eBTC Protocol: Purple Paper

Spadaboom
spada@badger.com

Saj Rajdev
saj@badger.com

Dapp Whisperer
dapp@badger.com

BadgerDAO

July 2023

Contents

1 Abstract

eBTC is a protocol that allows anyone to use Lido's Staked Ether (stETH) as collateral to borrow a synthetic Bitcoin asset with zero borrowing fees. Powered by non-custodial, immutable, governance-minimized smart contracts, it aims to be the most trustless and censorship-resistant synthetic Bitcoin in DeFi.

eBTC is the first protocol to focus exclusively on the ETH/BTC ratio. While most of the trading and strategies for this pair are currently done off chain using centralized counterparties, eBTC empowers users to now bring this activity on chain with extreme transparency. Further, due to its immutability and composability, it enables any protocol to integrate its functionality and build on top of it.

Its vision ignited by the abundance of highly publicized financial collapses in 2022, eBTC has been designed as a direct response to the shortcomings of the centralized and opaque financial infrastructure that is commonplace within the blockchain space. By moving more ETH/BTC activity on chain within immutable smart contracts, eBTC moves the space further away from the centralized solutions for borrowing Bitcoin currently seen in the market today.

2 Introduction

Decentralized protocols that offer ETH/BTC trading strategies (money markets, perpetual exchanges, etc.) often suffer from capital inefficiency when compared to other centralized options. Large over-collateralization requirements, high (often variable) fees, and reliance on utilization are the primary issues limiting the growth of these activities and associated on-chain protocols.

eBTC was designed as a collateralized debt protocol using the ETH/BTC asset pair with low minimum overcollateralization requirements, no reliance on system utilization, and without the need for fees.

With the evolution to proof-of-stake and the rise of liquid staking derivatives, the eBTC model became viable as a more financially attractive alternative to existing DeFi and CeFi options in the market today.

3 Protocol Mechanics

3.1 Borrowing

A **Collateralized Debt Position (CDP)** is the unit of accounting used to track a specific borrowed debt amount, the respective collateral that backs it, as well as the ratio between the value of these two assets, known as the **Individual Collateral Ratio (ICR)**. Each CDP is owned by a single Ethereum account and is non-transferable.

CDP owners have the freedom to make adjustments to their CDPs at any time by increasing their collateral, withdrawing some collateral, borrowing more debt, or repaying a portion of the outstanding debt. Any modification to the CDP triggers a corresponding adjustment to the ICR.

eBTC accepts Lido's stETH[1] as the ***only*** collateral.

eBTC can be borrowed by opening a CDP and depositing a certain amount of collateral into it. The borrower can then choose an amount of debt (eBTC) to take on the CDP while preserving an ICR higher than the **Minimum Collateral Ratio (MCR)** of 110%. CDPs must have a size of at least 2 stETH worth of eBTC at the moment of their creation and throughout their duration.

For as long as a CDP has an ICR higher than the MCR, the owner may increase their debt and borrow more eBTC. Once eBTC is borrowed, the collateral is stored in the protocol's Smart Contracts system, and eBTC is minted and transferred to the borrower.

The system allows for multiple CDPs to be created from the same account. This is especially handy for users wishing to borrow eBTC with different Collateral Ratios or 'risk' profiles for their different strategies.

In order to open a CDP, the system requires the user to transfer an additional 0.2 stETH (known as the **gas stipend**) along with the specified collateral amount. This amount is separate from the collateral and is not included in the ICR's calculation. When a borrower repays their CDP's debt, the system returns the full gas stipend along with the collateral. The gas stipend exists to ensure the CDP is profitable enough to liquidate if the CDP's ICR falls below the MCR; in this case, it is transferred to the liquidator as an incentive to cover their transaction's associated gas cost.

[1] See: https://etherscan.io/token/0xae7ab96520de3a18e5e111b5eaab095312d7fe84

3.2 Fee-less Borrowing

Borrowing eBTC is done without any upfront fees and without any interest on the principal or debt. Instead, the protocol earns revenue by taking a percentage of accrued staking yield from the total system collateral. This percentage is called the **Protocol Yield Share (PYS)**. Initially, the PYS will be set to 50% of the accrued yield, and this percentage is subject to adjustment through the minimized governance system.

