NETHXEUM

N T U

Private · Scarce · Untraceable

"What Bitcoin would be if Satoshi had built privacy in from day one."

Whitepaper Version 2.0

June 2026

Codebase: Monero v0.18.3.3 Fork

License: MIT Open Source

Website: nethxeum.io

Founded by Rony Katie

Table of Contents

1. Abstract

Nethxeum (NTU) is a decentralized, privacy-preserving cryptocurrency that combines the proven scarcity model of Bitcoin with the battle-tested cryptographic privacy of Monero. Founded by Rony Katie, it introduces a hard supply cap of 42,000,000 NTU, a Bitcoin-style halving schedule every 420,000 blocks, zero tail emission, and full transaction confidentiality enforced at the protocol level.

Every transaction on the Nethxeum network is private by default. Sender identity, recipient identity, and transaction amounts are all cryptographically concealed through Ring Signatures, RingCT, and Stealth Addresses — the same technology securing Monero since 2014. Privacy is not optional. It is mandatory.

Mining is performed using the RandomX proof-of-work algorithm, optimized for commodity CPUs and resistant to ASIC hardware dominance. Nethxeum is open-source, has no premine, no ICO, and no developer tax. Every NTU in existence is earned through proof-of-work from block zero. The genesis block was mined on May 31, 2026, carrying the message: "In a world of surveillance, privacy is not a crime, it is a right."

Parameter	Value	Notes
Max Supply	42,000,000 NTU	Hard cap — enforced in consensus
Initial Reward	50 NTU / block	Epoch 1 — block 0 to 419,999
Halving Interval	420,000 blocks	~4 years at 5 min/block
Block Time	5 minutes (300s)	DIFFICULTY_TARGET_V2
Algorithm	RandomX (PoW)	CPU-optimized, ASIC-resistant
Privacy Stack	Ring Sigs + RingCT + Stealth	Default — cannot be disabled
Tail Emission	None (0 NTU)	Hard stop at 42M NTU
Premine	0 NTU	Fair launch from block 0
Block Maturity	100 blocks	Bitcoin-like confirmation
Decimal Places	8 (nanoNTU)	1 NTU = 10^8 atomic units

2. The Problem — What Money Lost

For thousands of years, physical cash possessed two fundamental properties that humanity took entirely for granted: scarcity and confidentiality. A banknote is limited in quantity, and no record exists of who passes it from hand to hand. The digital revolution dismantled both simultaneously.

2.1 Bitcoin — Scarcity Without Privacy

Bitcoin solved the double-spend problem and introduced mathematically enforced digital scarcity. Its 21 million coin cap and halving schedule represent a genuine breakthrough in monetary engineering. However, Bitcoin's transaction ledger is entirely public. Every address, every balance, and every transaction is permanently visible to anyone on Earth.

Chain analysis firms — Chainalysis, Elliptic, CipherTrace — generate hundreds of millions of dollars in revenue by tracing Bitcoin flows for governments and corporations. A business competitor can monitor your wallet. An exchange can refuse your funds because they once touched a blacklisted address. Bitcoin's transparency is a fundamental design limitation that undermines its utility as everyday money. Not all BTC are equal — 'tainted' coins are rejected by exchanges, violating the most basic property of money: perfect fungibility.

2.2 Monero — Privacy Without Scarcity

Monero solved the privacy problem with cryptographic elegance. Ring Signatures, RingCT, and Stealth Addresses make transactions genuinely untraceable. Monero is the gold standard of financial privacy. However, Monero has no supply cap. Its tail emission — 0.6 XMR per block, forever — means there is no predictable scarcity, no halving narrative, and no sound money story. Monero cannot serve as a long-term store of value because its supply is unbounded.

2.3 The Era of Digital Surveillance Money

Governments worldwide are accelerating development of Central Bank Digital Currencies (CBDCs). These instruments are designed from inception to be programmable, traceable, and revocable. A CBDC can expire. It can be restricted from purchasing certain goods. Every transaction can be permanently logged by the state. The need for censorship-resistant, private, and scarce money has never been more urgent.

