

디라이브(Derive)

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.

초록

본 논문에서는 OP Stack 기반 Ethereum 롤업인 Derive L2에서 동작하는 범용 리스크 엔진인 Derive Protocol을 소개한다. 이전 버전을 근본적으로 재설계한 Derive Protocol은 트레이더에게 자본 효율적이고 모듈화되며 빠르게 업그레이드 가능한 플랫폼을 제공하는 동시에, 사용자가 자신의 자산에 대한 셀프 커스터디를 유지할 수 있도록 한다.

1. 소개

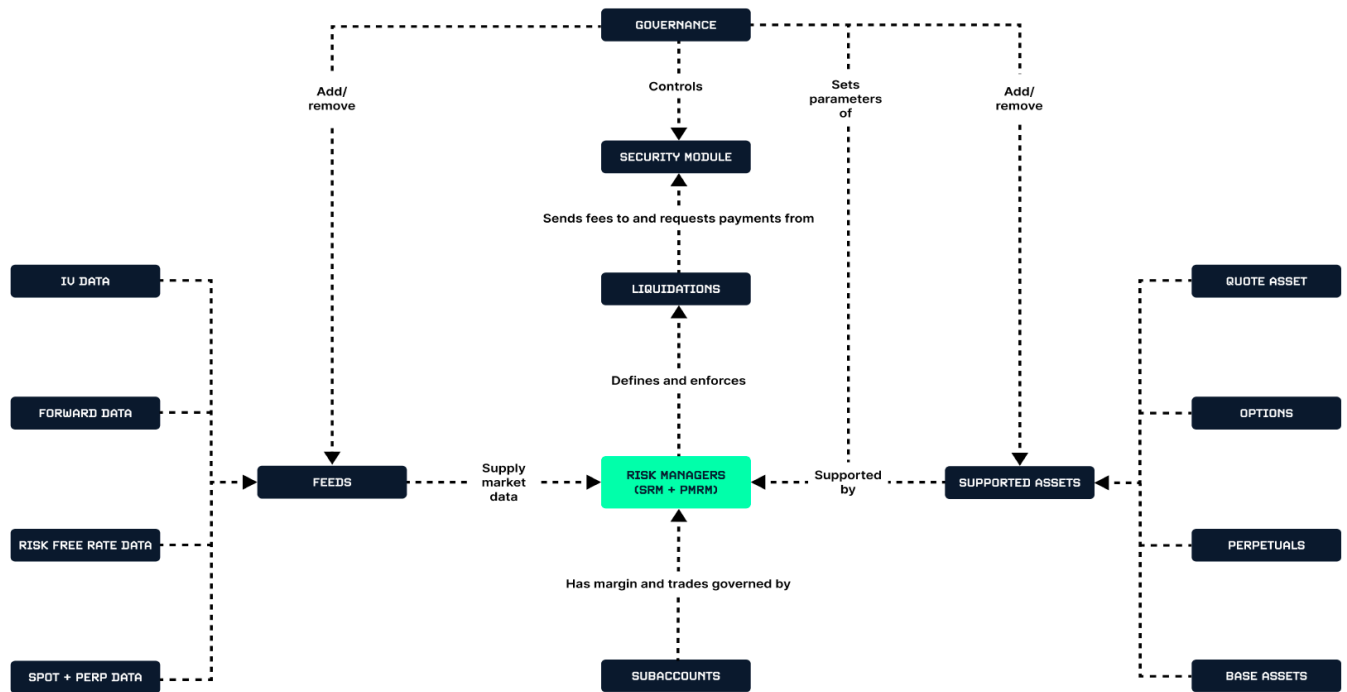
2021년 출시 이후 Lyra V1 [1]과 이후 업데이트인 Avalon 및 Newport는 15억 달러 이상의 명목 거래량을 기록하며 탈중앙화 옵션 거래소를 선도해 왔다.

이는 놀라운 성과이지만, 이러한 수치를 전통 금융 시장과 비교하면 겸손해질 수밖에 없다. 이러한 거래소들의 거래량은 일반적으로 하루 수백억 달러, 많게는 수천억 달러에 이른다. 따라서 Derive의 거래량은 중앙화 거래소와 경쟁하기 위해 현재보다 몇 단계 이상의 규모로 성장해야 한다.

