



Cointelegraph
Research

A Comparative Overview of Bitcoin Wrapping Mechanisms



Content

Introduction	3
Exploring the Spectrum of Bitcoin Wrapping Solutions	3
cbBTC	5
wBTC	5
The Recent wBTC Controversy	6
tBTC	7
renBTC	9
Adoption Metrics and Market Impact	11
The Future of Wrapped Bitcoin	12
Disclaimer	13



Kyrian Alex
Research Analyst

Introduction

Bitcoin ([BTC](#)) is the largest cryptocurrency by market capitalization and an emerging store of value asset. However, its [limited programmability](#) has historically restricted its utility in decentralized finance (DeFi) applications. Wrapped Bitcoin tokens help address this limitation and facilitate the transfer of Bitcoin's value to platforms that are faster and more expressive (Table 2).

However, recent developments have cast a shadow on the reliability of bridged BTC tokens. The node infrastructure of renBTC, once a popular BTC bridge, was [undermined](#) by its financial dependence on Alameda Research, and the project shut down in 2022. WBTC, the largest bridged BTC token, is facing scrutiny due to its [centralized custodianship](#), compounded by the recent involvement of Justin Sun in the project.

These concerns have sparked interest in how bridged Bitcoin protocols operate. This article presents a comparative analysis of Bitcoin bridging solutions and will evaluate their adoption, challenges and future prospects. While trust-minimized solutions have been available for the last few years, bridging infrastructure is still highly centralized at present.

Exploring the Spectrum of Bitcoin Wrapping Solutions

Bitcoin-wrapping solutions exist on a spectrum of decentralization. On one end of the spectrum are fully custodial tokens, such as cbBTC, which rely on a single entity for issuance and custody. While this streamlines their technical implementation, such projects have a single point of failure and are vulnerable to censorship and regulation. Simple federations of keyholders are the most common way to reduce this centralization.

Some federated bridges require all keyholders to sign transactions, while others only need a majority of holders. WBTC, for example, operates with a 2-of-3 multisignature model managed by the BitGo consortium. Despite this added layer of decentralization, wBTC is still considered centralized due to the small number of custodians and their close relationship. The [Liquid Federation](#), on the other hand, has a more distributed trust model in which a large number of trusted, independent companies collectively manage Bitcoin reserves and sign transactions. It operates on an 11-of-15 multisignature scheme.

More advanced bridging models typically achieve decentralization through more sophisticated key-sharing schemes that rely on additional cryptography. One such project that will be discussed later in the article is tBTC v2. Unlike federations that rely on a set of authorized, trusted entities, tBTC v2 uses a staking system. However, at present, it still remains permissioned due to limitations of current cryptography.

Each approach on this spectrum presents its own set of trade-offs between security, decentralization and efficiency. In what follows, we undertake a comparative analysis of four prominent Bitcoin bridging solutions: wBTC, renBTC, cbBTC and tBTC (Table 1). We will delve into their respective architectures and market performance.

Table 1: Comparison of Wrapped Bitcoin Solutions

	cbBTC	wBTC	renBTC	tBTC
Custody model	Centralized	Centralized	Decentralized	Decentralized
Proof of reserve	Not yet implemented (In development)	Implemented	Implemented	Implemented
Governance model	Coinbase manages issuance and custody	BitGo consortium	Darknodes	Threshold DAO
Wrapping mechanism	Custodial	Lock and mint via merchants	Lock and mint mechanism via HTLC	Threshold signatures for issuance
Smart contract mutability	Upgradable	Upgradable	Upgradable	v1 was immutable v2 is upgradable
Transaction fees (excluding gas fees)	0% to mint 0% to redeem	~0.25% to wrap and unwrap	0.2% to mint 0.1% to redeem	0% to mint 0.2% to redeem

Table 2: Exchange Availability of Wrapped Bitcoin Tokens

Token	Tradeable exchanges
cbBTC	Aerodrome, Curve, Aave, Morpho, Compound, Moonwell, Spark and more
wBTC	Uniswap, Aave, Curve, Balancer, MakerDAO, Compound and more
tBTC	Curve, Uniswap, Balancer, Aerodrome and more

cbBTC

Launched by Coinbase, cbBTC operates on a fully custodial model. Coinbase holds users' Bitcoin and issues the corresponding amount of cbBTC on Ethereum or Base. The market share of cbBTC is currently at \$1.3 billion. It thus remains relatively small in comparison to wBTC's \$13.3 billion. However, the product only launched in September 2024 and thus likely still has room to grow. CbBTC is available on several protocols, such as Aerodrome, Curve, Aave, Morpho, Compound, Moonwell and Spark, among others.

