Outlier Ventures

Proposal: Token Swap Watcher

Outlier Ventures

Version: Final, v5, 2020-06-19

Disclaimer

This document (the "Document") is produced by Outlier Ventures Operations Limited and its affiliates ("Outlier"). The Document may contain material that is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in any locality, state, country or other jurisdiction where such distribution, publication, availability or use would be contrary to law or regulation or which would subject Outlier to any registration or licensing requirement within such jurisdiction.

All material presented in this Document, unless specifically indicated otherwise, is under copyright to Outlier and/or Outlier's licensors.

The Document should not be considered a recommendation by Outlier or any of its directors, officers, employees, agents or advisers in connection with any purchase of or subscription for securities or otherwise. Recipients should not construe the contents of this Document as legal, tax, regulatory, financial, investment, trading or accounting advice or services and are urged to consult with their own advisers in relation to such matters. The information contained in the Document has been prepared purely for informational purposes.

Information and opinions presented in this report have been obtained or derived from sources believed by Outlier to be reliable, but Outlier makes no representation as to their accuracy or completeness. Outlier accepts no liability for loss arising from the use of the material presented in this report. Outlier may have issued, and may in the future issue, other communications that are inconsistent with, and reach different conclusions from, the information presented in this report. Those communications reflect the different assumptions, views and analytical methods of the analysts who prepared them and Outlier is under no obligation to ensure that such other communications are brought to the attention of any recipient of this Document.

Past performance should not be taken as an indication or guarantee of future performance, and no representation or warranty, express or implied, is made regarding future performance. Information, opinions and estimates contained in this Document reflect a judgment at its original date of publication by Outlier and are subject to change without notice.

This Document may provide the addresses of, or contain hyperlinks to, websites. Except to the extent to which the report refers to website material of Outlier, Outlier has not reviewed any such site and takes no responsibility for the content contained therein. Such address or hyperlink (including addresses or hyperlinks to Outlier's own website material) is provided solely for your convenience and information and the content of any such website does not in any way form part of this document. Accessing such website or following such link through this report or Outlier's website shall be at your own risk.

Summary

A community effort is under way to enable swapping ENG tokens to SCRT tokens, the native token of the Secret Network. Technical work is close to completion and all required parties are lined up to successfully launch and operate the swap mechanism.

Assuming a successful launch of the token swap, there is a need for end users, network stakeholders, core protocol developers and the token swap team to have clear visibility on the status and history of all swapped tokens. There is a need to independently verify the correct operation of the token swap, on an ongoing basis as long as the swap mechanism is in operation, and beyond that time to provide accountability and transparency to all stakeholders.

To meet these needs, we propose building a Token Swap Watcher, and hosting and maintaining a public-facing instance of it. The Token Swap Watcher can be accessed as a web interface for the general public, and as an API endpoint and as easily runnable code for more technical users.

Who is submitting

Outlier Ventures partners with, invests in and supports the development of technologies for an open data economy. The main way we support teams is through the Base Camp accelerator. Alongside Base Camp we maintain a selected amount of strategic partnerships with cryptonetworks and businesses.

We are an active open source contributor with an in-house development team, with over 30 open source repositories going back to 2015.

Outlier Ventures is one of the genesis validators of the Secret Network, and has maintained a highly available validator ever since the genesis. We have been actively involved in the Secret Network community, and have tracked, reviewed and given feedback on the token swap effort. Outlier Ventures nor any of its people are however a direct contributor to the token swap, and hence can play an independent role.

The entity submitting is Outlier Ventures Operations Ltd, registered in UK Companies House with company number 10722638.

Problem

A community effort is under way to enable swapping ENG tokens to SCRT tokens. ENG tokens have the form of an ERC-20 token on the Ethereum mainnet, and SCRT tokens are the native token of the Secret Network, a DPoS network based on Cosmos SDK.

