Battery Pack Aadhaar Anchored in the BMS: Hardware-Signed, Hash-Chained Health Records for Indian Two- and Three-Wheeler Packs Without a Blockchain

Why the integrity of a battery passport is settled at the point of measurement, not at the ledger

[1]Saswat Swain, [2]Chandrasekhar Panda, [3]Pravat Satpathy
[1]Ph.D Scholar, [2]Researcher, [3]Researcher
[1]KSOM — KIIT Deemed to be University,
Bhubaneswar, Odisha, India
[2,3]Research and Development Division,
Tekstein Solutions Private Limited, Bhubaneswar, Odisha, India
[1]saswat.mck@gmail.com, [2]contact@chandrasekharpanda.com, [3]analytics.pravat@gmail.com

***Abstract*—India's draft Battery Pack Aadhaar guidelines ask for a tamper-proof dynamic record of every traction battery, including state of health, yet leave that record to be uploaded by producers and service providers. Most published battery passport designs answer the integrity question with a blockchain. A ledger, however, protects data only after it has been written; it cannot show that a state-of-health figure was ever measured by the pack it describes. This paper moves the root of trust into the battery management system. A secure element inside the pack holds a non-exportable signing key bound to the pack identifier at end of line and a monotonic counter that numbers every daily health record. Records are hash-chained and signed, a fresh-nonce attestation exposes rollback, and a government registry stores chain heads in a witnessed Merkle transparency log. The scheme was implemented with standard elliptic-curve signatures and evaluated on 4000 simulated Indian two- and three-wheeler packs over six years under four duty cycles. Every cryptographic tampering attempt in the test suite was rejected with no false alarms on honest logs. Rollback of an exported log file went undetected unless the verifier challenged the live pack or held a registry anchor, a limitation we report rather than design around. A physics-based screen on the signed stress history detected state-of-health inflation with ninety percent probability once it exceeded about five to fourteen percentage points, depending on duty cycle and age, at a one percent false-alarm rate, but could not catch an attacker who controls the firmware and falsifies the stress counters consistently. Storage stays near 520 KiB for ten years of daily records. Because every log has exactly one writer, ordering needs no consensus, and a witnessed log gives the same tamper evidence without tokens, gas or wallets.**

***Index Terms*—Battery passport, Battery Pack Aadhaar, battery management system, secure element, tamper-evident logging, state of health, transparency log, electric two-wheeler, electric three-wheeler.**

I. Introduction

Two- and three-wheelers carry India's transition to electric road transport. Vahan-based counts for FY2025-26 put national EV registrations at 2.55 million, with electric two-wheelers (e2W) and three-wheelers (e3W) together accounting for more than 91 % of the total; electric L5 three-wheelers crossed 31 % penetration of their own segment [1]. These packs are small (roughly 2–10 kWh), they change hands often, and a growing share move into fleets, battery-swapping pools and second-life storage. Each transfer raises the same question: how much of the battery is left, and can the seller's number be believed? Lenders and repurposers price exactly this uncertainty, and without credible health evidence they either discount heavily or re-test every pack [2].

Regulators on both sides have answered with digital battery records. From 18 February 2027, the EU Battery Regulation requires a battery passport for every light-means-of-transport (LMT) battery, every EV battery and every industrial battery above 2 kWh placed on its market [3]. India's Ministry of Road Transport and Highways (MoRTH) released draft guidelines in December 2025 for a Battery Pack Aadhaar system that gives each L, M and N category traction pack a 21-character Battery Pack Aadhaar Number (BPAN), a QR code for offline static data, and a lean server layer for Battery Dynamic Data (BDD) such as status and state of health (SoH) [4]. The draft states that BDD should be a tamper-proof representation of the battery's technical state, but it assigns uploads to producers, service providers and recyclers, and it explicitly leaves SoH validation methodology for later [4]. The draft builds on the Battery Waste Management Rules, 2022 [5] and on the e-Mobility R&D roadmap of the Principal Scientific Adviser [6], and it states the intent to map onto EU passport schemas, whose data points per battery category the European Commission has since detailed [7], [8]. Industry has moved too: Volvo issued a passport for its

EX90 ahead of the EU deadline, built with a blockchain supply-chain partner at a reported cost of about USD 10 per car [9].

The academic literature has largely followed the blockchain path. A 2025 design mints composable non-fungible tokens (NFTs) for EV battery passports and reports simulated cost and security results, while noting that adoption in real supply chains remains unvalidated [10]. BlockBaRT registers batteries on a public ledger with selective disclosure, but covers only manufacture-time data and defers use-phase records [11]. A unified framework proposes passports, blockchain, reinforcement learning and zero-knowledge proofs together [12]. What these designs share is a guarantee about the *storage* path: once a value is on-chain it cannot be quietly changed. None of them constrains the *origin* of a use-phase value. If a service technician, a reseller or a compromised gateway submits SoH = 92 % for a pack that measures 74 %, an immutable ledger faithfully preserves the false number.

For dynamic health data, the only party that observes the cells directly is the battery management system (BMS). AIS-156 already requires a microprocessor-based BMS with data logging in Indian L-category packs, though it leaves the logging format and memory unspecified [13], [14]. This paper argues, and then tests, that the right place to anchor a battery passport for dynamic data is inside that BMS, in hardware, and that once this is done a blockchain contributes little that a government-run, independently witnessed transparency log does not already provide.