The Protocol Yield Share is processed on each operation involving a CDP and is always up to date within the system. The borrower sees the value of their collateral grow via the accrued yield, which is retained by the CDP $((100\% - PYS) \times$ stETH's yield). With the compounding yield from the collateral positively affecting the ICR of each CDP, it will be clear that the overall health will continue to naturally improve over time.

The Gas Stipend is accounted for separately from the collateral, and it does not incur the PYS. Upon its return to the borrower, it will have accrued the full yield amount for the borrow period.

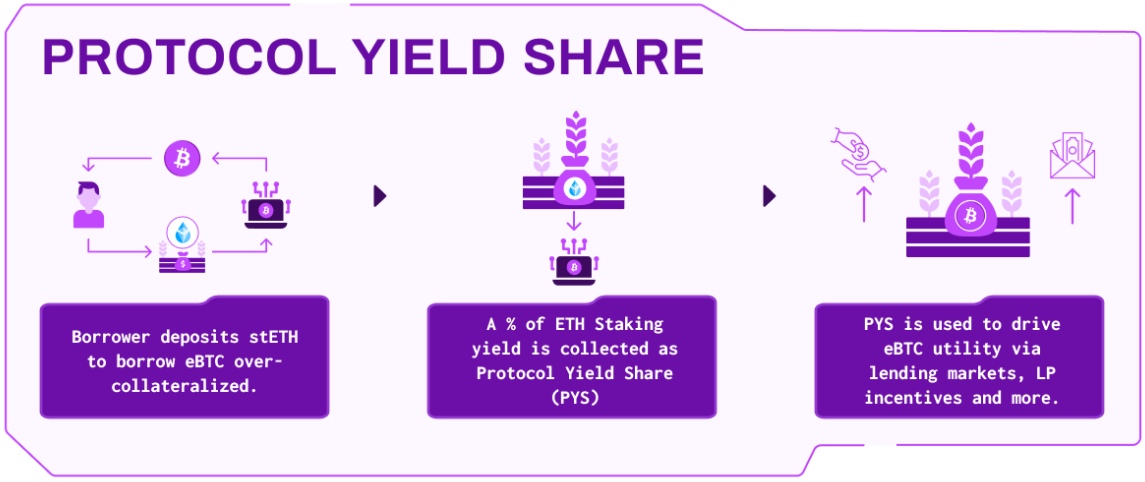

Figure 1: Protocol Yield Share.

3.3 Liquidations

Liquidations serve as a mechanism for ensuring the solvency of the system. If the ICR of a CDP falls below the MCR of 110% when in **Normal Mode** or the **Total Collateral Ratio (TCR)**–the ratio between the sum of all the collateral in the system and its emitted debt–when in **Recovery Mode**, the CDP is said to be open for liquidation. At this point, the outstanding debt can be repaid by any market participant (liquidator) in exchange for some surplus collateral and the Gas Stipend as an incentive.

To fully liquidate a CDP, the liquidator must obtain the total amount of eBTC owed by the CDP and pay it to the system, which is then burned. By fully liquidating a CDP, the position at risk is effectively closed, resulting in an improvement in the system's TCR.

Multiple CDPs can be liquidated simultaneously within the same transaction, provided that all of them have an ICR below the MCR (or the TCR during Recovery Mode).

In the event that the debt associated with a liquidatable CDP is too large to be repaid in full, a liquidator may opt for a partial liquidation. However, it is important to note that for a partial liquidation to be allowed, the CDP must end up with more collateral than the minimum CDP size requirement of the system (which is set at 2 stETH). Similarly to a full liquidation, partial liquidations

also receive an incentive in the form of the collateral asset according to the criteria in the section below.

