

SADT One-pager

THE PROBLEM THIS SOLVES

Southeast Asia's 70 million smallholder farmers generate *continuous, high-value agricultural data* — but receive almost none of its economic benefit, because no trusted institution exists that a rice farmer in the Mekong Delta, a Singapore bank, and an EU commodity buyer can all rely on simultaneously. The Singapore-ASEAN Data Trust (“**SADT**”) is that institution.

HOW IT WORKS

Think of it as three systems running in parallel: a **land registry** that proves who owns what and where; a **private safety-deposit box** that stores the data locally and never sends the contents anywhere; and a **notary** that travels to the box, verifies a specific claim, and issues a certificate — without ever touching the underlying documents.

The certificate — a machine-readable confidence score wrapped in the banking standard (ISO 20022) that SWIFT, DBS, and Vietcombank already speak — is what crosses borders. The data does not.

L1 Identity & Land Anchor

Vietnam's national biometric ID (VNeID) + digital land registry (Decree 357) bind every data record to a verified citizen and a registered GPS polygon. Like a deeds registry, but live and cryptographic.

L2 Local Storage — Private IPFS Node

Sensor logs and harvest records are stored locally on village hardware using content-addressed storage *like BitTorrent, but private*. Only a fingerprint (hash) is published — not the file. External parties see that data

THE MARKETPLACE MODEL

Vendors — agronomists, input suppliers, banks, buyers — post structured **Data Request Offers** specifying what they want and what they're offering in return. The village cooperative evaluates offers on behalf of its members *like a rights management organisation* (think PRS for Music, but for rice data). Farmers browse, negotiate, and sign vendor-specific consent contracts — on-chain, under their own cryptographic identity.

Solution providers are privileged over financial intermediaries. Agronomists get whitelisted access and lower fees. Commodity trading houses go through individual approval and higher obligations. The system is designed so the farmer's first relationship is with the agronomist — not the bank.

FOUNDATION STRUCTURE

exists; they cannot read it.

L3 Verified computation - CtD + ZK Proofs

For complex scores: the algorithm travels to the data and runs locally — only the result leaves. For binary claims (deforestation-free? above threshold?): a **zero-knowledge proof** — a mathematical proof the claim is true, without revealing the underlying data. The GPS coordinates never leave Vietnam.

L4 Registry - Decentralized Knowledge Graph

Verified outputs are registered on OriginTrail's DKG *like SGX's settlement layer — immutable, independently verifiable, no single operator*. Each record gets a permanent address (UAL). Under Singapore's MLETR, this can function as a legal transferable instrument.

L5 Audit & Attribution

Every query generates a tamper-evident receipt on-chain, visible to the farmer and cooperative — not mediated by AgriG8. Agreed payments flow from receipts. Settlement connects to SGTraDex.

The most urgent use case — EUDR compliance: Every existing platform makes farmers surrender GPS coordinates to prove deforestation-free status. The SADT's ZK-proof layer proves the claim without transmitting the coordinates. No competitor offers this. 15+ platforms reviewed; all require data surrender.

GOVERNANCE MODEL

The SADT operates as a Singapore IPC (Institution of a Public Character) — a foundation with a statutory fiduciary duty to its beneficiaries (farmers and cooperatives), not to its revenue. The Commissioner of Charities oversees it. No single company controls it.

Board: farmer cooperative representatives hold blocking votes on access policy and fee changes. Independent technical experts. MAS and Vietnam MOIT as non-voting observers. A separate Farmer Data Ombudsman handles disputes — the Foundation produces evidence; it does not adjudicate.

Revenue: tiered access fees from external firms.

Agonomists pay less. Banks and commodity buyers pay more. A 2% levy on Tier 2 fees funds the dispute reserve.

LEGAL INNOVATION REQUIRED

Data Fiduciary category

Recognise a legal category between Data Controller and Data Processor — a neutral steward with fiduciary duty. Precedent: India DPDP Act, EU Data Governance Act.

Virtual Residency for CtD nodes

Data residency law focuses on where files are stored. Under Compute-to-Data, the file stays in Vietnam; the insight crosses Singapore. Current law can't accommodate this. Fix: treat SADT nodes as domestic infrastructure for residency purposes.

Seasonal algorithmic consent

PDPA/PDPL require per-transaction consent. A farmer should b

able to authorise a full growing season's query class in one acti
Sandbox permission required.

Consent Agreement VCs as binding contracts

Verified outputs are registered on OriginTrail's DKG like SGX's
settlement layer — immutable, independently verifiable, no sing
operator. Each record gets a permanent address (UAL). Under
Singapore's MLETR, this can function as a legal transferable
instrument.

Cooperative legal standing in arbitration

Farmers can't file at SIAC. Cooperatives need explicit authority
represent members in data rights disputes. Vietnam's Law on
Cooperatives (2023) is close; sandbox extension needed.

CLOSEST GOVERNANCE MODEL	CLOSEST SINGAPORE INITIATIVE	CLOSEST ADVISORY MODEL
<i>JoinData (NL)</i>	<i>MAS ESGpedia</i>	<i>Digital Green</i>

Policy Brief

Establishing the Singapore–ASEAN Data Trust (SADT):

A Fiduciary Infrastructure for Smallholder Agricultural Data

Prepared by Liyana Mahirah, AgriG8

Policy Brief v0.9, March 2026

Confidential: not for public distribution

Contact: [contact@agrig8.com]

Abstract

Southeast Asia's smallholder farmers generate a continuous stream of high-value agricultural data — soil readings, harvest yields, input records — yet they receive almost none of its economic benefit. Banks cannot underwrite them without verified records. Commodity buyers cannot confirm quality without costly physical audits. The data exists; the institutional infrastructure to make it trustworthy across borders does not. The Singapore–ASEAN Data Trust (SADT) is a proposed foundation-governed fiduciary designed to close this gap.

.

SECTION 1. THE PROBLEM

"The challenge is that we have these powerful technologies to collect and analyze data, but we lack the frameworks to ensure that data is used in ways that are perceived as fair and legitimate. The bottleneck isn't the information; it's the infrastructure of trust required to make that information actionable across boundaries."

— Rachel Botsman, *The Architecture of Trust*

"A goal is not attained except through asabiyyah (social glue)... and when the sense of functional trust disappears, the civilization, though wealthy in knowledge, begins its decline."

— Ibn Khaldun, *The Muqaddimah*

1.1 Why precision agriculture keeps stalling

The dominant explanation for slow agri-tech adoption in ASEAN is a technology deficit: farmers lack sensors, connectivity, or skills. This is incomplete. Vietnam alone has over 70 million mobile subscribers and a mature national biometric identity system. The actual constraint is institutional: there is no credible, neutral entity that a smallholder, a Singaporean bank, and a commodity trading house can all trust simultaneously.

Farmers have rational reasons to withhold data. In fragmented commodity markets, granular production data — the exact yield of a specific plot, the timing of a harvest — has been used to suppress farmgate prices or selectively exclude smallholders from premium supply chains. The current data economy asks farmers to supply market intelligence without receiving enforceable protection in return.

1.2 Why existing frameworks are insufficient

Consent forms and privacy policies do not resolve this coordination problem. Smallholders lack the negotiating power to enforce contractual protections against large commodity buyers. Centralised corporate data lakes create liability and concentration risk. Existing legal categories — Data Controller and Data Processor, as defined in Singapore's PDPA and Vietnam's 2024 Law on Data — do not accommodate a neutral fiduciary that holds data in trust for a rights-holder rather than for commercial purposes.

The core failure:

It is not a shortage of farm data. It is the absence of a legal and institutional structure that allows that data to be trusted — and therefore used — across the commercial, regulatory, and geographic boundaries that define ASEAN agricultural trade.

SECTION 2: THE PROPOSAL: A NON-CUSTODIAL DATA FIDUCIARY

2.1 The founding principle: data stays local; truth travels

Raw farm records — soil sensor logs, harvest weights, identity-linked field photographs — remain in the physical custody of the farmer, village cooperative, or local gateway. External parties such as banks, insurers, and commodity buyers do not receive the underlying files. Instead, they receive verified attestations: machine-readable confidence scores that answer specific questions (“Is this plot’s yield consistent with satellite imagery?”) without exposing the evidence that generated the answer.

This is made possible by a technique called Compute-to-Data, in which an algorithm travels to where the data lives and runs inside a controlled environment on the local node. Only the output — a confidence score and a verifiable audit record — crosses the border. The raw data does not.

2.2 Why a foundation, not a company

A private company cannot credibly play a neutral stewardship role because commercial incentives eventually lead to extraction. The SADT must be structured as an independent foundation with a fiduciary mandate — legally obligated to act in the interest of the rights-holders (farmers and cooperatives), not its own balance sheet. This is the same logic that underlies public utility commissions and academic data trusts.

2.3 The farmer as author, not subject

The SADT frames the farmer as the author and rights-holder of primary agricultural records — not a data subject to be measured. Every verified truth unit carries a provenance trail identifying which rights-holder’s data contributed to it, creating the basis for attribution, reciprocity, and value-sharing that purely transactional models cannot support. This framing has operational precedent: Fairfood International’s fiduciary governance of farmer data in an Indonesian nutmeg supply chain pilot demonstrated measurably increased trust, stronger farmer understanding of consent, and improved negotiating position for growers relative to buyers — outcomes that advisory and compliance platforms without fiduciary obligations did not achieve.

2.4 Active consent: the cooperative negotiation marketplace

Authorship implies more than the right to be informed after the fact. The SADT includes a vendor marketplace layer in which firms post structured Data Request Offers — specifying what data they want, what they are offering in return, and the terms of the exchange — before any access is granted. Cooperatives evaluate offers on behalf of their members, provide comparables and red-flag analysis, and facilitate negotiation. Individual farmers browse, counter-propose, accept, or decline before a single query is authorised.

Access under this model requires a vendor-specific, bilaterally signed Consent Agreement — not a standing permission. A farmer who has accepted an offer from a trading house at a negotiated 7% price premium has a cryptographically signed contract on-chain under their own decentralised identity. They can revoke it at any time. The cooperative’s role mirrors that of a rights management organisation: it does not replace the farmer’s decision, but ensures that decision is made with full information and genuine negotiating capacity.

SECTION 3: THE FIVE POLICY ASKS

The SADT's technical architecture is functional. What it currently lacks is legal personality. Three specific regulatory interventions are required to make the system operational across the Vietnam–Singapore corridor.

Policy Ask	Current Legal Gap	Proposed Sandbox Fix
1. Recognise the Data Fiduciary as a legal category	Singapore's PDPA and Vietnam's 2024 Law on Data recognise only Data Controllers and Data Processors. No category exists for a neutral steward holding data in trust for a rights-holder.	A Regulatory Sandbox — jointly governed by MAS and Vietnam's MOIT — grants the SADT formal fiduciary status, enabling it to issue Oracle Truth Signals that financial institutions can treat as legal transferable records under MLETR.
2. Shift data-flow regulation from Residency to Access	Cross-border data laws focus on where files are stored. Under Compute-to-Data, raw files never leave Vietnam — but the resulting insight crosses to Singapore. Current law cannot accommodate this distinction.	Grant SADT nodes 'Virtual Residency' status: treated as domestic infrastructure for data residency purposes, even when queried by a foreign financial institution under approved compute conditions.
3. Enable seasonal algorithmic consent	Singapore's PDPA and Vietnam's PDPL require manual, per-file consent for data processing. This makes automated seasonal analytics legally impractical at scale.	The sandbox permits 'Algorithmic Consent': a farmer authorises the SADT oracle to handle defined categories of query (e.g., harvest verification) for a full growing season, without per-transaction re-consent.
4. Recognise Consent Agreement VCs as binding data licensing agreements	Neither SG nor VN law currently recognises a cryptographically signed, DID-anchored Verifiable Credential as a legally binding contract. This leaves vendor-specific data access agreements in a legal grey zone, undermining their enforceability.	The sandbox grants bilateral Consent Agreement VCs — signed by both farmer and vendor DIDs and anchored on a public decentralised registry — the same legal standing as electronic contracts under Singapore's Electronic Transactions Act and Vietnam's Law on E-Transactions (2023). This makes cooperative-negotiated data licences legally enforceable against commercial counterparties.
5. Recognise cooperatives as legal representatives in formal arbitration	A smallholder farmer in the Mekong Delta cannot practically file or pursue a claim at SIAC or VIAC. Without an institutional representative, the farmer's formal dispute rights are theoretical rather than exercisable. Existing cooperative law in both jurisdictions does not explicitly authorise cooperatives to act as legal representatives in data rights disputes.	The sandbox grants registered SADT cooperatives explicit standing to file and represent member farmers in formal arbitration proceedings arising from Consent Agreement VC disputes — at SIAC for Singapore-seated matters and VIAC for Vietnamese-seated matters. This makes the dispute mechanism practically accessible, not just formally available.

Precedents for each ask exist. India's Digital Personal Data Protection Act introduced a data fiduciary framework. The EU's Data Governance Act created 'data altruism organisations.' Singapore's existing MLETR adoption provides the pathway for digital oracle signatures to function as transferable instruments. The SADT applies and extends these precedents to the specific conditions of ASEAN agricultural trade.

SECTION 4: THE VIETNAM-SINGAPORE PILOT

4.1 Why Vietnam is the only viable production-side pilot country

The SADT's verification architecture requires a biometric anchor: a way to link ground-level sensor data to a specific, legally registered farmer and land parcel, so that the resulting confidence score cannot be spoofed. Vietnam is currently the only country in ASEAN with the digital infrastructure to provide this anchor at scale.

Vietnam's VNeID system provides unified biometric identity for over 90 million citizens. Decree 357 provides a national digital land registry with unique property identifiers linked to GPS polygons. Together they create the foundation for unforgeable ground-truth data — the critical requirement for any data-based trade finance or insurance product that cannot rely on physical audits.

Singapore provides the complementary financial and legal infrastructure: MLETR adoption, MAS-regulated institutions capable of acting on verified digital signals, and SGTraDex as an existing data exchange framework for trade logistics. Neither country alone is sufficient; the corridor between them is where the pilot's value is created.

4.2 What Vietnam receives: national agricultural query intelligence

Access to Decree 357's land registry API is not a concession Vietnam makes to a Singapore foundation. It is the first half of a reciprocal arrangement. Every query run against SADT data generates a tamper-evident receipt. In aggregate — stripped of all farmer, cooperative, and firm-level identifiers — those receipts constitute something MARD and MOIT do not currently have: a real-time signal of where global agricultural finance is concentrating its attention in Vietnam's food system.

The SADT commits, as a structural condition of its operating licence in Vietnam, to deliver a quarterly National Query Intelligence report to MARD and MOIT. The report contains: query volume by district and crop type; query volume by firm category (trade finance, insurance, commodity procurement, agri-advisory, research); average Confidence Score thresholds requested, indicating what quality standards the market is applying; and ZKP verification volumes by claim type, indicating which ESG compliance pathways are active. No farmer records, no firm names, no cooperative identities — aggregate market intelligence only.

A Vietnamese trade ministry that knows in February that European trading houses are running unusually high jasmine rice verification queries in Tiền Giang has information it did not previously have — and which the trading houses did not intend to share. The SADT transforms the land registry relationship from a permission request into an intelligence exchange. That is a different negotiation.

4.3 Scope and milestones

The initial deployment targets the Mekong Delta's Cái Bè district. Three to five cooperative nodes, covering several hundred farmers, is sufficient to demonstrate a complete end-to-end truth unit — from biometric harvest verification in Vietnam to trade finance release in Singapore.

Phase	Milestone	Key Partners
2026 Q1–Q2	Deploy village gateways in Cái Bè; integrate VNeID and Decree 357 APIs with SADT oracle	AgriG8, MARD (VN), VNPT
2026 Q3	Execute first live Truth Unit trade: SADT-verified harvest accepted as collateral by Singapore bank under MLETR pilot	MAS-regulated bank, Vietcombank, AgriG8
2026 Q4	Publish pilot audit results and policy evaluation report; open sandbox to additional participants	MAS, MOIT, ASEAN Secretariat
2027+	Expand to additional ASEAN members as biometric identity and land registry infrastructure matures	ASEAN Coordinating Committee on e-Commerce

SECTION 5. GOVERNANCE AND FARMER PROTECTIONS

5.1 The Co-operative Clause

Access to SADT-verified data is not unconditional. Every firm granted sandbox access must sign a master access agreement containing a Co-operative Clause: a commitment to share usage logs with the relevant cooperative's audit mirror and to negotiate data royalties or input discounts once commercial value is established. Non-compliance results in access revocation. This mechanism ensures that the SADT does not create a more sophisticated form of data extraction.

5.2 Usage transparency for farmers

Every data query generates a tamper-evident read receipt. Farmers and cooperatives can audit exactly which firms accessed their verified records, when, and for what purpose. The dashboard is presented in the farmer's language and summarises material outcomes: "Your harvest was verified as Grade-A. This verification secured a 5% price premium over the local spot rate." This converts abstract data sovereignty into legible economic benefit.

5.3 Foundation sustainability

The SADT foundation is governed by a multi-stakeholder board including cooperative representatives, an independent academic advisory panel, and regulatory observers from MAS and MOIT. Sustainability relies on access fees charged to external firms — commodity buyers, banks, insurers — with a proportion allocated to cooperative infrastructure maintenance and farmer attribution payments. The foundation does not trade data or take positions in agricultural markets.

SECTION 6. THE STRATEGIC CASE

The specific ask:

Regulatory sandbox recognition of the Data Fiduciary category, Virtual Residency for Compute-to-Data nodes, and Algorithmic Consent for seasonal queries — governed under a joint MAS–MOIT framework with a 12-month pilot evaluation period.

AgriG8 is prepared to engage with regulatory counterparts to define sandbox parameters, data protection conditions, and evaluation criteria at the earliest opportunity.

The yield gap in ASEAN agriculture is not primarily a technical problem. It is a capital allocation problem: smallholders cannot access the credit, inputs, and market relationships that would allow them to improve, because information asymmetries are too large and verification costs are too high.

The SADT does not close the yield gap directly. It closes the trust gap that prevents the capital, insurance, and market access needed to close the yield gap from reaching smallholders. When a Singaporean bank can release trade finance against a machine-readable confidence score rather than a physical audit, transaction costs fall. When an insurer can automate parametric payouts against verified IoT moisture readings, coverage becomes affordable at scale. When a commodity buyer can verify sustainability claims without sending an auditor to the Mekong Delta, premium supply chain access becomes realistic for smallholders.

This is a structural intervention in the regional political economy of agriculture — one that aligns the interests of smallholders, financial institutions, regulators, and commodity markets around a shared infrastructure of verifiable truth. It requires a narrow but critical set of regulatory accommodations to make legal what is already technically feasible.

6.1 The EU Deforestation Regulation

The most immediate forcing function is the EU Deforestation Regulation (EUDR), which requires every exporter of rice, coffee, palm oil, and four other commodity categories to prove their products are not associated with deforestation after December 2020 — backed by geolocated farm data. Every existing EUDR compliance platform requires farmers to surrender GPS coordinates and production records to a company's cloud. For ASEAN smallholders, this means disclosing precise land location data to foreign platforms as the price of EU market access. The SADT's zero-knowledge proof layer allows a farmer to prove their plot is deforestation-free without transmitting their coordinates to anyone — compliance without data surrender. No other platform in the EUDR compliance market currently offers this. For Singapore and Vietnam as agricultural export corridors, the SADT's architecture is both a farmer protection mechanism and a trade infrastructure asset.

For Vietnam specifically, the SADT also functions as a national intelligence asset. The aggregate of all queries run against Vietnamese farm data — stripped of individual identifiers — reveals where global agricultural capital is concentrating before it translates into price movements. That intelligence, delivered quarterly to MARD and MOIT as a structural operating condition, is the consideration Vietnam receives in exchange for Decree 357 API access. It reframes the entire regulatory relationship: not a foreign foundation requesting government data, but a reciprocal infrastructure arrangement in which both parties gain something they could not produce independently.

