OMATrust Whitepaper

Version 1.1 | January 2026 | OMA3

1. Executive Summary

The open internet is missing a universal trust layer. Today, trust depends on fragile signals: SSL certificates only prove domain ownership, audits live in PDFs instead of onchain, and reputation is siloed inside centralized platforms. As billions of AI agents begin transacting and interacting online, the inability to programmatically verify legitimacy becomes a systemic risk.

OMA3 is a Swiss non-profit consortium addressing this gap by building trust infrastructure for the open internet. The architecture has two integrated layers:

1. **OMATrust**- a cross-chain **verification protocol** where anyone, including end users and trusted third parties, can publish provable cryptographic attestations on any internet service, allowing humans and machines to verify legitimacy before using a service. This reputation/attestation framework, combined with a standards-based **identity registry**, brings **app store level trust** to the open internet.

2. **OMAChain**- an Ethereum Layer 2 that hosts **canonical coordination** contracts and provides additional **utility** and **ease of use** to OMATrust such as tracking OMAChain data across chains, subsidizing gas to reduce friction for OMATrust end users, and indexing cross-chain data in a decentralized manner.

This two-layer system solves two critical challenges:

- **Credible Neutrality**- decentralized control is a requirement to get the whole internet ecosystem to cooperate on shared infrastructure.

- **Sustainable Economics**- a native chain token and protocol revenue (from verification and query demand) allow OMATrust to be self-maintaining without relying on the generosity and influence of centralized entities.

OMATrust is launching at a pivotal moment. As the internet becomes more automated, driven by bots and AI agents, it needs more reliable, machine-verifiable trust signals. By combining cross-chain registries, cryptographic attestations, and subsidized coordination on OMAChain, OMATrust provides the foundation for a verifiable, AI-ready internet.

OMA3 is more than a standards organization — it is building the **trust layer of the open internet**.

2. The Problem: A Trust Crisis in the Open Internet

The internet is the backbone of commerce, communication, and entertainment — yet it was never designed with an **effective, universal trust layer**. Existing mechanisms like SSL certificates or platform reviews solve small parts of the problem, but they are incomplete. Every day, people and businesses still face the same basic question: **“Can I trust this service?”**

For individual users, the risks are familiar:

- You find a website selling discount tickets — is it a real vendor or a scam?
- You're reading a product review site — is this genuine advice or just advertising clickbait?
- You get a text message with a link — is it safe to click, or a phishing attempt to steal your credentials?
- In crypto, a new DeFi protocol promises high yields — is it actually audited, or just pretending with a fake badge?

These are not edge cases. They are everyday experiences that show how trust online is fragile, fragmented, and unverifiable.

2.1 Walled Gardens Show What's Possible — and What's Missing

Inside walled gardens like the Apple App Store, Google Play, Roblox, or Amazon, trust systems exist and deliver real consumer value. Many users won't download a Mac app unless it's in the App Store. Roblox players rely on platform curation before games are listed. Amazon shoppers depend on product reviews.

These examples prove that **trust infrastructure works and improves adoption**. But they also expose the problem: these systems are closed, proprietary, and inconsistent. Trust does not extend across ecosystems, and vast parts of the internet — websites, APIs, SaaS tools, and smart contracts — have no equivalent.

2.2 The Limits of Today's Trust Signals

The mechanisms we rely on today were never designed to provide universal, programmatic trust:

- **SSL certificates** prove domain ownership and enable encrypted traffic. But they don't prove legitimacy or safety. A phishing site can display the same lock icon as a bank.
- **Audits and certifications** are published as PDFs or badges on websites. Even if an AI model can parse the document, neither humans nor machines can know if it's authentic, current, or tamper-proof.
- **Centralized reputation systems** like Amazon reviews or App Store ratings work only inside their platforms. Even there, checks are partial — Apple verifies an app binary but not the app's servers, which can change at any time.
- **The broader internet** — websites and APIs — lacks any consistent reputation system. APIs power critical services like weather, stock prices, payments, and marketplaces, yet there's no standard way to verify their legitimacy or security.

Users and businesses are not "blind" to these risks; they rely on **social signals** like reviews, ratings, forums, and brand reputation. But these are inconsistent, siloed, and easily manipulated — and they cannot provide the cryptographic verifiability that AI agents and automated systems require.

