Can BTX Be Faked? Authenticity, Supply and Anti-Counterfeiting

Counterfeiting BTX is not possible without breaking consensus. Here is why, in precise terms, and how anyone can verify it.

JULY 5, 2026 · 9 MIN READ · EASYBTX.COM/RESEARCH/BTX-AUTHENTICITY

ABSTRACT

Can counterfeit BTX exist? How BTX's fixed supply, mining-only issuance, and inherited Bitcoin consensus rules make fake coins impossible, and the real risks worth knowing.

A common and healthy question from people holding or receiving BTX is: could someone create fake BTX, or counterfeit coins that the network accepts as real? We looked at this the way an auditor would, working from the BTX consensus rules, the reference node source code, and the public ledger.

The short answer: **counterfeiting BTX is not possible without breaking the network's consensus rules, the same protection that secures Bitcoin.** BTX has a fixed supply, no premine, and no way to issue "another token" on the chain. Every coin that exists was created by mining and is traceable, block by block, back to a mining reward. The genuine risks that do exist are different in kind, and we cover each below.

What BTX actually is

BTX is a post-quantum hard fork of Bitcoin Knots v29.2. It keeps Bitcoin's proven ledger and monetary design and changes exactly two things:

- **Proof-of-work.** Bitcoin's SHA-256d is replaced by MatMul PoW, where miners perform large matrix multiplication over a finite field and hash the computation transcript. The same math that powers AI and GPU workloads secures the chain.
- **Signatures.** Elliptic-curve (ECDSA) keys are replaced by post-quantum primitives. This is why BTX addresses look like `btx1z...`, a pay-to-Merkle-root (P2MR) address encoded with Bech32m.

Everything about money, the supply cap, the block subsidy, the rule that a transaction cannot spend more than it holds, the range and overflow checks, is inherited unchanged from the most battle-tested financial software in existence.

Can BTX be counterfeited? Three independent reasons it cannot

1. There is no token layer. There is only BTX. BTX is a UTXO chain, an accounting ledger of unspent coins, not a smart-contract platform. There is no minting function, no token-creation standard like ERC-20, and no staking issuance. Nobody can create a new asset on BTX. Just as there is only one Bitcoin, there is only one BTX. The only thing that could theoretically be counterfeited is BTX itself, and that is blocked by the next two points.

2. Fixed supply, mining-only issuance, no premine. BTX has a hard cap of 21,000,000 coins. New coins are created only through mining, in each block's coinbase (the reward transaction). The schedule is public and fixed: an initial reward of 20 BTX per block, halving every 525,000 blocks, trending to zero. There was no premine, no genesis allocation, no ICO, and no founder allocation. Because issuance happens only through mining rewards, every unit of BTX has a birth certificate: the block that minted it.

3. The "no coins from nothing" rule is enforced by every node. In the reference node's transaction-validation code, a transaction is rejected outright if the sum of its inputs is less than the sum of its outputs (the classic inputs-greater-than-or-equal-to-outputs rule). Every value is range-checked, and every sum uses overflow-safe arithmetic. There is no code path where outputs can exceed inputs. A miner cannot even overpay their own block reward: a node rejects any block whose coinbase pays more than the allowed subsidy plus fees. On the live chain, mined blocks pay exactly the expected subsidy.

Put together: no new asset can be invented, no coins can appear except by mining, and no transaction can output more value than it takes in. That is what "you cannot fake BTX" means in precise terms.

Every coin is auditable back to mining

Because BTX is a public ledger, the origin of any coin can be traced. Follow any balance backward through its transactions and you eventually reach one or more coinbase transactions, freshly mined coins. In practice, most coins reach a holder through mining-pool payout wallets: pools accumulate exactly-sized block rewards and distribute them to miners in the normal pattern. Anyone can perform this trace themselves on the public block explorer; it requires no special access. Authenticity on BTX is not a matter of trust, it is a matter of arithmetic that every node re-checks.

