Annex A

Technical Architecture & Verified Results

Document: *GS-ORILIFE-GA-01 · Annex A*
Version: *v6.1*
Updated*: April 2026*
IP Disclaimer: *Architecture described at feasibility-evaluation level. Core technologies protected by 4 USPTO PPAs. Open-source components at https://github.com/OriLifeTrace.*

Table of Content

1. From TonFarm to OriLife

Why DDC Failed — and What Was Learned

TonFarm (2024) deployed dozens of staff across Dak Lak farms: manually attaching QR codes, photographing trees, recording GPS, uploading to a single server, and hashing each fruit as a separate on-chain transaction. Verifiable on-chain: TON blockchain NFT collection.

Five failures DDC experienced directly:

Weakness	Real-world consequence
QR labels detachable	Peeled and re-attached — zero anti-fraud. Exactly the 2025 scandal
Single server	Anyone with access could modify data; blockchain only anchored the hash
1 fruit = 1 tx	180M fruits = 180M transactions — impossible to scale
Farmer dependent on DDC staff	Staff leaves = data stops
Hash ≠ validation	Proves "data unchanged since hashing," not "data was correct"

Despite failures, DDC built irreplaceable assets: UX validated with farmers aged 50+ over 2 harvest seasons; relationships with the Farmers' Union and Extension Center across 46 communes; standardized onboarding; offline queue logic with zero data loss. Copyright Certificate No. 4420/2025/QTG confirms this is not a new project.

Architecture Comparison

Criterion	Legacy (TonFarm 2024)	OriLife on Cardano
Identity carrier	QR label — detachable	Fruit skin texture (Bio-ID) — inseparable
Data processing	Staff upload to central server	AI on-device → 80 bytes sent
Raw data storage	1 modifiable server	LampNet 100+ nodes, encrypted
Pre-chain validation	None	5-layer validation before anchoring
On-chain cost	1 fruit = 1 tx (linear)	15,000 fruits = 1 tx — O(1)

Scale to 180M fruits	180M tx — infeasible	~12,000 tx/harvest — $1,530 *(Note A)*
Consumer image access	Days (manual)	~5 seconds (Three-Layer Read Model)
Commercial privacy	Fully public	Midnight View Keys per party
User identity	Password, managed by DDC	PhoenixKey — biometric, self-sovereign

Note A: *~12,000 tx = theoretical floor (1 VeData anchor per farm per harvest season). In production, VeData runs weekly → ~600,000 anchor events/year → ~6,000–7,500 actual L1 batch transactions. Full ecosystem: ~1,200,000 L1 events/year across all activity types. See Section 6.*

The Alliance

- **DDC Holdings** — field operations and government relations. Brings institutional trust across 46 communes that no tech company can replicate quickly.
- **GreenSun Tech** — R&D and core IP. Holds 4 USPTO PPAs directly related to OriLife. Also deploying 1,000 EV charging stations with V-Green (VinFast) — proving capacity to operate physical infrastructure at scale.
- **Aladin Contract** — product development. Building Aladin App 2.0 (June 2026): Chat, Work, and Trace modules. Users join Cardano via fingerprint and face — no seed phrase.

Why Cardano: eUTXO enables O(1) batch cost. Midnight enables commercial privacy. Identus enables government-scale DID. No other blockchain simultaneously provides all three.

The Alliance has self-invested nearly $500,000 USD before this proposal.

2. System Architecture — Four Layers

Data flows **one direction only**: farm → blockchain.

Layer 1 — Edge (Farmer's phone): AI processes on-device. Signs data with PhoenixKey hardware key. Sends <1KB package. Works on 2G.

Layer 2 — LampNet (Distributed storage and compute): Photos, videos, logs encrypted and distributed across 100+ physical nodes in Vietnam. Available to consumers within seconds of upload — before any blockchain confirmation.

Layer 3 — VeData (Validation & aggregation): 5-layer validation. Aggregates thousands of records into one Merkle root. Operates two independent settlement paths (Section 5).

Layer 4 — Cardano Mainnet (Immutable evidence): Path A: direct L1 batch updates. Path B: Hydra audit decommits. Anyone can verify; no one can modify.