Making the token swap possible is non-trivial. It requires changes to existing software and newly built software, a group of actors running that software, and power given to that group of actors through the governance mechanism of the Secret Network:

- Changes to the code of the Secret Network node software, and a network upgrade to activate those changes
- An Ethereum smart contract for burning tokens
- A swap worker process, to be run by a leader and operators in a committee
- A database for leader and operators to coordinate
- A web interface for end users to initiate token swaps
- Configuration in the Secret Network of the addresses of the leader and the operators to be able to mint SCRT through multisig transactions

The token swap is a sensitive operation, because of the high monetary value of the operations involved and the non-reversibility of the transactions. In building and operating the token swap, many things small and large could go wrong.

There is a need for all network stakeholders, including end users, token holders, core protocol developers and the token swap team to get insight in the status and history of swapped tokens. There is a need to independently verify the correct operation of the token swap, on an ongoing basis as long as the swap mechanism is in operation, and beyond that time to provide accountability and transparency to all stakeholders.

Solution

To meet these needs of the Secret Network community around the token swap, we propose building and operating the Token Swap Watcher, an independent continuous monitoring and analysis tool.

The Token Swap Watcher sources its data directly from nodes from the respective blockchains, the Ethereum mainnet and the Secret Network mainnet.

The Token Swap Watcher can be accessed in three main ways:

- Web interface: The general public can access the Token Swap Watcher as a web interface.
- API endpoint: An API endpoint will be provided, which third party-applications such as block explorers can use to access the data. Integration of the API with one open source block explorer is included as a deliverable.
- Run the code: Technically capable users can run the code themselves on their own premise.

The Token Swap Watcher is able to answer questions like the below:

- Can all minted tokens be traced back to an Ethereum burn transaction?
- Is the total amount of minted SCRT by the swap mint module equal to the total amount of burned ENG in the burn contract?
- What is the total count of swaps?
- What is the total amount of swapped tokens?
- What is the total current supply of SCRT?
- For a burn transaction X on Ethereum, what is the mint transaction Y on Secret Network?
- For a token swap operation S:
  - Has the leader initiated a multisig transaction? What is the transaction hash?
  - Which operators have signed the multisig transaction?

Non-functional requirements:

- The web frontend will be usable from modern web browsers, without the requirement for a wallet for either the Ethereum mainnet or the Secret Network to be installed.
- The data processing components of the Token Swap Watcher are idempotent: they can be run repeatedly and will deliver the same result, no matter what the current state of the database is.

High-level components:

- Independent Ethereum mainnet node
- Independent Secret Network mainnet node
- Database
- Backend
- Web frontend
- API endpoint

Technical foundations:

- Only stable and widely supported programming languages and open source components will be used.

- Existing components and libraries will be reused as much as possible.

Out of scope - What is this not?

No active role in token swap: the Token Swap Watcher has no influence on the token swap. It does not submit any transactions. It only ingests publicly available data from the Ethereum and Secret Network blockchains, processes and aggregates that data, and makes the results available.

No additional data: the Token Swap Watcher doesn't store any additional data. It merely shows raw and processed data from the underlying public data sources.

No opinion: while the Token Swap Watcher will include some interpretation of events, for example to analyse the current state of a swap operation, it doesn't provide an opinion on what has been done or what should be done.

Questions

How does this relate to a code audit of the token swap?

A full code audit might address a small part of the needs mentioned. It could give some confidence that there are no severe errors in the code. However a code audit has several limitations:

1. A complete code audit for all modules involved is unrealistic considering the large code bases.
2. An audit is generally a one-off event, while the swap is expected to be run over a prolonged period, with the network node software being further developed.
3. In case an unforeseen incident happens in practice, an audit document isn't helpful in analysing and solving that incident.
4. An audit doesn't consider or give insight about the state at any given moment, only the code to produce that state.

The Token Swap Watcher is therefore complementary to any audit and code review efforts.

How does this relate to existing block explorers?

Existing block explorers on both Ethereum and the Secret Network provide insight into data on the chains on either end. They don't combine the data and analyse it specific to the token swap. The Token Swap Watcher will link to existing block explorers where appropriate to provide further details on transactions.

Furthermore, the Token Swap Watcher API is explicitly meant for third party applications including block explorers to integrate with. The integration of the Token Swap Watcher API with one block explorer is included as a deliverable.

How does this relate to Puzzle?

