

Das BTX-Handbuch

Was BTX ist, wie das Mining funktioniert, wie die Chain an diesen Punkt kam und wo du jede Aussage selbst nachprüfen kannst.

Nur zu Bildungs- und Unterhaltungszwecken. Keine Finanzberatung. easyBTX ist nicht das Kernteam von BTX, und BTX hat keinen etablierten öffentlichen Markt.

Inhalt

- 1 Wer das hier geschrieben hat, und wer nicht
 - 2 Was BTX ist
 - 3 Die Arbeit ist Matrixmultiplikation
 - 4 Zwei Arbeitsfunktionen, und warum es die zweite gibt
 - 5 Wie ein Block geprüft wird, und wie sich auch das geändert hat
 - 6 Was hier wirklich ungewöhnlich ist
 - 7 Eine kurze Geschichte der Chain
 - 8 Gesamtmenge und Ausgabe
 - 9 Lässt sich BTX fälschen?
 - 10 Drei Wege mitzumachen
 - 11 Wallets und Anmelden ohne Konto
 - 12 Wo du mehr erfährst
 - 13 Der ehrliche Teil
-

1 Wer das hier geschrieben hat, und wer nicht

easyBTX macht Software für BTX: einen Miner, eine Node-App und ein paar kostenlose Werkzeuge.

easyBTX ist nicht das Kernteam von BTX. Die Konsens-Software der Chain wird vom BTX-Projekt geschrieben und veröffentlicht. easyBTX hat an diesem Projekt keinen Anteil und darüber keine Autorität. Wir lesen dessen Quellcode und dessen Releases so, wie es jeder andere auch kann.

Das ist wichtig dafür, wie du dieses Handbuch lesen solltest. Nichts hier ist eine Ankündigung, eine Roadmap oder ein Versprechen im Namen der Chain, denn so etwas steht uns nicht zu. Es ist die Lesart eines unabhängigen Teilnehmers, gestützt auf öffentliche Quellen und so geschrieben, dass du sie nachprüfen kannst. Wo die Faktenlage unklar ist, sagen wir das, und wo wir früher falsch lagen, sagen wir das ebenfalls.

Zwei Offenlegungen, denn sonst nimmst du am Ende etwas Freundlicheres an, als es der Wahrheit entspricht. Erstens: easyBTX hat ein Interesse daran, dass es BTX gut geht, und nimmt eine Gebühr vom Mining. Zweitens: Die hinten aufgeführten Projekte sind nicht alle unabhängig von uns. **BTX selbst ist wirklich getrennt**, und das ist die Trennung, auf die es am meisten ankommt. Aber btx.best und btxscan.io werden von easyBTX gebaut und sagen das auch in ihren eigenen Fußzeilen, und PQ Wallet, die bonuz-Wallet und qID teilen sich Leute mit easyBTX. Wo dieses Handbuch diese Produkte beschreibt, lies es als die Beschreibung eines Beteiligten, der daran mitgebaut hat. Die Chain, die Pools und postquantum.wiki gehören nicht uns. Dass ein Projekt hinten aufgeführt ist, heißt nicht, dass wir dafür garantieren, und keines dieser Projekte steht für die anderen ein.

2 Was BTX ist

BTX ist ein Fork von Bitcoin, gebaut, um Quantencomputern standzuhalten.

Bitcoin signiert jede Transaktion mit ECDSA, einem klassischen Verfahren auf Basis elliptischer Kurven. Ein ausreichend großer Quantencomputer könnte es brechen und Coins ausgeben, die ihm nicht gehören. BTX ersetzt dieses Signaturverfahren durch Post-Quanten-Signaturen. Deshalb sieht eine BTX-Adresse anders aus als eine Bitcoin-Adresse: BTX-Adressen beginnen mit `btx1z`.

Alles andere ist bewusst wie bei Bitcoin gehalten:

- Eine feste Menge von 21.000.000 Coins, ohne jede Möglichkeit, mehr zu erzeugen.
- Kein Premine. Coins entstehen ausschließlich als Mining-Reward, Block für Block.
- Mining per Proof of Work. Es gibt niemanden, den du um Erlaubnis fragen musst, und keine Instanz, an der du vorbeikommen musst.
- Selbstverwahrung. Es gibt keine Konten und keinen Verwahrer. Du hältst die Schlüssel, und die Schlüssel halten die Coins.

Die Chain ist jung. Block 0 trägt den Zeitstempel 19. März 2026, geschürft wurde der erste Block tatsächlich am 23. März 2026.

