CONFIDENTIAL

UNITED KINGDOM INTELLECTUAL PROPERTY OFFICE

PATENT APPLICATION

Applicant

The Bitcoin Corporation Ltd

Title of Invention

Bit Trust: A Blockchain-Native Intellectual Property Registration System Using Identity Token Threads

Field of the Invention

The present invention relates to systems and methods for registering intellectual property on a blockchain using cryptographic identity tokens as provenance threads. More particularly, the invention concerns a system that combines a signing tool, on-chain identity tokens (referred to as "$401 tokens"), and an encrypted vault to create a tiered, blockchain-native IP registration mechanism with graduated evidentiary weight and selective disclosure capabilities.

Background of the Invention

Problem Statement

Intellectual property registration and protection suffer from several longstanding deficiencies:

1. **Cost and Delay** — Formal IP registration (patents, trade marks, copyright registration in jurisdictions that offer it) is expensive and slow. Creators, particularly independent developers, artists, and small enterprises, often cannot afford or justify the cost of formal registration for every piece of work they produce.

2. **Proof of Prior Art** — Establishing that a work existed at a particular point in time (prior art evidence) traditionally requires trusted third parties: solicitors, notaries, registered post services, or centralised timestamping authorities. These are cumbersome, costly, and introduce counterparty risk.

3. **Identity Binding** — Existing blockchain timestamping services (e.g., OpenTimestamps, OriginStamp) can prove that a document existed at a given time, but they do not cryptographically bind the document to a verified identity. A timestamp proves existence but not authorship.

4. **Graduated Evidence** — The legal weight of IP evidence varies by jurisdiction and context, yet existing systems offer only binary registration: either you have a formal registration or you do not. There is no mechanism for graduated, tiered evidence that accumulates strength over time as additional attestations are added.

5. **Confidentiality vs. Disclosure** — Registering IP often requires disclosing its contents (e.g., patent specifications become public). For trade secrets, unpublished works, and pre-patent ideas, creators need to prove existence and authorship without revealing the actual content to the public or to potential competitors.

6. **Fragmented Identity** — Creators may have multiple online identities (GitHub, Google, LinkedIn, domain ownership) but no unified mechanism to aggregate these into a single, verifiable identity chain that can be attached to IP registrations.

Prior Art Limitations

Blockchain timestamping services prove existence but not identity. Traditional IP registries bind identity but are slow, expensive, and centralised. Self-sovereign identity systems (e.g., DID/Verifiable Credentials) provide identity but lack a native IP registration mechanism. No existing system combines verified multi-provider identity, blockchain timestamping, encrypted content vaulting, and tiered evidentiary weight in a unified IP registration framework.

Summary of the Invention

The present invention provides a blockchain-native IP registration system (“Bit Trust”) comprising:

a. A signing tool that captures intellectual property content, generates a cryptographic hash thereof, and signs the hash using the creator’s private key;

b. An identity token system (“$401 tokens”) comprising on-chain identity inscriptions, each linked to a verified OAuth identity provider, that form an identity chain (or “identity thread”) establishing the creator’s verified identity;

c. An encrypted vault that stores the actual IP content in encrypted form, accessible only to authorised parties, whilst the cryptographic hash of the content is inscribed on-chain;

d. A tiered trust registration mechanism that assigns graduated evidentiary weight to IP registrations based on the strength of the accompanying identity verification, the number of independent attestations, and the elapsed time since registration;

e. A selective disclosure mechanism that allows the creator to prove the existence, timestamp, and authorship of registered IP without revealing the actual content, and to selectively reveal specific portions of the content to designated parties.

Detailed Description of the Invention

1. System Architecture

The Bit Trust system comprises the following principal components:

1.1 The $401 Identity Token System

The $401 identity token system provides the identity layer for IP registration. It operates as follows:

1. **Root Inscription** — When a user first registers, a root identity inscription is created on the BSV blockchain. This root inscription contains: a public key, a unique user identifier, and metadata establishing the identity chain.

2. **Strand Inscriptions** — For each OAuth identity provider the user connects (e.g., GitHub, Google, LinkedIn, X/Twitter, Microsoft, domain ownership via DNS TXT record), a "strand" inscription is created on the BSV blockchain. Each strand inscription contains: the provider name, a cryptographic proof of the user's account on that provider (e.g., a signed challenge), the timestamp of verification, and a reference back to the root inscription.