Research gap. Existing passport work (i) treats integrity as a ledger property and leaves the measurement-to-record path unauthenticated, (ii) rarely states a threat model for the use phase, where the realistic adversary is an owner or reseller with physical access, and (iii) does not quantify what a signed record still cannot prove, namely that the BMS itself told the truth.

Contributions. The paper makes the following contributions:

1) A tamper-evident health log (TEHL) for BPAN dynamic data in which a secure element (SE) in the BMS signs a fixed 82-byte daily record, chains it by SHA-256, and numbers it with a hardware monotonic counter; a fresh-nonce attestation converts that counter into offline rollback detection.
2) A threat model with eight concrete adversaries for Indian 2W/3W use, four security goals, and propositions that bound what any storage layer, ledger or not, can add once the origin is fixed.
3) A full implementation with standard ECDSA P-256 and an RFC 6962 Merkle registry, evaluated against the adversaries on signed logs from 160 packs and against three verification modes, including the mode in which the scheme fails.
4) A physics-plausibility screen that re-predicts SoH from the signed stress counters, with calibrated false-alarm rates, five verifier variants, and a consistent-falsification adversary that the screen does not catch.
5) Closed-form storage, wear, energy, readout and fleet-scale models, and a direct comparison with blockchain passport designs.

Section II reviews related work. Section III states the problem and threat model. Sections IV–VI give the design, the mathematical model and the algorithms. Section VII describes the simulation setup, Section VIII the results, Section IX the comparison, and Sections X–XI the outcomes and conclusions.

II. Related Work

Berger *et al.* framed the digital battery passport as a circular-economy instrument and grouped its data into four families, one of which is diagnostics, maintenance and performance [15]. Rufino Júnior *et al.* surveyed the regulations and standards that govern second-life batteries and showed how much of the repurposing decision depends on trustworthy usage history [16]. Butera and Gatteschi mapped the EU Regulation's passport obligations onto blockchain capabilities and argued for compatibility [17]. These works establish *what* the passport must contain; they say less about *who* is trusted to say it.

Among blockchain designs, Hasan *et al.* use composable NFTs on Ethereum with off-chain storage, evaluate four cathode chemistries on ten sustainability indicators, and analyse gas cost and known attacks in simulation [10]. Kanjere *et al.* implement BlockBaRT on the public Algorand chain with hashed records and selective disclosure; their own limitations note that operation-phase data and a security evaluation are missing [11]. Farhani's preprint combines passports, blockchain, reinforcement learning and zk-SNARKs into a conceptual framework [12]. The Volvo–Circulor deployment maps supply chains on a blockchain and promises SoH updates for 15 years [9].

A separate and older line of work studies logs kept on machines that the verifier does not trust. Schneier and Kelsey showed how hash chains and evolving keys make log entries written before a compromise impossible to alter undetectably [18]. Crosby and Wallach introduced history trees with logarithmic membership and consistency proofs [19], which became the basis of Certificate Transparency [20], [21]. Witness cosigning lets independent parties countersign an authority's statements so that equivocation becomes visible [22]. This body of work is directly applicable to battery records but is almost absent from the passport literature. Table 1 summarises the comparison.

Table 1 Related work on battery passports and tamper-evident logging

Ref., year	Approach	Use-phase SoH	Origin of data authenticated?	Evaluation	Stated limitation / gap
[15] Berger et al., 2022	DBP conceptualisation, data families and use cases	Listed as data family	Not addressed	Conceptual	No integrity mechanism
[17] Butera & Gatteschi, 2024	EU Regulation mapped to blockchain	Discussed	No	Review	No implementation
[10] Hasan et al., 2025	Composable NFTs, smart contracts, off-chain storage	Real-time KPI updates	No (uploader trusted)	Simulated; cost and attack analysis	Real supply-chain adoption unvalidated; scalability
[11] Kanjere et al., 2025	Public Algorand chain, hashed data, selective disclosure	Not covered	No	Functional test cases	Operation phase and security evaluation missing
[12] Farhani, 2025 (preprint)	DPP + blockchain + RL + zk-SNARKs	Proposed	No	Conceptual	Not peer reviewed; no measured results
[9] Volvo / Circulor, 2024	Commercial blockchain supply-chain passport	Promised, 15 years	Not disclosed	Deployed	Method of SoH sourcing not public
[4] MoRTH BPAN draft, 2025	BPAN + QR + central server for BDD	SoH, status, events	No (producer/service uploads)	Pilot example	SoH validation method deferred
[18], [19] secure logging	Hash chains, history trees on untrusted hosts	n/a	Logger-side	Formal / benchmarks	Not applied to batteries
This work	SE-signed, counter-numbered BMS log + witnessed Merkle registry	Daily signed records	Yes, at the BMS	160 signed logs, 8 adversaries, 4000-pack screening	Rollback undetectable from files; consistent firmware liar

III. Problem Statement and Threat Model

A. System model

A pack carries a BPAN, a BMS with an analogue front end, a microcontroller (MCU) with secure boot, and a discrete SE. At end of line, the manufacturer's certificate authority (CA) signs the binding (BPAN, *pk*), where *pk* is the SE's public key; the CA key is published through the BPAN registry. Once per day, or once per charge session in high-duty fleets, the BMS writes a record of its own observations. Verifiers include a used-vehicle buyer or financier with a phone app, an authorised service centre, a recycler and a market-surveillance authority. The registry is the MoRTH portal envisaged in [4].

