TSG

TSG LAB AG — USE CASE 1

IoT-Blockchain Integration Platform

Bridging Physical Devices to Immutable Digital Infrastructure

IOT | BLOCKCHAIN | SMART CONTRACTS | EDGE COMPUTING | MULTI-CHAIN

info@tsgag.com | tsgag.com

01 Executive Summary

> TSG Lab AG's IoT-Blockchain Integration Platform solves the fundamental trust deficit in machine-generated data. The platform provides a hardware-agnostic middleware layer that ingests telemetry from any IoT device, cryptographically signs data at the edge, and anchors immutable proofs to high-throughput blockchain networks. Smart contracts autonomously execute business logic — triggering payments, alerts, compliance reports, or supply chain state transitions — based on verified, tamper-proof sensor readings.

The proliferation of IoT devices across industries has created an unprecedented volume of machine-generated data. Yet this data remains overwhelmingly siloed, mutable, and vulnerable to tampering. Organizations making critical decisions based on sensor telemetry have no cryptographic guarantee that data has not been altered between capture and consumption. This platform delivers a paradigm shift from *data collection* to *data attestation* — providing real-time, auditable, and legally defensible records of physical-world events, while smart contract automation eliminates manual reconciliation and unlocks new categories of machine-to-machine commerce.

02 Business Challenge

- **Data Tampering & Fraud:** Sensor readings in conventional databases can be retroactively modified — a severe liability in regulated industries where audit trails carry legal weight.
- **Single Points of Failure:** Centralized IoT clouds create availability risks; a single outage can blind an organization to real-time operational conditions.
- **Interoperability Barriers:** Proprietary IoT ecosystems lock organizations into vendor-specific platforms, making cross-enterprise data sharing expensive and fragile.
- **Manual Reconciliation Overhead:** Gaps between data capture and action require human intermediation, introducing delays and errors in time-critical processes.
- **Regulatory Compliance Gaps:** EU Data Act, GDPR, and industry-specific mandates (GxP, ISO 22000) require provable data provenance that centralized systems cannot cryptographically guarantee.

03 Technical Solution

Four-Layer Architecture

Edge Layer — Secure Data Origination: Lightweight firmware agents on IoT gateways perform local preprocessing, anomaly filtering, and cryptographic signing using HSMs or TPMs. Each data packet receives a device-bound digital signature before leaving the edge.

Middleware Layer — Protocol Translation & Orchestration: A containerized microservices mesh handles protocol translation (MQTT → AMQP → REST → gRPC), data normalization, and batching. A proprietary *Merkle-DAG anchoring* strategy aggregates high-frequency sensor data into time-windowed Merkle trees — only root hashes are committed on-chain, preserving integrity while minimizing gas costs by up to 98%.

Blockchain Layer — Immutable Anchoring & Smart Contract Execution: Multi-chain strategy supporting Ethereum L1/L2 (Arbitrum, Optimism, zkSync) for high-value attestations; Solana for latency-sensitive sub-second finality; and Hyperledger Fabric for permissioned enterprise deployments. Smart contracts encode SLA enforcement, automated escrow releases, compliance reporting, and cross-organizational event subscriptions.

Application Layer — APIs & Dashboards: RESTful and GraphQL APIs expose verified data streams to ERP, MES, and SCM systems. A real-time monitoring dashboard provides device health, data integrity status, on-chain transaction history, and smart contract execution logs.

04 Implementation Approach

Phase	Activities	Duration
Phase 1: Discovery & Design	IoT estate audit, blockchain selection, smart contract specification, security threat modeling	4–6 weeks
Phase 2: Edge Integration	Firmware agent deployment, HSM/TPM provisioning, MQTT/CoAP broker configuration	4–6 weeks
Phase 3: Middleware & Chain	Kubernetes deployment, microservices, Merkle-DAG engine, smart contract testnet deployment	6–8 weeks
Phase 4: Smart Contract Dev	Business rule encoding, formal verification (Certora/Slither), oracle integration	4–6 weeks
Phase 5: Testing & Audit	End-to-end validation, penetration testing, third-party audit, load testing	4 weeks
Phase 6: Production Launch	Phased rollout, monitoring activation, gas optimization, operator training	2–4 weeks

05 Technology Stack

Layer	Technologies
Edge / IoT Protocols	MQTT 5.0, CoAP, MQTT-SN, OPC-UA, Modbus TCP, BLE 5.3, LoRaWAN
Edge Security	ARM TrustZone, TPM 2.0, ATECC608B HSM, X.509 device certificates
Middleware	Kubernetes (K3s), Apache Kafka, NATS, gRPC, Protocol Buffers
Blockchain (L1)	Ethereum, Solana, Hyperledger Fabric 2.x
Blockchain (L2)	Arbitrum, Optimism, zkSync Era, Polygon zkEVM
Smart Contracts	Solidity 0.8.x, Rust/Anchor (Solana), Chaincode (Go)
Data Integrity	Merkle-DAG, SHA-256, ECDSA (secp256k1), Ed25519
Storage	IPFS/Filecoin (off-chain), TimescaleDB, PostgreSQL
Monitoring	Grafana, Prometheus, The Graph, custom alerting

06 Key Features & Capabilities

✔**Universal Device Connectivity** — Hardware-agnostic integration supporting 50+ IoT protocols and gateway platforms from Siemens, Bosch, Advantech, and others.

