ROOTSTOCK COLLECTIVE

WHITEPAPER

Version 1.0

12th September 2024

ABSTRACT

This paper introduces the structure of RootstockCollective, a Decentralized Autonomous Organization (DAO) that will serve as a platform for community-driven stewardship and growth of the Rootstock ecosystem. The paper lays out an overview of the token-based governance system under which the DAO will operate, introducing the governance token and voting mechanism. From day one, the DAO will decentralize the allocation of grants to builders to foster the development of innovative applications and use cases on the Rootstock blockchain. Additional functionalities will then be incorporated over time as guided by the community and implemented through on-chain governance.

INTRODUCTION

RootstockCollective, or The Collective, is a DAO (Decentralized Autonomous Organization) designed to develop the Rootstock ecosystem by empowering and rewarding builders and users of Rootstock, and RIF token holders. As a merged-mined Bitcoin sidechain, Rootstock's heartbeat is inextricably linked to Bitcoin. With blocks separated by seconds, instead of minutes, the Rootstock network 'beats' a lot faster, and serves as a scaling solution for Bitcoin. On Rootstock, developers are able to build rich, EVM-compatible, web3 apps – and they can do this using Bitcoin as the native currency, in the form of RBTC.

RootstockCollective was formed to address a critical challenge faced by Bitcoin builders; value capture. Historically only Bitcoin miners and holders benefited from the Rootstock network's growth. This changes today with the introduction of the RootstockCollective.

By using the RIF token for governance, RootstockCollective puts builders, RIF token holders and community members at the heart of Bitcoin's evolution, giving them a voice through decentralized governance over a community-led Treasury. The RootstockCollective Treasury will be organised into purpose-aligned sub-Treasuries – Grants, Growth, and General – ensuring targeted support and sustainable development. By moving towards decentralized governance, the creation of the RootstockCollective will encourage community members to continue developing, promoting, and using Rootstock and RIF tokens.

The initial implementation of RootstockCollective will be a hybrid of centralized and decentralized components with a path toward maximal decentralization in the future. This is to allow for appropriate guardrails to be established whilst allowing community interaction for early adopters.

RootstockCollective is more than a response to community needs; it is an exciting step towards a decentralized future where Bitcoin works for everyone. RootstockCollective is on a mission to bring Bitcoin to the next billion by ensuring builders are rewarded and championed for their work. Welcome to the future of Bitcoin. Welcome to RootstockCollective.

---

[1] Prepared by the RootstockCollective Foundation. As the RootstockCollective DAO evolves and matures, this paper will be updated to reflect changes in its scope and functioning.

ROOTSTOCKCOLLECTIVE FOUNDATION

The RootstockCollective Foundation is registered in the Cayman Islands as a Foundation Company whose purpose is to support the operation and administration of DAOs within the Rootstock ecosystem. The Foundation is self-governed by a board of directors. The Foundation is not permitted to undertake any activities of a virtual assets service provider, including without limitation, custodial, token sale, or crypto exchange services.

The RootstockCollective Foundation will facilitate the transition towards community-driven decision-making for the Rootstock ecosystem. The Foundation's role is to make this process transparent and credible, which will encourage community members to engage with and take ownership of the future of the Rootstock ecosystem.

The Foundation will help bootstrap the initial version of the DAO by assisting with off-chain tasks. These can include responsibilities such as maintaining software repositories, computing infrastructure, websites, acquiring domain names, and managing social media accounts. In the initial phase of the DAO, the Foundation will direct the deployment of the initial software required for the DAO to go live as a decentralized application.

The Foundation will also help manage the initial seed funds intended for the DAO's treasury operations such as grant allocations, or expenses related to software development, deployments, security audits, and security bounties. The Foundation can also help meet regulatory requirements, if necessary.

For many of the above responsibilities, the Foundation will need to engage with contractors, service providers, organizations, and enterprises on behalf of the ecosystem.

The Foundation will also serve as a guardian of the DAO's assets. For example, consider a malicious proposal attempting to withdraw funds fraudulently from the DAO's grants program. If the proposal is flagged by the community as fraudulent, then the Foundation can intervene to block it in two ways. If the malicious proposal is identified before on-chain voting has concluded, then the Foundation can cancel (terminate) the voting process for that proposal. If the malicious proposal is not detected on time and the vote succeeds – then it is still possible to avoid the loss of funds. This is because all successful proposals are added to an execution queue – where they must wait for a predetermined amount of time before they can be executed. The Foundation can take emergency action to remove malicious proposals from this queue.

