Risk Assessment - “**wBTC**” Collateral Asset on FiRM

Useful Links

- Coingecko
- Website
- Github
- Twitter

Background

Wrapped Bitcoin (wBTC) was introduced in January 2019 as a solution to integrate Bitcoin into the Ethereum network and its DeFi ecosystem. Unlike traditional Bitcoin, which cannot participate in DeFi, wBTC acts as an ERC-20 token representation of Bitcoin, with each wBTC pegged to and backed by a real Bitcoin. This conversion is facilitated either through smart contracts or trusted custodians. When users deposit Bitcoin, it's locked by a custodian and an equivalent amount of wBTC is minted on Ethereum. Conversely, when wBTC is returned, it's burned and the corresponding Bitcoin is released. However, wBTC is not a direct substitute for Bitcoin. It introduces layers of trust not present with native Bitcoin: the reliability of oracle data, the integrity of the conversion bridge, and the solvency of the custodian. Issues like potential hacks, the centralization of decision-making, and dependency on custodians or smart contracts raise security concerns. Such complexities can lead to financial crises in the crypto space, such as a market contagion. Even though wBTC brings Bitcoin's value into other ecosystems, it introduces new risks, and those using wBTC should be cognizant of these challenges and decide accordingly.

BitGo, as the primary custodian of WBTC, plays an instrumental role in ensuring the security and transparency of this tokenization process. However, as with any financial mechanism, it's crucial to assess the inherent risks, especially when introducing asset-backed tokens to decentralized platforms. As such, Inverse Finance’s RWG is undertaking this risk assessment to ensure that all stakeholders are aware of potential vulnerabilities and are equipped to address them proactively.

Protocol Analysis

Org. Structure

- ☐ **Is the Protocol a DAO? How is it governed eg. delegates , snapshot (7)**

BitGo, as the primary custodian for WBTC, is responsible for safeguarding the actual Bitcoin that backs each WBTC token issued on the Ethereum network. BitGo is not a DAO. Instead, it is a centralized company. In the context of the WBTC token, however, there is mention of a "WBTC DAO member," but this refers to the broader WBTC governance structure and not BitGo's internal organizational model. Typical centralized companies like BitGo are governed by an executive team, board of directors, and shareholders. While the whitepaper highlights roles such as the custodian (played by BitGo), merchant, user, and WBTC DAO member, it does not explicitly detail the governance model of BitGo itself.

- ☐ **Does Protocol publish analytics / transparency via Dune or similar (10)**

BitGo operates the wBTC website (https://wbtc.network/) which presents a Dashboard page. The dashboard page presents:

- Order book - A record of all minting and burning of WBTC on Ethereum.
- Partners list - WBTC is a “community-led” project and its partners include merchants, custodians, exchanges, and DAO members.
- Proof of reserves - The custodian performs audits on a regular basis to show transparency through publicly viewable and verifiable transactions.

□ **working group structure (10)**

In the wBTC framework, there are distinct roles that different parties play. Each role comes with its own responsibilities and potential risks.

- **Custodian**: The custodian holds the most crucial role in the wBTC ecosystem. They are responsible for the safekeeping of the actual Bitcoin that backs every wBTC token. For wBTC, BitGo has been named as the custodian.
    - **Responsibilities**: Holding the actual BTC which backs wBTC. Ensuring a 1:1 peg between BTC and wBTC. Executing minting and burning processes for wBTC in response to merchant requests. Participating in regular audits to prove possession of the assets under custody.
    - **Risks & Concerns:**
        - Centralization: BitGo, as a single entity, becomes a central point of failure. If BitGo's systems are compromised, it could jeopardize the backing of all wBTC tokens.
        - Regulatory: As an asset custodian, BitGo must comply with various legal and regulatory standards. Changes or clampdowns in regulatory environments could affect their operation.
        - Trust: Users have to trust that BitGo is faithfully holding the exact amount of BTC corresponding to the circulating wBTC. Even though there are periodic audits, this still presents a trust-based model, somewhat contrary to the decentralized ethos of cryptocurrencies.
        - Operational: Delays or errors in the minting or burning processes could result in users losing funds or facing long wait times.
        - Liquidity: In scenarios where multiple merchants request burning of wBTC for BTC simultaneously, there may be concerns if BitGo doesn't have adequate liquidity to handle all requests immediately.

- **Merchant**: Merchants play a key role in the distribution of the wBTC token. They can request the custodian to mint or burn wBTC. Merchants also handle KYC and AML processes for users. Kyber and Republic Protocol are initial merchants for wBTC.

