[CLASSIFIED — TECHNICAL BRIEFING]

ARXIA

.EXE

LAYER 1 ◆ OFFLINE-FIRST PROTOCOL ◆ MESH CONSENSUS

Technical Implementation Document // v29.0 — Seed Round Ready

For developers, analysts & investors

First blockchain protocol natively designed for fragmented and intermittent networks.

2026 // CONFIDENTIAL

We live in the illusion of stability.

Geopolitical tensions are escalating. Power struggles are multiplying. Critical infrastructure is a target. Every day that passes looks like the one before — until the day it looks like nothing you've ever known.

That day, the internet goes down. Power grids fail. Servers shut off. And with them — silently, completely — your entire digital wealth becomes inaccessible. Not stolen. Not destroyed. **Just useless.**

580 million people hold crypto. $3 trillion in value stored on-chain. Entire savings, lifetimes of wealth, institutional capital. And the entirety of this edifice rests on a single condition: that a server somewhere in the world is online.

The internet is humanity's largest critical infrastructure. And the most fragile. And the most targeted.

In movies, in games, in scenarios we watch thinking "it will never happen" — a medium of exchange always emerges from chaos. Bottle caps. Rations. Hours of labor. Anything that allows two people to agree on value and survive together. Because humans trade. Always. Even when everything collapses.

No one planned a cryptographic currency for that moment. Bitcoin goes down with the internet. Ethereum goes down with the internet. Solana, USDC, every stablecoin, every wallet — all silent, all useless, the moment the network disappears. The crypto industry spent 15 years building revolutionary financial systems that rely entirely on the same fragile infrastructure as the banks they claim to replace.

Arxia is built for the aftermath.

For the moment when networks go down and people still need to transact. For the refugee crossing a border with their wealth on a phone. For the investor whose portfolio is worth millions and who cannot buy water from their neighbor if the network is dead. For everyone who understood that true monetary sovereignty cannot depend on a connection.

This is not a feature. This is not an offline mode bolted onto an existing architecture. It is the architectural foundation of Arxia — a Layer 1 designed from scratch so that your monetary power follows you everywhere. Even where nothing else works anymore.

▶1. THE PROBLEM NO ONE HAS SOLVED

Every existing blockchain was built with a fundamental assumption: the internet is available. This assumption is false. Not just in war zones. Everywhere. For everyone. Overnight.

> ⚠️ **LE RISQUE UNIVERSEL — 2026**
> 580 millions de détenteurs de cryptomonnaies dans le monde. Plus de 3 000 milliards USD de valeur stockée on-chain. Fortune personnelle, épargne d'une vie, capital institutionnel, réserves souveraines. La totalité de cette richesse devient inaccessible — zéro transaction, zéro transfert — dès qu'internet tombe. Pas dans une guerre. N'importe où. N'importe quand.

This is not a hypothetical scenario. These are documented, cyclical, and accelerating events.

- ◆ Carrington-type solar storm — In 1859, a coronal mass ejection destroyed the entire global telegraph infrastructure. The modern equivalent: fried satellites, internet backbone down, regional electrical blackout. NASA estimates a 12% probability of a major event within the next 10 years. Bitcoin becomes unusable. Arxia continues.
- ◆ Cyberattack on internet infrastructure — Large-scale BGP hijacking, submarine cable sabotage (already happened in the Red Sea, 2024), attacks on root DNS servers. In February 2024, three submarine cables cut simultaneously isolated 25% of West Africa from the internet for weeks. This type of event does not only target war zones.
- ◆ Cascading electrical blackout — The 2003 cascading power failure left 55 million people in the United States and Canada without power for several days. Data centers go down. Blockchain nodes shut off. Centralized exchanges become inaccessible. A $10 million USD crypto portfolio is worth zero transactionally — as long as the electrical grid is offline.
- ◆ Government network shutdown — including in democracies — 182 deliberate internet shutdowns in 35 countries in 2023 (Access Now). Gaza, Ukraine, Iran, Myanmar — but also India (recurring regional shutdowns during civil unrest), Ethiopia, Brazil. The network kill switch has become a standard political tool. No current blockchain can withstand it.

💸 QUAND INTERNET TOMBE — VOTRE RICHESSE CRYPTO

Bitcoin, Ethereum, Solana, tout stablecoin — inaccessibles. Zéro transaction possible. Le wallet hardware garde vos clés mais personne ne peut rien transférer. L'homme le plus riche du monde avec 1 milliard USD en BTC ne peut pas acheter une bouteille d'eau à son voisin via crypto si le réseau est mort. Il n'existe aujourd'hui aucune monnaie d'échange cryptographique fonctionnelle sans internet — exactement le moment où une monnaie résiliente est la plus nécessaire.

In post-apocalyptic movies and video games, an improvised medium of exchange always emerges — bottle caps, cigarettes, ration points — to access shelter, food, protection. This currency improvises where nothing was planned. Arxia is what should have been planned. A secure cryptographic currency that works when everything else stops — not by accident, but because it's its architectural purpose.

Active conflict zones are the most extreme case — and the best testing ground. If Arxia works in Gaza or Ukraine when the internet is intentionally cut, it works everywhere else. War is not the sole target market — it's the proof of maximum resilience.

Arxia solves this problem at the protocol layer — not with an external patch.

▶ 2. GENERAL ARCHITECTURE

Arxia is a Layer 1 whose consensus protocol was natively designed for fragmented and intermittent networks. The internet is the optimal use case — not the prerequisite.

LAYER	SPEC TECHNIQUE
TRANSPORT	Multi-modal : LoRa (Meshtastic), Bluetooth BLE, SMS/GSM, WiFi Direct, Satellite (Blockstream). Chaque nœud choisit le meilleur canal disponible.
CONSENSUS	Block Lattice (inspiré Nano). Chaque compte a sa propre chaîne SEND/RECEIVE indépendante. Consensus ORV adapté offline. Reconciliation globale asynchrone par poids de stake.

STATE	Modèle de compte local signé (inspiré M-Pesa). Chaque wallet maintient son propre ledger signé par clé privée. Pas d'UTXO global requis offline.
RECONCILIATION	CRDTs (Conflict-free Replicated Data Types) + Vector Clocks pour merger les DAGs locaux sans conflit lors de la reconnexion réseau.
IDENTITÉ	DID (Decentralized Identifiers) W3C standard — identité souveraine portable, vérifiable sans serveur central, compatible offline.

▶3. WHY A LAYER 1 — AND NOT JUST A TOOL

Technically, it is possible to sign a transaction with Ed25519 and send it via LoRa without any blockchain. This is true. Meshtastic already does it with text messages. The legitimate question is therefore: why a Layer 1? What does a blockchain bring that signed messaging over LoRa cannot?

The answer is in five points. Together, they define the difference between a tool and a monetary protocol.

3.1 LE PROBLÈME DU « COMBIEN T'AS ? »

Without L1, each phone has its own version of reality. Alice says she has 100 ARX. Bob says Alice already sent him 80. Charlie says Alice sent him 60 on the same day. Who is right? In two isolated network partitions, all three claim to have a valid signed transaction. Without a shared global ledger, there is no answer — there are only local opinions.

The Layer 1 is exactly this reconciliation mechanism — the single source of truth toward which all partitions converge when they reconnect. Without it, Arxia is digital hawala: trust tokens, not a currency.

3.2 DOUBLE-SPEND AT SCALE

A signed messaging tool does not protect against inter-partition double-spending. Alice can send the same 50 ARX to Bob in partition A and to Charlie in partition B — simultaneously, both locally valid. Without a global consensus protocol, both transactions have a correct signature. Both recipients believe they have received. Alice has duplicated her wealth.

The Arxia L1 solves this problem via the unique nonce per wallet + ORV consensus at reconciliation (Section 4). The partition with the highest stake weight wins. The other is rolled back. It's a protocol — not a social convention.

3.3 THE INCENTIVE THAT MAKES NODES EXIST

Why would someone spend $31 on a T-Beam, place it on their roof in a conflict zone, and run a LoRa node 24/7 on solar battery? Not out of philanthropy — because they earn ARX. The node operator reward (25% of supply, decreasing over 60 months) is the economic mechanism that makes the physical network exist.

Without L1, there is no token. Without a token, there is no incentive. Without incentive, no one deploys a node. Without nodes, the mesh network does not exist. It's the same logic as Helium (LoRa IoT), Filecoin (storage), or Ethereum (smart contracts) — the token is the fuel that powers the physical infrastructure. Note on the Helium analogy: Helium deployed 900,000 hotspots but generated near-zero real IoT traffic. The failure is documented and the analogy deserves to be made explicit. Arxia's structural difference is that the target users (populations in conflict zones, refugees, NGOs) exist independently of the token price — it is not a network waiting for hypothetical IoT demand. But the bootstrap circularity problem remains real: ARX rewards have value only if the token has a price, and the token has a price only if there is

demand. Arxia's answer is that Phase 1 deployment relies on non-token bootstrapping: nodes subsidized via the Ecosystem Fund, institutional NGO deployment, and community nodes — before the token incentive takes over at M12+. The two mechanisms are sequential, not simultaneous.

3.4 SOVEREIGN IDENTITY WITHOUT A CENTRAL SERVER

A DID (Decentralized Identifier) anchored on an L1 has verifiable proof of precedence by anyone, anytime, without trusting Arxia or any server. Farid leaves Syria with his diplomas, property rights, medical history — cryptographically signed and anchored on the chain. In Turkey, any node can verify authenticity without contacting Syria.

Without L1, this DID relies on a database managed by Arxia — i.e., a centralized database with a decentralized logo. The L1 is what makes verification mathematically independent of any trusted entity, including Arxia.

3.5 TOOL VS PROTOCOL — THE DIFFERENCE THAT MATTERS TO INVESTORS

Without L1, Arxia is an open source tool — useful, copyable in a week, non-monetizable, non-investable. Anyone can fork the code and deploy the same thing without ARX. There is nothing to raise, nothing to buy, no economy to capture.

With the L1, Arxia is a monetary protocol with its own economy. The ARX token captures the value of every relayed transaction, every active node, every anchored DID. The ecosystem depends on the Arxia network — not on Arxia Labs. It's the difference between a product and an infrastructure.

