easyBTX

BTX 手册

BTX 是什么、它的挖矿如何运作、这条链一路是怎么走过来的，以及每一条说法你可以去哪里自己核对。

> 仅供学习和娱乐之用。不构成财务建议。easyBTX 不是 BTX 核心团队，BTX 也没有成熟的公开市场。

第一版 · 数据截至 2026 年 8 月 23 日 · EASYBTX.COM/BTX

目录

1 谁写了这本手册，谁没有写

easyBTX 为 BTX 开发软件：一个挖矿应用、一个节点应用，以及一些免费工具。**easyBTX 不是 BTX 核心团队。** 这条链的共识软件由 BTX 项目编写并发布，easyBTX 既不参与其中，也对它没有任何决定权。他们的源代码和发布版本，我们和其他任何人一样，都是从公开渠道读到的。

这关系到你该怎么读这本手册。这里没有任何内容是代表这条链发出的公告、路线图或承诺，因为这些本来就轮不到我们来发。它只是一个独立参与者对公开资料的解读，写出来就是为了让你能自己去核对。凡是记录本身不清楚的地方，我们会直说；凡是我们以前弄错过的地方，我们也一样会说。

这里要交代两件事，因为不交代，就等于让你把情况想得比事实更好看。第一，easyBTX 在 BTX 走得好这件事上是有利害关系的，而且从挖矿里抽取费用。第二，手册末尾列出的那些项目，并不是每一个都和我们保持距离。BTX 这条链本身是真正独立的，而这也是最要紧的那一层独立。但 btx.best 和 btxscan.io 是由 easyBTX 开发的，它们自己的页脚上就是这么写的；PQ Wallet、bonuz 钱包和 qID 则和 easyBTX 有共同的成员。本手册凡是在介绍这几个产品的地方，请把它当作一个参与者在讲自己参与开发的东西。这条链、各个矿池和 postquantum.wiki 不是我们的。把它们列出来并不等于为它们作担保，它们彼此之间也不为对方负责。

2 BTX 是什么

BTX 是比特币的一个分叉，为抵御量子计算机而打造。

比特币用 ECDSA 为每一笔交易签名，那是一种经典的椭圆曲线方案。足够强大的量子计算机能够破解它，花掉本不属于自己的币。BTX 用后量子签名取代了这套签名方案，这也是 BTX 地址长得和比特币地址不一样的原因：BTX 地址以 `btx1z` 开头。

其余部分都刻意保持比特币的样子：

- 固定总量 2100 万枚，无法再增发。
- 没有预挖。币只能作为挖矿奖励产生，一个区块一个区块地出现。
- 工作量证明挖矿，无需向谁申请许可，也没有守门人。
- 自我托管。没有账户，也没有托管方。你掌握密钥，密钥掌握币。

这条链还很年轻。区块 0 的时间戳是 2026 年 3 月 19 日，第一个区块实际是在 2026 年 3 月 23 日挖出的。

3 这份工作就是矩阵乘法

比特币矿工在搜索哈希，BTX 矿工则在做矩阵乘法，也就是现代 AI 加速器专门为之设计的那种稠密运算。在 BTX 文档里，无论哪里出现“matmul”，指的都是这件事：用矩阵乘法作为守护这条链的工作。

实际效果是，GPU 天然就是跑 BTX 的机器，而这份工作是一次真实的数值计算，不是一场哈希彩票。

这句话到底意味着什么、不意味着什么，值得说清楚，因为它是最常被夸大的一条。每次运算的输入都以链本身为种子生成，结果也只保留一个摘要，所以算出来的乘积不会交付给链之外的任何人。**BTX 今天并不出售 AI 算力**。所谓可验证计算市场，也就是由外部方提交真实任务、并为结果付费，只是 BTX 自己的规范里点名的一个后续方向，它并不存在。

今天真正成立的事情要安静得多，也更耐久：挖 BTX 会给一群分散的普通人一笔回报，让他们愿意拥有具备 AI 能力的硬件，并让它保持通电、保持在线，分散在许多互相独立的人手里，而不是集中在少数几个数据中心。

easybtx.com 上的 easyBTX 挖矿应用，显示实时链高度、对照 2100 万上限的发行量，以及可连接公共节点的数量。

4 两套工作函数，以及第二套为什么会存在

BTX 从诞生到今天只用过两套挖矿算法。这一点值得直说，因为 BTX 设计文档里的版本号很容易被误读：它们描述的是一条研究路线图，而不是一连串真实上线过的链。

MatMul v3 从第一个区块起就在运行。 那时一次尝试就是一次 512 × 512 的矩阵乘法，运算发生在一个特意挑选过的素数域上，好让它同时干净地映射到 CUDA 和苹果的 Metal 上。一次尝试只需要微秒级的时间，所以一块显卡每秒能做上百万次，挖矿速度当时也是这么报的。

有三点让它成为合理的选择。这份工作是标准的稠密线性代数，所以天然的机器是 GPU，而不是一块除此之外什么都干不了的芯片。它所依赖的构造相比一次普通的矩阵乘法几乎不增加额外开销，所以浪费在证明机制本身上的电力非常少。而且它为将来可能在链外也有用处的工作留了一扇门。

v3 被加固过好几次，但工作本身没有变。在区块 125,000，矩阵被绑定到区块头中可变的那一部分，这样矿工就不能再把一对准备好的矩阵反复用在很多次尝试上。在区块 130,500，矩阵还被一并绑定到父区块上，这样就不能拿针对某个父区块构造好的模板，去套用到另一个被扣住不发的父区块上。这两次改动都没有改变挖矿在算什么，它们堵住的是捷径。