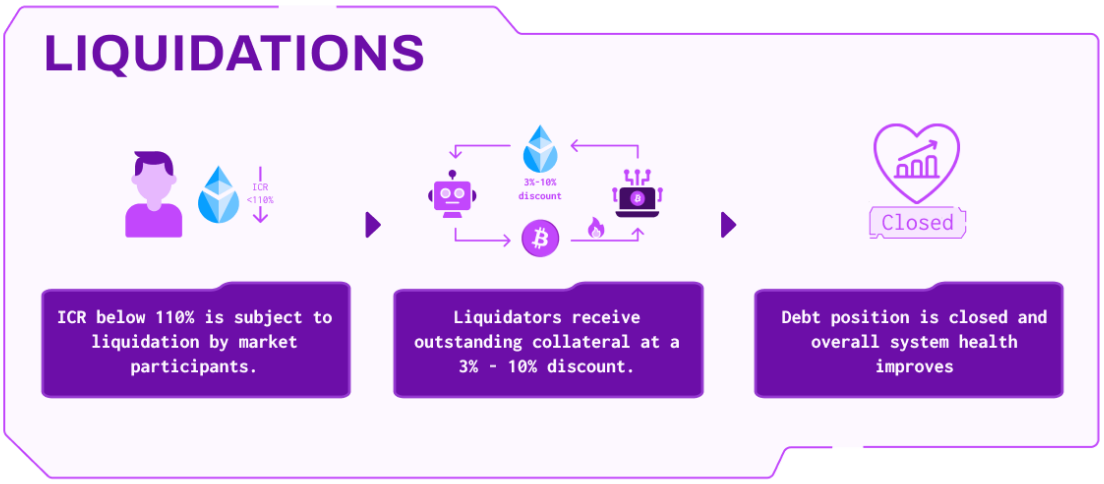

Figure 2: Liquidations under Normal Mode.

Liquidators are compensated differently depending on the ICR at which the CDP is liquidated and on whether they execute a full or partial liquidation. Below is a breakdown of the liquidation incentives under these conditions.

3.3.1 Full Liquidation Incentives

Full liquidations incentives are determined by the following general formula:

$$LiquidatorIncentive = \max(1.03, \min(ICR, 1.1)) + GasStipend$$

Where Gas stipend is equal to 0.2 stETH, plus the accrued staking yield on that 0.2 stETH while the CDP has been active.

The same logic can be better visualized for different values of ICR, as follows:

ICR	Debt to Repay	Liquidator Incentive	Owner's Coll. Surplus	Outstanding Debt
>110% (Recovery Mode)	Full CDP's Debt	(Full CDP's Debt worth of Collateral * 110%) + Gas Stipend	Full Collateral of CDP - Liquidator Incentive	0
>103%, ≤110%	Full CDP's Debt	Full CDP's Collateral + Gas Stipend	0	0
<103%	Full Coll. worth of Debt / 103%	Full CDP's Collateral + Gas Stipend	0	Full CDP's Debt - Repaid Amount

Table 1: Breakdown of incentives for full liquidations.

The table above demonstrates that eBTC's innovative incentives algorithm has been crafted to guarantee liquidation profitability in all cases, even in cases where a CDP becomes under-collateralized. This is accomplished by offering a 3% collateral incentive to all CDPs with an ICR of 103% or less. However, it is important to note that this means that any full liquidation with an ICR below this threshold will result in the CDP having no collateral and a small amount of bad debt outstanding. The mechanism for handling bad debt will be explained in the next section.

In summary, the maximum possible incentive for a full liquidation is 10% of the CDP's collateral + Gas Stipend, and the minimum incentive possible is 3% of the CDP's collateral + Gas Stipend, regardless of the mode of operation. These bounds also apply for Recovery Mode liquidations; CDPs liquidated at a 125% ICR are also subject to a maximum liquidation penalty of 10% and are able to claim any resulting collateral surplus.

3.3.2 Partial Liquidation Incentives

Partial liquidation incentives are determined by the following general formula:

$$LiquidatorIncentive = \max(1.03, \min(ICR, 1.1))$$

Partial liquidations operate on a slight variant of the full liquidation formula that does not include the additional Gas Stipend as an incentive. This is because there is only one Gas Stipend allotted per CDP, and it is reserved to incentivize fully closing a CDP, via liquidation or otherwise. Full liquidations lead to a more favorable outcome for the system; hence, they are prioritized over partial liquidations.

