easyBTX

Le manuel BTX

Ce qu'est BTX, comment fonctionne son minage, comment la chaîne en est arrivée là, et où vérifier vous-même chaque affirmation.

> Uniquement à des fins pédagogiques et de divertissement. Ce n'est pas un conseil financier. easyBTX n'est pas l'équipe centrale de BTX, et BTX n'a pas de marché public établi.

PREMIÈRE ÉDITION · CHIFFRES ARRÊTÉS AU 23 AOÛT 2026 · EASYBTX.COM/BTX

Sommaire

1 Qui a écrit ce manuel, et qui ne l'a pas écrit

easyBTX développe des logiciels pour BTX : un mineur, une application de nœud et quelques outils gratuits. **easyBTX n'est pas l'équipe centrale de BTX.** Le logiciel de consensus de la chaîne est écrit et publié par le projet BTX, auquel easyBTX ne participe pas et sur lequel il n'a aucune autorité. Nous lisons son code source et ses versions publiées comme n'importe qui peut le faire.

Cela compte pour la façon dont vous devez lire ce manuel. Rien ici n'est une annonce, une feuille de route ou une promesse faite au nom de la chaîne, car ce n'est pas à nous de les faire. C'est la lecture de sources publiques par un participant indépendant, écrite pour que vous puissiez la vérifier. Là où les faits sont incertains, nous le disons, et là où nous nous sommes trompés par le passé, nous le disons aussi.

Deux mises au point s'imposent, parce que l'autre solution serait de vous laisser supposer quelque chose de plus flatteur que la vérité. D'abord, easyBTX a intérêt à ce que BTX se porte bien, et prélève des frais sur le minage. Ensuite, les projets cités en fin de manuel ne sont pas tous indépendants de nous. BTX lui-même est réellement distinct, et c'est la séparation qui compte le plus. Mais btx.best et btxscan.io sont développés par easyBTX et le disent dans leurs propres pieds de page, et PQ Wallet, le portefeuille bonuz et qID ont des personnes en commun avec easyBTX. Là où ce manuel parle de ces produits, lisez-le comme le propos d'un participant qui décrit une chose qu'il a contribué à construire. La chaîne, les pools et postquantum.wiki ne sont pas à nous. Citer un projet ici ne constitue pas une garantie à son sujet, et aucun de ces projets ne répond pour les autres.

2 Ce qu'est BTX

BTX est un fork de Bitcoin conçu pour survivre aux ordinateurs quantiques.

Bitcoin signe chaque transaction avec ECDSA, un schéma classique à courbe elliptique. Un ordinateur quantique suffisamment puissant saurait le casser et dépenser des coins qui ne lui appartiennent pas. BTX remplace ce schéma de signature par des signatures post-quantiques, et c'est pour cette raison qu'une adresse BTX ne ressemble pas à une adresse Bitcoin : les adresses BTX commencent par `btx1z`.

Tout le reste reprend délibérément la forme de Bitcoin :

- Une offre fixe de 21 000 000 de coins, et aucun moyen d'en émettre davantage.
- Aucun premine. Les coins n'apparaissent que sous forme de récompense de minage, bloc après bloc.
- Un minage en preuve de travail, sans autorisation à demander ni gardien à convaincre.

- L'auto-custodie. Il n'y a ni comptes ni dépositaire. Vous détenez les clés, et les clés détiennent les coins.

La chaîne est jeune. Le bloc 0 est daté du 19 mars 2026, et le premier bloc a réellement été miné le 23 mars 2026.

3 Le travail, c'est de la multiplication de matrices

Les mineurs de Bitcoin cherchent des hachages. Les mineurs de BTX multiplient des matrices, le même calcul dense que les accélérateurs d'IA modernes sont conçus pour exécuter. C'est ce que veut dire « matmul » partout où vous le croisez dans la documentation BTX : la multiplication de matrices, employée comme le travail qui sécurise la chaîne.

Concrètement, le GPU est la machine naturelle pour BTX, et le travail est un vrai calcul numérique plutôt qu'une loterie de hachage.

Il vaut la peine d'être précis sur ce que cela veut dire et sur ce que cela ne veut pas dire, car c'est l'affirmation la plus souvent exagérée. Les entrées de chaque calcul sont dérivées de la chaîne elle-même, et seule une empreinte du résultat est conservée. Le produit calculé n'est donc livré à personne en dehors de la chaîne. **BTX ne vend pas de calcul pour l'IA aujourd'hui.** Un marché de calcul vérifiable, où un tiers extérieur soumettrait une vraie tâche et paierait pour le résultat, est cité comme une direction ultérieure dans la spécification de BTX elle-même, et il n'existe pas.

Ce qui est vrai aujourd'hui est plus discret et plus durable : miner BTX rémunère une foule dispersée de gens ordinaires pour qu'ils possèdent du matériel capable de faire tourner de l'IA et le gardent allumé et connecté, entre de nombreuses mains indépendantes plutôt que dans quelques centres de données.

Le mineur easyBTX sur easybtx.com, affichant la hauteur de chaîne en direct, l'émission rapportée au plafond de 21 000 000 et le nombre de nœuds publics joignables.

4 Deux fonctions de travail, et pourquoi la seconde existe

BTX n'a connu que deux algorithmes de minage dans toute son existence. Il vaut la peine de le dire clairement, car les numéros de version qui figurent dans les documents de conception de BTX se prêtent aux malentendus : ils décrivent une feuille de route de recherche, et non une succession de chaînes en production.

MatMul v3 a tourné dès le tout premier bloc. Une tentative consistait en une seule multiplication de matrices 512 par 512 sur un corps premier choisi pour que l'arithmétique se transpose proprement aussi bien sur CUDA que sur le Metal d'Apple. Une tentative prenait quelques microsecondes : une carte en effectuait donc des millions par seconde, et les vitesses de minage s'exprimaient dans cette unité.

Trois arguments plaidaient en sa faveur. Le travail relève de l'algèbre linéaire dense standard : la machine naturelle est donc un GPU, et non une puce incapable de faire quoi que ce soit d'autre. La construction sur laquelle il repose n'ajoute presque aucun surcoût par rapport à une multiplication de matrices ordinaire, de sorte qu'une part infime de l'électricité se perd dans la machinerie de la preuve

elle-même. Et il laissait une porte ouverte vers un travail qui pourrait un jour servir en dehors de la chaîne.

v3 a été durcie à plusieurs reprises sans que le travail lui-même change. Au bloc 125 000, les matrices ont été liées à la partie mutable de l'en-tête de bloc, si bien qu'un mineur ne pouvait plus réutiliser une même paire préparée pour de nombreuses tentatives. Au bloc 130 500, elles ont en plus été liées au bloc parent : un modèle de bloc ne pouvait donc plus être préparé à partir d'un parent puis rejoué sur un autre, gardé en réserve. Ni l'une ni l'autre de ces modifications n'a changé ce que le minage calculait. Elles ont fermé des raccourcis.