	Bitcoin	Monero	Nethxeum	Zcash
Hard Supply Cap	21M cap	Unlimited	**42M cap**	21M cap
Halving Schedule	Yes	No (smooth emission)	**Yes**	Yes
Tail Emission	None	0.6 XMR/block forever	**None**	None
Default Privacy	Public	Mandatory	**Mandatory**	Opt-in
Sender Hidden	No	Yes (ring sigs)	**Yes (ring sigs)**	Shielded only
Amount Hidden	No	Yes (RingCT)	**Yes (RingCT)**	Shielded only
Fungible	Tainted coins exist	Perfect	**Perfect**	Partial
ASIC-Resistant	No (SHA-256)	Yes (RandomX)	**Yes (RandomX)**	No
No Trusted Setup	Yes	Yes	**Yes**	No
Fair Launch	Yes	Yes	**Yes (no premine)**	Founders reward

3. The Solution — Nethxeum

Nethxeum is the first cryptocurrency designed to restore both fundamental properties of sound money simultaneously: mathematical scarcity and cryptographic confidentiality.

> *"Nethxeum — Privacy by default, freedom by design."*

3.1 Four Pillars

I. Confidentiality. Every transaction is private by default. No opt-in required. The protocol enforces privacy at every layer using Ring Signatures, RingCT, and Stealth Addresses. Your balance, counterparties, and transaction history are yours alone.

II. Fungibility. Because all transactions are opaque, no NTU can ever be 'tainted'. 1 NTU = 1 NTU, always and everywhere. No exchange can discriminate between NTU based on transaction history. This is the true definition of money: perfect interchangeability.

III. Scarcity. 42,000,000 NTU. Never one more. The halving every 420,000 blocks creates a monetary policy that anyone can verify, anticipate, and trust. No central authority controls it. No governance vote can change it. It is written in the protocol.

IV. Accessibility. RandomX ensures that mining NTU is efficient on any modern CPU. No specialized ASICs. No industrial GPU farms. Anyone with a standard computer can participate in securing the network and earning newly minted NTU. Decentralized from day one.

3.2 Design Philosophy

Nethxeum inherits the Monero codebase (v0.18.3.3) because Monero's privacy cryptography has been battle-tested for over a decade under adversarial conditions. Rather than reinventing cryptographic primitives, Nethxeum replaces Monero's inflationary emission model with a Bitcoin-style hard cap and halving schedule. The result is a chain that maximizes both security (proven privacy tech) and monetary soundness (fixed supply).

4. Technical Architecture

4.1 Chain Parameters

The following parameters are hard-coded in the consensus layer and cannot be changed without a network fork:

Parameter	Value	Notes
Name	Nethxeum	—
Ticker	NTU	—
Codebase	Monero v0.18.3.3	Fork
Consensus	Proof-of-Work	RandomX
Block Time	5 minutes (300s)	DIFFICULTY_TARGET_V2
Max Supply	42,000,000 NTU	Hard cap — never exceeded
Decimals	8 (nanoNTU)	1 NTU = 10^8 atomic units
Initial Reward	50 NTU / block	Epoch 1
Halving Interval	420,000 blocks	~4 years
Tail Emission	None (0 NTU)	Hard stop at 42M
Block Maturity	100 blocks	Bitcoin-like
Address Prefix (Standard)	130	Base58 encoded
Address Prefix (Integrated)	120	Embedded payment ID
Address Prefix (Subaddress)	133	Unlinkable addresses
P2P Port (mainnet)	18333	—
RPC Port (mainnet)	18331	—
ZMQ Port (mainnet)	18332	—
P2P Port (testnet)	28333	—
P2P Port (stagenet)	38333	—
Genesis Message	"Privacy is not a crime..."	Block 0, May 31 2026
Network ID	Bender's nightmare	Unique network identifier
License	MIT Open Source	—

