

DeStake - Liquid, Incentivised Staking

December 2020

<https://destake.io>

Twitter: @DestakeHQ

Telegram: <https://t.me/DeStakeHQ>

Table of Contents

Technology

[Overview](#)

[Core Components](#)

[Staking UI](#)

[Staking Smart Contract System](#)

[Synthetic Assets](#)

[Lending Protocol](#)

[Incentive System](#)

[User Functions](#)

[Staking and Receiving Synthetics](#)

[Managing Rewards](#)

[Using Synthetics](#)

[Unstaking](#)

[Implementations](#)

[Roadmap](#)

Governance

[Networks](#)

[Network Integration](#)

[Lending](#)

[Funds](#)

[Rewards](#)

[Upgradeability](#)

Token

[Distribution](#)

[Economics](#)

Introduction

Our Mission is to increase decentralised participation in the securing of proof of stake blockchains and use derivatives to create liquidity.

Proof of Stake Networks are the blockchains of the future due to being exponentially more scalable and environmentally friendly; however, they rely on the active participation of thousands of users all over the world to remain decentralised and secure.

Currently, an alarming amount of staking power is coming from major exchanges. This poses a threat to the decentralisation of these proof of stake blockchains. Exchanges are a more user friendly option because they bypass any lock-up periods and allow users to trade, lend, or otherwise use (within the exchange platform) the tokens while they are staked. Decentralised solutions cannot currently compete with this because no equivalent solutions for providing liquidity exist.

This is why we are creating DeStake.

To solve this and compete with centralised exchanges, DeStake has taken a creative approach and has incorporated an incentive model using a native governance token, paired with the issuance of synthetic assets.

It works simply. Users stake ETH (or any supported token) on the DeStake platform and in return, receive synthetic assets such as ETH2 (sETH2). Thus solving the liquidity crisis of staked ETH being locked and inaccessible for ~2 years in the case of Ethereum and many other projects with lock-up/unbonding periods.

Synthetic assets have many uses. They can be traded (on UniSwap), used on lending platforms to receive interest or to borrow against, or providing liquidity to UniSwap Pools such as sETH/ETH and receive the DeStake Governance Token in return for staking their LP tokens.

This creates much added value out of locked staking assets. Instead of traditional staking models where users just receive staking rewards, with DeStake users receive staking rewards + governance token rewards, lending APY, or some other creative form of monetisation they may have constructed.

As we saw with the rapid growth of users in DeFi, we hope this first iteration of a staking incentive model triggers the explosion of proof of stake.

Market Size

As of September 2020, the **Market Size** of staked assets was \$14 Billion. With the launch of ETH2 phase 0, an additional ~\$60 Billion at the time of this writing becomes available for staking. It is projected that there will be \$100+ Billion in staked assets by 2022.

DeStake's Core Goals

Goal 1: Compete with exchanges.

Goal 2: Drive new user participation in staking.

Goal 3: Create Liquidity to efficiently utilise capital.

Technology

Overview

We have designed the DeStake liquid, incentivised staking platform in a way which focuses on security first, with a strong focus on UX and overall usability. Our intention is for it to become a catalyst which initiates a massive migration away from staking on centralised exchanges by providing equivalent services such as being able to trade and lend staked assets. We achieve this in a decentralised manner through the use of synthetic assets. And second, capitalises on the built-in incentive system to drive new users to participate in staking, much similar in many ways to the growth hacking technique of liquidity mining among DeFi protocols which lead to rapid, parabolic growth.

Core Components

Staking UI

The user interface to interact with the liquid, incentivised staking smart contracts. This is maintained by TokenWeb.

Staking Smart Contract System

The decentralised, liquid, incentivised staking application(s). This is where the governance tokens, the reward system, and the lending protocol all live. It is fully managed by on-chain governance by holders of the DeStake Governance Token.

Synthetic Assets

Equivalent of staked assets, received when depositing native tokens to staking contract. Burnt, when withdrawing native tokens back to your local wallet. For example: when ETH is deposited, an equivalent amount of sETH2 (Synthetic ETH2) is automatically minted and transferred to the users wallet.

Lending Protocol

This is based on Compound Finance and enables the lending of synthetic assets in return for receiving interest from borrowers, as well as makes using synthetics as collateral for borrowing against possible.

Incentive System

On a protocol level, this is designed to create deep liquidity among synthetic - native trading pairs. Users receive the DeStake Governance Token in exchange for depositing liquidity in

approved (via on-chain governance) pairs such as sETH2 - ETH, sGRT - GRT, sGRT - ETH, etc. From a business standpoint, this reward system should drive exponential growth in the staking sector as occurred in the DeFi sector during summer 2020.

User Functions

Staking and Receiving Synthetics

Graphic: User sends native token to staking contract, receives back synthetics. Native token delegated to validator(s) (based on on-chain governance). Rewards begin accumulating.

