OT-RFC 07

Multichain OriginTrail Decentralized Network - Starfleet initiative

Proposed by:

Trace Alliance Decentralization & Tokenomics Working Group - Starfleet Task force

Document editors:

FamousAmos, Guinnessstache, Kirk, Milian, bbnm

Document authors:

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

Versions:

- 2020-10-12 (v1.1)
- 2020-10-11 (v1)
- 2020-10-10 (Draft 2)
- 2020-10-04 (Draft 1)

Summary

This document intends to introduce the next stage of OriginTrail Decentralized Network development called Starfleet. It explains the rationale and solution implementation steps required to achieve a multi-blockchain ODN for increased adoption potential and a more efficient ODN market. The solution introduces several new ecosystem components - the Starfleet Blockchain, Starfleet Transporter bridge and supporting ecosystem components and explains their interaction, development direction, governance structure and future exploitation potential.

Problem statement

The OriginTrail protocol has been designed to support and grow the global linked-data-first decentralized knowledge graph (DKG) to enable interoperable, trusted data exchanges. The OriginTrail DKG is therefore growing according to emerging W3C and GS1 standards to support multiple functionalities for DIDs, verifiable credentials and enterprise data sharing, supported by consensus-enabling protocols as the trust foundation in data exchange. As such, **the design of OriginTrail envisions a blockchain-agnostic approach for the long-term evolution of the technology** [1], being able to leverage the progress of blockchain ecosystems.

As the OriginTrail's adoption increased significantly, the reliance on a single blockchain implementation has at times presented challenges due to Ethereum network congestion. Although OriginTrail utilizes Ethereum in a minimal fashion, the sharp rise in the Ethereum gas market has caused the service costs to increase for the ODN node runners as well. To enable the OriginTrail Decentralized Knowledge Graph to take advantage of the growing multi-chain universe of solutions and decouple from a single blockchain service market, the core developers are now proposing an evolutionary path to achieving neutrality in the protocol's consensus layer as envisioned in the original OriginTrail whitepaper.

Proposed solution

In order to make the transition from one to many chains in the most efficient manner, the core developers propose a new multi-chain development phase, dubbed Starfleet (inspired by the famous series Star Trek and its interplanetary organization for conducting deep space exploration, research, defense, peacekeeping, and diplomacy), with an initial dual-chain protocol implementation.

The proposed solution incorporates a second, community-operated OriginTrail Starfleet chain, implementing a modified set of existing EVM smart contracts, alongside the existing implementation on the Ethereum Mainnet. The Starfleet chain is bridged with the Ethereum mainnet to ensure consistency in the incentive mechanisms, while the incorporation of multi-chain DID identity resolution and utilization of verifiable credentials data model enables the interoperable operation of the Decentralized Knowledge Graph within a multi-chain environment.

Starfleet chain will enable an effective decoupling from the gas market of Ethereum blockchain and evade dependency on any single blockchain "gas-like" market. It provides a parallel consensus solution that relies entirely on TRAC and significantly lowers the barrier for utilizing the services of the ODN. The incorporation of the Starfleet chain in no way hinders the functioning of the current ODN and is not a breaking change — it extends the choice of blockchains, adding a second option to Ethereum. Choosing to utilize Starfleet will be at the discretion of the OriginTrail Node runners willing to operate OT nodes together with Starfleet, based on their preference for different capabilities and characteristics of Starfleet and Ethereum.

Support for additional blockchains beyond Starfleet chain (e.g., the upcoming blockchain ecosystems such as Polkadot) will enable integrating the benefits of their respective functionalities in the OriginTrail consensus layer and further decoupling from a single ecosystem market, making the ODN a truly blockchain-agnostic solution. This proposal does not envision an increase in total Trace (TRAC) supply nor requires TRAC holders to perform token swaps from the Ethereum chain — TRAC remains ERC20.

