Optimal DAO: An Optimal Smart Contracts based Ecosystem Design for a Systematic Solution to the Principal-Agent Problem

Costin Oarda*

[1] Optimal Contracts Ltd (https://optimalcontracts.com)
[2] Optimal DAO (https://optimaldao.com)

Abstract. The Principal-Agent problem is prevalent in any contract in any industry, where a provider exchanges a product, such as a good, a service, or a liability, for a settlement with a user. The information asymmetry between provider and user regarding the product and the misalignment of incentives from the provider, who may exploit his informational advantage over the user, diminish economic activity and therefore welfare. We introduce the *Optimal Smart Contracts* framework, a hybrid smart contract with two features: first, an industry-specific Oracle based on AI and blockchain technologies which incorporates product information and the utility functions of both provider and user, and second, an algorithm that, based on the information produced in the first stage, solves a generalised Principal-Agent model between the provider and the user. Assuming the technical feasibility of developing such Optimal Smart Contracts in each specific industry, the objective of this paper is to assess the potential of Decentralised Autonomous Organisations (DAOs) to support their development and promote their adoption The major benefit for user groups that are members of such a DAO is that they have control over the development and parameters of Optimal Smart Contracts. This novel approach allows users to internalise externalities that would otherwise arise from Principal-Agent problems in a centralised organisational structure. This is due to the fact that DAOs enable power to be redistributed among different user groups and that the underlying blockchain technology can enhance transparency and trust. The paper examines the potential of combining the two elements of a DAO and blockchain technology to develop a framework that addresses the Principal-Agent problem in a variety of business models. First, the Principal-Agent problem is described formally. Subsequently, a framework is developed that incorporates the above described elements. Finally, the proposed framework is compared to the status quo and relevant conclusions are drawn. The findings suggest that the combination of increased transparency and trust, as well as shifting operational power can effectively mitigate the Principal-Agent problem, provided that the technical feasibility of developing Optimal Smart Contracts is ensured.

* Costin Oarda (https://www.linkedin.com/in/costin-oarda) is fully qualified actuary of the French & Swiss Associations of Actuaries (IA & SAA), founder & CEO of Optimal Contracts Ltd, and founder & contributor of Optimal DAO.

1 Introduction

In this introduction, we first introduce the Principal-Agent problem and some basics on contract theory. We then address the Oracle problem and finally give our definition of Optimal Smart Contracts and DAOs to finally set out the research objectives.

1.1 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: the provider (the Agent) is better informed about the product than the user (the Principal). Salanié (2005)[20] draws a major distinction in this context between "hidden action" and "hidden information". Information asymmetry on the characteristics of the product (adverse selection) or on the behaviour of the provider (moral hazard) threatens the equilibrium of contracts. Arrow (1963)[2] defined moral hazard as "the effect of insurance on incentives". We suggest referring here to Baker's genealogy of moral hazard (1996)[3] and to the most famous example of adverse selection in the literature, the "Market for Lemons" (Akerlof, 1970)[1]. The provider may 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). The lack of transparent information and incentives reduces the market efficiency associated with these contracts and sometimes leads to market failure.

1.2 Contract Theory

Introduced some fifty years ago by Kenneth Arrow, contract theory is a useful instrument for studying and modelling the behaviour of economic agents within a contractual relationship in the presence of asymmetric information and solve the Principal-Agent problem. In 2016, the Nobel Prize in Economics was awarded to Oliver Hart and Bengt Holmström for their contributions to this theory, which is now recognised as a high potential discipline in the field of economic research. Contract theory provides tools for determining optimal contracts, 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. Mirrlees (1976)[13], Hölmstrom (1979)[8], and Grossman and Hart (1983)[7] pioneered the First Order Approach (FOA) which is often used on a theoretical level to prove the existence of a solution and to reduce the complexity of solving

Principal-Agent models. Rogerson (1985)[18] and Jewitt (1988)[10] then gave different sets of conditions under which the First Order Approach is valid, when the effort is assumed continuous in one dimension. Kirkegaard (2017)[12] unified these approached and generalised them to a higher dimensional effort for moral hazard problems. However, this First Order Approach is often criticised for its non-applicability to many real-world contexts, especially dynamic contracting (Battaglini and Lamba (2019)[4]). Moreover, too few practical cases in industries apply today the teachings of contract theory to solve the Principal-Agent problem in real value exchanges. This paper aims to address these shortcomings and enable industrial applications of contract theory.

