# FixedCoin

Technical Whitepaper | Core v30.0.0

7 November 2026 | Mainnet edition

## One network. A defined activation point.

FixedCoin (FIX) is a peer-to-peer currency secured by independent SHA-256 proof of work. Its software derives from Bitcoin Core, with FixedCoin-specific network parameters, monetary rules and difficulty adjustment.

Core v30 introduced a corrected ASERT calculation and a longer mining reward schedule. Both activated at **block 52,560**, together with the change in the monetary limit from **10,000 to 21,000 FIX**. Earlier blocks continue to follow their historical rules.

| Before block 52,560 | Activation block 52,560 | Current rules after block 52,560 |
|---|---|---|
| Historical issuance and difficulty rules remain valid for historical blocks. | New monetary rules began; difficulty exactly matched block 52,559. | ASERT V2 adjusts every block; the v30 reward schedule is active. |

**The activation is complete.** Mainnet reached block 52,560 on **16 October 2026 at 08:21:26 UTC**. The activation block hash is `000000000000000760196d78b7e58312478d44c1ca9e2f7cf86e00872321b0c6a`. Software and wallet improvements became available when v30 was installed; the monetary and difficulty changes became active at the defined block height. [8]

FixedCoin Core v30.0.0 is the mandatory baseline for the active mainnet rules. Nodes, mining pools, exchanges and services must use v30 or a later compatible release. Older software does not implement the active consensus rules and can follow an incompatible chain.

## Contents

1. Network parameters and activated transition

2. Historical monetary rules

3. The v30 emission schedule

4. Difficulty adjustment

5. Validation, frozen output and wallets

6. Current operator guidance and references

7. Appendix A: exact consensus mathematics

This document describes the rules in the published v30.0.0 source. The source code defines the exact validation behavior; the mathematical target formula below is explanatory. All monetary values are expressed in FIX unless stated otherwise. [1]

# 1. Network parameters and activation

## What changes, and what stays the same

| Parameter | Historical mainnet | Mainnet from block 52,560 |
|---|---|---|
| Monetary limit | 10,000 FIX | 21,000 FIX |
| Subsidy schedule | 1 FIX base; halving every 4,200 blocks; special block-1 reward | 0.10466639 FIX initially; halving every 52,560 blocks |
| Difficulty adjustment | Initial retarget rules; legacy FIX ASERT from block 1,000 | ASERT V2, with exact continuity at activation |
| ASERT half-life parameter | 172,800 seconds (48 hours) | 86,400 seconds (24 hours) |
| ASERT reference | Block 999 target, with its parent's timestamp in the legacy calculation | Block 52,559 target and timestamp on the branch being validated |
| Frozen-output rule | Active from height 628 | Unchanged; no expiry or v30 exception |

The cap is a monetary bound, not a measurement of coins in circulation. Mining rewards, integer rounding, unclaimed rewards and unspendable outputs determine how much can actually be issued or spent. [2, 3]

## Shared network properties

| Property | Value |
|---|---|
| Ticker / precision | FIX / 100,000,000 base units per FIX |
| Proof of work / target interval | SHA-256 / 600 seconds |
| Mainnet P2P / RPC ports | 24768 / 24767 |
| Address formats | Legacy, P2SH, native SegWit and Taproot; witness prefix `fix` |
| Coinbase maturity | 100 blocks |
| Maximum block weight | 4,000,000 weight units |
| Chain identity | Existing genesis and transaction history preserved |

Ports are defaults, not an instruction to expose RPC publicly. SegWit and Taproot remain enabled. Coinbase maturity is a consensus rule; the number of confirmations required for an ordinary payment is a recipient or exchange policy, not a universal six-block requirement. [2, 6]

## Height, not a timer

v30 did not require a miner-signaling threshold or a manual activation flag on mainnet. Every block is checked against the rules for its height. Reorganizations and reindexing retain the old rules below 52,560 and apply the new rules from that height. The same genesis, addresses and existing balances remain in use.