SANS L1 — OUTIL	AVEC L1 — PROTOCOLE
Messaging signé sur LoRa	Protocole monétaire avec économie propre
Bons de confiance locaux	Ledger global partagé — source de vérité
Aucun incentive nœud	250M ARX pour les opérateurs de nœuds
Open source, forkable, non monétisable	Token ARX capture la valeur du réseau
Double-spend non résolu inter-partitions	Double-spend résolu par consensus ORV
Rien à lever. Rien à acheter.	**Infrastructure. Pas un produit.**

4.1 POURQUOI UN DAG PLUTÔT QU'UNE BLOCKCHAIN LINÉAIRE

A classical blockchain requires a global transaction ordering validated by all nodes simultaneously. Impossible without real-time network synchronization. A DAG natively tolerates parallel transactions without strict global ordering.

ANALOGIE TERRAIN

10 villages isolés par une guerre. Chacun tient son propre registre des échanges. Quand les routes rouvrent, ils comparent et réconcilent. Personne n'a eu besoin d'un serveur central pendant l'isolement.

4.2 DOUBLE-SPEND PREVENTION WITHOUT REAL-TIME SYNC

Each transaction carries a unique, incremental nonce signed by the sender's private key:

```
Transaction { sender: 0xABC, receiver: 0xDEF, amount: 5, nonce: 47, signature:
sign(privKey, hash(tx)) }
```

- Nonce 47 can only be used once by this wallet.
- At reconciliation, two transactions with the same nonce = conflict automatically detected.
- Resolution rule: for ordered events (vector A < vector B), the causally earlier transaction is accepted. For concurrent events (incomparable vectors, e.g. [A:3,B:2] vs [A:2,B:5]), the tiebreaker is deterministic: the transaction with the lowest lexicographic hash is accepted (hash(tx_A) < hash(tx_B) → A wins). This tiebreaker is computable offline and gives the same result on all nodes at reconciliation.

4.3 VECTOR CLOCKS — COMPRESSION AND GARBAGE COLLECTION

Without a common clock (NTP impossible offline), Arxia uses Vector Clocks (Lamport, 1978). Each node maintains a vector of counters. Comparison determines whether events are ordered or concurrent. Use in the protocol: the Vector Clock is embedded in each block and merged in receive() during RECEIVE block creation — it captures the causal ordering of transactions at the time of their creation. Its role in conflict resolution at reconciliation is defined as follows: (1) for causally ordered events, the Vector Clock determines precedence — the earlier transaction wins; (2) for concurrent events (incomparable vectors), the deterministic lexicographic hash tiebreaker applies. The Vector Clock integration in the ORV resolution algorithm — where it is consulted first before the hash tiebreaker for each nonce conflict — is validated in PoC v0.4.0 (resolve_conflict_orv, cascade stake_weighted → vector_clock → hash_tiebreaker). Production integration in the main transaction flow is the M6-M12 deliverable from the ORV backlog.

```
NodeA: [A:3, B:2, C:1]  NodeB: [A:2, B:5, C:1]  → Concurrent (neither before / nor after)
```

Scalability problem: in a mesh with constantly joining/leaving nodes, vectors grow in O(n). Arxia addresses this via two mechanisms: (1) Periodic pruning — entries for nodes silent for more than 7 days are compressed into a signed aggregate counter. (2) Dotted Version Vectors (DVV) — a compact variant of vector clocks designed for distributed systems with high turnover. The maximum size of a vector clock in Arxia is capped at 256 active entries. Behavior beyond the cap (documented edge case): if 256 active entries are reached despite pruning (exceptionally dense partition), entries with the lowest counter and inactive the longest are force-pruned in ascending activity order until back under the cap. This forced pruning is logged and reported to the operator. Documented risk of forced pruning: forced removal of active entries can introduce causal ordering ambiguities — two previously ordered events can become concurrent after pruning. In practice, this triggers the deterministic hash tiebreaker, not a coherence bug. This behavior has not yet been tested under load with active pruning — it is an M6 deliverable. Justification for the 256 cap: a T-Beam deployment at ~$25 in a dense urban km² reaches LoRa radio saturation before reaching 256 simultaneously active nodes (SF9 range ≈ 15 km, physical density limited by duty cycle and radio collisions). Field estimate: an NGO camp of 10,000 people typically represents 5-20 deployed relay nodes, not 256. The parameter is configurable by governance for dense urban deployments if necessary.

▶5. MULTI-MODAL TRANSPORT LAYER

5.1 LORA VIA MESHTASTIC — PRIMARY OFFLINE CHANNEL

LoRa (Long Range) is a low-power radio technology on unlicensed bands (868 MHz EU, 915 MHz US). Meshtastic is the open source firmware that turns a LoRa module into a mesh node.

- ◆ 2–15 km urban, up to 40 km open terrain — Range
- ◆ 250 bps – 5 kbps (sufficient for signed transactions ~500 bytes) — Throughput
- ◆ **~100mW en transmission, fonctionne sur batterie ou panneau solaire** — Power consumption
- ◆ **ESP32 + module LoRa SX1276 = ~15 USD** — Hardware

5.2 SMS FALLBACK

Even when the internet is cut, the GSM network often remains available. An Arxia transaction encoded in base64 fits in 2–3 SMS. The recipient validates the signature locally without a server.

PREUVE DE CONCEPT

M-Pesa Kenya traite 50 milliards USD/an via SMS sans blockchain. Arxia emprunte ce mécanisme et l'applique à un ledger cryptographiquement sécurisé.

5.3 BLOCKSTREAM SATELLITE

Satellite broadcast services (Blockstream Satellite or equivalents) continuously broadcast data on 4+ satellites covering 99% of the Earth's surface. An Arxia node can receive updates without internet via a low-cost antenna (~$50). Reception is entirely offline. An integration agreement with a satellite operator is being negotiated — the architecture supports any unidirectional DVB-S2 broadcast service.

▶ 6. FLOW COMPLET D'UNE TRANSACTION OFFLINE

Scenario: Alice (Gaza, internet cut) pays Bob 5 ARX for water. Both have the Arxia app on Android.

01	Alice ouvre l'app. Son wallet affiche $100 ARX — state local, signé, stocké en mémoire chiffrée sur le téléphone.
02	Alice entre 5 ARX, scanne le QR de Bob ou active BLE. Son téléphone construit la transaction : {sender, receiver, amount:5, nonce:47, timestamp_vectoriel}.
03	Alice signe la transaction avec sa clé privée (Ed25519). La signature prouve que c'est bien elle, sans serveur tiers.
04	La transaction (~500 bytes) est envoyée à Bob via BLE. Son app valide : signature correcte ? Nonce 47 jamais vu ? Solde suffisant ?
05	Validation OK. Bob affiche +5 ARX. Alice affiche $95 ARX. La transaction est stockée dans leurs DAGs

	locaux.
06	Les deux téléphones propagent la transaction aux nœuds Arxia à portée LoRa. Propagation en flood dans le mesh.
07	Quand internet revient (1h, 1 jour, 1 semaine), les nœuds synchronisent leurs DAGs avec le réseau global. Réconciliation déterministe via vector clocks.

▶ 7. RECONCILIATION AND CRDTS

When two mesh partitions rejoin, Arxia merges their local DAGs without losing data or creating double-spends.

CRDTs (Conflict-free Replicated Data Types) are data structures mathematically designed so that two states are always merged deterministically.

◆ balance = sum of credits received — sum of debits issued — PN-Counter CRDT (two opposing G-Counters: one for incoming credits, one for outgoing debits. balance = G-Counter credits – G-Counter debits. Merge is monotone on each counter independently). Important caveat on negative balances: a pure mathematical PN-Counter can return negative values — this is inherent to the structure. The PoC demo intentionally displays “Partition A: -5” to prove the CRDT convergence properties, not to model a real balance. In production Arxia, the PN-Counter never manages the balance alone: decrements are first validated by the Block Lattice (checking the current balance in the account chain) before being applied to the CRDT. A decrement that would make the balance negative is rejected by the Block Lattice before even reaching the CRDT — this is the sequence documented in Section 7 (chain validation as prerequisite for CRDT merge).

◆ each transaction is a unique element (hash). Merge = union. Duplicates eliminated automatically. — OR-Set CRDT

CRDT / Block Lattice articulation: The Block Lattice enforces strict intra-chain ordering (nonce n before nonce n+1 — cannot skip). CRDTs operate on balances and transaction sets, not on the internal ordering of chains. The reconciliation sequence is therefore: (1) validate the internal coherence of each account chain (block ordering, continuous nonces) — this step is a prerequisite for merge; (2) apply CRDT merge only on validated chains. A block whose internal chain is incoherent is rejected before entering the CRDT — the two paradigms are not in conflict but in sequence. PoC v0.4.0 status: DELIVERED. The PN-Counter is validated as a mathematical primitive (convergence, commutativity, idempotence, associativity) AND integrated in reconcile_partitions() which computes the reconciled balances from validated SEND/RECEIVE blocks of each partition. Tests confirm convergence after real partition on both platforms.

◆ transaction with the oldest vector clock wins. The other is marked ‘rejected’ and archived. — Nonce conflict

▶ 8. DECENTRALIZED IDENTITY (DID)

Arxia implements the W3C DID (Decentralized Identifiers) standard natively at L1 level. An Arxia DID is a sovereign identity, verifiable without a central server, portable across borders, resolvable offline via the local DAG.

Identifier format: did:arxia:{base58(blake3(pubkey_ed25519))} — the identifier is deterministically derived from the wallet’s Ed25519 public key. No central registry required for creation.

DID Document (structure): { "id": "did:arxia:3vZ9...", "verificationMethod": [{ "id": "did:arxia:3vZ9...#key-1", "type": "Ed25519VerificationKey2020", "controller": "did:arxia:3vZ9...", "publicKeyMultibase": "z6Mk..." }], "authentication": ["did:arxia:3vZ9...#key-1"], "assertionMethod": ["did:arxia:3vZ9...#key-1"] }

Offline resolution: the Arxia DID resolver looks up the DID document in the node's local DAG (anchored via an Open block on the Block Lattice). No DNS calls, no third-party servers. Resolution time: O(1) on a synchronized node, O(local lookup) in an offline partition.

