[ SUBJECT TO CHANGE — INTERNAL DOCUMENT ]

# ARXIA

.EXE

IMPLEMENTATION ROADMAP ◆ 2026

**For developers, analysts & investors**

*All milestones, timelines, and parameters are subject to change based on technical progress, market conditions, and regulatory environment. This document is not an offering.*

## ▸ FULL ROADMAP — M0.1 THROUGH MAINNET

*Milestones M0.1 through M0.9 are completed. Each represents a real, tested, versioned deliverable — not a promise. The development history is fully traceable in the public repository.*

**M0.1** ✓ **PROTOCOL SPECIFICATION & ARCHITECTURE**

*Designed from first principles for offline-first operation. No prior L1 could be adapted — the architecture had to be purpose-built.*

- ✓ Block Lattice consensus model (inspired Nano, extended for partitions)
- ✓ ORV (Open Representative Voting) adapted for offline mesh networks
- ✓ 4-level finality model: PENDING / L0 / L1 / L2
- ✓ CRDT-based reconciliation for split-brain partition recovery
- ✓ Multi-transport stack: LoRa / BLE / SMS / Satellite DVB-S2
- ✓ W3C DID identity model specified (did:arxia: format)
- ✓ Ed25519 + Blake3 + ChaCha20-Poly1305 cryptographic primitives selected
- ✓ 193-byte compact block format designed for LoRa 256-byte MTU
- ✓ Threat model and attack vector analysis completed

**M0.2** ✓ **PoC v0.1.0 — CRYPTOGRAPHIC PRIMITIVES**

*First working implementation. Core cryptographic primitives validated end-to-end.*

- ✓ Ed25519 keypair generation and signing
- ✓ Blake3 block hashing
- ✓ Basic Block Lattice — OPEN / SEND / RECEIVE blocks
- ✓ Block verification (hash + signature)
- ✓ Insufficient balance rejection
- ✓ Initial test suite passing on x86_64

**M0.3** ✓ **PoC v0.2.0 — SERIALIZATION & ESP32**

*Compact binary format validated. First cross-compilation to ESP32 hardware target.*

- ✓ Compact binary serialization — 193 bytes per block
- ✓ 73% size reduction vs JSON (711 bytes → 193 bytes) — fits LoRa 256B MTU
- ✓ to_compact_bytes() + from_compact_bytes() roundtrip validated
- ✓ Double-spend detection ported to ESP32
- ✓ Hardware RNG via esp_random() — cryptographic TRNG
- ✓ Tamper detection: hash mismatch + signature forgery rejection
- ✓ Replay attack prevention: destination mismatch
- ✓ LZ4 compression for LoRa packet batching
- ✓ Cross-compilation to ESP32 QEMU (Xtensa LX6, ESP-IDF v5.3.2)

**M0.4** ✓ **PoC v0.3.0 — CRITICAL BUG FIX + CHAIN INTEGRITY**

*Critical cryptographic vulnerability identified and corrected. Ed25519 signing was performed on hex ASCII representation (64 bytes) instead of raw Blake3 hash bytes (32 bytes) — invalidating all prior signatures.*

- ✓ **CRITICAL FIX: Ed25519 now signs raw Blake3 bytes (32B) not hex ASCII (64B)**
- ✓ **Chain integrity: sequential nonce enforcement + hash chain**
- ✓ **Vector Clock integration in block structure**
- ✓ **All prior tests re-validated with corrected cryptography**

M0.5

## ✓ PoC v0.4.0 — ORV CONSENSUS + CRDTs — 24/24 TESTS

*Full consensus engine validated. CRDT mathematical properties proved. Both platforms passing identical test suites.*