1.3 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. 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 can make the reasonable assumption that the future of value exchange will involve more use of smart contracts than traditional contracts. The use of smart contracts reduces frictional costs 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 (2021)[5] 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.

1.4 Optimal Smart Contracts

We define in this paper *Optimal Smart Contracts* as hybrid smart contract with two features: first, an industry-specific Oracle based on AI and blockchain technologies which incorporates product information and the utility functions of both provider and user, and second, an algorithm that, based on the information produced in the first stage, solves a generalised Principal-Agent model between the provider and the user. Therefore, Optimal Smart Contracts solve both the Principal-Agent problem and its underlying Oracle problem in the exchange of value between the provider and the user. In this paper, we will explore a possible design for this framework in the model section, drawing on some theoretical lessons from the contract theory in the theory section, but without claiming to prove that its implementation is possible.

1.5 DAOs

In this paper, we will adopt the definition of a Decentralised Autonomous Organisation (DAO) of Ding et al. (2023)[6] as an organisation that enables individuals with common goals to collaborate using a blockchain infrastructure to enforce a set of shared rules. DAOs, as member-owned communities without centralised management, seem to be good candidates to help solve major problems, such as those discussed in the previous sections with the main agent and Oracle problem. We want to investigate whether DAOs are good organisational structures for redistributing power and value to users and thus countering centralised and monopolistic powers that may abuse their position to control and extract maximum value. However, caution should be exercised as, according to Sims (2024) [21], some DAOs use centralised structures and processes, given the difficulties of implementing a fully decentralised decision-making process in DAOs. These are known as DINOs (DAO in Name Only or Decentralised in Name Only).

1.6 Research objectives

Assuming the technical feasibility of developing such Optimal Smart Contracts in each specific industry, the objective of this paper is to assess the potential of Decentralised Autonomous Organisations (DAOs) to support their development and promote their adoption.

2 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) [11]. 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 notations and more details of this framework of the contract theory are given in the appendix. Only the most important results are given here. The sets of types $\varTheta$, actions $\mathcal{A}$, signals $\mathcal{S}$, and rewards $\mathcal{R}$ can be multi-dimensional and may even be a wide range of function spaces. We denote $\varDelta$ 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 $\mathbb{Q} \in \varDelta(\varTheta), \mathbb{A} \in \varDelta(\mathcal{A}), \mathbb{S} \in \varDelta(\mathcal{S}), \mathbb{C} \in \varDelta(\mathcal{R})$. Applying the principle of revelation (Myerson, 1982)[14], we define a mechanism as the tuple $(\tilde{\mathbb{A}}, \tilde{\mathbb{C}})$ in which $\tilde{\mathbb{A}} \in \mathbb{A}_{\varTheta}$ and $\tilde{\mathbb{C}} \in \mathbb{C}_{\mathcal{S},\mathcal{A},\varTheta}$. $\mathcal{M}$ is the set of mechanisms on $\mathcal{R} \times \mathcal{S} \times \mathcal{A} \times \varTheta$. For any incentive compatible mechanism $(\tilde{\mathbb{A}}, \tilde{\mathbb{C}}) \in \mathcal{M}$, let:

$$L(\tilde{\mathbb{A}}, \tilde{\mathbb{C}}) \equiv \int\limits_{\mathcal{R} \times \mathcal{S} \times \mathcal{A} \times \varTheta} l\left(r, s, a, \theta\right) d\tilde{\mathbb{C}}\left(r\right) d\mathbb{S}_{a,\theta}\left(s\right) d\tilde{\mathbb{A}}(a) d\mathbb{Q}\left(\theta\right),$$

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

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

The set of solutions to this problem are called optimal mechanisms and therefore define the optimal contracts associated solutions between the provider and the user. 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 mechanism and therefore an optimal contract solution.

3 Model

In this section we propose a possible design to systematically solve the Principal-Agent problem.

