Overview

This is a review of Phoenix Labs' proposal to reactivate the WBTC market on Mainnet as a collateral and borrowable asset.

Purpose

While WBTC in circulation has fallen significantly during the bear market, from 280,000 BTC at peak to a trough of 150,000 BTC, it still represents one of the largest and most liquid ERC20 tokens. Additionally, circulating supply has been growing somewhat since February of this year, and currently stands at 163,000 BTC (~$5.5 billion). WBTC is widely used as collateral across lending and stablecoin protocols, including over 30,000 WBTC supplied on Aave and 80 million DAI borrowed from Maker core.

[

693×471 13.8 KB

](//makerdao-forum-backup.s3.dualstack.us-east-1.amazonaws.com/original/3X/c/7/c775ed6b16a2cc47f519b7b442c15a3e69765efe.png)

Source: Coingecko WBTC Marketcap Chart

Adding WBTC support to Spark may drive increasing DAI borrowing and overall increase in adoption, and provides a differentiated value proposition versus using WBTC vaults: cross margining with other collaterals, earning yield on WBTC, and being able to short other assets such as ETH (to put on a short ETH/BTC position).

While WBTC was initially frozen on Spark due to concerns over alignment with scope rules such as decentralized collateral rebate, this is no longer a primary concern. As such, the strategic benefits of adding WBTC to Spark outweigh the costs as long as risk can be effectively managed.

Risk Evaluation

WBTC is a fully collateralized BTC token on the Ethereum network. It has broad integrations across CEX and defi protocols, including core Maker vaults. BTC is generally considered the most lindy and highly liquid asset in crypto, and WBTC can take advantage of the deep global liquidity for Bitcoin via minting and redemption from the issuer Bitgo.

Our previous risk assessment of WBTC can be foundhere. While market conditions have changed, overall WBTC liquidity remains robust.

While WBTC is expected to closely track BTC price in normal conditions, it bears additional risk factors due to being a centralized bridged token. At a high level, risk factors include:

- Custody and key management risk
- Misappropriation or other failure of internal controls
- Counterparty risk with respect to the Bitgo legal entity
- Censorship risk
- Business continuity risk

We discuss each class of risk in more detail below.

Custody and Key Management Risk

Bitgo keeps custody of underlying native BTC used to back issued WBTC. If relevant wallets are hacked or private keys are lost, WBTC would no longer be fully backed. The process for dealing with a capital loss are unclear, and may include recapitalization with Bitgo's own funds, pro-rata socialization of losses to all WBTC holders, or taking no action and continuing to process mints and redemptions as normal. The default option of taking no action would likely result in a disorderly bank run with the last to redeem bearing all of the losses.

Bitgo also manages the Ethereum network keys used for minting and redemption of WBTC tokens. If the mint keys are compromised, an attacker may be able to mint unlimited WBTC, draining all liquidity pools and resulting in WBTC becoming underbacked. While Bitgo may be able to salvage some value by freezing redemptions and reissuing new WBTC tokens via a snapshot, this would cause severe disruption and would likely involve significant realized losses for holders.

Misappropriation

Certain Bitgo employees and service providers may have privileged access to WBTC wallets and other critical systems. While Bitgo has a long and relatively successful track record as a crypto custodian, the risk of misappropriation and other

insider attacks cannot be ruled out. Relatively little information is known about Bitgo's internal controls and key management processes; this makes sense to avoid giving potential attackers sensitive information, but also limits the publics' ability to assess the adequacy of these protections.

Counterparty Risk

Bitgo is a qualified custodian, which provides significant legal protections to custody service users including a requirement to segregate assets and ensure client funds are senior to other creditors. However, it is unclear if WBTC would benefit from these protections in the event of insolvency, as WBTC holders do not have custody accounts at Bitgo. WBTC also lacks the formal legal structuring of investment trusts and other regulated tradfi products. In the event Bitgo becomes insolvent, WBTC holders may be treated as general unsecured creditors, with claims potentially having equal or lower priority to other Bitgo creditors and clients. This may be the case even if the insolvency is unrelated to the WBTC business. Therefore, WBTC holders may have general credit risk exposure to Bitgo and business lines unrelated to WBTC.

