



TSG LAB AG — USE CASE 2

Diamond NFT Authentication & Provenance System

Immutable Digital Twins for the World's Most Valuable Natural Assets

NFT

BLOCKCHAIN

IOT INSTRUMENTS

ERC-721

DEFI COLLATERAL

01 Executive Summary

TSG Lab AG's Diamond NFT Authentication & Provenance System creates a cryptographically secured, on-chain digital twin for every certified stone. Each diamond receives a unique Non-Fungible Token capturing its full identity — 4C grading data, laser inscription registry numbers, 3D scan models, spectroscopic fingerprints, and the complete chain of custody from mine to owner.

The global diamond industry, valued at over USD 90 billion annually, remains plagued by authentication and provenance challenges. The Kimberley Process relies on paper certificates that can be forged, duplicated, or detached from the physical stone. IoT-enabled grading instruments, IPFS-based media storage, and Ethereum smart contracts create an ecosystem where authentication is instant, provenance is irrefutable, and ownership transfers are frictionless.

02 Business Challenge

- ▶ **Documentation Fraud:** An estimated 5–8% of diamonds in secondary markets carry fraudulent or mismatched documentation — paper certificates can be forged, re-used, or detached from the original stone.
- ▶ **Conflict Diamond Infiltration:** Conflict diamonds continue to enter legitimate supply chains through Kimberley Process documentation gaps, creating ethical and reputational risk.
- ▶ **Synthetic Substitution:** Lab-grown diamonds are increasingly sold fraudulently as natural stones — a trend growing at 15% annually, virtually undetectable without advanced spectroscopic analysis.
- ▶ **Fragmented Chain of Custody:** A diamond changes hands 10–15 times from mine to retail with no interoperable documentation, creating information asymmetry and trust gaps.
- ▶ **Insurance & Resale Friction:** Without verifiable provenance, insurance requires expensive appraisals and resale markets suffer 30–40% price discounts due to buyer uncertainty.
- ▶ **Lack of Consumer Transparency:** End consumers have no practical way to independently verify origin, treatment history, or ethical sourcing.

03 Technical Solution

IoT Capture — Digital Fingerprinting

Integration with gemological instruments (Sarine DiaMension, OGI Metropro, Raman spectroscopy) enables automated capture of each diamond's unique physical fingerprint. High-resolution 360° imaging, photoluminescence spectra, and 3D laser scan point clouds are digitized at grading. A dedicated scanner firmware plugin hashes all captured data at the instrument level before transmission to the minting pipeline.

NFT Minting Engine

A purpose-built minting pipeline validates incoming gemological data against schema standards (GIA, AGS, HRD format compatibility) and deploys NFTs to Ethereum mainnet using ERC-721 with custom extensions (ERC-4907 for rental/lending, ERC-5192 for soulbound attestations). Large media assets are pinned to IPFS via Filecoin with CIDs embedded in on-chain metadata.

Smart Contract Suite

DiamondRegistry.sol — Core NFT contract with diamond-specific metadata extensions and grading authority whitelisting.

ProvenanceTracker.sol — Append-only event log recording every custody transfer, re-grading, setting, and insurance event.

AuctionHouse.sol — English and Dutch auction contracts with automated escrow and royalty distribution.

InsuranceBridge.sol — Parametric insurance integration with automatic claim initiation upon verified theft or loss events.

Verification Application

A consumer-facing mobile application (iOS/Android) enables instant authentication: scanning a diamond's laser inscription number or NFC-enabled jewelry tag retrieves the on-chain NFT, displays the full provenance timeline, renders the 3D scan model, and confirms current ownership — all without requiring blockchain knowledge from the end user.

04 Implementation Approach

Phase	Activities	Duration
Phase 1: Industry Partnership	GIA/HRD/IGI schema alignment, instrument integration planning, NFT-certificate legal framework	6–8 weeks
Phase 2: IoT Integration	Firmware plugins for Sarine/OGI/spectroscopy, digital fingerprint capture pipeline, data validation	6–8 weeks
Phase 3: Smart Contract Dev	NFT contract (ERC-721 + extensions), provenance tracker, auction module, insurance bridge + audit	8–10 weeks

Phase 4: IPFS & Media Pipeline	3D scan rendering, spectral data visualization, IPFS/Filecoin pinning, CDN integration	4–6 weeks
Phase 5: Consumer Application	React Native mobile app, NFC integration, 3D model viewer (Three.js/WebGL), provenance timeline UI	6–8 weeks
Phase 6: Pilot & Rollout	Pilot with 3–5 dealers, 500+ stone tokenizations, feedback integration, production launch	6–8 weeks