MatMul v4.7 a remplacé la fonction de travail au bloc 185 000, le 10 août 2026. Une tentative a cessé d'être une petite multiplication pour devenir un épisode unique et indivisible : quatre tours successifs à travers seize couches, des matrices de 4 096 de côté, environ 141 000 milliards d'opérations entières de multiplication-accumulation, à peu près 4,8 Go de mémoire GPU, et de l'ordre de trente secondes de travail continu. On ne peut ni mettre un épisode en pause, ni le reprendre, ni en faire soixante pour cent et en toucher soixante pour cent du crédit.

Le raisonnement mérite d'être compris, car il va à l'inverse de ce que l'on suppose d'ordinaire. Une loterie dont les billets sont extrêmement bon marché invite quelqu'un à construire une machine qui ne fait rien d'autre qu'acheter des billets très vite. Rendre chaque billet coûteux, séquentiel et gourmand en mémoire supprime l'essentiel de cette marge : le travail est déjà l'opération pour laquelle les cœurs tensoriels existent, il reste donc peu de chose qu'une puce spécialisée puisse faire plus habilement, et aucune étape ne peut être sautée puisque vérifier un bloc rejoue l'épisode à l'identique. Les documents de conception citent directement un second motif : mettre les GPU grand public loués hors de portée d'une attaque sur une chaîne jeune.

Le coût a été réel, et le projet ne l'a jamais nié. Les Mac n'ont pas pu miner du tout pendant neuf jours, parce que le solveur du nouveau travail n'existait pas pour Metal le jour de l'activation. Les nœuds qui faisaient tourner un logiciel plus ancien se sont arrêtés au bloc 184 999 et y sont restés. La difficulté a dû être recalibrée d'un facteur d'environ 120 000 en une seule fois. Les shares acceptées sont devenues assez rares pour qu'une machine en bonne santé puisse désormais rester silencieuse pendant une heure. Des cartes qui minaient BTX de façon rentable en juillet ne le minent plus du tout aujourd'hui.

5 Comment un bloc est vérifié, et comment cela aussi a changé

L'histoire de la vérification est la partie qui mérite le plus d'être comprise, et elle a évolué dans le sens inverse de celui que l'on pourrait attendre.

Sous v3, la vérification était astucieuse et peu coûteuse. Plutôt que de refaire une multiplication 512 par 512, le vérificateur multipliait la réponse annoncée par deux vecteurs aléatoires et comparait. C'est l'algorithme de Freivalds, et deux tours de ce test ne laissent à un résultat faux que moins d'une chance

sur 2 puissance 62 de passer au travers. Coûteux à produire, peu coûteux à vérifier : c'est exactement la propriété que l'on recherche.

Sous v4.7 telle qu'elle tourne aujourd'hui, le réseau vérifie en rejouant l'épisode entier à l'identique et en comparant les empreintes. Il n'existe aucune vérification bon marché. C'est un choix d'échelonnement délibéré et non un oubli : les preuves succinctes, qui rendraient de nouveau la vérification peu coûteuse, sont décrites comme des époques ultérieures et **aucune d'entre elles n'a de hauteur d'activation**. Le plan publié en cite quatre, dont seule la première est en service.

Le projet le dit sans détour, et cela vaut la peine d'être cité plutôt que paraphrasé :

> L'histoire de la vérification a changé de forme. Sous l'étape de v4.7 qui est en service aujourd'hui, le réseau vérifie en rejouant l'épisode à l'identique et en comparant les empreintes. Les preuves succinctes qui rendraient de nouveau la vérification peu coûteuse sont annoncées comme une étape ultérieure, sans hauteur d'activation. L'élégante propriété « coûteux à produire, peu coûteux à vérifier » est donc, pour l'instant, un objectif de conception plutôt que le comportement déployé.

Une conséquence compte pour quiconque fait tourner un nœud. Rejouer un épisode exige un GPU qualifié : la plupart des machines ne peuvent donc pas vérifier elles-mêmes le travail le plus récent. Elles suivent à la place un petit enregistrement signé, de 208 octets par bloc. C'est pour cela que le réseau tient tant aux nœuds qui acceptent de servir ces enregistrements, et pour cela qu'une interruption de la signature a figé des parties du réseau à deux reprises en août 2026 alors que la chaîne elle-même se portait bien.

6 Ce qui est vraiment inhabituel ici

Marketing mis à part, plusieurs aspects de cette conception sont remarquables pour qui lit du code de consensus par métier.