Three physical constraints resolved:

Constraint	Response
Rural 2G/3G	AI on-device; <1KB upload
GPS drift 5–20m under canopy	Local grid coordinates replace absolute GPS
Android 4GB RAM	Biometric compressed to 80 bytes on-device

3. Collection Layer

Smart Capture via Sensor Fusion: Accelerometer + compass integration triggers capture only when device is stable and object is identified. Eliminates blurry images; keeps upload under 1KB.

Automatic Harvest Capture: Phone sensors detect cutting motion → auto-capture + timestamp → linked to mother tree on-chain. No farmer action required. Triggers `PRIORITY_HIGH` in VeData pipeline — see Section 5 for latency impact.

Offline: SQLite local queue, auto-sync on reconnect. Validated over 2 harvest seasons in Dak Lak with zero data loss.

4. LampNet — Encrypted Distributed Storage

USPTO #64/031,472

About 100+ physical nodes in Vietnam. End-to-end encrypted. Content-addressed via `lamp://CID` — accessible globally within seconds of pinning. Only PhoenixKey owner can decrypt.

Why not Cardano for raw data: 180M fruits × 10 images × ~500KB ≈ 900TB. Blockchains store proofs, not raw data. LampNet stores data; Cardano stores the 32-byte Merkle root that proves data is authentic.

Data sovereignty: Cardano stores only 32-byte hash — no PII, no violation of Vietnam Cybersecurity Law 2018. LampNet nodes prioritized in Vietnam with on-chain Sovereign Data Residency Proof per Decision 1236/QĐ-TTg.

Try it: lampnet.cloud

5. VeData Mosaic — Validation, Aggregation & Settlement

USPTO #64/032,593 · Specification: GS-VEDATA-MOSAIC-SPEC-01 v1.5.0

Validation (5 layers)

Device origin → image authenticity → GPS vs registered farm boundary → temporal validity → biological plausibility. All 5 must pass. Any failure → data rejected → never reaches Cardano. This is what legacy TonFarm lacked: hashing bad data produces bad hashes.

Batch Aggregation — O(1) Cost

Each Farm NFT stores only a 32-byte Merkle root (Sparse Merkle Tree). Updating 50 of 150 trees recomputes ~700 nodes; the other 100 trees and 15,000 fruits cost zero recomputation. Result: 1 datum update on-chain regardless of how many entities changed. Datum size is permanently bounded at ≤580 bytes — never grows with record count.

Two-Path Settlement

```
Validated records from LampNet
    │
    ├── PATH A — NFT Datum Updates (direct L1)
    │   80–100 Farm NFTs per tx · every 20s or 100 NFTs
    │   PRIORITY_HIGH: bypass timeout, submit immediately
    │   Cost: ~8,900 lovelace per NFT (~0.0089 ADA)
    │
    └── PATH B — Audit Proof Trail (via Hydra)
        Accumulate off-chain · Decommit every 4–8 hours
        Cost: ~450,000 lovelace per decommit (~0.45 ADA)
        = ~2.70 ADA/day fixed for entire system
```

Farm NFTs never enter the Hydra Head. They stay on Cardano L1 at all times, updated only via Path A. Path A functions correctly regardless of Hydra status or version.

Three-Layer Read Model — Consumer Data Availability

Consumers see images within seconds. Blockchain confirmation comes later. These are independent.

Layer	Latency	Basis	UI

0 — Optimistic	3–7s	LampNet CID	🔵 Image available
1 — Pending	15–25s	VeData operator signature	🟡 Processing
2 — Confirmed	41–61s	Cardano L1 consensus	✅ Verified on Cardano

End-to-end: Farmer in Dak Lak → Consumer in Ha Noi

Event	Time
Farmer triggers harvest capture	T+0s
Image available on LampNet	T+3–7s → **Layer 0**
VeData validation + SMT root computed	T+15–25s → **Layer 1**
Path A tx confirmed on Cardano	T+41–61s → **Layer 2**
Consumer app auto-updates via push	T+42–62s

For `PRIORITY_HIGH` events (harvest, quality inspection): Layer 2 at **~25–35 seconds** by bypassing batch timeout.

