Grox (GROX) Whitepaper

Version 1.0 · November 18, 2026

Abstract

Grox (GROX) is a private, CPU-mineable cryptocurrency with a hard cap of 21,000,000 coins and a new block every 60 seconds. It builds on the Monero codebase (v0.18.5.4), so every transaction hides its sender, receiver and amount by default.

Grox uses its own proof-of-work, rx/grox: the RandomX v2 program with a Grox-specific salt. It keeps mining efficient on ordinary computers, and existing Monero miners or rented hashrate cannot be pointed at Grox without software built for it. Mining is open to anyone, solo or through a public P2Pool with a 0% fee.

Motivation

Most proof-of-work coins today are mined by ASIC farms, GPU rigs or rented hashrate, which leaves ordinary users out. Grox is built for the opposite: the computer someone already owns should be enough to mine, and finding a whole block solo should be a realistic event, not a lottery ticket.

Three choices follow from that goal:

- **CPU-first proof-of-work**, so general-purpose processors stay competitive.
- **A separate algorithm variant**, so large existing RandomX hashrate cannot be redirected to Grox without dedicated software.
- **Private by default**, inherited from Monero, because a coin that people mine at home should not publish what they earn or spend.

Proof of work: rx/grox

rx/grox is RandomX with two changes: it runs the RandomX v2 program, as specified by the upstream RandomX project (design notes; 384 instructions per program instead of 256, plus its rounding, AES and prefetch changes), and uses its own Argon2 salt, `GroxRandomX\x01`. The 2 GB dataset, 2 MB scratchpad, 8 programs per hash and the seed-key schedule are the same as Monero's.

The salt gives Grox its own dataset and cache, so hashes are not interchangeable with Monero's rx/0 and existing Monero miners, pools and rented hashrate cannot mine Grox as they are. RandomX's design keeps CPUs efficient: it needs fast caches, branch prediction and a large memory footprint, which makes ASICs and GPUs a poor fit.

The v2 program does more work per hash, but newer processors run it more efficiently, so the net effect depends on the CPU generation. Measured with Grox XMRig on the same machine, back to back (2 threads, `--bench=1M`, 60-second average, November 18, 2026):

CPU	Generation	rx/0, Monero (H/s)	rx/grox (H/s)	rx/grox vs rx/0
AMD EPYC 9V45	AMD Zen 5	1,082	1,288	119%
AMD EPYC 9V45	AMD Zen 5	1,030	1,205	117%
Intel Xeon 6975P-C	Intel Granite Rapids	808	855	106%
AMD EPYC 9V74	AMD Zen 4	966	989	102%
AMD EPYC 7763	AMD Zen 3	904	750	83%

On current CPUs, a machine mines Grox at about the same speed as Monero or faster; on older ones it is somewhat slower. This matches the upstream RandomX v2 design notes.

Grox takes RandomX v2 unchanged from upstream and adds no new cryptography. RandomX v1 was independently audited before Monero adopted it in 2019; the v2 changes are published by the same authors with their rationale and benchmarks.

Blocks and difficulty

Grox targets one block every 60 seconds. Difficulty is set by LWMA (linearly weighted moving average) over the last 90 block solve times, which gives more weight to recent blocks and reacts within minutes when miners join or leave.

Newly mined coins unlock after 60 blocks, about one hour. Ordinary transaction outputs follow Monero's standard 10-block lock.

Monetary policy

The total supply is capped at 21,000,000 GROX, divisible to 11 decimal places. There is no tail emission: the block reward shrinks smoothly toward zero and no coin beyond the cap can ever be created.

Each block's base reward is the coins not yet issued divided by 2^22:

reward = (21,000,000 − already issued) / 2^22

At launch this gave about 4.76 GROX per block, and it falls by roughly half every 5.5 years of 60-second blocks. Transaction fees go to the miner in full on top of the base reward.

Premine: 5% (1,050,000 GROX). Paid once, at block 2, to the development fund address. It is a consensus rule checked by every node.

Development fund: 5% of every block's base reward. The other 95% goes to the miner. Fees are not shared. Every node rejects a block whose dev-fund output is missing or wrong.

Why no tail emission. Grox keeps a fixed, predictable supply: 21,000,000 GROX is the most that can ever exist, and every holder can rely on it. The reward falls slowly, so it stays meaningful for decades: about half of today's reward after 5.5 years, about a quarter after 11 years. Over that time, transaction fees are expected to carry a growing share of miners' income. This is a deliberate trade-off: Monero added a small permanent reward to secure its network long term. If Grox ever needs the same, it can only be introduced through a network upgrade that node operators choose to run.

Launch and distribution

The first Grox mainnet block was mined on November 9, 2026. The premine was paid at block 2, as the consensus rules require, and all other coins have been mined in public since then.

During the first days, some of the developer's own test mining was pointed at the development-fund address by mistake: about 2,300 GROX in blocks 757 to 6,464, before November 14, 2026. These coins stay in the development fund and follow the same rules as the rest of it. Anyone can verify them with the published view key.

Privacy

Grox inherits Monero's privacy stack, enabled for every transaction with no opt-out:

- **Stealth addresses:** each payment goes to a one-time address, so outsiders cannot link payments to a public address.
- **Ring signatures (CLSAG, ring size 16):** each spent input is mixed with 15 decoys, hiding which output was spent.
- **RingCT with Bulletproofs+:** amounts are hidden, while range proofs show no coins were created from nothing.

