C64 CHAIN

The Commodore 64 of Crypto

A privacy-first, CPU-mineable cryptocurrency built on Monero/CryptoNote technology. Fair launch with no premine, no ICO, and no insider allocation. Featuring rx/c64 mining algorithm, 90-day anti-dump vesting, consensus-enforced 2% dev fund, and LWMA-1 difficulty adjustment.

Version	1.0
Date	February 2026
Website	https://c64chain.com
GitHub	github.com/oxynaz/c64chain-mainnet
License	GNU GPL v3.0

Table of Contents

1. Abstract

C64 Chain is a privacy-focused, CPU-mineable cryptocurrency forked from Wownero (itself a fork of Monero). It combines the battle-tested CryptoNote privacy protocol with novel economic mechanisms designed for long-term sustainability: a 90-day staggered vesting schedule on all mining rewards, a consensus-enforced 2% development fund, and a custom RandomX variant (rx/c64) optimized for CPU mining. With a fixed supply of 19,640,000 coins and a smooth exponential emission curve, C64 Chain aims to be a fair, private, and accessible cryptocurrency that anyone can mine from home. The project launched on mainnet on February 19, 2026, with no premine, no ICO, and no insider allocation.

2. Introduction

The cryptocurrency ecosystem has grown enormously since Bitcoin's inception, yet several fundamental problems persist. Most proof-of-work currencies have become dominated by specialized hardware (ASICs and GPUs), making mining inaccessible to ordinary users. Many new projects launch with premines, insider allocations, or ICOs that benefit founders at the expense of the community. And when coins do get listed on exchanges, early miners often dump large quantities immediately, crashing the price for everyone.

C64 Chain addresses these issues directly. By using a CPU-only mining algorithm, we ensure that anyone with a computer can participate in securing the network. By launching with zero premine and no ICO, we guarantee that every coin in existence was earned through proof of work. And by implementing a novel vesting mechanism, we protect the coin's value during the critical early listing period.

The project takes its name and aesthetic from the Commodore 64, the best-selling home computer of all time. Just as the C64 democratized computing in the 1980s by making it affordable and accessible, C64 Chain aims to democratize cryptocurrency mining by keeping it within reach of ordinary people with ordinary hardware.

The maximum supply of 19,640,000 C64 pays tribute to 1964, the year the MOS 6502 CPU was designed — the processor that would go on to power the Commodore 64 and shape personal computing history.

3. Technology — CryptoNote Privacy

C64 Chain inherits the full CryptoNote privacy stack from Monero, providing three layers of transaction privacy that work together to make all transactions untraceable and unlinkable by default.

3.1 Ring Signatures

When a user spends C64 coins, the transaction is signed using a ring signature that mixes the real input with several decoy inputs from the blockchain. External observers cannot determine which input is the real one, providing sender ambiguity. The current ring size ensures a meaningful anonymity set for every transaction.

3.2 Stealth Addresses

Every transaction creates a unique one-time address for the recipient using a Diffie-Hellman key exchange. Even if someone knows a user's public address, they cannot determine which transactions were sent to that user by examining the blockchain. This provides receiver privacy.

3.3 RingCT (Ring Confidential Transactions)

Transaction amounts are hidden using Pedersen commitments and range proofs. While the network can verify that no coins were created from nothing (inputs equal outputs), the actual amounts transferred are invisible to anyone except the sender and receiver. This provides amount privacy.

4. Mining Algorithm — rx/c64

C64 Chain uses rx/c64, a custom variant of the RandomX algorithm family. RandomX was specifically designed to be efficient on general-purpose CPUs while being resistant to GPU and ASIC optimization. It achieves this through several mechanisms:

- Random program execution that leverages CPU features like branch prediction, out-of-order execution, and speculative execution
- Large memory requirements (2 GB dataset) that exceed typical GPU cache sizes
- Heavy use of floating-point operations that are inefficient on specialized hardware
- Dynamic program generation that prevents hardware shortcut optimization

The rx/c64 variant includes custom seed hash parameters and configuration specific to C64 Chain, ensuring that miners cannot reuse RandomX computations from other currencies. This protects against hashrate rental attacks from larger RandomX networks like Monero.