MatMul v4.7 在 2026 年 8 月 10 日、区块 185,000 处替换了工作函数。 一次尝试不再是一次小规模的乘法，而变成一个不可分割的完整 episode（一整段连续的运算）：四轮依次穿过十六层，矩阵宽度 4,096，约 141 万亿次整数乘加运算，约 4.8 GB 的 GPU 显存，以及大约三十秒不间断的运算。你没法暂停一个 episode，没法把中断的接着跑完，也没法做完六成就拿到六成的功劳。

这里的道理值得弄明白，因为它和人们的直觉正好相反。如果彩票的票价极其便宜，就会有人专门造一台除了飞快买票之外什么都不干的机器。把每一张票变得昂贵、必须按顺序完成、而且吃内存，就把这样的余地抹掉了大半：这份工作本来就是张量核心存在的理由，所以留给专用芯片去“更聪明地做”的空间所剩无几；而且没有哪一步可以跳过，因为校验一个区块就是把这个 episode 原样重跑一遍。设计文档还直接点明了第二个动机：在一条年轻的链上，把用租来的消费级 GPU 发动攻击的成本抬到够不着的高度。

代价是真实的，这个项目也从来没有假装不是这样。Mac 有九天完全无法挖矿，因为新工作函数的求解器在激活当天还没有 Metal 版本。运行旧版软件的节点停在区块 184,999，就一直停在那里。难度不得不一次性重新校准了大约 120,000 倍。有效份额稀少到了这种地步：一台状态良好的机器现在也可能整整一个小时都没有动静。七月还能有利可图地挖 BTX 的显卡，今天完全挖不动了。

5 一个区块是怎么被校验的，以及这一点同样变了

校验这件事是最值得弄明白的部分，而它移动的方向和你可能以为的正好相反。

在 v3 下，校验既巧妙又便宜。校验方不必重做一遍 512 × 512 的乘法，而是把声称的答案乘上几个随机向量再做比较。这就是 Freivalds 算法，两轮下来，一个错误的结果能蒙混过关的概率不到 2 的 62 次方分之一。产出昂贵、校验便宜，这正是你想要的性质。

而在今天实际运行的 v4.7 下，网络的校验方式是把整个 episode 原样重跑一遍，再比对摘要。没有便宜的校验。这是一个刻意的分阶段决定，而不是疏忽：能让校验重新变便宜的简洁证明，被写成了后续的几个 epoch 阶段，而**它们没有任何一个有激活高度**。已公布的计划一共列出四个，其中只有第一个已经上线。

项目方对此说得很直白，与其转述，不如直接引用：

> 校验的形态变了。在 v4.7 目前上线的这个阶段下，网络的校验方式是把 episode 原样重跑一遍，再比对摘要。能让校验重新变便宜的简洁证明，被列为一个没有激活高度的后续阶

段。所以“产出昂贵、校验便宜”这个优雅的性质，眼下只是一个设计目标，而不是已经部署的行为。

有一个后果对任何运行节点的人都很重要。重跑一个 episode 需要一块合格的 GPU，所以大多数机器没法自己校验最新的工作。它们转而依赖一份很小的签名记录，每个区块 208 字节。这就是为什么这个网络如此在意那些愿意对外提供这类记录的节点，也是为什么 2026 年 8 月签名中断两次冻住了网络的一部分，而当时链本身是好的。

