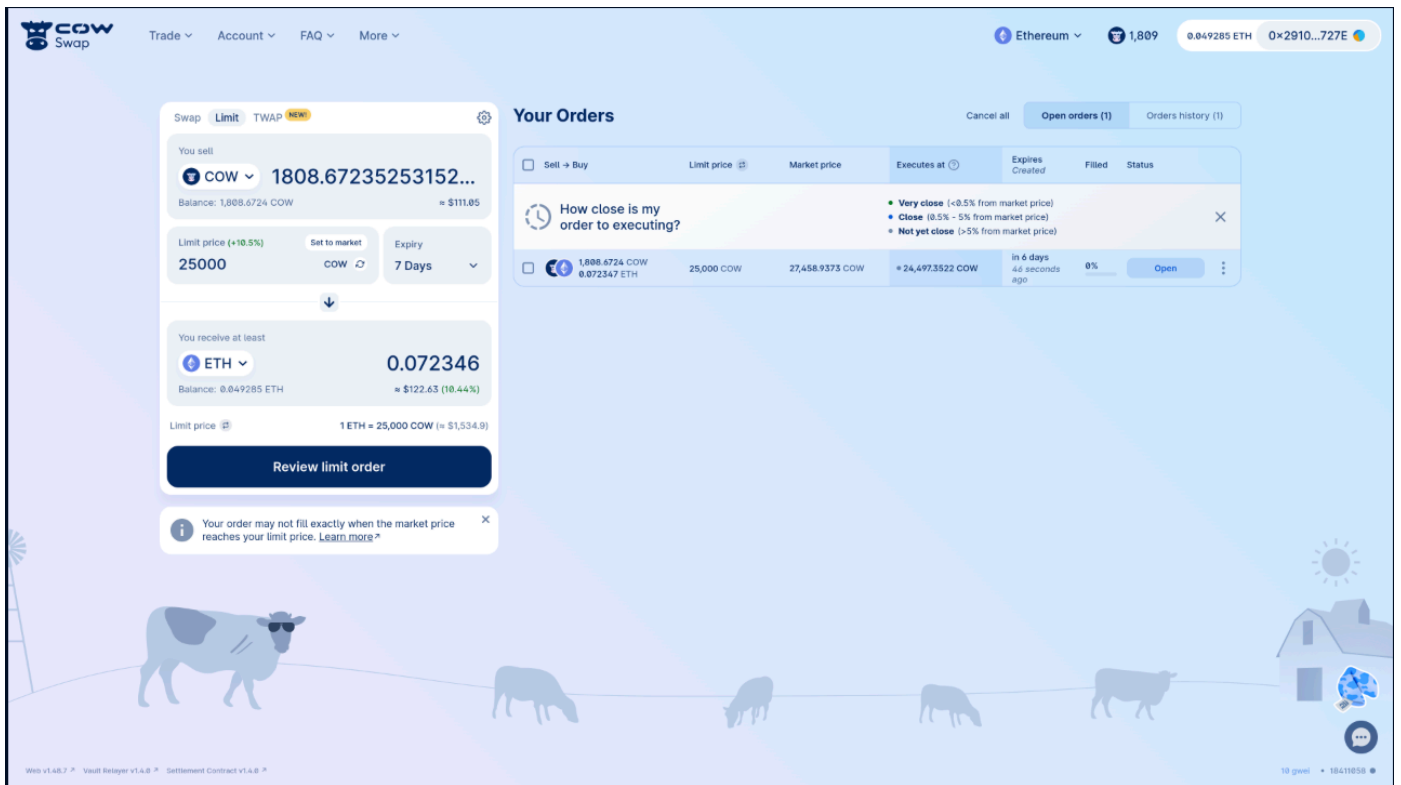
그러나 남은 체결 금액이 정산에 필요한 네트워크 수수료에 비해 작을 경우, 주문이 완전히 체결될 수도 있다.

이로 인해 계정에 판매 토큰의 잔여 금액이 남을 수 있다. 스왑 패널 설정에서 부분 체결 가능한 지정가 주문을 끄고 fill or kill 방식으로 되돌릴 수 있다.

지정가 주문을 검토한 후 “Place limit order” 버튼을 클릭하여 주문 서명을 진행한다.



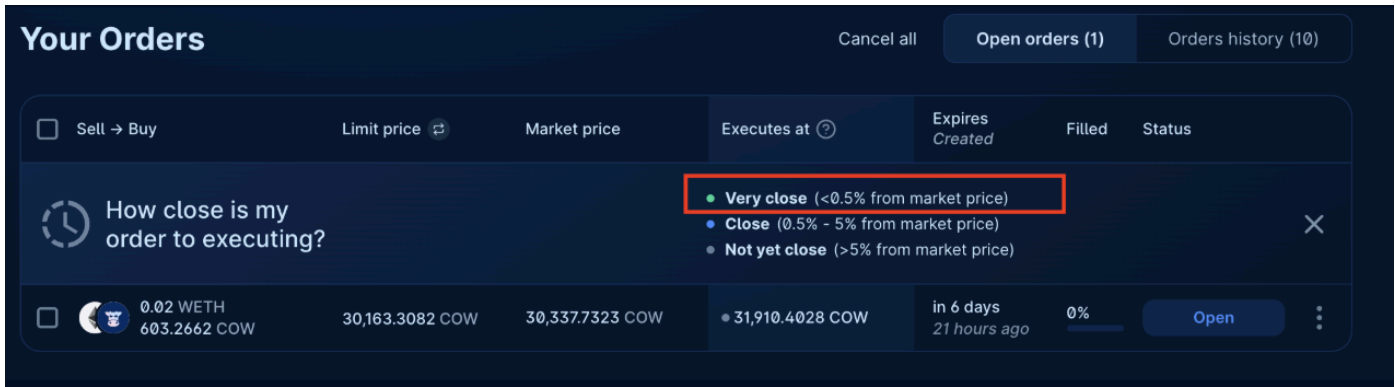
지갑에서 주문에 서명하면, 지정가 주문이 Open Orders(미체결 주문) 목록에 표시된다:



지정가 주문 추적 (Track a limit order)

앞서 언급했듯이, CoW Protocol의 지정가 주문은 지정가에 도달하더라도 즉시 실행되지 않을 수 있다. 이는 프로토콜이 네트워크 수수료를 충당하기 위해 더 나은 가격을 기다리기 때문이다.

CoW Swap UI는 미체결 주문의 실행 가격(execution price) 과 지정가(limit price) 를 함께 표시하여 이를 명확히 보여준다. 미체결 주문 패널의 “Executes at” 열을 보면, 현재 네트워크 상태를 기준으로 주문이 실행되려면 토큰 가격이 어느 수준에 도달해야 하는지 확인할 수 있다.



“Executes at” 열에는 주문 실행까지의 거리를 시각적으로 보여주는 신호등(traffic light) 시스템이 있다. 이는 현재 네트워크 수수료, 주문 규모, 시장(스팟) 가격을 함께 고려한다.

해당 열 위에 마우스 포인터를 올리면, 주문이 실행 구간에 진입하기 위해 가격이 얼마나 움직여야 하는지에 대한 설명이 표시된다.

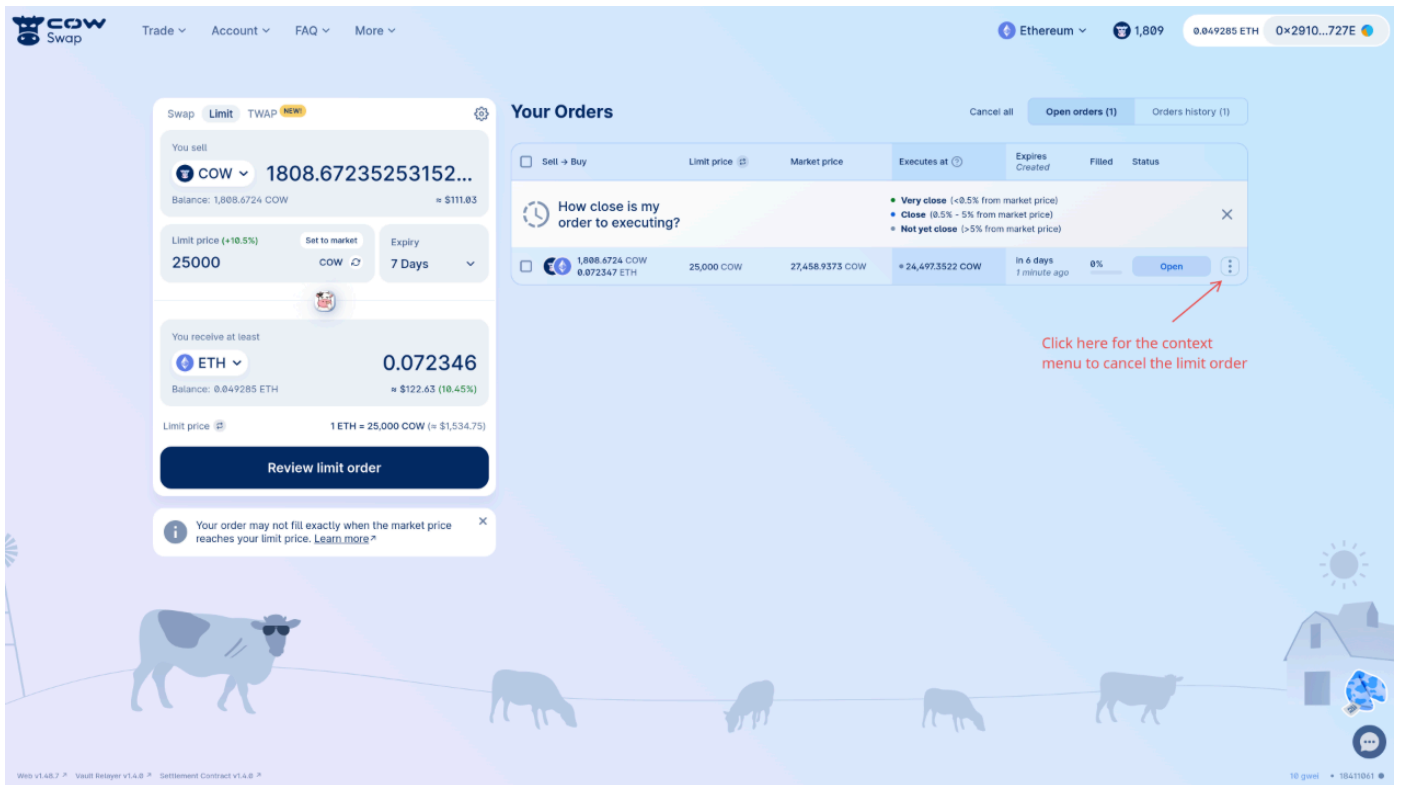


해당 필드를 클릭하면 개별 주문의 가격 표시 방향이 반전되며, 마우스 오버 시 표시되는 텍스트도 이에 따라 변경된다.



지정가 주문 취소 (Cancel a limit order)

이제 생각해 보니 COW를 팔지 않는 것이 좋다고 판단되었다면, 지정가 주문을 취소할 수 있다. 주문의 컨텍스트 메뉴를 클릭하고 “Cancel order”를 선택한다.



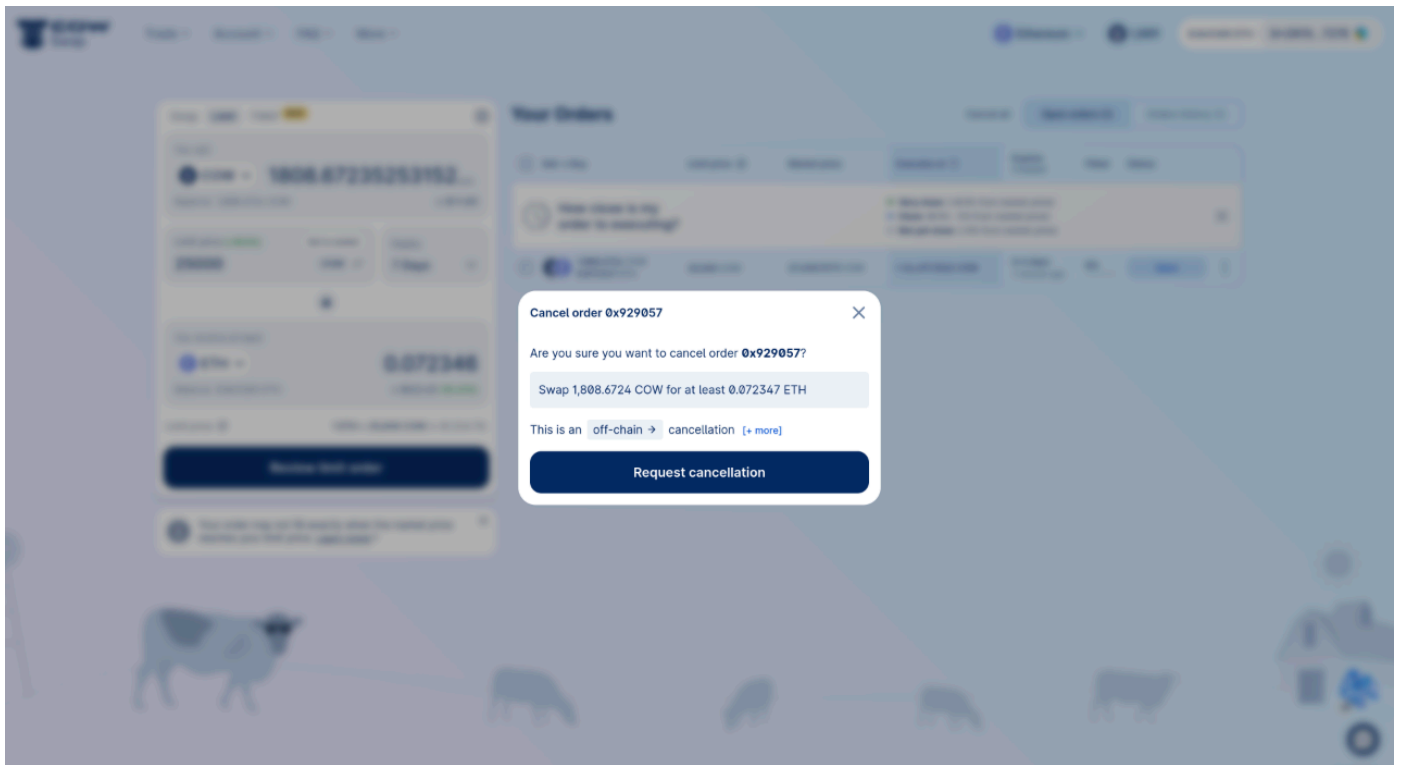
“Cancel order” 를 선택하면 이 작업을 확인하라는 메시지가 표시된다.

오프체인(off-chain) 취소는 무료이며 트랜잭션이 필요 없다. 하지만 취소 요청과 오프체인 처리 사이에 주문이 매칭될 가능성이 있다.

Note

취소는 즉시 이루어지지 않으며, 취소가 처리되기 전에 주문이 체결될 수 있다.

오프체인 취소를 진행하려면 아래와 같이 Request cancellation을 클릭한다.



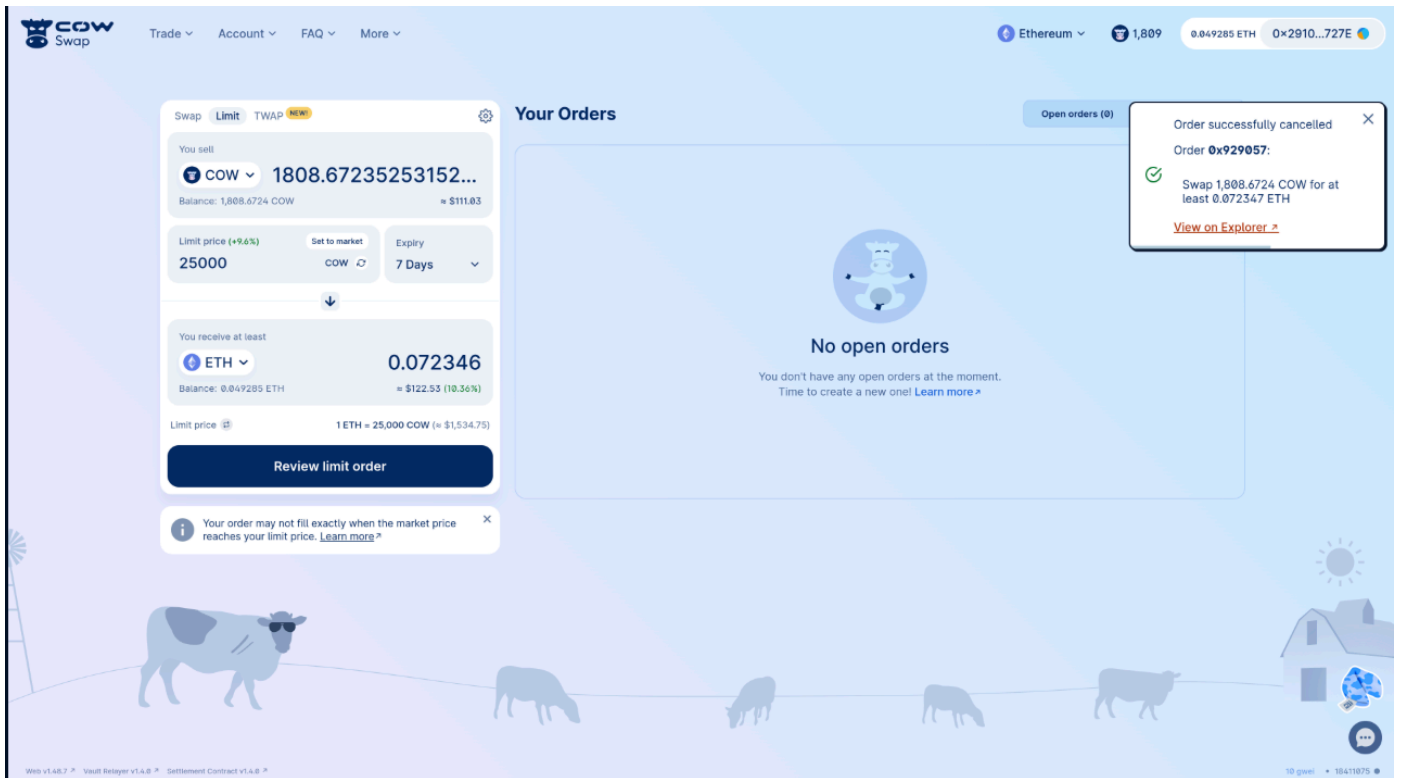
API를 신뢰하지 않고 주문을 직접 취소하고 싶다면, 온체인(on-chain) 트랜잭션을 통해 주문을 취소할 수 있다. 이 경우 가스비가 발생한다. off-chain을 클릭하여 취소 유형을 on-chain으로 전환한다.

Note

온체인 취소의 경우에도, 취소 트랜잭션이 블록에 포함되기 전에 주문이 매칭될 수 있는 위험이 있다. 우선순위 수수료로 높게 설정하고 신속하게 서명하라.

CoW Protocol의 지정가 주문 취소는 오프체인 방식일 경우 무료이므로, 원하는 만큼 자유롭게 지정가 주문을 생성하고 취소할 수 있다. (단, 빠른 취소를 원한다면 온체인 취소를 선택할 수도 있다.)

주문이 취소되면 미체결 주문(Open Orders) 목록에서 제거되고, 주문 내역(Orders History) 으로 이동한다.



TWAP 주문 (TWAP orders)

시간가중평균가격(Time-Weighted Average Price, TWAP) 주문은 CoW Protocol의 고급 기능으로, 대규모 주문을 일정 시간 동안 분산 실행함으로써 가격 충격을 최소화하고 보다 안정적인 평균 가격을 달성하는 데 적합하다.

소개 (Introduction)

TWAP 주문은 대규모 거래를 여러 개의 작은 부분으로 나누어 일정한 간격으로 실행할 수 있게 한다. 이를 통해 시장 충격을 줄이고, 결과적으로 더 나은 평균 가격을 달성할 가능성이 높다.

장점 (Benefits)

- 대규모 주문의 가격 충격 완화: 예를 들어, 3시간 동안 6단계로 100만 달러 상당의 ETH를 매수할 경우, TWAP은 30분마다 16.6만 달러 규모의 주문을 실행하여 가격 충격을 크게 줄이고 시장 회복 시간을 확보한다.
- 시간에 따른 평균 매입가 확보: 선택한 기간 동안 가격을 분산시켜 높은 가격에서 매수할 위험을 낮춘다.
- 반복적 또는 대규모 거래에 적합: 메인넷의 최소 주문 금액은 1,000달러이며, Gnosis Chain, Arbitrum One, Base에서는 최소 5달러이다.

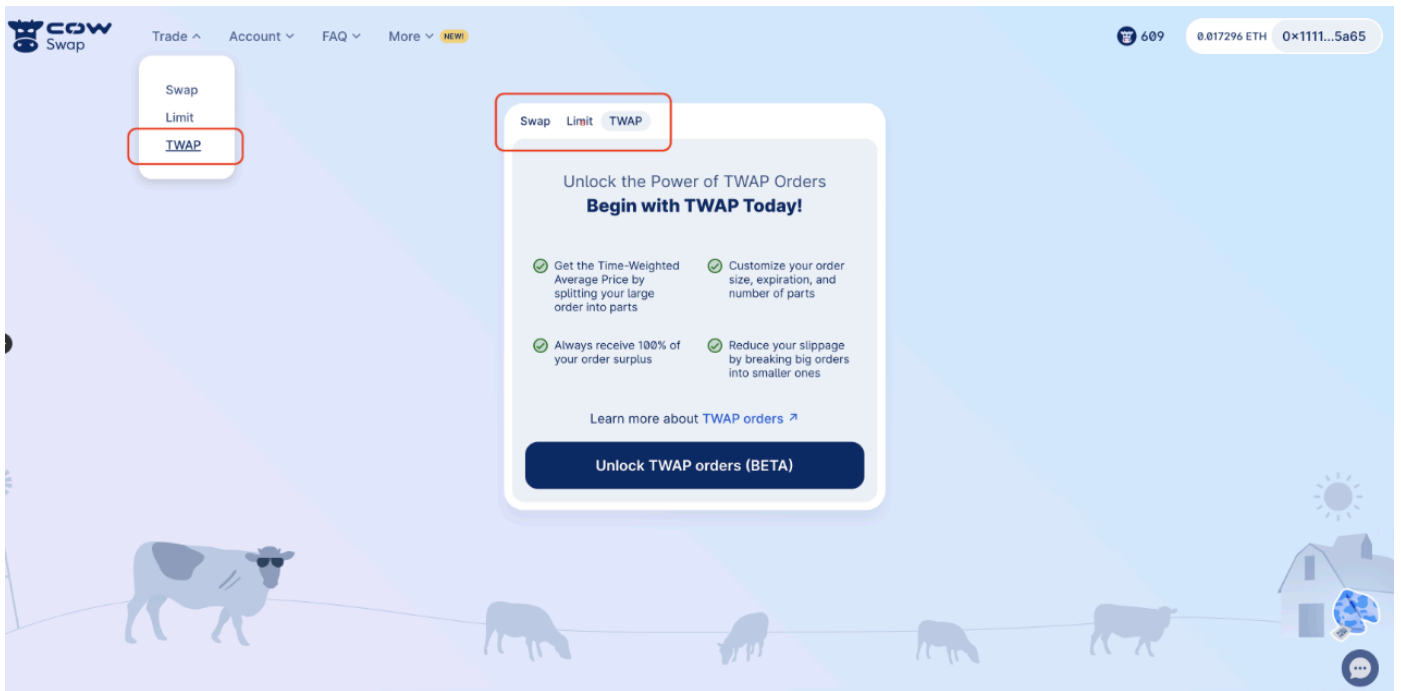
TWAP 주문 생성 (Placing a TWAP Order)

Safe 지갑 연결 (Connect your Safe wallet)

CoW Swap의 TWAP 주문은 Safe 지갑이 필요하다.

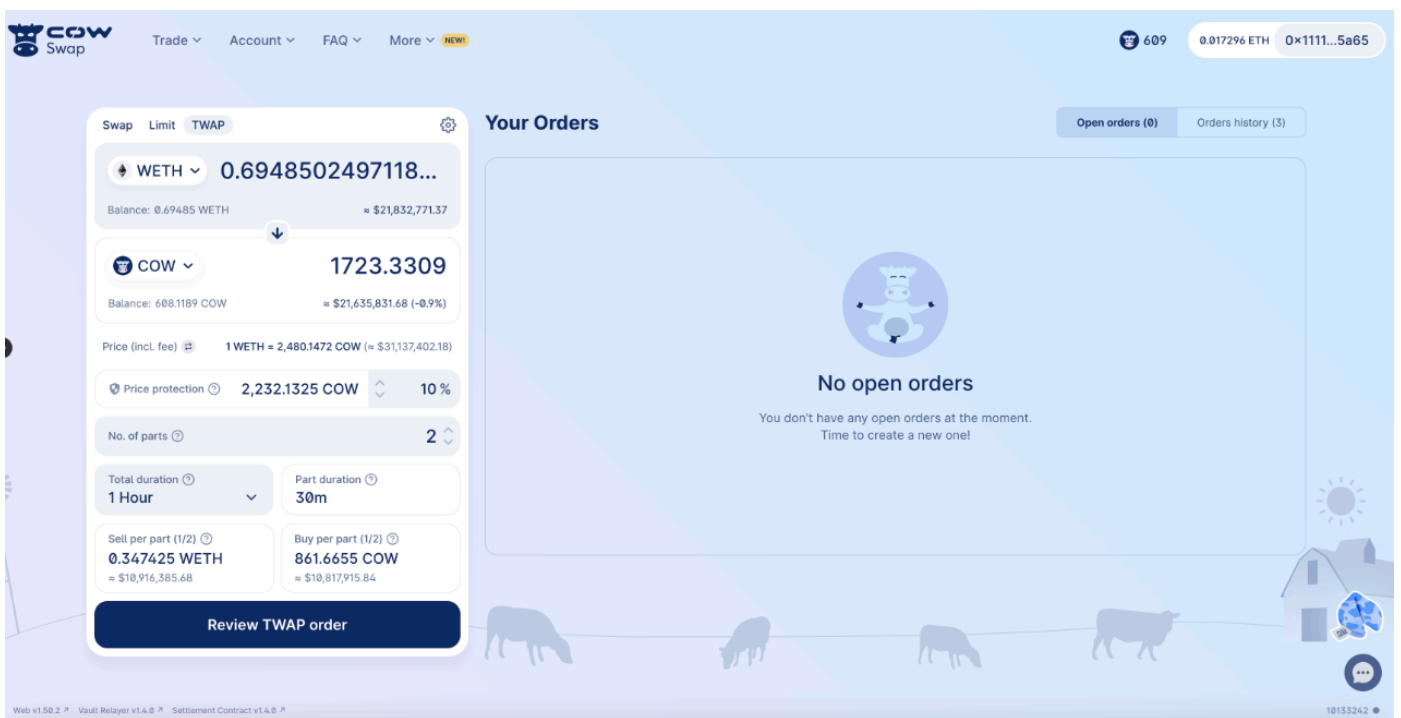
- 아직 Safe 지갑이 없다면 Safe 지갑 생성을 통해 만들 수 있다.
- Safe 지갑을 연 뒤 CoW Swap (Safe App)을 실행한다.

CoW Swap이 Safe와 연결되면 중앙 모듈 근처의 “TWAP” 탭 또는 CoW Swap 로고 옆 드롭다운 메뉴를 통해 TWAP 주문 기능에 접근할 수 있다.



토큰 선택 (Select tokens)

판매하려는 토큰(예: WETH)을 선택하고 총 판매 금액을 입력한다.



매개변수 지정 (Specify parameters)

이 단계는 주문이 시간에 따라 어떻게 실행될지를 정의하는 중요한 단계이다. TWAP 주문 설정을 조정하는 방법은 다음과 같다:

Price (incl. fee)

1 WETH = 2,480.1472 COW (≈ \$31,137,402.18)

1

Price protection 2,232.1325 COW 10 %

2

No. of parts 2

3

Total duration 1 Hour

4

Part duration 30m

5

Sell per part (1/2) 0.347425 WETH
≈ \$10,916,385.68

6

Buy per part (1/2) 861.6655 COW
≈ \$10,817,915.84

1. 가격 보호 (Price Protection):

주문이 제출 시점의 시장 가격에서 지나치게 벗어난 가격으로 실행되는 것을 방지한다. 가격 보호 비율(거래 허용 가격 범위)을 설정한다. 예를 들어, 10% 가격 보호를 설정하면 주문 시점에서 가격이 10% 이상 불리하게 변동하면 해당 부분은 실행되지 않는다.