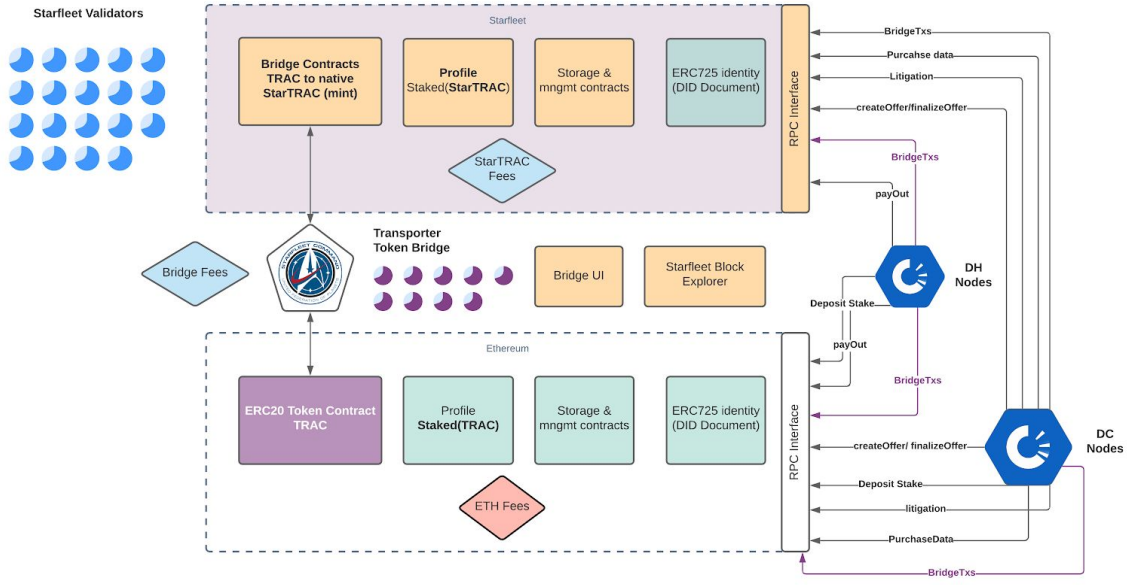
High level solution Architecture

The core ecosystem components:

1. **The OriginTrail Decentralized Network**, which is a permissionless, community operated peer-to-peer network of OT nodes hosting the Decentralized Knowledge Graph (DKG) based on the Verifiable Credentials and Decentralized Identifiers frameworks
2. **The Ethereum blockchain**, as the initially supported blockchain, accessible by the OT nodes through a user chosen Ethereum RPC service (such as Infura)
3. **The Starfleet blockchain**, as the second OriginTrail community operated permissionless blockchain, accessible to OT nodes via a community operated Starfleet gateway (RPC) service
4. **The Transporter Bridge**, which enables TRAC token transfer between the two chains, run by a set of community operators

Supporting ecosystem components:

1. **OriginTrail Network Explorers** - the Google like search engines for the public DKG, with data integrity validation tools
2. **OT Hub** - a community run OriginTrail Network activity monitoring interface
3. **The Starfleet Block explorer** - user friendly interface for Starfleet blockchain data
4. **Transporter UI** - a user friendly interface supporting the operation of the Transporter bridge
5. External components relevant to core components, such as **wallets**, **liquidity providers** and decentralized **applications** (e.g. Houston)



System operation description

The OriginTrail network nodes host the Decentralized Knowledge Graph within their local semantic data stores in the form of verifiable credentials and according to utilized data standards (such as GS1 EPCIS for supply chain visibility event tracking). The OriginTrail nodes exchange data in an open market, publishing data service requests as offers (by Data creator - DC nodes) to the other network participants (Data holder - DH nodes). ODN offers are objects on the blockchain which present an ask to perform actions such as decentralized dataset storing or purchasing, with associated parameters such as dataset metadata (DIDs), service conditions and necessary cryptographic material needed to ensure the service is trusted from the initiation phase to completion.

From the perspective of ODN nodes (DCs and DHs) it is important that the required service be performed in the context of the ODN, while there can be a multitude of blockchains used as channels for ensuring service conditions are met within the TRAC market available on that chain (TRAC on Ethereum, StarTRAC on Starfleet, or any other TRAC bridged market). It is expected that ODN nodes will be willing to participate in a multitude of blockchain markets in order to maximize the potential of their service utilization, while possibly choosing for preference at the time of operation (e.g. for lower cost, stronger security or performance differences). ODN nodes have the freedom to participate in multiple blockchain markets regardless of the blockchain they are initially set up on.