6 这里真正不寻常的地方

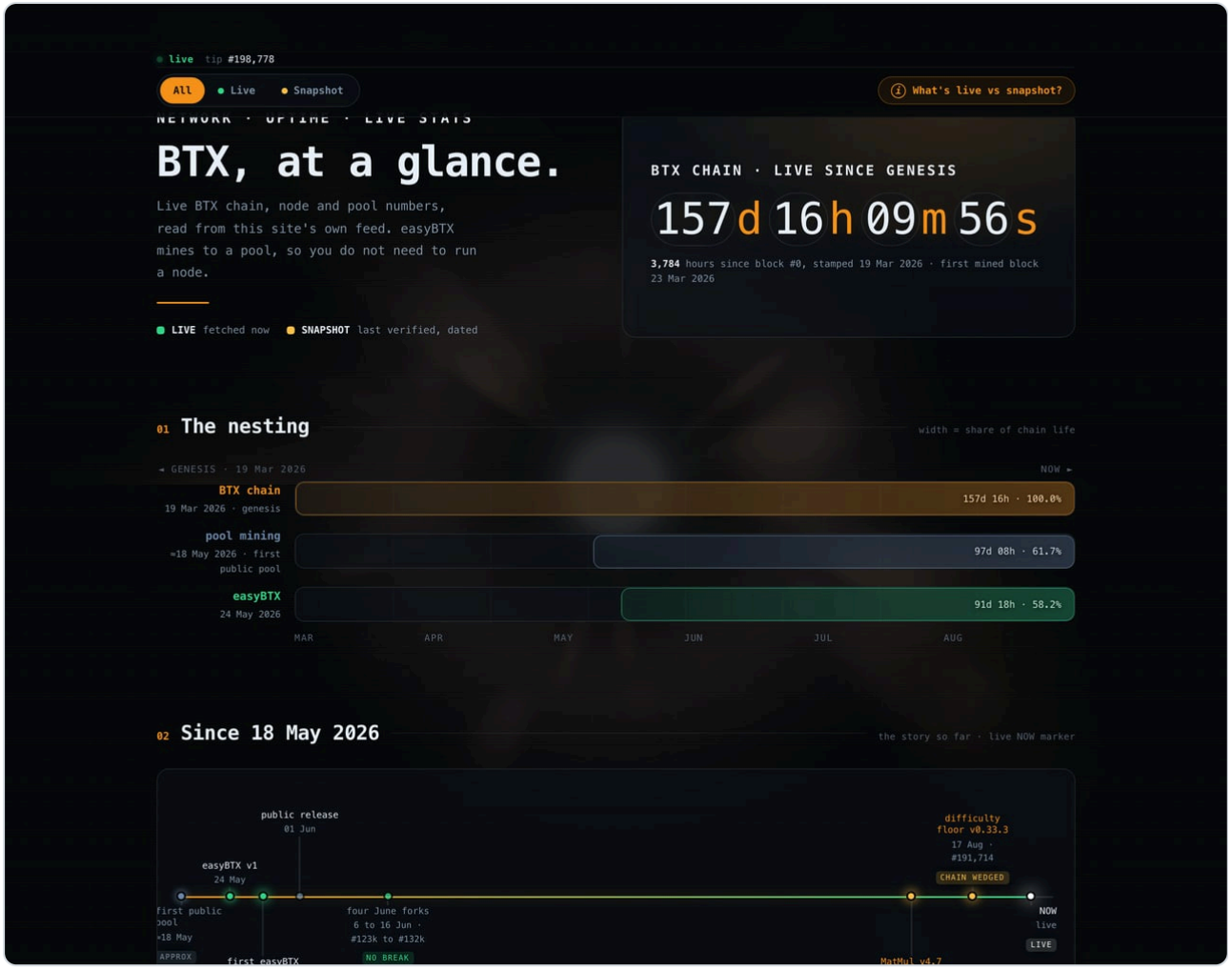
把宣传放到一边，对于以读共识代码为生的人来说，这套设计里有几点确实值得注意。

- **这份工作是真实的稠密整数线性代数**，是确定性的，而且在两套互相独立的 GPU 后端上逐字节一致。两家不同厂商的硬件必须算出完全相同的摘要。
- **每次尝试的成本变化是一次质的改变**，从微秒级变成大约三十秒。很少有链会去尝试这种改动，而它让一次尝试真正变得不可分割。
- **挖矿资格是一次测量，而不是一份名单。** 软件会要求设备复现一个已知结果，并相信它给出的答案，而不是拿芯片的名字去比对白名单。easyBTX 和引擎供应商都曾公布过后来被证明是错的硬件要求，两份要求最后都是被实测纠正的。
- **区块头从未改变。** 一次彻底替换工作量证明的改动，竟然没有给 182 字节的区块头增加哪怕一个字节，这正是矿池、矿工和线路协议能够完好无损地熬过来的原因。这件事一点都不光鲜，却是真的难。

这一切都不代表这份工作对链外的任何人已经有用。它还没有用处，第 2 节也是这么说的。但这套机制是真实的，上面那些数字来自共识源码而不是宣传册，而且这个项目会把自己否决掉的参数选择记录在案，也会在代码里禁用自己尚未完成的组件。这比任何声明都更能说明问题。

7 这条链的简史

时间	高度	发生了什么
2026 年 3 月 19 日	0	创世区块打上时间戳，MatMul v3 从一开始就是工作函数。第一个区块是在 3 月 23 日挖出的。
2026 年 6 月初	~123,000	v0.31.0 分叉。
2026 年 6 月 8 日	125,000	种子被绑定到区块头，一对准备好的矩阵不能再反复用于多次尝试。
2026 年 6 月中	~130,500	种子被绑定到父区块，堵住了模板重放的捷径。工作函数没有变。
2026 年 6 月中	~132,000	一次节点升级。
2026 年 8 月 10 日	185,000	MatMul v4.7 激活。一次尝试变成一个三十秒的 episode。
2026 年 8 月 17 日	191,690	网络卡死。BTX Core v0.33.3 当天发布，把难度下限设在区块 191,714，这条链随后恢复。
2026 年 8 月 22 日	197,000+	已发行约 396 万 BTX，约为总量上限的 19%。



easybtx.com/stats 的实时数据页，显示链、节点普查和每一个在运行的矿池。

8 总量与发行

每个区块支付 20 BTX。目标出块间隔是 90 秒，不过这条链诞生以来的实际平均值一直快于这个数。奖励每 525,000 个区块减半一次，而且这份时间表是精确的：20、10、5 这样一路减下去，每一档各 525,000 个区块，加起来正好是 2100 万。

减半还一次都没发生过。第一次还没到来。

撰写本手册时，这条链已经越过区块 197,000，也就是已发行约 396 万 BTX，略低于总量上限的 19%。想看当前数字而不是这里的快照，请查阅本手册末尾列出的实时数据页。

9 BTX 能被伪造吗?

不能，而且理由是结构性的，不是承诺。

总量固定在 2100 万枚，没有预挖，币只能通过挖矿产生。BTX 是一条从比特币衍生出来的链，没有代币层，所以除非打破每个节点各自独立执行的规则，否则根本没有机制能发出一枚假币。每一枚币都能

一个区块一个区块地追溯回某一次挖矿奖励。

这和这条链会不会被攻击是两个问题。掌握足够大比例算力的一方可以重组最近的区块，这一点对包括比特币在内的每一条工作量证明链都成立。研究存档里有一份完整研究，讲清楚什么可能、什么不可能，以及你自己验证真伪的具体步骤。

10 三种参与方式

挖它。easyBTX 是一个应用，同时支持 Mac、Windows 和 Linux。它加入矿池挖矿，把收益打到你自己掌控的钱包，并且会自动保持更新。Mac 需要 Apple 芯片和 macOS 26.4 或更高版本；某台 Mac 能不能挖，由应用对 GPU 跑一次半秒的实测来判定，而不是看芯片型号。Windows 通过 WSL2 运行 Linux 版本。Linux 需要一块 NVIDIA GPU。所有费用都事先讲明：easyBTX 收 4.99%，矿池收自己那一份，在 Windows 和 Linux 上 MATADOR 引擎再收 1%。目前所有平台都不提供单独挖矿。

