Hashrate Protocol

TECHNICAL PAPER

V1.0

info@zionodes.com

January 2023

Abstract

This document contains a fundamental overview of the Hashrate Protocol, the definitions, and its architecture, as well as an introductory note of the solutions to problems and opportunities it unveils.

Contents

1. Introduction

Hashrate Protocol is a PoW-based protocol to issue lending-permissible assets collateralized by redeemable hashrate power. The protocol shifts a paradigm of miner financing to a permissionless pool-based strategy unlike centralised loan services or P2P strategies. Standardising the hashrates and providing liquidity, it creates a foundational layer for lenders and borrowers to access instant cryptomining loans. The Hashrate Protocol will be first launched on the BNB chain with further support on multiple blockchains.

The protocol encompasses key functionalities which can be executed with the smart contracts:

- standardisation and asset-pooling
- tokenization of hashpower
- redemption of devices
- borrow and lend
- swap

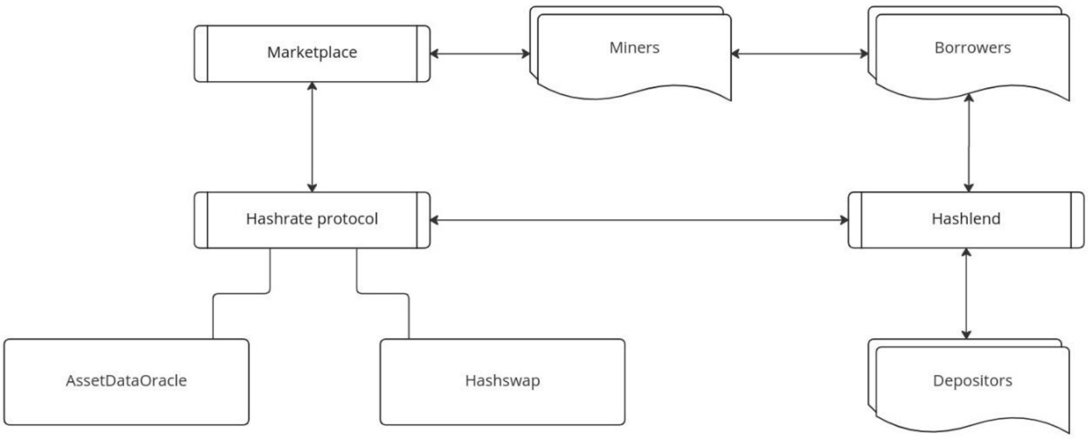

Figure 1: The Hashrate Protocol

1.1. Novel Implementations

Decentralized lending exchange (or "DLEX") is a novel architecture to participate in lending and borrowing, which matches bids and asks to define the average interest rate to the capital supplied. Paving the new way for decentralized loan structuring, the protocol uncovers a variety of tokenized underlying assets with dividend payouts, which can be loaned on-chain with the enhanced risk-management required for such tokenized tangibles.

1.2. Problems & Solutions

Significant amounts of value are stored in proof-of-work cryptocurrencies. Currently, the market capitalization of Bitcoin alone is approximately $325B as of Dec 27, 2022, with about 40% market dominance. However, most PoW blockchains only offer limited support for DeFi. As a result, there is a disconnect between DeFi as a set of emerging financial protocols and PoW assets as the primary value stores for cryptocurrencies. Despite the fact that Bitcoin Mining is one of the safest and proven long-term investments in cryptocurrency, miners struggle to generate sufficient cashflows during a bear market. To summarise, below are some of the issues that miners encounter, particularly during bearish cycles:

- Shortage of on-hand liquidity.
- Market inefficiencies and absence of standardisation tools.
- Lack of truly permissionless decentralized finance services for Bitcoin miners.
- Financing with only a few centralized institutions resulting in potentially high default ratio during a bear market as some cases have manifested.
- Barriers to entry and exit with strain and reduced transparency over-the-counter procedures.

