

INFRASTRUCTURE PAPER – VERSION 1.0

ProofMatter

Proof of Execution Infrastructure

Turning real-world actions into verifiable digital evidence.

DOCUMENT

Infrastructure Paper
Version 1.0
12.08.2026

AUTHORS

Marten Jung
Stefan Schmidt

CONTACT

www.spo.de
www.unibright.io
www.proofmatter.com
info@spo.de

Table of Contents

01 Executive Summary

03 The Problem

The Illusion of Trust · The Blockchain Paradox · Problem Statement

05 Architecture & Trust Framework

Architectural Overview · Core Concepts · Proof Lifecycle · Trust Architecture · Workgroups · Validator Layer · Security & Integration

07 Use Cases & Templates

Key Use Cases · Use Case Matrix · Templates as the Engine of Reuse · Open Ecosystem

09 Roadmap 2026-2028

Foundation · Build & Testnet · Public Launch · Scaling & Governance · Scale & Decentralization

11 Market, Competition and Differentiation

The Gap in Existing Systems · Comparative Analysis · Hybrid Validation · Market Opportunity · Competitive Moat

13 From Unibright Framework to ProofMatter

An Eight-Year Evolution · Unibright Innovations · Overarching Insights

— References

02 Vision

Core Idea · Why Now · Design Principles · From Unibright to ProofMatter · A New Standard for Trust · An Open and Incentivized Protocol

04 The ProofMatter Solution

Proof-of-Execution · How It Works · The Role of UBT · Open and Modular · What Makes ProofMatter Different

06 UBT Token Economy & Incentive System

Bridgeless Credits · Roles and Alignment · Assurance-Driven Economy · Supply & Treasury · Token Distribution · The UBT Utility Cycle

08 AI Use Cases — The New Verification Frontier

Federated Learning · AI Agent Attestation · Content Provenance · The UBT Utility Cycle

10 Governance & Ecosystem

Transition Model · Decentralization Statement · Governance Mechanics · Contributor Incentives · Community Infrastructure

12 Legal Framework

No New Token · MiCA Alignment · Risks & Limitations · Disclaimer

— Glossary

DISCLAIMER

This document is provided for informational purposes only. It does not constitute an offer to sell, a solicitation of an offer to buy, or a recommendation of any securities, tokens, or other financial instruments. Nothing in this document should be construed as investment, legal, tax, or other professional advice. The ProofMatter protocol and related technologies are under active development. All technical specifications, token models, and governance mechanisms described herein are subject to change without prior notice. Readers are strongly encouraged to perform their own due diligence and consult with qualified professionals before making any financial or technical decisions. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission from SPO Consulting GmbH.

Executive Summary

Blockchains prove transactions. ProofMatter proves execution.

As digital systems increasingly automate real-world decisions, the ability to prove execution becomes a structural requirement - not an optional feature. Today's verification infrastructure, PDF certificates, manual audits, and unverifiable screenshots, cannot independently verify that an action actually happened. ProofMatter closes this gap with cryptographic proofs that are immutable, auditable, and machine-readable. The ProofMatter architecture turns real-world execution into verifiable digital evidence by capturing actions as structured proofs, enriching them with attestations, and making the resulting trust layer accessible across applications.

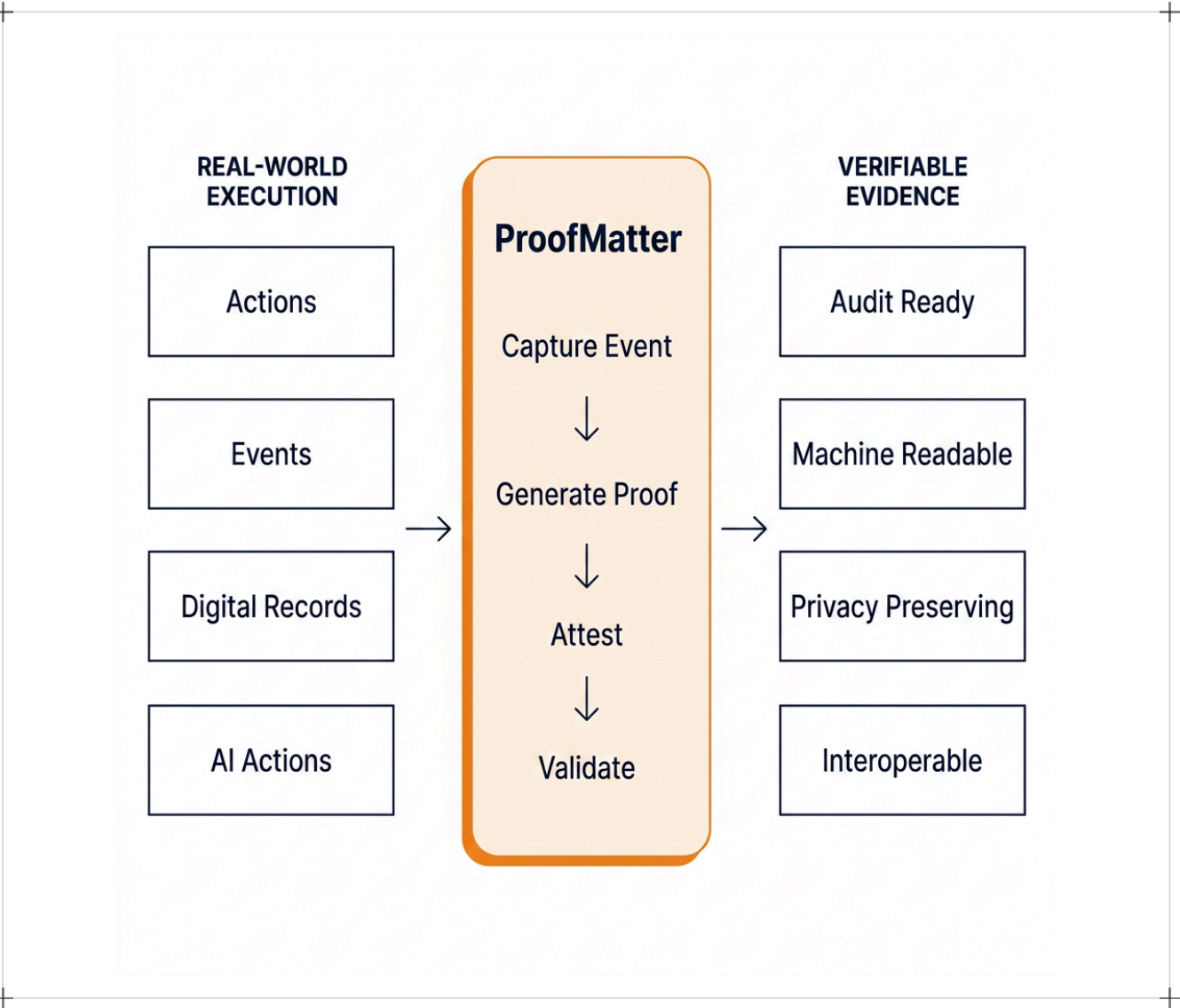


FIG. 01 – FROM REAL-WORLD EXECUTION TO VERIFIABLE EVIDENCE

The core primitive is simple: Party A records a proof. Party B confirms it. If they disagree, the process iterates until consensus is reached. The proof trail becomes a verifiable record of execution. Independent validators can add further attestations, raising trust levels from self-attestation (TL1) to publicly auditable verification (TLx).

Privacy is built in: ProofMatter's SyncTree technology enables selective disclosure at field level — a supplier can prove that emissions are below a regulatory threshold without revealing contract terms, pricing, or customer identity. Only the minimum data required to verify a claim ever leaves the holder's control.

This is not a theoretical problem; it is emerging across multiple trillion-dollar markets. The timing could not be more critical. Around the world, regulatory frameworks are tightening — from ESG disclosures to CO₂ reporting — while the digital economy expands at unprecedented speed. Trillions in assets and services move online, yet the mechanisms of verification remain rooted in a paper-based past. The global market for testing, inspection, and certification (TIC) already exceeds 250 billion USD, while governance, risk, and compliance (GRC) platforms are projected to surpass 120 billion USD by 2033. At the same time, three AI megatrends are creating an entirely new verification frontier. Federated Learning demands proof that distributed training participants behaved honestly. Autonomous AI agents acting on behalf of humans across industries require verifiable, accountable action trails. And AI-generated content flooding digital channels demands provable provenance. These markets exceed \$50 billion in addressable infrastructure spend by 2027. Across all these sectors - compliance, supply chains, AI infrastructure — enormous resources are spent to achieve trust, yet the underlying verification remains fragmented. In this landscape, the ability to prove not just transactions but actual execution and data integrity emerges as the missing layer - one that ProofMatter is designed to provide.

ProofMatter launches with digital rights management and AI content provenance — markets where the demand for verifiable proof is immediate and the regulatory pressure is acute. From this foundation, the same technical primitives extend to ESG and CO₂ reporting, green steel provenance, Digital Product Passports, supply chain traceability, certifications, federated learning verification, and AI agent attestation. Nine use cases, one architecture; only the proof templates differ.

At the core lies UBT, the Unibright Token, circulating since 2018 and broadly distributed. UBT is not a new or speculative launch but an established token that now gains renewed utility as the engine of the ProofMatter ecosystem. UBT grants access to proof creation, secures the network through validator staking, and incentivizes contributions such as templates, developer tools, or Explorer extensions. Proof creation is powered by UBT-based credits: UBT is deposited into the protocol, converted into credits, and these credits are consumed as proofs are generated — with a portion permanently removed from circulation. This establishes a direct utility link between adoption and token usage, while avoiding inflationary token models.

The result is an incentivized and balanced ecosystem. Proof creators bring real-world actions into the network. Validators stake UBT and are selected to verify proofs against predefined templates — checking hashes, timestamps, signatures, and anchoring — and, where required, performing

off-chain spot checks that produce signed attestations referenced to the proof ID. Honest validators earn rewards; dishonest behavior may lead to penalties on staked UBT. In the early phase, validator roles may be fulfilled by a small set of professional entities, with a planned transition to an open validator network over time. Developers expand the system by offering templates, building tools, and enabling new use cases. As more actions are proven, more credits are used, reinforcing adoption of the protocol. This dynamic fosters a sustainable loop: usage demonstrates utility, utility builds trust, and trust enables broader adoption.

ProofMatter is not another blockchain. It is not another speculative token. It is the missing Proof-of-Execution layer for a digital economy built on verifiable foundations — from ESG compliance to AI accountability, from supply chains to digital licensing.

ProofMatter transforms trust from a promise into a proof.

Vision

Core Idea

ProofMatter is built on a simple but powerful principle: **"Don't promise. Prove."**

In today's digital economy, most compliance systems rely on unverifiable PDFs, screenshots, or emails. The result? Fake ESG scores, broken audit trails, and loss of trust. Even in Web3, execution is often off-chain and unverifiable.

ProofMatter changes that. It introduces a verifiable execution layer where actions speak for themselves. Every completed process — from delivering a file to signing a document — leaves a cryptographic footprint: a proof trail. These traces are transparent, immutable, and independently auditable.

The vision is clear: trust should not depend on claims or intermediaries, but on verifiable evidence.

WHAT PROOFMATTER IS

- **An open protocol** — a minimal, composable set of primitives for proof generation, validation, and anchoring
- **A trust layer** — the missing execution-proof layer between real-world events and on-chain records
- **A selective disclosure engine** — proves any single field without revealing the rest (SyncTree)
- **A verification infrastructure** — built for enterprises, AI systems, and regulated industries
- **A utility engine for UBT** — renewed, concrete utility for the Unibright Token (circulating since 2018)

WHAT PROOFMATTER IS NOT

- **NOT a new token** — UBT has existed since 2018; ProofMatter provides renewed utility, not a new launch
- **NOT building AI** — ProofMatter verifies the AI of others; it does not train models or generate content
- **NOT a database** — ProofMatter anchors root hashes; data sovereignty stays with the data owner
- **NOT a blockchain** — ProofMatter runs on Ethereum L1 and Optimism L2; it does not operate its own chain
- **NOT a certification body** — validators are independent economic actors, not an accreditation authority

Why Now

The timing for such a layer has never been more urgent. Regulators worldwide are mandating detailed ESG disclosures and supply chain transparency. AI-generated content floods digital channels, making it harder than ever to distinguish truth from fabrication. Companies spend billions on audits and certifications, yet the results are still based on documents and claims rather than direct proofs of execution. Against this backdrop, the demand for a minimal, verifiable substrate is rising — and ProofMatter provides it.

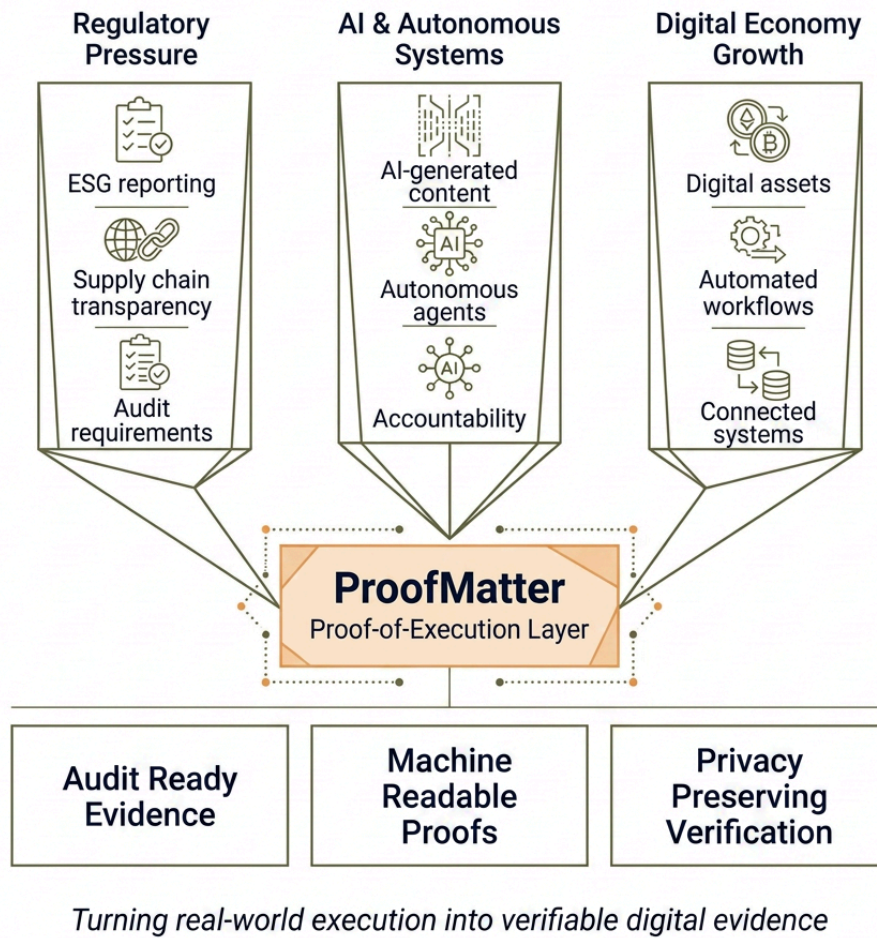


FIG. 02 – THREE CONVERGING TRENDS: REGULATION, AI, AND DIGITAL ECONOMY GROWTH

Design Principles

ProofMatter is following some core design principles, which are laid out in more detail in the following chapters:

- **Structured by default:** proofs follow standardized, machine-readable templates.
- **Verification first:** every proof is designed to be independently checked.
- **Hybrid validation:** optional spot-check policies (random N%, risk-weighted, SLA-triggered) executed by accredited validator classes (enterprise, auditor, community) yield signed attestations, "TrustMesh"
- **Selective disclosure:** Merkle/field-level proofs; ZK-ready, "Sync Tree"
- **Economic integrity:** UBT staking/fees deter spam and align incentives.

From Unibright to ProofMatter

ProofMatter is not a speculative concept. It is the focused result of years of building blockchain-based business infrastructure. In 2018, the Unibright Framework pioneered the use of smart templates, visual workflows, and code generation to bridge real-world processes with blockchain logic. The technology worked — but the enterprise world moved slower than innovation. The same behaviour was observable with the Unibright powered tokenization framework Freequity, the private/council-governed Network Baseledger and the Notarization Platform Unibright One.

This lesson shaped a sharper insight: instead of trying to transform entire business systems, we should focus on a universal, cross-industry need — the ability to prove that something actually happened — and include that in a framework that can integrate with every existing Enterprise Resource Planning system.

ProofMatter is that focus.

It refines the Unibright heritage into a minimal, reusable, and open infrastructure: the Proof-of-Execution layer. It doesn't aim to replace entire ERP systems or platforms but to seamlessly integrate into all these existing and established solutions. In order to capture what matters most: verifiable action which directly adds to the value of successful business integration.

A New Standard for Trust

ProofMatter aspires to become the global standard for digital proofs of execution. Whether in ESG reporting, supply chains, IP licensing, or certification, the logic remains the same:

If it was done — prove it. If it can't be proven — it's noise.

Instead of relying on a PDF that claims a company reduced 100 tons of CO₂, a ProofMatter proof shows exactly when and how the reduction was verified.

This standard rests on three building blocks: Templates that define what a valid proof looks like; Validators who verify execution and stake for integrity; and transparency tools like the ProofMatter Explorer that make proofs visible and auditable.

Together, they transform execution into truth — and remove the need for trust.

An Open and Incentivized Protocol

ProofMatter is not just a tool, but an open protocol. Anyone can contribute templates, build proof generators, or run explorer instances. Incentives ensure that this openness is sustainable: contributors are rewarded through UBT for adding value, whether by designing templates, verifying proofs, or extending the ecosystem. ProofMatter is built to be extended, forked, audited — and proven. This creates a self-reinforcing network effect in which adoption, proof generation, validation, and trust continuously strengthen each other.