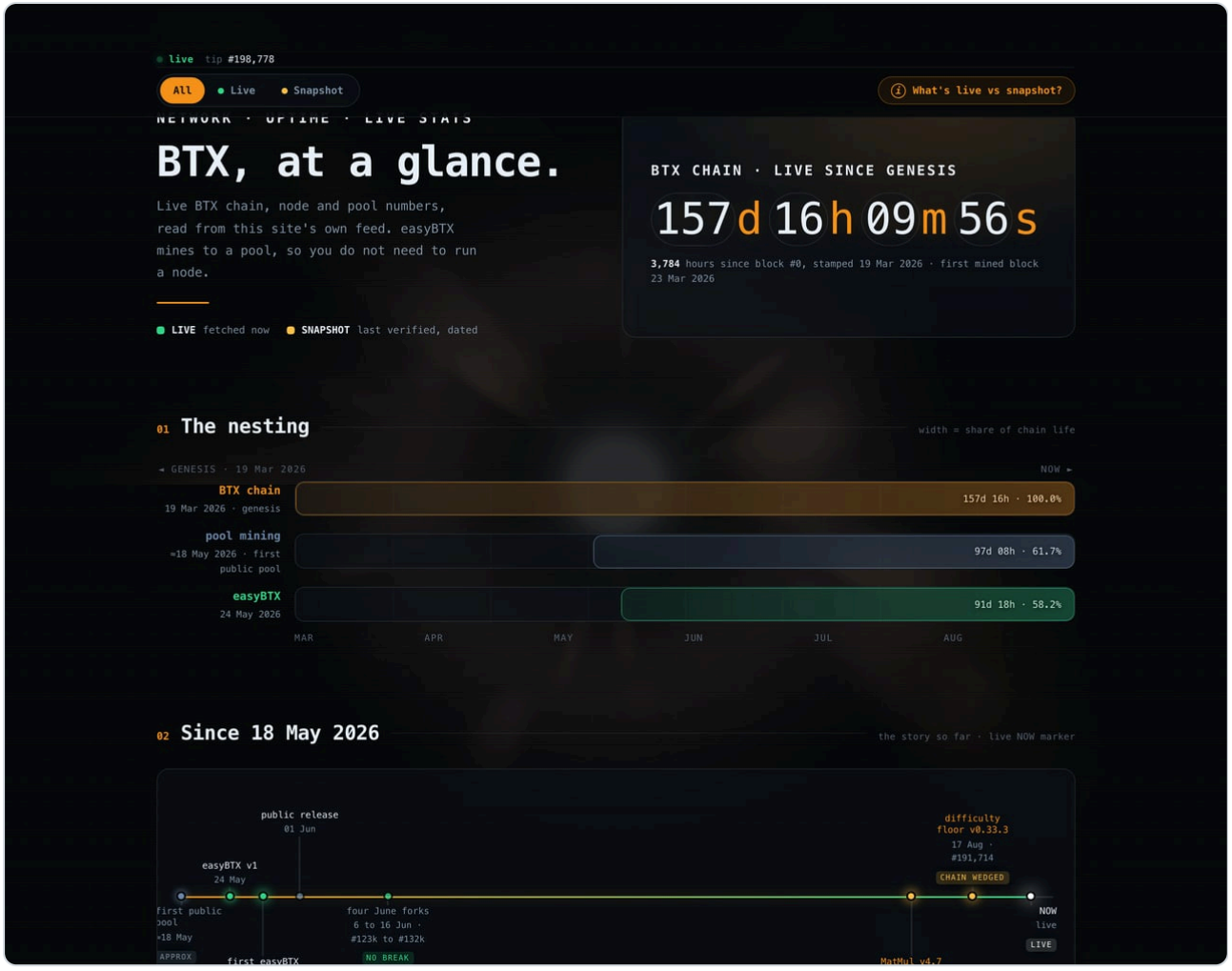
- **Le travail est de la véritable algèbre linéaire entière dense**, déterministe et exacte à l'octet près sur deux implémentations GPU indépendantes. Le matériel de deux fabricants différents doit produire une empreinte identique.
- **Le changement de coût par tentative est un changement de catégorie**, de quelques microsecondes à environ trente secondes. Très peu de chaînes s'y risquent, et cela rend une tentative réellement indivisible.
- **L'éligibilité au minage est une mesure, pas une liste.** Le logiciel demande à un appareil de reproduire un résultat connu et se fie à la réponse, plutôt que de comparer le nom de la puce à une liste d'autorisation. easyBTX comme le fournisseur du moteur ont publié des prérequis matériels qui se sont révélés faux, et les deux ont été corrigés par la mesure.

- **L'en-tête n'a jamais changé.** Un remplacement total de la preuve de travail a été livré sans ajouter un seul octet à l'en-tête de bloc de 182 octets, et c'est pour cela que les pools, les mineurs et les protocoles réseau y ont survécu intacts. C'est peu spectaculaire et réellement difficile.

Rien de tout cela ne signifie que le travail soit déjà utile à quelqu'un en dehors de la chaîne. Il ne l'est pas, et la section 2 le dit. Mais la machinerie est réelle, les chiffres ci-dessus figurent dans le code de consensus et non dans une brochure, et le projet documente les choix de paramètres qu'il a lui-même écartés et désactive dans le code ses propres composants inachevés. C'est un meilleur signe que n'importe quelle affirmation.

7 Petite histoire de la chaîne

QUAND	HAUTEUR	CE QUI S'EST PASSÉ
19 mars 2026	`0`	Le bloc de genèse est daté, avec MatMul v3 comme fonction de travail dès le départ. Le premier bloc a été miné le 23 mars.
début juin 2026	`~123 000`	Le fork v0.31.0.
8 juin 2026	`125 000`	Les graines sont liées à l'en-tête, si bien qu'une paire de matrices préparée ne peut plus servir à de nombreuses tentatives.
mi-juin 2026	`~130 500`	Les graines sont liées au bloc parent, ce qui ferme un raccourci permettant de rejouer un modèle de bloc. La fonction de travail est inchangée.
mi-juin 2026	`~132 000`	Une mise à jour des nœuds.
10 août 2026	`185 000`	MatMul v4.7 s'active. Une tentative devient un épisode de trente secondes.
17 août 2026	`191 690`	Le réseau se bloque. BTX Core v0.33.3 sort le jour même avec un plancher de difficulté au bloc 191 714, et la chaîne se rétablit.
22 août 2026	`197 000+`	Environ 3,96 millions de BTX émis, à peu près 19 % du plafond.



La page de statistiques en direct sur easybtx.com/stats, qui lit la chaîne, le recensement des nœuds et tous les pools en activité.

8 Offre et émission

Chaque bloc verse 20 BTX. L'intervalle visé est de 90 secondes, même si la moyenne observée depuis le début de la chaîne est plus rapide que cela. La récompense est divisée par deux tous les 525 000 blocs, et le calendrier tombe juste : 525 000 blocs à 20, puis autant à 10, puis à 5, et ainsi de suite, cela fait exactement 21 000 000.

Aucun halving n'a encore eu lieu. Le premier est toujours devant nous.

Au moment de la rédaction, la chaîne avait dépassé le bloc 197 000, soit environ 3 960 000 BTX émis, un peu moins de 19 % du plafond. Pour les chiffres actuels plutôt que ceux-ci, consultez la page de statistiques en direct indiquée à la fin de ce manuel.

9 BTX peut-il être contrefait ?

Non, et les raisons sont structurelles, ce ne sont pas des promesses.

L'offre est fixée à 21 000 000, il n'y a pas eu de premine, et les coins ne sont créés que par le minage. BTX est une chaîne dérivée de Bitcoin, sans couche de tokens : il n'existe donc aucun mécanisme permettant d'émettre un coin contrefait sans enfreindre les règles que chaque nœud applique de façon indépendante. Chaque coin est traçable, bloc après bloc, jusqu'à une récompense de minage.

