WORKING PAPER

ONU 2.0

Global Governance Platform

Architecture · Distributed Intelligence · On-Chain Philanthropy
Legal Compliance · Philosophical Foundations

Version	v2.0.0
License	MIT License
Compliance	LGPD · GDPR · FATF · COAF
Languages	10 (BRICS+ members)
Members	BRICS+ (12 nations)
Chain ID	Arkhe-Chain · 2140
Date	April 2026

Author

Rafael Oliveira
ORCID: 0009-0005-2697-4668

Arkhe(n) Research Group · ONU 2.0 Contributors

Abstract

ONU 2.0 is a next-generation global governance platform designed to coordinate public policy, development projects, and multilateral philanthropy across BRICS+ member states and international observer partners. Built on a hybrid architecture that combines traditional e-government systems with Web3 infrastructure and distributed artificial intelligence, it implements a complete workflow of submission → GPS jurisdictional validation → multi-level approval pipeline → audited execution → on-chain anchoring.

At the technical level, the platform is structured around seven architectural layers: GPS jurisdictional control, multi-level approval state machines, asynchronous message routing (AO protocol), cryptographically chained audit ledgers, BRICS+ policy exchange, Bitcoin OP_RETURN anchoring via Arkhe-Chain (Chain ID 2140), and Kuramoto oscillator-based network coherence consensus. The AI module is implemented as a Bittensor fork — the ONU 2.0 Subnet — with six specialized sub-networks for data validation, policy enforcement, audit surveillance, subnet mining, sovereign identity, and ethical oversight.

Philosophically, ONU 2.0 is grounded in the C/Z duality of the Arkhe(n) framework: governance as the projection of the field of possibility (C-domain: policy intent, legal norms, stakeholder consensus) into the field of actuality (Z-domain: executed transactions, immutable audit records, on-chain commitments). The Kuramoto coherence layer operationalizes this philosophical premise — network governance achieves legitimacy when the synchronization of operator nodes crosses the critical threshold phi_c = 0.618.

Keywords: *global governance, BRICS+, blockchain, Kuramoto synchronization, distributed AI, Bittensor, Arkhe-Chain, LGPD, GDPR, FATF, DAF philanthropy, C/Z duality, τ-field, gRPC, jurisdictional GPS control*

Table of Contents

1. Introduction and Vision

The twenty-first century has revealed a fundamental tension in global governance: international institutions designed for the post-World War II order — centralized, slow-moving, structurally biased toward a small number of powerful states — are increasingly inadequate to coordinate responses to challenges that are at once global in scope and local in impact. Climate change, pandemic preparedness, digital sovereignty, and development finance all require multi-jurisdictional coordination at speeds and granularities that traditional diplomatic channels cannot support.

ONU 2.0 is a direct response to this institutional gap. It is not a reform of existing multilateral bodies but a new infrastructure layer — a digital coordination substrate that existing institutions, national governments, and civil society actors can use to achieve binding, auditable, and sovereign coordination without ceding legal authority to a supranational entity.

1.1 Design Principles

The platform is governed by six core principles that permeate every architectural decision:

Digital Sovereignty. Each member state retains full legal sovereignty over its jurisdictional data. GPS polygon boundaries enforce territorial scope at the infrastructure level — no data crosses a border without explicit jurisdictional clearance.

Radical Transparency. Every governance action — project submission, approval, rejection, fund disbursement — generates an immutable, cryptographically chained audit record. The Merkle ledger makes retroactive falsification computationally infeasible.

Multilingual Inclusion. The platform natively supports 10 languages, including full RTL rendering for Arabic and Farsi. Language is treated as a first-class infrastructure concern, not an afterthought.

Progressive Decentralization. ONU 2.0 begins with a permissioned architecture and progressively decentralizes through the Bittensor-forked subnet model, eventually targeting full on-chain governance via the ZK-SNARK compliance module (Q1–Q2 2026 roadmap).

Measurable Social Impact. All philanthropic disbursements are linked to UN Sustainable Development Goals (SDGs) and tracked on-chain via the DAF module. Impact is not declared — it is cryptographically attested.

Compliance by Architecture. LGPD, GDPR, FATF, and COAF requirements are not applied as policy layers on top of the system — they are encoded into the data model, encryption choices, retention schedules, and AML pipeline at the schema level.

1.2 Strategic Context: The BRICS+ Opportunity

The BRICS+ bloc — comprising Brazil, Russia, India, China, South Africa, Egypt, Ethiopia, Iran, UAE, and Saudi Arabia, with Mexico and France as observer partners — represents over 40% of global GDP and approximately 45% of the world's population. This bloc has articulated a consistent demand for digital infrastructure that reflects its own legal traditions and governance preferences, rather than inheriting frameworks designed by and for Western financial systems.

ONU 2.0 is designed as sovereign-first infrastructure for the Global South: its legal anchor is Brazilian law (LGPD, Marco Civil da Internet), its financial compliance framework integrates COAF norms (Brazilian anti-money laundering authority), and its data residency defaults to national sovereignty. It is, by design, interoperable with — but not dependent on — Western-centric financial and data infrastructure.

2. Philosophical Foundations: Governance as Phase Projection

ONU 2.0 is not merely a software platform. Its architecture embodies a specific ontological claim about the nature of governance: that legitimate collective decision-making is a *phase projection process* — the crystallization of a field of distributed possibility into a field of durable, accountable actuality.

