Agorata

Lev Chizhov[1,2]

@ennucore

July 14, 2022

Abstract

Agorata is an implementation of the idealized economic agent, or, specifically, an aggregator of smart contracts. It combines one or more contracts proposed by the members of the network in a deal which can be evaluated as profitable for Agorata with low risks. Using this approach, Agorata can provide infrastructure for derivatives, loans, flashloans, bridging between chains, bets, and many more financial instruments. As a service, Agorata will also feature simple methods to create smart contracts.

Contents

[1] Moscow Institute of Physics and Technology
[2] Ludwig-Maximilians-Universität München

I. Introduction

There is a variety of standard financial organizations that provide their capital for some simple purely financial deals: banks, brokers, gambling institutions, betting institutions, and many more. Most of them have their own DeFi counterparts, as well as some services that are only possible on the blockchain — for example, flashloans.

All of these organizations can be generalized to an economic agent that has a utility function and accepts a proposed deal if and only if it is the most beneficial in terms of this function. These particular implementations, however, only consider a very limited subset of deals. Also, all of them work only with purely financial deals which consist of not more than 3 parties[1], including the financial organization.

Technologies of decentralization and smart contracts in particular provide the foundation for a much more fundamental entity — one which goes far beyond standard simple templated purely-financial deals. This entity can constitute the implementation of the general economic agent. It can analyze deal proposals and their combinations into more complex deals (for example, combining two proposal in a risk-free deal, like with betting), which it evaluates and participates in. As a result, this entity can serve as a liquidity provider, loan broker, a service for finding a counterparty. It is worth noticing that as the blockchain technologies spread into multiple fields (not only financial), a service like that can become much more versatile and participate in deals including various assets (domain names, art, computational resources are the examples of what can be possible now, future applications are limitless).

The goal of this whitepaper is to present such an entity — Agorata.

II. Overview

As a service, Agorata has the following path of the user:

1. User creates a smart contract, which is a proposal for a deal, using Agorata's smart contract builder, or just uploads the contract code directly to the blockchain. The smart contract builder is a web application that allows to create a smart contract in the following ways:

   - Using one of the predefined templates, which are based on the standard financial deals.
   - Using Agorata's simplified language for smart contracts, A-Lisp, which is based on the Lisp language. It is then compiled to the Fift assebly language.
   - Using the No-Code version for creating a finite state machine smart contract.

2. Agorata builds its own standardized representation of the smart contract.

3. Agorata evaluates the smart contract or a combination of smart contracts in its pool and decides whether it is profitable or not.

4. Agorata accepts the most profitable deal.

Agorata will be based on The Open Network blockchain, because, as will be apparent in the following sections, TON's actor model and messages are very native to the concept of Agorata and allow to implement the service in a very simple way (high transaction speed and low costs are, of course, also a factor). Later, Agorata will include other blockchains, such as Ethereum, which will allow to extend its functionality with cross-chain operations.

[1] An example of such a deal with three parties is a stanard deal on a financial market.

III. Contract representation

i. The structure

A smart contract is considered as an entity with which other entities (users, smart contracts) can interact via messages[2]. For a state of the contract we can determine the messages that can be sent to the contract and for each of them — the response messages and the next state.

The contract is represented as an actor with several states (a finite number of states which can have parameters — i.e., variables in the contract) that can receive several (a finite numer of) types of messages. When a message is received and processed, it changes the state. The graph of states, messages, and transitions fully describes the system. Each message has a fixed form with parameters and the output state, which parameters depend on the parameters of the message. This dependency is characterized by an algorithm in the form of code in a pure subset of Lisp — A-Lisp[3].

