tzBTC

Wrapped Bitcoin invented on Tezos

A Brief Overview

v. 2.0

Switzerland, April 2024

Overview

A “wrapped” token refers to the blockchain-based tokenization of a physical asset such as a fiat currency (US dollar) or commodity (gold), or another digital asset such as bitcoin (BTC) or ether (ETH). Wrapped tokens are controlled and custodied in a process that is combined with the increase (minting) and/or decrease (burning) of its circulating supply to ensure parity with the underlying asset.

In the case of tzBTC, the tokenized asset is Bitcoin (BTC), wrapped in a smart contract called tzBTC on the Tezos or any other selected blockchain. One tzBTC represents one BTC, parity that is ensured by a group of Keyholders and an independent third-party auditor. In short, the value of tzBTC aims to represent the value of BTC.

tzBTC allows users and applications on selected smart-contract enabled blockchains to directly transact in BTC, bringing BTC’s liquidity and brand to the wider blockchain ecosystem and enabling novel financial use-cases on-chain.

Governance, Key Stakeholders and Processes

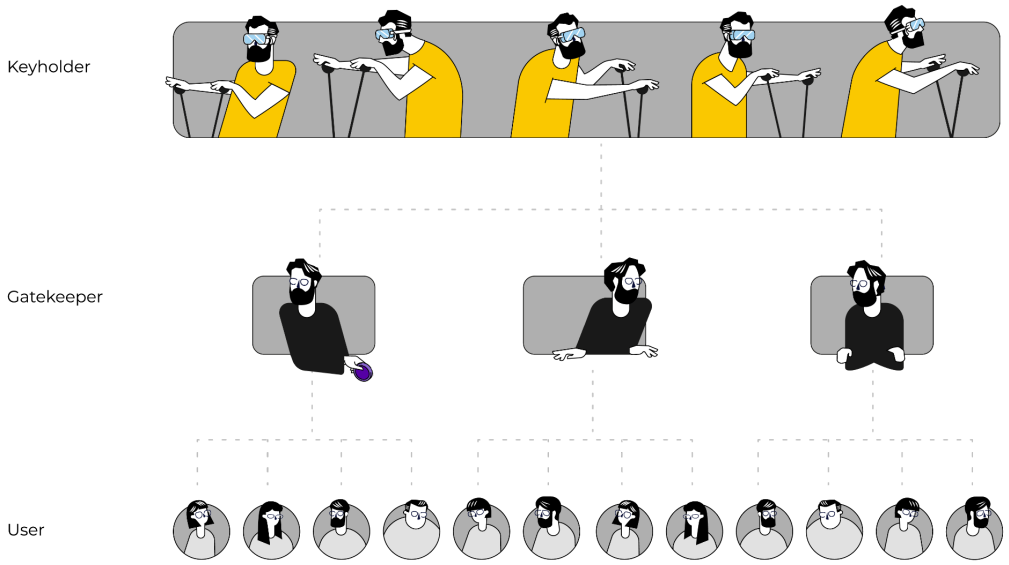
Governance and Key Stakeholders

The governance mechanism of the tzBTC contract allows for the compliant and secure issuance of BTC-backed tokens on a blockchain. The various responsibilities are managed by several key stakeholders: Keyholders, Gatekeepers, and Users.

Keyholders are responsible for the custody of BTC, the minting of the corresponding tzBTC, and the burning of tzBTC when BTC is redeemed. As the custodians of the BTC corresponding to the tzBTC in circulation, Keyholders may have legal and regulatory requirements that may differ between countries. Keyholders securely custody BTC using a multi-signature ("multi-sig") setup. A multi-sig setup is also implemented to secure the automated minting and burning of tzBTC.

Gatekeepers act as financial intermediaries and often serve business-to-consumer ("B2C") markets, which requires them to be compliant with know-your-customer (KYC), anti-money laundering (AML), and other regulations. Gatekeepers may accept BTC and allocate the corresponding tzBTC (minted by Keyholders) for Users after performing identity verification checks. Gatekeepers have individual bilateral contracts with Keyholders. A template for such a contract is made available here.

Users buy, sell, and hold tzBTC. tzBTC is acquired from Gatekeepers when Users and Gatekeepers enter into agreements. Users can freely transact tzBTC via any supported wallets and transactions may be publicly viewed via supported block explorers. A list of supported wallets and block explorers is available at https://tzbtc.io.



Picture: visualisation tzBTC governance structure

Processes

Three processes are involved in the tzBTC system: Initiating, Minting and Burning.

Initiating refers to the process whereby a User requests to acquire tzBTC from a Gatekeeper. Following a successful identity verification check performed by a Gatekeeper, that Gatekeeper will accept a User's payment (typically in BTC) and issue new tzBTC to its designated address (after Minting).

Minting refers to the process of creating new tzBTC which corresponds to the BTC held in custody. Minting cannot be executed by a single Keyholder (requires multiple Keyholder signatures) and happens in response to demand from Gatekeepers. In addition to a regular (quarterly) minting process, a User may pay a higher fee to execute an ad-hoc minting process. Minting new tzBTC increases the amount of tzBTC in circulation.

Burning refers to the process of redeeming tzBTC for BTC. Only Gatekeepers may initiate the process of burning tzBTC. By doing so, the amount in question is deducted from a Gatekeeper's tzBTC balance and the corresponding BTC is returned to a User. Burning tzBTC decreases the amount of tzBTC in circulation.

tzBTC: a wrapped token

Underpinning tzBTC is a smart contract representing the balances for the BTC held in custody by Keyholders.:

- Tezos: FA1.2 token standard (see TZIP-7),

Smart contracts enable multiple parties to transparently govern financial resources and permissions natively. As such, a key pillar of the tzBTC project is the ability to transparently display multi-stakeholder governance of the tzBTC supply and permissions, as visualized by the table below or in the supported Tezos block explorers.

For a more detailed overview of how the tzBTC contract and its underlying entry points work, check out the public tzBTC GitHub repository.

In addition to the tzBTC token contract itself, a specialized multi-signature contract is used by the Keyholders to manage a co-signing service. This allows the Keyholders to interact with the smart contract initiating and signing key processes required in the tzBTC system.

Ultimately, the tzBTC smart contract is an open-source tool and available for the entire community. To view tzBTC in circulation, check it out here:

- Tezos: tzkt, Better Call Dev.

Get involved

To get involved in the tzBTC ecosystem and help accelerate the adoption of this project, please contact a Keyholder.

Appendix I

Dispute Resolution Regarding Potential Forks

In the event of a fork of the Bitcoin, Tezos and/or any other blockchain involved, Keyholders, in their discretion, determine the canonical fork for tzBTC. Upon a Gatekeeper's request, a Keyholder informs the Gatekeeper of

its decision with respect to the canonical fork within a reasonable amount of time, but no later than 20 business days after the fork.