# Lemniscap

## Cryptoassets in DeFi derivatives - the option use case

Research in collaboration with

BOCCONI STUDENTS
BLOCKCHAIN
CRYPTOCURRENCIES
ASSOCIATION


Students participants
Dan Dubokovič
Leonardo Malighetti
Daniele Montagnani
Matteo Montani


5 November 2020

# EXECUTIVE SUMMARY

Lemniscap

The following presentation is a joint effort by Lemniscap and the Bocconi Students Blockchain and Cryptocurrency association.

Over the summer 2020 we have witnessed to a cambrian explosion of volumes, interests and new models coming into DeFi.

The aim of this current piece of research, along with the ones that will follow, is to step back to the grounding fundamentals of the cryptonetworks in analysis and study their challenges, their proposed solutions, their business models and their use cases.

We will dwell on what token design can better represent and coordinate the desired cryptonetwork and we will try to propose improvements on how well devised incentives can offset some DeFi native limitations, such as collateralization or oracles.

We conclude with major takeaways and guidelines to bootstrap network effects and sustainability loops.

Finally, we asked to founders and designers of the protocols subject of the study to answer the same, general question about their biggest challenges and their provided solution. You can find their explanation on the last page of the presentation.

# PROTOCOL AGENTS

Lemniscap

## Buyers

Buyers want to gain upside exposure to the underlying asset (**buyers of calls**), protect their underlying asset from price depreciation (**buyers of puts**) and/or want to bet on a sharp movement from the underlying asset, regardless of the direction (**buyers of volatility**)

## Sellers

**Sellers** agree to take the other side of those trade in exchange of a premium, which can be considered an additional income on their holding locked up as collateral.

# USE CASES

Lemniscap

Countless are the implementations and applications powered by the versatility of smart contracts. Developers create decentralized financial instruments with the aim of either replicating widely used ones in legacy finance or devising newly **crypto primitives**.

Options, besides their acute and often underrate complexity, are one of the most extensively traded financial instruments in the world. DeFi founders are heads down paving the way for the gradual, yet inevitable, decentralization of issuance, trading, and settlements of options contracts

**Legacy + Global + Open + Trustless + Non-Custodial + Permissionless + Interoperable = Decentralized Finance**

The full decentralization process of option trading, however, is bumpy and not without hardships.
So far, the two biggest burdens solidifying the gap between CeFi and DeFi options are:
i) **collateralization** (hence **pricing**), and
ii) the ability for a protocol to reflect the change of the premium due to different factors affecting it, especially time knowns as **theta** or **time decay**

**DeFi vs CeFi challenges**

The most intuitive use case for option is the ability to protect your assets from price depreciation upon the payment of a premium (**insurance on your assets)**

Options, in the case of calls, give you instead unlimited exposure to the upside price evolutions upon the payment of a premium known in advance (**playing directional volatility)**

**Use cases**

DeFi certainly won't change the basic rule of CeFi: for every given buyer, there is at least a seller.
Collecting premium attracts sellers of options that DeFi dubbed as **Liquidity Providers**.
Though, not without intricate risks and and difficulties for position management

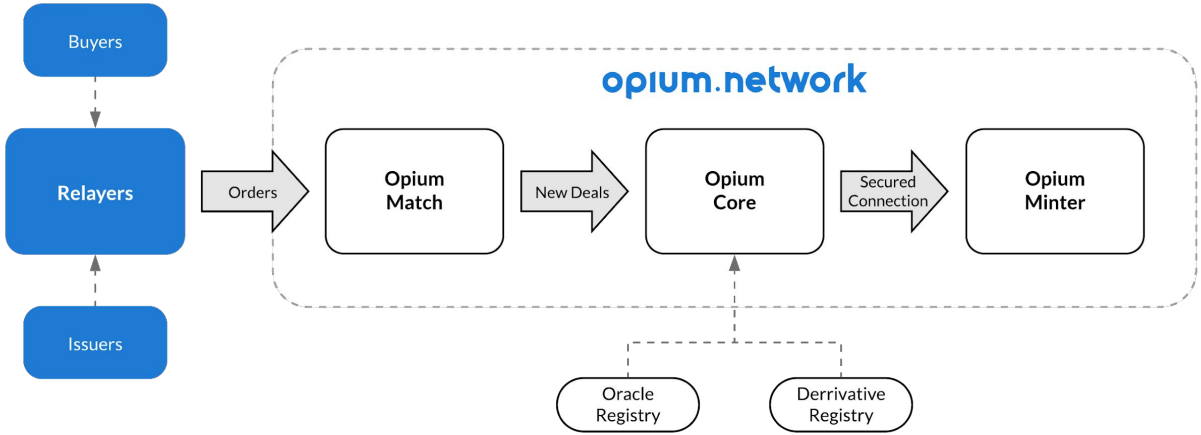
**LPs and the "Extra Income" narrative**

