

## tBTC

tBTC is Bitcoin on the Ethereum network. To summarize, users wishing to mint tBTC deposit Bitcoin into an address trustlessly created and controlled by a group of bonded signers. The bonds keep the system participants honest by incentivizing good behavior and punishing dishonesty. At the moment, deposits are only possible in fixed-sized lots of 1 Bitcoin and all signer bonds are denominated in ETH.

The depositor puts down a bond and sends a deposit request transaction to the tBTC smart contract on Ethereum. Sending a deposit request transaction signals to the smart contract that you would like to mint new tBTC by depositing Bitcoin. The depositor must put down a bond in the form of ETH to initiate this process. The bond serves as a form of anti-spam mechanism and is returned to the user when the deposit is completed.

A signing group is selected and the BTC wallet / deposit address they create is returned by the Ethereum contract. When creating the deposit address, the system randomly selects a group of signers which generate the Bitcoin wallet together. And so, this new Bitcoin wallet requires M of N signatures to generate valid Bitcoin transactions. In order to keep signers honest, those who wish to become a signer must put down a bond of ETH proportional to the risk they pose to the system. For example, if the BTC wallet requires 3 out of 5 signatures, the signers must each have a bond of ETH equal to 0.33 BTC.

The depositor sends the BTC to the deposit address and then sends a transaction with proof of the deposit to the tBTC smart contract. The depositor takes the deposit BTC address returned by the smart contract and sends it 1 BTC. After the transaction is confirmed, the depositor submits a transaction including a proof which is verified on-chain by the signers with a simple payment verification (SPV) system.

The contract mints tBTC and a beneficiary token both of which are issued to the depositor. The signing group verifies the proof of deposit and issues the tBTC tokens to the depositor. The tBTC smart contract keeps 0.0005 TBTC of every deposit as a beneficiary bond. Additionally, the depositor receives an ERC-721 token which signifies the beneficiary or who receives this bond in the future.

Redeeming tBTC for Bitcoin is pretty straightforward. However, it's worth noting that the underlying Bitcoin can only be redeemed after 6 months have elapsed since the initial deposit. After which point, it's possible for anyone to redeem the deposit. Submit a redemption request transaction to the smart contract which includes your desired recipient Bitcoin address. During which you'll repay the outstanding TBTC deposit amount, signer fees, and 0.0005 beneficiary bond. The beneficiary receives their 0.0005 TBTC and little bit extra back. And, the rest of the tokens are burned, including the ERC-721. Next, the signers wait for the transaction to be confirmed on the Ethereum blockchain. Finally, the signers produce a signature which can be submitted to the Bitcoin network to send your BTC to the address you specified.

Ethereum's known for being the leading programmable blockchain with a wildly active developer community. Effectively tokenizing BTC without a middleman opens up a world of possibilities for users and developers alike. tBTC makes it possible for Bitcoin holders to tap into Ethereum's growing list of decentralized finance (DeFi) DApps. For example, smart contract developers could integrate tBTC into their DApps as collateral enabling Bitcoin holders to be able to borrow against their BTC. Or, even something as simple as Bitcoin can now be trustlessly listed on decentralized exchanges (DEXes).

tBTC is expected to launch in early 2020 on the KEEP network. Genesis Block Fund owns a small position of KEEP tokens in its portfolio with some other prominent investors such as Andreessen Horowitz (a16z), Polychain Capital, Paradigm, Draper Associates and others.