4.2 Block Reward Function

The block reward function replaces Monero's smooth emission curve with a discrete halving schedule. The reward for any block at height h is computed as follows:

```
//               Block               reward               calculation               –
nethxeum/src/cryptonote_basic/cryptonote_basic_impl.cpp
halvings = height / NTU_HALVING_INTERVAL;     // integer division
base_reward = NTU_INITIAL_BLOCK_REWARD >> halvings;  // bit-shift// Guard: after 64
halvings reward becomes 0if (halvings >= 64) base_reward = 0;

// Hard cap enforcementif (already_generated + base_reward > NTU_MAX_SUPPLY)
    base_reward = NTU_MAX_SUPPLY - already_generated;

// Constants
NTU_MAX_SUPPLY = 4200000000000000ULL;      // 42M * 10^8 atomic units
NTU_INITIAL_BLOCK_REWARD = 5000000000ULL;     // 50 * 10^8 = 50 NTU
NTU_HALVING_INTERVAL = 420000;                // blocks
```

The bit-shift operator `>>` implements halving: each right shift by the halving count divides the initial reward by 2^{halvings}. After 64 halvings, the reward reaches zero due to integer underflow protection. The hard cap enforcement ensures the total supply never exceeds 42,000,000 NTU.

4.3 Address Architecture

Nethxeum uses the standard CryptoNote dual-key address system. Each wallet generates two keypairs: a spend key and a view key. The public address encodes both public keys. Subaddresses allow a single wallet to generate unlimited unlinkable receiving addresses. Integrated addresses embed a payment ID for merchant use cases.

Type	Prefix	Use Case
Standard Address	130	General purpose transfers
Integrated Address	120	Merchant payments (embedded payment ID)
Subaddress	133	Multiple unlinkable receive addresses

4.4 Network Ports & Configuration

Network	P2P Port	RPC Port	ZMQ Port
Mainnet	18333	18331	18332
Testnet	28333	28331	28332
Stagenet	38333	38331	38332

4.5 Block Maturity

Nethxeum implements a Bitcoin-like block maturity of 100 blocks for coinbase outputs (mining rewards). This means newly mined NTU cannot be spent until 100 additional blocks have been mined on top of the block containing the coinbase transaction. This prevents issues with blockchain reorganizations affecting freshly mined coins. Regular transaction outputs require 10 confirmations before being considered spendable.

5. Privacy Technology

Nethxeum inherits Monero's cryptographic privacy stack without modification. This stack has been subject to years of academic scrutiny and real-world adversarial testing, making it the most proven privacy technology in production cryptocurrency today.

5.1 Ring Signatures — Sender Anonymity

When you send NTU, your transaction is co-signed alongside a group of decoy outputs drawn from the blockchain (the 'ring'). An external observer sees a valid group signature but cannot determine which member of the ring is the actual sender. The sender is cryptographically hidden within the crowd. Ring size is enforced at the protocol level, ensuring a minimum anonymity set for every transaction.

5.2 RingCT — Amount Confidentiality

Ring Confidential Transactions hide the value of every transaction input and output using Pedersen Commitments. An observer can mathematically verify that no NTU were created or destroyed — inputs equal outputs plus fee — without learning the actual amounts. Bulletproofs provide compact range proofs that transaction amounts are positive without revealing the values. No transaction amount on the Nethxeum blockchain is visible to any third party.

5.3 Stealth Addresses — Recipient Anonymity

When you publish your Nethxeum address, senders derive a unique one-time address for each transaction using your public view key. Your published address never appears on the blockchain. Each payment lands at a different one-time address that only you can recognize and spend using your private spend key. An observer cannot link multiple payments to the same recipient, even knowing the recipient's public address.

5.4 Key Images — Double-Spend Prevention

Each output can only be spent once. When you spend an output, your wallet generates a cryptographic key image — a deterministic value derived from your private key and the output. The network rejects any transaction that includes a previously seen key image, preventing double-spending while preserving the anonymity of the spender within the ring.

5.5 RandomX — Democratic Mining

RandomX is a proof-of-work algorithm designed to be efficient on general-purpose CPUs while being economically impractical for ASICs and inefficient for GPUs. It achieves this through random code execution and memory-hard operations tuned to CPU cache sizes. This design keeps mining accessible to individual participants worldwide, resisting the hardware centralization that has concentrated Bitcoin mining in industrial farms.