✔**Cryptographic Data Provenance** — Every data point is signed at device level and anchored to blockchain, providing a tamper-evident chain of custody from sensor to smart contract.

✔**Merkle-DAG Batching Engine** — Proprietary mechanism reduces on-chain costs by up to 98% while preserving individual data point verifiability via inclusion proofs.

✔**Multi-Chain Abstraction** — A single API abstracts Ethereum, Solana, and Hyperledger, enabling per-use-case chain selection without application changes.

✔**Autonomous Smart Contract Triggers** — Configurable rule engines translate IoT events into smart contract calls — no human intermediation for SLA enforcement, payments, or alerts.

✔**Real-Time Integrity Dashboard** — Unified visualization of device status, data integrity scores, on-chain anchoring latency, and smart contract execution history.

✔**Offline Resilience** — Edge agents buffer and sign data during connectivity outages, syncing and anchoring upon reconnection without data loss.

07 Business Benefits & ROI

Elimination of Data Disputes

Cryptographic proof reduces dispute resolution costs by up to 70% in supply chain and insurance contexts

Automated Compliance Reporting

On-chain audit trails satisfy EU Data Act, GxP requirements with zero manual report generation

Reduced Settlement Times

Smart contract automation compresses multi-day reconciliation to near-real-time execution

Lower Insurance Premiums

Verifiable operational data enables parametric insurance with 15–30% premium reductions

New Revenue Streams

Monetization of verified IoT data through blockchain-based data marketplaces

Operational Continuity

Decentralized architecture improves system uptime to 99.97%+

08 Use Case Scenarios

Cold-Chain Pharmaceutical Logistics

A European pharmaceutical distributor deploys temperature and humidity sensors across 2,000 transport containers. Readings are anchored every 60 seconds to Ethereum L2. When a shipment's temperature exceeds the 2–8°C threshold, a smart contract automatically triggers a quality hold in the warehouse management system, notifies QA, and initiates a parametric insurance claim — all within 90 seconds of the excursion event.

Smart Building Energy Optimization

A commercial real estate operator connects 10,000 smart meters across a building portfolio. Energy data is anchored to Solana for sub-second finality. Smart contracts enforce peak-load curtailment agreements and automate demand-response participation with the grid operator, generating verified carbon offset certificates stored on IPFS.

Industrial Predictive Maintenance

A manufacturing conglomerate streams vibration, temperature, and acoustic data from CNC machines. On-chain anchored maintenance logs create verifiable equipment histories that increase resale values by 12–18% and satisfy ISO 55000 asset management requirements.

09 Security & Compliance

- **Device Identity Management:** X.509 certificate-based device authentication with automated rotation and revocation via on-chain certificate registries.
- **End-to-End Encryption:** TLS 1.3 for data in transit; AES-256-GCM at rest; HSM-backed key management at the edge.
- **Smart Contract Security:** Formal verification (Certora), static analysis (Slither, Mythril), mandatory third-party audits before mainnet deployment.
- **Access Control:** Role-based access control (RBAC) with multi-signature governance for smart contract upgrades.
- **Regulatory Alignment:** GDPR, EU Data Act, ISO 27001, SOC 2 Type II, GxP, HACCP, ISO 22000 — data minimization via hash-only anchoring.
- **Incident Response:** Automated anomaly detection with tiered alerting and forensic log preservation.

10 Future Enhancements

Zero-Knowledge Proofs: Integration of zk-SNARKs to enable third-party data verification without revealing underlying sensor values.

DePIN Networks: Enable IoT device owners to monetize hardware and data contributions through token-incentivized Decentralized Physical Infrastructure Networks.

AI-at-the-Edge Fusion: Lightweight ML models on edge gateways for real-time anomaly detection, feeding classified events to smart contracts.

Cross-Chain Interoperability: Integration with LayerZero, Chainlink CCIP, and Wormhole for seamless multi-chain attestation.

Digital Twin Synchronization: Real-time sync between on-chain verified IoT data and digital twin platforms (NVIDIA Omniverse, Azure Digital Twins).