TrustLogic

TRUSTLOGIC WHITE PAPER

A Dual-Token Architecture for Enforceable Digital Agreements

A Protocol Framework for Governed, Revocable, and Compliant Digital Rights Across IP, Finance, and AI Systems

Abstract

Digital assets have transformed how value is transferred and recorded, but they remain limited in their ability to encode and enforce the rights and obligations that govern real-world economic relationships. Tokens today operate primarily as bearer instruments—transferable, composable, and resistant to censorship—yet incapable of enforcing conditions such as royalties, usage restrictions, time-bound access, licensing terms, or revocable permissions. These limitations prevent blockchain systems from supporting high-value use cases across finance, entertainment, artificial intelligence, public-sector distribution, and enterprise environments.

TrustLogic introduces a protocol-level trust primitive enabling **conditional, revocable, and enforceable digital rights**. Through a dual-token architecture that separates **authority** (Trustee Token) from **rights** (Beneficiary Token), TrustLogic provides an enforceable, programmable framework consistent with legal, regulatory, and contractual requirements. A dedicated **Revocation Engine**, multi-wallet custody layer, and privacy-preserving identity design ensure that obligations remain enforceable across chains, marketplaces, and custodial environments—even in adversarial conditions.

This white paper presents the conceptual foundations, expanded threat model, architecture, and applications of TrustLogic. It demonstrates how enforceable rights unlock new possibilities for RWAs, CBDCs, creator royalties, AI dataset licensing, insurance claims, contractor payments, programmable banking, humanitarian aid, and public-goods provisioning.

Executive Summary

Digital assets are programmable, but they are not enforceable. Current token standards behave like bearer instruments—freely transferable, easily wrapped, and impossible to revoke or condition once issued. Marketplaces can ignore royalty logic, custodians can bypass restrictions, and tokens cannot enforce licensing terms, territorial limits, derivative permissions, purpose-bound spending, or compliance requirements. These gaps prevent Web3 systems from supporting real-world IP licensing, regulated finance, AI dataset governance, enterprise access control, or public-sector payment programs.

TrustLogic introduces enforceability as a protocol primitive by separating authority from rights.
The **Trustee Token** encodes authoritative rules—licensing terms, transfer constraints, royalties, revocation triggers, and compliance conditions. The Trustee's power is constrained by on-chain, time-delayed governance updates and subject to review by pre-defined judicial/arbitration panels, ensuring non-arbitrary enforcement.
The **Beneficiary Token** is a revocable, soulbound representation of the user's rights.
Transfers occur only through trustee-validated burn-and-mint, ensuring that obligations follow rights everywhere.

Identity and compliance are handled entirely off-chain by the Application Layer, which uses external KYC providers and passes only minimal, non-PII attributes into the trustee environment. This provides real-world compliance without exposing personal data or binding identity to transaction keys.

A dedicated enforcement environment surrounds the Trustee Token, allowing the trustee to suspend, revoke, modify, or restore rights based on rule violations or authenticated external signals. Optional expert panels provide domain-specific adjudication for complex licensing or regulatory disputes.

This architecture enables enforceable rights across asset categories that current token systems cannot govern—creative IP, AI datasets and model rights, software access, ticketing, purpose-bound payments and CBDCs, insurance claims, contractor milestones, stock options, enterprise entitlements, and existing ERC-20/721/1155 assets. Because enforcement occurs at the authority layer, TrustLogic integrates with existing ecosystems while ensuring that rights remain inseparable from obligations.

By embedding rule evaluation, revocation, and identity separation directly into the protocol layer, TrustLogic provides institutions, creators, and users with what Web3 has lacked: predictable, governed, and compliant digital rights that can be trusted across chains, marketplaces, and custodial environments.

TRUSTEE IS A FEATURE, NOT A BUG

TrustLogic does not aim for trustlessness. It digitizes and miniaturizes existing legal trustees that already control masters, stock options, insurance claims, CBDC accounts, humanitarian funds, etc. The risk profile is the same or lower than today.

Table of Contents

WHITE PAPER

1. Introduction

While blockchain systems have significantly reduced transaction costs and enhanced auditability, they lack native mechanisms to enforce obligations associated with digital assets. Smart contracts can encode rules but cannot compel compliance in adversarial or cross-platform environments. Marketplaces may ignore intended logic, wrappers can bypass restrictions, and tokens cannot revoke or update rights in response to misuse.

This architectural limitation prevents blockchains from supporting use cases that rely on **conditional, revocable, or purpose-bound rights**, such as:

- royalty guarantees for creators
- non-scalpable ticketing
- purpose-restricted aid or remittances
- insurance claims with fraud prevention
- enterprise licensing and source-code access
- AI training data governance
- stock-option vesting and revocable entitlements
- CBDC systems requiring privacy and compliance

TrustLogic introduces a structural solution grounded in legal trust models: **separate control from use**. Authority is held in one layer; rights are issued in another. This separation enables tokens to behave as enforceable agreements, not just transferable objects.

Risk / Property	Traditional Trust Systems Today	Bearer token / NFT	TrustLogic + registered trustee
Issuer/label can revoke on misuse	Yes	No	Yes
User loses seed phrase	Usually recoverable	Permanent loss	Recoverable via trustee + ID
Marketplace disables royalties	Already happening	Yes	Impossible
Government freeze order	Routine	Very hard	Instant
Wrapping bypass	N/A	Easy	Impossible

Table 1 – Comparison between Traditional Trust Systems, Existing Token Systems, and TrustLogic

2. Background: Why Enforceability Fails in Digital Assets

Digital asset systems were designed around the concept of freely transferable bearer instruments. While this architecture supports open markets and frictionless exchange, it also creates structural barriers to enforcing obligations, rights, or conditions. Traditional legal and financial systems depend on custodians, trustees, and enforceable agreements. By contrast, most blockchain assets lack the primitives required to govern rights or revoke entitlements once transferred. The limitations described below explain why current token standards cannot support institutional licensing, regulated finance, enforceable royalties, compliant CBDCs, or governed access to AI datasets.

BEARER INSTRUMENT CONSTRAINTS

Most tokens function like digital cash: whoever holds them controls them. Because the same token represents possession, ownership, and authority, all rights collapse into a single fragile object. Once a token is transferred, the issuer loses all control over how it is used, where it moves, or whether contractual restrictions are followed. This bearer model is fundamentally incompatible with systems that require enforceable obligations or conditional rights.

LACK OF TRUSTEE OR CUSTODIAL AUTHORITY

Legal systems rely on trustees, custodians, and fiduciaries to enforce rules and manage assets on behalf of beneficiaries. Conventional token standards provide no equivalent construct. There is no layer that can enforce licensing restrictions, revoke rights upon breach, manage access boundaries, or guarantee compliance. Without an authority layer, obligations cannot bind the asset as it moves between holders.

MARKETPLACE SOVEREIGNTY

Digital marketplaces operate independently of token issuers. They can decide whether to honor embedded royalty logic, transfer restrictions, or licensing constraints. In practice, many marketplaces disable or ignore these mechanisms to boost liquidity. When a platform can freely choose whether to enforce rights, creators and institutions cannot rely on token-level guarantees.

WRAPPING AND BYPASS MECHANISMS

Blockchain ecosystems support wrapping, meta-assets, and derivative tokens that can override or strip embedded restrictions. Once an asset is wrapped, the wrapper contract may ignore royalties, disable transfer checks, or issue unrestricted derivatives. Wrapped assets then circulate without obligation, breaking the continuity of rights and making enforcement impossible.

IDENTITY–TRANSACTION COUPLING IN CBDCS

Most CBDC pilot architectures bind user identity directly to transaction keys or wallets. This coupling exposes transaction histories to issuers and intermediaries, undermining privacy and creating public distrust. At the same time, decoupling identity from transactions without an enforcement mechanism weakens AML and compliance controls.

ABSENCE OF NATIVE REVOCATION

Traditional token standards do not support revocation or reversion. Once a token is transferred, it cannot be reclaimed or invalidated in cases of breach, fraud, misuse, regulatory violation, or expiration. Without native revocation, it is impossible to enforce licensing terms, retract rights, prevent misuse of datasets, or support conditional or purpose-bound financial flows.

2.1 Asset Categories TrustLogic Can Manage

TrustLogic is designed to govern rights across a wide spectrum of digital, financial, and real-world assets—regardless of whether those assets are on-chain, off-chain, custodial, or non-custodial. Because TrustLogic separates **authority** from **user-held rights**, the protocol can enforce obligations even when the underlying asset is not directly held or controlled by the trustee (e.g., songs, videos, datasets).

TrustLogic can manage rights for the following asset categories:

CREATIVE ASSETS

- songs, stems, master recordings
- video, film, raw footage
- digital art, written works, design files
- characters, models, animations

SOFTWARE & TECHNICAL ASSETS

- source code access
- internal tools and documentation
- development/build environments
- confidential technical materials

AI ASSETS

- training datasets
- fine-tuning datasets
- model weights
- inference rights
- lineage-aware derivative model governance

FINANCIAL & ECONOMIC RIGHTS

- purpose-bound payments
- CBDC spending authority
- conditional stablecoin transfers
- milestone-locked contractor payments
- escrowed or time-bound financial instruments

BUSINESS, LEGAL & INSTITUTIONAL RIGHTS

- stock options, vesting schedules, repurchase rights
- insurance claims and reimbursement rights
- certifications, credentials, admission rights

- governable subscription or membership access

TOKENIZED OR HYBRID DIGITAL ASSETS

- ERC-20, ERC-721, ERC-1155 tokens
- RWAs and tokenized ownership claims
- registry-based IP tokens (e.g., Story Protocol)
- cross-chain representations of rights

By decoupling rights from custody and enforcing obligations through a dedicated authority layer, TrustLogic can unify rights management across all these categories. The protocol provides enforceability where current token standards cannot—particularly in industries where rights must remain conditional, revocable, or compliant with contractual and regulatory frameworks.

2.2 Why Enforceability Fails

Taken together, these limitations reveal a fundamental architectural gap: digital assets lack a mechanism to separate authority from rights. As long as assets behave as bearer instruments without custodial governance or revocable entitlements, tokens cannot model the obligations and constraints that underpin real-world legal, financial, creative, and regulatory systems.

3. Threat Model

Digital asset ecosystems operate within complex economic, technical, and institutional environments. In such environments, even small deviations from intended behavior can generate significant downstream effects. This section outlines the adversarial behaviors, incentive misalignments, and structural vulnerabilities that TrustLogic is designed to mitigate. Each threat is presented with (1) a brief Summary and (2) a detailed explanation of how it manifests in real-world systems.

3.1 Marketplace Non-Compliance

Summary: *Marketplaces may ignore or override the rules embedded in smart contracts when those rules conflict with platform incentives.*

Blockchains allow developers to encode terms such as royalties, transfer restrictions, or usage conditions within smart contracts. However, these obligations are not self-executing. When a marketplace intermediates a transaction, the marketplace chooses which contract functions to call—or not call. The 2022–2023 royalty dispute between OpenSea and Blur illustrated this sharply: both platforms selectively disabled creator royalty enforcement to attract liquidity. Smart contracts that were believed to be immutable failed to produce the expected economic outcome because enforcement depended on marketplace cooperation. This reflects a fundamental misalignment: platforms optimize for transaction volume, not for contract fidelity. Without an authority layer, creators and rights-holders lack the means to ensure compliance across markets.

3.2 Wrapping-Based Rule Evasion

Summary: *Attackers can use wrapper contracts to circumvent embedded restrictions, creating derivative tokens with no obligations attached.*

Token wrapping allows users to encapsulate an asset within a new smart contract that exposes different functionality. While wrapping is a powerful composability feature, it also enables rule evasion. When a token with embedded royalty or transfer restrictions is wrapped, the wrapper—not the original token—becomes the transferable asset. The wrapper can simply omit the original restrictions, enabling unrestricted resale, avoidance of fees, or unauthorized reproduction of rights. Wrapping also undermines the ability to revoke rights, since the underlying asset is locked behind the wrapper. As a result, any enforceability encoded at the asset level can be rendered ineffective.

3.3 Unauthorized Resale and Ticket Scalping

Summary: *Economic actors exploit unrestricted transferability to circumvent pricing policies and resale constraints.*

In event ticketing, gaming assets, and limited-edition goods, token resale can distort prices and undermine policy objectives. Bots often acquire tickets at scale and resell them at inflated prices, harming fans, venues, and artists. Traditional NFT-based ticketing systems fail to prevent this behavior because transferability is unconditional and marketplaces prioritize liquidity over fairness. Even when

resale restrictions are encoded, users can circumvent them through wrappers or off-chain arrangements. The lack of enforceable transfer and pricing controls leads to speculation, exclusion, and reputational damage for event organizers.

3.4 Identity Leakage in Regulated Systems

Summary: *When identity and transaction authority are combined, financial systems risk exposing sensitive personal behavior.*

Regulated financial systems, especially CBDCs, require mechanisms for identity verification, sanctions screening, and compliance. However, if identity is encoded directly into transactional keys, every payment becomes traceable to an individual. Such designs introduce the possibility of pervasive surveillance, data breaches, and misuse of financial information. In many blockchain-based pilots, wallet addresses serve simultaneously as identity anchors and payment conduits, creating a structural privacy hazard. Without a separation layer, regulatory compliance and personal privacy cannot coexist.

3.5 Misuse of Directed Funds and Aid

Summary: *Once funds reach a recipient's wallet, they may be diverted or spent in ways that contradict the sender's intent.*

Humanitarian aid, public-sector distributions, scholarships, remittances, and other forms of directed funds depend on adherence to specified purposes. In traditional financial systems, intermediaries may monitor or condition disbursements. In blockchain systems, however, tokens cannot prevent misuse of funds once transferred. This creates risks that aid may be diverted, coerced, or spent fraudulently. The inability to encode purpose-specific restrictions or revoke access complicates oversight and reduces trust in digital distribution mechanisms.

