Coin Governance System

Powered by the wisdom of the crowd

Written by:

Alejandro Gómez de la Cruz

Adrián Calvo

Pablo Moreno de la Cova

Carlos Kuchkovsky

Version 0.6

Release date: March 7th, 2018

Coin Governance System

Powered by the wisdom of the crowd

Coin Governance System

Powered by the wisdom of the crowd

Alejandro Gómez de la Cruz

Adrián Calvo

Pablo Moreno de la Cova

Carlos Kuchkovsky

Version 0.5
February, 2018

1. Abstract

In decentralized networks, having a strong governance system to rule its participants is crucial. Each group of participants in a decentralized system has their own interests, it is essential to maintain them aligned. Therefore the system needs mechanisms to coordinate them around their common incentives to avoid imbalances in their power.

Initial Coin Offerings have demonstrated how easy it can be for a company to raise capital by selling tokens. However, the interests of the ICO launchers and those of the investors are not always aligned, especially in large ICOs. In this sense, an extremely capitalized company could lose sight of the initial vision on the company, while participants in the ICO seek the best execution of the company's business plan, the development of solid products and the appreciation of their tokens.

In this paper we propose what we call the "*Coin Governance System*", which consists of a series of smart contracts that will hold the funds raised in the ICO in escrow. Those funds will be released to the ICO sponsor over a period of time. However, if the participants in the ICO lose faith in the project, they may trigger a voting mechanism which could enable ICO token holders to withdraw the funds remaining in escrow.

2. Introduction

Good governance is a key point when we talk about decentralized networks in general, or blockchain in particular. Decentralized networks break with the traditional hierarchical models (vertical) and facilitates a model in which hierarchy does not exist (horizontal). In this sense, different groups of participants have different and common interests. Having a strong governance system to rule them is crucial. It is essential to maintain the incentives of those participants aligned. Therefore, **the system needs mechanisms to coordinate those participants around their common incentives, and avoid imbalances in their powers**.

Governance could be exercised on-chain or off-chain. On one hand, on-chain governance mechanisms could both ensure that a process is properly followed and allows fast decision making. However, it will not be not easy to change an on-chain governance mechanism once it is established. Furthermore, if it is not well designed it is exposed to exploits and hacks. On the other hand, off-chain governance mechanisms (i.e. Bitcoin Improvements Proposals -BIPs[1]- and mailing lists in the case of Bitcoin) could be modified easily but it makes the coordination of its participants more difficult.

An Initial Coin Offering (ICO), a process by which a company issues a series of tokens in exchange for cryptocurrencies (in general) through smart contracts, has both decentralized and centralized components.

On one side, the process by which the participants of an ICO send cryptocurrencies to a smart contract in exchange for tokens is managed autonomously by the referred smart contract in a decentralized way. On the other, the process of holding and spending the raised capital is fully controlled and centralized by the company itself.

This makes it harder to align the incentives of the ICO launcher with those of the token buyers and to enforce a mechanism of coordination between them, given that there is an imbalance of power. In this sense, **once the ICO is completed, ICO token holders have no control over the management of the funds, and if they are unsatisfied they can only sell their tokens in a secondary market**. This brings ICOs to the classic problem of *agency costs*[2] which economists have tried to solve for years.

To solve this issue, we have devised the "**Coin Governance System**", which is **an on-chain coordination mechanism that could strengthen and align the common interests of ICO launchers and token buyers, preventing that their individual interests create an imbalance of power between them.**

[1] Bitcoin. "*Bitcoin/Bips*." *GitHub*, 21 Feb. 2018, github.com/bitcoin/bips.
[2] Staff, Investopedia. "Agency Costs." Investopedia, 3 June 2016, www.investopedia.com/terms/a/agencycosts.asp.

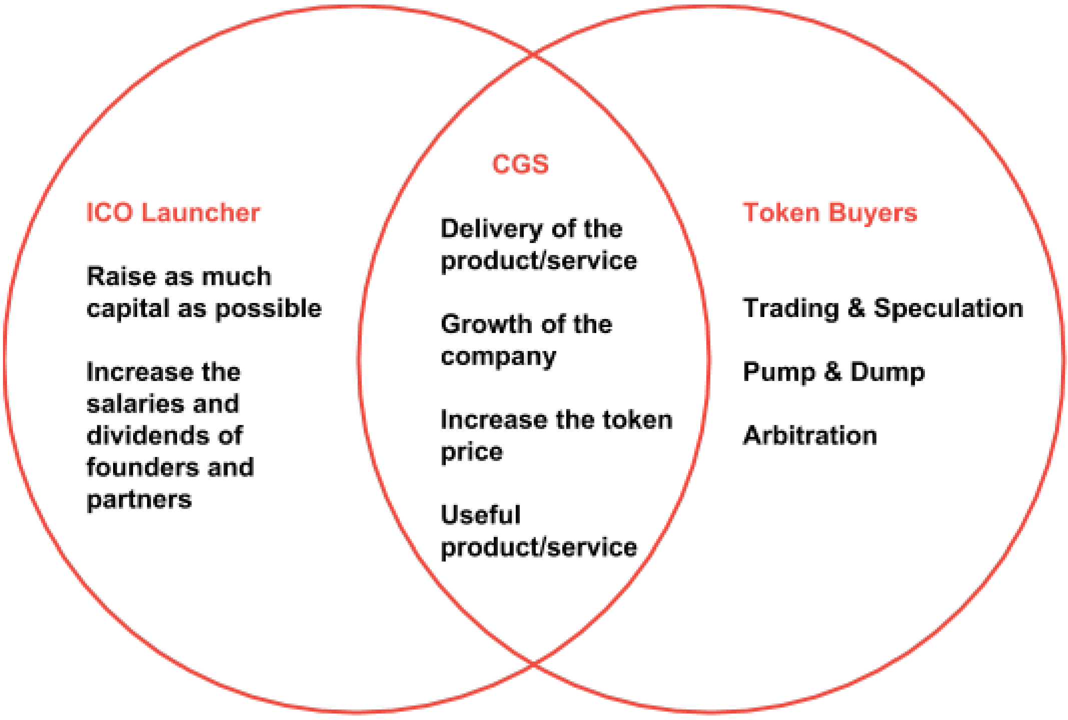


Figure 1: Venn Diagram showing divergent and common interests involved in an ICO

The mechanism of coordination between the ICO launcher and the token holders is a smart contract that receives and holds the capital raised during the ICO in escrow. As a general rule, that smart contract will be making the raised capital available to the company gradually (on a per day basis). Nevertheless, if the interests of the token holders and the ICO launcher were to become misaligned, they would have a way to withdraw the capital remaining in the smart contract.