The Problem

The Illusion of Trust in a Digital World

Today's digital economy depends on trust — yet the mechanisms used to establish it are broken. Enterprises and institutions still rely on audits, certificates, and static PDF reports to prove compliance or execution. These artifacts are expensive to produce, impossible to verify independently, and often easy to forge or misrepresent. They persist not because they are effective, but because no better alternative has been widely adopted.

The consequences of this illusion are visible across industries:

In ESG and compliance, companies publish glowing sustainability reports, but stakeholders cannot verify whether emissions were truly reduced or whether numbers were massaged for marketing purposes. A 2020 study by Dimson et al. found that ESG scores from different providers often diverge sharply — with the same company receiving both high and low ratings depending on the agency. This inconsistency undermines trust and comparability.

In supply chains, traceability often ends where documentation stops. From fashion to semiconductors, counterfeit and opaque sourcing practices cost global markets billions annually. A label may claim "sustainably sourced cotton," but without verifiable proof, the claim is little more than a story.

In the realm of digital assets and intellectual property, creative works are minted, sold, and claimed — yet proving how, when, and by whom they were used remains elusive. Copyright infringement, double-use, and disputes over ownership are rampant, especially in the age of generative AI and NFTs.

Even certifications and audits, which are supposed to safeguard critical sectors like food, pharma, or safety, are typically delivered as static files — snapshots in time whose trustworthiness depends entirely on the issuing entity. When such certificates are falsified, the consequences can be catastrophic.

The Blockchain Paradox: A Trust Gap

Blockchains were supposed to fix trust — and to some extent, they did. The Use Case of Cryptocurrencies successfully proves this: when the entire process, the asset, and the execution all reside on the chain itself, the technology provides verifiable, trustworthy, and immutable records.

What blockchains prove is that a transaction occurred under defined rules within the chain's confines. What they do not prove, however, is the connection to the physical or "real" world: that a shipment was actually delivered, that a machine was serviced, that a contract clause was executed, or that a process truly happened outside the digital ledger.

The following illustration summarizes this gap: blockchains provide reliable records of digital transactions, while ProofMatter extends verification into real-world execution.

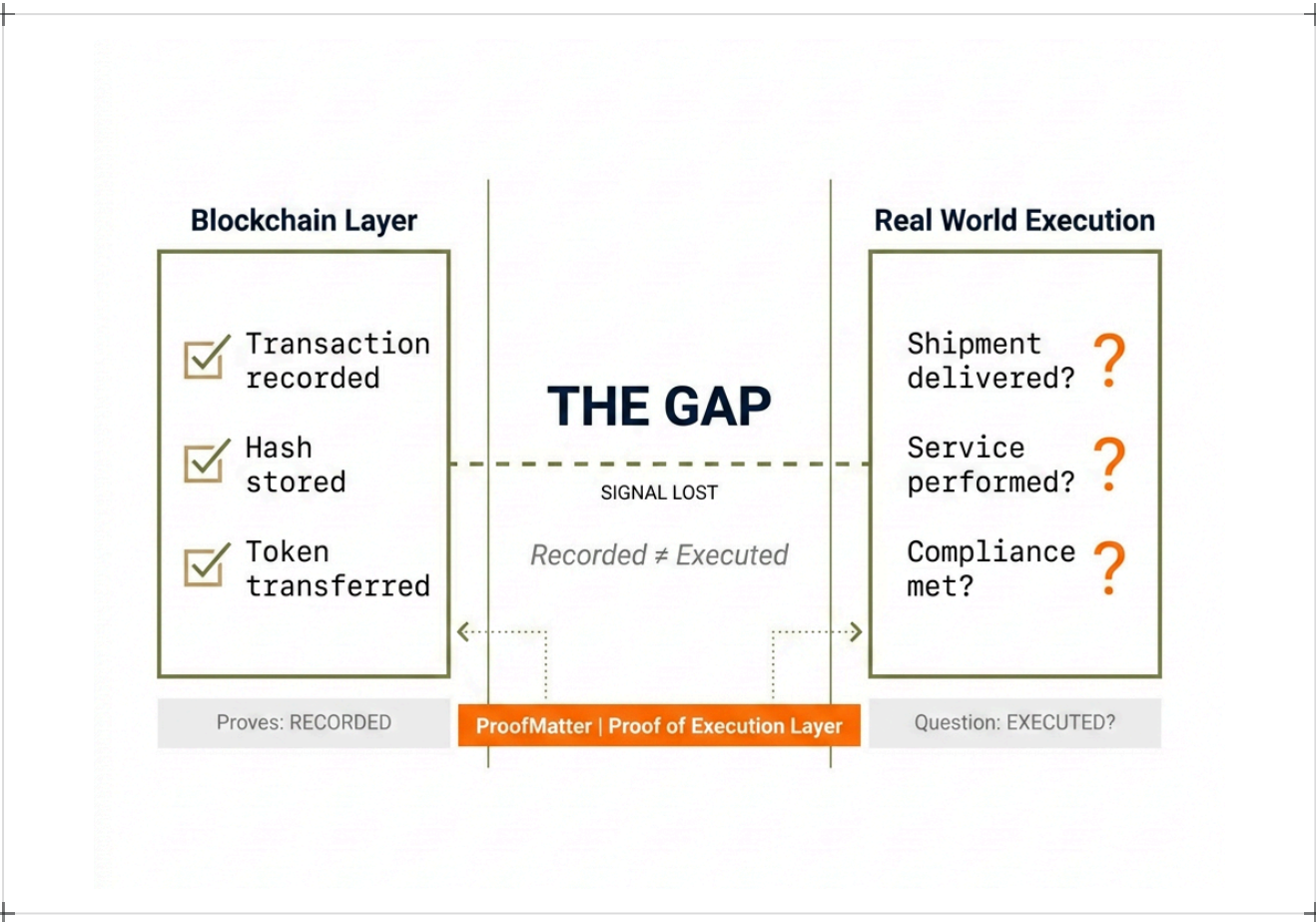


FIG. 03 – THE GAP: BLOCKCHAINS PROVE RECORDING – NOT REAL-WORLD EXECUTION

Even in Web3, execution often remains off-chain, unverifiable, or manipulable. Real-world actions become assumed rather than proven. This creates a fundamental gap: a space between what is claimed—and what is real.

This gap reveals that, for real-world integration, trust, verifiable through a robust Proof of Execution, should be the true currency, not the mere recording of digital transactions.

In a world of accelerating digital interaction, stricter regulation, and the tokenization of everything, this gap is not just inconvenient — it is dangerous: Fraud becomes cheaper than compliance. ESG becomes marketing and speculation. Supply chains become unverifiable black boxes. Certification becomes theatre. Web3 turns into "WebMaybe". Without Proof of Execution Web3 cannot operate in the mainstream. When execution cannot be proven, audits become performative, trust becomes fragile, and efficiency remains an illusion.

Problem Statement

The digital economy lacks a universal, trustless way to prove that claimed actions have actually been executed. As a result, trust collapses into reputation — and reputation can be bought. This is the gap ProofMatter is designed to close.

The ProofMatter Solution

Introducing Proof-of-Execution

ProofMatter delivers the missing trust layer for the digital economy: **Proof-of-Execution**.

Existing Blockchain systems can prove that a transaction was recorded, but they cannot prove that an action actually took place. ProofMatter extends beyond simple transaction logging by embedding evidence of execution—including its validation history—into a transparent, evolving data structure.

It does not merely store what was said or intended, but demonstrates what was done, how it was approved, and whether it was confirmed, revised, or rejected during its lifecycle.

Whether it is a license being activated, a file being delivered, or a sustainability metric being fulfilled, ProofMatter creates a tamper-proof record of what was executed, not just what was declared. In doing so, it allows trust to become a measurable, living value rather than a static assumption.

How It Works, at a glance

The ProofMatter process follows a simple but powerful flow.

An event occurs — a shipment is dispatched, a contract milestone is reached, or a digital asset is used. This event is captured by a Proof Service, a local or hosted module that generates a standardized and signed proof object. Such a proof contains essential attributes: the type of action, a timestamp, the actor, a hashed payload (partially revealable as a sparse Merkle tree, the Sync Tree), and a digital signature.

The proof is then committed on-chain via a lightweight and upgradable Proof Contract, ensuring transparency and immutability.

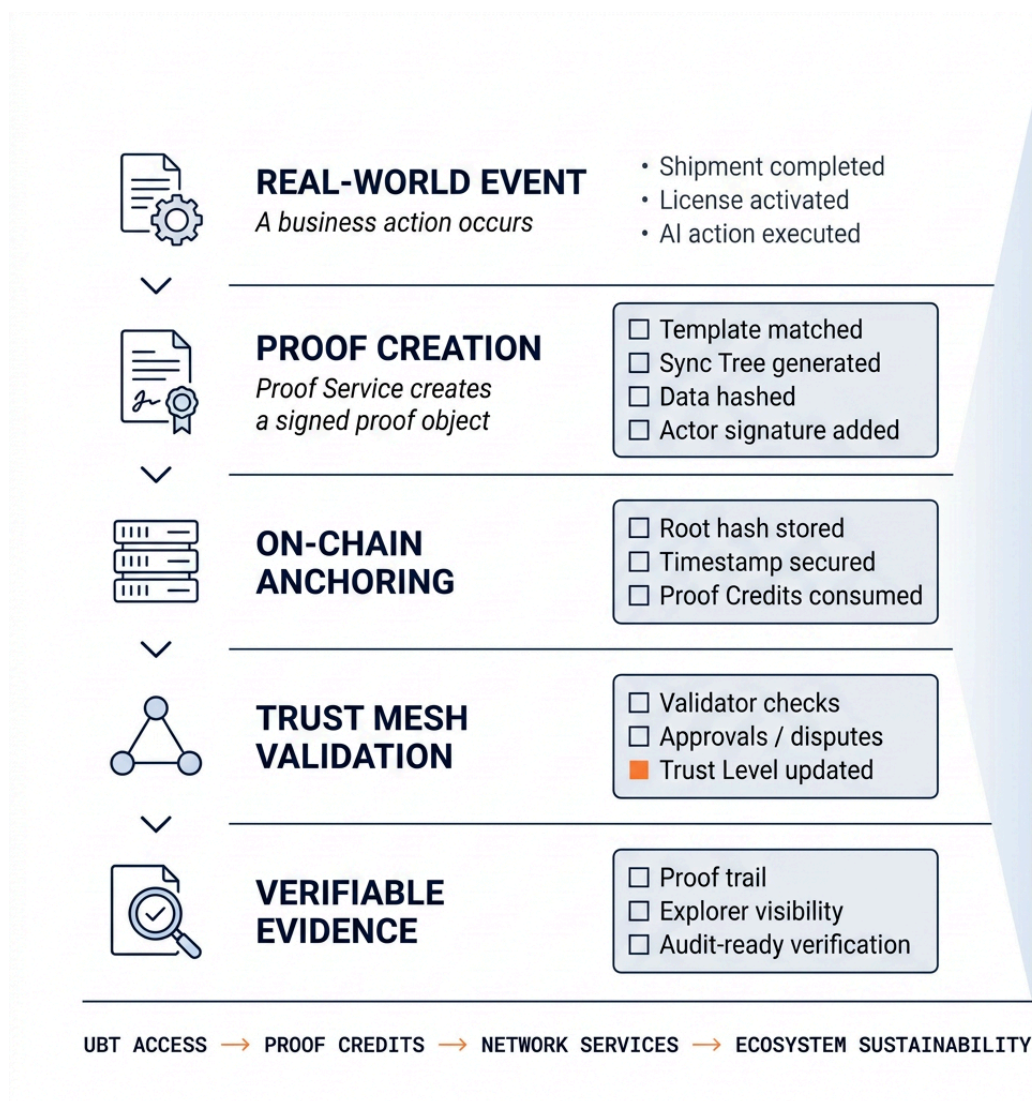


FIG. 04 – THE COMPLETE LIFECYCLE FROM REAL-WORLD ACTION TO VERIFIABLE EVIDENCE

From there, the ProofMatter Explorer makes all proofs visible: the number and type of proofs submitted, the active templates in use, the validators who secured them, and the corresponding UBT activity — including burns, deposits, and treasury flows.

Different versions and approvals in multi-party scenarios are also recorded in a dedicated data structure, the Trust Mesh: Each approval, rejection, or re-versioning generates a signed attestation linked to the original proof ID.

Crucially, Proof of Execution in ProofMatter is not a one-time event. Completed proofs remain subject to post-event validation: accredited auditors or validators may perform random or risk-weighted spot-checks on already executed processes. Their signed attestations are appended to the same proof chain, thereby changing its cumulative trust level in real time. Positive confirmations strengthen the proof's assurance score and may reduce future credit costs; negative or missing validations weaken it and increase cost or required sampling.

The complete lifecycle from real-world action to verifiable evidence is shown above. Over time, all these attestations form a verification graph in which the edges of successful confirmations compose the proof trail itself — the verified path of execution within the Trust Mesh.

This means that a user can reconstruct not only the existence of a transaction, but the entire lifecycle of its acceptance, amendment, or dispute, all without exposing sensitive business data. The result is a verifiable trail of actions — machine-readable, audit-ready, and continuously updatable — where trust is no longer fixed at the moment of recording but evolves with evidence.

The Role of UBT in the Solution

Every proof in ProofMatter is underpinned by the Unibright Token (UBT).

- Proof creators prepay UBT on Ethereum and receive usage credits on a Layer-2 network (currently Optimism), which are consumed whenever proofs are generated.
- Validators must lock UBT to participate and earn a share of fees for securing integrity.
- Template and tool developers can be rewarded with a portion of proof fees when their contributions are used.

Each proof therefore consumes UBT through the credit system, with the underlying value distributed according to transparent parameters: a portion is burned, a portion flows to validators, and a portion supports the ecosystem treasury.

When UBT is deposited into the protocol, the following distribution is designed to be applied automatically by the L1 smart contract:

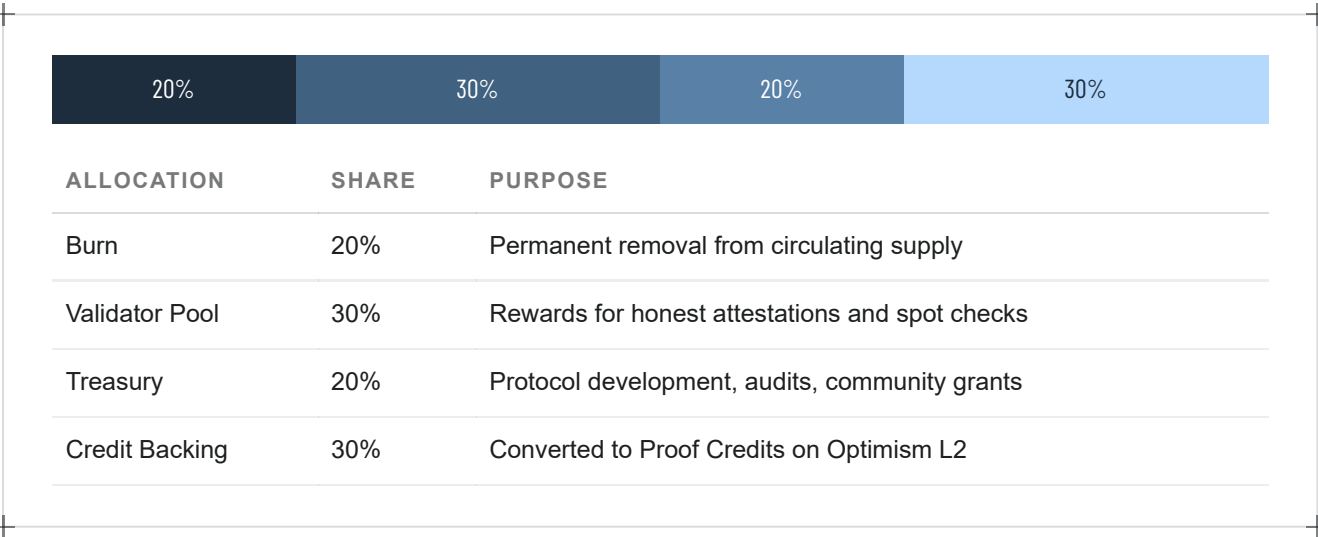


FIG. 05 – AUTOMATIC UBT DEPOSIT DISTRIBUTION AT THE L1 CONTRACT

These parameters are fixed at launch and governance-adjustable within defined bands. The distribution occurs at deposit time — before credits are issued — ensuring that every UBT entering the protocol immediately contributes to burns, validator incentives, and treasury funding. No manual intervention, no off-chain custody, no discretionary allocation. The contract enforces the split; the Explorer surfaces it in real time.

Because external audits and validator attestations can retroactively alter a proof's trust score, they also influence how many credits subsequent proofs of the same type will consume — linking economic weight directly to proven reliability.

This ensures that UBT utility reflects both activity and assurance, while all flows remain visible in the Explorer. (For details on token mechanics, see [Chapter 6](#).)

Open and Modular by Design

ProofMatter is not a closed product, but an open protocol.

Anyone can design templates or integrations — but for proofs to be recognized as ProofMatter-verified, they must follow the protocol's standards. This includes predefined template rules, validator participation, and the use of UBT credits as the underlying economic mechanism.

Because attestations, versioning, and spot-check results all conform to the same structural logic, the system can evolve without fragmentation: every new template, every audit layer, every integration feeds the same verifiable chain of execution.