2. 분할 수 (Number of Parts):

주문을 몇 개의 개별 부분으로 나눌지 결정한다. 이는 TWAP 전략의 세분화 수준을 결정한다. 예를 들어, 총 2 WETH를 2부분으로 나누면 각 부분은 1 WETH씩 거래된다. 메인넷의 최소 주문 금액은 1,000달러(또는 Gnosis, Arbitrum, Base에서는 5달러)이며, 각 부분은 온체인에서 개별적으로 실행되므로 각 실행마다 수수료가 발생한다.

3. 총 지속 시간 (Total Duration):

주문이 실행될 전체 기간을 설정한다. TWAP 전략은 해당 기간 동안 거래를 균등하게 분배한다. 1시간, 6시간 등의 사전 설정 시간 또는 맞춤 기간을 선택할 수 있다.

4. 부분 지속 시간 (Part Duration):

각 부분이 실행되는 주기를 설정한다. 이는 총 지속 시간을 분할 수로 나눈 값으로, 예를 들어 총 지속 시간이 1시간이고 분할 수가 2라면 각 부분은 30분마다 실행된다.

5. 부분당 판매량 (Sell per Part, 읽기 전용):

분할 수와 총 지속 시간을 설정하면 인터페이스에 각 실행 부분의 판매량이 표시되어 예상 체결량을 검토할 수 있다.

6. 부분당 구매량 (Buy per Part, 읽기 전용):

매수 TWAP 주문의 경우, 각 실행 부분에서 구매할 토큰의 수량을 표시한다.

시장 상황과 전략적 목표에 따라 매개변수를 신중히 조정하라. 이러한 설정은 TWAP 전략의 효율성과 성과를 향상시킬 수 있다. 세부 내용을 검토 후 서명을 진행하여 주문을 최종 확정할 수 있다.

지원되지 않는 지갑일 경우 – Safe Fallback Handler 업그레이드 (Unsupported wallet? Upgrade Safe Fallback Handler)

지갑이 지원되지 않는 경우, TWAP 주문에 필요한 특수 폴백 핸들러가 포함된 Safe로 업그레이드해야 한다. [Safe 폴백 핸들러 개요](#)와 [관련 블로그 게시물](#)을 참고하라. 이 업그레이드 프로세스는 [광범위한 감사](#)를 거쳐 안전성을 확보하였다.



Unsupported wallet detected

TWAP orders currently require a Safe with a special fallback handler. Have one? Switch to it! Need setup? [Click here](#). Future updates may extend wallet support!

검토 및 확인 (Review and confirm)

가격 보호 및 지정가를 포함한 모든 주문 세부 정보를 확인한 뒤, Safe 인터페이스에서 트랜잭션에 서명한다.

Caution

승인 트랜잭션에 서명할 때는 주의해야 한다. spender 주소가 올바른지(이 경우 TWAPContract의 주소) 반드시 확인하라.

위 사항에 대해 확신이 없다면 트랜잭션에 서명하지 말라. 승인 내역을 검토하려면 [revoke.cash](#)를 사용할 수 있다.

주문 서명 시 주의하라. 모든 관련 파라미터는 최종적이며, 서명 및 API 제출 후 변경할 수 없다. 실수가 있다면 주문 개요에서 주문을 취소한 후 새 주문을 생성해야 한다.

Review TWAP order



Sell amount



0.69485

Balance: 0.69485 WETH

≈ \$21,832,771.37



Estimated receive amount



1,723.3309

Balance: 608.1189 COW

≈ \$21,635,831.68 (-0.9%)

Price (incl. fee)

1 WETH = 2,480.1472 COW (≈ \$31,137,402.18)

↳ Price protection

10%

↳ Limit price

1 WETH = 2,232.1325 COW (\$31,420,829.7)

↳ Min received

1,550.9978 COW (≈ \$19,472,248.51)

TWAP order split in 2 equal parts

↳ Sell amount per part (1/2)

0.347425 WETH (≈ \$10,916,385.68)

↳ Buy amount per part (1/2)

≈861.6655 COW (≈ \$10,817,915.84)

Start time first part (1/2)

Now

Part duration

30 minutes

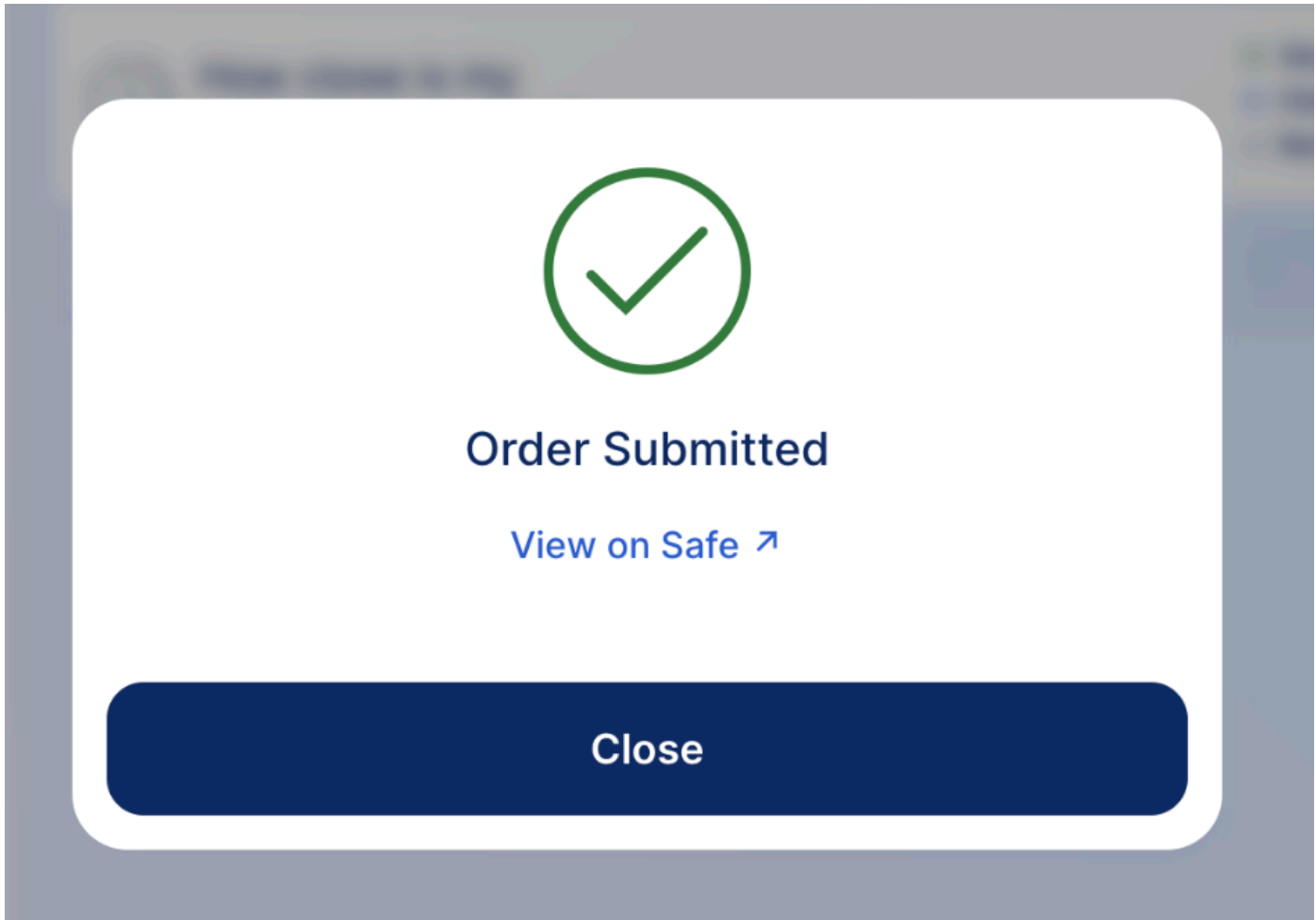
Total duration

1 hours

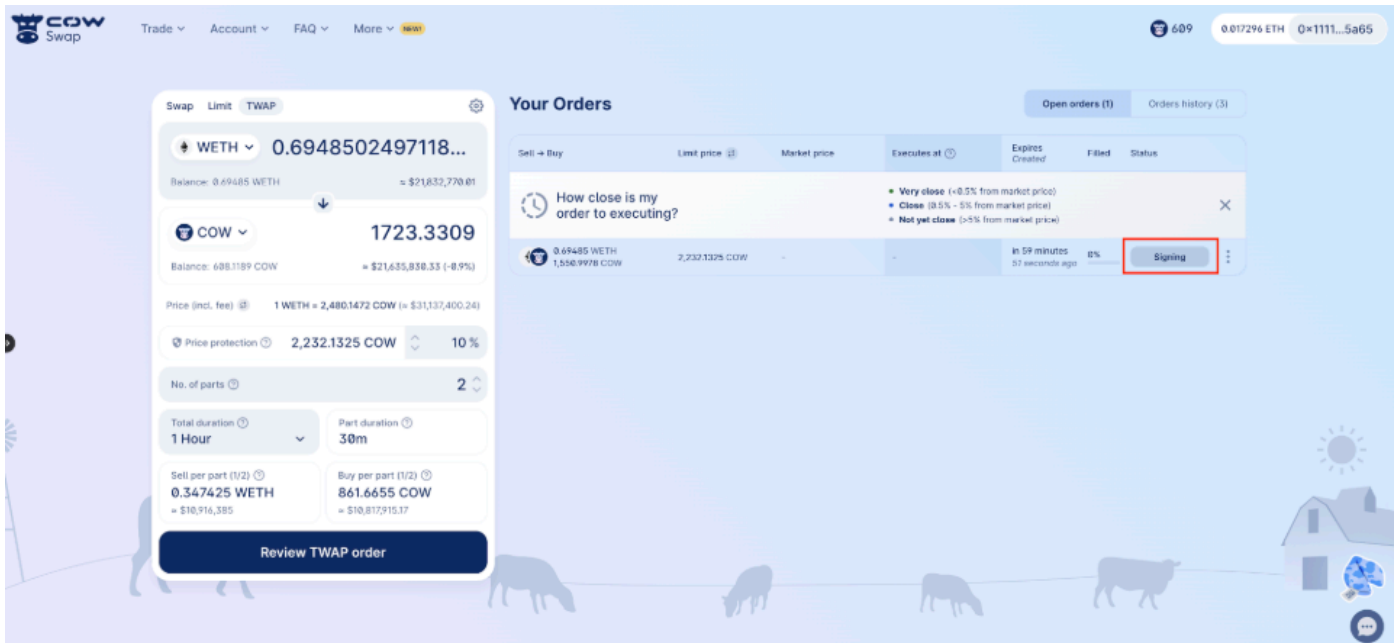
Place TWAP order

최종 확정 및 모니터링 (Finalization and monitoring)

주문에 서명하면 TWAP 주문의 최종 확정 및 모니터링 프로세스가 시작된다. 이는 주문이 안전하게 처리되고 활성화되도록 하는 다단계 절차다.

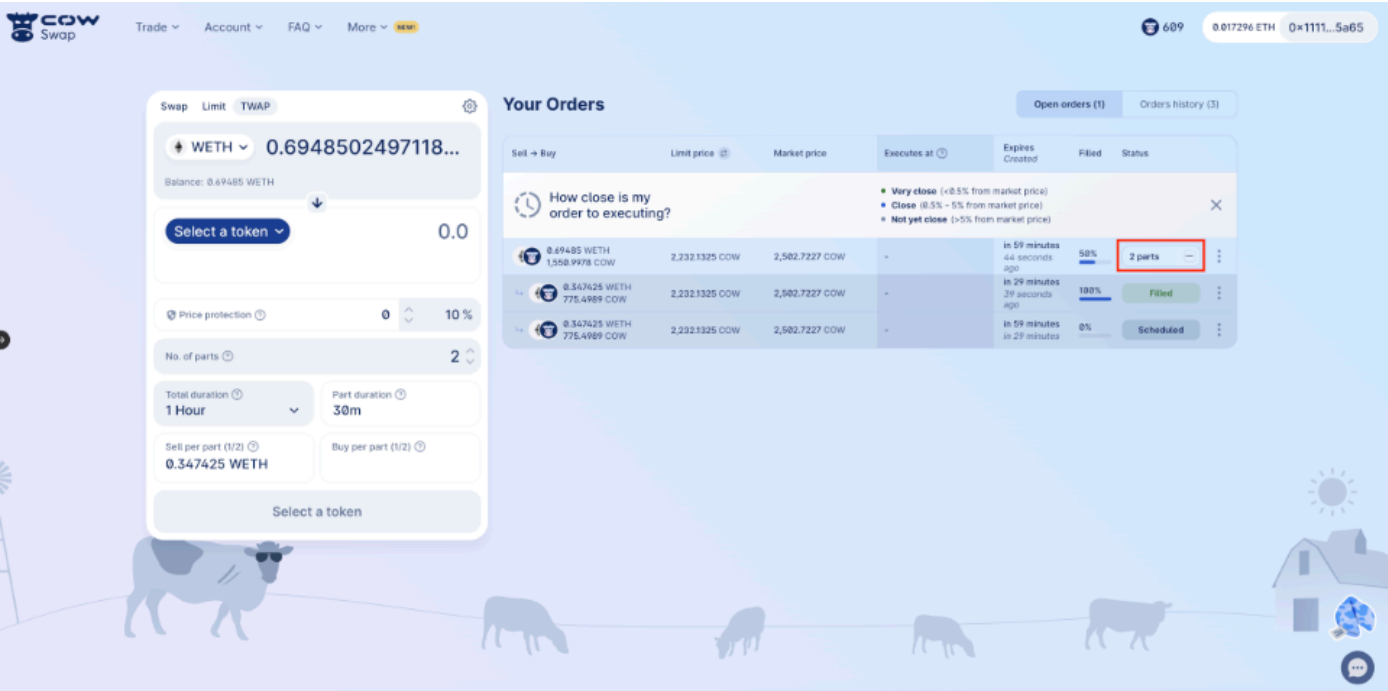


“Order submitted successfully” 화면은 주문이 초기적으로 승인되었음을 의미한다.

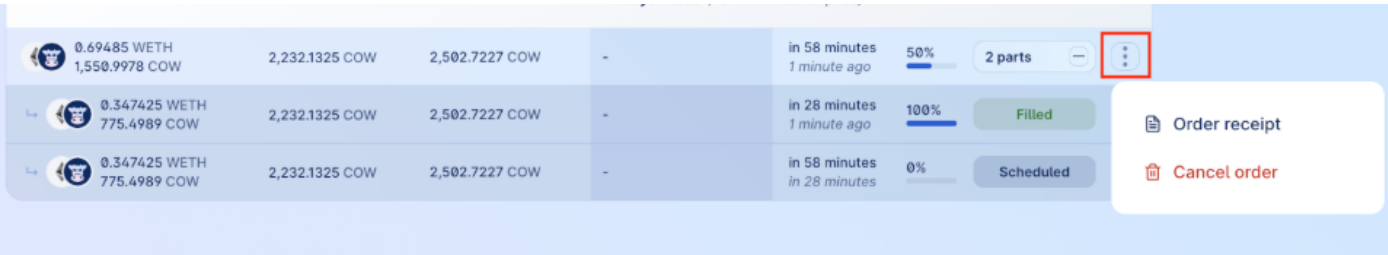


“Order in signing state” 화면은 Safe에서 추가 서명이 필요함을 나타낸다. 모든 서명자가 서명해야 다음 단계로 진행된다.

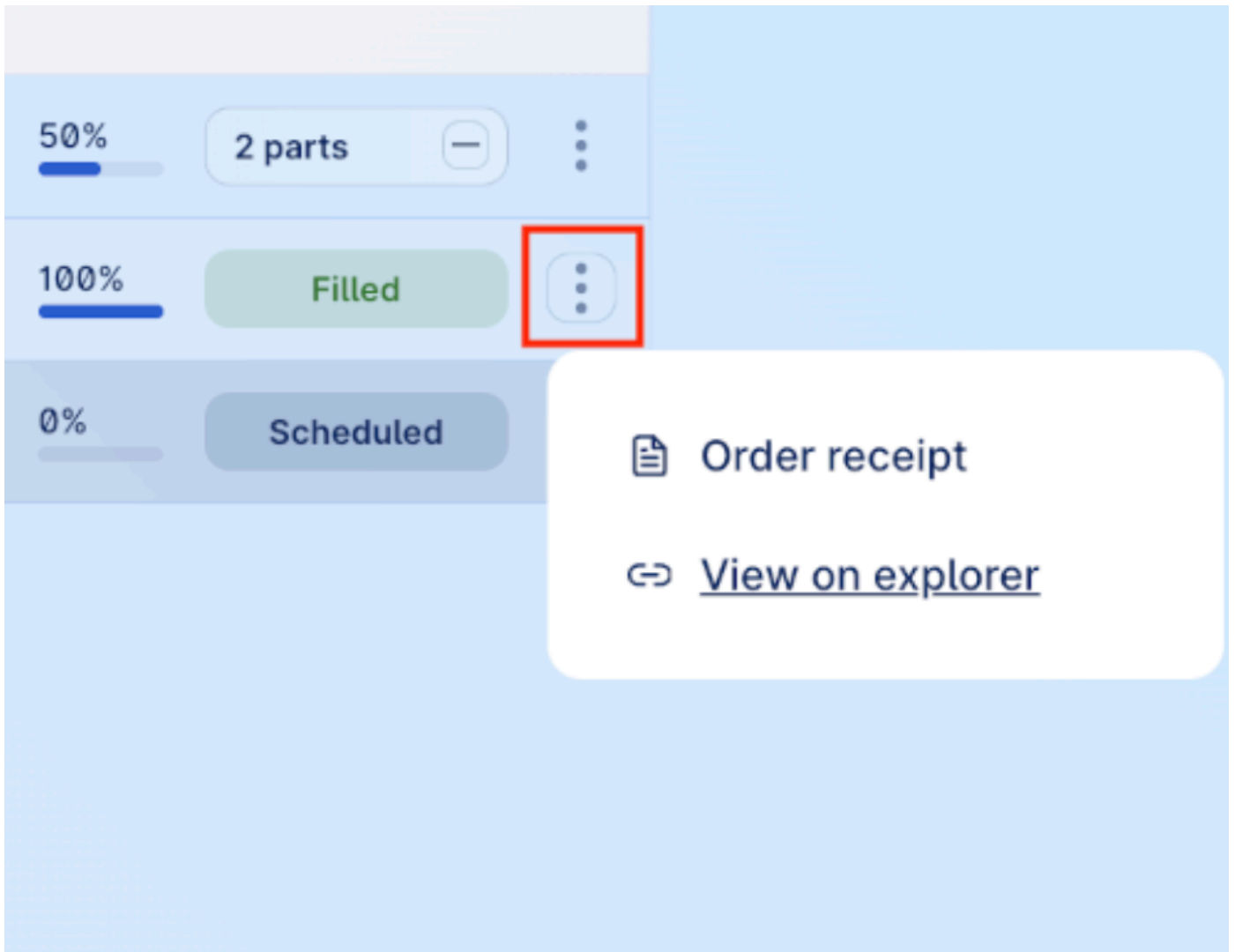
모든 서명이 완료되고 트랜잭션이 온체인에 제출되면 주문이 활성화(active) 상태가 된다. “Orders overview”에서 주문의 현재 상태를 모니터링하고 활성화 주문 전체 목록을 확인할 수 있다.



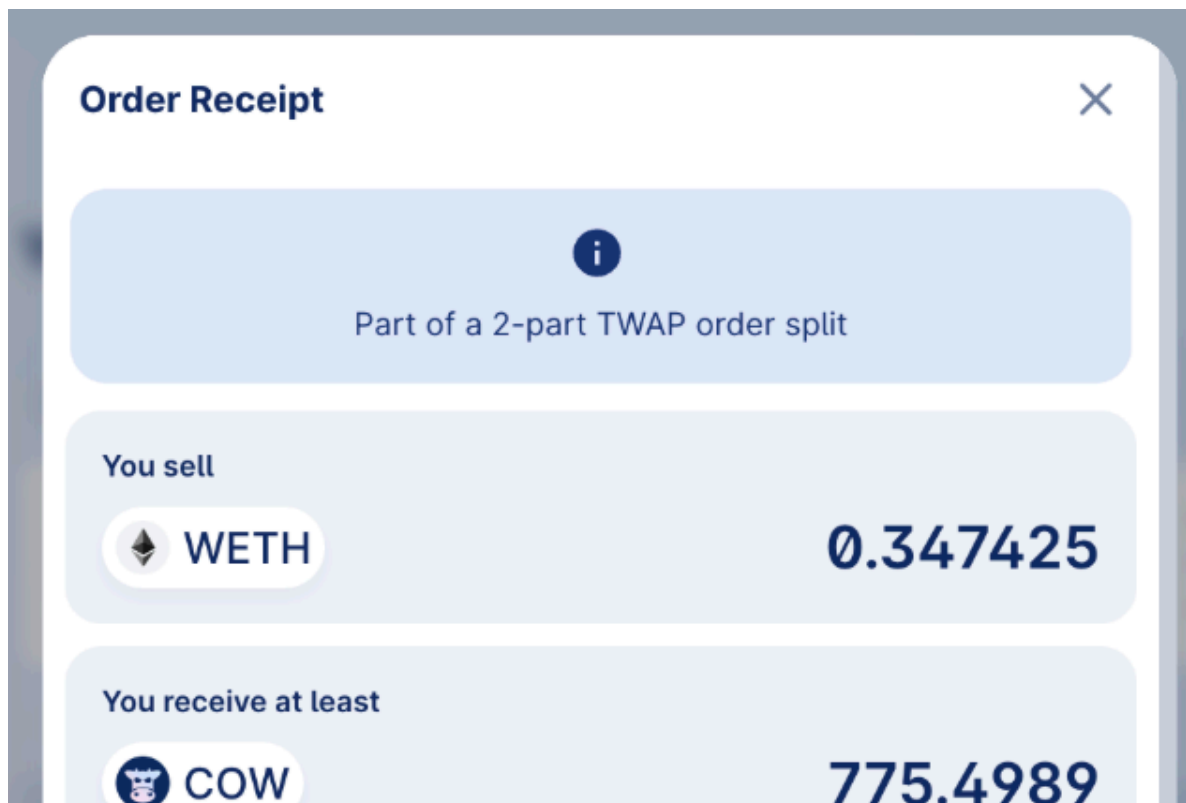
각 TWAP 주문은 개별 실행 부분을 확장하여 볼 수 있다.



상위 TWAP의 점 3개 메뉴(three-dot menu)에서는 모든 부분에 영향을 미치는 작업을 수행할 수 있다.



각 TWAP 부분별 메뉴에서도 해당 부분에만 적용되는 개별 작업을 수행할 수 있다.



Status	Filled
Recipient ⓘ	0x1111...5a65 ↗
Limit price ⓘ	1 WETH = 2,232.1325 COW
Execution price ⓘ	1 WETH = 2,480.1472 COW
Filled ⓘ	100% 0.347425 WETH sold for a total of 861.6655 COW
Order surplus ⓘ	+11.11% 86.1665 COW
Fee ⓘ	< 0.000001 WETH
Created ⓘ	1 minute ago (Nov 30 2023, 2:06 PM)
Expiry ⓘ	in 28 minutes (Nov 30 2023, 2:35 PM)
Order type ⓘ	Limit sell order (Fill or Kill)
Order ID	0xf442cd ↗

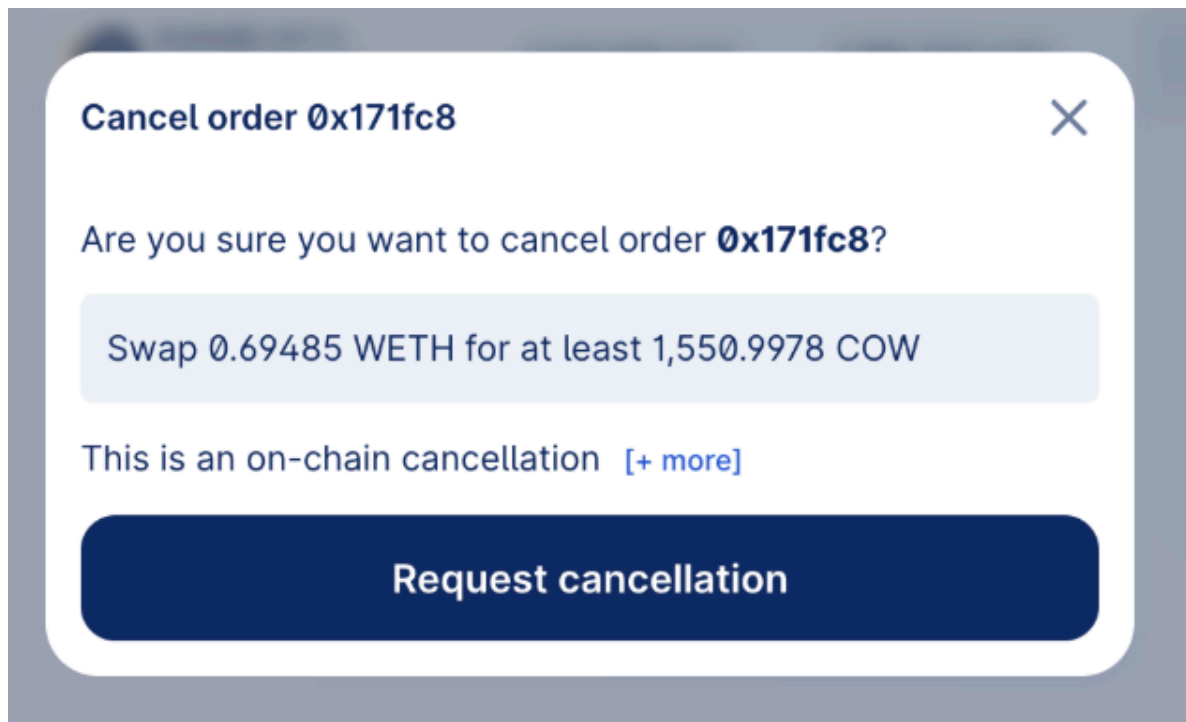
마지막으로 “Order receipt” 화면은 활성 TWAP 주문의 실행 세부 정보와 트랜잭션 정보를 포함한 상세 확인서를 제공합니다.

TWAP 주문 취소 (Cancelling a TWAP order)

TWAP 주문 취소는 몇 가지 간단한 단계로 이루어진다. “Your Orders” 섹션에서 활성 TWAP 주문을 찾아 관리한다.

0.69485 WETH 1,558.9978 COW	2,232.1325 COW	2,502.7227 COW	+	in 58 minutes 1 minute ago	58%	2 parts	⋮
0.347425 WETH 775.4989 COW	2,232.1325 COW	2,502.7227 COW	+	in 28 minutes 1 minute ago	100%	Filled	Order receipt
0.347425 WETH 775.4989 COW	2,232.1325 COW	2,502.7227 COW	+	in 58 minutes in 28 minutes	0%	Scheduled	Cancel order

주문 개요에서 취소하려는 주문을 찾아 행의 끝에 있는 점 3개 메뉴 아이콘을 클릭하여 추가 작업을 연다. 드롭다운 메뉴에서 “Cancel order”를 선택하여 취소 프로세스를 시작한다.



확인 창에는 취소하려는 주문의 세부 사항(스왑 정보 및 트랜잭션 유형 포함)이 요약되어 표시된다. 올바른 주문을 취소하는지 확인하는 단계다.

“Request cancellation” 을 클릭하여 취소를 확인하면 Safe 내에서 새로운 트랜잭션이 생성된다. 이 트랜잭션은 모든 서명자(Safe 소유자)가 서명하기 전까지는 최종적으로 실행되지 않는다.