3.1 Optimal Smart Contracts

As mentioned in the introduction, Optimal Smart Contracts solve both the Principal-Agent problem and its underlying Oracle problem in the exchange of value between the provider and the user. In this context, Oracle requirements are to provide trusted real-world information about a product of a complex nature such as a good, a service, or a liability and the utility functions of providers and users in order to be able to solve a generalised Principal-Agent model as seen in the previous section. More details on possible characteristics and features of underlying Oracles of Optimal Smart Contracts can be found in the Appendix.

The Optimal Smart Contract is the hybrid smart contract 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 industry and specific 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. More details on a potential algorithm design solving the Optimal Smart Contracts, called *Optimal Smart Contract Resolution Algorithm* (OSCRA), can be found in the Appendix.

3.2 Optimal DApps

Specific Decentralised Applications (DApps), called *Optimal DApps*, based on Optimal Smart Contracts, are designed in all sectors of activity. Each Optimal DApp become a marketplace for users and providers to agree on Optimal Smart Contracts. At first, use case-specific systems are designed 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 afterwards providers 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. For each Optimal DApp, initial conditions of the mechanism in place (e.g., corresponding to the existing probability measures tuple $(\mathbb{A}^0, \mathbb{C}^0)$, when the ecosystem is not used), lead to an initial loss L_0:

$$L_0 = L(\mathbb{A}^0, \mathbb{C}^0) \equiv \int\limits_{\mathcal{R}\times\mathcal{S}\times\mathcal{A}\times\Theta} l\left(r, s, a, \theta\right) d\mathbb{C}^0_{s,a,\theta}\left(r\right) d\mathbb{S}_{a,\theta}\left(s\right) d\mathbb{A}^0_{\theta}(a) d\mathbb{Q}\left(\theta\right),$$

The Optimal Smart Contract that minimises the user's expected loss solves:

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

In this way, the 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}: $G = L_0 - L_{min}$. Therefore, 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 in this design 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 $\beta \cdot G = \beta \cdot (L_0 - L_{min})$.

3.3 Optimal DAO

We call *Optimal DAO* our design of a DAO whose mission is to solve the Principal-Agent problem and whose vision is to achieve Pareto optimality in all exchanges of value across all industries. To meet this objective of creating value for users, Optimal DAO support the development of Optimal DApps, in all sectors of activity. Market efficiency would thus be restored and cases of market failure resolved. Optimal DAO would aim 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)[9], global GDP in 2024 is estimated at USD 109.53 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. See fig. 1 in the Appendix for an overview of a proposition of the ecosystem design.

In our design of Optimal DAO, we want to empower users by ensuring that governance is fully decentralised and under their control, guarantee confidentiality and also counter Sybil-attacks. Sanchez (2020) [22] has proposed zero-knowledge protocols that guarantee the public-verifibility of the correctness of the Sybil-resistant, anonymous identities committed in permissionless blockchain. Previous work had also considered permissioned ledger but without transforming them into anonymous credentials in order to obtain the equivalent of a permissionless blockchain. To avoid being a DINO (DAO in Name Only), a viable solution for our Optimal DAO design seems to use Zero-Knowledge Proof-of-Identity protocols (ZKPI). More details on a design of the governance can be found in the Appendix.

Economic tokens are gradually issued based on time and usage, allowing the ecosystem to scale across the economy in the long run. More details on a design of the tokenomics can be found in the Appendix.

4 Discussion

It can be reasonably argued that blockchain technology is more conducive to the assurance of transparency and user trust than are centralised servers. This presupposes a blockchain protocol based on a sufficiently decentralised architecture, that smart contracts are open source and auditable, and that resources are deployed commensurate with the stakes involved to ensure security, such as regular smart contract audits and bug bounty programs. On the other hand, the question of whether organisations other than a DAO are better placed to develop Optimal DApps that guarantee transparent and fair redistribution among users is open to debate. The case for and against can be discussed according to the decentralisation level of organisations:

- It is evident that centralised entities, such as companies, are designed to make a profit. Additionally, the case of centralised states, which have the weakness of favouring groups of people with more power, should be considered. In both cases, these entities will tend to exploit information asymmetries to leverage their informational advantages to the detriment of users. Consequently, they should be less appropriate than DAOs for the development of Optimal DApps, given that these centralised entities are not under the control of users. Furthermore, it is crucial to avoid repeating the inherent weaknesses of the plutocratic, centralised model, which is characterised by the intertwining of internal economic activities with governance. An illustrative example is the use of corporate shares to influence the governance of a corporation. This is to ensure that the investors who initially financed the development of an innovation do not seek to extract the maximum value from users over the long term.
- Entities such as associations or foundations, NGOs, and in certain rare instances in states with direct democracy distributed over several levels (federal to local), such as Switzerland, may be able to act in the interest of the user in certain cases. However, they may lack the transparency and efficiency that blockchain technology can offer, especially as Optimal Smart Contracts already incorporate it.