Verifiable Credentials (VC): any issuer with an Arxia DID can sign credentials conforming to W3C VC Data Model v2.0. Verification uses only the issuer's public key — verifiable offline without contacting the issuer.

Physical portability: the wallet seed (and therefore the private key controlling the DID) is encoded via SLIP39 (2-of-3 shares). Signed credentials are exported in compact JSON on physical media (QR code, NFC). A refugee can carry their DID + credentials without a phone — 2 SLIP39 shares are sufficient for reconstruction.

Offline revocation: an Arxia DID is revoked by creating a specific block (type REVOKE) signed by the controller key. Revocation propagates via the mesh upon reconnection. In an offline partition, a verifier sees the last known state — documented risk displayed in the UI.

Target implementation library: github.com/spruceid/ssi (Rust, W3C DID Core + VC conformant, already referenced Section 10.4). Integration M12-M18 in the React Native mobile stack.

USE CASE — RÉFUGIÉ

Farid quitte la Syrie avec son téléphone. Son DID Arxia contient ses diplômes, son historique professionnel, ses droits de propriété — tout signé cryptographiquement. En Turquie, les services sociaux vérifient ses credentials offline sans contacter la Syrie.

```
{   "id": "did:arxia:0xABCDEF...",   "verificationMethod": [{ "type": "Ed25519",
"publicKey": "..." }],   "credentials": [     { "type": "PropertyTitle", "issuer":
"did:arxia:municipality", "signature": "..." },     { "type": "Education",     "issuer":
"did:arxia:university",   "signature": "..." }   ] }
```

▶ 9. COMPLETE TECHNOLOGY STACK

LAYER	SPEC TECHNIQUE
LANGAGE CORE	Rust — sécurité mémoire, performance, compilation WASM pour clients légers mobile.
DAG CONSENSUS	Block Lattice exclusivement (Nano). Chaque compte a sa propre chaîne de blocs indépendante (SEND + RECEIVE blocks). Consensus : ORV (Open Representative Voting) adapté offline. En partition réseau : représentants votent localement, partition avec le plus grand poids de stake gagne à la reconciliation. Tangle (IOTA) explicitement abandonné — incompatible avec les partitions longues.
CRYPTOGRAPHIE	Ed25519 (signatures), Blake3 (hashing, 4x plus rapide que SHA256), ChaCha20-Poly1305 (chiffrement local).

TRANSPORT LORA	Meshtastic firmware (C++). Sérialisation binaire compacte bidirectionnelle (validée PoC v0.4.0) : 193 bytes par transaction — sous le MTU LoRa de 256 bytes sans compression. Format : clé publique Ed25519 raw (32 bytes) + hash précédent raw (32 bytes) + type de bloc (1 byte) + destination/source raw (32 bytes) + montant/balance/nonce/timestamp (8 bytes × 4) + signature Ed25519 (64 bytes). to_compact_bytes() + from_compact_bytes() implémentés et validés par roundtrip test (VALID sur x86_64 et ESP32). Compression LZ4 optionnelle pour les frames batch.
MOBILE APP	React Native + Rust via FFI. Android 8+ / iOS 13+. Wallet offline-first, synchronisation arrière-plan.
SMART CONTRACTS	Runtime WASM : Wasmer (github.com/wasmerio/wasmer) en mode sandbox isolé. Chaque contrat s'exécute dans une instance WASM indépendante sans accès mémoire croisé. Exécution déterministe : même bytecode + même inputs = même output sur tous les nœuds. Pas de système de fichiers, pas d'accès réseau depuis le contrat. Niveaux de connectivité et opcodes autorisés : L0/L1 (offline) — transfert ARX signé, vote de gouvernance signé, claim DID (vérification de credential), lecture de l'état local du compte. L2 uniquement (finalité absolue requise) — écriture dans le registre foncier, création de DID, émission de Verifiable Credential, modification de paramètres de gouvernance. Modèle de gas offline : le gas est comptabilisé en nombre d'instructions WASM exécutées (opcodes). Limite offline (L0/L1) : 100 000 instructions par appel. Limite L2 : 10 000 000 instructions. Gas consommé déduit du solde ARX du caller au taux BASE_FEE_ARX/1000 instructions. Un contrat qui dépasse la limite est terminé avec revert — les modifications d'état sont annulées, les frais de gas consommé sont perdus. Host functions exposées au contrat (ABI) : arxia_get_balance(pubkey: [u8;32]) -> u64, arxia_send(to: [u8;32], amount: u64) -> bool, arxia_get_block_hash(nonce: u64) -> [u8;32], arxia_did_verify(credential_json: *const u8, len: usize) -> bool, arxia_log(msg: *const u8, len: usize). Toute autre interaction système est interdite — le sandbox rejette les appels non-listés avec trap. Format de déploiement : un contrat est un fichier .wasm (<64 KB offline, <1 MB L2) ancré dans un bloc de type DEPLOY signé par le déployeur. L'adresse du contrat = blake3(bytecode). Le bytecode est immuable après déploiement — les mises à jour déploient un nouveau contrat. Langage source recommandé : Rust avec ink! (github.com/use-ink/ink) ou AssemblyScript.
DID STACK	W3C DID Core + Verifiable Credentials spec. Résolution via DAG local, pas de DNS.
STOCKAGE	RocksDB (nœud complet). Pruning : snapshot state tous les 100k blocs, archives sur IPFS. Estimation ~2 GB/an. SQLite (mobile) — wallet local uniquement, 50 MB max.

▶10. OPEN SOURCE RESOURCES

9.1 TRANSPORT LAYER

→ github.com/meshtastic/Meshtastic-device
→ github.com/meshtastic/Meshtastic-python

→ github.com/Xinyuan-LilyGO/LilyGO-T-Beam
→ github.com/Blockstream/satellite

9.2 CONSENSUS DAG

→ github.com/nanocurrency/nano-node
*→ [HISTORICAL REFERENCE ONLY — Tangle architecture abandoned in Arxia, incompatible with long network partitions, see Section 13] github.com/iotaledger/iota-core*github.com/iotaledger/iota-core
→ github.com/aleph-zero-foundation/aleph-node

9.3 CRDTS & VECTOR CLOCKS

→ github.com/automerge/automerge
→ github.com/josephg/diamond-types
→ lamport.azurewebsites.net/pubs/time-clocks.pdf

9.4 IDENTITY & DID

→ w3.org/TR/did-core/
→ w3.org/TR/vc-data-model/
→ github.com/spruceid/ssi

9.5 CRYPTOGRAPHIE

→ github.com/dalek-cryptography/ed25519-dalek
→ github.com/BLAKE3-team/BLAKE3
→ github.com/RustCrypto/AEADs

9.6 SMART CONTRACTS WASM

→ github.com/wasmerio/wasmer
→ github.com/use-ink/ink

▶ 11. IMPLEMENTATION ROADMAP

→ VOIR SECTION 22 — ROADMAP RÉVISÉE POST-AUDIT

La roadmap complète et à jour est présentée en Section 22. Elle intègre toutes les corrections issues des audits successifs : audit de sécurité avancé à M6, spécification Block Lattice M1-3, publication structure juridique M1-3, et ajouts liés au mécanisme de finalité L0/L1/L2.

▶12. REFERENCE HARDWARE

LAYER	SPEC TECHNIQUE
NŒUD MESH LORA	TTGO T-Beam (ESP32 + SX1278 LoRa + GPS + batterie 18650) — ~31 USD. Firmware Meshtastic + Arxia node. Autonomie 8–24h batterie.
CLIENT MOBILE	Tout Android 8+ ou iOS 13+. App ~50 MB. Wallet local chiffré. Fonctionne sans data plan (BLE + LoRa via nœud relais proche).
NŒUD COMPLET	Raspberry Pi 4 (50 USD) + module LoRa HAT (30 USD). Syncronise le DAG complet. Idéal hôpitaux, camps ONG, centres communautaires.
SATELLITE RX	Antenne plate Ku-band + LNB (~50 USD) + Raspberry Pi. Reçoit state global via service broadcast satellite DVB-S2 (Blockstream Satellite ou équivalent, accord en cours) sans internet. Réception seule.

▶13. OFFLINE FINALITY PROTOCOL

⚠ **PROBLÈME ADRESSÉ**

La règle nonce + vector clock seule ne protège pas le receveur pendant une partition longue. Bob livre ses biens contre une transaction qui peut être rejetée 2 semaines plus tard à la réconciliation. Arxia définit trois niveaux de finalité explicites.

12.1 FINALITY LEVELS

L0	OFFLINE SANS NŒUD — Transaction BLE/QR uniquement. Finalité probabiliste nulle. Plafond : 10 ARX (≈ 0.30–50 USD selon prix ARX). Avertissement explicite affiché au receveur. Usage : paiements de subsistance. Sémantique critique : une transaction au-dessus du plafond L0 avec zéro confirmation est en état PENDING — elle n'est pas L2. L2 (finalité absolue) requiert ≥67% des validateurs actifs sur le DAG global. Une transaction non confirmée n'atteint jamais L2 par défaut — elle doit être explicitement rejectée ou confirmée. Ce point est critique pour l'implémentation de assess_finality() : 0 confirmations + montant > plafond L0 = PENDING, jamais L2.
L1	OFFLINE AVEC ≥1 NŒUD LORA — Nœuds à portée synchronisent leurs registres de nonces via gossip protocol (délai max 3s) AVANT confirmation. Si sync impossible entre nœuds co-localisés, la transaction est automatiquement reclassée L0. Plafond : 50 USD équivalent ARX (calculé au dernier prix connu via satellite Blockstream, ou prix genesis si aucun oracle offline disponible). L'app affiche le poids de stake de la partition locale — si < 30% du stake total connu, avertissement de risque de rollback affiché explicitement. STATUT D'IMPLÉMENTATION : la finalité L1 repose entièrement sur le gossip protocol. Livré et validé dans le PoC v0.5.0 (34/34 tests PASS, x86_64) : L1 n'est accordé que si sync_nonces_before_l1() retourne SyncResult::Success — timeout, partition isolée ou conflit détecté déclenchent automatiquement le fallback L0. Gap restant : port ESP32 du gossip (contraintes no_std sur mpsc/Instant, livrable M3-M6).

