

The ĞARD Protocol

by Rylie Rueda, David McCabe, and Ryan Soscia

2/24/2022

Abstract

There is significant liquidity locked in Algorand's Governance protocol. Consequently, there is considerable demand for a solution to increase governance composability. The GARD Protocol effectively creates a system that will further reward the individual's governance position by allowing them to leverage their Governance commitment to mint GARD, a stable coin.

I. Background

GARD is the first truly decentralized dollar and the first algorithmic stablecoin on Algorand. By improving on ideas from prominent DeFi projects such as MakerDAO, Staticoin, Fei, and TerraLuna, GARD has been created for those seeking the most utility from their capital. Upon release, GARD will target Algorand Governance participants; however, with time it will spread across chains to drive demand, growth, and composability. While the protocol is launching with exclusively ALGOs for collateral, other assets from new chains, including Bitcoin, may also serve as collateral in the future to leverage new techniques to facilitate loans that reward the GARD Protocol's users.

Building on Algorand is the obvious choice for many reasons, including its eco-friendliness as a Pure Proof-of-Stake network, fast block finality, low transaction fees, and permissionless and decentralized nature.¹ Another particularly attractive benefit of building on Algorand is the

¹ <https://www.algorand.com/>

platform's built-in governance protocol, which effectively hands off the decisions over the future of the network from the founders.² ALGO holders are able to vote on policy decisions with their ALGOs in exchange for locking them up for a voting period. This means the community is able to actively select and fund the projects that yield the most benefit for the network. Last but not least, the Algorand team and community is full of passionate researchers, developers, and entrepreneurs with the common goal of improving the Algorand protocol for all.

The protocol is distinct in a few key ways: blockchain, collateralized debt position structure (CDP),³ and collateral. First and foremost, by building on Algorand, the protocol uses the only blockchain to solve the blockchain trilemma.⁴ Next, the way CDP positions are structured incentivizes "borrowers" to mint GARD and keep their positions open since this is more capital efficient.. Finally, it's important that CDPs

² <https://algorand.foundation/governance>

³ CDP=representation of a debt position that is backed by an underlying pool of assets

⁴ trilemma=security, scalability, and decentralization

are backed by ALGOs and not a floating, made-up token to ensure ample liquidity and prevent users from falling victim to a liquidity issue or bank run as experienced by many other stablecoin offerings.

Additional spend is created by tokenizing users' governance positions and giving them a line of credit based on the number of ALGOs they committed to governance. To mint GARD, users must commit at least 140% of the value minted in ALGOs. In order for users' positions to stay in good standing, their collateral must remain above 115% of the value of minted GARD. Users are encouraged to have much more than the minimum required to ensure they remain in good standing with little oversight. This incentive is further reinforced as all ALGOs currently locked up are not circulating, so even a small increase in utilization will result in a large impact. If the value of collateral drops below 115%, the protocol utilizes a Dutch Auction system similar to that of MakerDAO to sell the collateral on the open market for GARD, ensuring there is always enough collateral locked in the system for the GARD in circulation. All of this is facilitated by a system of proprietary oracles and smart contracts that belong to the GARD Protocol.

II. ALGO

ALGO is the native cryptocurrency on the Algorand blockchain designed to help create an open and borderless economy where everyone can participate. Algorand's blockchain is a Pure Proof-of-Stake system designed with the intent of solving the

blockchain trilemma; security, scalability, and decentralization. This high performing Layer-1 blockchain, with the introduction of governance, has effectively become a DAO⁵ by enabling Algorand Governors to vote on future developments while earning rewards (18% APY in governance Period #1 and an estimated 9.4% APY in governance Period #2 depending on the number of ALGOs contributed by governors) for staking their ALGOs on a quarterly basis.

III. GARD

GARD is the world's first algorithmic stablecoin on Algorand's blockchain. It is minted by Algorand Governors who choose to participate in governance through the GARD Protocol instead. These new governors i.e. GARDians⁶ will now send their ALGOs to a smart contract account and commit their ALGOs to create collateralized debt positions (CDPs).

