Litepaper v0.1

Optimal DAO: An Optimal Smart Contracts and Optimal DApps based Ecosystem

Costin Oarda*

January 1, 2024

Abstract.
An ecosystem based on Optimal Smart Contracts would enable users to minimise agency and frictional cost in the exchange of value with providers across potentially all industries. Solving the Oracle problem is a central part of the solution that addresses frictional costs associated with the need for trusted third parties, but is only effective if the Principal-Agent problem is solved jointly. We are proposing an applied solution to the Principal-Agent problem and its underlying Oracle problem in the exchange of value between the provider and the user by developing a general framework for Optimal Smart Contracts, founded on Blockchain and AI technologies applied to Contract Theory. Maximum information on the characteristics of the product and the behaviour of the provider is provided to the user, while preserving the privacy of users and providers. Next, the Oracle solves the Optimal Smart Contract Resolution Algorithm (OSCRA) and thus generates optimal incentive mechanisms between the user and the provider, thereby restoring the balance of contractual relationships in the initial presence of information asymmetry. We propose launching Optimal DAO with the vision of achieving Pareto optimality in all exchanges of value, in all sectors of activity, through the tailor-made development of Optimal DApps in each corresponding industry. Governance is fully decentralised, based solely on usage and totally under the control of users whose humanity and uniqueness has been verified by a zero knowledge proof protocol. The supply of the DAO's economic token is minted slowly as a function of time and usage until it is used globally to ensure the sustainable development of these Optimal DApps. Demand is mainly driven by usage.

KEY WORDS

1. Behavioural finance 2. Principal-Agent problem 3. Oracle problem
4. Contract Theory 5. Optimal Smart Contracts 6. Pareto optimality
7. Optimal Smart Contract Resolution Algorithm 8. DAO Governance
9. Tokenomics

---

* Fully Qualified Actuary IA & SAA
Founder & CEO @ Optimal Contracts AG (Zug, Switzerland)

1 Principal-Agent Problem

Exchange of value is at the heart of every human economic activity and collaboration. Providers and users agree on contracts that define the terms and conditions for achieving a fair and balanced value transfer in each direction. The provider produces a product and provides it to the user in exchange for settlement. If the product is an asset (e.g., delivery of goods or services), the user sends a cash payment to the provider. If it is a liability (e.g., risk or debt transfer), the provider sends the user a cash payment. However, almost all exchanges of value are affected by the Principal-Agent problem:[1] the provider (the Agent) is better informed about the product than the user (the Principal). The provider can use his informational advantage to ensure that the settlement is in his favour, resulting in a net loss of value for the user, known as agency cost (including fraud cases). According to Contract Theory, information asymmetry on the characteristics of the product (adverse selection) or on the behaviour of the provider (moral hazard) threatens the equilibrium of contracts. The lack of transparent information and incentives reduces the market efficiency associated with these contracts and sometimes leads to market failure.

2 Oracle Problem

Today, most of these contracts take the form of traditional contracts and are not economically efficient (in the context of Contract Theory), because their interpretation renders them incomplete, and their formation, negotiation, performance, enforceability and opposability entail large frictional costs.These include intermediary costs, which are often prohibitive, particularly in the legal industry. The intensity and cost of legal involvement is not proportionally contributing to contract certainty; in simple terms; users and providers are slaves of a legal industry, whom they pay large amounts of money to compile page long contracts, which still user and provider poorly understand and leave them uncertain about the contract conditions. Smart contracts, on the other hand, reduce the need for intermediaries and are determined entirely by code. The decentralised nature of blockchain technology enables these smart contracts to be self-executing and censorship-free. As a result of this increased efficiency, we are fully convinced that the future of value exchange will involve smart contracts rather than traditional contracts. The use of smart contracts reduces the cost of frictional in the exchange of value and makes it possible to design directly enforceable incentive mechanisms, but the optimal parametrisation of these mechanisms remains an unsolved problem. Crypto-assets can be transferred on a sufficiently decentralised blockchain without relying on trust. For on-chain value exchange of real-world assets (RWAs) and liabilities (RWLs), blockchain technology is not suitable on its own to avoid relying on trust, because the Oracle problem must first be solved. The Oracle problem is the underlying inability of blockchains and smart contracts to access real-world off-chain data. The Oracle then plays the role of data provider and source of truth for smart contracts. Decentralised Oracle Networks have made good progress in solving this problem in a number of use cases, particularly in the delivery of financial assets price data. The Chainlink 2.0 white paper[2] introduced the concept of the hybrid smart contract to refer to existing smart contracts having the ability to securely compose on-chain and off-chain data and computing resources. However, hybrid smart contracts need to have access to Oracles that are even more specific to exchanges of value, in particular to

obtain data relating to the characteristics of the product and the provider's actions. In addition, they must provide off-chain computational intelligence that reduces agency problems. If this is not the case, the savings in frictional costs will no longer compensate for the increase in agency costs. Without solving the Oracle problem for this specific data, the irreversible nature of these value exchanges makes the Principal-Agent problem even more critical.

