Microderiv Protocol: Peer-to-Peer Derivatives Trading via an Automated Central Counterparty Financial Market Infrastructure

Max Brillaugte
brillaugte@proton.me

14th July 2023

Updated: July 19th, 2023

Abstract

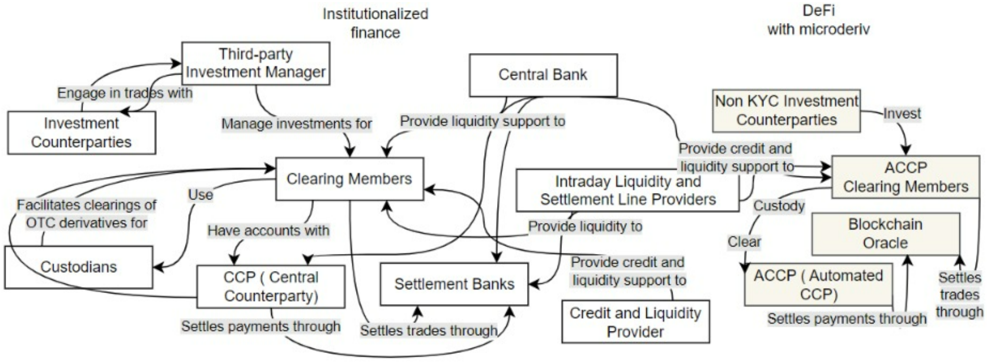
Derivatives underlie the vast array of financial products that drive the modern economy, yet they remain dependent on physical intermediaries for trust. This paper introduces a peer-to-peer solution, through an overview of the Microderiv financial market infrastructure. Our proposal aims to address the efficiency of decentralized derivatives through the implementation of an automatic over-the-counter (OTC) derivative infrastructure relying on threshold-signature-based oracles and low latency delta-neutral counterparties. By leveraging an Automatic Central Counterparty, we mitigate counterparty risk through a deterministic and modelable mutualized loss and reward system with off-chain conducted risk management exclusively computed by end users, enhancing the decentralization and scalability of the system.

Legal Disclaimer: This Whitepaper is presented by MicroDeriv for the sole purpose of obtaining public feedback. It does not constitute an offer to sell or a solicitation to buy any tokens or financial instruments. Should MicroDeriv issue tokens in the future, they will be offered through definitive documents that may differ from this Whitepaper. MicroDeriv's plans outlined herein are tentative and dependent on various external factors including market conditions. The realization of these plans is not guaranteed. Statements regarding future events are based on MicroDeriv's assessments which may not be accurate. MicroDeriv tokens, if developed, are intended for use within its network for specific functions such as trading and governance. These tokens are not investment instruments and should not be acquired for speculation or profit. Purchase them only if you understand their intended use and comply with legal requirements. MicroDeriv does not guarantee the tokens' future utility, performance, or value. MicroDeriv tokens are not securities and confer no rights or interests in MicroDeriv's equity or networks. MicroDeriv reserves the right to use proceeds from token sales for any purpose without conditions. This Whitepaper is for informational purposes and may change. The information is provided "as is" without warranties of any kind, either express or implied, and MicroDeriv disclaims all liabilities for damages arising from the use or reliance on this Whitepaper's content. MicroDeriv is evaluating legal and regulatory requirements for its proposed tokens and operations and may alter the tokens' functionalities accordingly. No regulatory authority has reviewed or approved this Whitepaper. Prospective token holders must exercise caution and carefully assess risks before deciding to purchase tokens.

Contents

1 Introduction

Modern finance has been crafted through countless crises and has iteratively created a global, standardized financial infrastructure capable of withstanding high stress. This paper is based on the inspirations of the Central Counterparty (CCP) architecture, mandated by the G20 since 2008 for systemically important financial institutions (SIFI) to emulate some features within the scope and constraints of DeFi technologies, in order to propose efficient and a wide range of trustworthy financial derivatives products.


Institutionalized finance
DeFi with microderiv
Third-party Investment Manager
Engage in trades with
Investment Counterparties
Manage investments for
Central Bank
Provide liquidity support to
Non KYC Investment Counterparties
Invest
Provide credit and liquidity support to
ACCP Clearing Members
Clearing Members
Intraday Liquidity and Settlement Line Providers
Custody
Facilitates clearings of OTC derivatives for
Use
Have accounts with
Provide liquidity to
Clear
Blockchain Oracle
Custodians
CCP (Central Counterparty)
Settlement Banks
Provide credit and liquidity support to
ACCP (Automated CCP)
Settles trades through
Credit and Liquidity Provider
Settles payments through
Settles trades through
Settles payments through

When addressing the problem of trustless derivatives, the literature proposes an adaptation of exchange-traded derivatives (ETD) framework without success; we propose an over-the-counter (OTC) derivatives framework. In finance, OTC swaps represent $>> 100k$ tradable instruments with ¡1k counterparties and large trading sizes, while listed futures offer $>> 1k$ tradable instruments and ¿¿ 100k counterparties with significant retail participation [1]. OTC derivatives are not widespread because they involve high additional costs and complexity. With smart contract automation, the technology is ready to automate these frameworks to make them mass-market.

Let's define the most basic interaction, a bilateral OTC derivative between P[a] and P[b] on an instrument F[k]. When P[a] and P[b] settle an on-chain swap contract F[1] where P[1] longs X as F[k1], P[2] shorts X as F[k2] where PnL P[1] - PnL P[2] = 0, and P[A] pays fees to P[B]. Additionally, $P[b]$ opens a position to be delta neutral in the form of a long X as $F[k3]$ with $P[c]$ that can be, for example, a broker or himself, where $\Delta F[k2] + \Delta F[k3] = 0$.

But here is the twist, if A wins, B loses, if A loses, B wins, but if A defaults, B also loses. If P[A] defaults and P[B] cannot close F[k3] at a good price, P[B] loses money, as well as P[A], who is using P[B]'s position to hedge the risk of a portfolio when P[B] defaults. This problem is compensable by asking both parties to post a default fee that will compensate the expected default loss. The bilateral solution works as long as P[c] is not trading with P[d] who trades with P[n] who trades with P[a]; the more interconnections grow in a financial system, the riskier the waterfall becomes.

A single trustworthy party needs to become the counterparty of all parties to reduce the expected losses and mechanically increase the capital efficiency. Crypto centralized exchanges have successfully created insurance funds to address these scenarios. An insurance fund by itself is not sufficient as it requires active risk management, which is where DeFi lacks solutions. The ACCP framework is based on a series of deterministic capital efficiency risks, that users can model individually and choose to expose themselves or not, and that together form a DeFi version of a traditional CCP. This can be compared to swarm organization, where instead of big blocks, we have millions of participants interacting with each other and moving at the same time as a group.

With AI development, we expect the financial industry to be either fully managed by a central entity, or each individual managing their own risk instead of delegating risk management to banks and various funds. We expect models based on automated financial players organization to emerge in the upcoming years.

2 Model assumptions, limitations and adaptations

KYC doesn't exist. Tentative attempts at decentralized identity have led to a secondary market where people buy identities. If the protocol wants to treat large and small players equally, it needs to be Sybil resistant. Moreover, DeFi systems don't yet have agreements with the government to force an entity to pay; the only collateral considered is collateral locked inside a contract, whether it's a bank with a good credit ratio or retail. If a country or a municipality signs an official deal on-chain, only then might its credit rating be considered.

This means no deliveries unless the product is tokenized on-chain with a contract mandating a trusted party. Some solutions, like molecule DAO IP-NFTs, are moving in this direction. Similarly, for a bond to be used as collateral, a bank needs to guarantee without being able to reduce the risk of a government freezing assets.

No KYC means no user can be held liable, and any loss above non-posted collateral can be counted as a loss for the protocol. This means the protocol needs to be deterministic and have restrictive rules on updates, denying unknown potential exploits during future market stress events without human interaction. The user needs to be able to decide the best risk/collateral efficiency ratio for themselves. The risk of mutual loss management to decrease counterparty risk as protocols grow needs to be quantifiable and protected by a circuit breaker from low liquidity assets.
DeFi oracles also rely on external data to define price without being able to attack bad data providers. Computation oracles are also used, but there is little scalability work on oracles as their usages are limited and relatively new compared to blockchains. DeFi liquidity is very narrow and limited to a number of assets; the liquidity providers (LPs) need to be able to port CEX liquidity. The prevailing model is quite more complex compared to an x*y=k LP. Automation of every complex process is mandatory to create a simple enough UX. To complicate matters, blockchain transparency adds a front-run constraint, forcing participants to implement mitigation strategies.

To generate enough counterparty trust, only a network effect with a large variety of assets and applications built on top is viable. A missing feature can generate friction that, with derivative leverage, makes the ecosystem uncompetitive.

Despite these limitations, smart contract determinism and blockchain transparency do offer some advantages, such as settlement risk elimination, XVA simplification, reduction of reconciliation and data management processes, decreased number of intermediaries, and simplified delegation of processes to third parties in free market competition.