C'est une question différente de celle de savoir si la chaîne peut être attaquée. Une part suffisamment grande de la puissance de minage du réseau pourrait réordonner les blocs récents, ce qui vaut pour toute chaîne en preuve de travail, Bitcoin compris. L'archive de recherche contient une étude complète de ce qui est possible et de ce qui ne l'est pas, ainsi que la marche à suivre pour vérifier vous-même l'authenticité.

10 Trois façons de participer

Minez-le. easyBTX est une seule application pour Mac, Windows et Linux. Elle rejoint un pool de minage, verse les gains sur un portefeuille que vous contrôlez, et se met à jour toute seule. Un Mac doit avoir une puce Apple silicon et macOS 26.4 ou plus récent, et la question de savoir si un Mac donné peut miner est tranchée par un test d'une demi-seconde que l'application exécute sur le GPU, pas par le nom de la puce. Windows fait tourner la version Linux sous WSL2. Sous Linux, il faut un GPU NVIDIA. Tous les frais sont annoncés d'avance : easyBTX prélève 4,99 %, le pool prélève les siens, et sous Windows et Linux le moteur MATADOR en prélève 1 % de plus. Le minage en solo n'est disponible sur aucune plateforme aujourd'hui.

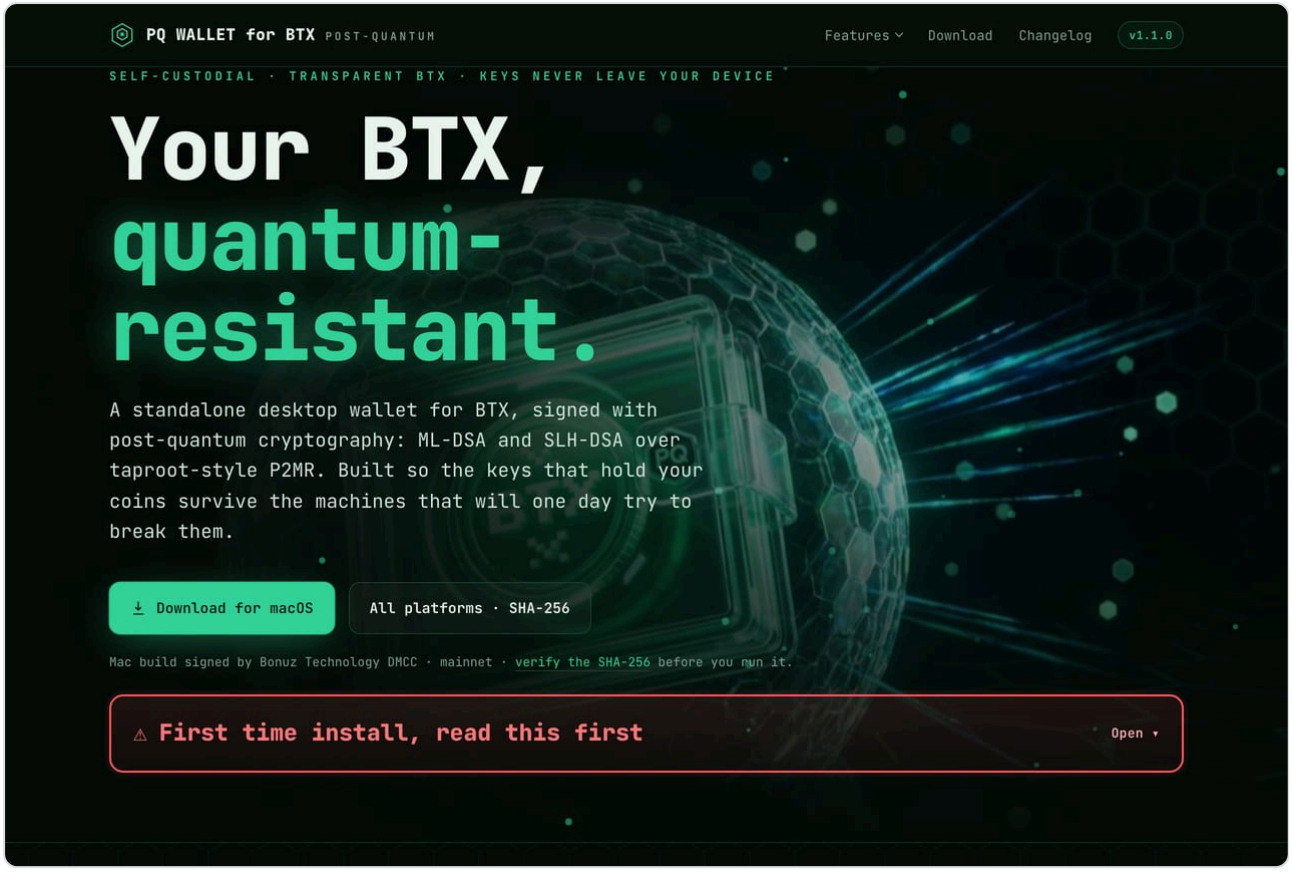
Vérifiez-le. Faire tourner un nœud complet est la seule façon de répondre à des questions sur la chaîne sans faire confiance au serveur de quelqu'un d'autre. easyNode réduit cela à un clic sur les trois plateformes. Node Guardian diagnostique un nœud qui n'avance plus, et Keeper transforme une machine inutilisée en nœud qui sert des confirmations de blocs signées, la ressource la plus rare du réseau.

Détenez-le. Les adresses BTX sont post-quantiques et les clés restent sur votre machine. Le mineur intègre un portefeuille ; deux portefeuilles dédiés vont plus loin, l'un sur ordinateur, l'autre sur mobile.

