

AURIQ

LITEPAPER

Version 0.3 · November 2026

Abstract

Auriq (AURIQ) is a transparent cryptocurrency mined with SHA256D and RandomX v2 and secured by proof of stake once staking activates. Mining issuance is capped at 768 million AURIQ. After that cap, every block is proof of stake and pays a tail emission of 4 AURIQ, about 2.1 million a year. Base fees are burned, so busy blocks cancel the tail and heavy use shrinks supply, by at most 0.5% a year, while stakers vote the minimum fee.

The ledger has no privacy features, avoiding the EU restrictions on coins with anonymity features. An 80 million AURIQ genesis treasury, which cannot stake, funds exchange listings, infrastructure, and development.

Auriq takes its name from aurum, Latin for gold, the metal of Rome's aureus [1].

Parameters

Parameter	Value
Ticker	AURIQ
Addresses	Bech32m, prefix **auriq1**; testnet **tauriq**, regtest **rauriq**
Divisibility	8 decimals, 1 AURIQ = 100,000,000 base units
Block time	60 seconds
Block weight	4,000,000 weight units, about 690 standard transactions
Block types	50% SHA256D and 50% RandomX v2 until staking; then 25% each and 50% proof of stake until the mining cap; then proof of stake only
Proof of work limit	5 blocks in a row once staking is active
Difficulty	Dark Gravity Wave, per block type
Treasury	80,000,000 AURIQ at genesis, on top of the mining cap; cannot stake
Staking	Activates at block 129,600; coins mature after 1,440 confirmations
Mining cap	768,000,000 AURIQ of block rewards, reached near year 17.7
Block reward	192 AURIQ, halving every 4 years
Tail emission	4 AURIQ per block after the mining cap, about 2.1 million a year
Fees	Base fee per vbyte, floating with block fullness above a floor that stakers vote; base fees burned, tips to the block finder
Deflation ceiling	0.5% of supply a year, enforced per block
Reorganization limit	1,440 blocks
Signatures	ML-DSA-65, versioned

Motivation

A fixed supply proof of work chain must eventually pay for security from fees alone. Auriq keeps a tail emission and burns base fees, so busy blocks cancel it.

Ethereum burns its base fee too, and when cheaper capacity arrived its base fees fell about 90% and supply turned inflationary [2]. Auriq accepts that trade on purpose: stakers keep fees usable at any price, and the tail emission pays for security either way.

From 10 July 2027, EU crypto service providers may not keep accounts that use coins with built in anonymity features [3]. Auriq has none.

Two mining algorithms, one for asics and one for general purpose cpus, open distribution to a wide range of hardware.

Consensus

Every block is a SHA256D proof of work block, a RandomX v2 proof of work block, or a proof of stake block, recorded in the header. SHA256D uses the standard Bitcoin header, so existing asics can mine it. Each type retargets with Dark Gravity Wave over its own blocks only, so more hashrate raises that type's difficulty, not its share of blocks, and a swing on one algorithm does not disturb the others. Blocks timestamped more than 75 seconds ahead are rejected. Veil runs this model in production [4] [5].

Treasury coins cannot stake, so the chain starts with proof of work only, split evenly between the two algorithms. Each algorithm starts at a low published difficulty, and Dark Gravity Wave raises it as miners join. Proof of stake activates at block 129,600, 90 days in, when about 24.6 million mined AURIQ will be mature. Its starting difficulty assumes half of those coins stake, and Dark Gravity Wave adjusts from there.

From activation to the mining cap, block targets are 25% SHA256D, 25% RandomX v2, and 50% proof of stake. Targets are difficulties, not reserved slots, but at most five proof of work blocks may come in a row before a proof of stake block is required, as in Veil [7]. If no block arrives for 10 minutes, stake difficulty eases the longer the gap lasts, so any online staker can restart the chain.

Stake weight is the mature balance, with no bonus for coin age or uptime, as in Veil [8]. Coins mature after 1,440 confirmations, the reorganization limit, so none can stake on both sides of a reorganization. Staking needs an online wallet. Stakers also vote the fee floor and signal upgrades.

Stake secures the chain, and mining distributes coins. The chain with the most trust wins. As in Peercoin, once staking is active, proof of stake blocks add trust by stake difficulty and proof of work blocks add almost none [9], so overriding the chain takes a majority of active stake, not hashrate. Before activation, each block adds the geometric mean of the current work on both algorithms, as in DigiByte [10], so overtaking the chain takes a majority of both. Running nodes refuse to reorganize more than 1,440 blocks, releases include hardcoded checkpoints, and no party can broadcast signed checkpoints that nodes must follow.

