FIN4Xplorer

Release 0.0.1

Jun 17, 2020

Contents

Welcome to the documentation of the FIN4Xplorer plattform.

The latest live version can be found at demo.finfour.net and more general information are available at finfour.net.

The basic idea is: anyone can create tokens and anyone can claim these tokens. Once a claim is made, the user has to provide proof that the associated positive action actually happened. Which proof or proofs these are, is decided by the token creator when designing the token. If all proofs on a claim are automatically (e.g. a location to be within a certain circle) or manually (e.g. someone involved in the action is asked to approve a photo) approved, the claimer gets an amount "minted" on that token. We say someone "gets tokens", which basically means that that persons public address gets an entry in the balance-sheet on the respective token with a positive number.

Getting started

1.1 Technical infrastructure

FIN4Xplorer consists of two parts:

- Smart contracts that are deployed to the Ethereum blockchain. The entire functionality is in these smart contracts. Everything could also be done by interacting with them via a command line.

- A frontend or client in the form of a *Web DApp* that acts as an user interface for convenient interaction with said smart contracts. Web apps run directly in the browser, both on desktop computers and on smartphones. DApp stands for distributed app, meaning they connect to a blockchain.

1.1.1 Infrastructure, programming languages and frameworks used

We decided to use the Ethereum blockchain for now. It satisfies our requirements of an open-source and public blockchain that supports smart contracts. Furthermore it is used widely these days and therefore plenty support resources are available.

The smart contracts are written in Solidity and we deploy them via truffle to the Rinkeby test network.

Rinkeby is one of a few Ethereum test networks and behaves similar to the main network. The difference is, that Ether, the "currency" used to pay for transactions, is not worth "real" money. On the main network Ether has to be earned via mining or bought on trading plattforms. On Rinkeby it can be requested from "faucets" for free, see section *Getting Ether*.

During development we use Ganache from truffle locally to simulate an Ethereum blockchain.

For storing media files that certain proof types require, we use IPFS via the Infura gateway.

As digital wallet to connect desktop or mobile browsers to the Ethereum network we use MetaMask, more about that in the following section *Digital Wallet*.

The frontend is a React app that uses drizzle from truffle to connect to the smart contracts on the Ethereum blockchain. For now we don't have native mobile apps. Mobile users have to use DApp browser apps and navigate to the same site as desktop users. The layout of the fronted works well on different screen sizes as relatively narrow boxes are

arranged per page. Depending on the width of the browser window, they will either be rendered next to each other or below one another.

1.2 Digital Wallet

The only, yet significant, difference a visitor of a Web DApp experiences compared to a Web App, is the need for a "bridge to the blockchain". Also called a digital wallet. Its first task is to establish the connection to the blockchain network - either via a full node that users run themselves or via a gateway service like Infura. Its second task is to pop up whenever the user seeks to write data to the blockchain and enable the convenient signing of such transactions with the users private key.

There are many organizations and projects out there offering digital wallets in different stages of maturity and compatibility. While the trend goes towards deeper and native integration into browser (or even operation systems), for now the market appears scattered.

The digital wallet we are using ourselves, and that seems to be the currently best supported one out there, is MetaMask: metamask.io. MetaMask is available both as extension for desktop browsers (Chrome, Firefox, Opera and Brave) and as early-stage mobile app (iOS and Android).

Once you have a digital wallet, either restore an existing account or follow the process to create a new account. In most digital wallets, creating a new account involves the randomized mathematical creation of a new and unique mnemonic (also called "seed phrase"). From this, one or more accounts, each with a public address and a matching private key, can be derived deterministically. Meaning you only have to remember/store (the digital wallet will probably remind you thoroughly to do so) the mnemonic to restore your account(s) anytime on any machine. Usually only the first account per mnemonic will be used.

After having created your new account, don't forget to switch to the *Rinkeby Test Network*. By default you will be on the *Main Ethereum Network*.

1.3 Getting Ether

After installing a digital wallet and creating an account, the last step before being ready to use FIN4Xplorer is to get some Rinkeby Ether (ETH). All transactions on the Ethereum (test) network cost Ether, the so called gas fee. The price depends on the current workload of the network as well as how many additions/changes to data on smart contracts your transaction causes. On test networks, Ether can be obtained for free from "faucets". On the main network, Ether has either to be earned by being an active participant in the network (running a full node and doing mining), has to be traded or has to be bought on exchanges.