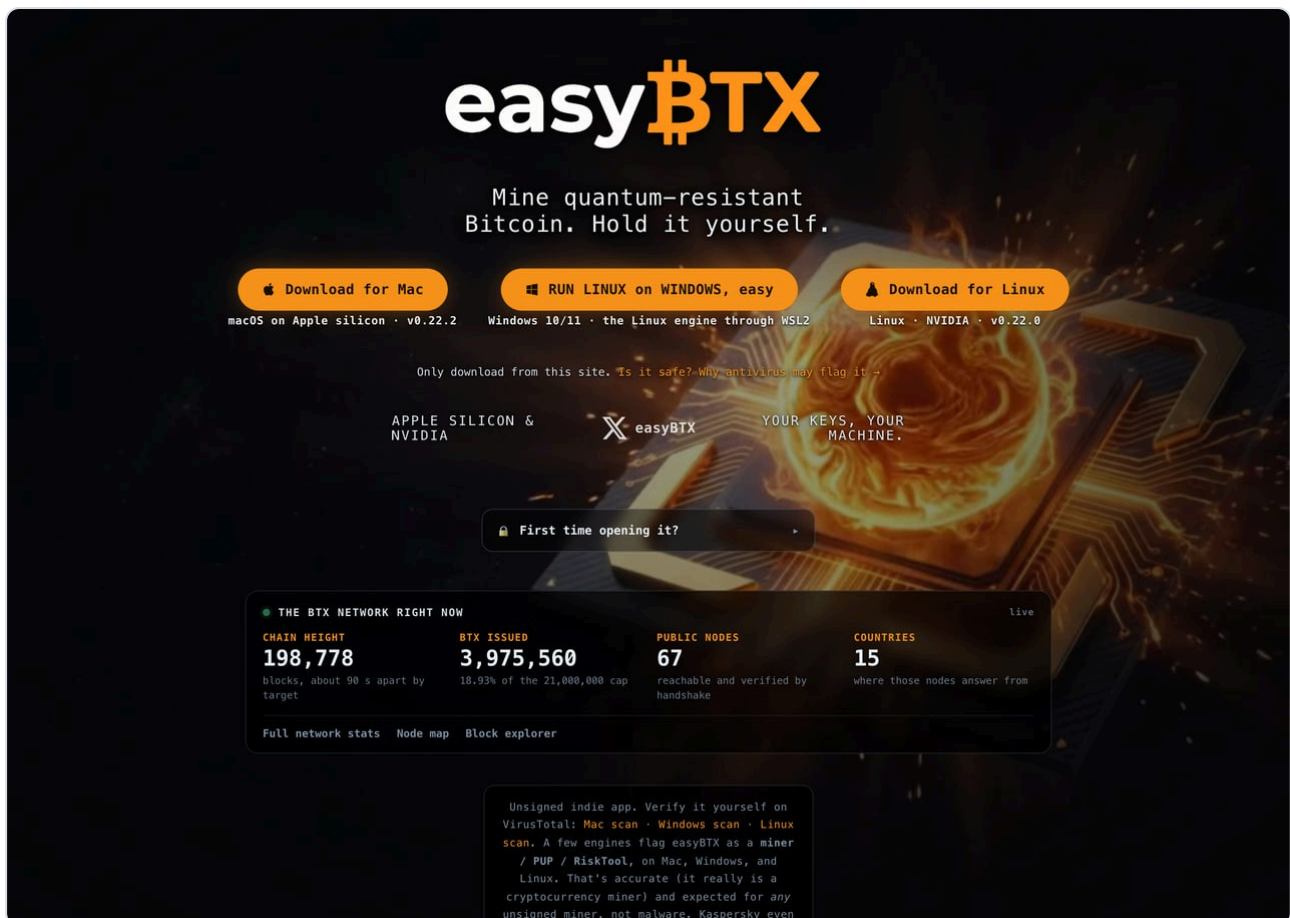
3 Die Arbeit ist Matrixmultiplikation

Bitcoin-Miner suchen nach Hashes. BTC-Miner multiplizieren Matrizen, also genau jene dichte Arithmetik, für die moderne KI-Beschleuniger gebaut sind. Genau das ist gemeint, wo immer dir in der BTC-Dokumentation „matmul“ begegnet: Matrixmultiplikation, eingesetzt als die Arbeit, die die Chain absichert.

Praktisch heißt das: Eine GPU ist die natürliche Maschine für BTC, und die Arbeit ist eine echte numerische Berechnung statt einer Hash-Lotterie.

Es lohnt sich, genau zu sein bei dem, was das bedeutet und was nicht, denn keine Aussage über BTC wird häufiger übertrieben. Die Eingaben jeder Berechnung werden aus der Chain selbst abgeleitet, und vom Ergebnis bleibt nur ein Digest übrig. Das berechnete Produkt wird also an niemanden außerhalb der Chain ausgeliefert. **BTC verkauft heute keine KI-Rechenleistung.** Ein Markt für verifizierbare Berechnungen, auf dem ein Außenstehender einen echten Auftrag einreicht und für das Ergebnis bezahlt, wird in der Spezifikation von BTC selbst als spätere Richtung genannt, und es gibt ihn nicht.

Was heute stimmt, ist leiser und dafür haltbarer: BTC-Mining bezahlt eine verteilte Menge ganz normaler Menschen dafür, KI-fähige Hardware zu besitzen, sie mit Strom zu versorgen und online zu halten, in vielen unabhängigen Händen statt in wenigen Rechenzentren.



Der easyBTX-Miner auf easybtx.com, mit der aktuellen Chain-Höhe, der ausgegebenen Menge gegenüber der Obergrenze von 21.000.000 und der Zahl der erreichbaren öffentlichen Nodes.

4 Zwei Arbeitsfunktionen, und warum es die zweite gibt

BTX hatte in seinem Leben genau zwei Mining-Algorithmen. Das sei klar gesagt, denn die Versionsnummern in den Entwurfsdokumenten von BTX lassen sich leicht falsch lesen: Sie beschreiben eine Forschungs-Roadmap, keine Abfolge von Chains, die tatsächlich liefen.

MatMul v3 lief vom allerersten Block an. Ein Versuch war eine einzelne Matrixmultiplikation von 512 mal 512 über einem Primkörper, der so gewählt wurde, dass sich die Arithmetik sauber sowohl auf CUDA als auch auf Apples Metal abbilden lässt. Ein Versuch dauerte Mikrosekunden, eine Karte schaffte also Millionen pro Sekunde, und die Mining-Geschwindigkeit wurde entsprechend angegeben.

Drei Dinge sprachen dafür. Die Arbeit ist gewöhnliche dichte lineare Algebra, die natürliche Maschine dafür ist also eine GPU und kein Chip, der sonst nichts kann. Die Konstruktion, auf der sie beruht, verursacht kaum Mehraufwand gegenüber einer ganz normalen Matrixmultiplikation, es geht also nur sehr wenig Strom für die Beweismechanik selbst verloren. Und sie ließ die Tür offen für Arbeit, die eines Tages auch außerhalb der Chain nützlich sein könnte.

v3 wurde mehrfach gehärtet, ohne dass sich die Arbeit selbst änderte. Bei Block 125.000 wurden die Matrizen an den veränderlichen Teil des Block-Headers gebunden, ein Miner konnte ein vorbereitetes

Paar also nicht länger über viele Versuche hinweg wiederverwenden. Bei Block 130.500 wurden sie zusätzlich an den Elternblock gebunden, damit eine Vorlage, die für einen Elternblock gebaut wurde, nicht gegen einen anderen, zurückgehaltenen erneut eingesetzt werden konnte. Keine dieser beiden Änderungen hat verändert, was das Mining berechnet. Sie haben Abkürzungen versperrt.