Starfleet technical implementation approach

Starfleet Blockchain implementation

Two approaches have been identified for the implementation of the Starfleet blockchain:

1. Utilizing the existing Ethereum client codebase together with supporting tooling
2. Utilizing the Substrate framework to build a custom blockchain with the EVM pallet

Both approaches allow the ODN to leverage the existing set of Solidity smart contracts used in the existing production Ethereum implementation which is advantageous for simplifying the implementation and consequently lowering the required resources in time for development. The protocol currently employs a set of Ethereum smart contracts in the consensus layer, which include ERC725 identity support, incentivization protocol contracts,

the Fairswap[2] data marketplace smart contracts, and contracts needed to support the DID/SSI infrastructure.

The OriginTrail Core developers and the Trace Alliance Starfleet Task force are actively investigating the two approaches and will determine the exact implementation direction in the following month.

The current findings indicate that:

- The Substrate[3] codebase (version 2.0 released on September 23, 2020) is built on the knowledge previously attained through years of development and iteration on the Parity Ethereum client and Substrate v1, making it a promising framework to build on
- The Substrate codebase would make OriginTrail integration with the Polkadot technology ecosystem significantly less complex and less time consuming, as the launch of Starfleet would be a midway milestone towards a Polkadot integration
- The existing OpenEthereum[4] codebase (formerly Parity Ethereum client) has a longer track record and is considered production ready, being utilized in a multitude of blockchains for a significant amount of time
- The OpenEthereum ecosystem has significant supporting tooling available

Since the recent joining of the Parity team in the Trace Alliance, the technical teams have been in communication and will continue collaborating to discover the optimal approach for the implementation route to be taken.

Impact on the ODN operation

The ODN requires blockchain for dataset and identity verification (as per the W3C DID[5] and Verifiable Credential[6] specifications) and service compensation, and observes blockchain as an external service and is agnostic to the underlying blockchain implementation.
The Starfleet blockchain is an additional extension to the OriginTrail Decentralized Network to provide an even more efficient alternative to the current blockchain implementation on Ethereum.The OriginTrail Decentralized Network OT node features are being extended to operate with Starfleet blockchain which will provide the same needed functionality as the current blockchain implementation on Ethereum.

The key difference in operation of ODN with Starfleet blockchain is that the required fees for utilizing the blockchain will be denominated in StarTRAC tokens, effectively enabling more of the service value provided to remain within the OriginTrail ecosystem. Additional performance improvements can be expected due to the ability of achieving higher throughput than Ethereum as the network is designed and optimised towards the needs of the OriginTrail Ecosystem.

The Starfleet Transporter Bridge

As the total number of TRAC will never exceed 500.000.000 of existing TRAC, it is required to enable it to be transferable across different blockchains. The function of the Starfleet Transporter bridge is to transfer TRAC tokens between the Ethereum blockchain and Starfleet blockchain. StarTRAC is an equivalent token on the Starfleet blockchain to the TRAC token on the Ethereum mainnet, having a value ratio of 1:1. The StarTRAC tokens can only be minted by locking an equivalent amount of TRAC tokens on the Ethereum side of the bridge.

The bridge is comprised of a set of smart contracts - the “escrow” on Ethereum locking TRAC tokens transferred to the Starfleet chain, and StarTRAC management contracts on the Starfleet blockchain which enable minting and burning of StarTRAC when parties using Starfleet decide to cross the bridge.

In order to utilize the Starfleet Transporter Bridge, a user friendly interface will be provided by the Bridge operators that enables users to perform bridge transactions from one chain to another. It's expected that the bridging operation will require a fee to perform the swap from TRAC to StarTRAC and vice versa due to the cost incurred by the bridge operators on both sides of the bridge, as well as for being compensated for the service.

Governance

Each of the core ecosystem components is governed by a separate group of entities.

