Algolend

Lite paper

28/03/2021

Table of contents

Abstract

The Algolend protocol designed by Blockchain Italia is an algorithmic money market protocol built and operated exclusively on the Algorand blockchain platform. It enables users to accrue interest on their deposits and borrow assets by collateralizing the deposit.

By depositing funds, users would be able to start earning continuously-compounding interest immediately. The interest rates are calculated by the protocol depending on the demand of the specific market.

By providing funds as collateral, users would borrow any supported token assets at an interest accrued in real block-time. Silo-ed money market liquidity pools, risk-adjusted credit, health factors and a strongly incentivized liquidation system would concur to ensure the protocol economic soundness.

Algolend utilizes the Algorand blockchain platform for fast, low-cost transactions. Algorand has been developed to speed up transactions and improve efficiency in response to standard blockchains' slow transaction times. Algorand, Turing Award Silvio Micali's brainchild, represents the first open-source, permissionless and pure proof-of-stake-based protocol.

The protocol governance has been designed to be controlled in its majority by the Algolend community and users. The aim is to provide benefits to all the parties involved in the protocol protocols regarding service, earnings and fairness.

This paper aims to give an overview of the principal actors and mechanism governing the Algolend protocol.

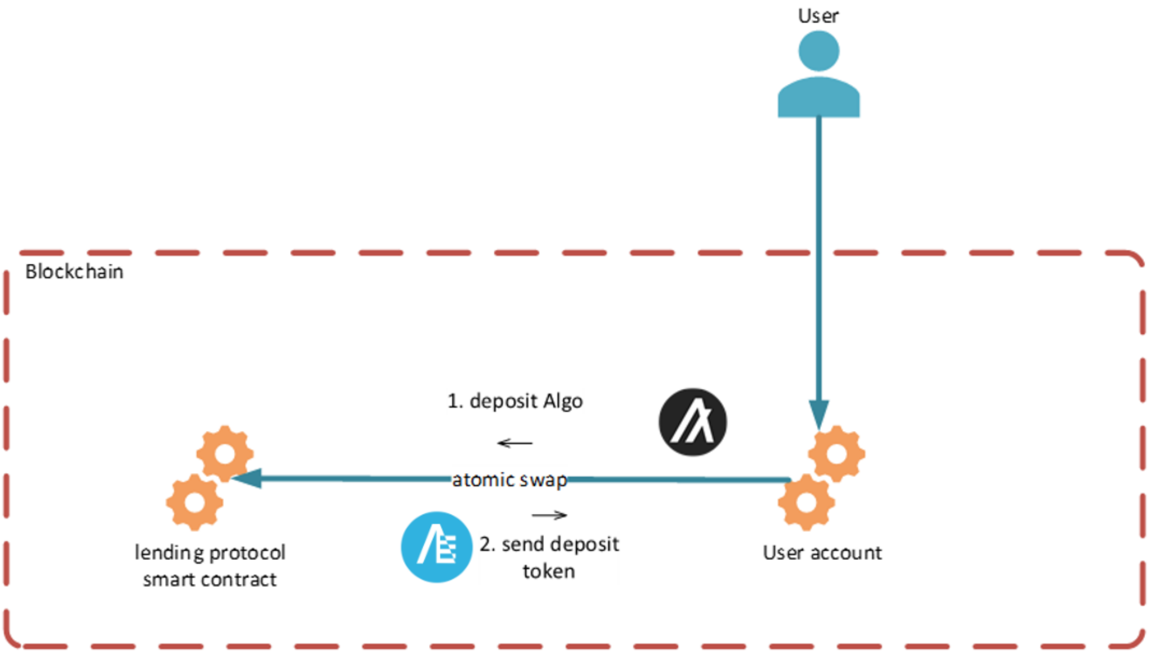
Intro

The protocol aims to support the lending and borrowing scenario described in the abstract paragraph. The following requirements and constraints have been intentionally chosen to increase the protocol quality:

- Tokens representing deposits and governance tokens are real ASA (Algorand Standard Asset) and not counters associated with a contract;
- Operations, as far as possible, do not rely on centralized elements trust-like (trustless).

This document will be treated as an ALGO-USDC crypto pair because it is the first pool implemented in the protocol. But the same mechanisms will apply to future integrated crypto pairs.

Lending



A deposit transaction allows a user to deposit a certain crypto amount and earn interest. The earned interest is paid by using those interest paid by the borrowers.