MatMul v4.7 hat die Arbeitsfunktion bei Block 185.000 ersetzt, am 10. August 2026. Ein Versuch war ab da keine kleine Multiplikation mehr, sondern eine einzelne, unteilbare Episode: vier aufeinanderfolgende Runden über sechzehn Schichten, Matrizen der Breite 4.096, rund 141 Billionen ganzzahlige Multiplikations-Akkumulations-Operationen, etwa 4,8 GB GPU-Speicher und in der Größenordnung von dreißig Sekunden ununterbrochener Arbeit. Du kannst eine Episode nicht anhalten, nicht fortsetzen, und du kannst auch nicht sechzig Prozent davon erledigen und dafür sechzig Prozent angerechnet bekommen.

Es lohnt sich, die Begründung dahinter zu verstehen, denn sie ist das Gegenteil dessen, was die meisten annehmen. Eine Lotterie mit extrem billigen Losen lädt jemanden dazu ein, eine Maschine zu bauen, die nichts anderes tut, als sehr schnell Lose zu kaufen. Jedes Los teuer, sequenziell und speicherhungrig zu machen, nimmt den größten Teil dieses Spielraums weg: Die Arbeit ist ohnehin genau die Operation, für die Tensor-Kerne existieren, für einen Spezialchip bleibt also wenig übrig, was er geschickter machen könnte, und kein Schritt lässt sich überspringen, weil die Prüfung eines Blocks die Episode exakt nachrechnet. Die Entwurfsdokumente nennen ein zweites Motiv ganz direkt: gemietete Consumer-GPUs bei einer jungen Chain preislich aus der Reichweite eines Angriffs zu drängen.

Der Preis dafür war real, und das Projekt hat nie etwas anderes behauptet. Macs konnten neun Tage lang überhaupt nicht minen, weil es am Tag der Aktivierung noch keinen Solver für die neue Arbeit unter Metal gab. Nodes mit älterer Software blieben bei Block 184.999 stehen und kamen nicht weiter. Die Difficulty musste in einem einzigen Schritt um einen Faktor von rund 120.000 neu kalibriert werden. Akzeptierte Shares wurden so selten, dass eine gesunde Maschine heute eine Stunde lang still dasitzen kann. Karten, die BTX im Juli mit Gewinn geschürft haben, schürften es heute gar nicht mehr.

5 Wie ein Block geprüft wird, und wie sich auch das geändert hat

Wie geprüft wird, ist der Teil, der sich am meisten zu verstehen lohnt, und er hat sich in die entgegengesetzte Richtung entwickelt, als du vielleicht erwartest.

Unter v3 war die Prüfung raffiniert und billig. Statt eine Multiplikation von 512 mal 512 noch einmal auszuführen, multiplizierte ein Prüfer die behauptete Antwort mit ein paar Zufallsvektoren und verglich das Ergebnis. Das ist der Algorithmus von Freivalds, und nach zwei Runden davon rutscht ein falsches Ergebnis mit einer Wahrscheinlichkeit von weniger als eins zu 2 hoch 62 durch. Teuer zu erzeugen, billig zu prüfen, und genau das ist die Eigenschaft, die du haben willst.

Unter v4.7, so wie es heute läuft, prüft das Netzwerk, indem es die gesamte Episode exakt nachrechnet und die Digests vergleicht. Eine billige Prüfung gibt es nicht. Das ist eine bewusste Staffelung und kein Versehen: Kompakte Beweise, die die Prüfung wieder billig machen würden, sind als spätere Epochen beschrieben, und **keine davon hat eine Aktivierungshöhe**. Der veröffentlichte Plan nennt vier, von denen nur die erste läuft.

Das Projekt sagt das unmissverständlich, und es lohnt sich, es zu zitieren statt zu umschreiben:

Die Art der Prüfung hat ihre Form verändert. In der Stufe von v4.7, die jetzt live ist, prüft das Netzwerk, indem es die Episode exakt nachrechnet und die Digests vergleicht.

Kompakte Beweise, die die Prüfung wieder billig machen würden, sind als spätere Stufe genannt, ohne Aktivierungshöhe. Die elegante Eigenschaft, teuer zu erzeugen und billig zu prüfen, ist im Moment also ein Entwurfsziel und nicht das ausgelieferte Verhalten.

Eine Folge davon ist für jeden wichtig, der eine Node betreibt. Eine Episode nachzurechnen verlangt eine dafür qualifizierte GPU, die meisten Maschinen können die neueste Arbeit also nicht selbst prüfen. Sie folgen stattdessen einem kleinen signierten Datensatz, 208 Byte pro Block. Deshalb liegt dem Netzwerk so viel an Nodes, die bereit sind, diese Datensätze auszuliefern, und deshalb hat eine Unterbrechung beim Signieren im August 2026 zweimal Teile des Netzwerks eingefroren, während mit der Chain selbst alles in Ordnung war.

6 Was hier wirklich ungewöhnlich ist

Marketing beiseite: Ein paar Dinge an diesem Entwurf fallen jedem auf, der beruflich Konsens-Code liest.