# PROTOCOL ARCHITECTURE: opium.network

Lemniscap

Being a DeFi platform, Opium relies on users (seller or buyer) to deposit a margin in Opium's liquidity pool. This margin acts as collateral and caps the maximum losses a participant may incur in. The collateral remains locked in the pool for the entire duration of the position. Once the margin is transferred and the specification of the option are established, the option order is passed on to the relayers. They are external agents who match orders from the option issuer and the option buyer.
Once an order is matched, it is passed on to the opium match engine and if all the correct information is present the contract is made valid. At this point, the order reaches the Opium core which is where, with the support of the Chainlink oracle, the premium is established by registering the oracle recipe and the derivative recipe. The last stage of the process is the opium minter which is where the position is tokenized in Opium derivative tokens (ERC-721 tokens).

**Products available:**
ETH Calls
ETH Puts




**Main protocol features:**

- Order matching
- Creation
- Settlement
- Payouts for financial contracts
- Secondary markets

A creation of an option must chronologically follow these steps:

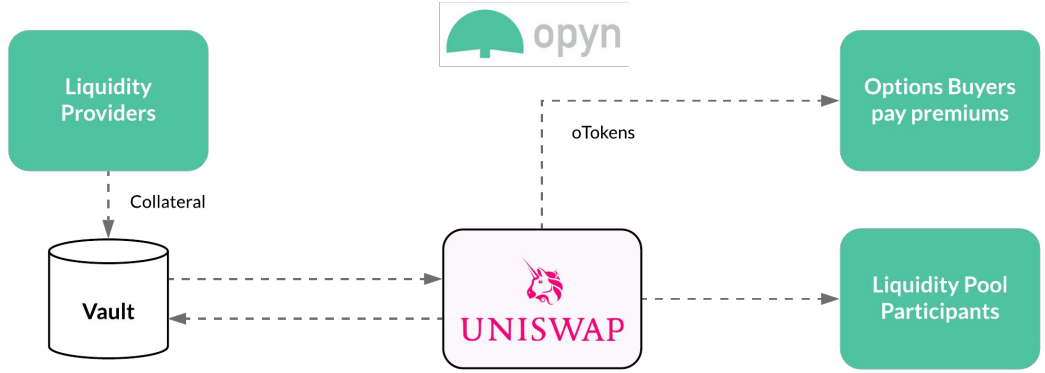
1. Relayers
2. Opium Match
3. Opium Core
4. Opium Minter

# PROTOCOL ARCHITECTURE: opyn

Lemniscap

Opyn brings to the DeFi world a sophisticated insurance platform built on the generalized options protocol Convexity. The architecture of the protocol is effective in its simplicity: by depositing crypto (especially ETH, but also other ERC-20) as collateral in a personal vault, the option writer can then mint oTokens and sell them for a premium.
The oTokens are ERC-20 tokens created by specifying a list of parameters which creates a unique options series. oTokens with the same series are fungible with each other. Buyers of oToken can purchase them on Uniswap, directly integrated with Opyn. If the buyers will not exercise the rights guaranteed by the specific option, the collateral of the option's seller will remain locked in the vault until the oToken expires unless she will close the position by buying back the previously minted oTokens and burning them. If the buyers exercises manually and autonomously the options bought, the protocol will automatically settle the contract by exchanging the underlying with the collateral (physical settlement).