A wallet owner can share a view key to let others see incoming payments without the ability to spend them. Grox uses this for its development fund (see Transparency).

Network upgrade v1.2.0 (block 12,000)

The v1.2.0 hard fork activated at block 12,000 on November 17, 2026 and completed without a chain split. From that block, the 5% development-fund output must pay a dedicated wallet whose view key is public, instead of the original development-fund address.

The change made the development fund auditable by anyone: every coin it receives from block 12,000 onward can be checked with the published view key.

Mining

There are two ways to mine Grox, both free:

- **Solo:** the desktop wallet mines with one click against the user's own node, and every block found pays its full reward to that user.
- **Pool:** `pool.groxcoin.com:3333` runs P2Pool, a decentralized pool with a 0% fee. Each block the pool finds pays every contributing miner directly in that block's coinbase, so there is no pool wallet holding miners' funds and no minimum payout.

Grox XMRig, a build of XMRig 6.26.0 with rx/grox added and a 0% donation, is published with each release. Pool earnings for any address can be checked on the explorer's pool page.

Mining only with consent. Grox supports mining on hardware the miner owns or is allowed to use. The official wallet and Grox XMRig mine only when the user starts them, show what they are doing, and stop when asked. Grox does not support or distribute hidden or bundled miners.

Wallets and infrastructure

Component	What it does	Where
Desktop wallet	Node, wallet and one-click solo mining, English and Arabic	Windows and Linux, GitHub releases
Command-line tools	`groxd` node, `grox-wallet-cli`, `grox-wallet-rpc`	Same releases, with SHA256 checksums
Web wallet	Wallet in the browser; keys never leave the device	wallet.groxcoin.com
Block explorer	Blocks, transactions, network and pool statistics	explorer.groxcoin.com
Seed nodes	Three public seed nodes in Europe and the US, found through DNS seeds	Built into every node

The node, wallets and miner are open source. Releases are built by public GitHub Actions workflows, so anyone can check that a download matches the published code.

What the development fund pays for

The premine and the 5% development fund pay for running and building the network. Grox runs on scalable AWS cloud infrastructure rather than low-cost virtual servers, so the network stays available as it grows:

- **Network infrastructure:** seed nodes in Europe and the US, the public node behind the web wallet, the block explorer, the mining pool, content delivery and TLS.
- **Web presence:** domains and business hosting for the website and services.
- **Development and operations:** the developer's time building releases, wallets, the pool and tools, and running the network day to day.
- **Community rewards:** the 100,000 GROX reserve described below.

GROX has no market price yet, so the fund cannot cover these costs today. Every expense since launch, together with the development time, has been paid by the developer. The fund repays that investment over the long term, which is why it is part of every block rather than a single launch payment.

Transparency

The development fund is public by design. Its wallet's view key is published, so anyone can load it into a view-only wallet and see every coin it receives. A view key can never spend.

```
Address:  GDGSHJXsxp8Y3EnLmGMnMcjLs5Qry6H5vibokRCFxKzNbZkggGkNYjd4iHwoMcJkuQKrsVN1Yt7mQY
View key: bb0dd5b0061a6c00f23586a5f11c6b08dbd557369137240449d990c89fe59f02
```

Community reserve: 100,000 GROX. Moved from the premine to this wallet at block 4,211 and set aside for community rewards such as bounties, translations, tools and contests.

Governance and decentralization

Keys. The development fund wallet is held by the developer. Its income is public through the view key, and payments from the community reserve, such as bounties and contest prizes, are announced on the official channels. The fund will move to a multisignature wallet once the project has additional trusted maintainers.

Upgrades. Network rules change only through new software releases with a fixed activation height, announced in advance on the website and community channels, as with v1.2.0. A rule change takes effect only on the nodes that choose to run the new version.

Infrastructure. Today the developer runs the seed nodes, the block explorer, the public node behind the web wallet and the pool node. The node and wallet software is open source, so anyone can run a full node and mine solo without depending on these services. Community-run seed nodes can be added to the DNS seeds without a new release, and spreading the infrastructure across independent operators is a goal as the community grows.

Specification

Parameter	Value
Ticker	GROX
Codebase	Monero v0.18.5.4
Proof of work	rx/grox (RandomX v2 program, Grox salt)
Block time	60 s
Difficulty algorithm	LWMA, 90 blocks
Maximum supply	21,000,000 GROX, no tail emission
Decimals	11
Premine	5% (1,050,000 GROX, block 2)
Development fund	5% of each block's base reward
Coinbase maturity	60 blocks
Privacy	Stealth addresses, CLSAG rings of 16, RingCT with Bulletproofs+
Address prefix	G
Ports	P2P 19880, RPC 19881, ZMQ 19882

Links

- Website: groxcoin.com
- Source code and releases: github.com/ahafarag/grox-coin
- Explorer: explorer.groxcoin.com
- Web wallet: wallet.groxcoin.com
- Community: Discord, Telegram, X @grox_coin, Bitcointalk ANN

This document describes the Grox software and network as of the date above. It is not financial advice and makes no promise about the value of GROX. The source code is the final reference for every rule described here.

© 2026 Grox · groxcoin.com