Octcoin (OCT)

A CPU-Native, Fair-Launch Decentralized Currency

Ashata Nakaawa

octcoin.native@gmail.com

Version 1.0 — March 29, 2026

Abstract

Octcoin (OCT) is a decentralized, peer-to-peer digital currency designed from the ground up for CPU accessibility and fair distribution. Unlike Bitcoin's SHA-256d algorithm, which has been dominated by specialized ASIC hardware since 2013, Octcoin uses a single-pass SHA-512 proof-of-work algorithm that is natively optimized for 64-bit general-purpose processors. This design choice keeps mining accessible to anyone with a standard computer, preventing hardware centralization. Octcoin launched on March 29, 2026 with zero premine, no developer allocation, and a fixed supply of 21,000,000 OCT. The project is fully open source under the MIT License, with governance transitioning to the community. This paper describes the technical design, economic model, and philosophical motivations behind Octcoin.

---

1. Motivation and Problem Statement

Bitcoin introduced the world to a trustless, decentralized monetary system in 2008. Its proof-of-work mechanism, built on SHA-256d, was initially mineable by anyone with a CPU. However, as Bitcoin's value increased, the economic incentive to build specialized mining hardware (ASICs) became overwhelming. By 2013, GPU mining had replaced CPU mining; by 2014, ASICs had replaced GPUs. Today, Bitcoin mining is dominated by a small number of industrial mining farms running purpose-built hardware, with ordinary individuals effectively excluded.

This creates a fundamental tension: a system designed for decentralization has become highly centralized at the mining layer. While Bitcoin's security model remains robust, the ideal of "one CPU, one vote" described in the original paper has been replaced by "one ASIC farm, more votes." This centralization raises long-term concerns about censorship resistance, geographic concentration, and the ability of ordinary people to participate in network security.

Octcoin is designed to address this problem directly. By choosing SHA-512 as its proof-of-work algorithm — a function that runs natively and efficiently on 64-bit CPUs but has not been targeted by ASIC manufacturers — Octcoin aims to restore meaningful CPU participation in consensus. Combined with a strict fair-launch policy and open governance, Octcoin is built for broad, accessible participation.

2. Why SHA-512: Technical Rationale

2.1 SHA-512 vs SHA-256d

Bitcoin uses double SHA-256 (SHA-256d) as its proof-of-work hash function. SHA-256 was designed with 32-bit word operations, making it well-suited to both 32-bit and 64-bit hardware. This characteristic made it straightforward to implement in silicon, leading to the development of highly efficient SHA-256 ASICs.

SHA-512, by contrast, uses 64-bit word operations throughout its compression function — 64-bit additions, 64-bit rotations, and 64-bit logical operations. On a 64-bit CPU (which includes every modern laptop, desktop, and server), SHA-512 runs at approximately the same speed as SHA-256. However, implementing SHA-512 in a 32-bit ASIC requires emulating 64-bit operations using pairs of 32-bit operations, approximately doubling the gate count and power consumption compared to SHA-256. This significantly reduces the economic advantage of building a SHA-512 ASIC versus using a general-purpose CPU.

2.2 Single-Pass vs Double-Hash

Octcoin uses a single-pass SHA-512 rather than a double hash. The double-hash design in Bitcoin (SHA-256(SHA-256(data))) was chosen to defend against length extension attacks on the Merkle tree. Octcoin's block header structure and Merkle tree construction are designed to avoid length extension vulnerabilities without requiring a second hash pass, reducing computational overhead per block validation by approximately 40% compared to Bitcoin.

2.3 Memory and Efficiency

SHA-512 produces a 512-bit (64-byte) digest, of which Octcoin uses only the first 256 bits (32 bytes) for the block hash. This truncation maintains 256-bit security against collision and preimage attacks while producing a standard 32-byte hash suitable for all downstream operations including Merkle trees, transaction hashing, and address derivation. The single-pass design is also more memory-efficient on general-purpose hardware, slightly favoring CPUs with larger L1/L2 caches over highly pipelined fixed-function circuits.

3. Fair Launch and Distribution

Octcoin launched on March 29, 2026 with a strict fair-launch policy. "Fair launch" means:

- Zero premine: No OCT was created before the public launch. The genesis block contains only the standard coinbase transaction with a reward of 50 OCT, available to anyone who mines it.
- No developer allocation: There is no reserved pool of coins for founders, developers, or investors. Every OCT in existence must be earned through proof-of-work mining.
- No ICO or token sale: Octcoin has not conducted and will not conduct any initial coin offering or token sale. There are no investors holding pre-allocated coins.
- Open source from day one: The complete source code was published on GitHub (github.com/octcoins/octcoin) before the network launched, giving anyone time to review the code before committing hash power.
- Public network: The network is open to any miner from the first block. No private mining period was conducted by the founders.

