OT-RFC-12

OriginTrail Parachain TRAC bridges

Authors: OriginTrail Core Developers

Version: 2
(version 1 available here)

Date: 2022-08-10

Introduction

The OriginTrail ecosystem is a two-layer system, driving its two symbiotic networks by their respective crypto tokens - the OriginTrail Decentralized Network (hosting the multichain OriginTrail DKG, as indicated in the whitepaper) driven by its utility token TRAC, and the underlying blockchains with their respective native tokens used for transactions.

The OriginTrail Decentralized Network utility enabled by the TRAC token therefore requires each of the respective blockchains to support the TRAC token according to the TRAC tokenomics design, and requires necessary bridge infrastructure between relevant chains. TRAC being an ERC20 token on Ethereum has been so far successfully bridged to two blockchains - Gnosis chain (formerly xDAI) and Polygon with their respective bridge infrastructure.

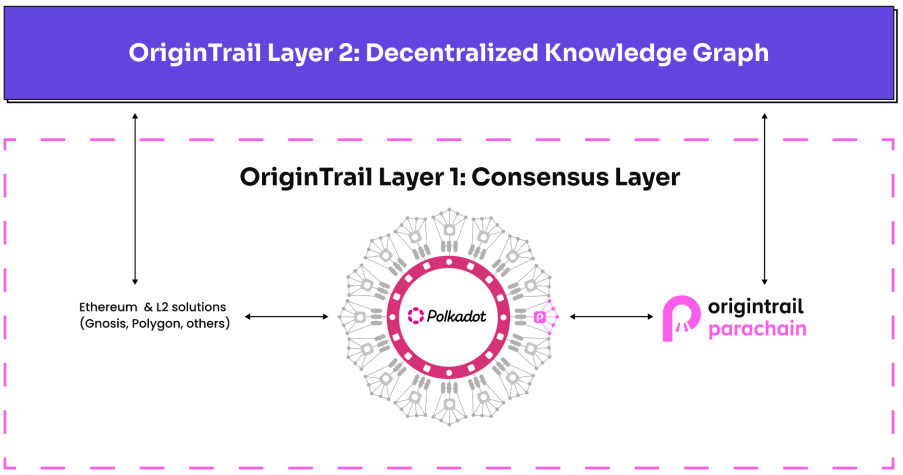
With the launch of the dedicated OriginTrail blockchain on Polkadot - the OriginTrail Parachain - the required bridge infrastructure needs to be created to facilitate the OriginTrail DKG operation on this new chain. Moreover, the same infrastructure will enable further network effects for TRAC on all of Polkadot emerging parachain infrastructure and solutions, such as Acala and its DeFi stack (DEX, aUSD stablecoin, etc).

The purpose of this document is to outline the technical approach to bridging the TRAC token to Polkadot via the OriginTrail Parachain and collect relevant feedback from the OriginTrail community.

This document presents **a second, revised version of the initial RFC detailing the bridging approach** based on the feedback received on the initial version from the OriginTrail community.

Bridging TRAC to OriginTrail Parachain and Polkadot

Polkadot is a network designed to enable high interoperability between blockchains and inter-blockchain trustless operations, such as bridging Polkadot based tokens on connected blockchains. As a multi blockchain network of parachains connected via the common Layer 0 Polkadot Relay Chain, bridging tokens is enabled by the powerful cross chain messaging format XCM. Using these inherent functionalities of Polkadot therefore solves the “bridging problem” within the entire Polkadot ecosystem - **once the TRAC token is available on the OriginTrail Parachain, making it available to other parachains is a non-issue**.



When it comes to external blockchains such as Ethereum however, there are a multitude of bridging approaches evolving in parallel. Two of the most promising approaches at the moment of writing this RFC are:

- Snowbridge, a general purpose trustless bridge in development by the Snowfork team, yet to be launched,
- Chainbridge, an EVM to Substrate bridge already available and in utilization by parachains such as Moonbeam and Centrifuge.

As development progresses, we can naturally expect new and improved bridging solutions in the years to come. Therefore, bridging of TRAC to the OriginTrail Parachain will, over time, most likely involve a multitude of different bridges and related infrastructure as the Polkadot ecosystem evolves. It is therefore essential to plan for this eventuality from the start and thus enable the bridge infrastructure evolution to be “inherited” by the TRAC bridges on the OriginTrail Parachain.

