OT-RFC 10
Starfleet boarding (staking) smart contract specs

Document editors:

Document authors:

Branimir Rakić, Tomaž Levak, Žiga Drev, Jurij Skornik (Trace Labs)

Versions:

- 2020-12-16 (v1.1)
- 2020-12-01 (v1.0)
- 2020-11-11 (v0.1)

Table of contents

Abstract

The purpose of this document is to present the detailed technical specifications for the Starfleet boarding smart contracts, crafted by the OriginTrail core developers in order to enable the OriginTrail community to successfully board the newly launched Starfleet blockchain when ready.

Details of the Starfleet initiative have been described in previous OT-RFCs and this specific document focuses on the staking smart contract implementation. It is used for development and security auditing purposes.

Boarding mechanism explanation

In order to provide the necessary consensus layer functionalities for functioning of the ODN, the Starfleet blockchain needs to be provided with TRAC liquidity. Therefore to have the system operational at Starfleet genesis, the initial boarding process to Starfleet blockchain will take place in the form of a staking procedure, followed by the initial StarTRAC generation on Starfleet blockchain (at 1:1 parity).

The procedure consists of the following phases:

1. **Preparation period:** Participant registration and smart contract security auditing.
2. **Boarding period:** Staking TRAC to launch OriginTrail Knowledge Economy
3. **Starfleet launch window:** StarTRAC launched on Starfleet (at parity with staked TRAC on Ethereum mainnet).
4. **Bridge launch window:** With an active bridge, StarTRAC can be exchanged for TRAC and vice versa. Movements of TRAC between chains are enabled
5. **Fallback window.** In case of unsuccessful launch of the bridge, the token holders will be enabled to withdraw TRAC in the amount of their current StarTRAC holding on Starfleet blockchain at a designated Starfleet snapshot block, decided by the Trace Alliance Starfleet Task Force.

Smart contract requirements

The requirements in this document follow the IETF RFC 2119 recommendations for keyword requirement levels.

Functional requirements

- **FR1** Token holders SHALL be able to deposit TRAC during the boarding period, if the maximum staking threshold (MAX_THRESHOLD) has not been reached.
- **FR2** Token holders SHALL be able to withdraw their deposited TRAC if the minimum staking threshold (MIN_THRESHOLD_REACHED) has not been reached.
- **FR3** Token holders SHALL NOT be able to withdraw TRAC tokens during the Starfleet launch window and Bridge launch window phases.
- **FR4** The contract manager SHALL be able to transfer TRAC during BRIDGE_PERIOD for bridge deployment.
- **FR5** The contract manager SHALL be able to perform direct accounting of StarTRAC in the smart contract during the fallback period (if the bridge has not been successfully launched during the bridge launch window).
- **FR6** Token holders SHALL be able to claim StarTRAC and withdraw TRAC in the same amount during fallback period (if the bridge has not been successfully launched during the bridge launch window).
- **FR7** The contract manager SHALL be able to change ownership of the contract to another address for bridge deployment or security reasons.
- **FR8** The smart contract SHOULD NOT be able to receive ETH.
- **FR9** The contract manager SHALL be able to set boarding period start time (t_zero) at contract deployment.

Functional requirements overview for each period

Period	Activities during period	Functional requirements
Preparation period	Smart contract security auditing Smart contract deployment	**FR9**
Boarding Period, MIN_THRESHOLD not reached	Staking period, Withdrawal possible	**FR1, FR2, FR7, FR8**
Boarding Period, MIN_THRESHOLD reached	Staking period, Withdrawal no longer possible	**FR7, FR8**
Starfleet Launch Window	Starfleet blockchain launch, Launch of StarTRAC tokens in the amount of staked TRAC	**FR3, FR7, FR8**
Bridge Launch Window	Transporter bridge launch, Two way TRAC <> StarTRAC bridge crossing enabled	**FR3, FR4, FR7, FR8**
Fallback Period	Transporter bridge launch not successful, StarTRAC accounting performed by contract manager, TRAC withdrawal available for token holders	**FR5, FR6, FR7, FR8**

Non-functional requirements

- **NFR1** The Starfleet staking smart contract SHALL be deployed on Ethereum mainnet and referencing TRAC token at address 0xaA7a9CA87d3694B5755f213B5D04094b8d0F0A6F.
- **NFR2** The Starfleet staking smart contract manager SHALL utilize a secure multisignature wallet for contract management.
- **NFR3** The Starfleet staking smart contract SHALL utilize standardized, proven and security tested Solidity libraries.

Conclusion & Next steps

This document presents the specific functional and nonfunctional requirements for the Starfleet boarding smart contracts and is to be used as input for developers, security researchers and the wider technical community to provide feedback and improvement proposals. The corresponding code implementation repository will be hosted on the OriginTrail Github when available.