2.3 Why This Hasn't Been Built Yet

The internet did create early **neutral standards** like SSL, IETF protocols, and W3C specifications. But after those foundations were laid, the economics shifted. Big Tech realized they could monetize trust inside their own platforms — through app stores, curated ecosystems, and review systems — and that's where investment went.

The open internet was left with partial fixes. Industry initiatives like the Linux Foundation's Open Source Security Foundation are important, but they remain fragmented and underfunded compared to the scale of the challenge. Building a global trust layer requires not just standards, but a **sustainable economic model** to maintain it.

This is where blockchain changes the equation: for the first time, we can align **neutral governance** with **sustainable economics** in one system.

2.4 Why the Problem is Urgent Now

The rise of AI agents makes this problem existential. Bots have quietly dominated internet traffic for years — scraping, crawling, and automating interactions at massive scale. Even without full-scale agent adoption, the lack of a verifiable trust layer has already created systemic vulnerabilities.

Humans can sometimes detect scams — they hesitate before clicking a suspicious link. AI agents, however, operate at **machine speed and global scale**. They may be "smarter" than humans, but intelligence alone isn't enough in this new world.

When a vulnerability is disclosed today, it is often exploited immediately across the internet. The same dynamic applies to unverified services:

- **Fraud at machine speed** — millions of AI agents could be tricked before humans notice.
- **Automation breakdowns** — entire workflows fail when APIs or contracts can't be verified.
- **Systemic risk to digital commerce** — without programmatic, verifiable trust, the growth of AI-driven commerce will be capped by mistrust.

At the same time, the **economic model of the internet is shifting.** The ad-driven web was built for human eyeballs, but bots and agents already dominate traffic. The next phase of the internet is **pay-per-call**: every API request, service interaction, or data query carries real economic value. The **x402 protocol** is a leading technology enabling these micropayments between agents and services, as is **Model Contact Protocol (MCP)** for agentic APIs, but neither defines a trust layer.

When every interaction involves a payment, **trust becomes non-negotiable**. It is one thing to browse a free website supported by ads; it is another to send money with every call. Without a universal, cross-chain trust layer, fraud and inefficiency will scale alongside bots and agents.

In short: the open internet cannot scale safely into an AI-driven, agent-powered, pay-per-call

future without a verifiable trust fabric.

3. The Solution: OMATrust and OMAChain

The shortcomings of today's trust mechanisms are clear: walled gardens, unverifiable PDFs, and social proof that can be manipulated. What the open internet needs is a **neutral, verifiable, and economically sustainable trust layer**. OMA3 delivers this through a two-layer architecture.

3.1 Overview: Two Integrated Layers

1. **OMATrust** — OMA3's first cross-chain decentralized solution, where developers tokenize apps, APIs, and websites, auditors and users publish cryptographic attestations, and humans or agents can verify legitimacy before engaging a service.
2. **OMAChain** — an Ethereum Layer 2 that serves as the canonical coordination environment for OMA3. It tracks OMATrust cross-chain, enables composability, and subsidizes trust functions so adoption is frictionless.

Together, these two layers create a **global trust fabric** for the open internet.

3.2 OMATrust: Cross-Chain Verification

OMATrust is the first expression of OMA3's vision: **turning trust into a machine-verifiable primitive**.

3.2.1 Attestation Framework

- Allows anyone to publish cryptographic attestations on any internet service.
- Types of attestations include:
    - **Security audits** (e.g., code verification, penetration testing).
    - **Compliance certifications** (e.g., GDPR, SOC2).
    - **User reviews** (where both humans and AI agents contribute structured feedback).
    - **Identity linking** (which keys belong to what entity)
- Allows attesters to prove interaction with a service to prevent sybil and spam attacks.
- Based on existing attestation systems so that proofs are transparent, tamper-resistant, and interoperable across chains.

3.2.2 Verification Standards

- End users and AI agents can instantly query tokenized entries and their attestations before engaging.
- No more digging through PDFs or relying on badges — verification becomes programmatic, universal, and real-time.

3.2.3 Identity Registry

- An app registry where apps, APIs, websites, and services are tokenized as onchain assets.
- It provides the ecosystem a persistent, verifiable identity that can be referenced across chains, completing the promise of decentralized app store level trust.
- Compatible with emerging community standards such as Ethereum's ERC-8004.

3.2.4 User Reputation

Attestations only work if the attesters themselves are credible. Without verification of the entities providing attestations, malicious actors could publish fake audits or reviews and undermine the trust layer.