모든 서명이 완료되면 취소 트랜잭션이 실행된다. 특히 시장 상황 변화나 전략적 이유로 빠른 취소가 필요한 경우 모든 서명자와 신속히 협력해야 한다.

취소 트랜잭션이 완전히 서명되고 제출되면 주문은 활성 주문 목록에서 제거되며 취소된 것으로 간주된다.

결론 (Conclusion)

TWAP 주문은 대규모 거래를 위한 전략적 접근 방식으로, 가격 충격을 완화하고 더 나은 평균 가격을 확보한다. 직접 시도해보고 경험을 info@cow.fi로 공유해보자.

네이티브 토큰 (Native tokens)

블록체인 네트워크에서 “네이티브 토큰”은 기본 디지털 화폐를 의미한다. 예를 들어, 이더리움, Arbitrum One, Base에서는 Ether(ETH), Gnosis Chain에서는 xDAI(xDai)가 네이티브 토큰이다. 네이티브 토큰은 네트워크 운영(예: 트랜잭션 수수료 지불)에 필수적이다.

“래핑된(wrapped)” 토큰 — 예를 들어 Wrapped Ether(WETH), Wrapped xDAI(wxDAI) — 은 이러한 네이티브 토큰의 ERC-20 호환 버전이다.

래핑된 토큰은 탈중앙화 애플리케이션 간 상호 운용성을 높이기 위해 존재한다. 네이티브 토큰과 그 래핑 버전은 서로 동등하며, 사용자는 항상 1:1 비율로 양방향 변환(“wrap” 또는 “unwrap”)할 수 있다.

CoW Protocol에서 ETH와 같은 네이티브 토큰을 구매하는 것은 간단하다. 그러나 CoW Protocol은 기본적으로 ERC-20 토큰만 판매 가능하다.

이는 프로토콜의 의도 기반(intent-based) 구조가 솔버를 통해 사용자의 판매 토큰을 거래하도록 설계되어 있기 때문이다.

이 과정은 특정 “spender” 컨트랙트가 사용자의 자금을 대신 관리할 수 있도록 하는 ERC-20의 승인(approval) 메커

니즘 덕분에 가능하다.

그럼에도 불구하고, CoW Protocol은 사용자가 네이티브 토큰을 판매할 수 있는 두 가지 방법을 제공한다:

옵션 1) 스왑 전에 네이티브 토큰 래핑

네이티브 토큰을 ERC-20 토큰으로 래핑 (예: ETH → WETH)한 뒤, CoW Protocol에서 가스 없이 WETH를 스왑.

옵션 2) Eth-flow 사용

단일 트랜잭션을 통해 래핑과 주문 생성을 동시에 수행하는 특수 컨트랙트를 사용.

Tip

래핑은 반복 사용자에게 가장 적합하다. 또한 네이티브 토큰을 여러 번 판매할 계획이라면, 한 번에 ETH를 모두 래핑하여 가스비를 한 번만 지불하는 것이 좋다.

단 한 번의 스왑이라면 Eth-flow 사용을 고려하라.

옵션 1) 스왑 전에 네이티브 토큰 래핑 (Wrap native tokens before swapping)

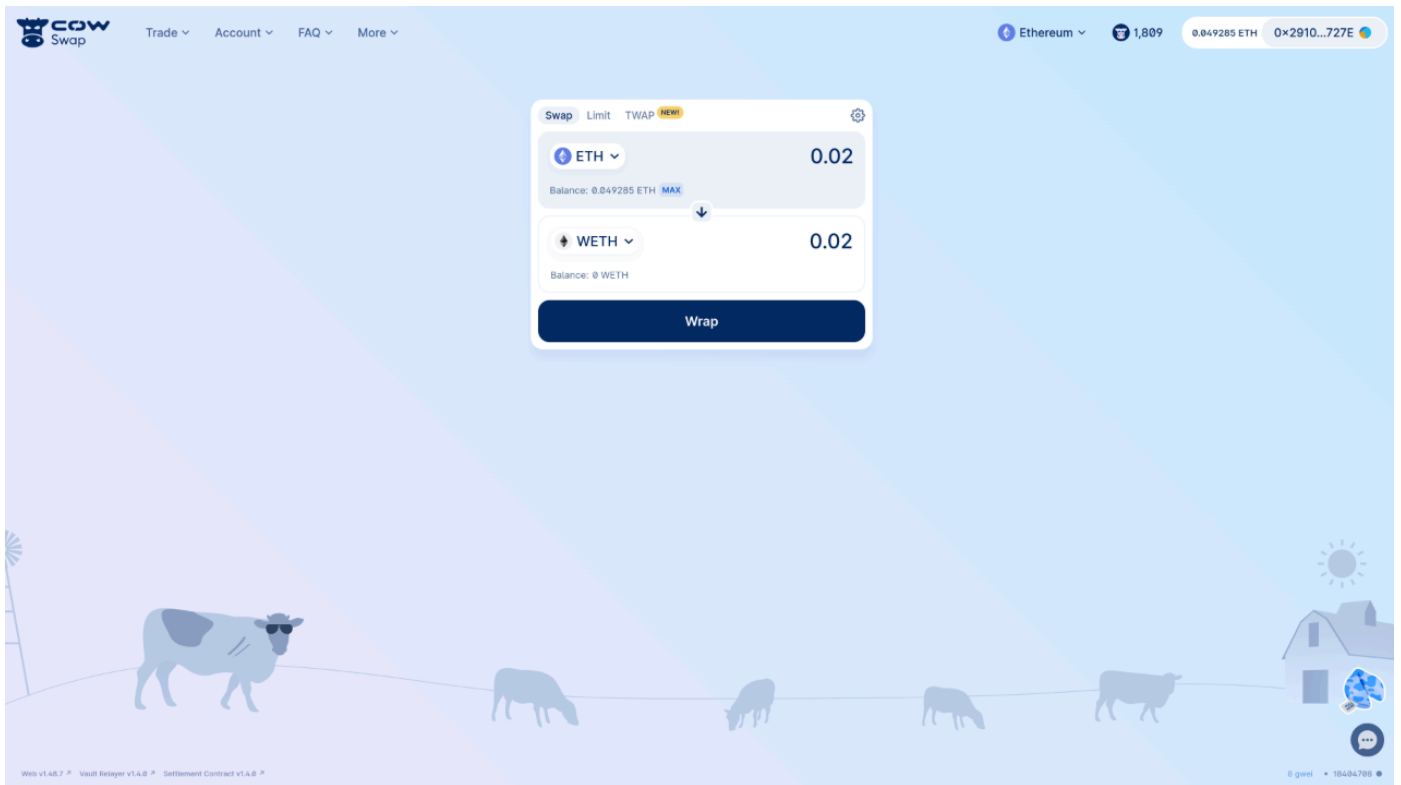
스왑 전에 래핑하는 것은 추가 단계가 필요하지만, 그만큼 다음과 같은 이점이 있다:

1. 여러 번 스왑할 경우 더 낮은 총 수수료.
2. 더 낮은 기본 슬리피지.
3. 실패한 스왑에 대한 수수료 없음.

CoW Swap UI는 네이티브 토큰 래핑을 기본적으로 지원한다.

이를 위해, 판매할 네이티브 토큰(예: ETH)을 판매 토큰으로 선택하고, 그에 해당하는 래핑된 ERC-20 버전(예: WETH)을 구매 토큰으로 선택한다.

버튼이 자동으로 “Swap”에서 “Wrap”으로 변경된다.



네이티브 토큰 래핑은 온체인 트랜잭션이며 가스비가 필요하다.

토큰을 래핑한 후에는, 해당 래핑된 토큰을 판매 토큰으로 선택하고 스왑을 진행하면 된다.

옵션 2) Eth-flow 사용 (Use Eth-flow)

사용자 경험을 개선하기 위해, CoW Protocol은 Eth-flow 컨트랙트를 도입했다.

이를 통해 사용자는 위 과정을 자동화하여 단일 온체인 트랜잭션에서 래핑과 스왑을 동시에 수행할 수 있다.

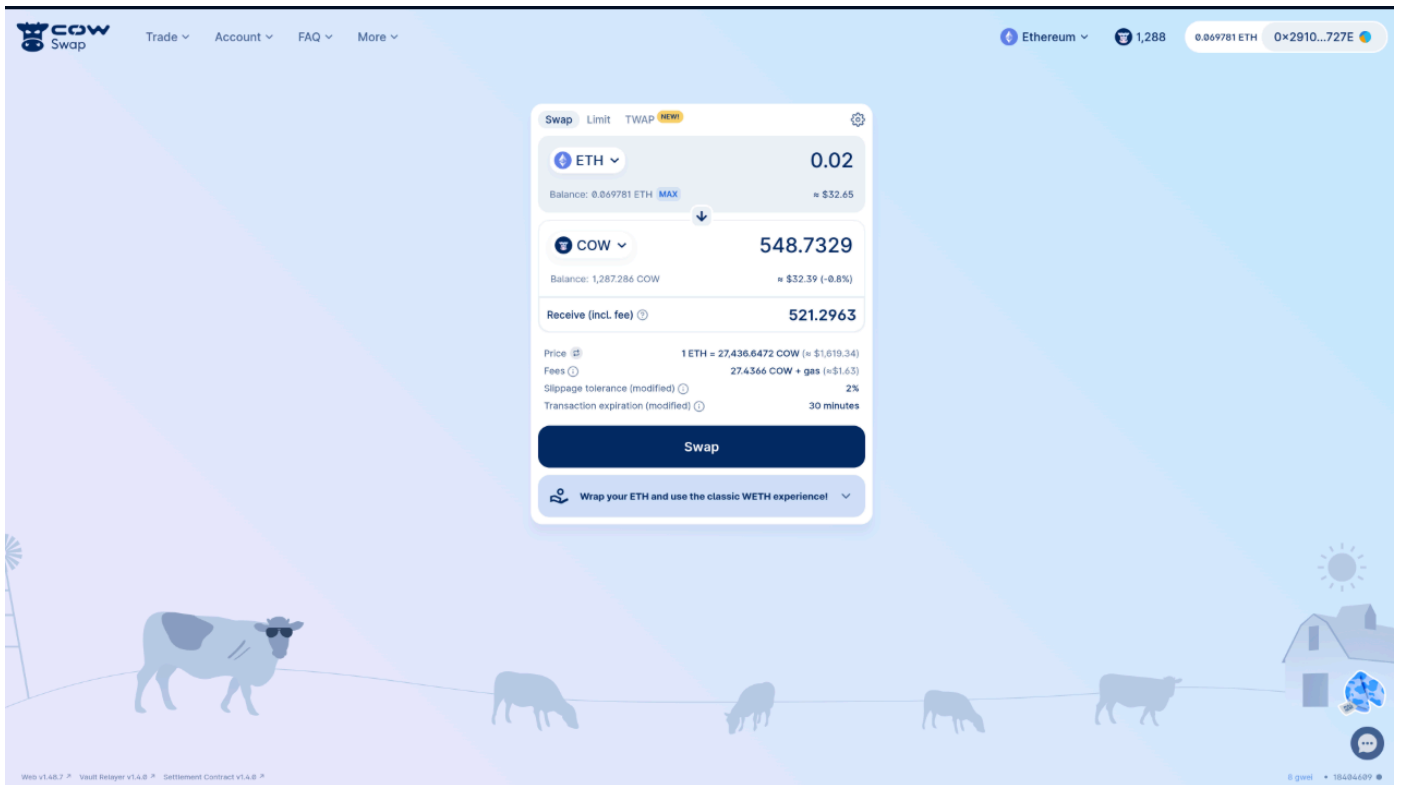
Eth-flow의 주요 이점은 다음과 같다:

1. 한 번만 스왑할 경우 더 낮은 총 수수료.
2. 더 간단한 UX (단일 트랜잭션).
3. WETH를 명시적으로 승인할 필요가 없음.

Eth-flow 컨트랙트 사용은 스왑 전 래핑보다 빠르지만, Eth-flow 트랜잭션은 온체인에서 수행되므로(대부분의 CoW Swap 스왑과 달리)

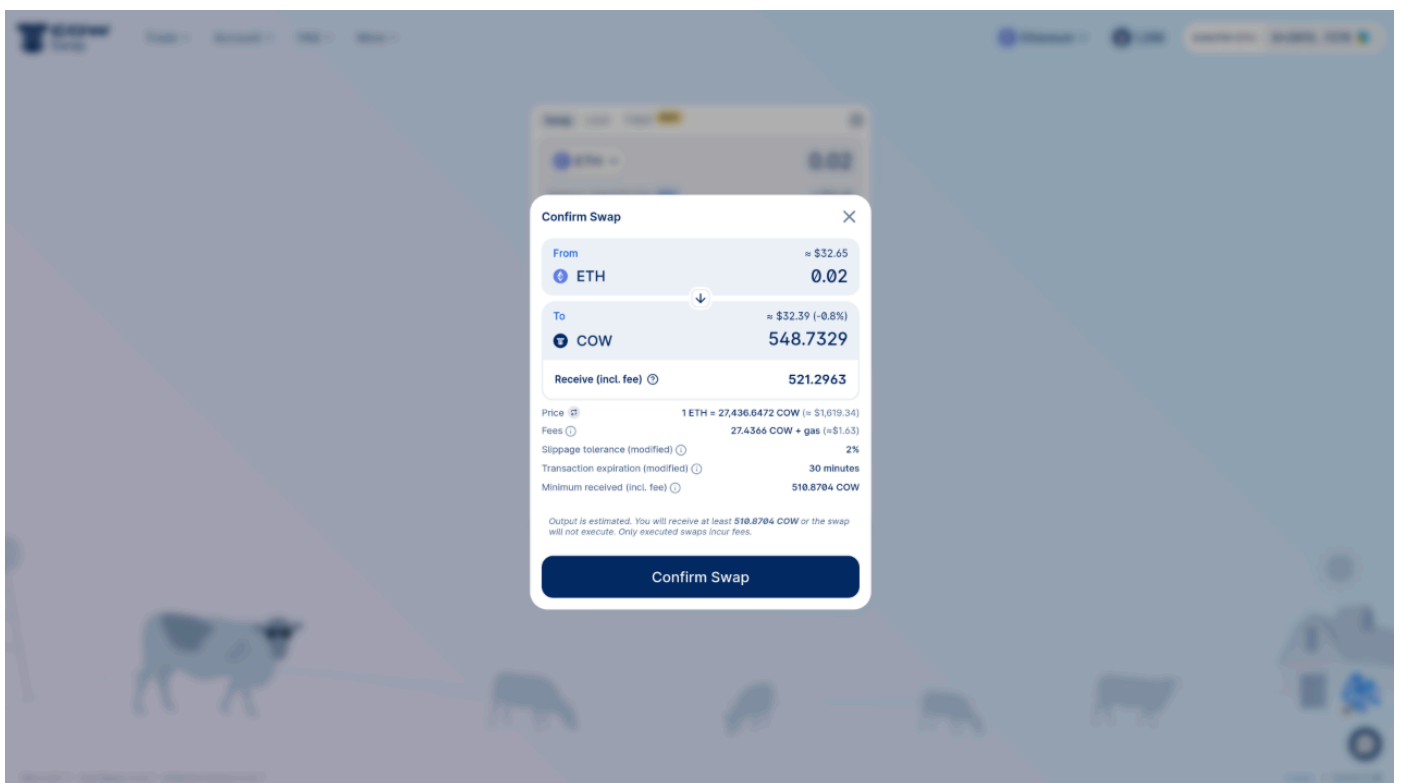
사용자는 네이티브 토큰으로 선불 가스비를 지불해야 한다.

주문이 실패하더라도 이 수수료는 환불되지 않는다.



Eth-flow 컨트랙트를 사용하는 방법:

1. 스왑하려는 네이티브 토큰(예: ETH)과 구매할 토큰(예: COW)을 선택한다.
2. “Swap”을 클릭한다. CoW Protocol은 네이티브 토큰이 래핑되어야 하는지 자동으로 감지하고, 사용자를 대신 해 Eth-flow 컨트랙트를 실행한다.
3. 토큰을 선택하면, CoW Swap이 스왑 확인을 요청한다. 이 온체인 트랜잭션은 네이티브 토큰을 래핑(필요할 경우) 하고 CoW Protocol에 주문을 등록한다.



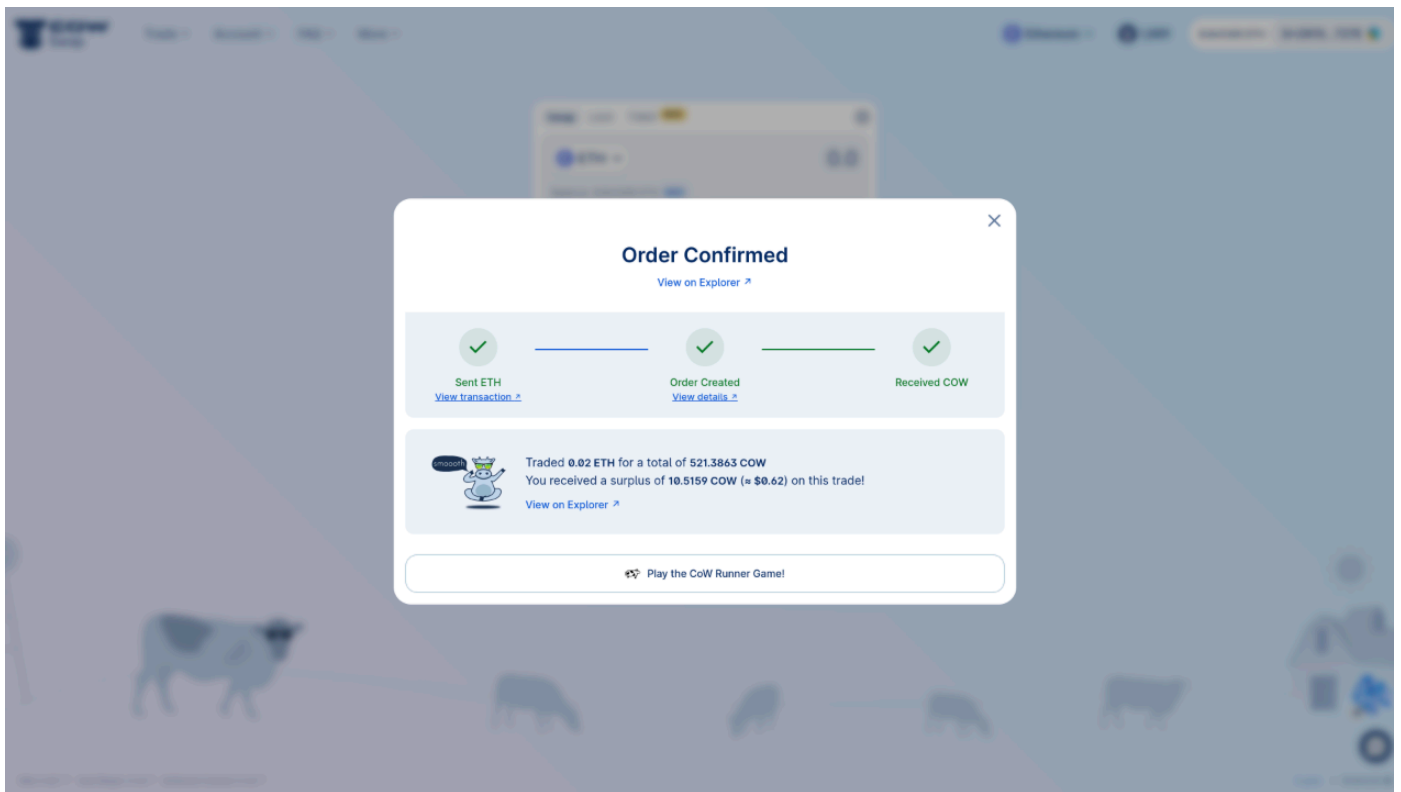
Tip

ETH를 자주 스왑할 계획이라면 일부를 WETH로 래핑해두는 것이 네트워크 수수료 절감에 도움이 된다.

Eth-flow를 여러 번 사용하는 것은 일반적으로 네이티브 토큰을 한 번 래핑하고 이후 WETH로 여러 번 스왑하는 것보다 비용이 더 높다.

또한, 비네이티브 토큰 스왑은 가스 없는(gasless) 취소가 가능하다.

스왑을 확인하면 지갑에서 [Eth-flow](#) 컨트랙트와 상호작용하는 온체인 트랜잭션을 서명하고 생성한다. 이 트랜잭션이 완료되면 주문이 CoW Protocol에 등록된다.



Note

Eth-flow 컨트랙트를 사용할 때, 주문은 ETH가 Eth-flow 컨트랙트로 전송되는 트랜잭션이 확인된 후에만 등록된다.

따라서 구매 토큰이 도착하기 전에 ETH 잔액이 일시적으로 줄어든 것처럼 보일 수 있다.

걱정하지 말라! 주문이 실패하면 ETH는 계정으로 환불된다.

환불은 누구나 트리거할 수 있으며, CoW Swap UI를 통해 주문한 경우 자동으로 처리된다.

그렇지 않은 경우 info@cow.fi로 문의하라.

Note

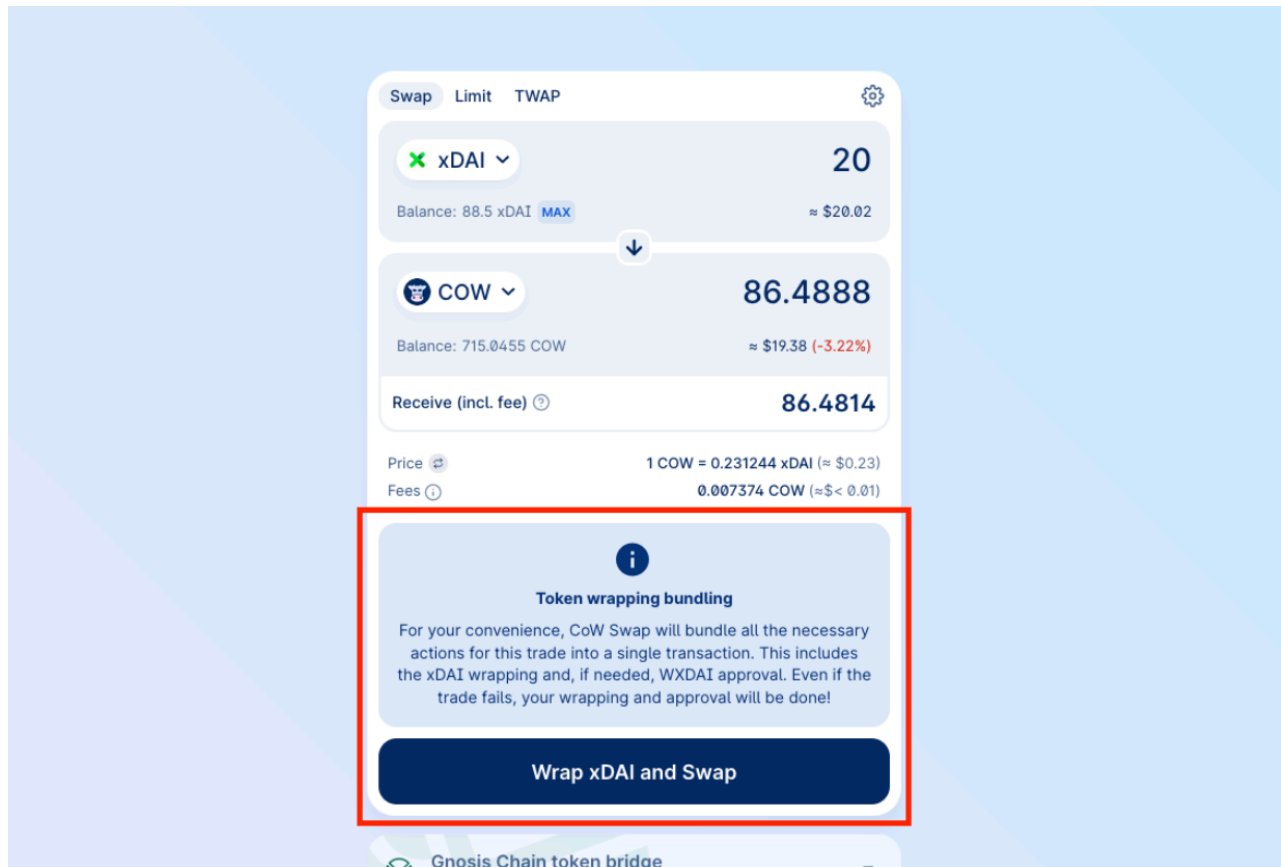
Eth-flow 옵션은 스왑(Swaps)에서만 사용할 수 있다.

Note

Eth-flow 옵션은 CoW Swap의 스마트 컨트랙트 지갑에서는 사용할 수 없다.

Tip

CoW Swap UI는 Eth-flow 컨트랙트를 직접 지원하지 않지만, CoW Swap Safe 앱을 사용할 때 래핑, 승인 (approval)(필요 시), 주문 생성을 단일 트랜잭션으로 묶을 수 있다.



Confirm transaction

Gnosis Chain

CoW Swap

Nonce # 258

Interact with: gno:0x

Approve access to

This allows contracts to spend the selected amounts of your asset balance.

Token

WXDAI

Unlimited (not recommended)

✓

Spender

gno:0xC92E8bdf79f0507f65a392b0ab4667716BFE0110

All actions

Expand all | Collapse all

<> 1 deposit

<> 2 approve

<> 3 setPreSignature

Transaction details

multiSend

Transaction status

Create

Confirmed (0 of 1)

Execute

Eth-flow 주문 취소 (Cancel eth-flow order)

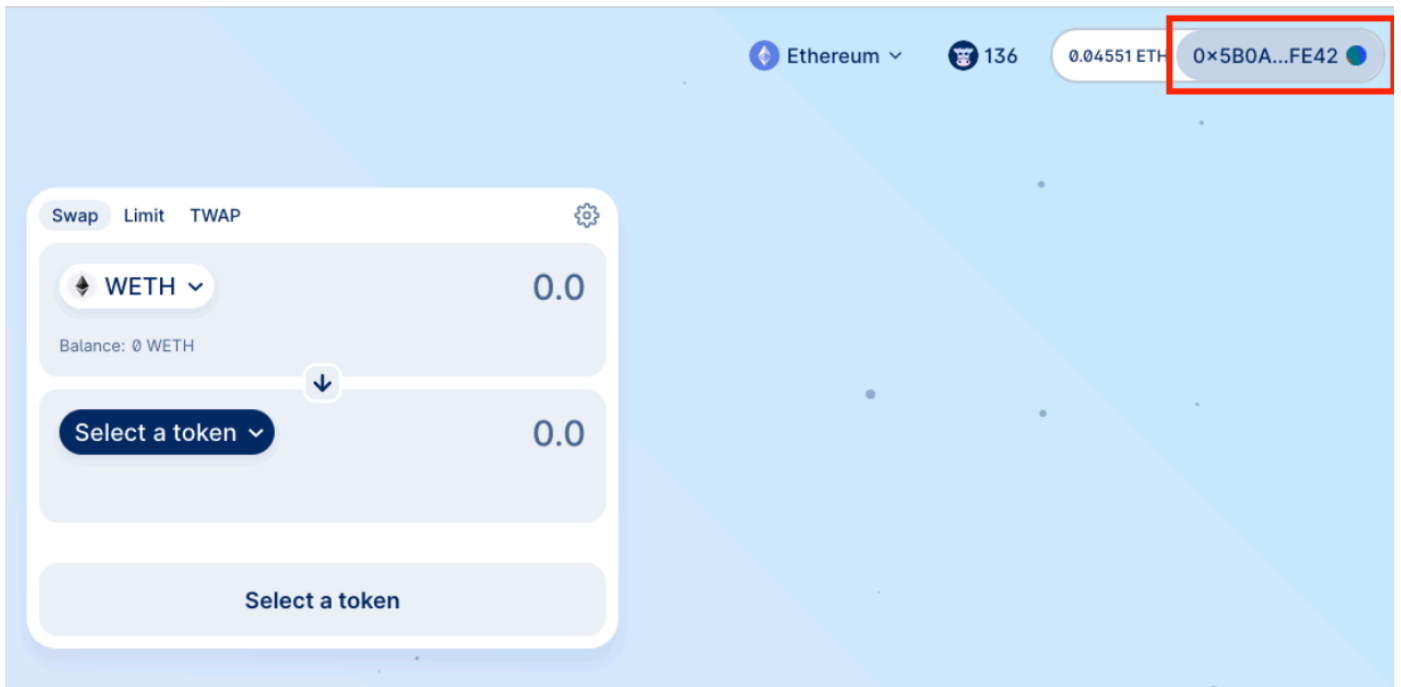
일반 스왑 주문과 마찬가지로, Eth-flow 주문도 취소할 수 있다.