3.6 Duplicate or Fraudulent Claims

Summary: *Insurance and entitlement systems are vulnerable to duplicate claims because no shared state registry exists across issuers.*

In insurance ecosystems, multiple carriers may issue overlapping coverage. Because claims are typically processed independently, users can submit the same claim to multiple providers. Tokenizing claims does not resolve this problem: if each carrier issues tokens independently, there is no canonical registry of claim state. This creates opportunities for double-claim fraud. Without a mechanism to ensure that only one valid rights token exists for a given claim, tokenization may accelerate—rather than mitigate—fraud.

3.7 Unauthorized Access to Software, Source Code, or Data

Summary: *Tokens granting access to code or data cannot enforce time limits, revocation, or usage constraints.*

In software development, code auditing, and AI training, granting access to sensitive materials must be reversible. Traditional digital access systems rely on central controls, time-limited credentials, and audit logs. Tokens, however, cannot revoke access once granted, nor can they enforce restrictions on copying or downstream use. A token representing access to a code repository or dataset is insufficient to prevent unauthorized retention or misuse. Without revocable permissions and usage monitoring, tokens cannot support secure access control.

3.8 Custodial Mismanagement

Summary: *Custodians may misuse, misallocate, or commingle assets if control is not segmented and monitored.*

Centralized exchanges and custodians have repeatedly demonstrated vulnerabilities associated with asset commingling, insufficient proof-of-reserves, and operational opacity. When custodial control is concentrated in a single wallet or contract, there is no technical barrier preventing misuse or fraud. In such systems, users depend entirely on the custodian's operational integrity. This exposes users to counterparty risk that blockchain systems are ostensibly designed to mitigate.

3.9 Key Loss and Irrecoverable Assets

Summary: *If keys are lost, assets become permanently inaccessible in the absence of a recovery mechanism.*

Self-custody offers autonomy but introduces irreversible failure modes. Lost private keys—whether due to user error, device failure, or coercion—lead to permanent loss of assets. Because traditional tokens lack a trustee or fiduciary role, there is no mechanism to reissue rights or recover misplaced entitlements. In regulated or institutional settings, this is unacceptable; users and entities require mechanisms for key recovery, identity verification, and asset reissuance under defined conditions.

3.10 Unauthorized Copying and Flight-to-Bearer

Summary: *Once a raw digital file is accessed, it can be copied and redistributed as an unrestricted bearer asset.*

Certain assets—such as song stems, video masters, datasets, source code, and 3D models—require users to access the underlying file in unencrypted form for legitimate use. When this occurs, nothing prevents the file from being duplicated and shared through uncontrolled channels such as file-sharing networks, cloud links, or private exchanges. After extraction, these copies circulate as pure bearer objects with no attached obligations or usage constraints. Anyone who obtains them can use, modify, or redistribute the asset without technical limitations, undermining exclusivity and enabling unmonitored downstream use. This risk reflects a longstanding structural vulnerability in digital media and software distribution: raw files, once exposed, can escape controlled environments and propagate indefinitely.

4. Architecture

TrustLogic's architecture is built around a simple but powerful principle: **separate authority from rights, and enforce all rights against a governed custodial boundary.**

Whereas traditional blockchain systems give users both the asset and the authority to act upon it, TrustLogic divides these functions into two distinct layers:

- The **Trustee Multi-Wallet**, which holds the underlying asset and the **Trustee Token** (the source of authority and rule enforcement).
- The **User Wallet**, which holds a **Beneficiary Token**, a soulbound, revocable representation of the rights derived from the underlying asset.

This separation enables enforceability, revocation, institutional compliance, and granular scope control—capabilities that bearer tokens and existing Web3 licensing systems cannot deliver.

To support this dual-token model, TrustLogic uses a modular architecture that places the Trustee Multi-Wallet at the center of the protocol, while surrounding it with identity, oversight, compliance, and application layers. These layers provide verification, dispute resolution, auditability, and user interaction without ever compromising the custody boundary that guarantees enforceability.

4.1 Architectural Overview

Figure 1 provides a high-level view of the TrustLogic architecture. It illustrates how assets, rules, and rights flow through the system, and how the protocol separates institutional authority from user-held entitlements.

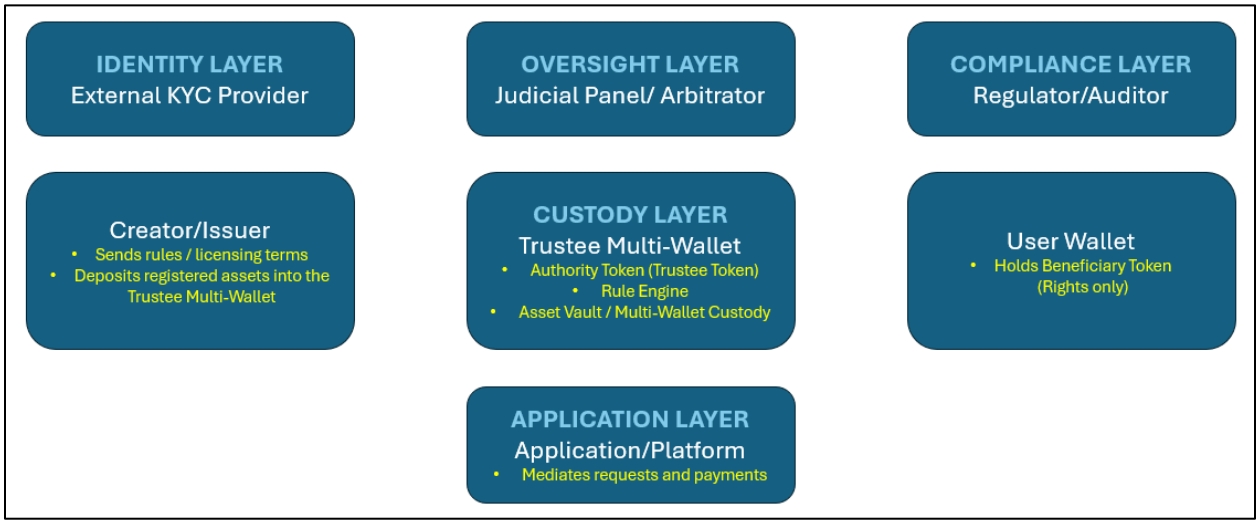

Figure 1. TrustLogic Static Architecture Overview

This figure depicts the six functional layers that form the TrustLogic protocol:

1. Identity Layer (External KYC Provider)

An independent verification provider performs KYC/AML checks and sends validated identity attributes to the Trustee Multi-Wallet.
The Trustee does not rely on self-attested identity data and never collects raw PII directly from users unless required for legal enforcement.

2. Oversight Layer (Judicial Panel / Arbitrator)

An external dispute-resolution body issues binding decisions when licensing terms, contractual conditions, or usage restrictions are contested.
These decisions are fed directly to the Trustee Multi-Wallet, which uses them to suspend, restore, or revoke rights.

3. Compliance Layer (Regulator / Auditor)

Regulators and auditors can access logs and compliance reports generated by the Trustee.
Because underlying assets never leave custody and all rights changes are logged, the system provides clear audit trails for financial, licensing, or data-use compliance.

4. Custody Layer (Trustee Multi-Wallet — *Authority + Custody*)

This is the core of the TrustLogic protocol.
The Trustee Multi-Wallet contains:

- **The Trustee Token (Authority Token)**, which encodes the governing rule set.
- **The Rule Engine**, which evaluates every transfer, access attempt, modification request, or revocation event.
- **The Asset Vault**, a multi-wallet custody system that holds all underlying assets in segregated sub-wallets.

Crucially, **users never hold underlying assets**.
All enforceability flows from this custody boundary.

5. User Wallet (Beneficiary Token Only)

Users hold only a **Beneficiary Token**, a revocable soulbound receipt representing their rights.
Rights may be:

- transferred (via burn-and-mint),
- suspended,
- expired, or
- revoked

depending on the trustee's evaluation of the rules and external attestations.

Users never take direct custody of the underlying asset, preventing wrapping attacks, unauthorized derivatives, mis-licensing, or marketplace bypass.

6. Application Layer (Platform / Interface)

The application (ticketing app, licensing marketplace, CBDC wallet, etc.) provides the UI and payment rails.
It mediates requests between the user and the trustee, but it does **not** hold authority and cannot override trustee-level enforcement.

Roles in the TrustLogic Architecture

To clarify how authority, rights, and identity flow through the system, TrustLogic relies on four distinct actors:

Creator/Original Owner: Defines the rules governing how the asset may be used, including licensing terms, transfer conditions, derivative permissions, and revocation criteria.

Application: Performs all required identity verification off-chain, constructs the rights and rule set, and mints both protocol tokens.

Trustee: Receives the **Trustee Token**, which encodes the authoritative rule set and grants the trustee the ability—and obligation—to enforce those rules throughout the asset's lifecycle.

User: Receives the **Beneficiary Token**, a revocable, soulbound representation of the rights granted to them under the encoded rules.

4.2 How the Dual-Token System Fits the Architecture

At the center of this architecture lies the **dual-token model**:

Trustee Token (Authority Token)

Lives exclusively inside the Trustee Multi-Wallet and controls:

- rule definition
- enforcement logic
- revocation
- dispute outcomes
- lifecycle transitions
- asset access gates
- derivative permissions
- territorial or time-bound usage rights

It is never visible to users and cannot be moved or wrapped.

Beneficiary Token (Revocable Soulbound Rights Token)

Lives exclusively in the User Wallet and represents conditional, governed, reissuable rights.

When rights transfer:

- the old Beneficiary Token is burned, and
- a new one is minted to the acquirer

—but only after the Trustee Token validates compliance with the governing rules.

This tight coupling between rights and authority is reflected structurally in Figure 1: rights flow outward to the user, while authority and custody remain centralized and governed.

5. Features

5.1 Lifecycle & State Machine

Every Beneficiary Token in TrustLogic follows a structured lifecycle defined by the rules encoded in the Trustee Token. Instead of representing a static state of "ownership," rights progress through a series of contractual stages that map directly to real-world entitlements. The Beneficiary Token is implemented as a **revocable, reissuable soulbound token**, ensuring that rights remain bound to the holder unless a trustee-approved transfer triggers a controlled burn-and-mint reissuance. These lifecycle transitions mirror the dynamics of licenses, claims, access rights, financial entitlements, and other governed permissions.

LIFECYCLE STATES

- **Creation** — Trustee Token rules instantiated; rights template defined.
- **Assignment** — Rights granted to a user via issuance of a soulbound Beneficiary Token.
- **Active** — Rights valid and exercisable under current contractual or regulatory conditions.
- **Transfer Attempt** — A user initiates a transfer; rights undergo rule evaluation by the trustee.
- **Re-Issuance** — The existing soulbound token is burned, and a new rights token is minted for the approved holder.
- **Suspended** — Rights temporarily disabled pending remediation, dispute resolution, or compliance review.
- **Revoked** — Rights permanently invalidated due to breach, fraud, misuse, or other rule violations.
- **Expired** — Rights conclude automatically upon reaching a time-bound or event-bound condition.

WHY THIS MATTERS

Traditional tokens collapse all stages into a single "ownership" state, making it impossible to enforce expiration, breach, remediation, conditionality, or other real-world contractual events. TrustLogic resolves this by introducing **stateful, governed rights** whose transitions are validated at each step.

In practice, a right may be temporarily suspended during a dispute, permanently revoked when misused, or allowed to expire when a contractual term ends. Because each state transition invokes a compliance check defined by the Trustee Token, the lifecycle becomes an active **enforcement surface** rather than a passive history. This aligns rights management with legal, commercial, and regulatory processes—something no traditional token standard is capable of providing.

5.2 Revocation Protocol

Revocation is a core component of enforceable digital rights. Traditional blockchain systems treat tokens as irrevocable bearer instruments—once held, they cannot be suspended, corrected, or retrieved even when misuse, breach, or fraud is detected. TrustLogic introduces a structured, governed revocation

system in which rights may be **paused**, **reviewed**, **modified**, **restored**, or **permanently revoked**, but never through automated or unilateral triggers.

In TrustLogic, external data sources—such as oracles, compliance services, or platform reports—**cannot revoke rights.** They may only **submit evidence** and, when authorized by the ruleset, **initiate a temporary pause** while a dispute is opened. Final decisions are made exclusively by the **trustee** or a **pre-defined judicial/arbitration panel** referenced in the Trustee Token.

Oracles are court clerks, not judges.
They deliver evidence; they do not determine outcomes.

REVOCATION MODES

- **Hard Revocation**
  Permanent termination of rights following a trustee or panel decision. Beneficiary Tokens remain burned or non-reissuable.
- **Suspension (Soft Revocation)**
  Temporary disabling of rights while a dispute, audit, or investigation is pending. Suspension may be triggered automatically, but final resolution requires a human-governed decision.
- **Conditional Revocation**
  Rule-defined conditions (e.g., territorial violations, expiration windows, milestone failures) may trigger a pause pending review.
- **Delegated Revocation (Human Triggered)**
  Authorized parties—such as creators, studios, banks, or insurers—may initiate a suspension or dispute, but cannot finalize revocation unless specifically granted that authority in the Trustee Token.

DISPUTE AND EVIDENCE HANDLING

Evidence may originate from:

- misuse reports submitted by rights holders
- oracle-delivered attestations (e.g., territorial use, dataset misuse)
- compliance or audit systems
- platform-level monitoring
- manual submissions

Regardless of source, the workflow is always:

1. **Event detected**
2. **Token paused**
3. **Dispute opened**
4. **Human decision**
5. **Outcome enforced**

This ensures that automated systems cannot seize or permanently alter rights and that all revocation outcomes map cleanly to legal and commercial expectations.

STRUCTURED REVOCATION FLOW

Figure 2 illustrates how revocation and restoration occur in a real-world scenario in which a film production studio licenses a song and later misuses it outside the licensed scope. The rights holder submits a misuse report, triggering a pause and a formal dispute review. A judicial/arbitration panel issues a binding decision, which the trustee enforces.

Flow Steps

1. **License Request** initiated through the licensing platform.
2. **License Issuance** granted by the trustee according to the encoded terms.
3. **Payment** routed to the creator or rights holder.
4. **Royalty Accrual/Distribution** when applicable.
5. **Misuse Report** submitted by the rights owner or authorized party.
6. **Token Suspension (Pause)** automatically triggered by the ruleset.
7. **Dispute Referral** to a judicial/arbitration panel.
8. **Binding Decision** returned by the panel (restore, modify, revoke).
9. **License Restoration, Modification, or Revocation** executed by the trustee.
10. **Compliance Logging** for audit, reporting, and institutional review.