We have studied two ways to implement a Coin Governance System system:

a. **ICO Token holders can vote directly to trigger the possibility of withdrawing the locked funds**

   We found that this system does not align 100% the interests of the different participants entirely. Allowing the token holders to vote directly could create perverse incentives. For example, a token holder with a huge amount of tokens could trigger the voting mechanism of withdrawing the locked funds for arbitrage related reasons (they could arbitrate on the price of the token and the funds held by the company, for example). This could damage the reputation or funding position of a project that is actually delivering on its execution.

b. **Create a specific role (a decentralized arbiter: CGS Token holders) to coordinate the governance system**

   This is the mechanism we have chosen to implement our Coin Governance System. Under this system, when the voting system is triggered, a certain percentage of ICO funds will be locked up while the voting is taking place.

With the tokens locked in the scrow, CGS Token holders will vote about whether to allow the withdrawal of the funds in the escrow contract. With this voting system, it would be the decentralized arbiter who would judge if the interests and incentives of the ICO launcher and the token buyers are still aligned, when deciding whether to enable ICO Token holders to withdraw their funds.

This mechanism solves imbalance of power issues that arise in point (a). With the proposed system, the users taking part in the decision of the decentralized judge are incentivized to vote correctly, because they can gain or lose CGS Tokens depending on it.

In summary, **we have built a governance system that aligns the incentives and interests of its participants, decentralizing the most conflictive point of an ICO, the management of the funds raised**.

3. State of the Art

Good governance is essential for a decentralized network to succeed in the long term. Therefore it is not surprising that there is a lot of literature about blockchain governance[3]. We can highlight an article written by Fred Ehrsam[4] in which he exposes the critical components of governance (incentives and mechanism for coordination) and potential governance strategies that could be tried on a blockchain like Ethereum:

a. **Liquid Democracy:** Every participant can vote by themselves, but they can also delegate their vote to someone else, or alternatively remove their vote delegation.

b. **Futarchy**[5,6,7]: It consists of aggregating knowledge from across a community of people using prediction markets.

c. **Quadratic Voting:** It consists of buying votes and each additional vote costs twice as much as the one before it.

d. **Quadratic Coin Lock Voting**: This is a mechanism that has been proposed by V. Buterin, in which N coins let a participant make N*k votes by locking up those coins for a time period of k^2. This system is quite interesting because it aligns incentives over time, as to increase voting power it requires maintaining a decision for longer.

Furthermore, in his post against on-chain governance, Vlad Zamfir highlights a relevant point. Although it could be possible to come up with an ideal governance proposal, it might not be possible for participants to adopt it, due to pre-existing constraints on the participants' ability to do so.

> *"Even if you somehow come up with an ideal governance design, you haven't "solved governance" for anyone until it is successfully adopted".*
> **Vlad Zamfir** *(Ethereum Foundation Researcher)*

Zamfir argues that blockchain governance is not an abstract design problem, it is a social problem, defined in the context of existing governance structures. Therefore, we need to look at the existing governance processes that we already have before we propose alternatives. However, his post refers to governance of blockchain networks understood in themselves (such as Bitcoin or Ethereum), where there are governance mechanisms (on-chain an off-chain) from day 1. However, there are few precedents related to

[3] "Notes on Blockchain Governance", 17 Dec. 2017, http://vitalik.ca/general/2017/12/17/voting.html

[4] Ehrsam, Fred. "*Blockchain Governance: Programming Our Future* – Fred Ehrsam – Medium." *Medium*, Medium, 27 Nov. 2017, medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74.

[5] "*Shall We Vote on Values, But Bet on Beliefs?*", by Robin Hanson, http://mason.gmu.edu/~rhanson/futarchy2013.pdf

[6] *Forecasting Elections Comparing Prediction Markets, Polls, and their biases*, by David Rothschild, Public Opinion Quarterly, Vol. 73, No. 5 2009, pp. 895–916. http://researchdmr.com/RothschildPOQ2009

[7] "*Prediction Market Accuracy in the Long Run.*" *International Journal of Forecasting*, Elsevier, 28 Apr. 2008, www.sciencedirect.com/science/article/pii/S0169207008000320.

governance mechanisms applied to the management of collective funds (except for THE DAO, and a few other examples).

The following are some blockchain projects and proposals of implementing governance structures using the abovementioned governance strategies:

ARAGON[8]

Aragon Project proposes a token-based digital jurisdiction with no borders in which governance plays a key role. In this sense, governance will rule aspects such as token issuance (generation of tokens, revenues, etc.), fund allocation (rewards) or the network rules (the establishment and removal of bylaws).

They initially propose a **liquid democracy**[9] to rule these aspects. However, they state in their white paper[10] that other governance mechanisms are being considered, such as futarchy.

The main elements of the Aragon Network are: the bylaws that define user permissions, the governance system to make decisions, the capital system for issuing and controlling tokens and an accounting system to manage funds. The main decisions are made by ANT (Aragon Network Token) holders through a system of proposal and voting.

Regarding governance, **Aragon's Arbitration mechanism proposal** is one of their most interesting features. In this sense, they advocate a three level arbitration system:

- First, the arbitrage applicant (posting a bond) opens an arbitration. Then a sample of **5 randomly chosen judges** post a blind bet (resolution). Afterwards, all of the judges reveal their secret bet, rewarding the judges that voted for the right answer (by majority) with a reputation of non-transferable tokens and penalizing the others.

- Second, if the applicant is not satisfied with the decision, they can request an upgrade to the next level, a **prediction market** (i.e. Gnosis or Augur) in which all of the network judges can participate.

- Finally, if the applicant is not satisfied with the two previous steps, they can request an upgrade to the ultimate level, which is a court composed of the **top 9 judges**, who are rewarded if they voted for the right answer and penalized if they vote the wrong one.

This mechanism could solve several types of dispute that could arise in a decentralized network but it could face relevant issues when put it in practice. First, the final decision is mostly based on individual decisions, so a strong reputation system is needed for that. In this sense, reputation is a pending matter when talking about blockchain. Second, part of the mechanism, the prediction markets, depends on third party developments that are not

[8] "*Unstoppable Organizations.*" *Aragon*, https://aragon.one/.
[9] "*Delegative Democracy.*" *Wikipedia*, Wikimedia Foundation, 20 Feb. 2018, https://en.wikipedia.org/wiki/Delegative_democracy
[10] Aragon White Paper: https://github.com/aragon/whitepaper/blob/master/Aragon%20Whitepaper.pdf

sufficiently developed. Finally, the process involves many steps, so it could be easy to find a lack of liquidity in the decision making (there is a chicken-egg problem between the problems to be judged and judges that solve them).