**Products available:**
ETH calls/puts
UNI calls/puts
WBTC calls/puts
SNX calls/puts
Compound Deposits Insurance on USDC and DAI collateral




**Main protocol features:**

- Tokenized options contracts for insurance (oTokens)
- Fungibility of oTokens with the same option series
- Non-custodial and permission-less
- Immediate Claim Payouts

Easy functioning mechanism:

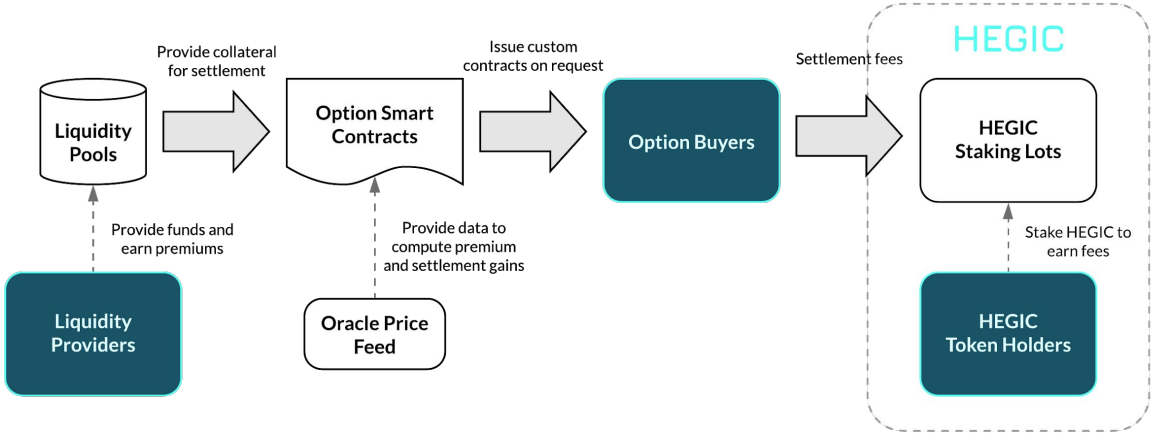
- Create oTokens by specifying options series parameter (whitelisted) and get a premium
- Collateralize the vault or liquidation for undercollateralized ones
- Exercising of oTokens during the expiry window

# PROTOCOL ARCHITECTURE: HEGIC

Lemniscap

Hegic uses a new approach in the options' market where option writers lock in the underlying capital in a liquidity pool. The settlement is done by computing gains or losses incurred by the holder on exercise. The funds held in the pool are used to pay such gains.
Being the funds packed together in pools, losses incurred by the liquidity providers are socialized. They depend on how much options' holders gained cumulatively. Basically it is like if liquidity providers were writing a small part of all options outstanding at the same time. When a user wishes to buy an option she just has to request it to the platform by setting the series' parameters. The protocol will computes the option premium using the Black-Scholes formula. Upon exercise, gains or losses are computed using a price feed from Chainlink.

**Products available:**
ETH Calls
ETH Puts




**Main protocol features:**

- LP funds are collected in pools
- Cash Exercise using liquidity pools funds as collateral
- Manual Exercise required
- Black-Scholes formula pricing.
- Complete personalization of option contracts
- Writers' gain and losses are socialized
- No secondary market for options
- Protocol token used for governance and to earn passive income by staking