This structured path ensures that rights never remain active during a dispute, rights holders can act quickly to protect assets, and licensees receive a fair, governed adjudication process.

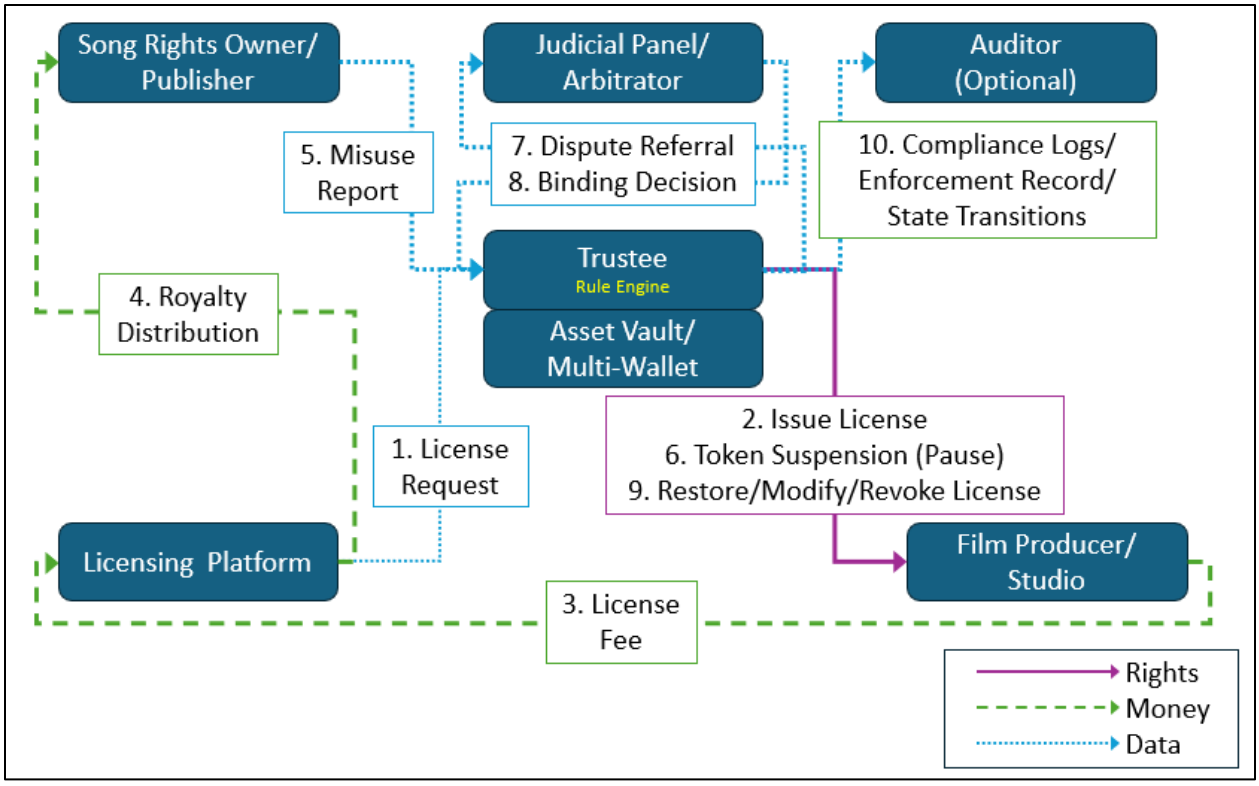

Figure 2 — Structured Revocation Flow (Licensing Misuse Example)

A film studio licenses a song, misuses it, triggers a misuse report, and enters a human-governed dispute process. The Beneficiary Token is paused automatically, a judicial/arbitration panel issues a binding ruling, and the trustee executes the final outcome—restoration, modification, or revocation—followed by compliance logging.

WHY THIS MATTERS

By preventing oracles from acting as judges and limiting them to evidence submission, TrustLogic enforces a clear separation between **data**, **process**, and **authority**. This avoids oracle-driven false positives, protects users against automated or adversarial revocation, and ensures revocation behaves like real-world contractual enforcement—deliberate, reviewable, and grounded in human judgment rather than automated triggers.

WHY THIS MATTERS

No existing token standard provides native support for revocation, suspension, or restoration. Licensing law, contract law, copyright enforcement, and financial regulation *all depend* on the ability to halt or reverse rights when misuse occurs. By embedding revocation as a core protocol primitive—and structuring arbitration and restoration paths—TrustLogic transforms digital rights from fragile, uncontrolled bearer tokens into enforceable contractual entitlements.

Revocation is no longer a hack layered on top of tokens; it becomes a **predictable legal mechanism encoded into the lifecycle of rights themselves**.

5.3 Multi-Wallet Custody Architecture

Enforceable digital rights require a clear separation between the underlying asset and the transferable entitlements associated with that asset. In most token standards, custody, ownership, and control are bundled together in a single bearer instrument. Once that token leaves its originating contract, the issuer loses the ability to enforce royalties, licensing terms, compliance rules, or revocation conditions. This architectural flaw makes it impossible to maintain control over assets in adversarial or multi-market environments.

TrustLogic introduces a multi-wallet custody architecture designed to keep underlying assets securely anchored to a designated authority while users interact with revocable rights derived from those assets. This structure eliminates the major failure modes found in traditional token systems and enables institution-grade governance and control.

THE LIMITATIONS OF SINGLE-WALLET CUSTODY

Most blockchain systems use a single contract or a single custodial wallet to store assets. This monolithic approach exposes issuers and users to several risks. Wrapping attacks become possible when an adversary locks an asset in a contract and issues new, unrestricted derivatives. Custodial mismanagement can occur when exchanges or platforms commingle assets or use customer-controlled tokens for internal operations. Once a bearer token moves off-platform, the issuer loses the ability to enforce royalties, licensing restrictions, use-scope limitations, compliance requirements, and revocation. Aggregated custody models also prevent asset-level auditing, making it difficult to satisfy regulatory or contractual reporting obligations.

SEGMENTED, TRUSTEE-CONTROLLED CUSTODY

To address these structural issues, TrustLogic uses a segmented custody model in which each asset—or asset group—is placed in its own dedicated sub-wallet under the control of the Trustee Token. Underlying assets never leave trustee custody. Instead, users receive Beneficiary Tokens that represent revocable rights, not physical ownership. Transfers occur through a burn-and-mint process that reassigns rights only after the trustee has validated compliance with the governing ruleset.

ENFORCEMENT ADVANTAGES OF SEGREGATED CUSTODY

This architecture provides several important enforcement benefits. Segregating custody prevents commingling and ensures that each asset can be governed independently. The trustee maintains immutable authority over rights, regardless of how they are used or where they attempt to move. All transfers and access attempts must pass through the trustee's rule evaluation, ensuring that unenforced or bypassed operations cannot occur. Sub-wallets allow granular, per-asset auditability and create clean boundaries for regulatory compliance. Because users can never extract or wrap underlying assets, all rule enforcement remains intact.

INSTITUTIONAL ALIGNMENT

Segmented custody aligns naturally with the expectations of regulated and rights-sensitive industries. Financial institutions benefit from FDIC- and OCC-compatible segregation. Entertainment studios gain the ability to maintain custody over digital assets in ways that reflect SAG-AFTRA and WGA contractual obligations. Public companies can maintain SOX-aligned audit trails, while regulated data environments

such as healthcare and research benefit from GDPR- and HIPAA-compatible access controls. Insurance providers and financial claims systems gain tamper-proof custody logs. CBDC issuers can maintain privacy-preserving transactional systems while preserving selective auditability.

WHY THIS MATTERS

Multi-wallet custody is the foundation of enforceable digital rights. If assets could be removed from the custody layer, wrapping attacks, marketplace bypass, resale manipulation, licensing violations, and irreversible misuse would become unavoidable. By ensuring that underlying assets remain under continuous authority control, TrustLogic transforms digital entitlements from fragile bearer tokens into governed, compliant, and enforceable rights suitable for institutional and public-sector environments.

5.4 Identity & Privacy Layer

Digital rights, licensing, and regulated transfers often require identity checks for creators, buyers, or both. However, embedding personal data directly into tokens or on-chain metadata is incompatible with privacy standards and exposes users to unnecessary risk. TrustLogic resolves this by handling identity verification entirely in the **Application Layer**, using an external KYC provider when required, and passing only *non-PII compliance attributes* into the Trustee Multi-Wallet.

In TrustLogic, identity is never stored on-chain and is never written into the Beneficiary Token unless explicitly configured by the application. Instead, the application validates identity off-chain, incorporates the minimal compliance references into the Trustee Token, and delivers fully vetted rights to the user. If identity verification fails at any point, the transaction ends at the application; no asset is deposited, no token is minted, and no information is forwarded to the trustee.

This model provides the level of privacy users expect, while giving platforms the flexibility to satisfy authorship verification requirements, AML/KYC obligations, high-value transaction checks, derivative-use restrictions, and regulatory standards without exposing private data.

IDENTITY FLOW BETWEEN APPLICATION, KYC PROVIDER, TRUSTEE, AND USER

Figure 3 shows how TrustLogic manages identity while ensuring that only compliant, verified rights enter the custody and enforcement layer. The Application orchestrates the entire identity process, while the trustee enforces rules *after* identity checks have already succeeded.

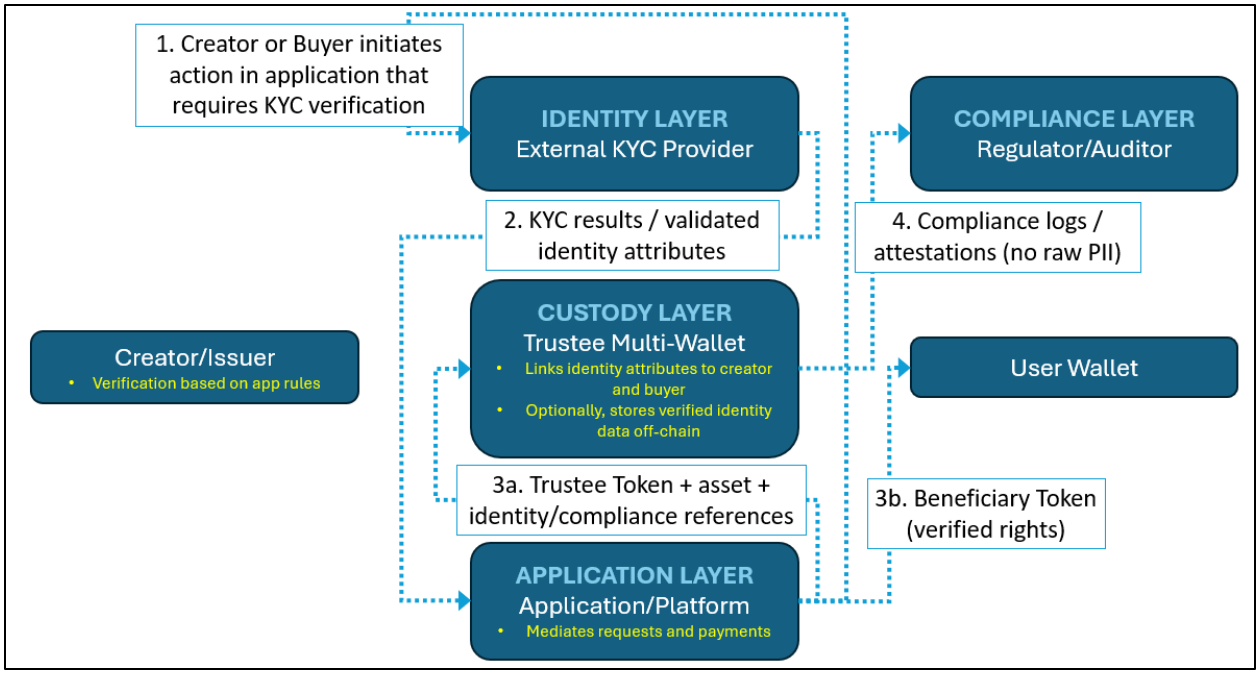

Figure 3. Identity and Compliance Data Flow

Step 1 — Identity Requirement Determined by the Application

When a creator registers an asset, or when a buyer initiates a rights purchase or high-value transaction, the **Application** checks its business rules to determine whether identity verification is required. Examples include:

- authorship verification for creative rights,
- high-value purchases (> $10,000),
- geographic restrictions,
- AML/sanctions checks,
- restricted-use licensing,
- eligibility for derivative permissions,
- rights restoration (e.g., lost/stolen wallet).

No on-chain or trustee involvement occurs until identity is resolved.

Step 2 — Application Sends Identity Data to External KYC Provider

The Application submits identity information to a third-party KYC provider for verification. This external provider performs:

- AML checks
- sanctions screening
- jurisdiction and residency validation
- age or eligibility verification
- creator authorship verification (when required)

The KYC provider returns only *validated identity attributes* to the application. Raw documents remain off-chain and never touch the trustee.

Step 3 — Application Receives Verification Results

The KYC provider sends back a pass/fail decision and any necessary compliance attributes (e.g., "US person," "AML Tier 2," "no sanctions flags").
If verification fails, the Application halts the transaction—**no Trustee Token is minted, and no Beneficiary Token is issued**.

Step 4 — Application Mints Trustee Token and Deposits It Into the Trustee Multi-Wallet

Once identity has been verified according to the application's rules, the Application:

- mints the **Trustee Token**,
- embeds only non-PII compliance references or hashed attributes,
- deposits the underlying asset into the Trustee Multi-Wallet, and
- transfers the Trustee Token to the same multi-wallet.

The Trustee Multi-Wallet now has all the information required to enforce rules later, without ever possessing sensitive user identity.

Step 5 — Application Issues the Beneficiary Token to the User Wallet

The Application mints the **Beneficiary Token** and transfers it to the buyer's wallet.
This revocable, soulbound token represents the user's rights, not their identity. It may contain:

- rights permissions
- versioning
- compliance flags (e.g., "verified purchase")
- derivative permissions

—but **no PII** unless explicitly configured.