본 논문에서는 Derive Protocol, 즉 V2를 상세히 설명한다. 이는 Lyra를 근본적으로 재설계한 버전으로, 우리가 믿기에 공정하고 민주적이며 탈중앙화된 금융 시스템의 기반이 되어 전통적인 금융 기관과 경쟁할 수 있을 것이다.

Derive Protocol의 핵심 특징은 다음과 같다.

- **범용 리스크 엔진(Generalized Risk Engine):** 모든 금융 상품(옵션, 만기 선물(Dated Futures), 바이너리 옵션 등)을 Derive Protocol에서 거래하고, 증거금을 관리하며, 정산하고, 청산할 수 있다. 출시 시점에는 유럽형 옵션(자본 효율적인 스프레드 포함), 무기한 선물(Perpetual Futures), 현물 자산(Spot Assets)을 지원한다.



- **자본 효율성(Capital Efficiency):** 출시 시점부터 정교한 증거금(Margin) 산정 방식을 제공하여 이전 버전에 비해 자본 효율성을 크게 향상시킨다.
- **모듈성(Modularity):** Derive의 스마트 컨트랙트는 계정 구조, 리스크 관리 및 다양한 지원 자산과 같은 핵심 기능을 정의한다. 이러한 구성 요소들은 이전 Lyra 버전보다 훨씬 쉽게 교체하거나 확장하여 구축할 수 있다.

2. 프로토콜

Derive Protocol은 DAO의 거버넌스를 받는 OP Stack 기반 Ethereum 롤업인 Derive L2 상에서 동작하는 스마트 컨트랙트들의 집합이다. 프로토콜은 크게 **서브어카운트(Subaccounts)**, **매니저(Managers)**, **자산(Assets)**의 세 가지 주요 구성 요소로 이루어진다.

프로토콜은 모듈식 구조로 설계되어 있어 빠른 반복 개발이 가능하며, 이러한 각 계층은 시간이 지남에 따라 더욱 개선될 예정이다. 프로토콜의 시각적 구조는 그림 1을 참고하라.

3. 서브어카운트(Subaccounts)

서브어카운트는 Derive Protocol의 기본 단위이다. 모든 사용자는 허가 없이(permissionlessly) 자신만의 서브어카운트를 발행할 수 있으며, 이 서브어카운트에는 지원되는 모든 자산이 저장된다. 또한 서브어카운트 내의 모든 자산은 아래에서 설명하는 하나의 매니저에 의해 관리된다.

서브어카운트는 ERC-721을 준수하는 NFT이며, 다음과 같은 형태의 목록을 저장한다.

```
{asset, subId, balance}
```

여기서,

- **asset**은 금융 상품의 기본 속성(예를 들어 옵션은 행사가를 가져야 한다는 사실 등)을 정의하는 규칙을 인코딩한 스마트 컨트랙트이다. Asset은 확장 가능하며 어떠한 목적에도 맞게 프로그래밍할 수 있다. 예를 들어 만기 선물(Dated Futures)이나 바이너리 옵션 자산도 추후 추가될 수 있다.
- **subId**는 금융 상품을 완전히 정의하는 데 필요한 매개변수를 지정하는 고유 식별자이다. 예를 들어 옵션의 subId에는 행사가(Strike), 만기(Expiry), 그리고 콜(Call)인지 풋(Put)인지에 대한 정보가 포함된다.
- **balance**는 해당 금융 상품의 순잔고(Net Balance)이다. 이는 양수(크레딧)일 수도 있고 음수(부채)일 수도 있다.

서브어카운트 컨트랙트는 두 가지 주요 기능을 가진다.

1. 권한이 있는 주체(사용자, 매니저)만이 서브어카운트의 잔고를 변경할 수 있도록 보장한다.
2. 서브어카운트와 관련된 모든 거래에 대해 관련된 모든 주체에게 이를 알린다.

