CIRCLE

cirBTC Whitepaper

Author
Circle

With special thanks to
Fujia Chen, Kanishka Maheshwari, Bohan Zhang, Ian Rowan, Khalid Aliweh, Nick Lagusis, Pauline Kim, Tim Titcomb

Contents

PART 1

What is cirBTC?

Circle Wrapped Bitcoin (“cirBTC”) is an ERC-20 token backed 1:1 by native Bitcoin (BTC). The underlying BTC is held in secure custody by Circle.

cirBTC uses the same audited smart contract architecture that powers USDC and EURC. Circle Mint customers can mint and redeem a corresponding amount of the cirBTC by transferring the underlying BTC into their Circle accounts. cirBTC is built to be seamlessly compatible with DeFi applications, giving customers the option to unlock financial utility from their Bitcoin holdings.

- **Token Name**
  Circle Wrapped Bitcoin
- **Symbol**
  cirBTC
- **Decimals**
  8
- **Standard**
  ERC-20
- **Issuing Entity**
  Circle International Bermuda Limited (CIBL)
- **Ethereum Contract**
  0x72DFB2E44f59C5AD2bAFE84314E5b99a7cd5075E
- **Arc contract**
  0x171A4217b86A807A64eB94757Db6849fb4bDbAA0

PART 2

Why cirBTC?

Bitcoin is widely recognized as the world's premier digital store of value, yet its native blockchain lacks the programmability required for DeFi.

Without wrapping, i.e. porting onto a different blockchain, market participants will be unable to unlock its full potential as collateral, in onchain trading, and in lending market deployment. cirBTC removes this friction by allowing customers to use Bitcoin they already hold in new ways onchain, as collateral in lending protocols, and as liquidity in decentralized exchanges.

cirBTC is differentiated from other wrapped Bitcoin products by Circle's institutional-grade infrastructure. It lives on the same platform trusted to issue USDC, the world's leading regulated stablecoin1. Here are cirBTC's defining characteristics:

Trusted and Neutral Issuer

Issued by a Circle affiliate, CIBL, the internet financial platform company behind USDC with a track record of operating USDC at scale across multiple blockchains.

Battle-Tested Smart Contracts

Built on the FiatTokenV2_2 contract architecture, the same audited and proven contracts underpinning USDC and EURC, rather than a novel or untested codebase.

Institutional Custody

The underlying BTC will be held in custody at Circle's regulated affiliate, held for the exclusive benefit of cirBTC holders and legally segregated from Circle's corporate assets. Circle's long-term model is designed around fiduciary-grade custody and clear asset segregation to support institutional

trust and transparency. BTC is stored in Circle's regulated custody infrastructure, including air-gapped cold storage vaults, with no reliance on third-party custodians.

Proof of Reserves

Onchain verifiability of BTC reserves via Chainlink Proof of Reserve integration, providing transparent and independent attestation.

Multichain by Design

Natively issued on Ethereum and Arc with planned expansion to additional networks via Cross-Chain Transfer Protocol (CCTP), enabling seamless cross-chain movement.

Regulatory Compliance

Compliant issuance from a regulated Bermuda entity, with KYC/AML enforcement and transparent reserve management.

Full-stack flexibility

cirBTC will integrate seamlessly with USDC, Arc, and Circle Mint to offer a single Circle-native end-to-end stack.

PART 3

Minting and Burning Process

cirBTC is fungible 1:1 with a dedicated reserve of BTC held at Circle. The process of minting (creating) and burning (redeeming) cirBTC ensures trust and transparency, providing a frictionless experience for users.

Minting

When a Circle Mint customer initiates a deposit of BTC for the purpose of receiving cirBTC:

1. The customer sends BTC to a Circle-provided deposit address.
2. Upon confirmation of the BTC deposit, the corresponding amount of BTC is transferred to Circle's reserve, as required by the issuance framework.
3. An equivalent amount of cirBTC is minted on-chain and credited to the customer's Circle account or sent to their specified destination address.

Burning

When cirBTC is deposited to a customer's Circle account for redemption:

1. The cirBTC is burned on-chain, permanently removing it from circulation.
2. The corresponding amount of BTC is released from Circle's reserve.
3. The BTC is sent to the customer's specified Bitcoin address.