GARD is backed by intrinsically valuable collateral and is designed to be a truly decentralized dollar. In other words, GARD is designed to be pegged to USD through a set of rules and balancing mechanisms.. Users may mint new GARD by sending their ALGOs to a personalized smart contract account. Users are then free to use their GARD to participate in DeFi. The GARD Protocol creates a system where actively participating users are able to obtain a yield higher than APY earned from participating in governance and reducing

⁵ DAO=Decentralized Autonomous Organization

⁶ GARDian=ALGO Governor participating through GARD Protocol

opportunity cost courtesy of the minted GARD.

IV. GAIN

GAIN is the token that governs the GARD Protocol. Those who hold GAIN will be able to vote on changes to the GARD protocol, vote on the fees that GARD users are charged, and vote on the organization that will protect/further develop the protocol. GAIN will be decentralized so the DAO can make the best decisions for its future without founder interference. See the DAO section for more details, including technical functionality and initial votes.

GAIN will allow users which have participated in the governance process to receive rewards from participation in protocol governance, which would entitle them to a portion of the TVL of ALGOs in the Treasury. Users which have fulfilled certain participation thresholds (e.g. voting turn-out, proposal submission) are able to extract the rewards they are entitled to by exchanging their tokens with the Treasury and the Treasury will send the token holder the ALGOs earned. GAIN tokens in the Treasury are out of circulation; there is no way for GAIN tokens to leave the Treasury smart contract account (unless governance votes otherwise). The exact equation for the TVL extracted using this method (without transaction fees) is:

$$ALGOs\ Sent\ to\ User = \frac{GAIN\ Exchanged * Treasury\ ALGO\ Balance}{Initial\ GAIN\ Supply - Treasury\ GAIN\ Balance}$$

This mechanism should lead to more ALGOs becoming locked within the Treasury due to protocol fees.

V. CDP

ALGOs are intrinsically valuable collateral that can be used to mint GARD in the GARD Protocol through smart contract accounts that act as Collateralized Debt Positions (CDPs). Users are able to mint GARD while sending their collateral to a personalized smart contract via Atomic Swap. Once their collateral is present in the contract, it is able to participate in Algorand Governance votes to earn yield. Importantly, for users to reclaim their collateral, they must return the GARD they minted to the GARD reserve plus a 0-3% fee determined by the DAO in ALGOs based on how much GARD is returned.

CDPs are custodial and will be associated with the original owner and thus the Algorand account by which they were generated. Users will directly interact with their CDPs to execute whatever functions of the GARD Protocol they desire from their appropriate accounts. The one exception of the CDPs being custodial is that if the value of the locked collateral drops below 115% of the value of the GARD minted, the collateral is sold via Dutch Auction (See “Liquidation”).⁷ The Dutch Auction is an essential part of the protocol that is the first line of defense utilized in maintaining a stable price of 1 USD for GARD. It’s important to note that there is no clawback and users will still hold any GARD minted plus whatever excess collateral is returned to them minus the liquidation fee if liquidated.

⁷ Dutch Auction=a method of selling in which the price is reduced until a buyer is found.

In order to prevent liquidation, users may deposit additional collateral at any time. In general, minting as much GARD as possible allows for higher yield, but brings a higher chance of liquidation: more risk and more reward. Of course, users are free to mint as much as they want to suit their own personal risk preferences.

i. CDP Lifecycle

Step 1: Creation and Minting

Users send their ALGO to a personalized smart contract and mint GARD from the reserve at the same time through an Atomic Swap. For every 1 GARD minted there must be 1.4 USD worth of ALGO deposited into the contract.