Step 6 — Trustee Multi-Wallet Provides Compliance Evidence (When Required)

At any time—such as during disputes, audits, or licensing reviews—the Trustee Multi-Wallet can produce **compliance attestations** based on the Trustee Token and the application's logged identity checks.
These attestations confirm that identity verification was performed before rights were issued, without disclosing personal information.

This enables:

- regulator audits,
- dispute resolution,
- commercial licensing compliance,
- CBDC or AML jurisdictional proof,
- insurance or legal evidence,
- authorship confirmation,
- rights restoration after wallet loss.

WHY THIS MATTERS

Most blockchain systems treat identity as an afterthought, tying wallets to identity in ways that undermine privacy or failing to meet institutional requirements altogether. TrustLogic's identity model creates a clear separation of roles:

- **Application** — performs identity checks, interacts with KYC, and embeds compliance references in tokens.
- **External KYC Provider** — verifies identity and keeps PII off-chain.
- **Trustee Multi-Wallet** — enforces rights after identity is verified, stores only what is necessary for compliance.
- **User Wallet** — receives rights tokens with zero PII.

This structure meets the needs of:

- creative licensing (authorship verification, derivative restrictions),
- financial compliance (AML/CTF thresholds, high-value checks),
- enterprise governance (audit logs, revocation authorization),
- consumer protection (wallet loss recovery),
- privacy-preserving design (no PII on-chain), and
- regulatory reporting (attestations, not documents).

TrustLogic provides identity where required, privacy where expected, and enforceability where essential—without compromising on any of the three.

Privacy Guarantees. TrustLogic delivers transaction-graph privacy and ensures that no personally identifiable information (PII) ever appears on-chain. The protocol maintains stablecoin-grade metadata privacy by separating identity from transactional authority, and value or amount privacy is inherited from the underlying payment rail. When stronger confidentiality is required, TrustLogic can interoperate with existing privacy-preserving L2s and execution environments without modifying the core architecture.

5.5 TrustLogic Does Not Require Zero-Knowledge Proofs to Achieve Privacy

Zero-knowledge proofs (ZKPs) are powerful cryptographic tools, but they are not required for TrustLogic to guarantee privacy, compliance, or selective disclosure. TrustLogic achieves privacy through **structural separation of roles**, not through cryptographic obfuscation. By isolating identity, authority, and user-held rights into separate layers, the protocol prevents sensitive information from ever entering the on-chain enforcement environment.

Identity is verified entirely off-chain, using external KYC providers selected by the Application. Only minimal compliance attributes or hashed attestations—not personal data—are passed to the Trustee Token. The Trustee never receives raw PII, and no identifying information is embedded in the Beneficiary Token unless explicitly configured by the application.

This architecture provides the practical privacy guarantees that institutions and regulated entities require:

- compliance checks occur without exposing identity
- rights enforcement does not depend on knowing who the user is
- user wallets retain full transactional privacy
- regulators receive auditability only when legally required
- identity data never appears on-chain or in public metadata

TrustLogic can integrate ZKPs in the future for enhanced compliance attestations, but it does not depend on them. Privacy emerges from **role separation, off-chain verification, and minimal-information attestations**, ensuring compatibility with GDPR, HIPAA, financial-compliance rules, and institutional privacy expectations—without the complexity, cost, or performance tradeoffs associated with mandatory ZK proofs.

5.6 Cross-Chain Compatibility

Digital assets increasingly move across multiple chains, rollups, and execution environments—each with distinct rules, capabilities, and security guarantees. Most cross-chain systems treat tokens as freely portable bearer instruments, allowing assets to be wrapped, re-issued, or represented on other chains without preserving the restrictions or governance rules attached to the original asset. This flexibility creates opportunities for innovation but breaks enforceability: once assets leave their native environment, the rules governing rights, licensing, compliance, or revocation rarely travel with them. TrustLogic is designed to operate seamlessly across chains while maintaining strict governance continuity, ensuring that rights remain conditional and enforceable regardless of where they move.

A GOVERNANCE-ANCHORED CROSS-CHAIN MODEL

TrustLogic differentiates between authority and rights when operating in multi-chain ecosystems. Beneficiary Tokens may be bridged or reissued cross-chain to support user mobility, application-layer innovation, and interoperability. However, the Trustee Token—the authoritative source of rules, restrictions, and revocation logic—remains anchored on a designated authority chain. This chain acts as the canonical governance environment where all rule evaluation occurs.

In practice, this means that enforcement rules travel with the rights, not with the underlying assets. Because underlying assets remain locked in trustee-controlled custody, they never leave the authoritative execution environment and are never exposed to weaker cross-chain security or permissive wrapper contracts. Rights may move; assets do not.

SUPPORTED NETWORK ENVIRONMENTS

TrustLogic is designed to function across the most widely used blockchain architectures, including:

- EVM chains and Layer-1 blockchains
- Layer-2 rollups
- appchains and subnets
- modular blockchain architectures
- execution layers with differing consensus or security models

The enforcement logic remains consistent across these environments, enabling rights to operate reliably even in heterogeneous execution contexts.

WHY THIS MATTERS

Cross-chain systems frequently undermine enforceability because assets can be bridged into environments where restrictions, royalties, licensing rules, and compliance logic are not recognized or cannot be enforced. Once an asset leaves its native contract or execution environment, obligations often disappear. TrustLogic eliminates this failure mode by keeping the Trustee Token—and therefore the rules—on the authority chain, ensuring that all rights remain governed by the original ruleset no matter where they travel. This architecture allows cross-chain mobility without sacrificing governance, compliance, or institutional trust.

5.7 Interoperability with Existing Token Standards

TrustLogic is designed to coexist with and enhance existing token standards such as ERC-20, ERC-721, ERC-1155, and other chain-specific asset formats. Rather than replacing current token types, TrustLogic adds a governed rights layer that ensures obligations remain enforceable even when underlying assets originate outside the protocol.

When integrating an external asset, the Application anchors that asset to a Trustee Token by depositing it into the Trustee's custody environment or by referencing it through an immutable rights mapping when custody is not applicable (e.g., songs, videos, datasets). The corresponding Beneficiary Token represents the governed entitlement to use, transfer, or license that asset. This structure allows TrustLogic to enforce royalties, licensing terms, transfer conditions, and revocation events regardless of the asset's original token standard.

Because the governed rights are enforced at the authority layer—not at the level of the original token—TrustLogic prevents rule bypass via wrapping, custodial transfers, or cross-marketplace activity. Existing tokens can therefore participate in a TrustLogic-governed ecosystem without modification, while benefiting from enforceable rights, compliance guarantees, and a unified enforcement lifecycle.

6. Use Cases

Use Case	Technical Feasibility	Implementation Risk	Regulatory / Compliance Risk	Market Adoption Feasibility
6.1 Ticketing & Anti-Scalping Enforcement	High	Low	Low	High
6.2 Creator Royalty Enforcement	High	Low–Medium	Low	High
6.3 IP Licensing & Rights Enforcement	Medium–High	Medium	Medium	High (studios)
6.4 Software Licensing & Confidential Access	High	Medium	Low	Medium–High
6.5 AI Dataset Licensing & Model Governance	Medium	Medium–High	Medium	High
6.6 Purpose-Bound Remittances & Aid	Medium	High	High	Medium–High
6.7 Contractor Milestone Payments	High	Medium	Low	Medium–High
6.8 Insurance Claim Integrity & Double-Claim	Medium–High	Medium	Medium–High	Medium
6.9 Stock Option Vesting & Transfer Governance	Medium	Medium	High	Medium

Table 2 – Use Case Feasibility and Risk Matrix

6.1 Ticketing & Anti-Scalping Enforcement

TrustLogic enables performers and venues to enforce resale, pricing, transfer, and gifting rules through a closed-loop rights architecture that eliminates scalping vectors and marketplace bypass.

THE FAILURES OF TRADITIONAL TICKETING MODELS

Ticketing markets suffer from persistent vulnerabilities that allow scalpers and automated bots to distort pricing, restrict fan access, and undermine performer intent. Traditional digital tickets behave as bearer instruments: once issued, they can be freely transferred, replicated, or resold through unauthorized channels. Secondary marketplaces frequently ignore resale rules, focusing instead on liquidity and volume. NFT-based ticketing attempted to address these issues but ultimately preserves the same weakness—transferable tokens that can be wrapped or resold without respecting issuer-defined constraints.

GOVERNED ACCESS INSTEAD OF TRANSFERABLE TICKETS

TrustLogic replaces this fragile model by treating tickets as **governed rights** rather than transferable assets. Underlying ticket assets remain anchored in trustee-controlled custody; users interact only through Beneficiary Tokens that represent conditional, revocable access rights. Every transfer, resale, or gifting event is validated against the performer's encoded policies, ensuring predictable behavior throughout the ticket's lifecycle.

RESALE, GIFTING, AND THE END OF SCALPING LOOPHOLES

This architecture supports a spectrum of ticketing policies, from prohibiting resale entirely to enabling controlled resale with fixed or capped pricing. Crucially, gifting becomes a **revocable access entitlement** rather than a full transfer. The original ticket holder retains ultimate control over the gifted ticket until the moment of entry.

This eliminates one of the most exploited avenues of scalping: selling "gifted" tickets outside official channels. Because the gifter retains the ability to revoke the ticket at any time, the recipient cannot treat it as a resaleable asset. No rational buyer will purchase a gifted ticket knowing it can be taken back instantly. The economic basis for gifting-based scalping collapses completely.

ENFORCEMENT EMBEDDED AT THE ARCHITECTURAL LAYER

All ticket behavior flows through the Trustee Token, making unauthorized resale structurally impossible rather than operationally discouraged. Instead of relying on monitoring or after-the-fact intervention, TrustLogic encodes enforceability directly into the rights architecture. Performers regain control over distribution, fans are protected from predatory pricing, and marketplaces are required to operate within the defined ruleset or lose access to inventory.

A RIGHTS-BASED FOUNDATION FOR FAIR DIGITAL TICKETING

By modeling tickets as governed digital rights instead of free-floating bearer tokens, TrustLogic mirrors the legal and contractual nature of event admissions in a digital setting. The result is a ticketing ecosystem where fairness, artist intent, and consumer protection are built into the system itself—creating a foundation for fraud prevention, equitable access, and more sophisticated ticketing experiences.

6.2 Creator Royalty Enforcement

TrustLogic guarantees royalty payments across marketplaces by embedding enforcement at the authority layer, preventing bypass via wrapping, off-platform transfers, or marketplace non-compliance.

Creator royalties fail in current digital asset systems because royalties depend on marketplace cooperation rather than protocol enforcement. TrustLogic replaces this brittle model with governed, enforceable revenue flows.

WHY ROYALTIES FAIL IN TODAY'S DIGITAL ECOSYSTEMS

Marketplaces routinely bypass on-chain royalty metadata. Once an asset leaves the originating platform, no mechanism forces secondary sellers to honor royalties. Wrapping, private transfers, custodial marketplaces, and derivative tokens all circumvent royalty logic. For major creators and institutions, this

makes secondary markets financially unpredictable and legally incompatible with existing rights agreements.

PROTOCOL-LEVEL ROYALTY ENFORCEMENT

TrustLogic enforces royalty obligations through the Trustee's authority layer rather than relying on platform behavior. The Trustee maintains canonical royalty rules—percentage splits, payout routing, sharing among collaborators, carve-outs, exemptions, or territory-based models. Every attempted rights transfer invokes the Trustee's validation logic. If a transfer does not satisfy royalty requirements, it simply does not execute.

This means creators no longer depend on marketplace goodwill. Royalties are paid because the protocol enforces them.

PREVENTING BYPASS AND UNAUTHORIZED TRANSFERS

Traditional tokens can be wrapped, privately sold, or moved into custodial pools. TrustLogic prevents these bypasses by ensuring that royalty logic follows *the rights*, not the asset. Every rights movement—secondary sale, sublicensing event, or derivative issuance—requires compliance validation from the Trustee. Unauthorized transfers cannot obtain valid rights and therefore cannot circulate as legitimate entitlements.

INSTITUTIONAL-GRADE ROYALTY MODELS

The enforcement model supports the full spectrum of professional royalty structures:

- Multi-party splits (artists, composers, producers, publishers)
- Time-based or usage-based royalties
- Minimum guarantees
- Territory-based royalty changes
- Streaming or view-based triggers
- Recurring royalties connected to derivative licenses

These capabilities bring royalty enforcement into alignment with industry practice rather than speculative marketplace norms.

TRANSFORMING SECONDARY MARKETS INTO RELIABLE REVENUE

By moving royalty enforcement from marketplaces to protocol logic, TrustLogic enables creators, publishers, studios, and labels to participate confidently in secondary markets. Royalty flows become predictable, enforceable, and auditable, creating a sustainable revenue layer for the creative economy.

6.3 Intellectual Property Licensing & Rights Enforcement

TrustLogic provides revocable, conditional, and scope-specific licensing rights that meet institutional IP requirements that Story Protocol and token-based licensing cannot support.

IP licensing demands precise, enforceable control over how creative works may be used. TrustLogic introduces governed, revocable, and scope-bound licensing that mirrors real-world legal contracts.

WHY DIGITAL LICENSING FAILS TODAY

Web3 licensing attempts—metadata rules, Story Protocol–style registries, or token-based "licenses"—cannot enforce:

- territorial restrictions
- duration or time-based rights
- derivative permissions
- embargo windows
- attribution requirements
- revocation in case of misuse

Once a token is transferred, the issuer loses all control. Studios, publishers, and music labels cannot adopt such systems because they violate basic licensing requirements.

LIMITATIONS OF REGISTRY-BASED APPROACHES (E.G., STORY PROTOCOL)

Registry-driven IP systems attempt to encode licensing terms as on-chain metadata or in shared registries. However, these approaches cannot enforce obligations across marketplaces, custodians, or derivative environments. Once a token leaves the registry's ecosystem, the licensing rules no longer bind downstream users. Wrapping, private transfers, custodial platforms, and derivative tokens can bypass registry logic entirely. TrustLogic resolves this structural limitation by enforcing licensing terms at the authority layer through the Trustee Token, ensuring that rights and obligations remain inseparable and enforceable regardless of where rights circulate.