The DAO's smart contracts will reflect such special powers in a transparent manner. All of the code for the DAO will be open source. In any case, deployed smart contract code is always public on the blockchain. The code can be examined by community members and third parties to verify the exact nature of special powers granted to the Foundation. As mentioned above, for security, all funds managed by the Foundation will be controlled by multisig wallet contracts. The Rootstock blockchain will have a record of all on-chain actions taken by Foundation officials.

Over time, the Foundation will play a less active role. As the community progressively assumes more control, the Foundation will step back. The DAO's smart contracts will be updated to reflect the increased responsibilities assumed by the community. However, given the nature and scope of the Foundation's activities, it may be difficult (or impossible) for the community to assume all responsibilities – and there may be a continuing need to rely on the Foundation. In the long term, the community can experiment with different organizational structures to receive assistance on tasks that cannot be fully decentralized.

GOVERNANCE SYSTEM

RootstockCollective will use a state-of-the-art, token-based, governance system with off-chain and on-chain components. For this purpose, a new ERC20 token, with voting-related smart contracting features, will be deployed on the Rootstock network.

Governance Token

To align governance rights with the existing ecosystem, the new token will be created as a wrapper around the RIF Token. A "wrapper" implies a direct dependency of the new token on the RIF token. Specifically, the new token can only be minted by locking RIF tokens to a governance system contract. This governance token is called stRIF, where the "st" stands for 'Staked'.

It is the norm for DAOs to launch with a new governance token. However, it is unusual for the new governance tokens to have links with any pre-existing tokens. Therefore, the decision to tie governance power in RootstockCollective with the RIF token merits some justification.

Unlike most DAOs, the RootstockCollective is not tied to any specific application. Rather, it is intended to serve as a decentralized decision-making platform and to capture value within an existing ecosystem. RIF is a core part of this ecosystem. Recall that RIF is a utility token that currently powers protocols such as RifOnChain (USDRIF stablecoin) and RIF Name Service (RNS). Another reason to link the governance of RootstockCollective with RIF is the economic sustainability of the DAO. As mentioned in the RIF Whitepaper, RootstockLabs is entitled to receive a share of the transaction fees generated by the Rootstock blockchain. To support this new role for RIF in community-led stewardship of the Rootstock ecosystem, the community can decide to redirect RootstockLab's share of fees to the DAO instead.

Additionally, by tying the governance token to RIF, RootstockCollective can easily integrate and onboard the governance of other RIF protocols in the future, such as the RIF Name Service and the RifOnChain protocols. This will allow the DAO to diversify its revenue stream, while also fostering well-established Rootstock protocols using RIF at the center.

With a new governance use case, RIF will gain additional utility. However, actual voting power will reside in stRIF. Community members can stake (i.e. lock) any amount of RIF tokens and receive an equivalent amount of stRIF tokens (in a 1:1 ratio). To keep this conversion precise, stRIF is issued using the same precision as RIF (i.e. 18 decimal points). Stakers can reclaim their underlying RIF tokens at any time through an unstaking process by returning stRIF tokens to the governance system. The returned stRIF tokens are burnt as part of the unstaking process. Therefore, each stRIF token in existence is always backed 1:1 by an underlying RIF token staked on the governance system.

PROPOSALS AND VOTING

Voting Power

In modern DAOs, ownership of the governance token endows a holder with the right to either vote by themselves, or to nominate someone else (called a delegate) to vote on their behalf. In the beginning, stakers in RootstockCollective are expected to vote directly. The initial version of the DAO will facilitate this by automatically assigning stRIF holders to be their own delegates (self-delegation) at the time of minting. Later, stRIF holders can delegate their voting power to third parties.

In terms of voting power, the DAO will adopt the rule of assigning one vote to each stRIF token. This approach is followed by several well-established DAOs, such as Compound, AAVE, and Uniswap.