The deposit contracts are unique for each crypto: a deposit contract for ALGO, one for USDC, etc. Each deposit contract has pre-signed ASAs to represent the deposit.

The ALGO deposit contract holds ALEND-A tokens, the USDC deposit contract holds ALEND-U tokens, and so on.

After depositing an A amount of ALGO tokens, the user receives an M amount of ALEND-A tokens according to the following formula :

$$M = A / I_{t_D}$$

This formula depends on the index of interest I_{tD} for the time at which the deposit took place.

At the withdrawal, the user returns the amount M of ALEND-A and receives back its deposited Algo and the accrued interest.

Borrowing

Algorithmic lending protocols require that each loan be secured by collateral.

In the Algolend protocol, a user who has made a deposit, e.g. ALGO, and consequently has a certain amount of ALEND-A tokens can apply for a loan, e.g. of USDC, by placing a part of its ALEND-A tokens to guarantee the loan. To an amount of M token ALEND-A corresponds to an amount A of ALGO that depends on the interest index at borrowing time (t_b) according to the formula:

$$A = M * I_{tb}$$

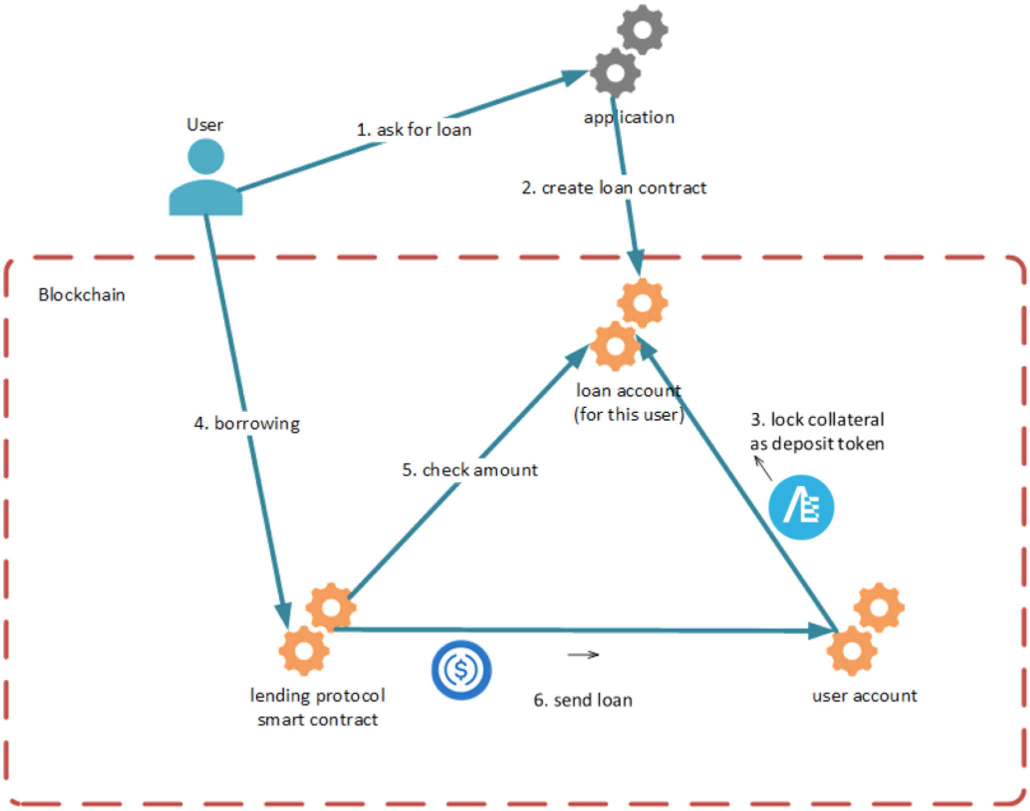
The borrowable amount (Q) of USDC depends on the USDC-vs-ALGO conversion rate (R). The following formula defines the quantity Q of USDC corresponding to A:

$$Q = A * R_{usdc\text{-}vs\text{-}algo}$$

For safety factors, the total amount of Q cannot be borrowed from the user; it is necessary to keep a part as a collateral factor to safeguard the loan in case of negative fluctuations in the value of ALGO and to guarantee the interest payment.