For obtaining Ether on the Rinkeby test network we suggest two options:

- Using the "authenticated faucet" at faucet.rinkeby.io requires a social media post

- We build our own little faucet server that gives a small amount of ETH per click if the user has less then a threshold value: click *Request Ether* on the landing page of demo.finfour.net and wait a little until you get a confirmation message.

Application overview

2.1 Home

Home acts as landing page and is the central place of the DApp.
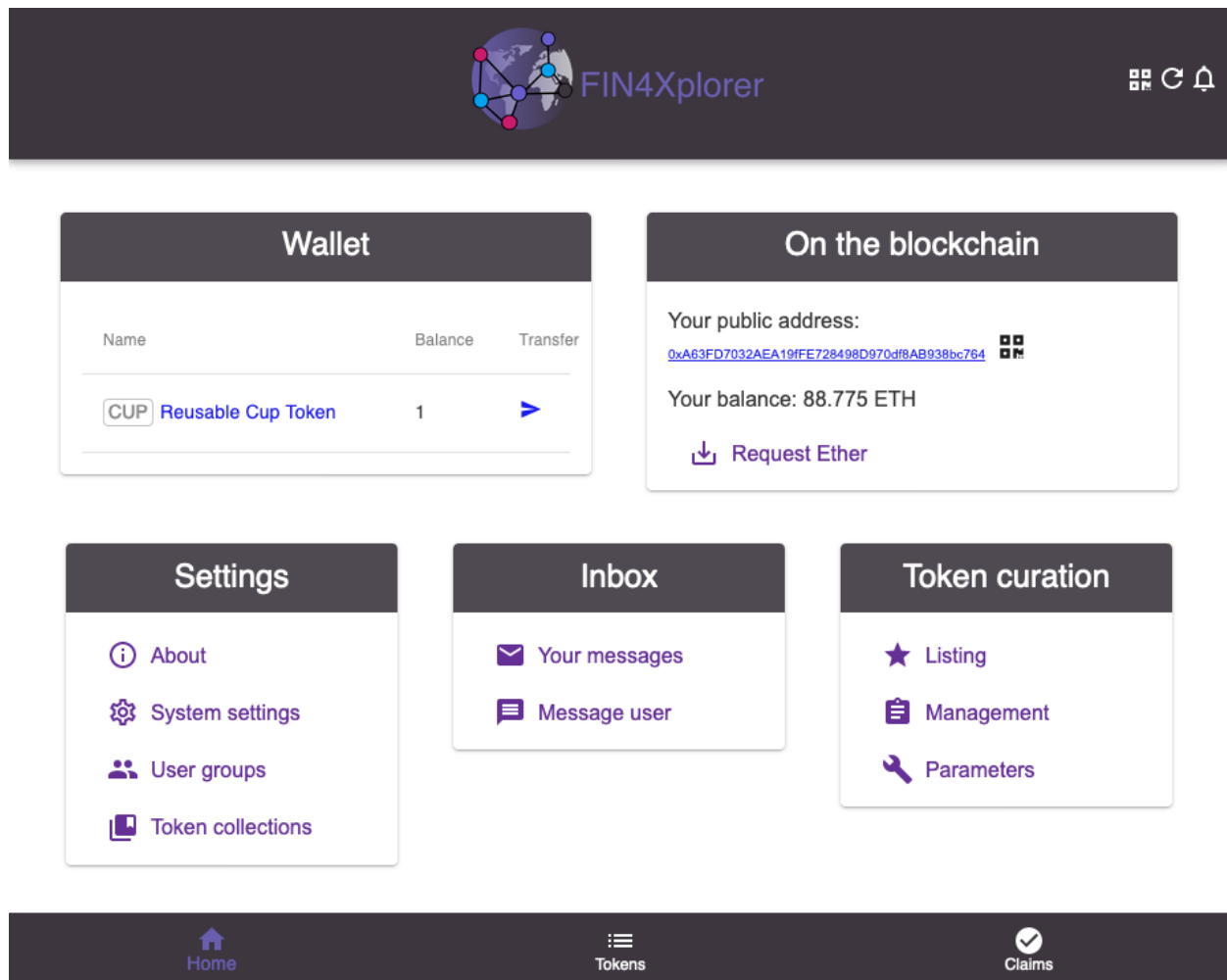
The two main subsites are accessible in the bottom bar: *Tokens* and *Claims*.

