BitMinti: The Decentralized Standard

Restoring the "One CPU, One Vote" Vision

BitMinti Core Development Team
January 1, 2026
bitminti.com

Abstract

Cryptocurrency was born from the desire for decentralization—a financial system operated not by banks or potentates, but by the people themselves. Satoshi Nakamoto's original vision for Bitcoin described a network where "one CPU" equaled "one vote." However, the emergence of Application-Specific Integrated Circuits (ASICs) has shattered this equality. Today, Bitcoin mining is an industrial activity dominated by massive facilities, creating a centralized elite that controls the network's security and policy.

BitMinti is a response to this centralization. It is a sovereign blockchain designed to restore the egalitarian nature of mining. By implementing **RandomX**, a Proof-of-Work algorithm optimized for general-purpose CPUs, and **LWMA**, a rapid-response difficulty adjustment algorithm, BitMinti ensures that anyone with a consumer-grade computer can meaningfully participate in the network. This document details the philosophical motivations, technical architecture, and economic model of BitMinti, explaining why a return to CPU-based consensus is critical for the long-term survival of decentralized money.

---

1. Introduction: The Broken Promise of Industrial Mining

1.1 The Centralization Vector

Bitcoin's success created an arms race. In the early years (2009-2010), users mined with CPUs. This was the golden age of decentralization because CPUs are ubiquitous; almost everyone owns one. By 2011, GPUs took over, raising the barrier slightly. But the real fracture occurred in 2013 with the introduction of ASICs.

ASICs (Application-Specific Integrated Circuits) are chips designed to do one thing: calculate SHA-256 hashes. They are millions of times more efficient than a CPU. This created a new reality:

1. **High Barrier to Entry**: Competitive ASIC miners cost $3,000 to $15,000.
2. **Centralized Supply Chain**: Only 2-3 companies in the world manufacture these chips.
3. **Geographic Concentration**: Mining migrates to regions with the cheapest industrial electricity, leading to massive server farms.

1.2 The "Cantillon Effect" of Crypto

In economics, the Cantillon Effect describes how those closest to the specific source of new money benefit the most. In modern Bitcoin, the "money printers" are the ASIC farms. They extract block rewards at industrial scale and immediately sell them to cover electricity costs, creating constant downward pressure on price while accumulating influence over network upgrades.

The average user is excluded from this production process. They are relegated to being passive consumers, forced to buy coins on exchanges. This turns a "Peer-to-Peer" currency into a "Business-to-Consumer" product, undermining the censorship resistance that makes cryptocurrency valuable.

1.3 The BitMinti Mission

Our mission is simple: **Make Mining Accessible Again.** We believe network security should come from millions of individuals running nodes on their laptops and desktops, not from five warehouses in remote regions. By effectively banning ASICs from the network via algorithmic design, BitMinti redistributes power from the industrial few to the retail many.

---

2. Consensus Architecture: The RandomX Revolution

2.1 Why SHA-256 Failed Decentralization

Traditional algorithms like SHA-256 (Bitcoin) are simple math problems. They require very little memory (RAM) and rely purely on crunching numbers. Ideally, this sounds good, but "simple math" is easy to print onto a silicon chip. An engineer can strip away everything from a chip except the "add" and "rotate" logic, creating a demonically fast processor that costs very little to run.

2.2 RandomX: The CPU's Native Language

To defeat ASICs, we must ask: *What can a CPU do that a cheap chip cannot?* The answer is **Complexity**. Modern CPUs are marvels of engineering. They have:

- Branch prediction (guessing code paths).
- Out-of-Order execution.
- Large, multi-level caches (L1, L2, L3).
- Floating Point Units.

RandomX is a Proof-of-Work algorithm that behaves like a complex computer program. Instead of asking the miner to solve a static math problem, it asks the miner to **execute a randomly generated piece of code**.

1. **Random Program Generation**: For every hash attempt, a new random program is created.
2. **VM Execution**: This program is run inside a Virtual Machine. It uses random math operations, jumps to different memory addresses, and complex logic flow.
3. **Memory Hardness**: The algorithm requires access to a static dataset of over 2 GB of RAM.

2.3 The "ASIC Resistance" Mechanism

If a hardware manufacturer wanted to build an ASIC for RandomX, they would need to build a chip that handles:

- Complex logic branching.
- Fast access to 2GB of RAM.
- Re-programmability for every hash.

By the time they engineer a chip that does all of this efficiently, they have effectively re-invented the **CPU** (Central Processing Unit). An Intel or AMD processor *is* the optimal hardware for this task. This closes the efficiency gap. An expensive ASIC might be 1.5x faster than a CPU, but it costs 10x more to develop. The economic incentive to build ASICs evaporates.

---

3. Network Stability: Linear Weighted Moving Average (LWMA)

3.1 The Volatility Problem

In small or medium PoW networks, hashrate can be volatile. Miners often use "profit-switching" software that jumps between coins depending on which is most profitable at that exact second. Bitcoin adjusts its difficulty every 2016 blocks (roughly 2 weeks). If 50% of miners leave, the network stalls for weeks. If 500%

of miners join (a "flash mine" attack), they mine all the blocks in hours and dump the coins, leaving difficulty sky-high for loyal miners.