Following best practices from the state of the art, a user's voting power is not derived from their current stRIF balance at the time of voting. Instead, when voting on a proposal, a staker's voting power is derived from the amount of stRIF they held before that proposal was created. This historical balance is derived from a reference block number, which is called a snapshot. The practical significance is that this allows the community to limit strategic behavior such as someone rapidly accumulating a large number of governance tokens just before an important vote is decided. Using historical (rather than current) balances for voting power also eliminates double voting – otherwise a voter could transfer governance tokens to a fresh address to vote again.

By default, RootstockCollective will use balances from a "snapshot block" just prior to when a proposal goes live. In the future, if deemed necessary, the community can modify the system such that each proposal can specify its own reference block to use as a snapshot.

Types of Proposals

In the initial stages, voting may be limited to just a few classes of proposals. The first is related to grants targeted to expand the Rootstock ecosystem. These proposals can be used to decide whether, and how much, to award to a particular builder or project.

There can also be proposals related to managing the DAO's treasury. At various points in time, the DAO will have a variety of assets in its treasury, such as RBTC and RIF. When there are multiple assets, the community can use voting to manage this portfolio, and set separate grant budgets for each asset.

The other class of proposals are those that can be used to perform updates to the governance system itself. This can include proposals to reset system parameters, such as quorum requirements, or security timelocks used to delay when major changes to system parameters or voting outcomes become effective. The community can also introduce guardians or a security council (a common practice in DAOs) with the ability to take some emergency action. Voting can be used to update the list of members with such privileged roles.

Proposal Lifecycle

On-chain voting always requires a fair amount of prior preparation that happens off-chain. The initial step is for a community member to introduce a proposal to the rest of the community. These are sometimes called improvement proposals. In the context of DAOs, the norm is to introduce proposals in a specific community discussion forum. The RootstockCollective Foundation will support the creation and management of a discussion forum for use by members of the RootstockCollective DAO.

Preliminary versions of proposals are often informal descriptions of ideas intended to inform and initiate conversation. Once proposals are initiated, they are expected to go through a process of deliberation, during which they continue to evolve and add more structure. In most communities, it is quite common for some proposals to not receive any attention and they stagnate. Only a few proposals generate sustained interest, and just a few of those ultimately develop into a mature proposal.

Once a proposal is mature and ready for on-chain voting, it has to be submitted formally to the DAO's governance system. This requires sending an on-chain transaction to call a specific function in a governance-system smart contract. The RootstockCollective Foundation will support the creation of user-friendly interfaces and dApps to make it easy for community members to participate in governance. The ability to introduce and vote on proposals will be one of the basic functionalities of such a dApp. Since the code for these applications will be open source, technically advanced users will be able to run the voting front-end dApp themselves instead of using the front-end service supported by the Foundation.

To prevent spam proposals, RootstockCollective will require anyone creating a proposal to have a balance of stRIF that exceeds some minimum threshold. This threshold will be one of several configurable parameters of the governance system. For example, the threshold can be a fraction (e.g. 0.1%) of the current total supply of stRIF, or it can be a fixed amount of stRIF (e.g. 1000 stRIF). Once created through the governance system, each proposal is assigned a unique ID. The ID is usually automatically created by the smart contracts using secure hash functions. This ID is separate from any other numbering that may be used for reference in the forum e.g. an improvement proposal numbering system.

The submission of a formal proposal to the governance contracts illustrates a stark difference between on-chain and off-chain processes. For instance, it is natural to assume that a formal proposal will only be submitted after it has been thoroughly discussed on the forum. In practice, nothing can actually prevent a direct submission of a proposal without any discussions. As long as the transaction to submit a proposal is formatted correctly, a proposal can be created in a permissionless manner. Of course, such a proposal is unlikely to pass without the community's involvement and off-chain discussions.

Voting will usually be open for a specified period of time that can last from a few hours to several days or weeks. This time period is called a voting window. For simplicity, the DAO may start with a fixed window expressed using block heights. This will be a configurable parameter. The window can differ across proposals. For example, critical changes may specify longer voting periods to allow more participants to vote.

While the voting window for a proposal is still open, a user can change their vote any number of times. Naturally, as these are on-chain transactions, they will have to pay the associated transaction fees each time they change their vote.