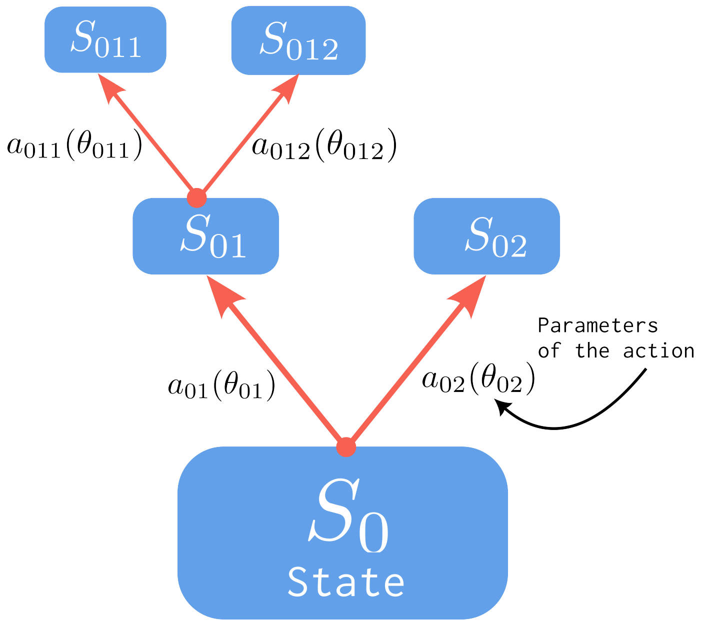


Figure 1: *Deal representation.*

Each action (message) has parameters θ, including:

1. s — the sender of the message.
2. t — the time (block number) at which the message is sent (may be omitted in the representation if it is unimportant for the next states).
3. tokens sent with the message.
4. any other possible information.

[2]The message concept used here is from The Open Network (TON). A message can include tokens, commands, information, code.

[3]The choice of Lisp is motivated primarily by the fact that it is a good unified way to represent an algorithm. There are also ways to use Lisp programs in formal proofs

The parameter space for each action can be constrained — the smart contract can reject some of the messages. For instance, this can lead to the entire space consisting of a limited number of elements (the contract rejects everything except for several specific messages, e.g. a specific person sending a specific amount of tokens).

The main parameters of the state are the financial outcomes for the smart contracts.

At the first stages of the project, the states and messages will not have variable parameters. The contract, therefore, will be a finite state machine. For that, the contract will have to check the incoming message on being in the list of allowed messages.

ii. Contract evaluation algorithms

As we will see in the following section, one of the most important parts of the process is finding out whether there exists any action that makes the deal profitable or unprofitable. It is also important to know which actions the agent should make to maximize its output. How do we do that?

The state parameters are represented as functions of action parameters expressed in a formal language. This allows to make all the decision based on mathematical proofs using theorem provers. In particular, with addition of meaningful parameters, maximization of the output in the formal language will be required.

However, for a contract with no parameters of messages and states this kind of an algorithm is not required. Instead, a search over a tree described in the next section will be sufficient. The usages of Agorata described below do not require these parameters. However, in the future their addition might be beneficial.

iii. Building the formal representation

At the first stages of the project, the formal representation will be obtained in two ways:

- Pattern matching on the Fift code for standard contracts made from templates
- The creation of the contract performed by the user through the constructor on the Agorata website

Pattern matching will be based on a set of templates with fields. Most prevalent field types will be addresses, token names, future timestamps (for example, deadlines for loans), and amounts. This algorithm will be able to recognize proposals of many types, including loans, derivative, flashloans, bets. For example, for a loan the paramters are the two involved tokens, sums in them, participating address.