- **User**: Users are the holders of wBTC. They can transact with wBTC just like any other ERC20 token in the Ethereum ecosystem. They can also approach merchants if they wish to convert wBTC back to BTC.

- **WBTC DAO member**: These members have rights related to the governance of wBTC, including contract changes and adding/removing custodians and merchants. This introduces a level of decentralized governance to the framework.

- ☐ **are core contributors compensated / Doxed (10)**

BitGo, as the main custodian, is a well-known company in the crypto space with a public team. The identities of the main team members of BitGo can be found on the company's official website or professional platforms like LinkedIn.

- ☐ **Any known controversies in crypto space (e.g. Sifu) (10)**

No specific controversy comes up from our preliminary research. However, there is plenty of controversy and tension in the crypto space revolving around the topic of centralized vs decentralized systems and BitGo is not immune to this. Risks with centralized entities such as BitGo include:

1. **Single Point of Failure:** Centralized systems have a more significant risk of becoming single points of failure. If the centralized entity is compromised, it can affect all users.
2. **Censorship:** Centralized entities can be coerced by governments or other organizations to censor transactions or freeze assets.
3. **Transparency Issues:** Without decentralized verification, users must trust that centralized entities are honest about their operations, reserves, etc.
4. **Regulatory Risks:** Centralized entities are more likely to be targeted by regulators, which can impact their operations and, by extension, their users.

- ☐ **do they have a security or risk management team (10)**

BitGo emphasized the importance of security due to its role as a custodian for digital assets. BitGo has always touted its multi-signature wallets, institutional-grade custody services, and pioneering cold storage solutions, which are all measures to enhance the security of the assets they manage. Given the nature of its business, it is highly likely that BitGo has a dedicated security or risk management team. Typically, companies that provide custodial services or manage digital assets on such a large scale will have professionals dedicated to ensuring the safety and security of their platforms, processes, and stored assets. However, specific details about their internal teams or their compositions are not publicly disclosed and might not be for security reasons.

Multisig Structure

- ☐ **Is protocol transparent of multisigs and signers, List/links of multisigs, purpose, and setup x of x (10)**

The WBTC smart contract is owned by a multisig controlled by different DeFi projects. The "Large DAO" multisig signers (listed below) consist of various DeFi protocols, however, the individuals with access to the multisig keys are unknown. Any 8 of these signers can come together to pause or unpause the WBTC smart contract (as well as all WBTC tokens in circulation): B Protocol, Badger, Balancer, BitGo, Chainlink, Compound, Gopax, Krystal, Kyber, Loopring, Multichain, Ren, Tom Bean (bZx)

- ☐ **Can multisigs interfere with collateral options? EOA minting (10)**

While there's no ability for any entity to blacklist or freeze WBTC tokens held in wallets or liquidity pools, it is possible that the 8-of-13 multisig contract can freeze everyone's WBTC and make them untransferable until the contract is unpaused.

Influence, Reputation, and Partnerships

- ☐ **How long has the protocol been around , have they endured long bear markets (10)**

BitGo was founded in 2013 by Mike Belshe and Ben Davenport. BitGo started as a security-as-a-service platform for Bitcoin but has since expanded its services to other cryptocurrencies and blockchain assets. wBTC was launched in January 2019 as a collaborative effort by several organizations, including BitGo, Kyber Network, and Ren (formerly Republic Protocol). So, by the current year (2023), BitGo has been around for approximately 10 years, and wBTC has been in existence for about 4 years.

- ☐ **Have they been exploited and how was it handled , was value restored to users (8)**

There have been no exploits to BitGo. However, recently (March 2023) BitGo's Ethereum (ECDSA) self-managed wallet was found to have a significant vulnerability dubbed the "Zero Proof" vulnerability. Discovered by the Fireblocks cryptography research team, this flaw allowed potential attackers to access the private key share of a client due to missing zero-knowledge (ZK) proofs in BitGo's TSS protocol. Initially identified in the BitGoJS SDK, the vulnerability meant that funds in the affected wallet could be compromised. Upon being notified, BitGo swiftly suspended the affected service and later released a patch to address the issue, mandating clients to update their systems by March 17. The provided information doesn't specify if any funds were stolen or if users were compensated, nor does it indicate any direct exploitation related to wBTC, which relies on BitGo as its custodian.

