



[Secretnodes.org](https://secretnodes.org)

Burn ENG for SCRT! Proposal

March 3, 2020

V 0.52

Summary

This proposal lays out the high level plan for **Burn ENG for SCRT!** SCRT (“Secret”) is used for staking, governance, and transaction fees within the Enigma network which is now [LIVE](#) based on Cosmos SDK/Tendermint. It is critical to the future of the Enigma protocol that the broader community that currently holds ENG tokens to be able to burn their tokens in exchange for SCRT being minted to participate in staking, governance, and transaction fees. This proposal will outline a brief background, technical approach, and detailed milestones to achieving an expeditious, straightforward and secure **Burn ENG for SCRT!**

Who is Submitting

This proposal is being submitted by Secretnodes.org. Seceretrnodes.org has deep roots in the crypto space. Secretnodes.org is a community-led group who care about privacy, security, and data rights. We are dedicated to supporting secret node runners. Secretnodes.org founder, Ian Dixon, got involved with cryptocurrency as early as 2011 and has been an avid researcher and node runner in Proof of Stake Protocols since their inception. [Brendan Kittredge](#) joined forces with Ian to provide business insight after much time spent supporting Enigma through the [Enigma Collective](#). The team compliments each other well and hopes to have contributions from many others that share their passion for privacy and belief in decentralized technologies as time moves on.

Secretnodes.org

<https://secretnodes.org>

<https://github.com/secretnodes>

Brendan Kittredge- Co-founder & CEO ([LinkedIn](#), [Twitter](#))

Ian Dixon - Co-founder & CTO ([Twitter](#))

Background/Problem

On February 13th, 2020, the first Enigma mainnet was successfully launched as a proof-of-stake-based blockchain based on Cosmos SDK/Tendermint and secured by a new native coin, Secret (SCRT). Twenty-two (22) participating validators from across the Enigma ecosystem representing 10+ time zones jointly agreed on the genesis block of the Enigma blockchain, which was signed on Thursday, February 13th. These initial validators now govern and operate the Enigma mainnet. Further details on the mainnet launch can be found in the article [here](#).

The most important detail relevant to this proposal is that the Enigma blockchain is secured by a native coin known as SCRT ("Secret"), which is used for staking, governance, and transaction fees within the network. Its sole purpose is utility within the network. Node operators for Enigma stake SCRT. Enigma's development team is committed to ensuring that operations and future actions are in strict compliance with relevant regulations. At this point in time the Enigma team has stated that, "We have worked tirelessly to explore legally compliant avenues for facilitating a token swap between the ERC-20 ENG token and the mainnet SCRT coin. We are continuing discussions with our legal counsel and regulators to identify an effective means of facilitating a swap that complies with all relevant securities regulations, but for the time being, our team is not able to proceed with facilitating a swap."

While the team has indicated that they are not **directly able to facilitate** a token swap due to legal/regulatory compliance there is no reason to believe that the broader community and decentralized set of validators cannot vote on and implement an open source **Burn ENG for SCRT!** process.

Validators are currently the de facto governance decision-makers for the EnigmaBlockchain. We're concerned that without enabling current ENG holders to burn their tokens in exchange for SCRT and participate in decentralized delegation, the EnigmaBlockchain governance mechanism will be dominated by centralized powers. Currently the network only has 22 validators; leaving 28 validator slots wide open. Furthermore, the broader community and

ENG holders are not able to participate in governance and delegate their tokens to validators who align with their best interests.

[Secretnodes.org](https://secretnodes.org) recognized the urgent need to unify the Enigma community and submitted [Proposal #2](#) on 17 Feb 2020, 12:33:26am UTC with Ian Dixon stating, “I propose we collectively find a way to achieve a token swap so we can unify the Enigma Community. We already have a diverse set of people ready to build on enigma, participate in governance, stake, and run nodes from all around the world. I welcome everyone interested in this to further discuss how it can be achieved here.”

The initial proposal served as a signal to solicit community feedback regarding a token swap, and was posted to [Secretnodes.org](https://secretnodes.org)'s GitHub to solicit comments here:

<https://github.com/secretnodes/secretnodes.org/issues/13>

As can be seen in the comment thread there is overwhelming support by the community for a 1:1 ENG to SCRT **burn to mint** ratio. The scope of this proposal is not to get into arguments regarding token supply, or details surrounding future supply (i.e. inflation). [Secretnodes.org](https://secretnodes.org) believes decisions regarding future token supply are best left to later proposals when the network has more stability and active participation in governance. Furthermore, given the time sensitive nature of executing **Burn ENG for SCRT!** for the health of the network and community it's best not to make the proposal terms herein any more complicated than they already are.

