



Wrapped Bitcoin on Tezos

Brief

v. 1.0

Switzerland, April 2020

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 BTC, wrapped in a smart contract on the Tezos blockchain. One tzBTC represents one BTC, parity that is ensured by a group of Keyholders and an independent third-party auditor. The value of tzBTC represents the value of BTC.

tzBTC allows users and applications on Tezos to directly transact in BTC on the Tezos blockchain, bringing BTC’s liquidity and brand to the Tezos ecosystem.

Governance, Key Stakeholders and Processes

Governance and Key Stakeholders

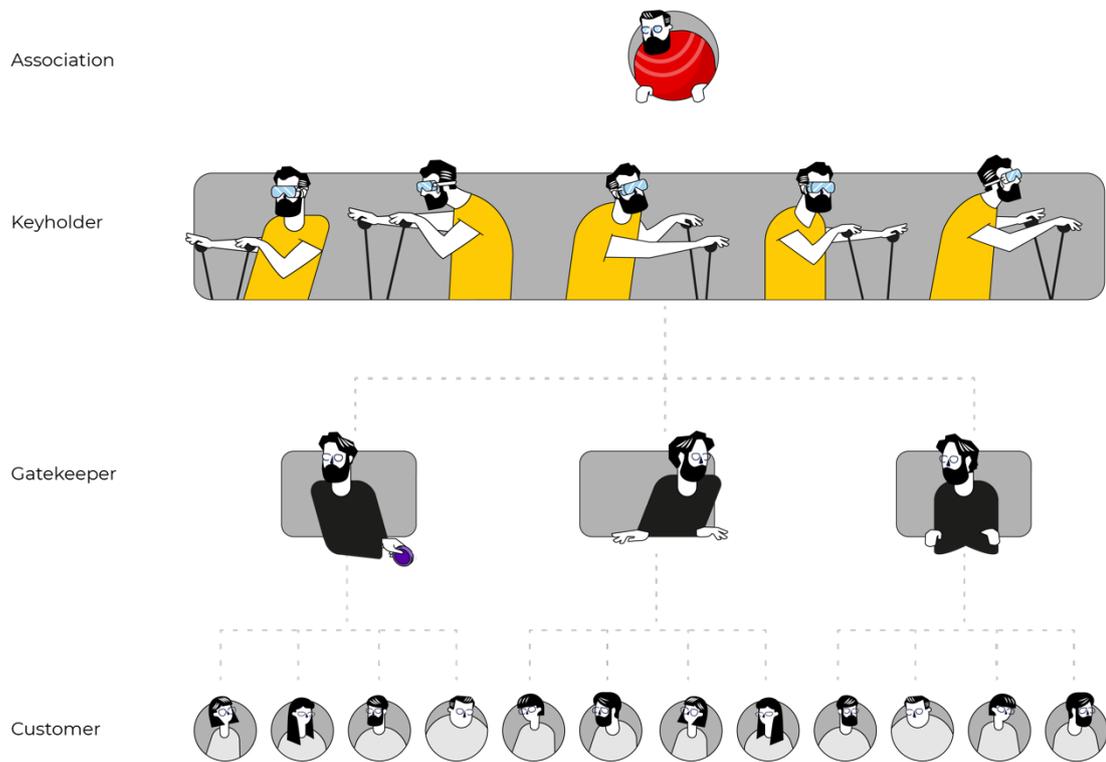
The governance mechanism of the tzBTC contract allows for the compliant and secure issuance of BTC-backed tokens on the Tezos blockchain. The various responsibilities are managed by several key stakeholders: Keyholders, Gatekeepers, and the Association.

The Association is an independent third-party that monitors the tzBTC issuance process and publishes quarterly audit reports to confirm that the amount of BTC in custody by Keyholders equals the amount of tzBTC in circulation. The Association attends Keyholder meetings where decisions to mint or burn the supply of tzBTC, as well as determine the fees for conducting such actions, are made.

Keyholders are responsible for the custody of BTC, the minting of the corresponding tzBTC, and the burning of tzBTC. 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 for the minting and burning of tzBTC.

Gatekeepers act as financial intermediaries and often serve B2C (business-to-consumer) markets, which requires them to be compliant with anti-money laundering (AML) and terrorist financing legislation. Gatekeepers may accept BTC and allocate the corresponding tzBTC for customers after performing identity verification checks. Gatekeepers have individual bilateral contracts with Keyholders. A template for such a contract is available on the tzBTC website at <https://tzbtc.io>.

Customers buy, sell, and hold tzBTC. tzBTC is acquired from Gatekeepers when Customers and Gatekeepers enter into agreements. Customers can transact tzBTC via FA1.2-supported wallets and transactions may be publicly viewed via FA1.2-supported block explorers. A list of supported wallets and block explorers is available at <https://tzbtc.io>.



Picture: visualization tzBTC governance structure

Processes

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

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

Minting refers to the process of creating new tzBTC. Minting cannot be executed by a single Keyholder (requires multiple signatures) and must be initiated by a Gatekeeper. In addition to a regular (quarterly) minting process, a Customer may pay a higher fee to execute an ad-hoc minting process.

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 on the Tezos blockchain and the corresponding BTC is returned to a Customer.

tzBTC: an FA1.2 token on the Tezos blockchain

Underpinning tzBTC is a smart contract on the Tezos blockchain based on the FA1.2 token standard (see TZIP-7), representing the balances for the Bitcoin held in custody by the keyholders.

To be finalized.

Next Steps

The launch of tzBTC marks an important step in the maturation of the Tezos ecosystem. By tokenizing assets on Tezos, users will gain access to novel financial products and capabilities. BTC is just the first asset to help facilitate this evolution.

To get involved in the tzBTC ecosystem and help accelerate the adoption of this project, please contact one of the Keyholders that are listed on tzbtc.io.