While cbBTC benefits from Coinbase's reputation and ease of use, it introduces the same centralization risks inherent in any custodial setup. Issuance and redemption are fully controlled by Coinbase and cannot be triggered by the user. Instead, users have to trade cbBTC through Coinbase or a decentralized exchange to convert it to a different asset.

Therefore, cbBTC is tightly integrated with Coinbase's existing infrastructure, which adheres to strict regulatory standards. For instance, Coinbase can refuse BTC deposits flagged for high Anti-Money Laundering risk or enforce Know Your Customer (KYC) requirements for deposits at any time. This structure aligns cbBTC more with institutional use cases but limits the appeal for those seeking a decentralized wrapped Bitcoin asset.

Coinbase also has not yet implemented a public proof-of-reserves mechanism, though one is reportedly in development. As of now, Coinbase does not publish the Bitcoin addresses backing cbBTC tokens, meaning users must trust the company's internal auditing processes. CbBTC is the only wrapped Bitcoin token in this comparison that does not currently have such a proof of reserve.

wBTC

Launched in 2019, wBTC was the first wrapped Bitcoin token. It currently dominates the market with a capitalization exceeding \$13 billion. WBTC provides real-time proof of reserves, which can be verified at wbtc.network. It has a flat trading fee of 0.25% to wrap and unwrap and is available across various DeFi protocols, including Uniswap, Aave, Curve, Balancer, MakerDAO and Compound, among others.

The custody of the Bitcoin backing wBTC is now managed by BitGo and Bit Global in a joint venture. The keys are geographically distributed between the United States, Singapore and Hong Kong. Funds are held in a 2-of-3 multisignature wallet. The custodians do not handle deposits and withdrawals from users, only from one of 74 so-called merchants elected by the wBTC decentralized autonomous organization (DAO).

The custody of the Bitcoin backing wBTC is now managed by BitGo and Bit Global in a joint venture. The keys are geographically distributed between the United States, Singapore and Hong Kong. Funds are held in a 2-of-3 multisignature wallet. The custodians do not handle deposits and withdrawals from users, only from one of 74 so-called merchants elected by the wBTC decentralized autonomous organization (DAO).

Merchants must first deposit BTC or initiate wBTC burns to trigger the custodians' actions to either mint new wBTC or release BTC to users. End-users, in turn, interact with the merchants to mint or redeem wBTC, optionally through trustless Hashed Timelocked Contracts (HTLCs). However, to do this, the vast majority of merchants impose KYC requirements. This compliance measure allows for regulatory safety but goes against the principle of decentralization that lies at the heart of DeFi.

The Recent wBTC Controversy

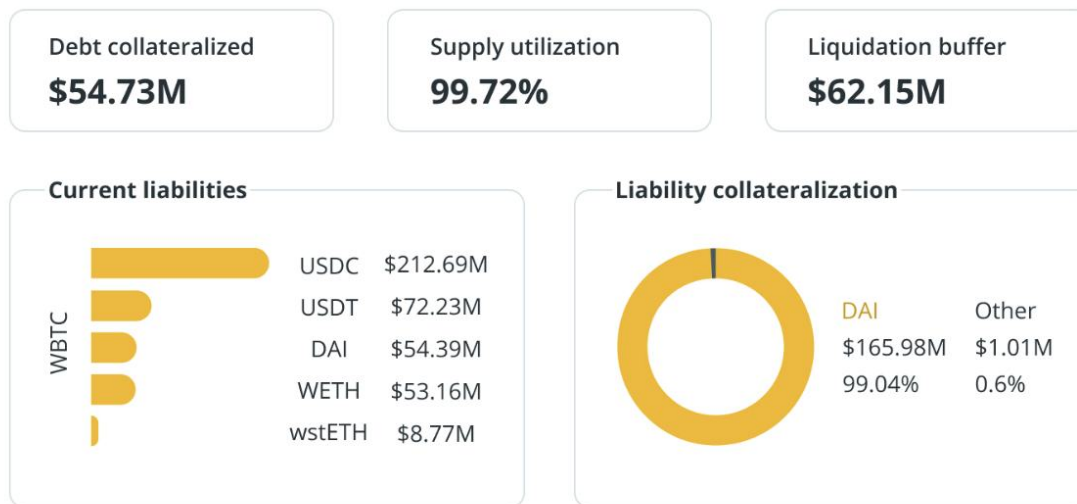
WBTC has recently faced significant controversy due to changes in its custodian arrangements. BitGo initially announced a joint venture with Bit Global, an entity reportedly tied to Justin Sun's Tron ecosystem. The arrangement splits custody across multiple jurisdictions, including Hong Kong and Singapore. Bit Global would control two of the three keys for wBTC's minting and custody.