- ☐ **Current and notable past partnerships , are they a net positive in the DeFi space (8)**

The "Large DAO" multisig signers list includes some well known names in the space, including Chainlink, Compound, Badger, Balancer, as well as some infamous names like Multichain and Republic Protocol (REN).

BitGo's contributions are generally seen in a positive light. As a primary custodian for WBTC, they've facilitated the seamless integration of Bitcoin into the Ethereum DeFi ecosystem. This has increased liquidity and expanded potential use-cases for both Bitcoin and Ethereum. However, some critics argue that the centralized nature of custodial services like BitGo goes against the ethos of decentralization core to the DeFi movement. The dependency on centralized entities introduces trust and central points of failure. This perspective, while important, should be weighed against the benefits of liquidity and integration they provide.

Audits & Bug Bounties

Previous and Ongoing

- □ **Previous and Ongoing audits & bounties with links (5)**

wBTC was audited by renowned blockchain security firm ChainSecurity in late 2018. ChainSecurity's audit primarily focused on the Ethereum smart contract implementations of the WBTC process. They assessed the management of merchants and custodians and the actions related to minting, transferring, and burning of WBTC on Ethereum. The result of the audit was generally positive, with ChainSecurity noting the high quality of the WBTC smart contract and its documentation. However, two issues were identified: one related to pausing the minting/burning process and the other, a possible hash collision issue. These concerns were acknowledged and addressed by WBTC, leading ChainSecurity to confirm that there were no remaining security issues in the latest version.

BitGo introduced the TSS Bug Bounty Program in late 2022. For more on TSS read here. While many MPC solutions remain proprietary, BitGo has opened its technology for scrutiny. Researchers can explore the TSS via tests provided on their GitHub repository for unit testing, key creation, and signing transactions. The primary areas of interest include vulnerabilities like malicious inputs leading to secret leakage, weaknesses in the usage of GPG messages, and potential attacks on the Wallet API. BitGo uses HackerOne to manage its bug bounty submissions. Qualifying vulnerabilities include those that compromise user data integrity, privacy breaches, and unauthorized system access. There doesn’t seem to be an active bug bounty program for wBTC.

Contracts in Scope

- □ **Is the scope a comprehensive list of contracts including collateral and wrappers (0)**

There doesn’t seem to be an active bug bounty program for wBTC.

Reward Payouts

- □ **Rewards paid, vulnerabilities found with severity (0)**

Rewards for qualifying vulnerabilities disclosed in the TSS Bug Bounty Program range from $100 to $20,000, paid in USD or Bitcoin. The reward spectrum covers a wide array of vulnerabilities, from those offering direct server access to those that cause service disruption. The exact reward amount is determined by a panel, factoring in the severity and cleverness of the identified vulnerability.

Though it is not explicitly stated, one can assume BitGo issued a top reward payout to Fireblocks following their vulnerability disclosure mentioned above and covered here.

Collateral Analysis

Oracles

- □ **Available Chainlink Oracles**

There are 13 Chainlink Data Feeds for wBTC Listed below:

PAIR	NETWORK
wBTC/BTC	Ethereum
wBTC/USD	Moonriver
wBTC.e Proof of Reserves	Avalanche
wBTC/USD	Polygon
wBTC/USD	Arbitrum
wBTC Proof of Reserves	Ethereum
wBTC/ETH	Polygon
wBTC/USD	Fantom
wBTC/USD	Avalanche
wBTC/USD	Moonbeam
wBTC/USD	Optimism
wBTC/USD	Harmony
wBTC/BTC	Arbitrum

- □ **Any advanced oracle or market implementation required (10)**

None. A sturdy price oracle mechanism is imperative for market stability and security. The Chainlink price feed for wBTC will act as the primary reference. Additional safety measures, such as FiRM's Pessimistic Price Oracle, will further ensure protection against potential malicious price manipulations.

- ☐ **Peg Risk if any (6)**

Given that BitGo is the sole custodian for the BTC backing WBTC, some trust is required in this centralized entity that they will not go bankrupt, get hacked or fall victim to a regulatory attack. If BitGo turns out to be dishonest or insolvent, then the value of WBTC could potentially diverge from the true value of BTC. Even if there are rumours that BitGo are insolvent or facing regulatory scrutiny, this could cause WBTC to de-peg and and trade at a price lower than Bitcoin's. There's currently no 'hard peg' mechanism in place to guarantee that 1 WBTC = 1 BTC.

wBTC should not be considered a fundamental equivalent to BTC. This common misconception is why many lose money in liquidation crisis events. The value of wBTC depends on three things:

- The quality of the oracle data
- The integrity of the bridge/conversion
- The solvency of the custodian

Wrapped tokens, in this way, require three layers of trust that the original token doesn't need. So, it may seem that the two have the equivalent value for a time. But in bearish markets, the perceived value of the wrapped tokens can drop faster than that of the originals, and in the case of a hack or insolvency, wrapped tokens can quickly break their peg.