Solution

Since February 17, 2020 [Secretnodes.org](https://secretnodes.org) has been in conversations with many validators and parties regarding the technical details around executing the plans detailed herein. There have been many iterations and suggestions for solutions, but we believe that the most expeditious, intuitive, and secure approach has been chosen. There are many steps that need to take place, and many parties that need to contribute from the community that to make this effort a success. Here is a brief outline of the steps necessary:

1. [Overarching Project Management](#)
2. [Increase Community Fund to be Earmarked for Code Development, Validator Incentives and Audit](#)
3. [Stand up EnigmaBlockchain Testnet and Faucet](#)
4. [Mathwallet Testing and Integration for SCRT Enigma Wallet](#)
5. [Create **Burn ENG for SCRT!** Code](#)
 - a. Code abstract can be found [here](#)
 - b. Code Repository Started [here](#)
6. [Security Audit](#)

- a. Access to codebase (GitHub or .zip)
 - b. Documentation
 - c. Tests
- 7. [Implement Code Front-End in Mathwallet](#)
- 8. [Proposal for M-of-N multisig threshold, and choosing leader/participants](#)
- 9. [Release Community Instructions](#)

Task 1: Overarching Project Management

Secretnodes.org has stepped up to generate a comprehensive plan and milestones for this effort, and has agreed to post the overarching proposal with details surrounding the efforts to **Burn ENG for SCRT!** Secretnodes will act as a rally point for the validators throughout the project. Secretnodes.org also has consulted some legal entities and has allocated SCRT for potential legal expenses through the process.

Responsible Parties: Secretnodes.org

Estimated Completion: 4/13/2020

Task 2: Increase Community Pool to be Earmarked for Code Development, Validator Incentives and Audit

To pay for the development of code, testing, standup of testnet, wallet integration, and to incentivize validators to participate in governance mechanisms and the execution of SCRT minting it has been discussed that the community pool of the network needs to be increased. The first plan for this increase was to submit a proposal for a parameter change to temporarily increase and divert inflation for a set number of blocks while at the same time increasing the community tax to fill the community pool. While this solution would provide us with a pool of funds to use for community spend proposals it is a bit time intensive as it requires another proposal for parameter changes, calculation of inflation impacts, a proposal voting and approval period, and actual implementation.

In interest of time and simplicity, it is hereby proposed that the minting module incorporate an additional 2% SCRT for each ENG that is burned. In doing so we would have a simple mechanism for increasing the community pool and to incentivise network participants. It is proposed that half of this newly minted SCRT be diverted to the community pool address, and that the other half be evenly distributed amongst validators selected and participating in the SCRT minting in Task 8.

It is proposed that said future community pool SCRT be earmarked for the efforts as defined and outlined in the [milestones plan](#) linked below. **Approval of this proposal by validators represents agreement with this proposed additional 2% SCRT minting and agreement with the proposed distribution detailed in the project milestones.**

Responsible Parties: Secretnodes.org, Agreement of all Validators on Proposal 4

Estimated Completion: 3/12/2020

Task 3: Stand up EnigmaBlockchain Testnet and Faucet

As part of wallet integration and testing it is necessary to have a testnet up and running for testing purposes.

Responsible Parties: Dan, Chain of Secrets

Estimated Completion: 3/5/2020

Task 4: Mathwallet Testing and Integration for SCRT Enigma Wallet

To prepare for the swap users will need to generate a wallet capable of storing keys for the new SCRT tokens. At **no point** in time during this **Burn ENG for SCRT!** process do any of the validators want to create user wallets or possess any private keys for such wallets. Doing so could put them at risk for being in a custodial capacity which is NOT the intent of this proposal. Allowing users to create and maintain their own SCRT wallets is thus integral. These generated wallet addresses must be supplied later on in the **Burn ENG for SCRT!** process for users to receive their SCRT tokens.

Responsible Parties: Eric, Mathwallet

Estimated Completion: 3/13/2020

Task 5: Create Code for Burn ENG for SCRT!