6.2 The Price Reporting Gap and the SADT as Benchmark Infrastructure

Rice looks like a “simple” staple, but pricing it in real time is structurally hard because there is **no liquid, centralized global rice exchange** setting a universally trusted benchmark the way oil or metals have. Instead, price discovery is **distributed across paywalled Price Reporting Agencies** (e.g., Platts' Thai/Viet 5% Broken FOB assessments and indices), **specialist rice intelligence services** (e.g., TRT, Oryza), and **national exporter associations** (e.g., TREA

weekly FOB Bangkok numbers; VFA grade/floor guidance). Each source covers different grades, shipment terms, and reporting methodologies, so even sophisticated buyers end up stitching together partial, non-interoperable signals. A **data trust / DTCC-like utility** is needed to standardize identifiers (grade, origin, incoterms, timing), govern access to proprietary feeds, and publish a neutral, auditable “reference layer” that can be safely used for valuation, financing, and farmer payout logic—without any single private data vendor becoming the de facto sovereign of rice price truth.

Prepared by Liyana Mahirah, AgriG8 · Policy Brief v0.9, March 2026 · Confidential: not for public distribution · Contact: [contact@agrig8.com]vb

APPENDIX A. Regulatory Exposure Matrix

APPENDIX A. Regulatory Exposure Matrix

The table below maps every material regulatory framework applicable to AgriG8 and the SADT as a cross-border agricultural data infrastructure operating in Singapore and Vietnam, with EU-market exposure via EUDR. Frameworks are grouped by domain. The ‘SADT Architecture Response’ column indicates how the system design addresses each obligation — or where a residual compliance gap requires active management. This matrix is intended to demonstrate to MAS and MOIT the breadth of the regulatory surface that a joint sandbox framework must accommodate, and to establish that the five policy asks in Section 3 are the minimum necessary interventions, not a comprehensive regulatory waiver.

Framework / Law	Jurisdiction	Domain	Key obligation for AgriG8	SADT architecture response
Personal Data Protection Act (PDPA) + PDPC Advisory Guidelines	Singapore	Data Privacy	Lawful basis for every data collection point; purpose limitation; mandatory data breach notification within 3 days; Data Protection Officer (DPO) appointment; right of access and correction for data subjects.	Consent Agreement VCs constitute lawful basis for each vendor-specific access event. Algorithmic Consent satisfies seasonal authorisation with farmer revocability. No raw farmer data stored by AgriG8; CtD means no centralised repository to breach. DPO to be appointed at Foundation registration.
IMDA Trusted Data Sharing Framework (TDSF)	Singapore	Data Privacy	Guidelines for data sharing arrangements including data trust structures; recommended governance, consent, and access control standards for intermediaries.	SADT Foundation governance design is consistent with TDSF data trust model. Formal TDSF alignment recommended as precondition for IMDA sandbox engagement.
Decree 13/2023/ND-CP — Personal Data Protection	Vietnam	Data Privacy	Lawful basis, purpose limitation, cross-border transfer requires MOIPT approval and security assessment, data subject rights (access, erasure, objection), mandatory breach reporting to Ministry of Public Security.	Local IPFS storage satisfies data localisation. No raw personal data leaves Vietnam. ZKP for EUDR means even GPS coordinates stay local. Cross-border transfer of ISO 20022 confidence scores — not personal data — requires legal assessment under Decree 13.
Law on Data (2024, Luật Dữ liệu)	Vietnam	Data Privacy	Data classification obligations; governance requirements for data intermediaries; data transaction registration with MOIPT; restrictions on commercial data activities without registration.	Foundation must register as a data intermediary under the Law on Data before commercial operation. DRO marketplace transactions may constitute ‘data transactions’ requiring registration. Active legal assessment required.
Law on Cybersecurity (2018) — data localisation provisions	Vietnam	Data Privacy	Important data and personal data of Vietnamese users must be stored on servers physically located in Vietnam. Cross-border transfer of localised data requires regulatory approval.	IPFS nodes are physically sited at village cooperatives in Vietnam. No farmer personal data transits outside Vietnam. Confidence scores and ZKP outputs are derived, non-personal records — legal assessment of whether these constitute ‘important data’ is required.
GDPR (Regulation 2016/679)	EU	Data Privacy	Applies if AgriG8 processes personal data of EU residents or targets EU market. Triggers: EUDR compliance services for EU importers; academic data sharing with EU institutions. Requires lawful basis, DPA registration, potential DPO, data subject rights.	ZKP architecture means EU importers receive a mathematical proof, not personal data — GDPR data subject rights may not be triggered. EU academic node data sharing requires GDPR-compliant data processing agreement. Legal opinion required before EUDR commercial launch.

APPENDIX A. Regulatory Exposure Matrix

Framework / Law	Jurisdiction	Domain	Key obligation for AgriG8	SADT architecture response
ASEAN Personal Data Protection Framework	ASEAN	Data Privacy	Baseline cross-border data flow principles; recommended alignment for ASEAN member states' national laws.	SADT architecture exceeds ASEAN baseline. Consent Agreement VCs provide stronger individual rights than the Framework's minimum standards.
PDPC/IMDA Model AI Governance Framework (2020, updated 2023)	Singapore	AI Governance	Explainability of AI-assisted decisions affecting individuals; human oversight mechanisms; accountability structures; internal governance of AI systems.	Score explanation layer (component breakdown per Confidence Score) addresses explainability. FDO provides human oversight and appeal path. Algorithm Registry provides accountability chain. Confidence Score is a measurement, not a behavioural inference — lower-risk classification anticipated.
PDPC Advisory Guidelines: AI Recommendation and Decision Systems	Singapore	AI Governance	Impact assessment for AI systems influencing access to financial services; documentation of model logic; fairness obligations; right to human review.	Confidence Score as input to trade finance or credit decisions triggers these guidelines. Impact assessment to be conducted and published before pilot. FDO score dispute mechanism satisfies right to human review. No autonomous financial decision — human underwriting uses SADT signal as input, not sole determinant.
National AI Strategy (Decision 127/QD-TTg, 2021)	Vietnam	AI Governance	Encourages responsible AI development across sectors including agriculture; no binding compliance obligations currently. Successor legislation anticipated.	Architecture consistent with strategy principles. No current binding compliance gap. Monitor for successor regulation during pilot period.
OECD AI Principles (2019)	International	AI Governance	Accountability, transparency, robustness, safety, human-centredness for AI systems. Referenced in MAS and MOIT regulatory guidance.	Algorithm hash registry satisfies transparency and auditability. FDO and cooperative governance satisfy accountability. Score explanation layer addresses human-centredness. Principles are non-binding but influence sandbox assessment criteria.
EU AI Act (Regulation 2024/1689, applying from 2026)	EU	AI Governance	High-risk AI classification likely if Confidence Score is used as input to credit scoring or trade finance decisions affecting EU-connected parties. Requires conformity assessment, technical documentation, human oversight, post-market monitoring.	Highest-risk compliance gap in this matrix. EUDR use case brings SADT within EU AI Act scope if outputs feed EU financial decisions. ZKP outputs (binary claims) may be lower-risk. Pre-launch legal opinion essential. May require EU notified body conformity assessment for Confidence Score system.
Payment Services Act (2019) + MAS licensing	Singapore	Financial Services	Licence required if AgriG8 facilitates cross-border money transfers or operates payment accounts for attribution settlements. Applicable licence types: Major/Standard Payment Institution.	Pilot uses Service Offsets (cooperative credits) rather than cash to avoid immediate licensing obligation. Direct cash attribution at scale will require Payment Institution licence or licensed payment partner. Licence application timeline: 6–9 months. Must be initiated before post-pilot commercial rollout.
MAS Technology Risk Management Guidelines (2021)	Singapore	Financial Services	MAS-regulated banks using SADT signals must conduct third-party vendor due diligence; SADT must provide audit rights, penetration testing results, BCP documentation, and SLA commitments.	Gateway hardware attestation and remote audit capability satisfy core requirements. SADT must produce a TRM-compliant vendor assessment package for each bank integration. Included in pilot preparation workstream.

APPENDIX A. Regulatory Exposure Matrix

Framework / Law	Jurisdiction	Domain	Key obligation for AgriG8	SADT architecture response
MAS Notice on Cyber Hygiene (MAS Notice on Technology Risk)	Singapore	Financial Services	Applies to regulated institutions; by extension to critical vendors. Patch management, access control, network segregation, multi-factor authentication, malware protection.	Village gateway security hardening must meet MAS Cyber Hygiene standards for bank vendor classification. Remote monitoring infrastructure satisfies patch and access requirements. Third-party security audit required before bank integration.
MAS AML/CFT Notices (MAS Notice 626, 1014, etc.)	Singapore	Financial Services	If AgriG8 facilitates financial flows: KYC/CDD on counterparties, transaction monitoring, suspicious transaction reporting, record-keeping for 5 years.	Attribution payment flows in pilot are cooperative service credits, below AML thresholds. At scale, cash settlement via SGTraDex will require AML/CFT framework implementation. Bank partner handles SGD-side obligations; AgriG8 must implement VND-side KYC through licensed Vietnamese financial institution.
Electronic Transactions Act s.16C — MLETR adoption	Singapore	Financial Services	Basis for treating electronic transferable records as equivalent to paper instruments (bills of lading, promissory notes) in trade finance. ISO 20022 SADT signals must satisfy MLETR criteria for recognition by MAS-regulated banks.	Third policy ask. MAS sandbox recognition required. Precedent from existing e-bill of lading pilots is supportive. Legal opinion on SADT-specific MLETR qualification to be obtained from Singapore law firm before pilot launch.
Decree 357/2024/ND-CP — Digital Property ID	Vietnam	Agricultural / Land	Access to the national digital land registry API requires a formal data-sharing agreement with MARD and MONRE. No automatic API access for private operators. Approval timeline is indeterminate.	Critical path dependency. On the pilot's risk register as 'Medium probability, Critical impact.' Fallback: manual land registry verification by Cooperative Field Agent. MARD engagement initiated; formal MOU required before automated integration.
Law on Land (2024, Luật Đất đai)	Vietnam	Agricultural / Land	Defines farmer land use rights, registration obligations, and data accuracy requirements. Agricultural data linked to land parcels must reflect registered boundaries. Disputes over land data are subject to People's Committee jurisdiction.	Decree 357 integration must comply with 2024 Law provisions. Cooperative Field Agent co-signature provides a human verification layer for boundary accuracy. Land boundary disputes are outside SADT scope but may affect Confidence Score validity; FDO dispute mechanism covers score challenges arising from boundary errors.
MARD CheckVN Traceability System	Vietnam	Agricultural / Land	MARD's national agricultural product traceability system. Export products increasingly expected to have CheckVN-registered traceability records. Integration or interoperability may be required for EUDR compliance pathway.	SADT UAL can serve as a CheckVN-compatible traceability anchor. Alignment with MARD CheckVN reduces documentation duplication for export. Formal interoperability assessment with MARD recommended in Q2 2026.
MARD Circulars on Agricultural Product Certification	Vietnam	Agricultural / Land	Certification requirements for export-grade agricultural products (VietGAP, GlobalGAP alignment). Digital certification records increasingly required.	SADT Confidence Score can underpin VietGAP certification claims. Algorithm Registry must include approved certification algorithms. Integration with MARD certification workflow to be designed in post-pilot phase.
Cybersecurity Act (2018)	Singapore	Cybersecurity	Critical Information Infrastructure (CII) designation obligations if SADT becomes part of Singapore's financial or government CII. SGTraDex integration creates potential CII adjacency. CSA oversight.	SADT must conduct a CII self-assessment with the Cyber Security Agency of Singapore before SGTraDex live integration. If CII designation applies, operational obligations include mandatory incident reporting, penetration testing, and CSA audit rights.

APPENDIX A. Regulatory Exposure Matrix

Framework / Law	Jurisdiction	Domain	Key obligation for AgriG8	SADT architecture response
Computer Misuse Act (Cap. 50A)	Singapore	Cybersecurity	Unauthorised access to computer systems. Relevant to gateway security architecture and to the legal status of attempted DKG record manipulation or Consent Agreement VC forgery.	Gateway hardware attestation and access control architecture addresses unauthorised access risks. Attempted forgery of on-chain records (cryptographically infeasible but legally relevant) would constitute a Computer Misuse Act offence — relevant for FDO evidence package in dispute proceedings.
Law on Cybersecurity (2018) — incident reporting	Vietnam	Cybersecurity	Mandatory reporting of cybersecurity incidents affecting information systems to the Ministry of Public Security (A05) within prescribed timelines. Critical information infrastructure designation possible.	Gateway incident reporting protocol must be designed to satisfy MPS reporting requirements. Cooperative Technical Officers must be trained on incident identification. Response plan to be included in pilot operational documentation.
EU Deforestation Regulation (EUDR) — Regulation 2023/1115	EU	Trade / ESG	Exporters of rice, coffee, palm oil, cocoa, cattle, wood, rubber and derived products to the EU must provide geolocated evidence of deforestation-free sourcing after December 2020. Non-compliant products face EU market exclusion.	Primary commercial entry point for SADT. ZKP-based deforestation proof provides cryptographic evidence of deforestation-free status without transmitting GPS coordinates to EU operators. No existing EUDR platform offers this. ZKP circuit requires Global Forest Watch dataset integration and trusted setup ceremony before launch.
EU Corporate Sustainability Due Diligence Directive (CSDDD)	EU	Trade / ESG	Large companies sourcing from ASEAN must conduct human rights and environmental due diligence across their supply chains. Applies to EU companies; flows down to ASEAN suppliers via contractual requirements.	SADT's fiduciary governance model and cooperative negotiation layer satisfy the spirit of CSDDD supply chain requirements. FDO dispute mechanism, revocation rights, and Consent Agreement VC structure provide auditable evidence of farmer-protective governance. Formal CSDDD alignment statement recommended for EU corporate clients.
OECD Guidelines for Multinational Enterprises	International	Trade / ESG	Data governance, supply chain due diligence, and stakeholder engagement provisions applicable to AgriG8 as a technology intermediary operating across jurisdictions.	Non-binding but referenced by institutional investors and development finance institutions. SADT's governance architecture exceeds OECD guidelines' expectations. Useful for impact investor and development bank engagement.
Electronic Transactions Act (Cap. 88, Singapore)	Singapore	Electronic Records	Legal recognition of electronic signatures and contracts. Basis for Consent Agreement VC legal standing as binding data licence. Section 16C provides MLETR pathway for transferable records.	Fourth policy ask: sandbox recognition that DID-signed, DKG-anchored Consent Agreement VCs constitute binding electronic contracts. Legal opinion from Singapore-qualified counsel required. Existing ETA framework is broadly supportive; sandbox extension needed for DID-specific signature format.
Law on E-Transactions (2023, Luật Giao dịch điện tử)	Vietnam	Electronic Records	Electronic contracts, digital signature standards (must use licensed digital signature service provider), and e-commerce governance. Bilateral contracts signed via DID must satisfy Vietnamese e-signature requirements.	DID-based Ed25519 signatures may not satisfy Vietnamese licensed digital signature provider requirement. Legal assessment required: either DID signatures are wrapped by a licensed Vietnamese digital signature, or legal argument made that DID signatures satisfy equivalent security standards. Active compliance gap.
UNCITRAL Model Law on Electronic Transferable Records (MLETR)	International	Electronic Records	International model law providing basis for electronic equivalents of bills of lading and other transferable documents. Adopted by Singapore; not yet adopted by Vietnam.	SADT's ISO 20022 Knowledge Assets are designed to qualify as MLETR-compliant transferable records in Singapore. Vietnam's non-adoption is a gap: trade finance triggered in Vietnam requires workaround until MLETR adoption progresses. Third policy ask

APPENDIX A. Regulatory Exposure Matrix

Framework / Law	Jurisdiction	Domain	Key obligation for AgriG8	SADT architecture response
				addresses Singapore-side recognition; Vietnam-side MLETR advocacy recommended as a medium-term objective.
ASEAN Data Management Framework (2021)	ASEAN	Cross-Border Data	Baseline governance principles for cross-border data flows among ASEAN members: accountability, openness, security, and purpose limitation.	SADT architecture satisfies and materially exceeds AMF baseline. Useful framing document for ASEAN Secretariat engagement.
ASEAN Model Contractual Clauses for Cross-Border Data Flows	ASEAN	Cross-Border Data	Standard contractual terms for cross-border data transfers between ASEAN member states. May be required where data transfers occur outside SADT's CtD architecture.	Consent Agreement VCs provide stronger individual rights protections than ASEAN MCCs. MCCs may be required as a fallback for any data flows that fall outside the CtD/ZKP architecture (e.g., Foundation metadata, academic node exchanges).
ASEAN Digital Economy Framework Agreement (DEFA)	ASEAN	Cross-Border Data	In negotiation; expected to be first binding regional digital economy agreement. Provisions expected on data flows, digital identity, and agricultural data governance.	SADT's architecture is designed to be DEFA-ready. Engagement with ASEAN Secretariat during negotiation phase recommended to ensure SADT-compatible provisions on data trust structures and ZKP-based verification.
Singapore-Vietnam Digital Economy Agreement	SG / VN	Cross-Border Data	Bilateral digital economy cooperation framework. Provisions on data flows, digital trade, and electronic invoicing. Basis for regulatory coordination on SADT pilot.	Primary bilateral instrument for the pilot corridor. MAS-MOIT joint sandbox framework should be structured as an implementation mechanism under this agreement. Provides existing institutional channel for regulatory cooperation.
Companies Act + IPC Registration (Commissioner of Charities)	Singapore	Corporate Structure	Foundation must be incorporated as a Company Limited by Guarantee and registered as an Institution of a Public Character (IPC) to obtain charitable status and fiduciary mandate. Commissioner of Charities oversight applies.	IPC registration is a prerequisite for the fiduciary mandate that distinguishes SADT from a commercial data broker. Registration timeline: 3–6 months. Governance documents (constitution, conflict of interest policy, board composition) must satisfy Commissioner of Charities requirements before sandbox application.
Law on Cooperatives (2023, Luật Hợp tác xã)	Vietnam	Corporate Structure	Defines cooperative governance, member rights, and representative authority. Basis for cooperatives to act as farmer data negotiators and, under the fifth policy ask, as legal representatives in arbitration.	Fifth policy ask: explicit recognition of cooperative legal standing in SIAC/VIAC data rights proceedings. 2023 Law's updated provisions on cooperative authority in commercial dealings are supportive. Sandbox extension needed to confirm this authority extends to data rights arbitration specifically.

Active compliance gaps requiring immediate legal attention are highlighted in the SADT Architecture Response column. The most time-sensitive are: EU AI Act conformity assessment for Confidence Score (if used in EU-connected credit decisions); Vietnamese Law on E-Transactions compatibility for DID-based signatures; Law on Data intermediary registration; and IPC registration timeline relative to pilot launch. None of these gaps invalidates the SADT's architecture; all are addressable with appropriate legal and regulatory engagement in the 12 months preceding commercial operation.

Technical Whitepaper

TECHNICAL WHITEPAPER

The Field as a Work of Authorship:

Architecture and Trust Model of the Singapore–ASEAN Data Trust (SADT)

Prepared by: Liyana Mahirah, AgriG8

Version: 0.9 — Draft for technical review

Intended audience: Technical implementers, integration partners, data infrastructure architects, protocol developers

ABSTRACT

The Singapore–ASEAN Data Trust (SADT) is a non-custodial, decentralised verification infrastructure designed to convert smallholder farm activity into high-integrity, cross-border signals — without extracting or centralising raw farmer data. This paper sets out the full technical architecture: the five-layer stack from biometric identity anchoring through compute-to-data fusion to ISO 20022 banking signals; the trust model and associated threat surface; resilience design for low-connectivity rural deployment; and the governance mechanisms that prevent the cooperative node layer from becoming a new form of extraction. It also addresses adjacent competitive infrastructure, risk registers, and the phased integration plan for the Vietnam–Singapore pilot corridor. The policy rationale and regulatory asks are treated in a companion policy brief; this document focuses on implementation.

