Shear: Continuity-settled Proof of Work

Shear project
shear.digital · Version 1.0 (testnet) · Network magic shear-testnet-v2

Abstract

Shear is a CPU-mined ledger whose coin, SHE, is created when a block is found and not before. There is no premine and no sale of SHE by the developers. Privacy is the default: the rest-frame identity never appears on the book; holders offer a silent ID and the chain writes revolving dests. Proof of work is ShearHash-v2, a RandomX light-mode parameterisation. A found block closes exactly one SHE. Accepted hashes carry a small bonus paid to the hasher who produced them. The only programme allowed to mint extra SHE is The Reserve, a vortice in which holders lock coin, vote on that hash bonus, and earn a 400-day stake. This note states the project's goals and the architecture that carries them.

Keywords: Shear, SHE, ShearHash-v2, RandomX, continuity-tethered Flow, Vortex, vort1, The Reserve, CPU mining

1. Goals

Shear is built around a short list of decisions that are not supposed to drift.

- Proof of work only. Coin comes from hashing, not from an allocation, an auction, or a snapshot of some other book.
- CPU only. ShearHash-v2 is RandomX light. GPU and ASIC farms are not the intended surface.
- Private by default. Rest-frame shear1 never goes on chain. Holders offer she1. Settled dests are ssa1.
- One coin per block. The pot is 1 SHE. Votes do not move it. The Reserve oracle does not move it.
- Hashers keep their own bonus. Finding the block does not let anyone take another person's hashes.
- Programmes may move coin you already have. They may not print SHE, other than The Reserve's interest.
- No catalog of third-party programmes. A vortice is installed with a vort1 deploy key, or it is not installed.

The public sites — shear.digital, pool.shear.digital, explorer.shear.digital, mempool.shear.digital — are the face of the testnet. Mainnet is scheduled for 21:00 UK time on 11 September 2026. Until then the network magic stays shear-testnet-v2. Testnet balances can vanish. Treat them as a practice run.

2. Architecture

2.1 Three names, one holder

A wallet is sealed by a password. That password is the view secret. From it the wallet derives a rest-frame identity (shear1), a public silent ID (she1), and a revolving family of chain dests (ssa1). The rest-frame string is never a vout and never a miner login. The silent ID is what you hand to a payer or to the pool. The dest is what the book actually writes. The same (rest-frame, view secret,

index) always regenerates the same dest. Nodes reject a block that puts shear1 on the wire.

Optional memos travel as ciphertext. The public explorer reports only whether a memo is present. Plaintext stays in the two wallets that already know the dest.

2.2 Header, work, and time

Blocks are 128-byte little-endian headers: version, previous hash, merkle root of packed transactions, continuity root, Unix-millisecond timestamp, compact bits, nonce, and a base-fee field. Proof of work is ShearHash-v2 of that header, compared with the target implied by bits. The continuity root commits this round's hash samples. After a hundred confirmations the sample bodies may be pruned; the header, the coinbase, and every user transaction stay.

Resistance retargets with ASERT toward ninety seconds. Floor 14 bits, ceiling 256 bits. Heaviest valid chain wins. Consensus spendable depth is six confirmations, counting the including block as one. Merchant desks may ask for more; they may not ask for less than six.

2.3 ShearHash-v2

ShearHash-v2 is RandomX v1.2.3 in light mode: 128 MiB cache, no 2 GiB DRAM dataset copy. The cache key is bound to previous hash, continuity root, merkle root, and bits, so it rebuilds every block and does not include miner identity. Mining may JIT if the digest matches the interpreter on the self-test vector. Verification is the light-mode interpreter. Wire algorithm name is ShearHash. Personalisation is ShearHash-v2. The official hasher is ShearK-Miner 1.5.

2.4 Emissions

Three paths, and they do not stand in for each other. First, the block pot: exactly 1 SHE in the coinbase. Solo, the finder takes it. On the public pool it is split by proven work in that round (PROP); the pool may keep one percent of the pot. Second, the hash bonus: one protocol unit, 10^-11 SHE, for each accepted hash, paid to the miner who produced it. Public pages show nine fractional digits so a single hash looks like dust; the unit is still written. Third, The Reserve: interest on staked SHE at the oracle rate, minted only by programme id shear-reserve-v1. Any other vortice that wants to pay rewards must top them up from coin already in circulation.

2.5 Flow and levy

Continuity-tethered Flow is how SHE moves between dests. A send quotes a levy L from current mempool depth. L_base is the greater of 100 units and two basis points of the amount; surge rises with waiting bytes. Lock and vote in The Reserve pay the same levy. Withdraw of Reserve principal does not. The Continuum dest pays L. Empty-mempool floor is 100 units.

2.6 Wallet

The wallet is a six-tab app. Continuum is spendable balance, silent ID, and the six-slice pending pie. Flow is send and receive. Resistance is a public CTF CLI. Vortex is where programmes live. Shearview is the holder's own explorer. Closure holds the rest-frame string and the shewall.bin

export. The file plus the password restore the same wallet. There is no paper seed. Lose the password and the file does not open.

2.7 Vortex, vortices, and vort1

Vortex is a drawer, not a chain of contracts you browse. Each programme in it is a vortice. The Reserve is already installed. Anyone else hosts their own bytes. A Shear node mints a vort1 deploy key that names the origin URL and pins a hash of those exact bytes. The holder pastes the key; the wallet fetches the origin, checks the pin, and deploys locally. No key, no programme. If the hosted file changes, the old key stops working. Third-party vortices cannot mint SHE, cannot ask for a password, and cannot move the 1 SHE pot.

2.8 The Reserve

The Reserve is the first vortice and the only one allowed to mint. A holder locks SHE into a personal portal. π SHE (about 3.14159265358 SHE) unlocks one vote for the current 400-day epoch. The first qualifying deposit opens the inaugural epoch; it is not started by an operator clock. Staked principal earns the oracle's 400-day APR. Idle coin earns nothing. Inside the last 99 days, new deposits still lock and may vote, but they sit idle. A vote may raise the hash bonus by one unit, lower it by one unit, or leave it. The pot is not on the ballot. Each portal votes once. At epoch end the unique plurality of the three piles moves the live bonus, or a tie leaves it. Principal and accrued interest return to Continuum on a signed withdraw. Miss the window and previous-epoch rewards stay claimable; a new epoch does not confiscate them.

2.9 Pool, explorer, node

The public pool is stratum in front of a validating node, not the ledger. Jobs are full 128-byte header templates. Shares that are not a valid header hash mint nothing. Stratum listens on pool.shear.digital:1111. Login is she1.worker. The explorer paints confirmed blocks and public amounts. It does not show ciphertext and it does not show rest-frame strings. A node is the book: append, verify, P2P, and the GATE that lets native Flow and pinned Reserve bytecode land in the same block model.

3. What this note is not

This is a testnet preprint. It is not a prospectus and it is not a promise that testnet coin will exist on mainnet. Constants here match the live fingerprint: 1 SHE pot, 10^-11 SHE per accepted hash, six-confirmation spendable floor, ASERT 90 s, ShearHash-v2 light, chain id 2701 for pool withdraw signatures. How-to pages — installing the wallet, pointing ShearK at the pool, opening The Reserve, minting a vort1 key — live at docs.shear.digital. The clients are the WALLET, MINER, and NODE buttons on shear.digital.

She is private.

Correspondence: shear.digital. Software under the MIT License, Copyright 2026 Shear. RandomX is vendored from tevador/RandomX v1.2.3 (BSD). Official miner ShearK-Miner 1.5. Wallet pin at publication: 0.25.