The table below shows the calculation for different values of ICR:

ICR	Debt to Repay	Liquidator Incentive	Owner's Coll. Surplus	Outstanding Debt
>110% (Recovery Mode)	Up to liquidator	Collateral worth of the partial debt repaid * 110%	Variable, must be at least 2 stETH	Variable
>103%, ≤110%	Up to liquidator	Collateral worth of the partial debt repaid * ICR	Variable, must be at least 2 stETH	Variable
<103%	Up to liquidator	Collateral worth of the partial debt repaid * 103%	Variable, must be at least 2 stETH	Variable

Table 2: Breakdown of incentives for partial liquidations.

As evident from the table above, partial liquidations are always incentivized, just as full liquidations are. The CDP's ICR does not affect this incentivization. However, unlike full liquidations, partial liquidations do not include the Gas Stipend. Therefore, a liquidator must estimate the correct amount to liquidate and the corresponding ICR to properly subsidize their gas costs based on the incentives offered by the operation.

In summary, the maximum possible incentive for a partial liquidation is 10% of the CDP's collateral, and the minimum incentive possible is 3% of the CDP's collateral, both proportional to the liquidation size, regardless of the mode of operation.

3.4 Bad Debt Redistribution

In the case that a CDP is not liquidated until after its ICR goes below 103%, the system allows for the depletion of its collateral to properly incentivize the liquidation operation at the cost of leaving some uncollateralized debt behind. The amount of **Outstanding Bad Debt** from an under-collateralized liquidation can be estimated as follows:

$$OutstandingBadDebt = TotalDebt \times (1 - \frac{ICR}{103\%})$$

Where ICR refers to the collateral ratio at which the CDP is liquidated in order to result in bad debt, and it must be below 103%. It is clear that there is a linear relation between the amount of Resulting Bad Debt and the ICR at which it was liquidated.

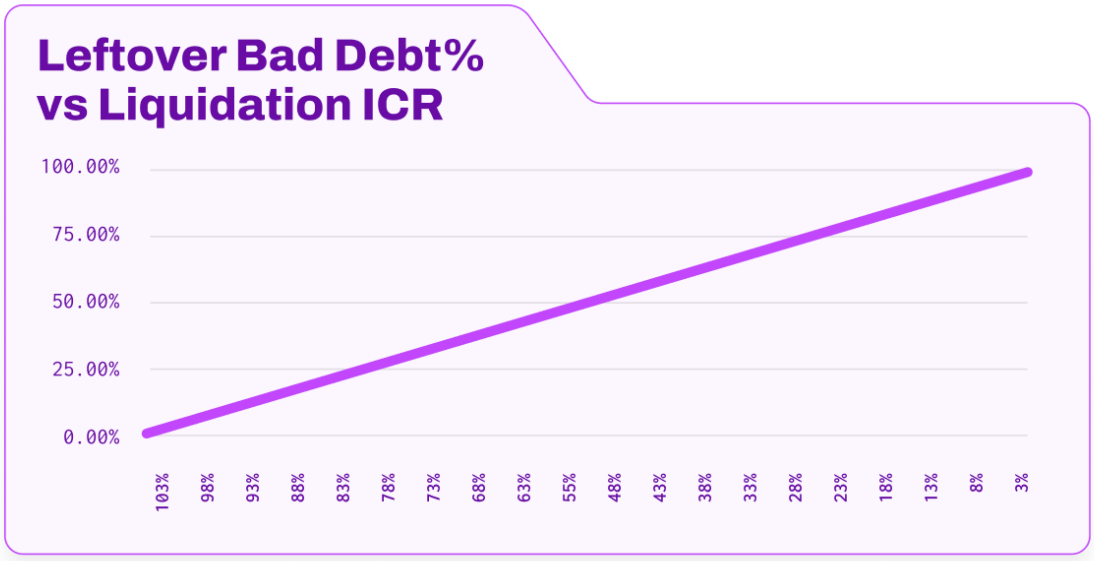

Figure 3: Resulting bad debt as % of total v.s. Liquidation ICR.