This schedule is specific to mainnet. Public testnet and signet retain their existing parameters. Regtest provides separate activation settings for isolated testing. [2]

# 2. Historical monetary rules

## The period before activation

Before block 52,560, rewards follow the historical schedule. The base reward is 1 FIX, halved every 4,200 blocks using integer right shifts. Block 1 is a special case with a 1,600 FIX reward. The genesis block contains a 1 FIX reward that cannot be spent because its transaction was not added to the spendable UTXO database. Both are included in the historical issuance budget. [2, 3]

```
For h < 52,560, in base units:
  era = floor(h / 4,200)
  base = 1600 * 100000000 if h == 1, else 100000000
  subsidy(h) = base >> era  (zero for era >= 64)
```

| Block heights | Ordinary reward per block (FIX) |
|---|---|
| 0-4,199 | 1.00000000; block 1 instead permits 1,600.00000000 |
| 4,200-8,399 | 0.50000000 |
| 8,400-12,599 | 0.25000000 |
| 12,600-16,799 | 0.12500000 |
| 16,800-20,999 | 0.06250000 |
| 21,000-25,199 | 0.03125000 |
| 25,200-29,399 | 0.01562500 |
| 29,400-33,599 | 0.00781250 |
| 33,600-37,799 | 0.00390625 |
| 37,800-41,999 | 0.00195312 |
| 42,000-46,199 | 0.00097656 |
| 46,200-50,399 | 0.00048828 |
| 50,400-52,559 | 0.00024414 |

At the target cadence, a 4,200-block interval is about 29 days. Actual duration depends on block production. A node already running v30 still enforces this table for all blocks below activation.

## The budget carried into v30

The sum of permitted subsidies from genesis through block 52,559 is **9,997.47652440 FIX**. This is a calculated allowance, not a claim that every reward was collected or that this amount circulates. It includes the unspendable genesis reward and does not subtract frozen outputs, lost keys or unclaimed rewards.

The future budget is **21,000 - 9,997.47652440 = 11,002.52347560 FIX**. v30 uses this historical allowance to determine the new reward; it does not use an explorer's rounded supply figure or the current UTXO balance. Transaction fees are transfers of existing coins, not new subsidy. Appendix A gives the exact base-unit calculation. [3]

# 3. The v30 emission schedule

From block 52,560, the initial subsidy is **10,466,639 base units (0.10466639 FIX)**. It is the largest integer reward whose complete halving schedule fits the remaining budget. The reward halves every 52,560 blocks, rounding down to the nearest base unit. [3]

```
For h >= 52,560:
  k = floor((h - 52,560) / 52,560)
  subsidy(h) = floor(10466639 / 2^k)  (in base units)
```

The table numbers schedule periods from 1, while the formula uses `k = 0` for the first period. The subsidy becomes zero when the integer result falls below one base unit.

| Era | Block heights | Reward (FIX) | Cumulative permitted FIX |
|---|---|---|---|
| 1 | 52,560-105,119 | 0.10466639 | 15,498.74198280 |
| 2 | 105,120-157,679 | 0.05233319 | 18,249.37444920 |
| 3 | 157,680-210,239 | 0.02616659 | 19,624.69041960 |
| 4 | 210,240-262,799 | 0.01308329 | 20,312.34814200 |
| 5 | 262,800-315,359 | 0.00654164 | 20,656.17674040 |
| 6 | 315,360-367,919 | 0.00327082 | 20,828.09103960 |
| 7 | 367,920-420,479 | 0.00163541 | 20,914.04818920 |
| 8 | 420,480-473,039 | 0.00081770 | 20,957.02650120 |
| 9 | 473,040-525,599 | 0.00040885 | 20,978.51565720 |
| 10 | 525,600-578,159 | 0.00020442 | 20,989.25997240 |
| 11 | 578,160-630,719 | 0.00010221 | 20,994.63213000 |
| 12 | 630,720-683,279 | 0.00005110 | 20,997.31794600 |
| 13 | 683,280-735,839 | 0.00002555 | 20,998.66085400 |
| 14 | 735,840-788,399 | 0.00001277 | 20,999.33204520 |
| 15 | 788,400-840,959 | 0.00000638 | 20,999.66737800 |
| 16 | 840,960-893,519 | 0.00000319 | 20,999.83504440 |
| 17 | 893,520-946,079 | 0.00000159 | 20,999.91861480 |
| 18 | 946,080-998,639 | 0.00000079 | 20,999.96013720 |
| 19 | 998,640-1,051,199 | 0.00000039 | 20,999.98063560 |
| 20 | 1,051,200-1,103,759 | 0.00000019 | 20,999.99062200 |
| 21 | 1,103,760-1,156,319 | 0.00000009 | 20,999.99535240 |
| 22 | 1,156,320-1,208,879 | 0.00000004 | 20,999.99745480 |
| 23 | 1,208,880-1,261,439 | 0.00000002 | 20,999.99850600 |
| 24 | 1,261,440-1,313,999 | 0.00000001 | 20,999.99903160 |