WINGS[11]

> *"WINGS creates a decentralized forecasting ecosystem that gives tangible incentives for WINGS token holders to put the effort in making the best available choices to maximize their rewards".*

As defined in its white paper[12], Wings is a blockchain platform that seeds and nurtures a community dedicated to the launching, backing and promotion of new project proposals through a fluid organizational model, referred to as a Decentralized Autonomous Organization (DAO). Although Wings is largely focused on forecasting markets, they also propose governance models in its White Paper.

Wings mentions in its white paper that it will work with a Liquid Governance (fluid delegation of power). It consists of a hybrid between direct and representative governance models, enabling the participants to freely lend and recover decision power to and from people they trust. However, they propose other variations based on community demands.

Liquid democracy will be used by DAO projects in order to take the most important decisions, such as modify a suggested DAO or update the smart contracts of a certain project.

Though Wings addresses governance in several use cases and situations, the project seems to be focused in forecasting markets, considering other use cases just for future implementations.

DAICO[13]

DAICO is a concept proposed by Vitalik Buterin that tries to merge the benefits of Decentralized Autonomous Organizations and Initial Coin Offering structures. This idea has several similarities with the Coin Governance System, but some issues have been approached in a different way.

A DAICO model works as follows. First, DAICO's smart contracts are in "*contribution mode*", where a single project raises funds for their project (ETH in exchange for tokens). Once the contribution period ends, the ability to contribute ETH stops, and the initial token balances are fixed, being the tokens tradeable from there. Then, the contract has one major state variable: tap (wei[14]/second), initialized at zero. Tap determines the amount per second that the project team can take ETH out of the smart contract. Token holders can vote on

[11] "Wings – DAO Platform." *Wings – DAO Platform*, https://wings.ai/.
[12] Wings whitepaper: https://wingsfoundation.ch/docs/WINGS_Whitepaper_V1.1.2_en.pdf
[13] Vbuterin, et al. "*Explanation of DAICOs.*" *Ethereum Research*, 5 Jan. 2018, https://ethresear.ch/t/explanation-of-daicos/465.
[14] 1 ETH = $1*10^{18}$ WEI

resolutions, such as: raising the tap (lowering the tap is not possible); or permanently self-destructing the contract (putting the contract into withdrawal mode).

In this sense, voters give the project a reasonable monthly budget, and raise it over time as the team demonstrates its ability to execute the project with the allocated budget. If they do not agree with the execution, they can always vote to shut down the DAICO and get their money back.

The idea of locking the funds during an ICO and unlocking them progressively aligns the incentives of the ICO launchers and the token holders more effectively than giving the former full control over the funds from the outset. However, governance is a matter of balance and this mechanism could in turn create an imbalance of power in favour of the ICO token holders, for example:

- A large ICO token holder could at any point try to self-destruct the contract for reasons totally unconnected to the execution of the project (to discredit the project, to arbitrate between the remaining ether and the price of its token or any other reason). This issue may arise because the token holder and the voter is the same person. We would expect small ICO projects, with a smaller community of users/followers and a lower market valuation, to be particularly vulnerable to this type of "attack".

- Another problem that could arise from the DAICO is that the self-destruct function is triggered by a majority vote, when there could be the case that some ICO token holders are happy with the way the project is being executed and would like to maintain their support.

BUILDING A TOKEN-BASED GOVERNANCE

We have found that **having a specific governance token distributed along a large community of ICO arbiters could solve this imbalance of power**. If we create incentive mechanisms to make governance token holders impartial in voting the successful/proper execution of the project, we will achieve the following:

- As the specific governance token is more distributed and used for multiple ICOs, the specific **ICO launcher would be more protected against unjustified attacks from big holders** of the specific token.

- In case the governance token holder community decides to open the "withdraw ether" function, **those holders who are happy with the project execution may maintain their tokens and respective funding to the project**.

- Finally, **the system would have a governance token community, incentivised by a prisoner's dilemma to vote correctly on the successful execution of the project**, playing the role of arbitrator of the system.

4. Product: The Coin Governance System

a. Introduction

After studying the functioning of many ICOs, we have come to the conclusion that governance is one of the most important problems which are still outstanding. As discussed previously, there is currently a dangerous imbalance of power in favor of the ICO launcher who has an almost absolutely free disposition of the raised funds.

However, as we have analysed in the previous section, we also believe that transferring all the control over the funds from the ICO launcher to the ICO token holders can cause the opposite effect, and generate new problems.

Therefore, **we propose a Coin Governance System (”CGS”) that introduces a third agent, the arbiter**, who will help keep the interests of the other two participants aligned. The arbiter will be incentivised to act properly.

b. Participants/Roles

- **ICO Launcher:** The company that launches an Initial Coin Offering and sells its tokens in exchange for Ether. They will implement the Coin Governance System. They will also receive the ether raised in the ICO as time goes by and it becomes available.
- **ICO Token holder:** Any person that holds tokens sold by the ICO launcher. They can open a claim on the suitability of the ICO launcher’s execution, and they can withdraw the remaining Ether if the result of the dispute is positive.
- **Arbiter: A community comprising** any person that holds CGS Tokens. They are independent from the ICO launcher and the ICO token holder. They can vote on the suitability of the ICO launcher’s execution and they are incentivised by a prisoner’s dilemma type game theory.

c. Functioning of the CGS

Simple diagram:

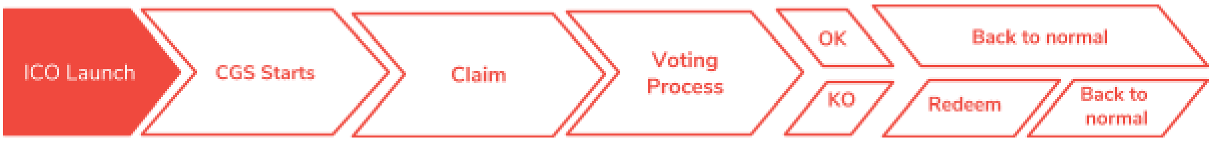
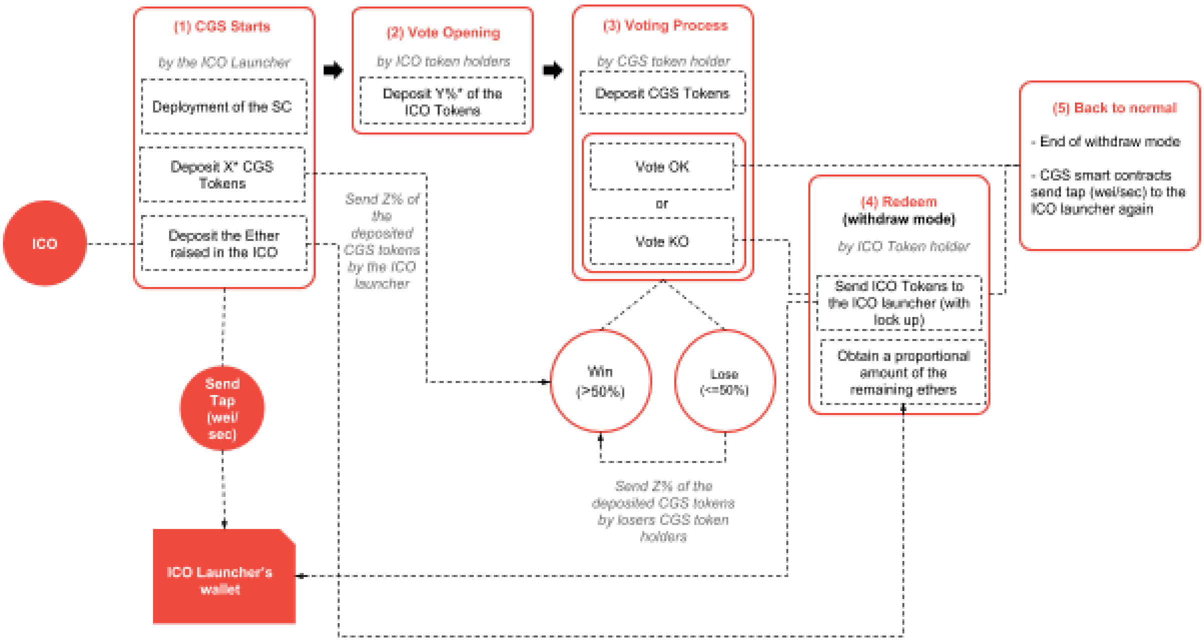