Step 2: Committing / Voting / Additional Minting

During the commitment period of Algorand Governance, CDP holders must send a commitment transaction to the Algorand Governance address. Once this transaction is complete, CDP holders can wait until the first voting period begins. During each voting period, a user must send a vote transaction to the proper governance address from the contract. In other words, a CDP holder is responsible for voting in Algorand Governance in order to receive the rewards. If users fulfill their commitments to vote from their CDP on all the proposals during a period, they will be automatically sent their Algorand Governance rewards by the Algorand Foundation (Note: these rewards

can be sent to the CDP or to another account).

It is also possible that the value of ALGO will rise after it has been initially deposited into a CDP. In this case, a CDP holder is able to mint additional GARD from their CDP, increasing their debt and ability to participate in DeFi. This means that long-term holders will be able to gain additional spend out of their CDPs in the future so long as the relative value of ALGO increases. In the future, users can choose to make their CDPs tradeable.

Step 3a: Closing CDP

A CDP holder is free to close their position at any time. To unlock their collateral, a user returns the GARD they minted back to the GARD reserve and transfers the ALGO (minus fees) from the CDP Smart Contract back into their account via Atomic Swap.

Step 3b: Liquidation

In the event that the value of the ALGO held in a CDP falls below 115% of the value of the GARD debt, the CDP may be liquidated. A blockchain monitor (“Keeper”) may profit from this situation by repaying the GARD debt of the CDP holder and claiming the collateral within. The collateral is sold via Dutch Auction to obtain as much GARD as possible for the collateral to maintain system integrity. After the GARD reserve has been sent their debt, the remaining GARD from the sale (minus fees) is returned to the CDP holder. So, even in the event of a liquidation, a CDP holder will still retain all the GARD

that they have minted. When a CDP is liquidated, governance rewards are forfeit.⁸

VI. Tokenomics

GAIN is the governance token for the GARD Protocol which allows holders to vote on protocol features and/or parameters.

Fundamentally, GAIN exists as a mechanism to control the GARD Protocol including voting on ecosystem changes, setting fees, and managing pricing information. Conversely, GARD is an algorithmic stablecoin with a theoretically unlimited supply.

i. GAIN Total Supply

GAIN has a fixed total supply of **2 billion tokens**, out of which there are currently **0** in circulation. **1.04B** are slated for the public while the remaining **960M** are to be used for private fundraising, hiring advisors, and compensating the team.

Upon launch, a small portion of tokens will be unlocked for presale, ecosystem incentives, and initial sale tokens. As each subsequent governance period passes, more tokens will be released from the DAO and traded publicly. Substantial withdrawals of public tokens from the manager account (>20M or 1% of all tokens) will be announced 2 weeks in advance by the DAO in case token holders wish to part ways with the project.

⁸ ALGOs must remain in the CDP Smart Contract account for the entire governance period to remain eligible.

Public Tokens: **1.04B** tokens will be controlled by the managing account (appointed by the DAO) and will be used to promote the growth of the GARD Protocol. These tokens are unlocked and owned by the GAIN token holders. **740M** of these tokens will be used to fund adoption initiatives like listings, partnerships, marketing, etc. **300M** will be used to strengthen the protocol as liquidity by the DAO Treasury.

DAO Treasury: **300M** tokens will be set aside specifically to fund the Treasury. The Treasury will serve as a liquidity pool of last resort for the protocol and play a vital role in stabilizing the price of GARD during periods of increased volatility. These tokens will be unlocked and controlled by the GAIN token holders.

Sale Tokens: **500M** tokens will go to purchasers and strategic partners to ensure the success of the project. Upon TGE,⁹ pre-seed and seed tokens will begin their vesting period and the rest of tokens sold to purchasers will follow a vesting schedule beginning when subsequent rounds are filled.