Note

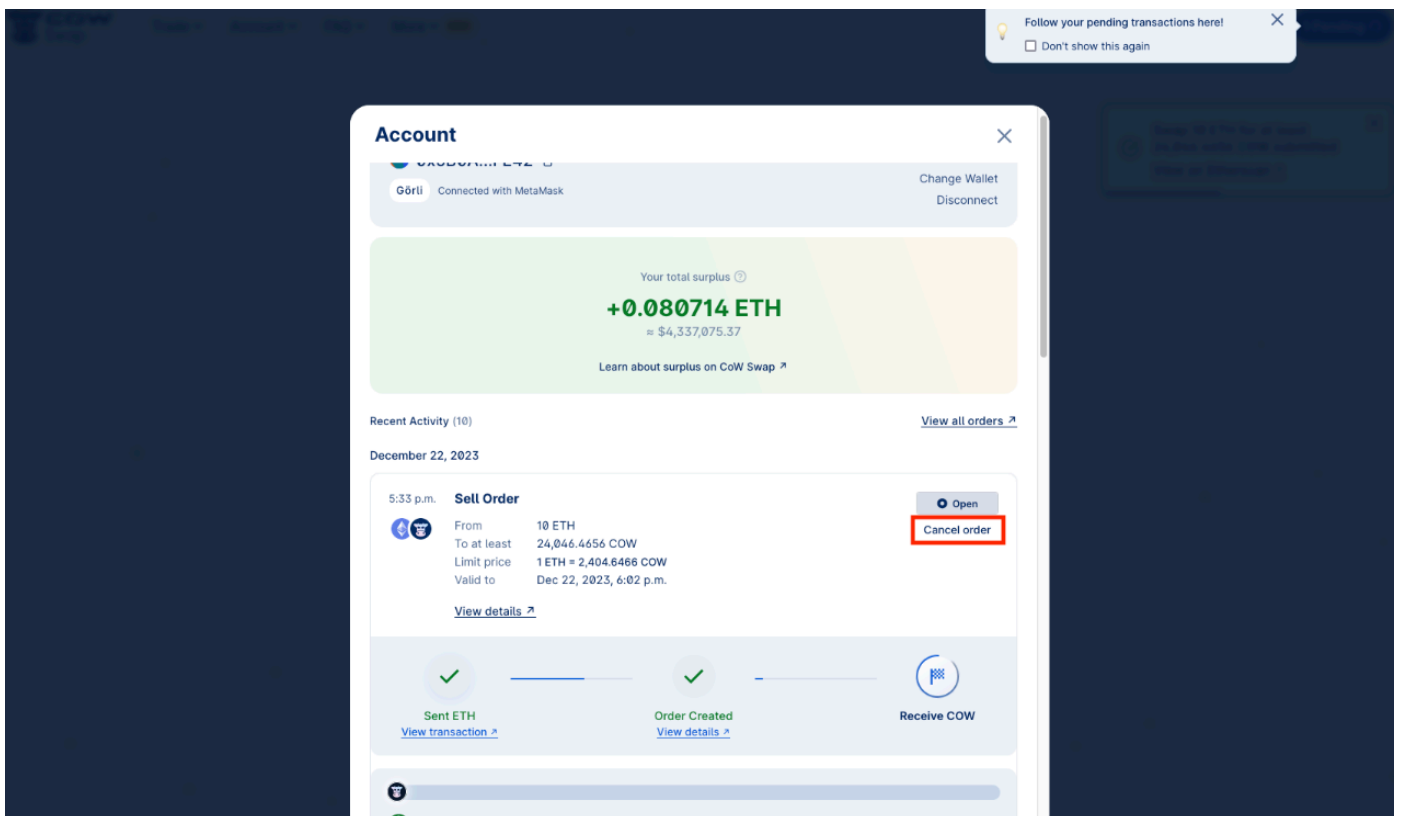
단, 온체인(on-chain) 취소만 가능하다.

먼저 오른쪽 상단의 주소를 클릭하여 활동 패널을 연다.

No. 64 / 110



그런 다음, 보류 중인 주문에서 Cancel order를 클릭한다.



취소를 확인한 후 지갑에서 트랜잭션에 서명한다. 이제 완료되었다!

Note

슬버의 반응 속도가 빠를 수 있으므로, 주문이 무효화되기 전에 이미 체결될 수도 있다.

원래의 ETH 금액은 취소 트랜잭션의 일부로 환불된다.

CoW 익스플로러 (CoW Explorer)

주문 조회 (Viewing orders)

CoW Protocol은 오프체인 오더북을 사용하고 온체인에서 정산되므로, CoW Protocol의 전체 상태를 파악하려면 온체인 및 오프체인 데이터를 결합해야 한다.

개별적으로는 다음에서 정보를 확인할 수 있다:

- [Order book API](#) (오프체인)
- CoW Protocol Subgraph (온체인)

이러한 도구 간 전환과 원시 JSON 데이터 분석은 사람보다는 컴퓨터에 더 적합하다.

이를 쉽게 시각화하기 위해 온체인 및 오프체인 데이터를 결합한 도구를 제작했다 — 바로 CoW Explorer이다 🐼🔍.

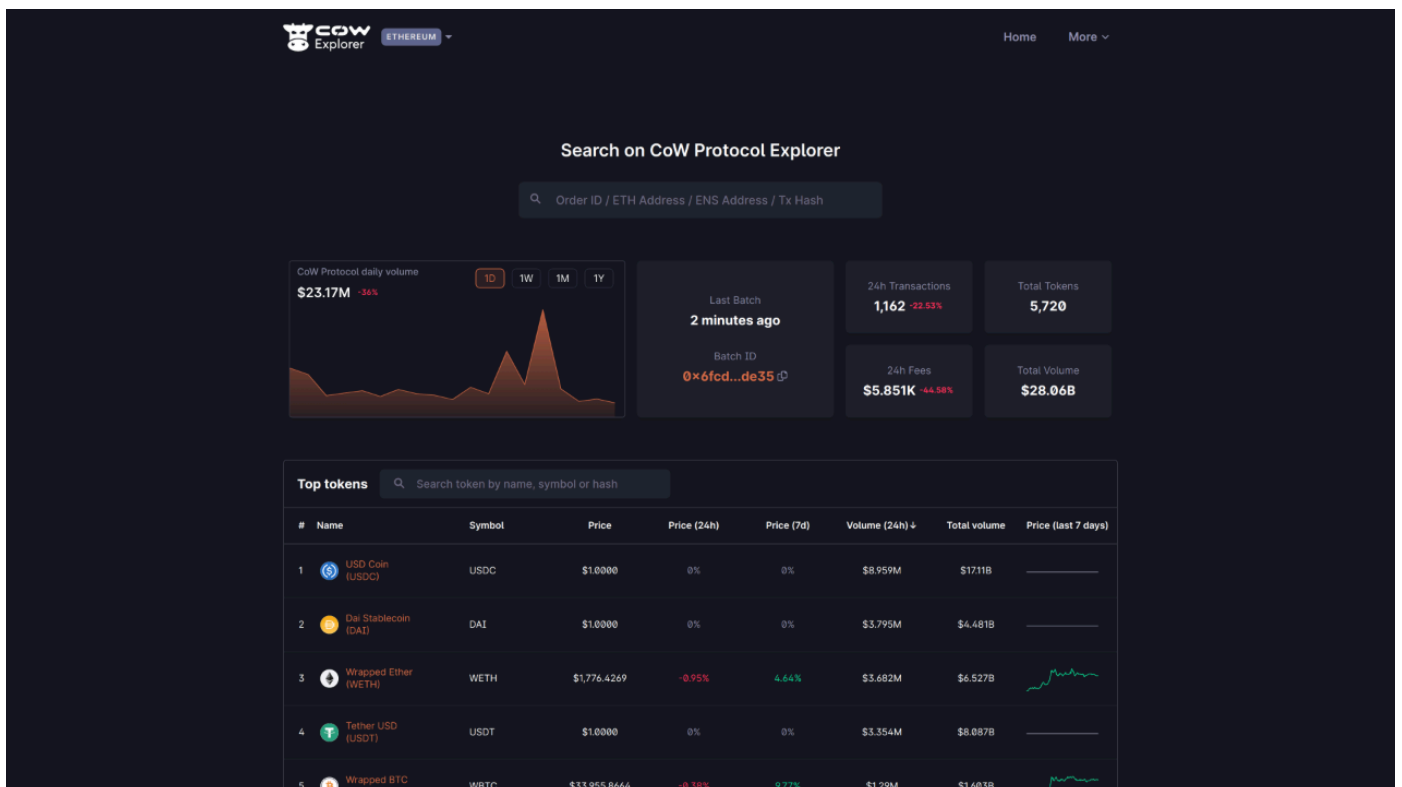
CoW Explorer

[CoW Explorer](#)는 CoW Protocol을 위한 “Etherscan”-유형 인터페이스다.

사용자는 프로토콜에 제출된 자신의 주문뿐만 아니라, 프로토콜이 배포된 모든 네트워크에서 실행된 주문을 시각화할 수 있다.

사용자는 다음 항목으로 검색할 수 있다:

- [orderID](#)를 통한 주문 상세 정보
- 특정 사용자의 [주소\(address\)](#)로 제출된 주문
- 특정 배치 경매의 [트랜잭션 해시\(transactionHash\)](#)로 정산된 주문



주문별 조회 (By order)

사용자는 자신이 제출한 특정 주문의 세부 정보를 보고자 할 수 있다. 이 경우 고유 식별자인 `orderId`로 주문을 검색할 수 있다.
이 식별자는 주문이 제출될 때 반환되며, 이를 통해 주문 세부 정보를 조회할 수 있다.

Note

간결성을 위해, `orderId`는 익스플로러에서 “Order ID”로 표시되며, `orderId`의 앞 8자만 축약되어 표시된다.

전량 체결 (Fill-or-kill)

아래는 5a1c1a59라는 Order ID의 간단한 예시로, 이미 전량 체결된 주문이다:

cow Explorer

ETHEREUM

Home More

Order details 56ac15a9

Overview

Order Id:

56ac15a9

From:

0x04084e1d86cfad5f5ea5e9ab833276481bf9e5e4

To:

0x04084e1d86cfad5f5ea5e9ab833276481bf9e5e4

Transaction Hash:

0x35f5ec4a9d84e27bdeb844f3e7cb72d9de62edf95855181bf57d69308fac

View batch graph

Status:

Filled

Submission Time:

15 September 2022 - 7:10 AM

Expiration Time:

15 September 2022 - 7:40 AM

Type:

Sell market order (Fill or Kill)

Amount:

From

50,526.4175

USD Coin (USDC)

To at least

31.0864

ETH

Limit Price:

1,624.6131USDC for ETH

Execution Price:

1,615.2007USDC for ETH

Filled:

100%

50,526.4175 USDC sold for a total of 31.2676 ETH

Order Surplus:

0.58% 0.18115189 ETH

Fees:

22.9317 USDC

AppData:

0xfda28b94d496c30e7bf8d159f8e2c439692657a362e79d263e7b37570fb59361

Show more

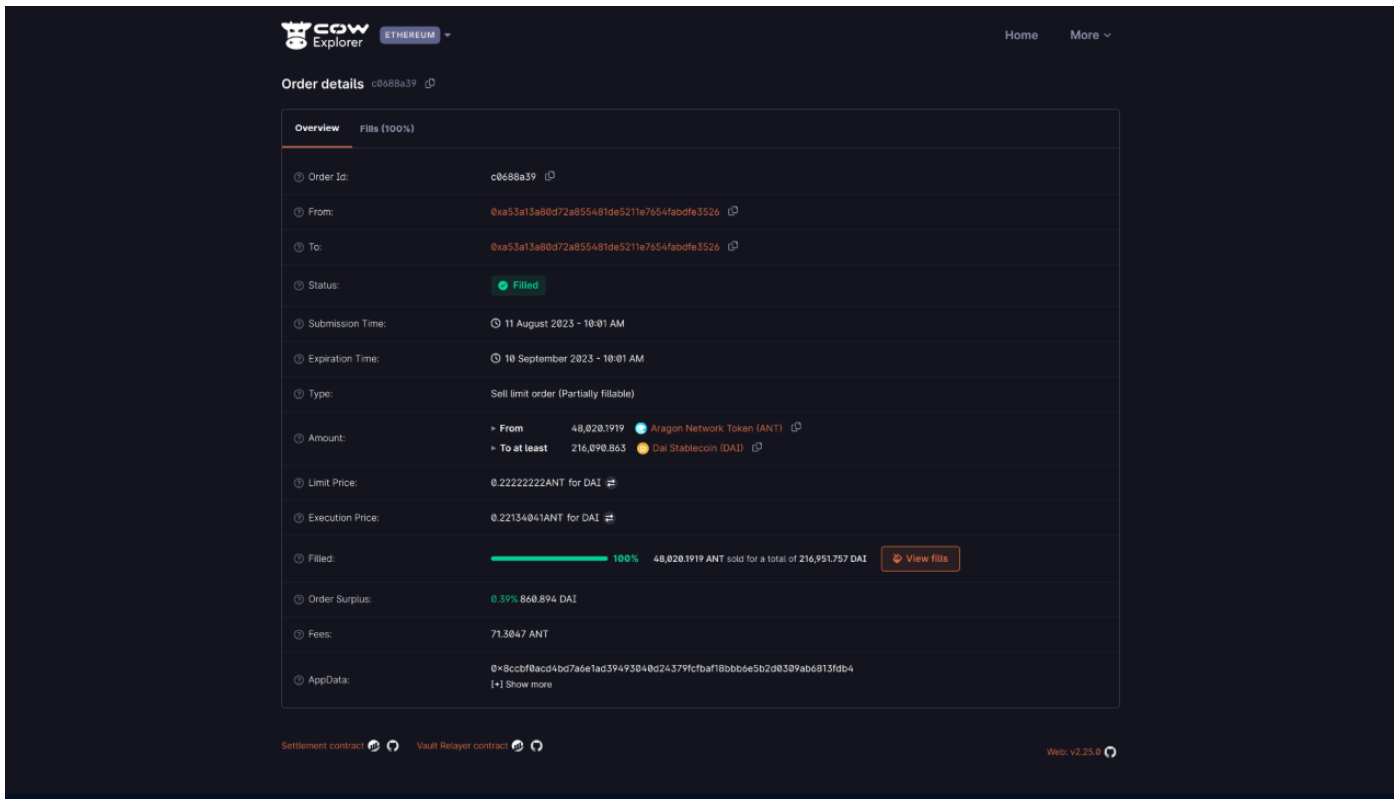
Settlement contract

Vault Relayer contract

Web: v2.25.0

부분 체결 가능 (Partially fillable)

좀 더 복잡한 예로, 사용자가 부분 체결 가능(partially fillable) 주문을 제출한 경우가 있다. 이는 사용자가 일정 수량의 토큰을 스왑하려는 의도를 표현했지만, 주문이 여러 배치(batch)에 걸쳐 체결될 수 있음을 의미한다. 이 방식은 지정가 주문(Limit orders)에서만 사용할 수 있다.



“View fills” 버튼을 클릭하면, 해당 주문에서 실제로 실행된 체결 내역을 확인할 수 있다.
아래는 위 예시의 체결 내역이다:

Order details c0688a39						
Overview Fills (100%) Rows per page: 10 Page 1 of 4						
FILLED 100% 48,020.1919 ANT sold for a total of 216,951.757 DAI		AVG. EXECUTION PRICE 0.22134041ANT for DAI		TOTAL SURPLUS 0.39% 860.894 DAI	LIMIT PRICE 0.22222222ANT for DAI	
Tx hash	Sell amount	Buy amount	Surplus	Execution price	Execution time	
0x4ed9...14a0	1,054.8632 ANT	4,756.5977 DAI	0.2% 9.7131 DAI	0.22176844 ANT	13 August 2023 - 2:14 PM	
0xb21e...23e7	1,006.012 ANT	4,533.5951 DAI	0.14% 6.5407 DAI	0.22190162 ANT	13 August 2023 - 2:18 PM	
0xf80a...dbcd	750.3154 ANT	3,379.6131 DAI	0.09% 3.1934 DAI	0.22201224 ANT	13 August 2023 - 2:18 PM	
0x2cd0...76dd	1,163.724 ANT	5,249.3411 DAI	0.24% 12.583 DAI	0.22168954 ANT	13 August 2023 - 2:19 PM	
0xbe78...b453	1,486.0253 ANT	6,713.2409 DAI	0.39% 26.1269 DAI	0.22135737 ANT	13 August 2023 - 2:21 PM	
0xb99a...ebbd	1,592.3503 ANT	7,196.3471 DAI	0.42% 30.7707 DAI	0.22127202 ANT	13 August 2023 - 2:22 PM	
0x3a69...cd4f	1,384.0314 ANT	6,249.2694 DAI	0.33% 21.128 DAI	0.22147091 ANT	13 August 2023 - 2:22 PM	
0x050e...c0f2	1,348.5175 ANT	6,087.8862 DAI	0.32% 19.5572 DAI	0.22150834 ANT	13 August 2023 - 2:23 PM	
0xd1a2...a18e	1,380.996 ANT	6,235.7737 DAI	0.34% 21.2915 DAI	0.22146346 ANT	13 August 2023 - 2:24 PM	

여기서 주문이 100% 체결되었음을 볼 수 있지만, 수십 개의 배치에 걸쳐 나뉘어 체결되었다.
분석을 용이하게 하기 위해 요약 정보가 함께 제공되며, 다음과 같은 내용을 포함한다:

- 총 체결 비율 (이 경우 100%)

- 평균 실행 가격 (이 경우 0.22134041 ANT / DAI)
- 총 잉여(surplus) (이 경우 0.39% / 860.894 DAI)
- 모든 체결에 적용된 지정가 (이 경우 0.22222222 ANT / DAI)

주문 상태 (States)

CoW Explorer는 사용자가 서명한 주문을 시각적으로 확인할 수 있도록 설계되었으며, 핵심적으로 표시해야 하는 매개 변수 중 하나가 주문 상태(state) 이다.

이 매개변수는 다음과 같은 상태를 가진다:

- Open (pending): 활성 주문 상태. 솔버가 주문을 검토 중인 단계다.
모든 주문의 초기 상태¹이며, 주문이 제출된 시점부터 기본 상태로 존재한다.
여기서 주문은 다른 모든 상태로 전환될 수 있다.
- Filled: 실행 및 정산된 주문 상태. 이 상태의 주문은 실행이 완료되었으며, 해당 자금이 목표 계정으로 전송되었다.
이 상태의 주문에는 이더리움 정산 트랜잭션으로 연결되는 링크가 제공된다.
정산 트랜잭션에는 해당 주문의 실행과 동일 배치 내의 다른 주문들이 포함된다.
- Expired: 만료된 주문 상태. 주문이 설정된 만료 시간 동안 실행되지 않았을 때 발생한다.
- Cancelled: 취소된 주문 상태. 사용자의 요청에 따라 주문이 취소되었음을 의미한다.
- Partially-filled: 부분 체결된 주문 상태. 주문의 일부가 실행되어, 해당 자금이 대상 계정으로 전송된 경우다.
- Pre-signing: 사전 서명이 필요한 주문 상태. 주로 Safe 지갑과 같은 스마트 컨트랙트 지갑에서 제출된 주문에 사용된다.

각주 (Footnotes)

1. 사전 서명된(pre-signed) 주문의 경우, 첫 번째 상태는 Pre-signing이다.

사용자 주소별 조회 (By user address)

사용자는 자신이 제출한 모든 주문의 세부 정보를 보고자 할 수 있다. 주소로 검색하면, 해당 사용자가 제출한 모든 주문의 개요를 확인할 수 있다.

예를 들어, 아래는 Gnosis Chain에서 CoW Protocol을 통해 여러 주문을 제출한 주소 0x2557...3af7을 검색한 예시다:

ONOSIS CHAIN

Home

More

User details

0x2557...3A17

Orders

Rows per page: 20 1 - 5

Order ID	Type	Sell amount	Buy amount	Limit price	Surplus	Created	Status
df36042b	Sell	2 WXDAI	1.95 USDC	1.0256 WXDAI per USDC	2.36%	17 November 2023 - 7:04 AM	Filled
9b715339	Sell	2 WXDAI	1.95T USDC	< 0.00000001 WXDAI per USDC	-	17 November 2023 - 6:55 AM	Expired
9197e8d0	Sell	1.9441 sDAI	1.95 xDai	0.99698836 sDAI per xDai	1.59%	16 November 2023 - 9:27 AM	Filled
1099b52c	Sell	195.48s sDAI	< 0.00000001 xDai	195,486,097.682T sDAI per xDai	162.465 xDai	13 November 2023 - 7:05 PM	Filled
c2c2107f	Sell	6.6666 WXDAI	6.4473 sDAI	1.034 WXDAI per sDAI	-	12 November 2023 - 4:45 PM	Cancelled

Settlement contract

Vault Relayer contract

Web: v2.25.0

기본적으로 익스플로러는 사용자가 제출한 모든 주문을 상태와 관계없이 최신 순으로 표시한다.

배치 경매별 조회 (By batch auction)

배치 경매(batch auction)는 온체인에서 단일 트랜잭션으로 정산되며, 이 트랜잭션 해시를 통해 배치 경매의 세부 정보를 조회할 수 있다. 트랜잭션 해시를 검색하면 해당 배치 경매의 개요가 표시된다.

배치 경매 상세 페이지에서는 다음 정보를 제공한다:

- 배치 경매에서 정산된 모든 주문 목록
- 배치 경매 내 라우팅을 시각화한 그래프

아래 예시 배치 경매 0x35f6...0fa6을 살펴보자.

주문 (Orders)

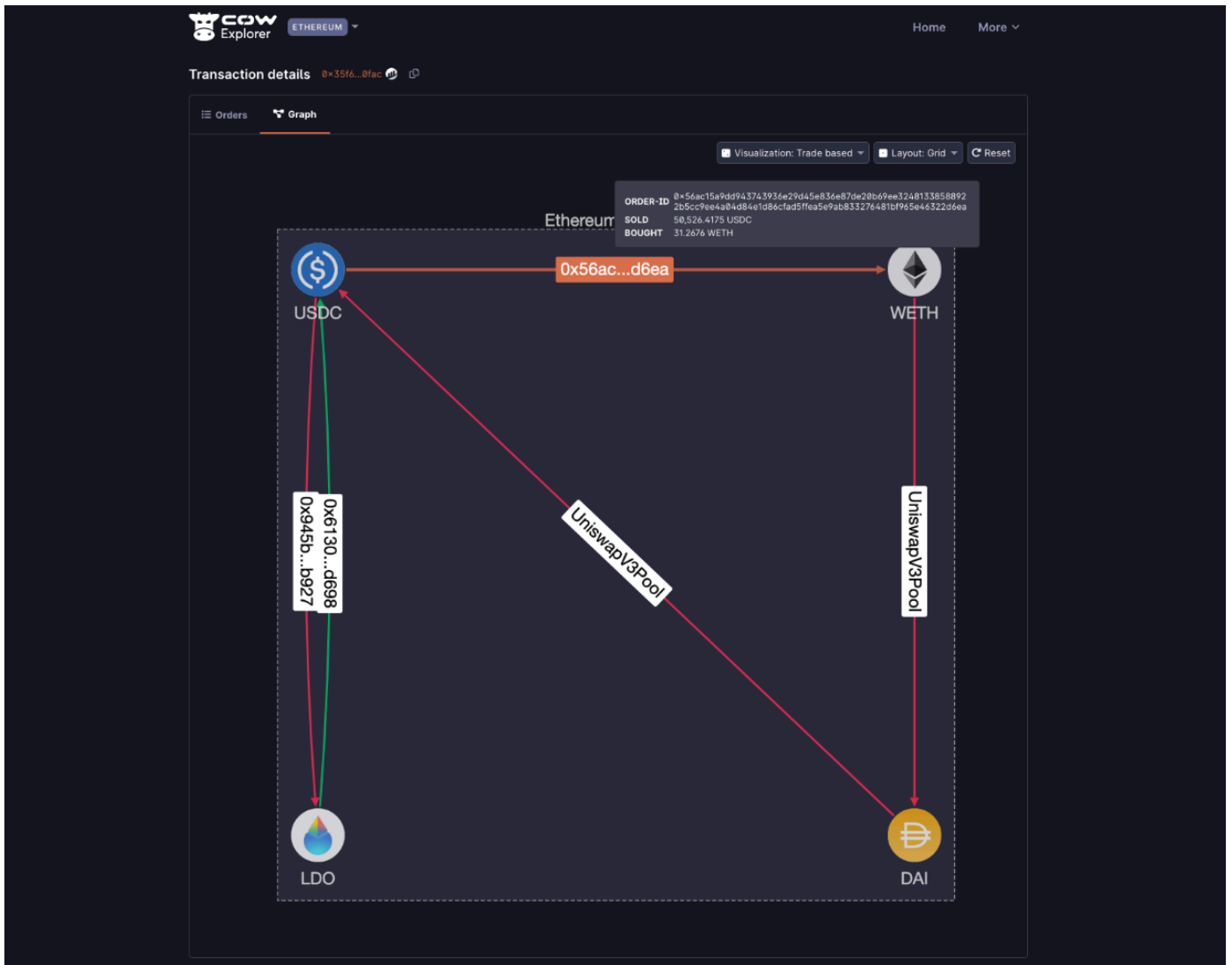
“Orders” 탭에서는 배치 경매에서 정산된 모든 주문을 확인할 수 있다. 각 주문 ID를 클릭하면 해당 주문의 세부 정보 페이지로 이동한다.



거래 기반 (Trade based)

이 그래프는 거래된 토큰을 노드로 표시하고, 노드 간의 연결선을 자금 흐름으로 나타낸다.

녹색 화살표는 프로토콜 내 거래를, 빨간 화살표는 거래가 이루어진 풀/AMM/유동성 소스를 통해 흐른 토큰을 의미한다.



MEV 블로커 (MEV Blocker)

개요 (Overview)

MEV Blocker는 트랜잭션 처리량과 리베이트 기준으로 업계 1위의 MEV 보호 RPC 솔루션이다.



MEV Blocker의 주요 목적

- 프런트리닝 및 샌드위치 공격(MEV 공격)으로부터 사용자를 보호
- 트랜잭션 플로우에서 발생하는 백러닝(backrunning) 기회로부터 사용자/통합자에게 리베이트 제공
- 가장 빠른 트랜잭션 포함 시간 제공

주요 장점 (Key Advantages)

다른 RPC와 비교했을 때 MEV Blocker가 제공하는 핵심 장점은 다음과 같다:

- 포함 시간(Inclusion time) → 혁신적인 Builder 수수료 메커니즘 덕분에 시장에서 가장 빠른 RPC
- 백런 리베이트(Backrun Rebates) → 견고한 OFA(Order Flow Auction) 및 탈중앙화된 서치 네트워크 덕분에 RPC 중 가장 높은 리베이트 제공
- 투명성(Transparent) → 모든 데이터가 30초 지연 내에 공개됨
- 맞춤화(Customizable) → 사용자/통합자는 필요에 따라 5개의 서로 다른 RPC 엔드포인트 중 선택 가능
- 퍼미션리스(Permissionless) → 모든 엔드포인트와 기능이 완전히 무허가형으로, 접근 제한이 없음.
MEV Blocker는 전문가에 의해 설계되어 사용자 친화적이며, 설정이 간단하고 무료로 통합 가능함.

MEV Blocker의 경쟁 우위

RPC 벤치마크 비교 연구를 통해 MEV Blocker의 속도, 백런, 성공률을 확인할 수 있다.

MEV Blocker RPC isn't like any other...