Figure 2: Simple flowchart showing a CGS process.

Complex diagram:


(1) CGS Starts
by the ICO Launcher
Deployment of the SC
Deposit X* CGS Tokens
Deposit the Ether raised in the ICO
(2) Vote Opening
by ICO token holders
Deposit Y%* of the ICO Tokens
(3) Voting Process
by CGS token holder
Deposit CGS Tokens
Vote OK
or
Vote KO
(5) Back to normal
- End of withdraw mode
- CGS smart contracts send tap (wei/sec) to the ICO launcher again
ICO
Send Z% of the deposited CGS tokens by the ICO launcher
(4) Redeem (withdraw mode)
by ICO Token holder
Send ICO Tokens to the ICO launcher (with lock up)
Obtain a proportional amount of the remaining ethers
Send Tap (wei/ sec)
Win (>50%)
Lose (<=50%)
Send Z% of the deposited CGS tokens by losers CGS token holders
ICO Launcher's wallet

X: Amount of CGS tokens that are needed to deploy CGS smart contracts.

Y: Percentage of ICO tokens that are needed to open a claim.

Z: Percentage of the deposited CGS tokens to be sent by the losers to the winners in the voting process

Figure 3: Complex flowchart showing a CGS process.

- **CGS Deployment**

This part of the process will be carried out by the **ICO Launcher**.

To deploy the smart contracts properly, the ICO launcher will need to deposit a certain amount of CGS tokens[15] in one of the CGS smart contracts. This deposit requirement responds to an incentive for the arbiters that will be explained below.

After making the deposit in CGS tokens, the CGS smart contracts will be deployed for the ICO launcher. Among them, a vault smart contract will be created to hold the ethers raised during the ICO. The ICO launcher will have to include the address of this smart contract in his ICO to collect the funds[16].

During the deployment of the CGS smart contracts, the ICO launcher will be able to set the configuration parameters, such as the tap rate

[15]The amount of CGS Tokens that will be set in the first version of the Coin Governance System will be 0, in future versions this amount will be voted among the CGS holders.

[16] If the ICO launcher decides to use the Coin Governance System once his ICO has started, he could deploy the CGS smart contract later, moving the funds raised in the ICO manually. However, it creates a point of friction, since during a certain period of time, the ICO launcher will have control over the whole raised funds.

or the ICO tokens needed to start a voting process. The tap is defined as the wei/second that the smart contract will release to the ICO launcher.

Once that it is done, the CGS smart contracts will be operational. The smart contracts will be releasing ether as specified by the tap unless a claim is opened by the ICO token holders.

- **Claim Opening**

This process can be carried out by **ICO token holders**.

If one or **several ICO token holders think that the project is not being executed properly, they can open a claim by depositing a certain percentage of the ICO tokens**[17] in one of the CGS smart contracts. Those tokens will be locked during a certain period of time while the dispute is being resolved[18].

This deposit lock up is required in order to avoid spam. As explained below, CGS tokens are incentivized to participate in the system and their participation have a cost for the network, so opening claims for no reason will not be entirely free of charge. The percentage of tokens required also ensures that there is sufficient interest within the ICO token holders to warrant opening a claim.

Once the required percentage of ICO tokens are held by the smart contract, the voting period will start, and will be opened during a certain period of time[19].

If the outcome of the vote does not agree with the ICO tokens holders that opened the claim, they will lose the 1% of their tokens on stake. These tokens will be sent to the ICO launcher.

- **Voting process**

This part of the process is carried out by **the arbiter community**.

The arbiters can vote in any ICO that has an open voting process. The vote will be carried out following the commit-reveal scheme to ensure the confidentiality of the vote during the process. They can vote “OK” if they believe that the execution of the project by the ICO launcher is satisfactory, or “KO” if not.

[17] The percentage stated in the first version of the CGS will be 5%.

[18] The period of time that will be set in the first version of the Coin Governance System will be 10 days.

[19] The period of time that will be set in the first version of the Coin Governance System will be 7 days. Then, voters will have 3 days to reveal their vote.

The result with more votes will be the winner[20], and a certain percentage of the CGS tokens[21] staked by the losers will be proportionally sent to the winners, plus a proportional amount of the CGS tokens deposited by the ICO launcher during the deployment of the CGS.

This type of mechanism is known in game theory as the "prisoner's dilemma"[22]. The possible results ("OK" or "KO") are neutral for the arbiters, whose incentives depends on the voting of the majority and not on the result itself. That is why this system is optimal to balance the powers between the ICO launcher and the ICO token holders.

Finally, if the result of the voting is "OK", the CGS smart contract that unlocks the ether raised in the ICO in favour of the ICO launcher will remain operational, as it was before the vote. In this case, the ICO Token holders that have opened the claim will lose 1% of the tokens that they deposited to open the claim, sending those tokens to the ICO launcher. This mechanism will deter ICO token holders from opening unnecessary claims, and will compensate the ICO launcher for the time he will have dedicated to addressing the claim.

If the result of the voting is "KO", the Coin Governance System will enter into "withdrawal mode", allowing ICO token holders to proportionally withdraw the remaining ethers.

