

# hashless

bitcoin's issuance schedule on ethereum, mined  
with eth instead of hashing

|          |                                                      |
|----------|------------------------------------------------------|
| site     | hashless.money                                       |
| contract | the address on hashless.money, verified on etherscan |
| formulas | hashless.money/spec                                  |

---

## abstract

hashless is an erc-20 on ethereum whose supply follows bitcoin's schedule exactly: 50 coins a block, halving every 210,000 blocks, 33 eras, at most 20,999,999.9769 coins, 8 decimals. there is no proof of work. a block is mined by paying eth for it, at a price set by how far mining runs ahead of one block per ethereum block.

most of what miners pay stays in the contract as a reserve. any holder can burn coins for their share of it at any time, less 1%. the reserve per coin, the floor, can only go up. the contract has no owner and can't be changed.

---

## 1 why

bitcoin's issuance is the best-known supply rule there is: a fixed amount per block, cut in half on a fixed schedule, a hard cap. most tokens on ethereum have no issuance at all. the whole supply exists at deploy, and whoever deploys decides who gets it.

hashless keeps the rule and changes the work. mining bitcoin costs electricity, and the electricity is gone once it's spent. mining hashless costs eth, and the eth stays: it becomes the reserve behind every coin. nobody is handed coins, and every coin in circulation was paid for at the price of its block.

---

## 2 the schedule

|            |                                                      |
|------------|------------------------------------------------------|
| subsidy    | 50 coins a block in era 0, halved every era          |
| halving    | every 210,000 blocks                                 |
| eras       | 33; the subsidy is 0 after that                      |
| max supply | 20,999,999.9769 coins                                |
| decimals   | 8                                                    |
| genesis    | block 0, 50 coins to 0x...dEaD, which can never move |
| target     | one block per ethereum block, every 12 seconds       |

at one block per ethereum block an era takes 29.2 days instead of four years, and the whole schedule fits in about 2.6 years instead of 132. half of all coins come out in the first era, three quarters by the end of the second. halvings go by height, not by date: when mining runs behind, they come later, and when it runs ahead, sooner.

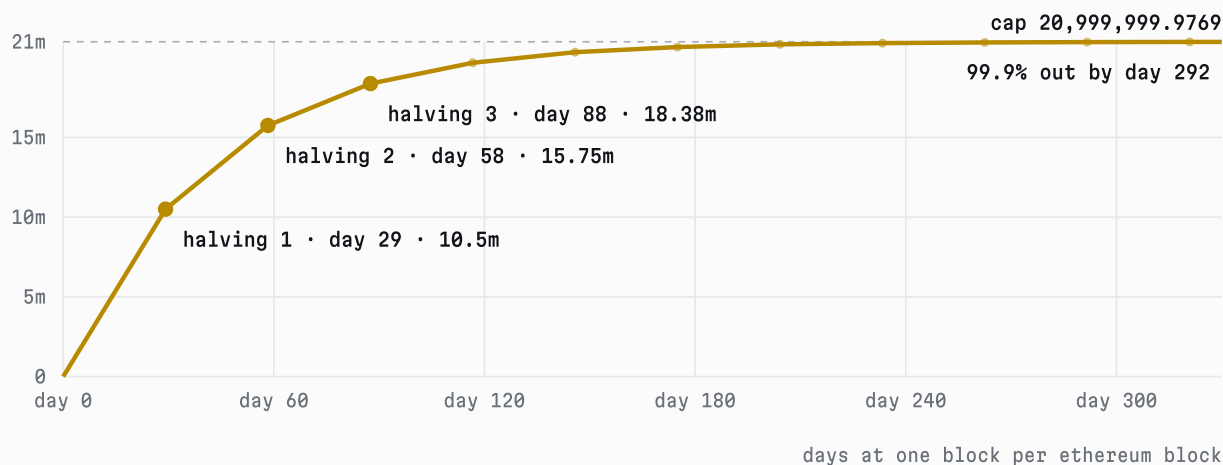


figure 1. supply over time if mining keeps exactly one block per ethereum block.

### 3 the price of a block

the price depends on one number, the lead: blocks mined so far minus ethereum blocks since the schedule started. mining exactly on schedule keeps it near zero. the difficulty is the price of a block over its floor value (section 4):

$\text{difficulty} = 2^{(1 + \text{lead} / 7200)}$       never under 1  
 $\text{price of a block} = \text{floor} \times 50 \times \text{difficulty}$       per block in era 0

7,200 ethereum blocks is about a day. on schedule a block costs twice its floor value. every day of lead doubles that, every day behind halves it, and it stops at 1: below that, a new coin would bring in less eth than the coins already out are backed by. when mining is more than a day behind, the schedule waits instead of getting any cheaper.