	Inclusion Delay	Price Improvement (vs. MEV Blocker)	Average Rebate	Success Rate
MEV Blocker	1.34 blocks —	— (baseline)	0.0035 ETH —	85% —
Flashbots Protect	1.49 blocks <i>1.68 seconds slower</i>	21 bps less	0.0016 ETH <i>54% less</i>	84% <i>1.2% worse</i>
Merkle	1.86 blocks <i>6.1 seconds slower</i>	9 bps less	0.0009 ETH <i>75% less</i>	70% <i>21.4% worse</i>
Blink	1.56 blocks <i>2.8 seconds slower</i>	9 bps less	0.0011 ETH <i>69% less</i>	84% <i>1% worse</i>

비교 연구 보기

지원 체인

이더리움: 모든 기능이 이더리움에서 지원된다.

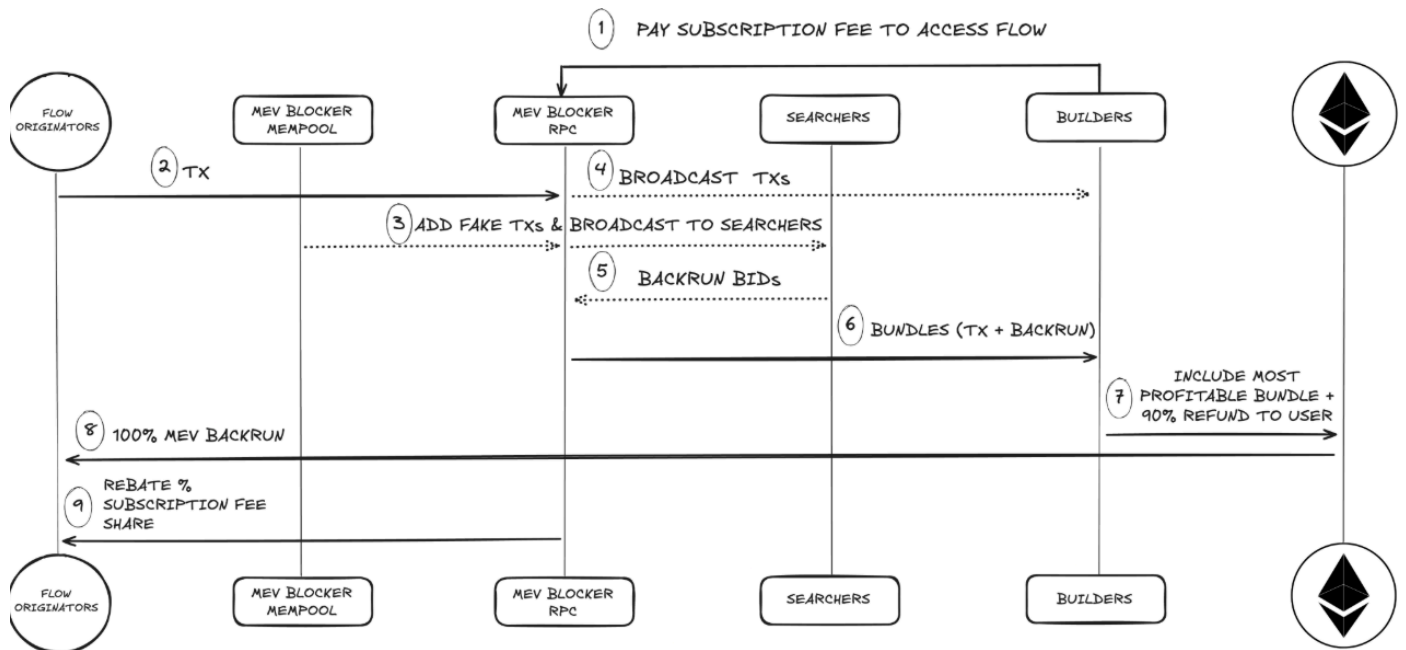
개념 (Concepts)

MEV Blocker의 주문 흐름 경매(order flow auction)는 트랜잭션을 신뢰할 수 있는 서처들의 프라이빗 멤풀로 전달함으로써 프런트리닝과 샌드위치 공격 같은 가장 심각한 형태의 MEV로부터 사용자를 보호한다. 이 서처들은 사용자 트랜잭션 이후 발생하는 백런(backrun) 기회를 포착하고, 그 가치의 최대 90%를 사용자에게 반환한다.

- MEV 보호: 퍼블릭 멤풀의 트랜잭션은 프런트리닝 및 샌드위치 공격에 취약하며, 이는 매주 수백만 달러의 손실을 초래한다.
MEV Blocker의 프라이빗 풀은 이러한 공격으로부터 사용자를 보호한다.
- MEV 리베이트: MEV Blocker는 서처들이 트랜잭션 백런에 입찰하도록 하여, 90%를 사용자에게 리베이트로 반환하고
10%는 빌더와 검증자에게 보상함으로써, MEV 가치를 회수하고 지갑 및 dApp 수익을 창출할 수 있게 한다.
- 더 빠른 트랜잭션 포함: MEV Blocker는 퍼블릭 멤풀을 우회하여 트랜잭션을 주요 빌더에게 직접 전달하여 포함 속도를 높인다.

작동 방식 (How it works)

MEV Blocker의 트랜잭션 플로우의 6단계로 구성된다. 아래 이미지는 트랜잭션 처리의 전체 흐름을 나타낸다.



1. 빌더가 구독료를 지불하고 MEV Blocker에 연결

빌더들은 MEV Blocker 접근을 위해 블록당 수익의 일정 비율로 계산된 주간 구독료를 지불한다. 이 수수료는 월 단위로 계산되고, 공개 데이터(Dune 쿼리 등)를 기반으로 주 단위로 온체인에 게시된다.

2. 오더 플로우 발신자가 MEV Blocker RPC 엔드포인트에 연결

오더 플로우 발신자는 API 키나 제3자 권한 없이 공개 엔드포인트를 통해 트랜잭션을 제출할 수 있다.

3. MEV Blocker 프라이빗 멤풀 작동 - 서처로부터 트랜잭션 보호

MEV Blocker RPC는 트랜잭션(서명 제외)을 허가된 또는 무허가형 서처 집합에 공유한다(엔드포인트에 따라 다름). 또한 실제 트랜잭션과 AI가 생성한 가짜 트랜잭션을 섞어 보안을 강화한다.

트랜잭션 유형에 따라 추가 세부 정보가 숨겨질 수 있다:

- 스왑의 경우, 슬리피지 허용치 등 민감한 정보를 제거하여 샌드위치 공격을 방지한다.
- 백런 가능성이 낮은 트랜잭션은 아예 서처에게 공유되지 않는다.

무허가형 환경에서는 서처가 데이터를 악용할 수 없도록 차단할 수 없으므로, 가짜 트랜잭션이 불확실성을 추가한다. 서처는 진짜와 가짜 트랜잭션을 구별할 수 없기 때문에, 존재하지 않는 트랜잭션에 반응할 위험을 감수해야 하며, 이로 인해 프런트러닝 시도가 비효율적이 되어 억제 효과가 생긴다.

3.1 트랜잭션이 MEV Blocker 연결된 서처 및 빌더로 전달됨

트랜잭션은 백런 실행을 위해 서처에게 공유되고, 빠른 포함을 위해 빌더에게 직접 전송된다.

4. 서처가 백런 입찰을 제출

서처들은 주문을 받은 후, 데이터를 분석하고 입찰을 제출한다. 가장 높은 사용자 리베이트 가치를 제공하는 서처(검증자에게 가장 높은 수수료를 내는 서처가 아님)가 선정된다.

5. 서처 번들이 빌더에게 전달되어 다음 블록에 포함

MEV Blocker 시스템은 서처 번들을 수집한 뒤, 가짜 트랜잭션이 포함된 번들을 제거하고 유효한 트랜잭션에는 다시 서명을 추가한다.

빌더에게 번들을 전달하기 위해 서처들은 임의의 ETH 금액으로 입찰한다. 서처는 번들의 백런 가치가 자신의 입찰가보다 큰 경우에만 입찰하도록 설계되어 있다.

빌더가 승리 번들을 선택하면, 입찰 가치의 90%는 사용자에게 환급되고, 나머지 10%는 검증자/프로포저에게 지급된다.

6. MEV Blocker 트랜잭션 조립 (Tx Assembly)

MEV Blocker는 가짜 트랜잭션이 포함된 번들을 폐기하고, 실제 트랜잭션만 전달한다. 트랜잭션 서명을 다시 추가하여 서처가 시스템을 우회하지 못하도록 방지하며, MEV 리베이트가 사용자에게 전달되도록 보장한다. 빌더는 사용자에게 가장 높은 리베이트를 제공하는 번들을 선택하여 온체인에 포함시킨다.

7. 빌더가 트랜잭션 및 번들을 수신

빌더는 MEV Blocker로부터 개별 트랜잭션과 번들을 수신한다. OFA 규칙에 따라, 블록 생성 중 더 높은 리베이트를 제공하는 번들이 있으면 이를 교체해야 한다. 빌더는 트랜잭션 실행 시 백런 가치의 90%를 사용자에게 환급한다.

만약 더 높은 입찰 번들이 블록 시뮬레이션에서 실패할 경우, 낮은 입찰 번들이 포함될 수 있다. 이를 통해 사용자는 지연 없이 가능한 최고 리베이트를 받을 수 있다.

8. 온체인 트랜잭션 포함 (Transaction Inclusion Onchain)

빌더는 사용자 트랜잭션, 백런, MEV 환급을 실행하며, 환급액은 자동으로 tx.origin 또는 지정된 주소로 전송된다. 이를 통해 사용자와 오더 플로우 제공자가 100%의 환급을 수령하며, MEV Blocker는 어떠한 수수료도 취하지 않는다.

9. 최종 단계: 오더 플로우 제공자 가스 리베이트 (Final: Gas Rebates for Orderflow Originators)

MEV Blocker는 빌더 구독료의 90%를 오더 플로우 제공자에게 재분배하여 가스 리베이트를 제공한다.

가스 리베이트 (Gas Rebates)

이더리움 가스 요금 소개 (Introduction to Ethereum Gas Fees)

모든 이더리움 트랜잭션은 온체인에 포함되기 위해 가스비가 필요하다. 가스비는 다음 두 가지로 구분된다:

- 기본 수수료(Base Fee): 네트워크 수요에 따라 자동 조정되는 필수 네트워크 요금이다. 이 수수료를 지불한 트랜잭션은 블록에 포함된다.
- 우선 수수료(Priority Fee): 자신의 트랜잭션을 다른 트랜잭션보다 빨리 포함시키기 위해 빌더에게 지불하는 선택적 팁이다. 이를 통해 빌더가 더 가치 있는 블록을 만들 수 있으며, 트랜잭션의 빠른 포함 확률을 높인다.

MEV Blocker가 우선 수수료를 회수하는 방법 (How MEV Blocker Recovers Priority Fees)

MEV Blocker는 검색자(searcher)와 빌더 모두가 공개 규칙에 따라 작동하는 퍼미션리스 Order Flow Auction을 운영하는 유일한 RPC이다. 현재 MEV Blocker는 이더리움 전체 일일 트랜잭션의 약 10%를 처리하며:

- 이더리움 메인넷 트랜잭션의 20% 이상을 보호 및 라우팅
- 트랜잭션을 블록에 포함시키는 주요 빌더들과 긴밀한 협력 관계 유지

MEV Blocker는 광범위한 네트워크와 트랜잭션 경로에 대한 직접 통합을 통해 일반적으로 손실되는 우선 수수료 (Priority Fee)의 일부를 회수할 수 있다 — 지연이나 속도 저하 없이.

이더리움이 Proposer-Builder Separation (PBS) 모델로 발전함에 따라, 검증자(프로포저)와 빌더의 역할이 분리되고 있다. 이로 인해 수수료 시장이 더욱 투명하고 효율적으로 발전하고 있지만, 사용자는 여전히 빠른 포함을 위해 과도한 수수료를 지불하는 경우가 많다.

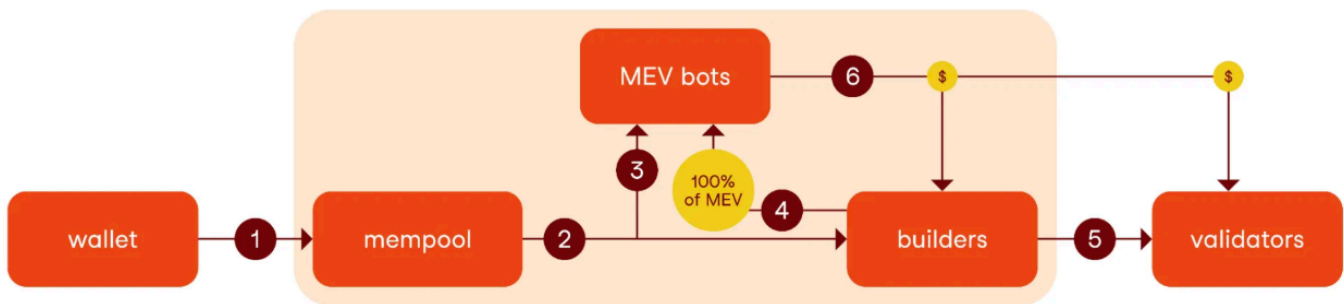
MEV Blocker는 이러한 간극을 메우며, 사용자가 실제로 필요한 금액과 지불한 금액의 차이를 회수하도록 돕는다. 즉, 현재 가스비 시스템의 비효율성에서 발생하는 잉여분을 환급 형태로 되돌려주는 역할을 한다.

MEV

MEV는 어떤 체인에서든 논쟁적인 주제다. MEV Blocker의 목표는 사용자에게 피해를 주거나 사용자의 이익에 반하는 모든 MEV를 줄이고, 사용자의 이익이 될 수 있는 MEV를 극대화하는 데 있다.

MEV Blocker 없이 (Without MEV Blocker)

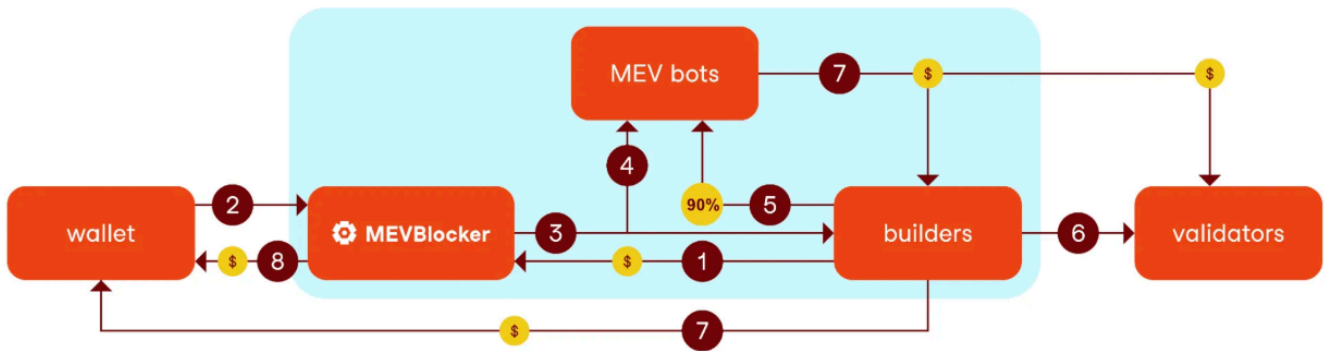
이더리움의 기본 메몰은 무법지대와 같아서 MEV 봇(일명 서처)이 눈치채지 못한 트레이더(일명 사용자)의 트랜잭션을 악용해, 시간이 지남에 따라 조금씩 이익을 빼앗을 수 있다.



1. 지갑이 사용자가 시작한 트랜잭션을 퍼블릭 메몰에 제출한다.
2. 누구나 메몰 트랜잭션을 볼 수 있다. 빌더는 수수료와 가치에 따라 트랜잭션을 선택한다.
3. MEV 봇이 메몰 트랜잭션을 노려 슬리피지 착취를 타겟으로 이익을 취한다.
4. MEV 봇이 번들을 만들어 순서를 강제하기 위한 뇌물과 함께 빌더에게 제출한다.
5. 빌더는 검증자에게 가장 수익성 높은 블록을 만들기 위해 가장 가치 있는 번들을 조합한다.
6. 검증자는 수익을 극대화하기 위해 빌더가 제시한 가장 가치 있는 블록을 선택한다. 선택되면 모든 트랜잭션(사용자, MEV, 뇌물)이 온체인에서 실행된다.

MEV Blocker 사용 시 (With MEV Blocker)

정형화된 메몰은 서처가 다음 블록에 트레이더를 프런트러닝하거나 샌드위치하지 않고 포함되도록 번들을 만들도록 인센티브를 제공한다 — 백런 기회의 일부를 서처에게 배분함으로써.



1. 지갑이 사용자가 시작한 트랜잭션을 MEV Blocker의 가상 메모리에 제출한다.
2. 빌더는 MEV Blocker의 트랜잭션 플로우에 접근하기 위해 구독료를 지불해야 한다.
3. 연결된 빌더는 MEV Blocker 플로우에 접근하여 수수료와 가치에 따라 트랜잭션을 선택할 수 있다.
4. MEV Blocker는 서처에게 백런 번들을 통해 트랜잭션을 공유하고, 90%를 사용자에게 반환한다.
5. MEV 봇은 번들을 만들고 순서를 강제하기 위한 뇌물과 함께 빌더에게 제출한다.
6. 빌더는 검증자에게 가장 수익성 높은 블록을 만들기 위해 가장 가치 있는 번들을 조합한다.
7. 검증자는 수익을 극대화하기 위해 빌더가 제시한 가장 가치 있는 블록을 선택한다. 선택되면 모든 트랜잭션(사용자, MEV, 뇌물)이 온체인에서 실행된다.
8. MEV Blocker는 빌더의 구독료 중 50%를 지갑 플로우 발신자와 공유한다.

MEV 공격 (MEV Attacks)

프런트러닝이란? (What is Frontrunning?)

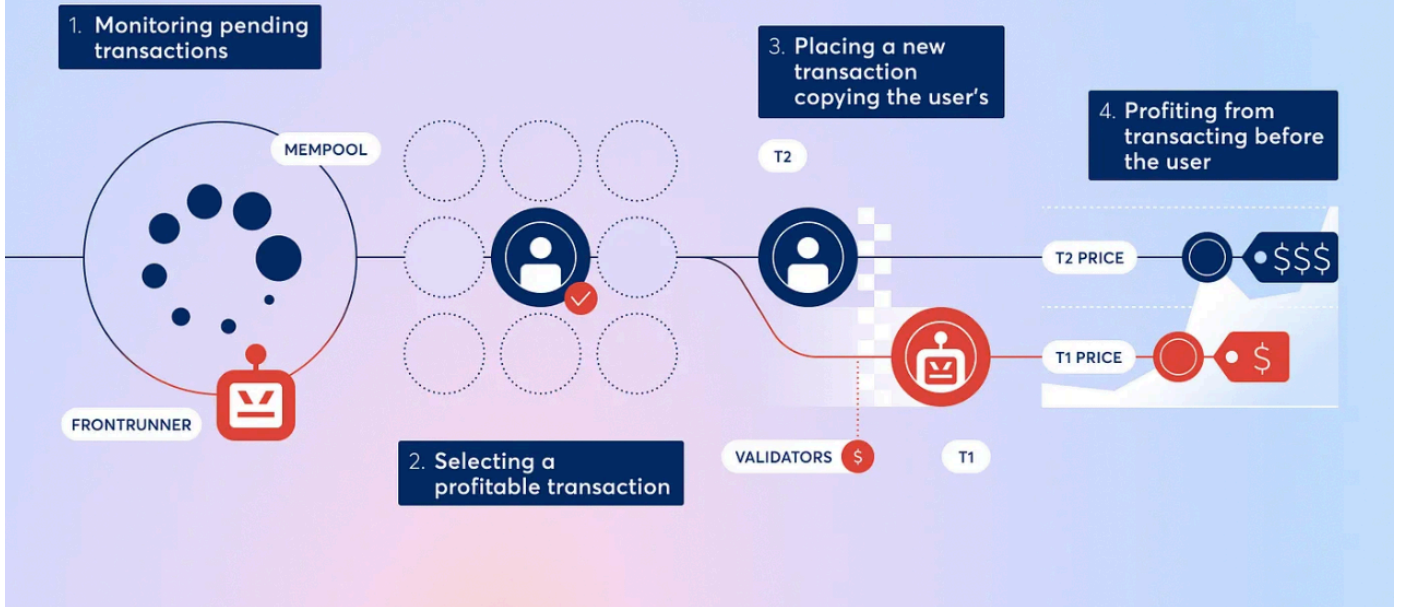
MEV, 즉 maximal extractable value는 이더리움 트랜잭션에 부과되는 보이지 않는 세금과 같아서, 지금까지 트레이더에게 수십억 달러에 달하는 가치 손실을 초래해 왔다.

프런트러닝은 거래, NFT 민팅 등 모든 형태의 이더리움 트랜잭션에 영향을 미치는 특정 유형의 MEV다. 이 글은 MEV 시리즈의 일부로, 다른 두 가지 일반적인 MEV 유형인 샌드위치 공격과 백러닝도 함께 다룬다.

프런트러닝은 무엇이며 어떻게 작동하나? (What is frontrunning and how does it work?)

프런트러닝은 사용자가 트랜잭션을 만들었지만, MEV 봇이 같은 트랜잭션을 앞서 실행해 “앞지르는” 상황에서 발생한다.

Frontrunning



프런트러닝 과정 (The Frontrunning Process)

프런트러닝은 누구나 트랜잭션을 볼 수 있는 블록체인 뱀풀의 개방성에 의존한다. MEV 봇은 이 투명성을 악용해 거래를 가로챈다. 과정은 다음과 같다:

- 1. 대기 트랜잭션 모니터링:**
첫 단계는 대기 트랜잭션이 모여 있는 뱀풀을 모니터링하는 것이다. 고도화된 봇은 차익거래나 조작 대상이 될 수 있는 고가치 트랜잭션을 식별한다.
- 2. 수익성 있는 트랜잭션 선별:**
잠재적 시장 영향이 확인되면, 프런트러너는 특정 트랜잭션이 가격에 미치는 효과를 분석한다.
예를 들어, 특정 토큰에 대한 대량 매수 주문이 감지되면, 프런트러너는 처리 후 해당 토큰 가격이 상승할 것을 안다.
- 3. 새 트랜잭션 제출:**
프런트러너는 같은 자산에 대해 자신의 거래를 즉시 발행하여, 목표 트랜잭션보다 먼저 처리되도록 한다.
일반적으로 검증자에게 더 높은 “팁”을 지불해 자신의 트랜잭션이 블록에 먼저 포함되도록 한다.

예시: 디파이에서의 프런트러닝 (Example: Frontrunning in DeFi)

디파이 프런트러닝의 대표적 사례로 악명 높은 MEV 봇 `jaredfromsubway.eth`가 있다. 어떤 사례에서 사용자 `0x3a7892`는 2 ETH를 \$B0B 토큰으로 교환하려 했다.

프런트러닝 공격이 수행된 방식 (How the frontrunning attack was executed)

이 거래는 뱀풀을 모니터링하던 `jaredfromsubway.eth`에 포착되었다.

트랜잭션이 뱀풀에 들어오자, 봇은 재빨리 ETH로 \$B0B를 매수하는 자체 트랜잭션을 먼저 실행했다. 사용자 주문에 앞서 매수함으로써 \$B0B의 가격을 끌어올렸고, 사용자의 주문이 실행될 때 사용자는 더 적은 수량의 토큰을 받게 되었으며, 봇은 곧바로 \$B0B를 되팔아 이익을 얻었다.

time	delay	mev	impact	action	txn hash	arrival time	from
07	miner	Frontrun		→ +1	0x4679d5745b86fc...	2023-06-18 18:41:12.888	0xae2fc483527b8e...
0	4 secs	Sandwich	\$-393.64	→	0xff31ba1a8a6193...	2023-06-18 18:41:08.072	0x3a78228c3296e7...
	12 secs	Swap		→	0x701157c3a3cede...	2023-06-18 18:41:00.122	0xba8d62918b2429...
108	miner	Backrun		→ +1	0x4f4d7108cdec8d...	2023-06-18 18:41:12.888	0xae2fc483527b8e...
109	miner	Frontrun		→	0x8801f8cf22383f...	2023-06-18 18:41:12.888	0x77ad3a15b78101...
95	4 secs	Sandwich		→	0xc82deec81cabfa...	2023-06-18 18:41:08.780	0x598cf959e4e6ce...
110	miner	Backrun		→	0x903b4f3f1afe14...	2023-06-18 18:41:12.888	0x77ad3a15b78101...
111	miner	Swap		→ +1	0xd56612d1e42780...	2023-06-18 18:41:12.888	0x36479f2865bbb5...
112	miner	Swap		→	0x2123ac54afaa5f...	2023-06-18 18:41:12.888	0xc5c9f6dda68422...
113	miner				0xf330ca91cf2426...	2023-06-18 18:41:12.888	0xc5c9f6dda68422...
37	10 secs				0xdc440025c2866f...	2023-06-18 18:41:01.989	0x562680a4dc50ed...

프런트러닝 공격의 결과 (The consequences of the frontrunning attack)

사용자 트랜잭션 전에 인위적 수요가 생겨 \$B0B 토큰의 가격이 상승했다. 사용자의 원래 160만 개 \$B0B 주문은 더 나쁜 가격에서 체결되며 적은 수량을 받게 되어 손실이 발생했다.

한편 MEV 봇은 상승한 가격에 즉시 토큰을 매도해 이익을 실현했다. 이 사례에서는 봇의 활동이 샌드위치 공격으로까지 이어져 손실이 더 커졌다.

사용자는 약 0.1 ETH의 손실을 봤고, MEV 봇은 이익을 챙겼다.

프런트러닝은 얼마나 해로운가? (How Harmful is Frontrunning?)

프런트러닝이 겉보기에는 무해하거나 영리해 보일 수 있지만, 개별 트레이더에게 악영향을 주고 이더리움 네트워크의 무결성을 훼손할 수 있다.

트레이더에 대한 영향 (Impact on traders)

프런트러닝은 대기 트랜잭션을 악용해 결과를 왜곡함으로써 공정한 시장 운영을 훼손한다. 트레이더는 인위적으로 변동된 가격 때문에 더 비싼 가격을 지불하거나 더 적은 자산을 받게 된다.

장기적 시장 결과 (Long-term market consequences)

프런트러닝이 지속되면 DeFi 시장에 대한 신뢰가 약화될 수 있다. 트레이더가 불리하거나 착취당한다고 느끼면 떠나게 되고, 유동성과 시장 효율성이 저하된다.

네트워크 효과 (Network effects)

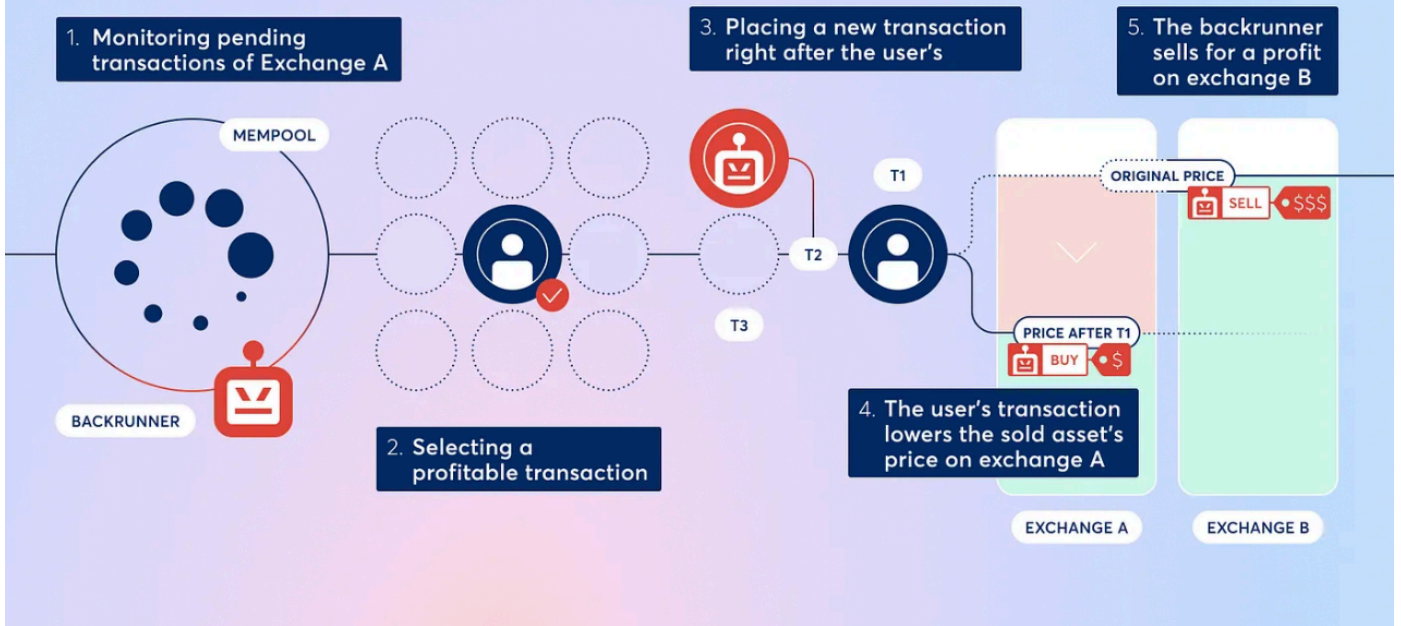
프런트러닝은 불필요한 블록 공간 경쟁을 반복적으로 유발해 혼잡을 키우고 트랜잭션 처리를 지연시키는 등 네트워크에도 영향을 미친다.