3 Contract Theory

Introduced some fifty years ago by Kenneth Arrow,[3] the Contract Theory is a very interesting instrument for studying and modelling the behaviour of economic agents within a contractual relationship in the presence of asymmetric information. In 2016, the Nobel Prize in Economics was awarded to Oliver Hart[4] and Bengt Holmström[5] for their contributions to this theory, which is now crowned and recognized as a true discipline with high potential in the field of economic research. Contract Theory provides tools for determining the optimal contract, including signalling and screening to limit adverse selection and the design of optimal incentive mechanisms to mitigate moral hazard. It can contribute to the development of new products that are profitable, competitive and sustainable, with a good incentive structure. Above all, it allows users to avoid financing high agency costs. Today, however, too few practical cases in industry apply the teachings of Contract Theory to solve the Principal-Agent problem in real value exchanges. This paper aims to address this shortcoming and enable industrial applications of Contract Theory.

In this paper, we extensively use the Principal-Agent framework of Kadan, Reny, and Swinkels from their paper "Existence of optimal mechanisms in principal-agent problems" (2017).[6] Indeed, the authors have put forward a quite general Principal-Agent framework (with single or multiple agents) and have outlined conditions that are the least restrictive in current literature, ensuring the existence of optimal contract solutions by addressing both adverse selection and moral hazard problems. The sets of types Θ, actions $\mathcal{A}$, signals $\mathcal{S}$, and rewards $\mathcal{R}$ can be multi-dimensional and may even be a wide range of function spaces. These sets Θ, $\mathcal{A}$, $\mathcal{S}$, and $\mathcal{R}$ are respectively associated with their sigma-algebras of measurable subsets $\mathscr{F}_\Theta$, $\mathscr{F}_\mathcal{A}$, $\mathscr{F}_\mathcal{S}$, and $\mathscr{F}_\mathcal{R}$. Therefore, $(\Theta, \mathscr{F}_\Theta)$, $(\mathcal{A}, \mathscr{F}_\mathcal{A})$, $(\mathcal{S}, \mathscr{F}_\mathcal{S})$, and $(\mathcal{R}, \mathscr{F}_\mathcal{R})$ are measurable spaces.

We denote Δ as the function which, given a set X endowed with a measurable space $(\mathcal{X}, \mathscr{F}_\mathcal{X})$, gives the set of probability measures $\mathbb{P}$ on the measurable subsets of $\mathscr{F}_\mathcal{X}$. Let $\mathbb{Q} \in \Delta(\Theta), \mathbb{A} \in \Delta(\mathcal{A}), \mathbb{S} \in \Delta(\mathcal{S}), \mathbb{C} \in \Delta(\mathcal{R})$. As a result, $(\Theta, \mathscr{F}_\Theta, \mathbb{Q})$, $(\mathcal{A}, \mathscr{F}_\mathcal{A}, \mathbb{A})$, $(\mathcal{S}, \mathscr{F}_\mathcal{S}, \mathbb{S})$, and $(\mathcal{R}, \mathscr{F}_\mathcal{R}, \mathbb{C})$ are probability spaces.

We denote the provider's von Neumann-Morgenstern utility function u and the user's von Neumann-Morgenstern loss (disutility) function l as follows: $u : \mathcal{R} \times \mathcal{S} \times \mathcal{A} \times \Theta \to \mathbb{R}$ and $l : \mathcal{R} \times \mathcal{S} \times \mathcal{A} \times \Theta \to \mathbb{R}$. u and l are measurable.