GOVERNED LICENSING THROUGH AUTHORITY–RIGHTS SEPARATION

TrustLogic anchors licensing logic in the Trustee layer. The Trustee encodes:

- permissible usage scope
- derivative permissions
- territorial boundaries
- commercial vs. non-commercial rights
- studio- or label-specific constraints
- revocation conditions

Licensees receive governed rights that must pass Trustee validation every time they are exercised. Unauthorized attempts to access files, export stems, create derivatives, or reuse protected assets simply do not succeed.

Licenses cease being metadata—they become enforceable entitlements.

IDENTITY VERIFICATION FOR CREATORS AND LICENSEES

Before a license can be issued:

- **Creators** may require identity verification to establish authorship or ownership.
- **Buyers/Studios** may require verification for anti-money-laundering compliance or when licensing fees exceed regulatory thresholds (e.g., >$10,000).

The application requests KYC checks from an external provider, receives the results, and forwards only the validated attributes needed by the Trustee. If requirements are unmet, the process halts before rights issuance.

This ensures both legal compliance and accurate attribution of rights.

PREVENTING UNAUTHORIZED DERIVATIVES AND DISTRIBUTION

TrustLogic prevents unauthorized creative reuse by requiring that every derivative creation event obtain a governed rights signature. Without Trustee approval:

- derivative works cannot be authorized
- unauthorized stems cannot be used
- character models cannot be exported into new media
- 3D assets cannot be redistributed
- unlicensed adaptations remain invalid

This addresses the core problem facing creative industries: *uncontrolled derivative circulation*.

MISUSE DETECTION, SUSPENSION, AND JUDICIAL REVIEW

If a licensee misuses IP (e.g., using a song in an unapproved region or distributing assets beyond scope), the Creator or platform may submit a misuse report.

1. The Trustee evaluates the report.
2. The license may be **temporarily suspended**.
3. A **Judicial Panel** (domain experts) reviews the dispute.
4. The panel issues a binding ruling.
5. The Trustee enforces the ruling: restore, modify, or revoke the license.

This structure mirrors real-world contractual dispute processes, but with deterministic, protocol-enforced execution.

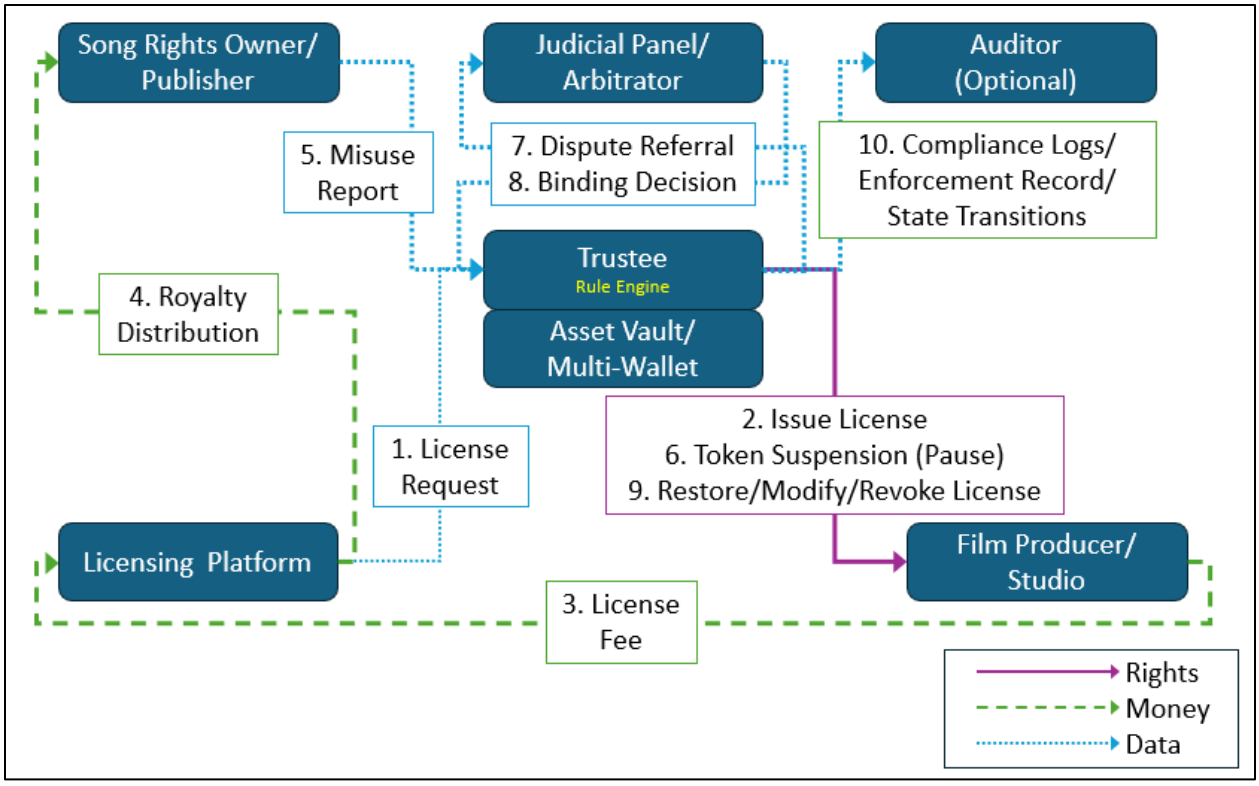

Figure 3 — IP Licensing & Rights Enforcement Workflow

SUPPORTING REAL-WORLD LICENSING MODELS

TrustLogic can enforce:

- Exclusive or non-exclusive licenses
- Synchronization rights (music to film)
- Sampling and derivative rights
- Territory-restricted distribution
- Time-bound promotional rights
- Digital-first or print-later publishing splits
- Character or model licensing for games or animation
- AI dataset usage rights and inference restrictions

These capabilities satisfy the requirements of film studios, labels, publishers, and enterprise IP owners.

6.4 Software Licensing & Confidential Access Control

TrustLogic enforces time-limited, revocable, and confidential access to code and internal systems that cannot be safely controlled by transferable tokens.

WHY SOFTWARE ACCESS CANNOT RELY ON TRANSFERABLE TOKENS

Enterprise software licensing often requires controlled, time-bound access to sensitive codebases, internal tools, technical documentation, or proprietary datasets. Traditional token-based access models treat software permissions as freely transferable assets, making it impossible to prevent unauthorized copying, persistence of credentials, or reuse of access entitlements. Once a key or NFT representing

access is transferred, cloned, or leaked, the issuing institution loses control. This contradicts how software licensing works in regulated industries, where revocation, monitoring, and confidentiality are essential.

GOVERNED, REVOCABLE ACCESS RIGHTS

TrustLogic introduces a rights-based model in which access to software resources is represented by Beneficiary Tokens that remain subordinate to trustee authority. Underlying assets—source code, build environments, or secure documentation—never leave their protected environment. Instead, access is granted through revocable rights that can be suspended, restricted, or terminated based on usage, time, role, or compliance triggers. This eliminates the possibility of users exporting, reselling, or indefinitely retaining access to sensitive materials.

CONFIDENTIALITY AND PRINCIPLE-OF-LEAST-PRIVILEGE ENFORCEMENT

Because each access request is evaluated against the trustee's rules, institutions can enforce granular access policies, including view-only permissions, environment-level restrictions, time-limited audits, or role-based access windows. When a contractor's engagement ends or when an auditor has completed their review, the trustee can revoke permissions instantly, ensuring the organization retains continuous control over confidential assets.

A SECURE FOUNDATION FOR MODERN SOFTWARE LICENSING

TrustLogic enables software licensing that resembles real-world contractual practice rather than the permissive assumptions of tokenomics. Enterprises can grant temporary or conditional access without the risk of leakage or unauthorized reuse. Developers and contractors receive the access they need; institutions retain the enforcement mechanisms they require. This creates a secure, auditable foundation for enterprise software licensing across cloud platforms, SaaS ecosystems, and internal development environments.

6.5 AI Dataset Licensing & Model Governance

TrustLogic enforces revocable dataset access, training rights, fine-tuning rights, and derivative model governance in a way that NFT-based licensing cannot.

CHALLENGES OF DATASET GOVERNANCE IN AI SYSTEMS

AI development depends on access to high-quality datasets that are frequently subject to licensing restrictions, privacy rules, or regulatory constraints. Today's systems provide no way to ensure that datasets are used only for permitted purposes, that derivative models comply with licensing terms, or that access can be revoked after training windows expire. Once a dataset is downloaded or shared, the licensor loses all practical control. This inability to enforce data-usage obligations is a major barrier to compliant AI development.

RIGHTS-BASED DATASET ACCESS

TrustLogic enables dataset licensing through Beneficiary Tokens that encode the right to train, fine-tune, or evaluate models using specific data, without granting possession of the underlying raw dataset. Access occurs only within controlled environments under trustee supervision. Each action—training,

inference, fine-tuning, or exporting model weights—is checked against the licensing rules defined by the Trustee Token.

MODEL LINEAGE AND DERIVATIVE GOVERNANCE

TrustLogic supports lineage-aware governance, allowing licensors to track how a dataset contributes to derivative models and to specify conditions such as non-commercial usage, embargo periods, or restrictions on downstream distribution. If a model is trained in violation of the terms, rights can be revoked, and downstream usage can be blocked by refusing to issue the required rights token for derivative operations.

A FRAMEWORK FOR COMPLIANT AI LICENSING

By decoupling dataset access from dataset possession and enabling enforceable licensing logic at the protocol level, TrustLogic provides a foundation for AI governance that reflects real-world legal requirements. Research institutions, enterprises, and model developers can collaborate without sacrificing compliance, confidentiality, or control—enabling responsible and auditable AI development.

6.6 CBDC Privacy & Compliance

TrustLogic separates identity (Trustee Token) from transactions (Beneficiary Token), enabling privacy-preserving CBDCs with selective auditability and programmable compliance.

THE IDENTITY–PRIVACY PARADOX IN DIGITAL CURRENCIES

Central bank digital currencies must meet strict standards for AML, KYC, and financial compliance while preserving user privacy and avoiding the creation of surveillance infrastructures. Most CBDC pilots struggle to balance these requirements because they bind user identity directly to transaction keys. This design exposes transactional behavior to centralized entities and undermines public trust.

SEPARATING IDENTITY FROM TRANSACTIONAL RIGHTS

TrustLogic resolves this tension by anchoring identity and compliance attributes at the trustee layer while issuing Beneficiary Tokens that contain no personally identifiable information. Users can transact privately, while institutions retain regulated oversight only when legally required. This achieves selective auditability without enabling universal visibility of user activity.

PURPOSE-BOUND AND CONDITIONAL SPENDING

Because rights are governed at the authority layer, CBDCs can embed spending constraints—such as merchant-category restrictions, expiration windows, or conditional subsidies—without requiring user-level monitoring. Misuse triggers revocation or suspension automatically, enabling compliant programmable money without compromising privacy.

A PRIVACY-PRESERVING ARCHITECTURE FOR PUBLIC-SECTOR VALUE

TrustLogic provides the missing enforcement layer needed for CBDCs to function as both private payment instruments and compliant financial assets. Users receive privacy; regulators receive transparency only when justified; and governments gain the ability to administer targeted, purpose-bound financial programs with confidence.

6.7 Purpose-Bound Remittances & Humanitarian Aid

TrustLogic enables senders, NGOs, and institutions to ensure funds are spent according to intended purposes, with revocation for misuse.

Remittances and humanitarian aid programs often suffer from diversion, fraud, and inability to enforce how funds are actually used. Once money reaches the recipient, neither donors nor implementing agencies can ensure that assistance is spent on approved goods or services. TrustLogic introduces governed, conditional spending authority that allows funders to define, enforce, suspend, or revoke spending permissions while still preserving user privacy.

CHALLENGES IN TRADITIONAL REMITTANCE AND AID SYSTEMS

Conventional payment systems provide no mechanism to bind funds to a specific purpose. As a result:

- humanitarian funds may be misused or resold
- NGOs cannot verify intended use
- government stipends and subsidies may be diverted
- multi-phase relief packages cannot enforce milestones
- duplicate or fraudulent claims are common
- regulatory reporting is inconsistent or unverifiable

Bearer-style digital money—whether mobile money, stablecoins, or CBDCs—cannot enforce purpose once funds leave the sender.

GOVERNED, PURPOSE-BOUND SPENDING

TrustLogic separates **ownership of funds** from **authority to spend**, enabling enforceable spending controls. Rather than transferring unrestricted funds directly to the recipient, the Application:

1. validates identity (recipient, guardian, NGO administrator),
2. receives or holds the funds,
3. defines spending rules and compliance constraints,
4. writes the necessary rule references into the Trustee layer, and
5. issues a Beneficiary Token that grants *conditional spending authority*.

The underlying funds remain controlled by the Application until each spending attempt is validated against the Trustee's rule engine.

Permitted rules include:

- **merchant or category restrictions** (food, shelter, medicine)
- **geographic limitations**
- **interval-based release** (weekly stipends, tranches)
- **milestone conditions** (attendance, check-ins, task completion)
- **non-transferability**
- **caps or per-transaction limits**

Unauthorized spending attempts simply do not execute.

REAL-WORLD EXAMPLES OF PURPOSE-BOUND SPENDING RULES

These rules can model practical aid scenarios. For example, a refugee assistance stipend may allow spending at grocery stores and pharmacies but block purchases of alcohol or tobacco. A school-attendance program may release weekly funds only after a parent or guardian completes a check-in or a child attends class. Disaster-relief allocations may restrict spending to a specific geographic region or expire automatically if not used within a defined emergency window. These examples illustrate how TrustLogic can encode policy goals directly into conditional spending rights while preserving user dignity and privacy.