This restructuring raised concerns about increased centralization and counterparty risk and prompted analysts at BA Labs to recommend limiting wBTC as collateral for Dai (DAI). They cited Sun's controversial history, including his involvement with TrueUSD (TUSD), the handling of Huobi's USDT (USDT) reserves, as well as his alleged connections to stUSDT.

In response to this controversy, MacLane Wilkison of the Threshold Network proposed a plan to integrate wBTC with tBTC's infrastructure. The proposal suggested transferring wBTC's governance to the Threshold DAO and allowing wBTC to be redeemed for tBTC or native BTC. The plan, although ultimately not implemented, proposed the minting of over 1.6 billion new T tokens, which would have been vested with BitGo. This would have significantly reduced the centralization of wBTC.

Despite community backlash over Sun's involvement, the new custodial structure has now been successfully implemented. This prompted MakerDAO (now "Sky") to hold a governance vote on Sept. 19, 2024, which passed with overwhelming support to phase out wBTC collateral. The process, which began on Oct. 3, will conclude by Nov. 28, removing all wBTC-backed debt from Sky's decentralized liquidity protocol, SparkLend (Figure 1).

Figure 1: SparkLend Exposure to wBTC



Source: [SparkLend](#)

tBTC

In September 2020, [Threshold Network](#) launched the tBTC bridge, which now issues the tBTC token. In its [earliest iteration](#), the system relied on [overcollateralization](#) and used the traditional 3-of-3 multisig model to manage Bitcoin wallets. However, it has now successfully switched to a highly distributed custody model that is based on threshold signatures (Figure 2).

Threshold's [minting](#) model relies on a set of [Guardians and Minters](#), the latter of whom are selected from a permissioned set of 35 [beta stakers](#). Minters are responsible for monitoring the Bitcoin main chain for valid deposits. When a deposit is confirmed, Minters initiate a so-called optimistic mint for the equivalent tBTC amount on the Ethereum chain. This process includes a three-hour delay for further verification, during which Guardians can assess the mint request.

Guardians form a larger group of users from the Threshold DAO and DeFi community who verify minting requests within this three-hour security window. If necessary, they can cancel any mint they find fraudulent or halt a Minter's activities. If a Guardian or Minter is found guilty of misconduct, the [Threshold DAO](#) has the power to remove them from the federation.