The protocol is minimal enough for any developer, flexible enough for any industry, and robust enough to secure real-world trust.

What Makes ProofMatter Different

Unlike static PDFs, centralized audit systems, or manually notarized processes, ProofMatter creates tamper-proof, cryptographic execution records that are machine-readable and open to all.

Unlike oracles, which only bring external data on-chain, ProofMatter verifies that the action itself was executed and validated — even after the fact.

Unlike generic gas-based tokens, where value is tied to computation or network congestion, UBT links economic activity directly to verifiable and audited execution.

ProofMatter therefore transforms execution into evidence that can grow in credibility over time — closing the trust gap between promise and reality.

[A claim on-chain is data; a proof trail is verified proof of execution.](#)

ProofMatter Architecture & Trust Framework

ProofMatter combines on-chain transparency with off-chain flexibility to form a coherent architecture for verifiable execution. It captures real-world actions as cryptographically provable artifacts, enables selective disclosure of sensitive fields, and augments those artifacts with optional, independent attestations. In contrast to systems that merely record hashes or store files, ProofMatter records execution itself and makes that execution auditable end-to-end. The result is a minimal but complete substrate: templates define what must be proven, services create proofs from events, contracts anchor those proofs immutably, a validator layer can elevate assurance through hybrid checks, and the Explorer renders the full trust surface visible.

Architectural Overview

The architecture centers on four building blocks that operate as a pipeline.

Proof Templates express, in a standardized, machine-readable form, what a valid action looks like: required fields, signatures, optional attachments, and disclosure rules.

Examples include:

- a delivery confirmation with timestamp, GPS, and actor signature,
- the issuance of a certificate with issuer, hash of the document, and signature,
- or the usage of a license with asset ID, context, and digital signature.

Proof Services turn actual events into signed proofs that conform to those templates; they timestamp, hash, and submit the minimal on-chain payload while optionally pinning large artifacts to decentralized storage.

Proof Contracts on Optimism validate structure and signatures, anchor the proof, and emit events that indexers and the Explorer can consume.

Finally, the **Explorer** provides a public lens into proof activity, template usage, validator participation, and UBT flows, including burns, validator rewards, and treasury allocations. This is the same logical flow already sketched in the Executive Summary; here it is presented as the single canonical reference.

In the initial phase, only a small set of Proof Contracts is authorized to consume credits. Governance expands this whitelist over time, maintaining integrity while opening the protocol to broader participation. The Explorer complements this with transparency on which contracts are active, what templates they accept, and how credits and UBT are accounted for at each step.

The following architecture overview illustrates how these components form a layered trust stack, separating execution verification from blockchain anchoring and protocol resource management.

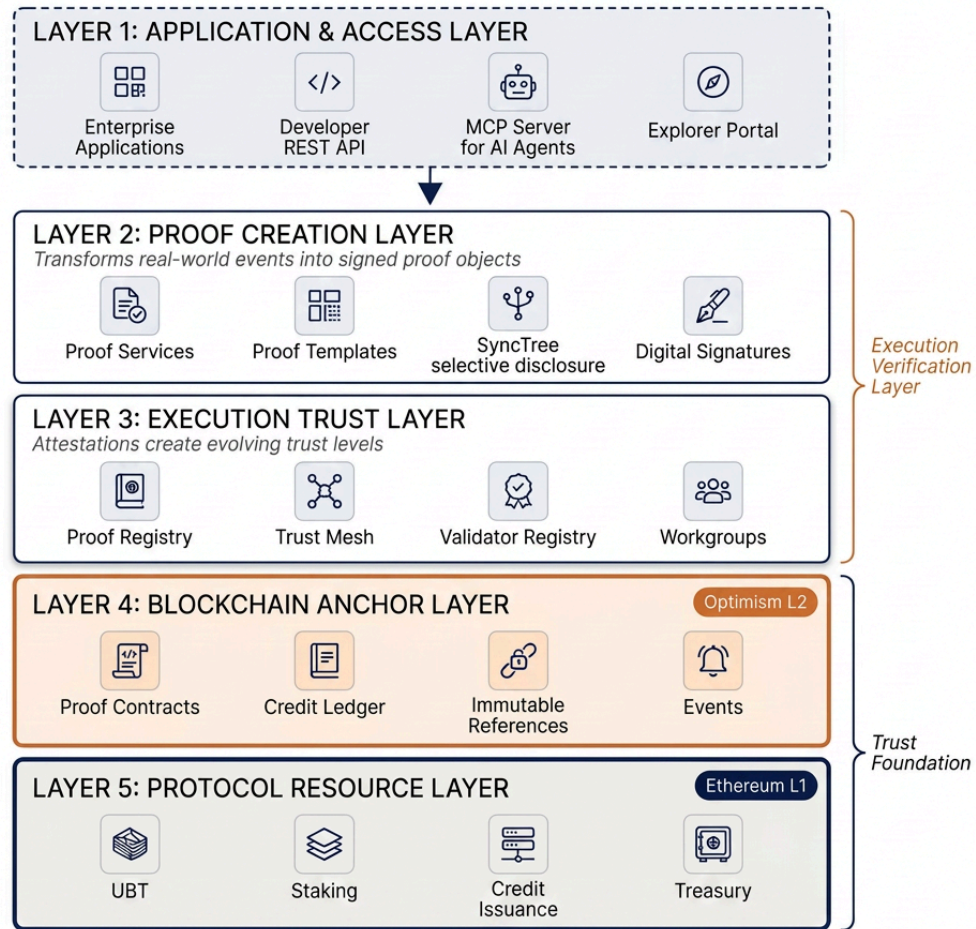


FIG. 06 – THE LAYERED TRUST STACK: EXECUTION VERIFICATION, ANCHORING, AND RESOURCE MANAGEMENT

Core Concepts

- A **proof** is a cryptographically signed representation of an executed action, anchored by a Proof Contract.
- An **attestation** is a signed, timestamped statement that references a proof ID and declares a validation outcome under a known policy.
- **Proof credits** are the metering unit on Optimism, deterministically issued from UBT deposits on Ethereum; each proof consumes credits, directly binding adoption to token utility.
- **Selective disclosure** is provided by Merkle-based techniques, extended through a masked structure (SyncTree) that preserves privacy while enabling field-level verification.
- **Trust levels (TL1–TLx)** quantify assurance depth: from self-commitment (L1) to multi-validator and regulatory confirmations (L4/Lx).
- **TrustMesh** denotes the verification graph formed by proofs (nodes) and attestations (edges).

Proof Lifecycle

A proof begins off-chain with an event: a shipment is dispatched, a license is activated, a compliance control is completed.

The relevant data are placed into a template, signed by the actor, and hashed by the Proof Service. The on-chain submission includes only essential metadata and the resulting digest; larger artifacts may be referenced via content-addressed storage. The Proof Contract validates the structure and signatures, records the proof type and references, and emits an event. From there, the Explorer surfaces the proof alongside its template, timing, and credit consumption. If validation is required, independent actors can perform checks and issue signed attestations that reference the original proof ID, increasing its trust level.

Trust Architecture: Verification Graphs, Selective Disclosure and Trust Levels

ProofMatter does not treat proofs as isolated entries. Through the TrustMesh, each proof becomes a node within a verification graph, linked by attestations from counterparties, auditors, or regulators. These edges are cryptographically signed and timestamped, and may be stored on-chain or off-chain so long as they are anchored by signed commitments (e.g., Merkle roots) that reference the proof ID. This design allows deterministic reconstruction of the graph at any time and introduces a measurable notion of assurance depth that can be inspected in the Explorer.

Because many proofs contain sensitive information, ProofMatter employs SyncTree for field-level disclosure. Each field is hashed with its own salt and arranged into a Merkle structure; auditors or regulators can verify inclusion of selected fields without learning the rest. This resolves the enterprise dilemma of proving enough to satisfy regulators while not exposing proprietary details, and it aligns with privacy requirements common in ESG and supply-chain reporting. The same approach positions ProofMatter for future zero-knowledge integrations, without adding unnecessary complexity in the initial release.

The following model illustrates how SyncTree separates cryptographic verification from data visibility: all fields contribute to the same immutable proof commitment, while different participants receive access only to the information required for their role.

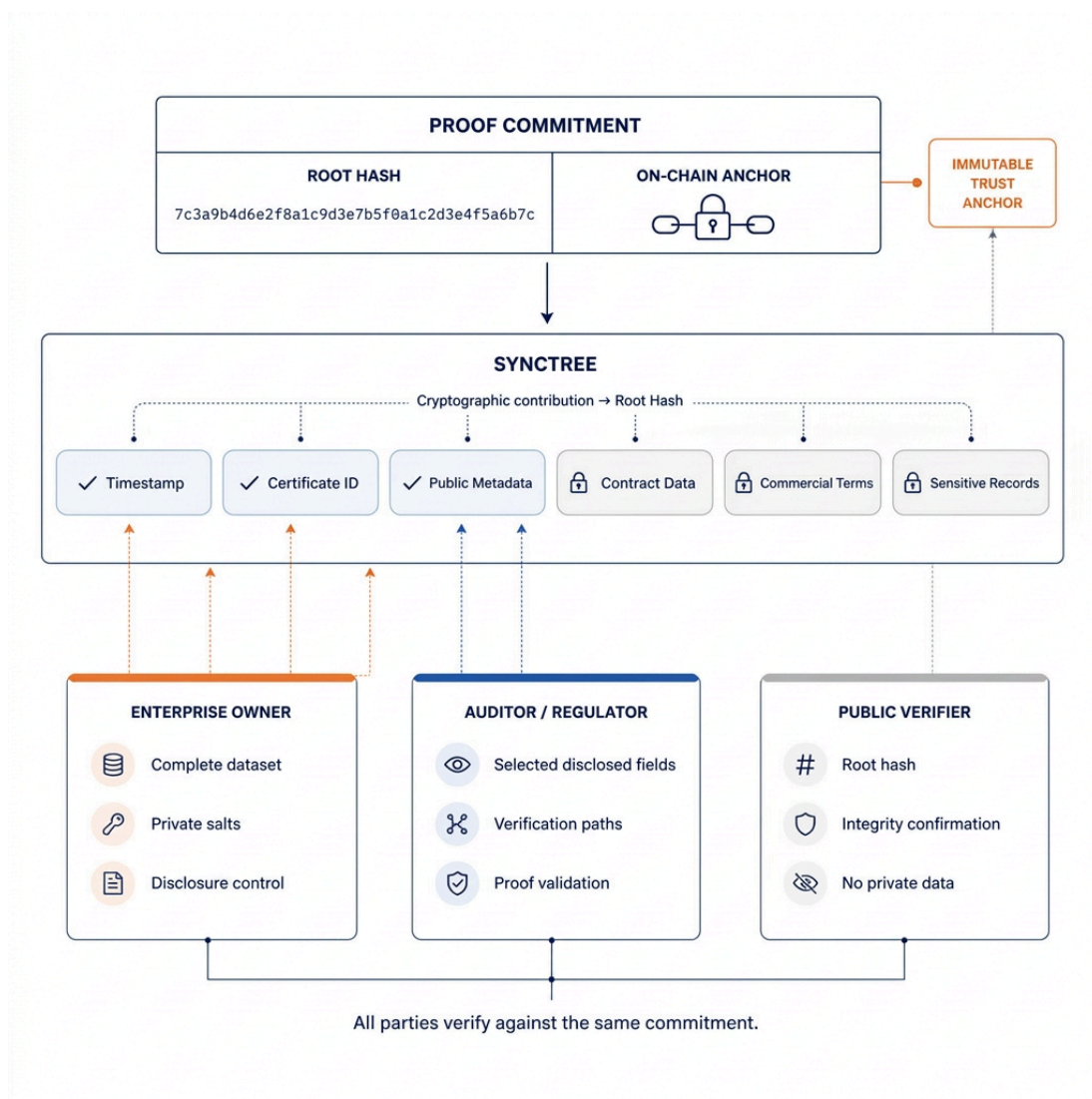


FIG. 07 – SYNCTREE: FIELD-LEVEL SELECTIVE DISCLOSURE OVER ONE IMMUTABLE COMMITMENT

ProofMatter supports both public and private proofs, providing flexibility across open ecosystems and confidential enterprise workflows. In both cases, the cryptographic foundation is identical — every proof contains a signed hash of the underlying data — but the degree of disclosure differs.

A **public proof** stores both the hash and a reference to its payload (for example, an IPFS CID or URL) directly on-chain. Such proofs are openly retrievable through the Explorer and are ideal for transparent use-cases such as ESG disclosures, open certifications, or NFTs. Public proofs maximize transparency and shareability, allowing anyone to verify content integrity without relying on the original issuer.

A **private proof**, by contrast, commits only the hash on-chain while keeping the full payload under the holder's control. Verification then depends on selective disclosure: the holder can reveal the underlying data or specific fields through Merkle or SyncTree paths when required by auditors, regulators, or partners. This mode is suited to licensing, trade documentation, and compliance processes where privacy, contractual obligations, or export-control rules apply.

Both types are structurally compatible and can coexist within the same templates and contracts. Enterprises can thus mix public transparency with confidential proofs in a single process chain — exposing what is necessary while preserving what is sensitive. Regardless of disclosure level, every proof remains verifiable and every attestation traceable, ensuring that privacy never compromises integrity.

ProofMatter expresses assurance depth via trust levels TL_n.

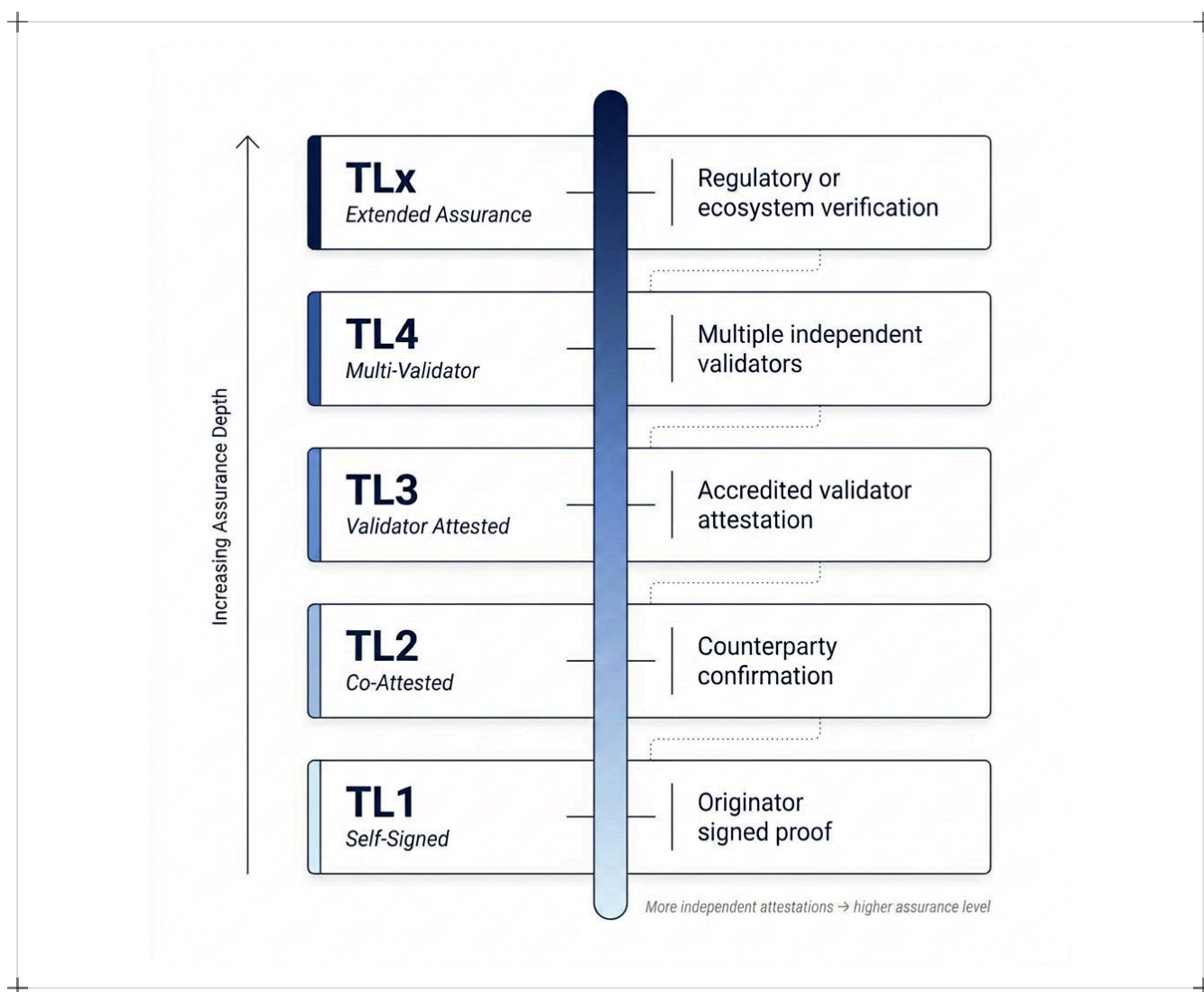


FIG. 08 – TRUST LEVELS: ASSURANCE DEPTH GROWS WITH INDEPENDENT CONFIRMATION

- **TL1** denotes a self-signed proof by the originator.
- **TL2** adds a counterparty co-signature.
- **TL3** includes an accredited validator attestation.
- **TL4** aggregates multiple independent validators;
- **TL_x** captures extended confirmations such as regulator endorsements or community-based verification. Each level increases evidential weight and may require additional credits, reflecting the economic cost of higher assurance.