Managing Rewards

Single-token reward systems are straightforward. This is where the reward token is the same as the staking token. Under these models, which are currently the most common, users simply begin accumulating synthetic reward tokens which they can withdraw at any time. For example, users stake GRT and receive sGRT. As rewards are generated in the native token, an equivalent amount of synthetics are being minted and distributed to simulate the native rewards. These are the same exact synthetics as received when initially depositing into the staking contract and can be redeemed at a 1:1 ratio (by interacting directly with the contracts) or at a rate determined by price discovery on the free market such as UniSwap.

While on the native chain, reward tokens are most commonly distributed every block. Depending on the network, DeStake implementers may choose to batch these withdrawals to mitigate gas costs. For example, instead of every block, every hour or day rewards would be batched together and synthetics issued. At this time native tokens are auto-compounded at the moment the equivalent synthetics are issued (this is where the 2 transactions in 1 block discussed next becomes important). This makes sure rewards stay in sync with the actual native token balances.

We most likely will have to assess a fee to users here to cover the gas costs for doing this -> we need to run higher gas costs to ensure that both transactions are included in the same block so natives and synthetics stay in sync. If they are not included in the exact same block, it is not the end of the world. The amount differences would be extremely minimal and possibly even beneficial (more than stated) depending on which transaction was picked up in an earlier block.

Using Synthetics

Borrowing : Deposit tokens in the DeStake Synthetic Lending Platform to use their value as collateral to receive peer to peer loans in any supported cryptocurrency (determined via on-chain governance)

Lending : Using the DeStake Synthetic Lending Platform, users can receive interest by securely loaning their synthetic tokens to others.

Providing Liquidity to earn Governance Token : This is the most interesting case, which we expect a majority of users to participate in. Users can receive the DeStake Governance Token simply by depositing their synthetics along with a native asset into a supported uniswap pool (chosen via on-chain governance).

Once users provide the liquidity, they receive UniSwap Pool Tokens. We refer to these commonly as uniswap LP (liquidity provider) tokens. Next, they stake these LP tokens on the DeStake interface to begin accruing Governance Tokens every block (amounts determined via on-chain governance). Uses of the Governance Token are expanded on in detail in the Governance and Token sections of this paper.

Trading Synthetics

Users can choose to trade synthetics for any asset with liquidity on uniswap (synthetics or natives). There can be a variety of reasons for users to do this such as: hedging positions, exiting staking positions, liquidating rewards while maintaining their staking position, and so forth. We believe this will be extremely common as it is more user friendly for users who wish to exit staking positions partially or completely because it bypasses any unbonding/lock-up periods. Additionally, people using staking as a form to generate passive income will be able to sell their reward tokens instantly while maintaining their staked position.

Unstaking (by Burning Synthetics)

Most commonly we believe that when a user chooses to unstake, they will simply sell their synthetic equivalents to another party who is interested in taking over their staked position and associated future rewards.

However, if someone chooses to unstake their own tokens, they must burn the synthetics. To initiate this process of unstaking their assets, they first send their synthetics back to the staking contract where they are automatically burnt. This will call the native chain function to initiate any unbonding or lock-up period. As soon as the unbonding begins, rewards stop being generated.

We cannot keep the synthetics liquid during the unbonding period, as it can create many potential issues such as users trading synthetics during unbonding, reward - balance mismatching, native tokens in limbo in the contract, etc. These risks are all mitigated by requiring synthetics to be deposited to the staking contract to begin this process.

Once the unbonding is completed, the native tokens become available for withdrawal.

Design approach. We need to place some restrictions on the ability to withdraw tokens. If there were no restrictions other than User1 is eligible to withdraw x tokens and User2 is eligible to

withdraw y tokens, then it could create an almost front-running type of environment. For example if User1 begins unbonding 100 tokens today and they take 21 days to mature. User2 could in theory begin unbonding any value up to 100 tokens on Day 22, such as 50 tokens and instantly claim them from the staking contract is User1 has not done so yet. This could be done continuously by more savvy users who can design bots and algorithms to automate this. To prevent this we created a simple time-lock requirement. The user is not eligible to call the withdraw function until the unbonding period is reached. For example, if the unbonding period is 21 days, the user will not be eligible to withdraw anything until after 21 days. We acknowledge there are most likely better ways to implement this, especially at scale; however, this solution works adequately and is very simple to implement - simple implementations typically mean a lower margin of risk for technical bugs as well.

Implementations

The first release will be for GRT, The Graph's native token used for indexing and curating subgraphs. All of our outlined components above work perfectly for this integration. The Graph also has a vibrant community of thousands of active participants which make this ecosystem the perfect launchpad.

Future Releases

KyberDAO - Same Implementation, except rewards are paid in ETH. KNC is staked, sKNC is issued. Rewards being in ETH requires some slight re-working, but it can simply be implemented by having rewards issued as sETH to the same account as the sKNC. Although, we will work towards designing a solution with better UX, so users do not have to manage 2 separate tokens and sign twice as many transactions.