3 Market overview

Liquidity issues can occur with small caps as well as bonds; the main factor is the size of the position compared to the market. A scalable derivative model must be able to take advantage of all existing liquidity sources to allow custom instruments with as few as two trades a day.

The following is a list of existing solutions and their non-operational designs:

- Simulating liquidity: This is equivalent to saying there is a model to predict the market.
- Order books: Liquidity requires throwing millions at market makers to maintain untraded pairs. There's a reason why AMMs are so popular.
- Pooled liquidity: Here, the counterparty is betting against clients and raising trading costs so that market manipulators can't be profitable until the market becomes volatile enough to make attacks successful. Moreover, trading cost is often the difference between profitable and losing traders.
- Funding to incentivize counterparties: This relies on expecting counterparties to stay when market conditions are bad unless they're paid absurd daily interest rates.
- Options as collateral: Options are much less liquid than futures since they represent 5 percent of the market. Moreover, options require a convenient futures market to hedge.
- OTC products are the only asset class designed to address illiquidity problems and allow the implementation of front-run mitigation strategies.
- For Interest Rate Derivatives (IRDs), which represent 80 percent of the market open interest, slight inefficiencies bring costs that can render the product irrelevant.

The design must take into account the netting/compression efficiency through ACCPs to be competitive. Many solutions above only work with overcollateralization, disqualifying them for any scalability.

4 Core Architecture

The architecture is based on on-chain collateral management, updated with an on-chain definition where the state is updated by an oracle network. For each position F[k] between parties P[a] and P[b], rules are defined upon contract initiation. The set of oracle models use data such as volatility and other classic metrics of modern finance to define automatic pricing and collective risk management. Each position is the result of a set of risk models run locally by each party before agreeing on contract parameters on-chain. In this way, the protocol can benefit from the best optimization while being as simple as possible on-chain.

$P[k]$ is an entity known as a party and $P[k]'$ is its counterparty. We define $IM[k]$ as the Initial Margin of $F[k]$, $uPnL[k,n]$ as unrealized profit and losses of position $F[k]$ of $P[n]$, $CA[k]$ as the collateral agreement k for party $P[k]$ holding a set of $F[k]$ and collateral $C[k]$, $H[k]$ as the haircut of $C[k]$.

This is a Locked IM architecture.

The definition of $IM[k]$ contains a set of contracts, methods, parameters and oracles allowed to update its stats of a $P[k]$ or multiple $P[k]$. Upon $IM[k]$ creation or update to $CA[k]$, $C[k]$ is transferred or received from/to $IM[k]$.

$IM[k]$ is updated by a smart contract called an $IM_{\text{update method}}$ defined on creation that can take into consideration the amount of free $C[k]$ to secure a liquidity buffer in case of default.

Though the future $F[k]$ PnL cannot be predicted, $IM[k]$ exists to secure $C[k]$ while allowing active $F[k]$ to be open inside the same $CA[k]$. For each $F[k]$, the counterparty $P[k]'$ is responsible for choosing an $IM_{\text{update method}}$ to avoid loss due to volatility where $IM[k] < -PnL$ or lack of liquidity not allowing to exit their hedge.

For example, if inside the same $CA[k]$, $F[1]$ is liquidated while the market for $F[2]$ is closed, $IM[2]$ is not affected and $P[k]'$ can close the position on market opening, if $IM > |uPnL|$ where $uPnL < 0$, the position is not liquidated and will be when $IM < |uPnL|$.

The main feature of the IM locked architecture is highly efficient IM updates allowing near any asset cross-margin without the risks of any asset cross-margin because every position is isolated.

- $CA[k]$ as Collateral Agreement where:

CA[k] is a set of whitelisted C[k] where each C[k] unit is priced in C[0] quantity.

C[k] is collateral free from any IM[k] and withdrawable.
For each C[k], a H[k] is associated which represents a haircut ratio that acts as a liquidity buffer for volatile collateral.
H[k] is updated by an oracle based on a volatility, liquidity and concentration model, where H[k] is restricted by a max variation per ms. For any C[k] transfer to any CA[1], C[k] is removed from CA[2] unless deposits and withdrawals occur.
A CA[k] default event is triggered when the sum of IM[k] ¡ the sum of C[k] * H[k].
Maintaining a minimum amount of C[k] in CA[k] can be required in IM[k] methods to avoid liquidation.
This minimum amount can be defined by a model that indicates the CA[k] recommended amount, if optimized between deposit speed capacity in a time liquidity risk 99th percentile model, added to a prediction on H[k] variations based on H[k] update contract.

A collateral default can be fatal for an ACCP, and other dApps using the protocols instruments like centralized stablecoins or risk-free assets like bonds issued by trusted parties are exposed to the mood of the SEC.
Decentralized collaterals, like BTC which are speculative, require a haircut and more fees to cover hedging costs. To cover an instrument labeled in dollars, an LP can simply borrow BTC to short while depositing BTC in the CA[k].

- Bilateral :

A bilateral contract is a F[k] between P[a] and P[b] where uPnl[k,a] - uPnL[k,b]= 0.
To cover each P[k] from P[k]' default losses, a default fund (DF) is mandated. The DF allows non-defaulting P[k] to be compensated for early contract termination and the liquidity cost to close a hedge.
IM[k] is defined to cover default risk for the settlement period T + liquidation period T'.
PnL = (initial MtM - current MtM) * qty, VM for variation margin is a liquidity buffer to be added to cover the IM[k] risk period.

- ACCP P[k] are defined as :

We consider a set of $F[k]$ where $\Sigma(\delta\text{uPnL}) = 0$. If this is not equal to 0, losses are distributed to ACCP members according to predefined layers.
Losses occur when a Clearing Member (CM) defaults and the cost of replacing his portfolio exceeds the Initial Margin (IM) + Default Fund Contribution (DFC).
Each position begins with $P[a]$ and $P[b]$ in a bilateral trade $F[1]$, and then novates to the ACCP. At this point, the ACCP becomes the counterparty of $P[a]$ and $P[b]$.

Members are required to contribute a locked Default Fund Contribution (DFC) that is proportional to their clearing size in order to participate in the ACCP.
We denote the sum of all DFCs as DF, i.e., DF = ΣDFC, and ACCP members are referred to as CMs for Clearing Members.
Each F[k] IM owned by a CM is optimized based on correlation and diversity risk optimization.
Losses are deterministically mutualized among CMs, increasing ACCP's trustability as a counterparty exponentially by the number of users.

If retail wants to become a counterparty to an OTC position, there is a high risk that they default, making them ineligible as a counterparty for other market participants. Only large institutions can play in the derivative OTC market, and even with a high credit rating, bilateral architectures have failed. To tackle this, in modern finance, retail puts money into an institution that, when large enough, becomes a trusted counterparty, and for the largest ones, becomes ACCP members.

Before DeFi, market-making was a big barrier since few people were able to operate. This has been solved by AMMs, suddenly everyone could become their own market maker, allowing every project to access market making. AMMs are not perfect but efficient enough to allow sleeping capital to be active, the same case applies to ACCPs. In our case, the physical limits for ACCPs are much higher than those for MMs as it requires big teams and is only limited to the biggest actor of a few biggest countries. It is extremely hard to forecast the market fit of ACCPs.

Small caps are not economically viable for big institutions and without DeFi will never have access to advanced financial market infrastructure. It becomes risky for one entity to hedge 100 percent of the derivatives of a small cap, but less risky for 10,000 entities to hedge 0.01 percent of a small cap that represents a small percentage for each individual.

An ACCP on small, unregulated markets has the advantage of adapting to local market needs and can force a form of regulation by not doing business with non-ACCP members. Even though small, this kind of market regulation can reduce the volatility of an asset and increase its liquidity,

5 Attacks

The most basic risk is front running. For example, if P[a] knows P[b] is going to buy X because he has accepted a position from P[c] and will hedge it, A will attempt to front run the position. Mitigation of this risk is discussed in “Automation and Transparency.” A second common scenario is BP[b] knows P[C] is going to close his position on Xm with the oracles computing MtM on price, P[B] might attempt to manipulate the oracle price. Mitigation of this risk is discussed in “Oracle and Blockchain.” The easiest way to alleviate these risks is to pass through fees to compensate the expected sell side hedging risk. However, the lower the front running costs, the lower the fees.