We denote $\mathbb{A}_\theta$ as the conditional probability measure $\mathbb{A}$ conditional on the event $\theta \in \Theta$ and $\mathbb{C}_{s,a,\theta}$ as the conditional probability measure on the event $(s, a, \theta) \in \mathcal{S} \times \mathcal{A} \times \Theta$. Let $\mathbb{A}_\Theta$ be denoted as the set of all conditional probability measures for $\theta \in \Theta$ and $\mathbb{C}_{\mathcal{S},\mathcal{A},\Theta}$ as the set of all conditional probability measures for $(s, a, \theta) \in \mathcal{S} \times \mathcal{A} \times \Theta$.

Applying the principle of revelation (Myerson 1982),[7] we define a mechanism as the tuple $(\tilde{\mathbb{A}}, \tilde{\mathbb{C}})$ in which $\tilde{\mathbb{A}} \in \mathbb{A}_\Theta$ and $\tilde{\mathbb{C}} \in \mathbb{C}_{\mathcal{S},\mathcal{A},\Theta}$. $\mathcal{M}$ is the set of mechanisms on $\mathcal{R} \times \mathcal{S} \times \mathcal{A} \times \Theta$.

A mechanism, denoted by $(\mathbb{A}_\theta, \mathbb{C}_{s,a,\theta})$, operates in the following way: the provider's type is

drawn from Θ by nature, based on $\mathbb{Q}$. Once the provider learns their type, θ, the provider reports a type, θ' to the mechanism. The mechanism then recommends to the provider an action a' that is generated by the probability measure $\mathbb{A}_{\theta'} \in \Delta(\mathcal{A})$. After learning the recommended action a', the provider chooses an action $\mathbb{A}_\theta$ from $\mathcal{A}$. It is important to note that the report on the type and choice of action by the provider does not alter the fact that contracts can remain "self-executing". Finally, given the signal s generated by $\mathcal{S}_{a,\theta}$, the mechanism generates the provider's reward r according to the probability measure $\mathbb{C}_{s,a',\theta'}$. Signals are generated according to the provider's true type and action, while rewards depend on the reported type and recommended action.

The function $\mathbb{C}_{\cdot,a,\theta} : \mathcal{S} \to \Delta(\mathcal{R})$, which gives a conditional probability measure in $\Delta(\mathcal{R})$ for a given set of type and action $(a,\theta) \in \mathcal{A} \times \Theta$ is then interpreted as a contract. The formulation of the Principal-Agent problem here is general enough to allow the user to randomise the rewards offered to the provider according to the observed signal. The provider knows the design of the contract before choosing his action.

We define a mechanism $(\mathbb{A}_\theta, \mathbb{C}_{s,a,\theta})$ as an *incentive compatible* if for $\mathbb{Q}$-almost every type θ and for every type θ',

$$\int_{\mathcal{R}\times\mathcal{S}\times\mathcal{A}} u(r,s,a,\theta)\, d\mathbb{C}_{s,a,\theta}(r)\, d\mathbb{S}_{a,\theta}(s)\, d\mathbb{A}_\theta(a)$$
$$\geq \int_{\mathcal{A}} \left(\sup_{a\in\mathcal{A}} \int_{\mathcal{R}\times\mathcal{S}} u(r,s,a,\theta)\, d\mathbb{C}_{s,a',\theta'}(r)\, d\mathbb{S}_{a,\theta}(s) \right) d\mathbb{A}_{\theta'}(a')$$

For any incentive compatible mechanism $(\tilde{\mathbb{A}}, \tilde{\mathbb{C}}) \in \mathcal{M}$, let

$$L(\tilde{\mathbb{A}}, \tilde{\mathbb{C}}) \equiv \int_{\mathcal{R}\times\mathcal{S}\times\mathcal{A}\times\Theta} l(r,s,a,\theta)\, d\tilde{\mathbb{C}}(r)\, d\mathbb{S}_{a,\theta}(s)\, d\tilde{\mathbb{A}}(a) d\mathbb{Q}(\theta),$$

be the user's expected loss when the provider reports honestly and takes the recommended action. The user's problem is then as follows:

$$\min_{(\tilde{\mathbb{A}},\tilde{\mathbb{C}})\in\mathcal{M}} L(\tilde{\mathbb{A}}, \tilde{\mathbb{C}}).$$

According to Kadan, Reny, and Swinkels (2017), there is a set of known conditions that can be used to prove the existence of an optimal contract solution.