The total supply of cirBTC can be verified at any time via the **totalSupply** function on the token smart contract per chain.

Reserve Integrity

The minting and burning process uses a set of audited and secure smart contracts. These contracts are designed to support minting and burning controls so that cirBTC supply can be reconciled against BTC reserves. On-chain minter allowances enforce hard caps on the maximum cirBTC that can be minted at any time, providing an additional layer of supply discipline.

PART 4

Smart Contract Architecture

cirBTC is built using Circle's FiatTokenV2_2 smart contract architecture, the same proven contract system used for USDC and EURC. The smart contract code is open source and can be found on GitHub.

Contracts

- **FiatTokenV2_2**
  Implementation contract containing mint, burn, transfer, and permit logic
- **FiatTokenProxy**
  ERC-1967 upgradeable proxy, the token's canonical on-chain address
- **MasterMinter**
  Manages minter roles and on-chain minting allowances

Administrative Roles

The following are key roles of the token contract managed by Circle. These roles are protected by Circle's cold storage key management systems, and usage requires the cryptographic consensus of multiple individuals across different functions, including security, engineering, and finance. No single individual has control over any administrative role.

- **Proxy Admin**
  Can upgrade the token implementation contract.
- **Owner**
  Can assign all roles except the Proxy Admin.
- **Blocklister**
  Can add or remove addresses from a blocklist, preventing them from transferring, minting, or burning cirBTC.

- **MasterMinter Owner**
  Can assign minters and configure their on-chain allowance limits.
- **Minter**
  Can mint and burn tokens up to the configured allowance.
- **Pauser**
  Can pause and unpause all transfers, mints, and burns for the contract.

PART 5

Proof of Reserves

cirBTC integrates with **Chainlink Proof of Reserve** to provide independent, on-chain verification that the BTC reserves backing cirBTC are sufficient. Chainlink node operators query Circle's reserve address API to verify the BTC balances held across both hot and cold custody wallets.

This Proof of Reserve feed is designed to:

- Provide transparent, near-real-time attestation of reserve adequacy.
- Enable DeFi protocols to programmatically verify backing before accepting cirBTC as collateral.
- Include a safety "ripcord" mechanism that can halt DeFi operations if reserves ever appear insufficient.

Reserve addresses, including both hot wallet and pre-provisioned cold storage addresses, are made available to operators with no freshness delay, ensuring continuous verifiability.

PART 6

Multichain Strategy

cirBTC natively issued first on Ethereum and Arc, where the majority of wrapped BTC liquidity currently resides.

This enables users and market makers to direct liquidity with minimal friction.

cirBTC is built for interoperability. While launching first on Ethereum and Arc, there is a multi-chain roadmap anchored in the same CCTP infrastructure already securing billions in USDC movement across supported chains.

PART 7

DeFi Compatibility

cirBTC is designed for seamless integration with the DeFi ecosystem[2]. Key integration areas include:

Decentralized Exchanges

Permissionless listing on protocols, enabling liquid trading pairs (e.g., cirBTC/USDC, cirBTC/WBTC) critical for price discovery and liquidation support.

Oracle Feeds

Integration with Chainlink and Chronicle oracle networks for reliable on-chain price feeds, leveraging existing BTC/USD data.

Lending Protocols

Onboarding as collateral on lending platforms, enabling users to borrow against their Bitcoin holdings. Because cirBTC and USDC are issued by the same entity, USDC serves as the natural borrow asset, giving institutions a single trusted counterparty for both Bitcoin collateral and dollar liquidity.

Broad ERC-20 Compatibility

As a standard ERC-20 token, cirBTC is compatible with any DeFi protocol that supports the ERC-20 interface, including yield aggregators, structured products, and payment applications.