RandomX v2 is released and has run on Monero's stress test network since the 5 October 2026 fork, without a mainnet date yet [11]. Auriq pins the exact version.

Monetary policy

Mining issuance is capped at 768 million AURIQ. The cap counts block rewards issued, not coins in circulation, so burns never extend mining. The block reward starts at 192 AURIQ and halves every four years, the same for every block type. The mining cap is reached about 17.7 years after launch, near block 9.3 million. After that, proof of work blocks are invalid and each proof of stake block pays a tail emission of 4 AURIQ, about 2.1 million AURIQ a year, so the network keeps a security budget forever and total issuance has no fixed limit.

The genesis block also creates an 80 million AURIQ treasury, on top of the mining cap, to pay for exchange listings, infrastructure, and development without a later treasury block. It is spendable from launch and held in a published two of three ML-DSA multisig, so every spend is visible on the ledger. Treasury outputs can never stake, which leaves chain security with miners and independent stakers; coins the treasury pays out stake normally. About 848 million AURIQ exist when mining ends, 9.4% of them from the treasury.

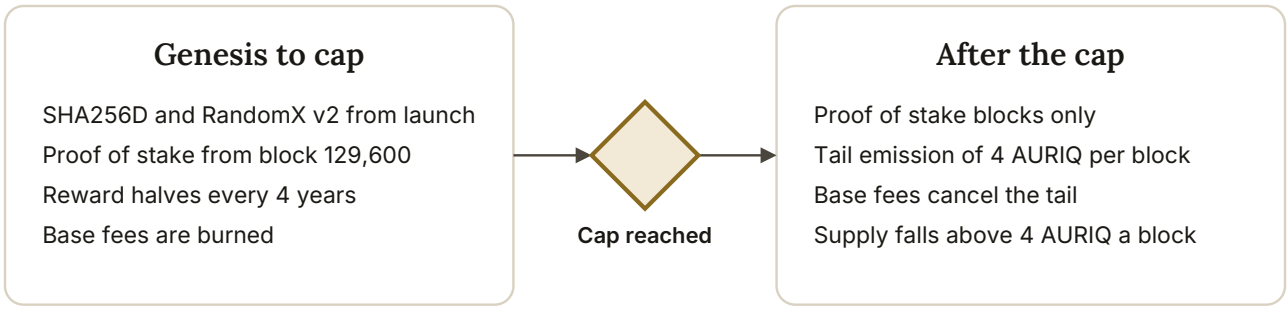


Figure 1. Mining hands off to staking at the mining cap.

Years after launch	Reward per block	Issued in period	Total created
Genesis	Treasury	80.0M	80.0M
0 to 4	192 AURIQ	403.9M	483.9M
4 to 8	96 AURIQ	202.0M	685.9M
8 to 12	48 AURIQ	101.0M	786.9M
12 to 16	24 AURIQ	50.5M	837.4M
16 to 17.7	12 AURIQ	10.6M	848.0M
After 17.7	4 AURIQ, tail emission	2.1M a year	Ongoing

Table 1. Emission schedule at 525,960 blocks a year.

Fees and burn

Every transaction pays a base fee per vbyte, plus any tip it chooses. The base fee rate floats with demand: after each block it rises by up to 12.5% when the block was more than half full and falls by up to 12.5% when it was emptier, never below a floor, as with Ethereum's base fee [19]. A burst of spam gets expensive within minutes, about a thousandfold after an hour of full blocks, and fees sink back to the floor once blocks empty. The rate is checked across each block, so a child transaction can pay for its parent.

Stakers set the floor. Each proof of stake block votes to raise it, lower it, or hold, and it moves at most 1/4096 per block, so it can halve or double in about four days but cannot jump overnight, much as Ethereum's block proposers move its gas limit by at most 1/1024 a block [20]. No price feed is needed. If AURIQ rises a thousandfold, stakers walk the floor down so a transaction costs about the same in dollars, and if spam turns cheap they walk it up. The floor starts at 100 base units per vbyte, about 0.0015 AURIQ for a standard transaction, and holds there until staking activates.

Base fees are burned and tips go to the block finder, who earns the block reward and tips whatever the base fees are, so stakers gain nothing by voting fees up. After the mining cap the burn cancels the tail emission: a block with 0.5 AURIQ of base fees adds only 3.5 new AURIQ, a block with 4 adds none, and more than 4 shrinks supply. The burn in any block is capped at the block reward plus 0.5% of supply a year:

$$\text{Burn cap} = R + 0.005 \times S / 525{,}960$$

R is the block reward, *S* the current supply, and 525,960 the number of blocks in a year. Base fees above the cap go to the block finder, so supply falls at most 0.5% a year, and because the ceiling is a share of current supply it never reaches zero. At the ceiling supply halves about every 140 years.