Puzzle is a project in development (proposal 8, proposal document) with the aim to "radically improve the ability of end-users to stay up to date on events that occur on the Secret Network", "solving for the biggest pain points around governance, assessing network performance, and tracking updates from projects in the ecosystem". Like block explorers, combining data from the Ethereum mainnet and the Secret Network is not in scope, and The Token Swap Watcher might link to Puzzle where appropriate. It can also be imagined that Puzzle links to or integrates some of the functionality of the Token Swap Watcher.

How does this relate to the testnet(s)?

The developed code can be run on the main Secret Network testnet (as maintained under proposal 9) and any other instances of the Secret Network code by anyone. As part of this proposal we might run versions of the Token Swap Watcher on testnets from time to time, but do not include a working implementation on the testnets as an explicit deliverable.

Deliverables and timeline

Deliverables

- Open source code, released under Apache 2 license:
  - Backend
  - Web frontend
  - API endpoint
  - Devops scripting
- Hosted version

Timeline

Release	Target release date	Description
MVP	At moment of token swap launch or shortly thereafter	Initial version, optimising for timely delivery over feature completeness

Feature release	1 month after swap launch	Feature release with additional functionality and API endpoint
Final release	2 months after swap launch	Final release with all remaining points from the roadmap
Maintenance period	As long as the token swap is in operation, and for a maximum of 9 months	Active maintenance of the code and the hosted versions. This includes any compatibility updates required to deal with changes, e.g. network upgrades and hard forks.

We intend to maintain the code and the hosted version beyond this time, to ensure the long-term availability of the Token Swap Watcher. We will evaluate the best way to do this before the end of the maintenance period, taking into account the state of the network, ecosystem, and other available tooling at that point. Possibilities include a follow-up proposal.

Budget

The requested budget is based on estimates for the development work, uncertainties in the future value and liquidity of SCRT, the risk we are willing and able to take, and our determination to deliver great results that are of long-term value to the Secret Network and its community for a highly competitive budget.

Milestone	Duration	Deliverable	Description	Cost (SCRT)
Setup	7d	Set up development environment		6,400
		Dev environment	Set up development environment of all components including token swap	
MVP	14d	Initial version, optimising for timely delivery over feature completeness		14,400
		Web interface	Initial web interface with most essential user-level functions. I.e. "what's the state of my transaction?"	
		Backend	Initial backend, scraping of Secret Network and Ethereum nodes, linking transactions	
Feature release	30d	Feature release with additional functionality and API endpoint		19,200

		API endpoint	Deliver API endpoint for public consumption	
		Improved web interface	Advanced analysis of individual transactions	
		Overview and analytics	Overview pages, aggregates	
		Backend	Expand backend to enable additional functionality in this phase	
Final release	30d	Final release with all remaining points from the roadmap		16,000
		Further features	Remaining features from roadmap and feedback	
		Local Ethereum node	Scripting and config to use a local Ethereum node	
		Devops scripting	Deliver devops scripts to help other parties deploy an instance	
Hosting	9m	Hosting and deployment of live versions		12,600
		Web interface hosting	Hosting of the Web interface on a public URL	
		API hosting	Hosting of the API endpoint on a public URL	
		Monitoring and management	Monitoring and proactive management of the hosted versions	
Maintenance	9m	Active maintenance of the code and the hosted versions		14,400
		Code maintenance	Active maintenance of the code and the hosted versions. This includes any compatibility updates required to deal with changes to the Secret Network, e.g. network upgrades and hard forks.	
Project management	9m	Overarching project management and admin		8,300
		Project management	Overarching project management and admin	
Total budget				91,300

Relationships and disclosures

Outlier Ventures is structured as a partnership. The partnership has ENG and SCRT token holdings. Some of the individuals within the partnership have ENG and SCRT token holdings.

Outlier Ventures has a strategic partnership with Enigma, announced in August 2019, before the birth of the Secret Network.

References

For further details on the token swap, the below sources are a good start:

- Proposal 4 - Burn ENG for SCRT (proposal document, milestones)
- Proposal 6 - Burn ENG for SCRT budget allocation (proposal document)
- Forum thread with progress reports
- Channel #the-secret-swap on the Secret Network RocketChat