Wrapped Bitcoin on Tezos

A Brief Overview

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 Bitcoin (BTC), wrapped in a smart contract called tzBTC on the Tezos 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 Tezos to directly transact in BTC on the Tezos blockchain, bringing BTC’s liquidity and brand to the Tezos ecosystem and enabling novel financial use-cases on-chain.

Governance, Key Stakeholders and Processes

Governance and Key Stakeholders

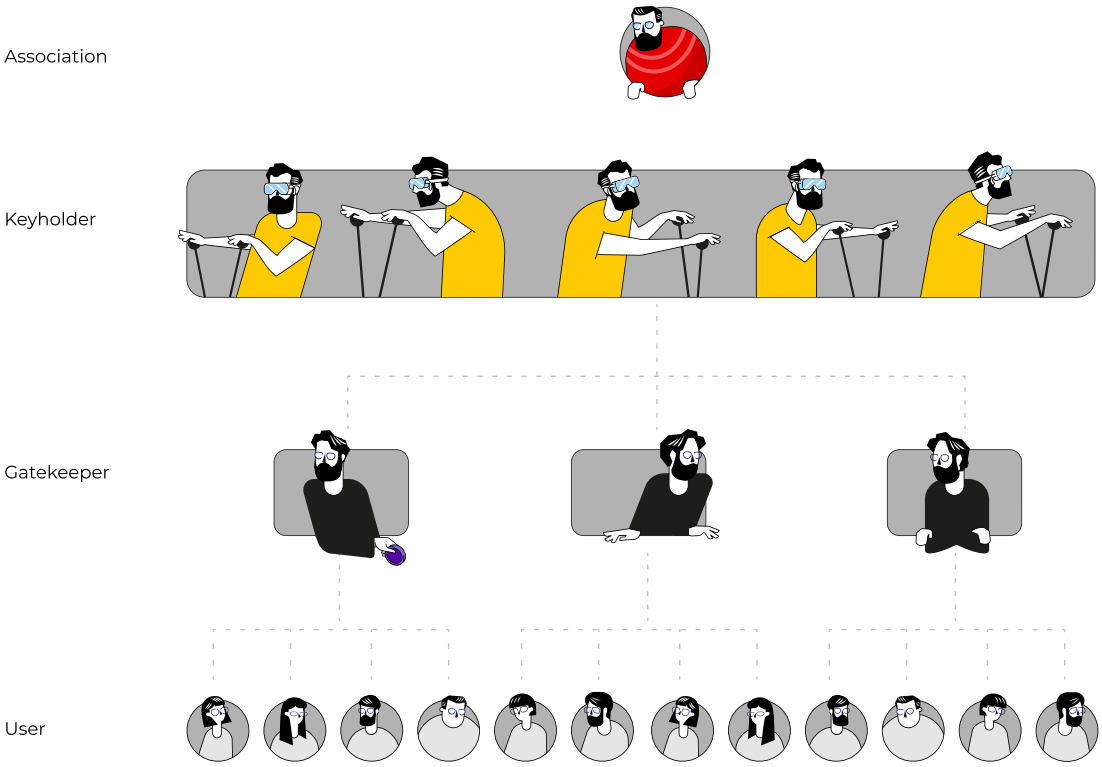
The governance mechanism of the tzBTC contract allows for the compliant and secure issuance of BTC-backed tokens on the Tezos blockchain. The various responsibilities are managed by several key stakeholders: the Association, Keyholders, Gatekeepers, and Users.

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 supervises Keyholder meetings to manage the supply of tzBTC (mint and burn) and to determine the fees for conducting such actions. The Association also mediates any dispute arising with respect to the interpretation, performance, or termination of the Keyholder Agreement, prior to engaging in a dispute in court. For more information on this topic, see Section 10 of the Keyholder Agreement.

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 for the 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 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 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: 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 BTC held in custody by Keyholders.

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 and the chart in Appendix II below.

In addition to the tzBTC FA1.2 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 Tezos community. To view tzBTC in circulation, check it out on a Tezos block explorer like TzStats and tezblock. To inspect the contract itself, check out Better Call Dev and Misualizer. An independent external audit of the contract was completed by Least Authority. Those interested may find Least Authority's full audit report here.

Next Steps

The launch of tzBTC is one of the first examples of tokenization and DeFi (decentralized finance) on Tezos. Blockchains enable us to expressively encode financial permissioning and governance rules in a publicly transparent way. In the future, we hope to explore novel mechanisms for governing, using, and transacting in wrapped assets on the Tezos blockchain.

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 and/or Tezos blockchains, 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.

Appendix II
A guide to the tzBTC contract permissions

The table below describes the permissions provided to the main stakeholders in the tzBTC smart contract.

Functionality (entrypoint)	Keyholders (as Owner)	Gatekeepers, Users
getVersion	x	x
getAllowance	x	x
getBalance	x	x
getTotalSupply	x	x
getTotalMinted	x	x
getTotalBurned	x	x
getOwner	x	x
getRedeemAddress	x	x
getTokenMetaData	x	x
Run	x	x
Upgrade	x	
epwBeginUpgrade	x	
epwApplyMigration	x	
epwSetCode	x	
epwFinishUpgrade	x	
Transfer	x	x
Approve	x	x
Mint	x	
Burn	x	
addOperator	x	
removeOperator	x	
setRedeemAddress	x	
Pause	x	
Unpause	x	
transferOwnership	x	
acceptOwnership	x	