SLA Tiers

Under normal conditions queue depth stays below 100 NFTs. During peak periods (harvest season), Mosaic signals queue state to consumer apps automatically:

Tier	Queue depth	Confirmation target	Consumer UI
Normal	<100	40–60s	"Verifying..."
Congested	100–500	2–5 min	"Confirming (~3 min)"
Overloaded	>500	5–15 min	"Confirming (up to 15 min)"

Images remain visible at Layer 0 regardless of tier — only confirmation latency changes.

Automated Push — CID Subscription API

WebSocket-based. Buyers, export enterprises, customs subscribe to Farm NFT IDs and receive:

- `cid_available` → image on LampNet
- `root_pending` → Merkle root queued

- `datum_confirmed` → TxHash + merkle_proof_cid on-chain
- `datum_failed` → auto-requeue notification

No polling. No manual intervention. GACC customs in China receives automatic proof packets at harvest capture in Dak Lak.

Update Frequency — Why Standard Batch

Strategy	Cadence	Used for
A — Standard Batch	1/hour–1/day	Farm logs, harvest events ← OriLife
B — Lazy Anchor	>1/minute	IoT sensors, solar panels (not in this GA)
C — Scheduled	<1/day	Annual audits

Farm updates occur ~weekly per farm — 20-second batch cycles are optimal. Consumer image availability (Layer 0, ~5s) is independent of batch cycle length. Mosaic v1.5.0 introduces Lazy Anchor (Strategy B) for ultra-high-frequency data sources — not used in the current GA, but positioned for future expansion to coffee and aquaculture traceability where sensor integration is planned.

Fee Calculation — Why 0.0089 ADA Per NFT

Single NFT update costs ~0.25–0.42 ADA. Batching 100 NFTs with a reference script (CIP-33):

Base fee: 155,381 lovelace

Size fee: 44 × ~15,300 bytes = 673,200 lovelace

Ref script fee: ~61,440 lovelace (validator ~4KB, Tier 0 ≤25,600 bytes)

Total: ~890,021 lovelace for 100 NFTs

Per NFT: ~8,900 lovelace (~0.0089 ADA) — 98% reduction

The reference script fee (`refScriptFee`) is incurred once per batch transaction and does not scale with batch size — making larger batches increasingly efficient per NFT. The Mosaic validator must remain below 25,600 bytes to stay in Tier 0; exceeding this causes non-linear fee growth.

6. Cardano — Immutable Evidence

eUTXO Advantages

Feature	Benefit
Deterministic execution	VeData pre-computes — no failed transactions, no wasted gas
Parallelism	12,000 farms update simultaneously, no UTXO contention
Native tokens	Farm NFT requires no separate token contract

Transaction Model — Three Figures Reconciled

1) **~12,000 tx** — *Minimum to record 180M fruit Bio-IDs (theoretical floor)*

Model	Transactions	Cost/fruit	Total
Legacy: 1 fruit = 1 tx	180,000,000	~$0.17	~$30,600,000
OriLife VeData batch	**~12,000**	**~$0.000009**	**~$1,530**
Reduction	15,000×	~19,000×	~20,000×

Legacy cost from TonFarm 2024 TON fees — verifiable at tonviewer.com.

2) **~600,000 events → ~6,000–7,500 L1 tx** — *VeData actual annual output*

VeData runs weekly per farm: 12,000 farms × ~50 cycles/year = ~600,000 anchor events. Each L1 batch covers 80–100 farms → **~6,000–7,500 actual L1 transactions from VeData alone**.

3) **~1,200,000 events/year** — *Total ecosystem footprint*

Activity	Path	Events/year	Per ha/year
VeData batch anchors	A — Direct L1	~600,000	~50
Labor contracts (farmer ↔ worker)	A — Direct L1	~300,000	~25
Commercial escrow (farmer ↔ trader)	A — Direct L1	~60,000	~17
One-time setup (DID, NFT minting)	A — Direct L1	~100,000	~8
Path B audit decommits	B — via Hydra	~2,190	fixed
Total		**~1,202,190**	**100/ha/year**

Labor contracts and commercial escrow are direct Plutus L1 transactions — they need independent enforceability, not just Merkle inclusion. DID registrations (24,000) are within the ~100,000 setup events. minADA locks (~75,000 ADA) are created within these setup transactions.