4 Optimal Smart Contracts

We define Optimal Smart Contracts as hybrid smart contracts that solve both the Principal-Agent Problem and its underlying Oracle problem in the exchange of value between the provider and the user. Optimal smart contracts are founded on Blockchain and AI technologies applied to Contract Theory. The Oracle is a combination of off-chain AI and on-chain reputation scoring/certificates, based on privacy-enhancing technologies that guarantee strict privacy for both users and providers. Optimal Smart Contracts achieve Pareto optimality by solving the Optimal Smart Contract Resolution Algorithm (OSCRA). Optimal Smart Contracts therefore generate optimal incentive mechanisms between the provider and the user, thereby restoring the balance of contractual relationships in the initial presence of information asymmetry. The main

steps in this OSCRA Algorithm are modelling the effort and the cost of effort of the provider, modelling the utility functions of the user and provider, and estimating the value of the reservation utility (next best option of the provider in a competitive market). The Optimal Smart Contract is then the one that minimises the user's expected loss (e.g., maximises the user's expected utility) as a function of the provider's effort and the parameters of the feasible contracts for the user under constraints, which are generally as follows, depending on the uses cases:

- The Incentive Compatibility (IC): the provider chooses, from among all the feasible contracts that the user can agree to, the one that maximises its own expected utility function;
- The Individual Rationality (IR): the provider accepts contracts only if this effort generates a utility greater than its reservation utility; and,
- Finally, the Solvency Constraint (SC): the various components of the provider's capital must remain positive (e.g., financial and health capital).

These constraints generally apply in the case of the free market. Other contracts may also be subject to other constraints (regulatory, technical, market dynamics) which must be taken into account in a specific way for each industry. The very broad formulation of the framework proposed by Kadan, Reny, and Swinkels (2017) allows all these constraints to be taken into account, particularly in the design and modelling of the probability spaces for types, actions, signals and rewards, and the provider's utility and user's loss functions.

5 Optimal DAO

We are convinced that Decentralised Autonomous Organisations (DAOs), as member-owned communities without centralised management, are the most appropriate structure for solving the major problems facing humanity, as addressed in the previous sections with the Principal Agent and Oracle problem. We want to give power and value back to users to counter the centralised and monopolistic powers that often abuse their position to control and extract maximum value.

We propose to launch Optimal DAO with the vision of achieving Pareto optimality in all exchanges of value across all industries. Market efficiency is thus restored and cases of market failure resolved. Optimal DAO aims to create value for users by enabling them to retain the value associated with agency and frictional costs, which account for a significant proportion of global GDP (according to the International Monetary Fund (IMF),[8] global GDP in 2023 is estimated at USD 104.48 trillion dollars). If 10% of all contracts can achieve Pareto optimality and deliver 40% efficiency, the benefit to the global economy from Optimal DAO's action would be around USD 4 trillion dollars a year in value creation. Our future work will further test these benefit assumptions. To meet this objective of creating value for users, we design specific DApps (Decentralised Applications), called Optimal DApps, in all sectors of activity, based on Optimal Smart Contracts.

The following tokens are introduced, to enable the superalignment of the various ecosystem players' interests with those of the DAO:

- OPTIU is the DAO's usage token and a non-transferable and non-burnable NFT usage token, designed to be a usage indicator and confer specific rights to the users who own it. For each year of usage of at least one Optimal DApp in the ecosystem, the user is allocated one OPTIU. Its supply is therefore uncapped and strictly non-decreasing;

- OPTIB is the DAO's board token and a transferable and non-burnable NFT token allocated to board members for the agile execution of DAO operational decisions and protection in the event of critical events. Its supply is constant. It is initially allocated to the founder and early advisors. It is transferable by a vote of the governance, motivated by the reputation of the members of the Board of Directors and designed to meet the best compromise between agility and decentralisation for each stage of the project. More information will be provided when the whitepaper is published;
- OPTIG is the DAO's governance token and a non-transferable and burnable voting NFT used to vote on DAO strategic decisions. Each usage token OPTIU associated with an active user and each board token OPTIB gives access to an OPTIG. The supply is therefore equal at the beginning to the supply of OPTIB to allow agile development of the DAO. Over time, as OPTIGs are distributed through usage, the weight of the board in the DAO's strategic decisions becomes insignificant compared to the one of the users. This transition also makes it possible to reduce the operational risk at the start of the project by enabling the project to be scaled up in an agile but centralised way, to become fully decentralised in the long run;
- OPTIM is the DAO's economic token. Since we are convinced that Bitcoin will be the world's storage of value in the long term, the maximum supply is 21 million so that we can easily measure OPTIM's market cap against Bitcoin in the long term. More information on supply (emission, allocation, circulation and vesting), demand and equilibrium forces can be found in the Tokenomics section of this Litepaper. A more in-depth study can be found in the whitepaper.