이는 **후크(hooks)**의 사용을 통해 가능해졌다. 후크는 자산 이전(asset transfer) 도중 및 이후에 관련 컨트랙트로 호출되는 외부 함수 호출이다. 후크는 다음과 같다.

- **asset hook**: 자산(asset)을 호출하여 이전을 검증하고 최종 잔고를 결정한다. 예를 들어 자산 컨트랙트는 이전 이벤트에 대해 누적된 이자를 적용하거나 마지막 이자 지급 이후 경과한 시간을 추적할 수 있다.
- **manager hook**: 매니저(manager)를 호출하여 서브어카운트의 최종 상태를 검증한다. 매니저는 최종 상태를 유효하지 않게 만드는 이전을 되돌림(revert)으로써 다양한 규칙을 강제할 수 있다. 서브어카운트의 매니저는 증거금 요구사항을 계산하기 위해 오라클이나 자산 컨트랙트로부터 필요한 모든 데이터를 읽을 수 있다.

이러한 아키텍처는 서로 다른 매니저와 자산이 다양한 서브어카운트 동작에 대해 고유한 검증 규칙을 생성할 수 있는 유연성을 제공한다.

4. 자산(Assets)

자산 컨트랙트는 이전(transfer), 거래(trade), 입금(deposit), 출금(withdrawal), 또는 정산(settlement)의 결과를 결정하는 역할을 담당한다. 입금과 출금뿐 아니라 이자의 누적을 지원하기 위해 자산은 모든 서브어카운트에서 자신의 잔고를 직접 업데이트할 수 있는 권한을 가진다.

자산과 매니저는 서로 연결되어 있으며, 특정 자산은 특정 매니저에서만 지원되고 그 반대도 마찬가지이다. 이는 자산이 여러 매니저 간에 대체 가능(fungible)할 수도 있음을 의미한다. 이러한 관계는 앞서 설명한 후크를 통해 유지된다.

출시 시점에는 네 가지 유형의 자산이 제공된다.

- **cashAsset:** 각 매니저는 하나의 cashAsset(예: USDC)을 지원한다. 이는 일반적으로 **기준 자산(quote asset)** 이라고 불린다.
- **option:** 특정 기초자산(Underlying Asset)에 대한 유럽형 옵션.
- **perp:** 특정 기초자산에 대한 무기한 선물(Perpetual Futures). 다른 거래소와 달리 무기한 선물은 사용자가 언제든지 정산할 수 있다. 이를 **연속 정산(continuous settlement)** 이라고 한다. 또한 사용자가 지급하거나 수취하는 펀딩(Funding) 역시 연속적으로 적용된다.
- **wrappedERC20:** wBTC와 같은 Wrapped ERC20 자산. wrappedERC20의 잔고는 크레딧(credit)만 가질 수 있다.

자산은 정산 과정이나 서버카운트 상태 검증 과정에서 매니저를 지원할 수도 있다. 예를 들어 CashAsset 컨트랙트는 서버카운트에 누적된 이자와 관련된 모든 데이터를 저장한다. 매니저는 포트폴리오의 리스크를 평가할 때 이러한 이자를 고려할 수 있다.

4.1 CashAsset

각 리스크 매니저는 하나의 기준 자산(quote asset)을 지원한다. 옵션과 무기한 선물과 마찬가지로 사용자는 기준 자산에 대해 크레딧 잔고 또는 부채 잔고를 보유할 수 있다. 그러나 다른 자산과 달리 부채 잔고를 가진 사용자는 해당 금액에 대해 이자를 지급해야 한다. 이 이자는 다시 크레딧 잔고를 보유한 모든 사용자에게 분배된다. 따라서 기준 자산은 해당 매니저에서 네이티브 대출 시장(native lending market)을 제공한다.

출시 시점에는 USDC만이 지원되는 기준 자산이다.

예를 들어 ETH의 현물 가격이 2000이라면, 사용자는 계정에 보유한 1ETH를 담보로 약 1600의 USDC를 차입할 수 있다. 이 경우 사용자는 부채 잔고를 가지게 되며 5%의 이자를 지급한다. 반대로 크레딧 USDC 잔고를 보유한 모든 사용자는 이 이자 지급액의 일부를 분배받는다.

