# Opacra: a private coin built for a young chain

The Opacra Project. Version 1.0, November 2026.

**Abstract.** Opacra (OPCA) is a proof-of-work cryptocurrency with its own blockchain, forked from Monero v0.18.5.1 and kept current with Monero's fixes up to v0.18.5.4. It keeps Monero's privacy layer unchanged and hides the sender, receiver and amount of every payment. Opacra changes the block time, emission, proof of work and difficulty algorithm, and adds a development fund enforced by consensus. It also adds protections designed for a new chain's early period. This paper describes those changes. The full specification is in the source repository, and where the two differ the code and specification are authoritative.

## 1. Motivation

Monero's privacy design has protected real payments for over a decade. Opacra has no reason to replace it, and doesn't invent any cryptography. A new chain has different needs from an established one, so Monero's parameters don't carry over directly. Opacra's work is in timing, economics and protection: making received coins spendable sooner, funding development in a way anyone can audit, launching without a head start, and staying strong from the first block.

## 2. Privacy

Transaction format, signatures and proofs behave exactly as in Monero v0.18.5.4.

- **Sender.** CLSAG ring signatures. Ring size is enforced at exactly 16.
- **Receiver.** Stealth addresses give every payment a one-time output key. View tags speed up wallet scanning.
- **Amount.** RingCT hides amounts, and Bulletproofs+ range proofs let nodes verify them without seeing them.
- **Origin.** Dandelion++ relays a new transaction through a few nodes before it spreads.

Privacy applies to every payment by default. Transaction fees, sizes and block times remain public.

## 3. Selective disclosure

An owner can reveal specific facts without giving up spending power. A payment proof shows that a payment reached an address and binds that to a message such as an invoice number. A reserve proof shows that a balance exists without revealing its history. A view key gives a view-only wallet sight of incoming payments. These are Monero's existing tools. Opacra treats them as a central feature because they let businesses and auditors work with a private coin.

## 4. Parameters

| | |
|---|---|
| Block target | 30 seconds (2,880 blocks a day) |
| Spendable age | 10 blocks, about 5 minutes |
| Coinbase maturity | 60 blocks, about 30 minutes |
| Ring size | 16, enforced exactly |
| Future time limit | 180 seconds (Monero: 7,200) |
| Median-time-past window | 11 blocks (Monero: 60) |
| Penalty-free block size | 75 kB, scaled to match Monero per unit of time |
| Decimals | 12 |
| Address prefixes | Pa standard, Ps subaddress, Pi integrated |
| Ports | 29960 P2P, 29961 RPC, 29962 ZMQ |

## 5. Proof of work

Opacra uses RandomOPCA, which is RandomX with its own Argon2 salt, `"RandomOPCA\x01"`. RandomX's documentation asks every implementation to choose a unique salt. The algorithm's design and memory requirements are unchanged, so it stays suited to ordinary CPUs. Every hash differs from Monero's `rx/0`, so Monero's miners, pools and rental markets can't mine Opacra without Opacra-specific software.

## 6. Difficulty

Monero's 720-block window with a 15-block lag takes about a day to react, which invites profit-switching and rented hash power on a small chain. Opacra uses LWMA-1 with N = 60, a linearly weighted moving average that gives recent blocks the most weight. Blocks 1 to 12 use a startup difficulty of 10,000.

```
L      = sum over i=1..N of  i * min(6T, t_i - p_(i-1))
L      = max(L, N^2 * T / 20)
D_next = (C_N - C_0) * T * (N+1) * 99 / (200 * L)
```

In simulation over 20 random runs, a 10× jump in hash rate for 200 blocks brought difficulty to 80% of the new level after about 61 blocks, with a mean block time of about 30.9 seconds. After a sudden 90% drop, the

next 60 blocks averaged about 106 seconds, and difficulty returned to within 10% after 110 to 165 blocks.

## 7. Emission

```
base_reward = max( (MONEY_SUPPLY - generated) >> 22 , TAIL_EMISSION_REWARD )

MONEY_SUPPLY         = 10,000,000 OPCA
TAIL_EMISSION_REWARD = 0.05 OPCA
```

There is no premine, no ICO and no slow start. Block 1 pays the full reward of about 2.384 OPCA, because full rewards attract the most hash power in the first week. The main curve has a half-life of 2.76 years.

| After | Emitted, OPCA | Share of 10M |
|---|---|---|
| 1 year | 2,218,201 | 22.2% |
| 2 years | 3,944,359 | 39.4% |
| 3 years | 5,287,621 | 52.9% |
| 5 years | 7,146,352 | 71.5% |
| 10 years | 9,185,669 | 91.9% |
| 15 years | 9,767,618 | 97.7% |

Rewards reach the 0.05 OPCA floor at about block 16,219,000, roughly 15.4 years in. The tail then adds about 52,600 OPCA a year, about 0.5% at that point and falling. Transaction fees are added to the reward and go to the miner.