백러닝이란? (What is Backrunning?)

백러닝은 트레이더가 자신의 거래에서 발생할 수 있었던 잠재적 이익을 놓치게 만드는 MEV(최대 추출 가능 가치)의 특정 유형이다.

실무적으로, 백러닝은 고가치 트랜잭션 직후에 전략적으로 트랜잭션을 실행하는 것을 말한다. 이렇게 하면 최초 트랜잭션의 가격 영향으로 남겨진 차익거래 기회를 포착할 수 있다.

Backrunning



백러닝의 작동 방식 (How Backrunning Works)

백러닝은 이더리움 멤풀(대기 트랜잭션이 모여 있는 영역)의 정보를 전술적으로 활용하여, 고가치 거래 직후에 트랜잭션을 배치해 이익을 얻는다.

세 가지 주요 MEV 유형(프런트러닝, 샌드위치 공격, 백러닝) 중에서 백러닝은 가장 덜 해로운 것으로 간주된다. 백러닝 단독으로는 대규모 거래가 남긴 차익거래 기회를 포착할 뿐 최초 거래 자체에 영향을 주지는 않는다. 그러나 프런트러닝과 결합되면 가장 해로운 형태인 샌드위치 공격이 된다.

숙련된 트레이더에게는 자신의 거래로 생긴 잔여 차익거래를 포착하는 것이 수익이 될 수 있지만, 대부분의 리테일 트레이더에게는 이는 놓친 기회다. 다행히 MEV Blocker 같은 도구를 통해, 사용자는 수동 거래 없이도 이러한 기회에서 발생하는 백런 리베이트를 자동으로 받을 수 있다.

백러닝의 구체적 동작 (How backrunning works)

백러닝의 주요 행위자는 대개 MEV 봇으로, 이들은 대기 중인 이더리움 트랜잭션을 모니터링하도록 프로그래밍되어 있다. 이 봇들은 기존 거래 바로 뒤에 전략적으로 거래를 배치해, 가격 영향으로 생긴 차익거래를 포착한다.

이는 보통 자동화된 마켓 메이커(AMM)에서 발생한다. 대규모 거래가 AMM을 통과하면 유동성 풀이 불균형해지며 — 매도된 자산의 가격은 하락하고 매수된 자산의 가격은 상승한다. 이 가격 불균형이 차익거래 기회를 만들고, MEV 봇은 후속 거래를 배치해 이익을 얻는다.

백러닝 예시 (Backrunning example)

단순한 시나리오를 살펴보자:

Alex라는 사용자가 대규모 거래를 시작해 — Uniswap에서 1만 달러 상당의 ETH를 매도하고 COW를 매수한다. 이 스왑은 AMM 메커니즘상 COW의 가치를 올리고 ETH의 가치를 약간 내린다.

동시에 한 MEV 봇이 Alex의 대규모 트랜잭션을 감지하고 즉시 반응한다. 봇은 낮아진 가격의 ETH를 매수하고, 곧바로 아직 가격이 조정되지 않은 다른 거래소에서 ETH를 매도한다(혹은 반대 방향). 봇은 거래소 간 일시적 가격 차이에서 이익을 얻는다.

기술적 관점에서, Alex는 원래 거래에서 돈을 잃지는 않는다 — 기대한 가격을 받는다. 그러나 자신의 트랜잭션이 만든 차익거래 기회를 놓치게 되며, 그 기회에서 생긴 이익은 MEV 봇이 가져간다.

더 넓게 보면, MEV 봇이 차익거래를 독점하여 일반 트레이더가 이러한 이익을 얻지 못하게 만들고, 거래소 전반의 트랜잭션 혼잡을 증가시키는 부작용이 생긴다.

샌드위치 공격이란? (What is a Sandwich Attack?)

샌드위치 공격은 사용자의 트랜잭션이 두 개의 적대적 트랜잭션 — 하나는 앞에, 하나는 뒤에 — 의해 포위되어 “샌드위치”되는 공격이다.

결과적으로 원래의 트랜잭션은 불필요하게 높은 가격으로 실행되어, 사용자는 부풀려진 가격을 지불하게 되고 공격자는 이 차이로 이익을 얻는다.

샌드위치 공격의 작동 방식 (How a sandwich attack works)

서처가 샌드위치 공격 기회를 포착하면, 대상 트랜잭션 앞에 (프런트러닝) 하나의 거래를, 뒤에 (백러닝) 또 하나의 거래를 배치해 가격을 조작한다.

Uniswap 같은 자동화된 마켓 메이커(AMM) 구조상, 이러한 거래는 자산의 가격을 전략적으로 조작하여 이익을 남긴다. 이를 완전히 이해하려면 몇 가지 핵심 개념을 먼저 살펴볼 필요가 있다.

핵심 개념 (Core concepts at play)

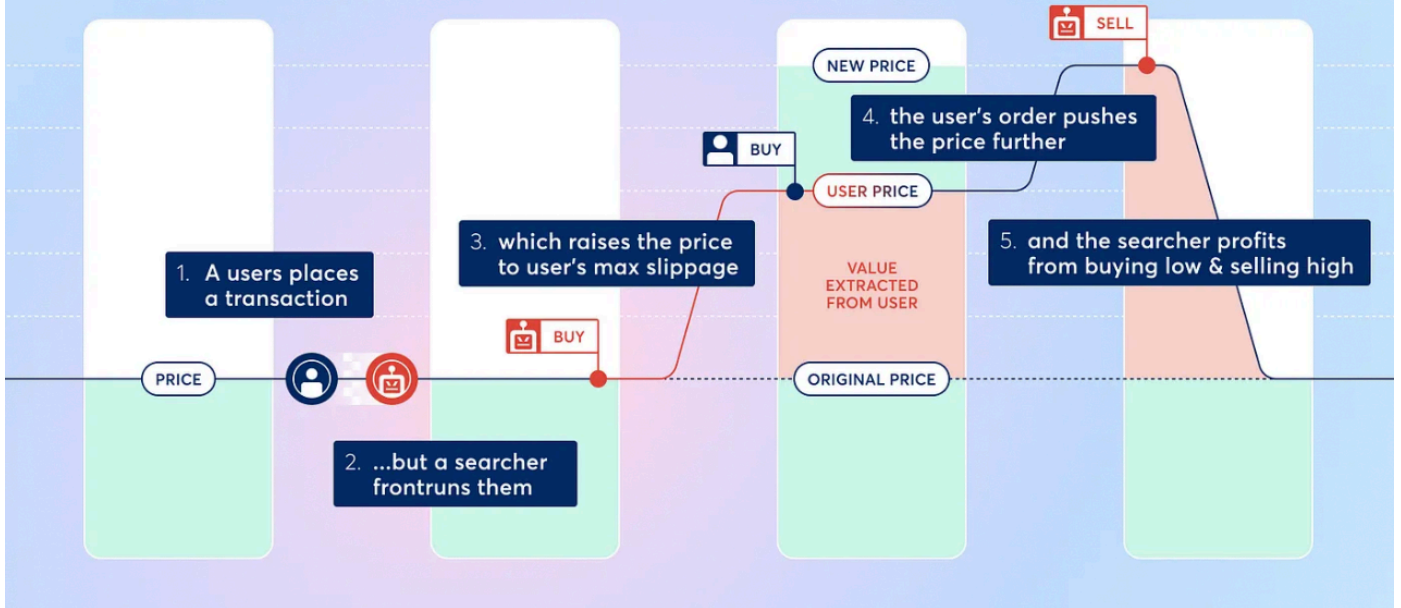
- 자동화된 마켓 메이커(AMM, Automated Market Makers):
AMM은 전통적 오더북 없이도 실시간으로 자산을 거래할 수 있게 하는 메커니즘이다.
유동성 풀 내 두 자산의 가격 비율을 일정하게 유지하며, 예를 들어 COW/ETH 풀에서 누군가 COW를 팔아 ETH를 사면 COW의 가격은 떨어지고 ETH의 가격은 상승한다. 이 관계는 $x \times y = k$ 공식을 따른다.
- 슬리피지 허용치(Slippage Tolerance):
사용자는 거래 시 수락 가능한 최대 가격 편차(슬리피지)를 설정한다. 예를 들어, ETH가 2,000달러일 때 5% 슬리피지를 설정하면 최대 2,100달러까지 지불할 수 있다.
가격이 이 범위를 초과하면 거래는 실패한다. 슬리피지 허용치가 높을수록 서처가 샌드위치 공격을 할 여지가 커진다.
- 가격 영향(Price Impact):
각 거래는 유동성 풀의 일부를 소모하며 가격을 이동시킨다. 거래 규모가 클수록 가격 영향도 커진다.
예를 들어, 100달러 규모의 ETH 거래는 거의 영향을 미치지 않지만, 100만 달러 규모의 거래는 가격을 크게 움직인다.
- 트랜잭션 재정렬(Transaction Reordering):
블록체인의 트랜잭션은 제출된 순서대로 반드시 실행되지 않는다. 검증자는 서처의 뇌물을 받아 블록 내 트랜잭션 순서를 바꿀 수 있으며, 이는 프런트러닝 및 샌드위치 공격을 가능하게 한다.

샌드위치 공격 단계별 예시 (The sandwich attack: Step by step)

ETH와 COW 거래를 예로 들어 단계별로 살펴보자.

Sandwich Attacks

COW Swap



1. Bessie가 트랜잭션 제출:
Bessie는 DEX(예: Uniswap)에서 ETH로 4,000 COW를 구매하려 한다.
10%의 슬리피지 허용치를 설정했으며, 이는 최대 1.1 ETH까지 지불할 의향이 있다는 뜻이다.
2. 서처가 트랜잭션을 프런트러닝:
서처의 봇이 멤풀에서 Bessie의 대기 거래를 감지하고, 그녀보다 먼저 1 ETH로 4,000 COW를 매수하여 가격을 끌어올린다.
결과적으로 Bessie의 거래는 4,000 COW를 1.1 ETH에 구매하게 된다 — 그녀가 설정한 최대 한도 가격이다.
3. Bessie의 거래가 부풀려진 가격으로 실행:
거래가 실행되어 1.1 ETH에 4,000 COW를 받지만, 이는 서처의 가격 조작으로 인한 과다 지불이다.
4. 서처가 백러닝 수행:
공격자는 앞서 산 4,000 COW를 부풀려진 가격에 다시 팔아 0.1 ETH의 이익을 챙긴다.

결과 요약 (Summary of the outcome)

샌드위치 공격은 MEV 봇에게 매우 수익성이 높다.
이들은 예측 가능한 AMM 메커니즘을 악용해 무위험으로 이익을 얻는다.
반면 Bessie는 단지 슬리피지 허용치 때문에 거래에서 10% 더 많은 비용을 지불하게 된다.

성능 벤치마크 (Performance Benchmark)

다음 논문에서는 네 가지 주요 MEV 보호 RPC — MEV Blocker, Flashbots, Blink, Merkle — 를 동일한 트랜잭션으로 비교하여 실행 품질을 평가했다. 이를 통해 각 RPC의 OFA(Order Flow Auction) 설계 차이가 사용자 혜택에 어떤 영향을 미치는지 실증적으로 분석했다. 이 연구는 오더플로우 제공자들이 마케팅 문구를 신중히 검토하고 트랜잭션을 전송하는 대상을 면밀히 파악해야 함을 보여준다.

비교 결과, 각 RPC 제공업체는 다음과 같이 순위가 매겨졌다. MEV Blocker는 모든 지표에서 최고 수준의 성능을 보이는 유일한 RPC였다. Flashbots는 포함 속도와 백런 가치에서 MEV Blocker와 유사하거나 약간 낮았으나, 실행 가격은 가장 낮았다. Merkle과 Blink는 매우 낮은 리베이트를 생성했으며, 특히 Merkle은 낮은 성공률로 두드러졌다.

MEV Blocker RPC isn't like any other...



	Inclusion Delay	Price Improvement (vs. MEV Blocker)	Average Rebate	Success Rate
MEV Blocker	1.34 blocks —	— (baseline)	0.0035 ETH —	85% —
Flashbots Protect	1.49 blocks <i>1.68 seconds slower</i>	21 bps less	0.0016 ETH 54% less	84% 1.2% worse
Merkle	1.86 blocks <i>6.1 seconds slower</i>	9 bps less	0.0009 ETH 75% less	70% 21.4% worse
Blink	1.56 blocks <i>2.8 seconds slower</i>	9 bps less	0.0011 ETH 69% less	84% 1% worse

더 자세히 알고 싶다면 각 카테고리의 분석을 읽거나 아래 전체 논문을 참고하라:

Private MEV Protection RPCs: Benchmark Study

백런 품질 (Backrun Quality)

먼저 각 RPC가 생성한 백런을 측정했다:

RPC Provider	MEV Blocker	Merkle	Flashbots	Blink
Backrun (in ETH)	0.00350	0.00108	0.00088	0.00173

Table 2: Backrun value per RPC.

MEV Blocker와 다른 RPC 솔루션 간의 비교는 스왑 가격 개선 분석과 유사한 방법론을 따른다.

양쪽에서 동일 트랜잭션이 온체인에 포함된 경우만 비교 대상으로 삼았다.

첫 번째 플롯은 전체 트랜잭션의 평균 백런 및 분포를 나타내며, 두 번째 플롯은 적어도 한쪽(RPC 또는 MEV Blocker)에 비-제로 백런이 있는 트랜잭션만 포함한다.

스왑은 두 가지 범주로 나눌 수 있다: 유동성이 높은 페어(ETH-USDC)와 유동성이 낮은 페어(ETH-GNO, ETH-COW, ETH-AAVE). 유동성이 높은 페어에서는 차익거래가 발생하지 않아 0 값이 많다. 이는 해당 풀의 유동성이 충분해, 단일 거래로는 가격 불균형이 생기지 않기 때문이다.

유동성이 낮은 페어도 항상 백런을 발생시키지는 않는다. 분석 결과, MEV Blocker의 백런 규모는 다른 RPC보다 10% 이상 높은 신뢰도 수준에서 더 컸다.

그러나 사용자에게 실제로 전달된 백런 리베이트를 보면 Blink와 Merkle은 이를 사용자에게 반환하지 않아 차이가 나타난다.

RPC Provider	MEV Blocker	Merkle	Flashbots	Blink
Backrun (in ETH)	0.00350	0	0.00088	0

Table 3: User Rebate per RPC.

MEV Blocker와 Flashbots 간 비교는 변함없다 — 두 RPC 모두 사용자에게 100%의 리베이트를 돌려준다. 따라서 리베이트 가치 측면에서 MEV Blocker와 Flashbots가 Merkle과 Blink보다 사용자에게 더 유리하다고 결론 내릴 수 있다.

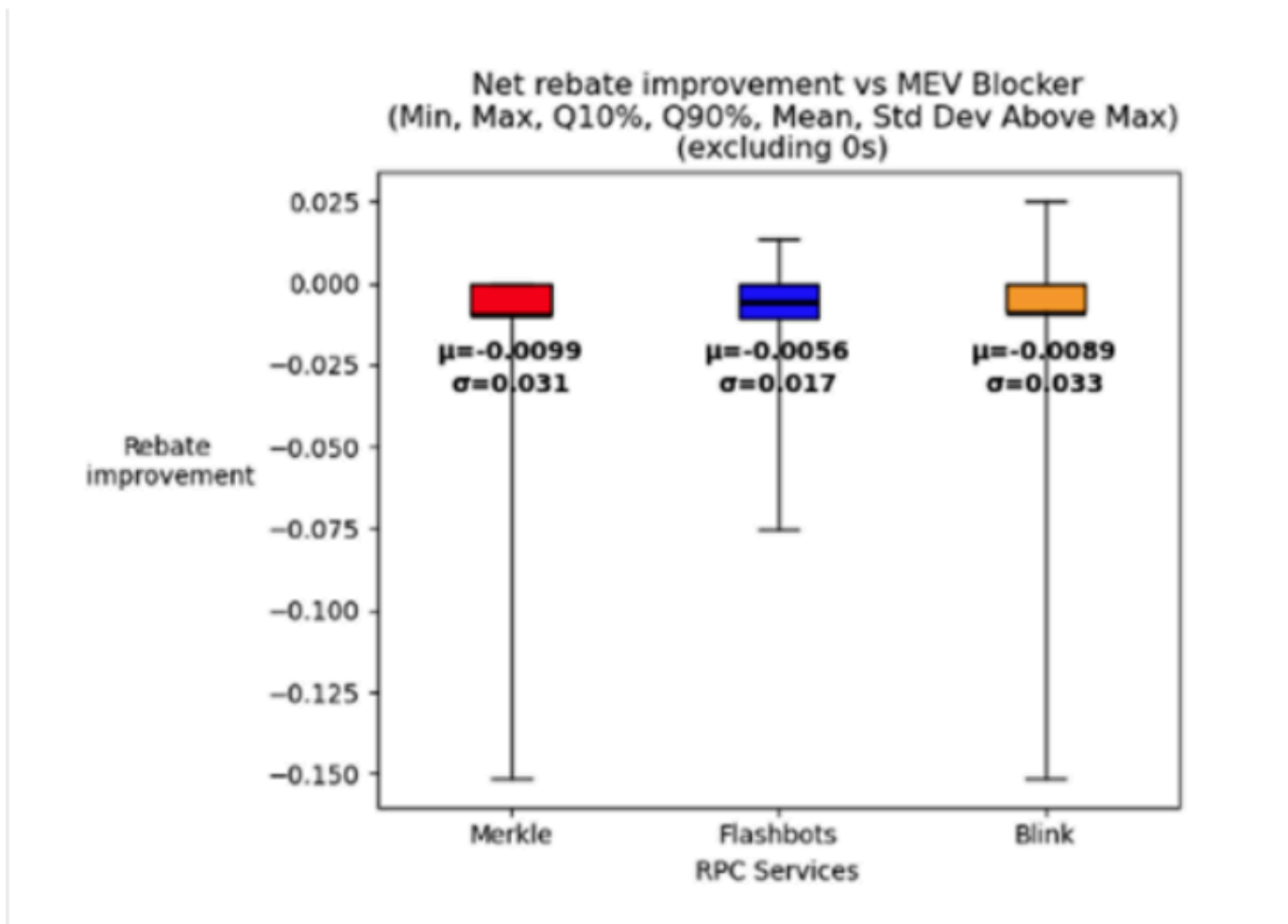


Figure 8: Transaction flow in MEV protection RPCs.

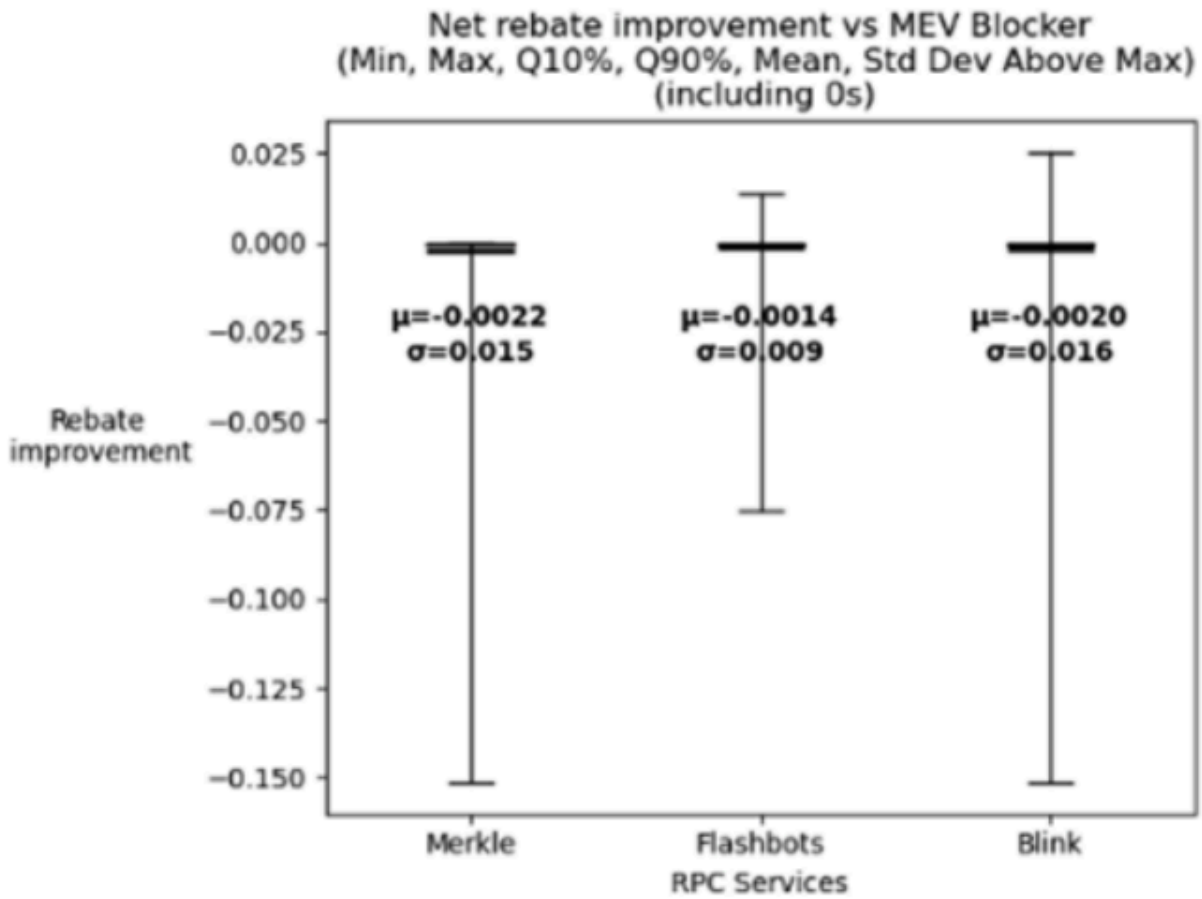


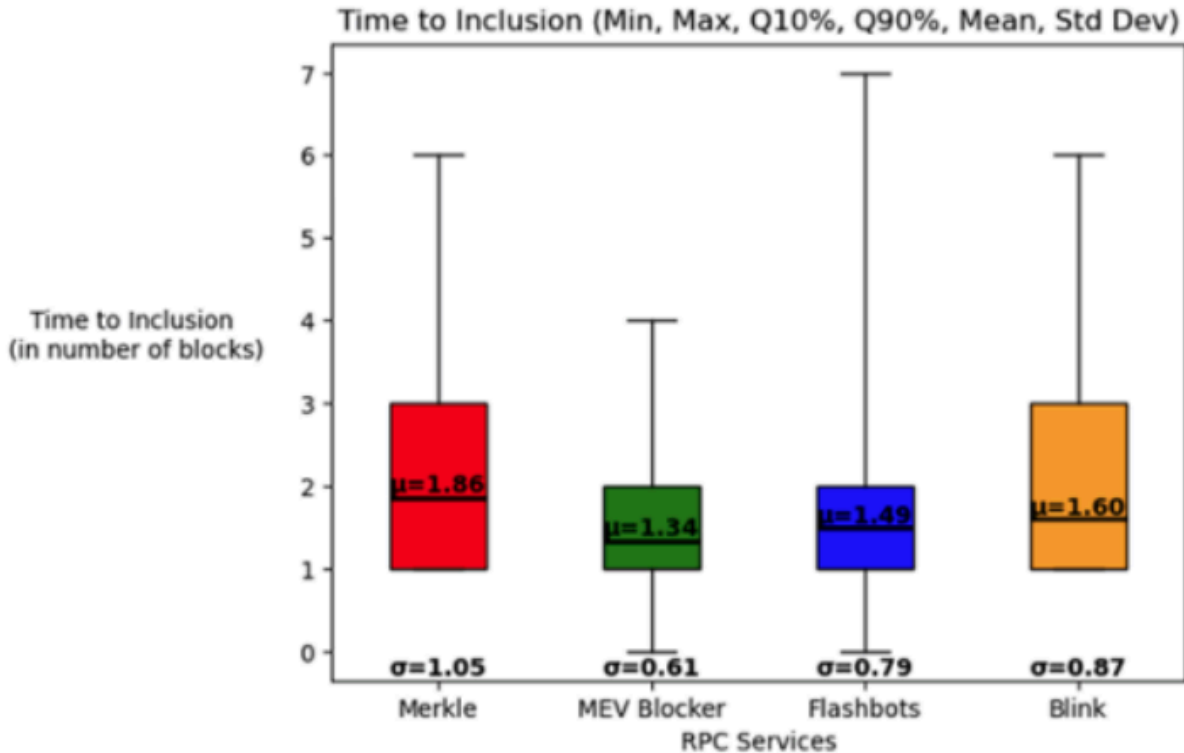
Figure 9: Transaction flow in MEV protection RPCs.

RPC	Including 0			Excluding 0		
	Sample size	T-test	P-value	Sample size	T-test	P-value
Merkle	120	-1.586	5.765e-2	27	-1.624	5.826e-2
Flashbots	120	-1.761	4.042e-2	30	-1.811	4.085e-2
Blink	120	-1.373	8.623e-2	27	-1.391	8.800e-2

Table 4: T-test and p-value comparisons including and excluding zero backrun values

포함 속도 (Inclusion Speed)

이제 성공적으로 온체인에 포함된 트랜잭션에 대해, 제출과 포함 사이의 블록 수를 비교한다.
각 RPC 제공자의 성공률 기준에 따라 모든 성공 트랜잭션을 고려했다.



포함까지 걸린 블록 수의 분포를 상자 그림(box plot)으로 표현했으며, 최소값, 10백분위수, 평균, 90백분위수, 최대값을 표시했다. 평균과 표준편차 모두 RPC 제공자를 같은 순서로 랭크한다.

샘플 결과, MEV Blocker가 가장 빠른 실행 속도를 보였으며, 그 다음이 Flashbots, Blink, Merkle 순이었다. Flashbots는 포함까지 7블록이 걸린 단일 큰 이상치(outlier)를 보였지만, 두 번째로 큰 값은 4블록이며 표본 크기가 충분해 평균에는 큰 영향을 주지 않았다. 이 세부 사항을 고려했을 때, 전체 성능 결과는 일관되었다.

