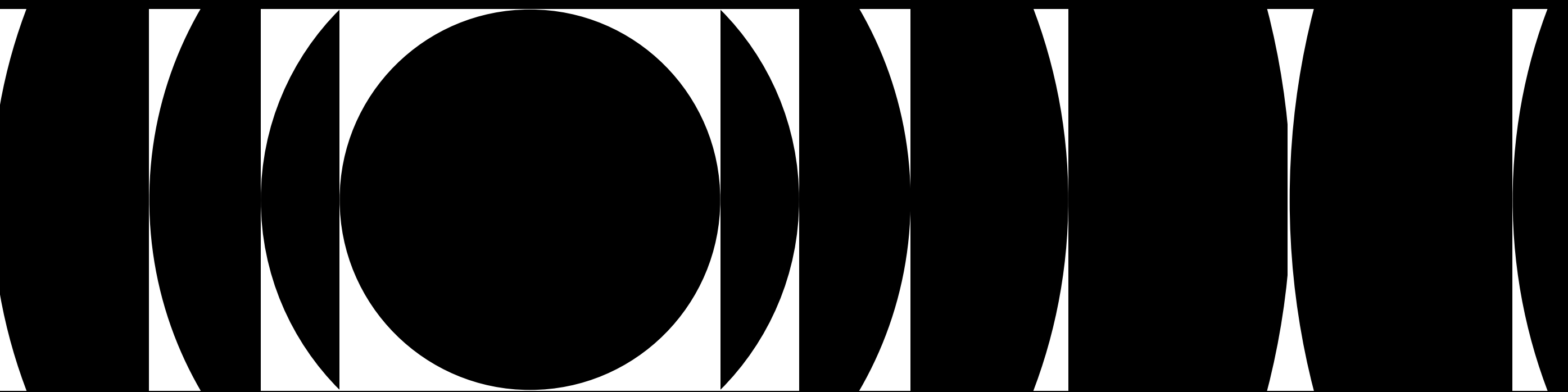




xBTC Whitepaper



What is xBTC

OKX Wrapped BTC ("xBTC") is a token backed 1:1 by Bitcoin (BTC) securely custodized by OKX.

As a wrapped asset, xBTC is redeemable by its underlying asset, BTC, on supported blockchains. To start with, OKX users could simply withdraw BTC to the supported blockchains and receive xBTC, which is available for use across DeFi apps. To redeem the BTC, they can deposit xBTC back into their OKX accounts, and get the equivalent amount of underlying BTC. With xBTC, users could now seamlessly utilize their Bitcoin assets within the DeFi ecosystem.

Why xBTC

xBTC expands the use cases of users' BTC holdings, unlocking a new way of utilizing Bitcoin on-chain. Users can seamlessly use xBTC in DeFi applications to access a wide range of services, including lending, borrowing, and more. For instance, xBTC could be used as collateral for borrowing crypto assets.

xBTC minting and burning process

The processes of minting and burning xBTC are securely managed on a 1:1 basis and highly transparent, providing a frictionless experience for users:

- **Minting:** When users withdraw BTC from their account via supported networks (Sui, Aptos or Solana), the BTC is transferred to our reserve address. An equivalent amount of xBTC is minted and transferred to the designated address or wallet accordingly.
- **Burning:** When users deposit xBTC back to OKX via supported networks (Sui, Aptos or Solana), the xBTC is burned, and the equivalent BTC is released from our reserve address back to users' account.

The total supply information of xBTC in its smart contract is available on the explorer sites of [Sui](#), [Aptos](#) or [Solana](#).

Role and authority management

On Sui and Aptos, xBTC follows Sui coin standard and Aptos FA (Fungible Asset) standard respectively. OKX owns and manages the following capabilities:

- **Mint/Burn Capability:** To mint and burn xBTC tokens.
- **Blacklist Capability:** To block specific addresses from transferring xBTC tokens.
- **Pause/Thaw Capability:** To pause and resume the transfers, mints, and burns of xBTC tokens.

On Solana, xBTC follows SPL token standard. OKX owns and manages the following authorities:

- **Mint Authority:** To mint tokens.
- **Freeze Authority:** To block specific addresses from transferring xBTC tokens.
- **Update Authority:** To change token information when needed.

Security measures and transparency

Smart contract security and audit

OKX employs third-party security experts to perform comprehensive audits of smart contracts, ensuring the security of xBTC. On Sui and Aptos, Certik and Movebit have carried out the xBTC smart contract audit. The results of audits are now available in Certik's [audit report](#) and Movebit's [audit report](#) respectively. You can find the full open source code of xBTC for Sui and Aptos chains on <https://github.com/okx/xBTC>.

On Solana, OKX follows the [Solana Token Program](#), which was audited multiple times. Hence, xBTC is created in Solana directly without any smart contract source code in xBTC github. You can refer to the [Token Program Github](#) if you want to learn more.

PoR

OKX ensures full transparency of xBTC, with all key information on the [xBTC page](#), including:

- The total amount of BTC held in a designated locked address.
- The total amount of xBTC minted in the supported networks.

Governance and regulatory compliance

The underlying BTC reserves backing xBTC are held 1:1 at OKX, and redemption rights remain with xBTC holders, subject to the applicable [xBTC User Agreement](#) which outlines OKX's services and terms specific to xBTC holders.

OKX is committed to operating within the legal frameworks of the jurisdictions in which it operates. The launch of xBTC will comply with all relevant regulations, including Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements.

Risk warning & disclaimer

Smart contract risk

xBTC operates as a smart contract with inherent technical considerations. The code, while carefully designed and audited, may carry potential risks not yet identified. Additionally, despite OKX's employment of robust internal private key management systems to help protect privileged accounts, potential risks of user accounts being compromised still exist.

xBTC price risk

The price of xBTC on the blockchain will be determined by individual market forces and is not pegged or maintained by OKX in any way. As with any asset traded in free markets, there is always a certain level of price risk associated with trading xBTC compared to BTC on markets.

Fees

Users only need to pay gas fees for supported blockchains for xBTC withdrawals from OKX. No fee will be charged for minting and burning xBTC.