B. Trust assumptions

(T1) The SE keeps its signing key secret and its counter monotonic. (T2) The MCU runs only firmware signed by the producer. (T3) SHA-256 is collision resistant and ECDSA P-256 is existentially unforgeable under chosen-message attack [23], [24]. (T4) At least one registry witness is honest. The attacker may read, erase and rewrite external and internal flash, replay or inject CAN and BLE traffic, swap BMS boards, and collude with a service centre. Invasive key extraction from the SE and malicious firmware signed with a stolen producer key are outside the cryptographic guarantees; the latter is modelled separately as adversary A8b in Section IV-F.

C. Adversaries and goals

Table 2 lists the adversaries. The security goals are: (G1) *authenticity*, every accepted record was produced by the BMS bound to this BPAN; (G2) *completeness and order*, no accepted log omits, reorders or truncates records; (G3) *registry non-equivocation*, the registry cannot show different histories to different parties without detection; and (G4) *plausibility*, an accepted SoH is consistent with the pack's own signed stress history.

Table 2 Adversaries considered

ID	Adversary and capability	Goal
A1	Owner edits a field in flash	Raise SoH
A2	Rewrites 180 days and recomputes chain	Erase heavy use
A3	Deletes days with abuse events	Hide abuse
A4	Restores an older flash image	Look younger
A5	Relabels a healthier pack's log	Transplant history
A6	Presents another BPAN's log	Swap identity
A7	Forges key and certificate	Fabricate log
A8	Reorders records	Disguise timing
A8b	Controls firmware; falsifies stress and SoH coherently	Undetectable inflation
A9	Registry insider edits or rebuilds tree	Equivocate

Proposition 1 (origin bound). Let a dynamic field x be produced at an origin O and stored through a write path W, so the stored value is $x' = W(O(x))$. If W is perfectly tamper evident, then

$$\Pr[x' \neq x \text{ undetected}] = \Pr[O(x) \neq x \text{ undetected at } O]. \quad (1)$$

Proof. A perfectly tamper-evident W implies $W(y) = y$ for every accepted y, so the only remaining source of error is the origin. ∎ The bound is elementary, but it fixes the design target: a blockchain improves W, whereas the attacks that matter to a used-pack buyer act on O. When O is a person typing into a portal, Eq. 1 is limited by that person's honesty however good the ledger.

IV. Proposed Methodology

A. Architecture

Fig. 1 shows the architecture. Sensors feed the MCU, which runs the SoH estimator and builds the daily record. The MCU never holds a signing key: it passes the chain head h_i to the SE,

which returns a signature and supplies the sequence number from its counter. Records and signatures are appended to flash. A verifier reads the log over CAN or Bluetooth Low Energy (BLE) and, when the pack is physically present, sends a nonce that the SE answers. Service centres upload (seq, h_{seq}) to the registry at each visit; the registry appends these anchors to a Merkle log whose tree heads are cosigned by independent witnesses such as type-approval test agencies.

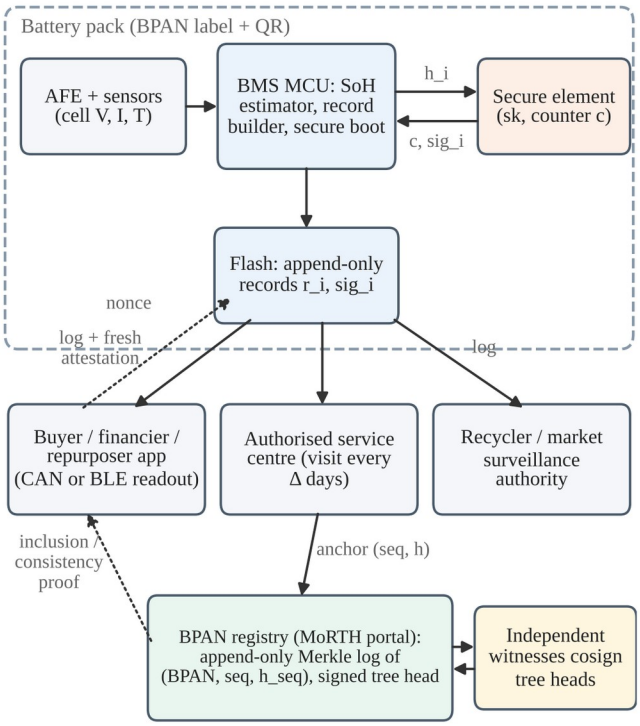


Fig. 1. Architecture of the BMS-anchored tamper-evident health log. Solid arrows carry data; dotted arrows carry challenges and proofs. Only the secure element holds the signing key.

B. Record format

The daily record (Table 3) is 82 bytes. It contains the SE counter value, a timestamp, cumulative discharge and charge throughput, cumulative full-equivalent cycles, the BMS estimates of SoH, capacity and resistance, the Ah-weighted active temperature, daily extremes, the depth of discharge, minutes in operation and charging, a minutes-at-temperature histogram over eight bins, a state-of-charge (SoC) dwell histogram over five bins, cumulative abuse-event counters, and a four-byte firmware measurement. Cumulative counters make deletion visible even without cryptography, since a gap shows up as a jump; the histograms are what the plausibility screen in Section IV-F consumes. Every field maps onto a BDD parameter in [4] or onto the stress factors the draft names for SoH validation (charge throughput, temperature history, imbalance and anomaly events).