Base fees per block	New AURIQ per block	Net supply change
None	4	+0.25% a year
1 AURIQ	3	+0.19% a year
4 AURIQ	0	Flat
8 AURIQ	−4	−0.25% a year
12.1 AURIQ or more	−8.1	−0.5% a year, the ceiling

Table 2. Base fees after the cap, with supply near 848 million AURIQ. The block finder earns 4 AURIQ plus tips in every case.

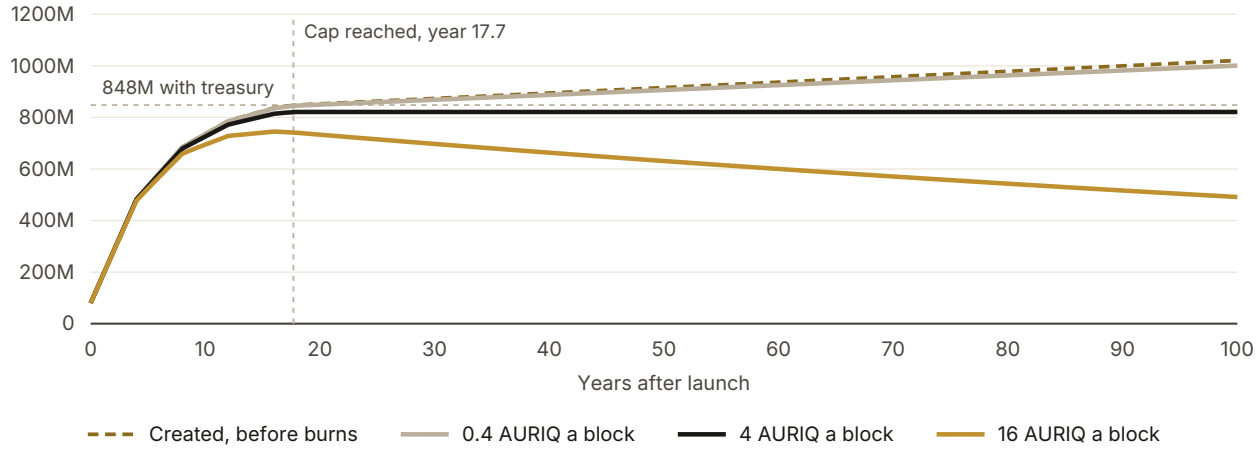


Figure 2. Coins created and in circulation by average base fees burned per block, ramping up over 10 years.

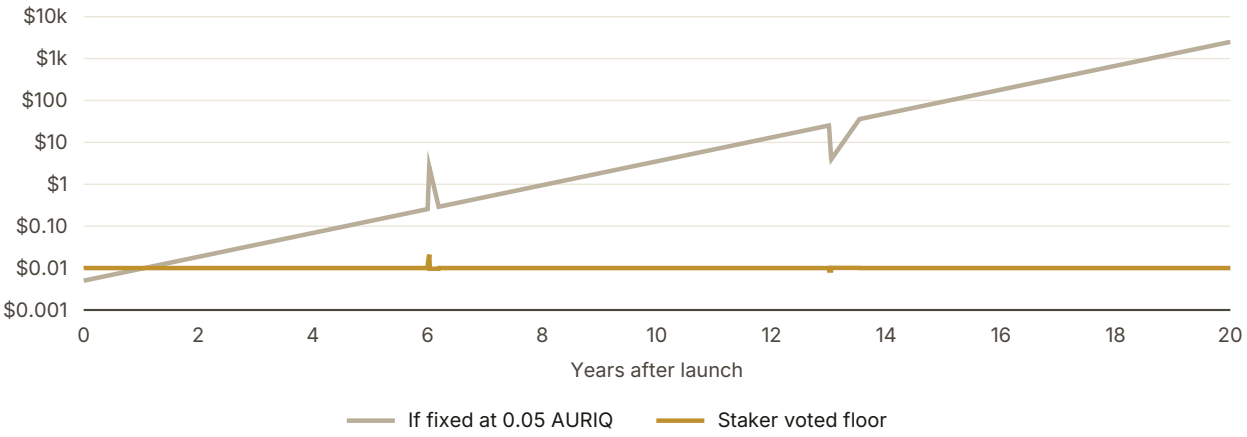


Figure 3. Fee per standard transaction in dollars as AURIQ rises from $0.10 to $50,000 with a boom and a crash, under a fixed fee and under a floor stakers steer toward about a cent. Illustrative price path.