L2	SYNC RÉSEAU COMPLÈTE — Confirmée par ≥67% des validateurs actifs sur le DAG global. Finalité absolue et irréversible. Aucun plafond. Délai : quelques secondes en ligne, différé à la reconnexion offline.

12.2 ANTI-DOUBLE-SPEND PROTECTION BY LEVEL

In L0: the receiver sees an explicit warning and configures their acceptance cap. The recipient field is included in the signature — a captured transaction cannot be replayed to a third party (BLE replay attack blocked).

Stake snapshot: the local partition weight is calculated from the last stake distribution snapshot received via satellite broadcast service or network sync. Satellite trust model: each snapshot is signed by the Arxia Foundation Ed25519 key (public key hardcoded in the protocol, rotatable only by critical governance vote §15.4). A node rejects any snapshot whose signature is invalid. If the snapshot age exceeds 30 days, the display switches to degraded mode and the rollback risk threshold is raised from 30% to 50% as a precaution. Escalation: beyond 60 days without a valid signed snapshot, all L1 confirmations are automatically suspended — only L0 (10 ARX cap, explicit warning) remains available. This behavior is displayed to the user with a satellite status message. Beyond 90 days, the app enters total degraded mode with high-risk warning before any transaction. An attacker controlling satellite broadcasting would need to forge a valid Foundation signature or maintain this control for more than 30 days to benefit from an obsolete snapshot — high attack cost.

In L1: before any confirmation, nearby LoRa nodes synchronize their nonce registries via gossip protocol. If node A and node B are co-located but not synchronized with each other, neither can issue an L1 confirmation — the transaction falls to L0 automatically. This mechanism eliminates L1 double-spend via co-located unsynchronized nodes.

Conditional L1 guarantee: L1 confirmation is secured provided the local partition represents sufficient stake weight. The mobile app displays this weight in real time. A receiver in a minority partition (< 30% stake) sees an ORV rollback risk warning — exactly like L0 displays its risk warning. No hidden guarantees.

```
Transaction { sender, receiver, amount, nonce, vector_clock, max_level_accepted, sig:
sign(privKey, hash(all_fields)) }
```

The receiver field in the cryptographic signature makes any replay attack impossible: the transaction signed for Bob cannot be accepted by Charlie — the signature would not match.

▶14. DAG ARCHITECTURE — BLOCK LATTICE

CLARIFICATION ARCHITECTURALE

Suite aux retours d'audit : Arxia adopte exclusivement le modèle Block Lattice (Nano), et non le Tangle (IOTA). Ces deux paradigmes sont incompatibles. Le Block Lattice est nativement supérieur pour l'offline-first.

14.1 WHY BLOCK LATTICE AND NOT TANGLE

LAYER	SPEC TECHNIQUE
BLOCK LATTICE (Arxia)	Chaque compte a sa propre chaîne de blocs indépendante. La validation locale ne nécessite que l'historique du compte concerné — disponible offline sans synchronisation globale.
TANGLE (IOTA)	Chaque transaction valide deux transactions précédentes via tip selection. Requiert une vue partielle du DAG global pour choisir les tips — structurellement incompatible avec les partitions réseau longues.

14.2 ARXIA BLOCK LATTICE SPECIFICATION

Each wallet maintains two parallel chains: a SEND block chain and a RECEIVE block chain. Each transaction generates an atomic pair:

```
SEND block  { type: SEND,    account: 0xABC, prev_hash, balance: 95, dest: 0xDEF,
amount: 5, nonce: 47, sig } RECEIVE block { type: RECEIVE, account: 0xDEF, prev_hash,
balance: 105, src_block: hash(SEND), sig }
```

- ◆ A SEND block is valid from local creation — it reduces the balance immediately.
- ◆ A RECEIVE block is created by the recipient in response — it increases their balance.
- ◆ Without internet, the RECEIVE block is created offline and propagated to the LoRa mesh.
- ◆ At global reconciliation, SEND/RECEIVE pairs are verified. A SEND without a corresponding RECEIVE remains pending until confirmation.
- ◆ Orphan RECEIVE block — if the recipient loses their device or dies before creating the RECEIVE block: the SEND block has deducted Alice's balance permanently. Mitigation: 90-day timeout. If no RECEIVE block is created within 90 days following the L2 confirmation of the SEND, an automatic refund protocol is triggered — the SEND block is cancelled and the balance restored to Alice. In L0/L1 (offline), the timeout starts at the first network sync of the SEND block. The recipient can delegate RECEIVE block creation to a trusted node via advance offline signature. Documented edge case — temporary liquidity loop: an actor controlling both wallets (sender and receiver) could send funds, never create the RECEIVE block, and recover the funds after 90 days — creating a voluntary blocking cycle. This behavior generates no economic gain (funds are immobilized for 90 days) and is detectable on-chain (repeated SEND blocks without corresponding RECEIVE to the same wallet). Mitigation: a wallet presenting ≥ 3 unanswered SEND blocks to distinct destinations within a 30-day window is marked as suspect and its future transactions are automatically reclassified to L0 (warning to receiver) until resolution.

14.3 CONSENSUS — OFFLINE ORV: SPECIFICATION

Nano uses Open Representative Voting (ORV). Arxia adapts this mechanism for network partitions with the following rules:

- ◆ any wallet with ≥ 0.1% of total supply delegated in its favor. In an offline partition, the 10 representatives with the largest local delegated stake are de facto representatives for that partition. — Representative eligibility
- ◆ ≥ 2/3 of representatives present in the partition, collectively representing ≥ 20% of the partition's total known stake. — Local quorum

- if two partitions voted differently on the same conflict (e.g.: double-spend), the partition with the highest combined stake weight wins. The other is rolled back. In case of a tie (< 5% gap), the conflict is escalated pending L2 confirmation. — Conflict rule at reconciliation
- if a partition contains fewer than 3 eligible representatives, transactions are processed in L0 mode (10 ARX cap, explicit warning) until sufficient representatives return. — Graceful degradation

ORV stake-weighted delivered and validated PoC v0.4.0 (x86_64 + ESP32 QEMU, 24/24 tests PASS). Implementation: struct VoteORV {block_hash [u8;32], voter_pubkey [u8;32], delegated_stake u64, nonce u64, vector_clock VectorClock, signature [u8;64]}. Validated functions: cast_vote (Ed25519 on Blake3), verify_vote (silent rejection if invalid signature), collect_votes (eligibility threshold ≥0.1% supply), resolve_conflict_orv. Resolution cascade: (1) stake_weighted — gap >5% between the two sides, the majority partition wins; (2) vector_clock — if gap ≤5%, Vector Clock causality; (3) hash_tiebreaker — if concurrent, smallest hash wins. Validated scenarios: 60/40 stake → stake_weighted PASS, 50/50 tie → vector_clock fallback PASS, forged vote → silently ignored PASS, 0.1% eligibility threshold → correct exclusion PASS. Out-of-scope PoC (production M12-M18): on-chain delegation, vote propagation over physical LoRa mesh, vote timeout/deadline, vote revocation. Parameters adjustable by governance: min_delegation_pct (0.1%), min_delegation_age_days (7d), stake_tie_threshold (5%).

▶15. ARX TOKENOMICS — COMPLETE

15.1 SUPPLY & ALLOCATION

LAYER	SPEC TECHNIQUE
SUPPLY TOTAL	1 000 000 000 ARX (1 milliard). Fixe. Aucune inflation post-genesis.
IDO PUBLIC — 15%	150 000 000 ARX — Fjord Foundry LBP sur Base (L2 Coinbase, ERC-20). Prix de départ : 0.08 USDC. Prix plancher : 0.03 USDC. Durée : 72h. Levée attendue : 4.5M–12M USDC selon comportement des participants. Note LBP : si tous les participants attendent le prix plancher (comportement rationnel documenté dans les LBPs), la levée totale est 150M × 0.03 = 4.5M USDC. Si achat uniforme sur la durée, la levée est ~12M USDC. L'équipe planifie sur une base conservatrice de 4.5M USDC. Le terme hard cap est retiré — il ne s'applique pas à la mécanique LBP. La levée réelle dépend du prix de clearing. Choix de Base : frais ~0.01 USD/tx (participation retail accessible), backing Coinbase (crédibilité institutionnelle), ERC-20 standard (compatibilité SAFT et outils juridiques établis). Le token ARX ERC-20 sur Base est un token de financement intermédiaire — il sera migrable 1:1 vers le ARX natif Arxia L1 au mainnet (voir Section TGE).
ÉQUIPE — 15%	150 000 000 ARX — Cliff 12 mois, vesting linéaire 36 mois (total 48 mois). Multisig 3/5 fondateurs requis pour tout transfert.
INVESTISSEURS — 12%	120 000 000 ARX — Seed round. Cliff 6 mois, vesting linéaire 24 mois. Prix seed : 0.02 USDC/ARX. Scénarios de multiple seed : bear 1.5× (prix IDO 0.03 USD) / base 5× (0.10 USD) / bull 15× (0.30 USD) / ultra 50× (1.00 USD). Note sur le multiple conservateur bear 1.5× : le scénario bear correspond au prix plancher LBP — il évite le dump seed massif au TGE car le gain marginal est insuffisant pour motiver une vente immédiate. La valeur investisseur est dans les scénarios base/bull. Note de dilution : le vesting seed s'étale sur 30 mois (cliff 6 mois +

	linéaire 24 mois) — zéro dump seed possible à l'ouverture du LBP IDO, les tokens seed ne sont pas encore libérés à ce stade.
OPÉRATEURS NŒUDS — 25%	250 000 000 ARX — Distribués sur 60 mois. Courbe d'émission décroissante, arithmétique vérifiable : M1-12 : 6 250 000 ARX/mois × 12 = 75 000 000. M13-24 : 4 583 333 ARX/mois × 12 = 54 999 996. M25-59 : 3 333 334 ARX/mois × 35 = 116 666 690. M60 : 3 333 314 ARX (ajustement final). Total : 75 000 000 + 54 999 996 + 116 666 690 + 3 333 314 = 250 000 000 ARX. Distribution mensuelle basée sur score de relais vérifié × géo-multiplicateur. Formule : reward_nœud = (score_nœud / score_total_réseau) × émission_mensuelle.
ÉCOSYSTÈME — 20%	200 000 000 ARX — Grants développeurs, partenariats ONG, bug bounty, hackathons. Géré par la Fondation Arxia (multi-sig 5/9).
TRÉSORERIE — 13%	130 000 000 ARX — Réserve opérationnelle. Vesting 48 mois. Utilisable uniquement par vote DAO (quorum 5% du supply circulant — cohérent avec Section 15.4).