05 Technology Stack

Layer	Technologies
IoT / Instruments	Sarine DiaMension HD, OGI Metropro, Raman spectroscopy (Renishaw inVia), NFC tags (NTAG 424 DNA)
Blockchain	Ethereum Mainnet, Polygon PoS (cost-efficient minting), Arbitrum (high-frequency updates)
Token Standards	ERC-721 (core NFT), ERC-4907 (rentable), ERC-5192 (soulbound), ERC-2981 (royalty)
Smart Contracts	Solidity 0.8.x, OpenZeppelin, Chainlink VRF (auction fairness), Chainlink Functions
Storage	IPFS, Filecoin (persistent pinning), Arweave (permanent archival of grading reports)
Consumer App	React Native, Three.js/WebGL, NFC reader SDK, WalletConnect/Web3Auth
Identity	W3C DIDs for grading labs, Verifiable Credentials (W3C VC) for authorized graders
Backend	Node.js, GraphQL (The Graph subgraph), PostgreSQL, Redis, AWS Lambda

06 Key Features & Capabilities

- Unique Digital Fingerprint** — Multi-modal fingerprint (spectroscopic, photographic, geometric) that is computationally impossible to replicate or transfer to another stone.
- Immutable Provenance Timeline** — Every lifecycle event recorded as an on-chain event, creating a fully auditable history from mine to owner.
- Instant Consumer Verification** — Mobile app returns full provenance data, 3D visualizations, and ownership confirmation in under 3 seconds via NFC or inscription scan.
- Fractional Ownership Support** — High-value investment-grade diamonds fractionalized via ERC-1155 companion tokens for democratized collective ownership.

✓**Automated Royalty Distribution** — ERC-2981 royalty enforcement ensures original dealers receive a configurable percentage on every secondary market resale.

✓**Anti-Fraud Safeguards** — Cross-reference engine detects duplicate inscription numbers, re-used certificate images, and suspicious transfer patterns.

✓**Insurance Integration** — Parametric smart contracts enable automatic claim initiation and settlement upon verified loss/theft events.

07 Business Benefits & ROI

Fraud Elimination

Elimination of certificate forgery and synthetic substitution — projected industry savings of USD 2–4 billion annually

Increased Resale Value

Verified provenance narrows secondary market discount from 30–40% to 5–10%

Consumer Trust Premium

Retailers with NFT-authenticated diamonds report 18–25% higher conversion rates in pilot programs

Insurance Efficiency

Automated parametric insurance reduces claim processing from 45 days to under 72 hours

Regulatory Compliance

On-chain provenance satisfies Kimberley Process and EU due diligence regulations

New Revenue Channels

Secondary market auction platform generates 1–2.5% transaction fee revenue per sale

08 Use Case Scenarios

Mine-to-Retail Full Lifecycle

A 3.2-carat diamond extracted in Botswana receives an NFT at rough grading capturing mine location, extraction date, and rough stone characteristics. As it is cut and polished in Antwerp, metadata is updated. GIA grades the finished stone; 4C data is appended on-chain. The diamond is sold in Zurich, then to a consumer who scans the NFC tag in their engagement ring to view the complete journey.

Investment-Grade Diamond Fractionalization

A rare 15-carat Type IIa diamond appraised at USD 8 million is fractionalized into 10,000 ERC-1155 tokens. Accredited investors purchase fractions, with smart contracts governing voting rights on storage, insurance, and eventual sale decisions. When auctioned at Christie's five years later, proceeds are automatically distributed proportionally.

Insurance Claim Automation

A collector reports the theft of an NFT-authenticated 5-carat diamond. Upon filing a verified police report, the InsuranceBridge smart contract automatically initiates the parametric insurance claim, locks the NFT preventing fraudulent resale, and triggers a settlement payment within 72 hours.

09 Security & Compliance

- **Physical-Digital Binding:** NFC tags use NTAG 424 DNA with cryptographic authentication — each tap generates a unique, verifiable signature preventing cloning.
- **Grading Authority Verification:** Only whitelisted grading labs (verified via DIDs and Verifiable Credentials) can create or update diamond NFTs.
- **Transfer Restrictions:** Smart contracts enforce KYC/AML compliance via zero-knowledge proofs for high-value transfers, preserving privacy.
- **GDPR Compliance:** Personal ownership data stored off-chain with encrypted references; only pseudonymous wallet addresses appear on-chain.
- **Kimberley Process Alignment:** On-chain provenance records satisfy and exceed Kimberley Process certification requirements.
- **Smart Contract Audits:** Formal verification (Certora) and independent audits (Trail of Bits, OpenZeppelin) before mainnet deployment.

10 Future Enhancements

AI-Powered Grading Verification: Computer vision models trained on millions of grading images to detect inconsistencies between stated grades and visual evidence.

Cross-Chain Diamond Passport: Interoperable NFTs verifiable across Ethereum, Solana, and private enterprise chains via LayerZero omnichain messaging.

Metaverse Integration: Render NFT-authenticated diamonds as photorealistic 3D assets in metaverse environments for virtual try-on and digital showcasing.

Carbon Footprint Tracking: Extend provenance data to include verified carbon emissions at each supply chain stage for sustainability-conscious purchasing.

DeFi Collateralization: Enable NFT-authenticated diamonds to serve as collateral in DeFi lending protocols, unlocking liquidity without physical asset transfer.