All three figures are accurate — they answer different questions.

① is the cost-floor.

② is VeData's actual cadence.

③ is the full ecosystem planning footprint.

M3 Demo vs M7 Threshold

"10,000 updates → 1 tx" (M3 demo) proves VeData batching. "≥100,000 on-chain tx" (M7 requirement) is the cumulative total across all four transaction types over 1–2 months — not a single batch.

Peak Load — M7

100,000 events ÷ 30 days ÷ 86,400s = **~0.039 events/second**. Peak burst ~0.12–0.20/s. Cardano capacity: ~10 tx/s. **OriLife peak = <2% of Cardano throughput.** No congestion risk.

ADA Locked

Location	ADA
minADA in 12,000 Farm NFTs	~24,000
minADA in 24,000 farmer wallets	~48,000
Commercial escrow	~3,000+
Total	**~75,000+**

Per NFT: coinsPerUTxOByte (4,310) × ~307 bytes ≈ 1.32 ADA × 12,000 = ~15,840 ADA minimum; ~24,000 accounts for optional datum fields. Returned to owners on NFT burn.

7. PhoenixKey — One Identity, Many Applications

USPTO #64/031,291

Architecture: PhoenixKey is built on Cardano's DID infrastructure (Identus/Atala PRISM standard), extending it with biometric hardware key management and seedless recovery. Identus handles W3C-compliant DID anchoring on Cardano; PhoenixKey adds the farmer-facing layer — fingerprint + face registration, hardware key generation, and app delegation — making the same DID standard usable by a farmer with no technical knowledge.

Problem solved: TonFarm and Aladin were separate accounts with separate identities. PhoenixKey creates one DID anchored on Cardano, recognized across all OriLife-integrated apps — one source of truth on-chain.

Capability	Detail
Registration	Fingerprint + face. No email, phone, or seed phrase
Hardware key	Lives in secure chip, never leaves device
App delegation	Apps receive scoped session keys; master key stays safe
Recovery	Face auth on new device → full wallet recovery
Key rotation	Swap key → DID unchanged → assets intact

24,000 farmers will have Cardano DIDs without knowing what blockchain is. Each PhoenixKey registration = 1 L1 transaction, counted within the ~100,000 setup events in Section 6.

8. Midnight — Commercial Privacy

Cardano is public — anyone can read transactions. Export businesses won't accept blockchain if competitors can see contract prices and partner lists.

Midnight generates per-party View Keys:

Party	CAN verify	CANNOT see
GACC (Chinese Customs)	Origin, harvest date, GACC code	Contract price, quantities, partners
EUDR Inspectors	GPS, deforestation-free proof	Commercial data
Consumers	Cultivation history, region	Business data

View Keys generated automatically on `datum_confirmed` event for export shipments. No manual distribution. No other blockchain simultaneously provides traceability transparency AND commercial privacy — this combination is unique to Cardano.

9. Multi-Application Architecture

Both TonFarm and Aladin read from the **same Farm NFT datum** and **same LampNet CIDs** — one source of truth, no sync needed.

One durian, four actors, one source of truth:

T+0s: Farmer scans harvest on TonFarm → Bio-ID written to LampNet

T+3–7s: Consumer in Ha Noi sees images on Aladin Trace (Layer 0)

T+41–61s: Cardano confirms → GACC dossier auto-generated

→ Customs receives View Key via Midnight

→ Consumer app: "✅ Verified on Cardano"

OriLife SDK (MIT, GitHub from M5): Bio-ID registration, origin verification, GACC/GS1 export, Midnight View Key creation, CID subscription.

10. Hydra — Path B Audit Settlement

GS-VEDATA-MOSAIC-PUBLIC-01

Hydra serves **one function**: audit proof trail. It has no role in NFT datum updates, consumer image delivery, or consumer verification.