A percentage of the CGS tokens locked in the CGS smart contract by the ICO launcher will also be sent to the winners of the voting process. This proportion will be a function of the time that the CGS smart contracts has been operational with respect to the total duration of the CGS.

So the winners will obtain CGS tokens from the losers of the vote and the ICO launcher. CGS vote winners will be allowed to withdraw those CGS tokens once the withdrawal period has ended.

In conclusion, this mechanism incentivises the arbiters to vote on the success of the execution of the project regardless of the interests of the ICO launchers and the ICO token holders. On the other hand, the ability to open a claim corresponds to the ICO token holders for two reasons: (1) they are the main party interested in opening this vote if they think the ICO launcher is not doing things properly; and, (2) it

[20] If there is tie in the voting (50-50), OK will be deemed as the winner.

[21] The percentage that will be set in the first version of the Coin Governance System will be 20%.

[22] Hofstadter, Douglas R. (1985). «Ch. 29 - The Prisoner's Dilemma computer tournaments and evolution of cooperation». Metamagical Themas: Questing for the essence of mind and pattern. Basic Books. ISBN 0465045669.

avoids possible spam from CGS token holders opening unnecessary claims.

- **Redemption** (Ether withdrawal by ICO token holders)

  This part of the mechanism is carried out by **ICO token holders**.

  If the result of **the voting by the arbiters is "KO", the Coin Governance System will enter into "withdrawal mode"**. This means that **every ICO token holder can send their ICO tokens to the CGS smart contracts in exchange for the proportional remaining ethers**, during a certain period of time[23]. Once this period is over, the Coin Governance System will end its "withdrawal mode" and the CGS smart contract that unlocks the ethers raised in the ICO in favour of the token launcher will resume its normal function.

  The abovementioned allows any ICO token holder to withdraw their ethers and leave the project by sending their ICO tokens, but it also allows for any satisfied ICO token holder to keep their tokens, so the ICO launcher can continue with its activity.

  The ICO tokens redeemed will be locked until the CGS duration is over and will not be taken into account in case of future redemptions, so the ICO launcher cannot manipulate the system during that period. This lock up will guarantee the funding of the project if the ICO launcher continues with the development of the project.

- **Back to normal**

  If the result of the voting is "OK", the CGS smart contracts return to its status before the claim automatically.

  If the result of the voting is "KO", once ICO token holders have withdrawn their ethers from the smart contract the CGS smart contracts return to normal. The speed of release of the funds will remain the same as before (*tap:* wei/second), but there will be less funds available.

  From this point, after a period of time[24], a new claim can be opened in the same way it was done initially.

[23] The period of time that will be set in the first version of the Coin Governance System will be 10 days.

[24] The period of time that will be set in the first version of the Coin Governance System will be 100 days.

d. Use Case Example

John Doe intends to launch an ICO process to finance project XYZ by selling $10 million XYZ tokens.

John Doe decides to introduce the CGS in the ICO of XYZ in order to provide additional assurance to XYZ token buyers.

Deploying the CGS in XYZ ICO provides two advantages for John Doe: i) XYZ ICO is now more attractive to token buyers, as they may have the optionality of retrieving their funds if they are unhappy with the execution of the project, and ii) the introduction of the CGS will give XYZ ICO more visibility, as the CGS community will be incentivised to monitor the project.

XYZ´s ICO concludes successfully raising $10mn equivalent in Ether. The ether raised in the ICO will be held in the CGS smart contract, and will be released over two years since the date of the end of the ICO.

John Doe will, at any time since the end of the ICO, be able to access a certain amount of the ether held in the CGS. This amount will calculated as follows[25]:

$$\text{released ether} = (\$10\text{mn} * n) \; / \; 730$$

Where n is the number of days passed since the ICO.

As time goes by, there can be two scenarios:

i) XYZ token holders are satisfied about the evolution of the project during the CGS two years duration, and John Doe continues access the entirety of the funds raised in the ICO.

ii) XYZ token holders are unsatisfied about the evolution of the project and decide to open a claim using the Coin Governance System. XYZ token holders will need to deposit 5% of all XYZ tokens in the CGS contract to open the claim.

Once the claim is open, CGS token holders will act as an arbiter to vote whether the project is being managed properly (“OK”) or not (“KO”). If the “OK” vote wins, the ether from the ICO will continue to be released as before the claim.

If the “KO” vote wins, the XYZ token holders will be able to withdraw part of the ether raised by XYZ in the ICO. The amount XYZ token holders will be able to retrieve will be the following[26]:

[25] Note: this is an illustrative formula that represents the released ether in case there are no claims. Please refer to the code for the full formula.

[26] Note: this is an illustrative formula that represents the ether available to withdraw in case of a single claim during the life of the CGS. Please refer to the code for the full formula.

Ether available to withdraw = \$10mn * ((730 - n) / 730)

Where n is the number of days passed since the ICO.

e. Future Implementations

The Coin Governance System and CGS Token functionalities described in the current section corresponds to the initial design of the MVP. Once the MVP is tested and fully operational, there are several additional functionalities that can be built on the platform and that will be analysed, along with any other exciting ideas that may appear.

Some of these ideas are just improvements or new functionalities of the Coin Governance System as we know it. Some other ideas are entirely new product concepts that can be deployed for the use of the CGS token community. The following are a mix of both:

- **Delegated Vote**

  The concept of "Liquid Democracy" explained in section 3, whereby a voter can delegate his voting power (or remove this delegation) is absolutely compatible with the Coin Governance System in its current form. We believe the implementation of the delegated vote, could make the CGS more appealing and we look forward to implement it in the future.

- **Quadratic Vote**

  As pointed out in Section 3, this refers to the idea of a vote that increases its voting power as a function of the time that it remains unchanged. This could be applied to ICO token holders when opening claims.

- **Escrows in Fiat Currency**

  One of the criticisms that the CGS has encountered is the fact that it locks funds in Ether, meaning that the funding of the project is subject to the volatility of the price of Ether.

  We find this is a fair criticism, that is however countered by two facts: i) over time, we expect the growth and maturity of the Ethereum network will lead to higher stability in its price, ii) the reality is that the large majority of projects that have have launched an ICO are keeping the vast majority of the funds raised in cryptocurrency (therefore assuming that same risk).

  In order to limit this risk we are currently exploring the possibility of having a bank escrow account in fiat money governed by the CGS voting mechanism in partnership with a European banking group. Should this initiative prosper, this problem will be solved for good, while creating an exciting range of new possibilities for blockchain smart contracts.

- **Reputation**

  Once the CGS is tested with several ICOs, several CGS token holders would have voted through the system. Once that is done, we could build a reputation system to improve how arbitration of the ongoing of a project is being carried out.

- **Buffer**

  The buffer[27] is an option for a one-time payment, so if at any time the project has a major expense which the tap doesn't cover, they can propose a buffer vote to token holders.