CONTENTS

ABSTRACT	1
CONTENTS	2
SECTION 1. PROBLEM FRAMING AND INSTITUTIONAL CONTEXT	4
1.1 The yield gap is a trust gap	4
1.2 Why farmers withhold data	4
1.3 Why centralized solutions fail	4
1.4 The required properties of a trustworthy system	4
1.5 EUDR compliance: the immediate forcing function	5
SECTION 2. ARCHITECTURE OVERVIEW: THE NON-CUSTODIAL VERIFICATION MODEL	6
2.1 The core principle	6
2.2 System actors	6
2.3 Five-layer stack summary	6
SECTION 3. LAYER 1 — IDENTITY AND PROVENANCE	9
3.1 The biometric anchor problem	9
3.2 VNeID Level 2 authentication	9
3.3 Decree 357 Digital Property ID integration	9
3.4 Session initialisation and CID chaining	10
SECTION 4. LAYER 2 — INPUT INGESTION AND LOCAL DISCOVERY	11
4.1 Sensor infrastructure	11
4.2 Manual narrative logs	11
4.3 Local IPFS storage and metadata seeding	11
SECTION 5. LAYER 3 — COMPUTE-TO-DATA FUSION AND ANALYSIS	12
5.1 The Compute-to-Data model	12
5.2 Compute job lifecycle	12
5.3 The satellite data integration	12
5.4 Algorithm governance	13
5.5 Zero-knowledge proofs for binary claims	13
SECTION 6. LAYER 4 — REGISTRY, NOTARISATION, AND BANKING SIGNAL	15
6.1 From confidence score to banking instrument	15
6.2 ISO 20022 wrapping	15
6.3 OriginTrail DKG registration	15
SECTION 7. LAYER 5 — AUDIT, SETTLEMENT, AND ATTRIBUTION	16
7.1 The read-receipt architecture	16
7.2 Attribution and service offsets	16
7.3 SGTraDex integration	16
7.4 Measurement transparency: what the Confidence Score is and is not	16
SECTION 8. FARMER-SOVEREIGN TRACEABILITY — DECENTRALISED IDENTITY AND ON-CHAIN VERIFICATION	18
8.1 The mediated dashboard problem	18
8.2 W3C Decentralised Identifiers (DIDs)	18
8.3 DID issuance at enrollment	18
8.4 Rights-holder registration on Knowledge Assets	19
8.5 Read Receipts as W3C Verifiable Credentials	19
8.6 Independent DKG verification in practice	20
8.7 Key custody, loss, and recovery	20

8.8 Limitations and open technical questions	21
8.9 On-chain dispute filing and the evidence package	21
SECTION 9. THE DATA MARKETPLACE AND COOPERATIVE NEGOTIATION LAYER	23
9.1 The demand-pull problem and why it inverts farmer agency	23
9.2 Tiered vendor registry: solution providers first	23
9.3 Data Request Offers (DROs): the vendor posting layer	24
9.4 Cooperative evaluation and the advisory role	25
9.5 The farmer opt-in and negotiation interface	26
9.6 Vendor-specific Consent Agreement VCs	26
9.7 Revocation and post-access accountability	27
9.8 Salespeople, field agents, and vendor outreach	27
9.9 The implications for ‘farmer as author’	28
9.10 Integration with the existing layer stack	28
SECTION 10. THE ACADEMIC NODE: FEDERATED HISTORICAL DATA INTEGRATION	29
10.1 The historical integrity problem	29
10.2 Onboarding research institutions as Data Guardians	29
10.3 The federated blind join	29
10.4 Institutional reciprocity	29
SECTION 11. TRUST MODEL AND THREAT ANALYSIS	30
SECTION 12. RESILIENCE DESIGN: LOW-CONNECTIVITY AND FIELD CONDITIONS	32
12.1 The connectivity reality of rural Vietnam	32
12.2 Degraded-mode operation	32
12.3 Sensor calibration and physical integrity	32
12.4 Hardware supply chain	32
SECTION 13. FOUNDATION GOVERNANCE AND SUSTAINABILITY	33
13.1 Why a foundation structure	33
13.2 Governance structure	33
13.3 Sustainability model	33
13.4 The Co-operative Clause in detail	34
13.5 The Farmer Data Ombudsman	34
13.6 Farmer revocation rights: the full scope	35
SECTION 14. COMPETITIVE AND ADJACENT LANDSCAPE	37
SECTION 15. RISKS, MITIGATIONS, AND OPEN QUESTIONS	38
15.1 Open technical questions	38
SECTION 16. PILOT PLAN: VIETNAM–SINGAPORE 2026	40
16.1 Pilot objectives	40
16.2 Detailed milestone plan	40
16.3 Success criteria	41
16.4 Budget overview	41
CLOSING NOTE	42
TECHNICAL WHITEPAPER — THE SINGAPORE-ASEAN DATA TRUST MARCH 2026	2

SECTION 1. PROBLEM FRAMING AND INSTITUTIONAL CONTEXT

1.1 The yield gap is a trust gap

Southeast Asia's 'yield gap' — the difference between actual smallholder output and agronomically achievable productivity — is typically framed as a technology deficit. The literature cites poor access to quality seeds, fertiliser, water management, and agronomic advisory. These are real constraints. But they are downstream of a more fundamental problem: capital does not reach smallholders at the price and speed required to close the gap, because financial institutions cannot verify the inputs and outputs that would allow them to price risk accurately.

The verification problem is circular. Banks require production history to underwrite credit; farmers require credit to improve production; cooperatives require verified throughput data to negotiate supply contracts; commodity buyers require verified quality data to offer premiums; and insurers require verified field conditions to automate parametric payouts. Every participant in the chain is waiting for someone else to prove something. Physical audits — the current solution — are expensive, slow, easily corrupted, and impossible to scale.

1.2 Why farmers withhold data

The conventional assumption in agri-tech design is that farmers are passive subjects who will share data if provided with sufficiently easy tools. Field experience contradicts this. Farmers in fragmented commodity markets have learned, correctly, that granular production data can be used against them. A trading house that knows the precise timing and volume of a specific cooperative's harvest can structure its offers accordingly. An input supplier that knows a farmer's fertiliser budget can price to that limit. Data sharing, without enforceable protections, is a form of unilateral disarmament.

The result is a market failure: the data required to reduce transaction costs throughout the agricultural supply chain exists at the farm level but is systematically withheld because the institutional structure for protecting its generator does not exist. This is not a problem that better mobile interfaces or more capable sensors can solve.

1.3 Why centralized solutions fail

Most agri-data platforms respond to this problem by building centralized repositories: a company collects farmer data, manages it in its cloud, and sells access to buyers, banks, and insurers. This model fails structurally for three reasons.

First, it replicates the extraction problem at a higher level of sophistication. The aggregator captures the value that was previously captured by the trading house; the farmer's position relative to the market does not improve. Second, centralized repositories create catastrophic liability — a single breach exposes the production data of an entire cooperative or region. Third, the aggregator becomes a single point of failure: if the company pivots, gets acquired, or becomes insolvent, the farmers' data history disappears or changes hands without their consent.

1.4 The required properties of a trustworthy system

A system that can close the trust gap must satisfy five properties simultaneously. It must be technically verifiable: the signal it produces must be checkable by an external party without taking that party's word for it. It must be non-custodial: raw data must not move to a central repository. It must be legible: outputs must be expressed in the standards that banks, insurers, and commodity buyers already use. It must be attributable: the rights-holder whose data generated a given signal must be identifiable and compensable. And it must be sustainable: the infrastructure must be able to maintain itself without depending on the commercial incentives of a single actor.

The SADT is designed to satisfy all five properties. No existing platform in the region does.

1.5 EUDR compliance: the immediate forcing function

The EU Deforestation Regulation (EUDR), which came into force in 2023 and applies to seven commodity categories including rice, coffee, and palm oil, requires exporters to prove that products are not associated with deforestation or forest degradation after December 2020. The operative requirement is a geolocated, verifiable claim that specific farm plots are deforestation-free — backed by GPS coordinates, satellite evidence, and supply chain documentation. Non-compliant products cannot enter the EU market.

This creates an immediate, high-stakes verification demand for every smallholder supplying EU-bound commodity chains in ASEAN — and a structural problem that no existing compliance platform solves fairly. Every current EUDR compliance tool — across 15+ platforms reviewed — requires the farmer to surrender raw GPS coordinates and production data to a company's cloud. The compliance platform becomes the custodian of precise farm location data for millions of smallholders. For a Vietnamese jasmine rice farmer supplying an EU buyer, this means disclosing the exact location of their land — data that, in the wrong hands, could be used to assess their market position, price their land, or exclude them from future contracts.

The SADT's architecture resolves this structurally. A zero-knowledge proof can demonstrate that a specific GPS polygon does not overlap with any deforestation event in the Global Forest Watch dataset after December 2020, without transmitting the GPS polygon to the compliance platform or the EU buyer. The verifier receives a cryptographic proof that the claim is true; they never receive the coordinates that would let them build a land database of smallholder plots. EUDR compliance is therefore the most immediate and commercially urgent use case for the SADT's 'data stays local, truth travels' architecture — and the use case where its advantage over centralised alternatives is most concrete.

SECTION 2. ARCHITECTURE OVERVIEW: THE NON-CUSTODIAL VERIFICATION MODEL

2.1 The core principle

The SADT operationalises a single architectural principle: data stays local; truth travels. Raw farm records — sensor logs, photographs, identity-linked harvest weights — remain in the physical custody of the farmer, village cooperative, or local gateway node. External parties never receive these files. They receive instead a verified attestation: a machine-readable confidence score, provenance-linked to a specific registered land parcel and farmer identity, expressing the result of a defined analytical question.

The mechanism that makes this possible is Compute-to-Data (CtD): rather than moving data to a computation environment, the computation environment travels to where the data lives. An approved algorithm is executed inside a sandboxed container on the local node; only the output crosses to the requesting party. The underlying data never leaves the jurisdiction of origin.

2.2 System actors

The SADT involves five distinct actor categories, each with defined roles and access levels.

Actor	Role	Data access
Farmer / Rights-holder	Generates primary records; authorises algorithmic consent; receives attribution and audit receipts	Full access to own records; read receipts of all queries against their data
Village Cooperative	Operates local node; co-signs harvest data; manages physical access to gateway hardware	Access to aggregated cooperative-level signals; cannot access individual farmer raw records without consent
SADT Foundation	Governs access policy; maintains registry; enforces Co-operative Clause; processes no raw data	Access to metadata, CIDs, and audit logs only; no access to raw sensor or biometric data
External Firms (banks, buyers, insurers)	Initiate approved Compute-to-Data queries; receive confidence scores and ISO 20022 signals	Receive only outputs of approved compute jobs; no access to raw data or identifiers
Research Institutions	Register historical datasets as restricted research assets; participate in federated joins	Retain full custody of own datasets; receive read receipts when data contributes to a query

2.3 Five-layer stack summary

The architecture is organised into five functional layers. Each layer uses a specific combination of protocols, but the protocols are implementation choices — what matters is what each layer actually does. Each layer is also independently replaceable: if a better tool emerges, it can be swapped without redesigning the layers above or below it.

L1

Identity & Provenance

What it does: Proves that a specific, legally registered person owns a specific, legally registered piece of land — and that both were verified at the moment the data was recorded. Without this, a sensor could be anywhere and the data could belong to anyone.

How: Vietnam's national biometric ID system (VNeID) confirms the farmer is a real, verified citizen via a live face scan on their phone. Vietnam's national land registry (Decree 357) confirms the GPS coordinates of their registered plot. Every data record generated in a session is stamped with both. This is the lock that makes spoofing structurally difficult rather than merely prohibited.

Protocols: VNeID Level 2 · Decree 357 Digital Property ID

L2

Input Ingestion & Local Discovery

What it does: Collects sensor readings, farmer photos, and cooperative co-signatures, stores them locally on village hardware, and publishes a searchable index — but not the data itself — so external parties know a verified dataset exists without being able to access its contents.

How: Sensor data and manual logs are fingerprinted (each record gets a unique cryptographic hash, like a tamper-evident seal) and stored on a local server at the village cooperative. The raw files never leave. A separate index entry — describing what crop, what district, what season, with a pointer to the fingerprint — is published to a marketplace so vendors can discover and request access. Think of it as a library catalogue that tells you a book exists without letting you read it.

Protocols: IPFS local node (private, not public) for storage · LoRaWAN for sensor transmission · Ocean Protocol V4 for the discoverable index

L3

Compute-to-Data Fusion

What it does: Allows an external party to run an approved analysis on local data and receive only the result — never the underlying data. The analysis travels to the data; the data does not travel to the analysis.

How: An approved algorithm is packaged and sent to the village gateway. It runs inside a sealed, temporary environment on the local server, reads the sensor logs and photos it needs, cross-references with independent satellite imagery, and produces a single verified output — a Confidence Score and yield classification. The sealed environment is then destroyed. Nothing the algorithm touched leaves the village. This is what allows raw farm data to stay in Vietnam while a verified signal reaches Singapore.

Protocols: Ocean Protocol Compute-to-Data · Docker sandbox · Sentinel-2 satellite imagery (ESA)

L4

Registry & Notarisation

What it does: Converts the verified output into a legal record that a bank or trading house can act on — in the format their systems already understand — and permanently anchors that record so it cannot be altered or disputed after the fact.

How: The Confidence Score is packaged into the financial messaging standard that banks worldwide use (ISO 20022), then registered on a decentralised record-keeping network where it receives a permanent unique address (UAL). Any party with that address can independently verify the record is unchanged. Under Singapore's legal framework, this can be treated equivalently to a physical bill of lading. The record is not stored in any single company's database — it is distributed across an independent network that no single party controls.

Protocols: OriginTrail Decentralised Knowledge Graph (DKG) for permanent anchoring · ISO 20022 XML for banking-standard packaging · MLETR for legal recognition

L5**Audit & Settlement**

What it does: Creates a permanent, tamper-evident receipt every time a query is run against a farmer's data — visible to the farmer and cooperative, not suppressible by the querying party — and triggers the attribution and payment obligations that follow from that query.

How: Every approved analysis generates a signed receipt, stored on the same decentralised record network as the verified output. The farmer sees who accessed what, when, and for what stated purpose — directly on their phone, without relying on AgriG8 to relay it accurately. The cooperative sees the full picture across all its members. Agreed payment or service credit obligations flow from these receipts. Settlement connects to Singapore's trade data exchange infrastructure for logistics and finance workflows.

Protocols: OriginTrail DKG for audit receipts · SGTraDex for trade settlement · Cooperative dashboard for farmer-facing visibility

SECTION 3. LAYER 1 — IDENTITY AND PROVENANCE

3.1 The biometric anchor problem

Any decentralised verification system faces a fundamental spoofing threat: without a reliable link between a digital record and a physical reality, a motivated actor can move sensors between plots, fabricate logs, or register fictional parcels. The value of the SADT's confidence scores depends entirely on the strength of this link. This is why Layer 1 is the most critical and, in some respects, the most legally complex component of the architecture.

Vietnam is uniquely positioned to provide this anchor. No other ASEAN member state currently operates a unified biometric identity system (VNeID) linked to a digital land registry (Decree 357) at national scale. This combination allows the SADT to bind every data record to both a verified citizen identity and a legally registered geographic polygon — making spoofing practically impossible without compromising both systems simultaneously.

3.2 VNeID Level 2 authentication

Vietnam's VNeID system, operated by the Ministry of Public Security, provides chip-based electronic identity to citizens. Level 2 authentication requires a biometric liveness check — a face scan matched against the chip data on the physical ID card — and confirms that the authenticated individual is a live, registered citizen, not a photograph or replay attack.

In the SADT pilot, the farmer performs the Level 2 face scan via the SADT interface — a Telegram Mini-App running on the farmer's smartphone. The biometric verification is performed on-device using the national VNeID SDK; the raw biometric data (face image) is processed locally and never transmitted to the SADT, the cooperative, or any external server. What the system receives is a signed verification token from the VNeID infrastructure confirming "Citizen [citizen ID hash] has been verified at Level 2 at [timestamp]."

Biometric data handling:

Raw biometric data (face images, fingerprints) is processed entirely within the VNeID national infrastructure or on-device. The SADT receives only a signed verification token — a hash of the citizen ID, the verification timestamp, and a MPS-issued signature. No biometric images are stored, transmitted, or accessible to AgriG8, the cooperative, or any external party.

This is a critical compliance requirement under Vietnam's PDPL and must be contractually confirmed with the Ministry of Public Security before pilot launch.

3.3 Decree 357 Digital Property ID integration

Following identity verification, the SADT Oracle pings the Vietnamese National Land Database API (governed by Decree 357, 2024) to retrieve the Digital Property ID associated with the verified citizen's registered land holdings. The returned Property ID is a structured string (format: VN-[province code]-DC357-[parcel number]) containing the precise GPS polygon of the registered field, its area in hectares, the registered crop type, and the legal ownership status.

This Property ID 'wraps' all subsequent data records generated within that harvest session. Every sensor log, photograph, and cooperative co-signature is tagged with the Property ID at the point of creation, establishing an unbroken provenance chain from physical plot to digital record.

Integration dependency:

Access to the Decree 357 API for commercial verification purposes requires a data-sharing agreement with the Ministry of Natural Resources and Environment (MONRE) and potentially the Ministry of Agriculture and Rural Development (MARD). As of March 2026 this API is not publicly accessible to private oracles. Securing this agreement is a pre-condition for the pilot and is on the critical path. See Section 16 (Pilot Plan).

3.4 Session initialisation and CID chaining

Once identity and property verification are complete, the Oracle generates a Session Root CID: a Content Identifier (SHA-256 hash) of the combined {citizen ID token + Property ID + session timestamp}. All subsequent data objects generated in that harvest session — sensor logs, photographs, cooperative co-signatures — are hashed individually and chained to the Session Root CID in a Merkle-tree structure. This means that any post-hoc modification of any record in the session is immediately detectable: the chain of hashes will not verify.

SECTION 4. LAYER 2 — INPUT INGESTION AND LOCAL DISCOVERY

4.1 Sensor infrastructure

The SADT is sensor-agnostic: it does not specify particular hardware but defines an ingestion interface that any compliant sensor can address. The pilot deployment uses solar-powered IoT nodes measuring soil NPK (nitrogen, phosphorus, potassium) and moisture at 6-hour intervals, transmitting via LoRaWAN to a village gateway. LoRaWAN is selected for the pilot because it provides adequate range (2–15 km in flat terrain) with very low power consumption, suitable for deployments without reliable mains electricity.

The village gateway — a ruggedised edge compute device running Ubuntu 22.04 LTS — receives sensor payloads, appends the Session Property ID tag, computes the SHA-256 hash of each payload, and writes both the hash (CID) and the raw payload to local IPFS storage (Kubo v0.26+). The raw payload never leaves the gateway without an explicit approved Compute-to-Data request.

4.2 Manual narrative logs

Continuous sensor data is necessary but not sufficient for full harvest verification. The SADT supplements it with three categories of manual narrative log, submitted by the farmer via a Telegram Bot interface:

- Input photographs: GPS-tagged images of fertiliser bags, pesticide containers, or seed packets, submitted at point of application. These are hashed and stored locally alongside the automated sensor logs.
- Pest and event logs: Free-text or voice-note observations of field events (flooding, pest sightings, equipment failures), timestamped and tagged with the session Property ID.
- Harvest gate records: At the moment of harvest, a Cooperative Field Agent uses a ruggedised tablet to co-sign the farmer's weight and quality data. The co-signature is a second VNeID-verified identity token (the agent's), cryptographically appended to the harvest record. This creates a two-party attestation that the recorded yield was physically weighed and graded.

The manual log layer is important for two reasons. First, satellite imagery and IoT sensors cannot independently verify critical events like fertiliser application or pest treatment; human observation fills this gap. Second, the act of co-signing creates a cooperative accountability structure: the agent's identity is on the record alongside the farmer's, creating a disincentive for falsification.

4.3 Local IPFS storage and metadata seeding

All data objects — sensor logs, photographs, co-signatures — are stored on the village gateway's Kubo IPFS node. The node is configured in a restricted mode: it does not participate in the public IPFS DHT and does not serve content to arbitrary requests. It is a private, local content-addressed store, accessible only to authorised Compute-to-Data jobs initiated through the SADT Foundation's access control layer.

