IDHUS Token — Whitepaper

SPL token for SCCM-driven Smart Cities on Solana

November 19, 2025

Legal Disclaimer

This document is a technical and economic description of the IDHUS token and its role within the SCCM-based Smart City stack. Nothing herein constitutes investment, legal, tax, accounting, or engineering advice. Features, token parameters, and timelines are subject to change. Local regulations may restrict participation in token-related activities; stakeholders must comply with applicable law. The IDHUS token does not grant ownership in any legal entity. The network is experimental; risks include smart contract defects, market volatility, regulatory changes, and operational failures.

Abstract

IDHUS is an SPL token on Solana designed to coordinate, secure, and incentivize data flows and service execution across the Smart Cities Cohesive Model (SCCM), created by the IDHUS Institute. IDHUS powers staking for IoT data attestors and NCC operators, pays for application-level services via fee abstraction, enables decentralized governance, and aligns incentives for municipal partners, operators, and citizens. The architecture anchors sensor attestations on-chain through Solana programs, while large data payloads remain off-chain with cryptographic commitments and optional state compression. This whitepaper outlines the reference architecture, token design, tokenomics, governance, security model, and roadmap for city-scale deployments.

1. Motivation & Context

Cities are complex systems spanning energy, mobility, waste, safety, water, human flow, demographics, and more. SCCM (Smart Cities Cohesive Model) organizes these domains into coordinated layers governed through per-layer control nodes (NCCs) and a city-wide governance nexus (NCG). Blockchain ensures integrity, interoperability, and auditability of cross-layer data and controls, while the IDHUS token aligns economic incentives and decentralizes governance across ecosystem stakeholders.

2. SCCM Overview (Summary)

The SCCM structures the city into interoperable layers: Natural Ecosystem, Energy, Waste & Recycling, Mobility, Communications, Safety, Tracking, Supply, Human Flow, Demographics, Augmented Reality, Sustainability, and Control. Each layer operates an NCC (Node for Communication and Control) that aggregates IoT device data and enforces per-domain policies. All NCCs anchor critical events to the blockchain; an AI-assisted NCG coordinates cross-layer governance and builds a real-time Digital Twin for predictive operations.

This whitepaper adopts SCCM's architecture as the reference operating model and positions IDHUS as the coordination token for data integrity, service metering, and governance across layers.

3. Design Goals

- **Integrity:** Cryptographically anchor critical IoT events and control actions.
- **Scalability:** Handle high-frequency, city-scale telemetry with low latency and cost.
- **Interoperability**: Standardize metadata and schemas across SCCM layers.
- **Security:** Provide robust identity, attestation, and slashing for misbehavior.
- **Governance:** Empower citizens, operators, and municipalities with transparent decision-making.
- **Sustainability:** Incentivize efficient resource usage and green outcomes.

4. Platform Choice: Why Solana

Solana offers a high-throughput, low-latency L1 with a parallel execution engine (Sealevel), a time-source for efficient consensus (Proof of History), and low transaction costs. These properties make it suitable for anchoring high-frequency IoT attestations and enabling responsive smart city applications. IDHUS is implemented as an SPL token, leveraging composability with existing Solana programs, token extensions, and DAO tooling.

5. System Architecture

The stack comprises on-field devices, per-layer NCCs, an attestation/oracle network, Solana on-chain programs, and a Digital Twin layer:

5.1 Components

- **IoT Devices:** Field sensors/actuators per SCCM layer. Lightweight clients sign readings and send to the NCC of their layer.
- **NCCs (Per-Layer):** Gateway services that authenticate devices, pre-aggregate data, enforce thresholds, and submit transactions to Solana.
- **NCG (City Governance Nexus):** AI-assisted node that coordinates cross-layer policies and Digital Twin operations.
- **Attestation Network:** Independent verifiers checking device proofs and NCC submissions; slashed for misbehavior.
- **On-chain Programs:** Registry, Data Attestation, Payments, Staking/Slashing, Governance, and optional Transfer Hooks.
- **Data Lake & Indexers**: Off-chain storage for bulk telemetry (e.g., IPFS/Arweave/hybrid cloud) with on-chain commitments and state compression.
- **Digital Twin & AI:** Predictive analytics, simulations, and service optimization powered by standardized datasets.

5.2 Data Flow

1) Devices sign readings → 2) NCC authenticates and normalizes payloads → 3) Attestors verify device and NCC integrity → 4) On-chain Data Attestation Program records hashes/roots (optionally via compressed state) → 5) Off-chain payloads persist with content-addressing → 6) Digital Twin ingests indexed data for analytics and control loops.