An important distinction: on-chain analysis proves a coin is real BTX created by mining. It does not, and cannot, tell you who mined it or the identity behind a wallet. Authenticity and identity are separate questions. Every confirmed BTX is authentic by construction; custody and identity are what you verify through your counterparty, not the chain.

The real risks, and how to handle them

None of the following can counterfeit BTX. They are worth understanding anyway.

51% attacks and double-spends

Like every proof-of-work chain, BTX's ordering of transactions is secured by mining. If a single party controlled more than half of all mining power, they could attempt a double-spend: pay someone, let that payment confirm, then secretly mine a longer alternative chain in which the same coins return to themselves, and finally publish it so the network reorganizes to their version. The coins never exist twice; the earlier payment is erased, and a counterparty who already released value is the loser.

What a majority attacker cannot do is just as important: they cannot create coins from nothing, cannot forge signatures to spend coins they do not own, cannot rewrite old and deeply-buried transactions, and cannot change the rules such as the 21 million cap. The only real leverage is reversing their own recent transactions and censoring.

The defense is simple and effective: wait for enough confirmations before treating a large incoming payment as final. Each additional block makes a reversal exponentially harder. The cost of such an attack also scales directly with the network's total mining power, which for BTX has grown rapidly as more miners join, making a majority takeover far more expensive over time.

The shielded (privacy) pool

BTX inherited an optional privacy pool, a shielded-value turnstile, from its lineage. This is the one money-related component that is not inherited from Bitcoin, and it is being wound down: by consensus, new deposits into the shielded pool are disabled, and the network has eased the exit path so holders can move shielded funds back to transparent addresses. The easyBTX wallet works only with standard transparent `btx1z...` coins and does not create shielded transactions. If you hold any shielded BTX, unshield it to a transparent address while the exit path is available. Retiring this pool is a net positive for authenticity: it removes the only surface where a supply bug could ever hide.

Impersonation and off-chain scams

Because the chain itself cannot be faked, realistic scams target people, not the protocol: a counterfeit wallet app, a phishing website, a spoofed payout address, or a completely different coin that merely borrows the name BTX. A common technical variant is clipboard-hijacking malware that silently swaps a copied address for an attacker's. Defenses are straightforward: download wallet and mining software only from official sources, verify the destination address (check the first and last characters) before sending, and remember that anything calling itself BTX that is not on this chain is not BTX.

How to verify BTX for yourself

You do not have to take anyone's word for it. Everything here is publicly checkable:

- **The rules and the code** live in the open-source BTX reference node. The supply schedule, the coinbase subsidy, and the value-conservation checks are all readable.
- **The ledger** is public. Any transaction or address can be inspected on the block explorer, and any coin can be traced back to the mining reward that created it.
- **Your own coins** can be validated by running a full node, which independently re-verifies every rule from the genesis block forward.

Authenticity on BTX is built on verification, not trust. That is the entire point of a public, rule-enforced blockchain.

Postscript added 22 August 2026
Published 5 July 2026. Nothing this article argues about counterfeiting, supply or issuance has changed, but two details around it have, and one link had to be repaired.

The mining algorithm changed, the money rules did not. On 10 August 2026, at block 185,000, BTX replaced MatMul v3 with MatMul v4.7. Mining is still large matrix multiplication over a finite field, so this article's description holds, but the workload is now a single deterministic inference episode per attempt rather than millions of cheap attempts per second. None of this touches the cap, the subsidy, the value-conservation rules or anything else that makes a fake coin impossible. See what MatMul v4.7 actually does.

Supply, refreshed. At block 197,897 on 22 August 2026, with the subsidy still at 20 BTX and no halving yet, 3,957,940 BTX have been mined. That is 18.85 percent of the 21,000,000 cap.

The explorer link was replaced. This article originally pointed at explorer.minebtx.com, which is now offline. The link goes to btxscan.io, which serves the same public ledger and supports the same address and transaction lookups the verification steps above describe.