The three icons in the top bar are for showing the users QR code, reloading the page and for getting notified about new messages.

The various boxes shown are explained in the chapter More functionalities.

2.2 Tokens

Under *Tokens* new tokens can be created as described in Create tokens. On the right side all existing tokens are listed with direct links to claiming them or to view more details about them.

Clicking on *View* on a Token brings up a dedicated site showing details about the design and some performance statistics of the token.

2.3 Claims

The layout of the *Claims* site is analog to the *Tokens* site: submitting new claims can be done on the left side and a list of previous claims is displayed on the right side. If users get to this site via a *Claim*-Link on a token directly, the

Token Type will be prefilled. More info about the claiming process can be found in Claim tokens.
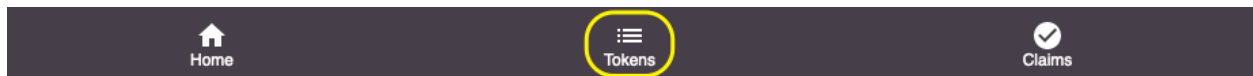
Create tokens

The ability for anyone to create new tokens on the FIN4Xplorer plattform is at the heart of its concept. Once a token is created, it can be claimed by anyone. A successful claim results in having a balance on the respective token. Since we base our token contracts on the ERC-20 standard this balance will show up on any Ethereum digital wallet app that supports the ERC-20 standard. Note that also in such apps you have to switch to the Rinkeby testnet.

3.1 Token creation wizard
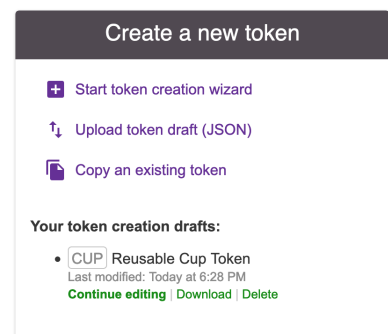
The effort put into creating a token can range from a quick 1-min-clicktrough to a lengthy eloborate planning in a multi-disciplinary team. The possible entry points for the token creation process are:

- Creating a new token from scratch

- Uploading a token draft in JSON format

- Copying an existing token design as template

The last two will import a token creation draft showing up at the bottom of the box. The first option will take you directly into the token creation wizard. It consists of 5 steps: *Identity*, *Design*, *Actions*, *Minting* and *Proving*. In each step, an info box can be opened that provides explanations.
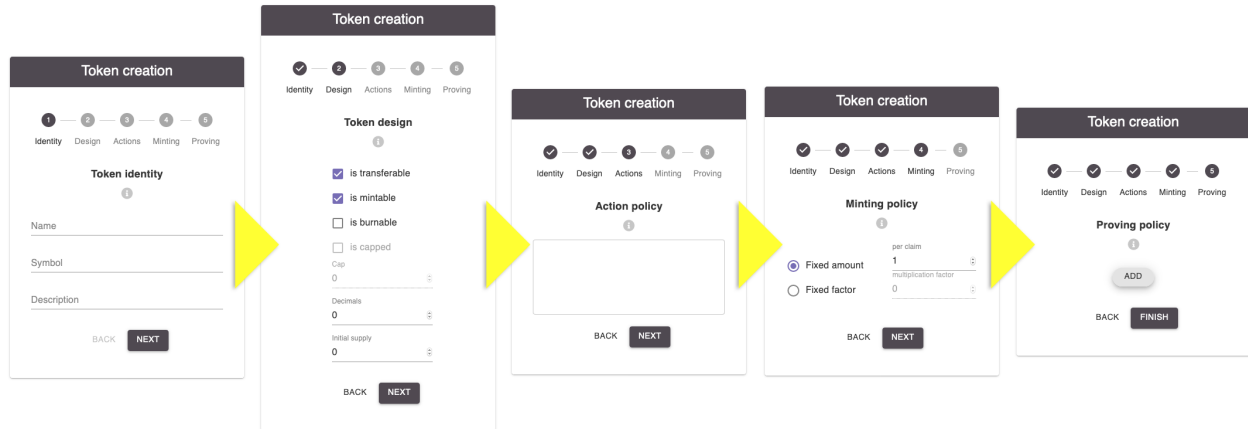

Note that at any point you can leave the wizard and your progess will be stored as draft. Drafts can be used to resume the process later on or to download, share and import them.

