Risk Assessment - cbBTC Collateral on FiRM

Useful Links

Documentation

- Coinbase Campaign

GitHub Repositories

- Github

Community and Social Media
- Coinbase Twitter

Governance and Proposals
- Proposal to onboard cbBTC to AaveV3 on Base and Mainnet
- Aave Governance
- Compound Governance
- Radiant Capital Snapshot

Sources
- Coinbase Whitepaper
- Wrapped-tokens-os
- OpenZeppelin Audit Report

Key Considerations:

This document has been designed to educate the reader of adherent risks of cbBTC as a collateral token on FiRM, Inverse Finance's fixed-rate lending protocol. While custodial crypto assets inherit similar risks that should be cautioned, cbBTC also carries unique risks to its counterpart wBTC. Highlighted below are key considerations when determining the risk profile of cbBTC; each has been expanded within the Risk Assessment.

- **Business Trust and Transparency**
  - Lacking Proof of Reserves
  - Lacking contract administrative policy
  - Potential for future fees for minting/wrapping or burning/unwrapping
- **Centralization Risks**
  - GeoBlocking
  - KYC dependency
- **Contract**
  - Upgradable proxy
    Permissioned Roles
  - Owner EOA*
  - Admin EOA*
  - Blacklister
  - Pauser EOA*
  - MasterMinter EOA*

* "As part of Coinbase's risk mitigation efforts, wallet private keys are not stored in plaintext format in any location and the cryptographic consensus of multiple human operators is required to decrypt a private key for both hot and cold wallets. No single individual has control of Coinbase's wallet private keys. Coinbase performs internal audits of the private key

management process and reconciliations between Coinbase wallets and third-party blockchain data. Coinbase does not use sub-custodians in connection with the storage of digital assets." *-Coinbase*

Overview

Background

Coinbase and Circle co-founded *Centre* in 2018, an open-source entity responsible for overseeing USDC, a stablecoin. By 2023, with increasing regulatory clarity around stablecoins, Circle took over the direct management of USDC, and Centre was dissolved.

Coinbase continued leveraging the USDC smart contract (FiatTokenV2_1) for its wrapped cbASSETS initiative, such as cbBTC. While the core structure of the FiatTokenV2_1 contract remained unchanged for cbBTC, Coinbase introduced extended functionality (FiatTokenV1) for staked wrapped cbASSETS like cbETH, which underwent a rigorous audit by OpenZeppelin. This architecture allows for trusted, scalable use of wrapped assets like cbBTC across multiple chains, fostering a more interconnected and efficient DeFi ecosystem.

Architecture

cbBTC is a wrapped version of Bitcoin (BTC) issued by Coinbase. It is a 1:1 representation of BTC, fully backed by Bitcoin held in Coinbase's custody, ensuring security through Coinbase's decade-long experience in safeguarding billions in Bitcoin for institutions and customers worldwide. cbBTC offers seamless compatibility with DeFi applications, enabling users to utilize their Bitcoin in novel ways on chain, such as providing liquidity to DeFi protocols or using it as collateral to borrow other crypto assets.

Centralization Risks

Use Restrictions

"cbBTC deposits and redemptions are currently **unavailable** to customers in New York, Canada, Mexico, Germany, Singapore, United Arab Emirates, Colombia, Argentina, South Africa, South Korea, Nigeria, Ghana, Chile, Dominican Republic, Jamaica, Ecuador, Peru, Costa Rica, Taiwan, Kuwait, Kazakhstan, Cameroon, Serbia, Trinidad and Tobago, El Salvador, Kenya, Indonesia, Bahrain, Bangladesh, Pakistan, Thailand, Saudi Arabia, Sri Lanka, Morocco, Vietnam, Malaysia, Algeria, Ethiopia, Guatemala, Honduras, Panama, Egypt, Israel, Tunisia, Nepal, Benin, Armenia, Georgia, Mongolia, Paraguay, Cote d'Ivoire, Bolivia, Kyrgyzstan, Angola, Burkina Faso, Togo, Moldova, Albania, Cambodia, Niger, Senegal, Barbados, Maldives, Cayman Islands, Macedonia, Mozambique, Republic of the Congo, Gabon, Saint Lucia, Bermuda, Turkey, Ukraine, British Virgin Islands." *-Coinbase*

This extensive list of cbBTC Geo-blocked territories could presumably add friction to cbBTC's arbitrage in the event of an on-chain depeg by limiting the ability for 1:1 redemptions and deposits. Its competitor WBTC is making efforts to mitigate these jurisdictional risks by decentralizing its custody globally. However, any user with a Coinbase account outside of the restricted jurisdictions can redeem or mint. This open access model is likely to result in numerous automated arbitrage participants (market makers and bot runners), which should maintain a tight peg to BTC.