Table 3 Daily health record (82 bytes, little-endian)

Field(s)	Type	Bytes	Use
ver, flags	u8 × 2	2	format, status bits
seq (SE counter)	u32	4	order, rollback
timestamp	u32 min	4	BDD date/time
Ah discharged, Ah charged (cum.)	u32 × 2	8	throughput
FEC (cum.)	u32	4	cycle stress
SoH, capacity, resistance	u16 × 3	6	BDD SoH
T active, T max, T min	i16, i8 × 2	4	thermal stress
DoD max, mean SoC	u8 × 2	2	cycle depth
minutes operating, charging	u16 × 2	4	C-rate
cell V max, V min	u16 × 2	4	imbalance
T histogram (8 bins)	u16 × 8	16	calendar stress
SoC histogram (5 bins)	u16 × 5	10	calendar stress
events: DD, OT, OV, UV, OC	u16 × 5	10	abuse history
firmware measurement	4 B	4	build check

C. Chain construction and signing

Let ‖ denote concatenation and H denote SHA-256. The chain is seeded with the identity binding and then extended record by record:

$$h_0 = H(01 \,\|\, \mathrm{BPAN} \,\|\, pk), \tag{2}$$

$$h_i = H(02 \,\|\, \mathrm{BPAN} \,\|\, r_i \,\|\, h_{i-1}), \tag{3}$$

$$\sigma_i = \mathrm{Sign}_{sk}(h_i) \;\text{ if }\; \mathrm{seq}_i \bmod k = 0, \tag{4}$$

where r_i is the serialised record, seq_i is the SE counter value written into r_i, and k is the signature interval. Domain-separation prefixes 01, 02 and 03 prevent a value of one type being replayed as another. Because σ_i covers h_i, and h_i commits to every earlier record, one signature authenticates the whole prefix. Fig. 2 illustrates the structure. With $k = 1$ every day is individually signed; Section VIII-F shows why we recommend $k = 1$ for daily records.

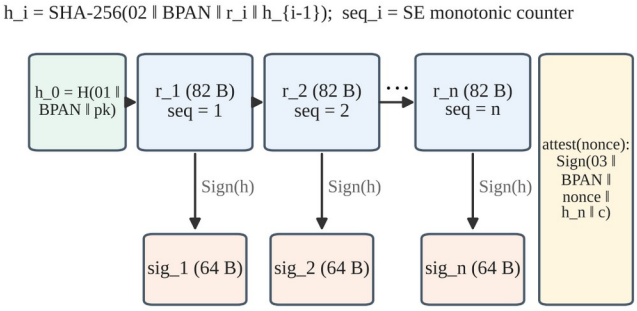


Fig. 2. Hash chain and signatures. The sequence number of every record is issued by the secure element's monotonic counter, not by the MCU.

D. Attestation and rollback

A signed chain proves that a prefix is authentic; it does not prove that the prefix is the whole history. An attacker who restores a two-year-old flash image presents a valid log of a younger, healthier pack. TEHL closes this gap with the counter. On request, the firmware recomputes the head h_n from flash, reads the counter c from the SE, and the SE signs

$$a = \mathrm{Sign}_{sk}(H(03 \,\|\, \mathrm{BPAN} \,\|\, \mathrm{v} \,\|\, h_n \,\|\, c)), \tag{5}$$

where v is the verifier's fresh nonce. The counter lives in the SE and cannot be decremented, so a rolled-back flash image yields $c > n$. The verifier accepts only if

$$\text{Bind} \wedge \text{Seq} \wedge \text{Sig} \wedge (c = n) \wedge \text{Anc}, \quad (6)$$

where Bind is a valid CA signature on (BPAN, *pk*), Seq requires $\text{seq}_i = i$ for all i, Sig requires every σ_i to verify against h_i, and Anc requires every registry anchor (j, g) for this BPAN to satisfy $j \le n$ and $h_j = g$. The firmware cannot be made to lie about c without breaking assumption T2, and the SE cannot be made to sign an old counter value.

E. Registry transparency log

The registry stores leaves (BPAN, seq, h_{seq}) in an append-only Merkle tree with RFC 6962 hashing (prefix 00 for leaves, 01 for nodes) [20]. It publishes a signed tree head each epoch, and witnesses cosign a head only after checking a consistency proof from the previous head [22]. A buyer who holds a cosigned head can obtain an inclusion proof for the latest anchor of a pack in $\lceil \log_2 N \rceil$ hashes. A registry insider who edits a stored anchor, or rebuilds the tree, fails either the inclusion check or the witnesses' consistency check.

F. Physics-plausibility screening

Signatures settle G1–G3. They cannot settle G4, because a BMS with miscalibrated or maliciously modified SoH logic signs its own wrong number. The screen re-predicts SoH from the signed stress counters with the ageing model of Section V, drawing $M = 256$ samples of the pack-specific rate multipliers from a population prior, and flags a report that lies too far above the prediction. Two verifier variants matter. V0 uses only the population prior. V5 also weights the prior samples by the pack's own signed SoH reports at days 90, 180, 270 and 364, on the assumption that a compromise, if any, occurs after the first year. Variants V1–V4 deliberately mis-specify the verifier's model to test robustness. Adversary A8b is the strongest case: it controls the firmware, lowers recorded throughput by 30 % and recorded temperature by about one histogram bin, and then reports the verifier's own median prediction for the falsified stress.