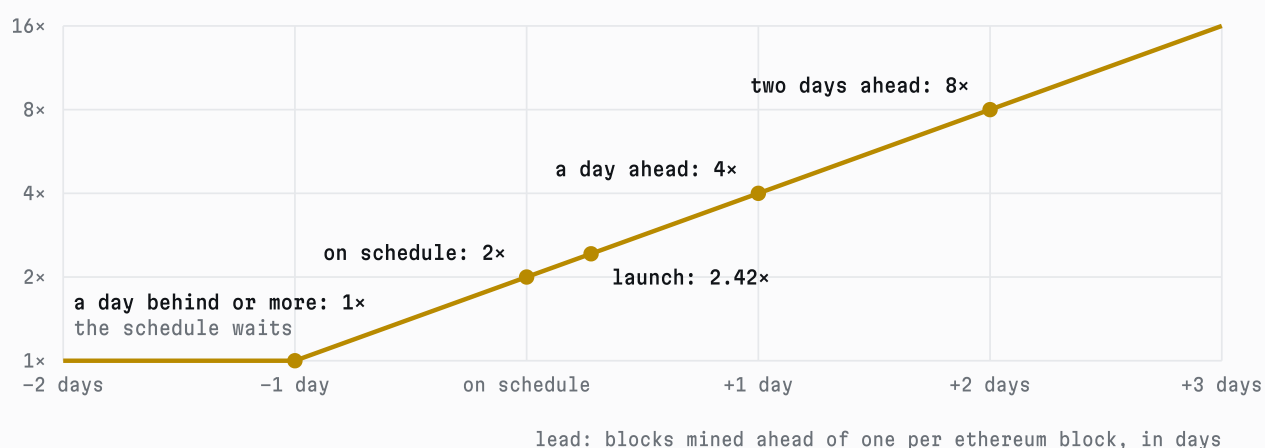
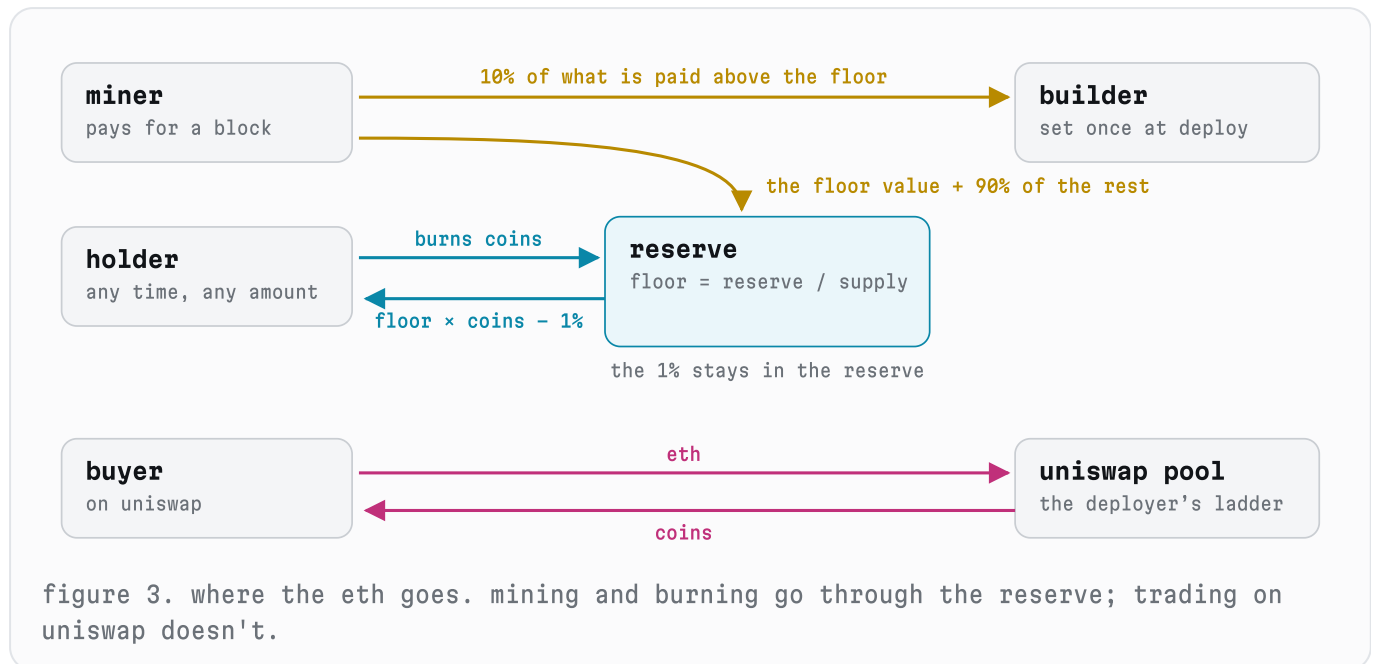


figure 2. difficulty against the lead. the launch starts 2,001 blocks ahead, at 2.42x.

nobody sets the price. if nobody mines, it halves every day until it reaches the floor. if many people mine at once, every block they take pushes it up. a run of blocks in one transaction costs the sum of each block at its own lead; the exact formula is in the spec.