Separately, the cooperative's SADT interface publishes a metadata record to the Ocean Protocol V4 marketplace. This metadata record contains no raw data: it lists the district, crop type, growing season, approximate yield range, and the session root CID. It is essentially an index entry, allowing external parties to discover that a verified dataset exists and to initiate a Compute-to-Data query against it without ever seeing the underlying content.

SECTION 5. LAYER 3 — COMPUTE-TO-DATA FUSION AND ANALYSIS

5.1 The Compute-to-Data model

Compute-to-Data (CtD) is a cryptographic access control paradigm in which computation is brought to data rather than data being moved to computation. A requesting party submits an approved algorithm (packaged as a Docker image) to the data custodian; the algorithm executes inside a sandboxed container with read-only access to the local dataset; and only the container's output is returned to the requester. The underlying data objects are never transmitted.

In the SADT context, CtD resolves two otherwise irreconcilable requirements: external parties need to verify claims about a farmer's harvest, but the farmer needs the underlying data to remain in local custody. CtD satisfies both simultaneously. It also resolves the cross-border data residency problem: the raw data never crosses a border, so it does not trigger data residency restrictions under Vietnamese law. Only the insight travels.

5.2 Compute job lifecycle

A typical Compute-to-Data job proceeds as follows:

1. The external requester (e.g., a commodity trading house) discovers a SADT dataset via the Ocean V4 marketplace metadata and initiates a CtD job request, specifying the dataset CID, the algorithm Docker image hash, and the query parameters (e.g., harvest season, plot identifier).
2. The SADT Foundation's access control layer validates the request against the farmer's Algorithmic Consent token for that season. If the query type is covered by the consent scope, the request proceeds. If not, it is rejected and the farmer is notified.
3. The Ocean Protocol infrastructure spins up a Docker container on the village gateway's compute environment. The container is granted read-only access to the relevant IPFS objects via a time-limited access token. No write access is granted.
4. The algorithm executes inside the container. For the standard harvest verification query, the algorithm: (a) retrieves the Sentinel-2 satellite NDVI readings for the registered GPS polygon for the growing season; (b) cross-references these with the IoT soil moisture and NPK logs; (c) cross-references with the cooperative co-signature harvest weight; and (d) computes a composite Confidence Score (0–1) and a VerifiedYield classification (High / Medium / Low / Unverified).
5. The container outputs a single signed JSON object containing the Confidence Score, VerifiedYield classification, session root CID, property ID, and a cryptographic hash of the algorithm image used (for auditability). The container then terminates and all temporary files are purged.
6. The output JSON is transmitted to the SADT Foundation's Registry layer (Layer 4) for notarisation, and a summary is transmitted to the requester.

5.3 The satellite data integration

Sentinel-2 satellite imagery (ESA Copernicus programme, freely available, 10m resolution, approximately 5-day revisit cycle) is used as the primary independent verification source. NDVI (Normalised Difference Vegetation Index) provides a proxy for crop biomass and greenness that is independent of ground-level reporting. The fusion algorithm compares the NDVI time series for the registered GPS polygon with the farmer-reported growing schedule and the IoT moisture logs.

A field that shows NDVI consistent with healthy jasmine rice at expected growth stages, with soil moisture consistent with adequate irrigation, and a registered harvest co-signature, receives a high Confidence Score. A field that shows

NDVI inconsistent with the reported crop type, or moisture logs inconsistent with the satellite-inferred growing season, receives a low score and triggers a manual review flag.

This cross-referencing makes simple data falsification — a farmer or cooperative agent submitting fabricated sensor logs — detectable without requiring a physical audit. The satellite cannot be bribed.

5.4 Algorithm governance

The algorithms available for CtD execution are governed by the SADT Foundation's Algorithm Registry. An algorithm must be submitted, reviewed for safety (no data exfiltration, no persistent writes), and registered with a cryptographic hash before it is eligible for deployment against farmer data. The algorithm's hash is recorded in every output JSON, allowing any downstream party to verify exactly which computation was run against which data. This creates an auditable chain of algorithmic custody.

External firms can propose new algorithm types (e.g., carbon sequestration verification, drought stress scoring) but cannot deploy them without Foundation approval. Algorithm review includes a data-minimisation assessment: if a proposed algorithm requests access to more data objects than required for its stated purpose, it is rejected.

Container security note:

Ephemeral Docker containers provide meaningful but not unconditional isolation. A malicious operator of a village gateway node could theoretically log container outputs before purge or instrument the underlying filesystem. The SADT mitigates this through: (a) hardware attestation of the gateway node at enrollment; (b) periodic remote audit of gateway configurations; and (c) anomaly detection on output distributions — a node producing systematically higher confidence scores than satellite data would predict is flagged for investigation. See Section 11 (Threat Analysis) for full discussion.

5.5 Zero-knowledge proofs for binary claims

Compute-to-Data with Docker is the right tool for the SADT's primary verification tasks — the multi-variable Confidence Score, agronomic analysis, historical lineage joins. These require complex computation, satellite API calls, and flexible analytical logic that cannot be efficiently expressed in another form. But a different class of verification task arises where CtD is unnecessarily heavy: binary or threshold claims where the question is not 'what is the score' but 'does this meet the requirement.'

EUDR compliance is the clearest example. The question is: does this GPS polygon overlap with any deforestation event after December 2020? The answer is yes or no. To answer it, the algorithm needs the farmer's precise GPS coordinates. Under CtD with Docker, those coordinates stay local but the algorithm still 'sees' them inside the container — the isolation protects against external access, not against a compromised node operator. For a binary deforestation check, there is a stronger approach: a zero-knowledge proof (ZKP).

A ZKP allows a prover to demonstrate that a statement is true without revealing the information that makes it true. For a deforestation check: the farmer's device or gateway generates a proof that 'polygon P, which I know and you do not, does not intersect any cell in dataset D' — and the verifier can confirm the proof is valid without ever learning the coordinates of P. The proof is cryptographically binding: it cannot be fabricated, and it reveals nothing about the underlying data beyond the binary conclusion.

The SADT implements ZKPs as a Layer 3 sub-capability for binary and threshold claims. The use cases are: EUDR deforestation-free certification; green loan eligibility (yield history meets minimum threshold, without disclosing exact yields); legal land registration confirmation (parcel is registered, without disclosing location to a third party). For each,

the ZKP is generated on the local gateway and transmitted alongside the proof's public verification key. Any party — the EU importer, the bank, the certification body — can verify the proof independently using only public information. The proof system used is Groth16 (a succinct non-interactive argument of knowledge, or SNARK), implemented using the `snarkjs` library for browser and Node.js compatibility. Circuit compilation and trusted setup are performed by the Foundation's technical team and published openly for independent audit.

CtD vs ZKP: when each applies

Use CtD with Docker when: the output is a composite score or analytical result requiring multi-variable computation, satellite API integration, or ML inference. The output is not sensitive; the inputs are protected by container isolation and hardware attestation.

Use ZKP when: the output is a binary or threshold claim (yes/no, above/below), and the underlying data — particularly location data — must be protected even against a compromised node operator. ZKPs provide mathematical, not operational, privacy guarantees.

SECTION 6. LAYER 4 — REGISTRY, NOTARISATION, AND BANKING SIGNAL

6.1 From confidence score to banking instrument

A confidence score in a JSON file has no legal standing. For the SADT to unlock trade finance, the verified output must be expressed in a form that financial institutions recognise, and it must be legally registerable as a transferable instrument. Layer 4 performs this translation.

6.2 ISO 20022 wrapping

ISO 20022 is the global standard for financial messaging, used by SWIFT, TARGET2, and most major interbank payment systems. DBS, OCBC, and Vietcombank all support ISO 20022 message processing. The SADT uses the camt.052 message class (bank transaction report) as the wrapper for verified agricultural signals, extended with custom supplementary data fields carrying the SADT-specific payload.

The cooperative's gateway server constructs the ISO 20022 XML message containing: the Confidence Score and VerifiedYield classification; the Decree 357 Property ID and GPS polygon; the Session Root CID (linking to the immutable provenance chain in IPFS); the algorithm hash; the VNeID verification token hash (not the biometric data — only the hash of the verification token); and the cooperative co-signature identifier. This message is then digitally signed using the cooperative's registered cryptographic key.

6.3 OriginTrail DKG registration

The signed ISO 20022 message is submitted to the OriginTrail Decentralised Knowledge Graph (DKG), where it is registered as a Knowledge Asset — a permanent, content-addressed record anchored to a distributed network of OriginTrail nodes. The Knowledge Asset receives a UAL (Universal Asset Locator), which serves as the globally unique identifier for that specific verified harvest record.

The UAL is then the single reference that external parties — banks, insurers, commodity buyers — use to retrieve the verified signal. The UAL resolves to the signed ISO 20022 message, which can be independently verified against the on-chain hash.

Under Singapore's MLETR framework, a digitally signed, tamper-evident record meeting specified criteria can be treated as a Legal Transferable Record — equivalent, for trade finance purposes, to a bill of lading. The SADT's policy ask (detailed in the companion policy brief) is for MAS to recognise SADT-issued ISO 20022 Knowledge Assets as meeting these criteria within the proposed regulatory sandbox.

Protocol dependency risk:

OriginTrail is a commercial decentralised knowledge graph protocol with its own tokenomics (TRAC token) and governance. The SADT's reliance on OriginTrail creates a dependency risk: changes to OriginTrail's terms, pricing, or protocol could affect the availability or cost of Knowledge Asset registration.

Mitigation: The SADT's Architecture Review roadmap includes evaluation of alternative DKG protocols (e.g., Ceramic Network, Veramo) for Layer 4 redundancy. All Knowledge Assets are also mirrored to a Foundation-operated archive node, ensuring data availability independent of OriginTrail's commercial status. Farmer records are never exclusively held by OriginTrail.

SECTION 7. LAYER 5 — AUDIT, SETTLEMENT, AND ATTRIBUTION

7.1 The read-receipt architecture

Every successful Compute-to-Data job generates a Read Receipt: a tamper-evident log entry on the OriginTrail DKG recording the query type, the requesting party's registered identifier, the dataset UAL queried, the timestamp, and the algorithm hash used. Read Receipts are generated automatically by the Ocean Protocol compute infrastructure and are not suppressible by the requesting party.

The cooperative's SADT dashboard aggregates Read Receipts for all data under its custody and presents them in a simple interface: which firms queried which datasets, when, and for what stated purpose. Individual farmers receive a personalised summary showing queries against their specific records. This creates a form of data use transparency that is structurally enforced rather than relying on voluntary disclosure by the querying party.

7.2 Attribution and service offsets

Read Receipts are the trigger for the attribution payment system. Under the Co-operative Clause (detailed in Section 11), firms accessing SADT data commit to a usage-linked attribution schedule. When a Read Receipt is generated for a commercial query — one initiated for trade finance, commodity pricing, or insurance purposes — it triggers a micro-attribution calculation based on the query type and the commercial value of the outcome.

For the pilot phase, attribution is expressed as Service Offsets rather than cash payments: verified data usage earns the farmer credit against cooperative services such as input purchasing, equipment hire, or storage fees. This avoids the complexity of cross-border micropayment infrastructure while still creating a tangible, legible economic return for data contribution. Post-pilot, the architecture is designed to support direct payment settlement via SGTraDex or equivalent payment rails.

7.3 SGTraDex integration

SGTraDex (Singapore Trade Data Exchange) is the Singapore government's secure, consent-based data exchange platform for supply chain logistics. The SADT's Layer 5 integration with SGTraDex allows SADT-verified harvest signals to be incorporated into broader trade logistics flows: customs declarations, freight bookings, and letter of credit workflows can reference the SADT UAL as a verified quality and provenance attestation, reducing documentation overhead and enabling faster settlement.

7.4 Measurement transparency: what the Confidence Score is and is not

The Confidence Score is a measurement, not an inference about the farmer's character, behaviour, or creditworthiness. It expresses the degree to which a specific set of physical conditions — satellite-observed canopy state, soil sensor readings, cooperative co-signature — is consistent with the farmer's registered harvest claim on a specific date. It is closer to a calibrated instrument reading than to a behavioral profile. This distinction matters both technically and legally: the SADT is not an AI system producing predictions about people; it is a verification system producing attested measurements of events.

The practical consequence is that score explanation is a measurement transparency obligation, not an algorithmic accountability obligation. A farmer who receives a Confidence Score below a lender's threshold has a right to know which component drove that result — not because the SADT has characterised them, but because the reading may be wrong and they need enough information to dispute it through the FDO or to correct the underlying condition. Every Confidence Score output therefore includes a structured component breakdown: the NDVI contribution, the IoT sensor contribution, and the co-signature contribution, each expressed as a sub-score and a flag status. The farmer

sees this in plain language via their Telegram interface; the requesting party sees it in the signed JSON output alongside the composite score.

The SADT does not store Confidence Scores in a farmer profile. Scores are session-specific records anchored to a Session Root CID and a specific date. A farmer's score from the 2026 wet season is a record of that harvest; it is not an attribute of that farmer. Downstream parties — lenders, insurers, buyers — who wish to use historical score patterns to make inferences about a farmer are conducting their own analytical activity, under their own PDPA and PDPL obligations, using outputs that the SADT generated for a different, time-bounded purpose. That activity is outside the SADT's scope and outside its accountability.

7.5 National Query Intelligence: the host country reporting layer

Every query run against SADT data generates a Read Receipt. Individually, these are farmer-facing audit records. In aggregate, they are something different: a real-time signal of where global agricultural finance is concentrating its attention in the host country's food system. Which districts are receiving the most trade finance queries? Which crop types are attracting premium pricing verification? Which months see the highest insurer activity? Which firm categories — trading houses, development banks, insurers — are growing their query volume fastest?

This aggregate intelligence is a byproduct of the architecture, not an additional data collection requirement. The Read Receipt layer already exists. What the National Query Intelligence layer adds is a reporting pipeline that aggregates those receipts — stripped of all farmer identifiers, all cooperative identifiers, and all firm-specific identifying information — into a structured quarterly report delivered to MARD and MOIT as a structural condition of the SADT's operating licence in Vietnam.

The report contains: query volume by district and crop type, indexed to the same period in the prior year; query volume by firm category (trade finance, insurance, commodity procurement, agri-advisory, research), with no firm-level detail; average Confidence Score thresholds requested by firm category, indicating what quality standards the market is applying; and ZKP verification volumes by claim type (deforestation-free, green loan threshold, land registration), indicating which ESG compliance pathways are active in the market.

This reframes the Decree 357 API access negotiation structurally. The SADT's request for access to Vietnam's digital land registry is not a one-way ask from a Singapore foundation to the Vietnamese government. It is the first half of a reciprocal arrangement: Vietnam provides the land registry anchor that makes the SADT's signals trustworthy; the SADT provides Vietnam with advance intelligence about where international agricultural capital is looking, six months before it translates into price movements and supply chain decisions. A Vietnamese trade ministry that knows in February that three European trading houses are running unusually high jasmine rice verification queries in Tiền Giang has information it did not previously have — and which the trading houses did not intend to share.

The query aggregate is not personal data:

The National Query Intelligence report contains no farmer records, no cooperative identities, no firm-level identifying information. It is a statistical summary of market behaviour derived from on-chain records. It does not require a separate data sharing agreement under Decree 13 or the Law on Data — it is aggregate, non-personal market intelligence, analogous to a central bank reporting aggregate credit flows by sector without disclosing individual loans. The Foundation's legal counsel should obtain a formal opinion confirming this classification before the reporting mechanism is activated.

A secondary version of this report, at lower granularity, can be made available to the ASEAN Secretariat as part of the DEFA agricultural data governance pilot. This gives the regional body visibility of cross-border agricultural finance flows across the corridor without requiring access to any underlying farm data — and positions the SADT as infrastructure that generates public-good intelligence as a byproduct of its commercial operation.

SECTION 8. FARMER-SOVEREIGN TRACEABILITY — DECENTRALISED IDENTITY AND ON-CHAIN VERIFICATION

8.1 The mediated dashboard problem

The architecture described in Section 7 gives farmers a dashboard showing their Read Receipt history. This is meaningfully better than nothing. But it has a structural limitation that must be stated directly: a farmer using that dashboard is trusting AgriG8 to accurately relay what is recorded on the OriginTrail DKG. If AgriG8's servers were to show a different picture from the chain — suppressing certain Read Receipts, or misrepresenting which firms accessed which data — a farmer with no independent access to the chain has no way to detect this.

True traceability requires that the farmer — or any party acting on their behalf — can independently verify the complete history of their data's use without routing through AgriG8's infrastructure at any point. This requires two things: a persistent cryptographic identity that the farmer controls (not AgriG8), and a chain record where that identity is the registered rights-holder. The SADT's DID architecture provides both.

8.2 W3C Decentralised Identifiers (DIDs)

A Decentralised Identifier (DID) is a URI defined by the W3C DID 1.0 specification (2022). Unlike a username or account number assigned by a service provider, a DID is generated by the controller and derives its authority from cryptography rather than institutional registration. A DID looks like:

```
did:key:z6MkhaXgBZDvotDkL5257faiztiGiC2QtKLgpbnnEGta2doK
```

It resolves to a DID Document — a JSON-LD file containing the controller's public keys and optional service endpoints. The DID Document is publicly resolvable by anyone; resolution requires no contact with AgriG8 or the SADT Foundation. The DID is permanent: it does not expire, cannot be revoked by a third party, and continues to function regardless of whether AgriG8 remains in operation.

The farmer's DID is generated at SADT enrollment and becomes their canonical identifier for all data rights within the system. Every Knowledge Asset, Read Receipt, and Verifiable Credential issued by the SADT references this DID — not an AgriG8-managed account identifier.

8.3 DID issuance at enrollment

The SADT uses the did:key method for the pilot deployment. did:key generates a DID directly from a public key, requiring no network connection, no registration transaction, and no token fee. The generation process is:

1. The SADT Telegram Mini-App generates an Ed25519 asymmetric keypair on the farmer's device. The private key is stored in the app's device-level secure storage (Android Keystore / iOS Secure Enclave where available). The private key never leaves the device.
2. The public key is encoded using the multibase/multicodec conventions specified in the did:key method specification, producing the DID string.
3. The DID Document (containing the public key and a service endpoint pointing to the farmer's SADT data node) is registered on the OriginTrail DKG as an anchored record. This on-chain registration is what creates the verifiable link between the farmer's self-sovereign identifier and the public registry.
4. The DID is associated with the farmer's VNeID verification token hash in the SADT Foundation's access control layer — linking the cryptographic identity to the legally verified citizen identity, without exposing biometric data.

Pilot-phase custody compromise:

For farmers without modern smartphones or in areas with poor connectivity during enrollment, the Foundation operates a custodied key management service during the pilot. The keypair is generated by the Foundation, stored in an HSM-backed encrypted vault, and associated with the farmer's VNeID hash. The farmer receives the DID but the private key is Foundation-held.

This is an explicit trust compromise, accepted as a bootstrapping necessity. The pilot plan includes a migration path to device-native key custody for all participating farmers by the end of the pilot season, with the Foundation's custodied key shard invalidated after successful migration. Farmers on custodied keys are clearly disclosed as such in the Foundation's governance reporting.

8.4 Rights-holder registration on Knowledge Assets

Every Knowledge Asset written to the OriginTrail DKG by the SADT — harvest verification records, Read Receipts, Lineage Truth Units — includes the farmer's DID in its structured metadata under the rights-holder field. This is not a pointer to an AgriG8-managed record; it is the farmer's own cryptographic identifier, permanently embedded in the on-chain record at the time of creation.

The practical consequence: the OriginTrail DKG public API supports queries filtered by DID. A query of the form 'retrieve all Knowledge Assets where rights-holder = did:key:[farmer DID]' returns the complete set of on-chain records associated with that farmer — every harvest verification, every Read Receipt for every query run against their data, every Lineage Truth Unit that referenced their records. This query requires no AgriG8 API key, no authentication against AgriG8's servers, and no trust in any intermediary. It is a direct read against a public decentralised network.

8.5 Read Receipts as W3C Verifiable Credentials

The current architecture logs Read Receipts as DKG records. The DID architecture extends this: each Read Receipt is also issued as a W3C Verifiable Credential (VC) addressed to the farmer's DID and signed by the SADT Foundation's DID.