- The OriginTrail Decentralized Network is operated by the OriginTrail node runners community (500+ estimated nodes at the time of this writing). The system is permissionless and anyone obtaining a sufficient amount of TRAC tokens can engage in the network, becoming a node runner
- The Ethereum blockchain is operated by the Ethereum community of validators operating on a proof-of-work probabilistic finality consensus, which is utilized in the ODN consensus layer
- The Starfleet blockchain will be operated by the Starfleet group of validators from the OriginTrail Community
- The Starfleet Transporter bridge will be operated by a group of Transporter validators from the OriginTrail community (different from the Starfleet blockchain validators)

It is important to note that each of the above ecosystem components is of a different nature and has a distinct threat model. To achieve separation of concerns and treath decoupling, each of the components will be operated by a different group of entities, in order to mitigate possible attack vectors.

The Starfleet blockchain

Validators on the Starfleet blockchain are members of the wider OriginTrail community. The Starfleet blockchain will operate on a combined Proof of Authority / Proof of Stake model (a Proof of Work type of algorithm would pose a security risk to the network, making it vulnerable due to its relatively small size, at least during the inception period). This scheme requires an honest majority ***2f + 1*** validators in the presence of ***f*** malicious validators[7]. Depending on the specific implementation (of the two scenarios outlined above) the details of the protocol will be specified, the most likely candidates being Aura and Babe/Grandpa protocols. Validators will be compensated for their activities by transaction fees in StarTRAC tokens on the Starfleet chain.

Two initial planned phases for the Starfleet blockchain evolution are proposed to make for a streamlined process of its development. Phase 1 will incorporate the launch of the network with a genesis state of a total of **N1 = 13** validators (tolerating up to 4 malicious nodes). Phase 2 will introduce an additional number of **N2 = 24** validators **reaching a total of 37** (tolerating up to 12 malicious colluding nodes) to further increase the resilience of the Starfleet chain once its utilization grows. Further updates to the validator list will be governed by the Starfleet on-chain governance tools enabling community driven decisions for the future state of the chain.

To provide a high level of confidence in the network, the **validators are to be publicly known, trusted entities** and they need to post a certain amount of stake in TRAC locked as collateral. This scheme eliminates the possibility of an unknown, potentially malicious actor becoming a potential validator in the network in case they have accumulated enough TRAC. The initial pool of validators will be proposed by the core development team.

The validators will be required to run a highly available service deployment and coordinated to achieve sufficient geographical dislocation in order to protect the network from potential service outages due to possible data center problems.

The intention is to have validators supporting the network be part of the OriginTrail wider community, which includes enterprises, the Trace Alliance and the TRAC holders community. The detailed mechanics of operation, including the process of validator group administration

(adding or removing validators), incentive structure and participation requirements are to be presented and discussed through further publications.

Chain access & utilization

In order to utilize the chain, two conditions must be met:

1. The user of the chain needs to be able to access the chain state and be able to run network RPC calls in order to perform actions needed (sending transactions and reading state). Access to the chain can either be provided by running a blockchain node by the user (a user can run a blockchain node, without having to be a validator) or via an external RPC service offered by a third party (such as Infura in the Ethereum ecosystem). The core development team will initially provide a Starfleet chain RPC service, while more such service providers might become available during the chain evolution (e.g. existing validators or third parties running Starfleet non-validator nodes might provide additional RPC service endpoints).
2. The user needs to "cross the bridge" by transporting a sufficient amount of TRAC tokens (and receiving StarTRAC tokens on the Starfleet chain) to be able to utilize the Starfleet chain.

The Starfleet Transporter Bridge

The Transporter bridge is one of the core components of Starfleet, with its own governance structure and roadmap of development. As with the Starfleet chain validators, the Transporter bridge operators are to be publicly known trusted entities that will operate the bridge in a transparent manner. The initial group of bridge operators are to be picked by the core development team, which will present the details of operation and initial number of bridge operators in further publications based on the decided Starfleet implementation approach.

Reward distribution

The rewards for validators running the starfleet blockchain and starfleet transporter bridge are paid out by the users of the systems as fees in the StarTRAC and TRAC tokens. The exact fee structure is to be determined during the development process depending on the specific implementation, and will be estimated based on the system running cost (in case of the Starfleet blockchain, the costs of running blockchain nodes).