The choice of CPU-only mining is philosophical as well as practical. By keeping mining accessible to anyone with a standard computer, C64 Chain promotes decentralization and prevents the concentration of mining power in the hands of large GPU farms or ASIC manufacturers.

5. Tokenomics & Emission

Parameter	Value
Max Supply	19,640,000 C64
Algorithm	rx/c64 (RandomX variant)
Block Time	5 minutes (300 seconds)
Initial Block Reward	~149 C64
Emission Speed Factor	21
50% Mined	~10 months
80% Mined	~2 years
96% Mined	~4 years
Dev Fund	2% of each block reward

5.1 Emission Curve

The emission follows Monero's smooth curve formula: reward = (supply_cap - already_mined) >> ESF, where ESF (Emission Speed Factor) is 21. This means block rewards decrease gradually with every single block, creating a smooth exponential decay rather than Bitcoin's abrupt halvings every 4 years.

This design has several advantages. Miners never experience a sudden 50% drop in revenue. The emission is mathematically predictable and transparent. And the gradual decrease naturally transitions the network's security model from block rewards to transaction fees over time.

6. Vesting Mechanism

C64 Chain introduces a novel vesting mechanism for mining rewards. Every coinbase transaction (block reward) is automatically split into 4 equal outputs, each with a different unlock time. This is enforced at the consensus level — blocks that do not follow this structure are rejected by the network.

Portion	Unlock After	Blocks
25%	~24 hours	288 blocks

25%	~30 days	8,640 blocks
25%	~60 days	17,280 blocks
25%	~90 days	25,920 blocks

6.1 Why Vesting Matters

Without vesting, early miners can accumulate large amounts of coins at low difficulty and dump them immediately when the coin is listed on exchanges. This creates a massive sell wall that crashes the price, discouraging new participants and potentially killing the project.

With 90-day staggered vesting, selling pressure is distributed over time. Even if a miner wants to sell everything, they can only access 25% of their rewards after 24 hours, 50% after 30 days, 75% after 60 days, and 100% after 90 days. This gives the market time to develop organic demand and liquidity.

6.2 Technical Implementation

Each coinbase transaction contains exactly 5 outputs: 4 vesting outputs for the miner (each 25% of the miner's reward) and 1 output for the development fund (2% of the total block reward). The unlock heights are calculated deterministically from the current block height. This triple enforcement at the database, node consensus, and wallet level ensures that vesting cannot be circumvented.

7. Development Fund

A 2% development fund is taken from each block reward and sent to a designated address. This fund is consensus-enforced: every node on the network independently verifies that each new block contains the correct dev fund output with the correct amount. Blocks without a valid dev fund output are rejected.

The dev fund unlocks after approximately 24 hours (288 blocks), aligning with the first vesting tier. This provides ongoing funding for development, infrastructure, exchange listings, and community initiatives while keeping the allocation minimal and transparent.

Unlike many projects that allocate 10-20% or more to founders through premines or token sales, C64 Chain's 2% dev fund is modest, earned block-by-block alongside regular miners, and verifiable by anyone running a node.

8. Difficulty Algorithm — LWMA-1

C64 Chain uses Zawy's LWMA-1 (Linearly Weighted Moving Average) difficulty algorithm, active since HF21 at block 2. The algorithm dynamically adjusts mining difficulty to maintain the 5-minute block time target, with full auto-adjustment kicking in at block 1001 after an initial bootstrap phase.