A Verifiable Credential is a tamper-proof, cryptographically signed claim. Its signature is verifiable against the issuer's public DID Document — which is on-chain and publicly resolvable. Verification requires only the Foundation's public key, not any AgriG8 server. The credential structure for a SADT Read Receipt VC is:

```
{
  "@context": [
    "https://sadtfoundation.org/contexts/v1",
    "https://www.w3.org/2018/credentials/v1"
  ],
  "type": ["VerifiableCredential", "SADTReadReceipt"],
  "issuer": "did:key:[SADT Foundation DID]",
  "credentialSubject": {
    "id": "did:key:[farmer DID]",
    "queryingParty": "[registered firm identifier]",
    "datasetUAL": "[OriginTrail UAL of queried Knowledge Asset]",
    "algorithmHash": "[SHA-256 of algorithm Docker image]",
    "queryType": "HarvestVerification",
    "commercialPurpose": "TradeFinance",
    "timestamp": "[ISO 8601 datetime]"
  },
  "proof": {
    "type": "Ed25519Signature2020",
    "verificationMethod": "[Foundation DID key ref]"
  }
}
```

The farmer's Telegram wallet stores the complete collection of Read Receipt VCs issued to their DID. This collection is the farmer's portable, self-sovereign audit trail. It can be presented to any third party — a development finance inspector, an NGO advocate, a government regulator — and independently verified against the Foundation's public DID Document without any AgriG8 involvement.

8.6 Independent DKG verification in practice

The OriginTrail DKG provides a public browser-based explorer at dkg.origintrail.io. A farmer's DID can be entered directly to retrieve all associated Knowledge Assets and Read Receipt VCs. For farmers who want to check for themselves, or for cooperative technical officers auditing on behalf of their membership, this is a zero-cost, direct read against the chain.

The critical property is this: the SADT Foundation's dashboard cannot show a different picture from the chain without creating a detectable discrepancy. If the Foundation were to suppress a Read Receipt from the dashboard, the VC would still exist in the farmer's wallet and on the DKG, with a valid cryptographic signature. If the Foundation were to fabricate a Read Receipt that doesn't exist on-chain, its hash would not verify. The chain is the ground truth; the dashboard is a convenience interface that cannot contradict it.

In practice, three groups will perform direct DKG verification rather than relying on the dashboard. Cooperative Technical Officers, trained as part of the pilot onboarding programme, will run quarterly DID audits for their membership using a simplified cooperative audit tool built on the DKG API. Third-party advocates — NGOs, legal aid organisations, development bank monitors — will use direct DKG queries as part of their own due diligence on the SADT's claims. And regulatory inspectors evaluating the MAS/MOIT sandbox will use DKG queries as their primary evidence source, independent of any reporting provided by AgriG8 or the Foundation.

Being honest about farmer usage:

Most farmers will not personally query the DKG. A rice farmer in Cái Bè will use the Telegram dashboard, not a blockchain explorer. This is not a failure of the architecture — it is the correct design.

The purpose of the DID/VC/DKG layer is not to require farmers to become blockchain users. It is to ensure that the system's claims about transparency are structurally verifiable by any technically capable party acting on the farmer's behalf, without needing AgriG8's cooperation. The farmer's DID and VC wallet give them the right to independent verification; whether they exercise it directly or through a trusted representative is their choice.

8.7 Key custody, loss, and recovery

The farmer's private key is the control mechanism for their DID. Loss of the private key means loss of control — the DID cannot be used to sign new transactions, and new VCs cannot be issued to it. For the custodied keys in the pilot phase, the Foundation can restore access. For device-native keys, a recovery scheme is required.

The SADT implements a 2-of-3 threshold signature recovery structure for device-native keys. The farmer's key can be recovered from any two of three shards: the farmer's device key (primary); the cooperative field agent's signing key (secondary); and a Foundation-held recovery shard (tertiary). No single party can unilaterally recover a farmer's identity. A malicious Foundation cannot reset a farmer's DID without the cooperative agent's cooperation. A malicious cooperative agent cannot do so without the Foundation's cooperation. A farmer who loses their phone can recover their DID via the agent plus the Foundation, without either party gaining control of the DID.

The cooperative field agent as a recovery party is deliberate. They are the farmer's existing trusted local representative — the same person who co-signs harvest records. Recovery through them is a socially natural process, not a technical procedure that requires digital literacy the farmer may not have.

8.8 Limitations and open technical questions

The did:key method generates a DID from a key without on-chain registration. The DKG registration of the DID Document is what creates the on-chain anchor. If OriginTrail changes its terms or the DKG becomes unavailable, the anchor must be migrated to an alternative registry. This is a known dependency addressed by the Layer 4 redundancy plan described in Section 6.

OriginTrail DKG public queries incur small TRAC token costs. For occasional manual verification by a farmer or cooperative officer, costs are negligible (sub-cent range at current TRAC prices). For Foundation-operated automated monitoring, costs are covered from operating budget. If TRAC prices increase materially, query costs are a budget line item that must be tracked.

W3C Verifiable Credential wallet interoperability across different implementations remains inconsistent in 2026. The SADT uses JSON-LD serialization with the VC Data Model 2.0 specification. Cross-wallet portability — a farmer exporting their VC collection from the Telegram wallet to a different wallet app — should be technically possible under the standard but is not guaranteed to be seamless across all wallet implementations. Wallet portability testing is included in the pilot evaluation plan.

The Telegram Mini-App wallet stores private keys within Telegram's infrastructure. Telegram is a centralised service. For the pilot, this is an acceptable convenience trade-off: the farmer population is already Telegram users, enrollment friction is minimised, and the pilot's primary purpose is operational proof-of-concept rather than full decentralisation. The long-term architecture roadmap includes migration to a device-native wallet (Android/iOS Wallet VC integration) that removes the Telegram dependency for key custody.

8.9 On-chain dispute filing and the evidence package

A farmer's right to revoke a Consent Agreement VC is described in Section 9. But revocation is an exit, not a remedy. A farmer who believes their Confidence Score was calculated on incorrect data, that a query was run without valid consent, that a cooperative agent co-signed records inaccurately, or that a vendor failed to deliver agreed attribution terms needs more than the ability to leave the system. They need a structured path to challenge a specific act and receive a binding determination.

The SADT provides this through a standardised on-chain dispute filing. A farmer or their cooperative initiates a dispute by submitting a Dispute Record VC, signed with their DID, to the OriginTrail DKG. The Dispute Record references the specific Knowledge Asset, Read Receipt, or Consent Agreement VC being contested, states the nature of the dispute in one of four defined categories, and attaches supporting evidence as IPFS-hosted documents linked by CID.

Dispute category	Typical grounds	Evidence the farmer can attach	Routing
Score dispute	Confidence Score calculated on sensor data the farmer believes was faulty, missing, or tampered with	Sensor diagnostics log CID; cooperative agent statement; alternative yield evidence	Farmer Data Ombudsman (Tier 1)

Consent violation	Query run without a valid Consent Agreement VC, or query type not covered by the farmer's Algorithmic Consent scope	Read Receipt VC; Consent Agreement VC (or absence thereof); DKG query log	Farmer Data Ombudsman (Tier 1)
Agent conduct	Cooperative field agent co-signed incorrect harvest data, or disclosed farmer records outside their authorised role	Session CID; co-signature record; farmer's conflicting evidence	Farmer Data Ombudsman (Tier 1), with right of appeal to Foundation board
Vendor non-delivery	Vendor failed to deliver attribution terms agreed in a Consent Agreement VC after successful queries	Consent Agreement VC; Read Receipt VCs confirming queries ran; evidence of non-payment or non-delivery	Formal arbitration — SIAC (Singapore-seated) or VIAC (Vietnam-seated), cooperative acting as farmer's representative

The Foundation's role in disputes is strictly evidentiary. When a Dispute Record VC is filed, the Foundation produces an Evidence Package: a compiled, certified export of all on-chain records relevant to the dispute — the relevant Knowledge Assets, Read Receipts, Consent Agreement VCs, Session Root CIDs, algorithm hashes, and access control logs — presented in a human-readable format alongside the raw chain references. The Foundation does not interpret this evidence, does not recommend an outcome, and does not participate in the adjudication. It produces the record and delivers it to the relevant dispute body within 5 business days of a valid dispute filing.

The Foundation is the record keeper, not the judge:

This separation is structural, not just procedural. A foundation that adjudicates disputes between parties it serves has an inherent conflict of interest — particularly when one of the parties is a high-value commercial vendor whose access fees fund the Foundation's operations. The Foundation's evidentiary role gives it neither the incentive nor the authority to influence outcomes. The adjudicating bodies — the Farmer Data Ombudsman for Tier 1 disputes, SIAC/VIAC for Tier 2 — are independent of the Foundation and cannot be instructed by it.

SECTION 9. THE DATA MARKETPLACE AND COOPERATIVE NEGOTIATION LAYER

9.1 The demand-pull problem and why it inverts farmer agency

The consent model described in Section 7 is a standing-permission structure: the farmer pre-authorises a category of query for a season (harvest verification, soil quality assessment), and any firm with SADT marketplace access can initiate that query class against their data. The farmer's participation in the transaction is largely retrospective — they see who ran a query after it happens, via Read Receipts.

This model works for commodity verification — where the same standardised question is asked by many parties and the farmer has no particular preference between them. It does not work when the farmer's data has differentiated value to specific buyers, when the terms of access matter (not just whether access is granted), or when vendors want to approach farmers with solutions, services, or commercial offers in exchange for data rights. In those cases, the standing-permission model is still a demand-pull architecture: external actors initiate, farmers react. The farmer's claimed status as 'author' of their data is undermined by the fact that they have no active voice in how that authorship is marketed or traded.

The Data Marketplace and Cooperative Negotiation Layer resolves this by inverting the flow. Vendors post structured offers on the SADT marketplace. Cooperatives evaluate those offers on behalf of their members. Farmers browse, deliberate, and negotiate before any consent is granted. Access to a specific farmer's data requires a vendor-specific, bilaterally signed Consent Agreement — not a standing seasonal permission. The farmer is no longer a passive subject of queries; they are a party to a negotiated transaction.

9.2 Tiered vendor registry: solution providers first

Not all vendors are equal in purpose or in the risk they pose to farmers. The SADT maintains a tiered vendor registry that determines who can post Data Request Offers, under what conditions, and at what access cost. The tiers are designed to privilege vendors whose primary offer is agronomic or practical value to the farmer — solution providers — over vendors whose primary interest is financial extraction from verified farm data.

Tier	Who qualifies	Posting rights	Access fee	Additional conditions
1 - Solution Providers	Agronomists, input suppliers, extension services, cooperative input programmes, seed companies, equipment providers, farmer advisory NGOs	Whitelisted by default on Foundation approval. Can post DROs immediately. Prioritised in the cooperative matching engine.	Lowest tier — subsidised from Foundation operating budget to lower barrier to entry	Must offer primary value in agronomic, input, or advisory form. DROs must specify the farmer-facing deliverable before any data access is granted. Cannot monetise Confidence Scores downstream.
2 - Financial Intermediaries	Trade finance providers, commodity buyers, insurers, credit scoring firms, impact investors requiring verified output data	Approved individually by Foundation vendor review. Subject to additional Co-operative Clause conditions. 30-day minimum review period.	Standard tier — cost-recovery pricing	Must demonstrate that farmer attribution terms are proportionate to commercial value extracted. Read Receipt audit mandatory for first two seasons. Escalating obligations if query volume exceeds 50/season.

3 - Research & Academic	Universities, CGIAR centres, government research institutes, development finance impact teams	Approved under a separate non-commercial track. IRB-equivalent review by Foundation academic advisory panel.	Nominal fee or waived for verified non-commercial research	Data may not be used for commercial purposes without reclassification to Tier 2. Outputs must acknowledge SADT and cooperative data sources. Results shared back with cooperatives.
-------------------------	---	--	--	---

The tier structure reflects a deliberate design choice about who the SADT marketplace primarily serves. An agronomist who posts a DRO offering personalised soil input recommendations in exchange for verified NPK baseline data is delivering value to the farmer first — the data access is the means, not the end. A commodity trading house posting a DRO to verify harvest quality for trade finance purposes is delivering value to itself first — the price premium to the farmer is the consideration, not the primary product. Both are legitimate, but they are not equivalent, and the marketplace should not treat them as if they were.

Tier 1 priority in the cooperative matching engine means that when a cooperative's dashboard receives new DROs, solution provider offers are presented first, with a clear visual distinction from financial intermediary offers. This is not exclusionary — Tier 2 offers are visible and can be accepted — but it sets a default ordering that reflects the SADT's foundational commitment to farmer benefit before market efficiency.

9.3 Data Request Offers (DROs): the vendor posting layer

A Data Request Offer (DRO) is the structured object through which a vendor expresses what they want, what they are offering, and under what terms. Vendors registered with the SADT Foundation can post DROs to the marketplace. Each DRO is registered as a Knowledge Asset on the OriginTrail DKG under the vendor's DID, making it tamper-evident and publicly auditable from the moment of posting.

A DRO must contain the following mandatory fields:

DRO Field	Description	Example
dataRequest.queryTypes	The specific CtD algorithm types the vendor wants to run, by registered Algorithm Registry ID	HarvestVerification_v2, SoilNPK_Baseline
dataRequest.duration	The period for which access is requested	2026 wet season (May–September)
dataRequest.targetGeography	The district or cooperative scope of the offer	Cái Bè district, Tiền Giang province
offer.valueType	The type of value the vendor is offering in return	CashPayment / InputDiscount / PremiumPricing / ServiceCredit / ResearchCredit
offer.valueTerms	Specific, quantified terms of the offer	5% price premium on verified Grade-A rice, paid at point of sale
offer.triggerCondition	What event triggers payment/delivery of the offer	On successful CtD query returning Confidence ≥ 0.85
vendor.purpose	Stated commercial purpose for the data	Trade finance underwriting for wet-season rice export

vendor.algorithmHash	Cryptographic hash of the algorithm Docker image to be run	sha256:4f3a...
vendor.registeredDID	Vendor's SADT-registered DID, verified against the Foundation's vendor registry	did:key:z6Mk...
offer.expiryDate	Date after which the DRO lapses if not accepted	2026-04-15

DROs without complete mandatory fields are rejected by the Foundation's access control layer and are not published to the marketplace. This prevents vendors from posting vague or asymmetric offers that obscure unfavourable terms.

What vendors cannot post:

DROs may not request raw data (sensor logs, photographs, biometric tokens) — only approved CtD algorithm types from the Algorithm Registry. DROs may not request perpetual or transferable data rights — all access is time-bounded and non-transferable. DROs may not specify exclusivity terms that would prevent the farmer from accepting offers from other vendors. Any DRO violating these constraints is automatically rejected at the access control layer; the violation is logged against the vendor's DID.

9.4 Cooperative evaluation and the advisory role

When a DRO is posted that matches the geographic or crop-type profile of a cooperative's membership, the Foundation's matching engine notifies the cooperative's Technical Officer via the cooperative dashboard. The cooperative does not make the decision on behalf of farmers — individual farmer consent is always required for access. But the cooperative's role is to evaluate the DRO before farmers see it, filter out predatory or poorly structured offers, and equip their members to make an informed decision.

The Foundation provides cooperatives with a standardised DRO Evaluation Toolkit containing:

- A comparables report: what similar DROs have offered in the same district, so the cooperative can assess whether the offer is above or below market
- An algorithm disclosure summary: a plain-language description of what the requested algorithm actually does, what data it accesses, and what information it infers — translated from the technical Algorithm Registry entry
- A red-flag checklist: automatic flags for DROs with unusually short payment trigger windows, unusually broad query scope, purpose statements that are vague or inconsistent with the algorithm type, or vendors with prior Co-operative Clause violations
- A counter-offer template: pre-structured terms the cooperative can propose back to the vendor if the offer is worth engaging with but needs modification

The cooperative Technical Officer produces a one-page DRO summary for their membership — in the local language, using the cooperative's communication channel (village meetings, Telegram group, or posted notices). Farmers receive the DRO summary, the cooperative's assessment, and their individual opt-in interface, typically with a minimum deliberation window of 7 days before the opt-in closes.

9.5 The farmer opt-in and negotiation interface

A farmer seeing a DRO summary in the Telegram interface has four options: Accept the offer as posted. Decline individually (their data is excluded from any consent agreement with that vendor, even if other cooperative members accept). Counter-propose modified terms (e.g., a higher premium, a shorter access duration, or an additional trigger condition). Hold for collective negotiation (flag to the cooperative that they want the cooperative to negotiate on their behalf as a group before individual decisions are made).

The collective negotiation path is the most powerful mechanism for farmers with small individual datasets but significant aggregate value. A cooperative of 200 farmers controlling verified jasmine rice data for an entire district holds substantially more leverage over a trading house than any individual farmer does. The DRO architecture enables this leverage by allowing cooperatives to aggregate individual opt-in signals and present a unified counter-offer: ‘180 of our 200 members will accept at 7% premium, not 5%.’ The vendor can accept the collective counter, decline it, or counter again. All exchanges are logged on-chain under both the vendor’s and the cooperative’s DIDs.

9.6 Vendor-specific Consent Agreement VCs

When a farmer accepts a DRO — either as posted or following negotiation — the SADT issues a Consent Agreement Verifiable Credential. This is structurally different from the standing Algorithmic Consent described in Section 7. Algorithmic Consent is a farmer’s standing permission for a query category (any approved vendor can run harvest verification queries this season). A Consent Agreement VC is a bilaterally signed, vendor-specific, terms-specific contract: this farmer consents to this vendor running this algorithm, for this duration, in exchange for these terms.

The Consent Agreement VC is signed by both the farmer’s DID and the vendor’s SADT-registered DID, and countersigned by the SADT Foundation’s DID as witness. Its structure:

```
{ "type": ["VerifiableCredential", "SADTConsentAgreement"],
  "issuer": "did:key:[SADT Foundation DID]",
  "credentialSubject": {
    "farmer": "did:key:[farmer DID]",
    "vendor": "did:key:[vendor DID]",
    "permittedAlgorithms": ["HarvestVerification_v2"],
    "accessWindow": { "start": "2026-05-01", "end": "2026-09-30" },
    "agreedTerms": { "valueType": "PremiumPricing",
      "value": "7% above district spot rate",
      "triggerCondition": "Confidence >= 0.85" },
    "exclusivity": false,
    "transferable": false,
    "revocableByFarmer": true
  },
  "proof": {
    "farmer": { "type": "Ed25519Signature2020", ... },
    "vendor": { "type": "Ed25519Signature2020", ... },
    "foundation": { "type": "Ed25519Signature2020", ... }
  }
}
```

The Consent Agreement VC is stored in the farmer’s wallet, on the vendor’s records, and anchored to the OriginTrail DKG. It is the sole authority for the vendor’s access. The Foundation’s access control layer checks for a valid,

unexpired, vendor-matched Consent Agreement VC before authorising any CtD job. A vendor without a valid VC for a specific farmer cannot run any query against that farmer's data, regardless of their broader SADT registration status.

9.7 Revocation and post-access accountability

A farmer can revoke a Consent Agreement VC at any time before its expiry by signing a revocation transaction with their DID. Revocation is immediate: the Foundation's access control layer updates within minutes, and the vendor loses the ability to initiate new CtD jobs. Queries already in progress at the time of revocation complete — the data integrity of in-flight compute jobs is not disrupted — but no further queries are authorised.

Revocation does not eliminate attribution obligations for queries already completed. If a vendor ran 10 successful queries before revocation, they still owe the agreed attribution for those 10 queries. The Read Receipts from those queries remain on-chain under the farmer's DID, providing the evidentiary basis for any attribution dispute. A vendor who fails to deliver agreed attribution terms after revocation can be escalated to the Foundation's arbitration process and, ultimately, have their vendor registration suspended.

A separate accountability boundary applies to the downstream use of historical score patterns. A single Confidence Score is a measurement of a harvest event. A vendor who accumulates multiple seasons of Confidence Scores for the same farmer and uses those patterns to build a creditworthiness model or behavioural inference is conducting their own analytical activity — profiling, in the data protection sense — and bears full responsibility under PDPA and PDPL for that activity. The SADT's accountability ends at the output of the approved CtD job. Vendors whose DROs indicate an intent to use historical score patterns for purposes beyond the stated query scope must declare this as a separate, explicitly scoped DRO for the pattern analysis use case, subject to Tier 2 review and additional Co-operative Clause conditions. A DRO that understates its analytical scope is a consent violation under Section 8.9.