2.1 The C/Z Duality in Governance

The Arkhe(n) framework distinguishes two ontological domains that, applied to governance, yield precise and productive mappings:

Domain	Formal Name	Governance Instantiation	ONU 2.0 Implementation
C	Phase / Possibility	Policy intent, legal norms, stakeholder consensus, proposed projects, draft regulations	Project submissions, SDG alignment proposals, DAF donor intentions
Z	Structure / Actuality	Executed transactions, ratified decisions, legally binding agreements, published audit logs	Approved projects, Merkle-chained records, Bitcoin-anchored hashes
M	Projection Operator	The governance process itself: deliberation, approval, legal authorization	Multi-level approval pipeline, GPS jurisdictional validation, Kuramoto

2.2 The Ontology X Axioms Applied to Governance

The Ontology X framework — derived from the isomorphism between quantum measurement theory, Curry-Howard correspondence in type theory, and Husserlian phenomenology — provides three axioms that any coherent system distinguishing possibility from actuality must satisfy. Applied to ONU 2.0:

Axiom I: Z = M[C]. A governance outcome is the image of a governance intention under the institutional process that actualizes it. A project submission (C) becomes an approved, funded reality (Z) only by passing through the multi-level approval operator (M). The Merkle ledger records this transformation irreversibly.

Axiom II: M ∈ C. The governance process is itself a subject of governance. The approval pipeline, the agent network, the consensus algorithm — all are objects that can be queried, audited, reformed, and re-specified within the same platform that executes them. No homunculus, no external authority: the system is recursively accountable to itself.

Axiom III: M[M] = M. Legitimate governance is idempotent: auditing an already-audited record produces the same record. Approving an already-approved project at the same level has no additional effect. The Merkle verification function embodies this: verify(verify(chain)) = verify(chain). Recursive application preserves coherence.

2.3 The Kuramoto Threshold as Democratic Legitimacy

The choice of the Kuramoto synchronization model for network consensus — and specifically the critical coupling threshold phi_c = 0.618 (the reciprocal of the golden ratio) — is not accidental. In the Kuramoto model, the order parameter R represents the degree to which independent oscillators have achieved spontaneous synchronization through local coupling:

```
R(t) = | (1/N) * sum_j exp(i * theta_j(t)) |
```

When R < phi_c, the network is in an asynchronous, disordered phase: operators have not achieved sufficient coherence to produce legitimate collective decisions. When R >= phi_c, the network has crossed the phase transition into coherent governance: individual operator states are sufficiently aligned that the collective output has systemic validity.

This operationalizes a deep democratic intuition: a decision is not legitimate merely because it is recorded, but because the network of actors producing it has achieved a threshold of alignment. ONU 2.0 makes this threshold explicit, measurable, and enforceable at the infrastructure level.

3. Architectural Overview: Seven Layers

The ONU 2.0 platform is organized as a seven-layer stack. Each layer addresses a distinct dimension of the governance challenge — geographic, procedural, communicative, evidentiary, policy, cryptographic, and consensus — and exposes well-defined interfaces to adjacent layers.

Layer	Name	Function
1	GPS Jurisdictional Control	Geographic boundary enforcement via GPS polygon validation. Every operation is pre-au
2	Multi-Level Approval Pipeline	State machine governing the lifecycle of governance actions: PENDING → AWAITING_A
3	AO Message Queue	Asynchronous typed message routing between all platform modules, inspired by the AO p
4	Compliance Ledger & Merkle Chain	Append-only, SHA-256-chained audit log of all critical operations. Tamper-evident by con
5	BRICS+ Policy Exchange Network	Peer-to-peer policy sharing infrastructure across 10+ member states, with thematic categ
6	Arkhe-Chain (Bitcoin OP_RETURN)	External cryptographic anchoring of governance records to the Bitcoin blockchain via OP_
7	Kuramoto Consensus	Network coherence measurement via coupled oscillator model. Alerts when synchronizati

4. Layer 1 — GPS Jurisdictional Control

The first architectural challenge of any global governance platform is the question of *where* a governance action is valid. Traditional international law resolves this through treaty frameworks negotiated over years. ONU 2.0 resolves it in real time through GPS polygon validation — a computational encoding of territorial sovereignty.

4.1 Jurisdictional Polygon Architecture

Each jurisdiction registered in the platform is defined as a polygon of up to 64 GPS vertices (longitude/latitude pairs, precision ±1 meter). Jurisdictions are hierarchically organized:

Municipal → State/Province → National → Supranational (BRICS+)

The hierarchy supports non-contiguous geometries — enclaves, overseas territories, and special economic zones are represented as multi-polygon objects within the same jurisdictional entity. This allows, for example, France's overseas territories to participate in BRICS+ observer protocols under French jurisdictional scope.

4.2 Pre-Execution Validation

Before any governance action — project submission, fund disbursement, agent registration, policy proposal — is processed, the platform executes the CHECK_JURISDICTION function:

```
CHECK_JURISDICTION(project_id, lat, lon) → point_in_polygon(lat, lon,
jurisdiction.boundaries) → hierarchy_check(jurisdiction.level, action.required_level) →
returns: {authorized: boolean, jurisdiction_id: uuid, audit_ref: hash}
```

Rejections are **automatic and immutable**: they generate a Merkle-chained audit entry without requiring human review. This is a deliberate design choice — territorial validation is a matter of fact, not judgment, and should not consume human approval capacity.

