CLEAR

An object-oriented protocol for open derivatives

ABSTRACT

Decentralized derivatives signify the maturation of DeFi, and whether the explicit or hidden risks in DeFi derivatives can be effectively managed is the most important indication of maturity. Therefore, this paper proposes an open protocol that provides risk management for decentralized derivatives, and will assist users to control risks more effectively and more rationally. It aims to create an open protocol for all derivatives, allowing users to freely assume the seller or buyer position and to easily create any financial derivatives with a controllable risk profile.

1 Preface

1.1 Decentralized Infrastructure: From Bitcoin to Ethereum

Cross-border payment is a fundamental driving force for the global economy. Traditional cross- border payment infrastructure is built on messaging systems led by SWIFT and various national Clearing and settlement systems (such as CHIPS and CIPS). SWIFT is a Belgium-based, supposedly politically neutral international financial messaging system set up in 1973. Based on publicly available information, by the end of 2015, SWIFT has been serving over 11,000 banks, securities firms, infrastructure facilities and corporations spread over 200 countries and jurisdictions around the world. It processes 15 million messages daily.

However, as the global economy and internet connectivity grow relentlessly, this half-a-century old financial system can barely keep pace with the high velocity of global capital flow. Hence the velocity of capital flow has lagged further and further behind the velocity of information flow, and has become a burden to the development of the global economy.

On the other hand, since the collapse of the gold standard, the world has moved towards full fiat currency led by the US Dollar. However, the US Dollar has been devaluing ever since. After the cascading defaults of subprime loans led to the global financial crisis in 2008, central banks around the world had no choice but to resort to "quantitative easing", and can no longer escape from the inflation/devaluation trap.

Given the state of affairs described above, a group of geek coders launched a highly disruptive social experiment in order to create a decentralized economic system that combines Clearing and settlement capabilities to address these issues. And that has become what is known as Bitcoin today, whose anonymous creator Satoshi Nakamoto has wryly remarked in the genesis block of Bitcoin:

"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks".

Bitcoin is the first decentralized network to successfully combine payment, clearing and settlement capabilities. It is fundamentally a distributed ledger built on a P2P network, whose principal design objective is a point-to-point digital cash system. Bitcoin has since become the template of a

decentralized economic system, spawning a great number of modifications on top of it. Modifications built on the Bitcoin protocol blossomed and gave rise to various blockchain protocols with far reaching impact, such as the famous Omni (originally called Mastercoin), which is a second generation blockchain creation built on the Bitcoin protocol, and eventually morphed into the well- known Stablecoin Tether(USDT)'s initial issuance protocol.

However, since the Bitcoin protocol is designed as a digital cash system and not as a general purpose foundational protocol, developers can only build and modify on it with very limited options, and are practically unable to write complex applications on it. Increasingly the Bitcoin protocol could no longer fulfill the demands of a truly decentralized economic system, and hence a second generation decentralized infrastructure was born – the decentralized application platform Ethereum based on Turing complete smart contracts. Turing complete refers to a logical machine (in the computer science sense) that can process any finite mathematical program, which means that it enables the developer to construct any arbitrary programming language to accurately describe any realizable application. Even though Ethereum's lack of scalability and high gas fees (i.e. transaction costs) are still being criticized today, there can be no contention that Ethereum has truly provided robust infrastructure for the proliferation of real-life applications. In the span of a few years, a number of decentralized economic systems, driven by DeFi, covering trading, lending, governance, NFT and other important applications came into existence.

1.2 The Dilemma and Explosion of On-chain Liquidity: from EtherDelta to Uniswap

Liquidity lies at the heart of capital markets. Before the birth of Ethereum, blockchain protocols could only function as payment transfer instruments. Blockchain native assets such as Bitcoin still relied on centralized exchanges such as Coinbase for liquidity. However, centralized exchanges not only broke the chain of trust in decentralized ecosystems; they also succumb to criticisms due to security, transparency and centralization issues. Their reputation also suffered after the Mt.Gox exchange hack incident.