This is where the Hashrate Protocol comes into play. Hashrate Protocol aims to address these common barriers that miners face and provide a hassle-free mining experience to the whole ecosystem players, enabling them to run operations in more risk-mitigated scenarios with open-access to permissionless transaction of ownership and financing.

1.3. Use Cases

Mark has acquired a batch of 10 Antminers S19 95TH a couple of months ago, hosted right now at one of the medium-scale facilities in Canada. Since the market has declined, Mark is looking at financing options to purchase more devices at lower prices. However, the bankers have rejected his application as such volatile debt financing structures can be offered to corporate clients which are mining at a large-scale e.g., Bitcoin stocks, and are not procured to small-scale individual miners. Mark has also been proposed to access crypto collateralized loans to pledge crypto assets against the loan. However, this option neither appeals nor benefits as Mark hasn't mined enough coins to cover a total value of the pledge, unless he increases CapEx to acquire more BTC getting exposed to downside risk. A friend has also recommended a few brokers to secure a loan for Mark under the terms of use applied that would be subject to relocation of hardware assets and full control at the rate of about 15 percent per annum, but again requiring some initial capital to facilitate this deal along with cumbersome due diligence procedures to undergo.

Mark is a #Bitcoinmaxi who trusts the technology and believes in the long-term growth of Bitcoin. So, he dives deeper into more innovative capital-efficient solutions to solve this issue with least capital exposure requirement. Mark has discovered the marketplace earlier and submitted to onboard his devices to the system. As it's pre-connected now, Mark has accessed the Hashrate Protocol by swapping his devices into tokenized crypto assets and placed an ask offer for 8 percent p.a. to pledge 10 devices at the present value. The current market LTV stands at 0.7, so that Mark can receive a 70% value loan collateralized by hashrate tokens. Mark’s ask offer has been matched with a bid of 7 percent p.a. and closed at 7.5 p.a. with a respective token pair created. Hence, Mark can now take out a total loan value equal to 7 devices while remaining an owner of 10 devices.

As per protocol architecture, Mark can now receive 50 percent of mining rewards generated by 10 devices during the life of the token pair and utilise a loan to acquire up to 7 devices more.