11 Les portefeuilles, et la connexion sans compte

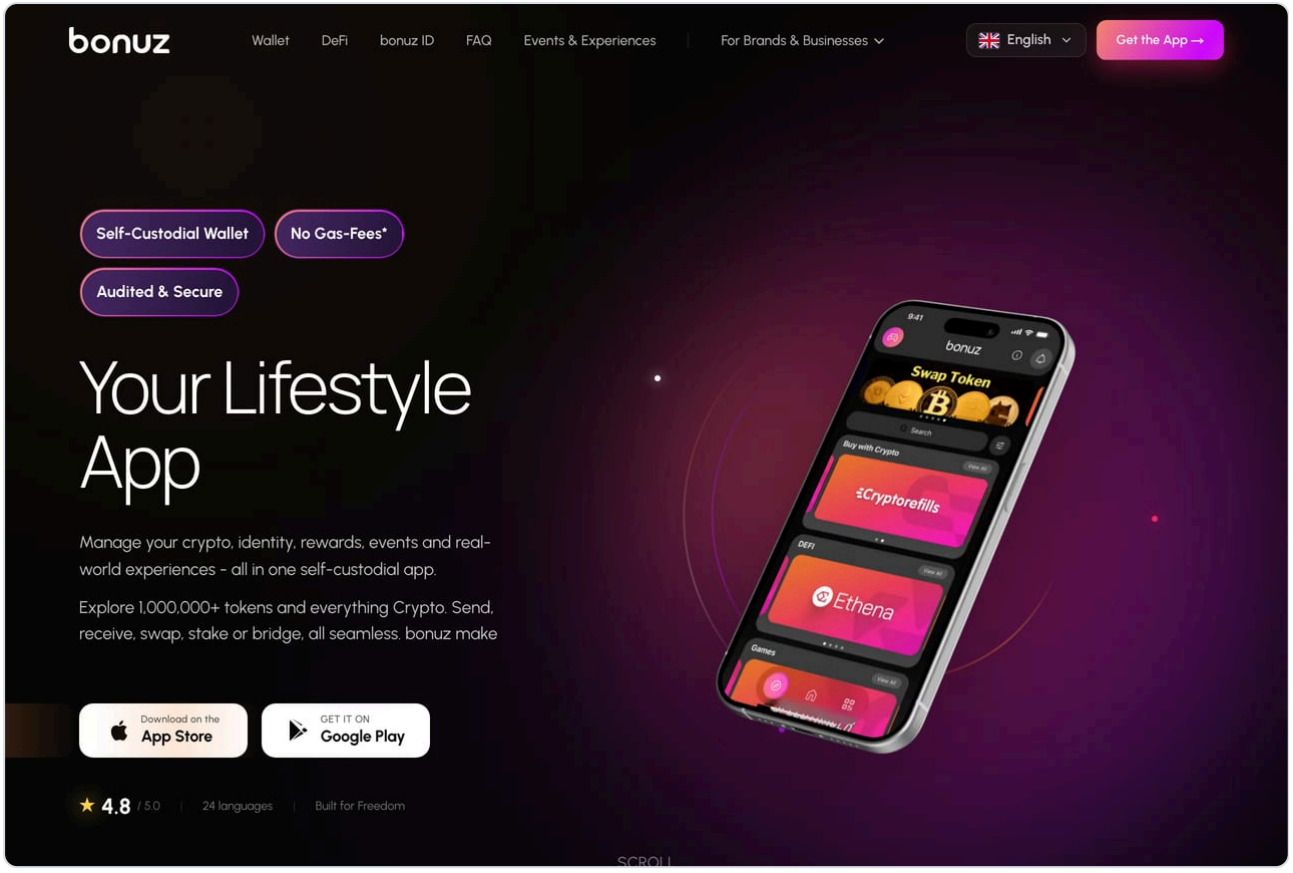
Un portefeuille BTX est une clé que vous contrôlez : choisir un portefeuille, c'est donc choisir où cette clé réside.

PQ Wallet est le portefeuille de bureau, pour macOS, Windows et Linux. Il signe avec des schémas post-quantiques et garde la clé sur la machine.



PQ Wallet, le portefeuille de bureau post-quantique pour BTX.

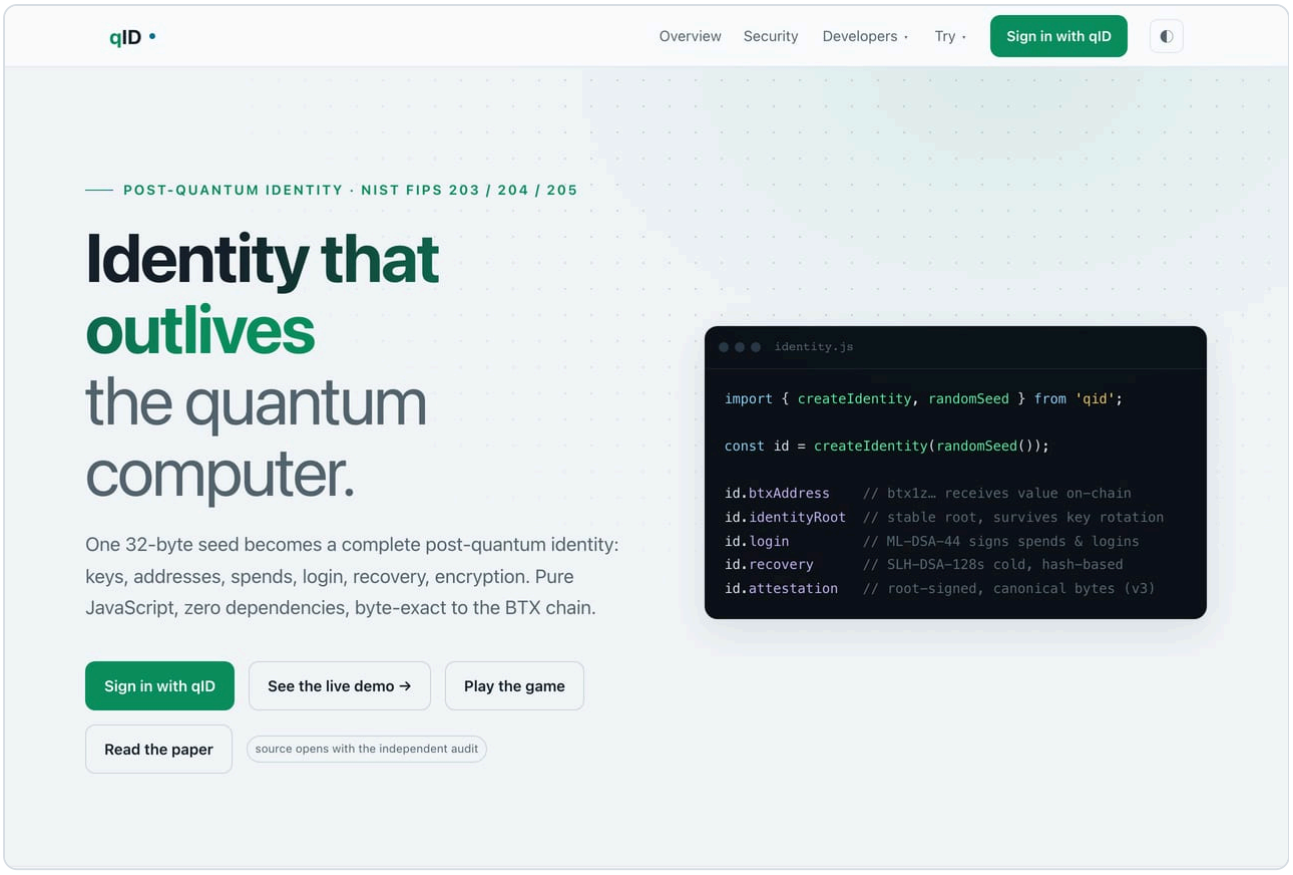
bonuz est le portefeuille mobile, pour iPhone et Android, et il porte votre identité sur la chaîne en plus des coins.



bonuz, le portefeuille mobile pour BTX.