Custodial

“The underlying BTC reserves backing cbBTC are held 1:1 at Coinbase, and redemption rights remain with cbBTC holders. Please reference the applicable Coinbase User Agreement to learn more about Coinbase’s custodial services and terms specific to users holding cbBTC.

“Coinbase utilizes both hot wallets and cold wallets in its custodial solutions. Cold wallet private key materials are stored and secured at facilities within the United States and Europe. As part of Coinbase’s risk mitigation efforts, wallet private keys are not stored in plaintext format in any location and the cryptographic consensus of multiple human operators is required to decrypt a private key for both hot and cold wallets. No single individual has control of Coinbase’s wallet private keys. Coinbase performs internal audits of the private key management process and reconciliations between Coinbase wallets and third-party blockchain data. Coinbase does not use sub-custodians in connection with the storage of digital assets.” *-Coinbase*

Several high impact roles are centralized to Coinbase control and referenced below in “Technical Contract Analysis”. Among these risks are masterMinter and minters which are assigned to facilitate the deposits and redemption of Coinbase user Bitcoin.

Any custodial crypto (WBTC, cbBTC, USDC, USDT, any RWA) is no safer than the jurisdiction in which their underlying assets are custodied.

Transparency

Proof of Reserves

Currently, there is an absence of proof of reserves. The claim of 1:1 BTC backing without proof of reserves readily available and audited by a third party (see: Paxos, Circle, wBTC, etc) damages the integrity of cbBTC. This failure of transparency fosters a significant dependency of trust in Coinbase; opposite to the moral compass of Inverse Finance, and the mission statement of DOLA as a decentralized debt-backed stablecoin.

Admin Policy

Coinbase is non-transparent of all asset administrative policy including but not limited to:

- Contract upgrades
- Assigning minters
- Blacklisting
- Ownership configurations
- Pausing

Particularly concerning is the ability to upgrade, blacklist and pause cbBTC triggering a stopped state for all users or targeted users. Mentioned above, these risks are common among custodial assets and creates a dependency on the issuing entity and jurisdiction of custody.

A key difference between cbBTC and similar sUSDe assets lies in their blacklisting mechanisms. In the case of cbBTC, during any transfer, the system checks whether the `msg.sender` is blacklisted. This applies to any actions involving collateral on FiRM, including deposits, withdrawals, and liquidations. Essentially, if the market (i.e., the entity involved in these actions) is blacklisted, the system will block further transactions, effectively bricking the market.

In contrast, sUSDe operates with a different approach. It does not check the `msg.sender` during transfers. Instead, individual escrows associated with specific accounts would need to be blacklisted for restrictions to be enforced. This makes the blacklisting process in sUSDe more granular, targeting individual participants rather than the entire market in the way cbBTC does.

Security Operations

“Coinbase employs state-of-the-art wallets, regular audits, and comprehensive monitoring systems to safeguard the BTC backing cbBTC. Additionally, all smart contracts involved in the minting and redemption process are rigorously tested and audited by third-party security experts. Coinbase engaged OpenZeppelin in an audit of the cbETH smart contract contract (link) which was also used for cbBTC. **No material contract code has been modified in deploying cbBTC**.” *-Coinbase Whitepaper*

Contract Audits

- ☐ **Audit -** OpenZeppelin

“The goal of this project is to introduce wrapped assets for Coinbase whether they are staked or not. The StakedTokenV1 staked token, which inherits and extends from Centre’s FiatTokenV2_1, is issued to represent the corresponding staked wrapped asset, while a plain FiatTokenV2_1 is used for non-staked wrapped tokens. The only difference between the two is that staked wrapped tokens implement an exchangeRate parameter to improve composability with the ecosystem.” *-OpenZeppelin*

- ☐ **Unresolved Issues**

“In the initialize functions of the ExchangeRateUpdater and MintForwarder contracts, the newTokenContract parameter is not checked to be either a valid contract or an ERC20 token. Moreover, the newOwner can be either an EOA or a contract but this is not described in the docstrings.