See Fig. 1 for an overview of the ecosystem.

6 Optimal DApps

In each Optimal DApp, we develop a marketplace for users and providers to agree on Optimal Smart Contracts. At first, we design use case-specific systems that induce the greatest possible transparency on the characteristics and behaviour of the provider. Next, the Oracle solves the OSCRA Algorithm. By observing a fairly accurate approximation of the provider's real effort, strong incentives are created on-chain that make it costly to lose reputation because of adverse behaviour. In addition to the reputation, on-chain financial retention mechanisms at the start of the contract, reward providers afterwards who have made the most effort and therefore punish (or reward less) providers who have made the least effort. The Oracle also helps the provider to deliver better services/goods or reduce the frequency and intensity of the risk. The Oracle can also be seen as a judge of quality and can help to settle any disputes (DAO governance can settle in the last instance in the event of an appeal by the user or provider).

For each Optimal DApp, we study the initial conditions of the mechanism in place which induce an initial loss for the user: $\tilde{\mathbb{A}}, \tilde{\mathbb{C}}$:

$$L_0 = L(\tilde{\mathbb{A}}, \tilde{\mathbb{C}}) \equiv \int_{\mathcal{R}\times\mathcal{S}\times\mathcal{A}\times\Theta} l\,(r,s,a,\theta)\, d\mathbb{C}_{s,a,\theta}\,(r)\, d\mathbb{S}_{a,\theta}\,(s)\, d\mathbb{A}_{\theta}(a) d\mathbb{Q}\,(\theta)\,,$$