1.2.1 EtherDelta and Bancor

Since the birth of Ethereum, its Turing complete smart contract capabilities truly empowered developers to create rich and diverse applications. Due to natural pairing of blockchain protocols with financial systems, the first batch of core applications on Ethereum centered around management and usage of on-chain native digital assets, including DAO and DEX. However, in the process of developing on-chain applications, aside from the security issues of smart contracts, the "liquidity dilemma" of on-chain assets had frustrated developers a great deal, and became a major obstacle to the blossoming of Ethereum applications.

To resolve liquidity challenges for on-chain assets, trading platforms and tools for these asset must first be addressed, i.e. decentralized exchanges (DEX). In 2016, first generation of order- book driven DEX such as EtherDelta was born on Ethereum, and represented the first step to trade on-chain assets while maintaining decentralization, transparency and fairness in every step of the transaction. On the other hand, because the first generation of DEX as exemplified by EtherDelta utilized an order book template, contracts interacted in a complex manner and user experience suffered. Besides, liquidity remained dismal due to the lack of market making strategies. It could neither satisfy the demands of coins at end of the long tail, nor could it satisfy the large scale trading requirements of mainstream coins. Hence, the Ethereum project Bancor proposed a solution - using smart contracts to continuously provide liquidity for on-chain assets, and the exchange of the asset pair is guaranteed through a price mechanism based on their bonding curves. The price discovery mechanism of the Bancor protocol solved the liquidity problem for thinly traded on-chain assets, and was subsequently used for the trading of EOS memory and asset exchange for the famous gaming application Fomo3D.

Unfortunately, the price discovery mechanism of the Bancor protocol is extremely complex, and never fully incorporated the role of liquidity provider. Hence, it could barely resolve the issues of liquidity growth and aggregation for on-chain assets. It had to rely on the liquidity available at the time when the smart contract was created, and could not support large scale transactions of on- chain assets. This "liquidity dilemma" had been a major stumbling block for the development of Ethereum applications, and not completely resolved until the explosion of Uniswap.

CLEAR

1.2.2 Uniswap and DeFi 2.0

The thinking behind Uniswap can be traced all the way back to 2016 when the Ethereum founder Vitalik Buterin published an article titled "Let's run on-chain decentralized exchanges the way we run prediction markets". The article described a design concept that circumvented the order book exchange idea and was later implemented by Hayden Adams. Compared to the complex design of Bancor, Uniswap employed the simple and elegant x*y=k pricing curve, and introduced the AMM (Automated Liquidity Provider) mechanism to resolve issues of liquidity growth and aggregation. Uniswap also allowed users to freely exchange arbitrary ERC20 tokens on DEX through multiple routes of existing trading pairs. As the market recovered in 2020, DeFi ecosystems blossomed with infrastructure such as Uniswap and Compound. As of the end of Q1 2021, the accumulated trading volume of Uniswap already exceeded USD 246bn with over 72,000 liquidity providers. More importantly, Uniswap is highly composable, and has been integrated in over 200 DeFi projects. It has since become an open ecosystem with sustainable growth, and the fundamental liquidity infrastructure for the booming DeFi world. The Uniswap Pool and AMM designs have been widely adopted by various DeFi application, and drove the boom in EVM-based public chain ecosystems including BSC and Polygon.

According to the ConsenSys' 2021 Q1 research report protocols and financial instruments on Ethereum are growing robustly, with over 146M addresses and a total ecosystem valuation of over 53bn USD, covering stable coins, lending protocols, prediction markets, leveraged tradings, payments, insurance and NFT trading. The entire blockchain industry, obviously, is more than just Ethereum. Public chain ecosystems such as BSC, Polygon, Solana are also growing rapidly. According to data from CoinmarketCap, the total locked asset value for the entire crypto industry is approaching USD 2.5 tn. We can thus infer that we are at a historic turning point of DeFi 2.0 where fundamental liquidity infrastructure has increasingly improved and liquidity has reached critical mass.

1.3 DeFi 3.0: Decentralized Derivatives and Open Risk Management Protocol

Uniswap built the iconic infrastructure for DeFi 2.0, and now, the infrastructure and liquidity provision for the entire industry stand ready for the next phase known as DeFi 3.0: a mature financial system with decentralized derivatives at the core. Drawing on the developmental history of the traditional financial industry, DeFi's new trends will be the genesis of sophisticated and professional derivative products built on the foundation of full-fledged infrastructure, and the industry does desperately need mature and sophisticated derivatives for risk hedging and management in an environment of ample on-chain liquidity. Hence derivatives will be the inevitable in the next phase of DeFi development.