Once the 5 steps are completed, the token can be created on the blockchain. One ore more transactions have to be confirmed for that. One for the token-creation itself and one for each proof that has parameters. Until all proof-parameterization transactions are confirmed, the token will remain in a disabled state.

Claim tokens

| Home	Tokens	Claims
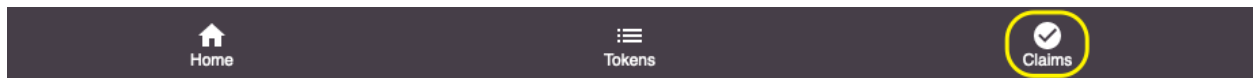
Tokens that have been created as outlined in Create tokens, can be claimed.

Claim Tokens

Token Type
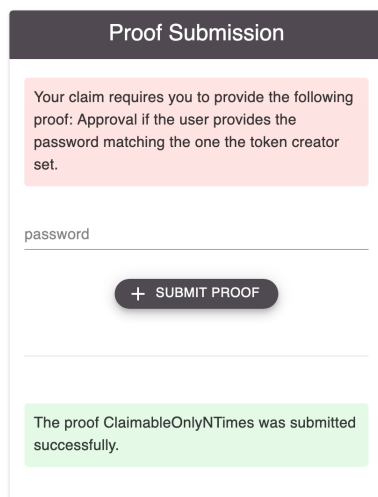CUP Reusable Cup Token

Comment

+ SUBMIT

Submitting a claim is the first step to obtaining a balance on the token in question. Once made, it shows up under *My previous claims*. Claims there can be in one of three stages:

- In red with a prompt to *Submit proof*, this is the default after submitting a new claim

- In green, the approved state, which also means that a balance has to be minted to the claimer

- In gray, the rejected state, if one or more of the proofs got manually or automatically rejected

My previous claims

Reusable Cup Token   1 CUP
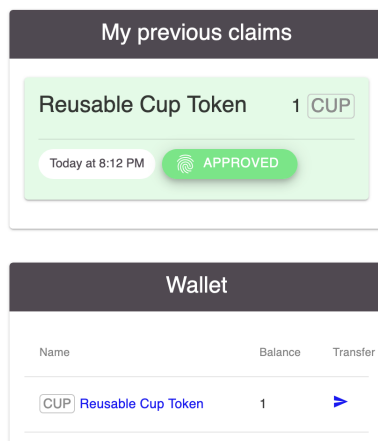
Today at 8:06 PM   SUBMIT PROOF
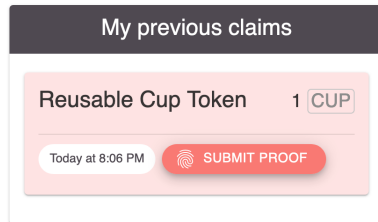
4.1 Proving

For a claim to be successful, all the proofs specified by the token creator have to be provided and get approved - automatically or by the chosen person, group or sensor. A proof submission site might look like this.

Proof Submission

Your claim requires you to provide the following proof: Approval if the user provides the password matching the one the token creator set.

password

\+ SUBMIT PROOF

The proof ClaimableOnlyNTimes was submitted successfully.

Here, a proof is shown (*ClaimableOnlyNTimes*) that didn't have to be initated manually. It belongs to the category of proofs that automatically give their approval or rejection once a claim is made.

Once all proofs are provided and approved, the claim appears as green and the claimer gets a balance on this token.

My previous claims

Reusable Cup Token   1 CUP

Today at 8:12 PM   APPROVED

Wallet

Name	Balance	Transfer
CUP Reusable Cup Token	1	➤

Once any proof of a claim is rejected, the entire claim gets rejected. It is not possible to recover this claim by resubmitting proofs - a new claim has to be made if the user wants to try again.

More functionalities

All the functionalities presented below are accessible via the Home site.

5.1 Wallet

The wallet box shows the users balance on all tokens with approved claims. The token name links to its respective detailed site (TODO ref).

The transfer icon links to a site allowing the *transfer* of balances on transferable tokens to other users.

5.1.1 Transfer Tokens

Note that once a transfer has been made, there is no way to undo it from the senders site. Only the recipient could choose to send it back.