## 4 the reserve and the floor

everything paid for mining goes into the reserve, except the builder's cut (section 5). the floor is the reserve divided by the supply, in eth per coin. any holder can burn coins at any time: the contract pays the floor for each one, less 1%, and the 1% stays in the reserve.



the floor never goes down in eth:

- a block never costs less than its floor value, so mining adds at least the floor per new coin.
- a burn takes out at most the floor per coin, and the 1% fee raises it.
- the builder's cut was never part of the reserve, so claiming it changes nothing.
- eth sent to the contract directly joins the reserve.

in eth, the most a holder can lose is what they paid above the floor, plus 1%, as long as the contract has no bug. in dollars, the floor moves with eth.

## 5 the builder

a tenth of whatever is paid above the floor goes to one address, the builder, set once at deploy. on schedule (difficulty 2) that's 5% of a payment, at difficulty 4 it's 7.5%, and at difficulty 1 it's nothing. the cut waits in the contract until someone calls `claim()`, which anyone can, and it goes only to the builder.

## 6 launch

**genesis.** the deploy mines block 0: 50 coins to 0x...dEaD, paid for with 0.00002 eth, which is the first reserve. those coins can never move, so the supply never reaches zero. the hash of the ethereum block before genesis is stored in the contract: nothing could have been mined before it.

**seed.** in the same transaction the deployer mines 2,000 blocks, 100,000 coins, at the price anyone would pay at that moment: about 0.088 eth in all. that puts the lead at +2,001, and the next block at 2.42 times the floor.

**closed until the pool.** after the deploy, mining stays closed and the clock stands still until uniswap v4 holds coins. only the deployer has coins that can move, so the deployer decides when, and however long it takes, the price of the next block stays where the deploy left it.

**the pool.** the 100,000 seed coins go into a uniswap v4 pool, eth / hashless, 1% fee, no hook, as a ladder of one-sided positions: coins only, no eth. the bottom of the ladder is the price of the next block, never above it and never under the floor. a pool above the mining price would only sell coins that mining sells for less. one contract opens the pool, adds every rung and opens mining in the same transaction, so the pool never trades without the coins in it.

| rung | market cap at launch supply     | coins  | share |
|------|---------------------------------|--------|-------|
| 1    | about \$500 (the ask) to \$100k | 40,000 | 40%   |
| 2    | \$100k to \$500k                | 25,000 | 25%   |
| 3    | \$500k to \$2m                  | 18,000 | 18%   |
| 4    | \$2m to \$8m                    | 11,000 | 11%   |
| 5    | \$8m to \$20m                   | 6,000  | 6%    |

market caps here are at the launch supply of 100,050 coins, with eth at \$2,484. mining adds coins, so the same price shows a higher market cap later. the positions belong to the deployer: as the price climbs through them, the coins sell, and the eth buyers pay collects in them. that eth is the deployer's, not the reserve's.

## 7 two ways to get coins

- **mine** on the site: you pay the price of the next block, and at least 90% of it goes into the reserve every holder shares.
- **buy** on uniswap: you pay whoever sells, at first the deployer's ladder, later anyone.

the two stay close. when the pool trades above the price of mining, mining and selling into the pool pays, and the eth paid for mining lands in the reserve. when the pool trades under the floor less 1%, buying from it and burning pays. nobody has to run that arbitrage, but anyone can, and the site shows both prices side by side.

## 8 numbers at launch

|                                      |                                                                     |
|--------------------------------------|---------------------------------------------------------------------|
| genesis                              | 0.00002 eth, 50 coins to 0x...dEaD                                  |
| seed                                 | 2,000 blocks, 100,000 coins, about 0.0882 eth                       |
| reserve after the seed               | about 0.0834 eth                                                    |
| supply                               | 100,050 coins                                                       |
| floor                                | about 0.000000834 eth per coin                                      |
| price of the next block              | about 0.00000202 eth per coin, 2.42× the floor                      |
| pool opens at                        | the ask, about \$500 market cap                                     |
| if nobody mines                      | the ask reaches 2× in about 7 hours and the floor in about 31 hours |
| a buyer at the ask who burns at once | gets back about 41%                                                 |

---

## 9 what nobody can do

- change the contract. it has no owner, no admin functions, no proxy, no pause and no upgrade path.
- take eth out of the reserve, other than by burning coins. that includes the deployer.
- move the price with an oracle. there is none: the price comes from the lead and the reserve, and opening reads only the token's own record of what uniswap's pool manager holds.
- mint coins outside the schedule. every coin comes from a block, and every block is paid for.

what the deployer does have: the builder's cut, and the ladder positions, which it can collect fees on or take out like any liquidity provider.

---

## 10 risks

- not audited. the contract is tested with unit, fuzz and invariant tests and a run through all 33 eras, but it can't be changed, so a bug couldn't be fixed.
- the price above the floor is demand. if nobody mines or buys, the price of the next block halves every day until it reaches the floor, and the pool has no reason to stay above it.
- the floor is in eth. its dollar value moves with eth.
- the ladder is the deployer selling: every buy from the pool is the deployer's coins until the rungs run out.
- mining is a public transaction and can be front-run like any purchase. the site sends the quote plus a margin, and the difference comes back in the same transaction.
- a large holder can push the schedule ahead by mining and burning in one transaction. it costs them part of the premium and raises the floor for everyone, but it brings the next halving closer.

not audited. nothing here is advice. the contract is the source of truth: its address and source.