- **Increase the tap**

  We will give ICO token holders the possibility to open a voting to increase the tap (Wei/second) of a certain CGS in further developments.

- **M&A for ICO Projects**

  A. Gómez de la Cruz proposed a methodology in which two projects with a token previously issued could merge, not just their legal companies, but also their circulating tokens. CGS could serve as a mechanism to do so.

[27] "Vitalik Has a New Idea for ICOs – And It's Being Tested." *CoinDesk*, 21 Feb. 2018, www.coindesk.com/vitalik-new-idea-icos-tested/.

5. Technical Overview

The CGS is developed as a decentralized application on top of the Ethereum blockchain. It uses smart contracts for the coordination of the process between the different actors and a visual interface for an easy interaction.

Smart contracts

The CGS is composed by five different types of smart contracts:

- **CGSFactory**: is responsible for creating the smart contracts needed for each project.
- **CGSToken**: ERC20 token smart contract. The token is used to vote as a decentralized judge when a claim is open by the ICO token holders.
- **CGSBinaryVote**: manages the voting process for the arbiters. There is only one CGSBinaryVote smart contract used by all projects.
- **CGS**: collects ICO tokens to open claims and manages the funds stored in the Vault. One of these contracts is deployed per project.
- **Vault**: stores the Ether collected in the ICO. It is created by the CGS. There is one Vault contract deployed per ICO.

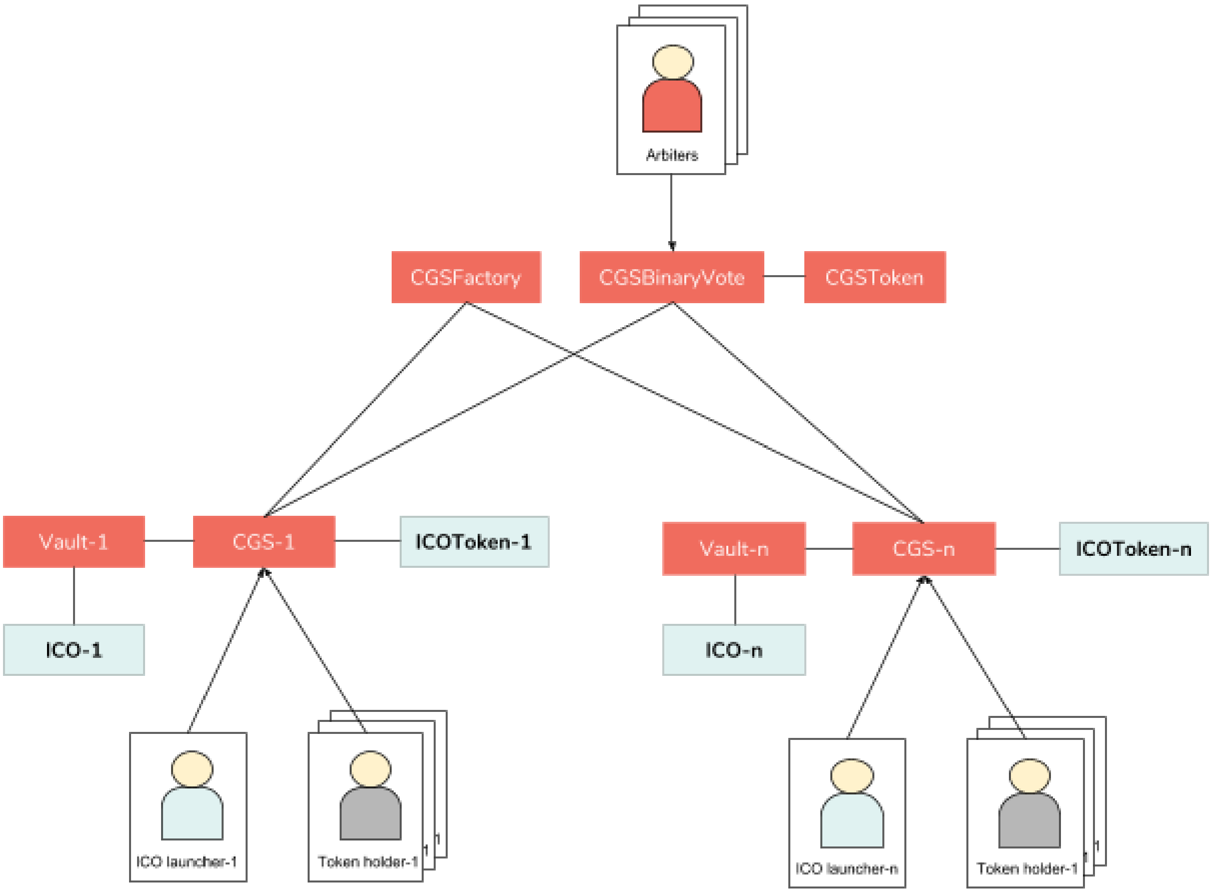


Figure 4: How the smart contracts are connected between them.

The two main contracts operating the system are CGSBinaryVote and CGS. Both manage the interactions of the arbiters and the ICO launcher and ICO token holders respectively. These smart contracts are described in more detail in the following sections.

CGSBinaryVote

This smart contract is unique and manages the voting process for all projects using a commit-reveal scheme, where each CGS token represents a vote. Anyone can start a voting process, and each one is handled separately. Each voting process has a callback address associated, that will be informed of the outcome of the vote. Once a voting process has started, the process is divided in three steps, similar to a binary SchellingCoin[28]:

- **Secret Vote**: During this phase, the arbiters deposit their tokens with a hash of their vote to ensure its confidentiality. The hash is composed by the desired vote (true or false) and a random salt composed by a "secret" in the following way:

  keccak256(vote, keccak256("Super secret random words"))

  The voters must save the secret to reveal their vote in the next step. This phase lasts for seven days and changes to the Reveal Vote phase automatically.

- **Reveal Vote**: Once the secret voting period ends, the votes must be revealed in order to settle the outcome. Only the addresses that voted during the previous phase are allowed to reveal their votes. In order to reveal the vote, the voter must provide the secret used in the previous phase. As there are only two possible values for the vote (true/false), there is no need to provide it. It will be automatically processed by the smart contract to improve the user experience.

  During this phase, no more votes are allowed, so the values of the revealed votes do not affect the decision of other voters. This phase lasts for three days and changes to the Settlement phase automatically.

- **Settlement**: With all the revealed votes, the smart contract calculates the winner option and calls the binaryVoteResult function of the callback address specified. 20% of the loser votes (CGS tokens) plus the proportional amount of CGS tokens deposited by the ICO launcher during the deployment are distributed to the addresses of the winners, proportionally. The arbiters that did not revealed their vote during the previous phase are penalized as losers.

