Swaptor Whitepaper

Berry Block

Marko Ivanković marko@berryblock.io
Domagoj Ravlić domagoj@berryblock.io

Abstract

Peer-to-peer (P2P) swaps on blockchain have the potential to greatly benefit users by eliminating the need for intermediaries in the exchange of assets. However, the use of P2P swaps on blockchain also presents several challenges, including trust issues that must be addressed in order to ensure their success. Since there is no intermediary to oversee the exchange of assets, users must rely on the trustworthiness of the other party to the transaction. In the absence of a trusted third party, it is difficult to verify the authenticity and quality of the assets being exchanged, which can lead to disputes and losses for users.

Furthermore, P2P swaps on blockchain are subject to potential security risks, such as hacking and fraud. Since the transactions are conducted directly between users, there is a greater risk of malicious actors attempting to exploit vulnerabilities in the system. This risk is exacerbated by the fact that blockchain transactions are irreversible, meaning that users have no recourse if their assets are stolen or lost.

In this paper we describe Swaptor, a decentralized P2P exchange dapp which aims to eliminate problems mentioned above.

Contents

1 Architectural Overview

As most modern dapps, Swaptor's architecture is a mix of on-chain and off-chain components:

- **On-chain**: Smart contracts
- **Off-chain**: Backend, Frontend and Database

1.1 On-chain Architecture

Smart contracts are written in Solidity, and their architecture is designed to be minimalistic. Specifically, the Swaptor contract is a singular entity whose sole purpose is to verify digital signatures and execute swaps upon successful verification. Digital signatures encode the specific terms under which a given swap is considered valid.

1.1.1 Signatures

In order to verify the signature, the smart contract must possess both the original swap elements and the signature itself. Prior to being passed as an argument to one of the *acceptSwap* functions, these elements are encoded using the *abi.encode* function. The signature is generated by creating a *keccak256* hash of the encoded arguments and signing it with the private key belonging to the seller. This method dramatically reduces the gas fees because the seller never had to transfer their assets to Swaptor contract.

1.1.2 Swap types

At present, Swaptor facilitates the swapping of ERC-721 and ERC-20 tokens, enabling the execution of any combination of swaps involving these types of tokens. In the future, Swaptor intends to extend its support to include native currency and ERC-1155 tokens.

1.1.3 Fees

To accept the swap, an address will need to pay a fixed fee of $5 in the native currency, which is calculated using Chainlink oracles[1]. It should be noted that the fee is not fixed and may be subject to change.

1.2 Off-chain Architecture

1.2.1 Backend

The purpose of the backend is to reduce the number of operations on the blockchain, which would result in higher gas fees paid by users. It also caches some information retrieved from the blockchain to improve the user experience, such as reducing wait times. Upon client request, it retrieves details about swaps, including the original swap terms and signature.

1.2.2 Frontend

The Swaptor frontend application is a user interface that allows users to interact with the Swaptor protocol on the supported networks. It enables users to easily swap supported token types without the need for a centralized exchange. Each user is capable of creating, deleting, sharing and accepting a swap. The application is accessible through a web browser or mobile device and is designed to be user-friendly and intuitive.

2 Swaptor token (SWPTR)

Swaptor introduces its very own token called the Swaptor Token (SWPTR), which plays a crucial role in the Swaptor governance model. By actively participating in voting rounds, SWPTR holders have the opportunity to unlock a share of the rewards generated from Swaptor's swapping fees. This mechanism allows for a fair and inclusive system that rewards only those who contribute to the platform's decision-making process.

2.1 Governance

2.1.1 Initial stage

As an essential part of the Swaptor governance model, the initial stage of the project will involve the Swaptor developer team taking on the role of the Swaptor Committee. This dedicated team will be responsible for facilitating the governance process by overseeing the submission of proposals, managing the voting procedures, and ensuring the seamless operation of the Swaptor project. The Swaptor Committee plays a crucial role in creating important questions and proposals that are later shared with the Swaptor community for voting.

2.1.2 Swaptor DAO

Over time, the influence of the Swaptor developer team within the project will gradually diminish. Initially, they will actively listen to the community's feedback and opinions through channels such as Twitter and Discord, incorporating necessary code changes accordingly. Ultimately, the Swaptor project will evolve into a fully-fledged decentralized autonomous organization (DAO). In this future state, any holder of the SWPTR token will have the ability to propose changes to the project, and only those who possess SWPTR tokens will be eligible to participate in the voting process. The voting power will be determined by the amount of SWPTR tokens held, as well as the proportionate share of fees allocated as rewards for voters. After each vote, SWPTR holders will have the chance to unlock a portion of these rewards, which promotes a fair and interactive ecosystem.

2.2 Tokenomics

The maximum supply of Swaptor tokens is set at 1,000,000. These tokens will be introduced in two distinct phases, each serving a specific purpose in the evolution of the project.

2.2.1 First phase

In the first phase, which focuses on the initial stage of the project, the Swaptor developer team aims to involve and empower contributors from the community. During this phase, a total of 300,000 tokens (30% of the total supply) will be made available for purchase. The pricing of these tokens will be determined by the Swaptor developer team, ensuring a fair and reasonable value that reflects the project's goals and potential.

2.2.2 Second phase

Moving to the second phase, the distribution of the remaining 700,000 tokens (70% of the total supply) takes a different approach. Rather than being sold or offered directly, tokens will be minted exclusively through successful swaps conducted via the Swaptor smart contract. With each successful swap, where users exchange one cryptocurrency for another using Swaptor, one token will be allocated to each of the participant. This mechanism promotes active engagement with the platform and incentivizes users to participate in swaps, contributing to the growth and liquidity of the Swaptor ecosystem. It is important to mention that every token that is not sold in the first phase will be minted during this phase.

By adopting this two-phase approach, Swaptor aims to involve early contributors while also fostering a dynamic and sustainable token distribution model. It ensures that tokens are not only accessible to those who support the project from its inception but also rewards users who actively participate in successful swaps, aligning incentives and creating a vibrant community of token holders.

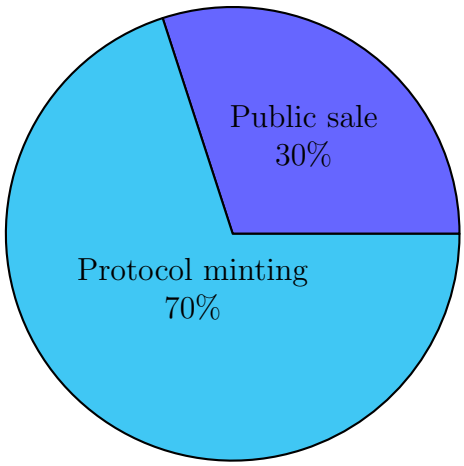

Figure 1: Token distribution

3 Roadmap

Q3 2023
Deployment of Swaptor contracts to Ethereum mainnet

Q4 2023
Mobile app development

Q1 2024
Support for remaining token standards

Q2 2024
Multichain & ENS names support

Q3 2024
Swaptor messaging & notification system - enabling direct communication between users through Swaptor website

Q4 2024 - Q1 2025
Order book model for ERC-20 tokens.

References

[1] What is an oracle in blockchain? explained — chainlink, `https://chain.link/education/blockchain-oracles`