2. Protocol Architecture

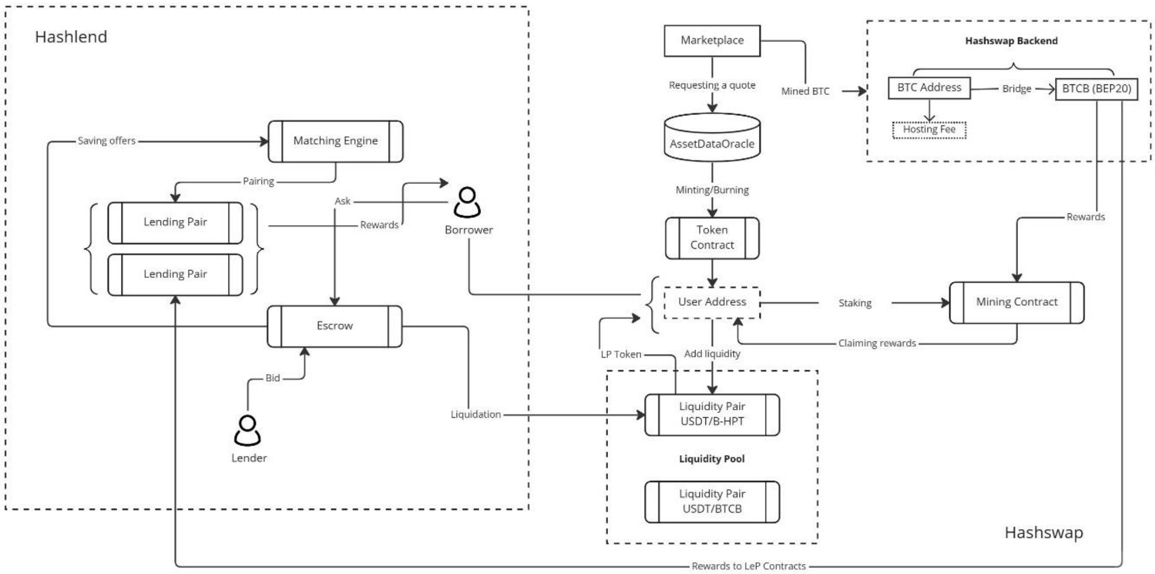

Figure 2: The current implementation of the Hashrate Protocol

2.1. Hashswap

Hashswap represents a set of core features that can be used to allow supplied hardware assets to seamlessly tokenize and interact with the integrated applications such as lending. Given its specific architecture, a device is subject to initial screening by the system to ensure the submitted tokenization request is backed by the real-time operating unit of hardware. If so, a request is approved and detected as valid, thus transmitted later to the **AssetDataOracle** for quoting.

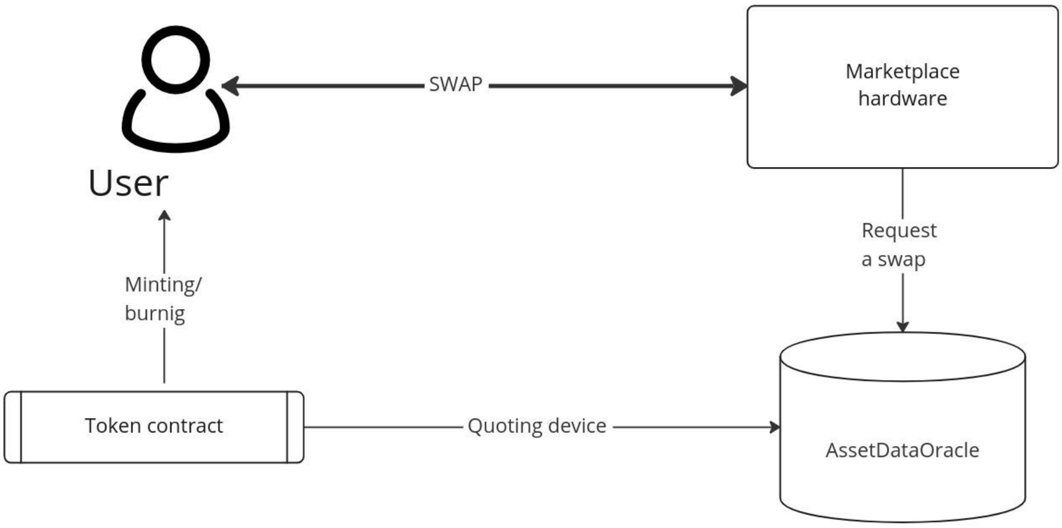

Figure 3: Hashswap of Devices to Tokens

2.1.1. AssetDataOracle

A process of miner assets (de)tokenization is executed through **the Oracle** and **the Issuer** (the marketplace token contract). Database oracle collects, stores, and retrieves device information while assessing a set of basic parameters of each unit to allow it for further seamless quotation. Any device connected to the system can be swapped in a matter of minutes under the condition of its full operation, if any device is missing out hashrates, it will be automatically detected as invalid by the system and thus rejected the quotation.

The AssetDataOracle calculates a present value of a miner asset based on the following parameters:

- Hashrate of a device
- Real-time hashrate
- Power of a device
- Real-time power
- Efficiency (W/T)
- Future cashflows during the 3-year-life
- Revenues
- Operating cost per terahash
- Bitcoin price

Essential factors with a direct impact on device profitability such as halving, shutdown price, network difficulty, etc. were taken into account.

Based on the above-mentioned parameters, a device can be quoted at a different price than that offered in the market, which will manifest overvaluation/undervaluation of a particular model.