6. Emission & Tokenomics

6.1 Supply Schedule

The total supply of Nethxeum is mathematically fixed at 42,000,000 NTU. The emission follows a geometric series: each epoch of 420,000 blocks produces half the NTU of the previous epoch. The series converges precisely to 42,000,000 NTU and then stops. There is no tail emission, no continued reward, and no mechanism to mint additional NTU beyond this cap.

Total = 50 NTU x 420,000 x SUM($1/2^n$, n=0 to infinity) = 50 x 420,000 x 2 = 42,000,000 NTU

6.2 Halving Schedule

Epoch	Block Range	Reward/Block	Epoch Emission	Cumulative	% of Max	~Year
1	0 – 419,999	50 NTU	21,000,000	21,000,000	50.00%	0–4
2	420,000 – 839,999	25 NTU	10,500,000	31,500,000	75.00%	4–8
3	840,000 – 1,259,999	12.5 NTU	5,250,000	36,750,000	87.50%	8–12
4	1,260,000 – 1,679,999	6.25 NTU	2,625,000	39,375,000	93.75%	12–16
5	1,680,000 – 2,099,999	3.125 NTU	1,312,500	40,687,500	96.88%	16–20
6	2,100,000 – 2,519,999	1.5625 NTU	656,250	41,343,750	98.44%	20–24
7	2,520,000 – 2,939,999	0.78125 NTU	328,125	41,671,875	99.22%	24–28
...	...	→ 0	...	→ 42,000,000	100%	~160

6.3 No Premine, No ICO, No Developer Tax

Block 0 starts with zero coins in existence. Every NTU in circulation is earned through proof-of-work. There is no allocation to founders, venture capitalists, or early investors. There is no developer fund taking a percentage of block rewards. The genesis transaction contains only the embedded message — no coin output. The founder, Rony Katie, mined the genesis block under the same conditions as any other miner.

6.4 Fungibility & Monetary Properties

Sound money must be scarce, durable, divisible, fungible, and portable. Nethxeum achieves all five: scarcity through the hard cap, durability through the distributed blockchain, divisibility to 8 decimal places, fungibility through mandatory privacy, and portability through digital transfer anywhere in the world.

7. Comparison

Nethxeum occupies a unique position in the cryptocurrency landscape — the only project combining a hard supply cap with mandatory full transaction privacy. Unlike Bitcoin, every Nethxeum transaction is private. Unlike Monero, Nethxeum has a fixed supply with predictable scarcity. Unlike Zcash, Nethxeum requires no trusted setup and privacy is mandatory, not optional.

Feature	Bitcoin	Monero	Nethxeum	Zcash
Hard Supply Cap	21M	Unlimited	**42M**	21M
Halving Schedule	Yes	No	**Yes**	Yes
Tail Emission	None	Forever	**None**	None
Default Privacy	Public	Mandatory	**Mandatory**	Opt-in
Sender Hidden	No	Yes	**Yes**	Shielded
Amount Hidden	No	Yes	**Yes**	Shielded
Recipient Hidden	No	Yes	**Yes**	Shielded
Fungible	No	Yes	**Yes**	Partial
ASIC-Resistant	No	Yes (RandomX)	**Yes (RandomX)**	No
No Trusted Setup	Yes	Yes	**Yes**	No
Fair Launch	Yes	Yes	**Yes**	Founders reward

8. User Guide — Getting Started

8.1 Installing the Daemon

Component	Minimum	Recommended
OS	Ubuntu 20.04 / Windows 10	Ubuntu 22.04 LTS
CPU	2 cores (x86_64)	4+ cores (RandomX benefit)
RAM	4 GB	8 GB+
Disk	50 GB SSD	200 GB NVMe
Network	10 Mbps	100 Mbps