4.3 LGPD Compliance: GPS Pseudonymization

A direct consequence of storing GPS coordinates is the risk of re-identification of data subjects through location. Article 12 of Brazil's LGPD distinguishes anonymized data (not subject to the law) from pseudonymized data (subject to the law with reduced obligations). ONU 2.0 pseudonymizes all GPS coordinates in audit logs via SHA-256 before persistence:

```
pseudonymized_coord = SHA-256(lat || lon || entity_salt)
```

> *The semantic reference is preserved via the jurisdiction UUID — auditors can verify that an action occurred within a given jurisdiction without accessing the raw coordinates. This satisfies LGPD Art. 12 and Art. 13 (research use of pseudonymized data).*

5. Layer 2 — Multi-Level Approval Pipeline

Governance decisions cannot be binary — approved or rejected by a single authority. Legitimate multilateral governance requires layered deliberation: technical review, legal validation, political authorization, and ethical oversight, each producing an independent, immutable record.

5.1 State Machine

Every governance action passes through a formal state machine:

PENDING → AWAITING_APPROVAL → { APPROVED | REJECTED }

The state machine supports configurable escalation: actions can require sequential approval from multiple levels (e.g., municipal → state → national) or parallel approval from a defined quorum. Each level transition produces an independent Merkle-chained audit entry containing: reviewer identity (pseudonymized), review notes, timestamp (ISO 8601 UTC), and IP address (pseudonymized under LGPD).

5.2 LGPD Art. 20 — Human Review of Automated Decisions

Article 20 of Brazil's LGPD grants data subjects the right to request human review of decisions made solely by automated means. ONU 2.0 encodes this right at the architectural level: no automated decision with significant impact on a data subject can be final without a human review node in the approval pipeline. The EthicsOversight sub-network (SN06) flags high-impact actions for mandatory human-in-the-loop review.

5.3 Timeout and Escalation

Each approval level has a configurable timeout. On expiry, the AO Message Queue (Layer 3) automatically routes an escalation message to the supervisor level and broadcasts a WebSocket notification to all registered stakeholders. Timeout events are themselves Merkle-chained — inaction is as auditable as action.

6. Layer 3 — AO Message Queue

Distributed governance systems face a fundamental coordination problem: modules must communicate reliably across network partitions, without requiring synchronous coupling that would make the system fragile. The AO Message Queue solves this through an actor-oriented asynchronous routing protocol inspired by the AO supercomputer protocol developed for the Arweave ecosystem.

6.1 Message Taxonomy

All inter-module communication is typed through five canonical action classes:

Action Type	Direction	Purpose
`INIT_CONFIG`	System → All	Initialize or update platform configuration across nodes
`CHECK_JURISDICTION`	Any → Layer 1	Request GPS boundary validation before action execution

`JURISDICTION_STATUS`	Layer 1 → Any	Return result of GPS validation with jurisdiction metadata
`EXECUTE_SANDBOX`	Layer 2 → Agents	Trigger sandboxed execution of approved governance action
`AGENT_HEARTBEAT`	Agents → Monitor	Liveness signal from gRPC Arkhe(n) agents to Kuramoto layer

6.2 Delivery Guarantees

The AO Message Queue provides at-least-once delivery semantics with a replay journal for failure recovery. Each message is assigned a unique ID and tracked through states: sent → delivered → processed. The journal allows complete replay of the message history for forensic audit or disaster recovery — equivalent to the Write-Ahead Log in database systems, but for governance events.

Measured throughput on commodity hardware: **847 messages/second**. This is sufficient for the anticipated governance volume of BRICS+ coordination at full deployment.

7. Layer 4 — Compliance Ledger & Merkle Chain

The evidentiary foundation of ONU 2.0 is an append-only, cryptographically chained audit ledger. Every governance action — approval, rejection, disbursement, agent registration, jurisdiction check — generates an immutable entry whose integrity is provable without trusting any single authority.

7.1 Hash Chain Architecture

Each audit entry is linked to its predecessor via SHA-256 chaining:

```
entryHash = SHA-256( prevHash // hash of previous entry (or 'GENESIS') + entityType //
type of affected entity + entityId // entity identifier + action // action executed +
performedBy // executor (pseudonymized under LGPD) + timestamp // ISO 8601 UTC )
```

This construction has a critical security property: modifying any single entry invalidates every subsequent hash. The tampered entry produces a different hash, which propagates as a chain break detectable via GET /api/audit/verify-chain — a linear scan that returns {valid: boolean, checked: number, broken: number}.

7.2 External Anchoring to Bitcoin

The Merkle chain provides integrity guarantees within the platform. For external, jurisdiction-independent immutability, periodic snapshots of the chain root hash are anchored to the Bitcoin blockchain via OP_RETURN (Layer 6: Arkhe-Chain). This creates a two-level immutability guarantee: internal (Merkle chain) and external (Bitcoin finality, approximately 6-of-6 confirmation depth).

7.3 LGPD Art. 18 — Right to Erasure

Brazilian LGPD Art. 18 grants data subjects the right to deletion of their personal data. This creates a tension with the append-only nature of the audit ledger. ONU 2.0 resolves this through *pseudonymization-as-deletion*: upon a verified deletion request, the personal data payload in the affected

entries is replaced with a SHA-256 hash of the original data. The audit entry itself is preserved (maintaining chain integrity), but the personal data is irrecoverably removed. The deletion event itself is Merkle-chained to the lgpd_deletion_requests table.

8. Layer 5 — BRICS+ Policy Exchange Network

Public policy does not emerge in isolation. Effective multilateral governance requires that member states can learn from each other's policy experiments, adapt successful approaches to their own legal frameworks, and avoid duplicating failures. The BRICS+ Policy Exchange Network provides the infrastructure for this structured knowledge sharing.

8.1 Policy Lifecycle

Policies move through a five-stage lifecycle:

`proposta` → `em revisão` → `aprovada` → `implementada` → `arquivada`

Each transition is Merkle-chained and timestamped. The platform tracks statistical trends by country and thematic category, enabling dashboard-level visibility into which policy areas are generating the most cross-member interest.