Empirical evidence and case studies required to validate the feasibility and effectiveness of Optimal Smart Contracts in solving the Principal Agent problem are currently lacking. Further research will be conducted when data on the first Optimal DApp becomes available to address this knowledge gap.

5 Conclusion

Assuming the technical feasibility of developing Optimal Smart Contracts is established, we have demonstrated that the combination of increased transparency and trust from the blockchain technology, as well as shifting operational power from DAOs, can effectively mitigate the Principal-Agent problem. The Optimal Smart Contracts framework, as outlined in this paper, enables Optimal DAO to contribute to the gradual resolution of the Principal-Agent and Oracle problems, while enabling users to minimise agency and frictional costs in the exchange of value with providers across potentially all industries. This ultimately leads to the achievement of Pareto optimality. To achieve this, a highly decentralised governance structure, controlled by users only, is required, along with a strong alignment of tokenomics with usage and positive incentives for its participants. In such circumstances, Optimal DAO would empower people and re-establish their genuine ownership and contract certainty.

Appendix 1 - Optimal DAO Design Overview

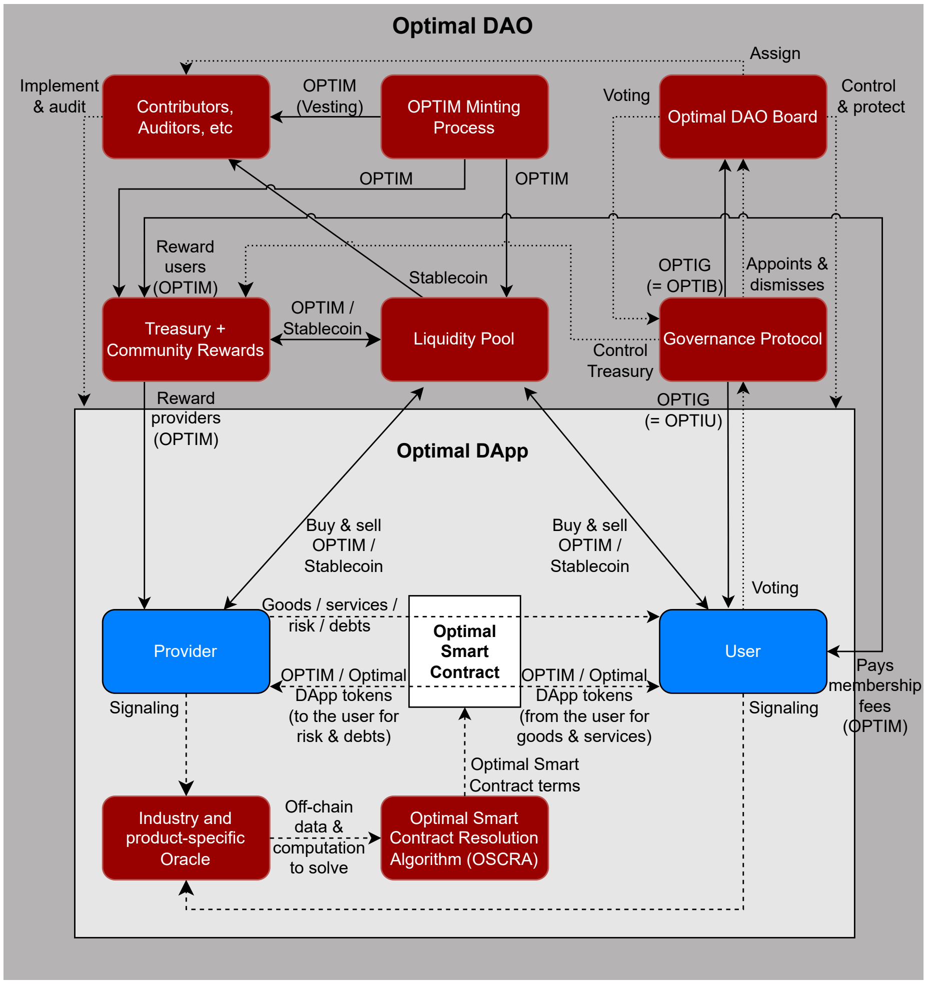
Optimal DAO
Assign
Implement & audit
Contributors, Auditors, etc
OPTIM (Vesting)
OPTIM Minting Process
Voting
Optimal DAO Board
Control & protect
OPTIM
OPTIM
Reward users (OPTIM)
Stablecoin
OPTIG (= OPTIB)
Appoints & dismisses
Treasury + Community Rewards
OPTIM / Stablecoin
Liquidity Pool
Governance Protocol
Control Treasury
Reward providers (OPTIM)
OPTIG (= OPTIU)
Optimal DApp
Buy & sell OPTIM / Stablecoin
Buy & sell OPTIM / Stablecoin
Voting
Goods / services / risk / debts
Provider
Optimal Smart Contract
User
OPTIM / Optimal DApp tokens (to the user for risk & debts)
OPTIM / Optimal DApp tokens (from the user for goods & services)
Pays membership fees (OPTIM)
Signaling
Signaling
Optimal Smart Contract terms
Industry and product-specific Oracle
Off-chain data & computation to solve
Optimal Smart Contract Resolution Algorithm (OSCRA)