Starfleet Blockchain network launch

To launch the Starfleet blockchain the Trace Labs team will coordinate a launch of a Starfleet canary network with the initial group of validators together with the initial Transporter bridge implementation for the purposes of testing and validating the implementation, reaching system TRL7[8] (expected in Q4 2020). After a period of testing and proving a sufficient level of system maturity the Starfleet mainnet chain & Transporter Bridge launch will be coordinated with the validators to achieve system TRL8 (expected in early 2021). With the TRL8 infrastructure in place, the core development team will release the 5.0 version of OT node, supporting operations on both Ethereum and Starfleet chains in both testnet and mainnet networks.

ODN v5 - Multi-chain ODN connected with Starfleet blockchain

Required OT-node updates

The current implementation of the OT Node Blockchain service is implemented in such a way that the OT node can listen and communicate with one blockchain at a time, but having the system prepared to a large degree to support multiple blockchains. The Starfleet release of the OT node requires that this be updated, meaning that a node should be able to listen to and communicate with multiple blockchains simultaneously.

The solution is to improve the decoupling of blockchain features from other services of the node and move more logic away from specific blockchain implementations and into the generic blockchain service.

The proposed solution has three main sections:

1. Communication of the blockchain service with specific implementations
2. The internal architecture of the blockchain service
3. Communication of the blockchain service with other node modules and services

The specifics of this effort are explained in detail in another RFC document which will be circulated in Q4.

Security considerations

The implementation of Starfleet and v5 OT node is an extension to the existing ODN model of operation with the Ethereum network, which introduces additional security assumptions

for the users intending to utilize Starfleet. Users who choose not to participate in Starfleet (which is a perfectly valid choice) can rely on the same set of security assumptions offered by the Ethereum implementation.

As aforementioned, the trust assumptions of Starfleet are that:

- There should be less than ⅓ of malicious colluding validators in the Starfleet blockchain
- The users of Starfleet inherently decide to trust the bridge operators to perform their token swaps in both directions of the bridge

Both of these trust assumptions are necessary to operate the system as outlined above and are to be minimized through the development of the ecosystem by introducing additional parties in the operator and validator groups to achieve extended decentralization. Upcoming ecosystem developments are expected to provide additional trust minimization (e.g. the upcoming development of solutions such as the Parity Rialto Trustless bridge[9])

Future directions

The proposed solution above is intended to bring the ODN to the envisioned blockchain agnosticism and to mitigate the observed problems in the technical ecosystem, as explained in the problem statement. Additionally, Starfleet aims to be the midway point in the potential integration of ODN with the emerging ecosystem of Polkadot, which is a topic under active exploration of the Trace Alliance Decentralization and Tokenomics Working Group Polkadot task force[10], which at the time of this writing consists of Parity and Trace Labs team members. The group is expected to leverage the findings and experiences of the Starfleet task force in order to produce a direction for an impactful implementation for both the OriginTrail and Polkadot ecosystems and this knowledge to be reused for subsequent multichain implementations.

References

1. *OriginTrail Whitepaper (https://origintrail.io/storage/documents/OriginTrail-White-Paper.pdf)*
2. *Fairswap - How to fairly exchange digital goods - Stefan Dziembowski (Institute of Informatics, University of Warsaw), Lisa Eckey,Sebastian Faust (Department of Computer Science, TU Darmstadt) [https://eprint.iacr.org/2018/740.pdf]*
3. *"Substrate 2.0 is here" - Phil Lucsok (https://www.parity.io/substrate-2-0-is-here/)*
4. *OpenEthereum Wiki (https://openethereum.github.io/wiki/)*
5. *W3C Decentralized Identifiers (https://www.w3.org/TR/did-core/)]*
6. *W3C Verifiable Credentials Data Model (https://www.w3.org/TR/vc-data-model)*
7. *Reaching Agreement in the Presence of Faults, M. Pease, R, Shostak, and L. Lamport, SRI International, Menlo Park, California*
8. *Horizon 2020 – Work programme 2014-2015 General Annexes - Technology Readiness Levels (TRL) (https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf)*
9. *Substrate Seminar - Trustless Bridges, Hernando Castano. [https://present.readthedocs.io/en/latest/gallery/trustless-bridges/]*
10. *Parity Technologies joins Trace Alliance's working group on decentralization and tokenomics (https://medium.com/origintrail/parity-technologies-joins-trace-alliances-working-group-on-decentralization-and-tokenomics-8eaad2843ca7)*