🅱 cbBTC whitepaper

What is cbBTC?

Coinbase Wrapped BTC ("cbBTC") is a token that is backed 1:1 by native Bitcoin (BTC) held by Coinbase, meaning that for all cbBTC in circulation, there is an equivalent amount of BTC held in a secure custody solution (including cold storage) provided by Coinbase. Wrapped assets, like cbBTC, are transferable tokens that are redeemable for the underlying asset. Coinbase customers can unwrap cbBTC and redeem a corresponding amount of the underlying BTC simply by depositing the cbBTC into their Coinbase accounts. cbBTC is built to be seamlessly compatible with DeFi applications, giving customers the option to tap into DeFi and unlock financial utility.

Why cbBTC?

cbBTC removes a key point of friction by allowing customers to use Bitcoin they already hold in new ways onchain. cbBTC is built to be seamlessly compatible with DeFi applications, so users can now tap into novel DeFi use cases like providing their Bitcoin as liquidity to DeFi protocols, using it as collateral to borrow other crypto assets, or spending it as a payment method. Wrapped assets like cbBTC are a mature concept in the crypto world, helping to bring more liquid assets onchain and facilitate an expansive financial ecosystem.

Minting and Burning Process

cbBTC is fungible 1:1 with a dedicated reserve of BTC held at Coinbase. The process of minting (sending) and burning (redeeming) cbBTC ensures trust and transparency, providing a frictionless experience for users. When a user requests a withdrawal of cbBTC, Coinbase holds the corresponding amount of BTC in its custody to back the cbBTC minted.

- **Minting**: When a user initiates a withdrawal of BTC held in their Coinbase account to the Ethereum,Base or Solana networks, an equivalent amount of cbBTC is minted on the network and sent to the user's destination address / wallet.
- **Burning**: When cbBTC is deposited to a user-specific Coinbase address, the cbBTC is burned and the corresponding amount of BTC is released from Coinbase's reserve and assigned to the user's Bitcoin account.

The total supply of cbBTC can be found in the token smart contract under totalSupply ([Base](), [Ethereum](), [Solana]()).

On EVM chains, the process of minting and burning cbBTC involves using a set of audited and secure smart contracts. These contracts are designed to mint and burn cbBTC as needed,

ensuring that the total supply of cbBTC always matches the amount of BTC held backing it. cbBTC is built using the core elements of the Coinbase wrapped token contract that was also used for Coinbase Wrapped Staked ETH (cbETH). The smart contract code open source repository for Coinbase's wrapped tokens – including both cbBTC and cbETH – can be found on [Github](#).

The following are key roles of the wrapping contract managed by Coinbase. These roles are protected by Coinbase's key management systems and usage requires approval from a number of people in different functions, including security, engineering, and finance.

- Admin: can upgrade the wrapped token implementation contract
- Owner: can assign all roles except the Admin
- Blacklister: can blacklist an address from transferring, minting, and burning
- MasterMinter: can assign minters and their limits
- Minter: can mint and burn tokens
- Pauser: can pause transfers, mints, and burns for the contract

On Solana, cbBTC is an SPL token. Coinbase manages and controls the mint and burn cbBTC as needed, ensuring that the total supply of cbBTC always matches the amount of BTC held backing it.

The following are key authorities of the SPL token are owned and managed by Coinbase. These roles are protected by Coinbase's key management systems and usage requires approval from a number of people in different functions, including security, engineering, and finance.

- Mint Authority: can mint tokens
- Freeze Authority: can pause/unpause transfers to/from specified addresses
- Update Authority: can update token metadata

Security Measures & Compliance

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 Solidity smart contract contract ([link](#)) which was also used for cbBTC. No material contract code has been modified in deploying cbBTC.

Custodianship and Governance

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.

Regulatory Compliance

Coinbase is committed to operating within the legal frameworks of the jurisdictions in which it operates. The launch of cbBTC will comply with all relevant regulations, including Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements. Coinbase has obtained numerous licenses to operate in the United States and internationally, including multi-state money transmission licenses, and crypto asset trading and custody licenses in New York, Germany, Singapore, Canada, Bermuda, and more. Coinbase is also a registered Virtual Asset Service Provider in a number of countries.

Risks

Smart contract security risk
cbBTC is at its core a smart contract, and with that comes risk that the code may be exploited in unforeseen ways. This risk is partially mitigated by the fact that the foundation of cbBTC is based on heavily audited and battle tested smart contracts (like USDC and cbETH).

External cbBTC price risk

The price of cbBTC onchain will be determined by the individual markets and is not pegged or in any other way maintained by Coinbase. As with any asset trading in free markets, there is always some degree of price risk inherent in the trading of cbBTC in relation to BTC on other markets.

Fees

There are no fees associated with minting/wrapping or burning/unwrapping cbBTC today. Users will be charged network fees for withdrawals from Coinbase.