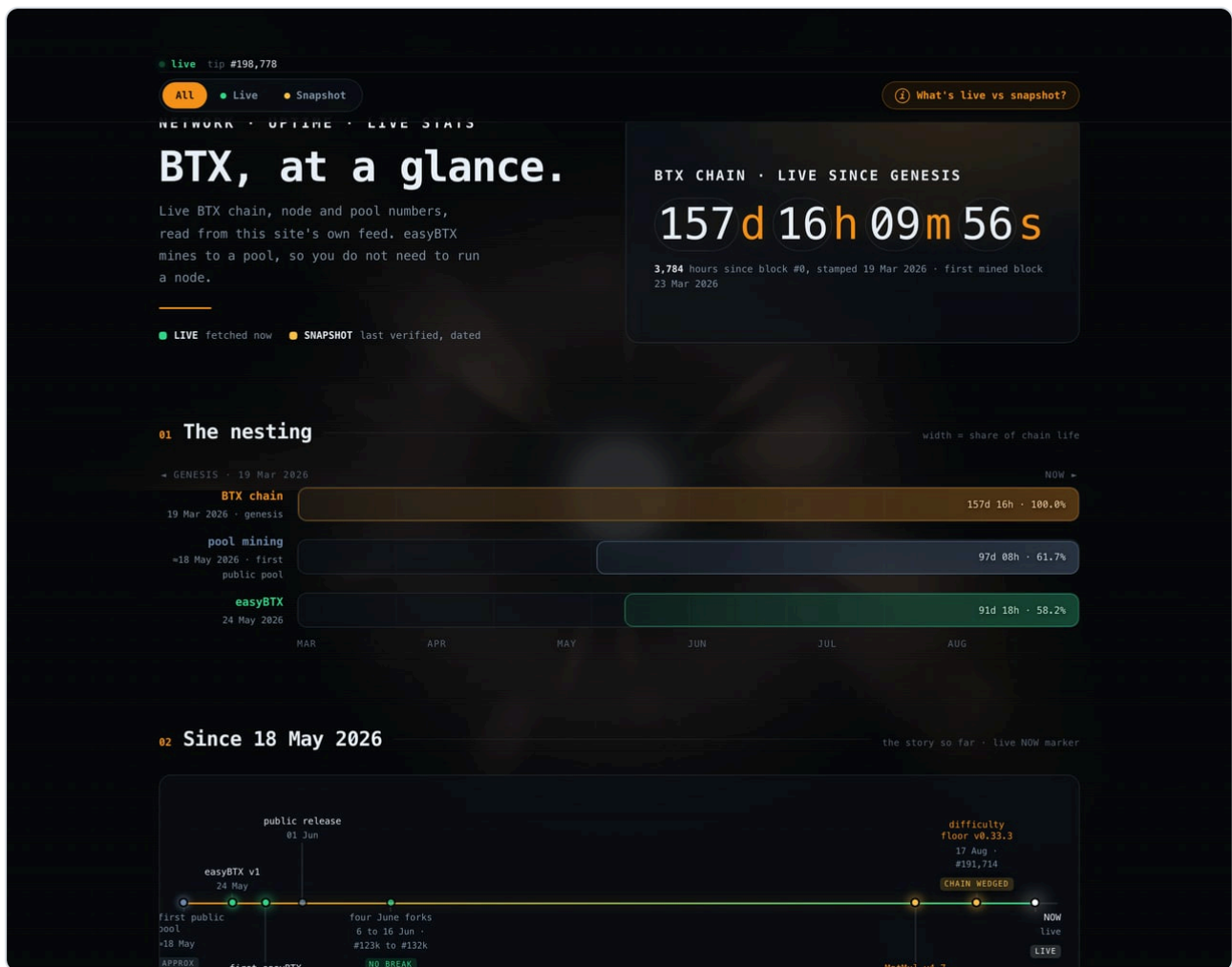
- **Die Arbeit ist echte dichte ganzzahlige lineare Algebra**, deterministisch und byte-genau über zwei unabhängige GPU-Backends hinweg. Hardware von zwei verschiedenen Herstellern muss denselben Digest liefern.
- **Die Änderung der Kosten pro Versuch ist ein Kategoriewechsel**, von Mikrosekunden auf rund dreißig Sekunden. Nur sehr wenige Chains versuchen so etwas, und es macht einen Versuch wirklich unteilbar.
- **Ob eine Maschine minen darf, ist eine Messung und keine Liste**. Die Software bittet ein Gerät, ein bekanntes Ergebnis zu reproduzieren, und glaubt der Antwort, statt den Namen des Chips gegen eine Freigabeliste zu prüfen. Sowohl easyBTX als auch der Hersteller der Engine haben Hardware-Anforderungen veröffentlicht, die sich als falsch herausstellten, und beide wurden durch Messung korrigiert.
- **Der Header hat sich nie geändert**. Ein vollständiger Austausch des Proof of Work ging in Betrieb, ohne dem 182 Byte großen Block-Header ein einziges Byte hinzuzufügen. Deshalb haben

Pools, Miner und Wire-Protokolle das unbeschadet überstanden. Das ist unspektakulär und wirklich schwer.

Nichts davon heißt, dass die Arbeit schon jemandem außerhalb der Chain nützt. Sie tut es nicht, und Abschnitt 2 sagt das auch. Aber die Mechanik ist echt, die Zahlen oben stehen im Konsens-Quellcode und nicht in einer Broschüre, und das Projekt dokumentiert seine eigenen verworfenen Parameterwahlen und schaltet seine eigenen unfertigen Bestandteile im Code ab. Das ist ein besseres Zeichen als jede Behauptung.

7 Eine kurze Geschichte der Chain

WANN	HÖHE	WAS PASSIERT IST
19. März 2026	0	Der Genesis-Block bekommt seinen Zeitstempel, mit MatMul v3 als Arbeitsfunktion von Anfang an. Der erste Block wurde am 23. März geschürft.
Anfang Juni 2026	~123.000	Der Fork v0.31.0.
8. Juni 2026	125.000	Die Seeds werden an den Header gebunden, ein vorbereitetes Matrizenpaar kann also nicht mehr viele Versuche bedienen.
Mitte Juni 2026	~130.500	Die Seeds werden an den Elternblock gebunden, das versperrt die Abkürzung, eine Vorlage gegen einen anderen Block erneut einzusetzen. Die Arbeitsfunktion bleibt unverändert.
Mitte Juni 2026	~132.000	Ein Node-Upgrade.
10. Aug. 2026	185.000	MatMul v4.7 wird aktiv. Ein Versuch wird zu einer Episode von dreißig Sekunden.
17. Aug. 2026	191.690	Das Netzwerk bleibt hängen. BTX Core v0.33.3 erscheint noch am selben Tag mit einer Difficulty-Untergrenze ab Block 191.714, und die Chain erholt sich.
22. Aug. 2026	197.000+	Rund 3,96 Millionen BTX ausgegeben, etwa 19 Prozent der Obergrenze.