5.3 Storage Strategy

- On-chain: Metadata, pointers (CIDs), Merkle roots for batched events, staking/penalty state, governance records.
- Off-chain: High-volume telemetry and media stored in content-addressed systems (e.g., IPFS/Arweave) and/or municipal clouds.
- Compression: Use Solana's state compression to anchor large event sets efficiently while enabling proof-based verification.

6. IDHUS Token (SPL)

IDHUS is an SPL token used to coordinate economics and governance across SCCM. It does not replace SOL for network fees; instead, a relayer-based "Gas Station" abstracts fees so end users may pay in IDHUS while relayers settle fees in SOL.

6.1 Standard & Extensions

- **Standard:** SPL Token (Token-2022 for extensions).
- **Extensions** (as supported on the target cluster): Transfer Hook for policy checks; Default Account State; Metadata; optional Confidential Transfers for privacy-preserving balances when compliance permits.

6.2 Token Parameters

Name	IDHUS
Symbol	IDHUS
Standard	SPL (Token-2022)
Decimals	6
Max Supply (cap)	1,000,000,000 IDHUS
Initial Circulating Supply	To be defined at TGE
Mint Authority	DAO multisig (time-locked)
Freeze/Transfer Hook Authority	DAO via governance
Cluster	Solana mainnet-beta (TBD at launch)

6.3 Utilities

- Staking by NCC operators, data attestors, and oracle providers (with slashing).
- Service metering: pay-per-use APIs for SCCM apps (e.g., mobility, energy, water).
- Data marketplace: permissioned access to anonymized datasets and analytics credits.
- Governance: proposal deposits, voting power, and parameter changes via DAO.
- Incentives: rewards for high-quality data, bug bounties, and community programs.

7. Economic Flows

Protocol revenue (from API metering, dataset licensing, and municipal integrations) is collected in IDHUS. A portion is routed to the treasury, a portion to operator rewards, and a configurable share is used to buy-and-burn IDHUS to align long-term incentives.

7.1 Staking & Slashing

Operators (NCCs, attestors, oracles) must stake IDHUS. Misbehavior (invalid attestations, downtime, data tampering) is penalized via on-chain slashing. Quality-of-service metrics feed a reward curve that boosts reliable operators.

7.2 Fee Abstraction (Relayers)

End users and devices may pay application-level fees in IDHUS. Relayers bundle transactions, pay SOL network fees, and receive IDHUS reimbursements plus a spread. Transfer Hooks and program constraints ensure fee capture and discourage bypass.

8. Tokenomics (Proposed)

Numbers below are reference values for discussion and community review; they can be adapted per city rollout and regulatory guidance.

Allocation	Share	Vesting / Notes
Ecosystem & Sensor Incentives	35%	Event-driven rewards; emissions over 6–8 years
City Partnerships & Grants	15%	Milestone-based disbursements; 2–4 year schedules
Operator Staking Rewards	15%	Performance-weighted; halving-style decay
Treasury / DAO Reserve	10%	Used via governance; transparent policies
Team & Advisors	10%	4-year vest, 1-year cliff; subject to lockups
Public Sale & Liquidity	10%	AMM and market liquidity provisioning
Strategic Sale	3%	Capped discounts; 2-year linear vest
Community Airdrops	2%	Citizen engagement, pilots, bug bounties

Emission Policy: capped supply with scheduled unlocks; governance may adjust reward curves without exceeding the cap.

9. Governance

Governance for each SCCM project implementation is implemented via an on-chain DAO (e.g., SPL Governance/Realms). Stake-weighted voting with optional quadratic modifiers can be used for citizen-focused polls. Treasury actions, program upgrades, and parameter changes (fees, slashing rates, reward weights) are executed via time-locked multisig.

9.1 Councils & Roles for the SCCM implementation

- **Technical Council:** protocol upgrades, audits, emergency patches.
- **Municipal Council**: public policy alignment, data ethics, compliance.
- **Citizen Council**: participatory budgeting, service priorities, pilots.

9.2 Role Tokens

Non-transferable role tokens (credentials) can gate specific permissions (e.g., NCC operator, auditor). Transfer Hooks ensure policy checks before sensitive operations.

10. On-chain Programs (Reference Design)

- **Registry Program:** Registers devices, NCCs, and attestors; maintains metadata PDAs and revocation lists.