Parameter	Value
Algorithm	LWMA-1 (Zawy)
Window Size	144 blocks
Activation	Block 2 (HF21, all features from genesis)
Auto-adjusting from	Block 1001
Target Block Time	300 seconds (5 minutes)

LWMA-1 gives more weight to recent blocks when calculating the next difficulty, allowing it to respond quickly to hashrate changes. The 144-block window provides a good balance between responsiveness and stability. This provides protection against hashrate oscillation attacks (where miners switch between chains to exploit slow difficulty adjustment) and ensures a smoother mining experience with block times that stay closer to the 5-minute target.

9. Security & Audit

C64 Chain has undergone a comprehensive code audit covering all modifications from the Wownero/Monero codebase. Key security measures include:

- **Dev fund consensus validation:** every node verifies that coinbase transactions contain exactly 5 outputs with correct amounts and structure.
- **Vesting triple enforcement:** unlock times are enforced independently at the database level, the node consensus level, and the wallet level.
- **Clean codebase:** all legacy Wownero checkpoints, hardcoded difficulty values, and workarounds have been removed.
- **LWMA-1 difficulty:** responsive difficulty adjustment protects against hashrate manipulation and timewarp attacks.
- **Cryptographic verification:** the dev fund address is verified cryptographically at consensus level, preventing substitution attacks.

10. Hard Fork History

Hard Fork	Block	Description
HF17	0 (genesis)	RandomWOW algorithm, base protocol
HF21	2	All features: 19.64M supply, rx/c64, vesting 4x25%, dev fund 2%, LWMA-1 difficulty, view tags, fixed unlock (288 blocks)

Unlike the testnet which activated features progressively (HF17 through HF20), mainnet was launched with all protocol features bundled into HF21, activated at block 2. This means LWMA-1 difficulty, vesting, dev fund, and all privacy features have been active since the very beginning of the mainnet chain.

10.1 Difficulty Bootstrap Phases

To ensure a smooth launch, the LWMA-1 algorithm includes three difficulty phases on mainnet:

- **Blocks 0-280:** Bootstrap difficulty of 100 (allows initial blocks to be mined quickly)
- **Blocks 281-1000:** Fixed difficulty of 300,000,000 (stable launch phase, predictable block times)
- **Blocks 1001+:** Fully dynamic LWMA-1 with 144-block window (auto-adjusting difficulty)

11. Network Configuration

Parameter	Value
P2P Port	19640
RPC Port	19641
ZMQ Port	19642
Wallet RPC Port	19643
Seed Nodes	5 nodes across 3 continents

Five seed nodes are hardcoded in the node binary, distributed across Europe and North America. New nodes automatically discover and connect to peers through the seed nodes. The block explorer is available at c64chain.com, providing real-time network statistics, block and transaction search, and historical charts.

12. Roadmap

Completed:

- Testnet launch and testing
- Security audit with all critical fixes applied
- HF20: LWMA-1 difficulty algorithm, dev fund cryptographic verification
- Mainnet launch — February 19, 2026
- Block explorer with real-time stats, GeoIP peer mapping, and Arena visualization
- Mining pool integration (rplant.xyz, suprnova.cc)

Planned:

- Additional mining pool partnerships
- Exchange listings (CEX and DEX)
- Mobile wallet development
- Community governance framework
- Cross-chain atomic swaps

13. Conclusion

C64 Chain combines proven CryptoNote privacy technology with thoughtful economic design to create a cryptocurrency that is fair, private, and sustainable. The CPU-only mining algorithm ensures broad participation, the vesting mechanism protects against early dump attacks, and the consensus-enforced dev fund provides transparent ongoing funding for development.

By paying homage to the Commodore 64 — a machine that made computing accessible to millions — C64 Chain carries forward the same spirit of democratization into the cryptocurrency era. Mining should be for everyone, privacy should be the default, and economic incentives should protect all participants, not just early insiders.

The project is fully open source under the GNU GPL v3.0 license, and all code is available for public review and contribution on GitHub.

C64 Chain — The Commodore 64 of Crypto

https://c64chain.com | https://discord.gg/yj2vACFJCj | github.com/oxynaz