ProofMatter's innovation extends beyond isolated proofs. Each proof becomes a node in a larger verification graph, connected through attestations issued by validators, counterparties, or regulators. These signed edges transform linear records into relational evidence: not only that something happened, but that it was witnessed and confirmed by multiple independent actors.

Each completed check produces a signed attestation — a compact record containing the hash, signature, timestamp, and applied validation policy — that is cryptographically linked to the original proof ID.

Multiple attestations collectively form a verification graph, the TrustMesh, whose edges trace the confirmations of an executed process. The subset of edges that connect all successful steps in sequence constitute the proof trail itself: a continuous chain of proven execution.

As this verification graph evolves, each additional independent attestation can increase the assurance level of a proof. ProofMatter represents this progression through Trust Levels, providing a transparent measure of verification depth.

This relationship between the TrustMesh and the proof trail defines the protocol's essence. The TrustMesh captures the universe of all possible attestations; the proof trail emerges as its verified backbone — the demonstrable path of what has actually been done – turning execution into a measurable and reviewable artifact of trust.

Workgroups – Defining the Circle of Trust

Every verification network requires clarity about who is entitled to participate. In ProofMatter, this boundary is defined through Workgroups — discrete sets of actors authorized to create, receive, and attest to proofs within a shared TrustMesh.

A Workgroup functions as the operational perimeter of trust: it determines which entities may issue proofs, which may validate them, and which may view or disclose related metadata.

A Workgroup can represent a consortium of companies, a regulated supply-chain cluster, or an internal enterprise domain. Membership is defined through registered participant identities — cryptographic addresses or credential hashes — recorded in the Proof Template or Workgroup Registry. Only members of that group can submit attestations that become part of the verification graph; attempts from outside addresses are rejected at the contract level. This ensures that every edge in the TrustMesh originates from a verified participant.

For privacy-sensitive environments, Workgroups operate in a selective disclosure mode: Proof data are structured through SyncTree so that each field is salted and hashed; participants reveal only the branches relevant to their role or authority. In this configuration each participant holds a unique path into the Merkle structure, guaranteeing that even within the group, access remains granular while external parties see only aggregated commitments.

Workgroups therefore provide the missing link between technical verification and organizational trust. They make it possible to prove that all recorded actions were executed by legitimate members of an agreed circle, without revealing unnecessary business details to the outside world.

Across industries, from ESG collaborations to digital-asset licensing networks, Workgroups allow ProofMatter to balance openness with operational confidentiality — ensuring that verifiable execution remains both inclusive and controlled.

Validator Layer, Hybrid Policies and Feedback Loops

The validator layer exists to connect digital assertions to real-world execution. ProofMatter supports enterprise validators for internal compliance, accredited auditors as independent third parties, and community validators for controlled open participation.

Policies define how checks are selected: random sampling, risk weighting, or SLA-triggered conditions. Each completed check yields a signed attestation that references the proof ID and the applied policy.

Validators are economically bonded through UBT staking; honest behavior is rewarded, while false or negligent attestations may lead to partial or full forfeiture. Beyond individual penalties, aggregated validation outcomes directly influence the assurance score of related templates and contracts.

If repeated spot-checks reveal inconsistencies or negative attestations, the corresponding proof types gradually become more expensive to issue, consuming additional UBT-backed credits and potentially requiring higher trust levels for acceptance. Conversely, consistently reliable validations lower cost and sustain confidence.

Through this feedback loop, validator diligence shapes not only individual rewards but also the overall economics of future proofs — translating integrity into tangible, measurable value. Together, Workgroups, Validators, TrustMesh, and SyncTree transform ProofMatter from a passive record of events into an adaptive trust system — where verification, access, and assurance continuously evolve with real-world evidence.

Security, Openness, and Integration

Security is enforced through signature verification on proofs and attestations, template validation to reject malformed submissions, and credit-based gating to ensure that each action bears economic weight.

Sybil resistance for validators is achieved by staking and identity constraints; public endpoints are protected by throttling.

Core libraries and contracts are open-source under permissive licenses; the Explorer is forkable and can be self-hosted; templates are submitted via transparent governance.

This combination removes vendor lock-in while preserving a coherent standard for proofs of execution.

Summary: The Integrated View

ProofMatter brings data, execution, and trust together within one coherent and verifiable framework.

At its foundation, templates define what a valid proof must contain — the structure, the required signatures, and the permissible disclosure rules. Proof services translate real events into those proofs, signing and hashing them so that each action becomes cryptographically unique. Proof contracts then anchor these records on-chain, ensuring immutability and global accessibility without exposing sensitive details. Where confidentiality is required, SyncTree allows selective disclosure, revealing only the information needed for compliance or audit.

Above this foundation, the TrustMesh links proofs and attestations into a dynamic verification graph, while validators bridge digital claims with real-world execution. Their checks, confirmations, and occasional rejections shape the evolving assurance level of every process — and through economic feedback, even the cost of future proofs.

The Explorer renders this entire ecosystem transparent, surfacing proofs, attestations, validator performance, and UBT activity in real time.

Finally, UBT itself ties everything together: it governs access, fuels validation, distributes rewards, and transforms integrity into measurable economic value.

With these layers working in concert, ProofMatter becomes far more than a recording tool — it is the missing proof of execution layer of the digital economy: a system where every action can be proven, every proof can evolve, and trust is no longer claimed but continuously verified.

UBT Token Economy and Incentive System

ProofMatter introduces no new asset. Instead, it employs the Unibright Token (UBT), circulating since 2018 with a fixed supply of 150 million, as the sole access and incentive layer. The token's role is not speculative; it is operational. Credits for proofs are deterministically minted on Optimism from UBT deposits on Ethereum, Validators post UBT to participate in verification, and contributors are rewarded in proportion to verifiable value added. This continuity avoids dilution and aligns the protocol with a transparent, MiCA-aligned utility model. Each proof consumes credits backed by UBT deposits. A portion of each allocation may be routed to protocol-defined burn mechanisms, while the remaining resources support validation, infrastructure, and ecosystem development.

The following model illustrates how UBT functions as an operational resource layer within ProofMatter, converting protocol access into proof execution capacity, validation incentives, and ecosystem resources.

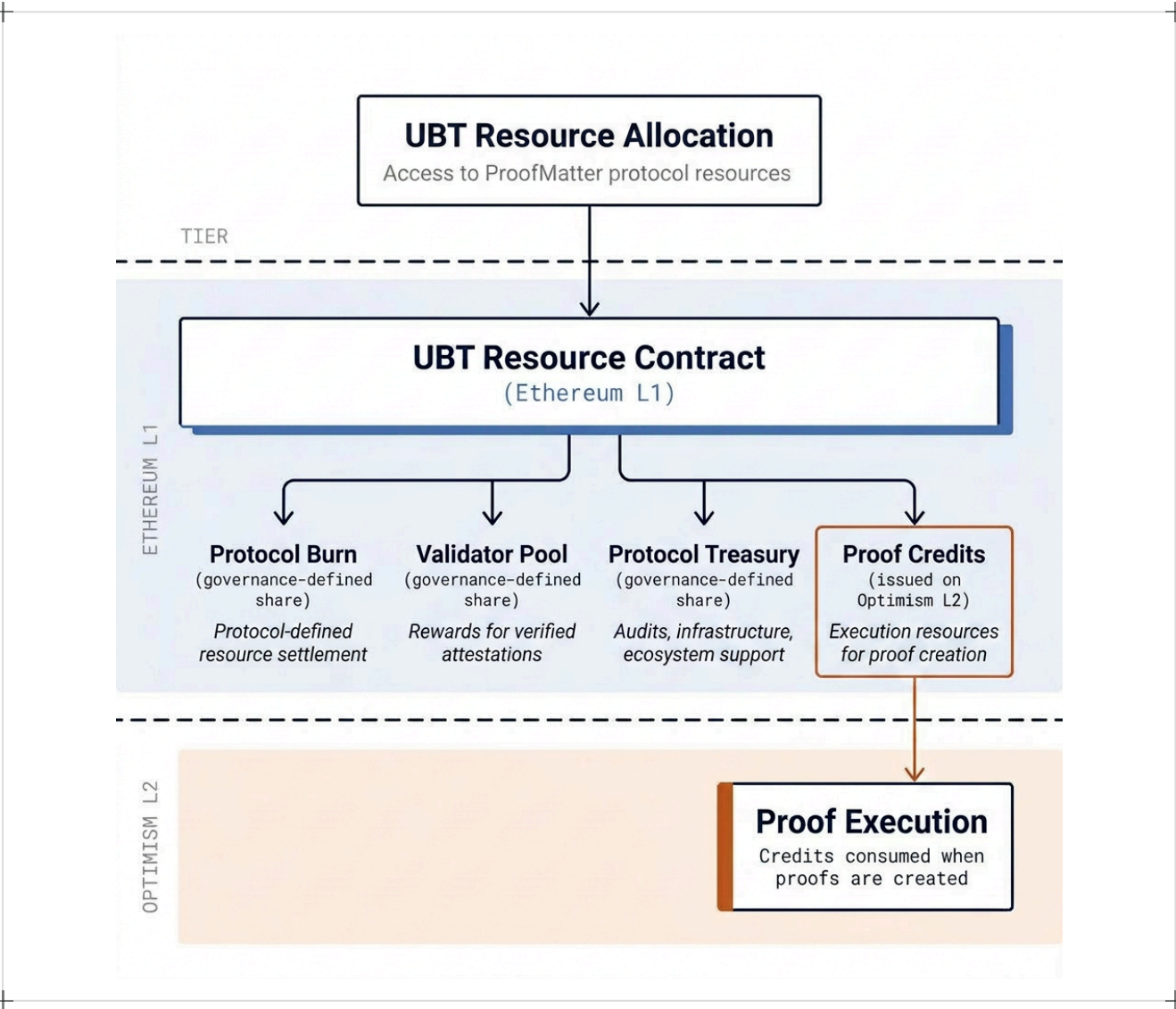


FIG. 09 – UBT AS THE OPERATIONAL RESOURCE LAYER OF PROOFMATTER

Bridgeless Credits and Transparent Flows

Proof creators deposit UBT on Ethereum. The L1 contract enforces distribution rules — burn, validator rewards, treasury allocations — and triggers credit issuance on Optimism through the native messaging bridge. When proofs are generated, credits are consumed; the underlying UBT flows are fully visible in the Explorer. There is no manual custody, no opaque treasury handling, and no external bridge dependency: the protocol itself guarantees accounting and settlement. This is the economic spine that turns proofs into measurable token activity.

Roles and Alignment

The economy is designed around explicit, auditable roles. Proof creators prepay and consume credits, directly driving UBT utility as they generate proofs. Validators stake UBT, perform checks, and earn rewards for accurate attestations; low-quality or dishonest behavior may be penalized through slashing or suspension. Template builders publish reusable proof definitions and receive a share of fees whenever their templates are used. Tool developers extend explorers, analytics, or SDKs and can monetize usage or receive grants. This arrangement creates a feedback loop: more proofs lead to more credit consumption, more burns and rewards, more participation, and, ultimately, more trust.

Parametric Distribution and Governance Bands

Fee distribution is defined parametrically at the proof-contract level within governance-approved bands — for example, minimum burn ratios and maximum treasury shares. Contracts that comply are marked as ProofMatter-Verified in the Explorer; non-verified contracts remain usable but are clearly labeled. This model fosters competition around fairness and efficiency without requiring central enforcement and keeps all economic parameters legible to the market.

An Assurance-Driven Economy

ProofMatter links economic weight directly to verification quality.

Rather than pricing proofs by volume or network congestion, the protocol continuously adjusts costs and rewards according to how reliably a template or contract is being verified in practice. Trust is therefore not static; it accumulates or erodes over time, and the token economy reacts accordingly.

Assurance Score

Each template or proof contract maintains a dynamic Assurance Score derived from ongoing validation statistics: how frequently its proofs are sampled against governance targets, and how often those checks confirm or contradict the declared execution. When spot-checks return negative or inconsistent results, or when sampling frequency falls below policy thresholds, the Assurance Score decreases.

A lower score automatically raises the price of subsequent proofs that use the same template. More credits must be consumed for each new proof, and a higher minimum trust level (for example, TL3 instead of TL1) may be required before the proof is accepted by counterparties or displayed as verified in the Explorer.

This creates a direct financial consequence for low-assurance behavior: unreliable processes literally become more expensive to certify. Conversely, consistently clean and adequately audited templates gain efficiency — their proofs cost fewer credits and enjoy greater visibility and market preference.

The Assurance Score is recalculated periodically from validator attestations and displayed alongside each template and contract. It becomes a public signal of reliability and a self-regulating feedback loop between operational quality, assurance, and economic terms.

Validator Quality

Validator performance follows the same principle: Frequent, well-documented, and consensus-aligned attestations increase a validator's effective reward multiplier, while proven detection of real irregularities yields additional bounties.

Repeated negligence, missed checks, or contradictory attestations reduce rewards and can trigger partial or full stake loss and temporary delisting.

Because template Assurance Scores and validator reputations are mathematically linked, careless validation does not only hurt the individual—it raises the overall cost of the proofs that validator serves, providing a system-wide incentive for diligence.

Governance Control

Audit-frequency targets, acceptable error ranges, bonus multipliers, and distribution bands are defined and adjustable through UBT governance. Templates and contracts that remain within these parameters retain their "Verified" badge; those falling short are flagged and automatically face higher credit consumption until their Assurance Scores recover.

The result is a market in which assurance becomes a measurable commodity: transparency drives trust, trust determines cost, and cost reinforces integrity.

Supply, Treasury, and Transparency

UBT has a fixed supply of 150 million tokens. No inflation occurs, and ProofMatter introduces no secondary asset. All burns, validator deposits, and treasury allocations are recorded on-chain and indexed in the Explorer. The treasury funds audits, grants, community initiatives, and infrastructure. Governance defines allocation policies and can adjust burn ratios or fee bands as the network matures. The goal is not to maximize extraction but to sustain a credible, open utility.

Token Distribution

UBT has been in circulation since 2018. The total supply of 150,000,000 tokens was minted at launch; no further minting is possible.

Unlike most protocol tokens, UBT has no insider allocation, no team reserve, no vesting schedules, and no locked supply held by the protocol steward. The entire supply is in public circulation, freely tradeable, and distributed across thousands of holders. SPO Consulting GmbH, as protocol steward, does not hold a strategic UBT reserve.

This is a deliberate design choice. ProofMatter's economic model does not depend on controlled token releases or insider selling pressure. Instead, it relies entirely on organic utility demand: proof creation consumes credits, credits require UBT deposits, deposits trigger burns. The protocol is designed to provide renewed utility for existing UBT usage within the ecosystem — not a promise of future token unlocks.

PROPERTY	VALUE
Total supply	150,000,000 UBT (fixed, non-mintable)
In public circulation	100%
Team / insider allocation	None
Vesting schedules	None
Protocol-held reserve	None
Secondary token	None planned or intended

TAB. 01 – UBT DISTRIBUTION PROFILE

This distribution profile eliminates several risks common in token-based protocols: no cliff unlocks that create sell pressure, no insider information asymmetry about future token releases, and no governance capture through concentrated holdings. Every UBT holder participates on equal terms.

The protocol treasury, once operational, is funded exclusively through the 20% treasury share of each UBT deposit — not through pre-allocated token reserves. Treasury usage is designed to be governed by UBT holders through the governance process described in [Chapter 10](#).

The UBT Utility Cycle

As adoption grows, more actions are proven. Each proof consumes credits, which are anchored by UBT deposits. A portion of UBT is burned or locked; validators and builders are compensated; the treasury supports further development. The Explorer renders this loop visible: proofs beget utility; utility builds trust; trust compounds adoption. Over time, the network's assurance becomes a core driver of protocol utility and ecosystem trust.

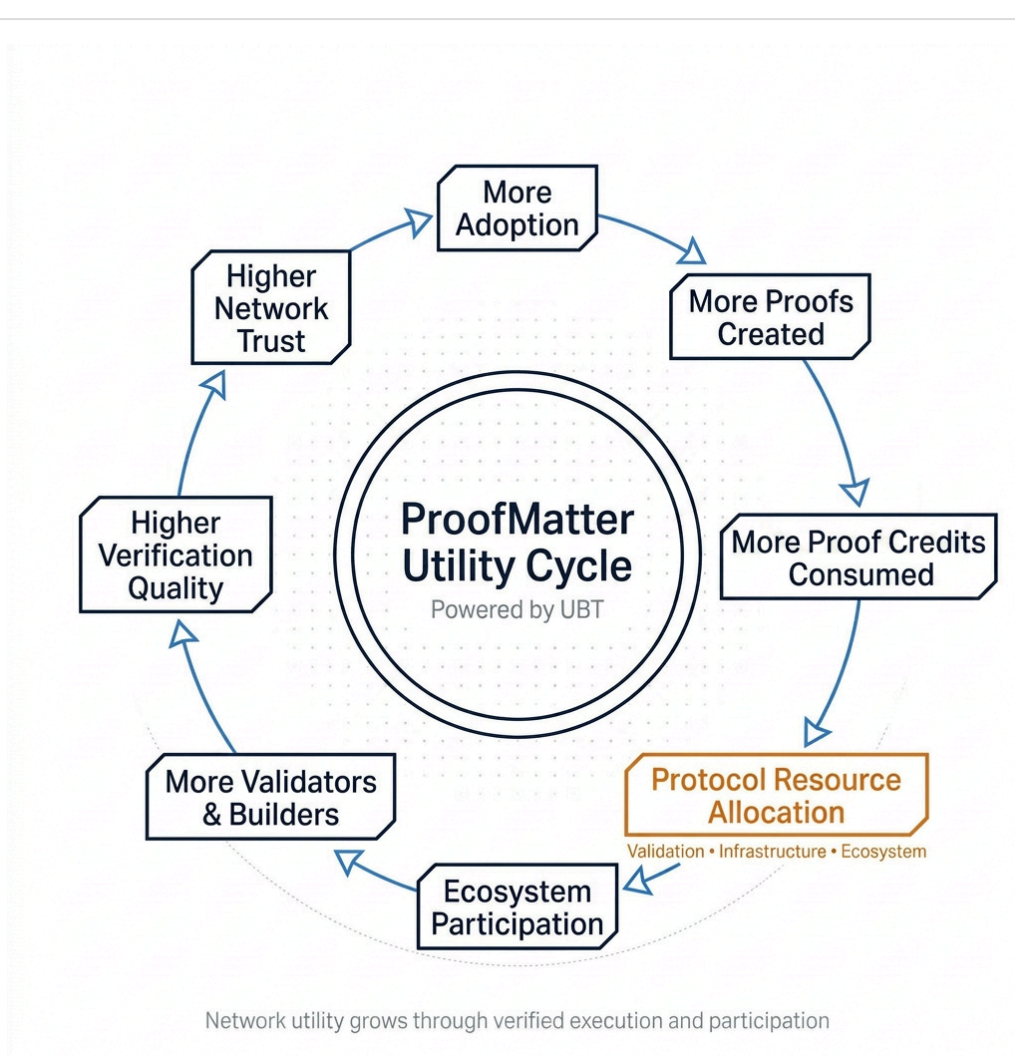


FIG. 10 – THE PROOFMATTER UTILITY CYCLE, POWERED BY UBT

This creates a continuous utility cycle in which protocol usage, verification activity, and ecosystem participation reinforce each other.