Fortunately, verifying users and organizations is a challenge that multiple solution categories already address. OMATrust is designed to work in conjunction with these identity layers, rather than duplicate them:

- ***Regulatory Identity Verification** — KYC (Know Your Customer) and KYB (Know Your Business) services that confirm the legal identity of individuals and organizations.
- ***Proof of Personhood** — systems that establish whether an account represents a unique human, reducing the risk of Sybil attacks.
- ***Decentralized Identity Protocols** — frameworks for issuing and verifying DIDs (Decentralized Identifiers) that can attest to attributes without revealing sensitive data.
- ***Privacy-Preserving Verification** — technologies that allow users to prove attributes or uniqueness without disclosing unnecessary personal information.

OMATrust addresses the other side of the equation: trust for services (apps, APIs, websites). While identity systems focus on verifying who the user is, OMATrust ensures the service itself is legitimate and secure. Together, these complementary layers create an ecosystem where both sides of an interaction can be verified.

3.3 OMAChain: Canonical Coordination

While OMATrust functions across chains, OMAChain provides the core coordination layer that makes the system scalable, composable, and user-friendly.

3.3.1 Multi Chain Management

- **Decentralized Data** infrastructure helps clients find and analyze attestations across all chains, significantly reducing effort and reliance on centralized indexers.
- **Coordination contracts** on OMAChain track OMATrust contracts and apps across chains. For example, deduplicator contracts ensure each app, API, or service can only be tokenized once globally. This prevents confusion and maintains a single source of truth across ecosystems.

3.3.2 Composability

- OMAChain allows **multiple trust operations in a single transaction**.
- Example: A single OMAChain transaction can tokenize an app, write to the deduplicator, and put metadata onchain — actions that would otherwise require multiple steps across chains.
- This reduces friction for developers and also makes the process simpler and cheaper for end users.

3.3.3 Gas Subsidization

- Trust functions like reviews or attestations must be free for users to encourage adoption.
- OMAChain allows OMA3 to subsidize these attestation writes.
- Subsidization will initially be funded by OMA3's treasury reserves, with the option to expand to other chains as resources grow.

3.3.4 Roadmap for Decentralization

- Most L2s today are not decentralized at the governance level.
- OMAChain is governed by OMA3, a Swiss non-profit consortium, ensuring **credible neutrality from day one** (Section 7).
- The roadmap (Section 8) includes further decentralization of OMAChain's sequencer and indexing infrastructure, giving the ecosystem more resilience and neutrality over time.

3.4 Benefits and Use Cases of the Two-Layer System

The OMA3 two-layer architecture — OMATrust + OMAChain — provides practical benefits across the ecosystem. These are not abstract principles; they translate directly into concrete use cases:

3.4.1 AI Agents

Autonomous agents routinely interact with services—such as APIs for stock prices, medical data, or weather feeds. Before initiating a micropayment to access these services, agents can query OMATrust to verify their legitimacy and compliance. This mitigates fraud risks at machine scale and ensures interactions with trusted endpoints. OMATrust complements systems that enforce post-transaction accountability, such as those verifying payment execution or task completion through mechanisms like slashing or intent-based signing.

3.4.2 Users

End users can see verifiable reviews and certifications before downloading an app or trusting a website. Because OMAChain subsidizes attestations, leaving a review or rating is free and

seamless — encouraging broader participation and stronger feedback loops.

3.4.3 Auditors and Certifiers

Security firms and compliance bodies can publish proofs directly to the Identity Registry. Instead of unverifiable PDFs or website badges, attestations are cryptographic and machine-readable. This increases transparency and raises the standard for what it means to be "audited."

3.4.4 Developers

App developers can tokenize their software once in the Identity Registry, gaining global discoverability. Their app's reputation — reviews, certifications, and audit attestations — travels with it across ecosystems. This reduces fragmentation and makes onboarding into new marketplaces or environments frictionless.

3.4.5 Enterprises

Enterprises operating APIs in finance, healthcare, or government often require strict compliance (GDPR, HIPAA, SOC2). OMATrust allows these certifications to be cryptographically verified, so integrations can be automated without relying on manual trust assumptions.

3.4.6 x402 Participants

OMA3 believes x402- an internet micropayment protocol invented by Coinbase and backed by Google, Cloudflare, and others- will be the foundational economic mechanism for the machine-driven internet. OMA3 is contributing multiple extensions to x402 that allow it to integrate seamlessly with OMATrust.