This approach stands in contrast to many cryptocurrency launches that allocate significant percentages of supply to founders and early investors, creating misaligned incentives and concentrated wealth from the outset. Octcoin's distribution is determined entirely by market participation and CPU work.

4. Network Architecture

4.1 Block Production

Octcoin targets a block time of approximately 10 minutes using a difficulty adjustment algorithm identical to Bitcoin's: the difficulty is recalculated every 2,016 blocks based on the actual time taken to mine the previous 2,016 blocks, with a maximum adjustment factor of 4x in either direction per period. This proven algorithm provides stable block times under normal conditions while accommodating significant changes in network hash rate.

4.2 SegWit from Genesis

Octcoin activates Segregated Witness (SegWit) from block 0 — the genesis block. SegWit separates signature data from transaction data, eliminating transaction malleability and enabling second-layer protocols such as payment channels. Because SegWit is active from genesis, there is no need for a soft fork to activate it, and all wallets and software are built with SegWit support from the start.

4.3 Bech32 Native Addresses

Octcoin uses Bech32 as the default address format with the human-readable part (HRP) "oct1". Bech32 provides superior error detection compared to Base58Check addresses, uses only lowercase alphanumeric characters (avoiding confusion between similar characters like 0/O and I/l), and is QR-code friendly. All new wallets generate Bech32 addresses by default.

4.4 UTXO Model

Octcoin uses the Unspent Transaction Output (UTXO) model for tracking balances, identical to Bitcoin. Each transaction consumes existing UTXOs as inputs and creates new UTXOs as outputs. This model provides natural parallelism for transaction validation, simple SPV (Simplified Payment Verification) proof construction, and excellent privacy properties when combined with address reuse avoidance.

4.5 Node Connectivity

The Octcoin network uses port 8555 for peer-to-peer connections and port 8554 for RPC communication. Nodes discover peers through DNS seeds hosted at seed.mainnet.octcoin.jo3.org, as well as through peer exchange (PEX) messages between connected nodes. The protocol is based on Bitcoin Core 30.0, inheriting its extensive testing and security audit history.

5. Economic Model

5.1 Fixed Supply

The total supply of Octcoin is permanently capped at 21,000,000 OCT. This cap is enforced in consensus rules: any block that claims a coinbase reward exceeding the allowed amount for that block height will be rejected by all nodes. No mechanism exists to increase the supply cap — doing so would require a hard fork with broad network consensus.

5.2 Halving Schedule

The block reward follows a halving schedule: the reward starts at 50 OCT per block and halves every 210,000 blocks. At a target block time of 10 minutes, each halving epoch lasts approximately 4 years.

Era	Block Range	Reward	OCT Issued	Cumulative
1	0 – 209,999	50 OCT	10,500,000	10,500,000
2	210,000 – 419,999	25 OCT	5,250,000	15,750,000

3	420,000 – 629,999	12.5 OCT	2,625,000	18,375,000
4	630,000 – 839,999	6.25 OCT	1,312,500	19,687,500
5	840,000 – 1,049,999	3.125 OCT	656,250	20,343,750
...	...	...	...	...
∞	—	~0	—	21,000,000

Table 1: Octcoin halving schedule and supply distribution

5.3 Transaction Fees

As the block subsidy diminishes over successive halvings, transaction fees become an increasingly important component of miner revenue. Octcoin's minimum relay fee is set at 1 satoshi per vByte (0.00000001 OCT/vByte), with the market determining fee levels based on block space demand. SegWit transactions receive a 75% discount on witness data weight, incentivizing efficient transaction construction.

6. Governance and Decentralization

Octcoin was created by Ashata Nakaawa in 2026 as a personal research and engineering project. The founder's role is explicitly transitional: the goal is to establish the network, publish all software and documentation, and hand governance to a distributed community of developers, miners, and users.

Governance in Octcoin follows the proven Bitcoin model: protocol changes require broad consensus among node operators, miners, and developers. No individual or organization holds special authority to impose changes. The codebase is maintained through open pull requests on GitHub, reviewed and merged by community contributors. The founder retains no special keys, no admin access, and no veto power over protocol changes.

The project actively seeks experienced C++ developers to take over as core maintainers. Interested contributors are encouraged to review the codebase at github.com/octcoins/octcoin, open issues and pull requests, and engage with the community. The transition to full community governance is a stated goal, not a distant aspiration.