9.8 Salespeople, field agents, and vendor outreach

Vendors are not limited to posting DROs on the marketplace platform. They can also approach cooperatives directly — through field agents, at cooperative meetings, or through introductions facilitated by the Foundation's vendor engagement team. The SADT marketplace structure accommodates this: a vendor who has verbally agreed preliminary terms with a cooperative can formalise those terms as a DRO and post it for individual farmer opt-in, with the cooperative's prior recommendation already noted in the DRO summary.

Vendor field agents registered with the SADT Foundation can attend cooperative meetings and present offers in person. Their attendance and any verbal commitments made are logged by the Cooperative Technical Officer via the cooperative dashboard — creating a record that can be compared to the formal DRO terms if discrepancies emerge. A vendor whose field agent verbally promises terms that the formal DRO does not reflect is flagged for a conduct review. This is important: the most common vector for predatory data acquisition in informal markets is a salesperson making promises that the contract does not deliver. The DRO structure makes that discrepancy detectable.

The cooperative as institutional memory:

One underappreciated function of the cooperative in this model is institutional memory. An individual farmer may not remember the terms they agreed to three seasons ago, or may not realise that the offer currently being pitched is worse than what they accepted previously. The cooperative's DRO history — archived on-chain under the cooperative's DID — provides a complete record of every offer ever made to their membership, every counter-proposal, and every agreed term. This gives cooperatives negotiating leverage that accumulates over time: a cooperative negotiating its third-season data agreement with a trading house has a full transaction history to reference, and the trading house knows it.

9.9 The implications for ‘farmer as author’

The current whitepaper claims that the SADT treats the farmer as the author and rights-holder of agricultural data. This claim is strengthened substantially by the marketplace and negotiation layer. Authorship implies more than the right to receive a read receipt after the fact. It implies the right to decide whether, to whom, and on what terms one's work is licensed — before access is granted, not after.

The DRO/Consent Agreement model operationalises this. A farmer who can browse vendor offers, deliberate with their cooperative, counter-propose terms, and grant or withhold vendor-specific access is genuinely exercising authorial agency over their data. The cooperative's advisory and negotiation role is the institutional equivalent of a literary agent or rights management organisation — it does not replace the author's decision, but it ensures the author is equipped to make that decision on informed and fair terms.

This also changes what the SADT's policy asks need to accomplish. The Algorithmic Consent sandbox permission described in the companion policy brief — which allows standing seasonal authorisation for query categories — remains appropriate for the commodity verification use case. But the marketplace and negotiation model requires a separate policy recognition: that a Consent Agreement VC, signed by both farmer and vendor DIDs and anchored on a public DKG, constitutes a legally binding data licensing agreement under Singapore and Vietnamese law. This is the fourth policy ask that the companion policy brief will need to reflect.

9.10 Integration with the existing layer stack

The marketplace layer sits logically between Layer 2 (Input Ingestion) and Layer 3 (Compute-to-Data). It does not replace any existing layer; it adds a pre-authorisation gate that CtD jobs must pass through. The access control layer in Layer 3 is extended to check for a valid Consent Agreement VC before spinning up a Docker container, in addition to the existing Algorithmic Consent check for non-marketplace queries.

Cooperatives already operating as Layer 2 nodes — hosting IPFS storage, managing co-signatures, monitoring the audit dashboard — take on the additional functions of DRO evaluation, farmer briefing, and negotiation facilitation without requiring separate infrastructure. The DRO interface and counter-offer tools are built into the existing cooperative dashboard. The Telegram farmer interface is extended with a DRO notification and opt-in flow.

The marketplace layer does introduce one new infrastructure requirement: a DRO matching engine that identifies relevant offers for each cooperative based on crop type, geography, and season. In the pilot, this runs as a Foundation-operated service. At scale, it can be implemented as a set of registered queries against the Ocean V4 marketplace metadata, using the same infrastructure already used for data discovery.

SECTION 10. THE ACADEMIC NODE: FEDERATED HISTORICAL DATA INTEGRATION

10.1 The historical integrity problem

A single verified harvest signal is useful. A signal cross-referenced against a decade of verified historical data from the same plot, and benchmarked against regional soil science research, is substantially more valuable — and substantially harder to fabricate. The SADT's Academic Node architecture enables this cross-referencing without either party — the farmer or the research institution — losing custody of their records.

10.2 Onboarding research institutions as Data Guardians

Research institutions such as NUS or the International Rice Research Institute (IRRI) register historical datasets on the Ocean V4 marketplace as Restricted Research Assets. They do not upload raw spreadsheets; they publish metadata describing the dataset's timeframe, GPS bounds, data parameters, and a CID pointing to their locally-hosted IPFS archive. The data remains physically on the institution's servers.

10.3 The federated blind join

When a commodity buyer or bank requests a Historical Integrity Check — asking whether a specific plot's current yield is consistent with the 10-year academic baseline — the SADT initiates a Multi-Node Compute-to-Data job. The fusion algorithm runs simultaneously across two independent containers: one on the cooperative's village gateway in Vietnam (accessing current farmer data) and one on the research institution's server in Singapore (accessing historical records). Neither container has access to the other's raw data.

The two containers exchange only intermediate aggregate statistics (not individual records) via an encrypted channel, and jointly compute a Lineage Confidence Score expressing how consistent the current harvest is with the historical baseline. This score is registered on the DKG as a Lineage Truth Unit, a higher-value attestation than a standard confidence score alone.

10.4 Institutional reciprocity

Under the Reciprocity Clause, research institutions whose historical data contributes to a commercial Lineage Truth Unit receive Read Receipts and attribution credit. This credit can fund further field research, subsidise data collection costs, or be converted to service offsets within the trust. This creates an incentive structure for institutions to maintain and expand their historical archives, benefiting the long-term accuracy of the SADT's signals.

SECTION 11. TRUST MODEL AND THREAT ANALYSIS

The SADT's value proposition is contingent on the integrity of its verification chain. This section analyses the primary threat vectors and the mitigations built into the architecture. Threats are categorised by the layer they target.

Threat	Layer	Severity	Mitigation
Sensor spoofing: farmer moves sensors between plots to inflate readings for one parcel	L1/L2	High	Decree 357 GPS polygon binding. Satellite NDVI cross-reference is independent of sensor position. A sensor reading inconsistent with satellite-observed canopy will depress, not inflate, the Confidence Score.
Fabricated logs: cooperative agent submits falsified harvest weights or co-signatures	L2	High	Co-signature requires VNeID Level 2 verification of the agent. Agent identity is on the record. Anomaly detection flags cooperatives with co-signatures inconsistent with satellite-observed yields. Repeated anomalies trigger a manual audit and potential suspension.
Malicious cooperative operator: node operator instruments Docker container to exfiltrate data before purge	L3	Medium	Hardware attestation at enrollment. Periodic remote configuration audit. Output distribution anomaly detection. Legal liability under Co-operative Clause. In practice, the marginal value to a cooperative of exfiltrating raw IoT logs is low; the primary threat is confidence score inflation, not data theft.
Confidence score inflation: operator manipulates container to return artificially high scores	L3	High	Algorithm hash is recorded in output and on-chain. Any modified algorithm produces a different hash. Satellite cross-reference is computed by the algorithm and visible in the output; a score inconsistent with satellite data is flagged. Foundation-operated benchmark nodes periodically re-run queries to verify output consistency.
Biometric replay: stolen VNeID token reused to authenticate for multiple sessions	L1	Medium	VNeID Level 2 liveness check requires real-time biometric confirmation; static tokens cannot be replayed. Sessions are timestamp-bound and single-use. The Ministry of Public Security's token infrastructure handles replay prevention.
Protocol failure: OriginTrail DKG becomes unavailable or changes terms	L4	Medium	Foundation-operated archive node mirrors all Knowledge Assets. UAL resolution falls back to Foundation mirror if OriginTrail is unavailable. Long-term: protocol diversity in Layer 4 is on the Architecture Review roadmap.
Connectivity failure: village gateway offline during harvest season	L2/L3	Medium–High	Addressed in Section 10 (Resilience Design). Gateway stores data locally indefinitely; CtD jobs can be queued and executed when connectivity returns. Partial harvest records (e.g., no IoT data for a period) reduce Confidence Score but do not invalidate the session.
Cooperative capture: cooperative management colluding with an external buyer to systematically favour one buyer's queries	L5	Low–Medium	SADT Foundation's Access Control Layer enforces query fairness; cooperatives cannot selectively suppress Read Receipts. Read Receipts are visible to all farmers in the cooperative, creating an accountability mechanism.

			Multi-stakeholder governance board includes farmer representatives with power to initiate investigations.
--	--	--	---

SECTION 12. RESILIENCE DESIGN: LOW-CONNECTIVITY AND FIELD CONDITIONS

12.1 The connectivity reality of rural Vietnam

The Mekong Delta is not uniformly well-connected. While 4G coverage is high in district towns, village-level connectivity is uneven and subject to outages during the wet season. A system that requires continuous internet connectivity to function is a system that will fail when it is most needed — at harvest, when transaction volumes and data generation are at their peak.

The SADT architecture is designed for intermittent connectivity. All critical operations — data ingestion, hashing, local storage, and session management — function fully offline. The gateway queues IPFS write operations and OriginTrail registrations locally when connectivity is unavailable and processes them in order when it is restored. The farmer's session and data integrity are unaffected by connectivity gaps.

12.2 Degraded-mode operation

The architecture defines a degraded-mode protocol for scenarios where connectivity is unavailable at the time a Compute-to-Data job is requested:

- The CtD job is queued in the gateway's local job manager with a requestor-specified timeout window.
- When connectivity is restored, the job executes as normal. The delay is logged in the Read Receipt with a connectivity-gap annotation.
- If the timeout window expires before connectivity is restored, the job fails and the requesting party is notified. Farmers are not penalised for connectivity failures outside their control — the Confidence Score calculation weights connectivity-gap annotations accordingly.

12.3 Sensor calibration and physical integrity

IoT sensors are subject to calibration drift, physical damage, and tampering. The SADT handles this through three mechanisms. First, sensors report a self-diagnostics payload alongside data readings; anomalous readings from a malfunctioning sensor trigger an automatic low-confidence flag on associated records. Second, the satellite cross-reference provides an independent check on extreme sensor readings — a soil moisture sensor reporting zero rainfall during a period when Sentinel-2 shows healthy crop growth is flagged for review. Third, the Cooperative Field Agent's annual gateway maintenance visit includes a physical sensor calibration check, logged as a maintenance co-signature on the session record.

12.4 Hardware supply chain

The pilot deploys commercially available IoT hardware (Dragino soil sensors, RAK Wireless LoRaWAN gateways) rather than proprietary devices, to avoid supply chain dependency on a single vendor and to ensure that replacements are available locally in Vietnam. Gateway software is open-source (IPFS Kubo, Docker CE, custom SADT middleware under Apache 2.0 licence) and can be maintained and updated by trained cooperative staff.

SECTION 13. FOUNDATION GOVERNANCE AND SUSTAINABILITY

13.1 Why a foundation structure

The SADT's architecture resolves most technical extraction risks. It does not, by itself, resolve institutional extraction risks: a commercially structured operator of the SADT infrastructure has an inherent incentive to monetise its position in ways that eventually disadvantage farmers. The only structure that can credibly commit to a non-extractive mandate over the long term is a foundation with a fiduciary obligation to its beneficiaries.

The SADT Foundation is proposed as a Singapore-incorporated Institution of a Public Character (IPC) with a statutory purpose defined as: to operate and maintain a non-custodial verification infrastructure for smallholder agricultural data in the ASEAN region, in the interests of the farming communities whose data it serves. The IPC structure subjects the foundation to oversight by the Commissioner of Charities and creates a legally binding fiduciary duty.

One risk specific to the foundation model requires explicit structural treatment: the Foundation legitimately accumulates a substantial metadata archive over time — Session Root CIDs, Read Receipt patterns, algorithm usage logs, cooperative throughput data, and DRO histories. None of this is raw farmer data; none of it is Confidence Score output. But it is data from which inferences could be drawn about farmers, cooperatives, and regional agricultural patterns. The Foundation's permitted uses of this aggregate metadata are therefore enumerated in the Foundation Charter and cannot be extended without a Board supermajority vote and public notification to all participating cooperatives. The enumerated uses are: operating and auditing the SADT infrastructure; producing anonymised aggregate statistics for governance reporting and academic research; and resolving disputes via the FDO evidence package process. The Foundation does not run predictive models on this metadata, does not sell or license it to third parties, and does not use it to make decisions about individual cooperatives' access to Foundation services.

13.2 Governance structure

The Foundation Board comprises seven members: two farmer cooperative representatives (elected by participating cooperatives, rotating every two years); two independent technical experts (appointed by the Board, subject to farmer representative approval); one representative from the SADT's primary academic partner (NUS or IRRI, rotating); one observer from MAS (non-voting); and one observer from Vietnam's MOIT (non-voting). The Board cannot approve changes to the Co-operative Clause, the data access policy, or the attribution payment schedule without approval by a supermajority of the cooperative representative seats.

13.3 Sustainability model

The Foundation's operating costs are covered by a tiered access fee structure charged to external firms. The fee schedule is:

Access tier	Query type	Fee (indicative)	Attribution split
Standard	Harvest verification (yield, quality, grade)	USD 0.50– 2.00 per query	60% Foundation operations, 30% Cooperative infrastructure, 10% Farmer attribution pool
Premium	Lineage Truth Unit (with historical academic node join)	USD 5.00–15.00 per query	50% Foundation operations, 25% Cooperative infrastructure, 15% Farmer attribution pool, 10% Academic institution

Bulk API	Automated seasonal monitoring (>100 queries/season per firm)	Negotiated annual licence	Same split ratios as Standard
----------	---	---------------------------	-------------------------------

The indicative fee levels are designed to be materially lower than the cost of physical audits (typically USD 50–500 per site visit) while generating sufficient revenue to sustain the Foundation’s node infrastructure, governance operations, and attribution payments. A full financial model for the Foundation is outside the scope of this paper but is available as a companion document.

13.4 The Co-operative Clause in detail

Every firm accessing SADT data under the sandbox framework must sign a Master Access Agreement containing the Co-operative Clause. The clause has three operative provisions:

7. Usage transparency: The firm’s query logs are made available to the SADT Foundation and, in anonymised aggregate form, to the relevant cooperative. The firm cannot suppress or modify these logs.
8. Attribution commitment: Once a firm has executed more than 20 verified queries against a specific cooperative’s data, it enters a value-establishment phase. Within 60 days of entering this phase, the firm must negotiate an attribution schedule with the cooperative, covering data royalties, input discounts, or equivalent forms of value return.
9. Escalation to the Foundation: If attribution negotiations fail, the Foundation’s arbitration process determines a binding attribution schedule based on the commercial value of the queries executed. Firms that refuse binding arbitration lose access.

Enforcement is structured to be practical. The Foundation does not enforce against foreign commodity buyers through litigation; it enforces through access revocation. Firms that want continued access to SADT signals — which are, by design, the most reliable and cost-efficient verification tool in the region — have a strong commercial incentive to comply.

13.5 The Farmer Data Ombudsman

The Farmer Data Ombudsman (FDO) is an independent dispute resolution body for Tier 1 disputes: Confidence Score challenges, consent violation claims, and cooperative agent conduct complaints. It is operationally separate from the SADT Foundation and cannot be instructed by it. The Foundation provides the FDO with evidence packages and implements its rulings — that is the full extent of the relationship.

The FDO is governed by a panel of five members: two farmer cooperative representatives drawn from the SADT’s cooperative membership (rotating annually, elected by cooperative vote); one independent data rights expert (appointed by the panel, subject to cooperative approval); one representative from a relevant civil society organisation operating in the agricultural sector; and one technical advisor with expertise in algorithmic systems and their fairness implications. The Foundation has no seat on the FDO panel and no voting rights.

The FDO operates a simple, low-barrier filing process. A farmer or their cooperative files a Dispute Record VC (described in Section 8.9). The FDO receives the Foundation’s evidence package and any additional submissions from the farmer, cooperative, or the party being complained about. It issues a written determination within 21 days for standard disputes, 10 days for urgent matters (where an ongoing query access is contested). Determinations are published in anonymised form on the FDO’s public record — on-chain, under the FDO’s DID — creating a body of precedent that informs future cooperative negotiations and Foundation policy.

The FDO’s remedies are proportionate to the dispute category. For score disputes, it can direct the Foundation to flag the contested session for re-evaluation and suspend the score’s use in active financial decisions pending resolution. For consent violations, it can direct immediate access revocation and a formal warning on the vendor’s registry.

record. For agent conduct complaints, it can recommend the cooperative's board review the agent's authorisation — the FDO does not have authority to dismiss cooperative employees, but its findings are admissible in any cooperative governance proceeding.

Why the FDO is not the Foundation:

A foundation that adjudicates disputes involving parties it serves — including high-value commercial vendors whose fees fund its operations — cannot be credibly neutral. The FDO's independence is structural: separate governance, separate funding (a dedicated levy on Tier 2 access fees), and no shared personnel with the Foundation. The Foundation's only role in the dispute process is to produce the on-chain evidence record accurately and completely. Its internal compliance obligation is to do so within 5 business days of any valid dispute filing, without omission or modification.

13.6 Farmer revocation rights: the full scope

Revocation in the SADT is not a single action but a spectrum of controls that a farmer can exercise at different levels of granularity. Understanding the full scope matters because farmers should be able to choose the least disruptive intervention for their situation, rather than facing a binary choice between full participation and complete exit.

Revocation type	What it does	Effect on active queries	Effect on attribution obligations	How to invoke
Consent Agreement VC revocation	Revokes a specific vendor's access to the farmer's data. Other vendors with valid Consent Agreements are unaffected.	Queries in progress complete; no new queries authorised for this vendor	Vendor still owes attribution for queries already completed under the agreement	Farmer signs revocation transaction with their DID via Telegram wallet
Algorithmic Consent suspension	Suspends standing seasonal consent for a defined query category. No vendor (including those without Consent Agreements) can run that query type against the farmer's data.	Queued jobs in that category are cancelled; running jobs complete	No effect on prior attribution obligations	Farmer updates consent settings via Telegram interface; logged on-chain under farmer DID
Cooperative data freeze	The cooperative suspends all external access to its data pool pending a governance review. Affects all farmers in the cooperative.	All queued and pending jobs suspended; running jobs complete	Foundation notifies all affected vendors; active Consent Agreements are paused, not terminated, pending review	Cooperative Technical Officer files freeze request via dashboard; requires FDO notification if dispute-related
Full DID deactivation	The farmer deactivates their DID entirely, terminating all active Consent Agreements and Algorithmic Consent authorities. The farmer's historical on-chain records remain (they are immutable)	All active queries suspended immediately	All pending attribution obligations survive — vendors owe amounts accrued before deactivation	Farmer initiates via wallet; cooperative agent must co-sign (threshold requirement prevents unilateral DID deactivation)

	but no new queries can be authorised.			from a compromised device)
--	---------------------------------------	--	--	----------------------------

The cooperative agent co-signature requirement for full DID deactivation is deliberate. It prevents a scenario where a compromised device or coerced farmer is used to unilaterally destroy a data history that the farmer might later want to recover. The cooperative agent acts as a circuit-breaker: they can confirm the farmer's intent, note concerns in the record, and in extreme cases refer the situation to the FDO before co-signing. This does not override the farmer's right to deactivate — a cooperative agent who refuses to co-sign a legitimate deactivation request is themselves subject to an FDO complaint — but it introduces a human checkpoint at the most consequential action available.

SECTION 14. COMPETITIVE AND ADJACENT LANDSCAPE

The SADT does not operate in a vacuum. Several platforms and infrastructure projects are operating in adjacent spaces, and a credible technical whitepaper must situate the SADT relative to them. This section identifies the primary categories of adjacent work and notes where SADT is differentiated, where it is complementary, and where it faces genuine competition.