Cumulative values include the historical allowance. Subsidies become zero at **1,314,000**; transaction fees remain available to miners. Total permitted subsidies are **20,999.99903160 FIX**, leaving **0.00096840 FIX** below the cap.

Each era lasts approximately one year at the 600-second target, not a guaranteed calendar year. There is no one-time allocation, new team reserve or developer levy at activation. Existing balances are not reduced, but their share of issued supply decreases as additional coins are mined. The longer reward schedule supports independent mining; it does not guarantee profitability or sufficient hashpower.

# 4. Difficulty adjustment

## Historical validation remains historical

The initial mainnet difficulty rules use a 1,800-second target timespan and 600-second spacing, giving a three-block retarget interval. From height 1,000 through 52,559, the legacy FIX ASERT implementation uses block 999's target and its parent's timestamp, with a 172,800-second half-life parameter. [2, 4]

That historical implementation has different arithmetic from the ASERT reference algorithm. v30 preserves it for earlier blocks rather than recalculating history with corrected arithmetic. Its legacy negative-fraction, scaling and overflow behavior must not be treated as the v30 algorithm.

## Exact continuity at block 52,560

```
nBits(52,560) = nBits(52,559)
```

The compact target field is copied exactly at activation. The new calculation then anchors to block 52,559 on the branch being validated. It carries no timing debt from the old block-999 reference. This avoids a reset caused by switching algorithms; it does not guarantee that the inherited difficulty already matches the available hashpower.

## The V2 response after activation

For a candidate block at height h > H, where H = 52,560, let T_ref be the decoded target of block H-1 and t(k) the timestamp of block k. The explanatory relationship is:

```
time_error = t(h-1) - t(H-1) - 600 * (h-H)
next_target approximately = T_ref * 2^(time_error / 86400)
```

A larger target means lower difficulty. Blocks ahead of the target schedule produce a negative time error and higher difficulty; blocks behind it produce a positive time error and lower difficulty. The 24-hour half-life is the response scale: adjustment is calculated for each block, not once per day.

Consensus uses deterministic integer arithmetic, not floating-point exponentiation. V2 uses a 16-bit fractional exponent, floor decomposition for negative exponents, the ASERT polynomial approximation, and a 320-bit multiplication intermediate. It bounds the result between 1 and the proof-of-work limit, then encodes the compact target. Appendix A reproduces the exact calculation; `CalculateASERTV2` remains the authoritative implementation. [4]

## Reorganizations and limits

The anchor is looked up on the branch being validated. A reorganization across activation can therefore select a different H-1 anchor; blocks below H still use the historical path. Missing or invalid V2 anchors are errors, not a reason to silently substitute minimum difficulty.

Difficulty adjustment cannot guarantee ten-minute intervals, prevent every hashpower oscillation or eliminate reorganization risk. FixedCoin has its own mining participation and security budget; using SHA-256 and Bitcoin-derived code does not give it Bitcoin's aggregate network security.