Initially, voting options in RootstockCollective will be restricted to three discrete choices: YES, NO, and ABSTAIN. Following standard practices, RootstockCollective will require votes to meet quorum requirements – to ensure some minimum level of engagement by the community. The quorum criteria are based on comparing the cumulative voting power cast for a proposal with the cumulative voting power of the entire community. The cumulative voting power of the community (at any point in time) is just the total existing supply of stRIF tokens. Quorum computations take both YES and ABSTAIN votes into account. Once the quorum requirement is satisfied, the ultimate outcome of a vote is based on whether the YES votes surpass a Support threshold. For example, to implement a simple majority rule, a proposal can set the threshold at 50 percent. ABSTAIN votes are disregarded and do not matter when determining whether a proposal succeeds or not.

Once the voting window is closed, the outcome is fully determined. If the community settles on NO, then no further action is needed. Typically, the YES option is associated with an explicit follow-up action. For example, the YES outcome may be a decision to award a grant to a specific project. When a proposal passes, the outcome is not activated immediately on the blockchain. Instead, the (now successful) proposal is added to a queue by a TimelockController, where it will wait for a set number of blocks before it can be executed. As explained later, this intentional delay in the execution of a successful vote is a standard security measure adopted by most DAOs.

Once this waiting period is over, the proposal can be activated on-chain through a specially crafted transaction that can be triggered by anyone. In some cases, sending this on-chain transaction to execute the proposal may be quite expensive (in terms of gas). For example, this may be the deployment of a new set of contracts to upgrade some components of the system. To avoid relying on the generosity of an altruistic community member, the RootstockCollective Foundation can make arrangements to ensure that successful voting outcomes are activated without unnecessary delays.

Multiple proposals can be open for voting at the same time, and stakers can vote for parallel proposals at the same time. However, depending on the snapshot block, a staker's voting power can differ across these independent proposals. This can happen if the user's balance of stRIF changes between the blocks used as a snapshot reference for the first and second proposals.

Security

In the initial stages, the Foundation can help prevent unauthorized withdrawals from the DAO's treasury. The Foundation will have the ability to halt and terminate the on-chain voting process for proposals that are flagged by the community as being malicious. Suppose a proposal is identified as erroneous or malicious only after it has already passed on-chain vote. In this case, the Foundation can remove the proposal from the execution queue.

Post initial deployment, the Foundation will maintain ownership of the contracts to prevent unauthorized upgrades to the governance system. As mentioned earlier, all successful proposals are placed in a queue before they can be activated. This design introduces a time delay by default. The delay is a configurable parameter and it prevents a voting outcome from becoming active (on-chain) before a certain time or block number. This is useful as a security feature when voting on critical changes to the system, or making large payments from the DAO's treasury. In case of security exploits, this delay parameter allows the community some time to evaluate their options. A common approach is for the community to assign special intervention rights to a designated group called "pause guardians" or "security council". In case of emergency, this group (usually a multisig for additional security) can halt the system, or act in a more fine-grained manner, such as delaying the time when a highly contentious proposal (that has already been voted in favor) can become effective. A security council can also be empowered by the community to make emergency upgrades to the contracts. Given their power, such intervention mechanisms require careful selection of the members of the security council. Given the sensitivity, RootstockCollective will not have this enabled at the start. The community can discuss their introduction and the selection process for membership at a later point in time. Until then, the RootstockCollective Foundation can provide some level of security against theft by actively authorizing withdrawals from the DAO's treasury contracts.

BOOTSTRAPPING THE DAO

To operate effectively, all DAOs need access to resources. In the absence of any revenue sources, RootstockCollective must rely exclusively on community support, at least during the bootstrapping phase. This support can come in the form of donations and also through contributions of services such as software development, security audits, moderation of community discussion forums or social media channels, etc.

Contributions

Direct donations can be challenging for the wider community to coordinate and manage. This is where the RootstockCollective Foundation can take an active role. Donations can be directed to the Foundation, which can then set up a schedule, to make these resources available to the DAO's treasury.

Since the inception of the Rootstock Blockchain, RootstockLabs has been a leading contributor to the growth of the network. This direct engagement and support have been important for the growth of the Rootstock ecosystem. Given its history, RootstockLabs can be expected to support the DAO through both donations and service contributions to the RootstockCollective Foundation. RootstockLabs can also serve the community by participating in governance, and providing research and technical support to the Foundation and the community. The creation of the RootstockCollective is also an opportunity for the community to progressively assume greater influence in the ecosystem, including its growth and long-term economic sustainability.