Die Live-Statistikseite auf easybtx.com/stats, mit den Zahlen zur Chain, zur Node-Zählung und zu jedem funktionierenden Pool.

8 Gesamtmenge und Ausgabe

Jeder Block zahlt 20 BTX. Der angepeilte Blockabstand liegt bei 90 Sekunden, wobei die Chain über ihre gesamte Laufzeit im Schnitt schneller lief als dieses Ziel. Der Reward halbiert sich alle 525.000 Blöcke, und das Schema geht exakt auf: 525.000 Blöcke zu je 20, dann zu je 10, dann zu je 5 und so weiter ergeben in der Summe genau 21.000.000.

Ein Halving hat es noch nicht gegeben. Das erste steht noch bevor.

Zum Zeitpunkt dieses Textes hatte die Chain Block 197.000 überschritten, es waren also rund 3.960.000 BTX ausgegeben, knapp 19 Prozent der Obergrenze. Aktuelle Zahlen statt dieser findest du auf der Live-Statistikseite, die hinten in diesem Handbuch aufgeführt ist.

9 Lässt sich BTX fälschen?

Nein, und die Gründe dafür sind struktureller Natur, keine Versprechen.

Die Menge ist fest auf 21.000.000 begrenzt, es gab kein Premine, und Coins entstehen ausschließlich durch Mining. BTX ist eine von Bitcoin abgeleitete Chain ohne Token-Ebene, es gibt also keinen Mechanismus, einen gefälschten Coin auszugeben, ohne die Regeln zu brechen, die jede Node unabhängig durchsetzt. Jeder Coin lässt sich Block für Block bis zu einem Mining-Reward zurückverfolgen.

Das ist eine andere Frage als die, ob die Chain angegriffen werden kann. Ein ausreichend großer Anteil an der Mining-Leistung des Netzwerks könnte die jüngsten Blöcke umsortieren, und das gilt für jede Proof-of-Work-Chain, Bitcoin eingeschlossen. Im Forschungsarchiv liegt eine vollständige Untersuchung darüber, was möglich ist und was nicht, dazu die Schritte, mit denen du die Echtheit selbst prüfst.

10 Drei Wege mitzumachen

Minen. easyBTX ist eine einzige App für Mac, Windows und Linux. Sie schließt sich einem Mining-Pool an, zahlt an eine Wallet aus, die du kontrollierst, und hält sich selbst aktuell. Ein Mac braucht Apple Silicon und macOS 26.4 oder neuer, und ob ein bestimmter Mac minen kann, entscheidet nicht der Name des Chips, sondern eine halbe Sekunde dauernde Prüfung, die die App an der GPU durchführt. Windows führt den Linux-Build unter WSL2 aus. Linux braucht eine NVIDIA-GPU. Jede Gebühr wird offen genannt: easyBTX nimmt 4,99 %, der Pool nimmt seine eigene, und unter Windows und Linux nimmt die MATADOR-Engine weitere 1 %. Solo-Mining ist heute auf keiner Plattform verfügbar.

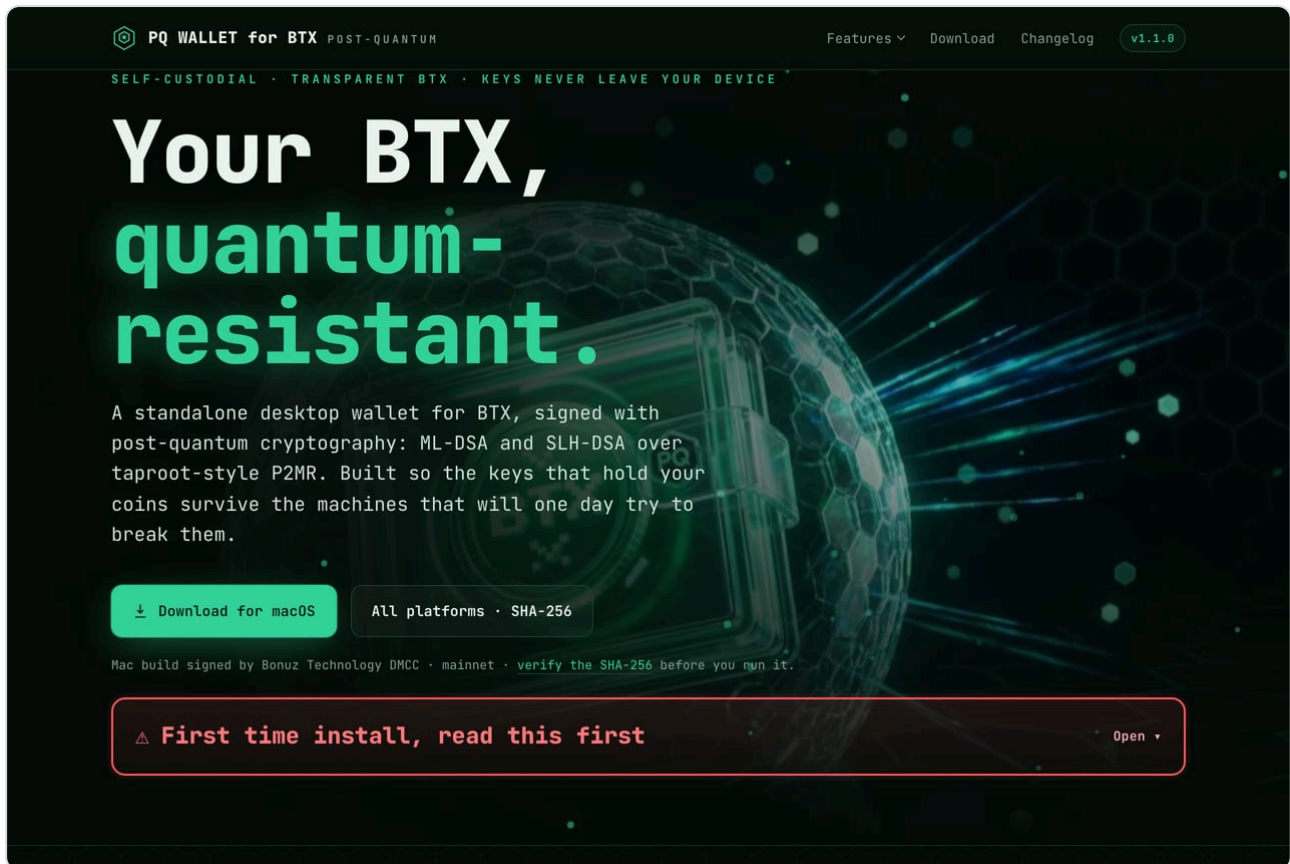
Prüfen. Eine vollständige Node zu betreiben ist der einzige Weg, Fragen zur Chain zu beantworten, ohne dem Server eines anderen vertrauen zu müssen. easyNode macht daraus auf allen drei Plattformen einen Klick. Node Guardian diagnostiziert eine Node, die stehen geblieben ist, und Keeper macht aus einer ungenutzten Maschine eine, die signierte Blockbestätigungen ausliefert, und das ist die knappste Ressource im Netzwerk.