Les deux sont en auto-custodie, et aucun ne vous demande de créer un compte. Le mineur intègre lui aussi un portefeuille, ce qui suffit pour recevoir ce que vous minez, et vous pouvez tout aussi bien diriger les versements vers l'un ou l'autre des portefeuilles ci-dessus.

qID est l'élément qui relie un portefeuille à un site web. Les sites BTX s'en servent pour vous connecter : au lieu d'une adresse e-mail et d'un mot de passe, vous prouvez que vous contrôlez votre clé. Il vaut la peine d'être exact sur ce que le site apprend. Il n'apprend ni votre nom, ni votre adresse e-mail, ni votre clé. Il apprend en revanche votre adresse BTX, et une adresse BTX est une entrée publique du registre : un site auquel vous vous connectez peut donc consulter ce que cette adresse détient et ce qu'elle a fait. C'est un vrai compromis, et ce n'est pas la même chose que l'anonymat. Une chose que qID fait bien mérite d'être dite clairement : une preuve de connexion ne peut jamais déplacer vos coins. Les connexions et les transactions sont signées sur des empreintes différentes, portant chacune une étiquette distincte, de sorte qu'une signature produite pour l'une ne peut pas être rejouée comme l'autre. Une graine de 32 octets devient une identité post-quantique complète, avec clés, adresses, dépenses, connexion et récupération, et cette même graine peut détenir de la valeur sur la chaîne. Si vous avez déjà utilisé wallet-connect sur une autre chaîne, qID est cette idée reconstruite pour survivre à un ordinateur quantique.

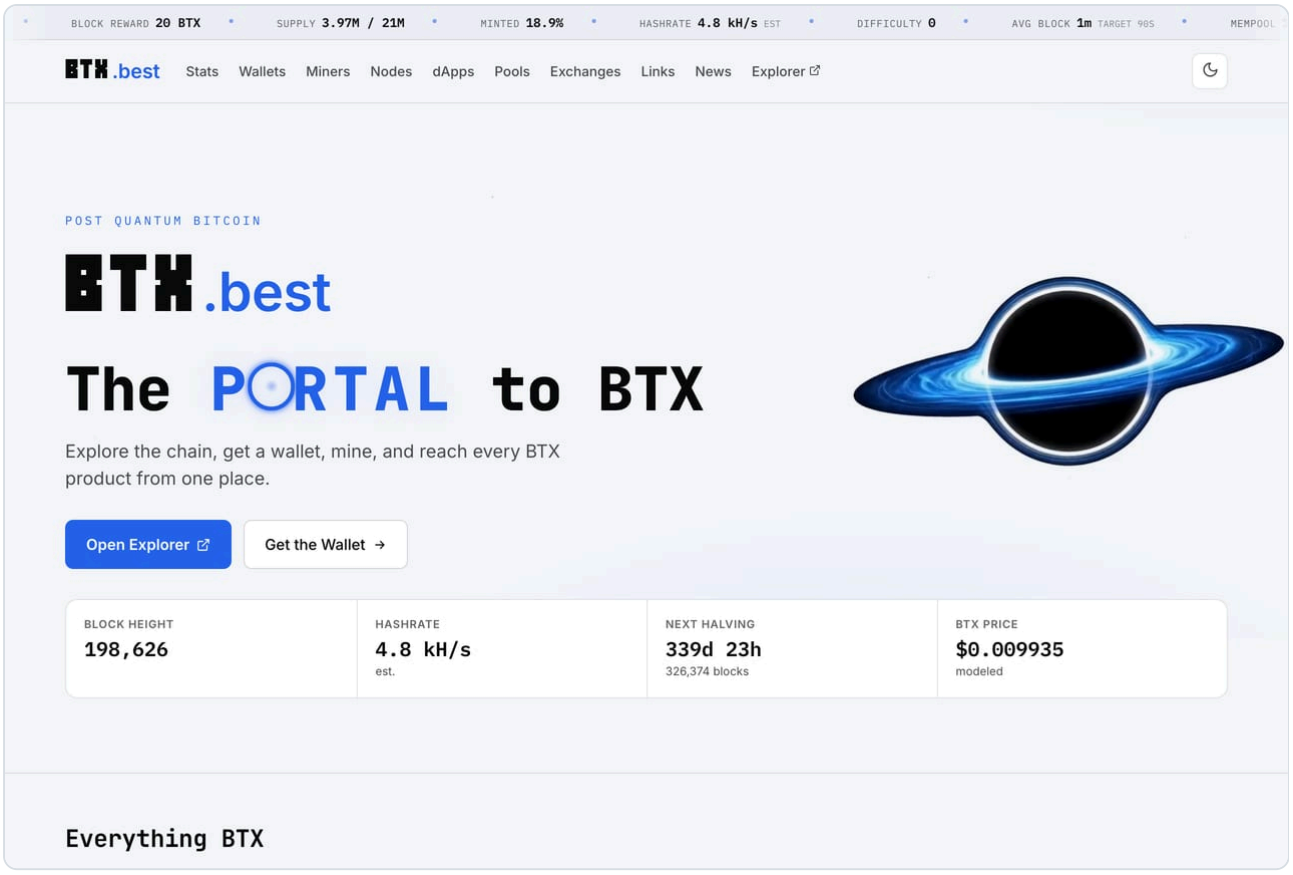


qid.dev, l'identité post-quantique que les sites BTX utilisent pour la connexion.