One of the big issues with the CA[k] with a cross portfolio is that a trusted party can be used as a proxy by an untrusted party to steal collateral. Here is an example where F[1] and F[2] make a bilateral trade:

T:0
P[a][F[1][IM : 10 , uPnL : -2]], C[0] = 0
P[b][F[1][IM : 10 , uPnL : +2], F[2][IM : 1, uPnL : 0]]], C[0] = 0
P[c][F[2][IM : 1 , uPnL : 0]]], C[0] = 0
T:1
P[a][F[1][IM : 10 , uPnL : -2]], C[0] = 0
P[b][F[1][IM : 10 , uPnL : +2], F[2][IM : 1, uPnL : -10]]], C[0] = 0
P[c][F[2][IM : 1 , uPnL : +10]], C[0] = 0
T:2 without locked IM
P[a][], C[0] = -2
P[b][], C[0] = 0
P[c][], C[0] = 11

T:2 with locked IM
P[a][F[1][IM : 10 , uPnL : -2]], C[0] = 0
P[b][F[1][IM : 10 , uPnL : +2]], C[0] = 0
P[c][], C[0] = 1

Locked IM avoids counterparty credit risk, with the drawback of capital efficiency. This drawback can be smoothed with the IM Model associated with the underlying F[k]. It is about finding the best risk/reward for both parties. We can continue the previous example for an ACCP:
T:0 where F[1] - F[2] = 0
P[a][F[1][IM : 10 , uPnL : -2]], C[0] = 0
ACCP[a][F[1][IM : 10 , uPnL : +2], F[2][IM : 10, uPnL : 0]]], DF = 1000
P[c][F[2][IM : 10 , uPnL : 0]]], C[0] = 0
T:1
P[a][F[1][IM : 10 , uPnL : -22]], C[0] = 0
ACCP[a][F[1][IM : 10 , uPnL : +2], F[2][IM : 10, uPnL : 0]]], DF = 1000
P[c][F[2][IM : 10 , uPnL : 20]]], C[0] = 0 T:2 P[a][], C[0] = 0
ACCP[a][F[1][IM : 10 , uPnL : +2], F[2][IM : 10, uPnL : 0]]], DF = 988
P[c][F[2][IM : 10 , uPnL : 0]]], C[0] = 20

In this scenario, the F[k] derived asset did a jump far above IM+DF (considered as IM in this example). To make an attack like this, let's define P[1] and P[2] controlled by the same player, opening a huge F[k] in bilateral between players, novate to the ACCP, then exploit high liquidity to profit from one side defaulting at a cheap price while the other side is still in position, creating a positive delta between both accounts. To counter this, each CM can ask to be replaced before a novation is accepted, this way each individual player can define its risk limit.

6 Contract initiation

Once a user wants exposure on an instrument, they can find a counterparty through an aggregator, matchmaking service or by submitting an on-chain RFQ/Quote. To facilitate the task, interactions are automatically filtered by local risk models to make the interaction as simple as possible and ensure decentralization.

The quote contains a set of parameters that will define the PnL of the parties involved, IM, how the positions will be closed, and when the position can be liquidated. Parameters can involve advanced computation, for example, pricing the IM based on liquidity, concentration, and correlation risk models. As long as oracles can agree on data, this data can be used to define these parameters upon position opening. A natural improvement is to determine a variable termination fee depending on the market context through a model that takes sensitivity parameters as input.

7 Parameters

The goal behind this part is to give an overview of common parameters that can be used through microderiv contracts.

- Instrument type: Swap, future, option, repo, forward
  Each type brings a different set of parameters:
- Quantity
- Initial Price
- Instrument Expiration
- Initial IM
- Default Fee: (can be a model)
- Position status: Allocated, Cancelled, Exercised, Expired, Matured, Novated, Terminated
- Settlement method: Cash, token, or trusted third party For example, a Bitcoin future needs to be delivered with warped Bitcoin, and a real estate option with a house token. In the case where settlement is determined by institutional custody, the designated party can define if settlement has been through.
- Collateral Agreement: List of collaterals, Haircuts, Haircut update method
- MtM method: Mark to Market, defines the computation method of the price of the instrument.

- IM model: Value at Risk, defines locked collateral that if it drops below the IM threshold will trigger a liquidation event.

- Funding/interest rates: In case of a party hedge position, hedging position cost and compensation for collateral immobilization must be paid to incentivize the liquidator. The interest rates can be collected anytime by the LP.

- Termination method: Define conditions under which the contract can be terminated by one party. Allows to manage the risk of default in case one party fails to fulfill its obligations.

```
Define the struct for parameters.
struct Parameters {
    uint256 P0; % entry price
    uint256 qty; % quantity
    uint256 IM0; % initial IM
    ...
}

struct Methods {
    uint256 default_Auction_method_k;
    uint256 waterfall_resolution_method_k;
    uint256 update_VM_Method_k;
    ...
}

struct Party {
    % Identifier for the instrument contract
    uint256 instrument_contract;
    uint256 ACCP_id; % Identifier for the ACCP or none
    % Mapping of parameter names to values
    mapping(uint256 => uint256) parameters;
    % Mapping of method names to identifiers
    mapping(uint256 => uint256) methods;
    % Flag to track if the party has signed the contract
    bool hasSigned;
    ...
}
```

PartyA pushes the contract on-chain, PartyB signs it.

8 Repo

Repo, short for repurchase agreement, are contracts where P[a] sells an instrument that he promises to buy back later.

In the scenario where P[a] and P[b] are in a bilateral agreement F[1], P[a] wants to close out the contract but spread defined by MtM and P[b] is too high. P[a] buys a repo on his position to P[c] against a fee and interest rates. The costs for P[c] are usually hedging costs and capital immobilization. P[c] can be mandated to negotiate spread with P[a] at a fair trade or P[a] can repurchase his position when the spread comes back to acceptable bounds. In the case where the cost of the repo is lower than the MtM close, P[a] is incentivized to use a repo. P[c] is incentivized to find spread not reachable to P[b], to allow P[a] to have a price oracle-less closeout.

9 Settlement

Settlements are made to avoid one party getting away with too big uPnL, causing a potential loss in case of default. The shorter the settlement periods, the lower the margin requirements needed. With on-chain transparency and efficiency, continuous settlements are possible, where some nodes can be called.

For scalability, to avoid calling oracles nodes for settlement, P[a] can call P[b] on-chain for settlement, and if P[b] doesn't answer in x blocks, P[a] and P[b] or only P[b] pay the computing fees. If the calling of the oracle signature was unjustified, the caller pays the fee. These settlements can also be requested each x percent of uPnL and be done by the LP, otherwise, he will cover the cost of computing nodes. Regular settlements are unnecessary for independent actors that don't move the market, as the risk of loss exceeding their IM and DF is very low. Other regular off-chain settlements can be based every day on a set time and x percent change on underlying assets with concentration risks.

IM must be deterministic for all positions. If IM is set to be defined by a non-deterministic third party, an excessive IM call won't cause default to the underlying position, but can trigger a default to other positions as there is not enough collateral to update their IM.

While defining IM computation method, IM must take into consideration confidence levels, margin period of risk ("MPOR"), initial margin scenarios and look back periods. The MPOR is based on the defaulter's portfolio asset neutralization capabilities, often based on volumes, OIs, and other CMs activity. The only way to lower systematically the IM is by reducing the MPOR. This means that modelization needs to evolve with market participants capabilities. As long as there are enough incentives, we can assume the LPs will arbitrage opportunities. The ISDA recommends 5 days for OTC derivatives, for ETD it can be less.

When defining products inside an ACCP, the best prevention is to ensure that there will be a sufficient number of bidders during the auction process. Non-ACCP members can be allowed to be bidders in an auction but will have to answer capital requirements by the ACCP without the requirement of DFC.

10 Initial Margin

IM is the maximum loss at a given probability level over a defined period of time a counterparty is willing to risk on a given instrument or set of instruments. This means IM has a cost of locking collateral in a contract.

- Bilateral :

To define simple IM, a common model for normal tail assets is Expected Shortfall (ES). ES is calculated by taking the average of the portfolio losses that exceed the VaR level, considering the tail portion of the distribution of losses. Mathematically, it can be expressed as:

$$\text{ES} = \frac{1}{1-\alpha}\int_{\alpha}^{1} f(x)\,dx \tag{1}$$

Where α represents (1 - confidence level) and f(x) represents the probability density function of portfolio losses. The confidence level can be set at 95, 99, or 99.7 percent confidence levels depending on risk needs.

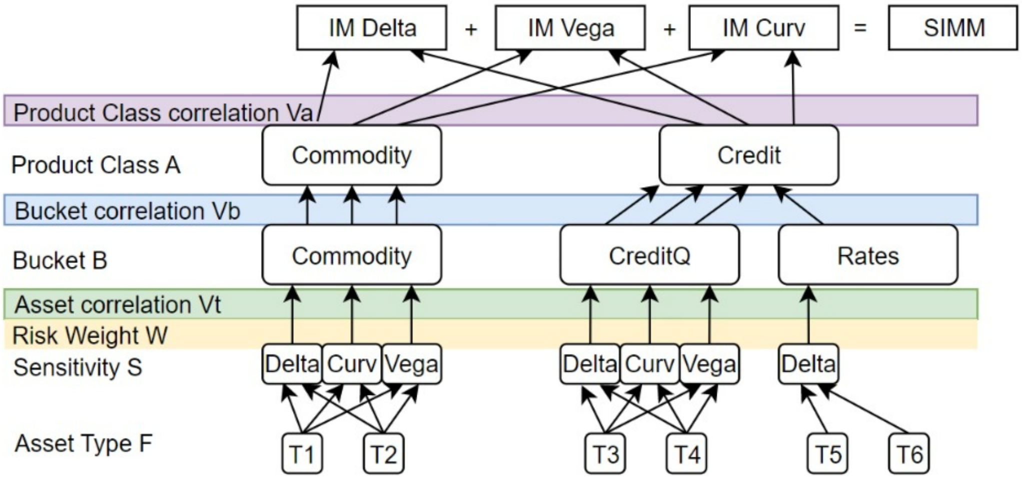
Both parties in a bilateral contract can have different IM definition methods.