Once an underwater CDP is liquidated to this point, the system distributes the remaining bad debt among all open CDPs in the system in proportion to their debt size. This means that the debt of each CDP will increase, and therefore, their ICRs decrease proportionally. Debt redistribution happens atomically with the underwater full liquidation, therefore it is triggered by this liquidator.

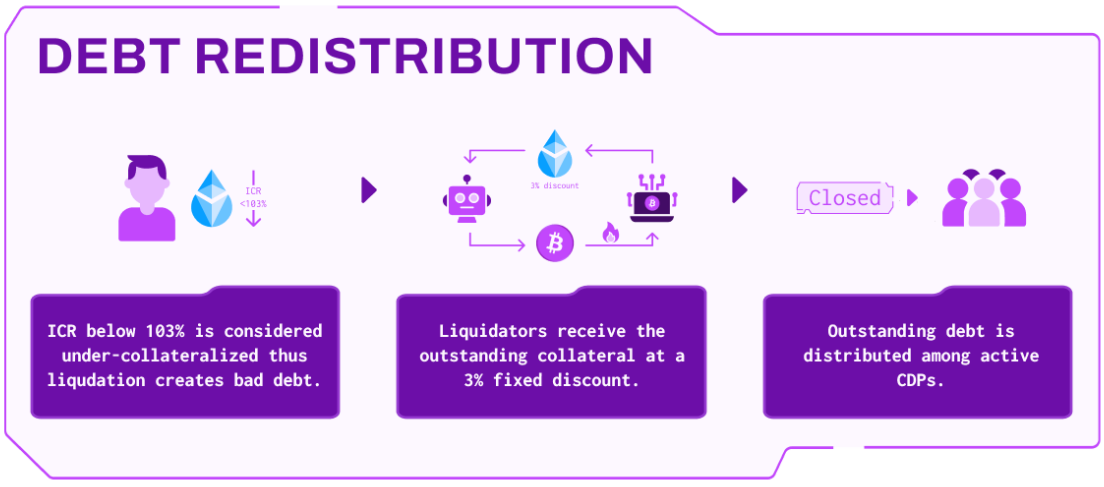

Figure 4: Bad debt redistribution flow.

3.5 Redemptions

A design originally introduced by Liquity[2] in their LUSD whitepaper[3], redemptions are the protocol's mechanism for exchanging eBTC for stETH at face value, based on the spot stETH/BTC Oracle price. This means that redemptions allow for swapping at price parity, regardless of the eBTC market price.

To initiate a redemption, a user must transfer the desired amount of eBTC into the system. The system then calculates the equivalent amount of stETH based on the latest price returned by the Oracle. The estimated stETH amount is withdrawn from the CDP with the lowest ICR (highest risk) in the system and transferred to the user, after deducting a fee. The eBTC transfer is subsequently deducted from the debt of the CDP being redeemed against and burned, and the fee is deposited into the protocol's Treasury.

Users can redeem eBTC for stETH at any time without any limit, but an exponentially scaling fee algorithm is in place to disincentivize this activity and prevent misuse of the mechanism. The redemption fee starts at 1% and varies according to the algorithm described in the section below.

Regardless of the fee applied, redemptions will always result in a net 0 impact to the holder of the CDP redeemed against. If a CDP is redeemed against with a value equal to or higher than its debt, the debt will be fully repaid, the CDP will be closed, and any excess collateral resulting from the redemption will become available for the CDP holder to claim. Therefore, the value of the eBTC that is borrowed plus the claimable collateral surplus will be equal in value to the collateral the CDP held initially, resulting in a net 0 impact.

The minimum CDP size is still enforced during the redemption process. Redemptions are only allowed if they result in the closure of the CDPs being redeemed or if they leave the CDP with at least the minimum amount of collateral required (2 stETH). CDPs below this minimum size are potentially unprofitable to liquidate and therefore are not allowed to exist within the system.