15.2 OFFLINE FEE MECHANISM

Problem identified during audit: if fees are calculated at reconciliation, ARX volatility creates unacceptable uncertainty for the payer.

Arxia solution: fees are fixed in ARX at the time of local transaction creation, locked in the signature.

```
fee = ceil(tx_bytes / 100) * BASE_FEE_ARX  // BASE_FEE_ARX = 0.001 ARX, fixe au moment T
```

- ◆ Fees are deducted from the local balance immediately upon creation.
- ◆ Distribution at reconciliation: 60% to the LoRa node that relayed first, 30% burned (deflationary), 10% to the final validator.
- ◆ In L0 (BLE only, no node): 100% of fees burned at reconciliation.
- ◆ `fee_arx_per_usd_cent` parameter adjustable by standard governance vote (5% circulating supply quorum) every 6 months. Documented risk: if ARX exceeds ~$5, BASE_FEE_ARX = 0.001 ARX > $0.005 — humanitarian acceptability threshold exceeded. Adjustment mechanism to be delivered at M3. In the meantime, the parameter is fixed at deployment and recalibrable without hard fork. — BASE_FEE_ARX Recalibration

15.3 OPERATOR STAKING, ANTI-SYBIL NODES & ANTI-SYBIL WALLETS

To prevent the proliferation of fake nodes at ~$31 that claim rewards without actually relaying:

- ◆ 500 ARX to activate a relay node and receive rewards. Recalibrable by standard governance vote if ARX price exceeds $2 (500 ARX × $2 = $1,000 — prohibitive threshold for operators in conflict zones). `min_stake_arx` parameter adjustable without hard fork. Target objective: threshold equivalent to $20–50 in real value. — Minimum staking
- ◆ Certifiable offline relay proof mechanism: each node that relays a transaction signs a RelayReceipt — structure: { tx_hash: [u8;32], relayer_pubkey: [u8;32], timestamp_vc: VectorClock, signature: Ed25519(tx_hash ++ relayer_pubkey ++ vc_bytes) }. This receipt is added in the compact transaction header (8 bytes fixed + 64 bytes signature = 72 bytes per hop). The transaction accumulates receipts from each traversed node. At reconciliation, the

network cryptographically verifies that each receipt is signed by the corresponding node's key — it is impossible to forge a receipt without possessing the node's private key. Relay score = number of verified valid receipts / transactions within node range over a 30-day sliding window. A node cannot lie about its relays: if it didn't sign the receipt, the receipt doesn't exist. Size limit: LoRa MTU 256 bytes — with compact header 193 bytes + 2 receipts × 72 bytes = 337 bytes exceeds MTU. Solution: receipts are collected in local memory and transmitted in a separate batch (RelayBatch) during synchronization, not packaged in each transaction. The RelayBatch is globally signed by the node and verified at reconciliation. Minimum required score: 85% over 30 days. Below 60% over 7 days: slashing and immediate exclusion. — Relay proof

- ◆ A node below 85% score over 30 days loses 10% of its stake. Below 60% over 7 days: immediate exclusion and loss of 25% of stake. — Slashing
- ◆ A slashed node waits 30 days before re-staking. — Cooldown

15.4 GOVERNANCE — QUORUM & OFFLINE VOTES

LAYER	SPEC TECHNIQUE
QUORUM STANDARD	Quorum progressif : 5% du supply circulant (benchmark secteur < 5%) avec clause d'escalade automatique si participation dépasse 30% du supply total (= majorité forte). Rationale : au TGE avec 150M ARX circulants, un quorum de 10% supply total = 100M ARX = 67% de participation — inatteignable. Un quorum de 5% supply circulant = 7.5M ARX = 5% de participation — réaliste et aligné avec les benchmarks secteur. La clause d'escalade garantit qu'une décision critique ne peut pas être imposée par une minorité si la communauté se mobilise massivement. Vote valide 72h après la fin de la période de vote.
QUORUM CRITIQUE	Upgrades protocole, changement de supply, allocation Treasury : quorum progressif — 15% du supply circulant au TGE (= 22.5M ARX sur 150M circulants, soit 15% de participation — atteignable) avec escalade automatique à 25% du supply circulant dès que le circulant dépasse 400M ARX (M18+). Approbation multi-sig Fondation (5/9) requise en parallèle dans tous les cas. Note : un quorum de 25% du supply total = 250M ARX est inatteignable au TGE avec 150M ARX en circulation (167% du circulant). Le quorum critique est donc exprimé en % du supply circulant avec un plancher absolu de 50M ARX, jamais en % du supply total.
MODÈLE DE VOTE	Stake-weighted exclusivement : 1 ARX = 1 vote. Le modèle '1 wallet = 1 vote' est retiré — incompatible avec un modèle stake-weighted et vulnérable aux attaques Sybil wallet. La dé-duplication des votes offline se fait par hash du vote signé par la clé du wallet votant, pas par adresse wallet. Plafond de voting power : un wallet ne peut pas exercer plus de 10% du quorum effectif total, quelle que soit sa détention. Mécanisme : votes_comptabilisés = min(balance_arx, 0.10 × total_votes_cast). Les ARX au-delà du plafond ne sont pas perdus — simplement non-comptabilisés pour ce vote. Rationale : sans ce plafond, équipe (15%) + opérateurs nœuds (25%) = 40% du supply peuvent imposer toute décision standard (quorum 5%) seuls. Avec le plafond à 10%, il faut au minimum 3 acteurs indépendants pour atteindre 30% — aucun bloc homogène ne décide seul. Paramètre `max_voting_power_pct` (défaut 10%) modifiable uniquement par vote critique (quorum 15% circulant + multi-sig Fondation 5/9).
VOTES OFFLINE	Un vote soumis offline porte un nonce de gouvernance unique signé. Dé-duplication par hash à la reconciliation. Si le même wallet vote dans deux partitions différentes sur la même proposition, seul le vote avec le vector clock le plus ancien est comptabilisé.

INVERSION MAJORITÉ	Si une décision change de majorité à la réconciliation, une période de contestation de 48h est ouverte avant application. Si la majorité s'inverse une seconde fois, la décision est annulée et resoumise au vote.

▶16. TEAM & LEGAL STRUCTURE

NOTE DE TRANSPARENCE

Arxia est en phase de constitution d'équipe publique. Les profils complets des fondateurs seront publiés au lancement du testnet (M6). La structure juridique est opérationnelle dès aujourd'hui.

16.1 PRE-DAO STRUCTURE

LAYER	SPEC TECHNIQUE
FONDATION	Fondation Arxia — enregistrée en Suisse (canton de Zoug). Structure non-profit dédiée au développement du protocole. Responsable de l'allocation Écosystème et Trésorerie.
VÉHICULE SEED & MiCA	La levée seed est structurée via SAFT (Simple Agreement for Future Tokens) — instrument standard pour les levées pre-token en droit US et compatible avec la majorité des juridictions européennes. Statut MiCA : le token ARX est conçu comme utility token (gaz du réseau) et non comme security token ou asset-referenced token au sens MiCA. Une opinion juridique formelle sera obtenue auprès d'un cabinet spécialisé crypto-assets (Lenz & Staehelin ou équivalent) avant l'émission des SAFT. L'IDO public sur Fjord Foundry (Base, ERC-20) sera soumis à une analyse MiCA séparée. Note structurelle : le ARX ERC-20 émis sur Base au TGE est un token de financement intermédiaire. Il sera convertible 1:1 en ARX natif sur la L1 Arxia au mainnet via un bridge dédié audité. Le contrat ERC-20 sera gelé post-migration. Les détenteurs qui ne migrent pas conservent leur ARX ERC-20 — la migration est optionnelle mais nécessaire pour utiliser le réseau Arxia natif.
MULTI-SIG CONTRÔLE	5/9 signataires pour toute décision concernant les fonds de la Fondation. Composition : 3 fondateurs (identités publiées au testnet M6) + 4 advisors externes indépendants nommés publiquement avant la levée seed + 2 signataires opérationnels (identités publiées au mainnet). Pour les fonds Équipe : 3/5 fondateurs. La composition complète du multi-sig sera publiée intégralement au plus tard au closing de la levée seed.
ENTITÉ COMMERCIALE	Arxia Labs SAS — entité opérationnelle pour les contrats, salaires et partenariats B2B. Filiale de la Fondation Arxia.
TRANSITION DAO	Critères de transfert de contrôle de la Fondation vers la DAO : (1) mainnet live depuis ≥ 6 mois, (2) supply circulant ≥ 40%, (3) ≥ 1000 nœuds actifs sur le réseau, (4) ≥ 3 audits de sécurité externes complétés et publiés. Une fois ces critères atteints, la Fondation dispose de 6 mois pour transférer les pouvoirs de gouvernance à la DAO via vote communautaire. Sans ces critères définis, la

	Fondation peut rester en contrôle indéfiniment — ce mécanisme est le garde-fou contre ce risque.
SMART CONTRACT LOCK	Tous les tokens Équipe et Investisseurs sont verrouillés dans un smart contract de vesting audité (Sablier V2 sur Base) dès le TGE. Aucun transfert possible en dehors du vesting schedule. Sablier V2 est déployé nativement sur Base — les streams de vesting sont visibles publiquement on-chain en temps réel.

16.2 FOUNDER PROFILES

LAYER	SPEC TECHNIQUE
FONDATEUR — CTO	Senior Protocol Engineer. 8 ans d'expérience en systèmes distribués. Contributeur open source sur des projets DAG et cryptographie appliquée. Profil complet publié au testnet M6.
FONDATEUR — CEO	Entrepreneur blockchain depuis 2016. Expérience en déploiements fintech en Afrique subsaharienne et Moyen-Orient. Réseau ONG et institutionnel établi.
FONDATEUR — CPO	Expert en UX pour populations vulnérables. Ancienne expérience en déploiement d'apps humanitaires offline (programmes UNHCR). Comprend les contraintes terrain réelles.