PART 8

Security Measures

Circle employs defense-in-depth security practices to safeguard the BTC backing cirBTC and the integrity of the smart contracts:

- **Audited Contracts**
  cirBTC uses the same FiatTokenV2_2 contract codebase that has been audited by third-party security firms. No material contract code has been modified from the audited version used for USDC and EURC.
- **Blocklist Enforcement**
  The Blocklister role can prevent specific addresses from interacting with cirBTC, supporting compliance and security incident response.
- **Comprehensive Monitoring**
  Real-time monitoring of total supply, reserve balances, and on-chain activity with automated alerting for anomalies. 24/7 cybersecurity monitoring and incident response capability.

The underlying BTC reserves backing cirBTC are held 1:1 at Circle, allocated in both cold storage and hot wallets to balance security with operational responsiveness. The following describes Circle's custody infrastructure for the underlying BTC reserves:

Cold Storage

Circle's cold storage infrastructure uses air-gapped vaults across geographically separated, secure facilities. Key properties include:

- **Encryption**
  All instructions for cold custody transactions require multiple levels of approval and are fully encrypted.
- **Regular audits**
  Circle performs audits of the private key management process and reconciliations between Circle wallets and third-party blockchain data.

Hot Wallets

A portion of BTC reserves is maintained in hot wallets to facilitate timely minting and redemption operations. Hot wallet infrastructure leverages Circle's existing Unspent Transaction Output (UTXO)-based systems with comprehensive monitoring and alerting.

BTC-Specific Considerations

Bitcoin's UTXO model creates unique custody dynamics compared to EVM-based assets:

- Each cold storage sweep generates a new receiving address (each used once), enhancing privacy and security.
- Cold-to-hot transfers cannot be pre-signed in advance because UTXO inputs are not known until the transfer is initiated.
- Address provisioning for Proof of Reserves is handled via pre-generated address batches to support timely reserve verifiability.

PART 9

Regulatory Compliance

cirBTC is issued by Circle International Bermuda Limited (CIBL), a regulated entity within Circle's corporate structure. Circle is committed to operating within the legal frameworks of the jurisdictions in which it operates.

- **Permissioned Issuance, Permissionless Transfer**
  Minting and burning of cirBTC is restricted to verified Circle Mint customers who have completed KYC/AML requirements.
  Once minted, cirBTC can be transferred as a standard ERC-20 token.

- **Bermuda Issuance Framework**
  BTC reserves are held by the Bermuda entity prior to minting, in accordance with the applicable regulatory framework for digital asset issuance.

- **AML/KYC Compliance**
  All minting and redemption activity is subject to Circle's Anti-Money Laundering and Know Your Customer policies. Circle performs risk and compliance checks on all transactions.

- **Licensing**
  Circle and its affiliates hold regulatory authorizations in various jurisdictions[1].

PART 10

Risks

Smart Contract Security Risk

cirBTC is built on smart contracts, which carry inherent risk that the code may be exploited in unforeseen ways. This risk is substantially mitigated by the fact that cirBTC uses the same FiatTokenV2_2 contract architecture that has been battle-tested in production with USDC (one of the most widely used tokens in crypto) and EURC, and has been audited by multiple independent security firms.

External Price Risk

The price of cirBTC on-chain will be determined by individual markets and is not pegged or in any other way maintained by Circle beyond the 1:1 BTC redemption rights available to eligible, verified customers. As with any asset trading in free markets, there is always some degree of price risk inherent in the trading of cirBTC relative to BTC on other markets.

Custody Risk

While Circle employs industry-leading custody practices, custody of digital assets inherently carries risk including but not limited to operational failures, key compromise, or physical security breaches. Circle maintains robust controls to mitigate these risks.

Regulatory Risk

The regulatory environment for digital assets continues to evolve. Changes in laws or regulations in jurisdictions where Circle operates could impact the issuance, transfer, or redemption of cirBTC.

Bitcoin Network Risk

cirBTC minting and redemption depend on the Bitcoin network for deposit and withdrawal transactions. Bitcoin network congestion, fee spikes, or protocol changes could impact the speed or cost of minting and redeeming cirBTC.

References

1. circle.com/legal/licenses

2. cirBTC is compatible with applications that support the ERC-20 interface. Availability on any DEX, lending protocol, oracle network, payment application, or other third-party protocol depends on third-party integration, protocol governance, risk parameters, and applicable law.