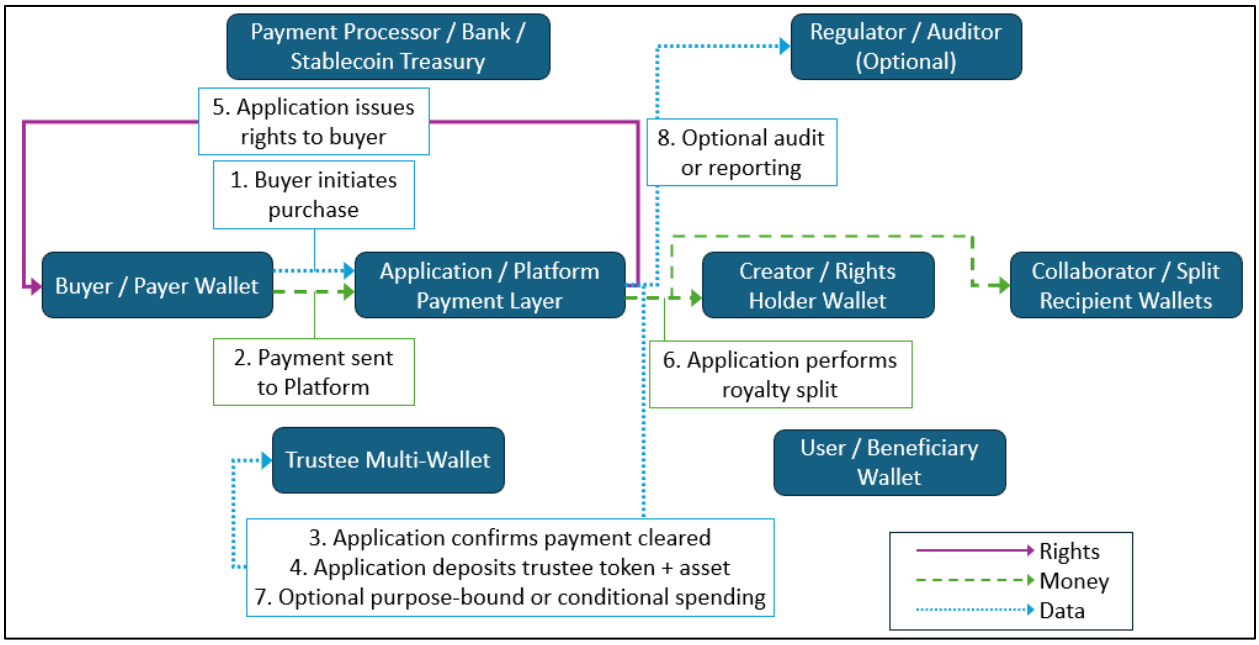

Figure 5 — Purpose-Bound Remittance & Humanitarian Aid Flow

The Application conducts identity verification, defines spending rules, and orchestrates fund disbursement; the Trustee enforces spending conditions; recipients receive conditional spending authority instead of unrestricted funds.

IDENTITY REQUIREMENTS FOR AID DISTRIBUTION

To prevent misuse and duplicate claims, the Application determines which identities must be verified:

- **Recipient identity** for eligibility
- **NGO administrator identity** for approvals
- **Guardian/proxy identity** for minors
- **High-value threshold checks** when aid packages exceed regulatory limits

The Application handles KYC through an external provider and passes only the minimal validated identity attributes (never raw PII) into the Trustee's policy context.

Conditional Release, Suspension, and Revocation

TrustLogic supports dynamic management of spending authority:

- **Conditional Release:** Funds unlock only when validated conditions are met.
- **Suspension:** Spending authority is paused in response to suspicious or non-compliant activity.
- **Revocation:** Rights can be removed if misuse is confirmed.
- **Dispute Review:** Recipients may contest actions through a Judicial Panel.

These mechanisms allow NGOs and agencies to operate transparent, accountable relief programs.

Auditability and Institutional Reporting

TrustLogic generates verifiable, PII-free compliance logs:

- identity attestation records
- spending-rule evaluations
- timestamps of releases, suspensions, and revocations
- transaction histories consistent with purpose-bound logic

These logs provide donors, NGOs, and regulators with the confidence that aid was used as intended.

6.8 Contractor Milestone Payments

TrustLogic enables conditional, revocable milestone releases based on oracle attestations or verified progress.

THE DIFFICULTY OF ENFORCING PERFORMANCE-BASED PAYMENTS

Milestone-based payments are common in software development, construction, consulting, and creative production. However, traditional processes involve trust-heavy workflows where contractors may receive partial payments without delivering the required work, or where disputes become costly and slow to resolve.

RIGHTS THAT UNLOCK ONLY UPON VERIFIED COMPLETION

TrustLogic enables milestone payments through rights tokens that represent the entitlement to receive funds only when specific conditions—defined in the Trustee Token—are met. Completed milestones can be verified through oracles, attestations, or authorized reviewers. Until verified, the right remains pending and non-transferable.

REDUCING DISPUTES AND INCREASING ACCOUNTABILITY

If work is not completed or is completed improperly, the trustee can suspend or revoke the milestone right. This dramatically reduces the risk borne by payers and aligns incentives for contractors to deliver verifiable progress. It also provides contractors with a clear and trustworthy pathway to payment once conditions are satisfied.

A MORE RELIABLE FRAMEWORK FOR PROJECT-BASED WORK

TrustLogic transforms milestone payments from informal trust-based agreements into enforceable digital contracts, reducing disputes and increasing efficiency across industries that rely on staged delivery.

6.9 Insurance Claim Integrity & Double-Claim Prevention

TrustLogic assigns canonical claim rights that prevent duplicate claims across carriers.

THE STRUCTURAL WEAKNESS OF TRADITIONAL INSURANCE SYSTEMS

Insurance systems often suffer from double-claim fraud, where the same loss is submitted to multiple carriers or across different policies. Coordination between insurers is limited, and claims processing relies heavily on manual validation. This creates opportunities for abuse, delays genuine payouts, and increases systemic cost.

CANONICAL CLAIMS THROUGH TRUSTEE-GOVERNED RIGHTS

TrustLogic assigns a unique, canonical claim right to each insured event. Only one Beneficiary Token representing the claim can exist at a time, preventing users from initiating parallel or duplicate filings. If an attempt is made to submit a second claim for the same event, the trustee simply refuses to issue the rights token.

IMPROVED AUDITABILITY AND FRAUD DETECTION

Because claims are represented as governed rights, insurers gain visibility into the lifecycle and status of each claim without compromising user privacy or requiring a shared centralized database. Revocation can occur if fraud is detected, and reinstatement is possible if errors are resolved.

MODERNIZING CLAIMS PROCESSING

TrustLogic provides insurers with a cryptographically anchored mechanism for ensuring claim integrity, reducing fraud, speeding up adjudication, and improving trust between carriers and policyholders.

6.10 Stock Option Vesting & Transfer Governance

TrustLogic enforces vesting schedules, expiration, clawbacks, and transfer restrictions for equity compensation.

COMPLEXITY AND RISK IN EQUITY COMPENSATION

Equity compensation requires precise tracking of vesting schedules, employment status, transfer restrictions, and clawback provisions. Traditional systems rely on manual processes, centralized cap tables, and trust in intermediaries. When employees leave, companies often struggle to enforce repurchase rights or prevent unauthorized transfers.

PROGRAMMABLE VESTING AND CONDITIONAL OWNERSHIP

TrustLogic enables stock option vesting through Beneficiary Tokens that mature or unlock based on predetermined conditions. Vesting schedules, cliff periods, forfeiture rules, and termination triggers are encoded in the Trustee Token. Rights can be revoked automatically if employment ends before vesting, or transferred only when contractually permitted.

COMPLIANT TRANSFERS AND CLAWBACK ENFORCEMENT

Because all transfers must pass through trustee validation, unauthorized equity transfers become impossible. Companies retain the ability to enforce clawbacks, handle repurchases, or freeze rights in the event of disputes, regulatory issues, or corporate actions.

A TRUSTWORTHY FOUNDATION FOR MODERN CAP TABLES

TrustLogic replaces fragile, manual equity-management systems with enforceable, programmable rights that ensure compliance, protect corporate interests, and support dynamic ownership structures across startups, enterprises, and global corporations.

WHITE PAPER

7. Economic Impact & Adoption Feasibility

Enforceable digital agreements open markets that have historically been inaccessible to Web3 technologies. Industries such as ticketing, IP licensing, royalties, software access, AI training, insurance, and government aid all require a level of control, revocation, auditability, and compliance that traditional blockchain assets cannot provide. By separating authority from rights and ensuring governed, revocable usage, TrustLogic activates entirely new digital markets—many of which represent multi-billion- or trillion-dollar opportunities.

This section evaluates the total addressable market (TAM), implementation risk, regulatory exposure, and adoption feasibility across all ten primary use cases. Together, these illustrate both the breadth and the economic potential of enforceable digital rights.

7.1 Cross-Industry Impact of Enforceability

Across creative industries, financial infrastructure, AI ecosystems, and institutional operations, the absence of enforceable rights is the limiting factor preventing high-value assets from entering open digital markets. When assets cannot be controlled, revoked, licensed, or governed after transfer, institutions simply refuse to adopt decentralized systems. TrustLogic removes this barrier.

The economic impact is twofold:

1. **Unlocking restricted markets** — industries previously unable to use Web3 can now participate because enforceability exists.
2. **Strengthening existing markets** — creator royalties, ticketing, licensing platforms, and software ecosystems gain durable protection against bypass and misuse.

7.2 TAM and Feasibility Assessment Across Use Cases

The following table summarizes economic scale and core problems solved for each use case. Values are provided as approximate global TAM ranges to guide strategic prioritization.

Use Case	What It Solves	TAM (Approx.)
6.1 Ticketing & Anti-Scalping Enforcement	Prevents unauthorized resale, price manipulation, and ticket duplication through enforceable transfer restrictions	**$25–35B** global ticketing
6.2 Creator Royalty Enforcement	Enforces guaranteed royalty payments on primary and secondary asset transfers	**$300B** global creator economy
6.3 IP Licensing & Rights Enforcement	Enforces license terms, usage scope, and revocation upon breach or misuse	**$1.4T** global IP licensing market
6.4 Software Licensing & Confidential Access	Grants revocable, time-bound access to software, APIs, or confidential systems	**$200–300B** enterprise software
6.5 AI Dataset Licensing & Model Governance	Controls dataset usage, training rights, derivative models, and downstream restrictions	**$100–150B** AI data & model economy
6.6 CBDC Privacy, Compliance & Spending Controls	Enforces programmable spending rules, privacy boundaries, and regulatory constraints on digital currencies	**$10T+** projected CBDC & digital currency flows
6.7 Purpose-Bound Remittances & Aid	Ensures funds are spent exclusively for authorized purposes and beneficiaries	**$1T** global remittances & aid
6.8 Contractor Milestone Payments	Releases payments only upon verification of contractual milestones or deliverables	**$500B+** global contractor economy
6.9 Insurance Claim Integrity & Double-Claim Prevention	Prevents duplicate, fraudulent, or conflicting insurance claims across providers	**$7T** global insurance industry
6.10 Stock Option Vesting & Transfer Governance	Enforces vesting schedules, transfer restrictions, and revocation conditions	**$300B+** equity compensation market

Table 3 - Market Opportunities Across Enforceable Rights Use Cases

7.3 Interpretation and Strategic Prioritization

High Feasibility, Low Regulatory Burden — Immediate Growth Markets

These use cases produce fast adoption and clear revenue without deep regulatory dependencies:

- **Ticketing (6.1)**
- **Creator Royalties (6.2)**
- **Contractor Payments (6.8)**

These should remain TrustLogic's **Phase 1 commercialization targets**.

Medium Complexity, High Enterprise Value — Strategic Expansion Markets

These areas require modest rule modeling but unlock extremely large enterprise TAM:

- **IP Licensing (6.3)**
- **Software Licensing (6.4)**

- **AI Dataset Licensing (6.5)**

These become **Phase 2**, focusing on strategic partnerships with studios, SaaS vendors, and AI governance entities.

High-Impact, High-Regulation Markets — Partnership-Driven

These areas have massive TAM but require NGO, insurance, or regulatory collaboration:

- **Purpose-Bound Remittances (6.7)**
- **Insurance Claim Integrity (6.9)**
- **Stock Option Governance (6.10)**

These should be pursued during **Phase 3**, after institutional integrations and compliance modules are well established.

7.4 Economic Rationale for TrustLogic as a Protocol

Across all use cases, the economic value derives from:

- **license fees paid for rule-enforced rights issuance**
- **revocation and dispute-resolution fees**
- **transaction fees for governed transfers**
- **custody or asset-hosting fees**
- **compliance and attestation processing**
- **institutional licensing of the trust layer**

Because TrustLogic controls the enforceability layer, it also controls the **economic choke point** for any market where rights must be governed.

7.5 Summary: Enforceability as an Economic Primitive

Enforceability is not merely a technical feature; it is an **economic primitive** that unlocks multi-trillion-dollar markets currently incompatible with decentralized systems. By providing conditional, revocable, auditable rights, TrustLogic enables:

- enterprise migration to Web3
- regulated financial flows
- secure IP licensing markets
- governed AI data ecosystems
- transparent aid distribution
- institution-grade compliance

This economic foundation underpins TrustLogic's commercial model and its broad adoption potential across creative, financial, industrial, and public-sector domains.

8. Governance

TrustLogic's governance model is designed to balance three competing requirements: the need for institutional authority and compliance, the flexibility required for creators and organizations to define their own rules, and the predictability necessary for users and integrators to interact with governed digital assets. Governance ensures that rights remain enforceable across their lifecycle, that rule changes cannot be executed arbitrarily, and that authority remains anchored to the trustee in a manner consistent with legal and commercial practices.

The framework is structured around layered responsibilities, allowing different participants—institutions, platforms, and optional decentralized bodies—to define policies, manage operations, and oversee protocol-level evolution without compromising enforceability.

8.1 Trustee Governance

AUTHORITY AND RULE DEFINITION

At the core of the governance system is the trustee, the entity responsible for defining and enforcing the rules that govern a digital asset or rights bundle. The trustee controls the Trustee Token, which encodes licensing terms, transfer conditions, revocation logic, royalty structures, usage restrictions, territorial boundaries, and any other contractual conditions associated with the asset.