Platform / Project	Focus	Relationship to SADT
Dimitra (DMTR)	AI-driven farm advisory platform; operates in VN, Africa, Pacific. Collects field data via mobile app.	Adjacent, not directly competitive. Dimitra focuses on advisory output; SADT focuses on verification and trade finance. Potential integration: Dimitra farmer records could be ingested as narrative logs into SADT sessions if privacy conditions are met.
AgUnity	Digital cooperative management for smallholders; operates in PNG, VN, Indonesia. Uses blockchain for cooperative records.	Complementary. AgUnity's cooperative registry infrastructure could serve as the identity layer for SADT cooperative onboarding. Active partnership conversation recommended.
Ricult	Credit scoring for smallholders in Thailand and Pakistan. Uses satellite and mobile data for loan underwriting.	Partially overlapping. Ricult's credit scoring model is centralised (data moves to Ricult's cloud) and does not include a data sovereignty mechanism. SADT's model is structurally different. Ricult operates as a lender; SADT operates as infrastructure. Not directly competitive.
GainForest	Satellite-based conservation finance and carbon credit verification.	Complementary. GainForest's satellite analysis methods are potentially usable as a CtD algorithm in the SADT's Layer 3 for carbon sequestration verification. Partnership opportunity.
Ocean Protocol	Decentralised data marketplace and Compute-to-Data infrastructure.	Foundational dependency. The SADT uses Ocean's CtD infrastructure. Ocean is not a competitor; it is a protocol layer. The SADT adds the identity anchor, governance, and banking signal translation that Ocean itself does not provide.
SGTraDex	Singapore government trade data exchange.	Layer 5 integration partner. SGTraDex provides the settlement and logistics data exchange rails that SADT signals feed into. Not competitive.
Agri3 Fund (UNEP/Rabobank)	Blended finance facility for deforestation-free agricultural supply chains in SE Asia.	Potential institutional customer. Agri3 requires supply chain verification at scale; SADT-verified signals could underpin Agri3 loan eligibility. Early engagement recommended.

The SADT's primary differentiator is the combination of biometric identity anchoring (via VNeID), non-custodial architecture, and banking-standard output (ISO 20022). No existing platform in the region offers all three. The risk is not competitive displacement; it is adoption speed — the SADT's policy dependencies mean it cannot scale until regulatory sandboxes are in place, giving centralised competitors a window to establish network effects.

SECTION 15. RISKS, MITIGATIONS, AND OPEN QUESTIONS

The following risk register identifies the material risks to the SADT's technical and operational success beyond the threat model covered in Section 9.

Risk	Probability	Impact	Current status / Mitigation
Decree 357 API access not granted before pilot launch	Medium	Critical	On critical path. MARD and MONRE engagement in progress. Fallback: manual land registry verification with Cooperative Field Agent, reducing automation but maintaining legal validity of provenance chain.
VNeID SDK not available for private integration before pilot	Low–Medium	Critical	VNeID Level 2 is available via approved government service providers. Engagement with Ministry of Public Security via MOIT channel is underway. Fallback: cooperative-held identity documents (citizen ID card) with agent co-signature as interim anchor. Lower anti-spoofing strength.
MAS does not recognise ISO 20022 SADT signals as MLETR-compliant in sandbox timeline	Medium	High	Policy brief submitted to MAS FinTech Office. Precedent from MAS's existing MLETR pilots (electronic bills of lading) is supportive. Fallback: signals used as supporting evidence for human underwriting decisions rather than automated release of trade finance.
LoRaWAN coverage insufficient in target Cai Be parcels	Low–Medium	Medium	Site survey planned for 2026 Q1. Fallback: NB-IoT or 4G-connected sensors for parcels outside LoRaWAN range. Higher operating cost but functionally equivalent.
Ocean Protocol V4 CtD infrastructure insufficiently stable for production deployment	Medium	Medium	Pilot will run Ocean CtD in a controlled environment with Foundation-operated fallback compute node. V4 mainnet stability is assessed during 2026 Q1 integration testing. If Ocean V4 is not stable, fallback to a Foundation-operated custom CtD implementation using standard Docker and IPFS.
Cooperative staff lack technical capacity to maintain gateway nodes	Medium	Medium	Training programme for Cooperative Technical Officers (CTOs) is built into pilot plan. Gateway software is designed for minimal maintenance. Remote monitoring allows Foundation technical staff to identify and resolve issues without on-site visits in most cases.
Farmer adoption below threshold for statistically meaningful pilot results	Medium	Medium	Target: minimum 300 farmers across 5 cooperatives. Adoption incentive: first-season participants receive guaranteed price premium on verified harvest via pre-committed trading house partner. Premium is funded from pilot budget, not ongoing model.

15.1 Open technical questions

The following questions are unresolved at the time of writing and will be addressed during the 2026 Q1 integration phase:

- Optimal NDVI fusion algorithm: The current algorithm uses a simple threshold model. A machine-learning approach trained on Mekong Delta rice data would likely produce higher accuracy but requires training data

that the pilot itself will help generate. The first season will use the threshold model; ML training begins in 2026 Q3.

- Cross-cooperative aggregation: The current architecture is designed for single-cooperative verification. Multi-cooperative aggregated signals (e.g., district-level verified yield for commodity pricing) require a federated aggregation protocol that preserves individual cooperative sovereignty. Architecture design for this is planned for 2026 Q4.
- Long-term IPFS pin management: Local IPFS nodes store data indefinitely by default, which creates storage cost growth over time. A data retention and archival policy — defining what data is retained locally, what is archived to distributed storage, and what is summarised and purged — needs to be formalised before the system scales beyond the pilot cohort.

SECTION 16. PILOT PLAN: VIETNAM–SINGAPORE 2026

16.1 Pilot objectives

The 2026 pilot has four measurable objectives: (1) demonstrate an end-to-end verified truth unit, from biometric harvest registration in Cai Be to trade finance release at a Singapore bank; (2) establish the technical baseline for Confidence Score accuracy against physical audit outcomes; (3) generate the Read Receipt and attribution payment data needed to demonstrate the viability of the Co-operative Clause; and (4) provide sufficient operational evidence for MAS and MOIT to evaluate the regulatory sandbox proposal.

16.2 Detailed milestone plan

Phase	Timeline	Deliverable	Owner	Dependency
Pre-pilot	June 2026	Secure MARD/MONRE API access agreement for Decree 357; confirm VNeID integration pathway with MPS	AgriG8 Policy	Critical path
Pre-pilot	August 2026	Site survey: LoRaWAN coverage mapping in Cai Be; gateway hardware procurement	AgriG8 Engineering	None
Pre-pilot	September 2026	Cooperative Technical Officer training programme (2-day, 5 cooperatives)	AgriG8 Field Ops	Cooperative onboarding agreements
Phase 1	November 2026	Deploy 5 village gateway nodes; install IoT sensors on pilot parcels; activate local IPFS nodes	AgriG8 Engineering	Hardware delivery, gateway power supply
Phase 1	Jan 2026	First live harvest session: VNeID + Decree 357 integration test with real farmers; Session Root CID generated	AgriG8 Engineering + Field Ops	API access
Phase 2	Feb–March 2027	First Compute-to-Data job: Sentinel-2 NDVI fusion with IoT logs; Confidence Score generated and validated against manual audit	AgriG8 Data Science	Ocean V4 stability confirmed
Phase 2	April 2027	ISO 20022 message constructed; Knowledge Asset registered on OriginTrail DKG; UAL issued	AgriG8 Engineering	DKG node operational
Phase 3	June 2027	Singapore bank counterparty reviews UAL-linked ISO 20022 message; trade finance released against verified harvest	Partner bank, AgriG8	MAS designation, sandbox MLETR recognition
Phase 3	Jul–Sep 2027	Full harvest season: 300+ farmers, 5+ cooperatives; Read Receipts generated; attribution payments processed as service offsets	AgriG8 Field Ops + Engineering	Phase 1 and 2 stability
Evaluation	Oct–Nov 2027	Independent accuracy audit: Confidence Score outcomes vs	Independent auditor (TBD)	Physical audit budget

		physical audit results on sample of 50 parcels		
Evaluation	Dec 2027	Pilot report: technical performance, policy findings, farmer economic outcomes, regulatory recommendations	AgriG8 + MAS + MOIT	All prior phases

16.3 Success criteria

The pilot is considered successful if it meets the following minimum criteria:

- Technical: ≥90% of Confidence Score outputs validated as accurate against independent physical audit (within one grade classification band).
- Adoption: ≥300 farmers complete at least one full harvest session with a valid Session Root CID and cooperative co-signature.
- Financial: ≥1 trade finance transaction completed by a Singapore bank against a SADT-issued ISO 20022 Knowledge Asset.
- Transparency: 100% of commercial CtD queries generating Read Receipts visible to the relevant cooperative within 24 hours of query execution.
- Policy: Sufficient evidence generated for MAS and MOIT to publish a formal regulatory sandbox determination by Q1 2027.

16.4 Budget overview

A detailed budget is available as a companion financial document. The indicative pilot budget envelope is USD 850,000–1,200,000, covering hardware procurement and deployment (USD 180,000), software integration and development (USD 240,000), field operations and cooperative training (USD 160,000), regulatory and legal engagement (USD 90,000), independent audit (USD 60,000), and contingency and project management (USD 120,000–470,000 depending on scope adjustments). The pilot is designed to be fundable as a blended finance arrangement: a combination of development finance institution grant (e.g., ADB Ventures, CGIAR), commercial co-investment from the participating bank and trading house, and AgriG8 equity contribution.

CLOSING NOTE

This document is a technical draft for review by implementation partners, protocol developers, and institutional co-investors. It will be revised as integration testing proceeds and as the regulatory landscape clarifies.

The architecture described here is not speculative. Each component — VNeID, LoRaWAN IoT, IPFS, Ocean Protocol CtD, OriginTrail DKG, ISO 20022, SGTraDex — is a deployed, production-grade technology. The novelty of the SADT is not in the components but in the specific combination: the biometric identity anchor that prevents spoofing, the non-custodial storage that preserves farmer sovereignty, the Compute-to-Data layer that allows verification without exposure, and the banking-standard output layer that makes the result usable by financial institutions.

The open questions are real but tractable. The regulatory dependencies are the most significant uncertainty. The companion policy brief addresses those in detail.

Prepared by Liyana Mahirah, AgriG8 · Technical draft v0.9, March 2026 · Confidential: not for public distribution ·
Contact: [contact@agrig8.com]

Team roles & descriptions

SINGAPORE–ASEAN DATA TRUST

Team Roles & Job Descriptions

AgriG8 · Confidential · March 2026

This document maps the full team required to bring the SADT from pre-pilot preparation through commercial launch. Roles are sequenced by hiring urgency. The Distributed Systems & P2P Architect and Vietnam Regulatory Engagement Lead are on the critical path for the 2026 pilot timeline. All other functional roles must be in place before commercial vendor onboarding begins.

ROLE OVERVIEW

Role	Engagement	Urgency
Executive Director & Founding Architect	Full-time — Founding Principal	FOUNDING ROLE
Distributed Systems & P2P Architect	Consultancy — part-time/fractional, view to full-time post-funding	PRIORITY HIRE
Lead UX Researcher & Systems Designer	Full-time or senior consultancy	PRIORITY HIRE
Vietnam Field Operations Lead	Full-time or senior consultancy	HIRE BEFORE PILOT LAUNCH
Regulatory & Legal Lead — Singapore	External counsel, Singapore-qualified law firm	ENGAGE BEFORE MAS SANDBOX
Vietnam Regulatory Engagement Lead	Senior advisory or consultancy, Vietnamese legal firm	CRITICAL PATH
Data Products & Commercial Partnerships Lead	Full-time or senior consultancy	HIRE FOR PILOT
Farmer Data Ombudsman	Independent panel appointment	INDEPENDENT APPOINTMENT
Foundation Chair — Inaugural Appointment	Non-executive; fixed 12-month term, annual Board reappointment vote	GOVERNANCE APPOINTMENT

0. Executive Director & Founding Architect

FOUNDING PRINCIPAL — ALL PHASES

FOUNDING ROLE — PRESENT ACROSS ALL STAGES

Engagement	Full-time — Founding Principal, SADT
Base	Singapore; required travel to Vietnam (Hanoi, Ho Chi Minh City, Mekong Delta) and regulatory engagements across ASEAN
Reports to	Foundation Board (jointly with Foundation Chair on governance matters)
Direct reports	Distributed Systems & P2P Architect · Vietnam Field Operations Lead · Data Products & Commercial Partnerships Lead
Phase	All phases — pre-pilot preparation through commercial operation

Why this role exists

The SADT is a novel technical and governance architecture with no direct precedent in the ASEAN agricultural data landscape. Its design requires a single principal who holds the full specification — technical, regulatory, commercial, and governance — simultaneously, and who is present at every consequential decision point from architecture sign-off through MAS sandbox engagement through cooperative field deployment. This role is not defined by a single functional lane. It is the integrating layer across all of them.

Core responsibilities

Governance Architecture

- Own and maintain the SADT constitutional framework — Foundation governance documents, Co-operative Clause, data access policy, attribution payment schedule, and Farmer Data Ombudsman mandate
- Chair the Foundation's Technical and Governance Committee (TGC), with casting-vote authority on policy changes, access tier decisions, and vendor onboarding approvals
- Hold veto authority over any modification to the five core policy positions in the MAS sandbox application
- Set the accountability boundary framework defining which decisions belong to each functional role and which require ED sign-off

Regulatory Strategy & Submissions

- Lead all MAS FinTech Office engagement — sandbox application strategy, five-ask positioning, and ongoing regulatory relationship management — with Singapore external counsel in a supporting brief role
- Direct Vietnam regulatory strategy: Decree 357 API access, MOIT sandbox framework participation, PDPL and Law on Data compliance positioning
- Final approval authority on all regulatory submissions, legal opinions, and policy positioning documents before external transmission
- Manage relationships with ADB, IFC, and development finance institutions at the institutional level

Technical Architecture Oversight

- Hold the authoritative specification of the SADT five-layer stack; sign off on all architectural deviations from the whitepaper specification
- Assess technical outputs from the Distributed Systems Architect against regulatory and governance requirements — not as a parallel engineer but as the accountable principal who specified the system

- Evaluate and approve or reject protocol dependency decisions, Layer 4 redundancy options, and vendor integration proposals on architecture-fit grounds
- Translate architecture decisions into regulatory language for MAS and MOIT technical reviewers

Cross-functional Coordination & Approvals

- Issue binding design briefs to each functional lead; receive execution updates; escalations from any lead require ED involvement only where the issue crosses remit boundaries or implicates regulatory exposure
- Approve all external-facing deliverables: vendor contracts, cooperative enrollment terms, DRO templates, regulatory evidence packages
- Maintain the Regulatory Exposure Matrix and direct its updates as sandbox conditions are defined

External Representation

- Primary spokesperson for the SADT architecture in investor, DFI, and regulatory contexts — with the Foundation Chair handling formal governance representation at Board level
- Lead commercial negotiations with Tier 2 vendor counterparties and institutional data consumers
- Represent AgriG8's interests to the Foundation while maintaining the governance architecture that keeps AgriG8's commercial interests structurally bounded

Authority and accountability boundaries

The following table defines what the ED owns and what sits with functional leads. Execution errors within a functional lead's defined remit are that lead's accountability. The ED is accountable for the design, policy, and governance decisions that set the terms within which functional leads operate.

ED authority	Functional lead accountability
Architecture specification and deviation approval	Technical implementation and delivery to spec
Regulatory strategy and submission sign-off	Execution of legal opinions and filing logistics
Governance policy and access rule changes	Operational compliance with approved policy
Vendor onboarding approval via TGC chair vote	Commercial negotiation within approved terms
Cooperative enrollment framework design	Field deployment and cooperative relationship management
Cross-jurisdictional regulatory positioning	In-jurisdiction regulatory relationship management

Essential qualifications

- Law degree or equivalent qualification; regulatory practice in financial services, fintech, or data governance in one or more ASEAN jurisdictions
- 10+ years across compliance, regulatory strategy, or product governance roles — with demonstrated experience translating legal and regulatory obligations into technical system requirements
- Technical literacy sufficient to engage directly with engineers, assess architecture decisions, and produce regulatory submissions that accurately reflect system design — formal computer science training is not required
- Cross-border regulatory experience in at least two of: Singapore (MAS), Vietnam (MOIT/MARD), Indonesia (OJK), or Thailand (SEC)

- Demonstrated experience managing regulatory relationships — not only producing compliance documentation but engaging regulators directly on novel or contested questions
- Southeast Asian language capability; Malay, Bahasa Indonesia, or Vietnamese an advantage

Desirable

- Prior involvement in agricultural data, rural finance, or cooperative governance in an ASEAN context
- Experience with MAS regulatory sandbox processes or equivalent innovation frameworks
- Background in distributed systems, blockchain infrastructure, or decentralised data governance — at a level sufficient to assess technical claims made by engineering counterparts
- Familiarity with development finance institution engagement (ADB, IFC, UNEP) and impact-oriented funding structures

The distinction between this role and the Foundation Chair is structural: the Chair holds non-executive governance authority and external credibility. The Executive Director runs the institution. As the SADT matures and operational leadership evolves, the governance framework provides for senior leadership to be considered for Board-level roles through the Foundation's standard appointment process.

1. Distributed Systems & P2P Architect

PRIORITY HIRE — NEEDED NOW

PRIORITY HIRE

Engagement	Consultancy — part-time or fractional, with view to full-time post-funding
Base	Remote; Singapore and Vietnam travel required
Reports to	Executive Director (Policy & Architecture)
Phase	Pre-pilot and Pilot (2026–2027)

Why this role exists

The SADT's technical architecture is specified but not yet built. The policy brief and whitepaper describe a five-layer stack — VNeID biometric anchoring, private IPFS local storage, Ocean Protocol Compute-to-Data, OriginTrail Decentralised Knowledge Graph, and ISO 20022 banking signal output — that requires someone who has deployed distributed systems in low-connectivity field conditions. This is the engagement that makes the architecture credible to technical reviewers at MAS, ADB, and integration partners.

Key responsibilities

- Own end-to-end architecture of the SADT five-layer stack from L1 identity through L5 settlement, translating the whitepaper specification into deployable components
- Lead integration of Ocean Protocol V4 Compute-to-Data with local IPFS nodes (Kubo v0.26+) running on village gateway hardware in rural Vietnam
- Implement Groth16 ZK-proof circuits for EUDR deforestation-free binary claims using snarkjs, including trusted setup ceremony and circuit audit
- Design and harden the Docker sandbox environment for CtD job execution, including container attestation, output-only exfiltration controls, and anomaly detection on score distributions
- Integrate W3C DID (did:key method) issuance, VC wallet (Telegram Mini-App), and OriginTrail DKG registration for farmer-sovereign traceability
- Spec and test the 2-of-3 threshold signature recovery scheme for farmer private key custody and loss recovery
- Design degraded-mode operation for intermittent LoRaWAN/4G connectivity in Mekong Delta field conditions
- Produce TRM-compliant vendor assessment documentation for MAS-regulated bank integration
- Translate architecture into regulatory language for MAS and MOIT technical reviewers, working directly with the ED
- Support evaluation and de-risking of OriginTrail DKG protocol dependency, including Layer 4 redundancy options

Essential qualifications

- Production experience with at least two of: IPFS/libp2p, Ocean Protocol, OriginTrail DKG, or comparable decentralised data infrastructure
- Working knowledge of ZK-proof systems — Groth16/snarkjs — beyond theoretical familiarity
- Experience deploying and maintaining distributed systems in low-resource or intermittent-connectivity environments

- Ability to produce technical documentation that serves engineering and regulatory audiences without requiring either to defer to the other

Desirable

- Prior work in agricultural data, supply chain traceability, or development finance contexts
- Familiarity with W3C DID/VC standards and self-sovereign identity systems
- Vietnamese language or prior Southeast Asia deployment experience
- Experience with MAS Technology Risk Management Guidelines or comparable regulated infrastructure requirements

The SADT's architecture uses established protocols in an unusual combination. The role requires the ability to distinguish between what is genuinely novel and what is engineering overhead — and to push back on over-engineering where a simpler solution serves the pilot better. Deep CS theory is not what this system needs; operational judgment is.