Team/Advisor Tokens: **460M** tokens will go to team members and advisors. These tokens will be locked for the first year and begin vesting linearly over 3 years.¹⁰

⁹ TGE - Token Generation Event

¹⁰ *Disclaimer* this breakdown is the best estimate but subject to change by DAO

Figure 1: Gain Token Distribution



VII. Key External Actors

The GARD Protocol doesn't solely rely on its smart contracts, instead, it entrusts its success to a number of external actors. These actors are Keepers, Price Oracles, DAO participants, and the DAO manager account. These actors will be discussed below.

i. Keepers

Individuals who help keep GARD at its 1 USD peg through arbitrage will be known as Keepers. One way Keepers maintain the system is through bidding with GARD on collateral (ALGOs) when a CDP position is liquidated. This ALGO can be acquired at a discount as it will be worth more than the debt owed to the reserve to claim it. Keepers will monitor the blockchain to know when a CDP is in default (value of collateral therein is below liquidation threshold of 115%). Our web app will also track the CDP positions in default and display the current price (in GARD) of a CDP that is being liquidated. When there are small fluctuations in the price of GARD, arbitrage opportunities will present themselves to community members

and enable them to capitalize on price discrepancies. Namely, if someone offers to buy GARD for over 1 USD, Keepers are able to profit by opening short-term CDPs without closing fees. Because our protocol is unbiased and will always treat GARD as worth 1 USD, users will be able to enter and exit CDP positions quickly to help maintain equilibrium without incurring fees.

ii. Price Oracles

In order to properly calculate the overcollateralization ratio of a CDP and the value of collateral in an account, it is necessary to bring pricing data on-chain for reference. A Price Oracle does this by storing the ALGO/USD price in the global state of a stateful smart contract.

Currently, there is no decentralized ALGO/USD price oracle live on MainNet. Algoracle aims to solve this problem, launching on MainNet in late Q2/early Q3 2022. However, until Algoracle launches on MainNet, the DAO-appointed managing account will maintain the integrity of the pricing data used by the GARD Protocol. This initial system involves a single oracle fetching prices from several APIs, taking the median, and pushing the data on-chain.¹¹

Once Algoracle launches, the DAO manager account will change the pricing data application referenced by the system to an Algoracle-controlled application. This application reference change can only occur

¹¹ Algoracle - A decentralized oracle system. See <https://www.algoracle.ai/>.

twice, which means that after the system has switched to Algoracle data, the DAO Manager account will have no further control over the pricing data source.

iii. DAO Participants

The GARD DAO makes the decisions needed to keep the GARD Protocol running smoothly. The DAO also has the ability to add new functionality and governance options at a future date. The DAO is composed of all holders of GAIN. GAIN holders may participate in the GARD DAO by participating and staking their GAIN (i.e. temporarily locking it in a smart contract for the duration of a vote, then re-claiming upon vote end). Each GAIN token represents one vote in governance decisions. At launch, three key voting contracts will be deployed:

1. Manager selection
2. GARD minting fee
3. GARD returning/CDP closing fee

Voting methodology varies based on the specific contract. Votes for the manager are based on a simple plurality winner.¹² Fees are set based on a majority winner¹³ (if no fee receives 50% of votes, then the previous fee rate remains). Anyone with GAIN may vote in these elections for any valid vote recipient. These votes are held on-chain in voting smart contracts. In both cases, there are fixed length voting periods, with fixed length breaks in between voting.

¹² Plurality=the person with the most votes (even if under 50% of all votes) wins

¹³ Majority=the fee option with over 50% of votes wins

The manager can be any arbitrary Algorand address. The manager serves an executive role, taking actions that must be done by a singular account throughout the system, including actions that occur off-chain such as web application maintenance. The manager may also introduce new voting contracts to the system, “lock-in” contracts as permanent votes of the DAO, and remove voting contracts that have not been “locked-in” as core contracts. New voting contracts enable system upgrades, as these contracts can contain arbitrary functionality, enabling updates over time and not locking the GARD Protocol into a completely immutable system. The initial three voting contracts are locked-in (i.e. are immutable), and may not be removed by anyone. In the long run, the manager should have little or no functionality, as all key decisions will be programmed into smart contracts as the system stabilizes and reaches maturity.