# PROTOCOL ARCHITECTURE: Potion

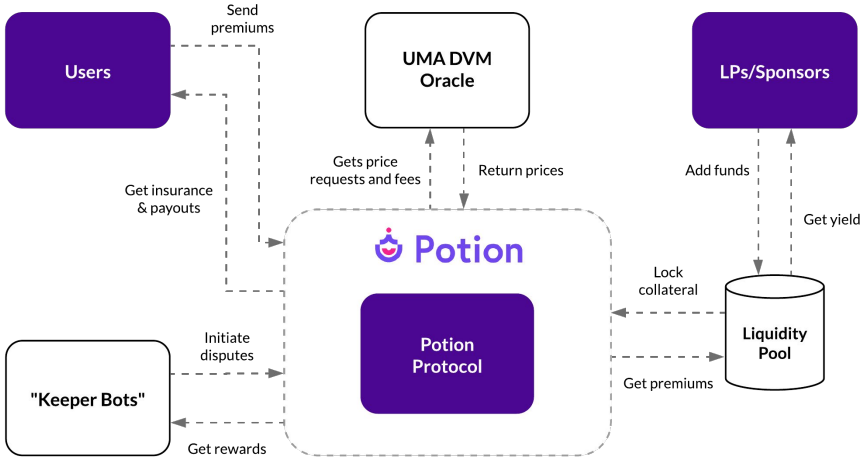
Lemniscap

Potion is a protocol betting on being very user friendly, with an as-simple-as-possible UI. One key feature of Potion is that users can choose the strike price, the duration of their contract, instead of having to choose from a small selection of options chosen by LPs. The liquidity providers can choose risk targets when depositing DAI to the liquidity pool. LPs can manage their risk profile at any point, deciding between higher risk and higher returns or lower risk and lower returns.
While Potion is still in development of their pricing engine, it is expected to be a new type of architecture, that seeks to provide a passive experience with LPs, based on an AMM architecture. Tied to the question of pricing is the use of oracles, needed both for initial pricing and eventual execution. Potion chose the UMA priceless oracle, only relying on it if there is a dispute in pricing that is initially done by users themselves. This method avoids fees and some of the other issues with oracles such as unreliability in high gas price periods. The Protocol is expected to be governed by a DAO in combination with its active users and LPs. They will vote on improvement proposals and decide on rewards granted to the developers.

**Future Products:**
Insurance of singular ERC20 assets

Risk-managed passive income as an LP

Broad range of option choices for users




**Main protocol features:**

- Freedom in choosing strike price and date
- Not relying on traditional oracle inputs
- AMM distributed pricing technique
- Decentralized tokenized governance through user base and DAO
- LPs can choose a risk and return profile that suits their preference

# RISKS, TRADE-OFFS & CHALLENGES

Lemniscap

## Collateralization

When talking about collateralization a clear tradeoff exists between capital efficiency and resilience.

The higher the capitalization ratio required, the less likely the protocol is to become insolvent.

However, requiring high collateralization allows users to open less positions and affects negatively their capital efficiency.

Due to the extreme volatility of the crypto markets, options writing is a very risky exercise.

The decentralized options' industry is always likely to require high collateralization ratios.

## Oracles

The oracle problem has been talked about at length in DeFi. Any protocol will have its end quality determined by its weakest link and in the Option market that might be oracles.

Option protocols have to be designed to work under extreme circumstances (such as the March Black Thursday event), when there might be extreme volatility and consequently congestion on the network.

Current oracle solutions have experienced some problems in such circumstances, stemming from a rapid increase in gas prices and the overloading of the system.

Currently, oracles present a big enough risk to the very idea of options in crypto.

## Pricing

We just discussed how in DeFi, decentralization often implies the usage of an oracle.

For options, getting pricing right is very crucial. The whole pricing exercise is additionally entangled by the convexity nature of the payoff.

Assessing, feeding and implying volatility is the real pricing challenge here.

The constant dependency from the underlier price along with time decay, makes the accuracy of a real time pricing extremely complex.

## Time Decay

Options (along with their price) are by definition dynamic assets.

A big factor on which the price depends on is the remaining time of their life.
So, option's price is technically constantly varying, even when nothing else really happen.

The speed on which options value decay increases when approaching expiry.

This adds complexity and increases the importance of constant price computation to allow for fairness and arbitrages opportunities with other exchanges (both centralized or decentralized).

## Secondary Market

By definition, the opportunity to freely trade a financial instrument increases its efficiency, affecting its growth and adoption.

As for today, option's protocols allow for partial flexibility on trading options after their issuance.

This is drastically reducing the possible use cases.

It cuts off all the volatility players who might want to trade options simply to speculate on short-term large price movements without waiting for the expiry.