8.2 Thematic Coverage

The network covers seven thematic categories aligned with BRICS+ cooperative frameworks: energy, health, finance, technology, environment, education, and security. Each category can be further subdivided by SDG alignment, enabling direct linkage between policy proposals and UN development goals.

8.3 Treaty Compliance Layer

Bilateral and multilateral treaty obligations among BRICS+ members create complex compliance requirements — a policy acceptable under Brazilian law may require modification before adoption in China or Iran. The treaty compliance layer maps policy proposals against registered bilateral agreements, flagging potential conflicts before a proposal enters the approval pipeline.

9. Layer 6 — Arkhe-Chain (Bitcoin OP_RETURN Anchoring)

The Arkhe-Chain is the external immutability layer of ONU 2.0. It anchors cryptographic commitments of governance records to the Bitcoin blockchain via OP_RETURN transactions, providing jurisdiction-independent, censorship-resistant proof of data existence at a specific point in time.

9.1 Technical Mechanism

Bitcoin's OP_RETURN opcode allows up to 80 bytes of arbitrary data to be embedded in a transaction output that is explicitly marked as unspendable — it does not contribute to the UTXO set and imposes no

ongoing cost on the Bitcoin network beyond the transaction fee. ONU 2.0 uses this capacity to embed SHA-256 hashes of Merkle chain root snapshots:

```
OP_RETURN <32-byte SHA-256 of Merkle root> <16-byte platform prefix> Platform prefix:
'ONU2' + Chain_ID(2140) + timestamp(4 bytes)
```

A commitment is considered immutable when it has received 6-of-6 confirmations from the Arkhe-Chain node network — approximately 60 minutes of Bitcoin block time.

9.2 Khovanov Topological Invariant

The Arkhe-Chain introduces a novel topological representation of network node relationships through the Khovanov homology invariant — a categorification of the Jones polynomial from knot theory. Each node configuration in the network is mapped to a braid word, and the Khovanov invariant provides a polynomial fingerprint of the network topology that is preserved under Reidemeister moves (topologically equivalent network reconfigurations).

This has a practical security implication: two network configurations that produce the same Khovanov invariant are topologically equivalent from a trust perspective — an attacker cannot gain additional influence by reorganizing node connections while preserving the topological invariant. The invariant is computed and stored alongside each Bitcoin anchoring event.

> *The Khovanov invariant is a well-established mathematical object (Khovanov, 2000; Duke Math. J.). Its application to network topology in governance systems is a novel contribution of ONU 2.0.*

10. Layer 7 — Kuramoto Consensus

Network governance requires not just that decisions be recorded, but that the network producing those decisions be in a coherent state. A split network — where different subsets of operators have divergent views of system state — cannot produce legitimate governance outputs. The Kuramoto Consensus layer provides real-time measurement of network coherence and automatic safety alerts when coherence falls below operational thresholds.

10.1 The Kuramoto Model

The Kuramoto model (Yoshiki Kuramoto, 1984) describes the spontaneous synchronization of coupled oscillators. Each operator node i is modeled as an oscillator with natural frequency omega_i and phase theta_i. The evolution equation is:

$$d(\theta_i)/dt = \omega_i + (K/N) * \sum_j [\sin(\theta_j - \theta_i)]$$

where K is the coupling constant and N is the total number of nodes. The order parameter R — the Kuramoto coherence score — is:

$$R(t) = | (1/N) * \sum_j \exp(i * \theta_j(t)) |, \quad R \in [0, 1]$$

R = 0 indicates complete incoherence (all oscillators at random phases); R = 1 indicates perfect synchronization. The critical coupling threshold above which spontaneous synchronization emerges is

K_c = 2 * sigma / pi (for Gaussian natural frequency distribution with standard deviation sigma).

10.2 Operational Thresholds

ONU 2.0 operates with two coherence thresholds:

Threshold	Value	Meaning	Action
Safety threshold	R = 0.70	Minimum coherence for normal operations	Alert broadcast via WebSocket to all operators; SN0
Governance threshold	R = phi_c = 0.618	Phase transition point; below this, the network is in disorder	Critical alert; high-impact decisions suspended pend
Optimal range	R in [0.80, 0.95]	Normal operating coherence for a healthy governance network	No action required; metrics logged to Parseable obs

10.3 Monitoring Infrastructure

The Kuramoto dashboard updates every 15 seconds via WebSocket push. Per-operator metrics include: current phase theta_i, natural frequency omega_i, contribution to R, latency to platform median, CPU load, memory usage, and timestamp of last gRPC Heartbeat from the Arkhe(n) agent. The Parseable observability integration provides configurable retention and external audit export.

11. ONU 2.0 Subnet — Distributed AI (Bittensor Fork)

The AI layer of ONU 2.0 is implemented as a fork of the Bittensor protocol (Rao et al., 2022). While the original Bittensor protocol creates a peer-to-peer market for machine learning services, the ONU 2.0 Subnet redirects the same incentive architecture toward public governance tasks: compliance validation, policy auditing, and public service delivery. TAO-equivalent emissions are denominated in governance units rather than financial tokens.