이자율은 Aave(참조 [3])와 유사한 단순한 구간별(piece-wise) 곡선을 통해 설정된다. 기준 자산의 이용률(Quote Utilization)은 전체 부채 잔고를 전체 크레딧 잔고로 나눈 비율로 정의된다. 이용률이 낮을 때는 차입자가 지급하는 이자율도 낮다. 이용률이 증가하면 이자율 역시 증가한다. 일정 임계값을 초과하면 이자율의 증가 속도는 크게 가속된다.

5. 매니저(Managers)

매니저는 자신에게 등록된(subscribed) 서버카운트에 적용되는 특정 규칙을 정의하는 스마트 컨트랙트이다. 출시 시점에는 거래 시 서버카운트가 적절한 증거금을 유지하도록 보장하는 두 종류의 매니저가 제공된다. 이들은 **표준 리스크 매니저(Standard Risk Manager, SRM)** 와 **포트폴리오 마진 리스크 매니저(Portfolio Margin Risk**

Manager, PMRM) 이다. 사용자는 서버카운트를 생성할 때 하나의 매니저를 선택하여 등록해야 한다. 매니저는 모듈식으로 설계되었다는 점을 강조한다. 이러한 설계의 가장 큰 장점은 어떤 자산 집합이나 목적에 대해서도 리스크 매니저를 쉽게 설계할 수 있어 다양한 거래 방식과 효과적인 리스크 관리를 가능하게 한다는 것이다.

매니저는 거래 정산과 청산을 담당하므로 서버카운트의 잔고를 변경할 수 있는 권한을 가진다. 매니저는 스마트 컨트랙트이므로 변경이 불가능(immutable)하며, 따라서 이러한 권한이 악의적으로 사용될 수는 없다.

Derive Protocol에서 리스크 매니저는 다음과 같은 기능을 수행한다.

1. **증거금 규칙 설정(Setting Margin Rules):** 매니저는 자신이 지원하는 모든 서버카운트의 증거금 요건을 설정한다. 청산 대상이 되는 것을 방지하기 위해 사용자는 유지 증거금(maintenance margin) 요건을 충족해야 한다. 새로운 포지션을 개설하기 위해서는 더 엄격한 초기 증거금(initial margin) 요건을 충족해야 한다. 이러한 규칙은 누구나 확인하고 검증할 수 있도록 투명하게 공개된다.
2. **청산(Liquidations):** 매니저는 청산이 이루어지는 조건을 정의하고 이를 집행한다.
3. **정산(Settlement):** 매니저는 모든 거래의 정산을 담당한다.

SRM과 PMRM은 모두 지원되는 기초 자산(Base Assets), 옵션 및 무기한 선물(Perpetuals)에 대해 (조정 가능한) 미결제약정(Open Interest) 한도를 가진다.

5.1 Standard Risk Manager

표준 리스크 매니저(Standard Risk Manager, SRM)는 트레이더가 Derive Protocol에서 옵션, 무기한 선물 및 기초 자산을 직관적이고 다양한 기능을 활용하여 거래하고 증거금을 관리할 수 있도록 하는 진입점을 제공한다. SRM은 다음과 같은 금융 상품을 지원한다.

- 기준 자산(Quote Asset) (출시 시점에는 USDC)
- 다양한 기초 자산(ERC20) (예: wETH, wBTC)
- 이러한 기초 자산을 기반으로 하는 유럽형 옵션 및 무기한 선물

SRM의 주요 기능은 다음과 같다.

1. **교차 증거금(Cross-margin):** 트레이더는 하나의 서버카운트 내에서 모든 기준 자산과 기초 자산 잔고를 모든 미결 포지션의 담보로 사용할 수 있다. 격리 증거금(Isolated Margin)은 별도의 서버카운트를 생성함으로써 구현된다.
2. **다중 자산 담보(Multi-asset collateral):** 트레이더는 다양한 기초 자산을 무기한 선물과 옵션의 담보로 사용할 수 있다. 예를 들어 사용자는 ETH를 담보로 BTC 무기한 선물 숏 포지션을 보유할 수 있다.
3. **자본 효율적인 스프레드(Capital Efficient Spreads):** 일반적으로 숏 옵션에 필요한 증거금은 옵션의 시가평가(mark-to-market) 가치와 현물 가격의 일정 비율을 기준으로 산정된다. 롱 옵션은 증거금 상쇄 효과를 제공하지 않으며, 기초 자산은 시장 가치보다 할인된 가치로 평가된다. 트레이더에게 자본 효율적인 스프레드를 제공하기 위해 SRM은 스프레드의 증거금 요구액을 최대 손실(Maximum Loss) 수준으로 제한할 수 있다. 예를 들