# PROTOCOL'S APPROACHES TO DeFi CHALLENGES

Lemniscap

| | Collateralization (and capital efficiency) | Oracles (price feeds for premium pricing and volatility) | Pricing (and premium calculated) | Time Decay (and prices updated) | Secondary Markets (and options tradability) |
|---|---|---|---|---|---|
| opium.network | The users' margin is locked in when ordering the position and remains locked for the duration of the position. Hence, collateralization ratio cannot be decided. | Opium collaborates with Chainlink to obtain pricing data for the oracle recipe . All the other parameters are inserted by the user. | The option's premium is computed when the derivative recipe and the oracle recipe are registered, and the options parameters are made available. | As Opium provides for a secondary market, option prices are updated. | Opium provides for a secondary market as part of "Opium exchange", which contains both a primary and secondary market. |
| opyn | The collateral put down in the vault (either USDC or ETH) upon minting is locked for all the length of the position. The minimum oTokens' collateralization ratio is 100% and the maximum is 140%. If the vault becomes undercollateralized, it is at risk of liquidation. | Currently, since oTokens are 100% collateralized, no oracle is required. The V2 will introduce Oracle to improve capital efficiency, initially providing options settlement prices for ETH. | Pricing is theoretically determined by the seller who supplies oTokens to Uniswap where buyers complete the trade. Seller, are exposed to any impairment losses incurred in Uniswap. | Opyn's options prices are subject to Uniswap AMM constant function that modify the price according to algorithms using as inputs only the relative volume of the buyers and sellers in a pool. The options' fundamentals, including time decay by approaching expiry, are not considered by the automated pricing mechanism. | Opyn is integrated with Uniswap for the exchange of oTokens, providing a primary and secondary market for the options. Uniswap and its pools ensures liquidity but implies Ethereum gas charges. |
| HEGIC | Being the protocol based on a liquidity pool there is no pure definition of collateralization ratio so to speak. Each liquidity provider decides how much capital to risk in the pool. | The price feed is provided by a Chainlink oracle, while the implied volatility is manually updated by the contract owner. | The premium is computed from series parameters provided by the buyer and from external data feeds. It is finally estimated utilizing the Black and Scholes formula. | Options' prices are not updated since there isn't a secondary market for Hegic options. The protocol does not provide a way to exit the position other than early exercise. | There is not a secondary market for Hegic options. One could resell write tokens outside the protocol but the team has been publicly advising not to do so. |
| Potion | Users and LPs are in direct control of collateralization and they can manage risk by choosing among different risk profiles. Their liquidity is then managed completely by the protocol, in a trustless fashion. | Using the UMA priceless oracle avoids many of the fees and issues associated with oracles. Users can then input their own prices and UMA being called only for resolving disputes. | Potion uses a reflexive pricing system born out of an AMM architecture. The users with their orders, automatically set the pricing of the system to market levels, without any external oracle. | Potion hasn't announced their plans in this regard yet. | Potion hasn't announced their plans in this regard yet. |

# A STEP TOWARDS A SOLUTION

Lemniscap

## Collateralization

There is not a clear solution to the collateralization problem as it constitutes a physiological and technical tradeoff.

An optimization could be done via caps and dynamic payoffs.

By performing stress tests and simulations, each protocol must try to set the collateralization ratio at the lowest value possible, while maintaining the threshold high enough to ensure protocol resilience.

An additional solution could be to have the token holders carry some of the burden.
A portion of tokens could be set aside (or newly minted) to overcome emergency scenarios.

## Oracles

One interesting solution has been offered by a relatively new player in the oracle market: UMA. Their oracle is priceless, meaning that there is no direct price feed for the token values.

Users are initially trusted to input correct prices in each step of the option lifecycle. If there is a dispute in the pricing, the holders of UMA tokens will offer an unbiased resolution.

Ethereum 2.0 will open up a lot of new possibilities for more traditional oracles like Chainlink: the likelihood of network congestion will decrease and layer 2 solutions like rollups could further speed up the processing of oracle information.

## Pricing

So far, the protocols are either:

**i)** relying on the participants themselves to set a price to agree upon, or
**ii)** creating some rules set by the protocol (using methods such as B&S or utilization) in order to propose a price for the buyer.

There are two ways forward:

**i)** Create a protocol allowing for a very accurate pricing including all the traditional factors (especially volatility). This would eventually resemble to a decentralized version of Deribit.
**ii)** Create a new DeFi primitive protocol much more flexible than the current solutions where participants fix their risks and the protocol works out the price matching.

## Time Decay

The issue of time decay translate into *price dynamicity*.

The decentralized nature of the ecosystem denies the presence of centralized price feeds. This delegates the burden over the sellers, who shall manually update their pricing.

The complexity and accuracy of the task limit this assignment to the only very professional bots able to continuously update and upload new prices.

AMMs, in their most sophisticated version of a volatility pools, could carry this load, but it's hard to envision one pool efficiently writing any option in one or more underlying.

## Secondary Market

One of the main factors distinguishing options from a pure insurance contract is the possibility itself to freely trade the instrument.

Along with collateralization and oracles, this is like the biggest challenge for protocol designers.

The flexibility on emission works against the grouping of liquidity across major strikes and maturities.

Since the vast majority of options expires worthless, it seems fairly prohibitive to demand for an AMM pool to buy back their own previously written options. Until further developments or newly ingenious designed protocols, it is likely to see buyers carrying their position till expiry or exercize.