스왑 가격 개선 (Swap Price Improvement)

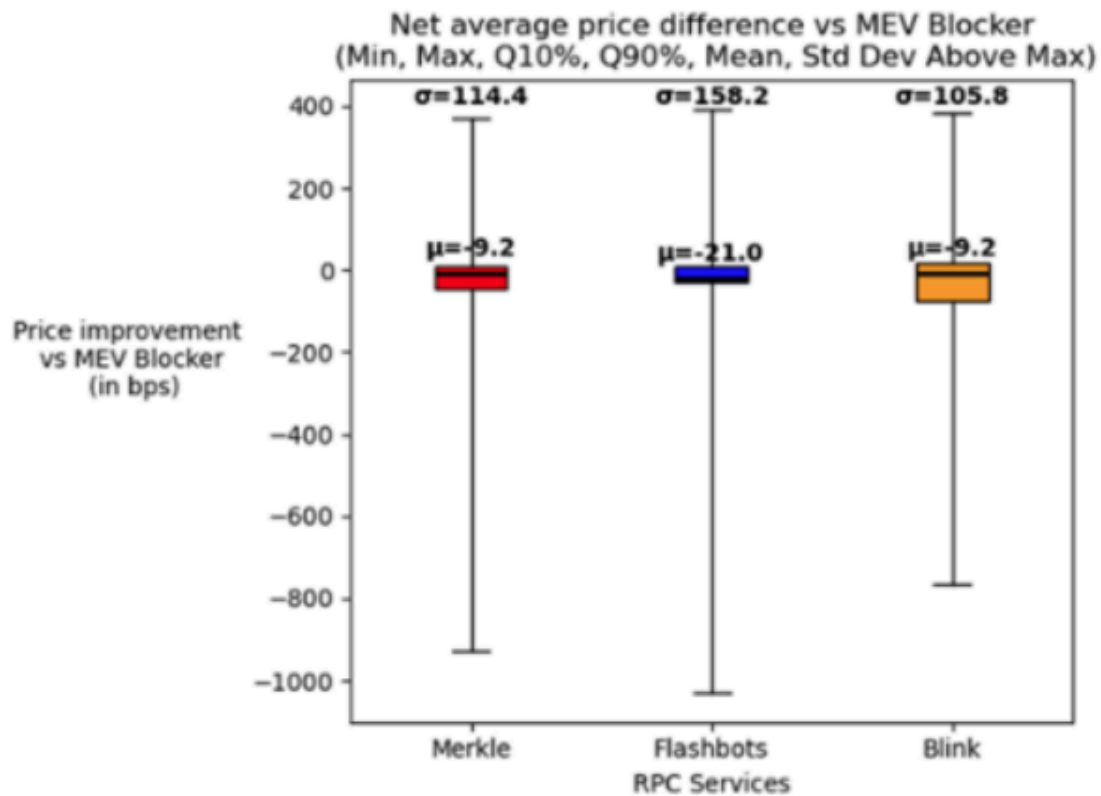
이번에는 스왑에만 초점을 맞춰, 각 RPC의 실행 품질을 비교했다. 이는 스왑 가격의 상대적 개선 정도로 측정된다. 각 RPC가 동일한 스왑을 실행했을 때를 비교하여, 거래별로 다음 공식을 적용했다:

$$\text{가격 개선율} = \text{price}(\text{RPC}) / \text{price}(\text{MEV Blocker}) - 1$$

$$\text{또는 price improvement} = \text{output}(\text{RPC}) / \text{output}(\text{MEV Blocker}) - 1$$

입력값이 동일하므로 두 식은 동일하다. 결과적으로 평균적으로 MEV Blocker가 모든 다른 RPC보다 우수했다: Blink 및 Merkle보다 약 9bps, Flashbots보다 21bps 더 좋았다.

또한 “ $H_0: \text{price improvement} = 0$ ” 가설로 t-검정을 수행하여 통계적 유의성을 확인했다. Flashbots의 경우 p-값이 10% 미만으로, MEV Blocker와 Flashbots 간 차이는 10% 유의수준에서 통계적으로 유의했다. 반면 다른 두 RPC와의 차이는 통계적으로 유의하지 않았다.



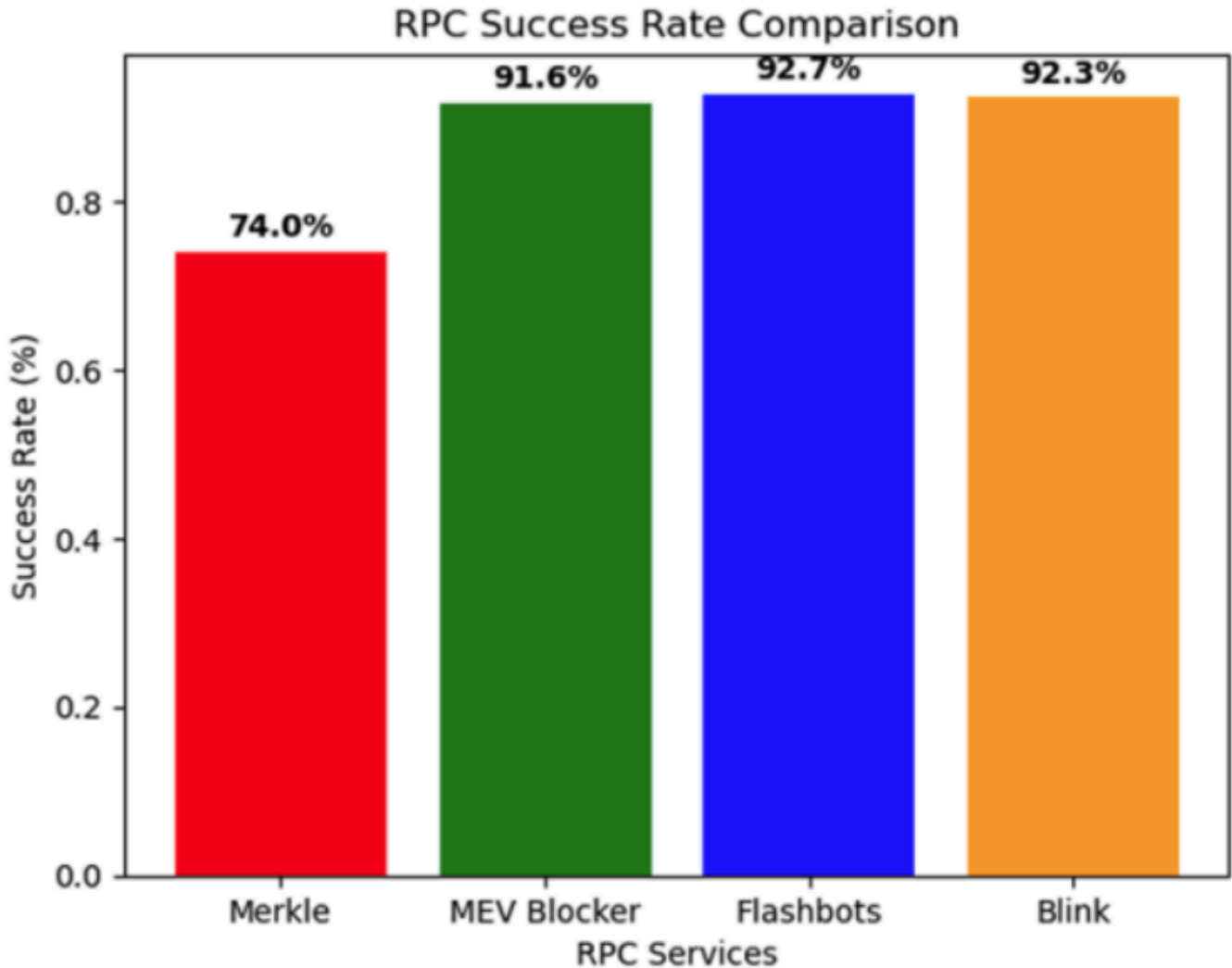
Sample Size	t-test (ETH)	p-value
Merkle 92	-0.764	0.223
Flashbots 98	-1.309	0.097
Blink 97	-0.851	0.198

성공률 (Success Rate)

성공률은 RPC를 통해 제출된 트랜잭션 중 온체인에서 성공적으로 실행된 비율로 정의한다. 즉, 온체인에 포함되었지만 되돌려진(reverted) 트랜잭션은 실패로 간주한다.

총 273건의 트랜잭션 중, MEV Blocker, Blink, Flashbots는 모두 90% 이상 성공률을 보였으며, Merkle의 성공률은 74%로 가장 낮았다.

각 RPC별 색상은 이후 모든 플롯에서 동일하게 유지된다.



CoW AMM: 최초의 MEV 포착 AMM (CoW AMM: The First MEV-capturing AMM)

CoW AMM은 LP를 LVR로부터 보호하여, 더 낮은 위험으로 더 높은 수익을 올리며 유동성을 공급할 수 있게 한다. CoW AMM은 기존 풀과 비교해 TVL이 거의 5% 더 높고, LVR로부터 수백만 달러를 보호했으며, 현재까지 LP에게 100,000 달러 이상의 서플러스를 포착했다.

AMM들은 LVR을 알려주고 싶어 하지 않는다 (AMMs don't want you to know about LVR)

유동성 공급자는 자신들의 토큰이 수익을 창출하길 기대하지만, AMM의 불편한 진실은 대부분의 유동성 풀이 손실을 본다는 점이다. 실제로 매년 수억 달러 규모의 LP 자금이 차익거래자에게 탈취된다. 이러한 손실은 리밸런싱 대비 손실(LVR, loss-versus-rebalancing)로 알려져 있다. LVR은 프런트러닝과 샌드위치 공격을 합친 것보다 더 큰 MEV의 원천이다.

LP를 위해 설계된 AMM (An AMM designed with LPs in mind)

CoW AMM은 배치 경매를 사용해 서플러스를 LP에게 보내는 방식으로 LVR을 근본적으로 제거한다.

1. 유동성 공급자는 보호된 CoW AMM 유동성 풀에 토큰을 예치하고, 트레이더는 이 유동성에 접근한다
2. 차익거래 기회가 있을 때마다 솔버들이 CoW AMM 풀의 리밸런싱에 입찰한다

3. 풀에 가장 많은 서플러스를 제공하는 솔버가 리밸런싱 권리를 획득한다
4. CoW AMM은 LP를 위해 차익거래 가치를 포착하고 MEV 봇으로부터 이를 차단함으로써 LVR을 제거한다

CoW AMM에 유동성 배치 (Deploy liquidity on CoW AMM)

Balancer와의 통합 덕분에, 이제 LP는 몇 번의 클릭만으로 유동성을 배치하거나 새 풀을 생성할 수 있다.

개념 (Concepts)

LVR의 문제 (The Problem of LVR (Loss-versus-rebalancing))

컬럼비아 대학교 연구팀이 처음 정의한 LVR은, AMM의 가격이 다른 거래 venue에 비해 오래되어(스테일) 있을 때 발생하는 차익거래의 한 형태다.

차익거래자는 AMM과 더 유동적인 거래소(보통 바이낸스 같은 중앙화 거래소) 사이의 가격 차이를 이용해 거래하며, 이 과정에서 가격을 바로잡는 동시에 LP로부터 가치를 추출한다.

LVR이 작동하는 방식 (How LVR Works)

대부분의 AMM(예: Uniswap)은 상수 함수 자동화 마켓 메이커 —CF-AMM의 예시다. 이러한 AMM은 두 자산을 예치받고 각 거래 후 자동으로 가격을 재계산하여 언제나 충분한 유동성을 보장한다. 이는 AMM이 거래되는 동안 자산 가격을 탐색(discovery)한다는 의미다.

하지만 암호자산은 중앙화 거래소를 포함한 다양한 플랫폼에서 거래되므로, CF-AMM의 가격은 더 유동적인 중앙화 거래소의 가격에 비해 오래될 수 있다. 이 괴리는 차익거래자가 유동적 거래소와 스테일 AMM 사이에서 거래하게 만들고, 가격을 교정하는 동시에 차익거래 수익을 포착하게 한다.

“리밸런싱 대비 손실(Loss-versus-rebalancing)”은 LP가 중앙화 거래소 같은 더 유동적인 venue 대비 가격이 스테일한 CF-AMM에 유동성을 공급하는 상황을 말한다. 자금을 풀에 그대로 두는 대신 AMM과 거래소 사이를 지속적으로 “리밸런싱”했다면 얻었을 수익만큼 벌지 못하게 되며, 결과적으로 “리밸런싱” 전략과 비교해 “손실”을 보게 된다.

LVR이 LP에 미치는 영향 (The Impact of LVR on LPs)

많은 유동성 공급자는 LVR을 들어본 적조차 없지만, 이는 그들의 유동성의 5–7%에 달하는 비용을 초래하며, 매년 수억 달러의 손실로 이어진다. 사실 LVR을 고려하면, 가장 큰 유동성 풀들조차 LP에게 수익성이 전혀 없을 수 있다.

이러한 손실 때문에 LVR은 프런트러닝과 샌드위치 공격을 합친 것보다 더 많은 가격 착취를 차지하는 MEV(최대 추출 가능 가치)의 한 유형이다.

CoW AMM의 작동 방식 (How CoW AMMs Work)

FM-AMM (FM-AMMs)

“함수 극대화(Function-Maximizing)” AMM은 CF-AMM 설계의 한계를 해결하고 LVR을 제거하는 새로운 AMM 메커니즘이다. FM-AMM은 거래를 배치로 모아 동일한 균일 청산가에서 실행한다. 이 가격은 AMM이 각 거래마다 “커브를 위로 이동”하도록 정해진다. 배치가 열려 있는 동안 누구나 거래를 제출할 수 있기 때문에, 차익거래자 간 경쟁이 FM-AMM이 항상 올바른 균형 가격에서 거래하도록 보장한다.

CoW AMM (CoW AMM)

CoW AMM은 CoW Protocol에서 발생하는 거래에 유동성을 공급하는 FM-AMM의 프로덕션 구현이다. 솔버들은 AMM을 상대로 거래할 권리를 두고 경쟁하며, AMM 커브를 더 위로 이동시키는 솔버가 승리한다.

CoW AMM 풀은 스테이블-투-스테이블을 제외한 모든 토큰 페어에 최적화되어 있다. 변동성은 특정 유동성 풀에서 발생하는 LVR의 양을 좌우하므로, CoW AMM 풀은 차익거래가 LP 수수료를 증가하는 변동성 높은 페어에서 가장 효과적이다.

CoW AMM 시작하기 (Getting Started with CoW AMM)

손쉬운 유동성 공급을 위해 CoW DAO는 Balancer와 협력하여 CoW AMM을 Balancer 생태계에 도입했다. LP는 [Balancer](#) 앱을 사용해 수십 개 이상의 유동성 풀 중 하나에 직접(LP directly) 참여할 수 있다.

다음 섹션에서는 LP가 Balancer 안팎에서 신규 자산에 대한 CoW AMM 풀을 직접 생성하는 방법을 배울 수 있다.

거버넌스 (Governance)

이 사이트는 CoW DAO의 현재 거버넌스 구조를 나타낸다.

거버넌스의 진화 (GOVERNANCE EVOLUTION)

CoW DAO의 거버넌스는 CoWmunity가 소유하고, 발전시키며, 집행한다. 따라서 이 문서는 살아 있는 문서로 간주되어야 하며, CoW DAO가 발전함에 따라 업데이트된다.

거버넌스 장소 (Venues)

CoW DAO 거버넌스에 참여할 수 있는 여러 장소가 있으며, 각각 고유한 목적을 가진다.

포럼 (Forum)

CoW DAO의 포럼은 거버넌스 관련 토론의 주된 장소다. 포럼에 가입하면 커뮤니티 구성원은 게시하고 토론에 참여할 수 있다.

스냅샷 (Snapshot)

CoW DAO의 스냅샷 스페이스는 구성원이 [CIP](#)에 투표할 수 있는 간단한 투표 인터페이스다. 스냅샷 투표는 투표에 사용된 주소가 보유하거나 위임받은 vCOW+COW의 수에 따라 가중치가 부여된다.

디스코드 (Discord)

CoW DAO 디스코드 서버는 현재 CoWmunity의 주요 토론 허브이자 비공식 거버넌스 토론 공간이다. `governance-discussion` 채널은 거버넌스 사안과 제안을 논의하는 곳이다.

미션 스테이트먼트 (Mission statement)

CoW DAO는 공정하고 더 보호적인 금융 시스템을 구축하려는 개발자, 마켓 메이커, 커뮤니티 기여자들의 개방형 조직이다. CoW DAO는 현재 사용자를 MEV 공격으로부터 보호하고 기대보다 더 나은 결과를 제공하기 위해 오더 플로우 경매를 활용하는 탈중앙화 트레이딩 제품인 CoW Swap, CoW Protocol, MEV Blocker를 지원한다.

비전 (Vision)

우리는 모든 종류의 자산이 이더리움과 다른 탈중앙화 블록체인 위에서 토큰화되고, 모든 사람 —개인과 집단—이 그들의 토큰화된 자산을 완전 보관할 수 있는 미래를 내다본다. CoW DAO의 비전은 전 세계의 사람들, 조직, 스마트 컨트랙트, 커뮤니티 사이에서 디지털 자산이 공정하고, 효율적이며, 신뢰할 수 있는 방식으로 거래되는 탈중앙화된 미래다. 우리의 미션은 사용자가 가능한 한 사용자 친화적이고 가격 효율적인 방식으로 디지털 자산을 교환하도록 돕는 제품을 구축하여, 모든 사용자가 안전하게 거래하고 거래가 보호받고 있음을 알 수 있게 하는 것이다.

우리는 지속적인 혁신을 적용하고, 지적 담대함을 기르며, CoW DAO 생태계를 확장함으로써 가장 빛나는 인재들이 커뮤니티에 합류하도록 초대하는 데 전념한다.

토큰 (Token)

CoW Protocol의 핵심에는 COW 토큰이 있으며, 이는 CoW Protocol 생태계 내의 거버넌스 토큰 역할을 한다. COW 토큰은 이해관계자들이 프로토콜의 개발 및 진화를 이끄는 의사 결정 과정에 직접 참여할 수 있도록 한다. 이 거버넌스 프레임워크는 프로토콜의 사용자, 개발자, 지지자 간의 인센티브를 일치시키기 위해 설계되었으며, 강력하고 커뮤니티 중심적인 거버넌스 시스템을 형성한다.

컨트랙트 주소 (Contract Address)

COW - 메인 토큰 (Main token)

체인	COW 토큰 주소
Ethereum	0xFfC41a87F8e0C7F79220a773794E4D5F947f49ab
Gnosis Chain	0x11772d22c6a0df340b957571e2ac3b793a13c8f4
Arbitrum One	0x8cbb5c0e0caedaa9a8ad1fd8383425f57a7ba04b
Base	0x649a1e80b71fb38ea10b043b33a7e9b5adad6a69
Polygon	0x2e4fed33a42e1a5e11c14547151b6ed6395985f8
Avalanche	N/A
BNB	N/A

vCOW - 베스팅 토큰 (Vesting token)

체인	vCOW 토큰 주소
Ethereum	0xb3763f5f6c6f19893a5d6579cba08076808488a5
Gnosis Chain	0xac29c91b53e3fcd845b347f213d36362e07ee81b
Arbitrum One	N/A
Base	N/A
Avalanche	N/A
Polygon	N/A
Lens	N/A
BNB	N/A

공급 및 인플레이션 일정 (Supply & Inflation Schedule)

COW 토큰은 CoW Protocol의 장기적인 지속 가능성과 자율성을 지원하도록 설계되었다. 최대 인플레이션율은 연 3%로 제한되며, 인플레이션 조치는 최소 365일 간격으로만 시행될 수 있다. 이 신중한 접근 방식은 토큰 공급 증가가 신중하게 이루어지도록 하여, 무분별한 발행으로 인한 리스크를 방지한다.

발행된 토큰 수 (How many tokens were issued?)

TGE(Token Generation Event)에서 10억 개의 토큰이 발행되었다.

토큰 배분 (How were tokens distributed?)

초기 10억 개 COW 토큰의 배분은 다음과 같다:

- CoW DAO 금고: 44.4% — 커뮤니티가 프로토콜 개발 및 유지보수의 중심 역할을 담당함을 강조
- 팀: 15% — CoW Protocol을 구축하고 발전시켜온 팀 구성원 보상
- GnosisDAO: 10% — CoW Protocol 공동 개발 파트너십에 대한 인정
- CoWmunity 에어드롭: 10% — 초기 사용자 및 기여자 보상
- CoWmunity 투자: 10% — 초기 사용자의 참여 및 기여 확대
- 자문단: 0.6% — 전략적 조언에 대한 보상
- 투자 라운드: 10% — 성장 자금 및 지원 제공

COW와 vCOW의 차이점 (The difference between COW and vCOW)

vCOW는 TGE 시점에 발행된 별도의 토큰 컨트랙트이며, 1:1 비율로 vCOW를 COW로 전환할 수 있는 “swap” 기능을 제공한다.

vCOW 토큰은 CoW Protocol의 핵심 토큰 COW의 가상 형태로, 팀 구성원, 자문단, 초기 투자자 등 장기적 참여를 유도하기 위한 인센티브로 사용된다.

vCOW는 선형 베스팅 일정에 따라 4년에 걸쳐 점진적으로 언락되며, 배포 시점부터 시작된다.

vCOW가 COW의 유통 공급량에 미치는 영향 (How does vCOW affect the circulating supply?)

과거에는 모든 vCOW가 유통 공급량에서 제외되었다. 그러나 베스팅이 완료되어 클레임 가능한 양이 증가함에 따라, 현재 API는 교환 가능한(vCOW → COW) 토큰의 양을 반영하도록 업데이트되었다.

업데이트된 API는 베스팅 완료(아직 미청구)된 vCOW 토큰을 포함한다. 이는 vCOW 보유자가 언제든지 COW로 전환할 수 있기 때문에, 유통 공급량을 보다 정확하게 반영한다.

유통 공급량 계산 방식 (How is the circulating supply calculated?)

현재 CoW DAO가 사용하는 유통 토큰 공급량 계산 공식은 다음과 같다:

$$\text{유통 공급량} = \text{총 공급량} - \text{미베스팅 토큰} - \text{DAO 금고 보유량}$$

각 항목의 의미는 다음과 같다:

- 1. 총 공급량 (Total Supply – 10억 COW)
이는 존재할 수 있는 COW 토큰의 최대 수량이다. CoW Protocol의 총 공급량은 1,000,000,000 COW로 고정되어 있다. 하지만 이 모든 토큰이 즉시 유통되거나 거래 가능한 것은 아니다.
- 2. 미베스팅 COW 토큰 (Unvested COW Tokens)
팀, 기여자, 자문단 등에게 할당되었으나 아직 잠금 해제되지 않아 사용 또는 판매가 불가능한 토큰이다. 베스팅 일정은 장기적인 인센티브를 맞추기 위해 일반적으로 사용되며, 예를 들어 4년 동안 점진적으로 언락되는 구조일 수 있다.
- 3. DAO 금고 보유량 (DAO Treasury Holdings)
DAO 금고는 장기적인 거버넌스, 생태계 성장, 파트너십, 보조금 등을 위해 토큰의 상당 부분을 보유한다. 이러한 토큰은 자유롭게 거래되지 않기 때문에 유통 중인 것으로 간주되지 않는다.
DAO가 투표나 인센티브 프로그램을 통해 이 토큰을 배포하기 전까지는 비유통 상태로 계산된다.

각주 (Footnotes)

- 1. 이 컨트랙트들은 CoW DAO에 의해 개발되거나 배포된 것이 아니며, Ethereum의 정식 토큰을 각 체인으로 브릿한 버전이다. Gnosis Chain은 Omni Bridge, Arbitrum One은 Arbitrum Bridge, Base는 Superbridge, Polygon은 Polygon Bridge를 사용한다.

수수료 (Fees)

Note
본 문서는 CoW Protocol의 수수료에 대한 내용을 다룬다.
MEV Blocker에 연결된 빌더들도 별도의 수수료를 지불하며, 이에 대한 내용은 별도로 설명되어 있다.

CIP-34는 CoW DAO 핵심 팀이 CoW Protocol을 통한 수익 창출을 위해 6개월간의 수수료 모델 테스트를 수행하도록 지시한다 (2024년 1월 16일 시작). 또한 핵심 팀은 테스트 진행 상황을 DAO에 지속적으로 보고해야 한다.

이 페이지의 목적은 사용자가 CoW Protocol(CoW Swap 포함)을 사용할 때 어떤 수수료 모델이 활성화 상태인지 그리고 어떤 수수료를 적용받는지 명확히 이해할 수 있도록 하는 것이다.

현재 수수료 (Current Fees)

시장가 외 지정가 주문에 대한 서플러스 수수료 (Surplus fee on out-of-market limit orders)

정의: 시장가 외(out-of-market) 지정가 주문의 서플러스 중 50%, 단 총 주문 금액의 1%를 상한으로 함

적용 대상: 생성 시점에 즉시 실행 불가능한 시장가 외 지정가 주문 및 개별 TWAP 주문

수수료 계산식:



$$surplus * 0.5 \text{ 또는 } volume * 0.01 \text{ 중 더 낮은 값}$$

시장가 주문에 대한 견적 개선 수수료 (Quote improvement fee on market orders)

정의: 시장가 주문(스왑)의 긍정적 견적 개선분의 50%, 단 총 주문 금액의 1%를 상한으로 함

적용 대상: 사용자가 최초 견적보다 더 나은 가격을 받은 모든 시장가 주문(시장가 지정가 및 TWAP 주문 포함)

수수료 계산식:



$$quote \text{ improvement} * 0.5 \text{ 또는 } volume * 0.01 \text{ 중 더 낮은 값}$$

Gnosis 체인 주문에 대한 거래량 수수료 (Volume fee on Gnosis Chain orders)

정의: 상관된 가격을 가진 토큰 페어를 제외한 주문 총액의 10bps (0.1%)

적용 대상: Gnosis Chain에서 실행되는 모든 시장가, 지정가, TWAP 주문 중 상관된 가격 관계에 있는 토큰 간 거래를 제외한 모든 주문

수수료 계산식:



$$volume * 0.001$$



Note

Surplus(서플러스) = 주문의 실행 가격과 최소 실행 가격의 차이

Quote improvement(견적 개선) = 주문의 실행 가격과 견적 가격의 차이 (단, 양수일 때만 적용. 음수일 경우 수수료 부과 없음)

파트너 수수료 (Partner fees)

CoW Protocol을 통합하는 파트너는 자체 수수료를 부과할 수 있다. 파트너 수수료 계산 방법, 예시, 지급 절차는 [파트너 수수료 문서](#)에서 확인할 수 있다.

파트너 수수료 계산 (Partner Fee Calculation)

파트너 수수료는 CoW Protocol과의 통합을 통해 거래된 모든 트랜잭션 중, appData에 정의된 Partner Fee 비율을 거래 총액에 곱해 계산된다.

주문별 파트너 수수료는 주문의 서플러스 토큰(즉, 매도 주문의 경우 구매 토큰, 매수 주문의 경우 판매 토큰) 기준으로 계산되며, 정산 시 외부 가격 제공자를 통해 WETH로 변환된다.

CoW Protocol은 전체 파트너 수수료 중 일정 비율을 서비스 수수료(Service Fee)로 유지한다. [CIP-61](#)에 따라 기본 서비스 수수료율은 총 파트너 수수료의 50%이며, CoW DAO를 대표해 핵심 팀과의 협상으로 조정할 수 있다.

서비스 수수료를 제외한 순수익(Net Partner Fee)은 매주 지급 대상이 된다. 자세한 계산 예시는 아래에 나와 있다.

Note

파트너는 위젯을 통해 사용자에게 최대 100bps(1%)까지의 거래 수수료를 부과할 수 있다. Partner Fee는 2024년 4월 4일(파트너 수수료 기능 출시일)부터 누적되며, 현재는 위젯을 통한 시장가 주문 거래에만 적용된다.