G. Why a blockchain is not required

A blockchain solves agreement on a single order of transactions among writers who compete for the same state, as in a double spend [25]. A pack's health log has exactly one writer, the SE, whose counter already defines a total order. The registry has one operator, the state, which is also the party the regulation trusts to run the portal [4]. What remains is to stop the operator from rewriting history or showing different histories to different people. That is detection, not agreement, and a witnessed Merkle log provides it.

Proposition 2 (single-writer sufficiency). Under T1–T4, for any accepted (log, attestation, anchors) triple, every record was produced by the bound SE in counter order, and any registry equivocation is detected by any one honest witness, except with probability at most $\varepsilon_{\text{sig}} + \varepsilon_{\text{col}}$, the forgery and collision advantages.

Proof sketch. An accepted record not produced by the SE requires either a valid σ on a head the SE never signed (forgery) or a second preimage path to a signed head (collision). Reordering or deletion breaks $\text{seq}_i = i$ or the chain. Truncation leaves $c > n$ in a fresh attestation. Two different trees served to two parties cannot both be consistent with the same cosigned head without a hash collision. ∎ A Byzantine fault-tolerant ledger with $3f + 1$ validators tolerates f faulty ones [26]; the witness scheme needs only one honest witness, but offers detection rather than prevention. For an evidence record, detection is the property needed.

We do not claim that blockchains are useless for battery passports. Material provenance, recycled content and cell origin for incentive verification involve many writers and no single measuring device, and a shared ledger can be defensible there. Our claim is narrower: for BDD, the integrity problem is at the origin, and once the origin is fixed in hardware a ledger adds operational dependencies (wallet keys, fee exposure, public-chain governance, data-sovereignty review) without adding tamper evidence.

V. Mathematical Modeling

A. Pack ageing model

Capacity fade is the sum of calendar, cycle and abuse terms. For pack p on day d, with time-weighted Arrhenius factor $\bar{A}_{\text{cal}}$, SoC s, active temperature T_{act}, effective C-rate C, depth of discharge D and cumulative full-equivalent cycles n_{FEC},

$$Q_{\text{cal}} = a_{\text{cal}}\, m_{\text{cal}}\, \bar{A}_{\text{cal}}\, [1 + g(s - 0.5)]\, \sqrt{t}, \quad (7)$$

$$Q_{\text{cyc}} = b\, m_{\text{cyc}}\, A(E_{\text{cyc}}, T_{\text{act}})\, \Phi_{\text{C}}\, \Phi_{\text{D}}\, n_{\text{FEC}}{}^{z}, \quad (8)$$

where $\Phi_{\text{C}} = 1 + \kappa_{\text{c}}(C - 0.5)$, $\Phi_{\text{D}} = 1 + \kappa_{\text{d}}(D - 0.8)$, $A(E, T) = \exp[-(E/R)(1/T - 1/T_{\text{ref}})]$, $T_{\text{ref}} = 298.15$ K, and m_{cal}, m_{cyc} are lognormal pack multipliers ($\sigma = 0.12$) that represent manufacturing spread. Because the stress varies daily, the power laws are integrated with the equivalent-state method,

$$t_{\text{eq}} = (Q_{\text{cal}}/k_{\text{cal},d})^2, \;\; Q_{\text{cal}} \leftarrow k_{\text{cal},d}\, \sqrt{(t_{\text{eq}} + \Delta t)}, \quad (9)$$

and similarly for cycles with exponent $1/z$. True SoH is then

$$\text{SoH} = 100 - Q_{\text{cal}} - Q_{\text{cyc}} - Q_{\text{pen}}, \quad (10)$$

with Q_{pen} adding 0.02 points per deep-discharge event and 0.015 points per over-temperature event. Parameters (Table 4) are representative values calibrated to typical datasheet claims (cycle-only fade of 15 % at 1000 FEC for NMC and 2500 FEC for LFP at 25 °C; Ea ≈ 50 kJ/mol calendar and 30 kJ/mol cycle), consistent in form with published semi-empirical models [27], [28]. They were not fitted to Indian packs. The integrity results in Section VIII do not depend on these values; the SoH trajectories and the plausibility numbers do.

B. BMS estimator and plausibility statistic

The BMS estimate is SoH plus an AR(1) error with one-day correlation 0.98 and stationary standard deviation $\sigma_{\text{est}} = 1.0$ point for NMC and 2.0 points for LFP; the larger LFP value reflects the flat open-circuit-voltage curve that makes LFP capacity estimation harder [29]. Given the verifier's predictive samples $\{\hat{s}_m\}$, the screening statistic is

$$Z = (\text{SoH}_{\text{rep}} - \text{med}\, \hat{s}) \,/\, \sqrt{(\text{Var}\, \hat{s} + \sigma_{\text{est}}{}^2)}, \quad \text{flag if } Z > \tau_\alpha, \quad (11)$$

with τ_α the empirical $(1 - \alpha)$ quantile of Z on a calibration half of the honest fleet and $\alpha = 0.01$. Variant V5 replaces uniform weights with

$$w_m \propto \exp[-\Sigma_j\, (\text{SoH}_{\text{rep},j} - \hat{s}_{m,j})^2 \,/\, 2\sigma_{\text{est}}{}^2], \quad (12)$$

over the four year-one anchor days j, and uses the weighted mean and variance in Eq. 11.