It is important to note that TRAC token will stay an ERC20 token on Ethereum and will be implemented as a bridgeable asset on the OriginTrail Parachain, which operates with its native token OTP.

OT-RFC-12 V2: Teleporting TRAC to the OriginTrail Parachain on Polkadot

The previous version of this RFC proposed the initial TRAC bridge for near-term utilisation be implemented via the Chainbridge system, while enabling emergent bridging infrastructure (such as the Snowfork bridge) as potential long term bridging solutions.
Due to the concerns expressed by the TRAC community regarding the inherent risks associated with such a bridge implementation (details below and in RFC comments), and demonstrated vulnerabilities of similar bridges seen recently within the crypto space (even while writing this update of the RFC), an alternative approach will be implemented - **"one way teleports".**

A one way teleport is an already proven approach within the OriginTrail community as it was successfully executed during the Starfleet stage of the OriginTrail Parachain development. Via a "one-time" TRAC bridge from Ethereum to the OriginTrail Parachain the OriginTrail community has successfully staked 100MM TRAC tokens to be transferred to the (then stand-alone) OriginTrail tailored blockchain.

The exact approach and details of the smart contract implementation are specified in OT-RFC-10, however for practicality an outline is presented here:

- A special smart contract is deployed on Ethereum blockchain designed to lock a specific amount of TRAC tokens, to be teleported to the OriginTrail Parachain. The contract is permissionless and anybody can deposit (lock) TRAC into it.
- The equivalent amount of TRAC tokens gets minted on the OriginTrail Parachain to the same address as the one that locked tokens on the Ethereum side (so tokens can be utilised by the same wallet).
- Special care is taken to ensure security of the smart contract - a thorough smart contract audit has been conducted, together with functionality minimization (to lower complexity and thus risk surface) as well as coding and testing best practices.

The near-term TRAC bridging proposal therefore is to:

- **Perform one way TRAC teleports** from Ethereum to the OriginTrail Parachain by reutilizing the same smart contract already proven in the previous 100MM TRAC Starfleet staking procedure. This contract implementation has been security audited by Quantstamp and proven functional and secure in a production environment. Additionally, the smart contract is built in such a way that the locked funds can be used to integrate with the future bridges.
- Execute teleports in a total of **15 batches in two week intervals.**
- **This approach removes third-party code** (non-OriginTrail ecosystem) from the bridging infrastructure, additionally minimising the risk surface until a more trust-minimising solution is available.
- **The approach enables continued exploration of bridging solutions** within the Polkadot ecosystem for the mid- and long-term viability of a two-way TRAC bridge. It

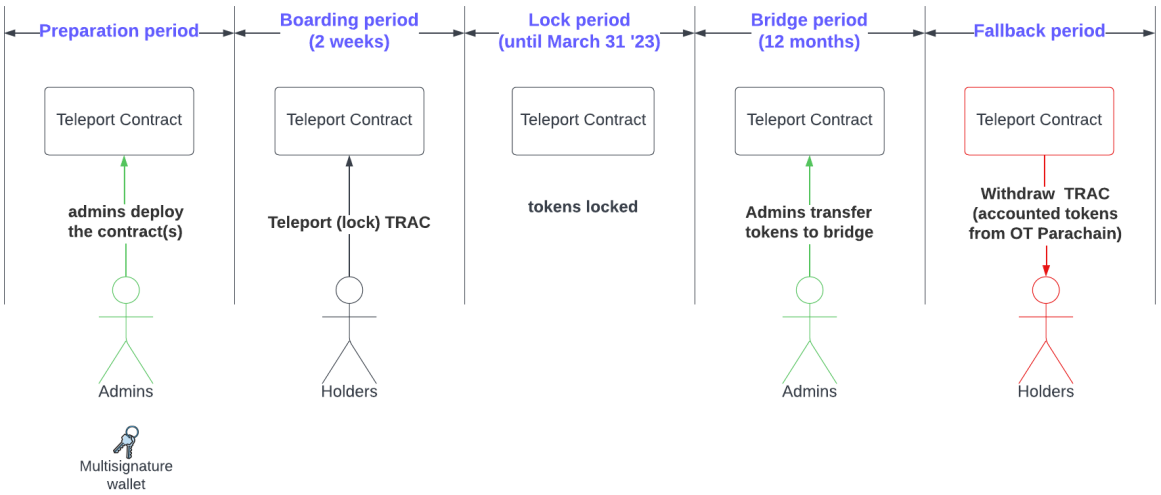
is expected that multiple options will be available, such as common-good parachain bridges, Snowfork and others, developed by the wider Polkadot community. Once a suitable bridge is available, all teleported tokens will be migrated (subject to the same RFC process as with this implementation).