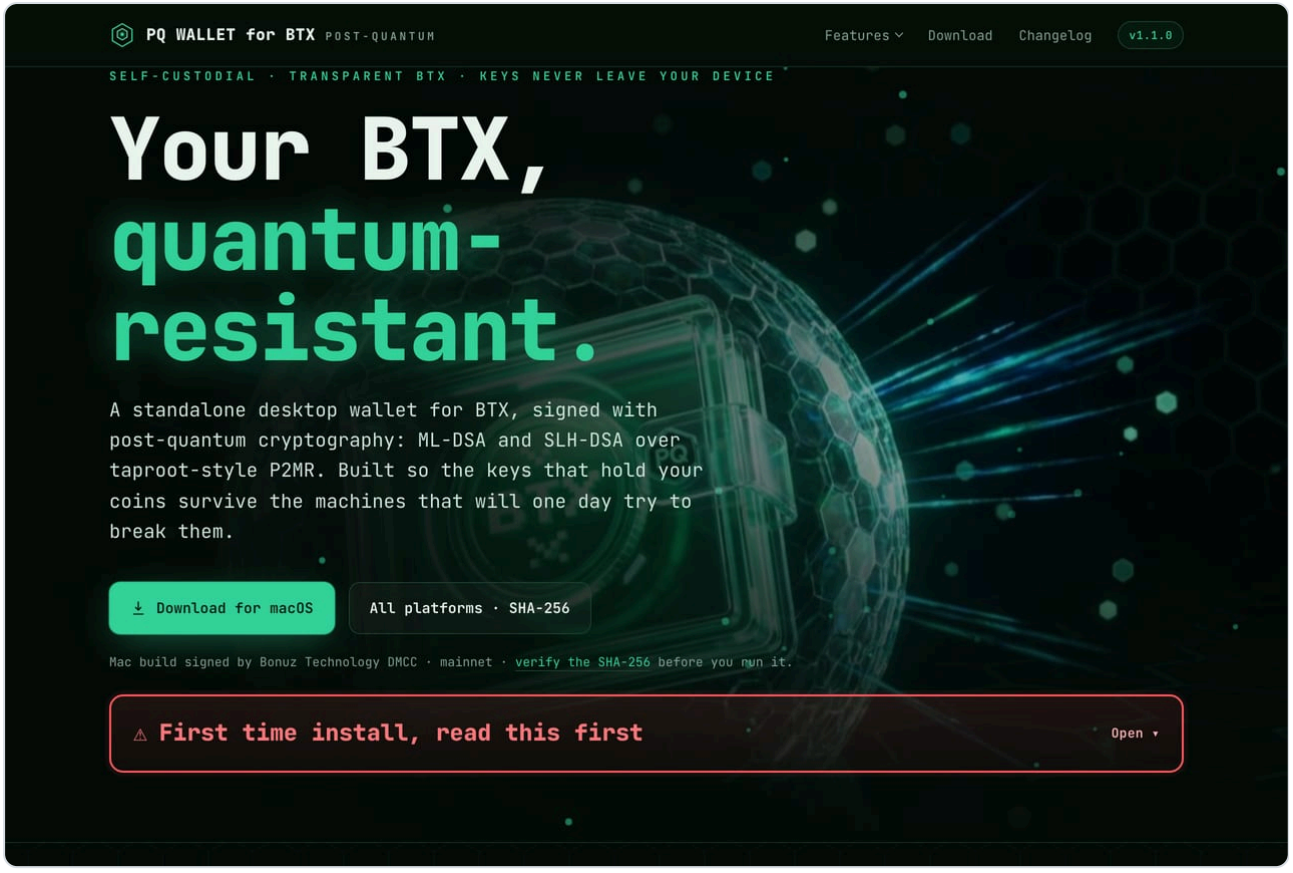
验证它。运行一个全节点，是在不依赖别人服务器的前提下回答链上问题的唯一办法。easyNode 在三个平台上都把这件事变成一次点击。Node Guardian 用来诊断停止前进的节点；Keeper 则把一台闲置机器变成对外提供带签名区块确认的节点，而这正是网络上最稀缺的资源。