Consider improving the docstrings to reflect the exact intended behaviour, and using Address.isContract function from OpenZeppelin’s library to detect if an address is effectively a contract. Moreover, consider adopting the Initializable to implement the current functionality.

Update: Partially fixed as of commit 273a2b8 in PR #3. While docstrings have been added, there are no checks for the input address parameters.”

Bug Bounty Program

- ☐ **Program**

Coinbase's bug bounty program is hosted on HackerOne. The program offers rewards based on the severity of the issue, with payouts ranging from $200 for low-severity bugs to $1,000,000 for critical vulnerabilities. Over $2MM in bounties have been paid up to date, and they maintain a transparent operation.

Competitive Analysis

Competitive Markets

- ☐ **Competitor Market**

cbBTC is set to enter a competitive landscape for wrapped Bitcoin assets, primarily dominated by WBTC. Aave has already signaled its intent to integrate cbBTC, which will allow users to supply and borrow against it in the Aave V3 markets. Currently, WBTC dominates the supply and borrow markets on platforms like Aave, Compound, and MakerDAO, with billions of dollars in TVL. Aave’s integration of cbBTC will increase competition in the wrapped Bitcoin space, and as liquidity deepens, it is likely that cbBTC will offer similar supply and borrow capabilities as WBTC. Chaos Labs and LlamaRisk, security providers for Aave, seem intent on deploying with iInitial conservative parameters, notably with a LTV (CF) of 73% and Liquidation Threshold (LF) of 78% and Liquidation Bonus (LI) of 7.5%.

- ☐ **Risk Assessment(s)**

https://governance.aave.com/t/arfc-onboard-cbbtc-to-aave-v3-on-base-and-mainnet/18988/11

- ☐ **Notable competitor failures**

There have been no notable failures related to cbBTC in lending protocols, as cbBTC was only recently launched on September 12th, 2024.

Technical Contract Analysis

Contracts

- ☐ **Collateral Contracts**

Collateral: cbBTC

- ☐ **Deployed Contracts**

Market: cbBTC Market

Escrow Implementation: SimpleERC20Escrow

Price Feed Contracts: Chainlink cbBTC/USD

Ownership and Operational Structure

- ☐ **Administrative**

- Admin **-** upgrade the contract, and re-assign itself
  - **EOA:** 0x5e8114643966B7FD7d5CfdD8695FfC5c51fF32c0
- Owner of RateLimit contract
  - can configure a caller and define their rate limiting parameters
  - can remove a caller
- Owner of MintForwarder contract
  - can initialize the contract by setting the token contract address where the mint calls are forwarded and transferring ownership to a new owner
- Owner of ExchangeRateUpdater contract
  - can initialize the contract by setting the token contract address for which the exchange rate is needed and transferring ownership to a new owner
- Owner of StakedTokenV1 contract
  - inherits all the owner privileges from Centre's FiatTokenV2_1
  - can update the oracle that provides exchange rates
- Caller
  - can mint tokens
  - update exchange rates

- ☐ **Roles**

- Owner **-** re-assign any of the roles except for admin

    - **EOA**: 0xCe56D20689D836EC7A728CEb94A15746696c16e6
- masterMinter - adds and removes minters and increases their minting allowance
    - **EOA:** 0x1302dFb1F806398f48650c75ab0fDA9a0186f47B
- minters - create and destroy tokens

Each minter has a *mintingAllowance*, which Coinbase configures. The mintingAllowance is how many tokens that minter may issue, and as a minter issues tokens, its mintingAllowance declines. Coinbase will periodically reset the mintingAllowance via the Interval Minter contract. The mintingAllowance is to limit the damage if any particular minter is compromised.