Fig. 1: Optimal DAO Design Overview

Appendix 2 - Contract Theory

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, $(\varTheta, \mathscr{F}_{\varTheta})$, $(\mathcal{A}, \mathscr{F}_{\mathcal{A}})$, $(\mathcal{S}, \mathscr{F}_{\mathcal{S}})$, and $(\mathcal{R}, \mathscr{F}_{\mathcal{R}})$ are measurable spaces.

We denote $\varDelta$ 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 $\mathbb{Q} \in \varDelta(\varTheta), \mathbb{A} \in \varDelta(\mathcal{A}), \mathbb{S} \in \varDelta(\mathcal{S}), \mathbb{C} \in \varDelta(\mathcal{R})$. As a result, $(\varTheta, \mathscr{F}_{\varTheta}, \mathbb{Q})$, $(\mathcal{A}, \mathscr{F}_{\mathcal{A}}, \mathbb{A})$, $(\mathcal{S}, \mathscr{F}_{\mathcal{S}}, \mathbb{S})$, 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: $u : \mathcal{R} \times \mathcal{S} \times \mathcal{A} \times \varTheta \to \mathbb{R}$ and $l : \mathcal{R} \times \mathcal{S} \times \mathcal{A} \times \varTheta \to \mathbb{R}$. u and l are measurable.

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

Applying the principle of revelation (Myerson, 1982)[14], we define a mechanism as the tuple $(\tilde{\mathbb{A}}, \tilde{\mathbb{C}})$ in which $\tilde{\mathbb{A}} \in \mathbb{A}_{\varTheta}$ and $\tilde{\mathbb{C}} \in \mathbb{C}_{\mathcal{S},\mathcal{A},\varTheta}$. $\mathcal{M}$ is the set of mechanisms on $\mathcal{R} \times \mathcal{S} \times \mathcal{A} \times \varTheta$.

A mechanism, denoted by $(\mathbb{A}_{\theta}, \mathbb{C}_{s,a,\theta})$, operates in the following way: the provider's type is drawn from $\varTheta$ 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 $\mathbb{A}_{\theta'} \in \varDelta(\mathcal{A})$. 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 $\mathbb{C}_{\cdot,a,\theta} : \mathcal{S} \to \varDelta(\mathcal{R})$, which gives a conditional probability measure in $\varDelta(\mathcal{R})$ for a given set of type and action $(a, \theta) \in \mathcal{A} \times \varTheta$ 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',

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

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

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

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

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

The set of solutions to this problem are called optimal mechanisms and therefore define the optimal contracts associated solutions between the provider and the user. 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 mechanism and therefore an optimal contract solution.