Due to the design of the oracle, any fluctuations of its underlying or produced coin, for example Bitcoin, will be fully correlating with the market resulting in the issuance of a different number of tokens every time depending on the current value. With the same principle, protocol participants can take advantage of the market volatility to maximise returns.

2.1.2. Reserve

With the aim of enabling exchange-grade liquidity for miners, the Hashrate Protocol initiates a Reserve of hashrates aggregated into a single pool account. Each token issued is collateralized by one terahash of Bitcoin power and is redeemable by any user address interacting with the protocol to detokenize hashrate power back to a device. The reserve balances are being adjusted every second as per total supply of tokens circulated in the market. The reserve consolidates the key account data: total circulated tokens (incl. daily minting/burning), total hashpower in a single pool, dividend per terahash of a token.

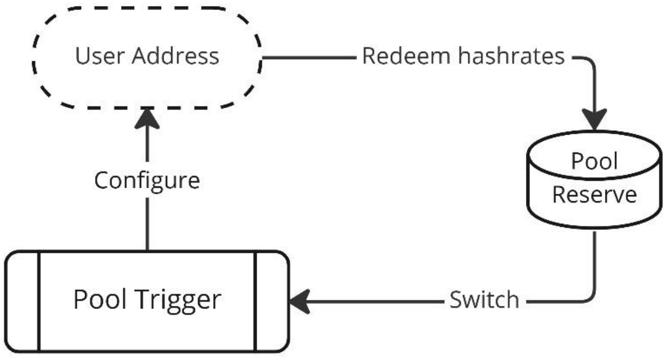

Figure 4: Hashpower Reserve

2.1.3. Wrapping

All accrued mining rewards are controlled by the Distributor smart contractor which converts BTC to its wrapped version depending on the chain it operates. In the version 1 of the protocol BTC is wrapped to BTCB through the Binance Bridge, hence reflects the equivalent balance of available rewards on the BNB chain-based single pool account. Prior to wrapping, the smart contract deducts hosting fees of all aggregated devices located across various locations. Consequently, the remaining balance is distributed among token holders through the mining contract and lending pair contracts.

2.1.4. Distributor & Staking

As per protocol design, mining rewards are received daily by all token holders according to the LP share in the mining contract and token balance on the LeP contracts.