Minter #	Address	Minting Allowance
1	0x000000000CBDC84a73055389D392710263Bb31e7	100000000
2	0xC2ddb1c13e566Fd29Ec86e3e2eD6eFf1aB1701C3	0
3	0xC2ddb1c13e566Fd29Ec86e3e2eD6eFf1aB1701C3	0
4	0x8CF8e70BbB643b083683fCE4896f2885F73Af8B7	10000
5	0x8CF8e70BbB643b083683fCE4896f2885F73Af8B7	10000
6	0xCE97003ea2E0a565A9a0b6e36209c6ddaaa14B05	10000
7	**0x000000000CBDC84a73055389D392710263Bb31e7**	**6086700000000**

- pauser - pause the contract, which prevents all transfers, minting, and burning
    - **EOA**: 0x1ac78dfcAE082E9fe286D1ccb12C17a3e906B906
- blacklister - prevent all transfers to or from a particular address, and prevents that address from minting or burning
    - Contract: 0xF903f3A8B30a7b645e76DB8511b4121cc96160EB
    - Blacklisted Addresses

☐ **Strategies or Supplemental Contracts**

None, as the asset is wrapped not staked. However an upgraded staked wrapped asset would adopt the following contracts

- RateLimit
- MintForwarder
- ExchangeRateUpdater
- StakedTokenV1

The Ownership of an upgraded contract would inherit all the owner privileges from the previous.

Contract Upgradability & Immutability

- ☐ **Is the Contract an Upgradable Proxy? What Mitigation is acceptable given the Risk Profile eg. Timelock, Multisig, Burning Keys**

Yes. cbBTC proxy contract has been initialized as a “non-staked” wrapped asset “StakedTokenV2_1” which inherits Centre’s battle tested StakedTokenv2_1 codebase.

The proxy includes upgradability to initialize a staked wrapped asset which would introduce an “exchangerate” parameter. In this event the underlying integrity of cbBTC is assumed unchanged, yet the architecture of the product would extend to include a yield bearing version.

- ☐ **Upgrading**

“The Fiat Token uses the zeppelins Unstructured-Storage Proxy pattern [https://docs.zeppelinos.org/docs/upgradeability_AdminUpgradeabilityProxy.html]. FiatTokenV1.sol is the implementation, the actual token will be a Proxy contract (FiatTokenProxy.sol) which will forward all calls to FiatToken via delegatecall. This pattern allows Coinbase to upgrade the logic of any deployed tokens seamlessly.

Coinbase will upgrade the token via a call to upgradeTo or upgradeToAndCall if initialization is required for the new version.
Only the admin role may call upgradeTo or upgradeToAndCall.” -*Wrapped-tokens-os*

Oracles, Liquidations & Escrow

Price Feed(s)

- ☐ **Chainlink / EMA / Advanced Solutions**

- cbBTC-USD Chainlink Price Feed (86400 , 2% Deviation Threshold)

To ensure accurate and reliable valuation of cbBTC on FiRM, we can utilize Chainlink’s cbBTC-USD price feed.

- ☐ **Fallback Feed**

None preferred at this time

- ☐ **Peg Risks**

Limited; assuming the Coinbase trust dependency, custodial and jurisdictional risk. Though the lack of proof of reserves is a repeated concern throughout the assessment. The Coinbase cbBTC whitepaper makes mention of fees, stating that there are no fees associated with minting/wrapping or burning/unwrapping today. If fees were implemented in the future, this would work slightly against the 1:1 peg arbitrage unless maliciously implemented which is unexpected.

Escrow

- ☐ **Does Implementation Require Voting or Claim Delegation?**

No, the cbBTC market will implement a SimpleERC20escrow

Liquidations

- ☐ **Liquidation Routes**

Simple On-Chain via dex liquidity or Coinbase users.

Collateral Analysis

Token Statistics (cbBTC)

Price	$63,267.52
Max Supply / Total Supply	∞
Circulating	1,968
veLocked & Average Duration	N/A
FDV / Market Cap	$124,556,777