Appendix 3 - Optimal Smart Contracts

Underlying Oracles of Optimal Smart Contracts

To solve the Optimal Smart Contract, access to off-chain data is necessary to model all inputs and solve the optimal mechanism problem. This allows for finding the parameters of the optimal contract between the provider and the user. Specific oracles for each industry and use case are developed to achieve this. Access to neutral, impartial and quality information about the product on the different markets today is often done with the help of an expert, but the cost of accessing this information is really high and often prohibitive, which exacerbates the problem of information asymmetry linked to the Principal-Agent problem. Artificial Intelligence (AI) technology can drastically reduce the cost of accessing this information and seems to be a good candidate for helping to solve the underlying Oracle problem of the Principal-Agent problem. The potential use of AI technology and other mechanisms enable the acquisition of knowledge about the transferred product, whether it be goods, services, risks, or debts, as well as the components of the provider and user's utility function. During each product transfer iteration, the provider's reputation and certificate rating is calculated, updated, and stored on-chain to prevent corruption. The Oracle would then be a combination of off-chain calculation using AI and on-chain reputation/certificate scoring. It should be based on privacy-enhancing technologies that ensure strict confidentiality for both users and providers. These desired features of the Oracle will be the subject of another paper, and we don't rely on its existence here. The parameters of the optimal contract solution of the Principal-Agent model as studied in the theory section are then encoded in smart contracts which then bind the provider and the user, providing them with transparency and trust in the agreement which binds them. We can therefore summarise that Optimal Smart Contracts are in principle founded on blockchain and AI technologies applied to contract theory.

Optimal Smart Contract Resolution Algorithm (OSCRA)

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). These algorithms must be designed, calibrated, tested, and validated according to the specificities and requirements of each use case. They are specific to each use case and will be the subject of specific research each time.

Appendix 4 - Optimal DApps

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.

Appendix 5 - Optimal DAO Governance

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

- OPTIU is the usage token of the DAO 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 board token of the DAO 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 governance token of the DAO 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.

Zero-Knowledge Proof-of-Identity protocols verify users to counter Sybil attacks while preserving their privacy. 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 decentralised, with users with longer duration in the ecosystem receiving more voting power. Similar to Bitcoin (Nakamoto, 2008)[15], 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. Users can now manage externalities that affect their assets, including wealth, health, data ownership, and the environment in the design of Optimal DApps. To address the common issue of misaligned interests between users and investors and for greater decentralisation, tokenomics is kept separate from governance. 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.

Appendix 6 - 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 of which 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 (Nakamoto, 2008)[15]) for one-year cycles (less than 4 years for Bitcoin[15]), starting on the date of the first publication of Oarda (2024)[16] introducing Optimal DAO (Optimal DAO 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) will be 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) will be 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 objectives of the DAO of scaling up worldwide.

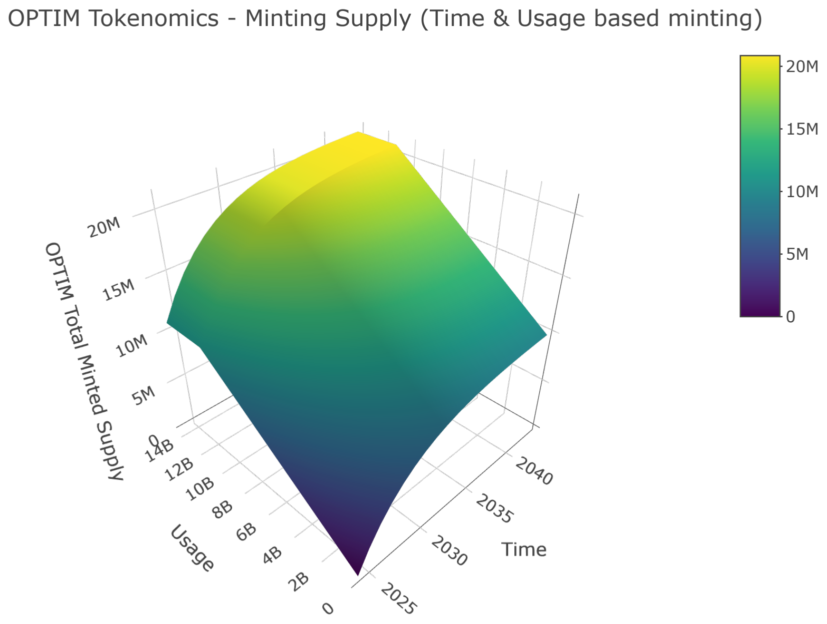

Fig. 2: OPTIM Tokenomics - Minting Supply (Time and Usage based minting)