파트너 수수료 계산 예시 (Partner Fee Calculation Examples)

예시 1: 사용자가 위젯에서 1 ETH를 DAI로 매도 (A User Sells 1 ETH for DAI on your Widget)

- Partner Fee: 100 BPS
- 사용자에게 제시된 견적:
 - 예상 매도량: 0.995 ETH
 - 예상 가스비: 0.005 ETH
 - 총 매도량: 1 ETH
 - 매수량: 3,500 DAI
- 슬리피지 = 0%

사용자 서명 주문 (Partner Fee 통합):

- 원시 매도량: 1 ETH
- 원시 수수료: 0 ETH (모든 주문은 기본적으로 0 수수료로 서명)
- 최소 매수량: 3,465 DAI (= 3,500 - 3,500 * 0.01)

실행 결과:

- 슬버는 0.003 ETH를 가스로 사용하고 0.997 ETH를 매도하여 3,525 DAI를 획득 (60 DAI 서플러스 발생)
 - 파트너 수수료: 35.25 DAI (3,525 * 0.01)
 - 사용자 수령액: 3,489.75 DAI (3,525 - 35.25)
 - 사용자 서플러스: 24.75 DAI (3,489.75 - 3,465)

예시 2: 사용자가 위젯에서 1 ETH를 DAI로 매수 (A User Buys 1 ETH for DAI on your Widget)

- Partner Fee: 100 BPS
- 사용자에게 제시된 견적:
 - 예상 매도량: 3,520 DAI
 - 예상 가스비: 30 DAI
 - 총 매도량: 3,550 DAI
 - 매수량: 1 ETH
- 슬리피지 = 0%

사용자 서명 주문 (Partner Fee 통합):

- 최대 매도량: 3,585.5 DAI ($3,550 + 3,550 * 0.01$)
- 원시 수수료: 0 DAI
- 매수량: 1 ETH

실행 결과:

- 슬버는 20 DAI를 가스로 사용하고 1 ETH를 3,500 DAI에 매수 (65.5 DAI 서플러스 발생)
 - 파트너 수수료: 35.2 DAI ($3,520 * 0.01$)
 - 사용자 지불액: 3,555.2 DAI ($3,520 + 35.2$)
 - 사용자 서플러스: 30.3 DAI ($3,585.5 - 3,555.2$)

파트너 수수료 지급 절차 (Partner Fee Payment Process)

1. 위젯에 Partner Fee 파라미터 구현을 완료하면, 위젯을 통한 사용자 거래에 대해 Partner Fee를 받을 자격이 부여된다.
2. 주간 단위로 데이터 스크립트를 실행해 프로젝트의 AppKey를 기반으로, appData에 정의된 Partner Fee가 있는 모든 거래를 집계한다.
3. 계산된 순수익(Net Partner Fee) 금액이 위젯의 “Recipient” 파라미터에 명시된 이더리움 지갑 주소로 주간 단위로 전송된다.

Note
누적된 수수료 금액이 0.001 WETH 이상이어야 지급이 이루어진다. 그보다 적은 금액은 무효 처리된다.

CoW 보조금 프로그램 개요 (CoW Grants Program Overview)

CoW Grants Program (CGP)은 [CoW DAO의 미션 스테이트먼트](#)에 따라 CoW Protocol 생태계의 성장을 지원하는 이니셔티브를 자금 지원한다.

현재 권한 (Current Mandate)

이 보조금 프로그램은 2025년 1월에 승인된 [CIP-63](#)에 따라 운영된다. 주요 내용은 다음과 같다:

- 보조금 활동을 위한 예산: 600,000 xDAI 및 1,465,260 COW
- 거래량 기반 보조금(Volume Grants) 예산: 4,990,000 COW 추가 할당
- 운영 기간: 2026년 1월 31일까지

중점 분야 (Focus Areas)

CoW Grants Program은 다음 주요 분야에 집중한다:

- 커뮤니티 성장: 활성 사용자 기반 확장 및 커뮤니티 참여 강화
- UI/UX 개선: 사용자 인터페이스 및 경험 향상
- 탈중앙화: 네트워크 회복력 강화 및 커뮤니티 참여 확대
- 솔버 생태계: 새로운 솔버 및 최적화 알고리즘 개발 지원
- 개발자 도구: SDK 및 빌더용 리소스 개발
- 통합: 파트너십 구축 및 프로토콜 오더 플로우 확보
- 혁신: 생태계에 이익이 되는 새로운 아이디어 지원

위원회 구조 (Committee Structure)

보조금 위원회는 총 5명(커뮤니티 구성원 3명 + 핵심 팀 구성원 2명)으로 구성되며, 4/5 다중 서명(multisig) 구조로 운영된다. 위원회는 제안서를 평가하고, 스튜어드 및 리뷰어를 지정하며, 보조금의 전체 라이프사이클을 감독한다.

운영 방식은 CIP-63에서 승인된 최신 구조를 따르며, DAO의 감독 하에 효율적인 운영이 가능하도록 설계되어 있다.

탐색 (Navigation)

- [How to Apply](#) – 신청 절차 및 가이드라인
- [Grant Types](#) – 지원 가능한 보조금 유형
- [Program Structure](#) – 거버넌스 및 운영 세부사항

보조금 신청 방법 (How to Apply for a Grant)

이 페이지는 신청 절차 개요를 제공한다. 전체 세부사항은 포럼의 [공식 프로세스 가이드](#)를 참고하라.

신청 단계 (Application Steps)

1. 기존 자료 검토

- [프로세스 가이드](#) 및 [보조금 계약 조건](#) 확인
- [보조금 프로그램 포럼 섹션](#)에서 유사한 과거 제안서 검토
- 아이디어가 필요하다면 [RFP 템플릿](#) 참고

2. 포럼에 제안서 작성

- [CoW Grants Program](#) 섹션으로 이동
- “New Topic” 클릭 후 [보조금 신청 템플릿](#) 사용
- 필수 항목 및 명확한 자금 요청 포함

3. 피드백 수용

- 커뮤니티 및 위원회의 질문에 응답
- 논의에 따라 제안서 수정
- 스튜어드가 배정된 경우, 협업하여 제안서 보완

4. Snapshot 제출

- 충분한 논의 후 [Snapshot](#)에 제안서 제출
- 포럼 논의 링크 및 최종 제안서 포함
- [CoW DAO 보조금 계약서](#) 링크 추가

5. 투표 절차

- 투표 기간: 3일
- 위원회 구성원이 평가 기준에 따라 투표
- Snapshot 링크를 포럼 게시물에 업데이트

평가 기준 (Evaluation Criteria)

제안서는 다음 기준에 따라 평가된다:

1. 실현 가능성(Feasibility): 현재 CoW Protocol 생태계 단계에서 구현 가능한가?
2. 영향력(Impact): 프로젝트가 CoW 생태계에 미칠 긍정적 효과는 어느 정도인가?
3. 작업량 추정(Workload estimation): 시간 및 자원 예측이 현실적인가?
4. 기술 전문성(Technical expertise): 제안한 결과물을 달성할 충분한 역량과 경험이 있는가?

승인 후 절차 (After Approval)

보조금이 승인되면 다음 단계로 진행된다:

1. 스튜어드가 지정되지 않았다면 새로 배정됨
2. 마일스톤 또는 시간 기반 약속에 따라 결과물을 제공해야 함
3. 마일스톤 완료 후 포럼을 통해 리뷰 요청
4. 검토 후 매월 말에 지급 처리

문의 및 지원 (Contact and Support)

보조금 프로그램 관련 문의:

- [CoW Grants Program](#) 포럼 섹션에 게시
- [CoW Protocol Discord](#)의 #grants 채널 방문

보조금 유형 (Grant Types)

CoW Grants Program은 다양한 프로젝트 필요에 맞는 여러 형태의 보조금을 제공한다. 차이를 이해하면 제안서에 적합한 구조를 선택할 수 있다.

마일스톤 기반 보조금 (Milestone-Based Grants)

명확한 결과물과 성과가 정의된 프로젝트에 적합하다.

주요 특징:

- 특정하고 측정 가능한 결과물을 기준으로 구성
- 각 마일스톤 달성 시 지급
- 개발, 통합, 연구 등 명확한 결과물이 있는 프로젝트에 적합
- 각 단계는 상세한 설명, 결과물, 기한, 자금액을 포함

선택 시점:

- 프로젝트의 결과물이 명확하고 측정 가능할 때
- 작업을 단계별로 구분할 수 있을 때
- 특정 목표 달성에 따라 자금이 필요한 경우

시간 기반 보조금 (Time-Based Grants)

특정 결과물보다는 일정 기간 동안의 기여를 기준으로 한다.

주요 특징:

- 구체적 결과물보다 시간과 노력에 기반
- 지속적 역할, 유지보수, 자문 등에 적합
- 시간(시간/일/월 단위)으로 구조화 가능
- 명확한 업무 범위 및 책임 정의 필요

선택 시점:

- 기여가 지속적이거나 유지보수 성격일 때
- 특정 산출물보다 꾸준한 참여에 가치가 있을 때
- 유연성이 필요한 역할일 때

하이브리드 보조금 (Hybrid Grants)

일부 프로젝트는 두 구조를 결합한 방식이 더 적합하다.

주요 특징:

- 고정된 결과물 + 지속적 시간 기여 결합
- 명확한 산출물과 유연한 기여를 병행 가능
- 마일스톤 기반 부분과 시간 기반 부분을 명확히 구분해야 함

제안서에는 선택한 보조금 유형을 명확히 명시해야 하며, 승인 과정에서 최종 확정된다.

보너스 지급 (Bonus Allocations)

CIP-63에 따라 위원회는 탁월한 성과를 낸 수혜자에게 재량 보너스를 지급할 수 있다.
보너스의 특징은 다음과 같다:

- 보너스 한도: 보조금당 10,000 xDAI 또는 이에 상응하는 COW
- 추가 마일스톤이나 결과물 불필요
- 위원회 재량으로 수여
- 탁월한 성과, 생태계 기여, 효율적 실행 등에 대해 수여 가능

자세한 보조금 유형 및 요구사항은 [CoW DAO 보조금 계약서](#)를 참고하라.

프로그램 구조 (Program Structure)

CoW Grants Program은 [CIP-63](#)에 정의된 구조화된 거버넌스 프레임워크 하에서 운영된다.

위원회 구성 (Committee Composition)

Grants Committee는 5명의 구성원으로 이루어진다:

커뮤니티 구성원 3명 (3 Community Members):

- @Kubesqrt
- @Chim9
- @mfw78

코어 팀 구성원 2명 (2 Core Team Members):

- @middleway.eth
- @Master_CoW

위원회는 보조금 승인에 4/5 정족수가 필요한 Gnosis Safe로 운영된다.

위원회 역할 (Committee Roles)

각 위원은 다음 역할 중 하나 이상을 맡을 수 있다:

테크니컬 리드 (Technical Lead)

- 보조금 신청서의 기술적 평가 수행
- 기술 인프라 관리
- 스튜어드와 그란티에게 기술적 가이드 제공

그랜트 스튜어드 (Grant Steward)

- 배정된 그란티의 주요 연락 창구 역할
- 보조금 마일스톤 모니터링 및 평가
- 안전하고 적시의 지급 실행 지원
- 커뮤니티를 위한 그란티 업데이트 취합

그랜트 모더레이터 (Grant Moderator)

- 신청서 스크리닝 및 적시 리뷰 보장
- 커뮤니케이션 채널 모니터링

- 프로세스의 질서와 투명성 유지

세이프 구조 (Safe Structure)

2025년 2월 업데이트 기준, Grants DAO는 간소화된 Safe 구조로 운영된다:

- Grants Committee Safe (0xCA1F000D520C21C47E6C34DD31b92b91A63B8bD) ([Gnosisscan](#))
가 보조금 집행을 직접 관리
- CoW DAO는 Committee Safe의 최종 실소유자(UBO) 역할을 수행
- 이 구조는 DAO의 감독을 유지하면서 운영 효율성을 향상

의사결정 프로세스 (Decision Making Process)

1. 보조금 제안이 포럼에 제출됨
2. 위원회가 스튜어드와 리뷰어를 지정
3. 커뮤니티 토론 및 피드백 진행
4. 제안이 Snapshot으로 이동하여 공식 투표 진행
5. 위원회 4/5 승인 시, 보조금 집행

보조금 라이프사이클 관리 (Grant Lifecycle Management)

각 승인된 보조금에 대해:

- 스튜어드가 진행 상황을 감독
- 리뷰어(내부 또는 외부)가 기술 마일스톤 평가
- 월간 지급 사이클로 승인된 마일스톤 지급 처리
- 정기 업데이트를 커뮤니티에 공유

커뮤니케이션 및 리소스 (Communication and Resources)

- 포럼(Forum): [Grants Program Forum Section](#)이 주요 커뮤니케이션 채널
- 디스코드(Discord): CoW Protocol Discord의 #grants 채널은 보조 채널로 사용
- 스냅샷(Snapshot): 모든 공식 투표는 [Grants Program Snapshot Space](#)에서 진행

프로그램 구조에 대한 질문은 포럼의 grants 섹션에 게시하라.

거버넌스 프로세스 (Governance Process)

이 사이트는 CoW DAO의 현재 거버넌스 구조를 나타낸다.

GOVERNANCE EVOLUTION

CoW DAO의 거버넌스는 CoWmunity가 소유개발 집행한다. 따라서 이 문서는 살아 있는 문서로 간주되며, CoW DAO가 발전함에 따라 업데이트된다.

이 문서는 CoW DAO를 발전시키기 위한 프로세스를 개요한다. 이 프로세스의 목적은 논의를 촉발하고 커뮤니티가 제안을 검토하고 투표할 수 있도록 필요한 정보와 충분한 시간을 제공하는 데 있다.

CoW DAO 개선 제안(CIP) (CoW DAO Improvement Proposals (CIPs))

CoW DAO 거버넌스의 핵심은 CoW DAO 개선 제안(CIP) 프로세스다. CIP는 신규 기능 제안, 특정 이슈에 대한 커뮤니티 의견 수렴, CoW DAO에 반영된 설계 결정을 문서화하는 주요 메커니즘이다.

CoW DAO에 유의미한 변화를 제안할 때는 CIP를 생성하는 게 모범 사례다. 이는 커뮤니티가 변경 사항을 인지하고, 반영 전에 피드백을 제공할 기회를 확보하는 데 도움이 된다.

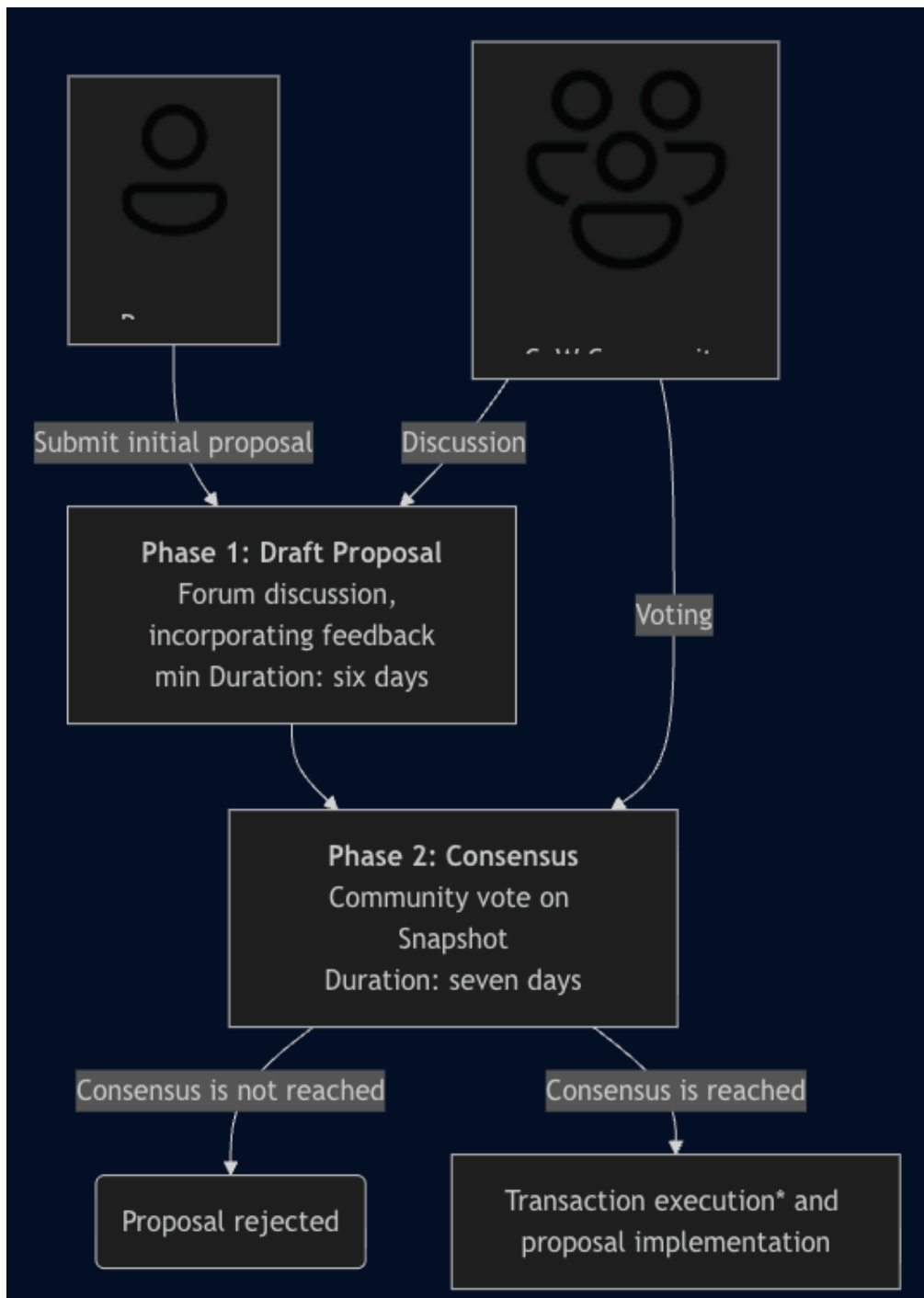


CIP 템플릿 (CIP TEMPLATE)

CIP를 작성하려면 [CIP 템플릿](#)을 참고하라.

방법론 (Methodology)

CoW DAO 거버넌스 프로세스는 제안 승인까지 두 단계로 구성된다:



(*) 참고: 온체인 자동 집행을 위한 oSnap 모듈을 사용하면, 실제 트랜잭션 집행에 3일 지연이 추가된다.

1단계: 커뮤니티 토론 (Phase 1: Community Discussion)

최소 기간: 6일

첫 단계에서는 초안 제안이 생성되어 포럼에 게시된다. 초안 단계의 목적은 잠재적 제안에 대한 공식적인 논의를 수립하는 것이다.

초안 제안 생성 절차:

- Governance 카테고리에 새 주제를 만들고, Governance Resources 카테고리 상단에 고정된 proposal

template을 사용

- 제안에 대한 지지를 구축하기 위해 토론에 참여
- 제안에 CoW DAO의 온체인 상호작용이 포함된다면, 초안 단계에서 제안의 코드를 작성해야 함
Tenderly 트랜잭션 시뮬레이션 제공은 필수

제안이 안정적 상태라고 확신되고, 최초 게시 이후 최소 기간이 경과하면, 제안자는 스스로 다음 단계로 이동시킬 수 있다.

참고: 일부 패스트트랙 제안은 포럼에서 72시간(3일)만 요구되어 6일 규칙에서 예외다. 여기에는 EBB0 위반으로 인한 슬래싱 제안(예: CIP-52 참고)이 포함된다.

2단계: 투표 (Phase 2: Voting)

투표 기간: 7일

- 10,000 COW 초과 보유자는 1단계 요건을 충족할 경우 CIP를 Snapshot에 게시할 수 있다.
- CIP 번호를 CIP-### 형식으로 부여
- 주제 상태를 *Draft Proposal*에서 *Active Proposal*로 변경
- 7일 기간의 Snapshot 투표를 생성하고, Snapshot 및 포럼 게시글을 상호 링크
- 집행 가능한 트랜잭션이 포함된 경우, 과정의 일부로 oSnap Snapshot 모듈에 트랜잭션을 생성
- 진행 전 제안을 면밀히 검토하고, 가능하면 다른 커뮤니티 구성원에게 리뷰를 요청

참고: CoW DAO의 oSnap 적용은 투표가 성공적으로 종료된 후 집행까지 3일 지연을 추가한다.

프로세스 개선 (Process Improvement)

위의 프로세스는 개선 가능하다. 제안이 있으면 포럼의 Governance 카테고리에 게시하라. 거버넌스 효율성 및/또는 탈중앙화를 높이는 제안은 환영하며, CoW Protocol은 보다 커뮤니티 소유·탈중앙화된 모델로 나아간다.

CIP 템플릿 (CIP Template)

 이 템플릿은 새로운 CoW DAO 개선 제안을 작성할 때 사용한다.

Note

CIP 번호는 제안이 2단계로 이동할 때 포럼 모더레이터가 할당한다. CIP 제출을 위한 주제 생성 시 다음과 같이 명명하라. CIP-draft: title

```

# CIP-Draft: Template

CIP: <to be assigned when moved to phase 2>
title: <CIP title>
author: <a list of the authors name(s) and/or username(s), email(s)>
status: Draft
created: <date created on, in ISO 8601 (yyyy-mm-dd) format>
requires (*optional): <CIP number(s)>
replaces (*optional): <CIP number(s)>

## Simple Summary

If you can't explain it simply, you don't understand it well enough. Provide a
simplified and layman-accessible explanation of the CIP.

## Motivation

The motivation is critical for gathering support within the community. Please
explain how your CIP is intended to advance CoW DAO and / or CoW Protocol, and
how it's aligned with CoW DAO's values.

## Specification

The technical specification should describe the syntax and semantics of any new
feature. The specification should be detailed enough to allow for it to be
reasoned about by participants in the CoW DAO.

## Rationale

The rationale fleshes out the specification by describing what motivated the
design and why particular design decisions were made. It should describe
alternate designs that were considered and related work. The rationale may also
provide evidence of consensus within the community, and should discuss
important objections or concerns raised during discussion.

## Execution

### Safe Transaction Data

Mandatory for every proposal that requires transaction from CoW DAO.

```
<payload>
```

### Tenderly Simulation

Mandatory for every proposal that requires transaction from CoW DAO.
Link to Tenderly simulation

## Snapshot

Phase 2 Proposal: Add a link to the corresponding CoW DAO Snapshot poll you've
created.

```

멀티시그 (Multisigs)

CoW DAO는 자금 및 운영 관리를 위해 Safe를 사용한다. 현재 배포된 세이프는 다음과 같다:

| 이름 | 설명 | 체인 |
|---|--|---------|
| CoW DAO | 0xCA771eda0c70a7d053aB1B2504559B918FE662
cow.eth 스냅샷 공간의 CoW 토큰 보유자 투표에 연동된 메인 DAO 세이프 | Mainnet |
| CoW DAO (USDC) | 0xA1cb7762f40318ee0260F53e15De835fF001cb7E
USDC 보관 전용, CoW DAO가 관리하는 세이프 | Mainnet |
| Solver payouts | 0xA03be496e67Ec29bC62F014a2B683D7F9c204930
DAO가 정의한 solver accounting rules 에 따라 솔버 지급 실행; 정산 컨트랙트에서 수집된 수수료 수령 | Mainnet |
| Solver controller | 0x423cEc87f19F0778f549846e8010Ee267a917935
DAO가 정의한 솔버 본딩 규칙에 따라 정산 컨트랙트의 허용 목록에 솔버 추가/제거; 수집된 프로토콜 수수료를 ETH로 변환 | Mainnet |
| CoW Treasury | 0x61d6E58c011f873f6a2c07Ac53527f6Fb9F06969
유휴 금고 자금의 수익 생성을 위해 Karpatkey DAO의 지원과 함께 관리 | Mainnet |
| CoW DAO (GC) | 0xCA771eda0c70a7d053aB1B2504559B918FE662
Gnosis Chain의 CoW DAO 메인 세이프 | GC |
| Grants Committee | 0xCA1F000D520c21C47E6c634DD31b92b91A63B8bd
7명의 위원회 구성원이 관리, CoW Grants 자금 집행 담당 | GC |
| Grants Funds | 0xDA0000B03dC0fC35d968e4451Ebed6e5950d63e
CoW DAO와 Grants Committee가 공동 관리, CoW DAO의 보조금 자금 회수(clawback) 가능 | GC |
| Grant Funds (Volume-based Partner Reward Program - COW) | 0xbd96CF4E53f1dA89a8bD3522BCEDfB2b056016b9
CoW DAO와 Grants Committee가 공동 관리, CoW DAO의 보조금 자금 회수(clawback) 가능 | GC |

스냅샷 (투표) (Snapshot (Voting))

CoW DAO는 [Snapshot](#)을 사용하여 [CoW DAO 개선 제안\(CIP\)](#)에 대한 투표를 진행한다. 스냅샷에서의 투표 가중치는 스냅샷 전략에 의해 결정되며, 보유 또는 위임된 vCOW + COW 수량에 비례한다.

투표 요건 (VOTING REQUIREMENTS)

제안이 통과하려면, 단순 과반의 YES 표와 35,000,000 표의 정족수를 충족해야 한다.

설정 (Settings)

| 파라미터 | 값 |
|-------------|------------|
| vote.type | Basic |
| vote.quorum | 35,000,000 |
| vote.period | 7 days |



Tip:

스냅샷 설정 변경은 *cow.eth*의 *snapshot* 텍스트 레코드를 변경하는 CIP가 필요하다.

Note:

설정은 IPFS에 저장된 JSON 파일에 위치하며, 해당 해시는 *cow.eth*의 *snapshot* 텍스트 레코드에 참조된다. JSON 파일은 GitHub 리포지토리에서 관리된다.

ENS 네임 컨트롤러 (ENS name controller)

Snapshot 공간은 ENS 이름에 연결된다. CoW DAO의 경우 *cow.eth*다. ENS 이름 컨트롤러 지정 방법은 원하는 컨트롤러의 주소를 *snapshot* 텍스트 레코드에 추가하는 것이다.

역할 (Roles)

슈퍼 어드민 (Super admin)

슈퍼 어드민은 작성자/관리자 추가, 전략 변경 등 공간의 모든 파라미터를 제어할 수 있다. 슈퍼 어드민 역할은 ENS 네임 컨트롤러가 부여하며, 현재 설정은 [CoW DAO 메인 세이프](#)다.

일반 관리자 (Regular admins)

[일반 관리자](#)는 슈퍼 어드민이 할 수 있는 대부분을 수행할 수 있으나, 관리자 추가/제외는 불가하다. CIP-31 기준, CoW DAO의 스냅샷 공간에는 슈퍼 어드민인 [CoW DAO 메인 세이프](#) 외에 관리자가 없다.

모더레이터 (Moderators)

모더레이터는 제안 생성·삭제가 가능하지만 공간 파라미터는 변경할 수 없다. CIP-31 기준, 스팸 제안 제거를 담당하는 커뮤니티 모더레이터 3명이 있다.

작성자 (Authors)

작성자는 공간 파라미터를 변경할 수 없지만 제안을 생성할 수 있다. CIP-31 기준, CoW DAO의 스냅샷 공간에는 작성자가 없다. [거버넌스 프로세스](#)에 따라 최소 10K COW를 보유한 누구나 스냅샷에 제안을 생성할 수 있다.

스냅샷 전략 (Snapshot strategies)

CoW DAO는 민주적이고 공정한 투표를 위해 포괄적인 스냅샷 전략을 구현한다. 이 전략은 ERC-20 COW와 vCOW 토큰의 잔액을, 체인 및 위임 상태를 포함해 다면적으로 반영하는 8개 전략의 조합을 사용한다.

| 전략 번호 | 전략 설명 | 토큰 유형 | 체인 | 위임 상태 |
|-------|------------------------------------|-------|------------------|-------|
| 1 | Balance of ERC-20 & vCOW | vCOW | Ethereum Mainnet | No |
| 2 | Balance of ERC-20 & vCOW | vCOW | Gnosis Chain | No |
| 3 | Balance of delegated ERC-20 & vCOW | vCOW | Ethereum Mainnet | Yes |
| 4 | Balance of delegated ERC-20 & vCOW | vCOW | Gnosis Chain | Yes |
| 5 | Balance of ERC-20 & COW | COW | Ethereum Mainnet | No |
| 6 | Balance of ERC-20 & COW | COW | Gnosis Chain | No |
| 7 | Balance of delegated ERC-20 & COW | COW | Ethereum Mainnet | Yes |
| 8 | Balance of delegated ERC-20 & COW | COW | Gnosis Chain | Yes |

CoW DAO 구성원의 총 투표권은 8개 전략 전반의 잔액 합계다. 이 시스템은 vCOW와 COW, 그리고 그 위치와 위임 상태를 불문하고 모든 토큰이 거버넌스에 기여하도록 보장한다. 베스팅된 토큰과 유동 토큰을 모두 고려하고 각자의 위임 선택을 반영함으로써, CoW DAO는 개인의 기득권과 참여를 온전히 스냅샷한다. 이 포괄적 접근은 각 이해관계자의 목소리가 집단적 의사결정에서 정확히 반영되도록 하려는 CoW DAO의 포용적·대표성 있는 거버넌스 의지를 보여준다.

현재 배포된 투표 전략은 [여기](#)에서 확인할 수 있다.