11.1 Six Specialized Sub-Networks

The subnet architecture consists of six specialized networks, each addressing a distinct dimension of AI-assisted governance:

SN	Name	Function	Key Capabilities
SN01	**DataValidator**	Project data and jurisdiction integrity verification	GPS polygon validation, CNPJ/CPF format verification, LGPD compliance
SN02	**PolicyEnforcer**	Real-time BRICS+ regulatory compliance analysis	Treaty conflict detection, SDG alignment scoring, cross-jurisdiction policy
SN03	**AuditSentinel**	Continuous Merkle ledger surveillance	Hash chain verification, inconsistency detection, anomaly flagging, forens
SN04	**SubnetMiner**	Consensus mining and emission distribution	Yuma Consensus v2 implementation, stake-weighted voting, emission ca
SN05	**IdentityGuardian**	Sovereign Self-Sovereign Identity (SSI) management	W3C DID resolution, credential issuance, DID resolution, credential revocation
SN06	**EthicsOversight**	Automated decision ethics supervision (LGPD Art. 20)	Human-in-the-loop routing for high-impact decisions, bias detection, expla

11.2 Yuma Consensus — Validator Reward Calculation

The Yuma Consensus algorithm (adapted from Bittensor) governs how validator contributions are weighted and rewarded. The adaptation for ONU 2.0 uses alpha = 0.41 (empirically determined for governance task stability):

```
W[i] = sum_j S[j] * W_tilde[j][i] # validator i weight R[i] = W[i] / sum_k W[k] # normalized reward E[i] = alpha * R[i] + (1 - alpha) * B[i] # emission with history (alpha = 0.41)
```

where S[j] is the stake of validator j, W_tilde[j][i] is the weight that validator j assigns to miner i, and B[i] is the historical baseline emission for miner i. The alpha parameter controls the balance between immediate performance (R[i]) and historical track record (B[i]).

11.3 Philosophical Note: AI as Governance Operator

The six sub-networks instantiate the Ontology X axioms at the AI level. Each SN is an M-operator: it takes inputs from the C-domain (policy proposals, project submissions, identity claims) and projects them into Z-domain outputs (compliance verdicts, audit flags, verified credentials). The Yuma Consensus algorithm ensures that M[M] = M — the consensus over validators produces the same result as the consensus over the consensus, satisfying the idempotence requirement of Axiom III.

12. gRPC Arkhe(n) — Distributed Agent Registry

The gRPC Arkhe(n) protocol defines the interface through which AI agents register with, communicate with, and are governed by the ONU 2.0 platform. It provides five remote procedure calls covering the full agent lifecycle, secured via a two-phase authentication scheme.

12.1 Protocol Definition

```
// arkhe_agent.proto service ArkheAgentService { rpc RegisterAgent (RegisterAgentRequest) returns (RegisterAgentResponse); rpc GetTask (GetTaskRequest) returns (GetTaskResponse); rpc ReportStatus (ReportStatusRequest) returns (ReportStatusResponse); rpc Heartbeat (HeartbeatRequest) returns (HeartbeatResponse); rpc RevokeAgent (RevokeAgentRequest) returns (RevokeAgentResponse); }
```

12.2 Two-Phase Authentication

Agent security uses a two-phase authentication scheme designed to prevent both credential theft and replay attacks:

Phase 1 — Enrollment (HMAC-SHA256): The agent presents its enrollment payload — agentId, name, role, subnet code, public key, capabilities, and a Unix timestamp — authenticated with an HMAC-SHA256 signature over the canonical payload, using the operator-managed enrollment key (ENROLLMENT_KEY). A ±5-minute timestamp window prevents replay attacks.

Phase 2 — Operational (JWT Bearer): Upon successful enrollment, the agent receives a JWT Bearer token (8-hour expiry, HS256 algorithm). All subsequent RPC calls — GetTask, ReportStatus, Heartbeat — must include this token in the Authorization header.

12.3 Agent Lifecycle States

`registered` → `active | idle | busy` → `suspended | revoked`

Agent state transitions are Merkle-chained, providing a complete and tamper-evident lifecycle audit trail. Revocation is immediate: the JWT Bearer token is invalidated and the agent's public key is removed from the active key set. Revocation events are also anchored to Bitcoin via Arkhe-Chain.

> *The gRPC server operates on port 50051 (internal network). A REST management API at /api/agents/* provides human-readable access to agent status and lifecycle events for platform administrators.*

13. DAF Philanthropic Fund — On-Chain Governance

The DAF (Donor Advised Fund) module represents ONU 2.0's philanthropic infrastructure layer. Inspired by the Endaoment protocol — which has facilitated USD 29M in on-chain charitable donations with 97.6% throughput efficiency — the ONU 2.0 DAF adapts this model for the Brazilian legal and financial environment, with automatic cryptocurrency-to-BRL conversion, comprehensive AML/KYC compliance, and SDG impact tracking.

13.1 Supported Assets and Conversion

The DAF accepts nine crypto assets and performs automatic conversion to BRL via registered exchange partners:

BTC	ETH	USDC	USDT	SOL	BNB	MATIC	DREX	BRL

13.2 Fee Structure

The DAF implements a tiered fee structure for inbound donations, incentivizing larger philanthropic commitments through reduced platform costs:

Donation Amount (BRL)	Platform Fee	Effective Cost per Million
< R$ 1,250,000	0.50%	R$ 5,000
R$ 1,250,000 – R$ 2,500,000	0.40%	R$ 4,000
R$ 2,500,000 – R$ 5,000,000	0.30%	R$ 3,000
> R$ 5,000,000	0.05%	R$ 500
Outbound grant (all amounts)	1.00%	R$ 10,000

13.3 AML/KYC Pipeline

Every donation and grant passes through a three-tier AML compliance pipeline, calibrated to COAF Resolution 36/2023 and FATF Recommendation 10:

Tier	Trigger	Process	Legal Basis
Routine	All transactions	OFAC SDN list check, PEP screening, risk score → APPROVED	FATF Rec. 10, COAF Res. 36/2023
Enhanced Due Diligence	Donation >= R$ 500,000	Fund origin verification, AML level → ENHANCED, manual review required, 3 business days	FATF Rec. 10, BACEN Circular 3.978/2020
KYC Mandatory	Anonymous donation >= R$ 1,250,000	Donation blocked pending KYC (document + selfie), re-check → APPROVED or BLOCKED	FATF Rec. 16, COAF Res. 36/2023 Art. 8

13.4 On-Chain Impact Tracking

Each donation and grant generates a Merkle hash recorded in the daf_donations and daf_grants tables. These hashes are linked to SDG (Sustainable Development Goal) categories in the ESG dashboard,

enabling real-time, cryptographically attested impact reporting. Donors can verify independently that their funds reached the declared beneficiary by checking the Merkle hash against the public ledger or the Bitcoin anchor.

NGO registration requires CNPJ (Brazilian tax identifier), CEBAS certification (social assistance qualification), Título de Utilidade Pública (public utility designation), and PIX/TED bank details. Each field is verified against official government registries via API integration.

14. PII Vault — LGPD / AES-256-GCM

Personally Identifiable Information (PII) in ONU 2.0 is isolated in an encrypted vault that ensures: (1) the raw data is never exposed in logs, URLs, or error messages; (2) the data cannot be decrypted without the platform's session secret; (3) data integrity is independently verifiable; and (4) deletion requests are honored in a way compatible with the append-only audit ledger.

14.1 Encryption Architecture

Each PII record is encrypted using AES-256-GCM (Galois/Counter Mode), an authenticated encryption scheme that provides both confidentiality and integrity verification in a single operation:

```
key = scrypt(SESSION_SECRET, salt, N=32768, r=8, p=1) # 256-bit key iv = random_bytes(12)
# 96-bit IV ciphertext, authTag = AES_256_GCM_encrypt(key, iv, plaintext) stored = iv ||
authTag || ciphertext # 12 + 16 + n bytes integrityHash = SHA-256(entityType || entityId
|| plaintext || salt)
```

The authTag (16 bytes) prevents silent tampering: any modification of the ciphertext causes decryption to fail with an authentication error rather than returning corrupted plaintext. The integrityHash provides an additional, out-of-band integrity check stored separately from the encrypted payload.

Access tokens are randomly generated UUIDs — the actual PII identifier is never transmitted over the API. This ensures that even a complete log compromise reveals no PII.

14.2 LGPD Compliance Operations

Storage (LGPD Art. 6, VII — Security): AES-256-GCM with scrypt key derivation exceeds the technical security standard implied by LGPD's security principle.

Pseudonymization (LGPD Art. 12): The UUID token system means PII is not accessible without the platform's internal token mapping — satisfying the Art. 12 definition of pseudonymized data.

Erasure (LGPD Art. 18, VI): Upon deletion request, the encrypted payload is replaced with a SHA-256 hash of the original data (irreversible one-way transformation), and the deletion event is Merkle-chained to lgpd_deletion_requests. The audit entry persists; the personal data does not.

15. Legal Compliance Framework

ONU 2.0 operates at the intersection of multiple legal frameworks across 12+ jurisdictions. The platform's legal compliance strategy is architecture-first: compliance requirements are encoded into the data model and processing logic, not applied as post-hoc policies.

15.1 Brazilian Law — LGPD and Marco Civil

Brazil serves as the legal anchor jurisdiction for ONU 2.0. The following LGPD articles have direct architectural implementations:

Article	Right/Obligation	ONU 2.0 Implementation
`Art. 7°, II`	Processing for legal obligation compliance	GPS validation is a legal prerequisite for cross-border data flows
`Art. 7°, VI`	Processing for legitimate interests	Audit logging for governance accountability
`Art. 12`	Pseudonymized data treatment	SHA-256 pseudonymization of GPS coordinates and donor identifiers
`Art. 13`	Research and audit use	Merkle ledger export for forensic audit and regulatory review
`Art. 16`	Data retention limits	GPS data deleted on project closure; see retention schedule
`Art. 18, VI`	Right to erasure	Pseudonymization-as-deletion with Merkle-chained deletion record
`Art. 20`	Right to review automated decisions	SN06 EthicsOversight; human-in-the-loop for high-impact decisions

15.2 Data Retention Schedule

Data Type	Retention Period	Legal Basis
Operational audit logs	6 months	Marco Civil da Internet, Art. 15
WebSocket connection logs	1 year	Marco Civil da Internet, Art. 13
Project data (complete)	5 years	LGPD + Lei de Arquivos (Lei 8.159/1991)
GPS coordinates (pseudonymized)	Duration of project	LGPD Art. 16 — elimination after purpose
AML/KYC records (DAF)	5 years	COAF Res. 36/2023 + FATF Rec. 11
NGO registration data	10 years	Lei de Arquivos + COAF
Merkle hashes / Arkhe-Chain anchors	Permanent	Cryptographic immutability — ANPD Circular 1/2021

15.3 Multi-Jurisdictional Compliance

Each of the 12 member/observer states brings distinct data protection requirements. ONU 2.0's compliance posture for the major frameworks:

GDPR (EU/France): The platform implements GDPR requirements for the French observer partner through: lawful basis documentation (Art. 6), data minimization (Art. 5.1.c), privacy by design (Art. 25),

and breach notification capacity (Art. 33). The DPO contact is registered with the French CNIL.

DPDP Act 2023 (India): India's Digital Personal Data Protection Act requires explicit consent for data processing. The platform's LGPD consent architecture is compatible with DPDP requirements, with localization adaptations for Hindi-language consent flows.