UBT extends its original utility role by powering a trustless proof infrastructure for verifiable execution at scale.

Use Cases & Templates

ProofMatter is not a niche protocol — it is a universal layer for verifiable execution. At its core lies a simple idea: any action, in any industry, can leave a proof trail.

Templates make this possible. Each template defines how a specific type of action is represented, verified, and stored on-chain. These templates are open, composable, and reusable — forming the backbone of an ever-growing proof ecosystem. The same ProofMatter infrastructure can support different industries by applying domain-specific templates while preserving a common verification and trust framework.

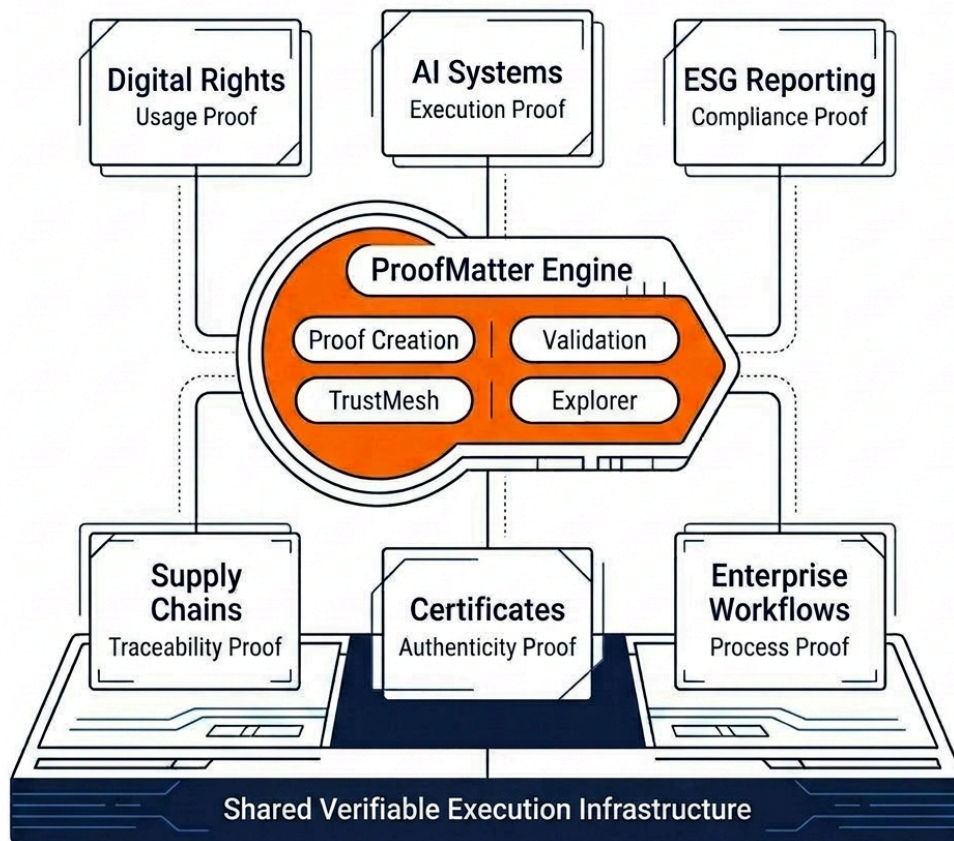


FIG. 11 — ONE ENGINE, MANY DOMAINS: SHARED VERIFIABLE EXECUTION INFRASTRUCTURE

Key Use Cases

1. Audio & Digital Content

Creative works, licenses, and royalties can be registered and tracked with verifiable proofs. Every license activation, download, or use generates a signed ProofMatter entry - from sound to signature.

EXAMPLE TEMPLATE

```
{
  "type": "license_activation",
  "asset_id": "track-4578",
  "user_wallet": "0xABC...",
  "timestamp": "2025-09-01T13:44Z",
  "signature": "0xDEF..."
}
```

Lisa, a music producer, publishes her work via a licensing platform that uses ProofMatter. Each activation or use of her tracks is recorded as a verifiable proof. When a copyright dispute arises, Lisa provides cryptographic evidence of each authorized use — resolving the conflict quickly and without lawyers. And because Lisa authored the licensing template, she also earns a small share of UBT every time it is reused across the ecosystem.

2. ESG & CO₂ Compliance

Emission reduction claims, audit steps, and policy checks are often unverifiable. With ProofMatter, every compliance action becomes provable — reducing greenwashing risks and audit costs. Compliance isn't a checkbox any longer. It's a hash.

ProofMatter-ready templates can map to the Corporate Sustainability Reporting Directive (CSRD) requirements in the EU or the Carbon Border Adjustment Mechanism (CBAM) tracking in global supply chains. Regulators, auditors, and partners can verify each reported event independently and on-chain.

For example, a steel manufacturer logs every emission reduction measure into a ProofMatter template. Each proof burns UBT, rewards validators, and contributes to the treasury. The Explorer shows all actions transparently, enabling both regulators and investors to confirm compliance without relying on unverifiable PDFs.

This regulatory context creates significant demand for verifiable and auditable solutions. ProofMatter provides the technical infrastructure to meet these requirements by enabling proofs that can be independently verified on-chain.

3. Supply Chains

From manufacturing to delivery, every logistical step can be hashed and verified. Whether it's organic certification, cold chain integrity, or factory origin: trust moves with the product.

Leading beyond traceability — into verifiability.

Imagine a coffee cooperative exporting beans to Europe. Each step — from harvesting, to roasting, to shipping — is recorded as a ProofMatter proof. Importers and regulators can see that the beans met fair-trade and organic criteria, while sensitive supplier identities remain selectively hidden using Merkle proofs. The farmer's cooperative uses a community-built supply chain template, and the developers behind that template receive UBT rewards each time it is used.

4. Certifications & Documents

Digital or paper certificates can be falsified — ProofMatter transforms them into immutable, signed proofs. Perfect for food safety, training, legal approvals, and more.

Example: A pharmaceutical company issues a GMP (Good Manufacturing Practice) certificate using a ProofMatter template. The certificate is stored as a verifiable proof on Optimism. Auditors and regulators can instantly confirm authenticity through the Explorer, without relying solely on the issuing authority. The template creator benefits economically, as each issued certificate consumes UBT and rewards their template design.

5. Green Steel & Material Provenance

"Green steel" is becoming a market requirement — but the claim is only as strong as its proof. Automotive manufacturers under EU Taxonomy reporting need verifiable evidence that their steel suppliers actually produce below 1.8 tonnes CO₂ per tonne of crude steel. Today, this evidence is a PDF certificate passed between intermediaries.

The EU Carbon Border Adjustment Mechanism (CBAM), effective from 2026, raises the stakes: importers must prove the embedded carbon content of materials entering the EU or pay a carbon price equivalent.

With ProofMatter, every step from raw material to delivery becomes a verified, auditable record. The steel producer creates a proof at each production stage — ore sourcing, smelting, processing, transport — with emissions data structured in a SyncTree. Commercially sensitive fields (supplier names, pricing, process parameters) remain masked, while emissions values are verifiable by auditors and regulators.

Template constraints enforce compliance directly: TotalCO₂PerTonne must be below the declared threshold. Validators, accredited auditors or industry verification bodies perform spot checks and issue attestations. Over time, the TrustMesh for a steel batch grows from a self-signed proof (TL1) to a multi-party verified provenance chain (TL3/TL4). For buyers, the Explorer shows a single view: this batch has a verified carbon footprint, attested by independent validators, anchored on-chain.

6. Digital Product Passport

Beginning in 2027, EU regulations mandate Digital Product Passports (DPPs) for batteries, textiles, and electronics. With further product categories to follow. Every product must carry a machine-readable record of its composition, origin, repairability, and environmental impact throughout its lifecycle.

The challenge is not data collection — most manufacturers already have this information. The challenge is verifiability. A Digital Product Passport controlled solely by the manufacturer provides no more assurance than the PDF certificates it replaces.

ProofMatter provides the verification layer. Each lifecycle event like manufacturing, quality control, shipping, repair, recycling, generates a proof anchored on Optimism L2. The SyncTree structure enables role-based disclosure: a consumer scanning a QR code sees material composition and repairability scores; a recycling facility sees disassembly instructions; a regulator sees the full provenance chain including supplier identities. Each party sees only what they need.

Template constraints enforce compliance thresholds directly: minimum recycled content percentages, maximum hazardous substance levels, mandatory disclosure fields. A product whose passport fails a constraint is visibly non-verified in the Explorer without requiring a human auditor to discover the violation.

Use Case Matrix

DOMAIN	EXAMPLE ACTION	PROOF TYPE	WHO BENEFITS
Audio / Content	License activation	License proof	Artists, platforms, IP lawyers, template authors
ESG & Compliance	CO ₂ reduction logged	Compliance proof	Regulators, investors, companies, auditors
Supply Chains	Fair-trade coffee shipment	Supply chain proof	Producers, importers, retailers, consumers
Certifications	GMP certificate issued	Document proof	Pharma firms, regulators, training providers
IoT (Emerging)	Machine maintenance log	IoT proof	Manufacturers, insurers, auditors
Green Steel	CO ₂ per tonne verified	Material provenance proof	Steel producers, automotive OEMs, regulators
Product Passport	Battery lifecycle tracked	DPP proof	Manufacturers, recyclers, consumers, regulators
Governance (DAOs)	Off-chain proposal anchored	DAO action proof	DAO members, communities, regulators

TAB. 02 – USE CASE MATRIX

Templates as the Engine of Reuse

Each use case is powered by templates:

- Templates define the schema, fields, and structure of proofs for a specific domain.

- Developers or domain experts can create and publish templates to the open registry.
- Each time a template is used, the original creator can receive UBT rewards.
- Templates are versioned, auditable, and subject to community governance.

Two tiers of templates may emerge:

- **Core Templates** — curated and maintained by the ProofMatter core team and approved by UBT governance.
- **Community Templates** — open submissions by anyone, visible in the Explorer, with optional review and ranking.

Templates that meet governance-defined criteria (e.g., transparency, efficiency, fair fee settings) may receive ProofMatter-Verified status and appear with a badge in the Explorer.

In future iterations, a Template Marketplace or Template Hub may emerge:

- Discoverable templates by category (e.g., Energy, Logistics, IP).
- Ratings, usage stats, and governance tags
- Integration with developer SDKs and contract generators.

This will turn templates into a true developer asset class — not just reusable logic, but also an ongoing economic opportunity.

Open Ecosystem & Emerging Scenarios

ProofMatter encourages new use cases through open participation and composability:

- **DAOs** can anchor off-chain proposals or decisions as immutable action logs.
- **AI systems** can generate proofs from training pipelines or content creation.
Example: An AI lab records every training dataset used for a model, providing regulators with verifiable logs of provenance and bias control.
- **IoT devices** can self-report maintenance, calibration, or location data.
Example: A wind turbine automatically logs each service event as a ProofMatter proof, ensuring maintenance compliance without manual paperwork.
- **Regulators** can independently verify policy enforcement across global systems.

The more templates exist, the easier it becomes to onboard new verticals — without central gatekeepers.

ProofMatter provides a universal, composable template system — enabling any action, in any industry, to become a verifiable proof.

AI Use Cases — The New Verification Frontier

ProofMatter does not build AI. ProofMatter verifies the AI of others.

The AI Verification Problem

AI systems are becoming decentralized, autonomous, and generative — operating across borders and executing decisions at speeds no human audit regime can match. This creates an unsolved problem: trust without central authority. Three specific failures define the gap:

- **Federated Learning at scale** — thousands of participants train shared AI models together, but any participant can submit fake results and collect rewards without detection. No mainstream FL framework provides a cryptographic proof-of-computation mechanism.
- **Autonomous AI Agents** — agents approve invoices, commit code, and negotiate contracts on behalf of humans. When an agent claims it performed an action, there is no independent attestation. Accountability trails do not exist.
- **Generative AI Content** — AI-generated images, videos, and documents flood digital channels. The C2PA standard (Coalition for Content Provenance and Authenticity) defines content credentials, but relies on centralized Trust Lists and Timestamp Authorities — single points of failure that cannot serve a global, decentralized ecosystem.

These three markets represent over \$50 billion in addressable AI infrastructure spend by 2027. All three share the same root cause: they need a verification layer that no single party controls. ProofMatter is that layer. The same primitives that prove CO₂ emissions and supply chain custody — SyncTree selective disclosure, TrustMesh multi-party verification, UBT-backed economic accountability — extend to the AI economy. The architecture does not change. Only the proof templates do.

Federated Learning Verification

INTEGRATION: FLOWER FRAMEWORK (CUSTOM STRATEGY PLUGIN)

Federated Learning (FL) enables thousands of participants — hospitals, banks, mobile devices — to train a shared AI model without sharing their private data. Each participant trains locally and sends back a gradient update. The problem: honest training is expensive. A cheating participant can submit a fake update and collect the same reward. Without verification, honest participants subsidize free-riders.

ProofMatter integrates into the Flower Framework — the most widely adopted open-source FL framework, developed at the University of Oxford — as a Custom Strategy Plugin. The plugin does not change how gradients are computed or aggregated. It adds one thing: before a gradient update is accepted, the submitting participant must provide a Proof-of-Computation — a signed,

cryptographically structured record anchored on Optimism L2. FL Verifier nodes (UBT-staked) check the proofs and attest valid rounds. The proof captures computational evidence — gradient hash, computation time, hardware attestation — without exposing the gradient values or training data. Verifiers can check constraints (gradient norm plausibility, minimum computation time) via selective disclosure without ever seeing sensitive data.

UBT Token Flow: Every FL participant stakes UBT before joining a training run. Each round proof consumes UBT credits (20% burned, 30% to validators, 20% to treasury, 30% to credit backing). Free-riders are slashed — stake forfeited, distributed to validators and burn. Honest participants see their stake returned plus round rewards. Cheating is economically irrational by design.

Market context: The global federated learning market is projected to grow from under \$200 million in 2024 to over \$3 billion by 2030. Healthcare alone has an estimated \$45 billion AI training market by 2030, of which a significant fraction will require federated approaches for regulatory compliance. Every dollar of that market is currently unverified.

AI Agent Attestation

INTEGRATION: MCP (MODEL CONTEXT PROTOCOL) + A2A (AGENT2AGENT PROTOCOL)

AI agents are taking consequential actions with increasing frequency — approving invoices, committing code, negotiating terms, delegating to other agents. Two protocols are emerging as universal standards: MCP (Anthropic, November 2024) defines how agents call tools; A2A (Google, April 2025) defines how agents communicate with each other. Both are backed by the Agentic AI Foundation under the Linux Foundation, with members including Anthropic, Google, Microsoft, AWS, and OpenAI.

MCP and A2A solve the communication problem. They do not solve the verification problem. An agent can claim to have executed an action with no cryptographic proof. Agent A delegates to Agent B — how does Agent A verify the result without trusting Agent B's self-report?

ProofMatter operates at two levels:

- **As MCP Server:** Any MCP-compatible agent (Claude, GPT, Gemini) can natively call three tools — `attest_action` (anchor cryptographic proof of an agent action on-chain), `verify_attestation` (check an existing attestation against the chain), and `get_trust_score` (retrieve the on-chain trust score of an agent). No agent modification required.
- **As A2A Verification Agent:** In agent-to-agent scenarios, ProofMatter acts as a trusted third party. Agent A delegates to Agent B, then calls ProofMatter to independently verify Agent B's reported result before accepting it. The entire chain of delegation is reconstructable months or years later.

UBT Token Flow: Agent operators register in the on-chain Trust Registry by staking UBT. Each attestation consumes a small per-attestation fee — small enough for high-frequency use, sufficient to deter spam. Trust scores build through verified attestations; contradictory attestations trigger slashing. Agents with high trust scores can command greater confidence from counterparties.

Market context: The EU AI Act requires documented action trails for high-risk AI systems by 2026. Every AI agent handling consequential actions is a potential ProofMatter integration point, generating recurring UBT demand through registration stakes and per-attestation fees.

