dApp Man's Switch

Litepaper

Markus Böck Elias Datler Philipp Lenz Dominik Russo

Version 1.0
March 2022

dApp Man's Switch is a decentralized dead man's switch that runs on the Internet Computer blockchain.

main usecase The main usecase is for users to upload secrets which will not be revealed until the user fails to prove that they are still alive for a set period of time. The uploader of a secret can specify 4 parameters on a per-secret basis: **(1)** The size of the interval in which they have to prove that they are alive, also called the heartbeat frequency. **(2)** The amount of users they want involved protecting the secret. The higher this number the higher the price of uploading the secret. **(3)** The expiration date of the secret. After this date uploaders don't have to prove that they are alive anymore and the secret will not be revealed. **(4)** Whether they would want the secret revealed publicly or only to select recipients.

For a concrete example let's assume Edward is a whistle-blower who has highly sensitive information and there is some organization that would go as far as kidnapping or killing him to prevent the information from being published. If Edward uploads the information to dApp Man's Switch, the organization would be implicitly publishing the information if they tried to incapacitate him. Edward would want to choose a short heartbeat frequency (1 day), provide a high reward to have more users safeguarding the secret, set the expiration date long enough into the future for him to accomplish what he set out to do and choose a public revealing.

Another common usecase example might be passing on inheritance information, keys to crypto wallets or master passwords to password managers after one's death. In this case the heartbeat frequency would be very long, maybe 1 year, the amount of users involved in keeping the secret could be chosen much smaller than in Edward's case, the expiration date as long in the future as possible and the secret should only be revealed to select recipients.

DeFi usecase The second use case concerns decentralized finance (DeFi). The way the secrets are safeguarded (conceptually) is that stakers of our heartbeat token (HRBT) receive small encrypted parts of a secret and are given HRBT as rewards for publishing them when the service tells them to. When the smart contract receives enough of these parts it can reconstruct the original secret and publish it.

Tokenomics

faucet Each internet identity anchor will be eligible to receive a small amount of HRBT, enough to upload a secret and create a small stake. This should lower the barrier of entry for participation and prevent few users from controlling the vast majority of the tokens. The amount of HRBT that can be claimed will be directly proportional to the amount of HRBT in the treasury, so it is expected to decrease over time. More on the treasury in a bit.

sacrifice phase and airdrop

During the sacrifice phase users can send cryptocurrency to our wallet to be the first to receive HRBT. We will be using a decreasing value multiplier, so the earlier in the sacrifice phase the sacrifice is made the higher it's value. After the sacrifice phase ends, 25% of the total supply of the HRBT token will be distributed amongst the participants in form of an airdrop. The proportion they each receive depends on the ratio of their sacrifice to the total amount sacrificed, taking into account the multipliers. The cryptocurrency we receive through the sacrifice will later be used to provide liquidity.

The motivation behind hosting a sacrifice phase is twofold: Firstly, the sacrifice serves as an opportunity to reward the commitment of early users. And secondly, the total value sacrificed determines the initial value of one HRBT token.

providing liquidity

After the initial distribution is completed, we will enable users to buy the HRBT token in our dApp directly. In addition to providing liquidity centrally, we also want to encourage holders of the token to create liquidity pools on decentralized exchanges (DEX) on the internet computer (e.g. Sonic, ICPSwap) which should further stabilize the token's price.

premature unstake penalty

If a staker wants to end their stake before it's due they will be penalized. This is to discourage stakers that were entrusted with secrets from abandoning the service while the encrypted partial secrets they hold are not yet expired. The panalty is calulated through a loss function, which decreases exponentially the nearer the stake's expiration date is. So if a staker is determined to unstake prematurely the most beneficial thing to do would be to postpone the unstaking as long as possible.

Of the tokens lost through the premature unstake penalty half will be distributed amongst other stakers relative to their stake size and the other half will go into the treasury.

treasury

The treasury is the wallet containing the HRBT that will be sold to users centrally and will be the source of the faucet. It will start out with 50% of the total token supply, but this will decrease until the faucet drain and the purchasing through the centralized exchange balance out with the premature unstake penalties.

Below are illustrations of the initial token distribution and the assumed equilibrium state.