Because the R factor varies over time, two operations must be allowed:

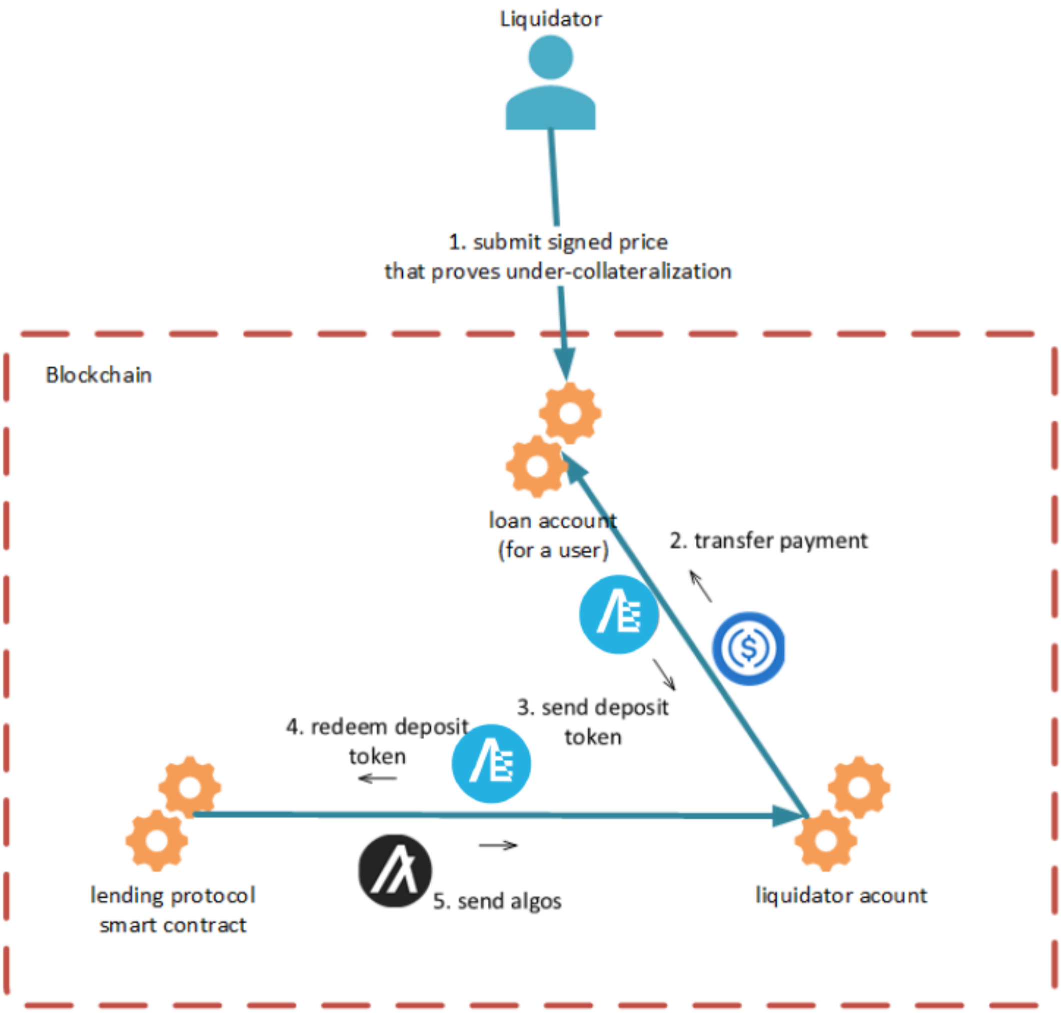
1. if the value of ALGO (compared to USDC) rises, the user must be able to withdraw other USDCs since his collateral covers a higher value
2. if the ALGO value (relative to USDC) drops, the user must put other ALEND-As in the contract to hold the collateral value above a threshold.



If the value decreases, the threshold under-collateralization arises, and the liquidation mechanism takes part.

Liquidation mechanism

In such under-collateralization, a liquidator would obtain that portion of the collateral needed to bring the outstanding debt below the relative safety threshold, according to protocol parameters of that specific borrowed token asset. The liquidator gains income due to the higher value of the bought debt (bought at a lower price) and a penalty fee paid by the user for being liquidated.