CGS

A CGS smart contract is deployed per project. It is the most important smart contract for the system to work, as it manages the interaction with the rest of the smart contracts. It is responsible for interacting with the ICO launcher and ICO token holders. It stores the configuration provided by the ICO launcher and manages the ICO tokens, claims, redemption, ether, etc.

[28] "SchellingCoin: A Minimal-Trust Universal Data Feed" *Ethereum Blog*, 15 Jan. 2018, https://blog.ethereum.org/2014/03/28/schellingcoin-a-minimal-trust-universal-data-feed/

The configuration and deployment is done by the ICO launcher through the CGSFactory. During the deployment, the ICO launcher must deposit CGS tokens and specify the financing requirements for his project in terms of tap (wei/second) and the number of ICO tokens needed to open a claim in his project. A Vault smart contract will be automatically created for the ICO launcher to integrate it with his ICO.

In the same way as the CGSBinaryVote, the CGS smart contract has different phases that define which actions can be performed.

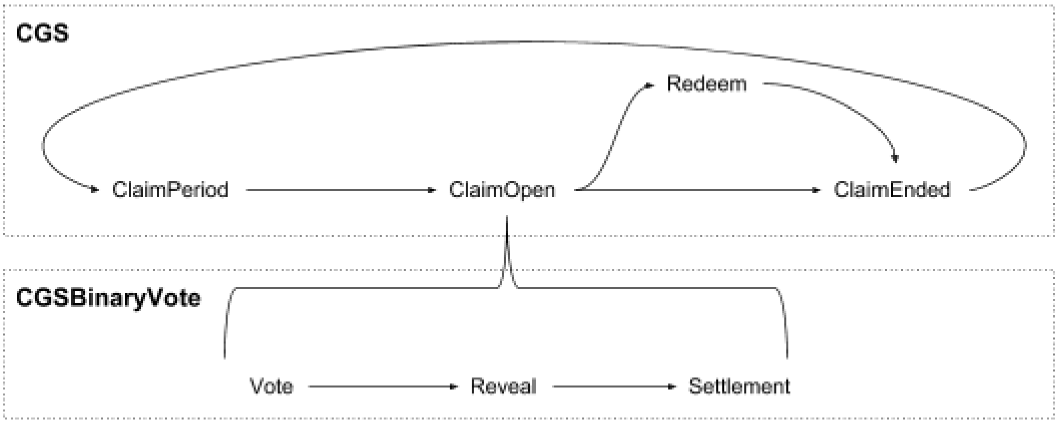


Figure 5. Phases of a CGS process.

- **ClaimPeriod**: During this phase, the ICO token holders can deposit and withdraw ICO tokens in the CGS smart contract. If at any point the number of tokens deposited is greater or equal than the number of tokens needed to open a claim, a claim will be opened and the ICO tokens deposited will be locked during the voting process.

- **ClaimOpen**: ICO token deposits and withdrawals are blocked while the arbiters resolve the claim. When the result of the voting is worked out, if the voting result agrees with the claim, the state moves to the Redeem stage. Otherwise, it moves to the ClaimEnded stage.

  The outcome of the dispute will decide the next step and if the ICO token holders that opened the claim should be penalized (in those cases where the claim is not successful). This penalization will consist in losing 1% of the ICO tokens deposited, that will be sent to the ICO launcher. Once a claim has been resolved, an ICO token holder must withdraw the ICO tokens deposited in a project before opening a new claim in the same project. This withdrawal can be carried out at any time for previous claims or during the Redeem/claimEnded phases of the current claim.

- **Redeem**: ICO token deposits are blocked. ICO token holders are allowed to exchange their ICO tokens for the ether remaining in the CGS at the beginning of the claim, proportionally. This phase will be opened for 10 days before changing to the ClaimEnded phase.

  The tokens redeemed by ICO token holders are sent to the ICO launcher with a *lock-up*. These tokens will be released once the ether balance of the Vault goes to 0. In case of an additional redemption in the future, these locked-up tokens will not be taken into account when calculating the proportional amount of ether attributable to each ICO token holder. The aim of this lock-up is to avoid the tokens redeemed through the CGS from further diluting other ICO token holders in the case of a new claim.

- **ClaimEnded**: ICO token deposits are blocked. This is a temporal stage until a new claim can be open. There must be a minimal period of 100 days between the start of two claims. After this period, the CGS contract returns to the ClaimPeriod stage.

Ether withdrawal by the ICO launcher

Absent an open claim, the ICO launcher can withdraw the ether locked in the smart contract at any moment as per the following formula:

max(etherBalance, time * weiPerSecond - weiWithdrawToDate)

Where:

- etherBalance is the remaining the remaining ether in the Vault smart contract.
- time is the seconds since the CGS started operating (usually when the ICO ends)
- weiPerSecond is the tap, the number of wei to be released per second. Specified by the ICO launcher at the beginning.
- weiWithdrawToDate is the amount of wei released so far.

If there is an open claim (between a ClaimOpen and ClaimEnded stages), the amount of ether available for the ICO launcher will be calculated as it would be at the moment just before the claim was opened.

6. Tokenomics

The CGS functionalities and the ecosystem where it will operate have been designed so that its use provides advantages for all stakeholders, and its users are incentivised to use it correctly.

Since the beginning, the idea has been to generate win-win situations for all the participants of the Coin Governance System: a) ICO Token holders, b) ICO launchers, and c) CGS Token holders. In this sense, the tokenomics of the CGS are simple.

a. Advantages for ICO token holders

The CGS token was designed to protect the interests of ICO token holders, and ensure that they remain aligned with those of the ICO launcher, helping to solve the classic problem of Agency Costs in ICO projects. This will provide a significant technological protection to investors in ICOs that have implemented the CGS versus other ICOs that do not.

Consequently, the ICO token holder community will award significant value to the functionality provided by the CGS: the option for ICO token holders to withdraw the funds contributed if the project is not managed suitably.

In this sense, we expect the ICO token holder community to become a prescriber of the CGS, requesting ICOs to deploy it, as a condition for contributing to the ICO.

b. Advantages for the ICO launcher

The value of incorporating the CGS to an ICO derives directly from the previous header. The fact that the CGS will align the interests of ICO launchers and ICO token holders, will make the ICO significantly more attractive for investors. This significantly more attractive ICO proposition will increase the chance of success of the ICO launcher.

Additionally, we expect investors who have the protection of the CGS to be more comfortable contributing to ICO projects that are very ambitious as to fundraising or may even seem overfunded.