16.3 ADVISORY BOARD

LAYER	SPEC TECHNIQUE
SYSTÈMES DISTRIBUÉS	Chercheur senior spécialisé CRDTs et consensus distribué. Publications académiques sur la tolérance aux partitions réseau. Institution : à confirmer et publier au testnet.
CRYPTOGRAPHIE	Expert protocoles de signature et zero-knowledge proofs. Contribution à des standards W3C DID. Institution : à confirmer et publier au testnet.
DÉPLOIEMENT TERRAIN	Spécialiste logistique humanitaire numérique. Expérience de déploiement d'infrastructure en zones de conflit (Syria, Yemen, Ukraine). ONG partenaire : à annoncer.

▶17. TGE STRUCTURE — ERC-20 ON BASE

Since the Arxia L1 does not exist at the time of the IDO, the ARX token is issued in two distinct phases. This structure is standard for any L1 under construction — it is used by Aptos, Sui, and the majority of L1s launched since 2022.

PHASE	SPEC TECHNIQUE

PHASE 1 — SEED	Instrument : SAFT (Simple Agreement for Future Tokens). Aucun token livré — accord contractuel de livraison au TGE. Prix : 0.02 USDC/ARX. Les investisseurs seed reçoivent leurs ARX ERC-20 directement sur Base au TGE, soumis au vesting Sablier V2 (cliff 6 mois, linéaire 24 mois). Aucune chaîne requise aujourd'hui.
PHASE 2 — TGE / IDO (M24+)	Déploiement du contrat ERC-20 ARX sur Base (Coinbase L2). LBP Fjord Foundry 72h. Vesting Sablier V2 pour équipe et investisseurs. Liquidité post-IDO sur Uniswap V3 (Base). Frais de transaction : ~0.01 USD — participation retail accessible. Le ARX ERC-20 est le token de marché pendant la période pré-mainnet.
PHASE 3 — MIGRATION MAINNET	Au lancement du mainnet Arxia L1 : ouverture d'un bridge officiel audité Base → Arxia L1. Conversion 1:1 ARX ERC-20 → ARX natif. Fenêtre de migration : 24 mois. Après 24 mois, le contrat ERC-20 est gelé (aucun nouveau transfert possible). La migration est optionnelle — les détenteurs qui ne migrent pas conservent leurs ARX ERC-20 comme actif EVM standard. La migration est nécessaire pour utiliser le réseau Arxia natif (staking nœud, gouvernance L1, transactions offline). Modèle de bridge retenu : Lock-and-Mint unidirectionnel. Le ARX ERC-20 est verrouillé dans un contrat custodial audité sur Base (jamais détruit) — un ARX natif équivalent est minté sur la L1 Arxia. La migration est à sens unique et définitive : il n'y a pas de chemin de retour L1 → Base après migration, ce qui élimine la surface d'attaque de réentrance bidirectionnelle responsable de plus de 2 milliards USD de pertes sur bridges en 2022 (Ronin, Wormhole, Nomad). Le contrat de custody Base sera soumis à un audit dédié (CertiK ou Trail of Bits) distinct de l'audit L1, avec publication du rapport avant ouverture du bridge. Risque résiduel documenté : le contrat de custody Base concentre l'intégralité du ARX ERC-20 migré — c'est un honeypot par construction. Mitigation : multisig 5/9 Fondation sur le contrat de custody + timelock de 72h sur toute opération administrative + monitoring on-chain temps réel. Note sur l'isolation des risques : le bridge ERC-20 → L1 est une infrastructure de financement pré-mainnet, pas une infrastructure de résilience opérationnelle. Le protocole Arxia L1 fonctionne indépendamment du bridge — en cas de compromission du contrat de custody Base, le réseau L1 et les transactions offline continuent de fonctionner normalement. Les risques bridge (centralisation du custody) et les risques protocole (consensus, double-spend) sont structurellement isolés. Ronin, Wormhole et Nomad avaient des multisigs — leur compromission provenait d'une surface d'attaque bidirectionnelle et de clés multisig insuffisamment sécurisées. L'unidirectionnel réduit la surface mais ne l'élimine pas : l'audit dédié et le monitoring temps réel sont non-négociables avant ouverture.
POURQUOI BASE	ERC-20 standard — compatibilité totale SAFT, outils juridiques, et infrastructure DeFi existante. Frais ~0.01 USD/tx — participation retail accessible vs Ethereum mainnet (20–80 USD/tx). Backing Coinbase — crédibilité institutionnelle maximale pour les fonds européens et américains. Fjord Foundry supporte Base nativement. Croissance Base 2024–2026 : 2e L2 par TVL après Arbitrum. Liquidité post-IDO sur Uniswap V3 (Base) — profondeur suffisante pour la taille de l'IDO Arxia.

▶ 18. SECURITY PLAN

CHANGEMENT AUDIT : SÉCURITÉ AVANCÉE À M6

Suite aux recommandations d'audit, l'audit de sécurité externe est avancé de M18-24 à M6. Un bug bounty public est lancé dès le premier testnet. La sécurité n'est pas une étape finale — c'est un processus continu.

18.1 ADDRESSED VECTORS

LAYER	SPEC TECHNIQUE
REPLAY ATTACK BLE	Champ receiver inclus dans la signature Ed25519. Une transaction capturée ne peut être rejouée que vers le destinataire original — mathématiquement impossible vers un tiers.
NŒUD MALVEILLANT MESH	Système de réputation des nœuds : score basé sur proportion de relais valides. Exclusion automatique si score < 60%. Limite du gossip blacklist : un nœud malveillant peut ne pas relayer les messages gossip qui le blacklistent — dans une partition de 5 nœuds dont 2 sont compromis, la blacklist ne se propage pas aux nœuds isolés. Mitigation : blacklist signée par les nœuds honnêtes et intégrée dans les headers de chaque transaction relayée (pas un message gossip séparé). Tout nœud recevant une transaction voit automatiquement la blacklist courante dans le header. Un nœud compromis qui censure les headers est lui-même détecté comme malveillant par les nœuds receveurs.
CLÉ PRIVÉE ANDROID	Android Keystore obligatoire (API 23+). Détection de root via Play Integrity API. Limite connue : Magisk + Zygisk contournent SafetyNet/Play Integrity sur la majorité des appareils Android — la garantie de sécurité sur appareils rootés n'est pas tenue en pratique sur les marchés cibles (appareils d'occasion, firmware modifié fréquents en zones de conflit). Mitigation réaliste : le Keystore matériel (StrongBox, disponible sur appareils post-2018) stocke la clé privée dans un enclave hardware indépendant du système — inaccessible même si le système est rooté. Arxia recommande et priorise les appareils avec StrongBox certifié pour les déploiements institutionnels.
ATTAQUE PAR ISOLATION	Un attaquant ne peut pas manipuler l'ordre des événements sans contrôler tous les nœuds LoRa à portée. Protection : chaque nœud relais signe le vector clock local de la transaction (pas un timestamp absolu — NTP est impossible offline). La manipulation du vector clock est détectable car elle violerait la cohérence causale du DAG local du nœud.
STAKE GRINDING LONG-RANGE	Un attaquant accumule du stake juste avant une partition pour manipuler le résultat ORV à la réconciliation. Mitigation retenue (option a) : délai de délégation minimum de 7 jours — le stake délégué à un représentant doit être antérieur d'au moins 7 jours à la création de la partition pour être comptabilisé dans le vote ORV de cette partition. Le stake délégué après le début de la partition est ignoré pour ce round de consensus. Paramètre `min_delegation_age_days` ajustable par gouvernance.
DUTY CYCLE LORA EU	Réglementation EU 868MHz : 1% duty cycle max. Arxia batch les transactions en frames agrégées. Une frame de 10 transactions = même temps d'émission qu'une. Débit réel calculé (transaction LZ4 ≈ 200 bytes = 1 600 bits) — SF12 (40 km) : 250 bps brut, 1 tx/640s sans batching, 56 tx/h/nœud avec batch ×10. SF9 (15 km) : 1 760 bps brut, ≈ 400 tx/h/nœud avec batch. SF7 (2 km) : 5 470 bps brut, ≈ 1 200 tx/h/nœud avec batch. Configuration recommandée par défaut : SF9 (équilibre portée/débit). SF12 réservé aux relais inter-quartiers. Le batching est non-optionnel en SF12 — il multiplie le débit effectif par 10. Overhead gossip

	L1 — estimation worst-case : la confirmation L1 requiert la synchronisation des registres de nonces entre nœuds co-localisés avant chaque transaction (délai max 3s, Section 12). Chaque échange gossip = 1 paquet ≈ 64 bytes (nonce + signature + adresse). Pour N wallets actifs simultanés dans une partition, le gossip génère N × (N-1) / 2 échanges en worst-case mesh complet. Estimation conservatrice pour une partition de 20 nœuds actifs : 190 échanges gossip × 64 bytes = 12 160 bytes/cycle de confirmation, soit ~13% du budget bande passante SF9 disponible par heure (≈ 90 000 bytes/h à 1% duty cycle). Ce budget est consommable sans saturation dans des conditions normales. Scénario de saturation : >50 nœuds actifs simultanés dans une même partition en SF9 — le gossip commence à concurrencer significativement les transactions applicatives. Mitigation : gossip batchable dans les mêmes frames que les transactions, priorité transactions sur gossip configurée au niveau protocole. Simulation complète sous charge et mesures terrain à publier M3.
SYBIL NŒUDS	Staking minimum 500 ARX + preuve de relais cryptographique obligatoire. Le coût économique du staking + le risque de slashing rendent l'attaque Sybil nœud non rentable.
SYBIL WALLETS L0	En L0, les wallets sont gratuits — un attaquant peut créer 100 wallets sans coût. Vecteur d'attaque : inonder le mesh de transactions invalides pour saturer la bande passante LoRa. Mitigation : rate limiting au niveau protocole — un wallet sans historique on-chain est limité à 3 transactions L0 par heure jusqu'à la première confirmation L2. Les wallets avec historique confirmé (≥ 1 transaction L2) ont des limites étendues. Vérifiable offline via le DAG local du nœud relais. Cas particulier bootstrap : dans un mesh sans historique DAG, le rate limiting par DAG local est inopérant. Mitigation bootstrap : les 48 premières heures d'un nœud nouvellement déployé opèrent en mode L0 strict (plafond 10 ARX, aucune confirmation L1) jusqu'à ce que le nœud ait relayé au moins 50 transactions vérifiées.