# 5. Validation, frozen output and wallets

## The existing frozen output

From spending height **628**, compliant nodes reject any transaction that spends this exact outpoint:

```
Transaction:
53968570e24004c7e1ec0b199766a4c088c219f2c319c7f43b6af74c69894147
Output index: 0
```

The public explorer reports **1,604.85615714 FIX** for this output. This amount is an observation of the referenced transaction; the consensus rule identifies the transaction ID and output index, independently of amount or address. [5, 8]

| Rule | Behavior before and after v30 activation |
|---|---|
| First rejected spending height | 628, inclusive |
| Rejection reason | `bad-txns-frozen-utxo` |
| Expiry | None in the published rules |
| Other outputs at the same address | Not frozen by this outpoint-specific rule |
| Effect of the new supply limit | No unlock, deduction or replacement issuance |

The input check applies in mempool admission and block validation, including reindexing and reorganizations. Freezing does not delete the output from the UTXO database. The funds remain part of historical issuance and are not reissued. This rule is separate from the special 1,600 FIX reward at block 1.

## Supply reporting

Maximum supply, cumulative permitted subsidies, actual issuance and circulating supply are different quantities. A UTXO total can include immature and frozen outputs while excluding genesis and outputs not in the UTXO set. It is not a circulating-supply RPC. Unclaimed subsidies, unspendable outputs and fees also require distinct accounting. Lost private keys cannot be inferred from inactivity.

This whitepaper therefore does not assign a fixed circulating-supply percentage or equate the difference between the cap and the frozen amount with available coins. Neither frozen nor lost coins increase the future subsidy budget.

## Wallet and software continuity

The v30 desktop wallet uses **Qt 6.8.4**, replacing Qt 5. Core also updates dependencies and includes targeted fixes for memory bounds, log rate limiting and costly validation paths. These software improvements take effect when installed; the consensus changes became active at block 52,560.

Existing addresses, keys, wallet balances, genesis and transaction formats are preserved. Descriptor and legacy wallets remain supported. Backups and normal upgrade care are still required; the upgrade does not transfer funds to a replacement token or ask users to disclose recovery material. [1, 7]

Full nodes validate proof of work, transactions, coinbase limits, SegWit and Taproot rules. Consensus rules are enforced by participating software and can evolve through coordinated upgrades; neither the cap nor the freeze is a claim that future participants can never propose a different rule set.

# 6. Current operator guidance and references

## Required software baseline

Node, exchange and mining-pool operators must run v30 or a later compatible release. Verify the package checksum, back up wallets, shut down the old process cleanly, replace the executables and restart with the intended data directory. Confirm version 30.0.0 or later and complete synchronization. Never run two nodes on the same data directory.

Historical blocks continue to validate under their original rules. No mainnet configuration option moves the activation height or disables the active rules. Changing these consensus parameters would require another coordinated software release.

## Active behavior from block 52,560

Block 52,560 used the new subsidy and monetary limit while keeping block 52,559's difficulty target. Every later block uses ASERT V2. Old versions do not implement this consensus and can reject valid v30 blocks or follow a different chain. Do not downgrade to old-consensus software.

Miners should confirm that their pools use a compatible v30 node. Pools and exchanges should verify their block templates, reward accounting, synchronization and node connectivity. Independent header-verifying clients must implement the height-dependent difficulty rules. Service confirmation policies remain operator decisions.

## Network access

Use the official source repository and releases. The configured DNS seed is `dnsseed.fixedcoin.org`; seeds assist peer discovery and are not trusted authorities for block validity. Mainnet P2P defaults to port **24768**, and RPC to **24767**. Keep authenticated RPC access restricted to local or explicitly trusted systems. [2, 6]

Project: fixedcoin.org | Support: help@fixedcoin.org

# Appendix A. Exact consensus mathematics

This appendix makes the active v30 calculations independently reproducible. All divisions and floors below operate on non-negative integers unless a signed rounding rule is stated explicitly. The published source remains authoritative for serialization, compact-target encoding and historical edge cases. [2, 3, 4]

## Proof of work and chain selection

Decode the compact `nBits` field into the target integer `T`. A proof-of-work header is valid only when:

```
0 < T <= powLimit
uint256(SHA256d(block_header)) <= T
```

A lower target requires more expected hashes. The work represented by a valid target and the cumulative work of a chain are:

```
work(T) = floor(2^256 / (T + 1))
chain_work = sum(work(T_i)) over all blocks in the chain
```

Nodes select the valid chain with the greatest cumulative work, not simply the chain with the greatest height. Compact encoding quantizes targets, so displayed difficulty and the ideal exponential relationship can differ slightly from the exact encoded result.

