PROVISIONAL PATENT APPLICATION: INTELLECTUAL PROPERTY, CYBERSECURITY, & DECENTRALIZED FINANCE

Invention Title: DECENTRALIZED LEDGER ARCHITECTURE FOR AUTOMATED ANCESTRAL PATENT TREE RECOGNITION, FRACTIONAL ROYALTY ROUTING, IMMUTABLE TRADE SECRET CUSTODY TRACKING, AND AUTOMATED PRIOR ART GENERATION

First Named Inventor:

Given Name(s): John Lawrence

Family Name: Coulson

City of Residence: Whistler

State/Province: British Columbia

Country: Canada V8E 1N7

Correspondence Address:

Name: John L. Coulson

Address: Suite 201 - 1330 Cloudburst Drive

City: Whistler

State/Province: BC

Country: Canada V8E 1N7

Email: jlc@sidogger.com

Entity Status: "Micro Entity"

U.S. Government Agency Interest: NO.

1. The Field of Invention

This invention relates to the intersection of intellectual property rights protection, decentralized finance (DeFi), and advanced cryptographic data custody tracking. Specifically, it provides a blockchain-based smart contract infrastructure designed to act as an automated digital Non-Disclosure Agreement (NDA), secure proprietary Trade Secrets against corporate espionage, execute automated Prior Art defensive publications, map the technological ancestry of composite inventions, and execute automated micro-royalty distributions across an entire development chain.

2. The Technical Problem

The current global patent paradigm, specifically under the "First to File" framework, exhibits a critical structural flaw: it forces independent inventors to publicly disclose highly sensitive technical architectures to centralized repositories before securing development funding. If an inventor attempts to pitch a major corporation without a signed Non-Disclosure Agreement (NDA) or a premature patent filing, they fall victim to the "Public Disclosure" loophole. This leaves independent architects exposed to industrial espionage and predatory corporate entities who routinely engage in "fishing expeditions" to misappropriate trade secrets and rush to file the patents themselves.

Traditional systems provide no structural mechanism to cryptographically prove "Prior Possession," financially penalize corporate breaches of confidence, or automatically invalidate predatory patent filings.

3. The Technical Solution: The "Ethical IP" Cryptographic Moat

The system resolves these existential vulnerabilities by establishing a decentralized cryptographic custody layer that wraps around an inventor's technical documentation, transforming a standard file transfer into an audited, trackable, and actively self-defending Trade Secret asset.

The Automated Digital NDA & Escrow Staking: An inventor registers their architecture on the decentralized ledger as a Trade Secret. To pitch a corporate entity, the inventor transmits a cryptographic access key. Accessing the key requires the reviewing corporation to lock a micro-financial deposit in a smart-contract escrow. Upon access, the contract permanently logs the recipient's digital identity and network IP address, establishing a legally binding Digital NDA and mathematical proof of Prior Possession.

The "Anti-Bury" Prior Art Trigger: The system utilizes semantic analysis to monitor global patent databases (USPTO, WIPO). If the system detects a corporate entity attempting to patent the locked architecture without authorization, the smart contract automatically forfeits the corporate escrow deposit to the inventor and executes an automated "Defensive Publication" to the blockchain. This instantly establishes global Prior Art, legally invalidating the predatory corporate patent application.

Ancestral Tech Tree Mapping ("A Cookie in Every Jar"): Upon any authorized commercial transaction within the network, the smart contract automatically splinters a micro-percentage of revenue, routing it back through the technical development chain to ensure all contributing architects and foundational creators are continuously compensated.

Zero-Knowledge Oracle & Heir Verification: The architecture utilizes decentralized Oracles running Zero-Knowledge Proofs to query off-chain legal registries, confirming the status of foundational inventors and automatically routing distributions to verified estate or heir wallets without human administration.

The "Orphaned Asset" Humanitarian Pool: In instances where an ancestral creator is deceased and no heirs can be cryptographically verified, the smart contract automatically routes those micro-royalties into an autonomous endowment pool strictly coded to fund environmental remediation and independent inventor micro-grants.

The "Poison Pill" Litigation Defense: The cryptographic transfer and acceptance of a micro-royalty to a node on the ancestral tree automatically registers an immutable "Covenant Not to Sue" on the ledger, instantly disarming predatory patent assertion entities.