Certain recent news may indicate the materiality of these risks. For example, Bitgo began an acquisition process for Prime Trust earlier this year, only to back out mid way through before it emerged that Prime Trust was insolvent and had severe issues with internal controls. If this acquisition had gone through, this additional debt burden may have impacted Bitgo's operations. Bitgo also signed a deal to be acquired by Galaxy Digital in 2021, but Galaxy backed out in 2022, citing a breach of contract due to Bitgo's failure to provide audited financial statements meeting requirements. Bitgo's subsequent court case against Galaxy was dismissed. While Galaxy had significant exposure to Terra and may have canceled the deal for other market related reasons, citing lack of audited financials does raise some concern over Bitgo operations.

Censorship Risk

While the WBTC token is non-upgradable and does not include a function enabling blacklisting of individual addresses, there are several other potential censorship risk vectors. The WBTC contract has a global freeze function that can be triggered to prevent any transfers; it appears that this function is triggerable by the 8 of 12 multisig that owns the controller contract for WBTC. Signers may take direction from or be under common control with Bitgo, and Bitgo could theoretically single out users by getting the multisig to pause the existing WBTC contract and reissuing new tokens. Bitgo also has discretion over who is permitted to mint or redeem WBTC. Finally, the underlying BTC reserves may be subject to legal or regulatory processes resulting in freezing or seizure. A global freeze on WBTC transfers would prevent any liquidations from taking place, while censorship of minting/redemptions or seizure of underlying reserves could cause WBTC price to diverge from BTC.

Business Continuity Risk

WBTC's parity with BTC depends on continuous minting and redemption capabilities. Bitgo's primary market operations may be interrupted unexpectedly, due to either technical or operational issues. While Bitgo has managed their creation and redemption program successfully in the past and maintained high uptime, it is theoretically possible for primary market liquidity to become unavailable for an extended period (eg. if their infrastructure is attacked, if key merchants involved in the primary market fail, if Bitgo enters administration or sells the WBTC product to another entity, etc). This may result in WBTC price diverging from BTC even if there has been no impairment of the underlying reserves.

In recent times, the greatest discount WBTC has traded at was 0.989 BTC, which occurred on 25 November 2022 in the aftermath of the FTX and Alameda collapse. This was driven by operational issues with merchants/market makers (Alameda was a key merchant and others may have been impacted by exposure to FTX), as well as general fear over wrapped assets and custody risk (eg. FTX's Solana Sollet wrapped assets became unbacked during the collapse). Bitgo released a statement at the end of November 2022 here.

Risk Mitigation

While BTC is a core crypto asset, with deep liquidity and relatively low volatility, additional risks attributable to WBTC pose non-negligible risk to defi integrations. The WBTC specific risks all tend to be bi-modal: while these risks are unlikely to materialize, in cases where they do they could cause significant and sudden impacts on WBTC, up to and including a complete loss of all token value. This makes certain standard risk mitigation levers for crypto assets, such as limiting LTV and liquidation thresholds, relatively less effective. Values that would be conservative enough to materially reduce these tail risks may drive away organic usage and lead to a winner's curse scenario where the borrowing capacity is only used in cases of adverse selection.

Maker core vaults have several useful mechanisms and features that help address WBTC tail risks. DC-IAM parameters limit the total debt available to be minted against WBTC at any one time, as well as the maximum rate of increase to exposure. Each vault type can also charge an individual stability fee, which allows Maker to earn a higher level of risk compensation for WBTC exposure versus alternative assets with lower tail risk such as ETH. And finally, Maker core vault collateral is not globally rehypothecated, which means that exposure to catastrophic WBTC failure is strictly limited to existing debt exposure plus maximum exposure increase until governance mitigations can be implemented. In protocols with rehypothecation such as Spark, failure of one collateral asset can potentially cause cascading insolvency across all markets within the protocol.

Given that the most prominent risks of WBTC are primarily tail risks with a potential for total loss, the most effective risk

mitigation mechanisms are limits on total collateral exposure. On Spark, the two options for limiting exposure are using isolation mode with corresponding debt ceilings, or limiting supply caps to indirectly limit maximum collateral exposure.

Using isolation mode has a negative impact on UX, as users are not able to use multiple collateral assets at once within a cross margined position. But, it has the benefit of a more direct limit on collateral exposure which doesn't fluctuate with collateral value. And in Spark's case, it also eliminates the risk of cascading failures from rehypothecation as the only asset borrowable in isolation mode, DAI, is not usable as collateral.

The alternative of using supply caps to limit risk preserves users' ability to cross margin positions, but makes total potential exposure more variable and potentially unbounded when considering the risk of losses in other rehypothecated collateral assets. This may also limit users' ability to top up their position with additional collateral, or could allow some users to be crowded out from borrowing capacity by large deposits with relatively low collateral usage.