3.2 The BitMinti Solution: LWMA-2

BitMinti implements the **Linearly Weighted Moving Average (LWMA)** Difficulty Adjustment Algorithm.

- **Continuous Adjustment**: Difficulty is recalculated **every single block**.
- **Responsive Window**: It looks at the past 45 blocks to determine network health.
- **Linear Weighting**: Recent blocks count more than older blocks.

3.3 How it Protects Users

If a massive botnet or mining farm points its power at BitMinti:

1. **Block 1**: Mined instantly.
2. **Block 2**: Difficulty shoots up immediately.
3. **Block 5**: Difficulty is so high that the attack is no longer profitable.
4. **Attacker Leaves**: Difficulty drops back down smoothly within 30-40 minutes.

This ensures that block times stay close to the **10-minute target**, providing predictable transaction confirmations for users regardless of global network chaos.

---

4. Economic Model and Fairness

4.1 The Importance of Fair Launch

Many modern projects (Solana, Ethereum 2.0, various tokens) launch with "Pre-mines." The developers print millions of coins for themselves and their investors before the public even knows the project exists. We consider this unethical and contrary to the spirit of open-source money.

BitMinti had:

- **Zero Premine**: No coins existed before Block 1.
- **Zero ICO**: No funding was raised; no tokens were sold.
- **Zero Dev Tax**: Block rewards go 100% to the miner.

4.2 Supply Schedule

BitMinti mimics the proven scarcity model of Bitcoin:

- **Max Supply**: 21,000,000 Coins.
- **Block Reward**: Starts at 50 BitMinti per block.
- **Halving**: Every 210,000 blocks (approx 4 years), the reward is cut in half.
- **Deflationary**: As adoption grows, the supply issuance shrinks, preserving purchasing power.

4.3 Distribution via Work

Because mining is accessible on CPUs, the distribution of BitMinti is naturally wider than Bitcoin's current distribution.

- A student in a dorm room can mine 5 BitMinti.
- An office worker can mine on their gaming PC at night.
- A developer can mine on a spare server. This creates a grassroots community of holders who "earned" their coins through work, rather than buying them from a VC fund.

---

5. Security Analysis

5.1 The 51% Attack Vector

The biggest threat to a PoW blockchain is a 51% attack, where one entity controls the majority of the hashrate.

- **In ASIC Chains**: You need to buy hardware. Manufacturer supply chains are the bottleneck.
- **In CPU Chains**: The hardware (CPUs) is everywhere. The threat is **Botnets** (hacked computers).

5.2 Mitigating Botnets

RandomX has a unique property: **It is heavy.** Because it requires 2GB of RAM and uses the CPU intensely, it is very noticeable.

- If a hacker installs a hidden miner on a victim's PC, the victim's computer slows down immediately. The fan spins up.
- Users notice and remove the malware.
- Unlike light algorithms (like Monero's old CryptoNight), RandomX is hard to hide. This creates a natural immune system against botnets, keeping the hashrate composed of legitimate, consenting participants.

---

6. Technical Specifications

Parameter	Value	Rationale
Proof of Work	RandomX (Dataset Mode)	ASIC Resistance, CPU Dominance
Block Time	10 Minutes	Global synchronization, low orphan rate
Block Size	4 MB (Weight)	High throughput capacity
Difficulty Algorithm	LWMA (45 blocks)	Rapid response to hashrate volatility
Symbol	BitMinti	The third era of Bitcoin technology
** RPC Port**	8332	Standard compatibility
** P2P Port**	13337	Custom network port
** Magic Bytes**	`0xfc 0xc1 0xb7 0xdc`	Unique network identifier

---

7. Why We Developed BitMinti

We looked at the crypto landscape and saw a divergence from reality. "Decentralized Finance" (DeFi) is run on centralized AWS servers. "Decentralized Money" (Bitcoin) is mined by centralized corporations.

We developed BitMinti to prove a point: **Technology can enforce democracy.** By choosing the right algorithms (RandomX + LWMA), we can force the network to remain open. We don't need laws or regulations to stop centralization; we just need code that makes centralization unprofitable.

BitMinti is not a "competitor" to Bitcoin in terms of price or market cap; it is a competitor in terms of **ideology**. It is a lifeboat for the original vision of peer-to-peer electronic cash.

---

8. Roadmap

Phase 1: Genesis (Current)

- Launch Mainnet.
- Stabilize Difficulty (LWMA).
- Distribute mining software.
- Secure exchange listings.

Phase 2: Useability

- Mobile Wallets (SPV).
- One-click miners for non-technical users.
- Merchant integration plugins.

Phase 3: Privacy & Scalability

- Investigate Layer-2 solutions (Lightning Network compatible).
- Evaluate privacy enhancements (Confidential Transactions) via soft-forks if community consensus approves.

---

9. Conclusion

The era of CPU mining was thought to be dead. The industry moved on to bigger, faster, more expensive machines. But in doing so, they left the users behind.

BitMinti invites you back. It invites you to turn on your computer, run a node, and actually *be* the bank again. The mathematics of RandomX prove that your CPU is valuable. The economics of BitMinti prove that your participation is rewarded.

Welcome to the decentralized renaissance.
