Dusk Network Preliminary Economic Model

Toghrul Maharramov
Dusk Foundation
toghrul@dusk.network

March 29, 2019

Abstract

Dusk Network is a permission-less and anonynimity-preserving blockchain protocol which enables both the transactional and computational changes to its state. The document defines an economic model of the Dusk Network protocol which will be made available during the preliminary launch of the public testnet. The model also specifies the the use of the Guru module and the slashing conditions.

1 Introduction

Ever since the first conversations about a distributed ledger took place in closed circles of cryptographers more than two decades ago, a search for a viable economic model for these databases has been rampant. When Satoshi Nakomoto published the infamous Bitcoin whitepaper, he (in reality, the identity of Satoshi Nakomoto is unknown, so the paper refers to the public pseudonym of the author of the paper as "he" rather than the identity behind it) introduced a concept of mining in which a user is rewarded for successfully solving a computationally-difficult problem (Hashcash Proof-of-Work algorithm, in this particular case) with newly minted digital currency (Bitcoin). Bitcoin is limited to only 21 million "coins" the emission rate of which halves every 4 years. Multiple alternative economic models (informally called "cryptoeconomics) have been proposed since the inception of Bitcoin. Ethereum, for example, has an unlimited supply of "coin" and currently rewards the "miner" who has managed to successfully solve the Proof-of-Work problem for a particular block with 2 Ether as well as rewarding the authors of "ommer blocks" (the blocks which are not included in the current longest chain). Monero has a "tail emission" model which continues to mint a small amount of "coins" (0.6 XMR) after the predetermined "total supply" (18.4 million XMR) has been "mined". Zcash's economic model includes a 10 percent "founders' reward" which provides the founders with a cut of the newly minted "coins".

2 Block Rewards

Dusk Network has a total supply of 1 billion DUSK "coins", which includes 500 million "pre-mined" DUSK and 500 million DUSK intended for the "miners". For the first 10 million blocks (roughly 9.5 years), each successfully forged block is going to be rewarded with 25 DUSK which will be followed by a declining emission rate of 20 percent per year until a base reward of 5 DUSK per block is reached. The logic behind the aforementioned model is that the block rewards alone are going to be enough of an incentive for the network participants to secure the blockchain in the beginning and, as the adoption increases, become more dependant on the transaction fees rather than the block rewards. However, as experienced with Bitcoin, even 10 years are not enough to make the protocol self-sustainable without block rewards, so the team has decided to prolong the emission to increase the probability of a mass-scale adoption. The block reward is going to be divided in three categories: Block Generator's reward, Provisioners' reward and Developers' reward. Block Generators are going to receive 10 percent of the total block reward. 80 percent of the block reward is going to be split between the Provisiors that have notarized the successfully forged block. Finally, another 10 percent of the total block reward is going to be awarded to the Developers' Fund, controlled by Dusk Foundation, to help preserve the long-term stable funding for continious research and development of the protocol.

3 Bids and Stakes

Both the bids and the stakes require an introduction of an upper and lower boundary to prevent the adversaries from gaming the protocol. Being obfuscated, bid amounts can be proven to be within the aforementioned boundary using an in-house developed zero-knowledge proofs for arbitrary value range proofs. Any stakes that do not fall within the predefined boundaries will be rejected by the network during the initial stake transaction propagation.

4 Guru

Guru is a reputation module which is utilized by Dusk Network protocol to further improve the resilience of the consensus mechanism. The reputation module effectively acts as a virtual stake multiplier which decays after as the time since the particular multiplier has been applied elapses. The exact parameters of multipliers and decay times will be determined during the public testing of the protocol.

5 Slashing

As with Slasher introduced by Ethereum, Dusk Network protocol utilizes slashing conditions as a deterrent to ”nothing-at-stake” attacks as well as other types of Provisioner misbehaviour. No new block can be successfully ”mined” if a slashing condition is triggered by a Provisioner, until the so-called ”slashing transaction” is included in the following candidate block. The stake of the Provisioner is instantly slashed if a ”double-vote” at any point during the run of the consensus.