18.2 SECURITY CALENDAR

M1	Publication du threat model complet. Identification de tous les vecteurs d'attaque par niveau de connectivité (L0, L1, L2).
M3	Audit interne du module de consensus offline par l'advisory board cryptographie.
M6	Audit de sécurité externe (CertiK ou Trail of Bits) sur le module consensus + double-spend prevention. Bug bounty public lancé : 250 000 USD équivalent ARX pour bug critique (standard industrie L1 : 100k-500k USD), 50 000 USD pour majeur, 10 000 USD pour modéré. Financé par l'Écosystème Fund. Programme permanent post-mainnet avec budget annuel dédié.
M12	Audit complet du stack (transport LoRa + WASM + DID). Pentest terrain simulé en environnement de conflit (réseau mesh perturbé, nœuds malveillants injectés).
M18	Audit final pré-mainnet. Rapport public disponible. Aucun mainnet sans audit clean.

▶19. TECHNICAL BACKLOG — POST-FUNDING

PREUVE DE CONCEPT — LIVRÉ v0.5.0

Le PoC Arxia v0.5.0 a été compilé et exécuté avec succès sur x86_64 (Windows 10/MSYS2, Rust 1.86.0). L'ESP32 reste sur la baseline v0.4.0 (24 tests — port gossip en cours, contraintes no_std). Le code source complet est publié sur le repo GitHub public Arxia. 34 tests passent sur x86_64, 24 sur ESP32. Primitives validées : Ed25519 (génération, signature sur bytes bruts Blake3, vérification), Blake3, Block Lattice OPEN/SEND/RECEIVE, PN-Counter CRDT (convergence + commutativité + idempotence + associativité + intégration reconcile_partitions()), Vector Clocks (ordonnancement causal + résolution de conflits), sérialisation binaire compacte bidirectionnelle (to_compact_bytes + from_compact_bytes, 193 bytes, roundtrip VALID), vrai double-spend inter-partitions (deux signatures Ed25519 valides, même nonce), assess_finality() correct (Pending / L0 / L1 / L2), tamper detection, replay attack prevention, intégrité de chaîne, HW RNG ESP32, métriques performance. ORV stake-weighted complet : VoteORV, cast_vote, verify_vote, collect_votes (seuil 0.1%), resolve_conflict_orv avec cascade stake_weighted → vector_clock → hash_tiebreaker — 5 scénarios validés dont rejet de vote forgé. Gossip protocol complet : GossipTransport trait + SimulatedTransport (latence + perte + PRNG seedé reproductible), GossipMessage avec BTreeMap<[u8;32], (u64, [u8;32])>, merge_nonce_registries (détection double-spend par block_hash), sync_nonces_before_l1 (timeout 3s, fallback L0), assess_finality conditionné à SyncResult::Success — 10 scénarios validés dont 3 topologies réseau (chaîne linéaire, pont unique, pont cassé). Supply totale préservée. Hors-scope PoC (production M12-M18) : délégation on-chain, propagation votes sur mesh LoRa physique, timeout/deadline de vote, révocation de vote, port gossip ESP32.

LAYER	SPEC TECHNIQUE
BOOTSTRAP VECTOR CLOCK	Un nœud factory-reset initialise son vector clock via signature d'au moins un nœud existant de confiance lors de l'onboarding. Un reset unilatéral est impossible — il requiert re-validation réseau ou nœud bootstrap désigné en offline. Spec complète M3.
DÉRIVATION CLÉ STOCKAGE	Dérivation PIN → clé ChaCha20 : Argon2id (m=64MB, t=3, p=4). Alternative sur appareils contraints : PBKDF2-SHA256 600 000 itérations (standard NIST 2023). Choix final spécifié M6 avec justification par plateforme (Android StrongBox vs software).

▶20. COMPETITIVE ANALYSIS

LAYER	SPEC TECHNIQUE
BITCOIN	Censure-résistant mais 100% internet-dépendant. Pas de DID. Satellite = réception seule.
ETHEREUM	Smart contracts complets mais internet-first. Frais élevés, inadapté aux micropaiements humanitaires.
SOLANA	Haute performance mais centralisation des validateurs. Pannes récurrentes. Aucune capacité offline.
NANO	Block Lattice similaire. Gratuit. Mais zéro support offline, pas de DID, pas conçu

	pour réseaux fragmentés.
STELLAR	Bonne traction humanitaire. Centralisée (SDF). Aucune capacité offline.
IOTA	Tangle DAG + travaux mesh (IOTA Streams). Concurrent sérieux. Mais architecture Tangle inadaptée à l'offline-first long terme. Pas de Block Lattice par compte.
ARXIA ◆	Seul L1 avec Block Lattice offline-first natif + CRDTs + LoRa mesh + DID W3C + finalité formalisée par niveau de connectivité.

▶ 21. RISKS AND MITIGATIONS

LAYER	SPEC TECHNIQUE
BOOTSTRAPPING HARDWARE	Qui déploie les nœuds LoRa en zone de conflit ? Mitigation : plan de déploiement en 3 phases — pilote avec 1 ONG partenaire identifiée, subvention hardware via Écosystème Fund, programme de don de nœuds via communauté.
SMS COUPÉ AVEC INTERNET	Le SMS peut être coupé en même temps qu'internet. Mitigation : SMS est un fallback secondaire. Le fallback primaire est LoRa mesh — indépendant des opérateurs télécom. L'antenne LoRa émet sur des fréquences libres non contrôlables par les opérateurs.
KEY RECOVERY RÉFUGIÉS	Si le téléphone est perdu ou confisqué. Mitigation : Shamir Secret Sharing (SSS) 2-of-3 — protocole offline : (1) À la création du wallet, la seed est divisée en 3 shares encodées selon SLIP39 (Satoshi Labs Improvement Proposal 39, standard Trezor pour SSS — distinct de BIP39) en 24 mots chacune. (2) Chaque share est imprimée sur carte plastifiée waterproof ou gravée sur plaque métal. (3) Distribuée à 3 contacts physiques de confiance. (4) Reconstruction : 2 contacts se retrouvent physiquement, l'app en mode Recovery sans réseau reconstitue la seed localement. (5) Si un contact est décédé ou déplacé : reconstruction impossible avec 1/3 seul — conçu pour résister à la coercition. Format des shares : SLIP39 compatible, lisible par toute app SLIP39 même hors réseau Arxia.
KYC/AML ONG INSTITUTIONNELLES	Les agences ONU ne peuvent pas ignorer les listes noires. Mitigation : couche KYC/AML optionnelle au niveau protocole. Les opérateurs institutionnels peuvent configurer une whitelist de wallets vérifiés sans modifier le protocole de base.
INCITATION CENTRALISATRICE	Les nœuds en zones connectées génèrent plus de rewards que ceux en zones de conflit. Mitigation : subsidy géographique — nœuds en zones classées conflit actif (liste ACLED) reçoivent multiplicateur x2. Distribution offline : la liste ACLED est diffusée en format binaire compressé (< 500 KB, ~5000 zones actives) via service broadcast satellite une fois par semaine, signée par la clé Ed25519 de la Fondation Arxia (même clé que les snapshots de stake — vérifiable offline, hardcodée dans le protocole). Les nœuds rejettent toute mise à jour sans signature valide. Les nœuds la mettent à jour automatiquement à réception. Si aucune mise à jour depuis > 90 jours, le nœud maintient sa classification précédente. Vote de gouvernance annuel pour mettre à jour les paramètres. Financé par l'Écosystème Fund.

RÉGULATION INTERDICTION	Les gouvernements peuvent interdire l'app et tracer les émissions LoRa. Mitigation réaliste (pas de comparaison TCP/IP naïve) : distribution APK hors stores, multi-bandes LoRa (433/868/915MHz). L'objectif est d'augmenter le coût de la censure — pas de la rendre impossible.
DUTY CYCLE LORA EU	Réglementation 1% duty cycle sur 868MHz. Mitigation : batch de transactions (×10 débit effectif), compression LZ4, SF9 par défaut (400 tx/h/nœud), SF12 pour longue portée (56 tx/h/nœud). Mesures terrain M3. Alternative : fréquence 433MHz (duty cycle moins restrictif) en fallback.
TRAÇABILITÉ LORA PHYSIQUE	Un nœud LoRa actif est localisable physiquement par TDOA (Time Difference Of Arrival) avec moins de 500 USD de matériel. Dans des régimes autoritaires, utiliser Arxia peut constituer un risque vital. Mitigations : transmissions en rafales courtes et imprévisibles, nœuds mobiles, mode silencieux (réception seule). Avertissement obligatoire dans l'onboarding utilisateur pour les zones de surveillance active. Ce threat model est intégré dès la v1.
FENÊTRE COMPÉTITIVE	Les concurrents (IOTA Streams, Stellar, fork potentiel) peuvent copier l'architecture — pas le réseau physique. Le moat d'Arxia est matériel, pas logiciel. (1) Chaque nœud LoRa déployé est un engagement hardware sur le terrain — un concurrent partant de zéro doit reconstruire le maillage physique, pas seulement forker le code. (2) Les intégrations ONG sont des décisions de procurement à 12–18 mois de cycle — une organisation qui déploie Arxia dans un camp ne change pas de protocole après 6 mois. (3) Les DID et titres fonciers ancrés sont chain-specific : la résolution DID pointe vers le DAG Arxia — migrer détruirait la chaîne de preuves. Ce lock-in ne vaut rien à zéro utilisateur — il devient insurmontable à 10 000. C'est pourquoi les 6 premiers mois de déploiement terrain (M12–M18) sont le véritable enjeu compétitif, pas le whitepaper.