Because the Trustee Token is non-transferable, authority cannot be sold or passed between entities through market activity. This ensures that the trustee's role mirrors real-world custodial and fiduciary responsibilities—stable, predictable, and anchored to identifiable authority.

INSTITUTIONAL ALIGNMENT

Trustee governance is essential for domains where obligations must be continuously enforced, such as:

- film, music, and creative licensing
- financial instruments and programmable assets
- CBDC issuance and public-sector programs
- insurance claims and regulated workflows
- enterprise software licensing and data access governance

In each case, the trustee defines and enforces the operational policies that govern how rights behave across their entire lifecycle.

8.2 Trustee Deployment Models

TrustLogic supports multiple trustee configurations. The protocol is deliberately agnostic: the same contracts and UI work with every model below.

Model	Trustee Identity	Who typically chooses it	Example use-cases	Default for end users?
A	Issuing Platform (Level 3 in earlier table)	The platform that creates and sells the asset	Ticketing (Ticketmaster, DICE), streaming royalties (Spotify, SoundCloud), game items (Steam, Epic), NFT marketplaces (OpenSea Pro), subscriptions	Yes – hidden & non-configurable
B	Single registered corporate trustee	Creator / rights-holder (or platform on their behalf)	Warner Music Trust Ltd., Coinbase Custody Trust, a dedicated "Universal Music Trustee"	Optional
C	Consortium / multi-institution trustee	Group of rights-holders or institutions	RIAA-wide royalty pool, inter-bank CBDC pilot, Premier League clubs joint trustee	Optional
D	Future crypto-native bonded trustee	Community / DAO	Progressive-decentralisation collections, open datasets	Future / optional

Table 4 – Trustee Deployment Models – From Default Platform to Optional Crypto-Native

MODEL A – DEFAULT: ISSUING PLATFORM AS TRUSTEE (THE 99 % CASE)

For almost every consumer and creator-facing product today — tickets, streaming, gaming, subscriptions, marketplace royalties — the platform that issues and sells the asset is the natural and intended trustee.

The musician does not want to pick or run a trustee.

The fan does not want a trustee selection screen.

Both already trust Ticketmaster / DICE / Spotify / Steam to issue, transfer, price-cap, and revoke tickets or licenses today.

In Model A the trustee is therefore declared once by the platform at asset-class creation and is non-configurable by creators or end users — exactly like you cannot today choose a different transfer agent for your Tesla stock options or a different escrow bank for your concert ticket. This is the default deployment mode for 99 % of real-world volume and requires zero extra UI or decision-making.

MODELS B–D – OPTIONAL TRUSTEE CHOICE (THE 1 % CASE THAT MATTERS A LOT)

Certain rights-holders do care deeply about who the trustee is and want explicit choice:

Who cares	Why they care	Which model they pick
Major record labels / publishers	Want a single, legally liable entity they control or already contract with (e.g., their own captive trust company or a trusted third-party like Iron Mountain Digital)	Model B – single corporate trustee
Collecting societies & royalty pools	Need a neutral, multi-label trustee so no single major can dominate	Model C – consortium trustee
Independent artists who distrust platforms	Want to route around the default platform trustee entirely and point to their own or a community trustee	Model B or future D
Institutional RWA funds, banks, insurers	Regulatory requirement to use a licensed, supervised custodian	Model B or C

Table 5 – Which Rights-Holders Need Trustee Choice and Why They Care

In these cases, the creator (or consortium) selects the trustee at asset registration time. The choice is immutable for that asset class and is clearly displayed to buyers ("Rights enforced by Warner Music Trust Ltd.") so there is no surprise.

End result:

- 99 % of users and creators never see trustee complexity (Model A – platform default).
- The 1 % who actually need control (majors, indies who hate platforms, consortia, regulated institutions) get it without forking the protocol.

8.3 Platform Governance

OPERATIONAL RULES AND APPLICATION LOGIC

Platforms that integrate TrustLogic—such as ticketing systems, licensing marketplaces, creative platforms, or financial applications—may implement their own governance layer to manage operational logic. Platform governance includes decisions about:

- user experience and interface behavior
- marketplace policies
- fee structures
- dispute intake processes
- default rule templates
- oracle selection and attestation logic

While platforms cannot override the authority encoded in the Trustee Token, they can define additional policies that govern how rights are surfaced, transferred, or presented to users.

ENSURING CONSISTENCY ACROSS INTEGRATIONS

Platform governance enables decentralized applications, custodial platforms, and enterprise systems to apply consistent logic without weakening trustee authority. This separation mirrors the distinction between application-layer governance and protocol-layer governance in traditional blockchain systems.

8.4 Ecosystem or DAO Governance (Optional)

PROTOCOL EVOLUTION AND ECOSYSTEM STANDARDS

For ecosystems that span multiple institutions or creators—such as industry consortiums, music rights collectives, or regulated asset networks—an optional decentralized or consortium-style governance system may oversee shared rules, standard templates, or protocol upgrades. This layer can coordinate:

- protocol improvements and versioning
- dispute resolution frameworks
- cross-institution standards
- interoperability schemas
- revocation arbitration
- ecosystem-wide security practices

DELEGATED AUTHORITY AND MULTI-STAKEHOLDER INPUT

Ecosystem governance allows participants to influence the evolution of the trust framework without compromising the sovereignty of individual trustees. It functions similarly to layer-zero governance in large protocol ecosystems, providing a common foundation for coordination while preserving flexibility.

8.5 Emergency Governance

CRISIS RESPONSE AND SYSTEM INTEGRITY

Certain situations require rapid, coordinated action to protect users, institutions, or the integrity of the asset network. Emergency governance provides controlled mechanisms for trustees or designated bodies to suspend rights, freeze transfers, or disable certain operations temporarily. Emergency actions may be triggered by:

- widespread fraud or system compromise
- major regulatory interventions
- security incidents affecting underlying assets or custody
- network instability or oracle failures

CHECKS, DELAYS, AND TRANSPARENCY

To prevent misuse, emergency governance may include safeguards such as:

- time-delayed activation
- multi-party approval
- quorum thresholds
- post-action transparency reports

These mechanisms ensure that emergency powers enhance resilience without undermining trust or enabling arbitrary intervention.

8.6 Time-Delayed Rule Updates

PREDICTABILITY AND USER PROTECTION

Rule updates are an essential part of governance, but they must not compromise user expectations or undermine existing rights. TrustLogic supports time-delayed rule updates, allowing users and integrators

to receive notice before changes take effect. This prevents sudden governance shocks and aligns protocol behavior with real-world contractual norms.

MIGRATING RIGHTS TO UPDATED RULES

Time delays and migration windows allow rights holders to adapt to new rules, exit the system, or transition their entitlements in an orderly fashion. This preserves fairness while allowing trustees to evolve policies responsibly.

8.7 Governance as a Foundation for Trust

ALIGNMENT WITH LEGAL AND INSTITUTIONAL FRAMEWORKS

The governance architecture reinforces the central design philosophy of TrustLogic: enforceability requires predictable authority combined with flexible, conditional rights. By layering governance across trustees, platforms, and optional consortium bodies—and by embedding safety mechanisms such as revocation, migration windows, and emergency controls—TrustLogic provides a governance structure that mirrors the layered authority models used in financial regulation, intellectual property management, and enterprise compliance systems.
Governance is not an add-on to the protocol; it is the mechanism that ensures enforceability, fairness, compliance, and long-term system integrity.

8.8 Judicial Panels and Specialized Adjudicators

DOMAIN-SPECIFIC EXPERTISE FOR COMPLEX REVOCATION DECISIONS

Certain revocation decisions require specialized legal, technical, or commercial expertise that goes beyond the capabilities or neutrality of a single trustee. Examples include patent licensing disputes, copyright and neighboring rights conflicts, complex trust arrangements, AI dataset usage controversies, or multi-jurisdictional financial instruments. To address these cases, TrustLogic supports the use of **judicial panels**—independent groups of domain experts authorized to issue binding determinations within the scope defined by the relevant Trustee Token.

A trustee may, at the time of rule definition, specify that particular categories of disputes or revocation events must be decided by a judicial panel rather than unilaterally. In such cases, the panel's determination is expressed to the protocol through a structured attestation or oracle mechanism, which then triggers the appropriate state transition (revocation, suspension, reinstatement, modification of scope) in the Beneficiary Tokens. This ensures that complex or high-stakes decisions benefit from expert review while remaining objectively enforceable at the protocol layer.

FLEXIBLE PANEL COMPOSITION AND PROCEDURES

Panel composition and procedures can be tailored to the asset class or domain. Panels may consist of:

- IP attorneys or licensing specialists for copyright, music, and film
- patent experts for technology licensing and FRAND-style arrangements
- trust and fiduciary law experts for complex custodial structures
- financial, regulatory, or risk experts for CBDCs and structured instruments
- technical experts for AI, data governance, or software licensing disputes

Procedural rules—such as how evidence is submitted, how conflicts of interest are managed, and how appeals or reconsideration are handled—are defined off-chain but referenced in the trustee's rule set. The protocol's role is to recognize the panel's attested outcome and enforce it consistently.

8.9 Panel Infrastructure and Independent Stewardship

SEPARATION BETWEEN ADJUDICATION AND ECONOMIC STAKEHOLDERS

To maintain legitimacy and reduce conflicts of interest, the infrastructure that manages judicial panels should be governed by an **independent body** rather than any single trustee or commercial platform. TrustLogic supports the creation of a dedicated governance entity—potentially a DAO, consortium, or non-profit foundation—responsible for administering panel registration, credential verification, selection mechanisms, and procedural standards.

This independent body does not decide individual cases. Instead, it:

- defines eligibility criteria and codes of conduct for panelists
- maintains registries of qualified experts by domain and jurisdiction
- oversees randomization or selection mechanisms to avoid capture
- manages slashing, removal, or disciplinary processes for panelists who violate rules
- coordinates integration of panel decisions into the protocol's attestation/oracle layer

By separating adjudication infrastructure from individual trustees and economic actors, the system reduces incentives for biased decision-making and strengthens the credibility of revocation outcomes.

DAO- OR CONSORTIUM-BASED GOVERNANCE MODELS

Where appropriate, panel infrastructure governance can be implemented as:

- a **DAO** with token- or stake-based participation from ecosystem stakeholders,
- an **industry consortium** representing major IP owners, financial institutions, or public bodies, or
- a **hybrid model** combining DAO-based input with foundation-level oversight.

These models allow multiple constituencies—creators, institutions, users, and technical contributors—to participate in setting standards without centralizing control in a single entity. The goal is not to replace courts, but to offer a **specialized, protocol-aware adjudication layer** that can act rapidly, consistently, and in harmony with the encoded rules of the Trustee Tokens.

FROM DECISIONS TO ENFORCEABLE OUTCOMES

Once a panel decision is reached, its outcome is transmitted to the protocol through a cryptographically authenticated attestation. The trustee's rule engine interprets that attestation and performs the corresponding state transitions: revoking, suspending, modifying, or reinstating rights. This closes the loop between **off-chain expert judgment** and **on-chain enforceable consequences**, ensuring that governance remains both human-informed and protocol-enforced.

8.10 Legal Trustee Registration and Fiduciary Status (Optional)

In addition to its protocol-defined authority, a trustee may optionally register as a legal trustee under applicable trust law, allowing the TrustLogic architecture to align with established fiduciary and custodial frameworks. When the trustee holds the underlying asset in a legally recognized trust structure, the

separation between legal ownership (held by the trustee) and beneficial ownership (represented by Beneficiary Tokens) gains full legal force. This provides several advantages:

- the trustee's revocation powers become supported by fiduciary duties
- beneficial rights gain recognition under trust and property law
- courts can enforce trustee obligations and beneficiary claims
- institutions can adopt TrustLogic within their existing legal and compliance processes

Legal trust registration ensures that protocol-enforced rights map cleanly onto traditional legal concepts, creating a hybrid digital–legal trust structure that is enforceable both on-chain and off-chain.

9. Licensing & Institutional Integration

Licensing and institutional integration determine how TrustLogic transitions from a technical protocol into a practical enforcement layer for enterprises, studios, labels, publishers, financial institutions, and public-sector agencies. These organizations require systems that align with established legal frameworks, contractual obligations, regulatory expectations, and operational workflows. TrustLogic's architecture enables institutions to migrate existing rights structures into a governed digital environment without sacrificing enforceability, confidentiality, or commercial flexibility.

Institutional integration is not simply a matter of supporting APIs or SDKs; it requires aligning protocol functionality with real-world licensing practices. TrustLogic's authority–rights separation, revocation logic, and custody architecture allow institutions to embed their policies directly into the enforceable lifecycle of digital rights.

9.1 Licensing Model

EMBEDDING LEGAL AND COMMERCIAL RULES INTO PROTOCOL LOGIC

TrustLogic's licensing model is designed to mirror the structure of real-world contracts. Instead of representing a license as static metadata or legal text attached to a token, licensing terms are encoded directly into the Trustee Token's rule layer. This ensures that conditions, restrictions, and obligations remain enforceable even as rights transfer or interact with downstream applications.

Institutions can define terms such as:

- usage scope (e.g., reproduction, distribution, adaptation, remixing)
- territory and jurisdiction
- exclusivity or non-exclusivity
- duration and expiration
- sublicensing or derivative rights
- attribution requirements
- royalty or revenue-sharing obligations

Because the rules are embedded in the authority layer, they persist across marketplaces, platforms, and wallets, eliminating the bypass and fragility inherent in current token-based licensing systems.

9.2 Open SDK and Protocol Access

INTEGRATION FOR DEVELOPERS, PLATFORMS, AND ENTERPRISES

TrustLogic provides an open set of SDKs, APIs, and smart-contract templates that allow marketplaces, data providers, custodial platforms, and enterprise systems to integrate the enforcement layer into their applications. Developers can issue Beneficiary Tokens, evaluate rulesets, trigger revocation events, verify license compliance, and perform rule-governed transfers without managing the complexity of the authority logic themselves.

The open-access model supports:

- marketplace integration
- creative platform licensing workflows
- enterprise entitlement systems
- custodial wallet support
- cross-chain rights issuance
- data-access governance
- programmable financial and CBDC applications

This interoperability ensures that TrustLogic can serve as a foundation layer across multiple sectors.