- **Data Attestation Program:** Batches device readings, verifies attestations, stores hashes/roots; supports state compression.
- **Payments & Metering Program:** Collects IDHUS fees, manages credits, routes revenue to treasury and operators.
- **Staking & Slashing Program:** Manages operator stakes, rewards, penalties, and performance oracles.
- **Governance Program:** Proposals, votes, timelocks, execution; integrates with treasury multisig.
- **Gas Station (Relayer) Program**: Enables fee abstraction; IDHUS settlements to relayers; anti-spam controls.

11. Data Standards, Privacy & Compliance

The SCCM requires data standardization and strong privacy-by-design. Personally identifiable information (PII) must never be written on-chain. Use pseudonymous device IDs, consent frameworks, role-based access, and differential privacy where applicable.

For regulated datasets, permissioned access and auditable trails are enforced. Optional confidential balance extensions (when supported) may be used for sensitive treasury operations.

12. Security Model

- **Smart Contracts:** formal verification where feasible; multiple independent audits before mainnet launch.
- **Key Management:** hardware-backed keys (HSMs/secure enclaves), m-of-n multisigs, emergency revocation.
- **Rate Limits & Circuit Breakers:** pause hooks for catastrophic bugs; bounded risk per epoch.
- **Oracle Security**: decentralized attestors, reputation weighting, cross-checks vs redundant sources.
- **Monitoring:** on-chain metrics and off-chain alerting with automated rollbacks where possible.

13. Interoperability & Ecosystem

To maximize liquidity and adoption, IDHUS can bridge to other networks through established bridge frameworks. SDKs expose standard APIs for devices, NCCs, and municipal applications. Open data licenses and schemas encourage third-party innovation while respecting privacy and policy constraints.

14. Digital Twin & AI Integration

Anchored telemetry feeds a city-scale Digital Twin for forecasting, anomaly detection, and scenario planning (e.g., mobility surge, grid stress). AI models execute with transparent data provenance and audit trails anchored on-chain. Rewards in IDHUS incentivize accurate labeling, model improvements, and high-quality data contributions.

15. Roadmap (Indicative)

- **Phase 0 —** Research & Standards: Finalize schemas per SCCM layer; security reviews; testnets.
- **Phase 1 —** MVP: Token mint, Registry, Attestation, and Payments on devnet; one pilot layer (e.g., Mobility).
- **Phase 2 —** Multi-Layer Pilot: Expand to 3–5 SCCM layers; DAO alpha; fee abstraction live; initial airdrops.
- **Phase 3 —** City Launch: Mainnet rollout with municipal partners; bridging; data marketplace beta.
- **Phase 4 —** Scale & Optimization: Performance tuning, broader city integrations, extended governance, and ecosystem grants.

16. Risk Factors

- **Technical:** smart contract bugs, oracle failures, key compromise, unexpected network behavior.
- **Regulatory:** evolving policies on data, tokens, identity, and municipal procurement.
- **Market**: liquidity shocks, price volatility impacting operator economics.
- O**perational**: device tampering, NCC downtime, data quality issues.
- **Adoption**: stakeholder misalignment or insufficient incentives.

17. Implementation Notes

- Use SPL Token-2022 where available to leverage Transfer Hooks and metadata
- Avoid storing raw PII on-chain; anchor only hashed, salted commitments.
- Employ state compression for event-heavy domains; rotate roots on fixed intervals.
- Provide city-facing dashboards and public transparency portals with tiered access.
- Maintain rigorous DevSecOps with canary releases, feature flags, and staged rollouts.

References

• **Smart Cities Cohesive Model (SCCM):** multi-layer architecture (ecosystem, energy, waste, mobility, communications, safety, tracking, supply, human flow, demographics, AR, sustainability, control), with per-layer NCCs and a central AI-assisted governance nexus

(NCG). The SCCM specification informs the token's role across data collection, blockchain anchoring, and Digital Twin integration.

Appendix A — Glossary

- SCCM: Smart Cities Cohesive Model; layered smart city architecture.
- NCC: Per-layer Node for Communication and Control.
- NCG: City-level Governance Nexus; AI-assisted orchestration.
- SPL: Solana Program Library token standard.
- PDA: Program Derived Address; deterministic program account.
- CPI: Cross-Program Invocation; Solana program-to-program call.
- State Compression: Merkle-tree based compression for large datasets.
- CID: Content Identifier used by content-addressed storage (e.g., IPFS).

Appendix B — Token & Program Addresses

- **Token Address:** 4HTBbihwqz1H9SpAKJS9THAJuBrqeyokPze42r7Cpump
- **Program IDs (Registry, Attestation, Payments, Staking, Governance, Relayer):** TokenkegQfeZyiNwAJbNbGKPFXCWuBvf9Ss623VQ5DA