12 Où en apprendre davantage

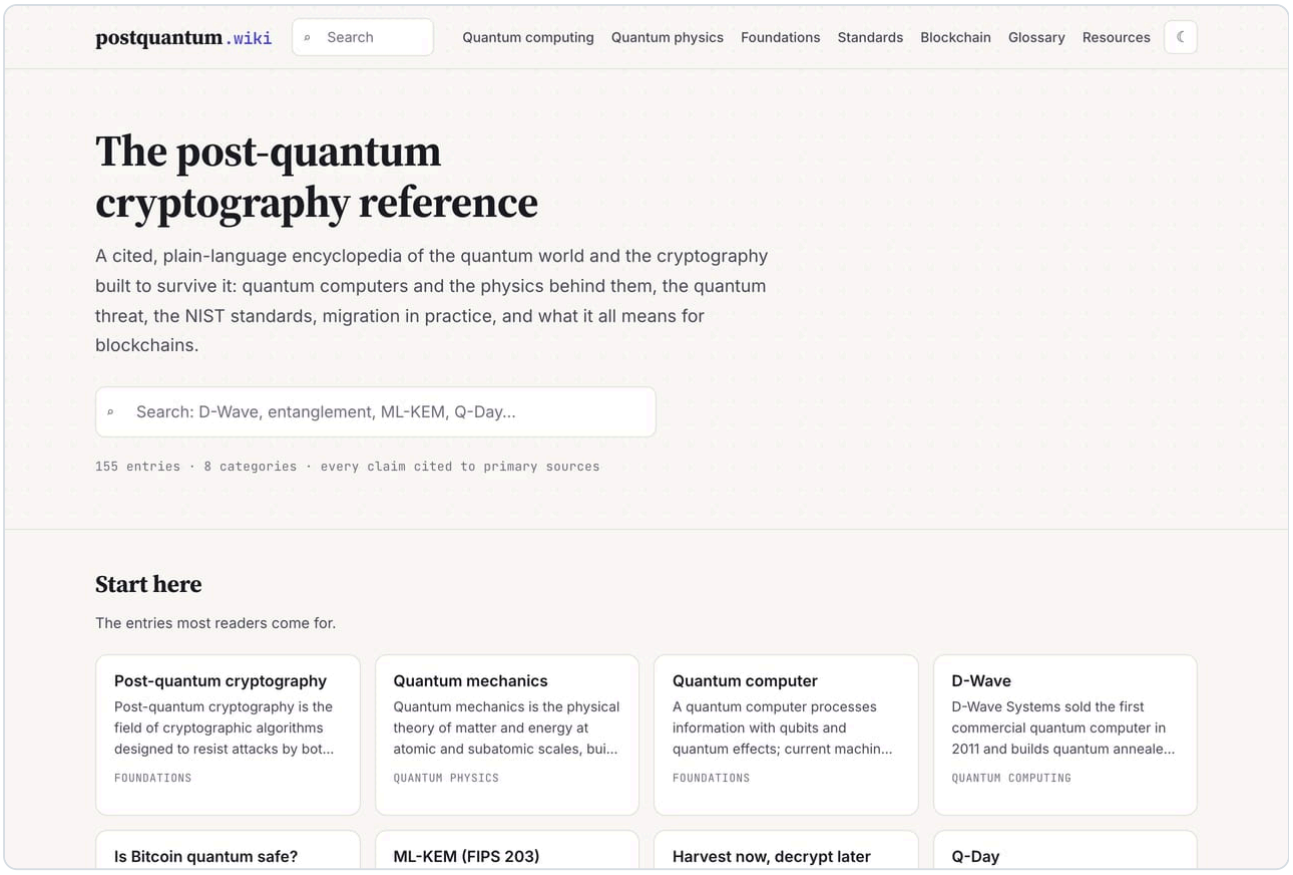
Deux adresses valent plus que toutes les autres.

btx.best est le portail. Il rassemble sur une seule page tous les produits, outils, explorateurs, portefeuilles, pools et dApps de BTX, classés selon ce que vous cherchez à faire. Si vous ne mettez en favori qu'une seule adresse de ce manuel, et que vous hésitez, retenez celle-là.



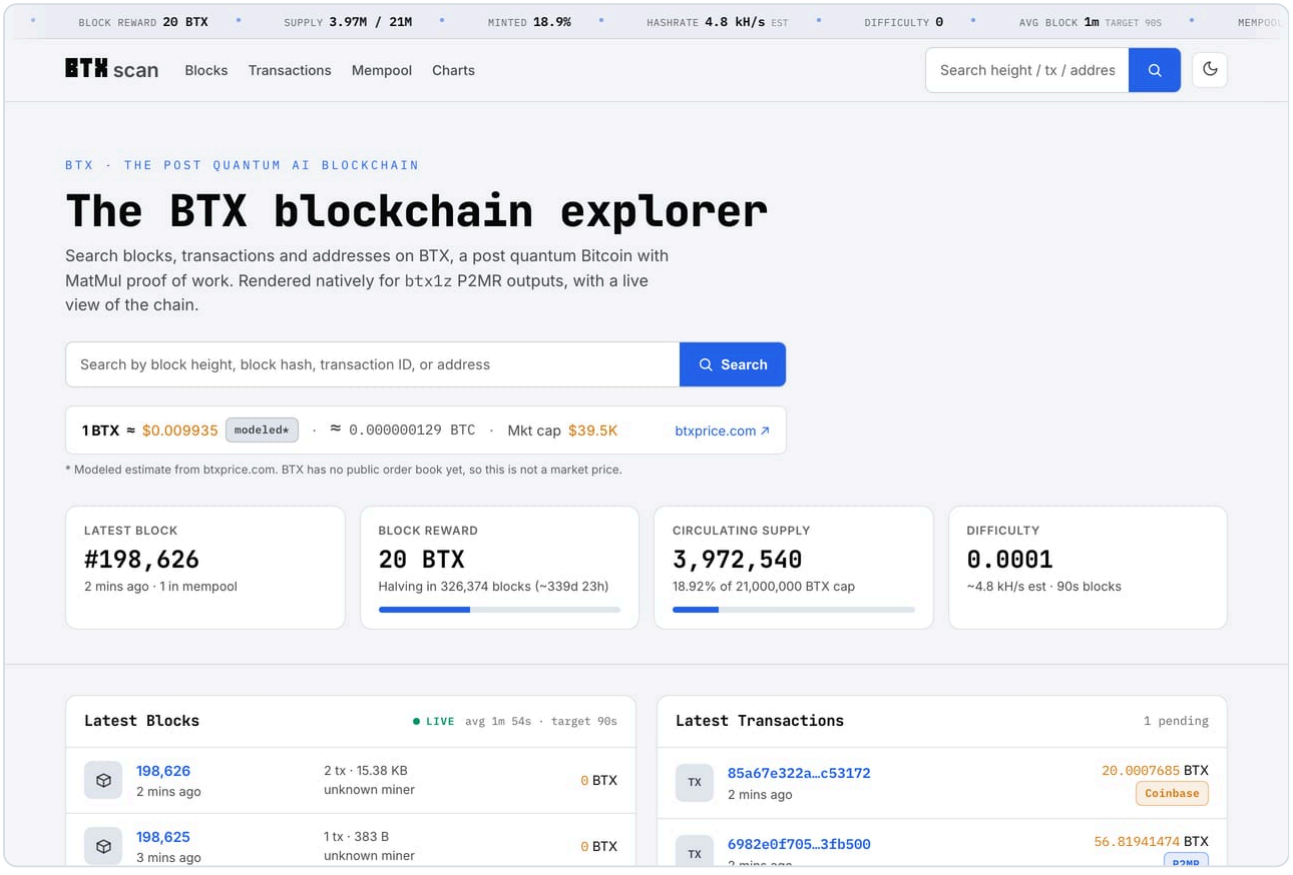
btx.best, le portail qui rassemble en un seul endroit tous les produits et liens BTX.