5.2 Settings

Settings contains Links to the *About* and *System settings* sites. The latter contains the language preference and a list of relevant smart contract addresses.

Furthermore, *User groups* and *Token collections* can be found there.

5.2.1 User Groups

User groups can be used for two purposes. Firstly to define "administrators" of a *token collection* who can add or remove tokens from a collection. Secondly, certain proof types can notify members of a user group about a pending approval that one of them should approve or reject.

Under *My groups* users can message the owner (unless they are the owner) and leave groups (also possible for owners). Upon leaving a group, users can choose to notify the group owner about it or not.

Editing a group as owner comprises the options to add or remove members and to transfer ownership of the group.

5.2.2 Token collections

Token collections are a way to curate a list of tokens with a much lower effort then the *token curated registry*.

They can be used for organisations to promote their tokens in one place, for individuals to create portfolios or other use cases.

The collection creator can add or remove tokens from the collection, appoint an admin group to do the same or transfer ownership of the collection.
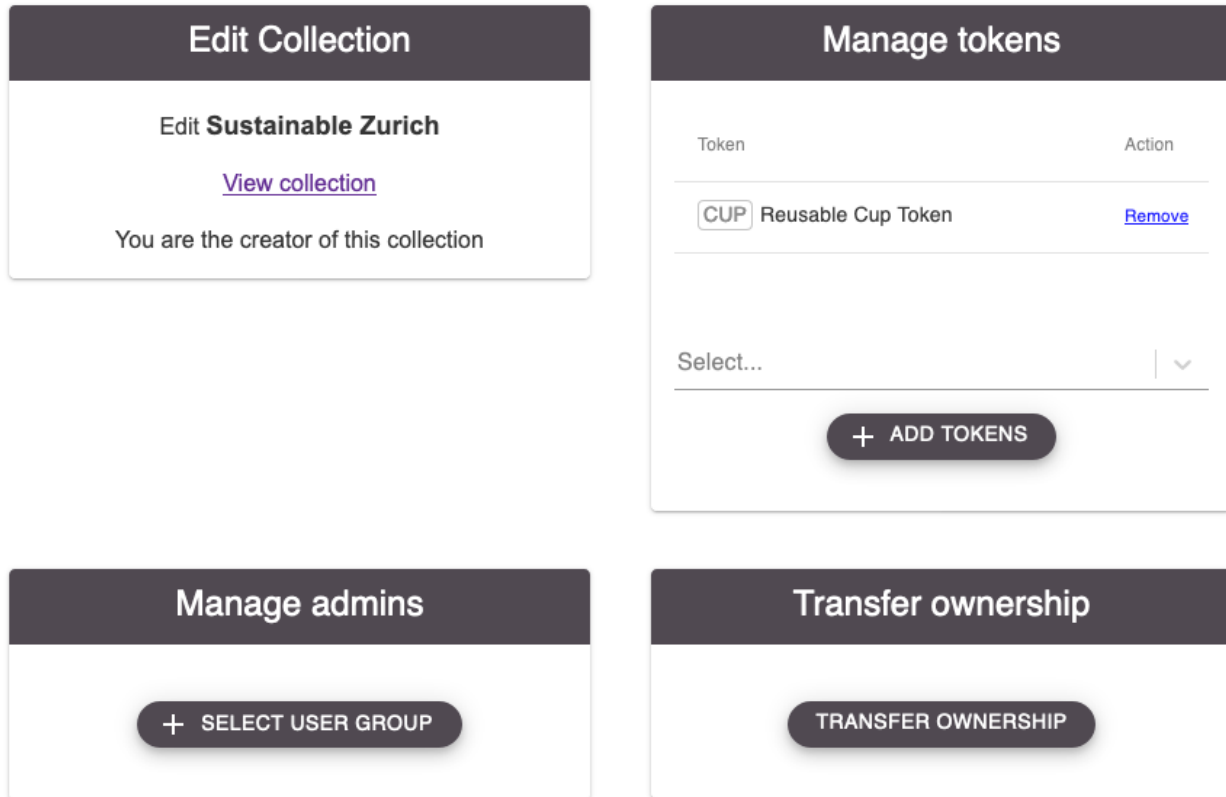
5.3 Inbox
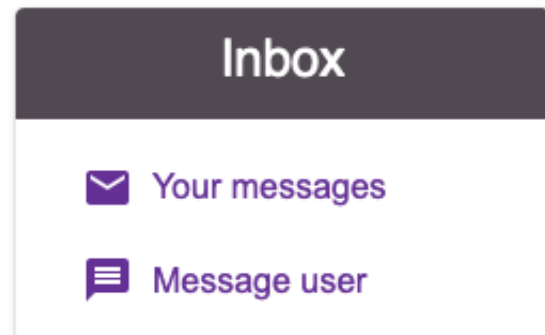
Your messages shows all messages sent to you. These can be