Token Statistics

- ☐ **Contracts**

wBTC

- ☐ **Price / Market Cap / Circulating Supply / Locked Supply / True Circulating / Total / Max**

Coingecko

Price	**Market Cap**	**Circulating Supply**
$29,165.00	$4,729,699,748	162,205

Liquidity

- □ **Mainnet Dex Liquidity**

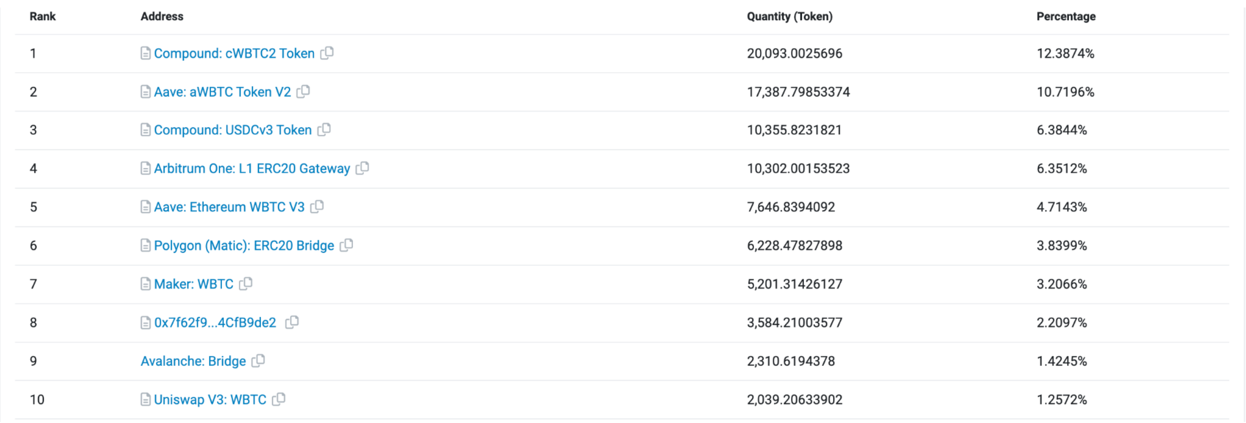
LP	Protocol	Liquidity ($)	24 Hour Volume ($)
TriCryptov2	Curve	$88.08M	$4.47M
wBTC/wETH	Uniswap v3	$204.3M	$1.4M
wBTC/wETH	Uniswap v3	$87.0M	$15.5M
wBTC/USDC	Uniswap v3	$37.8M	$1.6M
wBTC/USDT	Uniswap v3	$12.6M	$591k

- □ On-Chain Slippage

Trade	wBTC ->	DOLA	Slippage (%)
$50,000	1.715	50051	+0.1
$100,000	3.430	100018	+0.02
$250,000	8.575	249891	-0.04
$500,000	17.151	499557	-0.09
$1,000,000	34.302	998060	-0.19
$2,000,000	68.603	1992333	-0.38
$4,000,000	137.207	3972985	-0.68
$6,000,000	205.810	5941581	-0.97
$8,000,000	274.414	7904963	-1.19
$10,000,000	343.018	9839301	-1.61