2. Vietnam Field Operations Lead

HIRE BEFORE PILOT LAUNCH — Q3 2026

HIRE BEFORE PILOT LAUNCH

Engagement	Full-time employment or senior consultancy
Base	Mekong Delta / Ho Chi Minh City; Hanoi travel for MARD/MOIT engagement
Reports to	Executive Director / SADT Foundation (dual reporting during pilot)
Phase	Pre-pilot preparation and full Pilot season (2026–2027)

Why this role exists

Pilot success is determined in Cái Bè. This role manages hardware deployment, cooperative relationships, farmer enrollment, and ground-truth reporting across 3–5 pilot cooperatives in Tiền Giang province. It is the connective layer between the technical architecture and the field conditions the architecture must actually operate in.

Key responsibilities

- Lead deployment of village gateway hardware across 3–5 pilot cooperatives in Cái Bè district — site surveys, hardware installation, LoRaWAN coverage testing, and power infrastructure
- Design and deliver the Cooperative Technical Officer training programme covering gateway maintenance, farmer onboarding, harvest co-signature process, and dashboard use
- Manage farmer enrollment: VNeID Level 2 authentication setup, DID issuance via Telegram Mini-App, and Decree 357 land parcel verification for each participating farmer
- Serve as primary relationship manager for pilot cooperative leadership — village meetings, adoption concerns, and ongoing trust between farmers and the SADT system
- Coordinate Cooperative Field Agent network for harvest co-signature and sensor calibration visits
- Manage provincial-level MARD/MONRE engagement for Decree 357 API access, in coordination with the Vietnam Regulatory Engagement Lead
- Produce Vietnamese-language farmer-facing materials: DRO summaries, Confidence Score explanations, Read Receipt dashboards
- Manage pilot logistics: hardware supply chain (Dragino sensors, RAK LoRaWAN gateways), local procurement, and cooperative infrastructure maintenance budget
- Feed ground-truth observations into pilot evaluation — what the architecture assumed versus what the field requires

Essential qualifications

- Fluent Vietnamese; professional English for reporting and Singapore-side coordination
- Existing relationships with agricultural cooperatives in the Mekong Delta, or demonstrated ability to build them within the required timeline
- Prior experience in agricultural development, rural technology deployment, or cooperative management in Vietnam
- Practical comfort with technology deployment — hardware configuration, sensor calibration, connectivity troubleshooting in low-resource environments

Desirable

- Familiarity with VNeID system and Vietnam's digital identity infrastructure
- Prior engagement with MARD, MOIT, or provincial agricultural departments
- Experience with IoT sensor deployment or precision agriculture programmes
- Understanding of Vietnam's rice export sector and cooperative governance under the 2023 Law on Cooperatives

3. Regulatory & Legal Lead — Singapore

ENGAGE BEFORE MAS SANDBOX APPLICATION

ENGAGE BEFORE MAS SANDBOX APPLICATION

Engagement	External counsel (Singapore-qualified law firm) with possible in-house conversion post-funding
Base	Singapore
Reports to	Executive Director / SADT Foundation Board
Phase	Regulatory preparation, sandbox application, and pilot evaluation period

Why this role exists

The SADT has five specific regulatory asks — Data Fiduciary recognition, Virtual Residency for CtD nodes, Algorithmic Consent, Consent Agreement VC recognition, and cooperative arbitration standing — that require a Singapore-qualified lawyer with active MAS FinTech Office relationships. The EU AI Act conformity gap for the Confidence Score system and the MLETR recognition pathway both require legal opinions before pilot launch.

Key responsibilities

- Lead the MAS regulatory sandbox application — drafting, submission, and ongoing MAS FinTech Office engagement across the five policy asks in the SADT Policy Brief
- Obtain formal legal opinions on: SADT ISO 20022 signal qualification as MLETR-compliant transferable record; DID-anchored Consent Agreement VC standing as binding electronic contract under ETA; EUDR use case exposure under EU AI Act; Law on Data intermediary registration requirements
- Advise on IPC foundation registration with the Commissioner of Charities — constitutional documents, conflict of interest policy, board composition, and governance requirements
- Manage Singapore-side data protection compliance: PDPA consent framework, IMDA TDSF alignment, PDPC AI governance guidelines application to the Confidence Score system
- Draft and negotiate the Master Access Agreement and Co-operative Clause for external firm access
- Advise on Payment Services Act licensing timeline and structure for post-pilot cash attribution settlement
- Coordinate with Vietnam legal counsel on cross-border data flow analysis — status of ISO 20022 confidence scores under Decree 13 and the Law on Data
- Produce Regulatory Exposure Matrix updates as the sandbox framework is defined and new obligations emerge

Essential qualifications

- Singapore-qualified lawyer with practice in financial services regulation, fintech, or data governance
- Active working relationship with MAS FinTech Office or demonstrated experience in MAS regulatory sandbox engagements
- Familiarity with PDPA, Electronic Transactions Act (MLETR), and Singapore's benchmark and financial instrument regulatory frameworks
- Ability to produce legal opinions that are technically grounded — the SADT's regulatory questions are architecture-contingent, not generic compliance queries

Desirable

- Prior experience advising on cross-border data infrastructure, data trust structures, or agricultural finance
- Working knowledge of EU AI Act, GDPR, and EUDR compliance frameworks
- Familiarity with Vietnam's legal system or prior Singapore-Vietnam corridor regulatory work
- Understanding of DID/VC technical standards sufficient to assess electronic contract recognition arguments

4. Vietnam Regulatory Engagement Lead

CRITICAL PATH — PARALLEL WITH SINGAPORE

CRITICAL PATH

Engagement	Senior advisory or consultancy; Vietnamese legal firm with MARD/MOIT relationships
Base	Hanoi, with Ho Chi Minh City presence
Reports to	SADT Foundation / Executive Director
Phase	Pre-pilot (Decree 357 API access) through pilot and sandbox evaluation

Why this role exists

Decree 357 API access is on the critical path. Without it, the biometric anchor that makes SADT's provenance chain verifiable does not exist at pilot launch. This requires a Vietnamese advisor with existing MARD and MONRE relationships, knowledge of how G2G and semi-public data sharing agreements are structured under Vietnamese administrative law, and the capacity to work within a bureaucratic timeline that does not respond to urgency applied from Singapore.

Key responsibilities

- Lead MARD and MONRE engagement for Decree 357 Digital Property ID API access — MOU drafting, approvals process navigation, and ongoing relationship management
- Advise on Ministry of Public Security engagement for VNeID SDK private integration and contractual confirmation required for biometric data handling compliance
- Guide MOIT engagement for the joint MAS-MOIT sandbox framework — Vietnamese regulatory framing, PDPL and Law on Data compliance positioning, and MOIPT cross-border data flow approval pathway
- Advise on Law on Cooperatives (2023) provisions relevant to cooperative legal standing in data rights arbitration
- Manage CheckVN traceability system interoperability assessment with MARD
- Advise on DID-based Ed25519 signature compatibility with Vietnamese e-signature requirements under the Law on E-Transactions (2023)
- Produce Vietnamese-language regulatory positioning documents for MARD and MOIT engagement
- Monitor successor legislation to Vietnam's National AI Strategy (Decision 127) and advise on implications for SADT Confidence Score classification

Essential qualifications

- Vietnamese-qualified legal advisor or senior government relations professional with demonstrated MARD/MONRE/MOIT access
- Working knowledge of Vietnam's data protection framework: Decree 13/2023, Law on Data (2024), Law on Cybersecurity (2018)
- Fluent Vietnamese and professional English
- Understanding of Vietnam's agricultural regulatory environment and export licensing framework

Desirable

- Prior work on digital identity, land registry, or agricultural data initiatives with Vietnamese government bodies
- Familiarity with Vietnam's digital economy framework and Singapore-Vietnam Digital Economy Agreement
- Experience with ADB, World Bank, or CGIAR-funded agricultural programmes in Vietnam that have navigated similar government data access questions

The Decree 357 API access timeline is the single largest risk to the pilot schedule. This engagement must begin before the MAS sandbox application is submitted.

5. Data Products & Commercial Partnerships Lead

HIRE FOR PILOT — Q4 2026

HIRE FOR PILOT

Engagement	Full-time or senior consultancy
Base	Singapore
Reports to	Executive Director / SADT Foundation
Phase	Late pre-pilot through post-pilot commercial launch

Why this role exists

The SADT's revenue model requires banks, commodity trading houses, insurers, and agronomists to purchase and integrate Confidence Score access. This role owns the product specification, commercial negotiation, and vendor marketplace design that makes that commercially viable. It is the interface between the SADT's data architecture and the procurement workflows of its institutional customers.

Key responsibilities

- Own the vendor marketplace design — DRO template standardisation, tier classification criteria, the comparables engine for cooperative DRO evaluation, and the red-flag checklist for predatory offer detection
- Lead commercial engagement with committed pilot counterparties: the Singapore bank for the first live trade finance Truth Unit, and the trading house partner providing pre-committed price premiums for early farmer adopters
- Design the Confidence Score product specification for financial institution use — signal contents, integration with existing trade finance workflows, MAS TRM-compliant vendor assessment package
- Develop the attribution payment schedule and service offset mechanics for the pilot phase, and design the post-pilot cash settlement pathway via SGTruDex
- Engage EUDR compliance buyers — EU importers requiring ZKP-based deforestation-free certification — as the SADT's most commercially differentiated use case
- Manage Agri3 Fund (UNEP/Rabobank) and comparable DFI-linked blended finance engagement as potential institutional customers
- Develop the tiered access fee schedule and financial sustainability model for Foundation operations
- Work with the Regulatory & Legal Lead on MAS ESGpedia alignment

Essential qualifications

- Track record in agricultural commodity trading, trade finance, agri-fintech, or structured agricultural finance
- Understanding of how banks and commodity trading houses handle quality verification and what would make a machine-readable confidence signal operationally useful to them
- Commercial negotiation experience — this role closes engagements, not only scopes them
- Ability to operate across Singapore financial institution and Vietnamese cooperative contexts without requiring institutional translation

Desirable

- Familiarity with EUDR compliance requirements and the existing compliance platform landscape
- Understanding of SGTraDex and Singapore's trade data exchange infrastructure
- Prior work with DFI agricultural finance programmes (ADB, IFC, Agri3)
- Knowledge of ISO 20022 financial messaging standards and trade finance letter of credit workflows

6. Farmer Data Ombudsman

INDEPENDENT APPOINTMENT — BEFORE COMMERCIAL OPERATION

INDEPENDENT APPOINTMENT

Engagement	Independent panel appointment — not an employee of AgriG8 or the SADT Foundation
Base	Singapore or Vietnam; accessible to both
Appointed by	Multi-stakeholder FDO panel per Foundation governance documents
Funded by	2% levy on Tier 2 vendor access fees — separate from Foundation operating budget
Phase	Before commercial vendor onboarding through full operation

Why this role exists

The FDO's independence is structural. A Foundation that adjudicates disputes involving high-value commercial vendors whose fees fund its operations cannot be credibly neutral. The FDO exists because the SADT's design acknowledges this conflict. The appointment must precede commercial vendor onboarding — its existence at launch is itself a governance signal.

Key responsibilities

- Adjudicate Tier 1 disputes filed by farmers or cooperatives: Confidence Score challenges, consent violation claims, and cooperative field agent conduct complaints
- Receive and review Foundation-produced evidence packages — compiled exports of on-chain records relevant to each dispute — within the 5 business day evidence production window
- Issue written determinations within 21 days for standard disputes and 10 days for urgent matters where active query access is contested
- Publish anonymised determinations on-chain under the FDO's DID, building a body of precedent that informs cooperative negotiation and Foundation policy
- Refer Tier 2 disputes (vendor non-delivery of attribution terms) to formal arbitration at SIAC or VIAC as appropriate, with cooperatives acting as farmer representatives
- Report annually to the Foundation Board on dispute patterns, systemic issues, and recommended policy changes
- Maintain operational and financial independence from the Foundation and AgriG8 at all times

Essential qualifications

- Background in dispute resolution, data rights, consumer protection, or agricultural development — ideally combining at least two of these
- Demonstrated independence from commercial agricultural interests and from the organisations founding the SADT
- Sufficient technical literacy to understand what a Confidence Score is, what a Consent Agreement VC contains, and what a Read Receipt records — without requiring foundational explanation in each dispute
- Credibility with both Vietnamese farming community representatives and Singapore regulatory observers

Desirable

- Prior experience as an ombudsman, arbitrator, or independent reviewer in a regulated sector
- Familiarity with SIAC or VIAC arbitration procedure
- Regional civil society or development finance credibility that signals genuine independence to MAS and MOIT

7. Foundation Chair — Inaugural Appointment

GOVERNANCE APPOINTMENT — PRE-IPC REGISTRATION

GOVERNANCE APPOINTMENT — FIXED TERM, ANNUAL REAPPOINTMENT

Engagement	Non-executive; governance and strategic leadership of the IPC Foundation
Base	Singapore-based preferred; regional travel required
Appointed by	Founding governance board per Commissioner of Charities requirements
Term	Initial appointment: 12 months from IPC registration. Renewable annually by Board vote (simple majority of non-conflicted directors). Maximum two consecutive terms before mandatory reappointment vote. No automatic rollover.
Phase	IPC registration through pilot evaluation; term reviewed at end of Year 1

Why this role exists

The Foundation Chair provides the institutional credibility and non-executive governance accountability required to establish the SADT Foundation as a credible neutral body during its inaugural phase. The Chair is the public accountability point for Foundation neutrality in engagements with MAS, MOIT, ADB, and IFC, and holds fiduciary accountability to the Commissioner of Charities independent of AgriG8's commercial interests. The role is structured as a founding appointment with a defined term framework, reflecting standard IPC governance practice and the Foundation's expectation that its leadership composition will evolve as the institution matures.

Term and reappointment structure

The Foundation's constitutional documents provide for the following appointment framework, consistent with Commissioner of Charities governance requirements for IPC foundations:

- Initial appointment is for a fixed 12-month term, commencing at the date of IPC registration
- Continuation beyond the initial term requires a positive Board vote at the annual governance review, held no later than 30 days before term expiry
- A maximum of two consecutive terms may be served before the position is opened to the full appointment process under the Foundation's governance documents
- There is no automatic rollover — the Board must act affirmatively to renew; inaction results in the position becoming vacant and triggering the open appointment process
- The annual governance review assesses the Chair's performance against the Foundation's mandate, regulatory relationship objectives, and DFI engagement targets for the preceding term
- Internal candidates, including senior Foundation and AgriG8 leadership, are eligible for consideration in any open Chair appointment process

Key responsibilities

- Lead the Foundation Board in discharging its fiduciary mandate to farmer and cooperative beneficiaries
- Represent the Foundation in senior regulatory engagements with MAS and Vietnam MOIT — external-facing governance accountability, distinct from the Executive Director's operational and regulatory strategy role
- Ensure Board governance satisfies Commissioner of Charities IPC requirements: conflict of interest management, reporting obligations, board composition

- Chair the supermajority votes required for changes to the Co-operative Clause, data access policy, and attribution payment schedule — exercising casting vote when the Board is deadlocked
- Serve as the external public accountability point for Foundation neutrality
- Engage DFI and impact investor communities to support Foundation sustainability and pilot funding

Essential qualifications

- Regional credibility and policy stature sufficient to signal genuine institutional seriousness to MAS, MOIT, ADB, and IFC
- Clean independence from commercial agricultural trading, commodity finance, and the founding organisations
- Governance experience in a regulated or charitable institutional context, including familiarity with IPC or equivalent foundation governance requirements
- Genuine commitment to the Foundation's beneficiary mandate
- Comfort operating within the structured term and annual performance review framework standard to IPC foundations

Profile note

The target profile is a retired central banker, former ADB or FAO senior official, or senior academic with ASEAN agricultural or digital economy policy credentials. The appointment should be made before IPC registration is submitted. The Commissioner of Charities will assess board composition as part of the application. Candidates should be briefed on the Foundation's term structure and succession framework at the outset of any appointment discussion.

On sequencing

The Distributed Systems & P2P Architect and Vietnam Regulatory Engagement Lead are the two engagements that unblock everything else. Both should begin before the MAS sandbox application is submitted — not after approval.

The Foundation Chair is a fixed-term inaugural appointment. The annual reappointment vote and two-term maximum are standard IPC governance practice and should be reflected in the Foundation's constitutional documents from registration. The Farmer Data Ombudsman must be appointed before the first commercial vendor is onboarded.

All roles marked as consultancy or external counsel during the pilot phase should have explicit scope-expansion provisions post-funding. These descriptions reflect full-capability requirements, not what a single person must deliver on day one.

8. Lead UX Researcher & Systems Designer

PRIORITY HIRE — PILOT PREPARATION

Engagement	Full-time or senior consultancy
Base	Singapore; frequent travel
Reports to	Executive Director & Founding Architect
Phase	Pre-pilot through commercial operation

Why this role exists

The SADT's success is contingent upon the reduction of cognitive friction between a sophisticated five-layer distributed architecture and the operational reality of low-literacy, low-tech environments. While the technical stack is robust, the "last mile" of farmer participation and cooperative negotiation requires a translation layer that converts abstract cryptographic proofs into legible economic agency.

This role exists to ensure that the SADT does not become a "mediated dashboard" where farmers are passive subjects, but rather an active interface for authorial agency. The Lead UX Researcher & Systems Designer will bridge the gap between B2B SaaS complexity (for banks and buyers) and hyper-local mobile utility (for farmers), ensuring the system remains intuitive even for users with limited digital literacy.

Key responsibilities

- **Systemic Legibility Design:** Translate the five-layer technical stack—specifically VNeID authentication, "Read Receipts," and "ISO 20022" signals—into a unified, intuitive Telegram Mini-App for farmers and a high-throughput dashboard for cooperatives.
- **Human-Centric Research:** Conduct deep-field ethnographic research in the Mekong Delta to map the mental models of smallholders and cooperative agents, identifying friction points in harvest co-signatures and DID-based key recovery.
- **DRO Marketplace Interface:** Design the structured "Data Request Offer" (DRO) summary and counter-offer interface, ensuring that predatory terms are visually flagged and that farmers can exercise their "authorship rights" with a single tap.
- **Prototyping & AI Integration:** Rapidly develop and iterate high-fidelity system prototypes in Figma, utilizing AI-assisted design tools to simulate low-connectivity and degraded-mode UI states.
- **Cognitive Load Reduction:** Engineer the "Confidence Score" breakdown to ensure it functions as a transparent measurement rather than an opaque inference, allowing farmers to independently audit and dispute their own data signals.
- **Applied Leadership:** Define the UX governance framework, setting the standards for how solution providers (Tier 1) and financial intermediaries (Tier 2) present offers to the cooperative matching engine.

Essential qualifications

- **Hybrid Technical-Design Background:** Degree in Computer Science, HCI, or a related field; prior experience as a software engineer is mandatory to ensure the designer understands the underlying P2P and cryptographic constraints.
- **Dual-Sector Expertise:** Demonstrated track record in designing both complex B2B SaaS platforms and high-scale, consumer-facing mobile applications.

- **Research Leadership:** 8+ years of experience in applied UX research, with a focus on systems-level design rather than purely aesthetic UI; experience in "Scandinavian-style" human-centric systems design is highly preferred.
- **Tooling Mastery:** Advanced proficiency in Figma and AI-driven design workflows; ability to move from research insights to functional prototypes with brutal corporate efficiency.
- **Low-Literacy Contexts:** Prior experience designing for emerging markets or users with varying levels of digital literacy (e.g., agricultural, financial, or industrial "last mile" workers).

Desirable

- **Regional Experience:** Familiarity with Southeast Asian digital ecosystems, particularly the use of Telegram for commerce and government services (e.g., VNeID-adjacent apps).
- **Fiduciary Design:** Understanding of "Data Trust" or "Data Fiduciary" concepts and how to design for neutral, non-extractive institutional mandates.
- **Multi-Modal Communication:** Experience designing interfaces that utilize voice notes, iconography, and local language localization to replace dense text-based workflows.

Tab 5