4. OMATrust Protocol

OMATrust is OMA3's first cross-chain decentralized application. Its role is to make trust a machine-verifiable primitive, replacing PDFs, badges, and siloed reviews with cryptographic proofs that anyone — human or AI — can query in real time.

4.1 Attestations: Verifiable Proofs

OMA3 leverages **existing attestation projects** for reliability rather than reinventing the wheel, while extending them to cover the entire internet, not just Web3.

OMATrust introduces an **extension contract** that adds two capabilities to existing services:

1. **DID-native attestations** — Attestations can be bound to decentralized identifiers (DIDs) derived from URLs, contract addresses, or other identifiers. This makes OMATrust relevant for websites, APIs, and services outside traditional blockchain contexts.
2. **Improved searchability** — The extension contract associates additional metadata with attestations that improves onchain searchability and avoids reliance on centralized GraphQL APIs or ENS indexers.

Types of attestations supported include:

- **Security audits** from independent firms.

- **Compliance certifications** (e.g., ISO 27001, SOC2).
- **User reviews**, where both humans and AI agents contribute structured feedback.
- **Identity bindings**, so users can cryptographically prove shared ownership of online identities (e.g.- social handles) and signing keys (e.g.- blockchain accounts).

4.2 App Tokens: A Foundation for Trust

OMATrust allows service providers to register **app tokens**, represented as NFTs. Each tokenized app, API, or website becomes a verifiable onchain identity.

- On Ethereum and other EVM chains, app tokens follow the ERC-721 standard, with an upcoming Ethereum EIP for an ERC-721 extension that formalizes app-specific metadata.
- Parallel standards will be defined for other virtual machines, ensuring true **cross-chain compatibility**.
- Once minted, an app token serves as an additional anchor point for attestations and reviews associated with that service.

This simple but powerful primitive — turning software into NFTs — enables trust signals to be indexed, referenced, and queried consistently across the internet.

4.3 Verification and Attestation Flows

4.3.1 Verification Flow (for clients, users, or AI agents):

1. **Derive DID** — For example, from a URL (did:web) or contract address (did:eth).
2. **Query OMAChain Coordination Contract** — Find locations of associated attestations.
3. **Search for Attestations** — Collect and evaluate relevant proofs.
4. **Query App Token NFT** — Retrieve the token associated with the DID to gain more trust information.
5. **Decision** — Determine whether to engage with the service.

4.3.2 Attestation Flow (for auditors, users, or services):

- Auditors and compliance firms publish attestations directly to OMA3's contracts.
- Users can post reviews via **reputation.oma3.org** or other frontends.
- Websites may encourage their users to submit OMATrust reviews with a direct link.
- A **browser extension** may provide in-line visibility of OMATrust attestations, allowing users to see verification status while browsing.

OMATrust thus establishes the first programmatic, cross-chain verification layer for the open internet. Apps, APIs, and websites gain verifiable identities, while attestations transform audits, certifications, and user reviews into cryptographic proofs. The result: humans and AI alike can make trust decisions instantly and universally, without relying on intermediaries.

5. OMAChain Infrastructure

OMAChain is an **Arbitrum Orbit** Layer 2 that provides the coordination layer OMATrust needs to scale. It settles to Ethereum, stays fully EVM compatible, and aligns with the Orbit ecosystem's path toward sequencer decentralization. Beyond coordination, OMAChain integrates **Shinzo** to deliver two things that the trust stack requires:

1. decentralized, verifiable data access and
2. an economic model for high-volume reads.

5.1 Why Arbitrum Orbit

- **Ethereum Security \+ EVM Compatibility** — OMAChain settles to Ethereum while remaining fully EVM compatible.
- **Orbit Ecosystem** — Leveraging Arbitrum Orbit gives OMAChain a credible roadmap for sequencer decentralization.

5.2 Shinzo for Decentralized, Verifiable Data

Verification is a write problem *and* a read problem. If reads depend on opaque gateways, the trust layer breaks at the point of use. Shinzo fixes this by pushing indexing into the protocol's core data path:

- **Sequencer-integrated indexing**: as the sequencer orders transactions, it also emits the data needed for indexing (registry updates, deduplicator references, attestations) to a peer-to-peer network operated by Shinzo nodes.
- **Verifiability by design**: data is stored and propagated with cryptographic integrity (content addressing, authenticated histories, deterministic transforms), so downstream consumers can verify what they read instead of trusting a vendor's API.
- **Portable access**: anyone can run a Shinzo node to serve queries—no single API choke point—preserving neutrality across the ecosystem.