The Evolution of DeFi
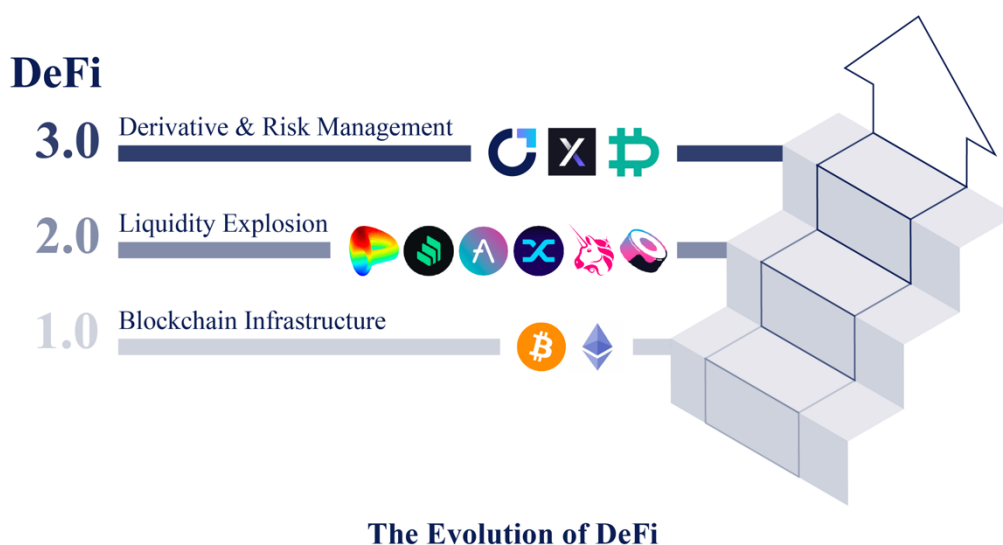
But derivatives risk profiles are open-ended, and the participants in the decentralized derivatives market including liquidity provider only have limited resources to hedge risk. To overcome this theoretically intractable challenge, derivatives in traditional markets are heavily regulated to manage the unlimited downside. In cryptocurrency markets, however, since the asset class is inherently open and globalized, no single party can impose a rigorous and comprehensive regulatory framework.

Hence, to overcome this challenge that stands in the way of DeFi's next phase, we believe that the cryptocurrency asset class desperate needs to establish a suite of Uniswap-like open risk management instruments to further the development of decentralized derivatives.

Thus the ClearDAO is born.

2 The ClearDAO

2.1 Vision and Features

ClearDAO is an object-oriented protocol for open derivatives, which enables users to control risk rationally and effectively. It aims to create a derivatives ecosystem, allowing users to freely assume the seller or buyer position and to easily create any financial derivatives with a controllable risk profile. To this end, ClearDAO exhibits the following core features:

• Open Derivative SDK

Highly adaptable SDK allows developers to create new derivatives. The SDK is the core product of the project. The ClearDAO team will keep adding support for more underlying asset classes and derivative templates to the SDK to expand its composability and expandability.

• Community Driven Market

The ClearDAO is designed specifically to invite community members to launch multiple trading platforms and build the ecosystem together. With different front end interface implementations and inclusion of additional elements such as gamification, the ClearDAO community as a whole will lead the next wave of DeFi that is the derivatives space.

• Risk Management Library

Quantitative tools that implement a two-tier reserve pool system to provide dynamic risk management for derivative instruments. This new module provides trading platforms with enhanced stability while minimize the resources required.