어 Alice의 포트폴리오가 200콜스프레드(*Long*200 Call Spread)로 구성되어 있다고 가정하자. 즉, 2주 후 만기의 ETH 1800콜옵션1개 롱(일반적으로 증거금 요구액은 0)과 동일한 만기의 ETH 2000콜옵션1개 숏(일반적으로 약 320의 증거금 요구)을 보유하고 있는 경우, SRM은 정확히 \$0의 증거금만 요구한다. 이는 이전 버전에 비해 자본 효율성이 크게 향상된 것이다. 숏 스프레드의 경우에도 최대 요구 증거금은 최대 손실 수준으로 제한된다.

4. **레버리지 무기한 선물(Leveraged Perpetuals):** 무기한 선물은 SRM을 통해 높은 자본 효율성으로 거래할 수 있다.
5. **차입(Borrowing):** 활성화되어 있는 경우 사용자는 자신의 Wrapped ERC20 기초 자산을 담보로 기준 자산(Quote Asset)을 차입할 수 있다.

관련 데이터 피드의 신뢰도(confidence)가 낮은 경우 SRM은 모든 기초 자산, 무기한 선물 및 숏 옵션에 대해 추가적인 초기 증거금을 요구한다. 또한 기준 자산이 디페그(depeg)될 경우 모든 무기한 선물과 숏 옵션에 대해 추가적인 증거금이 요구된다.

5.2 Portfolio Margin Risk Manager

PMRM은 높은 수준의 자본 효율성을 가능하게 하는 업계 표준인 포트폴리오 마진(Portfolio Margin)을 Derive에 도입한다.

PMRM은 기준 자산(Quote Asset), 단일 표시 기초 자산(Denominated Base Asset), 그리고 이에 대응하는 옵션과 무기한 선물을 지원한다. 따라서 사용자가 포트폴리오 마진을 이용하여 ETH 옵션과 BTC 옵션을 모두 거래하려는 경우 두 개의 PMRM 서버카운트가 필요하다.

포트폴리오 마진을 계산하기 위해 매니저는 다양한 시나리오에서 포트폴리오가 입게 되는 시장 손실인 **maxLoss**를 계산한다. 각 시나리오는 특정 현물 가격 충격(Spot Shock)과 내재변동성 충격(Implied Volatility Shock)으로 정의된다. 또한 maxLoss에 반영되지 않는 리스크 요소를 고려하기 위해 추가적인 **컨틴전시 증거금(Contingency Margin)**이 더해진다.

$$\text{Margin} = \text{mfactor} \times (\text{contingencies} + \text{maxLoss})$$

여기서 **mfactor**는 유지 증거금(Maintenance Margin)을 계산할 때는 일반적으로 1.0이며, 초기 증거금(Initial Margin)을 계산할 때는 이보다 큰 값이 사용된다.

매니저는 다음과 같은 컨틴전시(Contingencies)를 사용한다.

- **Base Asset Contingency:** 보유한 각 기초 자산에 대해 현물 가격의 일정 비율을 증거금에 추가한다.
- **Perpetual Asset Contingency:** 보유한 각 무기한 선물 계약에 대해 현물 가격의 일정 비율을 증거금에 추가한다.

- **Option Contingency:** 각 행사가(Strike)별 순(Net) 숏 옵션 수량을 계산한 후, 각 순 숏 옵션에 대해 현물 가격의 일정 비율을 증거금 요구액에 추가한다.
- **Oracle Contingency:** 관련 데이터 피드의 신뢰도 점수(confidence score)가 낮은 경우 각 기초 자산, 옵션 및/또는 무기한 선물에 대해 현물 가격의 큰 비율을 초기 증거금 요구액에 추가한다.