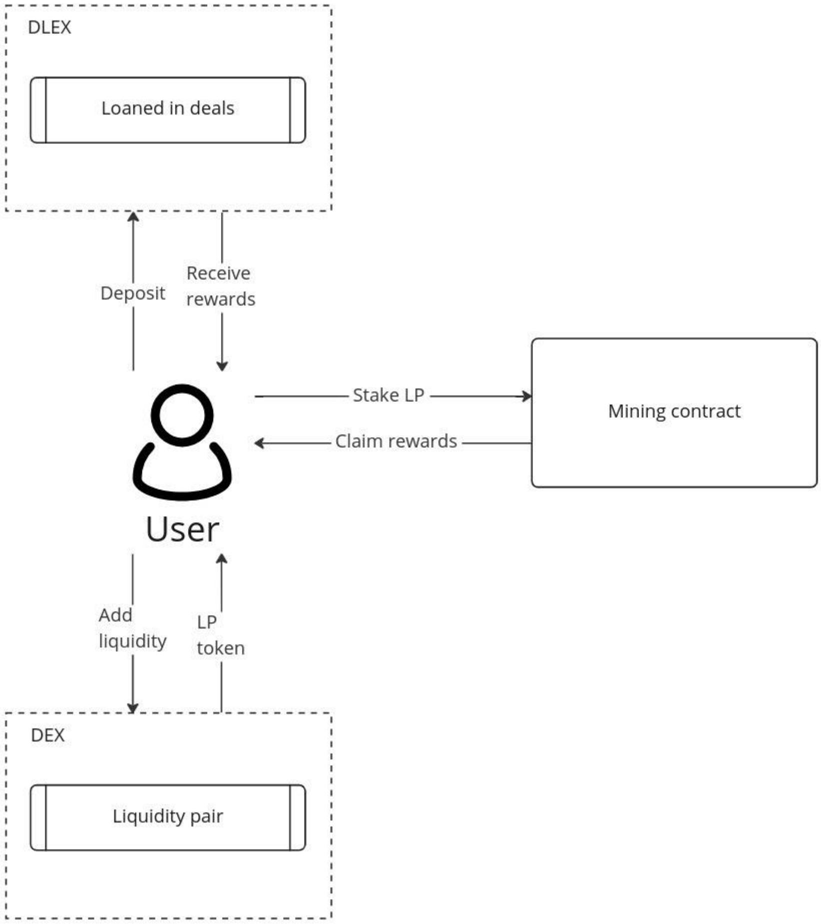

Figure 5: Distributor

In Figure 5, the distribution process is enacted with two scenarios. In the first one, mining rewards are claimed by users with an LP staked token in the mining contract. In the second one, reward balance is accrued in the lending pair contracts held securely until a loan is fully repaid to withdraw the collateral along with the accrued BTC balance.

Therefore, all rewards are proportionally allocated according to the token holder share in either the liquidity pool or lending contract. If tokens are held outside of both, rewards will not be credited to an address.

2.2. Hashlend

At the heart of the Hashrate Protocol is embedded lending allowance for tokenized hardware assets.

2.2.1. Basic Concepts

LTV (The Loan to Value) defines the weighted ratio of the total asset value depositors allocate to borrowers collateralized by tokenized hashrates. Initial LTV is set at 0.5 with possible increase up to 0.9 during the life of a token pair. Therefore, each dollar borrowed is provided two dollars of collateral value.

LTR (The Liquidation Threshold Ratio), calculated as the LTV weighted average of all LeP contracts, reflects price fluctuations of token pair and collateral value to liquidate a borrow position in case that **HR (The Health Rate)** drops below **the threshold**. A linear approximation between the previous and current LTR values construes the Health Rate. Given the next approximated LTR lower than LTV for the current **LeP (The Lending Pair)** plus unpaid reward, this pair shall be **liquidated**.

Unlike common lending structures with stable and variable interest rates, Hashlend introduces an algorithmic approach to match lend and borrow positions in a form of **decentralized lending exchange** to define the next optimised interest rate.

One of the advanced features incorporated into the lending contracts is the monitoring of **HRR (The Hashrate Reserve Ratio)**. Due to the asset-backed nature of the collateral, additional risk-management tools are provided to prevent the collateralization of unbacked tokens. In case HRR drops below 0.9, new lending pairs are temporarily ceased to be created.

Variable	**Description**
R (v) LTV	LTVnew = LTVold*(CL+CLtotal)/CLtotal CL - current collateral CLtotal = the sum of all previous active collaterals
R (l) LTR	LTR = Vb/Vc + liquidation fee Vb – value of borrowed asset Vc – value of collateral
R (h) HR	HR = (LTR-LTRprev) + LTR
R (r) HRR	HRR = Tu/Tt Tu – total uptime rate in TH Tt – total supply of tokens

2.2.2. Architecture

Compared to other lending protocols, Hashlend implements **the Matching Engine** and **Bid-Ask Storage** to correspond to borrowers and depositors. **The Escrow Contract** plays a key role in the proper functionality of the lending protocol. It maintains a reserve of all assets deposited and updates the state of all existing lending pairs. The basic logic of a loan pair execution is managed by the Escrow, which includes the following actions:

- Store offers
- Handle liquidation
- Accrue credits
- Return collateral
- Accept/cancel bids and asks
- Lock tokens