4. DETAILED DESCRIPTION OF THE DRAWINGS (LOGIC FLOWCHARTS)

Flowchart 1: The Automated Digital NDA & Escrow Staking

BOX 1: Inventor uploads proprietary technical documentation into the secure ledger-wrapped repository as an unregistered Trade Secret.

BOX 2: Inventor generates and transmits a localized cryptographic access key to a target enterprise entity for development and or funding pitching.

BOX 3: Enterprise entity must stake a predefined financial escrow deposit into the smart contract to unlock the cryptographic key.

BOX 4: System intercepts the access request, permanently logging the entity's digital signature, network IP address, and exact file kilobyte interactions.

BOX 5: Smart contract generates an un-erasable forensic receipt on the blockchain, establishing an automated Digital NDA and mathematical proof of Prior Possession.

Flowchart 2: Ancestral Micro-Distribution & Litigation Neutralization

BOX 1: Host technology suite executes a commercial licensing transaction, triggering the "Ethical IP" smart contract.

BOX 2: Contract splinters the designated revenue micro-percentage and maps it against the hardcoded development chain.

BOX 3 (Decision Node): Is the target foundational creator node active, or are legal heirs verified via the Zero-Knowledge legal Oracle?

If YES: Funds are instantly routed to the cryptographically verified wallet. Proceed to BOX 4.

If NO: Proceed to Flowchart 5 (Orphaned Asset Allocation).

BOX 4: The successful ledger transaction automatically mints and locks an immutable Covenant Not to Sue, shielding the network from retroactive infringement litigation.

Flowchart 3: Semantic Global Monitoring

BOX 1: System continuously runs a semantic diagnostic analysis of the inventor's Trade Secret payload against incoming global patent filings (e.g., USPTO, WIPO data streams).

BOX 2: System identifies a structural algorithmic match between the inventor's locked Trade Secret and a newly filed corporate patent application.

BOX 3: System verifies the filing corporate entity against the Digital NDA access logs from Flowchart 1 to confirm breach of confidence.

Flowchart 4: The "Anti-Bury" Prior Art Defense & Escrow Forfeiture

BOX 1: Breach of confidence is verified via Flowchart 3.

BOX 2: Smart contract instantly terminates the corporate entity's access to the Trade Secret repository.

BOX 3: Smart contract automatically liquidates the staked corporate escrow deposit and transfers the funds to the independent inventor as punitive damages.

BOX 4: System executes an automated, cryptographically time-stamped Defensive Publication of the core algorithmic concepts to a public blockchain node.

BOX 5: The Defensive Publication legally establishes global Prior Art predating the corporate filing, instantly invalidating the predatory patent application.

Flowchart 5: Orphaned Asset & Humanitarian Routing

BOX 1: Zero-Knowledge Oracle confirms a vacant lineage with no living heirs or verified estate for an ancestral patent node.

BOX 2: Smart contract diverts the unallocated micro-royalties directly into the autonomous Innovation & Charity Pool.

BOX 3: System executes automated disbursements to verified environmental initiatives and micro-grant portfolios for emerging independent inventors.

5. REPRESENTATIVE CLAIMS

Claim 1: A decentralized, computer-implemented system for tracking intellectual property data custody and executing automated financial routing, comprising: a secure ledger repository housing a technical data payload; a data custody monitoring protocol configured to intercept any external interaction with said payload and immutably record a forensic identity metric, access timestamp, and file-volume index onto a blockchain; and an automated smart contract configured to trace an ancestral technology tree and execute fractional revenue distributions to registered nodes on said tree upon a commercial transaction.

Claim 2: The system of Claim 1, wherein the data custody monitoring protocol establishes an automated digital non-disclosure agreement by generating an un-wipeable chain-of-custody log upon an authorized third-party accessing the payload, providing cryptographic proof of prior possession and trade secret custody.

Claim 3: The system of Claim 2, wherein accessing the technical data payload requires a reviewing entity to lock a financial deposit within a smart-contract escrow, said deposit being programmatically forfeited to the inventor upon verification of a breach of confidence.

Claim 4: The system of Claim 1, further comprising a semantic global monitoring module configured to cross-reference the technical data payload against global patent registries, wherein the detection of an unauthorized matching corporate filing automatically triggers a cryptographically time-stamped defensive publication to the blockchain to establish undeniable global prior art.

Claim 5: The system of Claim 1, wherein the cryptographic transfer of a fractional revenue distribution to an ancestral node automatically binds the recipient node to a verifiable Covenant Not to Sue.