추가적으로 다섯 번째 컨틴전시(contingency)인 **Basis Contingency**가 존재한다. 이는 모든 만기에 대해 선도 베이스(Forward Basis)가 사용자에게 불리한 방향으로 움직일 경우 포트폴리오가 입게 될 손실을 계산한다. 만약 이 값이 **maxLoss**보다 크다면, 증거금 계산식에서 **maxLoss** 대신 Basis Contingency가 사용된다.

마지막으로, 기준 자산(Quote Asset)이 디페그(depeg)될 경우 **mfactor**가 증가하지만, 이는 초기 증거금(Initial Margin)을 계산할 때에만 적용된다.

SRM 및 PMRM의 방법론에 대한 보다 자세한 내용은 추후 문서를 통해 제공될 예정이다.

5.3 Marking and Settlement

두 매니저 모두 옵션의 평가(마킹)에 **Black76 가격결정 모델**을 사용한다. 자세한 내용은 [2]를 참조하라.

트레이더가 헤지를 원활하게 청산할 수 있도록 하기 위해, 두 매니저의 옵션은 만기 전 30분 동안의 기초자산 가격의 **시간가중평균가격(Time Weighted Average Price, TWAP)** 으로 정산된다.

이 기간 동안 옵션은 선도가격(Forward Price)과 TWAP 가격의 선형 결합(linear combination)으로 평가되며, 각 가격의 가중치는 만기까지 남은 시간에 따라 결정된다. 정산 가격의 일부가 고정되므로 옵션은 이른바 **델타 감소(delta decay)** 를 경험하게 된다. 즉, 일반적으로 델타가 100인 콜옵션이라도 만기까지 15분이 남은 시점에서는 기초자산에 대한 델타 노출이 50만 남게 된다.

5.4 Risk Reducing Trades

두 매니저 모두에서 서버카운트는 최종 상태의 초기 증거금이 부족한 경우 새로운 포지션을 개설하거나 기존 포지션 규모를 확대할 수 없다. 그러나 거래가 서버카운트의 유지 증거금(Maintenance Margin) 요구사항을 감소시키는 경우(즉, 거래가 리스크를 감소시키는 경우)에는 해당 변경이 항상 허용된다.

5.5 Risk Assessors

Black76 함수 호출이 매우 많이 필요하기 때문에 포트폴리오 마진 계산은 가스 비용이 매우 크다. PMRM 계정 규모가 제한되는 것을 방지하기 위해, 거버넌스가 승인한 **Verified Integrators**는 온체인에서 하나의 리스크(즉, 시가평가(mark-to-market), 다시 말해 지급능력(Solvency) 검사)를 제외한 모든 리스크 검사를 우회할 수 있다. Verified Integrators가 청산 대상이 될 수 있는(그러나 지급불능은 아닌) 포지션을 발생시키는 거래를 승인하는 것은 가능하지

만, 이러한 계정은 참여자 누구나 즉시 청산할 수 있으므로 시스템에는 해당 리스크가 남지 않는다. 또한 Verified Integrator가 부적절하게 행동하는 것으로 확인될 경우 해당 권한은 철회될 수 있다.

중요한 점은 지급능력(Solvency) 검사가 존재하기 때문에 Verified Integrators는 지급불능 상태의 포지션이 생성되도록 허용할 수는 없다는 것이다.

6. 부분 청산(Partial Liquidations)

증거금 요건 아래로 떨어진 사용자는 부분 청산의 대상이 된다.

청산은 투명한 절차로 진행되며 모든 참여자에게 개방된다. 즉, 누구나 청산자(Liquidator)가 될 수 있으며, 청산 대상이 된 사용자 역시 이 과정 전반에 걸쳐 자신의 서버카운트를 모니터링할 수 있다.

청산 메커니즘은 시스템에서 리스크를 신속하게 제거하는 동시에 청산 대상 트레이더에게 최대한 유리한 사용자 경험을 제공하도록 설계되었다.