Halten. BTX-Adressen beruhen auf Post-Quanten-Kryptografie, und die Schlüssel bleiben auf deiner Maschine. Der Miner bringt eine Wallet mit. Zwei eigene Wallets bieten mehr, eine für den Desktop und eine fürs Handy.

11 Wallets und Anmelden ohne Konto

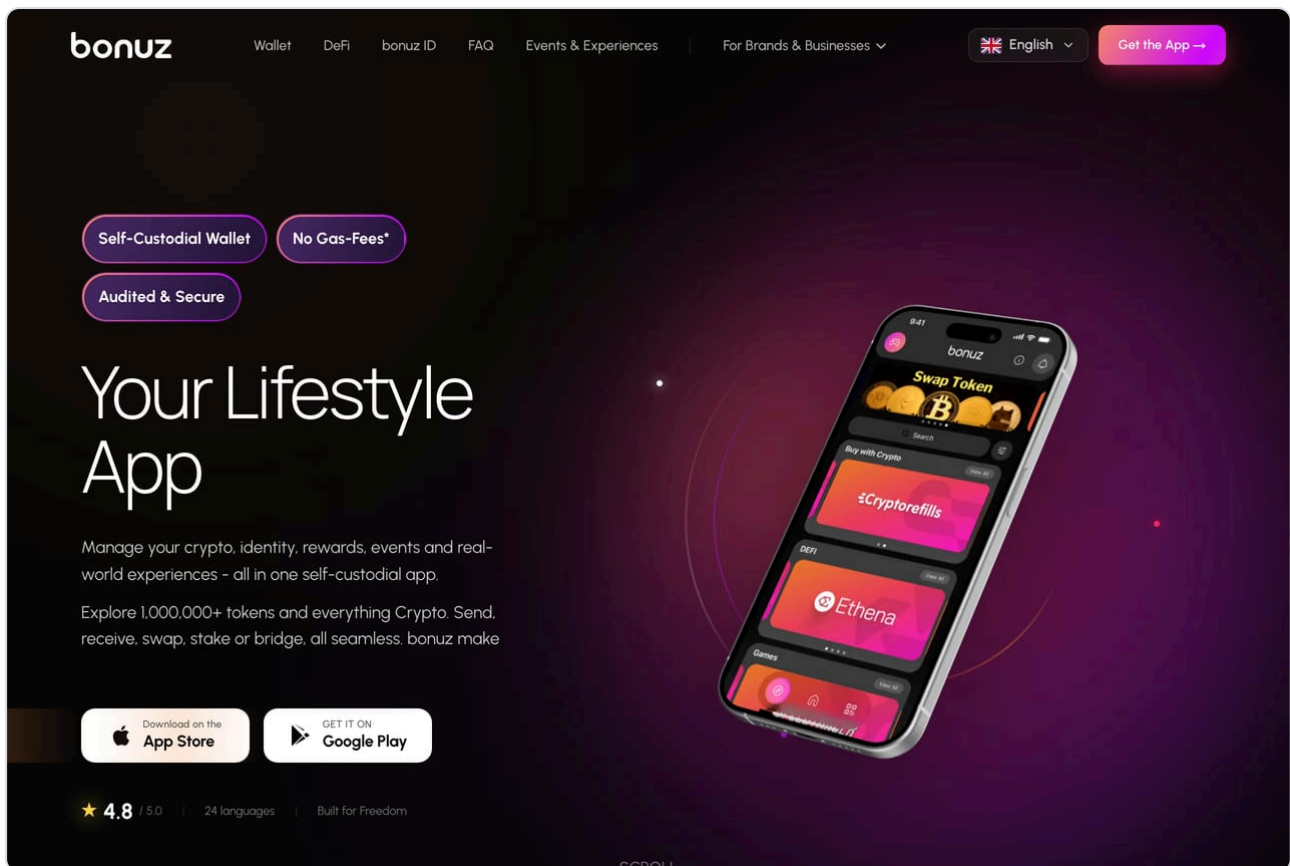
Eine BTX-Wallet ist ein Schlüssel, den du kontrollierst. Eine Wallet zu wählen heißt also zu entscheiden, wo dieser Schlüssel liegt.

PQ Wallet ist die Wallet für den Desktop, für macOS, Windows und Linux. Sie signiert mit Post-Quanten-Verfahren, und der Schlüssel bleibt auf deiner Maschine.



PQ Wallet, die Post-Quanten-Wallet für BTX auf dem Desktop.

bonuz ist die mobile Wallet, für iPhone und Android, und trägt neben den Coins auch deine Identität auf der Chain.



bonuz, die mobile Wallet für BTX.