Result: apps, websites, and AI agents can query **verifiable OMATrust data** from multiple independent nodes rather than a single provider, keeping the trust guarantees intact end-to-end.

5.3 OMA3's Read-Revenue Model

OMA3 is a non-profit and **cannot indefinitely subsidize unlimited reads**. The architecture therefore separates light, public access from high-volume commercial access:

- **Free but rate-limited RPC**: OMAChain exposes a public endpoint for casual use and testing. It's intentionally rate-limited so the non-profit isn't forced to underwrite unbounded traffic.
- **Run a Shinzo node for full access**: services that need sustained, high-volume reads (e.g., directories, trust dashboards, AI workloads) operate their own Shinzo nodes.
- **Pay to acquire the data stream**: Shinzo nodes require authorized access to the sequencer's data feed. Obtaining this feed (and operating the node—compute, storage, bandwidth) carries a cost, which places economic value on OMATrust's data and funds the network's sustainability.
- **Simple developer experience**: builders point their apps at their own node (or a third-party Shinzo provider) and get verifiable, low-latency reads—without relying on proprietary gateways.

This model keeps light usage open, while ensuring that large-scale consumers participate economically instead of free-riding. The separate tokenomics paper quantifies the market for reads and where this revenue can flow.

5.4 Why It Matters

- **Developers** get reliable, verifiable data without building bespoke indexers.
- Ecosystem services can scale by running Shinzo nodes and serving high-volume workloads sustainably.
- **OMA3** turns reads—traditionally a cost center—into a self-funding capability that supports write subsidization and long-term token value.

6. Economic Model: OMA Token

OMAChain, as an Ethereum Layer 2, has a native token called OMA. OMA functions as the gas token for executing transactions on OMAChain and for operations involving OMATrust contracts. Write operations such as tokenizing applications, publishing attestations, or submitting reviews require OMA to cover gas fees. Some write operations, such as user reviews, are subsidized so that users can participate at no direct cost.

To address the “tragedy of the commons” challenge faced by industry consortia and open-source projects, OMA3 issues OMA grants to members who contribute infrastructure, standards, or operational support. This ensures that those who maintain shared resources are compensated, aligning incentives for long-term sustainability.

For detailed information on OMA token mechanics, unlock schedules, and governance, please refer to the separate tokenomics paper.

7. Governance: Credible Neutrality

OMA3’s governance is designed to be credibly neutral from day one. Its structure ensures that no single company, investor, or group of insiders can capture the protocol. This neutrality is what allows competitors to cooperate under OMA3’s umbrella and build shared infrastructure for the open internet.

7.1 OMA3 as a Swiss Association

OMA3 is incorporated as a Swiss association (Verein), a legal form that is inherently decentralized. Swiss associations operate much like US 501(c)(6) organizations, which are the backbone of the world’s largest industry consortia. These are the structures where fierce business rivals — “arch-enemies” in the market — come together to build shared standards that benefit everyone.

Crucially, **a Swiss association has no owners and no equity**. It exists purely to serve its members. There are no shareholders demanding returns, and no possibility of conflicts between equity holders and token holders. This makes the association uniquely suited to govern open, neutral infrastructure like OMATrust and OMAChain.

7.2 OMA3 Board and Working Groups

The OMA3 Board is the ultimate overseer of governance, responsible for ensuring the protocol remains aligned with its mission of neutrality and openness. But the real work happens in working groups, where members collaborate to design specifications, build standards, and run infrastructure.

OMA3 is **open to any organization** today, and soon to individual members as well. Whether at the board level or within working groups, **all members have equal opportunity** to participate and contribute. Governance is not gated by influence, wealth, or seniority — it is open and inclusive by design.

7.3 One Member, One Vote

OMA3 follows a **one member, one vote** principle. This avoids the pitfalls of token-based governance, where decision-making power is concentrated in the hands of wealthy tokenholders. Instead, every member — large or small — has an equal voice in shaping the protocol. This simple rule is one of the strongest guarantees of decentralization in practice.

7.4 How OMA3 Differs from Most Crypto Projects

OMA3's structure stands apart from nearly every other crypto governance model:

- There are **no backroom "unofficial" decisions** by insiders. Governance is transparent and formalized.
- There is **no foundation run by a handful of board members** whose incentives may not align with the ecosystem.
- There is **no for-profit entity raising equity from venture capital**. In most projects, equity holders extract value, creating conflicts of interest with tokenholders. In OMA3, equity is impossible — Swiss associations do not have shareholders or ownership at all.