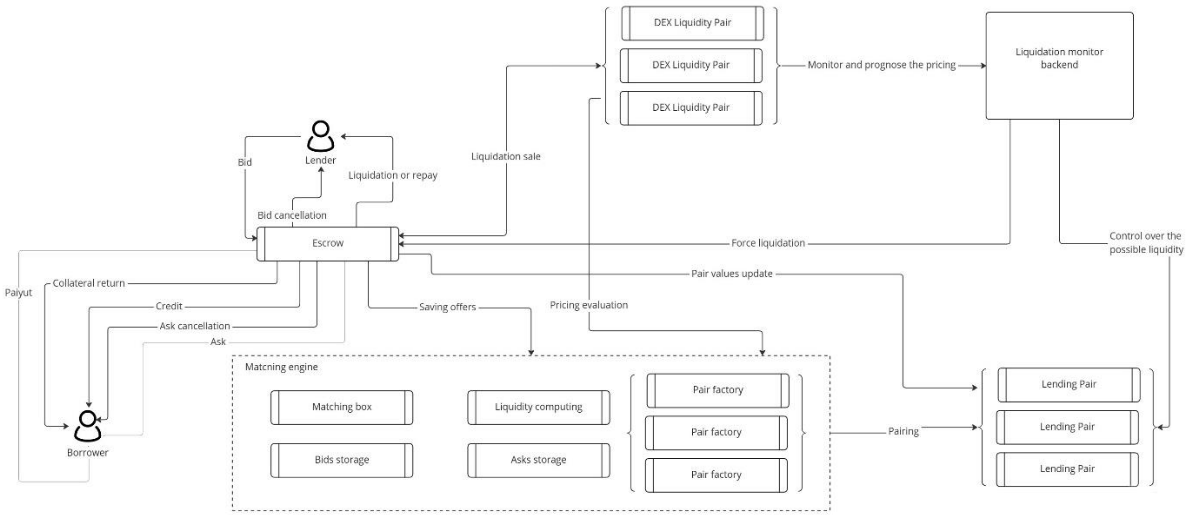

Figure 6: Decentralized Lending Exchange Architecture

2.2.3. Matching Engine

The Matching Engine determines the lending pairs (LeP) to be created. It consists of core components which participate in matching operations: **the Matching Box, Bid-Ask Storage,** and **Pair Factory.**

The Matching Box contract performs a set of executions and provides the relevant data to the Escrow contract. It performs the following:

- Matching interest rate positions
- Closing bid/ask positions
- Managing fees
- Revoking interest rates

The Bis-Ask Storage acts as a gatekeeper in formation and further execution of various positions. Placed bid/ask offers are redirected to the storage which can be accepted, cancelled, amended, or closed by the storage trigger.

The Pair Factory connects directly to the liquidity pair to analyse and define an appropriate LTV. It also creates lending pairs and holds summarised data on each one.

The Lending Pair contract stores and adjusts the lend-borrow values. It performs an analysis of LTR and HR for a particular transaction and can destroy the contract upon the liquidation.

2.2.4. Interest Rate Strategy

One of the advanced features of the DLEX is its interest rate strategy. The interest rate is derived algorithmically from the available market offers. Borrowers are permitted to place an ask with a maximum acceptable interest rate at a submitted principal amount. In a similar way, lenders are posting bids with a minimum interest rate that they are willing to gain at a total deposited capital to loan. Eventually, the market will be concluded at the highest rate transacted and a total sum of loanable capital which can be offered per one transaction.

For example, a borrower placed an ask of $5,000 at 7% p.a. while a depositor has posted $3,000 at 6% p.a. Therefore, the matching engine will pair these offers at 6.5% for a $3,000 collateralized loan. The next offer will not be lower than 7% p.a. with a maximum loan of $8,000.

2.3. The LeP Contract

All created lending pairs are backed by collateral corresponding to LTV ratio and are constantly monitored by the Admin contract to detect whether it is healthy and further liquidate in case of a default.