Beide setzen auf Selbstverwahrung, und keine von beiden verlangt eine Registrierung. Der Miner bringt ebenfalls eine Wallet mit, die reicht, um zu empfangen, was du schürfst, und du kannst die Auszahlungen stattdessen auch auf eine der beiden oben genannten Wallets leiten.

qID ist das Bindeglied zwischen einer Wallet und einer Webseite. BTX-Seiten melden dich damit an: Statt E-Mail und Passwort weist du nach, dass du deinen Schlüssel kontrollierst. Es lohnt sich, genau zu sein bei dem, was die Seite dabei erfährt. Sie erfährt nicht deinen Namen, nicht deine E-Mail-Adresse und nicht deinen Schlüssel. Sie erfährt sehr wohl deine BTX-Adresse, und eine BTX-Adresse ist ein öffentlicher Eintrag im Hauptbuch der Chain. Eine Seite, bei der du dich anmeldest, kann also nachschlagen, was diese Adresse hält und was sie getan hat. Das ist ein echter Kompromiss und nicht dasselbe wie Anonymität. Eines macht qID richtig, und das gehört klar gesagt: Ein Anmeldebeweis kann niemals deine Coins bewegen. Logins und Transaktionen werden über verschiedene, getrennt gekennzeichnete Digests signiert, eine Signatur für das eine lässt sich also nicht als das andere wiedereinspielen. Aus einem einzigen Seed von 32 Byte wird eine ganze Post-Quanten-Identität, mit Schlüsseln, Adressen, Zahlungen, Login und Wiederherstellung, und derselbe Seed kann auf der Chain Werte halten. Wenn du auf einer anderen Chain schon einmal Wallet Connect benutzt hast: qID ist dieselbe Idee, neu gebaut, damit sie einen Quantencomputer übersteht.

qID •

OverviewSecurityDevelopersTrySign in with qID

POST-QUANTUM IDENTITY • NIST FIPS 203 / 204 / 205

Identity that outlives the quantum computer.

One 32-byte seed becomes a complete post-quantum identity:
keys, addresses, spends, login, recovery, encryption. Pure
JavaScript, zero dependencies, byte-exact to the BTX chain.

Sign in with qID

See the live demo →

Play the game

Read the paper

source opens with the independent audit

```
identity.js

import { createIdentity, randomSeed } from 'qid';

const id = createIdentity(randomSeed());

id.btxAddress // btxlz... receives value on-chain
id.identityRoot // stable root, survives key rotation
id.login // ML-DSA-44 signs spends & logins
id.recovery // SLH-DSA-128s cold, hash-based
id.attestation // root-signed, canonical bytes (v3)
```

qid.dev, die Post-Quanten-Identität, mit der BTX-Seiten dich anmelden.

12 Wo du mehr erfährst

Zwei Adressen sind mehr wert als alle übrigen.

btx.best ist das Portal. Es sammelt jedes BTX-Produkt, jedes Werkzeug, jeden Explorer, jede Wallet, jeden Pool und jede dApp auf einer Seite, geordnet danach, was du gerade vorhast. Wenn du dir aus diesem Handbuch nur eine einzige Adresse merkst und nicht sicher bist, welche, dann nimm diese.

BLOCK REWARD

20 BTX

SUPPLY

3.97M / 21M

MINTED

18.9%

HASHRATE

4.8 kH/s

EST

DIFFICULTY

0

AVG BLOCK

1m

TARGET

985

MEMPOOL

BTX.best

Stats

Wallets

Miners

Nodes

dApps

Pools

Exchanges

Links

News

Explorer

POST QUANTUM BITCOIN

BTX.best

The PORTAL to BTX

Explore the chain, get a wallet, mine, and reach every BTX product from one place.

Open Explorer

Get the Wallet

BLOCK HEIGHT

198,626

HASHRATE

4.8 kH/s

est.

NEXT HALVING

339d 23h

326,374 blocks

BTX PRICE

\$0.009935

modeled

Everything BTX

btx.best, das Portal, das jedes BTX-Produkt und jeden Link an einem Ort sammelt.

postquantum.wiki ist das Nachschlagewerk für die Kryptografie dahinter. Es ist eine belegte, verständlich geschriebene Enzyklopädie des Quantencomputings und der Verfahren, die gebaut wurden, um es zu überstehen, samt der NIST-Standards, auf denen die Signaturen von BTX beruhen. Nützlich, ob du nun die Fassung in einem Absatz suchst oder die Standards selbst.

postquantum.wiki Search Quantum computing Quantum physics Foundations Standards Blockchain Glossary Resources ⌵

The post-quantum cryptography reference

A cited, plain-language encyclopedia of the quantum world and the cryptography built to survive it: quantum computers and the physics behind them, the quantum threat, the NIST standards, migration in practice, and what it all means for blockchains.

Search: D-Wave, entanglement, ML-KEM, Q-Day...

155 entries · 8 categories · every claim cited to primary sources

Start here

The entries most readers come for.

Post-quantum cryptography
 Post-quantum cryptography is the field of cryptographic algorithms designed to resist attacks by bot...
FOUNDATIONS

Quantum mechanics
 Quantum mechanics is the physical theory of matter and energy at atomic and subatomic scales, bui...
QUANTUM PHYSICS

Quantum computer
 A quantum computer processes information with qubits and quantum effects; current machin...
FOUNDATIONS

D-Wave
 D-Wave Systems sold the first commercial quantum computer in 2011 and builds quantum anneale...
QUANTUM COMPUTING

Is Bitcoin quantum safe?

ML-KEM (FIPS 203)

Harvest now, decrypt later

Q-Day

postquantum.wiki, eine belegte, verständlich geschriebene Enzyklopädie der Post-Quanten-Kryptografie.

Für BTX selbst ist der Block-Explorer der Ort, an dem du alles nachprüfst, was dir erzählt wurde.

BLOCK REWARD 20 BTX SUPPLY 3.97M / 21M MINTED 18.9% HASHRATE 4.8 kH/s EST DIFFICULTY 0 AVG BLOCK 1m TARGET 90S MEMPOOL

BTX scan Blocks Transactions Mempool Charts Search height / tx / address 🔍 ↺

BTX · THE POST QUANTUM AI BLOCKCHAIN

The BTX blockchain explorer

Search blocks, transactions and addresses on BTX, a post quantum Bitcoin with MatMul proof of work. Rendered natively for bttx1z P2MR outputs, with a live view of the chain.