Cryptography

Hashes need no change, since a quantum computer gives only a limited speedup against them. Signatures use ML-DSA-65 from genesis, so no coin is ever held under a quantum vulnerable key. Each output records a versioned signature type, so FN-DSA or another scheme can be added later by soft fork. ML-DSA-65 adds margin over ML-DSA-44 for signatures about 37% larger. Security categories follow [12].

Scheme	Status	NIST category	Public key	Signature
secp256k1, ecdsa or Schnorr	Used by Bitcoin, not quantum resistant	None	33 bytes	64 to 72 bytes
ML-DSA-44	FIPS 204 final [13]	2	1,312 bytes	2,420 bytes
ML-DSA-65	**FIPS 204 final, used by Auriq** [13]	3	1,952 bytes	3,309 bytes
ML-DSA-87	FIPS 204 final [13]	5	2,592 bytes	4,627 bytes
FN-DSA-512	FIPS 206 draft, final expected late 2026 or early 2027 [14]	1 [15]	897 bytes [15]	About 666 bytes [15]

Each input carries a 1,952 byte public key and a 3,309 byte signature, so a standard transaction is about 5.4 KB, or 1,455 vbytes, of which only 137 bytes are outside the witness. Blocks are limited to 4 million weight units, about 690 standard transactions or close to a million a day. At 230,400 transactions a day an archival node grows about 455 GB a year.

Transaction ids exclude witness data, so by default a node discards keys and signatures for blocks below the latest checkpoint in its release, and a new node syncing to that checkpoint never downloads them. As with Bitcoin's assumevalid, this trusts that blocks below a reviewed checkpoint were validly signed, and it relies on archival nodes keeping witness data public [18]. At that rate a witness pruned node grows about 12 GB a year, keeps every transaction for wallet rescans, and stakes normally. Fully pruned nodes keep the utxo set, which stores a 32 byte key hash per output, and at least the last 1,440 blocks. Verification speed and sync time will be benchmarked on testnet.

Regulatory posture

Auriq has no privacy features, optional or otherwise. The EU's Anti-Money Laundering Regulation treats coins with built in anonymity features, systematic or optional, as anonymity enhancing, and from 10 July 2027 EU crypto service providers may not keep accounts that use them [3]. MiCA Article 76(3) already bars trading platforms from listing such coins unless holders and transaction history can be identified [16]. Confidential transactions, ring signatures, stealth addresses, shielded pools, and mixing are therefore excluded from consensus and the reference wallet. This removes one obstacle to EU listings; exchanges still apply their own listing and anti money laundering checks.

This describes design intent, not legal advice.

Implementation

The reference client is built on the current Bitcoin Core release. The consensus changes are substantial, so they are kept in their own modules for upstream fixes to merge cleanly. Multi algorithm mining follows Veil [4] [5], and transparent staking and fee burning follow Peercoin [6] [17].

A public testnet runs first. Before mainnet, the project publishes a consensus specification with test vectors, runs attack simulations, and seeks an independent audit. The genesis parameters, treasury addresses, initial difficulties, binaries, and launch time are published in advance, and the genesis block commits to a recent Bitcoin block hash so no one can mine early.

References

[1] Aureus, Wikipedia

[2] Ethereum hits longest inflationary period since Merge, Blockworks

[3] AMLR for crypto: what CASPs must verify, Didit

[4] Veil v1.1.0.1 release notes, Veil Project

[5] Veil month's end update, August 2020, Veil Project

[6] Questions on 1% destruction and 1% growth of PPC, Peercointalk

[7] validation.cpp, CheckConsecutivePoW, Veil source

[8] Frequently asked questions about Veil staking, Veil support

[9] Peercoin chain trust, Peercoin Wiki

[10] chain.cpp, GetBlockProof, DigiByte source

[11] When is the next Monero hard fork?, Bitrue

[12] ML-DSA in Certificates, IETF draft

[13] crypto/mldsa package, Go standard library

[14] FN-DSA (FIPS 206), Encryption Consulting

[15] FN-DSA, PQ Crypto Registry

[16] MiCAR Compliance Toolkit: Anti-Money Laundering Requirements, Baker McKenzie

[17] Peercoin, encyclopedia entry

[18] Don't download witnesses for assumed-valid blocks when running in prune mode, Bitcoin Core

[19] EIP-1559: Fee market change for ETH 1.0 chain, Ethereum Improvement Proposals

[20] EIP-8261: Gas limit schedule, Ethereum Improvement Proposals

Important notice

This litepaper describes a protocol under development, and its design and parameters may change before launch. It is not an offer to sell or a solicitation to buy any asset, and it is not financial, investment, legal, or tax advice.