ETH2 - Same implementation, except for key management. Validators must generate 2 keys. A withdrawal and a signing key. We need to develop a system where the user generates the keys themselves and securely shares only the validator signing key with us. This way it is non-custodial where we can validate on behalf of the user, but have no control over their funds. We will outsource the development of this key generation and sharing system to a company who specialises in key security with a long-standing reputation.

Cosmos - This requires quite a re-working due to being a non-native chain to the original Ethereum-based dapp. We still have much research to be done to design a production-level solution for the Cosmos ecosystem, but it is definitely possible. We imagine it to exist on it's own application-specific cosmos-based blockchain as a dedicated liquid staking app that can easily be applied to any cosmos zone which is integrated with IBC. Additionally, (we have not tested this), the release of Ethermint (running EVM apps on Cosmos chains), may allow for the solidity codebase from the original app to be re-usable. If bridge solutions mature, maybe the Cosmos App can be directly integrated with the Ethereum based-app. As you can see Cosmos holds great potential with what can be done, but there is so much new technology coming out every

month there is much research that still needs to be conducted to effectively produce the application for this ecosystem.

Polkadot - this is planned, although we have not begun any substantial research on this implementation.

Roadmap

Phase 0: Destake launched to support Launch Partner Project

Phase 1: Governance Token Incentive Rewards for providing liquidity begin.

Phase 2: Lending Platform Released

Phase 3: Community Governance Begins and Admin Key Destroyed.

*initially DeStake is launched in a centralised way where the developer team has control over the application. This is because no Governance Tokens will have been distributed yet, so on-chain governance is not a possibility. This also allows for very quick updates to be made by the dev team if any vulnerabilities are found when released into the wild. The developer team's goal is to decentralise this ownership of the DeStake application as quickly as possible; therefore our goal is to begin the phase 3 migration to full community governance within 12 weeks of launching phase 0.

Phase 4: Continued Network Expansion. This is done via DeStake's upgradeability feature via on-chain governance, where new network contracts can be voted to be added into the master staking dapp. Governance Token holders approve networks, distribute funds from the community fund to cover integration costs, and vote on reward incentives.

Governance

Networks

Networks - The smart contracts/updates associated with any new network integrations will be voted on.

Synthetics - When a new network is approved, issuing synthetic assets for it must also be approved.

Validators - By default TokenWeb's validators will be the single validator which staked funds are distributed to when Phase 0 is launched. Additional validators can be added via governance by supplying their associated delegation address and opening a proposal to add them. (Staked assets are automatically evenly distributed among validators, there is no option to have dynamic percentage allocations on a per validator basis). Likewise, validators can also be voted to be removed.

Network Integration (Flow)

Approve Network (Staking + Synthetics)

Approve Dev Budget from community fund for integration

Approve Codebase after development

Approve DGOV incentives for Pool

Approve Synthetic to add to Lending

Lending

Synthetic assets must be approved to be added to the DeStake Synthetic Lending Platform.

Funds

Withdraw amount from community fund. Specify amount, recipient, and reason (txt). It would be common for this to be conducted for network integrations, security, platform maintenance expenses, and marketing related tasks.

Rewards

Add/Remove Pool pairs i.e sGRT - ETH , sGRT - GRT, etc. and liquidity reward amounts.

Change/Stop Reward Amounts (Frequency can be pre-set to automatically be distributed each block - users withdraw manually and pay their own gas costs, otherwise it is not sustainable).

Upgradeability

The contracts will be designed in a way where any new network addition can be completed via on-chain governance in a decentralised manner without the use of any admin keys. For example, a potential model is where there is a management contract which manages all specific network/project smart contract systems and allows them to participate in the reward system (a separate contract). This design is still evolving and will be reviewed by many experts prior to implementing.

Token

Distribution

5% to TokenWeb (Dev Team)
5% to Seed Investors/Launch Partners
90% to Rewards, managed on-chain.

Economics

Value of Governance Token

It is designed as a valueless governance token. If it does miraculously have any value then it will act as a form of rebate for those who delegate their tokens. For example: If a user pays a validator fee of 10% and is receiving an APY of 12% from DGOV tokens, then their effective validator fee is -2%. Pretty cool, eh?

Community Fund

10% of all Governance Token Rewards are automatically distributed to the community fund. This is fully managed on-chain by governance token holders and used to cover expenses such as platform maintenance, network integrations, feature additions, grants, marketing, etc.

Grants

In an effort to limit withdrawals from the community fund to a minimum, TokenWeb plans to actively seek grants from established proof of stake projects to cover integration costs and expand the DeStake network rather than pulling funding from the community pool. Anyone or company can follow this model to grow the DeStake Ecosystem.

Final Thoughts

We hope that you join us in our mission to ensure staking remains decentralised.

For more information please visit our [Site](#)
To Join the Conversation go to [Telegram](#)
To contribute to the project head over to [Github](#)

Disclaimer(s):

USA users not allowed. IP blocking and clear terms pop-up.

Staking is high-risk. Synthetics are high-risk. Use DeStake at your own risk.

Do not invest more than you are willing to lose. Cryptocurrencies are highly volatile and can lead to significant losses.