postquantum.wiki est la référence sur la cryptographie sous-jacente. C'est une encyclopédie sourcée et en langage clair de l'informatique quantique et des schémas conçus pour y survivre, y compris les standards NIST sur lesquels reposent les signatures de BTX. Utile, que vous vouliez la version en un paragraphe ou les standards eux-mêmes.



postquantum.wiki, une encyclopédie sourcée et en langage clair de la cryptographie post-quantique.

Pour BTX en particulier, l'explorateur de blocs est l'endroit où vérifier tout ce qu'on vous a dit.



btxscan.io, l'explorateur de blocs BTX.

13 La part d'honnêteté

Un manuel qui ne liste que les bonnes nouvelles est une publicité. Voici ce qu'il vaut la peine de savoir avant de dépenser de l'électricité ou de l'attention.

- **BTX n'a pas de marché public établi.** Tout prix que vous rencontrerez n'est rien d'autre que l'accord privé de deux personnes. Tenez ce que vous minez pour incertain, jamais pour un revenu.
- **Le minage coûte de l'électricité bien réelle** et sollicite fortement votre GPU, ce qui veut dire de la chaleur et de la consommation.
- **Les applications ne sont pas encore signées numériquement.** C'est pour cela que certains antivirus les signalent, et c'est aussi pour cela que chaque build publie une empreinte SHA-256 que vous pouvez vérifier vous-même avant de l'exécuter.
- **Les shares sont rares depuis le fork.** Une heure sans rien tient en général à la chance, pas à une panne.
- **Sauvegardez votre portefeuille.** Aucune partie de ce projet ne peut récupérer vos clés à votre place, ce qui est tout l'intérêt de l'auto-custodie et aussi son prix.

Où tout se trouve

Chaque adresse ci-dessous mérite d'être conservée. Aucune ne vous demande de créer un compte, et celles qui servent des données renvoient du JSON sans clé. Ils ne sont pas tous indépendants de nous : btx.best et btxscan.io sont développés par easyBTX, et PQ Wallet, le portefeuille bonuz et qID ont des personnes en commun avec easyBTX. La chaîne, les pools et postquantum.wiki ne sont pas à nous. Si un lien contredit un jour cette page, faites confiance au lien.

COMMENCER ICI

`easybtx.com/btx`	Ce manuel sous forme de page web vivante, tenue à jour.
`btx.dev`	Le site du projet BTX.
`btx.best`	Le portail vers BTX. Tous les produits, outils et liens de l'écosystème, en un seul endroit.
`btxscan.io`	L'explorateur de blocs. Consultez n'importe quel bloc, adresse ou transaction.

LOGICIELS

`easybtx.com/install`	easyBTX, le mineur en un clic pour Mac, Windows et Linux.
`easybtx.com/node`	easyNode, un nœud BTX complet sous forme d'application de bureau.
`easybtx.com/guardian`	Node Guardian, un script gratuit qui diagnostique un nœud qui n'avance plus.
`easybtx.com/keeper`	Keeper, un petit nœud élagué qui sert des confirmations de blocs signées.

DÉTENIR DES BTX

`easybtx.com/wallet`	Quel portefeuille utiliser, et pourquoi il y en a deux.
`pq-wallet.com`	PQ Wallet, post-quantique, pour macOS, Windows et Linux.
`bonuz.xyz`	bonuz, le portefeuille mobile.
`qid.dev`	qID, l'identité post-quantique que les sites BTX utilisent pour la connexion.

LECTURES ET PREUVES

easybtx.com/research/	L'archive de recherche. Sourcée, datée, et jamais réécrite en douce.
easybtx.com/stats	Chiffres en direct de la chaîne, des nœuds et des pools.
easybtx.com/nodes	Une carte en direct de tous les nœuds publics joignables.
postquantum.wiki	Une encyclopédie sourcée et en langage clair de la cryptographie post-quantique.

POUR LES MACHINES

easybtx.com/ai	Écrit pour les agents autonomes : points d'accès ouverts et limites annoncées sans détour.
easybtx.com/api/network	Hauteur de chaîne, émission, recensement des nœuds et pools, en JSON, sans clé.
easybtx.com/llms.txt	Un résumé de ce site pour les modèles de langage.

COMMUNAUTÉ

t.me/easyBTX	Le Telegram easyBTX, où l'on répond aux questions.
x.com/easyBTX	Notes de version et brèves mises à jour.
github.com/MendeMatthias/EasyBTX-releases/releases	Tous les builds publiés, avec leurs sommes de contrôle.

À LIRE

Uniquement à des fins pédagogiques et de divertissement. Rien dans ce manuel ne constitue un conseil financier, une offre ou une recommandation d'acheter, de vendre ou de miner quoi que ce soit. Publié par easyBTX, qui développe des logiciels pour BTX et n'est pas l'équipe centrale de BTX. Ce n'est pas un document officiel. BTX n'a pas de marché public établi, le minage peut ne rien vous rapporter, et vous êtes responsable de vos propres décisions.