Because participants both use GAIN and stake it to vote, any resulting vote is aligned with the interests of GAIN holders. GAIN holders are strongly incentivized to govern and create the most effective GARD system possible, ensuring all votes benefit the protocol through incentives, paired with sensible winner mechanics in each individual vote.

iv. DAO Manager Account

At first, the DAO Manager account will be controlled by the GARD team. This account will be initialized to a multi-signature account with 3 authorized signatories, at least 2 of whom must sign off on every

transaction. The DAO manager account can be changed by election each quarter. The DAO manager is responsible for web application management, protocol extensions, adding new DAO votes, deploying Treasury funds to maintain the GARD peg, and (only able to do twice) changing the pricing data source for the protocol. For overhead, the DAO Manager is entitled to 18% of the DAO revenue each quarter. The DAO Manager will be elected each quarter, immediately prior to receiving its share of the DAO revenue.

v. Treasury

The Treasury is a smart contract that holds all protocol fees from the system as well as the GAIN tokens from users. GAIN Token holders are able to withdraw liquidity from the system by transferring ALGO out of the Treasury while transferring GAIN into the Treasury via Atomic Swap. The Treasury pays 18% of its fee proceeds (in ALGO) to the DAO Manager account each quarter. It also pays 2% of its fee proceeds to a founder account each quarter.

The Treasury also can be thought of as a liquidity pool of last resort.¹⁴ If the market for GARD becomes particularly volatile, the DAO Manager account will use the ALGO balance of the Treasury to buy GARD through liquidity pools and/or exchanges to push the price up. Similarly, if the price of GARD rises too high, the DAO Manager account may mint GARD at a price slightly above \$1 and sell the GARD for the higher

¹⁴ Liquidity pool=a pot of cryptocurrency assets locked within a smart contract

price through liquidity pools and/or exchanges, depositing the arbitrage profits back into the Treasury and bringing the price down again.

The DAO Manager is the only account able to use the Treasury for price stabilization to aid in prevention of impermanent loss.¹⁵ Again, since this is a last resort, the DAO Manager will use this privilege sparingly, only taking action in periods of high volatility and market irrationality. The current plan is for the DAO Manager to take action if GARD drifts off its peg by 2%. Since the DAO Manager is elected by the DAO, this process will be delegated to GAIN holders as the GARD Protocol matures. The most important role of the Treasury will be to stabilize GARD price to the best of its ability. The Treasury will be most effective under strong capable management and will become a better mechanism as the TVL increases over time with usage of the GARD Protocol.

VII. Fees

Whenever protocol users mint GARD from the reserve, they must pay an opening fee to the Treasury. This fee is initialized to 2% of the value of the GARD minted but can range from 0-3% as determined by the DAO. There is also a liquidation fee; when the value of collateral in a CDP drops below 115% of the value of the outstanding GARD debt, the collateral is sold via Dutch Auction. After the GARD debt has been repaid to the reserve, 20% of the remaining

¹⁵ Impermanent loss=taking value out of the system by capitalizing on price volatility

GARD is sent back to the reserve, while the rest of the collateral (80%) is returned to the account that was liquidated (the CDP holder). There is also a CDP closing fee. Like the opening fee, this is initialized to 2%. Opening and closing fees can range from 0-3% and can be changed by vote of GAIN token holders.

IX. User Experience

A GARD user connects their wallet to a web application (via WalletConnect, Algorand Official Wallet, or AlgoSigner) and is able to lock up their ALGOs in exchange for new GARD. The user is free to transact with their GARD however they see fit, reaping the benefits of Algorand's fast block speed and low transaction fees.

To incentivize users to use the protocol to mint GARD, even though the ALGOs have been locked up, they can still earn governance rewards, participation rewards, and consensus rewards. The ALGOs will continue to accrue participation rewards until they are phased out and are eligible to participate in governance. In other words, the GARD user is still able to vote with their locked ALGOs in governance and can have the corresponding ALGO rewards deposited with their locked ALGOs at the end of each voting period. Accrued rewards in the form of ALGOs can be claimed from the Algorand Foundation along with the locked ALGOs at any time by returning the minted GARD.