Build from source (Ubuntu/Debian):

```
# Install dependencies
sudo apt update && sudo apt install -y build-essential cmake git \\
    libboost-all-dev libssl-dev libzmq3-dev libpgm-dev \\
    libunbound-dev libsodium-dev libunwind-dev liblzma-dev \\
    libreadline-dev libldns-dev libexpat1-dev libgtest-dev

# Clone repository
git clone https://github.com/nethxeum/nethxeum.git
cd nethxeum

# Build
mkdir build && cd build
cmake .. -DCMAKE_BUILD_TYPE=Release
make -j$(nproc)

# Binaries are in build/bin/
ls build/bin/
# nethxeumd  nethxeum-wallet-cli  nethxeum-wallet-rpc
```

8.2 Running a Full Node

```
# Start daemon (mainnet)
./nethxeumd --detach --log-file=nethxeum.log

# Start daemon (testnet)
./nethxeumd --testnet --detach

# Check sync status
./nethxeumd status

# Stop daemon
./nethxeumd exit
```

The daemon listens on port 18333 (P2P) and 18331 (RPC) by default. Allow these ports through your firewall to contribute to network decentralization.

8.3 CLI Wallet — Create & Receive NTU

```
# Create new wallet
./nethxeum-wallet-cli --generate-new-wallet=my_wallet

# You will be prompted to:# 1. Set a password# 2. Confirm seed mnemonic (write this
down securely!)# Show your address
[wallet NTU...]: address

# Check balance
[wallet NTU...]: balance

# Refresh / sync wallet
[wallet NTU...]: refresh
```

8.4 CLI Wallet — Send NTU

```
# Basic transfer
[wallet NTU...]: transfer NTUxxx...xxx 10

# Set custom fee priority (1=slow, 2=normal, 3=fast)
[wallet NTU...]: set priority 2

# View transaction history
[wallet NTU...]: show_transfers
```

8.5 Mining NTU

Nethxeum uses RandomX, optimized for CPU mining. You can mine directly using the daemon's built-in miner, or connect to a mining pool.

```
# Solo mining (via daemon)
./nethxeumd --start-mining --mining-threads 4

# Or from daemon console
start_mining 4

# Pool mining (XMRig compatible)
./xmrig -o pool.nethxeum.io:3333 -u YOUR_ADDRESS -p worker1 --coin nethxeum
```

8.6 RPC API Reference

The Nethxeum daemon exposes a JSON-RPC API on port 18331. Below are the most commonly used endpoints:

Method	Endpoint	Description
GET	/json_rpc get_block_count	Returns current blockchain height
GET	/json_rpc get_info	Node info: height, peers, sync status
GET	/json_rpc get_block_header_by_height	Block header by height
POST	/json_rpc submit_block	Submit mined block
GET	/get_transactions	Fetch transactions by hash
POST	/sendrawtransaction	Broadcast raw transaction hex

```
# Example: get blockchain height
curl -X POST http://127.0.0.1:18331/json_rpc \\
  -H "Content-Type: application/json" \\
  -d '{"jsonrpc":"2.0","id":"0","method":"get_block_count"}'

# Response
{"id":"0","jsonrpc":"2.0","result":{"count":142857,"status":"OK"}}
```

9. Ecosystem & Roadmap

Phase	Name	Timeline	Milestones
Phase 1	Foundation	Q1–Q2 2025	Fork Monero codebase; Implement Bitcoin-like emission; Configure 5-min block time; Set address prefixes; Mine genesis block; Testnet launch; Open-source publication
Phase 2	Infrastructure	Q3 2025	Mainnet launch (block 0); Blockchain explorer; Official mining pool; CLI wallet release; Seed node network; Developer documentation
Phase 3	Ecosystem	Q4 2025 – 2026	GUI wallet (Windows, Linux); Mobile wallet (Android); Exchange listings (DEX then CEX); Merchant payment tools; Security audit; Community governance forum
Phase 4	Maturity	2026+	Hardware wallet support; Layer-2 payment channels; Cross-chain atomic swaps; Institutional custody docs; Academic research partnerships

10. Governance & Philosophy

10.1 Protocol Governance

Nethxeum has no formal on-chain governance mechanism and no governance token. Protocol changes require community consensus expressed through discussion, code review, and ultimately miner adoption. The emission schedule and supply cap are considered constitutional — changes to these parameters would constitute the creation of a new coin, not an upgrade to Nethxeum.