Head config: 3 LampNet nodes · Hydra v1.3.0 · Long-lived Head (never closes in normal operation)

Why long-lived: 12-hour contestation period makes frequent Open/Close impractical. Head runs indefinitely via incremental deposit/decommit.

T=0: Open Head (one-time, ~580,000 lovelace)

T=4h: Decommit Merkle root → L1 (~450,000 lovelace)

T=8h: Next decommit → L1

... (repeat; Head never closes normally)

v1.3.0 costs (official benchmarks, 2025-07-28):

Transaction	3 parties	ADA
Init (one-time)	580,000 lovelace	0.58
Decommit (every 4–8h)	450,000 lovelace	0.45
Close (dispute only)	540,000 lovelace	0.54

Daily cost: 450,000 × 6 = **2.70 ADA/day** for entire system. Annual: ~985 ADA (~$246 at $0.25/ADA).

FanOut limit (~37 UTxOs) is not a constraint — Mosaic commits 1 Merkle root UTxO per epoch.

Hydra v2.0.0 roadmap: Directly Open Heads (no collectCom). Only `HydraSettlementAdapter` interface changes — Path A, SMT logic, datum schema, proof generation are entirely unaffected.

Path independence (formal property): Path A operates correctly regardless of Hydra Head status, Path B deployment status, or Hydra version. Path B is additive — not a dependency.

11. Verified Results

Verify: orilife.io/demo

Identification:

Metric	Result	Conditions
Precision	**~99%**	~100 trees, current test set
Recall	**>90%**	±45° angle variation
Re-identify after 30 days	✅ Pass	Same fruit
Distinguish 2 adjacent fruits	✅ Pass	Field conditions, Dak Lak

M1 commitment: maintain ~99% Precision + raise Recall to ≥95% on 10,000-tree benchmark (4+ varieties, 4+ stages, 5+ lighting conditions).

Operations:

Metric	Result
Response time	<3 seconds end-to-end
On-device speed	>30 FPS (mid-range Android)
Minimum device	Android 4GB RAM
Data package	<1KB

M1 target: <1 second response.

Consumer latency:

Layer	Latency	Event type
Layer 0 — Optimistic	~3–7s	All uploads
Layer 1 — Pending	~15–25s	All uploads
Layer 2 — Confirmed	~41–61s	Standard
Layer 2 — PRIORITY_HIGH	~25–35s	Harvest events
Push notification	<1s after confirm	WebSocket
Peak load vs Cardano	<2%	~0.039 events/s

On-chain evidence:

- VeData batch on Preprod
- TonFarm legacy on TON
- github.com/OriLifeTrace

12. Milestone Technical Mapping

Completed before GA:

Component	Status	Verify
TonFarm UX (farmers 50+)	✅ 2 seasons	tonfarm.co
AI PoC — fruit identification	✅ Working	orilife.io/demo
LampNet distributed storage	✅ Working	lampnet.cloud
VeData batch → Preprod (Path A)	✅ Working	Preprod TxHash
Institutional relationships 46 communes	✅ Confirmed	Letter 351-CV/HNDT
PhoenixKey DID concept	✅ Design complete	Prototype
Mosaic spec	✅ Frozen	GS-VEDATA-MOSAIC-PUBLIC-01

Per milestone:

Milestone	Key components	Status
M0	Escrow + IOB setup	Not deployed
M1	AI fine-tuning + pipeline + Three-Layer Read PoC	PoC ~1K trees
M2	Mobile app + contract freeze + PRIORITY_HIGH	TonFarm UX inherited
M3	Audit + Mainnet + BCT Portal + Hydra init + CID Subscription API	Preprod tested
M4	500 ha field ops + harvest module + GACC export	Not deployed
M5	SDK + Compliance adapter + TonFarm/Aladin integration	In development
M6	Scale 3,000 ha + SLA tiers	Not scaled
M7	12,000 ha + DR test + peak load	Not scaled
M8	B2B + MAGIC economics + impact report	Plan ready

Annex A v6.1 · April 2026 · GS-ORILIFE-GA-01 Open Source: github.com/OriLifeTrace · USPTO: #64/030,398 · #64/031,291 · #64/031,472 · #64/032,593