Revenue Sources

The broader Rootstock community can support the DAO through network fees. Currently, RootstockLabs receives a fraction of the transaction fees generated on the network. RootstockLabs can contribute some of these fees to the DAO (through the Foundation). The community can also propose changes to the core network protocol, so that some fees are sent directly to the DAO's treasury or to the Foundation. As with every consensus change to Rootstock, this kind of proposal will have to go through the standard RSKIP process (i.e. not through DAO proposals).

In the future, the DAO may also earn revenue through other means, such as by serving as a governance platform for other protocols or applications on the Rootstock network. Such applications could share some of their protocol fees with the DAO.
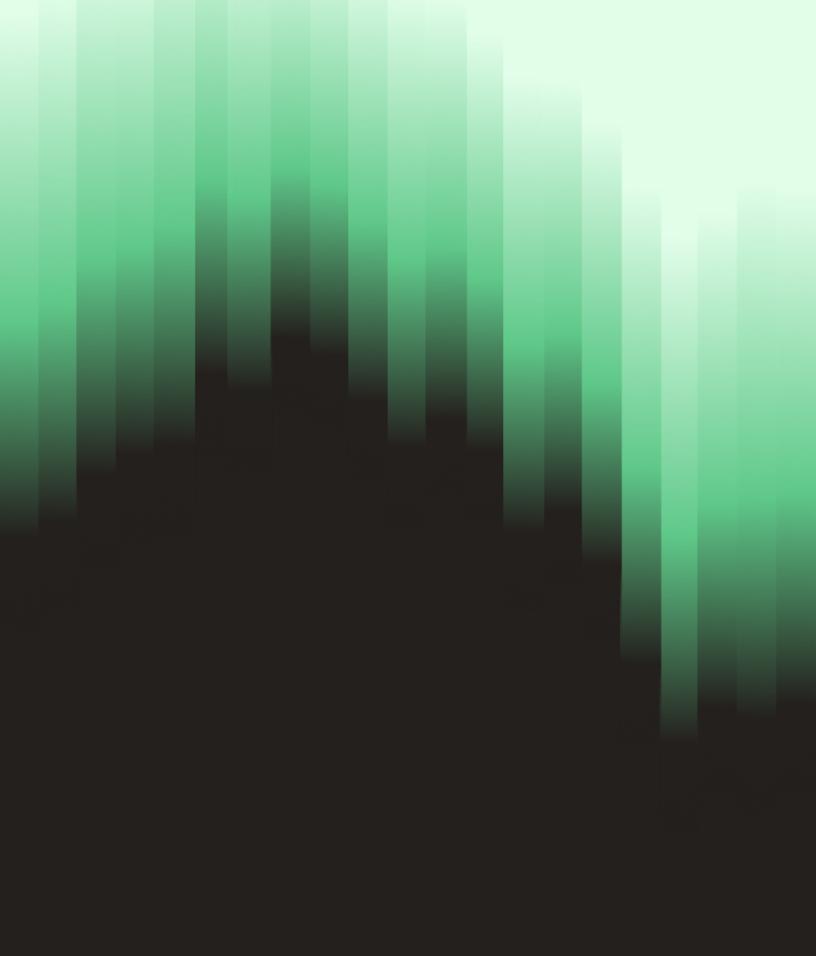
Value Capture and Growth

While the initial focus will be on decentralizing the allocation of grants, the DAO will also enable the realization of value capture for Bitcoin builders. For instance, in the future, builders may be eligible to receive a share of the DAO's revenues. This will encourage more developers to build great products on Rootstock, increasing transaction activity and revenue for the DAO as well as for the builders themselves. Community members, RIF stakers to be specific, may also be able to take part in the value capture. The distribution of fee shares and grant allocations will be decentralized, which will require stakers to vote on proposals. Stakers can be incentivized to actively engage in this process, and receive a portion of the funds distributed to builders.

TECHNICAL IMPLEMENTATION

Technical details including system architecture and specifications will be shared by the RootstockCollective Foundation at a later stage, once they are available. As stated previously, one of the goals of the initial design of RootstockCollective is to stay close to best practices observed at highly regarded DAOs. Continuing in this spirit, the new governance token and core governance contracts will be created using standardized, audited, open-source smart contract libraries such as those developed by OpenZeppelin.

ROOTSTOCK COLLECTIVE