Search by block height, block hash, transaction ID, or address 🔍 Search

1 BTX ≈ \$0.009935 modeled* ≈ 0.000000129 BTC · Mkt cap \$39.5K [btxprice.com](#)

* Modeled estimate from btxprice.com. BTX has no public order book yet, so this is not a market price.

LATEST BLOCK
#198,626
 2 mins ago · 1 in mempool

BLOCK REWARD
20 BTX
 Halving in 326,374 blocks (~339d 23h)

CIRCULATING SUPPLY
3,972,540
 18.92% of 21,000,000 BTX cap

DIFFICULTY
0.0001
 ~4.8 kH/s est · 90s blocks

Latest Blocks ● LIVE avg 1m 54s · target 90s

198,626	2 tx · 15.38 KB	unknown miner	BTX
2 mins ago			
198,625	1 tx · 383 B	unknown miner	BTX
3 mins ago			

Latest Transactions 1 pending

TX	85a67e322a...c53172	20.0007685 BTX
	2 mins ago	Coinbase
TX	6982e0f705...3fb500	56.81941474 BTX
	2 mins ago	BTX

bttxscan.io, der Block-Explorer von BTX.

13 Der ehrliche Teil

Ein Handbuch, das nur gute Nachrichten aufzählt, ist Werbung. Das hier solltest du wissen, bevor du Strom oder Aufmerksamkeit investierst.

- **BTX hat keinen etablierten öffentlichen Markt.** Hinter jedem Preis, der dir begegnet, stehen zwei Menschen, die sich privat einig geworden sind. Behandle alles, was du schürfst, als unsicher, nie als Einkommen.
- **Mining kostet echten Strom** und fordert deine GPU stark, das bedeutet Hitze und hohen Verbrauch.
- **Die Apps sind noch nicht code-signiert.** Deshalb schlagen manche Antivirus-Programme bei ihnen an, und deshalb veröffentlicht jeder Build auch einen SHA-256, den du selbst prüfen kannst, bevor du ihn ausführst.
- **Shares sind seit dem Fork selten.** Eine stille Stunde ist meistens Zufall, kein Fehler.
- **Mach ein Backup deiner Wallet.** Kein Teil dieses Projekts kann Schlüssel für dich wiederherstellen, und genau das ist der Sinn von Selbstverwahrung und zugleich ihr Preis.

Wo alles zu finden ist

Es lohnt sich, jede Adresse hier unten aufzuheben. Nichts auf dieser Liste verlangt ein Konto, und die als Daten gekennzeichneten Einträge liefern JSON ohne Schlüssel. Nicht alle davon sind unabhängig von uns: btx.best und btxscan.io werden von easyBTX gebaut, und PQ Wallet, die bonuz-Wallet und qID teilen sich Leute mit easyBTX. Die Chain, die Pools und postquantum.wiki gehören nicht uns. Sollte ein Link diesem Text je widersprechen, glaube dem Link.

HIER ANFANGEN

easybtx.com/btx	Dieses Handbuch als Webseite, laufend aktuell gehalten.
btx.dev	Die Projektseite von BTX.
btx.best	Das Portal zu BTX. Jedes Produkt, jedes Werkzeug und jeder Link im Ökosystem, an einem Ort.
btxscan.io	Der Block-Explorer. Schlag jeden Block, jede Adresse und jede Transaktion nach.

SOFTWARE

easybtx.com/install	easyBTX, der Ein-Klick-Miner für Mac, Windows und Linux.
easybtx.com/node	easyNode, eine vollständige BTX-Node als Desktop-App.
easybtx.com/guardian	Node Guardian, ein kostenloses Skript, das eine stehen gebliebene Node diagnostiziert.
easybtx.com/keeper	Keeper, eine kleine Node im Pruning-Modus, die signierte Blockbestätigungen ausliefert.

BTX HALTEN

easybtx.com/wallet	Welche Wallet du nehmen solltest, und warum es zwei gibt.
pq-wallet.com	PQ Wallet, mit Post-Quanten-Kryptografie, für macOS, Windows und Linux.
bonuz.xyz	bonuz, die mobile Wallet.
qid.dev	qID, die Post-Quanten-Identität, mit der BTX-Seiten dich anmelden.

LESESTOFF UND BELEGE

easybtx.com/research/	Das Forschungsarchiv. Mit Quellen, mit Datum, und nie stillschweigend umgeschrieben.
easybtx.com/stats	Aktuelle Zahlen zu Chain, Nodes und Pools.
easybtx.com/nodes	Eine Live-Karte aller erreichbaren öffentlichen Nodes.
postquantum.wiki	Eine belegte, verständlich geschriebene Enzyklopädie der Post-Quanten-Kryptografie.

FÜR MASCHINEN

easybtx.com/ai	Für autonome Agenten geschrieben: offene Endpunkte und ehrliche Grenzen.
easybtx.com/api/network	Chain-Höhe, Ausgabe, Node-Zählung und Pools, als JSON, ohne Schlüssel.
easybtx.com/llms.txt	Eine Zusammenfassung dieser Seite für Sprachmodelle.

MENSCHEN

t.me/easyBTX	Das Telegram von easyBTX, wo Fragen beantwortet werden.
x.com/easyBTX	Release-Notes und kurze Updates.
github.com/MendeMatthias/EasyBTX-releases/releases	Jeder veröffentlichte Build, mit Prüfsummen.

BITTE LESEN

Nur zu Bildungs- und Unterhaltungszwecken. Nichts in diesem Handbuch ist eine Finanzberatung, ein Angebot oder eine Empfehlung, irgendetwas zu kaufen, zu verkaufen oder zu schürfen. Herausgegeben von easyBTX, das Software für BTX baut und nicht das Kernteam von BTX ist. Dies ist kein offizielles Dokument. BTX hat keinen etablierten öffentlichen Markt, Mining bringt dir möglicherweise gar nichts ein, und für deine Entscheidungen bist du selbst verantwortlich.