## Exact ASERT V2 arithmetic

Let `H = 52,560`, let `a = H - 1` be the branch-specific anchor, and let `h > H` be the candidate height. `t(k)` is the block-header timestamp at height `k`. It is not Median Time Past; block timestamps remain subject to the protocol's timestamp-validity rules.

```
delta = t(h - 1) - t(a) - 600 * ((h - 1) - a)
Q = 65,536
L = 86,400

e = trunc_toward_zero(delta * Q / L)
q = floor(e / Q)
f = e - q * Q, where 0 <= f < Q
```

The fixed-point polynomial factor is:

```
P(f) = Q + floor((
    195766423245049 * f
  + 971821376 * f^2
  + 5127 * f^3
  + 2^47) / 2^48)
```

The unencoded target is then:

```
T_raw = floor(T_ref * P(f) * 2^q / Q)
T_next = clamp(T_raw, 1, powLimit)
```

The implementation uses a 320-bit intermediate for `T_ref * P(f)`. It returns `powLimit` directly when `delta >= 256 * L`, and target `1` when `delta <= -256 * L`. The result is finally encoded into compact `nBits`. For the activation block itself, the compact value is copied exactly: `nBits(H) = nBits(H - 1)`.

Because difficulty is inversely proportional to target, an error of `+L` ideally doubles the target and halves difficulty; an error of `-L` ideally halves the target and doubles difficulty. Miners can influence header timestamps only within accepted timestamp rules. ASERT targets cadence but does not provide finality or guarantee a particular network hashrate.

## Exact v30 reward derivation

Let `C` be the 21,000 FIX limit in base units, `L(H)` the authorized historical subsidy through block `H - 1`, and `I` the new halving interval:

```
H = 52,560
I = 52,560 blocks
C = 21,000 * 100,000,000 = 2,100,000,000,000 units

L(H) = sum(legacy_subsidy(h), h = 0 to H - 1)
     = 999,747,652,440 units

B = C - L(H) = 1,100,252,347,560 units
```

For an initial integer reward `r`, its complete future schedule is:

```
F(r) = I * sum(floor(r / 2^k), k = 0 to infinity)

R = max { r in integers, r >= 0 : F(r) <= B }
  = 10,466,639 units
```

The boundary calculation is exact:

```
F(R)     = 1,100,252,250,720 units
L(H)+F(R)= 2,099,999,903,160 units
C-total  = 96,840 units

F(R + 1) = 1,100,252,513,520 units
F(R + 1) - B = 165,960 units
```

Therefore `R = 0.10466639 FIX` is the greatest initial base-unit reward whose complete integer-rounded schedule stays within the limit. Increasing it by one base unit would exceed the remaining budget.

## Historical boundary

For the initial three-block retarget regime, the observed 1,800-second span is clamped to 450 through 7,200 seconds before scaling the previous target and applying `powLimit`. From height 1,000 through 52,559, FixedCoin preserves its historical ASERT arithmetic exactly. That legacy arithmetic is not replaced by the V2 equations above; independent validators must retain the pinned historical implementation when validating those blocks. [4]

## References

All code references below are pinned to the public v30 commit, **02e892e**, rather than a moving development branch.

[1] FixedCoin Core v30.0.0: official release and downloads.

[2] Mainnet and test-network parameters; activation parameter defaults.

[3] Historical budget and initial reward calculation; height-selected block subsidy; monetary limits.

[4] Legacy and V2 proof-of-work calculations.

[5] Transaction input validation and frozen-outpoint rule.

[6] RPC ports; maturity and block limits.

[7] Migration guide; dependency versions.

[8] Activation block 52,560 and frozen transaction on the public explorer, consulted 7 November 2026. Explorer values are observations, not a replacement for consensus validation.