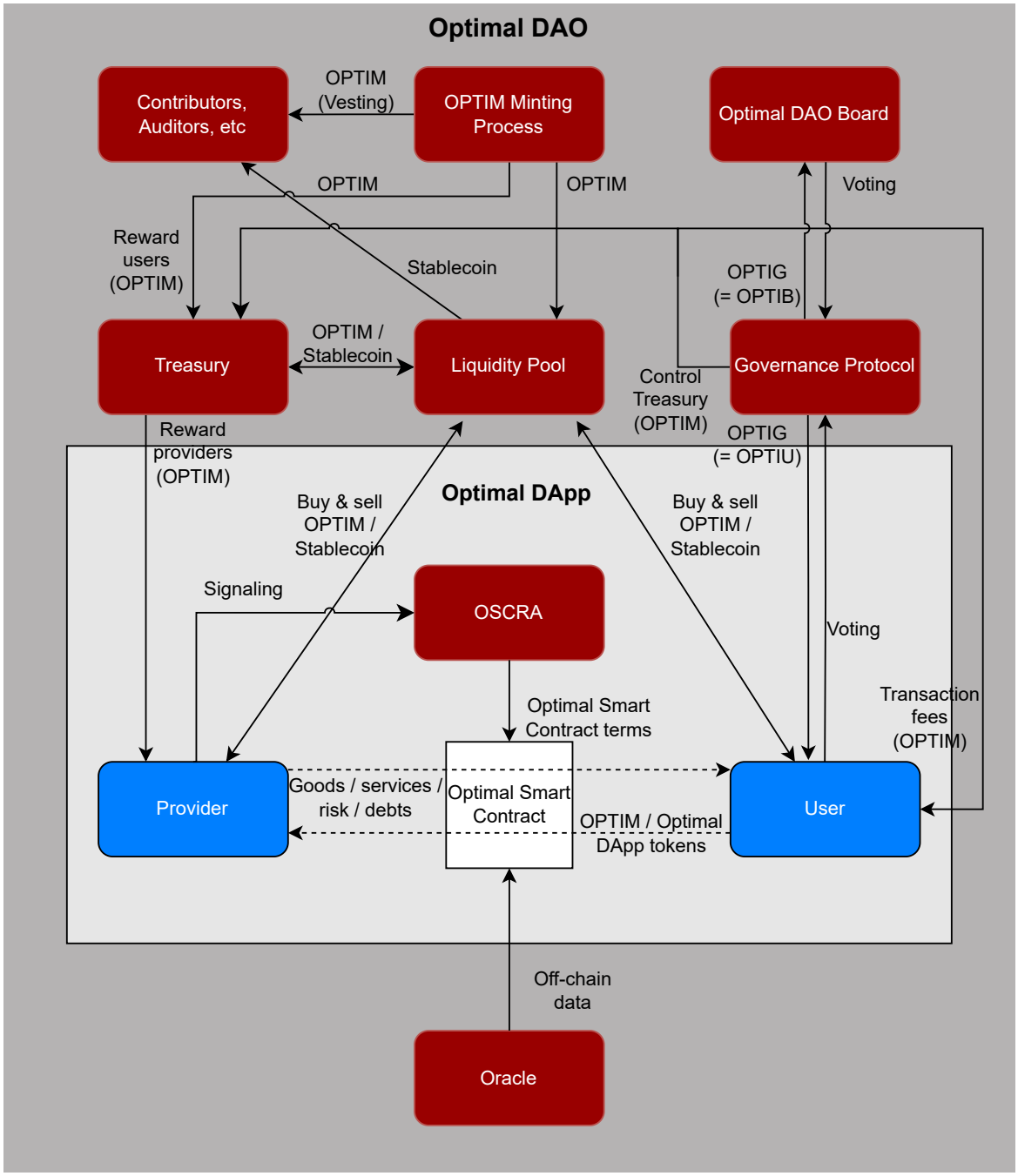

Fig. 1: Optimal DAO - Overview

We solve the Optimal Smart Contract that minimises the user's expected loss:

$$L_{min} = \min_{(\tilde{\mathbb{A}},\tilde{\mathbb{C}})\in\mathcal{M}} L(\tilde{\mathbb{A}},\tilde{\mathbb{C}}).$$

In this way, we have created value G for the user, which is the difference between the initial loss L_0 and the minimum loss generated by the Optimal Smart Contract L_{min}: $G = L_0 - L_{min}$. G has a positive or zero value, zero in the case where the contract was already optimal and strictly positive in the case where the contract was sub-optimal in the initial situation.

We propose to reward the protocol with a ratio α of the created value G and also the

most efficient providers by redistributing part of this created value with a rate β. The value capture for the protocol is therefore $\alpha \cdot G = \alpha \cdot (L_0 - L_{min})$. The total reward for providers is $\beta \cdot G = \beta \cdot (L_0 - L_{min})$.

The user of an Optimal DApp can subsequently be a provider of the product he has received and then transformed or developed as part of another Optimal Smart Contract with other users, in the same Optimal DApp or another one. For example:

- The buyer of intermediate goods is a user and can sell the final product and may become a goods provider in another optimal smart contract;
- The client of an outsourcing service is a user and may become a service provider in another optimal smart contract;
- The buyer of a property is a user and may become a debt provider in another Optimal DApp;
- The client of a risk prevention and repair service provider is a user and may become a risk provider in another Optimal DApp.

7 Optimal DAO Governance

Zero knowledge proof ID certifiers verify the humanity and uniqueness of users to counter Sybil attacks. There is no way of recovering the identity of users except by a massive vote by the DAO governance in the event of abuse of the system. The governance of the DAO is by design fully decentralized, with users with longer duration in the ecosystem receiving more voting power. Similar to Bitcoin,[9] it has been proven that trust, among others, is a function of time. Indeed, users receive one OPTIU, a non-transferable NFT for every year they use at least one Optimal DApp. When they actively use at least one Optimal DApp, they receive one OPTIG, a non-transferable voting NFT for each OPTIU they have collected. Voting power grows with time, not by buying more tokens. This solves the hostile takeover of power by buying economic tokens or the vote-buying phenomena in certain protocols.

Governance can also be distributed at the level of each Optimal DApps by introducing Optimal DApp-specific governance tokens to handle feature requests, for example. They also resolve voting fatigue if DAO members were to have to vote for DApps that did not concern them.

The full decentralised governance of the DAO is under the total control of real humans. They can decide on the strategic direction of DApp development, the scope, the values (e.g., decentralisation, privacy, justice), and on the handling of externalities (total privacy and ownership of data for users, impact on the environment, ...). The development of DApps relies heavily on artificial intelligence technologies (machine learning, deep learning) and have the potential to challenge the market of AI applications developed by web2 companies. These CApps (centralised applications) certainly meet the need for efficiency in the production of value for their users, but go against their privacy, which is an essential externality. This DAO's fully decentralised governance under the total control of real humans, while keeping values intact, guarantees safe AI applications to bring Pareto optimality to all value exchanges as a service to humans.

8 Optimal DAO Tokenomics

In addition to the usage token OPTIU, the board token OPTIB and the governance OPTIG, which are all non-economic tokens, Optimal DAO issues OPTIM, the DAO economic token. The key features of the Tokenomics of the DAO are listed below.