7. Comparison with Bitcoin and Other CPU Coins

Feature	Bitcoin (BTC)	Monero (XMR)	Octcoin (OCT)
PoW Algorithm	SHA-256d	RandomX	SHA-512
CPU Competitive	No (ASIC)	Yes	Yes
Max Supply	21M BTC	Tail emission	21M OCT
Block Time	~10 min	~2 min	~10 min
Block Reward	3.125 BTC	0.6 XMR	50 OCT
Premine	No	No	No
Privacy	Pseudonymous	Private by default	Pseudonymous
SegWit	Yes (soft fork)	No	Yes (genesis)
Smart Contracts	Limited	No	No
Launch Year	2009	2014	2026

Table 2: Feature comparison across selected cryptocurrencies

Octcoin occupies a distinct position: it combines Bitcoin's economic model (fixed supply, halving schedule, UTXO model, 10-minute blocks) with a proof-of-work algorithm that preserves CPU competitiveness in the near to medium term. Unlike Monero's RandomX, which uses memory-hard operations to resist ASICs, SHA-512 takes a different approach — relying on the 64-bit word size advantage of general-purpose CPUs. Both approaches have merits; SHA-512 is simpler, more auditable, and requires less memory bandwidth.

8. Risks and Limitations

Octcoin is a new network launched in 2026. Potential participants should be aware of the following risks:

ASIC development risk: If Octcoin's market value grows significantly, economic incentives to develop SHA-512 ASICs will increase. While the 64-bit word size provides a structural advantage for CPUs today, this advantage may erode over time. The project will monitor mining hardware developments and may consider algorithm updates via community consensus if ASIC centralization becomes a genuine threat.

Early network security: With a small hash rate in the early stages, the network is more vulnerable to 51% attacks than established networks. Users and exchanges should require more confirmations during the network's infancy. Security improves as more miners join.

Governance transition risk: The transition from founder-led to community-led governance carries execution risk. The founder's commitment to open governance is stated and designed into the project's structure, but outcomes depend on community participation.

Liquidity and adoption: As a new cryptocurrency, Octcoin has limited exchange listings and liquidity. Network effects take time to develop. Adoption is not guaranteed.

Software maturity: Octcoin Core v0.10.0 is based on Bitcoin Core 30.0 and inherits its extensive testing. However, Octcoin-specific modifications are newer and less battle-tested. Users should exercise appropriate caution.

9. Roadmap

Phase	Timeline	Milestones
Genesis	Q1 2026	Network launch, v0.10.0 release, GitHub publication
Growth	Q2 2026	Block explorer, community forum, first exchange listing
Community	Q3 2026	Core maintainer handover, documentation expansion
Ecosystem	Q4 2026	Mobile wallet, mining pool support, developer tools
Maturity	2027+	Protocol improvements via BIPs, broader exchange coverage

10. Technical Specifications

Parameter	Value
Ticker Symbol	OCT
Maximum Supply	21,000,000 OCT
Smallest Unit	1 satoshi = 0.00000001 OCT
Block Time Target	~10 minutes

Difficulty Adjustment	Every 2,016 blocks (±4x cap)
Initial Block Reward	50 OCT
Halving Interval	210,000 blocks (~4 years)
Hashing Algorithm	SHA-512 (single-pass, 64-bit native)
Output Hash Size	256 bits (truncated from 512)
Consensus	Proof-of-Work
Address Format	Bech32 (HRP: oct1)
SegWit	Active from block 0
Transaction Model	UTXO
P2P Port	8555
RPC Port	8554
DNS Seed	seed.mainnet.octcoin.jo3.org
Codebase	Bitcoin Core 30.0 fork
License	MIT Open Source
Premine	None
Developer Allocation	None
Launch Date	March 29, 2026
GitHub	github.com/octcoins/octcoin

11. Conclusion

Octcoin is not a reinvention of cryptocurrency. It is a deliberate return to first principles: a simple, fair, CPU-accessible digital currency with a fixed supply and no special privileges for any participant. The choice of SHA-512 is not arbitrary — it is a calculated attempt to preserve the democratic nature of CPU mining in an era when ASIC hardware has captured most major proof-of-work networks.

We acknowledge the risks honestly: the network is young, the hash rate is small, and the transition to community governance requires sustained effort. We do not claim that Octcoin is superior to Bitcoin or to any other cryptocurrency. We claim only that it is different in ways that matter to a specific set of values: accessibility, fairness, and decentralization of the mining process.

The codebase is open. The network is live. Every OCT must be mined. The rest is up to the community.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. https://bitcoin.org/bitcoin.pdf

[2] NIST, "FIPS 180-4: Secure Hash Standard (SHS)," National Institute of Standards and Technology, 2015.

[3] P. Wuille et al., "Segregated Witness (Consensus Layer)," BIP141, 2015.

[4] P. Wuille, G. Maxwell, "Base32 address format for native v0-16 witness outputs," BIP173 (Bech32), 2017.

[5] A. Nakaawa, "Octcoin Core v0.10.0," 2026. https://github.com/octcoins/octcoin

[6] Bitcoin Core Contributors, "Bitcoin Core 30.0," 2025. https://github.com/bitcoin/bitcoin

[7] Monero Research Lab, "RandomX: Proof of Work Algorithm," 2019. https://github.com/tevador/RandomX

This document is provided for informational purposes. Octcoin (OCT) is experimental software. Participate at your own risk. The author makes no representations regarding the future value or utility of OCT.