- ✓ **ORV stake-weighted — cast_vote(), verify_vote(), collect_votes()**
- ✓ **resolve_conflict_orv() — cascade: stake → vector_clock → hash_tiebreaker**
- ✓ **5 ORV scenarios: 60/40 stake, 50/50 tie, forged vote, threshold, valid collection**
- ✓ **PN-Counter CRDT — commutativity, idempotency, associativity proved**
- ✓ **OR-Set CRDT — transaction sets**
- ✓ **Vector Clocks — causal ordering + concurrency detection**
- ✓ **reconcile_partitions() — Block Lattice → CRDT pipeline**
- ✓ **Real double-spend: 2 valid Ed25519 signatures, same nonce, different partitions**
- ✓ **assess_finality() — correct output for all 4 finality levels**
- ✓ **x86_64: 24/24 tests PASS | ESP32 QEMU: 24/24 tests PASS**
- ✓ **ESP32 performance: keygen 15.5ms, verify 10ms, SEND 5.5ms, total suite 199ms**
- ✓ **Supply preserved across both platforms: 1700 ARX**

M0.6

## ✓ PoC v0.5.0 — GOSSIP PROTOCOL — 34/34 TESTS

*The last critical technical gap closed. L1 finality now exists in simulation — conditioned on gossip sync success. Without this deliverable, all transactions above 10 ARX were PENDING until L2.*

- ✓ **GossipTransport trait — abstraction over any physical transport**
- ✓ **SimulatedTransport — configurable latency, packet loss, seeded PRNG for CI**
- ✓ **GossipMessage with BTreeMap — deterministic hash → valid Ed25519 signature**
- ✓ **merge_nonce_registries() — coherent / higher nonce / ConflictDetected**
- ✓ **sync_nonces_before_l1() — 3s timeout, automatic L0 fallback**
- ✓ **assess_finality() conditioned on SyncResult::Success**

**10 TEST SCENARIOS:**

- ✓ **Test 25: sync OK → L1 GRANTED**
- ✓ **Test 26: same nonce, different block_hash → DOUBLE-SPEND DETECTED → L0**
- ✓ **Test 27: timeout 3s → L0 FALLBACK**
- ✓ **Test 28: forged message → REJECTED (invalid Ed25519)**
- ✓ **Test 29: 0 neighbors → L0 FALLBACK**
- ✓ **Test 30: 5-node linear chain → CONVERGENCE 4 hops, L1 GRANTED**
- ✓ **Test 31: single bridge topology → CONVERGENCE via bridge C, L1 GRANTED**
- ✓ **Test 32: broken bridge, C offline → L0 FALLBACK — partition isolated**
- ✓ **Test 33: degraded network (latency + loss, seed 42) → L1 GRANTED**

- ✓ Test 34: degraded network + double-spend → L0 FALLBACK
- ✓ x86_64: 34/34 PASS | ESP32: port in progress (no_std constraints)

M0.7

## ✓ PUBLIC GITHUB REPOSITORY — CI GREEN

*Monorepo Rust workspace publicly live. 98.7% Rust. CI passing. Branch protection active.*

- ✓ arxia-core, arxia-crypto, arxia-lattice, arxia-consensus, arxia-crdt
- ✓ arxia-gossip, arxia-finality, arxia-transport, arxia-relay
- ✓ arxia-did, arxia-wasm, arxia-storage, arxia-proto (stubs — M12-M18)
- ✓ bin/arxia-node, targets/esp32, examples (4 compilable), contracts
- ✓ cargo fmt + cargo clippy -D warnings + cargo test --workspace — all green
- ✓ cargo-audit + cargo-deny — dependency security
- ✓ ESP32 Xtensa cross-compilation workflow
- ✓ Dependabot — automated dependency updates
- ✓ Branch protection main — PR required, CI must pass

M0.8

## ✓ TECHNICAL DOCUMENTATION SUITE

*Whitepaper v29 (29 iterative versions). Public + internal audits. 5 complete technical docs in repository. 16/22 audit findings resolved.*

- ✓ **arxia_technical_v29.docx** — 55 KB — full protocol specification
- ✓ **arxia_audit_public_v29.docx** — 28 KB — investor-facing, 7.5/10 technical score
- ✓ **arxia_audit_v29.docx** — 16 KB — internal differential audit
- ✓ **TOKENOMICS.md** — Supply, allocation, vesting, fees, staking, IDO scenarios
- ✓ **HELIUM_LESSONS.md** — Honest failure analysis + structural differentiation
- ✓ **WASM.md** — Complete runtime spec, 5 host functions, contract examples
- ✓ **RUNNING_A_NODE.md** — ESP32 + x86_64, config, metrics, troubleshooting
- ✓ **WRITING_CONTRACTS.md** — Full guide, 3 patterns, compilable Rust examples
- ✓ **pruning.rs** — Implemented — 9 unit tests, 7-day expiry, 256-entry cap