- Proof contracts notifying you about pending approvals: for you directly or a group you are a member of
- Reasons why a proof you submitted got rejected
- System notifications like a user leaving a group you created
- Messages from other users

If you get a new message while being on the DApp, the notification bell in the top right corner of the site will turn yellow and take you to the messages site upon clicking.

Message user takes you to the option to message other users directly. The QR icon can be used to scan the public address of the recipient instead of having to type or paste it in.

5.4 Token curation

Token curation takes you to the Token Curated Registry (TCR). Here, anyone with enough *Governance Tokens* (GOV) can participate in curating a list of "official positive action tokens" (OPAT). Users can propose tokens to be voted into the listing as well as challenge them once they are in it.

5.4.1 Listing

Listing is the central place of the TCR, here, the curation of OPATs is happening. After applying a token to the listing that is not already on it, a voting period starts where users can vote for taking it in or not. Only in the reveal period where votes can't be changed anymore it will become public what users voted for, not before. Depending on the quorum parameter as can be seen under *Parameters* the majority of votes decide what happens. If a token makes it onto the listing, it can be challenged. This triggers another vote/reveal procedure which results in kicking the token off the listing or keeping it. The proposer or challenger has to put GOV on stake and gets rewarded if the vote turns out in their favor or looses GOV if it does not.

To participate in these procedures, a user must have sufficient GOV. This can be claimed under *Management* from *Reputation Tokens* (REP) beyond a certain threshold.

Curated Positive Action Tokens				
Name	Status	Due Date	Actions	Whitelisted
Reusable Cup Token	-		CHALLENGE	true

Reload to see changes, statuses won't change automatically.
TODO explain costs involved for making changes and potential rewards/losses.

All Positive Action Tokens	
Name	Apply
Reusable Cup Token	
Tree Token Zurich	APPLY
Bike to ETH Token	APPLY

Tokens on the listing will be displayed with a star icon in the list of all tokens.

All tokens		
Name	Supply	Actions
CUP Reusable Cup Token ⭐	0	View Edit Claim
TTZ Tree Token Zurich	0	View Edit Claim
BIKE Bike to ETH Token	0	View Edit Claim

5.4.2 Management

Here, users can claim GOV from REP if they are above a certain threshold. This claiming can be repeated once the user spends GOV and falls below the amount they have as REP.

The other functionality here is to delegate some of your GOV to a user of your choosing and see how much GOV in total was delegated to you, if any. The idea being that an user might trust another user to participate in governance procedures on their behalf because they are for instance more competent in a certain topic. Unlike all other token transfers, this amount can be refunded from the sender.

Governance Token Balances				Delegation	
Token	Balance	Actions		Type	Amount
Reputation Token	150	CLAIM GOV		GOV tokens delegated to me	0
Governance Token	0			DELEGATE	
				REFUND DELEGATION	

5.4.3 Parameters

Similar to collectively deciding if a token should be on the listing or not, the parameters of the system as a whole can be changed collectively. The procedure is similar and involves proposing a new value for a parameter, followed by vote and reveal phase after which the new value is accepted or rejected. The GOV required to put on stake for a proposed reparameterization are much higher then those for proposing a token. The idea being that reparameterizations should happen very rarely and only if a proposer is "serious" about it.

TCR Parameters

Reload to see changes, statuses won't change automatically.
TODO explain costs involved for making changes and potential rewards/losses.

Parameter	Description	Value	Actions	Status	Due Date
minDeposit	minimum deposit for listing to be whitelisted	100	PROPOSE	-	
pMinDeposit	minimum deposit to propose a reparameterization	100000	PROPOSE	-	
applyStageLen	period over which applicants wait to be whitelisted	120	PROPOSE	-	