Liquidity

- ☐ **Mainnet Dex Liquidity**

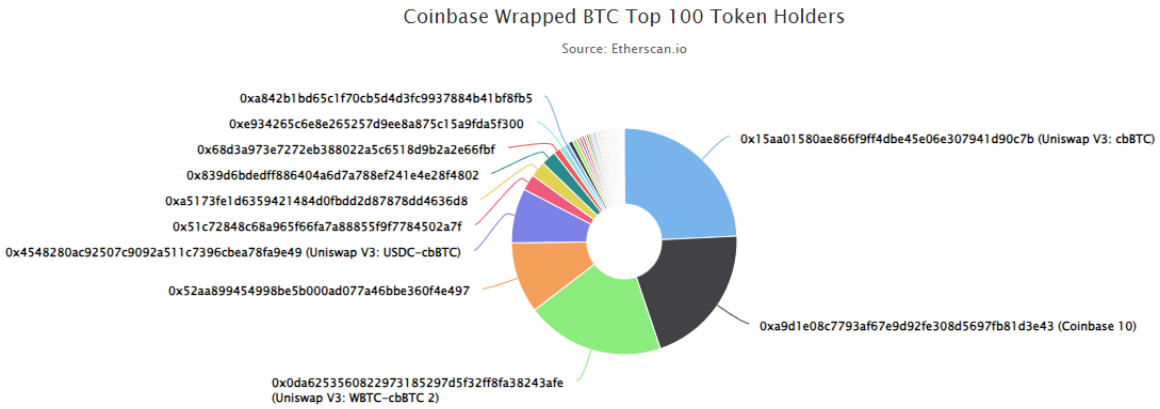
As of September 19, 2024…

LP	Protocol	TVL ($)	Paired Asset Depth ($)
ETH-cbBTC	UNIv3	$32M	$16M
wBTC-cbBTC	UNIv3	$28M	$15M
USDC-cbBTC	UNIv3	$12M	$6M

wBTC-cbBTC	Curve	$5.5M	$4M
TOTAL		**$77.5M**	**$41M**

☐ **Token Holders**

[Token Holders: 520]



cbBTC holdings are adequately decentralized with the top three holders being Uniswap V3 Lps and Coinbase.

Asset Score

Component	Link/Rationale	Score
Market Capitalization	MCS=min(10, (cbBTC Supply * cbBTC Price * 200) /(wETH Supply * wETH price)	3.46
DEX Trading Volume	TVS =min(10, (30 Day Avg Token Trading Volume * 200 / 30 Day Avg wETH Trading Volume)	0.79
Price Volatility	PVS =min(10, 10 - (Token Log Price Volatility / wETH Log Price Volatility) * 9)	9.59
Token Distribution	Token Distribution Score = min((1- Token Gini Index) * 10 / (1 - wETH Gini Index);10)	5.97

Conclusion

Parameter Model

LF and Min Debt FiRM Market Framework

Parameter Recommendations

The RWG utilizes both quantitative and qualitative measures to come up with market parameter recommendations. Background information on the data-driven methodologies can be accessed following the following links:

- FiRM's New Guard: Minimum Debt Amounts
- Balancing Act: An Insight into FiRM Market Parameter Setting
- Behind the Scenes: LP Analysis and FiRM Daily Borrow Limits Framework

The interaction between different parameters is complex and often non-linear. Our in-house models provide valuable insights into these dynamics, enabling us to fine-tune the parameters for optimal performance. When modeling for parameter values, we value above all else that current settings are generally favorable for liquidators. This is crucial as active liquidator participation is essential for the health of the protocol. At the same time, analysis should also suggest that parameters we decide on are such that liquidation cascades are extremely unlikely given present-day on-chain liquidity and competitive markets.

The following launch parameters will ensure a conservative approach, prioritizing security and stability while we gather live market data and run more simulations. This method allows us to mitigate risks and adjust parameters usually after an initial trial period based on real-world performance and analytics. The parameters also align closely with comparable market settings, which have been thoroughly tested and proven effective. These are:

Supply Ceiling	10,000,000 DOLA
Daily Borrow Limit	1,000,000 DOLA
Collateral Factor	80%
Liquidation Factor	50%
Liquidation Incentive	10%
Minimum Debt Amount	3000 DOLA

These settings are designed to provide a robust starting point that balances the need for sufficient liquidity and market activity with the need to manage risk prudently. The supply ceiling and collateral factor settings relate to the profiling of BTC due to trust assumptions already built into cbBTC. The daily borrow limit is set conservatively to accommodate for future increases

when the asset has gained further marketwide adoption. The liquidation factor was determined via simulations for total gasused and making use of our developed framework. Additionally, a liquidation incentive of 10% is designed to provide sufficient motivation for liquidators to maintain market health.

If the market reaches its limits or demonstrates stability, a comprehensive deep dive will follow, incorporating both qualitative risk assessments and further quantitative analytics to refine our parameter settings. This iterative process ensures that our market parameters remain responsive to actual market conditions and user needs, promoting both security and growth within the FiRM ecosystem.

The RWG is committed to continuous monitoring and analysis. We understand that the DeFi landscape is ever-evolving, and our models and strategies must adapt accordingly. We welcome feedback and discussions from the community on our findings and methodologies. Your insights are invaluable in helping us refine our approach and ensure the long-term success and security of FiRM.