- ACCP :

IM can commonly be combined in the case of netting, inverse correlation, or diversification where each remains independent to privatize risk. The goal behind portfolio IM optimizations is to reach, IM(X+Y) ¡ IM(X) + IM(Y) (isolated), with IM(X+Y) the perfect risk rewards for CMs.

For an ACCP portfolio IM model, an expected shortfall with a GARCH(1,1) based on FHS (filtered historical simulations) with addons can cover many assets. But this would mean that nodes need to compute the model in case of IM disagreement. This can be an attack vector as the computation can be intensive. In general, to avoid this kind of attack, limiting the number of assets and positions per CA[k] is good practice.

The SIMM, or Standard Initial Margin Model, is used in the OTC derivative industry as a standard to simplify everything. It is based on precomputed weight and correlations between buckets of assets grouped by industry and sensitivity, buckets that are grouped themselves into classes. When adding IM based on IM computed for each class, we get the SIMM.[2] The SIMM is specialized to group non cleared assets while the ES will be more useful for liquid assets. Based on the principle of SIMM, it is possible to compute a crypto assets version.



The ISDA SIMM model's shortcomings reside in sector-specific risk assessment, correlation dynamics, and market adaptations. Its general approach may not fully reflect unique sector risks. Static correlations falter during market turbulence, while fixed interest and exchange rates may not accurately track real-world shifts. Additionally, the model's heavy reliance on historical data might overlook market expectations, such as implied volatilities, and sudden events like price jumps. Hence, while ISDA SIMM serves as a valuable tool, its limitations necessitate caution and a quest for more responsive models. Other methods like GRID can also be used based on the range of assets.

ACCPs should avoid relying on minimum correlation but incorporate economic basis as a consideration and also utilize back-testing once the model is defined to ensure margin offsets are quantitatively appropriate.

11 Waterfall

The waterfall is the allocation mechanism of CMS mutualization default losses. In case of default, the first party to pay losses is the defaulting party with his own IM and DFC, then the junior tranche, then DF, then the senior tranche. While the overall goal is simplicity and equality among CMs to incentivize a skin in the game effect, more complex add-ons can be added above that for specific cases.

An ACCP must be profitable for all its members and the goal is to find the best balance between enough risks for CMs to have skin in the game and enough rewards to incentivize them.

- Default Fund Contribution :

Too little participation would make the Clearing Member not run due diligence on the ACCP models, contracts and other CM behavior. While too high DFC increase might raise the expected shortfall too much, attracting fewer capitals. A large junior tranche might have the same effect as too little DFC requirements, as well as disincentivizing CMs to bid on waterfall auctions.

DFC could define a higher share for players who bring less risk, but this would incentivize players to perform a Sybil attack. To avoid similar unwanted behavior and increase scalability, DFC must be defined locally without comparison with other members. Historically, giving small property owners rights has often led to economic development.

For the Bilateral case, the Default Fund adds to the Initial Margin mainly an incentive not to default. While IM is based on VaR, ES or other models, the extra liquidity buffer that DF represents must cover price jumps where the counterparty is incentivized to default; a diversified bilateral-only counterparty is unlikely to default because of other DFs in other positions.

The total default fund is calibrated to cover the default of X or X percent of participants defaulting within a short period of time. If the goal is to cover the loss of 20 percent of the participants, we first estimate the loss associated with scenario-based tests and then the amount required of DF deposit upon novation. Furthermore, at position closeout, an ACCP model can decide to lock it for more time to ensure all CMs have skin in the game, and are not here just to ride the bull market and go away. When CM locks DF, they can receive ACCP equity, which in case of loss, can be used to recover funds later.

To illustrate, let's calculate the expected loss due for a CM to compute an approximation; this formula is only to give an idea, production formulas are more complex and subject to future publication:

$$\begin{aligned}\text{EL} = \text{Margin} * \left(\frac{1 - \text{Recovery\_Rate}}{1 - \text{Tail\_Factor}}\right) * \left(\frac{\text{Default\_Volatility}}{\text{Current\_Volatility}}\right) \\ * (\text{Default\_Intensity} * \text{Period}) * P(\text{Loss} > \text{IM})\end{aligned} \tag{2}$$

This is computed on an outlier scenario where `Recovery_Rate` is the rate of recovery after the stress period, `Default_Volatility` is the volatility associated with defaulting, `Current_Volatility` refers to the present state of volatility, `Default_Intensity` represents the default intensity in basis points, `Period` is the intended time period for the evaluation, $P(\text{Loss} > \text{IM})$ is the probability of losses exceeding margin, and `Tail_Factor` is for tail behavior quantification.

- Junior tranch :

ACCP junior and senior tranches can be funded by non-CMs for a share of fees. Since the risk management rules are predefined by a smart contract, the decision of financing these tranches falls to speculators by modeling ACCP Risk Reward model. ACCP risk mutualization doesn't eliminate risk but will transform idiosyncratic risk into an aggregate risk, whose risk can be modeled.

Junior tranche depends on the return rate and risk ratio; a higher risk ratio is compensated by an increase of clearing fees going to the junior. Similar to AMM LPs, an ACCP with a bad risk model won't reach demand. If an asset holder or a foundation wants to make their token more attractive, they can invest in the junior tranche to reduce the risk on CMs, reducing DFC requirements and requiring fewer fees to cover risk.

The junior tranche deposits use the same collateral agreement as the ACCP with the same haircuts.

12 Default event

The default event happens when $-uPnL > IM + \sum C[k] = 0$. In the case where - uPnL ¿ only IM, a margin call is made, but because of locked IM, default of F[1] doesn't mean default of F[2] in the case where - uPnL F[2] ¡ IM. The defaulting party is responsible for margin calling his positive positions before a liquidation event, but this margin call can be triggered by a non-defaulting party to avoid their counterparty from defaulting, although if the default fee is high enough and market condition liquid, defaulting counterparty can be profitable.

To trigger a default, a liquidator, against a fee, calls oracles on a list of defaulting positions. Once a position is defined as defaulted, the defaulted method linked by ID in P[k] parameters is run.

Following the conditions for a default event, a procedural mechanism is encapsulated in the function `is_default(list` $P[k]$`)`. This function fetches real-time data, including the mark-to-market (MtM) values and initial margin (IM), to evaluate the default risk associated with each financial position $P[k]$.

The algorithm calculates the total cost C_{tot} by aggregating the weighted values of each position, and then computes the unrealized Profit and Loss (uPnL). A default is flagged if $uPnL - IM > C_{\text{tot}}$, prompting the invocation of `default_method(P[k])` to manage the defaulting position.

Post-default procedures are context-dependent. For bilateral contracts, the focus is on collateral management, while Automated Central Counterparties (ACCPs) may involve additional complexities, as described in the Waterfall Recovery section.

This function serves as a real-time computational tool for identifying and managing default risks, supplementing the mathematical framework previously described.

For a bilateral contract, `default_method()` will only involve some volatility threshold check and collateral management. For an ACCP, all `F[k]` IM owned by a `C[k]` novated in the managing ACCP can be used to avoid the default, and management of position neutralization to default requires some additional management partly described in Waterfall Recovery section. This results in a non-time deterministic collateral management. In the case where there is not enough collateral to repay a bilateral position and `C[k]=0`, the pending amount to be repaid is attached to the deposit function. A counterparty with a diversified portfolio is unlikely to default his whole portfolio for 1 volatile asset.

As everyone can predict when a position will default because of transparency and determinism, any CM can propose a pre-default price to buy a defaulting contract prior to the default. The best price will be closed at the default event. The CM with the best bid earns on premium between the defaulting price and the buyback price. To perform this action, the CM locks IM and DF + a buyback price locked for a period `T` to avoid spam. The buyback price can only be with a premium paid by CM IM+DFC. For additional premium that requires junior tranche and DF contribution, a post-default auction must be run. The bidding CM can be outbid by another CM that will lock itself collateral and unlock the outbid CM collateral. The best bid is taken when the position defaults; this allows to neutralize instantly ACCP defaults.

As creating a default method that doesn't apply if there is an earthquake or based on credit downrating of an entity, we define volatility kill switch that puts loss on non-defaulting CMs or counterparty in the case of a bilateral contract. Volatility is used as when an instrument reaches abnormal levels of volatility it is generally due to a fundamental event like a hack, law, catastrophe and other physical events and because it is callable by oracles. We remind that the ACCP responsibility is to cover defaults of its members, not to cover market risk itself.