The implementation of the CGS has another beneficial effect for the ICO ecosystem in that it will help to stabilise the valuations of traded ICO tokens. Traded ICO tokens have been extremely volatile to date, often due to low liquidity, market manipulation and other unknown factors. As the CGS provides the possibility of recovering the Ether raised by an ICO, it should mean that the market valuation of the tokens will be indirectly supported by the amount of ether that remains locked in the CGS. Consequently, this should provide a floor valuation linked to the value of Ether, which should tend to be more stable, as Ether has much higher liquidity and market valuation than any ICO.

Consequently, we would expect ICO launchers to be increasingly interested in implementing the CGS as part of their ICO value proposition.

c. Advantages for the CGS token holders

The functionalities of the CGS have been designed to achieve two objectives: i) Incentivise CGS token holders to vote "correctly" and ii) foster an increasing community of CGS users.

- Incentive to vote "right"

  The voting system is designed as described in section 4 of this White Paper. In summary, at the end of the voting of a dispute, the system rewards users who have voted "correctly" with more CGS tokens, and punishes users who voted "incorrectly" taking away CGS tokens. This simple mechanism should ensure users try to vote "correctly" to the best of their capacity.

- Foster an increasing CGS user community

  The CGS will be a decentralised application based on a community and as such it will enjoy network economies. The CGS will be increasingly more useful as there are more ICOs that have implemented the CGS.

  We expect the fundamental utility value of the CGS token to be driven by two main factors. On the one hand, it will be driven by the cumulative amount of Ether on escrow in all the CGS smart contracts, given the indirect power the CGS will have over these funds. On the other hand, the number of open claims will also drive the utility value of the token, as open claims will tend to dynamise their demand.

  The above incentives will lead CGS token holders to both encourage new CGS users, and to request ICOs to implement the CGS.

7. Road map (2018)

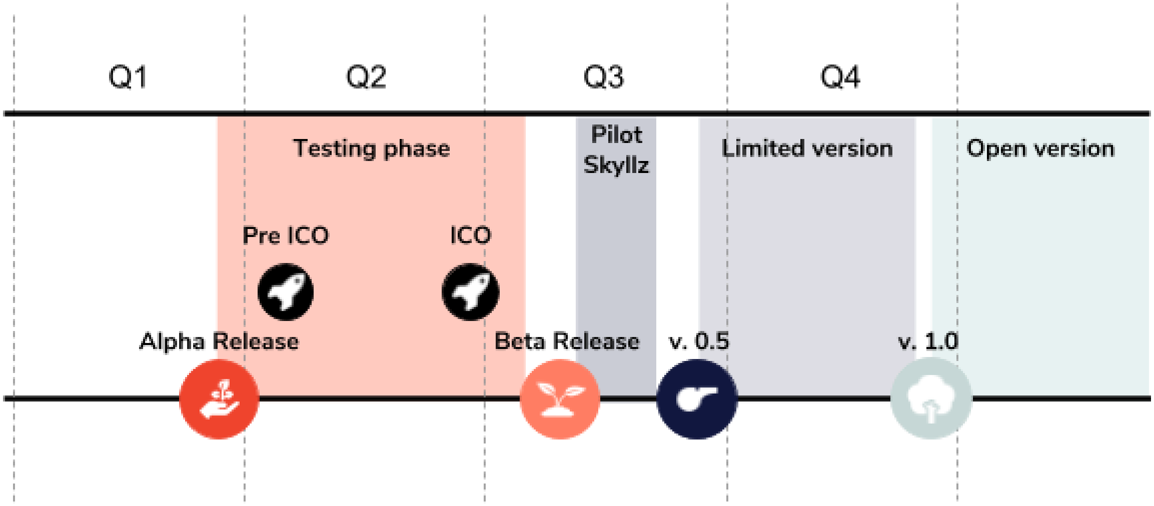


Figure 9: Roadmap

a. **Alpha Release**: the publication of the first working version of the CGS platform, which users will be able to interact with it.

b. **Testing Phase**: following the alpha release, a version of the platform will be open for the early adopters on Testnet. During the testing phase, users will receive testnet tokens to try the product and give feedback. Testers and users that help improve the platform will be incentivised with mainnet CGS tokens.

c. **Pre ICO**: a private token sale will take place prior the public one for a limited amount of participants.

d. **ICO**: an public token sale will take place towards the end of Q2 2018.

e. **V0.1 Beta Release:** this milestone marks the publication of the first working version of the CGS platform on the Ethereum Mainnet**.**

f. **Pilot - Skyllz**: the Skyllz platform is the first real life ICO project that will integrate the CGS. Investors will enjoy the protection of the CGS for the first time in live ICO.

g. **V0.5 - Limited Version**: more projects will be included in the CGS. The projects will be manually added after a prior review to avoid spam and monitor the proper functioning of the platform.

h. **V1.0 - Open version**: the CGS platform will be open for any ICO. The governance of the system will be delegated to the CGS community, that will decide through votings the certain parameters of the platform, such as number of tokens needed to create a project, etc.

8. Team

The Coin Governance System is the flagship project of the Icofunding Team. Icofunding is one of the pioneering ICO facilitators in Europe and has been involved in the advisory and execution of ICOs since 2016. The team is well balanced and made up of exceptional professionals with a strong background in blockchain and cryptocurrencies.

Alejandro Gómez de la Cruz, Cofounder and CEO
Alejandro is a lawyer specialised in blockchain technology who formerly managed the Grant Thornton Blockchain Lab, he is the founder of Octopocket and also worked as a lawyer at Allen & Overy and KPMG.

Adrián Calvo, Cofounder and CTO
Adrián is a software engineer specialised in Blockchain, who has been working on Ethereum since 2014. Before Icofunding, he worked as the lead developer at Grant Thornton Blockchain Lab and as an editor at CryptoCoinNews.

Pablo Moreno de la Cova, Cofounder and COO
Pablo is specialised in M&A, financial markets and cryptocurrencies. He formerly worked as VP at Highbridge European Equities, as a Director at Corpfin Capital and as an Analyst at Lehman Brothers.

Carlos Kuchkovsky, Cofounder and Chairman
Carlos is the CTO of New Digital Business at BBVA, leading the membership at the Ethereum Enterprise Alliance and Board Member at Hyperledger.

Anne-Lous van den Ende, CMO
Anne-Lous is a Marketing Strategist specialised in ICOs. She founded ICOMarketing and previously worked for marketing agencies such as McCann Worldgroup.

Fernando Alamillo, Business Development
Fernando is an industrial engineer and entrepreneur who has been involved in startups for 10 years and founded Kainve and Fintech Spain. Before joining Icofunding he worked at Opinno developing tech projects.

Carlos Mora, Software Architect
Carlos is a Software Engineer with more than ten years of experience in software development. He is an enthusiast of mobile development and cloud computing.

Esperanza Arquero, Visual Designer
Esperanza is a visual and web designer with almost ten years of experience in graphic design. She previously worked for communication and events agencies.