M0.9

## ✓ PUBLIC PRESENCE — SITE & SOCIAL

*Web presence established. Anonymous stack: Whonix + GoLogin + residential proxy + Njalla domain.*

- ✓ arxia.network — live
- ✓ Twitter/X account active
- ✓ GitHub organization: ArxiaLayer1
- ✓ 6-section technical problem/solution content published
- ✓ Metadata-clean pipeline — mat2/exiftool before any public push

---

## ▸ UPCOMING MILESTONES

*All future milestones are subject to change based on technical progress, market conditions, and funding.*

**M1-3**

## FOUNDATIONS — PRESALE READY

*Objective: legally and technically ready to receive capital.*

- ☐ LLC Delaware entity (500 USD, 1 week)
- ☐ MiCA legal opinion + ARX token classification (utility)
- ☐ SAFT structure for seed investors
- ☐ ERC-20 ARX smart contract deployed on Base
- ☐ Smart contract audit — CertiK or Trail of Bits — prerequisite for SAFT and IDO
- ☐ 2 named public advisors confirmed
- ☐ MOU signed with at least 1 named ONG
- ☐ Whitepaper public PDF — clean, metadata-stripped
- ☐ Discord server open

**SEED ROUND — 2.4M USDC @ 0.02 USDC/ARX**

SAFT | Cliff 6 months | Vesting 24 months | Sablier V2 on Base

Targets: Outlier Ventures, Spartan, NGC, Cogitent, CV VC (Zug)

Parallel grants: Ethereum Foundation, UNHCR Innovation, EU Horizon

**M3-6**

## PROTOTYPE TERRAIN + COMMUNITY WARM-UP

*Objective: first real LoRa transaction on hardware. Community primed for IDO.*

- ☐ Gossip protocol port to ESP32 (no_std channels + esp_timer)
- ☐ Meshtastic firmware integration on T-Beam
- ☐ ESP32 flash persistence (NVS — nonce registry)
- ☐ 2-5 T-Beams communicating in real field conditions
- ☐ First LoRa transaction filmed and published publicly — L1 finality, zero internet
- ☐ Private testnet operational
- ☐ Field measurements: SF9 throughput, gossip overhead, range
- ☐ Internal cryptography audit
- ☐ External security audit M6 — 150k USDC (CertiK / Trail of Bits)

**COMMUNITY PRE-IDO**

- ☐ Press release — CoinDesk, Decrypt, The Block
- ☐ KOL outreach — targeted crypto influencers
- ☐ Airdrop bounty program launched
- ☐ Discord — target 5,000+ members before IDO
- ☐ CoinGecko + CoinMarketCap listing submitted

**PRE-IDO**

## PUBLIC TOKEN LAUNCH

*Triggered when M3-6 is complete AND community benchmarks are met.*

**PREREQUISITES — ALL MUST BE ✓ BEFORE LBP OPENS**

- ☐ ERC-20 smart contract audited and published
- ☐ LoRa transaction video live
- ☐ M6 security audit published
- ☐ Discord 5,000+ members
- ☐ CoinGecko + CoinMarketCap confirmed

**FJORD FOUNDRY LBP — 72H ON BASE**

- ☐ LBP: 0.08 USDC start | 0.03 USDC floor | 150M ARX (15% supply)
- ☐ Uniswap V3 liquidity pool post-LBP (ARX/USDC on Base)
- ☐ Sablier V2 vesting activated — team + seed investors

| Scenario | IDO Price | Seed Multiple |
|---|---|---|
| Bear | 0.03 USDC | 1.5× |
| Base | 0.10 USDC | 5× |
| Bull | 0.30 USDC | 15× |
| Ultra | 1.00 USDC | 50× |