# BUSINESS MODEL AND INCENTIVES DESIGN

Lemniscap

**OPIUM**
Opium captures 10% of the derivative fee on an option. The derivative fee is what an option issuer requests to the buyer, hence, for every option issued, 10% of the premium will remain in the protocol. The system is made sustainable as the only external actors, the relayers, can profit from settlement fees and from arbitrage opportunities found on different platforms and markets.

**Opium incentivizes the users and the contributors of the platform by doling out its governance tokens which entitle the holders to vote on governance decision**

**OPYN**
At the moment, Opyn's business model has not been shaped yet and its protocol does not earn any fees.

**Economic incentives are currently not present in Opyn, which is currently relying on improving its UI and boosting its liquidity.**

**HEGIC**
The protocol generates value from its core option use case, and tries to capture it through settlement fees. When an option buyer requests or exercises an option, he has to pay a certain amount of fees, which are split between the liquidity providers and revenues to HEGIC token stakers. The latter are effectively costs added on top of the premium and transfer value from protocol "users" to protocol "rulers".

**Along with staking, in order to incentivize participation in the protocol some HEGIC tokens will be issued to early protocol users.**

**POTION**
Potion is launching as a public good without a profit model in its earliest iteration.

**While Potion intends to operate as a DAO, there are currently no public token plans for it.**

# TOKEN ECONOMICS & THE RECENT RISE OF GOVERNANCE

Lemniscap

The majority of the DeFi platforms are designed for a way to eventually employ a decentralized governance. Tokens are medium through which the users of the platform can engage in the governing and the developing of the protocol. The function behind the token is simple: allowing those users with rights to have an active role in the decision making of the protocol's future development. Means through which these tokens are acquired varies, and not all protocols currently have governance tokens.

**Current Landscape**

**OPIUM**

The Opium protocol envisions a decentralized governance model, powered by the utilization of OPIUM, a governance token . The model ensures that the protocol won't face liquidity issues during its evolution. Holders can cast and propose votes on governance proposals (especially regarding liquidity mining and token allocation), by interacting with AragonDAO.

**OPYN**

Opyn does not currently have a native token. It is owned and administered by a core team of developers and early investors. The long-term objective is to become fully decentralized and community governed. That will be possible by minimizing the role of governance altogether at some point or by launching a governance token.

**HEGIC**

The Hegic protocol includes a token (HEGIC) that was mainly devised for governance and staking. Initially, its issuance aims to incentivize the growth of the protocol. A large portion of tokens is issued to early participants acting as liquidity providers or option buyers. Some other tokens are reserved to finance the protocol development.

**POTION**

The protocol hasn't shared any plans for any tokens yet.

While governance is a more than noble "use case" for a DeFi token, there might be room for additional usage of a token. A token should fully coordinate a cryptonetwork and should help bootstrap both sides of a marketplace. By nature, option sellers are exposed to larger risks. Some idea on how a token could additionally expedite the growth of a DeFi options crypto network could be:

- An healthy **liquidity mining** program associated with a locking time for earned tokens
- Recurring **staking programs** that dynamically incentivize liquidity on different pools encouraging LP to commit to different series.
- A pool of tokens (a.k.a. **insurance fund)** could act as a buffer to the riskiest, but well defined, extreme tail events
- Give access to "**premium" features**, such as allowing buyers to resell to the pools only when holding a certain amount of tokens

**One step forward...**

# TAKEAWAYS: NETWORK EFFECTS & SUSTAINABILITY

Lemniscap

Network effects arise when the quality of a service is improved by the addition of new agents. In cryptonetworks they translate into additional value created by incremental users. They trigger a sustainability loop where the incentives formulated by the protocol encourage participants to carry on the work that the network needs the most. The participants are, eventually, rewarded for doing so.

**Network Effects**

**OPIUM**
Opium protocol implements an exchange for participants to freely trade (enhancing liquidity) and incentivizes Relayers (matching engines) to speed up and pair trades more efficiently.

**OPYN**
Opyn tries to group liquidity constraining the variety of options' series available.

**HEGIC**
Hegic constrains the pool's funds usage on side but rewards LPs with the native token for the resources provided.

**POTION**
Easiest LP experience makes the network more valuable to users with much greater choice, which in turn make it more valuable to LPs, in a loop effect.