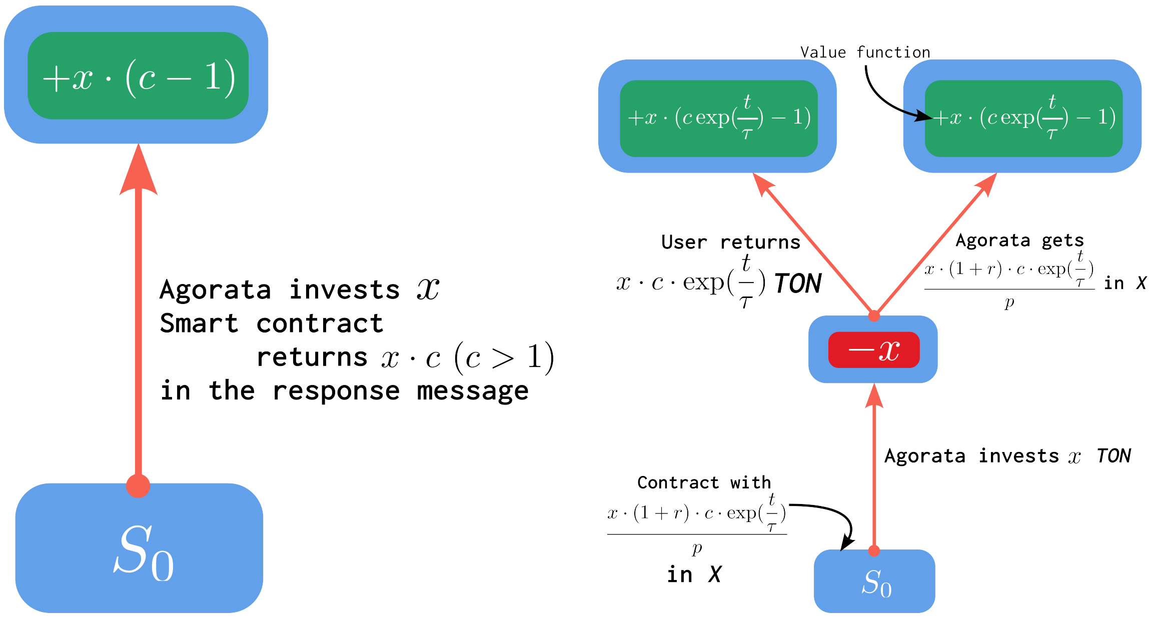
iv. Examples

Figure 2 show graphs for some simple deals.

IV. Decision-making algorithm

i. Agent parameters

1. T_0 is the maximum deal duration measured in blocks — i.e., the horizon after which the benefits of the deal are not considered.


$+x \cdot (c-1)$
Agorata invests x
Smart contract returns $x \cdot c$ $(c > 1)$
in the response message
S_0
Value function
$+x \cdot (c \exp(\frac{t}{\tau}) - 1)$
$+x \cdot (c \exp(\frac{t}{\tau}) - 1)$
User returns
$x \cdot c \cdot \exp(\frac{t}{\tau})$ TON
Agorata gets
$\frac{x \cdot (1+r) \cdot c \cdot \exp(\frac{t}{\tau})}{p}$ in X
$-x$
Agorata invests x TON
Contract with
$\frac{x \cdot (1+r) \cdot c \cdot \exp(\frac{t}{\tau})}{p}$
in X
S_0

(a) *Flashloan* **(b)** *Loan*

Figure 2: *Graphs for some simple contracts*

2. τ is the charachteristic time of discount — $\exp(\frac{1\,year}{\tau}) - 1$ is the minimal yearly rate for a loan.

3. r is the risk parameter for currency switching — the agent will only agree to swap no less than $(1+r)x$ in one currency for x in another.

Given these parameters, the value function $V((x_i), (t_i))$ (or $V(S)$) can be determined. It takes the sequence of values (x_i, t_i), where x_i are the incoming/outcoming tokens from the agent.

ii. Deal evaluation

The agent considers the worst case of the deal from the perspective of game theory: the best (from the perspective of the value function) actions of the agent and the "worst" actions of the counteragents. This sequence of events is the run through the value function in order to make a decision.

Thus, a deal is considered profitable for the agent (denoted by A) $\overset{def}{\iff} p(S_i) \iff$

$$V(S_i) > 0 \vee (\forall a_{ij}(p(S_{ij}) \vee a.s = A) \wedge \exists a_{ij} : V(S_{ij}) > 0)$$

Here, S_i is state that is analyzed (the state includes the token movements to and from the agent), a_{ij} are the possible actions (messages) in that state. The function $V(S)$ is the value function which analyzes the token movements in terms of profitability.