C. Overhead and scalability

With a 150-byte header (BPAN, public key, binding signature), n records and signature interval k, the log occupies

$$S(k, n) = 150 + n(82 + 64/k) \text{ bytes.} \quad (13)$$

If the registry receives anchors every Δ days with uniform phase and an attacker removes the last m days, an offline verifier detects the rollback with probability

$$P_{\text{det}}(m) = \min(1, m/\Delta), \quad (14)$$

whereas a live attestation detects any $m \geq 1$. For N packs each reporting once per day, per-record on-chain anchoring needs

$$\lambda = N/86\,400 \text{ writes per second,} \quad (15)$$

while a daily Merkle root needs one write per day for any N, with inclusion proofs of $\lceil \log_2 N \rceil \times 32$ bytes. Finally, an Ethereum-style anchor that writes a fresh 32-byte storage slot costs

$$G = 21\,000 + 16 \cdot 32 + 20\,000 + 2\,100 = 43\,612 \text{ gas,} \quad (16)$$

from the base transaction cost, non-zero calldata, and a cold zero-to-nonzero SSTORE [30].

VI. Algorithms

Algorithm 1: BMS daily append (runs on MCU + SE)

input: observations of day d, head h, interval k
$s \leftarrow$ SE.CounterIncrement()
$r \leftarrow$ Serialise(s, t, cumulative counters, SoH, histograms, events, fw)
$h \leftarrow H(02 \,\|\, \text{BPAN} \,\|\, r \,\|\, h)$
if $s \bmod k = 0$ **then** $\sigma \leftarrow$ SE.Sign(h) **else** $\sigma \leftarrow \perp$
Flash.Append(r, σ) // append-only region
keep h in RAM; recompute from flash after reset

Algorithm 2: Verifier

input: log L, CA key, optional nonce ν, attestation a, anchors A
reject if CA signature on (BPAN, pk) fails
$h \leftarrow H(01 \,\|\, \text{BPAN} \,\|\, pk)$; $j \leftarrow 0$
for each (r, σ) in L **do**
  $j \leftarrow j + 1$; **reject if** seq(r) $\neq j$ or cumulative fields decrease
  $h \leftarrow H(02 \,\|\, \text{BPAN} \,\|\, r \,\|\, h)$; store h_j
  if $\sigma \neq \perp$ **reject if** not $\text{Ver}_{pk}(\sigma, h)$
reject if last record unsigned
if a given: **reject if** bad signature, nonce $\neq \nu$, head $\neq h$ or $c \neq j$
for each $(u, g) \in A$: **reject if** $u > j$ or $h_u \neq g$
compute Z from signed stress (Eq. 11); **flag if** $Z > \tau_\alpha$
accept

Complexity. Algorithm 1 costs one hash and at most one signature per record: O(1) time and O(1) RAM beyond the 32-byte head. Algorithm 2 makes one pass over n records with O(n) hashes and O(n/k) signature verifications, and needs O(1) memory if anchors are checked as they stream past. The plausibility step costs O(nM) arithmetic, and registry proofs cost O(log N). On the evaluation host, appending a record including a software ECDSA signature took 35 µs on average, and verification grew linearly at about 88 µs per record (Fig. 7b).

VII. Simulation Setup

Software and hardware. All code is Python 3 with NumPy, SciPy and Matplotlib; signatures and hashes use the *cryptography* library (OpenSSL backend) with ECDSA over NIST P-256 and SHA-256. Experiments ran on a single x86-64 Linux container. No BMS hardware was used: the SE is emulated in software with the two properties the protocol relies on (non-exportable key, monotonic counter). Global seed 20261023 fixes every random stream; the code, logs and figure scripts are in the reproducibility bundle.

Fleet. Four duty cycles represent common Indian use (Table 4): a private commuter e2W, a delivery-fleet e2W, an L5 passenger e3W and an L3 e-rickshaw. Each profile has 1000 packs simulated daily for six years (2190 days), with lognormal daily distance, rest days, AR(1) weather around two climate regimes (humid east coast and hot northern plain), sun soak, Joule heating through pack resistance that grows with fade, and random deep-discharge events. Over-temperature events are counted when the cell hot-spot estimate exceeds 50 °C.

Table 4 Simulation parameters (assumptions)

Parameter	2W priv.	2W deliv.	3W L5	3W L3
Chemistry / energy	NMC 3.0 kWh	NMC 3.0 kWh	LFP 8.0 kWh	LFP 5.0 kWh
Mean distance (km/day)	30	105	120	85
Consumption (Wh/km)	30	32	60	48
Charging	every ~2 days	daily+	daily	daily, slow
Climate regime	humid east	hot north	hot north	humid east
R_0 (mΩ) / θ (K/W)	60 / 0.15	60 / 0.15	25 / 0.08	35 / 0.10
σ_{est} SoH (pp)	1.0	1.0	2.0	2.0
Packs × days	1000 × 2190	1000 × 2190	1000 × 2190	1000 × 2190

All profiles: $z = 0.60$ (NMC), 0.55 (LFP); E_a 50 kJ/mol calendar, 30 kJ/mol cycle; pack spread $\sigma = 0.12$; seed 20261023.

Test scenarios. (S1) Integrity: signed logs for the first 40 packs per profile (160 logs, 350,400 signed records), 80 attack trials per adversary across three verification modes: M1 log-only (an exported file), M2 live attestation with a fresh nonce, and M3 registry anchors uploaded every $\Delta = 90$ days. (S2) Registry: a Merkle log of 4,800 daily heads with 200 insider-edit trials. (S3) Plausibility: SoH inflation $\delta \in \{0, \ldots, 15\}$ points added at years 2, 4 and 6; thresholds calibrated on 500 packs per profile and tested on the other 500. (S4) Closed-form overheads from Section V-C.