3. **Identity Chain** — The root inscription plus all strand inscriptions form an "identity chain" or "identity thread." The strength of the identity is proportional to the number and diversity of connected providers. The system defines identity strength levels:

    - **Level 1**: Single provider (e.g., Google account only);
    - **Level 2**: Two providers from different categories;
    - **Level 3**: Three or more providers including at least one professional identity (GitHub, LinkedIn);
    - **Level 4+**: Additional attestations including domain ownership, corporate verification, or government-issued identity linkage.

4. **On-Chain Verifiability** — Any third party can verify a user's identity chain by reading the blockchain inscriptions and confirming the cryptographic proofs against the respective OAuth providers.

1.2 The Signing Tool

The signing tool is the primary interface through which creators register IP. It operates as follows:

1. **Content Capture** — The creator submits IP content to the signing tool. Content may be: source code, text documents, images, audio, video, datasets, designs, or any digital file. The signing tool accepts content via direct upload, URL reference, or API integration (e.g., Git commit hook, CI/CD pipeline integration).

2. **Hash Generation** — The signing tool computes a cryptographic hash (SHA-256) of the submitted content. For structured content (e.g., a Git repository), the tool may compute a Merkle root of all constituent files.

3. **Metadata Assembly** — The signing tool assembles registration metadata comprising: the content hash, a human-readable title and description (optional), the content type, the creator's $401 identity chain reference, the timestamp, and any additional tags or classifications.

4. **Signing** — The assembled registration data is signed using the creator's private key (the same key that anchors their $401 identity chain). The signature proves that the holder of the identity chain authorised the IP registration.

5. **Inscription** — The signed registration data is inscribed on the BSV blockchain as an immutable record. The inscription includes: the content hash, the signature, the $401 identity chain reference, and the timestamp. The actual content is NOT inscribed on-chain (see Section 1.3 — Encrypted Vault).

1.3 The Encrypted Vault

The encrypted vault stores the actual IP content whilst only the cryptographic hash is recorded on-chain. This solves the confidentiality-versus-disclosure problem:

1. **Encryption** — The IP content is encrypted using AES-256-GCM with a content encryption key (CEK) derived from the creator's master key. Each registration has a unique CEK.

2. **Storage** — The encrypted content is stored in a distributed storage system. The storage location reference (e.g., a content-addressable hash or a URI) is included in the on-chain inscription metadata.

3. **Access Control** — The creator holds the master decryption key. The creator may grant access to specific registrations by generating and sharing per-registration decryption keys. Access grants are themselves recorded on-chain as subsidiary inscriptions, creating an auditable access log.

4. **Integrity Verification** — Any party with access to the encrypted vault can decrypt the content and verify that its SHA-256 hash matches the hash inscribed on-chain, confirming that the content has not been altered since registration.

5. **Escrow and Dispute Resolution** — The system supports escrow arrangements whereby the decryption key for a specific registration is deposited with a trusted third party (e.g., a solicitor, an arbitration service) in a time-locked or condition-locked smart contract. In the event of a dispute, the escrow holder can unlock the content to verify the creator's claim.

1.4 Tiered Trust Registration

The tiered trust mechanism assigns graduated evidentiary weight to IP registrations. This is a significant innovation over binary registration systems:

Tier 1 — Timestamp Only - Content hash inscribed on-chain with timestamp. - No identity binding. - Evidentiary weight: proves existence at a point in time, but does not prove authorship. - Analogous to posting a sealed envelope to oneself.

Tier 2 — Identity-Bound Timestamp - Content hash inscribed on-chain with timestamp AND linked to a $401 identity chain (Level 1 or 2). - Evidentiary weight: proves existence and links to a verified online identity. Suitable for establishing prior art in informal disputes.

Tier 3 — Multi-Attestation Registration - Content hash inscribed on-chain, linked to a $401 identity chain (Level 3+), AND co-signed by one or more independent witnesses (other $401 identity holders who attest to having reviewed the content). - Evidentiary weight: proves existence, authorship (to a reasonable standard), and independent witness attestation. Suitable for pre-litigation evidence gathering.

