Dusk Network Governance Paper

Toghrul Maharramov
Dusk Network
toghrul@dusk.network

Jelle Pol
Dusk Network
jelle@dusk.network

March 8, 2021
Version 1.0.0

Abstract

This paper outlines the governance procedures for the privacy-oriented blockchain-based generalized compute protocol called *Dusk Network*. Specifically, the paper outlines the off-chain and on-chain governance procedures and the scope of the aforementioned two procedures.

1 Overview

Dusk Network [MKF21] is a privacy-oriented blockchain-based permission-less protocol which facilitates the deployment of quasi-Turing complete smart contracts with native support for zero-knowledge proofs and the accompanying zero-knowledge proof-friendly primitives. Concretely, the protocol was primarily conceived with regulatory compliant security tokenization and lifecycle management in mind.

Dusk Network[1] is comprised of the *Business Team* responsible for defining and executing the use cases for the underlying protocol (i.e. the Dusk Network protocol) as well as for deciding on the allocation of the company funds[2], and the Core R&D Team responsible for the implementation of the primitives capable of facilitating the aforementioned use cases within or outside the scope of the protocol. The *Core R&D Team* retains autonomy with regards to the technical decisions as long as the said decisions do not contradict the use cases defined by the Business Team.

2 Off-Chain Governance

Off-chain governance can be conceptually separated into two distinct categories:

1. *the Dusk Network protocol governance* and

[1] Denotes the legal entity from hereon, unless stated otherwise.

[2] https://dusk.network/uploads/Dusk-Network-Biannual-Report-2020.pdf

2. *the Dusk Network Development Fund governance.*

The former is under the oversight of the Core R&D Team, which is responsible for making amendments to the reference Dusk Network protocol specification, either in form of bug fixes or protocol upgrades. Specifically, the amendment decisions are predominantly based upon the protocol improvement proposals, the structure of which closely adheres to the RFC[Cro69] format. The protocol improvement proposals can be submitted by anyone.

The latter, on the other hand, is under the oversight of *Dusk Network Governance Council*, a community governance committee responsible for allocating funds to issues outside the scope of the reference protocol, such as wallet implementations, research efforts focusing on a specific problem, etc. The committee structure and election procedure is based upon the process outlined in [Cin19]. The Dusk Network Development Fund is community-funded through the procedure presented in [Mah20]. The aforementioned paper specifies that $\frac{1}{10}$ of the total block rewards from the Dusk Network Mainnet are allocated to the Dusk Network Development Fund, which is instantiated as a multisignature contract on the Dusk Network Mainnet. Dusk Network reserves the right to provide additional funding to the contract if a need arises.

3 On-Chain Governance

The protocol upgrade procedure is accomplished via an on-chain procedure derived from [Goo14]. Specifically, via a staking contract $\mathsf{Contract}^{\mathsf{Stake}}$ utilized to track the latest set of eligible Provisioners $\mathsf{Provisioners}$ as well as for the accounting of the deposits and the withdrawals of eligible stakes. The Dusk Network protocol versioning is defined with semantic versioning [Pre] comprised of three numbers denoted as major, minor and patch (e.g. `version 1.0.0`). Each valid stake stake includes a field defined as $\mathsf{version}$, which denotes the protocol version deployed on the device of the Provisioner in the possession of the secret key sk corresponding to the public key pk specified in the aforementioned stake. If $\geq \frac{3}{4}$ of the active amount of DUSK staked (equivalent to the total amount staked by the Provisioners eligible to participate in the consensus) are operated on a device running a protocol version with greater major or minor than the one recorded in the contract, then the protocol is to initiate the upgrade.

4 Future Work

The team at Dusk Network strives to achieve the balance between governance decentralization and efficiency. As a result, we are exploring the possibility of deprecating the Dusk Network Governance Council in favour of a Decentralized Autonomous Organization [Wan+19] in the future.

References

[Cro69] S. Crocker. *RFC 1*. 1969. URL: `https://tools.ietf.org/html/rfc1`.

[Goo14] L. M. Goodman. “Tezos : A Self-Amending Crypto-Ledger Position Paper”. In: 2014.

[Cin19] Josh Cincinnati. *The Zcash Foundation Community Governance Process*. 2019. URL: `https://github.com/ZcashFoundation/Elections`.

[Wan+19] Shuai Wang et al. “Decentralized Autonomous Organizations: Concept, Model, and Applications”. In: *IEEE Transactions on Computational Social Systems* PP (Sept. 2019), pp. 1–9. DOI: `10.1109/TCSS.2019.2938190`.

[Mah20] T. Maharramov. *Dusk Network Economic Model Paper*. 2020. URL: `https://dusk.network/uploads/Dusk_Network_Economic_Paper-v1.01.pdf`.

[MKF21] T. Maharramov, D. Khovratovich, and E. Francioni. *The Dusk Network Whitepaper*. 2021. URL: `https://dusk.network/uploads/The_Dusk_Network_Whitepaper_v3_0_0.pdf`.

[Pre] T. Preston-Werner. *Semantic Versioning 2.0.0*. URL: `https://semver.org/`.