VIII. Results and Discussion

A. Degradation trajectories

Fig. 3 shows the simulated true SoH. The delivery e2W, at a median of 2224 full-equivalent cycles in six years, crosses the 80 % boundary between BPAN status A (operational) and B (second life) [4] after a median of 650 days and ends at 57.5 %, with 67.6 % of packs below the 60 % end-of-life boundary. The private e2W and L5 e3W follow nearly the same median path (78.8 % and 79.3 % at year 6) for different reasons: the private pack is calendar dominated (579 FEC), while the LFP auto cycles three times as much but on a chemistry that tolerates it. The e-rickshaw ends highest at 80.5 %, and only 39.1 % of its packs fall below 80 % by year 6. The 5–95 % bands span about 7 to 8 points for the three slower profiles and about 18 points for

the delivery e2W at year 6. That spread matters below: it is what limits plausibility screening.

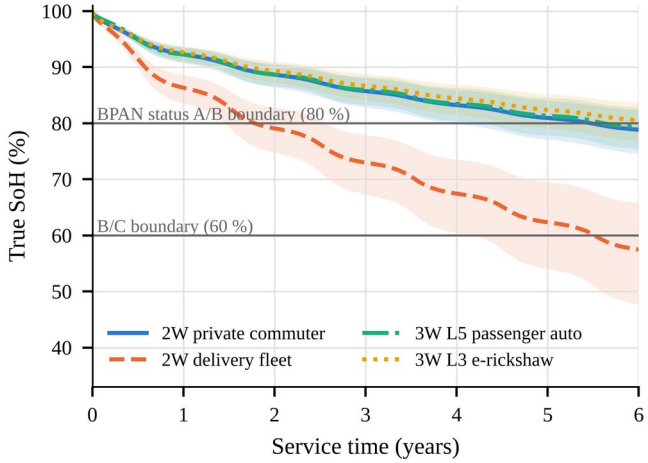


Fig. 3. Simulated true SoH for the four Indian duty cycles (median and 5–95 % band, 1000 packs each). Horizontal lines mark the BPAN status boundaries of the draft guidelines. Trajectories are model dependent (Section V-A).

B. Cryptographic tamper detection

Table 5 reports the adversary suite. All honest logs were accepted in all three modes (0 false alarms in 240 verifications). Field edits, rewrites with a recomputed chain, deletion of abuse-event days, transplanting another pack's log, presenting a different BPAN's log, forging a key with a self-issued certificate, and reordering records were all rejected in every mode; the failure codes in the last column show which check fired. Deleting abuse days is caught twice over, by the sequence gap and by the broken chain.

The rollback row is the important one. In M1 the verifier holds only a file, and a truncated prefix of a genuine log is itself a genuine log: **0 of 80** rollbacks were detected. This is not a flaw in the implementation; no signature scheme can prove the absence of later records from data alone. A live challenge (M2) caught all 80, because the SE counter exceeded the last record number. Registry anchors (M3) caught 76/80, missing only rollbacks shorter than the time since the last service visit. A replayed old attestation was rejected in 100/100 trials because its nonce was stale. The practical rule follows directly: a buyer should never accept an exported passport file as evidence of current health; the app must challenge the pack.

Table 5 Adversary detection by verification mode (detected/trials)

Adversary	M1 file	M2 live	M3 anchor	Main failure codes
A1 field edit (SoH +5 pp)	80/80	80/80	80/80	bad sig; unsigned tail
A2 rewrite 180 d + rechain	80/80	80/80	80/80	bad sig; unsigned tail
A3 delete abuse-event days	80/80	80/80	80/80	bad sig; seq gap
A4 rollback / truncation	0/80	80/80	76/80	rollback or truncation; anchor beyond log
A5 log transplant (BPAN relabel)	80/80	80/80	80/80	bad sig; key not bound
A6 whole-log swap (other BPAN)	80/80	80/80	80/80	bpan mismatch; bad attestation
A7 forged key + self-cert	80/80	80/80	80/80	key not bound; bad attestation
A8 record reorder	80/80	80/80	80/80	bad sig; seq gap
Honest logs (false alarms)	0/80	0/80	0/80	none

M1: exported log only. M2: fresh-nonce SE attestation. M3: registry anchors every 90 days. 160 packs, 2190 signed records each.

C. Rollback window and anchoring interval

Fig. 4 compares Eq. 14 with the measured M3 detection rate. The measured points follow the $\Delta = 90$ day line, confirming that the residual window for an offline verifier equals the anchoring interval. Shortening Δ to 30 days narrows the window to one month but triples service-visit uploads; the live attestation removes the window entirely and costs nothing at the registry. For a resale, where buyer and pack meet physically, M2 is the natural mode; M3 is the fallback for remote financing decisions.