10.2 Privacy as a Human Right

Privacy is not a synonym for secrecy. A doctor does not publish patient records. A business does not publish its supply chain negotiations. An individual does not publish their salary to neighbors. Financial privacy is a prerequisite for human dignity, political freedom, and economic autonomy.

The argument that 'only criminals need privacy' is historically illiterate and logically incoherent. Every surveillance system ever built has been abused. Nethxeum exists because financial privacy is a right, not a privilege to be granted by states or corporations.

10.3 Sound Money Principles

Sound money must be scarce, durable, divisible, fungible, and portable. Bitcoin established digital scarcity. Monero established digital fungibility. Nethxeum is the synthesis: a monetary system where scarcity is mathematically enforced and fungibility is cryptographically guaranteed. No unit can be discriminated against. No supply can be inflated. No transaction can be surveilled.

10.4 Fair Launch Commitment

Nethxeum launched with block 0 containing zero pre-allocated coins. No entity — including the development team or founder Rony Katie — holds NTU prior to the mainnet launch. Every NTU must be mined. This is not merely an ethical choice but a technical one: a fair launch is the only credible foundation for a decentralized monetary network.

11. Security Model

11.1 Consensus Security

Nethxeum uses Proof-of-Work with RandomX. The security of the chain is proportional to the total hash rate of honest miners. A 51% attack requires an attacker to acquire and operate more CPU compute than the entire honest network — a substantial economic barrier given RandomX's CPU optimization, which prevents cheap ASIC-based attacks.

11.2 Privacy Security Assumptions

The privacy guarantees of Nethxeum rest on the following cryptographic assumptions:

- Discrete Logarithm Problem (DLP) hardness — basis for ring signatures and stealth addresses
- Decisional Diffie-Hellman (DDH) hardness — basis for Pedersen Commitments in RingCT
- Collision resistance of the underlying hash function (Keccak-256)
- Bulletproofs inner product argument — zero-knowledge range proofs

11.3 Wallet Security Best Practices

- Store your 25-word seed mnemonic offline — never digitally
- Use a strong, unique wallet password
- Verify recipient addresses carefully before sending
- Use subaddresses to prevent address reuse
- Run your own full node for maximum privacy
- Never share your private spend key or seed phrase
- Use the view key for read-only auditing without spending risk

11.4 Network Security

Nethxeum nodes communicate over an encrypted P2P protocol inherited from Monero. Transaction relay uses Dandelion++ to prevent transaction origin tracking at the network layer. Running a full node behind Tor or I2P provides additional IP-level anonymity.

Threat	Mitigation
Transaction tracing	Ring Signatures + RingCT + Stealth Addresses
Amount analysis	RingCT — all amounts encrypted
IP-level tracking	Dandelion++ relay + Tor/I2P support
ASIC centralization	RandomX — CPU-optimized PoW
51% attack	Growing CPU hashrate network
Double spending	Key images — deterministic spend tracking

12. Conclusion

Nethxeum is not a modification of an existing idea. It is a synthesis of the two most important insights in cryptocurrency history: that money can be mathematically scarce, and that money can be cryptographically private. These two properties are not in conflict. Nethxeum proves they are complementary.

We are entering an era where money itself is becoming a surveillance tool. Central bank digital currencies promise programmability at the cost of financial autonomy. Chain analysis firms have industrialized the tracing of cryptocurrency flows. The infrastructure of financial surveillance has never been more sophisticated.

Nethxeum is the answer. 42,000,000 coins. No more. No inflation. No tail. Every transaction private. Every sender anonymous. Every amount hidden. Every coin equal to every other coin. Mined by CPUs worldwide from block zero.

> *"Nethxeum — Privacy by default, freedom by design."*

nethxeum.io — Official website

github.com/nethxeum — Open-source repository (MIT)

18333 — Mainnet P2P port

18331 — Mainnet RPC port

42,000,000 NTU — Maximum supply — forever