If the desired redemption amount surpasses the debt of the riskiest CDP, the system permits redemption across multiple CDPs until the redemption amount is fulfilled. CDPs are redeemable based on their ICRs, starting from the lowest in the system and moving upwards.

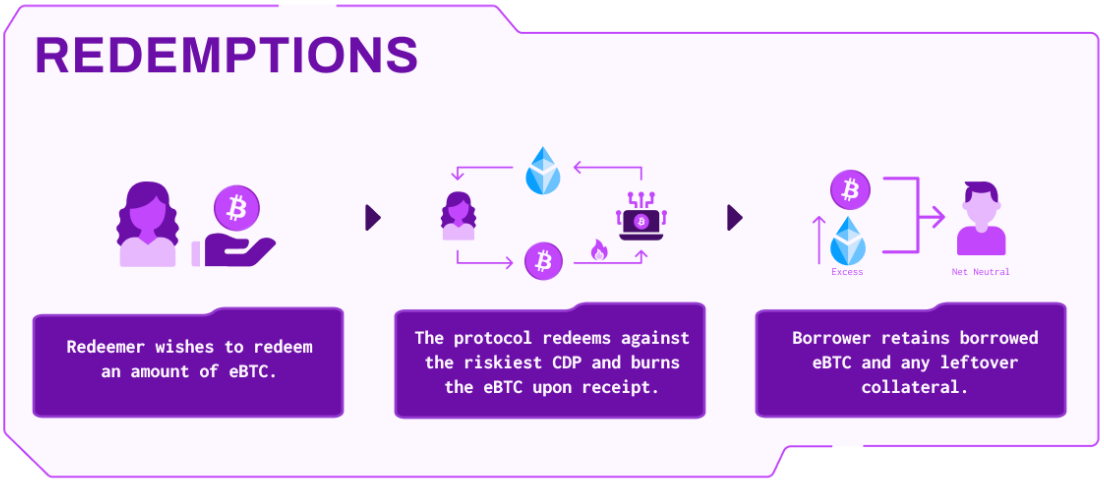

Figure 5: Redemption mechanism flow.

Redemptions are a crucial tool for establishing a firm price floor for eBTC and bolstering its peg. As they utilize the oracle price to estimate the redemption amount, an arbitrage opportunity arises

[2]See: https://www.liquity.org/
[3]See: https://docsend.com/view/bwiczmy

whenever eBTC trades below the price parity. Arbitrageurs can then buy eBTC at a discount and redeem it for a higher value until the peg is restored.

As mentioned, there is a minimum fee of 1% for redemptions, which determines the actual hard price floor of eBTC. In other words, for there to be an incentive to redeem and arbitrage the price back to its peg, eBTC would have to trade below 99% of the price of BTC (price parity - fee), assuming the fee is at its lowest.

In order for redemptions to effectively introduce peg stability, their daily volume should be limited to a small percentage of the total available liquidity of eBTC. For this reason, the protocol limits the utilization of the mechanism by increasing its fee in proportion to the daily usage volume. At any given time, the fee can be estimated according to the following logic, originally introduced by Liquity for LUSD's redemption fee:

$$RedemptionFee = BaseRate + FeeFloor = BaseRate + 1\%$$

Upon every redemption, the **Base Rate**, *b(t)*, at time t can be estimated as follows:

$$b(t) = b(t-1) + \alpha \times \frac{m}{n}$$

Where α or alpha is a constant value (modifiable by governance) that determines the slope of the fee's increment, **m** is the amount of eBTC redeemed, and **n** is its total supply.

The base rate decays over time towards 0 according to the following logic, which is applied upon every redemption before the estimation of the new base rate:

$$b(t) = b(t-1) \times \delta^{\Delta t}$$

Where δ or decay factor is a constant (modifiable by governance) chosen so that the half-life of the fee is 12hrs and Δt is the time elapsed since the last redemption.