2.2 Blockchain Architecture

As an open protocol for decentralized derivatives, ClearDAO will be built on Ethereum in the initial phase. It will later gradually support multiple mainstream public chains with an interoperability layer in later stages. Its basic schematic is as follows:
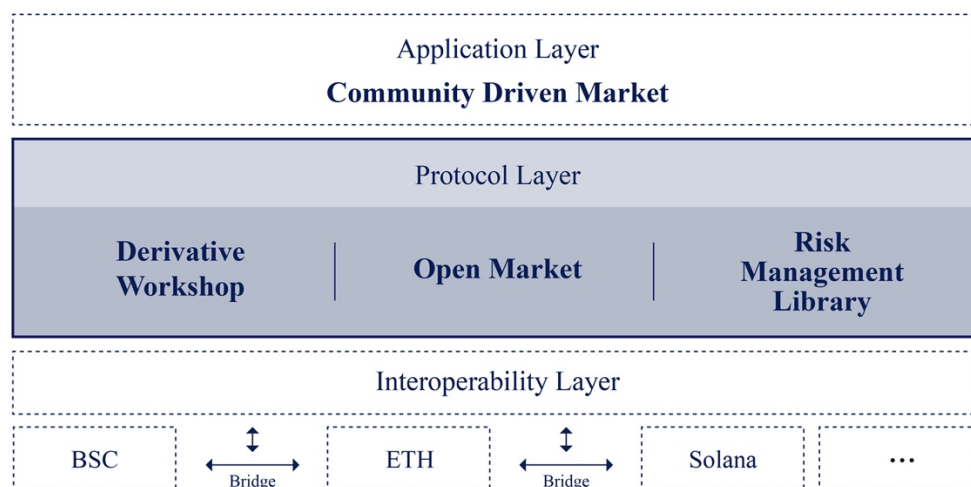
The core layers of the ClearDAO system are briefed as follows:

• Public Chain Layer

This layer refers to the underlying infrastructure that provides ClearDAO the interaction interface to all the major public blockchains. It can extend to more chains to capture more users across different ecosystems and communities.

• Interoperability Layer

The interoperability layer comprises two parts, the customized bridges between heterogeneous public chains and general interface across the homogeneous chains such as EVM-based interoperability interface. This layer is mainly responsible for regulating the interactions between the upper ClearDAO layer and all the underlying public chains. It also houses the cross-chain L2 solution.

• Protocol Layer

The protocol layer refers to the ClearDAO, which is the core of the entire system. The protocol contains three main modules: derivative workshop, open market, and risk management library. The derivative workshop is responsible for the creation of open derivatives. The open market is a trading platform template to allow entry-level developers to launch trading platforms with their own brandings and identities. The risk management library is a set of quantitative tools to allow trading platform users and the platform itself to manage risks in a resource-efficient manner.

• Application Layer

The ClearDAO SDK makes launching trading platforms on the application layer simple. Developers can also use the SDK to construct derivatives that meet the needs of the market. It is even possible to use the SDK to build new applications that centers around decentralized derivatives.

In this blockchain architecture, the public chain layer mainly provides security and liquidity for crypto assets; the interoperability layer mainly secures communication and transformation across various public chains, including cross chain assets and information; the ClearDAO contains the main code that defines the building blocks of derivatives; the application layer is where developers build on top of the ClearDAO using the Clear SDK.

2.3 The Design Principles of Core Applications

In the ClearDAO system, the application layer is the main object of user interaction. ClearDAO's core application modules, which run the main business, are designed according to the following principles:

• Option Pricing Principles and Models

The pricing of vanilla options normally follows the BSM (Black-Scholes-Merton) model, but the blockchain cannot guarantee that the option seller with limited liability can actively fulfill its obligations to pay on time. Thus, liquidity providers on ClearDAO provide spread options with barriers to traders who can bet long or short or both. The structure of spread option guarantees that liquidity providers have sufficient funds for their maximum payout so that they can definitely fulfill their contractual obligations.
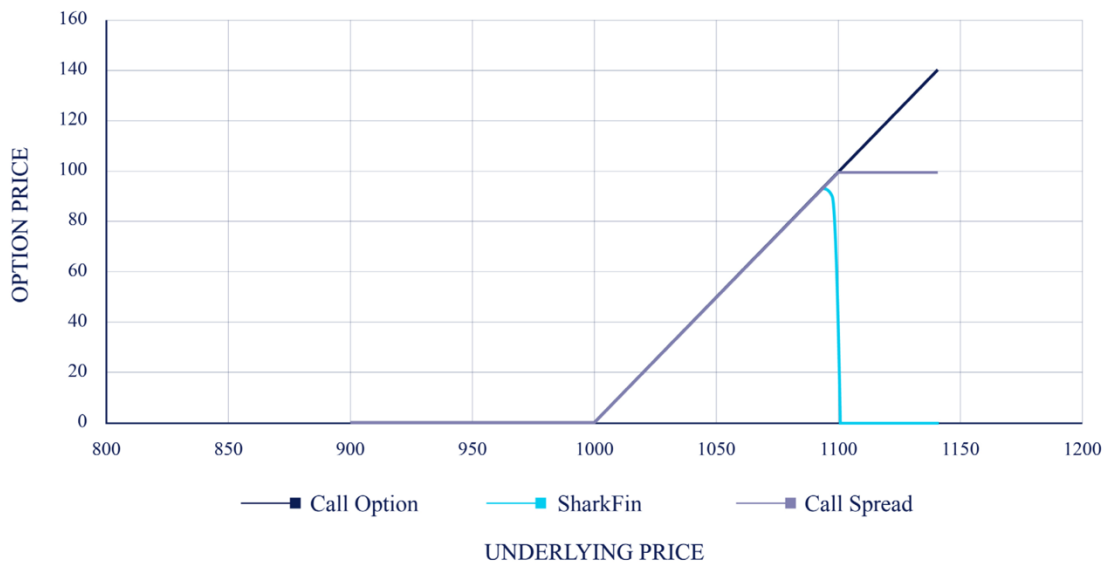
Theoretical Pricing Plot