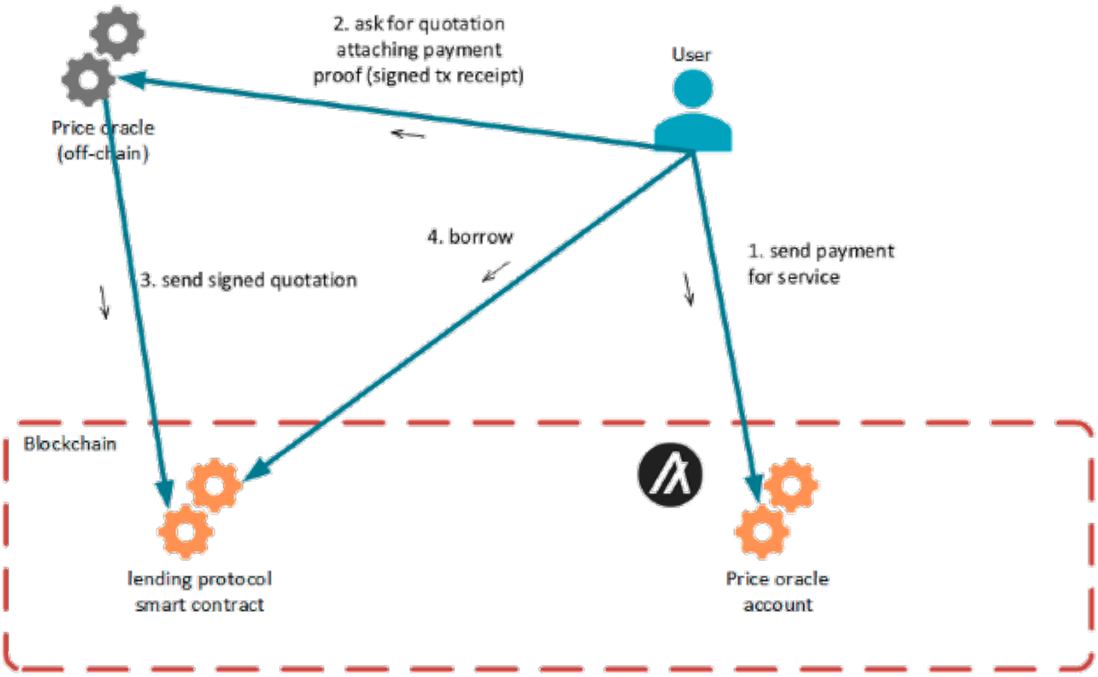


Trusted price oracle

The price oracle purpose is to calculate the effective exchange rate for the price quotation.

Since it is an external service, the user must pay for the oracle service. The following diagram represents the dynamics of the interaction with the oracle.

1. The user sends the payment to the Oracle Algorand account.
2. The user submits the payment signing it with its private key to demonstrate it owns the payment.
3. The Oracle sources the exchange rates across supported token pairs.
4. The Oracle updates the quotation in the lending protocol smart contract to allow a subsequent borrowing operation within a specific amount of time.

