NAB COIN
White Paper

Pioneering a Smarter, Decentralized Future

NAB Coin is more than a cryptocurrency — it's a movement towards a decentralized economy where trust, security, and speed power the next generation of financial systems.

NAB: A Decentralized Digital Currency System

A Trustless, Peer-to-Peer Electronic Cash Protocol

Abstract

NAB is a decentralized digital currency system that enables direct transactions between parties without intermediaries. By combining cryptographic proof with an innovative consensus mechanism, NAB solves the double-spending problem while maintaining security, transparency, and scalability. This document outlines the technical and economic framework of the NAB network.

1. Introduction

Traditional electronic payment systems rely on centralized authorities, creating inefficiencies, censorship risks, and exclusion. NAB eliminates these dependencies through:

- A public, immutable ledger secured by cryptographic hashing
- Distributed consensus for transaction validation
- Predictable monetary policy with fixed supply
- Adaptive block generation for faster confirmations

NAB is designed to be self-sustaining, with incentives that align miners, users, and developers toward network growth.

2. Core Protocol Design

2.1 Transaction Model

- Transactions reference previous outputs (UTXO model)
- Each transaction includes: -
-Sender's public key
-Recipient's address (hashed public key)
-Digital signature (ECDSA)
-Transaction fee (optional for priority)

2.2 Blockchain Structure

- Blocks contain:
  - Header (previous block hash, timestamp, nonce)
  - Merkle root of transactions
  - Target difficulty value
- Consensus:- Proof-of-Work (modified SHA-256)
- Block Time:- 150 seconds (adjusts dynamically)

2.3 Decentralized Validation

- Full nodes enforce consensus rules
- Miners compete to add blocks (reward: new NAB + fees)
- SPV clients verify transactions without full history

3. Security & Attack Resistance

3.1 Consensus Safeguards

- 51% Attack Mitigation:-
- Checkpointing for early blocks
- Economic disincentives (costly to attack)
- Sybil Resistance:- PoW requires real resource expenditure

3.2 Network Resilience
- *Auto-adjusting difficulty (every 360 blocks)*
- *Peer discovery via DNS seeds + manual connections*

4. Monetary Policy

4.1 Issuance Schedule

- Total supply:- 10 Billion NAB
  - Block reward:- Starts at 100 NAB, halves every 840k blocks (~4 years)
  - Final block reward:- 0 NAB (reached in ~84 years)
- Total Halvings:- 21 (adjusted for 10B supply).

Key Adjustments:
1. **Initial Block Reward:**
- Increased from 50 NAB → 100 NAB to ensure the 10B supply is fully minted over 84 years.

● Math: - Total blocks in 84 years = (84 yrs × 525,600 blocks/yr) ≈ 44,150,400 blocks. - Cumulative rewards = 100 NAB × (1 + 0.5 + 0.25 + ...) over 21 halvings ≈ 10B NAB.

2. Halving Intervals:
● Every 840k blocks (consistent with Bitcoin's 4-year cycle).
● Ensures predictable, diminishing inflation.

3. Final Supply:
● No tail emission (block reward → 0 after 21 halvings).
● Total supply asymptotically approaches 10B NAB.

Visualization:

Halving #	Block Reward (NAB)	Cumulative Supply (Est.)
0	100	~4.2B
1	50	~6.3B
2	25	~7.35B
21	0.00000001	10B

4.2 Fee Market

● *Base fee: 0.001 NAB/kB (burned to reduce supply)*
● *Priority fees: Optional for faster inclusion*

5. Governance & Upgrades

5.1 Decentralized Decision-Making

● *Node signaling:- Miners vote on protocol changes*
● *Developer fund:- 2% of block rewards for maintenance*

5.2 Upgrade Process

1. Proposal submitted to community forum
2. Discussion + reference implementation
3. Activation threshold: 75% miner support

6. Privacy Features

6.1 Optional Anonymity

● One-time addresses per transaction
● Coin mixing (trustless, non-custodial)

6.2 Transparency Controls

● View keys for selective auditability
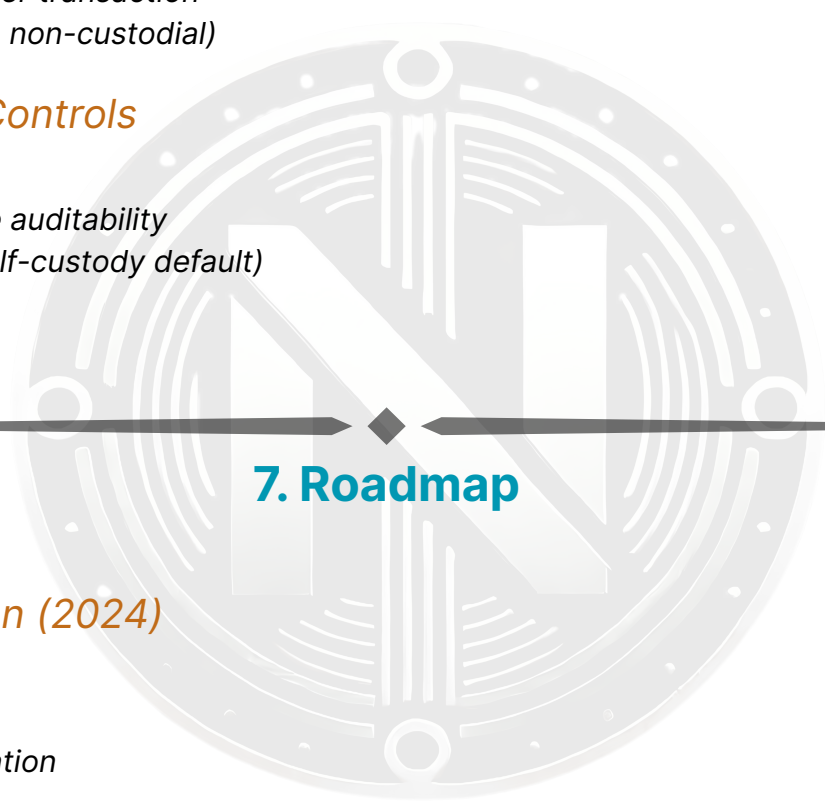● No mandatory KYC (self-custody default)

7. Roadmap

Phase 1: Foundation (2024)

● Mainnet launch
● Mining pool diversification

Phase 2: Scaling (2025)

● Compact block relay
● Payment channel prototypes

Phase 3: Expansion (2026+)

● Cross-chain atomic swaps
● Stateless client support

8. Comparison to Existing Solutions

Feature	NAB	Traditional Systems
Settlement Time	2.5 minutes	1-5 business days
Transaction Cost	~$0.01	1-3% + fees
Censorship	Resistant	Subject to freeze
Supply	Fixed (10B)	Inflationary

9. Conclusion

NAB delivers a secure, scalable, and sovereign monetary network through:
- Decentralized validation (no single point of control)
- Predictable issuance (hard-capped supply)
- Adaptive throughput (faster confirmations)

By prioritizing user autonomy and network resilience, NAB establishes a foundation for borderless digital commerce

Getting Started

- **Network specs:-** docs.nab.network
- **Source code:-** git.nab.network
- **Community:-** forum.nab.network

Key Differentiators

✓ No corporate or foundation control
✓ No pre mine or developer allocations
✓ Clear exit strategy for mining subsidies