We deployed QuantLib, a standard open source modeling suite, as our option pricing models. Liquidity providers on ClearDAO can choose a readily available reference asset pool or define their own, and then build their own options by setting their own barriers, maturity dates and other parameters. When users choose to buy a specific option, the parameters will be fixed, and Clear's pricing module will automatically quote a price based on QuantLib models.
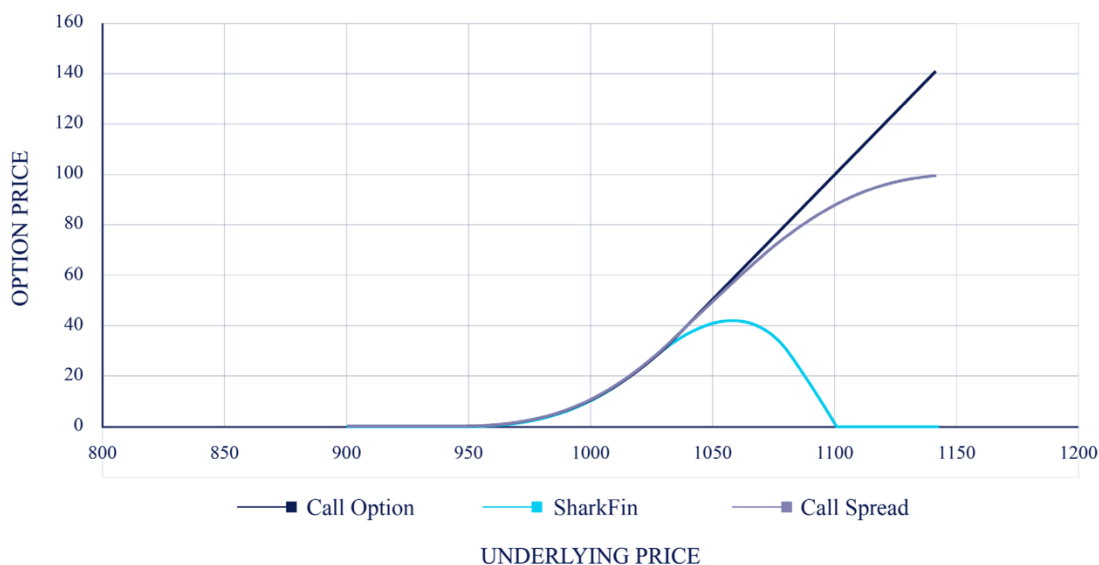
Pricing with Volatility

Furthermore, the pricing models deployed by ClearDAO are extendable by design so that liquidity providers can price with a Generalized Black-Scholes Process or a binomial tree as or Monte Carlo simulations as they see fit. Traders (users) can also choose quotes from liquidity providers that quote with pricing models that they approve. For professional investors, we suggest them to hedge their positions themselves according to the open pricing models that we offer. This stays in line with our risk management mindset.