What we did not re-check. We have no fresh reading on the shielded pool wind-down beyond what is written here. Treat that section as accurate to July 2026.

Frequently asked questions

Is BTX a real blockchain and real digital money?

Yes. BTX is a live, public, proof-of-work blockchain forked from Bitcoin Knots, with an independently verifiable ledger and a fixed coin supply.

Can someone create fake BTX?

No. Counterfeiting requires breaking consensus rules that every node enforces. There is no way to create coins from nothing, and no transaction that outputs more than it inputs is accepted.

Can BTX be counterfeited or duplicated like a copied file?

No. Coins are entries in a shared ledger validated by thousands of independent checks. A duplicated coin is simply a transaction the network rejects.

Are there other tokens on the BTX chain? Can people mint their own tokens?

No. BTX is a UTXO chain, not a smart-contract platform. There is no token-creation feature. There is only BTX.

Was there a premine, ICO, or founder allocation?

No. There was no premine and no genesis allocation. Every coin was created by mining.

What is the maximum supply of BTX?

21,000,000 BTX, a fixed hard cap identical in size to Bitcoin's.

How are new BTX created?

Only through mining. Each block's coinbase transaction issues the block reward to the miner. There is no other issuance path.

What is the block reward and halving schedule?

The initial reward is 20 BTX per block, halving every 525,000 blocks and trending toward zero, which is what enforces the fixed supply over time.

How do I know the coins I received are genuine?

If a transaction is confirmed in a block, every node has already validated that its inputs exist and cover its outputs. You can also trace the coins on the public explorer back to the mining rewards that created them.

What is a 51% attack?

An attempt by someone controlling a majority of mining power to reorganize recent blocks, typically to reverse a payment they made (a double-spend). It does not create new coins.

Can a 51% attack steal my coins or create fake BTX?

No. It cannot forge signatures, cannot spend coins it does not own, and cannot mint new coins. Its only leverage is reversing the attacker's own recent transactions.

How many confirmations should I wait for?

For everyday amounts a few confirmations are fine; for large amounts wait for more. Each confirmation makes any reversal exponentially harder.

What is MatMul proof-of-work?

BTX's mining algorithm. Instead of SHA-256 hashing, miners perform large matrix multiplications over a finite field and hash the computation transcript, reusing the same math that powers GPU and AI workloads.

Is BTX quantum-safe? What is a btx1z address?

BTX replaces elliptic-curve signatures with post-quantum cryptography. Its addresses use a pay-to-Merkle-root (P2MR) format encoded with Bech32m, which is why they begin with `btx1z`.

Is BTX a fork of Bitcoin?

Yes. BTX is a hard fork of Bitcoin Knots v29.2. It keeps Bitcoin's ledger and monetary rules and changes the proof-of-work and the signature scheme.

What is the difference between BTX and BTC?

BTX shares Bitcoin's 21M supply model and ledger design but uses post-quantum signatures and a matrix-multiplication proof-of-work, and it targets faster blocks. They are separate networks and separate coins.

Can the 21 million supply cap ever be changed?

Not without a network-wide consensus change that every participant would have to adopt. The cap is enforced by the rules each node runs, not by any single operator.

What is the shielded pool and is it safe?

An optional privacy feature inherited from BTX's lineage. It is being wound down: new deposits are disabled and holders are encouraged to move shielded funds to transparent addresses. The easyBTX wallet uses only transparent coins.

How do I avoid BTX scams?

Download software only from official sources, verify destination addresses before sending, and treat anything calling itself BTX that is not on this chain as fake. The protocol cannot be faked; scams target people.

How can I verify all of this myself?

Read the open-source reference node for the rules, inspect any transaction on the public block explorer, and, if you want maximum assurance, run a full node that re-verifies every rule from the genesis block.

Is easyBTX official, and how do I make sure I have the real app?

Download easyBTX only from the official website and releases. Genuine builds are signed, so an impersonating copy cannot masquerade as the real application without failing verification.