PIPL (China): China's Personal Information Protection Law requires data localization for Chinese citizens' data. The platform's GPS-based jurisdictional routing ensures Chinese project data remains within Chinese-sovereign infrastructure nodes.

16. Security Posture

JWT Control Plane: All mutating HTTP operations (POST, PATCH, PUT, DELETE) are intercepted by the Express.js JWT middleware. Tokens use HS256 algorithm with 8-hour expiry. Exceptions: /api/auth/login and /api/agents/simulate. Token issuance is logged and Merkle-chained.

AES-256-GCM (PII Vault): Authenticated encryption for all personal data. Key derived via scrypt (N=32768, r=8, p=1) from SESSION_SECRET. Unique IV per operation. authTag prevents silent tampering.

HMAC-SHA256 (Arkhe Enrollment): Agent enrollment authenticated via HMAC-SHA256 over the canonical payload. Replay window of ±5 minutes enforced via payload timestamp. Enrollment key (ENROLLMENT_KEY) rotated quarterly by platform operators.

HTTP Security Headers: X-Frame-Options: DENY, X-Content-Type-Options: nosniff, Referrer-Policy: strict-origin-when-cross-origin, Permissions-Policy: geolocation=(), camera=(), microphone=(). HSTS with 1-year max-age in production. Rate limiting: 120 requests/minute/IP.

GPS Pseudonymization: All raw latitude/longitude values are SHA-256 hashed with an entity-specific salt before persistence in audit logs. Semantic jurisdiction reference is preserved via UUID. Raw coordinates are never written to any persistent store.

Drizzle ORM (SQL Injection Prevention): All database queries use Drizzle ORM's parameterized prepared statements. Zero raw SQL execution. All API endpoint inputs validated via Zod schema before reaching the database layer. Schema-level type safety prevents type confusion attacks.

17. Data Model (PostgreSQL / Drizzle ORM)

The ONU 2.0 data model is implemented in PostgreSQL using Drizzle ORM for type-safe schema definition and query building. The model is organized into five modules, each corresponding to a major platform subsystem.

17.1 Core Module

```
jurisdictions id · name · level(municipal|state|national|supranational) country(BRICS+) ·
boundaries(GPS polygon, max 64 vertices) isActive · createdAt projects id · protocolId ·
title · description · category jurisdictionId(FK) · submittedBy · contactEmail · status
lat · lon · createdAt · updatedAt approvals id · projectId(FK) · level ·
status(pending|approved|rejected) reviewedBy · reviewNotes · reviewedAt · timeoutAt
ao_messages id · projectId(FK) · target · action · payload(JSONB)
status(sent|delivered|processed) · createdAt audit_logs id · entityType · entityId ·
action · performedBy ipAddress · prevHash · entryHash · details(JSONB) · createdAt
```

17.2 PII / LGPD Module

```
pii_vault id · token(UUID, unique) · entityType · entityId encryptedPayload(AES-256-GCM
bytea) integrityHash(SHA-256) · createdBy · pseudonymizedAt lgpd_deletion_requests id ·
token(FK → pii_vault) · reason · requestedBy prevHash · entryHash · completedAt
```

17.3 Subnet ONU 2.0

```
subnet_onus id · subnetId(SN01..SN06) · name · status emissionRate · activeMiners ·
activeValidators consensusAlgo · lastYumaRun · createdAt
```

17.4 gRPC Arkhe(n) Agent Module

```
arkhe_agents id · agentId(unique) · name · role · subnetCode publicKey · version ·
capabilities(JSONB) status(registered|active|idle|busy|suspended|revoked) nodeId · cpuLoad
· memoryMb · lastHeartbeat arkhe_agent_tasks id · taskId(unique) · agentId(FK) · type ·
payload(JSONB) status(pending|assigned|running|completed|failed) priority · result(JSONB)
· assignedAt · completedAt
```

17.5 DAF Philanthropic Module

```
nonprofits id · cnpj(unique) · razaoSocial · nomeFantasia categoria · email · pixKey ·
bankCode status(pending|active|suspended) · cebas(bool) utilidadePublica(bool) ·
totalReceived · createdAt daf_funds id · donorName · donorCpfHash(SHA-256) · donorEmail
fundName · balance · totalDonated · totalGranted status ·
amlLevel(routine|enhanced|blocked) daf_donations id · fundId(FK) · assetSymbol ·
assetAmount brlEquivalent · swapRate · platformFee · netAmount status · amlStatus ·
merkleHash · createdAt daf_grants id · fundId(FK) · nonprofitId(FK) · amount pixKey ·
description · status · merkleHash platformFee · netAmount · disbursedAt aml_screenings id
· entityType · entityId · screeningType result(clear|review|match|blocked) · riskScore
triggeredBy · amountBrl · screenedAt
```

18. Member States and Supported Languages

ONU 2.0 provides native support for 10 languages, with full RTL rendering for Arabic and Farsi. Language detection is automatic at the session level, and all platform interfaces — dashboards, approval workflows, audit reports — are fully localized.