▶ 22. REVISED ROADMAP

M1-3	FONDATIONS — Publication threat model complet. Spécification formelle Block Lattice Arxia. Recrutement advisory board (noms publics). Publication structure juridique Fondation + multi-sig.
M3-6	PROTOTYPE + AUDIT — Gossip protocol livré PoC v0.5.0 (x86_64, 34/34 tests). Port ESP32 en cours (contraintes no_std). Nœud LoRa + transactions Ed25519 + finalité L0 testée terrain. Finalité L1 testée terrain après port gossip ESP32. Audit interne cryptographie. Audit externe sécurité M6. Bug bounty lancé. Duty cycle simulation et overhead gossip sous charge publiés.
M6-12	DAG CONSENSUS — Block Lattice complet. ORV adapté offline. CRDTs réconciliation. Tests chaos réseau. Key recovery Shamir. Staking opérateurs + anti-sybil.
M12-18	APP MOBILE + DID + ORV PRODUCTION — React Native offline-first. Android Keystore. Social recovery UI. Module DID W3C complet (did:arxia:, résolution via DAG local, Verifiable Credentials). Intégration production ORV stake-weighted (délégation on-chain + propagation votes mesh LoRa + timeout/deadline de vote — spec Section 14.3 ; primitives et cascade de résolution validées PoC v0.4.0). Intégration CRDT dans pipeline de réconciliation du ledger. Pilote terrain ONG partenaire. Audit complet stack.
M18-24	MAINNET PREP — Registre foncier. Couche KYC/AML optionnelle. Audit final. Tokenomics live sur testnet. Governance DAO testée.

M24 +	MAINNET — IDO Fjord Foundry LBP sur Base (ERC-20 → migration ARX natif). Ecosystem grants. Partenariats UNHCR/IRC annoncés. Bug bounty permanent.

▶23. USE OF FUNDS & RUNWAY

The seed round targets 2.4M USDC (conservative base scenario, independent of LBP IDO M24+). The Fjord Foundry LBP (4.5M–12M USDC) is the post-prototype expansion funding — not the first 24 months funding. The seed runway covers M1–M24 with a burn rate of 100,000 USDC/month.

POSTE	MONTANT (USDC)	DÉTAIL
Équipe core (M1–M18)	1 080 000	3 ingénieurs seniors Rust/embedded + 1 CPO. 15 000 USDC/mois/personne × 4 × 18 mois = 1 080 000. Salaires marché pour profils cryptographiques, non-dilutifs.
Audits sécurité	480 000	Audit M6 consensus (150 000) + audit M12 stack complet (150 000) + audit bridge ERC-20→L1 dédié (100 000) + bug bounty M6 (80 000 réserve). CertiK ou Trail of Bits.
Infrastructure & hardware	200 000	Serveurs testnet, nœuds LoRa pilotes (50× T-Beam = 1 550 USD), cloud infra (CI/CD, monitoring), licences outils. Buffer matériel déploiement ONG pilote.
Juridique & compliance	320 000	Fondation Zoug (enregistrement + frais annuels), opinions juridiques MiCA + SAFT (Lenz & Staehelin), structure SAFT investisseurs, préparation TGE.
Marketing & communauté	200 000	Préparation IDO (M18–M24) : community management, KOLs, relations presse, développement écosystème. Non-prioritaire avant testnet public.
Réserve (imprévus)	120 000	5% du seed. Retards de développement, recrutements urgents, opportunités terrain imprévues.
TOTAL SEED	**2 400 000**	Burn rate : 100 000 USDC/mois. Runway : 24 mois (M1–M24). Extension possible si B2B pipeline signé avant M12 — un contrat ONG à 20 000 USD/an réduit le burn net de 1 700 USD/mois.

▶24. INVESTMENT THESIS

MARCHÉ ADRESSABLE — RÉSILIENCE CIVILISATIONNELLE

Marché primaire — utilisateurs on-chain actifs exposés au risque réseau : 580 millions de personnes dans le monde possèdent de la crypto (Chainalysis 2025). Clarification critique : la majorité de ces 580M détiennent sur des exchanges centralisés (Coinbase, Binance, etc.) et ne transactent pas on-chain. Leur problème en cas de coupure réseau est l'accès à leur exchange, pas le protocole blockchain sous-jacent — Arxia ne résout pas ce problème. Le marché primaire réel d'Arxia est le sous-ensemble des utilisateurs on-chain actifs en self-custody : wallets non-custodial, protocoles DeFi, transferts P2P directs. Estimation : 20–50 millions d'utilisateurs actifs on-chain (source : Dune Analytics, Nansen 2025). C'est ce marché — pas les 580M — dont les avoirs sont réellement inaccessibles lors d'une coupure réseau. Marché secondaire — zones de conflit et résilience humanitaire : 2+ milliards de personnes en zones de conflit/post-conflit. 100+ millions de réfugiés. 500 millions sans accès bancaire en zones instables. L'aide humanitaire internationale représente 30–50 milliards USD/an (OCHA 2026). Marché tertiaire — infrastructure de résilience institutionnelle : gouvernements, ONG, établissements financiers et fonds souverains exposant une partie croissante de leurs réserves en actifs numériques ont un intérêt direct à une couche de résilience protocol-level. Le marché de la cybersécurité et continuité d'activité représente 185 milliards USD/an (Gartner 2025) — Arxia adresse la partie résilience monétaire de ce segment. Arxia adresse ces trois marchés avec une seule architecture. Le use case guerre est la preuve de résilience maximale — pas le plafond d'ambition. SAM (marché adressable réellement atteignable) : parmi les 580M détenteurs de crypto, ceux actifs dans des juridictions à risque réseau élevé ou cherchant explicitement de la résilience — estimation conservatrice 5–10%, soit 29–58 millions d'utilisateurs potentiels. Sur le marché humanitaire : personnes en zones de conflit avec Android 8+ et accès à un nœud LoRa déployé — estimé à 500 000–2 millions en phase pilote (M12–M24), selon la vitesse de déploiement hardware ONG. SOM (marché obtenable année 1–3) : objectif réaliste post-mainnet — 50 000 wallets actifs (référence : Nano a atteint 100 000 wallets actifs en 18 mois post-mainnet en 2018 sans use case humanitaire), 10 nœuds institutionnels ONG déployés, 2–3 contrats pilotes B2B signés. Ces chiffres ne font pas d'Arxia une licorne en année 3 — ils établissent la preuve de traction nécessaire pour la série A. Clarification critique sur le modèle économique : les réfugiés et civils en zone de conflit ne sont pas les acheteurs de ARX — ils sont les utilisateurs. Le cycle économique est celui de toute infrastructure de protocole : les spéculateurs et opérateurs de nœuds financent le réseau via le token, les utilisateurs finals bénéficient du service. Ce modèle est identique à celui de Filecoin (stockage), Helium (LoRa IoT), ou Ethereum (smart contracts) — dans chaque cas, les utilisateurs finals ne paient pas en token spéculatif, ce sont les opérateurs d'infrastructure qui bénéficient de l'appréciation. Clarification sur les deux marchés et leurs timelines respectives : Arxia adresse deux marchés qui ont des logiques économiques et des horizons temporels différents — il est important de ne pas les confondre. Marché ONG/humanitaire (timeline M12-M24, concret) : c'est le marché de traction à court terme. Les ONG et institutions déploient des nœuds dans le cadre de leur infrastructure existante, indépendamment du prix ARX. Les revenus sont des licences B2B (15 000–80 000 USD/an). Ce marché a un cycle de vente de 12-18 mois — avec un runway seed de 24 mois, la fenêtre pour signer des contrats pilotes avant la série A est réelle mais étroite. Zéro pipeline signé à ce stade. Marché résilience/assurance monétaire (timeline long terme, spéculatif) : c'est le marché de valeur token. Les détenteurs de crypto acquièrent du ARX comme couverture contre les scénarios de coupure réseau. Ce marché est conditionnel à trois facteurs simultanés : (1) le token ARX a un prix, (2) suffisamment de nœuds sont déjà déployés, (3) les gens autour de l'utilisateur ont aussi l'app. Ce sont trois conditions rarement réunies à court terme. Sa matérialisation est réelle mais non garantie et non nécessaire au fonctionnement du réseau. Conclusion sur la priorité : le marché ONG est le marché qui valide la thèse terrain et finance la série A. Le marché résilience est le marché qui fait apprécier le token. Les confondre dans la même narrativa crée une confusion sur ce qui est mesurable à 24 mois.

- ◆ Crypto holders seeking to protect their monetary power against any network interruption — from individual to ultra-wealthy. P2P transfers, subsistence payments, resilient savings. Note on micro-fees: at 0.001 ARX/tx and ARX at $0.03, the revenue per transaction is $0.00003 — insufficient as a standalone revenue driver. The B2C model does not rely on transaction fees but on three levers: (1) demand for ARX for node operator staking (250M ARX locked out of circulation create structural upward pressure on the token); (2) the resilience value perceived by existing crypto holders who acquire ARX as monetary insurance; (3) fees at scale — at 1M tx/day (comparable to Nano in 2022), fees generate 10,000 ARX/day burned or redistributed, creating real deflationary pressure. The only immediate revenue lever is B2B/B2G — B2C is a vector for adoption and token value, not direct cash-flow. — B2C
- ◆ Infrastructure for NGOs, governments in reconstruction, UN agencies. Revenue model: institutional node deployment licenses (target range $15,000–$80,000/year depending on volume and SLA level) + custom KYC/AML integrations

(one-time service contract $50,000–$200,000). Realistic M18–M24 target: 3–5 pilot NGO contracts at $20,000/year = $60,000–$100,000 ARR. No signed pipeline at this stage — formal negotiations begin at testnet publication (M6). — B2B

◆ Post-conflict governments in reconstruction: land registry, national identity, local currency issuance. Multi-year contracts. Legal clarification: an Arxia land title has evidentiary value (cryptographic proof of precedence) but requires a recognition law in the relevant country to be legally enforceable. Identified pilot jurisdictions: Ukraine (digital assets law in ratification), Georgia (e-governance program), Rwanda (cadastral digitization). Strategy: complement to official registries, not substitute. — B2G

Timing is critical and the window is open now. The crypto ecosystem took 15 years to reach 580 million users and $3 trillion USD in market cap — without ever solving the network resilience question. The first protocol to anchor this field infrastructure creates irreversible lock-in: millions of DIDs, land titles and sovereign identities anchored on Arxia cannot migrate without destroying proofs of real rights.

ARXIA.EXE

The blockchain that runs when the internet is dead.

LAYER 1 ◆ OFFLINE-FIRST ◆ MESH CONSENSUS ◆ DID W3C