Content Provenance

INTEGRATION: C2PA-COMPATIBLE BLOCKCHAIN EXTENSION

The C2PA standard (Adobe, ARM, Intel, Microsoft, Truepic) defines Content Credentials — signed metadata that records who created content, when, and with what tools. C2PA is technically sound and gaining adoption across Adobe Creative Cloud, Leica, Nikon, and AI platforms. But it has three structural weaknesses:

- **Centralized Trust Lists:** only consortium-approved companies can issue credentials. A small group controls participation.
- **Centralized Timestamp Authorities:** if a Timestamp Authority goes offline or is compromised, existing credentials become unverifiable.
- **No AI Workflow Provenance:** C2PA records that content was created, but not which model, which parameters, or which training data produced it. Exactly the questions regulators and IP attorneys need answered.

ProofMatter extends C2PA without replacing it, through three additions:

- **Blockchain-Anchored Timestamps:** Instead of relying solely on a central Timestamp Authority, ProofMatter anchors each Content Credential hash on Optimism L2 — immutable, decentralized, no single point of failure. Additionally, ProofMatter obtains RFC 3161 qualified timestamps from accredited Timestamp Authorities for each block containing proof events. This dual approach provides both the decentralization of blockchain timestamps and the legal recognition required under the EU eIDAS regulation. The result: Content Credentials anchored through ProofMatter are not only cryptographically verifiable but designed to strengthen evidentiary integrity — a capability no purely blockchain-based or purely TSA-based solution offers alone.
- **Decentralized Trust Registry:** Any entity can register as a credential issuer by staking UBT, thereby replacing consortium gatekeeping with economic security. Track record replaces membership.
- **AI Workflow Provenance:** A new C2PA-compatible assertion type (pm.ai-workflow) captures the full AI generation context: model ID, inference parameter hash, training data reference, AI-generated flag, all anchored on-chain. Proprietary details are protected via selective disclosure while proving they were recorded.

UBT Token Flow: Issuers stake UBT to register. Each anchored credential consumes a per-anchor fee (standard 20/30/20/30 distribution). Verification is free by design, maximizing adoption. At media-scale volumes (a platform anchoring millions of images per day), anchor fees alone drive substantial, predictable UBT demand.

Market context: ARM is building C2PA into camera silicon. Within five years, most smartphones will capture Content Credentials at the hardware level. The EU AI Act's transparency requirements for AI-generated content take effect from 2026. ProofMatter's pm.ai-workflow assertion closes the specific gap between C2PA and what regulators actually require.

The UBT Utility Cycle

All three AI use cases generate UBT demand through the same mechanisms: staking, per-proof fees, and burning. Because UBT has a fixed supply of 150 million tokens with no mechanism for additional issuance, sustained activity reduces circulating supply through protocol-defined burn mechanics.

The usage loop: Increased protocol usage leads to higher proof activity and corresponding protocol-defined token flows, including burns, validator allocations, and treasury funding. As the network evolves, additional validators, templates, integrations, and verification services may strengthen the protocol's operational capabilities and support broader adoption across enterprise and AI-related use cases.

The three use cases are independent — an FL network, an agent platform, and a content platform can each adopt ProofMatter separately. Each generates standalone UBT demand. The combined effect is the feedback loop operating across all three markets simultaneously.

ProofMatter does not build AI. ProofMatter verifies the AI of others. In a world where AI acts, trains, and creates without central oversight, independent verification is not optional — it is the foundation of trustworthy AI infrastructure.

Roadmap 2026–2028

The roadmap outlined in this chapter reflects the current development intentions of the ProofMatter contributors as of publication date. Timelines, milestones, technical priorities, governance structures, and integrations may change due to technical, regulatory, operational, or market-related factors. Nothing in this roadmap should be interpreted as a guarantee, commitment, or binding obligation regarding future development, deployment, timelines, or functionality.

The ProofMatter roadmap reflects a step-by-step strategy: from concept to prototype, from prototype to public adoption, and ultimately toward a scalable, open, and governed ecosystem. It balances ambition with realism — providing a transparent path forward for contributors, partners, and token holders.

It is important to know that ProofMatter is not a spontaneous invention. It is the result of an eight-year journey that began with the Unibright Framework in 2018 — one of the earliest attempts to bring enterprise processes onto blockchain infrastructure. (Chapter 13 lays out the road to ProofMatter from 2018 to 2026).

ProofMatter enters its implementation phase in the spring of 2026. The groundwork is complete: technical specification documents have been finalized, the infrastructure paper has been drafted, and all major design decisions have been resolved.

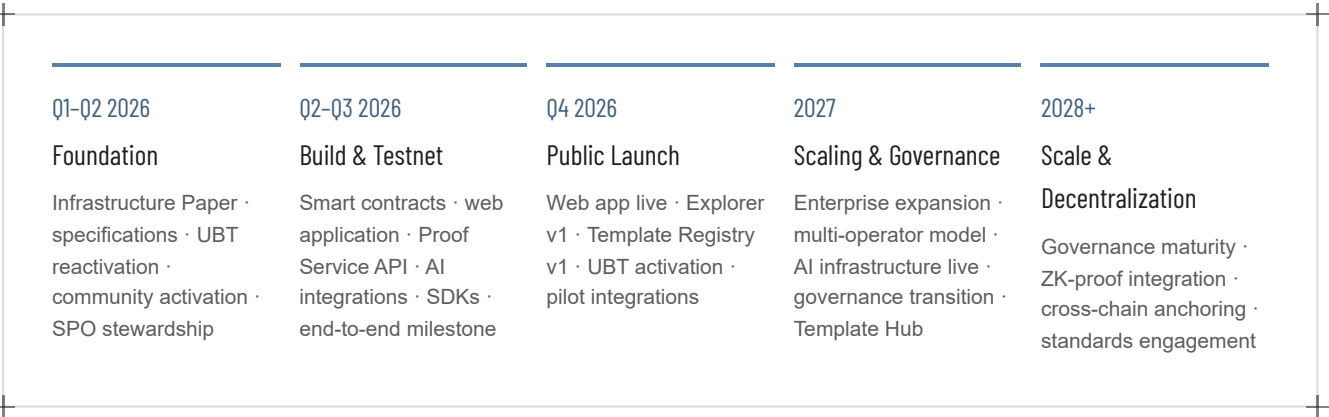


FIG. 12 — ROADMAP 2026–2028: FROM PROOF TO PRODUCT, FROM PRODUCT TO PROTOCOL

Q1-Q2 2026 — Foundation

ProofMatter enters the public stage with its first visible components.

- **Infrastructure Paper** — official release of the ProofMatter Infrastructure Paper, introducing the Proof-of-Execution model to both Web3 and compliance communities.
- **Specifications** — all technical specification documents finalized, covering architecture, smart contracts, SyncTree, token economy, API, and all use cases.
- **UBT Reactivation** — the role of UBT becomes visible again. Optimism confirmed as L2; UBT distribution set (20% burn / 30% validators / 20% treasury / 30% credit backing)

- **Education & Community Activation** — AMA and Interview series and workshops to guide first use-case builders.
- **Open Contributions** — GitHub contributions enabled for templates, Proof Services, and Explorers.
- **SPO Stewardship** — SPO Consulting GmbH formally assumes stewardship of the UBT ecosystem and the ProofMatter protocol.

First pilot integrations with partners in the digital content and licensing sector are underway. This phase is about establishing credibility: showing that Proof-of-Execution is real, that UBT is the protocol token, and that the system is open for builders.

Q2-Q3 2026 — Build & Testnet

The first implementation phase delivers working code on testnet.

- **Smart Contracts** — staking, credit issuance, proof anchoring, validator and workgroup registries deployed on Optimism testnet.
- **Web Application** — a fully hosted web app (Portal, Explorer, Admin) that allows customers to create, manage, and verify proofs through a graphical interface — no API or blockchain knowledge required. The system is designed to work at three access levels: directly against smart contracts (for advanced integrators), via the REST API (for developers), or through the hosted web application (for enterprise users and non-technical participants).
- **Proof Service API** — complete REST API with SyncTree integration, proof creation, verification, and template management.
- **AI Integrations** — MCP Server for AI agent attestation and Flower plugin for federated learning verification.
- **Developer Tooling** — SDKs (Python + JavaScript v1) with complete documentation.
- **End-to-End Milestone** — complete proof lifecycle demonstrable on testnet: deposit UBT → receive credits → create proof → anchor on L2 → verify → add attestation.
- **Community Challenges** — early access template challenges and proof bounties.

At this stage, developers begin to build with ProofMatter. Every proof consumes UBT credits, creating the first visible link between adoption and token usage.

Q4 2026 — Public Launch

From prototype to product: ProofMatter goes live.

- **Web Application Live** — the hosted ProofMatter web application goes public: Portal for proof creation and management, Explorer for transparent proof verification and UBT activity, and Admin interface for workgroup and validator management. Enterprise customers can begin using ProofMatter immediately — no integration work required.
- **Explorer v1** — full public Explorer with live proofs, templates, burn activity, validator stats, and UBT flows.

- **Template Registry v1** — first set of open-source templates: ESG, green steel, Digital Product Passport, supply chain, certifications, AI attestation.
- **UBT Activation** — first real UBT deposits, credit issuance on mainnet, burn counters running.
- **Pilot Integrations** — first enterprise pilots in production (ESG reporting, supply chain traceability).
- **Verification Badge System** — Explorer highlights proof contracts meeting governance-defined quality criteria.
- **Community Infrastructure** — GitHub opened for contributions, Telegram/Discord launched, AMA series begins.

This is where the ecosystem begins to scale operationally: verified templates attract adoption, adoption drives UBT usage, and Explorer visibility brings credibility.

2027 — Scaling, Governance & Ecosystem Flywheel

ProofMatter evolves from a product into a governed, multi-operator protocol.

- **Enterprise Expansion** — pilots graduated to production; co-development of industry-specific templates with enterprise partners.
- **Multi-Operator Model** — external parties deploy their own Proof Contracts via governance-approved registry.
- **AI Infrastructure Live** — Trust Registry for agent operators and content issuers; A2A Verification Agent deployed.
- **Governance Transition** — hybrid phase begins; UBT holders vote on template approvals, treasury allocations, and registry additions via Snapshot. SPO retains a veto on security-critical decisions during the transition.
- **Validator Program** — structured onboarding with published SLAs, slashing conditions, and public reputation scores.
- **Community Grants** — treasury-funded initiatives for audits, tooling, and template development.
- **Template Hub** — discoverable templates with ratings, usage stats, and developer fee shares.

At this stage, ProofMatter is no longer just a protocol — it is a public utility for verifiable execution, sustained by UBT governance and community-driven growth.

2028 and Beyond — Scale & Decentralization

As adoption grows, ProofMatter progressively decentralizes.

- **Governance Maturity** — governance scope expands as participation and tooling mature; the transition from hybrid to full on-chain governance proceeds based on demonstrated community readiness, not a fixed date.
- **ZK-Proof Integration** — zero-knowledge proofs evaluated and, where justified, deployed for highest-assurance use cases (TL4/TLx), building on the ZK-compatible architecture designed from v1.

- **Cross-Chain Anchoring** — optional anchoring across multiple L2s or directly to Ethereum L1 for high-value regulatory submissions.
- **Standards Engagement** — template schemas submitted to relevant bodies (C2PA working group, ESRS technical working group, ISO TC 307) for formal standardization.

The goal is not growth for its own sake, but a self-sustaining ecosystem where operators, validators, and template authors generate value independently of SPO.

Partner & Contributor Invitation

ProofMatter thrives through openness — and 2026 will be the year of collaboration.

We invite:

- Developers and SDK contributors
- Validators and infrastructure providers
- Compliance innovators and ESG technologists
- UBT holders and community curators

Together, we are not just proving actions — we are building a new trust layer for the digital economy.

Mini Example: A compliance startup could launch a "Carbon Credit Proof Template" on ProofMatter. Each time it is used, part of the fees flow to the startup, validators secure the proof, UBT is burned, and the Explorer shows a verified badge. This simple cycle illustrates how builders, validators, token holders, and end users all benefit in parallel.

ProofMatter grows step by step — from proof to product, from product to protocol, and from protocol to public utility.

Governance & Ecosystem

ProofMatter builds on a strong foundation of continuity. In 2025, SPO Consulting GmbH — a company with decades of enterprise software experience since 1989 — formally took over the stewardship of the UBT Token and all associated assets. This ensures that the legacy of Unibright is preserved and seamlessly connected to the broader SPO ecosystem, which has served global enterprises for more than three decades.

In the early phase, SPO provides professional stewardship, technical stability, and organizational continuity — supporting a reliable foundation for token holders, partners, and developers. The initial governance and operational setup is designed to prioritize regulatory awareness, technical robustness, and enterprise-oriented reliability.

But ProofMatter is not designed to remain centralized. From the beginning, it has been built with the goal of transitioning into a community-governed infrastructure. Over time, decision-making is set to shift from SPO stewardship toward transparent, token-based governance, powered by UBT holders.

Transition Model

ProofMatter's governance is planned to evolve in three interconnected phases:

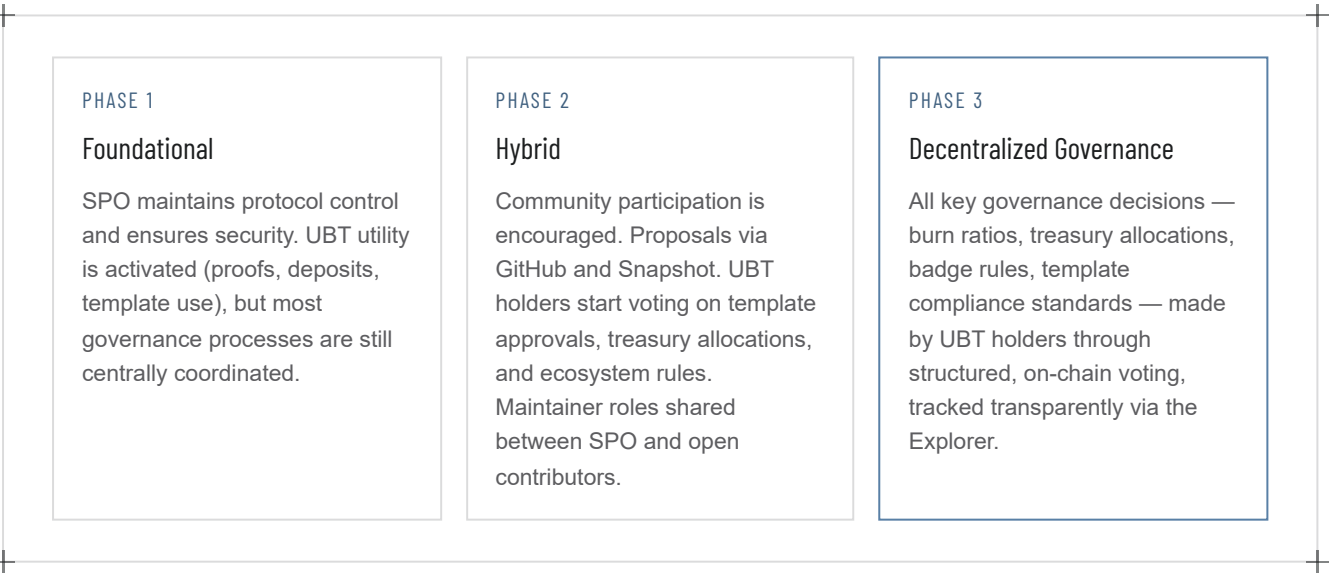


FIG. 13 — THE THREE-PHASE GOVERNANCE TRANSITION

- **Foundational Phase:** In this stage, SPO maintains protocol control and ensures security. UBT utility is activated (proofs, deposits, template use), but most governance processes are still centrally coordinated.
- **Hybrid Phase:** Community participation is encouraged. Proposals can be submitted via GitHub and Snapshot. UBT holders are included to start voting on template approvals, treasury allocations, and ecosystem rules. Maintainer roles for code repositories are intended to be

shared between SPO and open contributors.

- **Outlook to decentralized Governance:** A full transition is planned. At this stage, all key governance decisions — including burn ratios, treasury allocations, badge rules, and template compliance standards — are expected to be made by UBT holders through structured, on-chain voting. Validators and developers are expected to participate directly, while governance metrics (quorum, voter participation, outcomes) will be tracked transparently via the Explorer.

This phased model balances stability and innovation: early control ensures reliability, hybrid participation builds trust, and full decentralization unlocks resilience.

Decentralization Statement

ProofMatter's architecture is designed to minimize reliance on any single operator from the outset:

- **Automatic Distribution:** All UBT deposits are processed by an Ethereum L1 contract. Burn, validator rewards, treasury, and builder allocations are enforced automatically by contract logic — never by manual intervention.
- **Native Messaging (L1 <> L2):** Usage credits on Optimism are deterministically derived from L1 deposits via the official Ethereum–Optimism messaging system. L1 deposits automatically trigger credit issuance on L2 — with no off-chain relayer and no reliance on a single operator.
- **Governance Transition:** In the foundational phase, SPO Consulting GmbH safeguards protocol parameters. Over time, these controls are intended to migrate into community governance, with UBT holders voting on distribution ratios and ecosystem rules.

Governance manages the whitelist of Proof Contracts. In the bootstrap phase, a small set of trusted Proof Contracts — operated by SPO and selected partners — are authorized to consume credits. Over time, governance expands this whitelist, enabling further verified Proof Contracts to join the ecosystem. With this model, technical execution is already decentralized and verifiable, while governance is set to follow a transparent path from stewardship to full community control.