The supply side contains the following elements:

- Minting Supply (up to 21 million OPTIM tokens):
  - The majority is usage-based with 11 million OPTIM, minted progressively in a linear relationship with adoption, and the last OPTIM token will be minted (as far as usage is concerned) when the total usage duration of the ecosystem has exceeded 11 billion years (equivalent to an emission of 11 billion OPTIU tokens, for example, if 1 billion users have used at least one Optimal DApp of the ecosystem for an average of 11 years);
  - The other part of the minting process is time-based: 10 million OPTIM minted following a geometric series with a common ratio of 4/5 (1/2 for Bitcoin[9]) for one-year cycles (less than 4 years for Bitcoin[9]), starting on the date of the first publication introducing Optimal DAO (this Litepaper v0.1), namely 1 January 2024;
  - The minting function is therefore two-dimensional, as can be seen in the surface Fig. 2.
- Minting Allocation:
  - Half of the allocation, whether issued on a usage or time basis (10.5 million OPTIM), will go to the DAO's community treasury, which will own a large proportion of these minted tokens;
  - The other half of the tokens issued by usage (5.5 million OPTIM) is distributed to reward the community, for example to incentivise users and providers to develop marketplaces where optimal smart contracts can be concluded, and also to users to exercise governance of the DAO;
  - The other half of the tokens issued by time (5 million OPTIM) is used to reward contributors, intellectual property, long-term investors and audits.
- Circulating Supply and Vesting:
  - As far as circulation is concerned, part of the minting supply is sold dynamically directly (without vesting) to users, providers and investors against stablecoins to enable the financing of the DAO and to scale the development of Optimal DApps for all the different (industry) use cases;
  - Half of the vesting of the rewards to contributors, intellectual property and long-term investors is based linearly over time, up to 10 years, and the other half is released linearly between current usage duration and the objective of multiplying the usage duration by 10. This creates an incentive for contributors, researchers, and long-term investors to take actions that are aligned with the DAO's objectives of scaling up worldwide.

In terms of demand:

- Usage is the main driver, as this token enables interaction with all Optimal DApps;

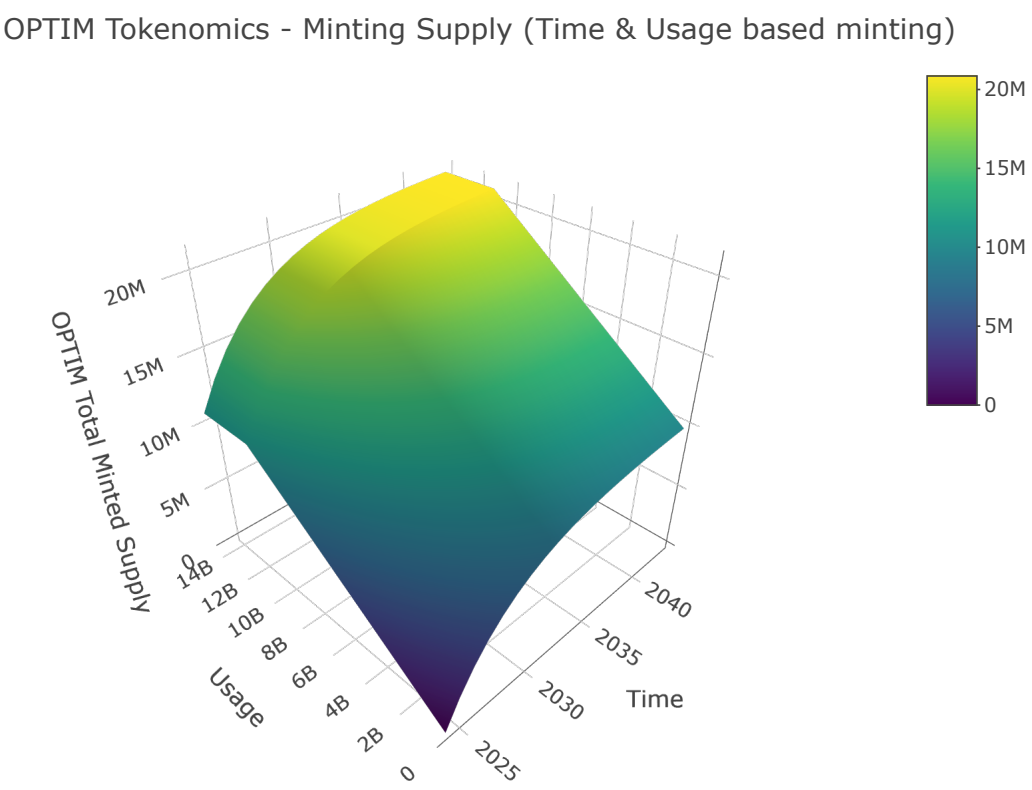

Fig. 2: OPTIM Tokenomics - Minting Supply (Time and Usage based minting)