13 Waterfall recovery

When a waterfall event could not have been prevented, the next step is to ensure the loss is reduced and distributed fairly.

An auction can be English, with the bidder increasing the buyback price, sealed-bid for time efficiency where all bids are submitted privately and the best bid wins at reveal, or Dutch, with a time decay modifier where the position value decays by x percent per block and the first bidder wins the auction. Multiple auctions can be run, for example, starting with an English auction for the first 5 minutes then continuing with a Dutch time decay auction.

The auction process serves multiple types—English, sealed-bid, and Dutch. Upon auction conclusion, assets are settled using a hierarchical financial structure starting with the defaulting party's IM. If insufficient, the process moves to the DFC, followed by Junior and Senior tranches.

In the absence of bids after time $X1$, the algorithm either cancels the auction based on a volatility check or launches a split portfolio auction. Beyond time $X2$ without bids, a time decay auction is activated.

Each ACCP chooses their auction method to minimize their loss, it can be a time decay of price, a 2 month standing, selling the portfolio as a whole, selling instruments individually, making a book of all defaulted contracts, coupon for non-defaulting counterparty, or CM closeout netting. Additionally, low participation in an auction by CMs can be used as a parameter in a model to delay the auction due to probable market mispricing. Requiring CMs to participate in auctions creates an additional skin in the game filter.

Default auction buyers, instead of finding instant liquidity, can take the risk of finding a statistical hedge, to mitigate loss until finding the proper liquidity and premium fee. Optimized liquidation strategies as shown by [9] can have a 50+ percent loss difference compared to blank default, CM buyback strategies can remain private to generate edge profit while benefiting the overall market. This default recovery process allows benefiting pricing hedge strategies impossible to implement at a smart contract level.

14 Mark to Market

Mark to market (MtM) is a valuation method that uses more computation than vanilla price definition based on market, highest, blended market/highest. The Average Blended Market/Highest method takes the average of the blended prices/highest obtained from multiple market sources. For example, for low liquidity markets, the spot price cannot be accounted as contract price, and so a valuation method is needed. The most basic ones in this case are VWAP and TWAP but can be more complex with asset triangulation or methods based on other external data like Black Scholes for options or floating index rate index methods or IRDs.

Instrument prices can differ from broker to broker. The MtM must be defined on the contract open to optimize the hedger's cost while being fair to the non-LP party. To get exact prices and compensate for oracle lag for hedgers, price is defined deterministically by a consensus and needs to be standardized among all participants based on an exact data timestamp agreed among all nodes. For this, multiple methods can be used like when a block is mined, on the third mined block, or at a defined timestamp in the price oracle call superior to the block mined timestamp.

Another class of MtM is XVA methods that are typically used especially by banks to account for the various costs and risks of low liquidity sophisticated OTC derivatives. We can count Counterparty Valuation Adjustment (CVA) which covers counterparty credit risk, Funding Valuation Adjustment (FVA) which quantifies the costs of collateral funding, Margin Valuation Adjustment (MVA) which covers the cost of posting IM and DF, and KVA or Capital Valuation Adjustment which captures the cost of holding capital against counterparty risk.

In finance, only a few highly specialized firms are cited as having reached a satisfying MtM model quality on low liquidity assets. It is unlikely that complex non-standard MtM definitions on OTC products are possible. To trade this kind of asset, instead of trading notional, IR might be more suitable or another instrument class.

15 Novation

Novation is the process of transitioning from a bilateral position to a state where the ACCP becomes the counterparty for each party.

As ACCP parameters are standardized, at novation, parameters need to be adapted and a new position F[k] emitted. It is obviously possible to compute in advance whether a novation is accepted or not as the acceptance relies on a set of on-chain parameters to check.

The function named `novation` serves as an algorithmic cornerstone in representing the novation process within the ACCP environment. Upon confirming the membership, the algorithm assesses whether these clearing members meet the ACCP's margin requirements. Subsequently, the algorithm checks the position to terminate the list to avoid unwilling concentration risk within the asset class under consideration. This step ensures that the financial entities are willing to proceed with the novation without breaching their internal risk parameters. Following mutual agreement, the algorithm proceeds to execute the novation. The original position, denoted as $P[k]$, is divested into two new positions, $P[k1]$ and $P[k2]$, with the ACCP assuming the role of the counterparty for both new contracts.

As explained in the possible Attack section, if a CM thinks the concentration risk is too big, he can pay a fee to the next CM who wants to take positions that would bring the ACCP OI above a level and deny every new position as his position is not filled. This allows to manage concentration risk without adding complex scripts. This concentration risk exit is based on correlated or same risk factor Asset_Class is defined with a list in the mapping, this allows a user opening \$1 billion on a BTC contract with a maturation of 10 days to be blocked by a user wanting to exit on a BTC contract with maturation 15 days.

```
def add_position_to_terminate(P[k], liquidation_premium):
```

```
check margin requirements
check if position is already in list
if not:
    add P[k] and liquidation_premium to mapping
```

This function is called by the CM to check if he can novate a position to the ACCP, if not the party must fill first the positions. The same asset but different maturity is considered the same asset class in concentration case.

The ACCP emits a list of parameters and context parameters (Oracle callable parameters like current volatility) to accept or not novation. As markets evolve, these parameters must be updated at least quarterly, participants based on their time-weighted DF can participate in a governance vote in the form of Uniswap governance to accept or not the changes. The novation parameters should also be designed to increase standardization for better netting and compression.

Similarly, when P[a] wants to transfer his position to P[c], the position is approved automatically in case the new ACCP is whitelisted in P[b]'s ACCP whitelist, otherwise, it requires the signature of P[b] and a margin requirements check on P[c] is run.

16 Netting

Netting induces complications as it can lead to modifications of hedge inventory. The standard way is requiring a prior agreement of the party involved. Automatizing this process would require hedging inventory managers to talk with each other to find the best solution for the whole network, this can be subject to future work. The most straightforward approach lies in broadcasting optimization proposals to each network participant, supplemented with an automaton that can either approve or reject the proposal automatically based on comparison tests.

With portfolio IM models, 2 positions can be statistically netted, for example +10 XAUUSD with 30 days expiration and -10 XAUUSD with 45 days expiration would cost very low IM in portfolio IM model like SIMM.

Solving netting is similar to solving a graph problem, first, the graph needs to be defined. For each standardized product, positions of CM vs ACCP, CM vs Non CM, CM vs multiple ACCP, and non-CM vs non-CM. Additionally, highly correlated products to be included, and spread positions excluded.

Multiple ACCP members induce contagion risks between ACCPs. Mitigating this risk is impossible as one of the main features of the protocol is to make use of closed system liquidity. The risk of contagion needs to be assessed at the ACCP level in the collateral requirements computation and novation process.

IM after netting ¡ IM before netting
For A, B, and C as LP
Without Netting A-B +6, B-A +3, A-C +3, C-A +4, B-C +7, and C-B +4, Global exposure +27
With Bilateral Netting $A-B+4$, $B-C+4$, $C-A+1$, Global exposure +9 (Complexity scale $O(n^2)$).
Multilateral Netting A-C +3, Global exposure +3 (with N participant exponential risk of counterparty default)
ACCP Netting A-ACCP +3, C-ACCP +3, Global exposure +6 (High exposure is normal as Portfolio IM is not involved in the example).

If we explore an IR swap example, where A exchanges a floating rate for B's fixed rate on a quarterly payment basis, the IM based on a 99 percent MPOR VAR will spike at maturity, necessitating constant IM requirements based on these spike levels. With ACCP netting, this risk can be partially neutralized amongst participants across diverse contracts.

To achieve this, a Network Simplex Algorithm can be used, where on each loop we verify that the optimization doesn't break the rules.[8] But to go further, third parties can be appointed to find the most efficient clearing path rewarded by a fee. Given that netting could potentially decrease margin requirements by 50 percents for certain asset classes, the gains are sufficient to incentivize the emergence of a third-party market for optimal solutions.

It should be noted that while network optimization reduces counterparty risk and enhances efficiency, it also increases liquidity, compression, and counterparty risk. As such, these factors must be vigilantly monitored.

17 Withdraw

Withdrawal is a critical part of the protocol because in the case of error, the money is gone, but a lengthy withdrawal process is a cost to liquidity providers that need quick capital transfers to hedge their trades. The goal of the withdrawal process is to not involve oracles but allow sufficient time for counterparties to react and update IM. If the withdrawer has the opportunity to withdraw too much, it is the responsibility of the IM updater as this collateral is locked.

The only way to send withdrawal delay to 0 is by having an actor locking his own collateral until normal withdrawal unlock. When collateral is locked, the withdrawer can instantly unlock his collateral in exchange for a fee.