In terms of demand:

- Usage is the main driver, as this token enables interaction with all Optimal DApps;
- 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 community treasury of the DAO, makes part of its OPTIM reserves available to the DAO's liquidity pool.
- The liquidity pool of the DAO allows the buying and selling of OPTIM against a stablecoin, which makes it possible to be collateralised.
- We use bonding curves, which are a type of Automated Market Maker (AMM) (2020)[17], introduced by Simon de la Rouviere (2017)[19]. 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.

References

1. Akerlof, G.: The market for "lemons": quality uncertainty and the market mechanism. Quartely Journal of Economics, 84, p. 488-500 (1970)
2. Arrow, K.J.: Uncertainty and the welfare economics of medical care. American Economic Review 53, 941-973 (1963)
3. Baker, T.: On the genealogy of moral hazard. Texas Law Review (1996)
4. Battaglini, M., Lamba, R.: Optimal dynamic contracting: The first-order approach and beyond. Theoretical Economics **14**(4), 1435–1482 (2019)
5. Chainlink: Chainlink 2.0: Next steps in the evolution of decentralized oracle networks. (accessed 15 April 2024) https://research.chain.link/whitepaper-v2.pdf (2021)
6. Ding, Q., Liebau, D., Wang, Z., Xu, W.: A survey on decentralized autonomous organizations (daos) and their governance. World Scientific Annual Review of Fintech Vol. 01, 2350001 (2023)
7. Grossman, S.J., Hart, O.D.: An analysis of the principal-agent problem. Econometrica, Vol. 51, No. 1 (Jan., 1983), pp. 7-45 (1983)
8. Hölmstrom, B.: Moral hazard and observability. The Bell Journal of Economics, Vol. 10, No. 1 (Spring, 1979), p. 74-91 (1979)
9. (IMF), I.M.F.: Gdp, current prices. (accessed 15 April 2024) https://www.imf.org/external/datamapper/NGDPD@WEO/OEMDC/ADVEC/WEOWORLD (2024)
10. Jewitt, I.: Justifying the first-order approach to principal-agent problems. Econometrica, Vol. 56, No. 5 (Sep., 1988), p. 1177-1190 (1988)
11. 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 (2017)
12. Kirkegaard, R.: A unifying approach to incentive compatibility in moral hazard problems. Theoretical Economics 12 (Jan., 2017), 25-51 (2017)
13. Mirrlees, J.A.: The optimal structure of incentives and authority within an organization. The Bell Journal of Economics, Vol. 7, No. 1 (Spring, 1976), p. 105-131 (1976)
14. Myerson, R.B.: Optimal coordination mechanisms in generalized principal–agent problems. Journal of Mathematical Economics **10**(1), 67–81 (1982)
15. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. (accessed 15 April 2024) https://bitcoin.org/bitcoin.pdf (2008)
16. Oarda, C.: Optimal dao litepaper v0.1. (accessed 15 April 2024) https://www.linkedin.com/posts/optimal-contracts_optimaldao-litepaper-v01-activity-7147723178943938560-r4SG (2024)
17. Phemex: What is an automated market maker? (accessed 15 April 2024) https://phemex.com/academy/what-is-an-automated-market-maker-amm (2020)
18. Rogerson, W.P.: The first-order approach to principal-agent problems. Econometrica, Vol. 53, No. 6 (Nov., 1985), p. 1357-1367 (1985)

19. de la Rouviere, S.: Tokens 2.0: Curved token bonding in curation markets. (accessed 15 April 2024) https://medium.com/@simondlr/tokens-2-0-curved-token-bonding-in-curation-markets-1764a2e0bee5 (2017)
20. Salanié, B.: The Economics of Contracts: A Primer. MIT Press, second edn. (2005)
21. Sims, A.: Daos (decentralised autonomous organisations) v dinos (dao in name only or decentralised in name only). (accessed 15 April 2024) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4716559 (2024)
22. Sánchez, D.C.: Zero-knowledge proof-of-identity: Sybil-resistant, anonymous authentication on permissionless blockchains and incentive compatible, strictly dominant cryptocurrencies (2020)