**Current efforts: boosting liquidity!**

**USAGE:**
The value of a cryptonetwork should be directly linked to usage.

- Staking rewards could also reflect usage milestone
- Usage linked to burning mechanism constraining supply

**SUSTAINABILITY:**
As usage grows, so should the token value which is then redistributed to its holders.

- Locking stakes dynamically to reward holders by loyalty
- Dynamic rewards that account for critical times and for moments when the network is in need of liquidity
- Usage and work provided to the network are metrics deployed to trigger mechanism of supply constraints

**ALIGNMENT:**
Participants are incentivized to provide "work" to the network to grow its revenues.

- Riskier contributions are dynamically more rewarded
- Users and consequently token holders are incentives to curate, to vote and to participate into the evolutions of the protocol

**TOKEN ROLE:**
Participant's work is accrued by the token that coordinates the growth of the sustainability loop.

- Provenience of tokens can differ the reward scheme, discerning users by speculators

**Design Inputs + The next steps to achieve them**

# GUEST SECTION

Lemniscap

***What is the biggest challenge a DeFi option's cryptonetwork is currently facing on reaching critical adoption? What is the solution and incentives you have designed to overcome that challenge?***

The biggest challenge for DeFi options is to find a way to both the end-user and centralized liquidity providers. Very few people wake up in the morning and go to buy votes, but many people would like to use insurance or invest in an attractive product. We have designed an Opium Insurance product that utilizes option contracts and offers exact value to the end-user. And to overcome the second challenge we use Opium Bridge, it is Humming bot that can connect centralized and decentralized liquidity providers. By providing orders to both centralized and decentralized space, this bot earns a fee, staying market neutral. Anyone can run this bot; the more people run it, the more stable the bridge is.

opium

Currently there are 2 main challenges we are facing at Opyn to reach critical adoption: education and liquidity. Options are relatively new in DeFi, in fact a large part of Opyn community is made by early adopters excited by the protocol and eager to learn more about Opyn and options. One of the main need of our early community was to hedge against DeFi risk, but since the protocol is growing we are attracting new use cases. One of the main challenges we are facing now is to make sure new users are able to understand how they can take advantage of Opyn's protocol, which strategies could be implemented using options and what are the risks in order to make informed decisions. We are currently working on a completely new user interface with a UX optimized to enable users to make informed trades. In addition we built the v2 of the protocol in order to attract different use cases and we are focusing our resources to build a community in order to facilitate the open discussion and shared knowledge around Opyn and DeFi options. In addition to education is critical to have a liquid options market to reach critical adoption. Opyn v1 is using Uniswap as AMM for options pool and has some limitations for Liquidity Providers, especially for assets such options. Using Uniswap in the early phase of Opyn gave us the opportunity to analyze Liquidity Providers' main needs and concerns. Based on this research we are currently designing an AMM optimized for assets such options in order to incentivize Liquidity Providers to add liquidity to Opyn's options pools and reduce their impermanent losses compared to Uniswap pools.

opyn

The biggest challenge is the Liquidity depth. I believe that 9 of 10 options trading protocols who will use a peer-to-peer model will die in the next 2-3 years or will have no adoption at all. Only peer-to-pool options trading protocols will survive. Hegic offers a peer-to-pool (or peer-to-contract as some people calling it) options trading model which is safer for liquidity providers as they are sharing P&L (both premiums & downside) in a pro-rata manner and won't b *rekt* individually in case of a big price move (individual naked options writers on the other exchanges/protocols will be *rekt so hard* that they will immediately forget what option is right after seeing their -70% balance on the interfaces). Hegic currently holds $12.7M in liquidity available in the WBTC & ETH non-custodial bidirectional pools and distributes liquidity mining rewards in HEGIC tokens among the early adopters. All in all, the future is bright.

HEGIC

Biggest challenges:
1. Lack of choice for users (only limited selection of strikes and durations available)
2. Lack of confidence for LPs (little track-record, no back-testing analytics)
3. Non-scalable architectures (fragmented LP liquidity prevents high utilization)

How Potion can help:
1. We will provide a much wider range of option choices. More durations, more strikes, more assets.
2. We will provide a totally new approach to option pricing, where LPs will be able to reflect their risk / reward preferences
3. We will create a highly scalable architecture where liquidity utilization is optimized

Potion