In addition, OMA3 is not starting from zero. It solves the cold start problem by driving adoption through its membership that represents hundreds of Web3 projects.

7.5 Why This Matters for Credible Neutrality

By combining the Swiss association model with open membership, one-member-one-vote, and transparent governance, OMA3 ensures it is **not beholden to any single entity, investor, or group of insiders**.

This credible neutrality is the foundation of trust: it gives enterprises, developers, and even direct competitors the confidence to build on OMA3's infrastructure. Unlike walled gardens, OMA3 is a **public good governed in the open** — a model built for pervasive critical infrastructure like OMATrust.

8. Roadmap

OMA3 has a staged roadmap that balances rapid deployment with long-term goals. Each milestone expands adoption while reinforcing OMA3's mission to provide a neutral trust fabric for the open internet. OMA3 has already launched a development testnet for OMAChain with initial OMATrust contracts. Future milestones are as follows:

Early 2026: Mainnet Launch

OMAChain will launch the mainnet of its **Arbitrum Orbit Layer 2,** leveraging the security of Ethereum. At launch, OMA3 will deploy **Ethereum Attestation Service** smart contracts and **OMATrust schemas**.

This marks the beginning of OMA3's utility era: auditors can publish cryptographic attestations and users can submit gas-subsidized reviews. Importantly, it also marks the moment OMA becomes a **utility token under FINMA classification**, enabling public trading of OMA. Soon after OMA3 will launch the identity registry, deduplicator and attestation registry contracts.

Mid 2026: Cross-Chain Expansion & Developer Tooling

Once OMAChain is live, OMA3 will expand OMATrust to **other major blockchains** ensuring the trust layer is accessible wherever developers build. To accelerate adoption, OMA3 will release **developer tooling** that makes it simple to write attestations, read trust data, and integrate verifiable signals directly into applications and AI agents.

The goal is to remove friction: developers should be able to plug OMATrust into their workflows as easily as they integrate payment APIs or identity providers today.

Late 2026: Shinzo Integration

OMAChain will integrate **Shinzo**, a decentralized indexing protocol, to power **verifiable, decentralized data access** at scale. By embedding indexing into the sequencer and distributing it through Shinzo nodes, OMAChain ensures that registry and attestation data can be queried reliably without depending on centralized APIs.

This integration also enables OMA3's **read revenue model**: light usage is available through a free, rate-limited RPC endpoint, but high-volume consumers must run Shinzo nodes and pay to access sequencer data. This ensures reads are sustainable, turning what is normally a cost center into a funding stream for write subsidies and long-term token value.

Early 2027: Expansion Beyond OMATrust

With OMATrust established, OMA3 will introduce **additional protocols** that extend the OMATrust's utility. Examples include:

* **Inter World Portaling System (IWPS)** — integrated with OMATrust to enable trusted cross-world identity and access.
* **MMXPGs** — massively composable game primitives that rely on OMATrust for cross-game interoperability.
* **Autonomous Agent Access to Virtual Worlds** — creating a standardized way for AI agents to interact safely with virtual environments.
* **Spatial Store** — a decentralized marketplace layer built on top of the Identity Registry.
* **Onchain Governance for OMA3** — moving association governance processes onchain, while maintaining the credible neutrality of the Swiss association.

This stage expands OMA3 from a single protocol (OMATrust) into a **multi-protocol trust-based ecosystem**.

Late 2027: Decentralization of OMAChain

The final milestone on the current roadmap is the **decentralization of OMAChain** itself. Transitioning from a centralized sequencer to a decentralized validator set — in alignment with Arbitrum Orbit's roadmap — ensures long-term security, liveness, and neutrality. At the same time, Shinzo becomes the fully decentralized read layer, and licensing/subscription models

move onchain.

Governance evolves from association-led oversight to **protocol-enforced neutrality**, while OMA3's Swiss association continues to provide the legal and organizational backbone.

9. Disclaimer

This whitepaper is provided for informational purposes only and describes the technical vision and architecture of OMATrust and OMAChain. It does not constitute financial, legal, or investment advice, nor an offer to sell or solicitation to purchase any tokens or securities. OMA3 makes no representations or warranties as to the accuracy or completeness of this information, which is subject to change without notice.