9.3 Commercial Enterprise Licensing

INSTITUTION-READY DEPLOYMENT MODELS

Organizations with substantial IP catalogs, regulated financial obligations, or confidential datasets require dedicated governance environments. TrustLogic supports enterprise-grade deployments in which institutions operate their own trustee environments, define custom rule sets, and manage internal user groups.

Commercial licensing models may include:

- enterprise licensing agreements
- institution-specific rule templates
- private or permissioned trustee deployments
- integration with internal compliance and entitlement systems
- on-premise or cloud-hosted governance modules
- SLA-backed enforcement guarantees

This enables institutions to adopt TrustLogic as a trusted internal subsystem rather than relying solely on public infrastructure.

9.4 Royalty- and Usage-Based Revenue Models

ALIGNING LICENSING ECONOMICS WITH PROTOCOL ENFORCEMENT

Where appropriate, TrustLogic supports royalty-based or usage-based monetization schemes that align with the governance guarantees provided by the protocol. Because all transfers and rights actions pass through the trustee layer, the system can enforce:

- royalty splits for secondary sales
- derivative royalties
- training-usage royalties for AI datasets
- fees for authenticated access or entitlement issuance
- platform-level transaction or service fees

These monetization structures remain enforceable because they are embedded into the rights lifecycle rather than delegated to marketplace discretion.

9.5 IP Defense and Compliance Pools

SHARED ENFORCEMENT INFRASTRUCTURE FOR ECOSYSTEMS

Institutions participating in a shared ecosystem—such as music collectives, film studios, or financial consortia—may contribute to an IP defense pool or compliance fund. This pool supports:

- patent and trademark defense
- enforcement actions against unauthorized use
- arbitration and dispute resolution
- governance audits
- compliance certification programs

This structure mirrors existing industry alliances (e.g., OIN in open-source software) but applies them to enforceable digital rights. Pooling resources strengthens the ecosystem's collective ability to defend and maintain the integrity of rights.

9.6 Integration Pathways

MULTIPLE ON-RAMPS FOR INSTITUTIONS

TrustLogic supports several integration pathways to match the operational needs of different industries:

- **Direct integration** via SDK and API for platforms and marketplaces
- **Private trustee deployment** for high-security or regulated environments
- **Consortium-based governance** for multi-party ecosystems
- **Cross-chain integration** using the authority-anchored model
- **Custom rule modules** for licensing, compliance, or industry-specific workflows

These pathways allow institutions to adopt TrustLogic incrementally or comprehensively, depending on their architectural requirements and regulatory constraints.

9.7 Institutional Adoption and Interoperability

ALIGNMENT WITH EXISTING LEGAL, CREATIVE, AND FINANCIAL SYSTEMS

The institutional integration framework is designed to ensure that TrustLogic can operate alongside existing legal agreements, compliance systems, and business workflows. Rights written in TrustLogic can reference off-chain contracts, regulatory filings, or licensing agreements, ensuring compatibility with conventional legal structures.

This alignment makes TrustLogic suitable for:

- film and TV studios managing character and content rights
- music labels managing stems, masters, and derivative rights
- publishers controlling digital distribution and adaptation rights
- banks issuing conditional financial instruments and CBDCs
- insurers managing claims and risk entitlements
- enterprises controlling access to confidential assets
- AI firms enforcing dataset and model governance

Institutions gain predictable enforceability, auditability, and compliance without sacrificing operational flexibility.

9.8 TrustLogic as the Enforcement Layer for Digital Markets

ENABLING STANDARDS-ALIGNED, RIGHTS-AWARE INFRASTRUCTURE

At its core, Licensing & Institutional Integration positions TrustLogic as the enforcement layer missing from digital markets. By providing a structured framework for rules, rights, revocation, and governance, TrustLogic transforms digital assets from free-floating, uncontrolled objects into governed entitlements aligned with industry standards.

This makes it possible for institutions to publish, license, distribute, and monetize digital assets with confidence that their rights will be preserved across platforms, jurisdictions, and execution environments.

10. Implementation Roadmap

The implementation roadmap outlines the phased deployment of TrustLogic across technical, institutional, and ecosystem layers. The objective is to deliver enforceable digital rights in a way that aligns with real-world licensing practices, compliance requirements, and market infrastructure. The roadmap emphasizes progressive decentralization of governance, iterative integration with industry partners, and a deliberate sequencing of features to ensure stability, interoperability, and adoption.

10.1 Phase I — Core Protocol Deployment

ESTABLISHING THE ENFORCEMENT FOUNDATIONS

Phase I focuses on deploying the core enforcement primitives that define the TrustLogic architecture. This includes the Trustee Token authority layer, Beneficiary Token rights layer, multi-wallet custody architecture, and the baseline revocation and rule-evaluation engine. The objective is to create a stable foundation that can support early integrations without compromising security or enforceability.

Key deliverables include:

- launch of the Trustee Token authority framework
- implementation of the burn-and-mint rights reassignment mechanism
- deployment of segmented sub-wallet custody
- initial rule-engine capable of enforcing basic licensing and transfer conditions
- SDKs and smart-contract templates for early integrators

This phase establishes the architectural bedrock required for enforceable digital rights and enables the first production use cases.

10.2 Phase II — Vertical Integrations

TARGETED DEPLOYMENTS IN HIGH-IMPACT DOMAINS

Once the core architecture is stable, TrustLogic will focus on integrating with industries where enforceability solves immediate, acute pain points. These integrations serve as proof points for broader institutional adoption and help refine rule templates, workflows, and compliance mechanisms.

Priority verticals include:

- creative IP licensing and royalty enforcement
- software licensing and confidential-access control
- ticketing and event access
- purpose-bound remittances and humanitarian aid
- AI dataset governance and model usage tracking
- insurance claim integrity and fraud prevention
- conditional financial instruments and programmable banking

Each integration demonstrates the utility of governed entitlements and provides industry-specific rule sets that can be reused across similar institutions.

LEGAL TRUSTEE ENTITY TEMPLATES & LICENSING PACKAGES

As vertical deployments mature, TrustLogic will develop standardized **legal trustee entity templates** and **licensing packages** tailored to the needs of creators, enterprises, financial institutions, and public-sector agencies. These templates define how a trustee entity may be structured under existing trust, fiduciary, or custodial law and provide ready-made legal frameworks for operating a Trustee Token governance environment.

Deliverables include:

- template legal structures for institutional trustees,
- licensing agreements governing commercial use of the trustee environment,
- standardized rule-definition packages for creative, financial, and AI-related rights,
- operational playbooks for trustee duties, dispute intake, and compliance workflows.

These templates and licensing packages ensure that organizations adopting TrustLogic can deploy a trustee entity that is both **legally aligned** and **protocol-compliant**, smoothing the transition toward the broader regulatory and institutional integrations planned in Phase III.

10.3 Phase III — Institutional-Grade Compliance and Governance

ALIGNING WITH REGULATORY AND COMMERCIAL REQUIREMENTS

Phase III expands the system to meet the requirements of regulated industries, including banking, payments, entertainment, insurance, and enterprise software. This phase introduces advanced compliance modules and operational governance features needed for broad institutional deployment.

Key focus areas include:

- enhanced identity–rights separation for GDPR, HIPAA, and financial compliance
- expanded revocation logic and delegated authority for regulated workflows
- audit-ready event logs and lifecycle tracking
- selective disclosure and ZK-based compliance attestations
- configurable time-delayed governance updates
- emergency-freeze and crisis-response mechanisms

This phase ensures that TrustLogic meets the security, auditability, and trust requirements of high-compliance markets.

10.4 Phase IV — Cross-Chain Expansion

EXTENDING ENFORCEABILITY ACROSS MULTI-CHAIN ECOSYSTEMS

TrustLogic's authority-anchored model enables rights to move across chains without sacrificing enforcement. Phase IV focuses on making this cross-chain capability robust, seamless, and widely interoperable.

Objectives include:

- bridging logic for cross-chain Beneficiary Token reissuance
- maintaining Trustee Token governance on a canonical authority chain
- ensuring custody-layer anchoring and no-wrapping protections
- integrating with major EVM chains, L2 rollups, and modular architectures
- supporting industry networks, appchains, and enterprise sidechains

This phase enables developers and institutions to deploy TrustLogic across diverse execution environments while preserving enforceability.

10.5 Phase V — Ecosystem Expansion & Marketplace Integration

SCALING INTO A NETWORK OF RIGHTS-AWARE DIGITAL MARKETS

As adoption increases, TrustLogic will expand into an ecosystem of interconnected applications, marketplaces, and institutional systems that share a common rights enforcement framework. This phase emphasizes interoperability, industry alignment, and network effects.

Focus areas include:

- standard rule libraries for media, finance, AI, and enterprise IT
- marketplace plug-ins and reference implementations
- DAO or consortium-based governance for multi-party ecosystems
- shared IP defense pools and compliance alliances
- developer grants and ecosystem incentive programs

This phase transforms TrustLogic from a protocol into a rights-aware digital infrastructure standard capable of supporting entire industries.

10.6 Phase VI — Broad Institutional and Public-Sector Deployment

ENFORCEABILITY AS A PUBLIC INFRASTRUCTURE LAYER

The final phase focuses on full-scale institutional and government adoption. TrustLogic becomes a foundational architecture for enforceable digital rights across public payments, regulated finance, content licensing, and AI governance.

Potential deployment domains include:

- national or regional CBDC architectures
- public-sector entitlement and subsidy programs
- cross-border regulatory cooperation
- global creative licensing standards
- AI safety and dataset governance frameworks
- international insurance and financial markets

At this stage, TrustLogic operates as a protocol-level enforcement layer across sectors, delivering the governance, revocation, and conditional rights management capabilities required for trusted digital economies.

10.7 A Roadmap Designed for Stability and Adoption

BALANCING INNOVATION WITH INSTITUTIONAL PREDICTABILITY

The implementation roadmap is designed to balance rapid innovation with the stability and trust demanded by real-world institutions. Each phase builds on the enforcement guarantees of the prior phase, ensuring that the system grows without sacrificing predictability, compliance, or security.

TrustLogic is not just a technical protocol—it is an evolving governance and rights infrastructure intended to support the next generation of digital markets, cultural economies, financial systems, and public-sector digital value networks.

10.8 Intellectual Property Status

TrustLogic's core architecture—including the separation of authority and rights, the revocable trust layer, the dual-token enforcement model, and the multi-wallet custody structure—is the subject of multiple patent filings (U.S. non-provisional and provisional applications filed in 2025).

These filings cover the protocol logic and the enforcement primitives that enable revocable, governed digital rights.

While the protocol is designed to be openly licensable, the existence of patent protection ensures that enterprises, institutions, and ecosystem partners can build on the technology with confidence that the enforceability guarantees are protected against unauthorized modification or fragmentation.

11. Conclusion

The TrustLogic architecture introduces enforceability as a first-class primitive for digital rights, addressing structural weaknesses in current token systems and enabling real-world licensing, compliance, and governance to exist within decentralized environments. By separating authority from rights, anchoring enforcement in the Trustee Token, and implementing a custody model that prevents unauthorized extraction or wrapping, TrustLogic restores the core mechanisms that legal and commercial systems rely on to maintain trust.

Traditional digital assets collapse ownership, control, and usage into a single transferable object—an architecture incompatible with licensing law, regulatory compliance, or institutional governance. TrustLogic provides a fundamentally different model: digital assets become governed entitlements whose behavior is constrained and validated at every stage of their lifecycle. This shift transforms digital assets from brittle bearer instruments into rights that behave predictably across platforms, chains, and jurisdictions.

ENFORCEABILITY AS A PROTOCOL LAYER

The dual-token architecture ensures that obligations, restrictions, and revocation rights remain enforceable even when Beneficiary Tokens circulate between users or across chains. Instead of relying on marketplaces, platforms, or intermediaries to uphold contractual terms, TrustLogic embeds enforcement directly into the protocol layer. This eliminates the fragility of metadata-based licensing systems, NFT royalty flags, and off-chain terms of service. Rights become enforceable by design, not by marketplace preference.

EMPOWERING INSTITUTIONS, CREATORS, AND USERS

TrustLogic enables institutions to adopt Web3-native rights with the same control they expect in traditional environments. Studios can enforce licensing boundaries; financial institutions can issue conditional or purpose-bound entitlements; insurers can prevent double-claims; data providers can control AI training rights; and governments can distribute CBDCs or aid with both privacy and enforceability.

At the same time, users retain clear, transparent, and predictable rights. Beneficiary Tokens provide a governed but portable representation of entitlements—capable of movement across wallets, platforms, and chains without forfeiting compliance guarantees. This balance between authority and flexibility creates a rights system that supports user freedom without sacrificing institutional trust.

A FOUNDATION FOR RIGHTS-AWARE DIGITAL ECONOMIES

As digital markets expand—from creative IP to AI, finance, public services, and global commerce—the ability to enforce rules becomes increasingly critical. TrustLogic provides the missing infrastructure required for these markets to function at scale: a governance-aligned, revocation-capable, identity-optional, cross-chain compatible enforcement layer.

By anchoring rules, rights, and revocation in a unified protocol framework, TrustLogic enables digital markets to behave more like the legal and commercial systems they are meant to complement. This creates the conditions for new categories of applications, marketplaces, and collaborations that were previously infeasible because enforceability was absent.

THE PATH FORWARD

The TrustLogic roadmap lays out a structured path for ecosystem growth: foundational protocol deployment, targeted vertical integrations, institutional regulatory alignment, cross-chain expansion, ecosystem scaling, and broad public-sector adoption. Each step builds on the enforcement guarantees established in the authority–rights architecture, ensuring that as the ecosystem grows, it does so with stability, accountability, and trust.

TrustLogic is poised to become the enforcement layer for the next generation of digital rights. By combining clear governance, programmable authority, identity–rights separation, and a secure custody model, it establishes a durable foundation for digital economies that are fair, compliant, and aligned with real-world contractual norms.

TrustLogic represents not only a protocol innovation, but a shift in how digital rights are defined, governed, and enforced—unlocking a future where institutions, creators, and users can participate in digital markets with confidence.