The code repository for the **Burn ENG for SCRT!** process has been started and lives at <https://github.com/scotchfinance/scrt-swap>. As outlined in the Github repo the subtasks include:

Development tasks:

- ✓ Smart contract that burns ENG (**DONE**)
- ✓ Leader that watches Ethereum, and unsigned tx to the db (mocked tx) (**DONE**)
- ✓ Operator watches Ethereum and sign the tx (mocked sig) (**DONE**)
- Leader ratifies the tx and submits to enigma cli
- Integrate enigmacli into the operator and leader (real tx and sig)
- ✓ Frontend React template integrate with Web and the smart contract (**DONE**)
- Burn ENG form in frontend
- ✓ End-to-end integration test (**DONE**)

Stress test and dry run
Minter module that authenticates the multisig address

Operational tasks:

Vote on operators and leader
Operators configure their private key in their enigmad
Leader creates the multisig address and imports operators public keys in enigmad

It should be noted that the minter module development task will likely include proposed changes to the enigmad file and must be initiated/implemented via a pull request to the Enigma repository. The validators are assuming that the Enigma repository maintainer is able to execute such a request. If this is **NOT** the case it is requested that responsible parties speak up on these technical details.

Responsible Parties: Scotch, Laura
Estimated Completion: 3/30/2020

Task 6: Security Audit

Once the code has been developed and thoroughly tested it will need to undergo a third party audit. Secretnodes.org will handle conversations with potential auditors, and an allocation of SCRT has been earmarked per [Task 2](#) above for this purpose.

Responsible Parties: Secretnodes.org, Auditor
Estimated Completion: 4/13/2020

Task 7: Implement Code Front-End in Mathwallet

Once the code has been completed and audited it is required that a front-end be developed so users can easily **Burn ENG for SCRT!** Mathwallet has indicated that they're able to provide users an easy user experience with dApps hosted in their application.

Responsible Parties: Eric, Mathwallet
Estimated Completion: 4/13/2020

Task 8: Proposal for M-of-N multisig threshold, and choosing leader/participants

Burn ENG for SCRT! Code will require that a number of validators participate in the process. As code completion nears a formal proposal for choosing the leader and participants will be issued.

Responsible Parties: Secretnodes.org

Estimated Completion: 4/10/2020

Task 9: Release Community Instructions

When all development, testing, and audits are complete the **Burn ENG for SCRT!** open source code will be ready for community use. Instructions will be posted for users wishing to **Burn ENG for SCRT!** It should be noted here that none of the parties participating in this development process are making any solicitations/offers whatsoever to ENG holders. Any burning of ENG is designed to be user initiated, we never take custody of user funds, we are not liable for the performance of this software, and do not offer warranties of any kind.

Responsible Parties: Secretnodes.org

Estimated Completion: 4/13/2020

Further details surrounding these steps and proposed SCRT allocations can be found in the [Community Spend, Milestones, & Deliverables](#) section below.

Notes and/or Future Considerations

Future governance proposals should address concerns such as inflation rate. While inflation rate is currently pegged to a target amount stake it is unclear at this time what the ideal target rate and resulting inflation rate should be for the health of the network. Secretnodes.org hears the communities voices on this concern, but does not believe it can be accurately addressed at this time.

Community Spend, Milestones & Deliverables

See this spreadsheet for full milestones, deliverables, responsible parties, and community spend:

Burn_ENG_for_SCRT_Milestones_Project_Tracking-DRAFT-v0.52.pdf

All code will be posted to public repositories. The community will be updated through the [Secretnodes telegram room](#) on **Burn ENG for SCRT!** progress.

Relationships & Disclosures

[Secretnodes.org](https://secretnodes.org) has not yet received any grants or investments related to the new EnigmaBlockchain. Relationships with all Enigma stakeholders, including validator operators, protocol and tool (wallet, staking interface) developers, SCRT stakers, ENG holders, and yet-to-be-identified stakeholders will be critical to carrying out these activities, and to upholding our standing in the community. For this reason, we want to operate with as much transparency as possible. While we propose an allocation of SCRT for validators in the proposal we do not believe we are asking for handouts or being rewarded for unwarranted efforts. We believe without these efforts, what we aim to achieve may never actualize. We ask that all stakeholders recognize the efforts we have put in and continue to put in supporting the Enigma protocol. We firmly believe that the SCRT allocation detailed herein is the only way to incentivize participation amongst validators, code creators, auditors, and all who will help make **Burn ENG for SCRT!** happen expeditiously. Furthermore, it should be noted that any user wishing to **Burn ENG for SCRT!** does so at their own risk. Secretnodes.org bears no responsibility for open source code functionality, and this proposal should in no way shape or form be construed as any solicitation/offer.