Time lock the withdrawn collateral for x minutes to allow oracle to liquidate position if needed.

```
def withdraw(amount):
if sum(C[k] * H[k]) - sum(uPnL) > sum(IM):
time lock for x minutes collateral for withdrawal

def withdraw_contest(withdrawal_id):
check margin requirements
if uPnL < 0:
maxWithdraw = uPnL ## transfer to counterparty
else:
maxWithdraw = ## owner withdraws
```

18 Oracle and Blockchain

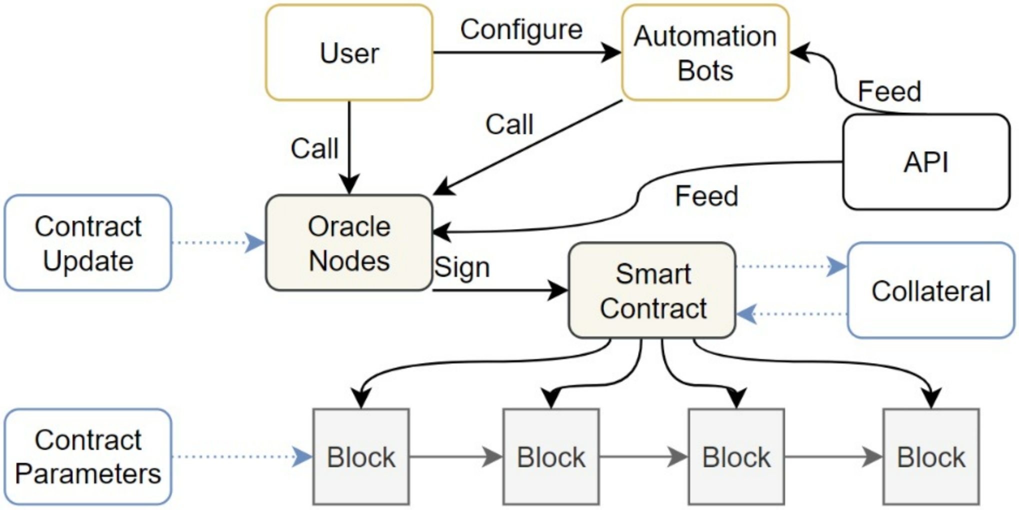
The protocol consists of an optimistic oracle network that signs on-chain transactions containing the result of computation and instrument price at a time t. The oracle network works with on-demand oracle or batched request oracle. In both cases, network delay must be compensated as discussed below.

Existing Oracle networks answering all the protocol's requirements don't exist yet in the exact form due to the lack of needs of this kind of technology to answer non-existent problems.

To keep contract parameters and collateral, the protocol is using a third-party Turing-complete smart contract blockchain. Working with an established chain is more a strategic choice than a technical one, it allows users to keep their same UX habits acquired with other protocols, doesn't add bridge liquidity needs and allows only focus on developing the oracle.

Oracle caller puts the result of his own computation and each address can delegate a node to always be selected when he is assigned to send the right computation or raise a dispute.

The choice for a dApp to run a POS with its own token is often criticized. The derivatives use case is big enough to generate sufficient fees to maintain incentives, moreover, Microderiv is only a base layer built to allow an entire ecosystem of dApps. In the case where the protocol scales, the protocol is unlikely to run on a single uncustomized oracle network. Basing security only on economic incentives with node slashing as collateral might not be sufficient to cover derivatives leveraged value. This problem is usually mitigated through token rarity and fair distribution.



With an optimistic network, one major threat is called the verifier's dilemma, it happens when no one verifies an attacker's transaction due to not enough attackers to make it worth getting rewards verifying the network. Since the protocol includes an economy of actors computing routines, this can be compensated with a user paying a set of trusted parties to verify his transactions. Moreover, IM locked reservation mechanism is made to avoid cross margin data and sequencer attacks.

An easy way to significantly increase security is by having different groups that are required to gather and treat the same information while each individual group have their own quorum and technology so the probability of an attack is low.

Scalability :
Many computation-intensive methods have been shown in this paper, and if all are required for nodes to compute, the protocol would unlikely be able to scale. We propose multiple optimizations where the goal is to reduce as much as possible the number of oracle calls, and to simplify the models with parameters like correlation computed bi-monthly.

Moreover, the protocol is made to reach small and big players, since every trade is individual, both of them might not require the same amount of collateral and consensus to secure users. Small players usually seek for speed and large players, since they impact liquidity, don't really care about speed but security. A large collateral trade can ask to reach a broader consensus. To have local and general consensus can be organized around every x percent of price move on an asset requires an 80 percent consensus, this way if an attacker can capture a local consensus, the loss will be limited, and so unlikely to provide enough incentives to the attacker.

Since IM is deterministic, both parties can compute the required IM without making oracle calls. Oracle calls are only used in case of disagreement and cost to the party who is not respecting the rules by itself. Also, IMs are designed as a fractal, an IM can hold an entire portfolio on a L2 with themselves IM who can hold a portfolio of IM itself.

Since the oracle network is specialized in one application this allows optimizations that a Turing-complete network couldn't reach. We can, for example, have a small group of nodes that validate x amount of withdrawal on a CA and then it needs to reach a greater consensus of the network to re-allow the small group of nodes to retract from their duty or be able to continue. Local groups are an important optimization as data availability is an important requirement, and some data price feed might be accessible only for a cluster of nodes.

- Price oracle :

Oracle computation for trading with hedging requires that the local hedger be able to predict future oracle outcomes in order to modify his hedge accordingly. This means contracts can request past values of AssetPrice, Correlation, InterestRate, Variance, Volatility, Curvature, Delta, Vega at a specified timestamp. Some of these metrics, like volatility, only require hourly close data of all years since asset inception for FHS; smaller data points like each second need to be stored in memory for the last x minutes and can be deleted after.

A message is sent with a timestamp that must be defined after the message is validated by the local blockchain consensus. It allows both parties to react instantly. This allows dealing with the optimistic network delays. This allows batching price calls together for scalability, for example, at t=1, a closing order at mtm is approved at 1000, and at t=2. At 1010, the oracle batch reaches consensus and pushes on-chain the exit price to be used in contracts.

Price oracle manipulation has led to many hacks, and some special price models might be required like VWAP, as it is naturally implemented in some DeFi protocols. The VWAP must be computed for other assets. In some cases, VWAP might be too inaccurate; in this case, short-term price manipulation can be avoided with the per-second price stored of the last x minutes with a volatility threshold as well as an error threshold between price sources. Another option to decrease price oracle risk is to pass the concerned asset into auction mode in case of a volatility spike to avoid rogue pricing.

The average of multiple data feed sources is commonly used to alleviate any data source exploits, at the cost of increased hedging costs. For larger trades, instead of an average price feed, a more practical solution for hedgers might be having multiple counterparties that individually are associated with a price feed and the sum of all subpositions is the same as a position with an averaged data feed from multiple sources.

As the third-party service economy develops around the protocol, there is a potential market for manipulation coverage. Someone can additionally lend money to avoid liquidation of a participant, and if the market recovers, they collect a fee. This would make market manipulations not worth it. The one to get trade cover enters an input of how much percents of his position he is willing to give after recovery. This can be especially useful to avoid CCP exploitation, and if exploitation arises, less money is lost.

In case of a stock split, one party is incentivized to not agree on updating the quantity inside a position. This event must be handled by compensating the oracle price feed on the oracle and creating a new price feed for positions. EffectiveDate and AdjustmentRatio parameters must reach a consensus.

19 Automatization and transparency

Blockchain transparency brings several advantages in risk management. As more positions are publicly displayed, so are their liquidation prices, leading to ease in modeling and forecasting shortfall, allowing participants to prevent shortfall, thereby lowering the risk of the event. Predictability is not to be underestimated; it is the single factor that motivates 30 tbonds buyers.

CCPs are recognized for their compression abilities due to their internal transparency in a private market. The blockchain, with the right incentives, allows third parties to specialize in compression and market automatization, eliminating some intermediaries between the product issuer and the end user.

Some might find the cons of transparency as the risk of front-running, copy trading, or losing alphas. Risk cannot be mitigated with privacy as a counterparty can be incentivized to reveal information to an exploitation specialized party. Front-running must be dealt with through time uncertainty of hedging while copy trading can be taken advantage of if systemic.

In the traditional OTC derivative market, when engaging in a trade, the costs typically involve establishing and maintaining relationships with multiple counterparties. These costs may include credit risk assessments, legal documentation, operational processes, settlement risks, and potentially higher capital requirements. All these costs are non-existent with a transparent blockchain. ISDA estimates that digital derivatives can cut half of the workforce, an economy that would make many financial entities profitable even if it means revealing data about trades.

In general, free competition between counterparties leads to better rates and fewer intermediaries, which are omnipresent in finance, as product issuers can trade directly with the end of the chain risk taker. Decreasing the number of counterparties and transparency decreases cascade risk and the margin requirements needed to compensate them.

Smart contract law is code automatization offers several advantages worth noting. OTC derivatives must be backed by a country's laws, making cross-legislation trades and products a huge burden to solve. When these contracts are determined by trustless smart contracts, this makes the operation a lot easier. Moreover, without automatization, retails will never be considered as the workload requires multiple specialized full-timers.