X. User Risk

In the event that the value of the collateral drops too low, the collateral will be sold in order to repay a user's GARD debt. This process is called Liquidation. The more GARD one mints relative to their collateral, the more susceptible their CDP is to being liquidated. However, more minted GARD relative to one's committed ALGOs also means more opportunity to participate in DeFi to earn extra yield. By using the protocol, the user acknowledges all known and unknown risks.

XI. Legal

TLDR: Use at your own risk.

You acknowledge, understand and agree that you are not eligible to participate in the distribution of GAIN or GARD, or utilize GARD Protocol if you are a citizen, national, resident (tax or otherwise), domiciliary and/or green card holder of a geographic area or country (i) where it is likely that GAIN or GARD, or GARD Protocol would be construed as the sale of a security (howsoever named), financial service or investment product or where participation in token distributions is prohibited by applicable law, decree, regulation, treaty, or administrative act (including without limitation the United States of America, Canada, and the People's Republic of China), and (ii) that is subject to U.S. or other applicable sanctions or embargoes (including without limitation Cuba, North Korea, Timor-Leste, Cambodia, Republic of the Union of Myanmar, Lao People's Democratic Republic, Tanzania,

Pakistan, Russia, Serbia, Tunisia, Uganda, Mali, Afghanistan, Albania, Angola, Botswana, Cameroon, Chad, Central African Republic, Eritrea, Ghana, Republic of Côte d'Ivoire, the Republic of Guinea, Guinea-Bissau, Somalia, Zimbabwe, Democratic Republic of the Congo, Republic of the Congo, Côte d'Ivoire, Ethiopia, Malawi, Montenegro, Mozambique, Madagascar, Crimea, Kyrgyzstan, Haiti, Azerbaijan, Bosnia and Herzegovina, Uzbekistan, Turkmenistan, Burundi, South Sudan, Sudan (north), Sudan (Darfur), Nicaragua, Vanuatu, the Republic of North Macedonia, the Lebanese Republic, Bahamas, Kosovo, Turkey, Iran, Iraq, Liberia, Libya, Syrian Arab Republic, Tajikistan, Uzbekistan, Yemen, Sri Lanka, Ukraine, Belarus, Bolivia, Trinidad and Tobago, and Venezuela)

References

Edge, P. (2017, October 16). *statiCoin and riskCoin*. GitHub. Retrieved February 20, 2022, from <https://github.com/genkifs/staticoin/blob/master/Staticoin%20-%20Whitepaper.pdf>

Emurgo. (2021). *The AgeUSD Stablecoin Protocol*. GitHub. Retrieved February 20, 2022, from <https://github.com/Emurgo/age-usd>

Kereiakes, E., Kwan, D., Di Maggio, M., & Platias, N. (2019, April). *Terra Money: Stability and Adoption*. Terra Money. Retrieved February 20, 2022, from <https://docs.terra.money/whitepaper>

MAKR. (2020, February). *The Maker Protocol White Paper*. Retrieved February 20, 2022, from <https://makerdao.com/en/whitepaper/#introduction>

Micali, S. (2020, November 24). *A Proposal for Decentralizing Algorand Governance*. Retrieved February 20, 2022, from <https://www.algorand.com/resources/blog/decentralizing-algorand-governance-nov2020>.

Sam, A. (2022). *Stablecoin Evolution: The Overall Unbiased History and Projected Future of Financial Technology*. Tech and Authors with Mass Crypto Publishing.

Santoro, J. (2021). *Fei Protocol: A Decentralized, Fair, Liquid, and Scalable Stablecoin Platform*. Fei Protocol. Retrieved February 20, 2022, from <https://fei.money/static/media/whitepaper.7d5e2986.pdf>