Tier 4 — Professional Attestation - All elements of Tier 3, PLUS attestation by a recognised professional (solicitor, patent attorney, chartered accountant) whose own $401 identity chain includes professional body verification. - Evidentiary weight: approaches the standard of a statutory declaration or notarised document. Suitable for submission as evidence in court proceedings or IP office examinations.

Tier 5 — Institutional Registration - All elements of Tier 4, PLUS registration with or recognition by an institutional body (e.g., a collecting society, a trade body, or an IP office that accepts blockchain evidence). - Evidentiary weight: equivalent to formal registration.

Each tier builds upon the previous, and registrations can be upgraded over time by adding attestations. The on-chain record preserves the history of all attestations, showing when each was added.

1.5 Selective Disclosure Mechanism

The selective disclosure mechanism allows creators to prove aspects of their IP registration without revealing the full content:

1. **Zero-Knowledge Existence Proof** — The creator can prove that they registered content with a specific hash at a specific time, signed by a specific identity, without revealing what the content is. This is achieved by simply pointing to the on-chain inscription, which contains only the hash, not the content.

2. **Partial Content Disclosure** — For structured content (e.g., a software project with multiple files), the Merkle tree structure allows the creator to reveal specific files or sections whilst proving they are part of the registered whole, without revealing the remaining files.

3. **Time-Locked Disclosure** — The creator can set a future date at which the vault content becomes automatically decryptable, using time-locked encryption (e.g., based on blockchain block height). This is useful for embargoed publications, patent filing strategies, or scheduled releases.

4. **Designated Verifier Proofs** — The creator can generate a proof that is verifiable only by a designated party (e.g., a potential licensee, a court, or an IP examiner), preventing the proof from being forwarded or used by unintended recipients.

2. IP Thread Architecture

The concept of an “IP Thread” is central to the system. An IP Thread is a sequence of on-chain inscriptions representing the lifecycle of a piece of intellectual property:

1. **Creation Inscription** — The initial registration (content hash, identity binding, timestamp).
2. **Attestation Inscriptions** — Subsequent witness or professional attestations that increase the tier.
3. **Version Inscriptions** — Registrations of updated or derived versions, each referencing the original creation inscription.
4. **Licence Inscriptions** — Records of licences granted, including licensee identity, scope, duration, and terms.
5. **Transfer Inscriptions** — Records of ownership transfers or assignments.
6. **Dispute Inscriptions** — Records of disputes raised, evidence submitted, and resolutions.

Each inscription in the thread references the previous inscription, forming a linked chain. The complete thread provides a full, auditable history of the IP from creation through to current status.

3. Integration with $401 Protocol

The Bit Trust system is built upon the $401 identity protocol. The $401 protocol provides:

- Six OAuth identity providers: GitHub, Google, LinkedIn, X/Twitter, Microsoft, and domain ownership (via DNS TXT record);
- On-chain root and strand inscriptions forming a verifiable identity chain;
- Identity strength levels from 1 to 4+;
- A signing infrastructure that binds actions to verified identities.

Bit Trust extends the $401 protocol by using the same identity chain and signing infrastructure for IP registration. A user who has already established a $401 identity can immediately begin registering IP without additional setup. The IP registrations inherit the identity strength of the user’s $401 chain.

4. Operational Flow

A typical IP registration proceeds as follows:

1. The creator authenticates with the Bit Trust system using their $401 identity.
2. The creator submits IP content via the signing tool (upload, URL, or API).
3. The signing tool computes the SHA-256 hash of the content.

4. The content is encrypted and stored in the vault.
5. The signing tool assembles the registration metadata: content hash, $401 identity reference, timestamp, content type, and optional description.
6. The registration data is signed using the creator's private key.
7. The signed registration is inscribed on the BSV blockchain.
8. The system returns a registration receipt comprising the transaction ID, the content hash, the timestamp, and the current tier level.
9. Optionally, the creator invites witnesses or professionals to co-sign, upgrading the tier.