Country	Language	Role	Data Protection Law
Brazil (BR)	Portuguese (BR)	Host · Legal Anchor	LGPD · Marco Civil · LAI
Russia (RU)	Russian	BRICS+ · Technical Partner	Federal Law 152-FZ
India (IN)	Hindi	BRICS+ · Technology Hub	DPDP Act 2023 · IT Act 2000
China (CN)	Simplified Chinese	BRICS+ · Infrastructure	PIPL · Cybersecurity Law
South Africa (ZA)	English	BRICS+ · Governance	POPIA 2020
Egypt (EG)	Arabic	BRICS+ · North Africa Corridor	Data Protection Law 151/2020
Ethiopia (ET)	Amharic	BRICS+ · Sub-Saharan Hub	Developing data framework
Iran (IR)	Farsi	BRICS+ · Asian Corridor	Cyber Space Law
UAE (AE)	Arabic	BRICS+ · Financial Hub	PDPL 2022 (DIFC)
Saudi Arabia (SA)	Arabic	BRICS+ · Energy	PDPL 2021
Mexico (MX)	Spanish	Observer · Latin America	LFPDPPP 2010
France (FR)	French	Observer · European Union	GDPR · Loi Informatique et Libertes

19. Roadmap 2025–2027

Q1–Q2 2025 · COMPLETED

• Platform foundation: GPS jurisdictions, project submission, multi-level approval pipeline

• Merkle ledger + Arkhe-Chain Bitcoin OP_RETURN anchoring (Chain ID 2140)

• OWL ontology (GeoSPARQL, PROV-O, ODRL) for semantic interoperability

• 3D Globe (WebGPU) with interactive BRICS+ markers

• JWT Control Plane + authentication middleware

• PII Vault: AES-256-GCM encryption + SHA-256 integrity verification

Q3–Q4 2025 · COMPLETED

• ONU 2.0 Subnet: Bittensor fork, 6 sub-networks (SN01–SN06), Yuma Consensus v2

• gRPC Arkhe(n) Agent Registry: 5 RPCs, HMAC-SHA256 enrollment, JWT Bearer

• DAF Philanthropic Fund: crypto→BRL swap, AML/OFAC pipeline, NGO registry

• i18n expansion: 8 → 10 languages (Spanish + French added)

• ESG/SDG On-Chain Impact Report dashboard

• Platform renamed from AGI-AO Parallax to ONU 2.0

Q1–Q2 2026 · PLANNED

• DREX integration (Real Digital — Banco Central do Brasil)

• ZK-SNARK compliance verification preserving data privacy

• Multi-signature governance for high-impact approvals (5-of-7 quorum)

• Public REST/gRPC API for integration with legacy municipal systems

• ISO/IEC 27001 and SOC 2 Type II certification track

• Sovereign cloud deployment (AWS São Paulo / GCP São Paulo)

Q3 2026–2027 · VISION

• Interoperability with UN OCHA Digital Humanitarian API

• Quadratic voting protocol for BRICS+ multilateral decisions

• Multilingual AI Policy Assistant (fine-tuned on BRICS+ legislation)

• W3C SSI/DID Sovereign Identity module for BRICS+ citizens

- Cross-chain bridge (Bitcoin ↔ Ethereum ↔ Arweave) for Arkhe-Chain
- UNDP partnership for integrated SDG tracking

20. References

[R01] LGPD — Lei Geral de Proteção de Dados. Lei nº 13.709/2018. Brasília: Senado Federal, 2018.

[R02] Marco Civil da Internet. Lei nº 12.965/2014. Brasília: Senado Federal, 2014.

[R03] GDPR (RGPD). Regulation (EU) 2016/679. Official Journal of the European Union, L 119/1, 2016.

[R04] Rao, Y. et al. (2022). Bittensor: A Peer-to-Peer Intelligence Market. arXiv:2210.01619. Available: https://arxiv.org/abs/2210.01619

[R05] Endaoment Protocol (2023). On-Chain Donor Advised Funds. Technical documentation. endaoment.org/whitepaper

[R06] Kuramoto, Y. (1984). Chemical Oscillations, Waves, and Turbulence. Springer-Verlag, Berlin. ISBN 978-3-642-96799-3.

[R07] Khovanov, M. (2000). A categorification of the Jones polynomial. Duke Mathematical Journal, 101(3), pp. 359–426.

[R08] OGC (2022). GeoSPARQL 1.1 — A Geographic Query Language for RDF Data. Open Geospatial Consortium Standard, OGC 22-047r1.

[R09] W3C (2013). PROV-O: The PROV Ontology. W3C Recommendation, 30 April 2013.

[R10] W3C (2018). ODRL Information Model 2.2. W3C Recommendation, 15 February 2018.

[R11] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Available: bitcoin.org/bitcoin.pdf

[R12] COAF (2023). Resolução nº 36/2023. Critérios de Comunicação de Operações Suspeitas. Brasília: COAF.

[R13] FATF/GAFI (2023). International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation. Paris: FATF.

[R14] Williams, S. et al. (2024). AO: The Actor-Oriented Supercomputer. ao.arweave.dev. Technical specification.

[R15] European Commission (2023). GeoDCAT-AP v2.0.0 — A geospatial extension for DCAT-AP. Joinup Collaboration Platform.

[R16] India Parliament (2023). Digital Personal Data Protection Act 2023. New Delhi: Ministry of Electronics and Information Technology.

[R17] ISO (2022). ISO/IEC 27001:2022 — Information Security Management Systems — Requirements. International Organization for Standardization.

[R18] United Nations (2015). Transforming our world: the 2030 Agenda for Sustainable Development. Resolution adopted by the General Assembly on 25 September 2015, A/RES/70/1.

[R19] Oliveira, R. (2026). Arkhe(n) τ-Field System: OrbVM Architecture and Kuramoto Synchronization Dynamics. Arkhe(n) Research Group. ORCID: 0009-0005-2697-4668.

ONU 2.0 · Global Governance Platform Whitepaper v2.0.0
Author: Rafael Oliveira · ORCID: 0009-0005-2697-4668
Arkhe(n) Research Group · April 2026