• Risk Management Principles and Models

ClearDAO builds in multiple levels of risk control mechanisms to handle multiple risk scenarios to assist users and liquidity providers to effectively control risk. As option buyers, users need not worry about receiving their promised payoff. A robust deposit scheme ensures sufficient funds exist to close out the trade smoothly. For liquidity providers, ClearDAO will establish the world's first mutual risk reserve funding pool. Liquidity providers can contribute to the risk reserve and receive a certain level of risk protection. If the account suffers a closeout, and the deposits cannot cover the open risk exposure, the risk reserve will allocate funds to ensure the trade closes out smoothly. The risk reserve spreads the risk and returns across market participants. Every liquidity provider, through a membership arrangement, is a

contributor and a beneficiary of the risk reserve. This avoids the moral hazard by resolving the conflict between the insured and insurer in a conventional insurance scheme. The members collectively manage and oversee the risk reserve, where each member is equally equitable. The returns of the risk reserve are enjoyed by all members. This design seeks to maximize member benefits and offers the most economically effective protection against risk for the members. In the initial stages of the project, the project operator will deposit a certain amount into the risk reserve to safeguard against large risk exposures.

2.4 System Roles and Governance Structure

Within ClearDAO system, there are three key main roles: liquidity providers, developers, and traders. They collectively make up the DAO governance council. The three roles are not mutually exclusive and are defined based on function alone. In theory, an user can assume multiple roles simultaneously. The functions of each role are defined below:
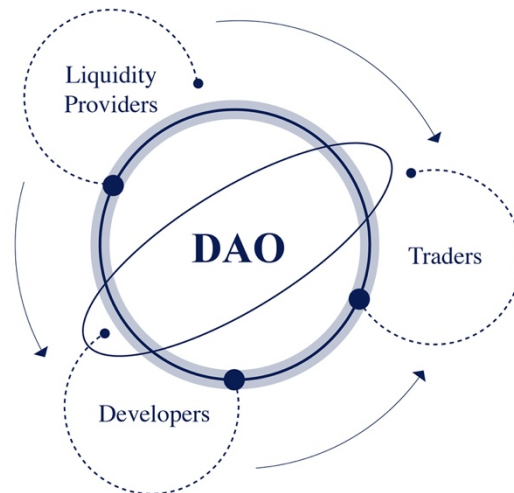
• Liquidity Providers

These are the product creators of the ClearDAO ecosystem. They define open derivatives for trading based on parameters on the Derivatives Workshop, and provide liquidity for the derivatives created. If liquidity providers lack sufficient funds, they could borrow from third- party funding sources or on other lending platforms such as Compound and Aave.

• Developers

Developers use SDK provided by ClearDAO to create and launch new trading platforms. Developers can also create their own derivatives products and assume the role of liquidity providers, or they could sell other products created by other liquidity providers. Since ClearDAO operates as an open protocol without permissions, theoretically developers can create their own products and sell them selectively to a specific clientele.

• Traders

Traders are the end users of derivative products. Hence their feedback will determine the steer the future development direction of ClearDAO.

• DAO Governance

As ClearDAO is an open risk management protocol, when all the governance tools have been developed, all updates to its core capabilities will come under the DAO governance framework including product development, roadmap and economic model.

3 Roadmap

Due to the rapid technological iteration of the entire blockchain industry, this roadmap is only for reference. Please refer to the official real-time update information for the specific development status. The roadmap is as follows:

Q1 2021

- Project genesis and planning.

Q2 2021

- Develop customization tools for reference assets, options and notes.

Q3 2021

- Deploy customization tools for testing.
- Begin development of perpetual futures and CDS customization tools.
- Add NFT support to reference assets.
- External audits on smart contracts.
- Begin development for Solana ecosystems.

Q4 2021

- Deploy perpetual futures and CDS customization tools.
- Launch Derivatives Factory SDK on mainnet.
- Release ClearDAO SDK v1.0 for developers.
- Active incentive program for platform participants.

2022

- Deploy community DAO governance.
- Integrate L2 solutions to improve scalability.
- Deploy ClearDAO on multiple blockchain ecosystems.
- Integrate cross-chain mechanism.
- Expand capabilities of customization tools.

CLEAR

ClearDAO was powered by DerivStudio,

innovators of crypto asset risk management methodology.

Follow ClearDAO on

hello@cleardao.com