6.1 Liquidation Auctions

두 매니저에서의 청산은 다음과 같은 방식으로 진행된다.

1. 사용자가 유지 증거금(Maintenance Margin) 요건 아래로 떨어지면 해당 계정이 표시(flag)된다. 누구나 `startAuction()` 함수를 호출하여 해당 서버카운트를 청산 대상으로 지정할 수 있다.
2. 포트폴리오 전체가 경매에 부쳐진다. 최초 제안 가격은 시가평가(Mark-to-Market) 가치에서 일정 비율 할인된 가격이다.
3. 할인율은 시간이 지남에 따라 증가한다. 어느 시점에서든 청산자는 현재 할인된 시가평가 가격으로 포트폴리오의 원하는 비율을 인수하는 데 동의할 수 있다.
4. 청산 대상 사용자에게 공정한 결과를 보장하기 위해 청산자가 인수할 수 있는 최대 비율은 현재 할인율, 포트폴리오의 시가평가 가치 및 현재 증거금 요건의 함수로 결정된다. 예를 들어 증거금 요건을 약간만 밑도는 포트폴리오는 약 10%만 청산하면 되지만, 지급불능에 가까운 계정은 거의 100%에 가까운 비율이 청산되어야 한다.
5. 할인율은 포트폴리오가 충분한 수준까지 청산될 때까지(여러 명의 청산자가 참여할 수도 있음) 계속 증가하거나, 할인율이 100%에 도달할 때까지 증가한다. 할인율이 100%가 되면 청산자는 포트폴리오 전체를 무상으로 인수할 수 있다.
6. 이후 지급불능(Insolvent) 경매가 시작된다. 입찰 가격은 \$0에서 시작하여 서버카운트의 초기 시가평가 가치를 기준으로 큰 음수 값까지 감소한다. 청산자는 항상 포트폴리오의 최대 100%를 인수할 수 있으며, 현재의 (음수) 제안 가격에 따라 Security Module(아래 참조)로부터 보상을 받는다.

6.2 The Security Module

Security Module(SM)은 지급불능이 발생했을 때 청산자에게 자금을 지급하기 위해 기준 자산(즉, USDC)의 준비금을 보유하는 스마트 컨트랙트이다.

만약 Security Module(SM)의 자금이 모두 소진될 경우, 지급불능 부채(Insolvent Debt)는 모든 사용자에게 분담된다.

이는 일시적 출금 수수료(Temporary Withdrawal Fee)를 통해 이루어진다. 시스템의 지급불능 부채를 **지급불능 부채와 총 예치(즉, 래핑된) 기준 자산(Quote Asset)의 합계**로 나눈 비율이 기준 자산을 출금하려는 사용자에게 수수료로 적용된다.

예를 들어 시스템에 10,000의 부실 부채(*BadDebt*)와 100,000의 USDC가 존재한다고 가정하자. 이 경우 다음과 같은 수수료가 적용된다.

$$\frac{10,000}{100,000 + 10,000} = 9.09\%$$

이 비율은 모든 출금에 적용된다. 따라서 Alice가 5000를 출금하려는 경우 454.5의 출금 수수료를 지불하게 된다.

이러한 일시적 출금 수수료는 먼저 출금하는 것이 유리하도록 하는 인센티브를 제거하며, 청산 연쇄(Liquidation Cascades)를 방지하여 시스템의 안정성을 향상시킨다.

7. 프로토콜 수수료(Protocol Fees)

아키텍처 내에서 리스크를 부담하는 모든 주체는 그에 대한 보상을 받을 수 있다. 프로토콜에는 세 가지 주요 수수료 발생원이 존재한다.

1. **거래 수수료(Trading Fees):** 시스템의 미결제약정(Open Interest), 즉 시스템의 리스크를 증가시키는 모든 거래에는 수수료가 부과된다. 이 수수료는 기초자산의 현물 가격과 거래 규모의 함수로 결정된다.
2. **청산 수수료(Liquidation Fees):** 청산되는 사용자는 자신의 서버카운트의 리스크와 시장가치에 비례하는 소액의 수수료를 부담한다.
3. **이자 스프레드(Interest Rate Spreads):** 기준 자산을 차입한 사용자가 지급하는 모든 이자의 일정 비율이 수수료로 징수된다.