Also note that Maker core can rapidly set the Spark D3M debt ceiling to zero with the MOM-line mechanism, which has an exception to the governance security module delay. This could prevent additional DAI from being supplied to Spark in a case where WBTC failure causes losses.

Parameter Selection

To gauge whether total exposure to WBTC is appropriate, we can compare it against Maker core surplus buffer, as well as Spark TVL metrics. If WBTC maximum loss exposure is equal to or less than Maker surplus buffer, this gives Maker governance and end users a high level of confidence that any issues with WBTC would not impact the health of the protocol overall. While Maker has additional exposure to WBTC with 85 million DAI debt from core vaults, these vaults use isolated margin and have higher collateral requirements, which limits overall risk.

In cases where WBTC exposure exceeds the surplus buffer by a reasonable ratio, comparison to TVL on Spark can also become important as this helps determine the risk of cascading market failure due to collateral rehypothecation. As an example, if WBTC fails while some positions are using it as collateral to borrow ETH, this increases liquidity risk of the ETH market as a certain share of borrowed ETH is effectively unbacked and will not be repaid. If ETH reaches 100% utilization (particularly if all remaining borrows are backed by insolvent WBTC accounts), then keepers will not be willing to participate in liquidations of this collateral, which can expose Spark to further losses based on ETHUSD price changes. The risk of this happening depends on user confidence; if confidence is lost, then users will rush to withdraw all assets, causing a bank run and cascading failure of all assets on Spark. Keeping total WBTC loss exposure within a reasonable threshold helps limit this risk, as users will remain more confident in Spark's ability to address any deficit without markets becoming illiquid.

We can gain some perspective on the insolvency levels required to provoke a bank run by reviewing losses at other lending protocols. Venus Protocol incurred significant losses from several manipulation and insolvency events, with bad debt peaking at around 10% of TVL, without causing a bank run. Inverse Finance suffered multiple hack and loss events, and while their core Compound fork lending market did suffer from cascading failure, their stablecoin DOLA was able to hold the peg despite bad debt representing as much as 50% of circulating token supply at certain points. Identifying specific tipping points is difficult, but generally risk parameterization should keep WBTC loss exposure at no more than 200% of surplus buffer and 20% of Spark TVL. This should be well within the capacity of Spark protocol to repay over time (potentially with assistance from Maker core, although Maker has an additional 85 million DAI exposure to WBTC through core vaults), and maintain sufficient user confidence to avoid a run. Note that use of isolation mode can significantly reduce risk due to lack of rehypothecation risk across unrelated collateral assets, but is not recommended here due to negative impact on user experience.

In addition to limiting total loss exposure, which protects against tail risk scenarios with significant impairment of WBTC, Spark can also carefully select liquidation penalties to ensure successful liquidations during less severe or temporary price divergence events. Aave markets apply a 5% penalty on Ethereum mainnet, and somewhat higher penalties (6.25% to 7.5%) on multichain deployments. Compound v3 USDC on Ethereum similarly applies a 5% penalty to WBTC liquidations. To ensure liquidations are processed promptly even when WBTC prices from BTC pricing used for oracles, it is recommended to use a 7% liquidation penalty on the Spark deployment. This will ensure WBTC collateral liquidations remain profitable until WBTC price discount vs BTC reaches up to 7%, and should also lead keepers to prioritize Spark liquidations when positions on multiple lending protocols are being liquidated concurrently via higher profit margins.

Selection of interest rate model parameters was roughly based on Aave v3 Ethereum parameters, which have proven safe over time. Optimal borrow rate was reduced from 4% to 2% and utilization kink increased from 45% to 60%, while maintaining a high maximum borrow rate of ~300% APR. With WBTC borrow costs trending towards an equilibrium of roughly 1%, this should increase expected WBTC supply yield from 0.09% seen on Aave to ~0.24%, while still maintaining more than adequate protection against liquidity risks.