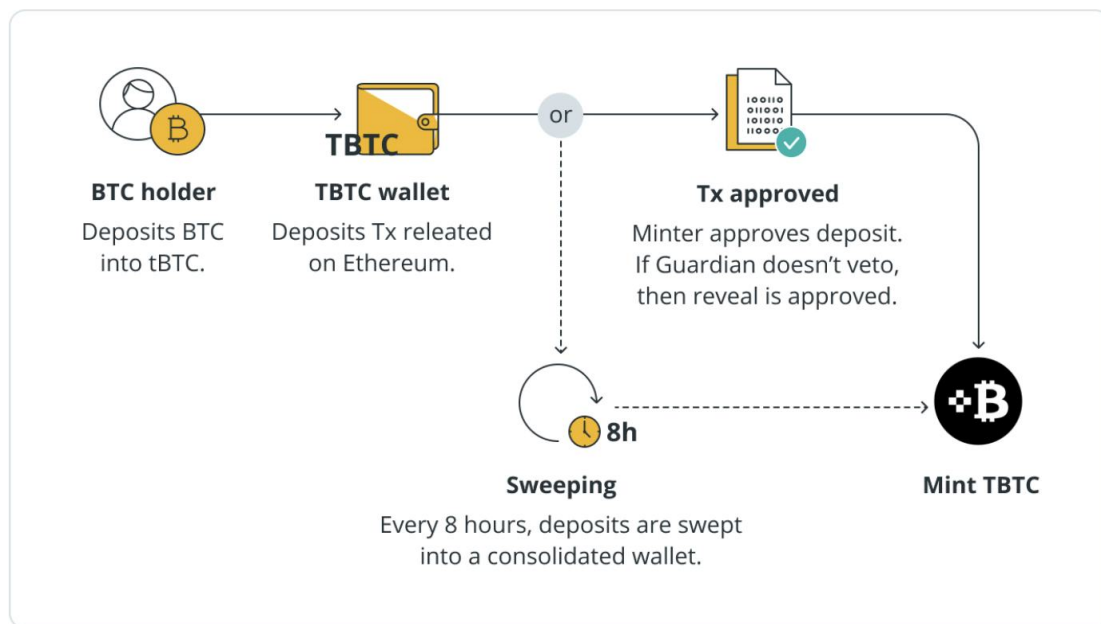
To reduce Bitcoin mining fees and refund time locks, deposit unspent transaction outputs (UTXOs) are periodically consolidated on the main chain by the confederation of signers. This also ensures that the system always maintains the tBTC supply peg, as it prevents small UTXOs from becoming unspendable in high-fee environments.

The BTC custody mechanism and validator infrastructure have changed over the years. Initially, tBTC started with a simple multisig federation. In tBTC v1, signers who held the keys to the multisig had to stake up to 150% of the value of the deposited BTC in the form of Ether ([ETH](#)) to be deterred from malicious behavior. However, this was very inefficient. To address this issue, a community member, Evandro Saturnino, [proposed](#) significant improvements, including transitioning to a threshold signature scheme in tBTC v2.

V2 replaced multisignature addresses with threshold cryptography based on so-called secure multiparty computation (MPC). It is now set to require 51 of 100 signers to access the funds. These changes allowed for improved decentralization and efficient scalability while maintaining security under the assumption of a two-thirds honest majority, a common cryptographic standard.

The validators on the Threshold Network lock up 40,000 T tokens each as collateral to secure the bridge. This staking requirement aligns their interests with network security, as penalties such as slashing can be imposed for downtime or attempted double signing. However, for now, the slashing mechanism is not yet live on the mainnet, which explains why the signing set on the network currently remains permissioned.

Figure 2: How tBTC Is Minted



Source: [Threshold Docs](#)

Threshold initially designed tBTC to be permissionless so that anyone with the required T stake could run a node and act as a custodian; however, there is currently a limitation in the GG18 multiparty signature algorithm, which cannot identify misbehaving signers. This means the implementation of the slashing mechanism remains stalled for the foreseeable future. Currently, alternatives are under development to address the limitation of the GG18 signature algorithm and enable permissionless custodianship in the future.

Despite the significant improvements that Threshold has made over traditional multisig federations, adoption metrics for tBTC remain modest compared to wBTC. It has only attracted a fraction of wBTC's market share at \$417 million. TBTC currently has a mint fee of 0% and a redemption fee of 0.2%. It is available on various DeFi platforms, including Curve, Uniswap, Balancer and Aerodrome.