## 8. Development fund

5% of each block's subsidy, from block 1 with no end date, is paid to a fixed address as the last coinbase output. That comes to about 110,000 OPCA in the first year and about 500,000 OPCA over the main curve. Blocks that don't follow the rule exactly are rejected.

The fund output uses a per-block transaction key derived from the height and the previous block's hash:

```
r_f = Hs("OpacraDevFund" || height || previous block hash)
R_f = r_f * G
output key = Hs(8 * r_f * A || n-1) * G + B      (fund address A, B)
```

Because the key is fixed by the chain, no miner can choose, reuse or burn the output, and nobody can plant a decoy with the same key in advance. The fund's secret view key is published, so anyone can audit what it receives. Its spends are visible through their change outputs, which is intended. The miner's own output keeps its random key and its privacy.

A public view key would normally expose which outputs are spent, and those would make poor decoys. So nodes mark fund outputs and wallets never choose them as ring members, which keeps the fund's openness from weakening other users' rings. The fund's spending keys are held offline.

## 9. Fair launch

1. The launch time is announced a week ahead, in UTC.
2. The genesis block is made on launch morning, with that day's headline in its message, and is kept private until mining opens. The headline only proves anything because the genesis stays unknown until launch.
3. The genesis output key is a "nothing up my sleeve" point derived from the message, so nobody has ever held a key for it.
4. Consensus rejects any block after genesis dated before the launch time, on the main chain and on side chains. With the 3-minute future time limit, no node accepts block 1 earlier than 3 minutes before launch.

## 10. Protecting a young chain

### Side-chain difficulty floor

Once the main chain is past 122 blocks, a side-chain block whose required difficulty is below a quarter of the main chain's reference difficulty is refused. Without this, a chain forked from far back could claim hours of slow blocks, walk its difficulty down and flood nodes with nearly free blocks. A competing chain that could really win never needs such a low difficulty, so honest reorganisations of any depth still work.

### Emergency checkpoints

The project can publish "block H has hash X" as DNS TXT records, which nodes read about every 5 minutes. A node uses them only if checkpoints.opacra.org and checkpoints.opacra.com both answer, both pass DNSSEC validation and both hold the same set. Each set carries a serial number, because DNSSEC proves an answer was signed but not that it's current. Nodes refuse lower serials, so an older signed answer can't be replayed to lift a checkpoint.

Seeds, pools and exchanges enforce checkpoints. Home nodes warn and can opt in. A node that rolls back keeps the removed blocks as a side chain, so a wrong record costs no blocks once it's corrected. Home enforcement is planned as the default once the two domains are at separate registrars with different people holding the logins.

### Monero behaviour removed or changed

Monero's hard-coded exceptions for its block 202612 are removed, since they would let any block at that Opacra height skip proof of work. Monero's checkpoints are removed. The reward function was rewritten because Monero's per-minute scaling truncates to zero below 60-second blocks. A block that's only ahead of a node's clock is rejected for now without penalising the peer, so a node with a slow clock can't end up banning honest peers.

## 11. Verification

`opacra-audit` checks every block against rules recomputed from the specification rather than taken from the node's code: chain links, timestamps, difficulty, coinbase form, rewards, the fund payment and total coins created. It needs only the Python standard library and a synced node. It was tested against ten kinds of tampering, and each was caught.

On a private 3-node network running mainnet rules, 30 of 30 functional checks passed on 31 October 2026, including a chain split that re-converged and a replay of all 128 blocks with no mismatches. Real-world conditions are covered by the public testnet, which has run mainnet's rules since 26 October 2026. Releases are signed with the Opacra release key, fingerprint D861 7219 6FEC AAB6 84F5 B3FD CB65 D212 D0B1 162B.

## 12. Network maturity

Like any new chain, Opacra gets stronger as it grows. A few practical notes apply in its early period.

- **Confirmations.** We recommend waiting 20 blocks, about 10 minutes, before treating a payment as final, and 120 blocks, about an hour, for large amounts or exchange deposits.
- **Anonymity set.** Ring signatures draw on past outputs, so privacy grows as the chain is used. Wallets need about 100 blocks of coinbase outputs before 16-member rings can be formed.
- **Network privacy.** The nodes a wallet connects to can see its IP address, but not the amount, the receiver or a balance. More public nodes spread this out, and an optional Tor connection is planned.
- **Infrastructure.** Mainnet launches with two seed nodes, in Europe and the US, and more at other providers are planned.
- **Wallets.** Command-line and RPC wallets ship at launch, with a desktop wallet planned. Windows builds aren't code-signed yet.

## 13. Future work

Planned after mainnet are a public mining pool, a desktop wallet, a bug bounty, an optional Tor connection and seed nodes at other providers. Two longer-term options are under consideration. FCMP++, Monero's planned replacement for 16-member rings, could be adopted through a network upgrade once it's released and audited. Merge mining with Monero could further strengthen the chain's security.

## References

- Opacra technical specification
- Emergency checkpoints
- Chain audit
- Test report
- Monero source code