- The unique value proposition, the marginal capture of the total value created combined with the potentially very high growth rate, the rising demand driven by usage of the DAO, together with a slowly increasing supply and the absence of pre-minted tokens, could result in significant upside for early token adopters, especially for users, providers and investors, and prove very attractive and secure for token holders.

Equilibrium (between supply and demand), after decades of potentially strong increases in the value of OPTIM (in other words, demand for OPTIM will exceed supply), should be achieved in the long term thanks to the following elements:

- The DAO's community treasury, makes part of its OPTIM reserves available to the DAO's liquidity pool.
- The DAO's liquidity pool allows the buying and selling of OPTIM against a stablecoin, which makes it possible to be colateralised.
- We use bonding curves, which are a type of Automated Market Maker(AMM),[10] introduced by Simon de la Rouviere.[11] These bonding curves are a mathematical function of the price as a function of the number of OPTIM tokens in circulation, the number of OPTIM tokens and stablecoins available in the liquidity pool.
- There is always a positive spread between the sell and buy bonding curve, which avoids arbitrage against the DAO.
- Bonding curve helps achieve stability between supply and demand.

9 Conclusion

We have proposed a user-centric ecosystem based on Optimal Smart Contracts for exchange of value of real-world asset and liabilities without relying on trust. Using the Optimal Smart Contracts general framework that we have outlined in this paper, Optimal DAO contributes to gradually tackling Principal-Agent and Oracle problems and enables users to minimise agency and frictional cost in the exchange of value with providers across potentially all industries, until eventually reaching Pareto optimality. The highly decentralised governance controlled by users only, and the strong alignment of tokenomics with usage and positive incentives for its participants are driving the acceleration in the worldwide development of Optimal DApps in all sectors, in order to optimise all exchanges of value as a service to human beings. Optimal DAO puts people back at the centre and re-establishes their real ownership and contract certainty.

Notes and References

[1] Salanié, B. *The Economics of Contracts: A Primer*. 2nd edition (2005).

[2] Chainlink "Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks." (2021) (accessed 24 November 2023) `https://research.chain.link/whitepaper-v2.pdf`.

[3] Arrow, K. J. "Uncertainty and the Welfare Economics of Medical Care." *American Economic Review 53, 941-973* .

[4] Grossman, S. J., Hart, O. D. "An Analysis of the Principal-Agent Problem." *Econometrica, Vol. 51, No. 1 (Jan., 1983), pp. 7-45* .

[5] Hölmstrom, B. "Moral Hazard and Observability." *The Bell Journal of Economics, Vol. 10, No. 1 (Spring, 1979), p. 74-91* .

[6] Kadan, O., Reny, P. J., Swinkels, J. M. "Existence of optimal mechanisms in principal-agent problems." *Econometrica, Vol. 85, No. 3 (Jun., 2017), p. 769-823* .

[7] Myerson, R. B. "Optimal coordination mechanisms in generalized principal–agent problems." *Journal of Mathematical Economics* **10.1** 67–81 (1982).

[8] (IMF), I. M. F. "GDP, current prices." (2023) (accessed 24 November 2023) `https://www.imf.org/external/datamapper/NGDPD@WEO/OEMDC/ADVEC/WEOWORLD`.

[9] Nakamoto, S. "Bitcoin: A Peer-to-Peer Electronic Cash System." (2008) (accessed 24 November 2023) `https://bitcoin.org/bitcoin.pdf`.

[10] Phemex "What is an Automated Market Maker?" (2020) (accessed 24 November 2023) `https://phemex.com/academy/what-is-an-automated-market-maker-amm`.

[11] de la Rouviere, S. "Tokens 2.0: Curved Token Bonding in Curation Markets." (2017) (accessed 24 November 2023) `https://medium.com/@simondlr/tokens-2-0-curved-token-bonding-in-curation-markets-1764a2e0bee5`.