2.3.1. Collateral Value

Lending permits the maximum LTV of 0.5 since the inception and later grows up to 0.9 LTV ceiling during the life of the token pair. A percentage of the collateral continues to decrease following the total raising value of all active collaterals optimising the borrowing power without sacrificing security.

2.3.2. Liquidation Mechanism

A proposed liquidation mechanism is designed in a way to reduce the risk of rapid price drop of collateral token and thus selling off the asset before it depreciates. Thus, lending pairs are always tracked the current HR and if the HR overperforms the current LTV of the LeP the contract gets immediately liquidated. Vice versa, each single payoff directly decreases the outstanding amount as well as the LTV for the LeP contract, therefore raising the total health rate of the contract.

2.3.3. Controller

The Admin smart contract creates all the interaction between other associated smart contracts. Every interaction performed with the protocol will be subject to initial validation before any function gets executed. The Admin contract verifies all token pairs, it can adjust, add or delete them.

2.3.4. Dual Collateralization

The aspect of sufficient collateral balance remains one of the crucial concerns over the security of loanable deposits. Despite the doubled value of initial LTV, lenders are looking at more protection for capital, especially financing miner deals. Due to the rewards accrual mechanism in the LeP contracts, the additional downside protection is secured for both lenders and borrowers. Under the failure state of the liquidity pool the rewards can be enabled as a pledged value and accessed for further liquidation if the token balance lacks on the pair. However, such cases are not possible by the Escrow design, which runs a liquidation procedure with a frontrun, if possible, to liquidate unhealthy pairs. In the borrower's perspective the dual collateralization notably decreases the risk of liquidation.

A reward accrual counts towards the calculation of LTV only, yet not utilised for liquidation by contract function unless its token balance can be fully recovered. During the life of a token pair, the rewards remain in a locked state. A user address receives the entire reward balance accumulated in the LeP contact after the withdrawal of the collateral.

3. Risk Management

3.1. Isolated Pairs

Given its specific design, each lending pair has a different interest rate and loan value unlike commonly seen lending protocols which in return helps to mitigate downside risk when most vulnerable pairs are getting quickly liquidated and sold-off. In a case of various interest rates, pairs with lower to health rate state will be liquidated. In the view of optimising the collateralization power, the liquidity tends to be more segregated by deploying assets to various pairs in a queue to match their risk exposure. So that a lender is diversifying the risk across multiple borrowers.

3.2. Escrow Liquidation Trigger

The liquidation backend monitors all unsigned blockchain transactions in order to determine the risk associated with a drop in the value or liquidity of each collateral. If for some transaction the value received after the disposing of the collateral becomes equal to or less than the current value of the issued loan plus the liquidation premium, the backend initiates the instant liquidation of this transaction. To carry this out, the Escrow contract instantly sells what is indicated in the liquidated transaction through the connected DEX and closes the transaction, crediting the received funds to the lender's account in Escrow.

4. Capital Efficiency

4.1. Liquidity Pool Rewards

As per protocol design, all mining rewards are allocated proportionally and thus a total token balance in the pool and lending pairs will determine its eventual reward count. With the aim of providing liquidity and reflecting the real value of hashrates, a pool-based payout scenario is structured to facilitate more opportunities for its participants. Specifically, if the market enters a meltdown followed by continuous disposal of tokens to the pool, a reward level per LP will increase due to the excess of hashrates in the pool, while a cost per terahash in a pool will be undervalued compared to the market price of devices. Vice versa, if the market bounces back a token price will be reflecting the hashrate prices bringing up arbitrage opportunities.

4.2. Repurchase & Liquidity Maintenance

LPs are entitled for the entire reward balance. All other rewards allocated to lending pairs will be eligible for 50 percent payout and the remaining 50 percent will be recycled for repurchase and liquidity maintenance operation.

A project will operate its public account for the liquidity maintenance operation. All lending-derived rewards are counted towards the same address and are published a weekly summary of the relevant data.