Future Risk Mechanisms

While the above risk strategies are available now, Spark may be able to take advantage of alternative mitigation strategies by implementing additional features. Possible options include:

- Parameter automation for debt ceilings, supply caps, and borrow caps (similar to DC-IAMs) to limit available exposure and maximum exposure growth rate

- Freezing WBTC market and preventing new debt from WBTC collateral triggered by price deviations (eg. using Chainlink WBTC/BTC oracle) or very large WBTC mints
- Advanced oracle filtering strategies using both BTCUSD and WBTCBTC feeds (eg. using min(WBTCBTC, 1) when measuring collateral value, and max(WBTCBTC, 1) for borrowed asset value)
- Proof of reserve oracles for WBTC
- Price discrimination mechanisms (eg. charging a premium on WBTC collateralized debt)

Specification

Reactivate (unfreeze) WBTC market and implement the following parameters:

- Maximum LTV: 70%
- Liquidation threshold: 75%
- Liquidation penalty: 7%
- Supply cap: 3,000
- Borrow cap: 2,000
- Reserve factor: 20%
- Base rate: 0%
- Optimal rate: 2%
- Max rate: 302%
- Optimal utilization: 60%
- Efficiency mode: No
- Isolation mode: No
- Debt ceiling: n/a
- ~$78,000,000 effective risk exposure (~10% of TVL, ~155% of Maker surplus)
- ~$78,000,000 effective risk exposure (~10% of TVL, ~155% of Maker surplus)

References

- Phoenix Labs parameter proposal: Proposal to Adjust SparkLend Parameters
- Original Maker WBTC listing discussion: [WBTC] - WBTC Collateral Request For Comment
- WBTC token contract: https://etherscan.io/token/0x2260fac5e5542a773aa44fbcfedf7c193bc2c599
- WBTC owner multisig (8 of 12): https://etherscan.io/address/0xB33f8879d4608711cEBb623F293F8Da13B8A37c5#code
- WBTC owner multisig (8 of 12): https://etherscan.io/address/0xB33f8879d4608711cEBb623F293F8Da13B8A37c5#code
- WBTC Coingecko listing: https://www.coingecko.com/en/coins/wrapped-bitcoin
- Bitgo details:
- Website: https://www.bitgo.com/
- WBTC website: https://wbtc.network/
- Reserve details: Wrapped Bitcoin (WBTC) an ERC20 token backed 1:1 with Bitcoin
- Website: https://www.bitgo.com/
- WBTC website: https://wbtc.network/
- Reserve details: Wrapped Bitcoin (WBTC) an ERC20 token backed 1:1 with Bitcoin

- Chainlink oracles:
- BTCUSD: BTC / USD | Chainlink
- WBTCBTC: wBTC / BTC | Chainlink
- BTCUSD: BTC / USD | Chainlink
- WBTCBTC: wBTC / BTC | Chainlink
- News and blogs:
- Galaxy acquisition announcement: Galaxy Digital to Acquire BitGo to Form Pre-Eminent Global Provider of Digital Asset Financial Services for Institutions
- Failed acquisition news: Galaxy Digital's Termination of $1.2B Acquisition of Crypto Custodian BitGo Upheld by Federal Judge
- https://www.newswire.ca/news-releases/galaxy-announces-termination-of-bitgo-acquisition-806604223.html
- Bitgo acquisition of Prime Trust (cancelled): BitGo Signs Letter of Intent to Acquire Prime Trust to Expand Digital Asset and Fintech Infrastructure Services Worldwide | by BitGo Editor | Official BitGo Blog
- Bitgo response to FTX collapse: WBTC Status: All Operations Continue to Run Smoothly | by BitGo Editor | Official BitGo Blog
- Bitgo series C funding round: BitGo Secures $100M Series C Funding At $1.75B Valuation
- Galaxy acquisition announcement: Galaxy Digital to Acquire BitGo to Form Pre-Eminent Global Provider of Digital Asset Financial Services for Institutions
- Failed acquisition news: Galaxy Digital's Termination of $1.2B Acquisition of Crypto Custodian BitGo Upheld by Federal Judge
- https://www.newswire.ca/news-releases/galaxy-announces-termination-of-bitgo-acquisition-806604223.html
- Bitgo acquisition of Prime Trust (cancelled): BitGo Signs Letter of Intent to Acquire Prime Trust to Expand Digital Asset and Fintech Infrastructure Services Worldwide | by BitGo Editor | Official BitGo Blog
- Bitgo response to FTX collapse: WBTC Status: All Operations Continue to Run Smoothly | by BitGo Editor | Official BitGo Blog
- Bitgo series C funding round: BitGo Secures $100M Series C Funding At $1.75B Valuation
- Bad debt evaluation
- RiskDAO dashboard: https://bad-debt.riskdao.org/
- Inverse transparency page: Inverse Finance - Transparency Bad Debts
- DOLA Coingecko page: https://www.coingecko.com/en/coins/dola
- RiskDAO dashboard: https://bad-debt.riskdao.org/
- Inverse transparency page: Inverse Finance - Transparency Bad Debts
- DOLA Coingecko page: https://www.coingecko.com/en/coins/dola