Governance Mechanics

ProofMatter governance is intended to be modular and transparent:

- **Proposal System:** Any UBT holder can propose a new template, contract rule, burn ratio, or ecosystem change.
- **Voting:** Snapshot and on-chain contracts (e.g., Governor modules) allow gasless and transparent voting.
- **Deposits:** To reduce spam, proposals may require deposits (e.g., 5,000 UBT refundable if quorum is reached).
- **Transparency:** All staking, burning, and governance data is surfaced in the Explorer.

For example, a UBT holder could propose adjusting the minimum burn ratio from 20% to 25%. The proposal would be posted on GitHub, staked with a UBT deposit, voted on by the community via Snapshot, and — if approved — reflected in the Explorer with updated parameters.

Contributor Incentives

Governance is not just about voting — it is about participation and contribution.

- **Template Authors** can earn UBT whenever their templates are adopted and used in proofs.
- **Tooling Developers** may receive treasury-funded grants for Explorers, SDKs, or analytics modules.
- **Validators** earn ongoing rewards for securing proofs and participating in governance.
- **Voters** may receive recognition or small incentives for active participation and quorum contribution.

Example: A developer submits a supply chain proof template. The governance process reviews and approves it. Each time this template is used, part of the proof fee is routed to the developer. In this way, governance itself becomes an engine for innovation, aligning incentives across all roles.

Community Infrastructure

ProofMatter combines technical openness with active community infrastructure.

- **Telegram** (or comparable platforms like Discord) enables open discussion, validator onboarding, and AMAs.
- **GitHub** hosts templates, proof contracts, tools, and governance proposals.
- **Medium & LinkedIn** are used for thought leadership and ecosystem updates.
- **Explorer** acts as the central transparency hub, surfacing proofs, burns, deposits, votes, and templates in real time.

These channels form a coherent communication fabric: fast-moving discussions in Telegram, structured proposals on GitHub, official updates on Medium/LinkedIn, and live data transparency via Explorer.

Ecosystem Growth: Breadth, Depth, Trust

ProofMatter's governance is designed to drive ecosystem growth along three axes:

- **Breadth** — more industries, templates, and proofs are onboarded as open participation grows.
- **Depth** — better tooling, analytics, and integrations emerge from treasury-funded contributions.
- **Trust** — governance ensures that the system is resilient, forkable, and community-driven, avoiding reliance on a single entity.

Over time, this governance framework ensures that ProofMatter matures from a guided launch into a self-sustaining ecosystem — governed not by a company, but by a community of contributors and token holders.

ProofMatter evolves from professional stewardship to resilient, community-driven governance — powered by UBT and open contributions.

Market, Competition and Differentiation

Across the global economy, trust is still largely established through reputation, certification, and authority. Auditors, inspectors, and compliance agencies issue documents that act as proxies for truth. These models are slow, expensive, and limited in scope: they verify intentions or signatures, not actual execution.

As transactions and value creation migrate into digital and decentralized environments, this approach no longer scales. The world is beginning to shift from trust-by-reputation to trust-by-proof — and ProofMatter is designed to power that transition.

Traditional and Emerging Approaches

Legacy assurance frameworks depend on manual processes and centralized intermediaries. ISO certifications rely on audits and site visits; ESG reports depend on self-reported spreadsheets; supply-chain traceability ends with paperwork. Even modern digital licensing or contract management systems merely record signatures or download logs rather than cryptographically provable execution. These mechanisms provide a semblance of trust, but not verifiability.

During the past few years, various blockchain initiatives have attempted to close parts of this gap. Decentralized physical-infrastructure networks (DePINs) like Helium prove hardware availability; real-world-asset platforms tokenize ownership claims; specialized compliance chains log audits within single industries; and projects such as POAP or Hypercerts attest to attendance or participation.

While innovative, these solutions remain partial. They validate existence or ownership but rarely prove execution — whether something was actually done. This gap is becoming increasingly visible under new regulatory frameworks such as the EU Artificial Intelligence Act (Regulation (EU) 2024/1689), which explicitly requires traceable data provenance, record-keeping, and auditability for AI systems.

As digital value creation becomes algorithmic and autonomous, verification cannot stop at a transaction hash — it must extend to proofs of execution and data lineage. ProofMatter provides this underlying layer, bridging compliance-grade traceability with blockchain-native verifiability.

The Gap in Existing Systems

Most current blockchain architectures provide immutable storage but not semantic context. Generic ledgers such as Ethereum or Polygon record hashes or transactions but cannot express what those hashes represent. Storage-focused systems like Filecoin or Arweave ensure data persistence but not correctness of action. Tokenized IP or NFT models attach metadata to assets but lack verifiable proof that the described event occurred.

Consequently, they secure data, not execution.

The result is a fundamental trust gap: blockchains can prove that a transaction was recorded, yet they cannot prove that the underlying process was carried out as claimed. ProofMatter addresses this precise void.

ProofMatter as the Proof-of-Execution Layer

ProofMatter introduces a missing layer above conventional blockchain infrastructure: Proof of Execution.

It transforms off-chain or hybrid processes into verifiable, structured proofs that can be anchored, validated, and audited. Each proof template defines not only a data structure but also verification rules and disclosure policies. Hybrid validation allows accredited validators or auditors to perform targeted checks, producing signed attestations that confirm the execution of real-world actions. These attestations form the edges of the TrustMesh; the successful path through that mesh constitutes the proof trail — the verified sequence of execution.

By combining on-chain anchoring, off-chain attestation, and economic incentives, ProofMatter achieves a level of assurance unattainable by storage-only or token-only systems.

Comparative Analysis

In comparative terms, ProofMatter differs from both traditional audit systems and blockchain-based attempts across several dimensions. To make this concrete, it is worth examining what existing players solve — and where they stop.

Scope and Universality

Traditional audits are industry-specific and episodic. Most blockchain solutions remain domain-bound. EAS (Ethereum Attestation Service) provides a flexible on-chain attestation schema, but defines no templates, no validation policies, and no economic incentive layer. An EAS attestation is a data point; a proof trail is a verified execution chain with trust levels, selective disclosure, and UBT-backed accountability. Chainlink Proof of Reserve verifies that off-chain reserves back on-chain tokens, critical but narrow (asset backing only, not execution verification). Hypercerts and POAP attest to participation and impact claims but lack structured templates, hybrid validation, and staking mechanisms — they prove presence, not execution. ProofMatter provides a universal, template-driven substrate where any action, in any industry, can be represented, verified, and proven.

Structure and Semantics

Generic ledgers such as Ethereum or Polygon store opaque hashes. Ceramic / ComposeDB provides decentralized data storage with mutable, schema-defined documents — it stores and syncs data, but does not verify that an underlying action was executed. ProofMatter enforces structured semantics through templates and validation rules. Every proof is interpretable, machine-readable, and self-describing.

Validation Model

Most systems rely on implicit trust in the data source. Traditional TIC firms (SGS, Bureau Veritas, TÜV) dominate the \$250 billion testing, inspection, and certification market with manual, episodic audits delivered as PDF reports. Their model is valuable but opaque and point-in-time. ProofMatter replaces assumption with verification: optional, policy-driven, off-chain spot checks generate attestations signed by independent validators. Hybrid validation is not an add-on; it is intrinsic to the protocol. ProofMatter does not replace traditional auditors — it provides the infrastructure that makes their attestations cryptographically verifiable and continuously auditable.

Privacy and Compliance

Storage-based systems expose either everything or nothing. ProofMatter, via SyncTree, enables selective disclosure at field level — satisfying auditors and regulators while maintaining confidentiality and GDPR compliance.

AI Infrastructure

C2PA (Adobe, ARM, Intel, Microsoft) defines content provenance credentials — technically sound but dependent on centralized Trust Lists and Timestamp Authorities. ProofMatter extends rather than competes with C2PA (see [Chapter 8](#)). No existing solution addresses federated learning verification or AI agent attestation with cryptographic proofs and economic accountability — these are greenfield markets where ProofMatter is first to deliver production-ready infrastructure.

Economic Integrity

Most networks secure trust through gas fees or inflationary tokens. ProofMatter uses the long-established UBT token with a fixed supply. Proof creation consumes prepaid, bridgeless credits; validators earn from transparent distributions; no new asset or inflation is introduced.

Governance and Transparency

Parameters such as burn ratios, validator rewards, and assurance thresholds are defined by token-holder governance and surfaced in the Explorer, ensuring that economics and oversight remain community-controlled.

None of the solutions examined above combine structured proof templates, hybrid on-chain/off-chain validation, field-level selective disclosure, and an established non-inflationary token economy. ProofMatter is not positioned against any single competitor — it occupies a layer that does not yet exist in production.

Hybrid Validation as the Differentiator

The decisive differentiator is ProofMatter's hybrid validation model. On-chain proof templates enforce structure and immutability, while off-chain validators perform targeted, policy-based checks. Each check yields a signed attestation — a verifiable artifact linking real-world observation

to on-chain evidence. Collectively, these attestations form the TrustMesh, and the verified sequence of successful confirmations forms the proof trail itself.

This dual-layer design balances the transparency of blockchain with the contextual assurance of professional validation. It allows trust to scale horizontally across industries without replicating the cost and rigidity of traditional audit frameworks.

Market Opportunity

The demand for verifiable execution is expanding rapidly across two fronts.

Compliance and enterprise verification — the global ESG-reporting software market is projected to exceed USD 8 billion by 2030; the market for digital certifications already surpasses USD 25 billion; the EU Digital Product Passport mandate (effective 2027) will require verifiable lifecycle data for batteries, textiles, and electronics across the single market.

AI infrastructure verification, three markets that did not exist five years ago now create urgent demand for independent proof of execution. The federated learning market is projected to grow from under USD 200 million in 2024 to over USD 3 billion by 2030. The autonomous AI agent market is expanding faster than any other AI infrastructure segment, with the EU AI Act requiring documented action trails for high-risk AI systems by 2026. And the content provenance ecosystem anchored by C2PA and driven by hardware integration from ARM, Leica, and Nikon is scaling toward billions of Content Credentials per year as camera silicon embeds provenance at the hardware level.

Meanwhile, DePIN and RWA initiatives continue to grow but stop at tokenization, not verification. ProofMatter occupies the missing middle layer between these raw actions and the assurance demanded by regulators, enterprises, and decentralized organizations alike.

Even modest adoption within these verticals would demonstrate that Proof of Execution is not a niche concept but a universal requirement for digital accountability. ProofMatter's modular, open-source approach ensures that new sectors can onboard without rebuilding the trust stack from scratch.

Competitive Moat

ProofMatter's competitive advantage lies in the convergence of four elements rarely found together:

- **Universality** — a data-agnostic proof engine applicable across domains.
- **Composability** — governed templates enabling reuse and standardization.
- **Hybrid Validation** — verifiable linkage between digital claims and physical execution.
- **Incentivized Integrity** — a proven, non-inflationary token (UBT) aligning all participants.

Rather than competing with blockchains or certification bodies, ProofMatter augments them: blockchains secure state, auditors verify reality, and ProofMatter connects the two through a shared, transparent proof layer.

Its moat is not built on exclusivity but on verifiable openness — every proof, every burn, every attestation can be inspected in the Explorer.

ProofMatter bridges the divide between legacy reputation-based assurance and cryptographically verifiable execution. It introduces the first universal, economically aligned Proof-of-Execution layer — a missing foundation for ESG compliance, digital licensing, supply-chain integrity, and AI provenance alike. By transforming verification from a service into infrastructure, ProofMatter redefines how trust itself is produced, measured, and exchanged in the digital economy.

Legal Framework

No new Token

ProofMatter introduces no new assets. It is fully powered by the Unibright Token (UBT), which has been in circulation since 2018. The design principle is continuity: rather than creating a parallel token or inflating supply, ProofMatter deliberately reuses UBT as its sole access and incentive layer.

The characteristics of UBT remain unchanged:

- The total supply is fixed.
- No new tokens are minted, and no inflation occurs.
- Token logic is fully on-chain and auditable.

This preserves the fixed-supply design of the token model and avoids protocol-level inflation. UBT continues to serve as the sole token for protocol access, governance, and proof processing within ProofMatter.

MiCA Alignment

ProofMatter is designed to operate within the framework of the Markets in Crypto-Assets Regulation (MiCA), applicable in the EU since 2024. By aligning with MiCA, ProofMatter provides clarity for enterprises and institutions seeking to engage with the protocol in a regulated environment.

ProofMatter is designed with the intention of operating within the framework of MiCA. UBT is intended to function as a utility token used for protocol access and technical execution. Specifically:

- It is **not an e-money token**: there is no redemption right into fiat currency.
- It is **not an asset-referenced token**: it is not backed by a basket of assets.
- It is intended to function as a **utility token**: used exclusively for protocol access and technical execution.

Additional safeguards reinforce this alignment:

- All token activity (deposits, burns, governance actions) is transparent and on-chain.
- The protocol is non-custodial and permissionless; no central party holds user assets.
- The protocol itself is designed to avoid storing personal data on-chain.

ProofMatter stores only cryptographic hashes on-chain, not personal data. The underlying business data remains under the holder's control and can be deleted at any time without affecting the on-chain proof integrity. Since a hash alone cannot be reversed to reconstruct the original data, this design is intended to be compatible with GDPR Article 17 (right to erasure).

TOKEN CATEGORY (MICA)	DEFINITION UNDER MICA	WHY UBT DOES NOT APPLY / APPLIES
E-Money Token (EMT)	Must be redeemable at par value into official fiat currency.	UBT is not redeemable into fiat. No redemption rights exist.
Asset-Referenced Token (ART)	Pegged to or backed by one or several assets (e.g. commodities, baskets of currencies).	UBT is not backed by any asset or basket. No collateral or peg exists.
Utility Token	Provides access to a good or service on DLT infrastructure.	UBT is exclusively used to access ProofMatter protocol services (proof creation, validation, governance).
Security / Investment Token	Represents ownership rights, profit participation, or debt claims.	UBT does not represent equity, profit-sharing, or debt. It conveys no legal ownership rights.

TAB. 03 – UBT UNDER THE MICA TOKEN CATEGORIES

In plain language: UBT is not money, not backed by external assets, and not a security. It is simply the access key for using the ProofMatter protocol. Based on the current protocol design, UBT is intended to function as a utility token within the meaning of MiCA.

Risks & Limitations

While ProofMatter is designed to operate as a transparent and utility-driven protocol, several risks and limitations must be acknowledged:

- **Technical Risks** – ProofMatter builds on Ethereum and the Optimism OP Stack. Dependencies on these infrastructures may lead to temporary downtime, higher transaction costs, or unforeseen changes in protocol design. Selective disclosure via Merkle proofs and potential future zero-knowledge integrations are under active development and not yet production-ready.
- **Governance Risks** – In its early phase, ProofMatter is stewarded by SPO Consulting GmbH. The transition to decentralized governance will require broad community participation and may face challenges such as low voter turnout, concentration of voting power, or delays in decision-making.
- **Market and Adoption Risks** – The long-term success of ProofMatter depends on adoption by enterprises, regulators, and developers. If adoption is slower than anticipated, or if regulatory frameworks such as MiCA evolve in ways that create additional compliance burdens, this may limit growth.
- **Operational Risks** - Off-chain validation depends on third-party availability and jurisdictional rules. Spot-check coverage may vary; absence of an attestation does not invalidate an on-chain proof, but reduces assurance level.
- **Regulatory Uncertainty** – Future legal frameworks across jurisdictions may diverge, creating uncertainty around compliance, cross-border data handling, or recognition of on-chain proofs.

Acknowledging these risks reflects the project's commitment to transparency and realism. ProofMatter is not immune to challenges, but it is designed to adapt, evolve, and improve as the ecosystem matures.

Disclaimer

This document is not a prospectus, investment solicitation, or securities offering. It is a technical and functional description of the ProofMatter protocol and of the role of UBT within it.

Participation in the protocol involves the use of blockchain technology, which carries inherent risks, including but not limited to:

- market volatility,
- changes in the regulatory environment,
- and potential technical vulnerabilities.

Nothing in this document should be interpreted as financial advice, price prediction, or a guarantee of future performance. Participation in ProofMatter is entirely voluntary, and users should conduct their own due diligence before engaging with the protocol.

ProofMatter builds on UBT – a proven token with fixed supply – and is designed to be transparent, utility-driven, MiCA-aligned, and non-custodial by design.

From Unibright Framework to ProofMatter — An Eight-Year Evolution

An Evolution, not an Invention

ProofMatter is not a spontaneous invention. It is the result of an eight-year journey that began with the Unibright Framework in 2018 — one of the earliest attempts to bring enterprise processes onto blockchain infrastructure.

As the original Unibright Whitepaper from 2018 put it:

"The Unibright Framework is the first unified approach to blockchain-based business integration, providing templates, connectors, lifecycle management and explorers to make blockchain technology usable for enterprises."

These ideas were visionary. They foreshadowed what would become today's demand for verifiable execution: transparent, cryptographic evidence that something has truly happened.

Unibright Innovations

Across these past eight years, each Unibright phase contributed tangible intellectual property, tested new business models, and produced concrete lessons that ultimately shaped the design of ProofMatter.

The progression from early visual modeling to verifiable execution reflects not only technological advancement, but also the organizational and regulatory realities of bringing blockchain into enterprise environments.