3.6 Flash Loans

The eBTC protocol provides the capability for Flash Loans on both eBTC and the stETH collateral in the system. When a user flash borrows eBTC, the debt is minted, transferred to the user, and burned upon repayment within the same block. The amount of debt that can be borrowed is limited to uint112.max $(2^{112} - 1)$ wei.

Similarly, stETH can also be flash borrowed. In this case, the requested amount is taken from the collateral pool, transferred to the user, and then returned to the pool once the loan is repaid. The amount of collateral that can be flash borrowed is limited by the amount held in the pool.

Users who wish to take out a flash loan will be required to pay a fee of 0.03% on the borrowed amount. This fee may be subject to future adjustments through protocol governance.

3.7 Recovery Mode

Normal Mode refers to the regular state of operation of the system in which it is considered to be safely distant from the potential for insolvency. As long as the TCR remains above the **Critical Collateral Ratio (CCR)** of 125%, the system remains in Normal Mode.

During Normal Mode, liquidations occur when the ICR falls below the MCR of 110%.

The system switches into Recovery Mode (a design first created by Liquity for LUSD) only when the TCR falls below the CCR of 125%. In this mode, the system introduces the following changes to its mechanisms in order to incentivize certain user behaviors that lead to a rapid rise of the TCR back above 125%:

- Any CDP whose ICR is below the TCR becomes liquidatable. In a way, during Recovery Mode, the TCR becomes the Minimum Collateral Ratio. This incentivizes rapid repayment or adjustment of CDPs with low ICR.

- CDPs liquidated during Recovery Mode are prone to the same liquidation penalty as those liquidated during Normal Mode. This means that if a CDP is liquidated at 125%, it incurs the same penalty as if it were liquidated at 110%.
- Borrowing is not allowed unless it helps improve the TCR. This means that borrowing is only permitted at or above the TCR.
- Adjusting a CDP is not allowed unless it helps to improve the TCR. This means that the CDP's resulting ICR from the adjustment must be higher than its initial.

3.8 Oracles

Since eBTC aims to maintain its peg to the price of BTC, the system needs to access accurate and consolidated price data of this asset in relation to its collateral at all times. Some Oracle services have demonstrated their ability to securely and dependably report the value of these two assets to the Ethereum Blockchain.

The architecture of eBTC depends on a primary and unchangeable Oracle, as well as a controlled backup Oracle that will only come into play automatically in the rare event that the primary Oracle becomes unresponsive or fails to meet the system's data reliability criteria. The backup Oracle system is governed by the protocol's minimized governance system through a highly rigorous, transparent, and safeguarded process.

3.8.1 Primary Oracle

eBTC relies on Chainlink as its primary Oracle Provider, a provider known for setting the industry standard for decentralized and secure price feed Oracles. The primary Oracle for eBTC is created by aggregating the following price feeds from ChainLink:

- ETH/BTC (0.5%, 1hr)[4]
- stETH/ETH (0.5%, 24hr)[5]

As a result from the aggregation, the eBTC Protocol manages to obtain reliable access to the stETH/BTC pair price with a maximum possible price deviation of 1% at any given time.

3.9 Minimized Governance

eBTC aims to be the most trustless and censorship-resistant synthetic Bitcoin in DeFi. However, eBTC must rely on external dependencies, such as the collateral asset (stETH) and oracle solutions (for pricing), which are still very much in development along the path to immutability.

To address potential economic security and security risks, a minimized governance mechanism has been introduced to eBTC to ensure resilience. This governance system was carefully designed to ensure a non-custodial and censorship-resistant protocol while enabling some flexibility around the margins to adapt to market and technical developments.

Governance can modify parameters surrounding fee competitiveness, peg stability, risk management, and economic and technical security of the system.

[4]See: https://data.chain.link/ethereum/mainnet/crypto-other/eth-btc
[5]See: https://data.chain.link/ethereum/mainnet/crypto-eth/steth-eth

3.9.1 Governable System Parameters

Parameter	Bounds
Protocol Yield Share	0% - 100%
Redemption Fee Floor	1% - 100%
Redemption Fee Alpha (α)	0 - ∞
Redemption Fee Decay Factor (δ)	0 - ∞
Flash Loan Fee	0% - 100%

Table 3: Bounds of governable parameters.