renBTC

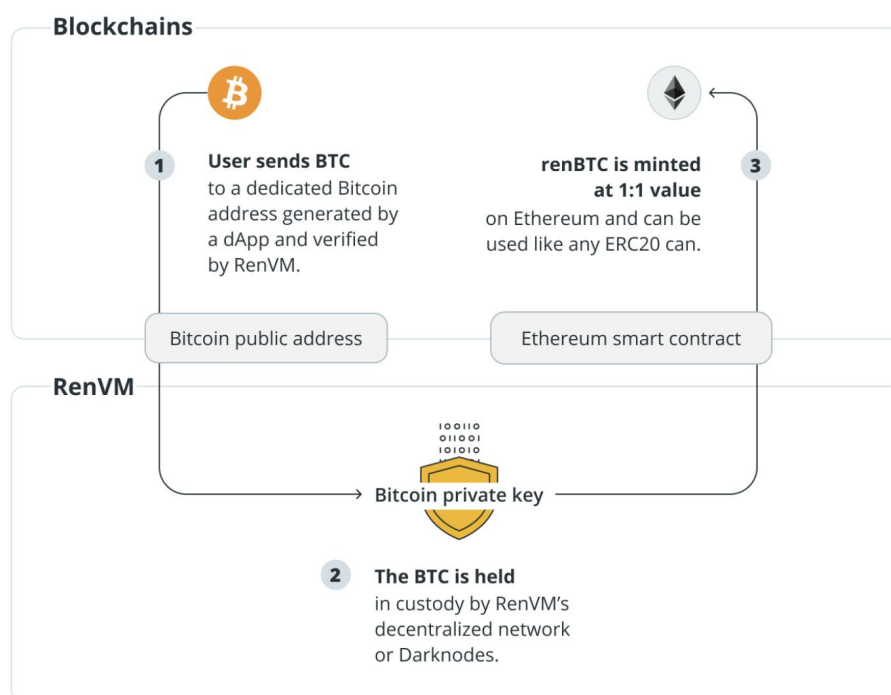
At one point, renBTC was the only major project to issue a wrapped Bitcoin token with its collateral custody using secure multiparty computation; however, it is now defunct. RenBTC used to position itself as a decentralized alternative to wBTC.

RenVM, the underlying protocol of renBTC, used an RZL MPC algorithm for distributed custody. This allowed Darknodes, the RenVM’s custodians, to collectively manage Bitcoin without any single node or machine controlling the private keys for the funds. Through MPC, the private keys used to lock BTC were never fully exposed, even to the Darknodes themselves (Figure 3).

The Darknodes were randomly selected to form shards that took collective custody of Bitcoin UTXOs. These shards would employ the RZL MPC algorithm to collectively generate an elliptic curve digital signature algorithm (ECDSA) private key. Corresponding addresses were generated to allow users to put BTC into the RenVM’s custody. Once the BTC was securely locked, RenVM returned a “minting signature” to the user, which authorized them to mint renBTC, an ERC-20 token with a 1:1 BTC peg. The locked funds could not be released without the cooperation of at least one-third of the Darknodes in a shard.

When a user wanted to redeem their renBTC for BTC, they initiated a burn transaction on Ethereum. The Darknodes collectively verified the burn and, using MPC, signed a release transaction that transferred the equivalent amount of BTC back to the user’s specified Bitcoin address. When a user wanted to redeem their renBTC for BTC, they initiated a burn transaction on Ethereum. The Darknodes collectively verified the burn and, using MPC, signed a release transaction that transferred the equivalent amount of BTC back to the user’s specified Bitcoin address.

Figure 3: RenVM’s Lock and Mint Process for renBTC



Source: [Matcha](#)

Fees were the main incentive for Darknodes to operate the RenVM. Darknodes earned an adjustable percentage fee for each BTC transfer made by users and had to bond 100,000 REN tokens. RenVM targeted a bonded value three times greater than the locked value to secure the network. This disincentivized attacks, as the loss of bonds would exceed any potential gain.

Ren’s model bears similarities to Threshold’s due to their use of secure MPC frameworks; however, their respective implementations differ in focus and operation.

RenVM’s reliance on RZL MPC places priority on privacy. Although MPC generally supports federation resizing, RenVM’s setup enforced a strict threshold and required a pre-defined number of nodes to complete transactions. Threshold Network, on the other hand, uses a modified GG18 implementation for ECDSA threshold signatures. Compared to RenVM, Threshold’s model favors efficiency over privacy. Its threshold signatures allow for offchain dynamic federation resizing, thus reducing the need for repeated verifications. This flexibility, while efficient, may expose metadata not seen in RenVM’s setup; for instance, Threshold Network reveals that a valid signature has been generated without indicating the specific participants involved (Table 3).