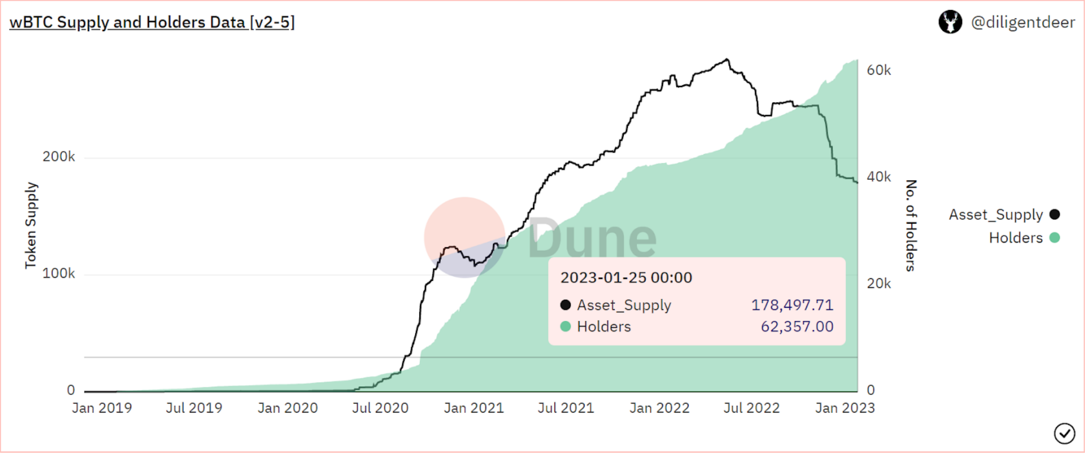
- □ **Token Holders**

Holders: 74,865



Rank	Address	Quantity (Token)	Percentage
1	Compound: cWBTC2 Token	20,093.0025696	12.3874%
2	Aave: aWBTC Token V2	17,387.79853374	10.7196%
3	Compound: USDCv3 Token	10,355.8231821	6.3844%
4	Arbitrum One: L1 ERC20 Gateway	10,302.00153523	6.3512%
5	Aave: Ethereum WBTC V3	7,646.8394092	4.7143%
6	Polygon (Matic): ERC20 Bridge	6,228.47827898	3.8399%
7	Maker: WBTC	5,201.31426127	3.2066%
8	0x7f62f9...4CfB9de2	3,584.21003577	2.2097%
9	Avalanche: Bridge	2,310.6194378	1.4245%
10	Uniswap V3: WBTC	2,039.20633902	1.2572%

WBTC supply peaked before the Terra collapse and at that time made up almost 83% of all the bridged BTC on Ethereum. Following the collapse of FTX in November 2022, FUD began circulating about BitGo's exposure to FTX and possible insolvency. Although BitGo provides proof of reserves, this led to rapid WBTC redemptions and a temporary depeg.



The decreasing WBTC supply coincides with increasing WBTC holders, so it can be inferred that exposure is shifting towards smaller holders of WBTC. Subsequently, it can be said that whales have shown less engagement after May 2022 (Terra collapse) and November 2022 (FTX collapse).

Utility & Use Case

- ☐ **Does the Token have utility (10)**

wBTC acts as a crucial bridge between the Bitcoin and Ethereum ecosystems. Its primary purpose is to represent Bitcoin on the Ethereum blockchain as an ERC-20 token, allowing Bitcoin to tap into the rich world of Ethereum's DeFi protocols. This representation paves the way for Bitcoin holders to participate in various DeFi activities. They can use their wBTC as collateral in lending platforms, provide liquidity on decentralized exchanges, engage in yield farming programs, and even integrate with Ethereum-based dApps. Moreover, wBTC has been pivotal in enhancing interoperability between Bitcoin and Ethereum, two of the largest blockchain networks. By bringing Bitcoin's value and liquidity into Ethereum's innovative decentralized applications landscape, wBTC has given Bitcoin holders expanded avenues to maximize the utility of their holdings in the burgeoning DeFi space.

□ **Goal of the token, where is value derived from (10)**

1. Interoperability: wBTC was introduced to bring the liquidity and value of Bitcoin to Ethereum's DeFi (Decentralized Finance) space. Bitcoin, being the most significant cryptocurrency by market cap, holds substantial liquidity, but its blockchain lacks compatibility with Ethereum's smart contracts. wBTC was developed to bridge this gap.
2. **Integration with Ethereum's DeFi**: By converting Bitcoin into an Ethereum-compatible format (i.e., an ERC-20 token), wBTC allows Bitcoin to be used in various Ethereum-based applications, from decentralized exchanges to lending platforms and more.

Where its value is derived from:

1. **1:1 Peg with Bitcoin**: Every wBTC token is backed by an actual Bitcoin. This means that for every wBTC minted, there's a corresponding Bitcoin locked in a reserve. This peg ensures that the value of wBTC is essentially the same as that of Bitcoin.
2. **Trust in Custodians**: The process of converting Bitcoin to wBTC (and vice-versa) involves trusted custodians. These custodians hold the locked-up Bitcoin and issue or burn wBTC as users deposit or withdraw. The trust in these entities and the verifiability of the reserves they hold underpin the token's value.
3. **Demand in Ethereum's Ecosystem**: As DeFi projects on Ethereum continue to proliferate, there's a growing demand for assets like wBTC. The utility that wBTC provides in Ethereum-based applications can influence its demand, and subsequently, its value, though its price largely follows that of Bitcoin due to the 1:1 peg.