모든 수수료는 프로토콜이 소유한 Security Module에 적립되며, 이를 통해 프로토콜의 견고성과 복원력이 향상된다.

거버넌스의 승인을 받은 주체는 예를 들어 다른 수수료 체계를 적용하는 조건 등을 약속하는 대신 거래 수수료를 면제 받을 수 있다. 해당 주체가 요구사항을 충족하지 못할 경우 이러한 승인은 철회될 수 있다.

8. Parameters and Governance

프로토콜을 제어하는 매개변수는 매우 많으며, 특히 매니저의 경우 더욱 그렇다. 이러한 매개변수는 트레이더의 자본 효율성과 보안을 모두 보장하기 위해 시장 상황이 변화할 때마다 업데이트되어야 한다.

프로토콜의 모든 매개변수는 스마트 컨트랙트에 의해 관리된다. Derive에서는 이 스마트 컨트랙트가 **Short Term Executor**에 의해 소유된다. Short Term Executor에 대한 자세한 내용은 [4]를 참조하라.

9. Data Feeds

매니저는 리스크를 정확하게 평가하고 관리하기 위해 오라클이 다음과 같은 데이터를 제공해야 한다.

1. **내재변동성(Implied Volatility, IV):** 지원되는 각 만기(Tenor)의 IV는 원시 **SVI(Stochastic Volatility Inspired)** 곡면 형태로 제공된다. 이는 다섯 개의 매개변수 (a, b, ρ, m, e) 로 정의된다. 자세한 내용은 [5]를 참조하라.

행사가를 K , 로그 머니니스(Log-Moneyness)를 k 라고 하자. 여기서

$$k = \log(K/F)$$

이며 F 는 만기까지의 시간이 τ 인 현재 선도가격(Forward Price)이다.

이때 행사가 K 의 내재변동성 σ 는 다음과 같이 정의된다.

$$\sigma = \frac{1}{\sqrt{\tau}} \frac{\sqrt{a + b[\rho(k - m) + \sqrt{(k - m)^2 + e^2}]}}{\sqrt{\quad}}$$

2. **선도가격(Forward):** 지원되는 각 만기의 선도가격도 함께 제공된다. 앞서 설명한 것처럼 만기가 가까워질수록 이 값은 기초자산의 TWAP와 선도가격의 선형 결합으로 전환된다.
3. **무위험금리(Risk Free Rates):** 지원되는 각 만기에 대해 정의된 금리 곡선(Interest Rate Curve)이다.
4. **현물가격(Spot):** 여러 데이터 소스로부터 수집되는 기초자산의 현물(Index) 가격이다.
5. **무기한 선물 가격(Perpetual Price):** 무기한 선물의 거래가격과 임팩트 가격(Impact Price)이다.

제공되는 모든 데이터에는 각각 **신뢰도 점수(Confidence Score)** 가 함께 제공된다. 데이터 피드의 신뢰도가 낮을 경우 SRM과 PMRM 모두에서 추가적인 초기 증거금이 요구된다.

내재변동성과 선도 베이스스(Forward Basis)를 산출하는 방법론에 대한 보다 자세한 내용은 추후 공개될 예정이다.

참고문헌(References)

- [1] **Lyra Whitepaper**. 2021, S. Dawson, N. Forster, D. Romanowski, M. Spain
<https://www.lyra.finance/files/whitepaper.pdf>
- [2] **The Pricing of Commodity Contracts**. 1976, *Journal of Financial Economics*, Vol. 3, pp. 167–179, F. Black
- [3] **Borrow Interest Rate – Aave V3 Documentation**
<https://docs.aave.com/risk/liquidity-risk/borrow-interest-rate>
- [4] **LEAP 51: Lyra Governance V2**. 2023, M. Spain
<https://leaps.lyra.finance/leaps/leap-51/>
- [5] **Arbitrage-free SVI Volatility Surfaces**. J. Gatheral, A. Jacquier, *Quantitative Finance*, Vol. 14, No. 1, pp. 59–71, 2014