Protocol Yield Share
Under minimized governance, the Protocol Yield Share can be adjusted for two primary reasons.

1. The yield of stETH can fluctuate over time due to complex market factors that are difficult to codify into rules within the system. It is essential to adjust the protocol's yield share percentage to ensure the protocol's ongoing market competitiveness and sustainability in response to these fluctuations.

2. Altering the protocol yield share can be used to incentivize or disincentivize borrowing, which in turn can lead to a tighter peg when required.

Redemption Fee Floor
The Minimum Redemption Fee serves to restrict arbitrage opportunities that may arise due to redemptions and establish a true price floor. Therefore, it is crucial that this fee is kept as small as possible. However, for security reasons, it must be at least equal to the maximum deviation threshold of the price Oracle. Setting the fee lower than the Oracle's reported price discrepancy can create an unrealistic arbitrage opportunity at the expense of the redeemed CDP. Given this, it is important to have the ability to modify this parameter in case the maximum deviation threshold of the Oracle changes or if the system switches to a fallback Oracle with a different maximum deviation threshold.

Redemption Fee Alpha (α)
This parameter determines the steepness of the value increase of the redemption fee in proportion to the redemption's volume. In other words, the higher it is, the larger the fee will scale for the same amount of volume. Given that the scaling fee algorithm is meant to limit the volume of redemptions to no more than 1% of the available liquidity for arbitrages per day, the alpha can be modified in response to redemption usage patterns, changes in liquidity pool volume and unforeseen peg dynamics.

Redemption Fee Decay Factor (δ)
The decay factor determines how long it takes for the redemption fee to return to its initial value after it has been increased through the use of the mechanism. A longer decay factor means it will take more time for the fee to return to its initial value, while a shorter decay factor will make the process quicker. It is important to find a balance where the decay factor is large enough to allow the market to naturally adjust to the increase in demand caused by redemptions, but short enough to enable effective arbitrage of short-term price volatility. In some cases, the initial decay factor may be too large or too short to meet these expectations, which may require an adjustment. Any changes to the decay factor must be justified through careful modeling using historical data and projections.

Flash Loan Fee
There are two primary reasons that justify the potential adjustment of Flash Loan fees. Firstly, to preserve competitiveness in the Flash Loan provider market, these fees can be either increased or decreased. Secondly, they may be modified to ensure they do not hinder or discourage liquidators and arbitrageurs from participating.

3.9.2 Governable System Mechanisms

Fallback Oracle System
To ensure the system's future-proofing and considering that Oracles come with a set of trust requirements that cannot be avoided, the fallback oracle can be replaced. It is important to note that the Primary Oracle cannot be replaced as it is immutable. A thorough process is in place to evaluate, test and approve new Oracles, and this can only be done transparently through open governance.

Extensible Minting
In order to future proof the system, the ability to add new contracts to the minters/burners list is preserved by governance. This is in case an opportunity arises to introduce new products that may, for example, help harden the peg without compromising on decentralization or censorship resistance.

Disabling of Redemptions and Flash Loans
In the rare event that the Redemption or Flash Loan mechanisms are misused in a malicious manner to harm the system, eBTC's governance may disable these features to ensure the security of the system.

4 Conclusion

The eBTC protocol intends to be the most capital efficient way to leverage stETH to borrow Bitcoin without forfeiting staking yield.

It combines a variety of mechanics that have proven to stand the test of time across many CDP-based stablecoin designs while focusing exclusively on the ETH/BTC pairing. This opens up new on-chain strategies between the two largest cryptocurrencies in the space that have not been possible before.

With the evolution of the Ethereum network to Proof-of-Stake, new possibilities arise for economic frameworks within protocols built on the ETH staking layer. In this context, the eBTC protocol stands out as an innovator, offering the groundbreaking feature of zero-cost BTC borrowing while eliminating custodial risks and providing the highest level of transparency.