To showcase the importance of transparency, let's take an example of a private blockchain. We will make the assumption that the same protocol with an oracle is possible. We would observe several new intermediaries as it is difficult to replace intermediaries that you don't know the source of, higher risk as an analysis of concentration risk is not possible, and hidden rehypothecation of collateral. [5]

20 Risk Management

Most of the following risks can be addressed simply by increasing margin requirements, which would be a faulty answer.

Counterparty Risk and Credit Risk:
These risks come next as they directly deal with the potential of a counterparty defaulting on its obligations, causing significant financial loss. The ACCP loss mutualization design is meant to address this risk.

Liquidity Risk:
Loss due to inability to convert an asset into cash at a given price and period,

this risk is often correlated to unpredictable market events making it hard to be efficiently covered by IM. To reduce this risk, CMs are incentivized to stop waterfalls, if there is liquidity in the market, CMs will find it.

Operational Risk:
These are the risks related to day-to-day operations, this mainly includes blockchain, oracle, and third-party automation failures.

Concentration Risks:
This is the risk of having too much exposure to a single asset or sector. If a significant crash occurs in that area, the entity can suffer severe losses. For example, if $100M$ is borrowed against $1B$ of a low liquidity token, even at 10:1 in case of a crash, $1B$ of the token won't be sufficient to get back $100M$ cash. To alleviate risk, we introduced a way to allow CMs to force exit their position before new novation on an underlying asset.

Correlation Risks: This risk emerges when different segments of the ecosystem become affected in case of a market downturn. The more an ecosystem has different usages/categories of users, the more it is covered to risk in case a segment takes a hit, same for derivative if 50 percents of OIs are in spread swaps and 50 percent in directional swaps on the asset, in case of high volatility fewer OIs will be liquidated compared to an ecosystem with 100 percent directional or 100 percent spread.

Collateral Risks:
If collateral devalues or becomes illiquid, it can lead to significant financial losses. To mitigate this risk, haircuts on collateral value are defined in the CA.

Wrong Way Risk:
This risk refers to the potential increase in exposure when the likelihood of counterparty default increases. The wrong way is often correlated to contagion risk, incentivizing diversification can offer an effective mitigation.

Model Risks:
If the models used to calculate and manage risk are incorrect or misused, it can lead to significant financial loss. This risk is to be mitigated by open sourcing models and through peer review.

Procyclicality Risks:
These are risks that can exacerbate economic downturns, potentially leading to significant losses often due to overestimation of future upside or negligence of outlier events in a low market volatility period. This can be alleviated using floors on IM and other factors, by installing a liquidity buffer which is adjusted lower as volatility increases; increase the look-back period and stress testing requirements.

Long tail/Fat tail Risks:
These are the risks of rare but extreme events, which are often underestimated or ignored in traditional models. Long tail assets require specific models like GRID instead of SIMM for portfolio IM calculations.

Backtesting and Stress testing:
Primarily used for validating and testing resilience models and strategies. Stress testing can be done by generating pseudo random scenarios based on parameters, like Monte Carlo simulations or through outlier market scenarios like "falling yield" scenario "inflation", "equity crash", "crypto black Thursday", "September 11", "dot com bubble", "2008 global crisis", and "2011 EU crisis". Scenario-based is more likely to be used in stress tests as it is less computation intensive and not parameter dependent. Not only stress testing oneself, but stress tests should include a framework for protocol participants to test their systems on a testnet.

Reverse Stress testing:
ACCPs reverse stress test results showcase minimum threshold to deplete waterfall mechanisms and the distribution of uncollateralized stress loss as a way of demonstrating the appropriateness of the coverage model. By showcasing the distribution of uncollateralized stress loss and the amount of stress needed to deplete waterfall mechanisms, the ACCP can provide evidence or proof that its coverage model is appropriate and effective.

We chose to ignore credit rating or other reputation systems due to the fact that even in a regulated world it can mislead risk calculation because it is not possible to control each position a regulated entity takes that can lead to substantial loss, the same assumption can be made in crypto with the fact that it would require a corruptible governance system.

- Open source risk management :

Open source and forkability make it easy to build in DeFi compared to modern finance, each builder can compound on what previous builder did achieve instead of wasting energy on the basics. Financial models and their implementation can become very studious and due to a lack of motivation, risk management becomes a secondary goal, giving a significant advantage to bigger structures, and in many cases, an entry barrier, increasing the risks on the financial market.

But yet in crypto, open-source risk management is not widespread, as some private actors (e.g., Glassnode, Nansen, Dune) represent the majority of the market and still not used by retail. It seems that risk models need to be automatic and integrated into the trading process, meaning built inside dApps, and fund management directly. As long as no few line implementation tools for that kind of tools and models are available, builders who don't know quantitative finance are unlikely to close the gap themselves, an outcome that can bring prejudice to microderiv scaling.

21 Advisors

A position can be promoted by a seller with an advisory address; this address will be paid a share of the fee upon position closure. The advisory is input into the transaction when the position is constructed on the frontend. A frontend can have multiple advisors in a similar way to how Amazon uses cookies for their advisors or advertising brands use influencer codes. These systems can be manipulated; one common preventative measure is converting the advisory code into a fee reduction and limiting the distribution of these codes. On the technical side, an oracle sends the money to the advisor when processing the position close.

It is said that Blackrock inflated the gold price tenfold due to their aggressive advisory strategy of selling gold to conservative investors for their portfolios. The vast majority of investors don't research the best investments with the best fees but will listen to an advisor. As all banks have armies of salespeople, it is crucial to compete in the following areas:

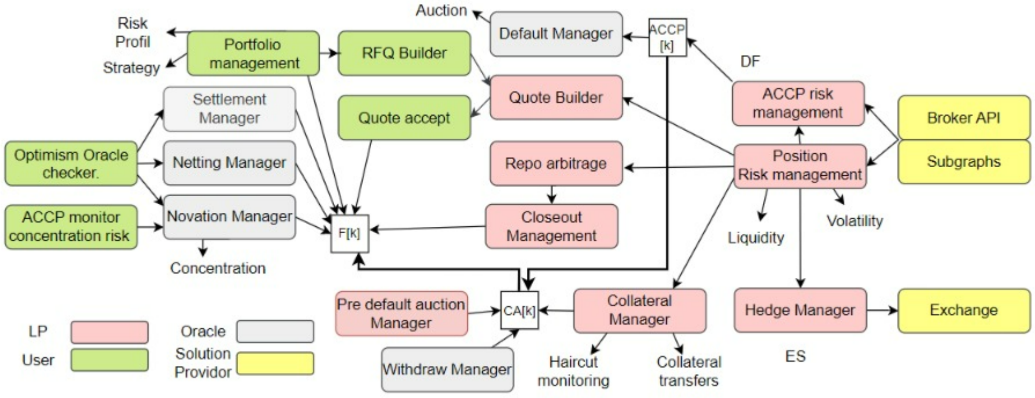
- Advertising and selling instruments

- Generating liquidity
- Assisting clients with position management
- Performing financial modeling, valuation, and providing analysis
- Creating and building relationships

Automating these tasks allows an ecosystem's advisor to go further and bring more liquidity, for example, enabling anyone to create their own trading app with their own tokens using global liquidity incentives greatly outperforms traditional employee advisors.

22 Methods

The following graph represents a rough representation of the interaction between methods discussed previously, where the LP can be represented by a set of automatization runnable by a low-knowledge user.



We can define the user experience flow more in detail through the following sets of services, which for many can be run by an open-source third party. Define Investment Objectives

- Establish investment goals, the budget for protection, and the maximum potential portfolio loss target.
- Use an automated tool to guide the user through the process, ensuring clarity and understanding of each step.

Evaluate Portfolio

- Review the current portfolio allocation using automated tools that provide in-depth analysis.
- Evaluate portfolio holdings, checking against a predefined list of assets by the system to ensure compliance.

Analyze Risk Exposure

- Use AI-driven tools to quantify risk exposures, taking into account the potential for black swan events.
- The system should identify tail risks and present them in an easy-to-understand format for the user.

Define Risk Tolerance

- Utilize an interactive, user-friendly tool for establishing risk tolerance levels, ensuring the user understands the risk/reward trade-offs.

Create and Optimize Hedge Portfolio

- Using AI-driven optimization tools, allow the user to create and optimize a hedge portfolio based on their risk tolerance and objectives.
- The system provides a suggested plan of action and recommended hedge benchmarks, which the user can accept or adjust.

Calculate Margin Requirements

- Using real-time data and complex calculations hidden behind a user-friendly interface, the system calculates new margin requirements.

Create Collateral Position

- The system assists in creating a collateral position based on the calculated margin requirements.

Monitor Collateral and Risk

- The system checks the eligibility of the collateral and calculates the risk associated with it, adjusting as necessary.
- It also calculates interest and possible substitutions.

Monitoring and Adjustments

- The user establishes a process by which hedges are adjusted over time, assisted by AI-driven recommendations from the system.
- An automated reporting system keeps the user informed about changes to VaR (Value at Risk), collateral adjustments, and other key metrics.