The algorithm starts at the node S_0, then considers all the possible actions (including the abscence of one) and calls the algorithm at S_{0i}. If there is any action of the counteragent that makes the contract non-profitable for the agent, the deal is considered non-profitable. If there is no possible action and the state includes profit for the agent, the deal is considered acceptable.

V. Applications

i. Loans

A loan on the blockchain is taken against another token: the user leaves some money in X, gets a sum in Y, then after some time can return Y and get some of X back. As seen in Figure 2a, the loan contract has a simple representation. It can also be easily matched from the Fift code, as it has only five fields: two tokens, the sums in them, and the address of the borrower. When Agorata will be only on one blockchain, the loans will be taken against tokens on TON. Later, support for tokens on multiple blockchains will be added. With the help of risk-taking counteragents or more complex risk analysis inside Agorata, NFTs from highly-liquid collections can be used as a collateral for the loan.

For example, a domain can be used. After the development of TON Sites, the following scenario will be possible: creator of a TON website needs money to pay for the development and hosting. They take a loan with the domain as collateral. While they still owe money to Agorata (i.e., the domain is on the balance of a smart contract and after some time might be taken by Agorata if the person doesn't return the loan), the domain is still used and the website is fully operational. Thus, Agorata secures the loan, while the loan recipient can get the money and keep the website running.

ii. Flashloans

In blockchains like Ethereum, some services offer flashloans. Users create a transaction where they take any available sum from the flashloan smart contract, perform operations with the money, then return it in the same transaction. If the returned sum is not less than the borrowed amount with comission, the transaction is approved by the smart contract. In TON, a system exactly like this is not possible. However, such an operation can be implemented by creating a smart contract that performs all the necessary tasks and retuns the money to the loaner. Agorata allows to implement that: such a contract is an acceptable deal for it, so the user can just create the flashloan contract in Agorata with the necessary operations and Agorata will take care of the rest.

iii. Bridges

After the initial stages of the project, Agorata will be expanded to multiple blockchain platforms. Agorata will just have instances (smart contracts) on different chains, and the connection between them will be represented as exchanges of virtual tokens. This will allow many more operations, including bridging and DEX functionality, because a bridge operation is nothing more than a value-increasing contract between the user and two instances of Agorata on the two platforms. DEX functionality in this case is even simpler, because it doesn't involve risk for Agorata.

iv. Bets and derivatives

TON's messages provide a great interface for bets. The user can bet on a certain message coming to the bet contract. It can be an external (signed) message or a message from another contract. Then, the bets of several users on the same event can be aggregated by Agorata into one (risk-free) deal. The message in question can relate to an event on the blockchain or be signed by several pre-chosen oracles. Blockchain events may include the number of users of a certain TON Site reaching a threshold, an NFT being sold, the median price of a domain being more/less than a certain value, etc.

Agorata can also issue derivatives (in fact, binary options function exactly like bets). For example, call and put options can be matched and turned into a profitable for Agorata risk-free contract. It works the same way for futures. Thus, many derivative financial instruments appear in the TON ecosystem.

v. More complex usages

Agorata can also be used as a platform for looking for a counteragent for a deal. As a service, it will also feature a constructor of smart contracts from the from the formal language (or its graphical, no-code, representation). This is an extremely useful service since writing programs in FunC is complex, while the logic in most cases is simple.

With the evolution of the decentralized internet (in particular, TON Sites and Storage), the potential of Agorata will become more and more apparent. The example with the domain in the loan section shows just a glimpse of the possibilities. Even options may later be applied to Proxy, Storage, or even to physical goods if decentralized marketplaces will appear.

VI. Conclusion

In this article, a simple yet very flexible service that can be used to easily create smart contracts and perform a multitude of operations has been presented. It can replace many financial services while having a common liqiudity pool. The proposed contract creator will also simplify the development and popularize the use of smart contracts (most people will never learn FunC, but the creation of simple contracts will be of interest to many). Agorata shows the true potential of smart contracts and TON's concept in particular. As decentralized applications spread into more aspects of the real world, its usages will become more and more diverse.