持有它。BTX 地址是后量子的，密钥留在你自己的机器上。挖矿应用内置了一个钱包；另有两个专门的钱包走得更远，一个在桌面，一个在手机。

11 钱包，以及不用账户就能登录

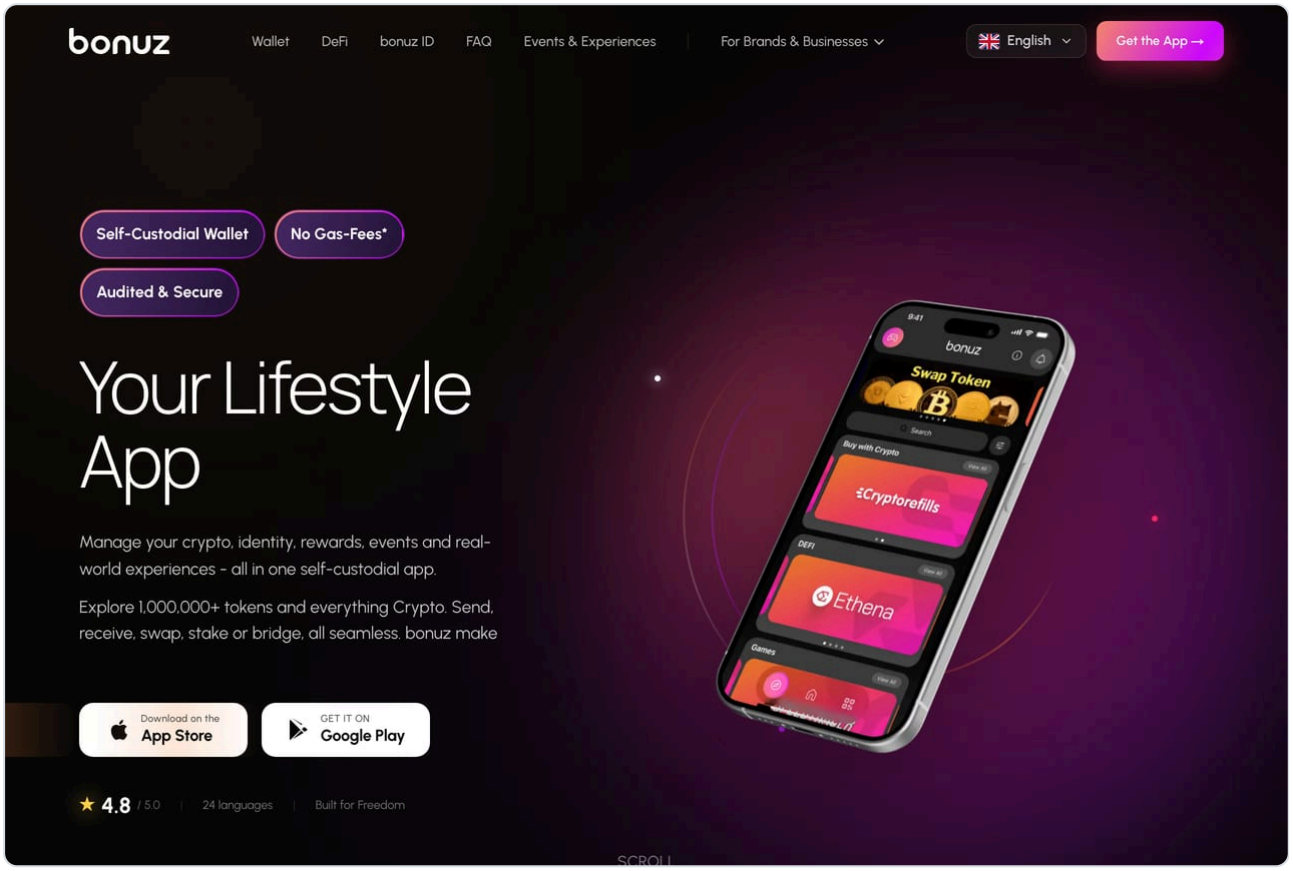
BTX 钱包就是一把你自己掌控的密钥，所以选钱包，选的是这把密钥放在哪里。

PQ Wallet 是桌面钱包，支持 macOS、Windows 和 Linux。它用后量子方案签名，密钥始终留在本机。



PQ Wallet，BTX 的后量子桌面钱包。

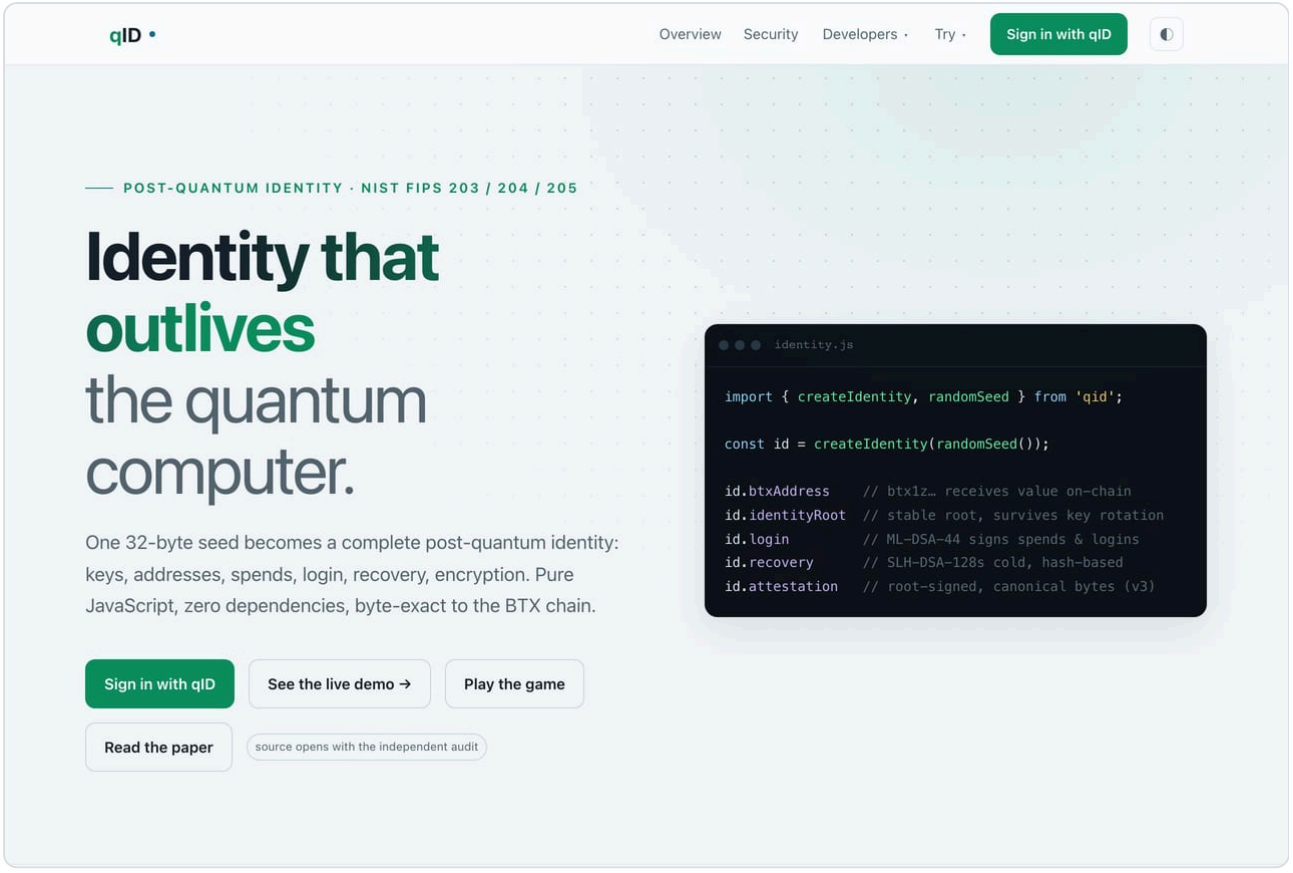
bonuz 是手机钱包，支持 iPhone 和 Android，除了币，还带着你的链上身份。