**M6–12**

## DAG CONSENSUS + PUBLIC TESTNET

- ☐ Block Lattice production — RocksDB, pruning 100k blocks
- ☐ ORV on-chain delegation
- ☐ CRDTs full reconciliation pipeline
- ☐ Chaos network tests — partitions, reconnections
- ☐ Key recovery SLIP39 2-of-3
- ☐ Node staking on-chain (500 ARX minimum)
- ☐ RelayReceipt + scoring + slashing
- ☐ L0 rate limiting anti-sybil
- ☐ Public testnet — open to external developers
- ☐ Bug bounty launched — 250k USD eq. ARX (funded by IDO)
- ☐ Full stack audit M12 — 150k USDC

**M12–18**

## MOBILE APP + DID + ONG FIELD PILOT

- ☐ React Native offline-first (Android 8+ / iOS 13+)
- ☐ Wallet: create, import SLIP39, send/receive ARX
- ☐ Android Keystore + StrongBox hardware enclave
- ☐ W3C DID complete — did:arxia:, offline resolution O(1)
- ☐ Verifiable Credentials W3C VC Data Model v2.0
- ☐ ORV on-chain delegation + LoRa vote propagation
- ☐ Named ONG partner — 50-node field deployment
- ☐ DVB-S2 satellite agreement + signed stake snapshots
- ☐ Full stack audit M18

**M18–24**

## MAINNET PREPARATION

- ☐ Land registry use case
- ☐ Optional KYC/AML layer (institutional ONGs)
- ☐ Tokenomics live on testnet — real rewards, active slashing
- ☐ DAO governance tested on-chain
- ☐ Wasmer WASM runtime — 5 host functions, instruction metering
- ☐ Final pre-mainnet audit — 2nd independent audit
- ☐ DAO transition criteria verified

**M24+**

## MAINNET

- ☐ Bridge ERC-20 → L1 — Lock-and-Mint, 5/9 multi-sig, 72h timelock

- ☐ ARX ERC-20 → ARX native 1:1 migration (24-month window)
- ☐ Permanent bug bounty
- ☐ UNHCR / IRC partnerships announced
- ☐ Ecosystem grants open — 200M ARX
- ☐ DAO transition

## ▸ NON-TECHNICAL BLOCKERS

*These three items are independent of technical progress. They condition access to institutional capital, ONG partnerships, and developer credibility.*

| ID | BLOCKER | IMPACT |
|---|---|---|
| B1 | Founders identifiable | Blocks all Tier 1/2 VCs (KYC mandatory) |
| B2 | 2 named public advisors | Blocks external credibility — 5/9 multi-sig unpopulated |
| B3 | MOU signed with 1 ONG | Blocks humanitarian use case — zero field proof |

**MITIGATION (acceptable for Tier 2 VCs)**

- → Strong pseudonyms with active public GitHub history
- → Private data room under NDA — real identities shared to VCs only
- → 2 public advisors endorsing the project publicly

## ▸ CHRONOLOGICAL SUMMARY

| | |
|---|---|
| M0.1 | ✓✓ Protocol specification + architecture |
| M0.2 | ✓✓ PoC v0.1.0 — crypto primitives |
| M0.3 | ✓✓ PoC v0.2.0 — 193 bytes, ESP32 cross-compilation |
| M0.4 | ✓✓ PoC v0.3.0 — critical crypto bug fixed |
| M0.5 | ✓✓ PoC v0.4.0 — ORV + CRDTs, 24/24 tests |
| M0.6 | ✓✓ PoC v0.5.0 — Gossip protocol, 34/34 tests |
| M0.7 | ✓✓ GitHub public, CI green, branch protection |
| M0.8 | ✓✓ Whitepaper v29, audits, 5 technical docs |
| M0.9 | ✓✓ Site web, Twitter/X, public presence |
| M1–3 | Legal + ERC-20 audited + Seed round |
| M3–6 | T-Beams terrain + LoRa video + Community 5k |
| PRE-IDO | LBP Fjord Foundry 72h → 4.5M–12M USDC |
| M6–12 | Public testnet + Bug bounty + ORV production |
| M12–18 | Mobile app + DID + ONG field pilot |
| M18–24 | Mainnet prep + Final audit + DAO governance |

| | |
|---|---|
| **M24+** | Mainnet + Bridge + ARX native migration |

All milestones, timelines, and parameters are subject to change.