At the time, renBTC’s model appealed to those valuing decentralization and trustlessness. However, the protocol’s reliance on Alameda Research for funding ultimately exposed a significant vulnerability. Following Alameda’s collapse, Ren’s infrastructure ceased to function, effectively ending the viability of renBTC. It was also exposed that Ren was effectively in full control of the signing set that held the BTC deposits.

Table 3: Comparing renBTC and tBTC

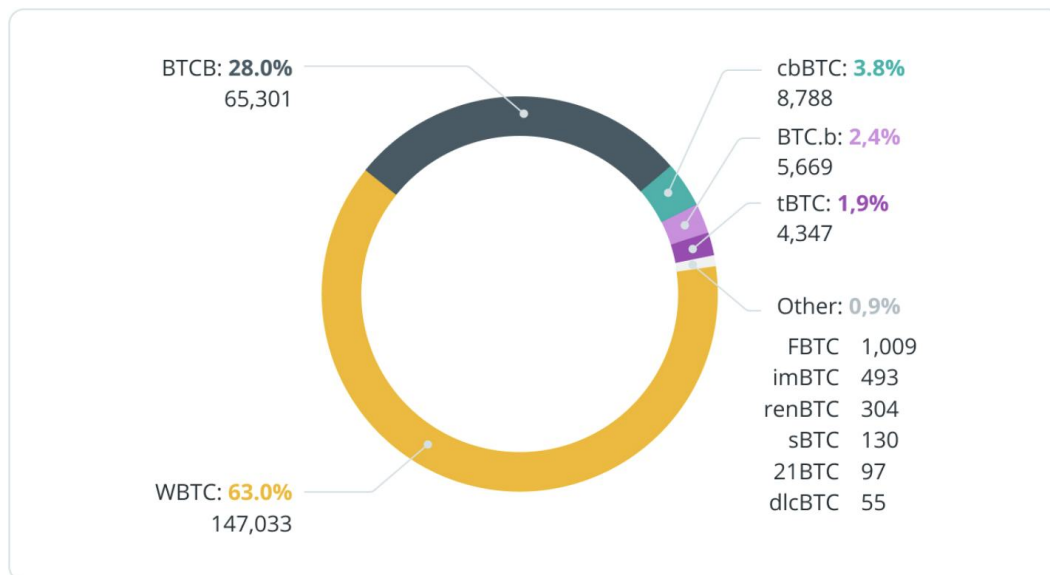
	renBTC	tBTC (v2)
Custody	Decentralised	Decentralised
Key tech	RZL MPC	Threshold signature
Security assumptions	MPC protects private key	Two-thirds honest majority
Redemption process	Burn transaction, MPC signs release	Burn transaction, validators sign release
Collateral asset	Ren tokens staked by Darknodes	T tokens staked by validators
Network operators	Darknodes	Signers (validators)

Adoption Metrics and Market Impact

WBTC dominates bridged Bitcoin tokens on Ethereum by far. It holds over 61.3% of its total market at a capitalization of \$13 billion. TBTC, while designed to be more decentralized, has had slower adoption and has, to this date, captured less than 2.2% of the market (Figure 4).

This is partly due to the delayed activation of its redemption mechanism, which limited its early growth. However, with this feature now live, there is still potential to increase its total value locked (TVL). Meanwhile, cbBTC has quickly reached a market cap of \$1.3 billion and thus surpassed tBTC's \$416 million. This is despite its centralized model and fairly recent launch on Sept. 12.