Brief Description of Drawings

The following drawings would accompany this application:

- **Figure 1** — System architecture diagram showing the signing tool, $401 identity token system, encrypted vault, and blockchain inscription layer, and their interconnections.
- **Figure 2** — $401 identity chain structure showing root inscription and strand inscriptions for each OAuth provider.
- **Figure 3** — IP registration data flow from content submission through hashing, signing, encryption, vault storage, and on-chain inscription.
- **Figure 4** — Tiered trust registration diagram showing the five tiers, the attestations required for each, and the graduated evidentiary weight.
- **Figure 5** — IP Thread lifecycle diagram showing creation, attestation, versioning, licensing, transfer, and dispute inscriptions as a linked chain.
- **Figure 6** — Selective disclosure mechanism showing zero-knowledge existence proof, partial content disclosure via Merkle tree, and designated verifier proofs.
- **Figure 7** — Encrypted vault architecture showing encryption, storage, access control, and escrow arrangements.

Initial Claims

Note: These claims are provided in sketch form for the purposes of establishing a priority date. Formal claims will be drafted and filed within 12 months in accordance with UKIPO rules.

Claim 1 — IP Thread System

A system for registering intellectual property on a blockchain, the system comprising: (a) a signing tool configured to receive intellectual property content, compute a cryptographic hash thereof, and sign the hash using a creator's private key; (b) an identity token system comprising on-chain identity inscriptions, each linked to a verified identity provider, forming an identity chain that establishes the creator's verified identity; (c) an encrypted vault for storing the intellectual property content in encrypted form; (d) an inscription engine configured to record, on a blockchain, an immutable registration comprising the content hash, the creator's identity chain reference, a timestamp, and the creator's cryptographic signature; wherein the registration cryptographically binds the intellectual property to the creator's verified identity and establishes the existence of the intellectual property at the time of inscription without disclosing the content itself.

Claim 2 — IP Registration Method

A method of registering intellectual property on a blockchain, the method comprising: (a) authenticating a creator using a blockchain-based identity chain comprising one or more on-chain identity inscriptions each linked to a verified OAuth identity provider; (b) receiving intellectual property content from the creator; (c) computing a cryptographic hash of the content; (d) encrypting the content and storing it in an encrypted vault; (e) assembling registration metadata comprising the content hash, a reference to the creator's identity chain, and a timestamp; (f) signing the registration metadata with the creator's private key; (g) inscribing the signed registration metadata on a blockchain as an immutable record.

Claim 3 — Tiered Trust Registration

A method of assigning graduated evidentiary weight to a blockchain-based intellectual property registration, the method comprising: (a) creating an initial registration at a first tier comprising a content hash and timestamp inscribed on a blockchain; (b) upgrading the registration to a second tier by linking the registration to a verified identity chain; (c) upgrading the registration to a third tier by obtaining and inscribing one or more independent witness attestations from additional verified identity holders; (d) upgrading the registration to a fourth tier by obtaining and inscribing a professional attestation from a verified professional identity holder; wherein each tier represents a higher evidentiary weight and each upgrade is recorded as a subsidiary inscription on the blockchain referencing the original registration.

Claim 4 — Selective Disclosure Vault

A method of proving the existence and authorship of intellectual property without disclosing its content, the method comprising: (a) storing the intellectual property in encrypted form in a vault, the vault being associated with a blockchain inscription containing a cryptographic hash of the intellectual property; (b) presenting the blockchain inscription to a verifier, the inscription comprising the content hash, a timestamp, and a reference to the creator's verified identity chain; (c) enabling the verifier to confirm the existence and timestamp of the registration and the identity of the creator from the blockchain inscription alone, without access to the vault content; (d) optionally, providing the verifier with a decryption key for all or a portion of the vault content, enabling the verifier to decrypt the content and confirm that its hash matches the hash in the blockchain inscription; wherein the creator controls what content, if any, is disclosed to the verifier.

Abstract

A blockchain-native intellectual property registration system comprising a signing tool, an on-chain identity token system (“$401 tokens”), and an encrypted vault. The signing tool computes a cryptographic hash of IP content and signs it using the creator’s private key. The identity token system provides verified identity chains composed of blockchain inscriptions linked to multiple OAuth identity providers. The encrypted vault stores IP content confidentially whilst only the hash is recorded on-chain. The system implements tiered trust registration with graduated evidentiary weight, from simple timestamping through to professional and institutional attestation. A selective disclosure mechanism allows creators to prove existence and authorship without revealing content. IP registrations form “IP Threads” — linked chains of inscriptions recording the full lifecycle of intellectual property from creation through licensing and transfer.

Document prepared for UKIPO filing. Priority date to be established upon submission. Applicant: The Bitcoin Corporation Ltd Date of preparation: 24 February 2026