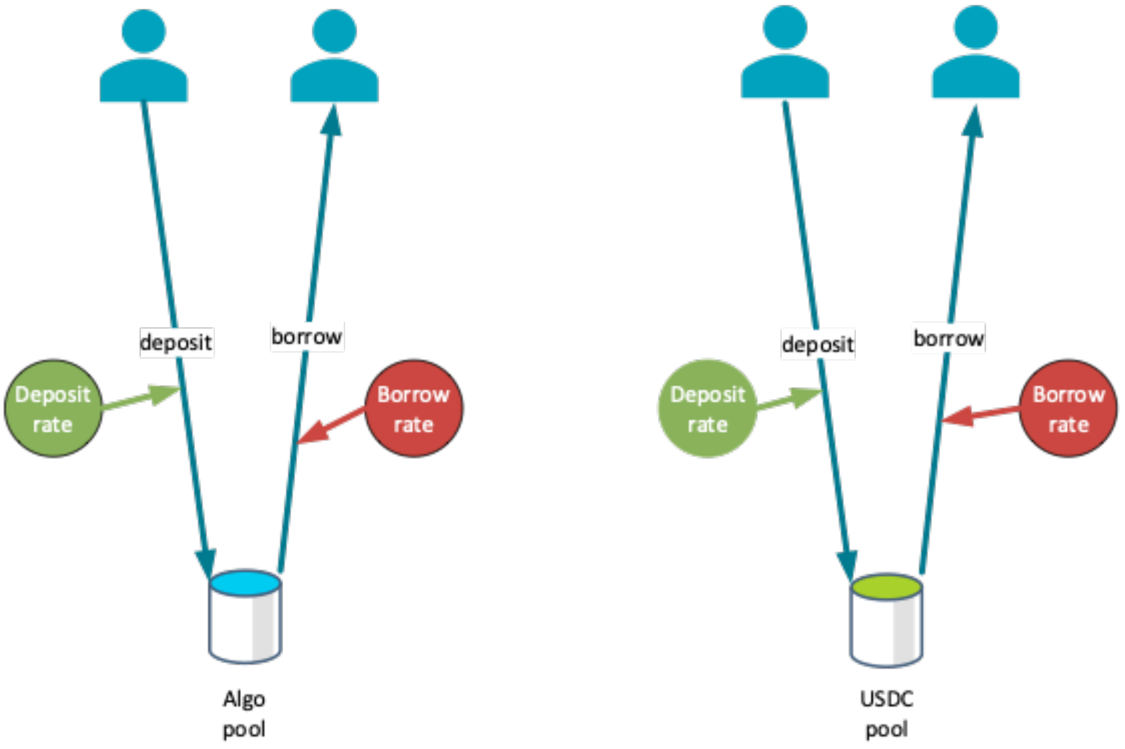

2. ask for quotation attaching payment proof (signed tx receipt)
User
Price oracle (off-chain)
4. borrow
1. send payment for service
3. send signed quotation
Blockchain
lending protocol smart contract
Price oracle account

Interest

The Interest index is a monotonic value that represents interest maturation across all protocol users. There are deposit interests and borrow interests.

Borrowers pay the borrowing interest accruing on the borrowed asset's type and amount until the latter is fully repaid. The depositors earn interests in their deposited asset. Algolend utilizes the interest paid by the borrowers to pay the interest accrued by the depositors.
Interests are calculated following basic free-market rules of supply and demand. This is achieved by linking the indexes to a utilization ratio U across all the protocols' pools.

To maintain the protocol balance among all crypto deposits, each pool utilizes its utilization ratio U. This ratio varies between a predetermined but adjustable range that ensures stability.



The utilization ratio is defined as the ratio between the total borrows and the total deposits:

$$U = \frac{Total\ borrows}{Total\ deposits}$$

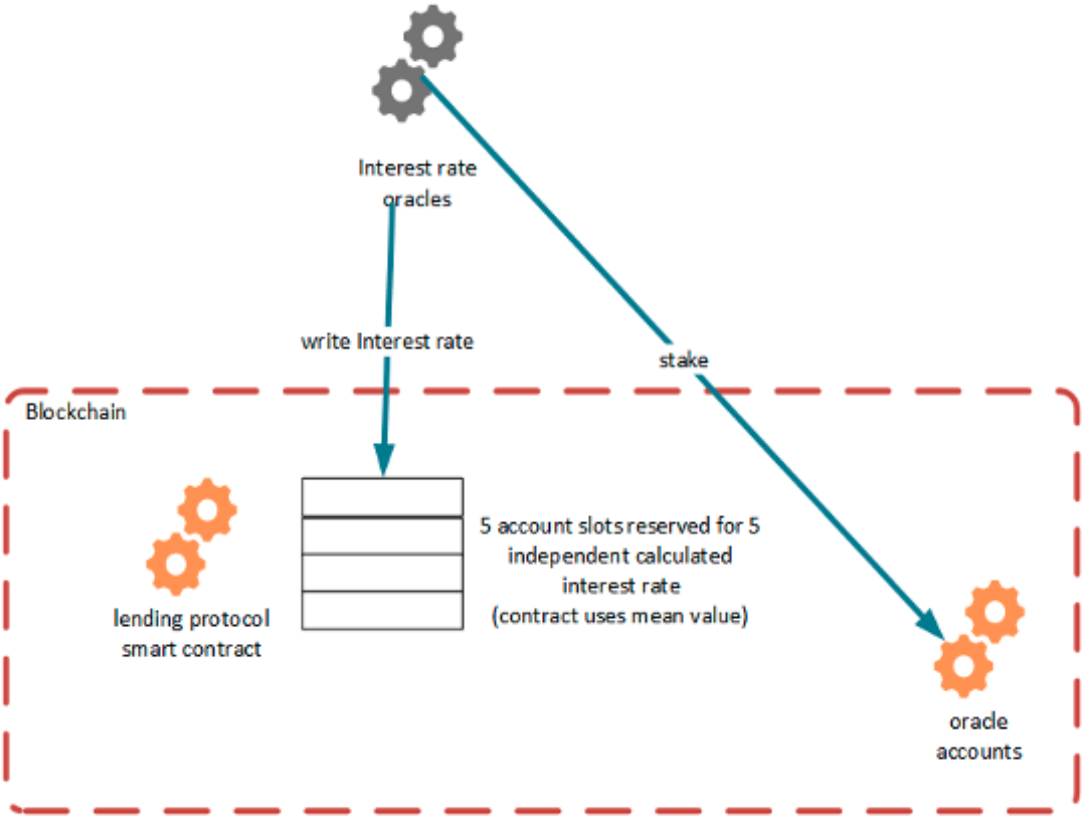
If the value of U is too high means that the protocol borrowing capacity is low. As a response, the deposit interest rate will be increased, and consequently, the borrow interest rate will be increased.
On the contrary, if U value becomes too low, the protocol exhibits low returns on capital, incentivizing new borrowers to lower the borrow and the deposit interest rates.
So, to leverage the utilization ratio, the protocol implements the following rules:

- high U => high rates => incentive deposits
- low U => low rates => incentive borrow

Interest rate calculating oracle

As suggested by the name of this oracle, it is used to calculate the interest rate. The following diagram shows the oracle structure, which is based on a competing scheme:

1. A number N of oracles submit an independently calculated interest rate in N predetermined memory slots.
2. Oracles share-in platform earnings for sharing genuine writes.
3. Oracles share platform earnings to do their job fairly. But to disincentive malicious behaviours, each oracle has a stake in the token.
4. Erroneous writes (i.e., limit percentage difference > medium value) is punished with stake-slashing.


Interest rate oracles
write Interest rate
stake
Blockchain
lending protocol smart contract
5 account slots reserved for 5 independent calculated interest rate (contract uses mean value)
oracle accounts

Governance

The Algolend protocol governance will feature an off-chain, signalling-only governance system where token holders will be given a chance to

- A. put up proposals for a community vote

- B. vote on community and developer sponsored proposals
- C. Adding new assets into the protocol
- D. Adding new yield strategies
- E. Modifying risk tolerance level

In this way, ALEND can be valued as a governance token whose holders can help decide key protocol parameters and weight in the project's future direction.

ALEND holders are responsible for answering the protocol's regulation parameters. Moreover, Algolend incomes will be distributed to ALEND holders.

Protocol features

The features of Algolend are the following:

- **A trusted oracle for inserting price on-chain:**
  Sources of the exchange rates across supported token pairs**.**
- **An ownership token to represent a deposit or a borrow:**
  i.e.denominated version of the lent/borrowed token**.**
- **A governance token to vote and modify protocol mechanics parameters and future upgrades:**
  The token gives its community of holders the ability to vote on key changes of Algolend.
- **Algolend will use Algorand unique features, for example, “Atomic swap”.**
  Users will be able to exchange crypto assets in a decentralized way.
- **Platform Incentives:**
  Algolend will be able to provide and distribute incentives.
- **Rekeying:**
  Algolend offers the flexibility for users and custody providers to change Private Spending Keys anytime without changing Public Addresses, giving Public address more permanence and reducing operational overhead while allowing for account novation.

IBCO

Algolend utilizes the Initial Bonding Curve Offering (IBCO), an innovative token public sale mechanism, with the same settlement price for all of the participants. The IBCO prevents front-running issues or manipulating the price of a token. IBCO is used to control the price at which a supply of tokens is released into circulation.

IBCO allows to buy and sell tokens at any time during the settlement period. The token price increase/decrease following the mathematics defined in IBCO smart contract. The Algolend team prior settles the IBCO behaviour.

The final price that the ALGOLEND tokens will be distributed will be the same for all contributors, resulting in eliminating the use by malicious actors of trading bots.

Conclusions

Algolend is the Blockchain Italia team’s research results to develop an innovative money market protocol on Algorand.

The higher aim of Algolend is to be the milestone of the Algorand DeFi ecosystem. The protocol will be under continuous improvement through time, based on its community request, following all decentralized applications ideals.

The team's aim is that Algolend enables its users to simply and fairly obtain financial service (borrowing/lending) worldwide.

Algolend is a community-centred platform. More than half of the token governance supply is devoted to the community, decentralizing the protocol governance, aiming to give the protocol control to its users.

The Algolend team has designed, on the same principles and aims mentioned above, a tokenomics which is fully detailed in the Algolend Tokenomics paper.