bonuz，BTX 的手机钱包。

两个都是自我托管的，都不要求你注册。挖矿应用本身也内置了钱包，用来接收你挖到的币已经够用；你也可以把收益直接打到上面这两个钱包中的任意一个。

qID 是把钱包和网站连起来的那一环。BTX 各站点用它来登录：不用邮箱和密码，而是由你证明自己掌控着那把密钥。网站到底拿到了什么，值得说得准确一点。它拿不到你的姓名、你的邮箱和你的密钥；它拿得到的是你的 BTX 地址，而一个 BTX 地址就是公开账本上的一条记录，所以你登录的网站可以去查这个地址持有什么、做过什么。这是一个真实的取舍，它和匿名不是一回事。qID 有一点做对了，值得直说：一份登录证明永远动不了你的币。登录和交易签的是不同的、各自带标签的摘要，所以针对其中一件事做出的签名，没法拿去当作另一件事重放。一个 32 字节的种子，就能派生出一整套后量子身份，包括密钥、地址、支付、登录和恢复，而同一个种子还能在链上持有价值。如果你在别的链上用过 wallet-connect，qID 就是把那个想法重做一遍，让它在量子计算机面前依然站得住。

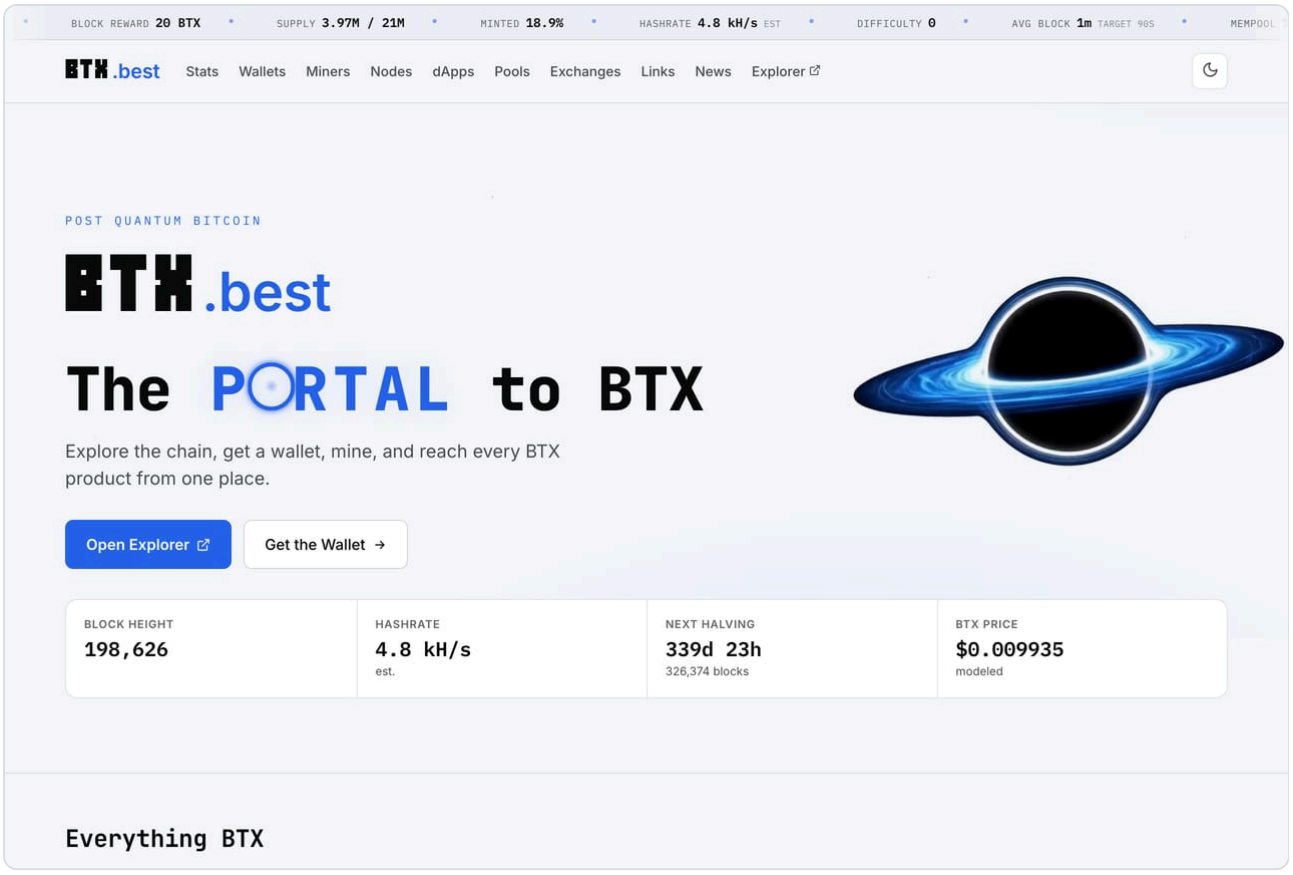


qid.dev，BTX 各站点用来登录的后量子身份。

12 去哪里了解更多

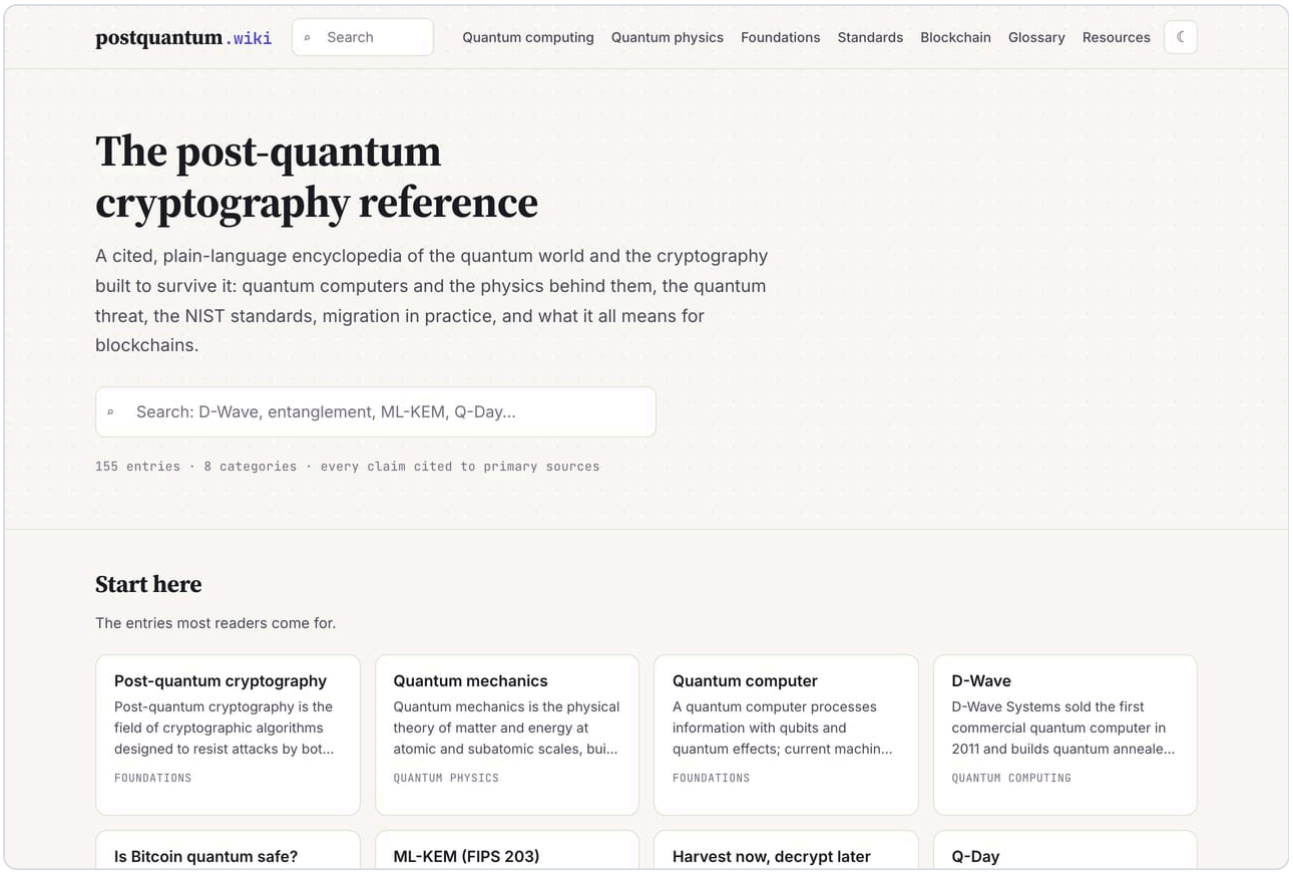
有两个地方比其他都更值得去。

btx.best 是门户。它把每一个 BTX 产品、工具、区块浏览器、钱包、矿池和 dApp 收进同一页，并按你想做的事情来归类。如果本手册里你只打算收藏一个地址，又拿不定主意，就收它。