Reporting

- Finally, a comprehensive but easy-to-understand report is generated, detailing all the steps taken, current risk levels, and other key metrics.

23 Automation economy

More common goods and services can be exchanged in return for fee sharing, which we can categorize into three groups.

The first group includes bots that offer all the automation discussed in this paper, avoiding liquidation, managing collateral, forecasting collateral requirements, and ACCP risk management.

The second group consists of trusted parties involved in trade settlement, such as third-party oracles, Mark-to-Market price definitions, and credit ratings. Finally, there are services to onboard brokers, original issuers of financial instruments like farmers, energy extractors, governments, etc., and services that allow retail participants to become LPs themselves by providing on-chain access to liquidity restricted by borders, for example, FIX and MT5 integration tools.

24 Application ecosystem

Making a DeFi version of existing applications in finance is important, but we also observe that DeFi users are willing to adapt to new kinds of products and are ready to pay more fees for them. We can explain this adaptation phenomenon by investors who came to DeFi due to greed with pump and dumps, and ones that came due to fear and frustration, often initiated by government restrictions such as age restrictions or trading instrument bans.

Idealists make up a small part of the population, and exceptional events that push adoption, as mentioned above, are hard to emulate. The second way to overcome the barrier of blockchain's bad UX is by providing products that are ten times better than what already exists in finance. Microderiv is a Financial Market Infrastructure and needs to allow independent builders to create unique products on top to be useful.

The foremost DeFi product is stablecoins; decentralized stablecoins for a decentralized store of value, and inflation stablecoins for a no-brainer store of value. A scalable stablecoin has to be built on credit, as there are not enough commodities to back a billion users' stablecoin. We don't provide an answer here on how to achieve decentralized credit, but we can forecast that credit needs efficient and decentralized credit and interest rate derivatives to scale. For this, we have seen before that OTC products have the best balance between efficiency and decentralization needs.

In a similar way to DAI, inflation-based stablecoins can be made with "Portfolio as Collateral". Overcollateralized CAs are used to mint inflation-based tokens where the portfolios generate the inflation value and pay the counterparty interest. To allow liquidity between multiple portfolios, the ACCP is required as a risk handler. Centralized stablecoins can be used as portfolio backing or wrapped bitcoins, coupled with the same sized bitcoin short positions, with the disadvantage of needing to take more risks on the portfolio to cover extra positions cost.

Mutual funds, pension funds, and insurance come second in interest from users. The non-existence of these products in DeFi comes from the fact that the instruments used to run them don't exist in DeFi. We don't claim to bring all the instruments, but derivatives are a good enough step toward that goal. The ten times factor is the transparent portfolio manager who can be tracked and limited in the range of assets he can trade as well as track record. If we simplify a lot, a pension fund is the sum of 100 top traders, each managing a portion of user-deposited capital.

Similar to this, Yearn Finance-like strategy protocols are limited to bearing tokens. The modularity of OTC derivatives allows for the creation of a derivative of a DeFi strategy, putting the execution risk on the LP and allowing execution strategies in non-bearing token protocols. IR derivatives represent 80 percent of open interest in finance derivatives and yet almost none in DeFi, while IR protocols represent 80 percent of DeFi TVL.

Asset-backed securities like Collateralized Debt Obligations (CDO) with a basket of illiquid assets of similar risk can create a liquid instrument likely to appear in DeFi. Examples include Real Estate, Tree Farming, Credit, Community NFTs, and GameFi. This kind of asset is hard to move on the spot asset, but their exposure is easily sellable with a diverse range of derivatives.

DeFi insurance protocols haven't reached adoption by DeFi users themselves, maybe because of complexity or inefficiency. OTC Credit Default Swaps (CDS) might be more suitable to insure default risk, as it is easier to automate CDS by selling it in a composite derivative instrument than selling insurance separate from its instrument. Also, for CDS LPs, rehypothecation on selected risk-free assets to allow generating extra yield might be easier to incentivize liquidity.

25 Use cases

- A POS node owner might want to sell his variable IRs in exchange for stable IRs coming from lending or bonds.
- A retail investor might want to hedge his portfolio against a credit rating downgrade but struggle to do so because of high entry barriers to this kind of product due to their lack of automation by banks.
- @ith on-chain transparency, a key large holder of a token might use derivatives to offload his risk without selling his spot asset.
- Index or basket instruments that are hard to create with tokens but can be hedged by an LP to trade the spread between different sectors, regions, or asset classes, like short GameFi long DeFi or short BRICS long USA.
- CDS to trade the spread between the risk-free IR and a risky yield-generating asset without owning the asset itself.
- If a protocol does an ICO with vesting, derivatives allow vested participants to offload their exposure before release, reducing volatility as

events can be considered pre-priced. For example, with token-settled futures.

- Companies are exposed to risks such as currency price changes, commodity fluctuations, and interest rate variation. The hedge that these companies require often involves some specialized advisors who, for many of them, are too pricey. This gives an edge to big enough companies that are able to regulate their risk exposure.

- Moreover, in many countries, legal compliance is not necessary and can be a hindrance to being exposed to higher markets. On-chain derivatives, in some cases, may remove the need for compliance and allow companies to offset their risk. For example, energy for every company that uses gas, for retailers hedging inflation, and taking exposure to their competitors, materials, food, and component companies to lock prices in advance.

- Buying automatically a hedge depending on your type of holding. Third parties can analyze your portfolio on-chain, and propose hedges with precomputed risk management reports while taking a small advisory fee in the case you buy it. Applications that require too much knowledge for a retail investor represent an average loss. Increasing the base layer of risk management practice makes it more mature, and in the case of unregulated markets like crypto, this might attract more capital to it if applied.

26 Governance and regulation

Microderiv is a protocol that allows interoperability between permissionless derivatives DApps. In this regard, we believe that neither a foundation nor governance can effectively decide on the best risk management procedure to follow. This requires advanced knowledge in risk modeling, an understanding of each specific market, and consideration of non-public market edges. Models' adoption should be defined in a free market for efficient adaptation.

Derivatives need to be as trusted as possible, and thus active governance at the protocol level brings unpredictability to builders and users. If third-party governance manages a model, changes in models should be limited by a smart contract. Furthermore, DApps are free to use any oracle network they want; it is the protocol's duty to remain competitive.

Many financial products fail under regulations; using official price feeds also requires regulatory compliance. A DAO cannot be liable for its members' actions, and it would be too complex to verify multiple regulations, making a microderiv DAO useless in this regard. A collateral agreement can be set up to force the whitelisting of interacting addresses where, for example, KYC needs to be verified. Furthermore, a non-profit third-party security DAO might be appointed to maintain DAO security without facing legal risk itself. KYC-limited assets can be used in a KYC-only environment.

Oracle official data, such as Bloomberg's data feed on-chain, CPI, temperature, rainfall, etc. Independent price discovery mechanisms are needed to avoid relying on arbitrage between the spot price and the derivative price. We need an automatic rollover methodology, a process to replace an expiring contract with a later delivery contract for the same asset.

It's crucial to maintain risk exposure to incentivize CMs to establish low risk/non-defaulting positions with trusted counterparties. Counterparty creditworthiness scores have the perverse effect of not modeling black swan events and incrementing them in the process.
High tail event circuit breakers should be used instead of instant liquidation. Open-source dynamic testing tools for ACCP configurations (scenarios based on Monte Carlo).

IM as collateral, an overcollateralized IM that can be used as collateral for minting a token, and if its collateral level goes below, it triggers a liquidation. This is necessary for stablecoins.

Oracle-less solutions.

ACCP models for AMM-based tokens and adaptation to lending.

References

[1] ISDA Common domains, 2019. https://www.isda.org/2019/10/14/isda-common-domain-model/

[2] ISDA SIMM®,1 Methodology, version 2.5, 2022. https://www.isda.org/a/Pf2gE/ISDA-SIMM-v2.5.pdf

[3] CCP Loss Allocation at the End of the Waterfall, 2013. https://www.isda.org/a/jTDDE/ccp-loss-allocation-waterfall-0807.pdf

[4] CCP best practices, 2019. https://ccp12.org/wp-content/uploads/2019/05/CCP-Best-Practices__CCP12_Position_Paper.pdf

[5] The Promise of Blockchain Technology for Global Securities and Derivatives Markets, 2019. https://link.springer.com/content/pdf/10.1007/s40804-019-00133-3.pdf

[6] CCP Best Practices, 2019. https://www.isda.org/a/cigME/CCP-Best-Practice.pdf

[7] Compressing over-the-counter markets, 2017. https://www.esrb.europa.eu/pub/pdf/wp/esrbwp44.en.pdf

[8] Managing risk in multi-asset class, multimarket central counterparties: The CORE approach, 2015. https://www.sciencedirect.com/science/article/pii/S0378426614002830

[9] Principles for financial market infrastructures, 2012. https://www.bis.org/cpmi/publ/d101a.pdf