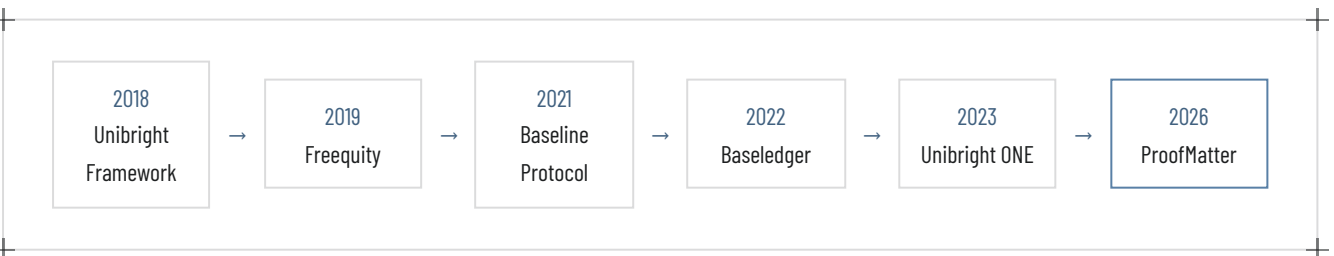


FIG. 14 — EIGHT YEARS OF ENTERPRISE BLOCKCHAIN INFRASTRUCTURE, DISTILLED INTO PROOFMATTER

The Unibright Framework (2018)

The Unibright Framework introduced five major building blocks:

- **Visual Templates** — drag-and-drop workflows for defining blockchain logic.
- **Contract Lifecycle Manager** — automatic deployment and management of smart contracts.
- **Connector** — integration layer to connect ERP systems like SAP.

- **Explorer** — dashboard for monitoring workflows and states.
- **Token (UBT)** — the Unibright Token as the gateway to framework usage.

With this ambitious vision, enterprises could model entire workflows visually, deploy them across blockchains, and monitor them in one unified system. The platform successfully went live late 2018.

Assets / Intellectual Property

Automatic smart-contract code generation from visual templates; graphical modeling tools that made complex blockchain concepts accessible to non-technical users.

Lessons Learned

- Graphical abstraction proved excellent for education and adoption, but less effective for real enterprise integration.
- While numerous proof-of-concepts were built, large corporations remained hesitant to operationalize an entirely new technology stack.
- The experience demonstrated that visual modeling can open minds—but APIs, standards, and measurable utility are what open budgets.

Freequity Tokenization Platform (2019)

In 2019, Unibright expanded into tokenization and DeFi with the launch of the Unibright Freequity platform, a full-stack 360° solution for token issuance, liquidity management, and compliance. Freequity enabled enterprises to issue tokens, establish regulatory-compliant platforms, and integrate issuance, trading and token-market processes into existing system landscapes. In February 2021, Unibright integrated with the Hedera Token Service (HTS) to scale asset tokenization for enterprises.

Assets / Intellectual Property

Automated token and NFT issuance, bonding-curve mechanics, real-time caches and limits operating above blockchain layers—technologies enabling time-critical tokenization.

Lessons Learned

- Technological innovation moved far faster than regulation.
- Despite technical readiness for on-chain financial instruments, the legal frameworks for security tokens and decentralized markets evolved slowly.
- Freequity proved that infrastructure alone is not enough; compliance readiness and regulatory dialogue are part of the product.

The Baseline Protocol (2021)

By 2021, Unibright was deeply engaged with the open-source Baseline Protocol, a standard developed by industries (including Microsoft, EY and ConsenSys) for multi-party business process synchronization via public blockchains with privacy guarantees. Unibright contributed its enterprise

integration expertise and architecture to this ecosystem, was voted into the Technical Steering Committee of the Oasis governance body, aligning the Framework and Freequity platforms with standardized workflow-notarization and zero-knowledge techniques.

Assets / Intellectual Property

- Concepts and implementations later known as SyncTree and TrustMesh—techniques for masked Merkle disclosure and multi-party verification.
- Collaborative standardization with partners such as EY, Microsoft, and ConsenSys validated the soundness of these ideas.

Lessons Learned

- Working within a standards body ensures conceptual rigor, but it slows time-to-market.
- Different strategic interests among contributors made rapid productization difficult.
- ProofMatter inherits the intellectual depth of these discussions but applies it in a leaner, executable form.

Baseledger (2022)

In 2022, Unibright launched its enterprise blockchain offering, Baseledger, designed explicitly for baselined processes and multi-chain workflow anchoring. Baseledger aims for cost-efficient, regulatory-compliant proof anchoring for enterprise workflows, providing a foundation for the next generation of process synchronization. These concepts were validated in early pilots, including a proof-of-concept with the European Investment Fund (EIF), where multi-level approvals and selective disclosure were tested in a regulated financial environment.

Assets / Intellectual Property

- A dedicated L2 infrastructure using roll-ups, deterministic bridging, and a credit system for representing and validating off-chain data through on-chain proofs.

Lessons Learned

- Operating a proprietary blockchain introduces vendor-lock-in and diverts focus from innovation to infrastructure maintenance.
- Running the ledger itself made clear that differentiation lies not in hosting consensus, but in defining verifiable execution above it.
- This insight directly inspired ProofMatter's bridgeless-credit architecture.

Unibright ONE (2023)

In 2023, Unibright publicly launched Unibright ONE, a service-oriented platform for enterprise-grade multichain and multiparty synchronization under optional zero-knowledge protection. Unibright ONE offers REST-API integration with ERP systems, workgroup management, access to

multiple notarization chains (Baseledger, Ethereum, Polygon, Bitcoin) and pay-per-use UBT or fiat payment models. It represents the culmination of the Framework + Freequity + Baseline + Baseledger evolution—now available as a ready-to-use service for enterprises.

Assets / Intellectual Property

- Blockchain-agnostic API layer, ERP-system integration, and a fiat-payment gateway enabling enterprises to consume blockchain functionality as a service.

Lessons Learned

- This architecture works in practice and forms the natural bridge to ProofMatter.
- Unibright ONE confirmed that enterprises want blockchain as a background component—an assurance layer, not a selling point.

Overarching Insights

From these phases, several cross-cutting lessons emerged that directly informed ProofMatter's design:

- **Abstraction was too high.**
Enterprises were not ready to adopt blockchain through drag-and-drop modeling. They required simple APIs and composable standards, not full workflow designers.
- **Atomic use cases outperform full-stack reinvention.**
Focusing on single, verifiable actions—such as proving a license, shipment, or certification—delivers faster adoption and clearer ROI.
- **Direct utility is essential.**
Token models succeed only when the asset is inseparably linked to protocol usage. The Unibright Framework hinted at this; ProofMatter realizes it: every proof consumes UBT through credits.
- **Perception matters.**
"Crypto" reputation can complicate enterprise sales. It is more effective to deliver classic integration and consulting projects where blockchain serves as the enabling layer rather than the headline.

Together, these anchors form the experiential foundation of ProofMatter: a protocol that distills eight years of enterprise blockchain learning into a minimal, verifiable, and economically aligned infrastructure for proof-of-execution.

ProofMatter doesn't just inherit the Unibright foundation — it fulfills its promise. From workflows to proofs, from abstraction to execution, from vision to standard.

Glossary

A2A (Agent2Agent Protocol)

An open communication standard announced by Google in April 2025 that enables AI agents built by different vendors to discover and communicate with each other. A2A defines how agents exchange capability manifests and task messages, but does not provide action verification or accountability. ProofMatter operates as an A2A Verification Agent, providing trusted third-party attestation for agent-to-agent interactions.

Action Proof

A cryptographically signed record of an event or action, generated by a Proof Service and anchored on-chain.

Attestation

A signed, timestamped statement referencing a proof ID and the applied spot-check policy, used to increase assurance about real-world execution.

Batch Poster

A component of the Optimism rollup stack that submits compressed batches of L2 transactions to Ethereum.

Bridgeless Credit System

Mechanism in ProofMatter where UBT deposits on Ethereum automatically issue usage credits on Optimism via native messaging, eliminating the need for manual token bridging.

C2PA (Coalition for Content Provenance and Authenticity)

An open technical standard governed by the Linux Foundation, with founding members including Adobe, ARM, Intel, Microsoft, and Truepic. C2PA defines Content Credentials — cryptographic metadata attached to media files that record creation context, origin, and provenance. ProofMatter extends C2PA with blockchain-anchored timestamps, a decentralized Trust Registry, and AI workflow provenance assertions.

CSRD — Corporate Sustainability Reporting Directive (EU)

EU directive that mandates standardized sustainability reporting for large and listed companies. Relevant to ProofMatter because proofs can map to required evidence fields for audit-ready disclosures.

CBAM — Carbon Border Adjustment Mechanism (EU)

EU mechanism that applies a carbon price on certain imports based on embedded emissions. Relevant to ProofMatter for verifiable reporting of emissions data and supply-chain events.

Content Credentials

Structured metadata attached to digital content that describes who created it, when, and with what tools. Signed with X.509 certificates. ProofMatter anchors Content Credentials on-chain and adds AI workflow provenance via the pm.ai-workflow assertion type.

DAO (Decentralized Autonomous Organization)

A decentralized governance structure where decisions are made collectively by token holders, typically via on-chain or Snapshot voting.

Digital Product Passport (DPP)

An EU regulatory mandate (Regulation (EU) 2024/1781) requiring verifiable, machine-readable product information for batteries, textiles, electronics, and further categories progressively from 2027. ProofMatter provides the tamper-proof verification layer for DPP data, enabling role-based selective disclosure via SyncTree — consumers, recyclers, and regulators each see only the fields relevant to their role.

ESG — Environmental, Social, and Governance

Umbrella term for non-financial performance factors used by investors, regulators, and companies. Relevant to ProofMatter because many ESG claims (e.g., carbon, labor, governance processes) require verifiable, audit-ready evidence.

EU AI Act

Regulation (EU) 2024/1689. Risk-based regulation for AI systems in the EU. ProofMatter is infrastructure, not an AI system, and therefore does not bear AI Act obligations itself. However, ProofMatter enables customers to satisfy their own AI Act compliance requirements — particularly record-keeping (Article 12), transparency (Article 13), and the Article 50 obligation to mark AI-generated content.

Execution Node

The part of an Optimism-based rollup that processes transactions and maintains the chain state.

Explorer

A public dashboard in ProofMatter that displays proofs, validator participation, UBT burns, credit balances, and governance activity.

Federated Learning (FL)

A machine learning approach where multiple participants (e.g., hospitals, banks, mobile devices) collaboratively train a shared model without sharing their private data. Each participant trains locally and submits only gradient updates. ProofMatter integrates with the Flower Framework to provide cryptographic Proof-of-Computation for each training round.

Flower Framework

The most widely adopted open-source Federated Learning framework, developed at the University of Oxford and maintained by Flower Labs. Framework-agnostic (supports PyTorch, TensorFlow, JAX, and others). ProofMatter integrates as a Flower Custom Strategy Plugin, adding blockchain-based accountability without modifying the underlying FL logic.

Governance

The process by which UBT holders propose and vote on changes to the protocol, including template standards, fee ratios, and treasury allocations.

Hybrid Validation

Combination of on-chain proof templates and optional off-chain spot checks.

Layer 1 (L1)

The base blockchain, in ProofMatter's case Ethereum, used for final settlement and token custody.

Layer 2 (L2)

A scaling solution built on top of Ethereum that processes transactions more efficiently while anchoring security back to L1.

MCP (Model Context Protocol)

A client-server protocol introduced by Anthropic in November 2024 that enables AI agents (Claude, GPT, Gemini, and others) to call external tools via JSON-RPC 2.0. ProofMatter operates as an MCP Server, exposing three tools: `attest_action`, `verify_attestation`, and `get_trust_score` — enabling any MCP-compatible AI agent to create and verify on-chain attestations natively.

Merkle Proof

A cryptographic proof that verifies the inclusion of specific data within a larger dataset, using a Merkle or Sparse Merkle Tree.

MiCA (Markets in Crypto-Assets Regulation)

The EU regulatory framework, effective 2024, defining rules for utility tokens, stablecoins, and crypto service providers.

Proof Contract

A lightweight smart contract deployed on Optimism to anchor proofs, verify structure and signatures, and emit transparent events.

Proof Credits

Unit of usage inside ProofMatter, backed by UBT deposits. Proof creators consume credits when generating proofs; validators earn from credit distribution. Credits are issued automatically on L2 via the bridgeless credit system, ensuring a direct utility link to UBT.

Proof-of-Execution (PoX)

ProofMatter's core concept: the ability to prove that an action was actually executed, not just recorded as a transaction.

Proof Service

A client library or hosted module that generates proofs from real-world actions and submits them to Proof Contracts.

RFC 3161 (Trusted Timestamp)

An IETF standard for trusted timestamps issued by accredited Timestamp Authorities (TSAs). ProofMatter obtains RFC 3161 timestamps for blocks containing proof events, providing legal recognition under the EU eIDAS regulation. Combined with blockchain anchoring, this dual approach makes ProofMatter proofs both cryptographically verifiable and designed for evidentiary robustness.

Selective Disclosure

The ability to reveal only specific fields of a proof while keeping other information private, enabled by Merkle structures.

Sequencer

The Optimism component that orders transactions and produces blocks for the rollup.

SyncTree

Masked Merkle structure enabling selective disclosure; ProofMatter's efficient alternative to zero-knowledge proofs.

Template

A standardized schema defining how a proof should be structured and validated, ensuring consistency and interoperability.

Template Hub

A planned module of ProofMatter where templates can be discovered, rated, reused, and monetized by developers.

Trust Level (L1-Lx)

Assurance grades assigned to proofs depending on how many parties/validators confirmed them.

TrustMesh

Graph model of proofs, approvals, and rejections; represents multi-party workflows as a verification graph.

UBT (Unibright Token)

The native utility token of ProofMatter, used for access, staking, burns, validator rewards, and governance.

Validator

A participant that stakes UBT to secure the system by verifying proofs, earning rewards for honest behavior. A validator may perform off-chain spot checks and issue signed attestations linked to a ProofMatter proof.

Verification Graph

The network of nodes (proofs) and edges (attestations) that define assurance depth in ProofMatter.

References

EU Regulations & Standards

- European Commission. (2023). Corporate Sustainability Reporting Directive — Directive (EU) 2022/2464.
- European Union. (2023). Markets in Crypto-Assets (MiCA) — Regulation (EU) 2023/1114.
- European Union. (2023). Carbon Border Adjustment Mechanism (CBAM) — Regulation (EU) 2023/956.
- European Commission. (2023). European Sustainability Reporting Standards (ESRS) — Commission Delegated Regulation (EU) 2023/2772.
- European Union. (2024). Artificial Intelligence Act (AI Act) — Regulation (EU) 2024/1689.
- European Union. (2024). Ecodesign for Sustainable Products Regulation — Regulation (EU) 2024/1781. (Digital Product Passport mandate)
- European Union. (2023). EU Deforestation-free Regulation (EUDR) — Regulation (EU) 2023/1115.

AI Infrastructure & Protocols

- Anthropic. (2024). Model Context Protocol (MCP) — Specification v1.0.
- Google. (2025). Agent2Agent Protocol (A2A) — Open Specification.
- Agentic AI Foundation (AAIF). (2025). Charter and Technical Roadmap. Linux Foundation.
- Beutel, D. J., et al. (2020). Flower: A Friendly Federated Learning Framework. University of Oxford / Flower Labs.
- C2PA. (2024). Coalition for Content Provenance and Authenticity — Technical Specification v2.1. Linux Foundation Joint Development Foundation.

Assurance & Accounting

- IAASB. (2013, rev.). ISAE 3000 (Revised): Assurance Engagements Other than Audits or Reviews of Historical Financial Information.
- IAASB. (2012). ISAE 3410: Assurance Engagements on Greenhouse Gas Statements.
- World Resources Institute & WBCSD. (2015). GHG Protocol: Corporate Accounting and Reporting Standard (Revised Edition).

Cryptography & Zero-Knowledge

- Merkle, R. (1989). A Digital Signature Based on a Conventional Encryption Function. In: Advances in Cryptology—CRYPTO '89.
- Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., & Virza, M. (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin. IEEE S&P.
- IETF. (2001). RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
- European Union. (2014). eIDAS Regulation — Regulation (EU) No 910/2014 on electronic identification and trust services.

Blockchain, Rollups & Attestations

- Buterin, V. (2021). An Incomplete Guide to Rollups. Ethereum Foundation Blog.

- Optimism Collective. (2025). OP Stack Documentation.
- W3C. (2022). Verifiable Credentials Data Model v2.0.
- Ethereum Attestation Service (EAS). (2024). Protocol Documentation.
- EIP-712. Ethereum Typed Structured Data Hashing and Signing.
- EIP-4844. Shard Blob Transactions (Proto-Danksharding).

Comparable Systems & Oracles

- Hedera. Hedera Consensus Service (HCS) Documentation.
- Protocol Labs. Filecoin Specification.
- Arweave. Arweave Yellow Paper.
- Chainlink. Proof of Reserve — Documentation.

Energy & Reporting Context

- International Energy Agency (IEA). (2024). Tracking Clean Energy Progress — CO₂ Monitoring.

Project History

- Unibright. (2018). Unibright Whitepaper: The Unified Framework for Blockchain-Based Business Integration.
- Baseledger. (2021). Baseledger Whitepaper — GDPR-Compliant Blockchain for Enterprises.

Context & Research

- Allied Market Research. (2023). ESG Reporting Software Market: 2023–2030.
- MarketsandMarkets. (2023). Testing, Inspection, and Certification (TIC) Market: Forecast to 2030.
- Statista. (2024). Digital Certification Market Size (2018–2030).
- Grand View Research. (2024). Digital Identity Solutions Market Size Report (2024–2032).
- MarketsandMarkets. (2024). Federated Learning Market: Global Forecast to 2030.
- Precedence Research. (2024). Autonomous AI Agents Market Size Report (2024–2034).
- World Steel Association. (2024). Climate Action in the Steel Industry — CO₂ Data Collection.