Competitive Analysis

Competitive Markets & Implementation

□ **Competitor Markets with supply & borrow capacity**

Platform	**TVL (MM) ($)**	**Debt (MM) ($)**	**CF (%)**	**Borrow Rate (%)**
Aave	249.97	26.93	73	0.96 (variable)
Curve (crvUSD)	42.93	23.26	N/A	0.63 (variable)
FraxLend	10.33	4.55	75	0.44 (variable)

□ **Competitor Oracle Solutions**

Chainlink

□ **Notable competitor failures**

renBTC by Ren Protocol. MultiBTC by Multichain.

Conclusion

In assessing the risks of wBTC, it's evident that while it offers a bridge between Bitcoin and the Ethereum DeFi ecosystem, it also introduces several layers of complexity and trust not inherent to native Bitcoin. The integration of oracles, conversion bridges, and custodians into the wBTC process can pose security vulnerabilities, centralized decision-making, and potential financial crises. Furthermore, the dependency on smart contracts or custodians, both of which can be exploited or become insolvent, amplifies these risks. Users must weigh the benefits of wBTC's interoperability against these risks.

Asset Score

August 15th, 2023: The RWG evaluated wBTC making use of our in-house comprehensive asset scoring model. This framework evaluates the relative "risk" of wBTC as an asset, using wETH as a benchmark, by considering six essential factors: market capitalization, trading volume, price volatility, token distribution, project fundamentals, and token utility. A breakdown of the Total Asset Score (TAS) follows:

Component	Link/Rationale	Score
Market Capitalization	MCS=min(10, (wBTC Supply * wBTC Price * 200) /(wETH Supply * wETH price)	10
DEX Trading Volume	TVS =min(10, (30 Day Avg Token Trading Volume * 200 / 30 Day Avg wETH Trading Volume)	10
Price Volatility	PVS =min(10, 10 - (Token Log Price Volatility / wETH Log Price Volatility) * 9)	9.17
Token Distribution	Token Distribution Score = min((1- Token Gini Index) * 10 / (1 - wETH Gini Index);10)	10

Project Fundamentals	Risk Assessment wBTC Collateral on FiRM - See Protocol Analysis, and Audits & Bug Bounties Sections	7.75
Token Utility	Risk Assessment wBTC Collateral on FiRM - See Collateral Analysis Section	10
Total Asset Score $TAS = 10 * 0.2 + 10 * 0.15 + 9.17 * 0.15 + 10 * 0.1 + 7.75 * 0.2 + 10 * 0.2$ $TAS = 9.43/10$		

wBTC scores exceptionally in all categories. From this we can draw the following conclusions:

1. Price Volatility: A high score in price volatility suggests that wBTC price experiences minimal fluctuations or instability compared to the benchmark (wETH). This volatility indicates a lesser level of risk associated with wBTC’s price movements.
2. Token Distribution: A high score in token distribution indicates that wBTC tokens are well distributed amongst numerous holders or addresses, potentially resulting in an even distribution of ownership. This distribution speaks to the asset’s decentralization, market stability, and deep liquidity.
3. Market Capitalization: A high score in market capitalization suggests that wBTC has a noteworthy overall market value relative to wETH. A high market capitalization score indicates that wBTC has attained a considerable level of adoption or popularity.
4. Trading Volume: A high score in trading volume indicates that wBTC experiences high levels of trading activity compared to wETH. Higher trading volume generally implies deep liquidity and market interest, making it easier for investors to buy or sell wBTC without significant price impact or slippage. This is also important in the context of liquidations.
5. Project Fundamentals: A high score in project fundamentals suggests that wBTC's underlying project has strong attributes, such as an experienced team, solid technology, and a promising roadmap. This positive evaluation indicates that the project has a strong foundation and potential for success.
6. Token Utility: A high score in token utility implies that wBTC's tokens have diverse use cases and functionality within the associated ecosystem. The higher the score, the more versatile and valuable the tokens are perceived to be. Token utility is essential as it reflects the demand and practical applications of wBTC within its ecosystem.

Parameter Recommendations

Supply Ceiling	5,000,000 DOLA
Initial Fed Supply	2,000,000 DOLA
Daily Borrow Limit	500,000 DOLA
Firm Global Supply Ceiling	47,000,000 DOLA
Collateral Factor	80%
Liquidation Factor	50%
Liquidation Incentive	10%
Minimum Debt	0 DOLA