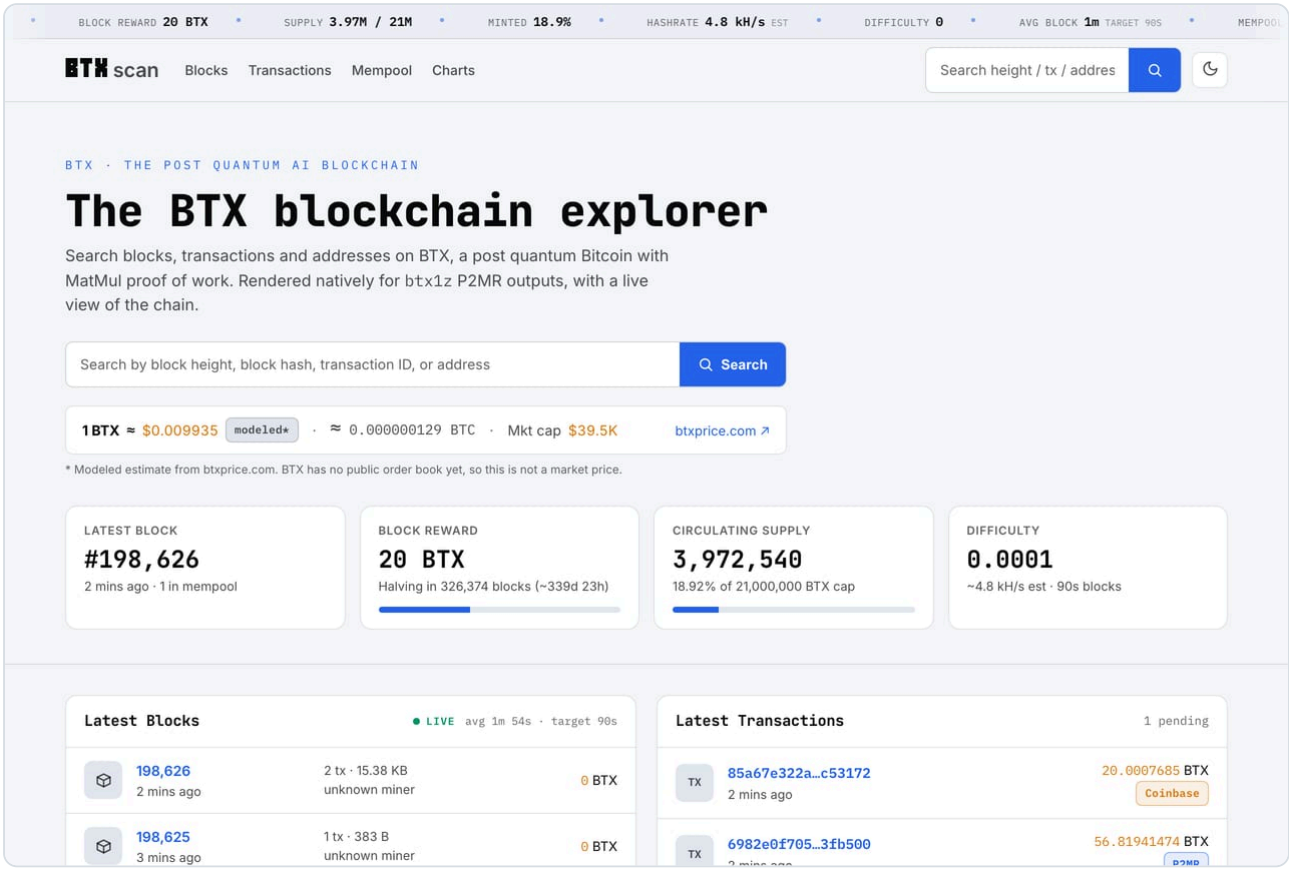
btx.best，把每一个 BTX 产品和链接集中到一处的门户。

postquantum.wiki 是底层密码学的参考资料。它是一部有引注、用大白话写的百科，既讲量子计算，也讲为抵御它而设计的各种方案，包括 BTX 签名所依据的 NIST 标准。无论你想要一段话的版本，还是想要标准原文，它都用得上。



postquantum.wiki，一部有引注、用大白话写的后量子密码学百科。

具体到 BTX，凡是别人告诉你的说法，都可以到区块浏览器上去核对。



btxscan.io，BTX 的区块浏览器。

13 诚实的部分

只列好消息的手册就是广告。在你花掉电费或注意力之前，下面这些事值得先知道。

- **BTX 没有成熟的公开市场**。你遇到的任何价格，都只是两个人私下谈成的。你挖到的任何东西都要当作不确定的，绝不要当作收入。
- **挖矿要烧真实的电**，而且会让你的 GPU 长时间满负荷运转，也就意味着发热和耗电。
- **这些应用还没有做代码签名**。这就是某些杀毒引擎会报警的原因，也是每个版本都会公布一个 SHA-256、让你在运行前自己核对的原因。
- **分叉之后份额本来就稀少**。安静一个小时通常是运气问题，不是故障。
- **备份你的钱包**。这个项目的任何一部分都无法帮你找回密钥，这正是自我托管的意义所在，也是它的代价。

所有东西都在哪里

下面每一个地址都值得留着。这份名单上没有任何一项要求你注册账户，其中标注为数据的那几个，不用密钥就能返回 JSON。它们并不都和我们没有关系：btx.best 和 btxscan.io 是由 easyBTX 开发的，PQ Wallet、bonuz 钱包和 qID 则和 easyBTX 有共同的成员。这条链、各个矿池和 postquantum.wiki 不是我们的。如果某个链接的内容和本页不一致，请以链接为准。

从这里开始

easybtx.com/btx	本手册的网页版，持续更新。
btx.dev	BTX 项目官网。
btx.best	通往 BTX 的门户。生态里的每一个产品、工具和链接，都集中在这一页。
btxscan.io	区块浏览器。任何区块、地址或交易都能查。

软件

easybtx.com/install	easyBTX，面向 Mac、Windows 和 Linux 的一键挖矿应用。
easybtx.com/node	easyNode，以桌面应用形式运行的 BTX 全节点。
easybtx.com/guardian	Node Guardian，一个免费脚本，用来诊断停止前进的节点。
easybtx.com/keeper	Keeper，一个小型修剪节点，对外提供带签名的区块确认。

持有 BTX

easybtx.com/wallet	该用哪个钱包，以及为什么有两个。
pq-wallet.com	PQ Wallet，后量子钱包，支持 macOS、Windows 和 Linux。
bonuz.xyz	bonuz，手机钱包。
qid.dev	qID，BTX 各站点用来登录的后量子身份。

延伸阅读与证据

easybtx.com/research/	研究存档。有出处、有日期，绝不悄悄改写。
easybtx.com/stats	链、节点和矿池的实时数字。
easybtx.com/nodes	所有可连接公共节点的实时地图。
postquantum.wiki	一部有引注、用大白话写的后量子密码学百科。

给机器读的

easybtx.com/ai	写给自主智能体：开放接口，以及诚实的边界。
easybtx.com/api/network	链高度、发行量、节点普查和矿池，JSON 格式，无需密钥。
easybtx.com/llms.txt	本站写给语言模型的摘要。

社区

t.me/easyBTX	easyBTX 的 Telegram 群，提问会有人回答。
x.com/easyBTX	版本说明和简短动态。
github.com/MendeMatthias/EasyBTX-releases/releases	每一个发布过的版本，附校验值。

请阅读

仅供学习和娱乐之用。本手册里的任何内容都不构成财务建议，不构成要约，也不构成买入、卖出或挖取任何东西的推荐。由 easyBTX 出版，easyBTX 为 BTX 开发软件，不是 BTX 核心团队。这不是官方文件。BTX 没有成熟的公开市场，挖矿可能让你一无所获，你要为自己的决定负责。