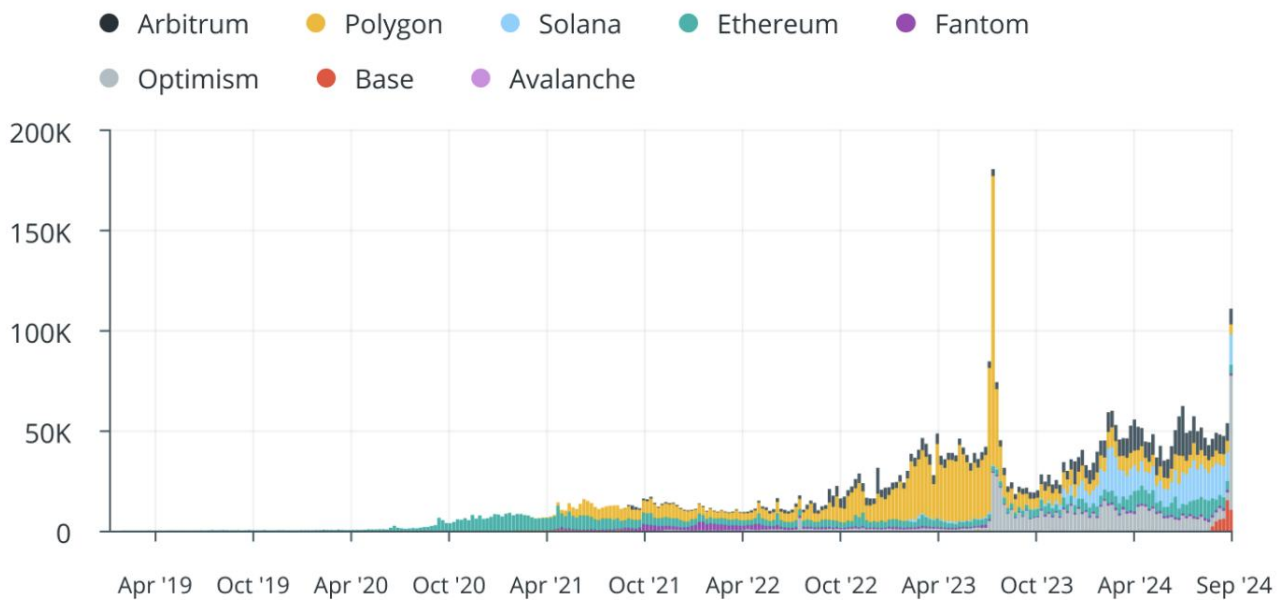
Figure 4: Wrapped Bitcoin Supply on Chains



Source: Yandhii/[Dune Analytics](#)

Initially, wBTC's growth was primarily driven by activity on Ethereum, which served as an important form of lending and borrowing collateral in DeFi protocols. Its past use in platforms such as MakerDAO, Aave and Compound has allowed users to leverage Bitcoin for yield farming and liquidity provisioning. As DeFi matured, wBTC expanded beyond Ethereum's ecosystem. Chains such as Solana, Polygon and Arbitrum are seeing increased weekly usage (Figure 5). The BNB Smart Chain (BSC) and Avalanche also support wrapped Bitcoin assets, though adoption on these chains is small in comparison to Ethereum's at a TVL of \$383 billion.

Figure 5: WBTC Weekly Usage Chart



Source: [Obchakevich/Dune Analytics](#)

The Future of Wrapped Bitcoin

The need for trustless, reliable BTC bridges is more critical than ever. As the Bitcoin ecosystem evolves, protocols that achieve a balance between liquidity, security and decentralization could define the next phase of Bitcoin DeFi. WBTC currently dominates in liquidity but faces growing scrutiny as DeFi users are once again becoming concerned with decentralization and censorship resistance. With increasing concerns over custodial risks, alternatives like tBTC could gain market share, but they face strong competition from entrenched corporate forces such as Coinbase.



Kyrian Alex

Research Analyst

Disclaimer

This document is for information only and does not constitute investment advice, an investment recommendation or a solicitation to buy or sell — it is merely a summary of key aspects of the Cointelegraph Report. In particular, this document is not intended to replace individual investment or other advice.

The information contained in this publication is based on the knowledge available at the time of preparation and is subject to change without notice. The authors were diligent with their selection of information but assume no liability for the accuracy, completeness or timeliness of the information provided.

Past performance is not a guide to future performance. Values may fall or rise, and you may not get back the amount you invested. Income from investments may fluctuate.

Cointelegraph does not endorse and is not responsible for or liable for any content, accuracy, quality, advertising, products or other materials on this page. Readers should do their own research before taking any actions related to the company.

Cointelegraph is not responsible, directly or indirectly, for any damage or loss caused or alleged to be caused by or in connection with the use of or reliance on any content, goods or services mentioned in this publication.