Teleporting details

Teleporting will occur in 15 batches, each of which will be performed with a process similar to the previously executed Starfleet staking. Due to the nature of the smart contracts and them being audited and tested, only parametric changes can be implemented and no changes in smart contract code will be performed.

Each of the 15 teleportation batches will deploy a separate Teleport contract on Ethereum, managed by a multisig wallet. The illustration below shows the lifecycle of each Teleport contract and its phases as per smart contract design (specified in OT-RFC-10). There are 5 distinct periods defined in the life cycle:

- **Preparation period:** used for contract preparation and deployment on Ethereum mainnet.
- **Boarding period:** the period during which TRAC can be deposited in the smart contract for teleportation. The boarding period will last 2 weeks for each batch (except for the first batch lasting 3 weeks).
- **Lock period:** the period during which tokens are immobile (locked) in the teleportation smart contract on Ethereum. TRAC tokens are teleported to the OriginTrail Parachain and available for use with the same address as used for locking. Each lock period will be set to expire on March 31st 2023.
- **Bridge period:** the period during which locked tokens can be transferred from the teleportation smart contract on Ethereum to a fully fledged bridge implementation (which is expected to be available in the bridge period). The bridge period lasts for 12 months (latest until March 31st 2024).
- **Fallback period:** period used in the fallback scenario of a fully fledged bridge not becoming available, after all previous periods have expired. In this period it will be possible to teleport TRAC tokens back to Ethereum, using the accounting feature as described in the contract spec (OT-RFC-10).



To incentivize the teleportation process and utility of the OriginTrail Parachain and the (then deployed) OriginTrail DKG v6, a designated amount of OTP bounty tokens will be made available for the users (to be announced).

The teleport timeline is as follows:

- **August 18th (tentative):** first Teleportation contract deployment and Batch #1 teleporting start, the first boarding period lasting 3 weeks
- **September**: first minting of TRAC on OT Parachain, added OTP bounty to enable the use of the OriginTrail Parchain (bonus size TBD)
- **Mid-September**: Once TRAC is available, execute OriginTrail DKG v6 launch
- Batch #2 and further teleportation batches continue immediately after the first teleportation is completed and validated as successful

The detailed timeline will be shared in the following documents as soon as this RFC is approved.

Long term approach - multiple bridges

We expect a multitude of improvements as bridging infrastructure evolves to support more than one bridge on the OriginTrail Parachain. These will most likely include improvements in security models (trustless bridges), efficiency and user experience. It's important to note however that having multiple bridge systems bridging the same asset effectively creates multiple "mirror versions" of the same asset on the OriginTrail Parachain.

To enable a sustainable, long term evolution of the bridging infrastructure therefore 3 key considerations need to be applied from the start:

1. **Ensuring equivalence** of bridged TRAC tokens as they might need to be implemented as “different” assets on the OriginTrail Parachain - for example, a TRAC token bridged via Chainbridge and a TRAC token bridged via Snowfork might be two “mirror version” assets on the parachain, with essentially the same value (1 TRAC). Equivalence would involve enabling the OriginTrail DKG and other systems utilizing TRAC to register all TRAC mirror versions on the Parachain as the same (equivalent).
2. **Appropriate mirror asset naming** should be applied to avoid confusion, especially as these assets move across the Polkadot ecosystem.
3. **“Phase out” capability for mirror assets** in case of potential bridge issues (such as a major flaw being discovered), which would enable a safe decommission of potentially problematic bridges, ensuring TRAC tokenomics preservation.

Having these points in place while implementing the first bridge is important and already taken into consideration by the core development team.

Conclusion

This document presents an updated version of the original RFC based on the comments and feedback received from the OriginTrail community. It outlines the near and long term approach of enabling the utilization of TRAC token in the Polkadot ecosystem via the OriginTrail Parachain token, focusing on utilising a batched teleportation approach via a secure smart contract on the Ethereum side. We invite the OriginTrail community to provide their improvement proposals, comments and suggestions via the official RFC repository.