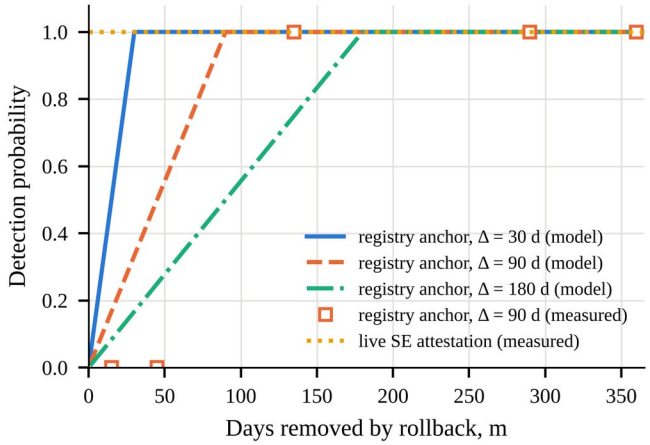


Fig. 4. Probability of detecting a rollback that removes the last m days. Lines: Eq. 14 for three anchoring intervals. Squares: measured with registry anchors every 90 days, binned by m. Dotted: live SE attestation.

D. Registry non-equivocation

In S2 the registry held 4,800 anchors. An insider who altered one stored head and served the honest inclusion path failed verification against the witnessed tree head in 200/200 trials; an insider who rebuilt the whole tree around the altered leaf failed the witnesses' consistency check in 200/200. Honest inclusion and consistency proofs all verified. Proofs held 9 hashes at this size and grow to 24 hashes (768 bytes) for a day's anchors from ten million packs.

E. Physics-plausibility screening

Fig. 5(a) shows detection probability against inflation δ at year 4 with the population prior (V0). Test false-alarm rates stayed between 0.2 % and 2.2 % across all profiles, ages and both main variants, close to the 1 % target. At year 4 the screen reaches 50 % detection at δ ≈ 3.6 points for the private e2W, 5.6 for the L5 auto, 6.0 for the e-rickshaw and 6.7 for the delivery e2W.

Two effects explain the ordering. For the delivery pack, the predictive band is wide because six years of heavy cycling amplify the pack-to-pack spread in m_{cyc}; this is visible in Fig. 3. For the two LFP profiles the predictive band at year 4 is about as narrow as for the private e2W (3.8 and 3.6 points against 3.9), yet detection is worse. The difference is the BMS estimator: σ_{est} = 2 points for LFP against 1 for NMC enters the denominator of Eq. 11. A flat LFP voltage curve therefore costs passport credibility as well as range accuracy; data-driven capacity estimators that cut σ_{est} [31] would narrow the gap directly.

Fig. 5(b) and Table 6 show what the pack's own signed first-year history buys (V5). For the delivery e2W the 90 % detection threshold at year 6 falls from 14.1 to 8.1 points, and for the private e2W from 7.4 to 6.4. For both LFP profiles the improvement is under one point, because a 2-point estimator noise makes four year-one reports nearly uninformative about the pack's own rate constants (effective sample size 866 and 900 of 1024). The deliberately mis-specified verifiers V1–V4 changed δ_{90} at year 6 by at most 0.7 points once the threshold was recalibrated on the honest fleet, so the screen is limited by pack-to-pack spread and estimator noise, not by model detail.

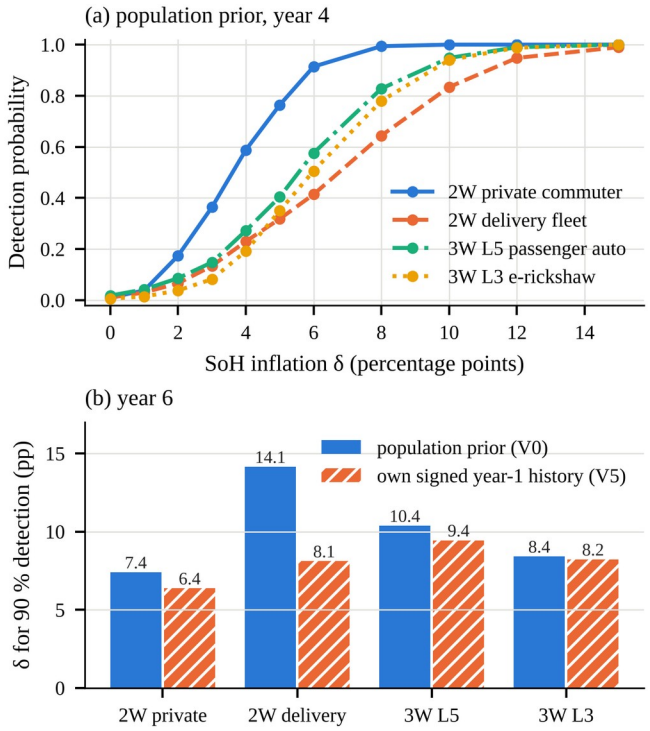


Fig. 5. Plausibility screening at 1 % false-alarm rate. (a) Detection probability against SoH inflation at year 4, population prior. (b) Inflation needed for 90 % detection at year 6, population prior (V0) against the pack's own signed year-1 history (V5).

Table 6 Inflation (pp) for 90 % detection; A8b detection % (median inflation pp)

Profile	V0 y4	V0 y6	V1	V2	V3	V4	V5	A8b y6
2W private	5.9	7.4	7.6	7.7	7.6	7.5	6.4	0.0 (6.6)
2W delivery	11.2	14.1	14.3	14.3	14.6	14.6	8.1	0.0 (14.1)
3W L5 auto	9.2	10.4	10.2	10.2	10.4	10.3	9.4	0.2 (6.3)
3W L3 e-rickshaw	9.5	8.4	8.7	9.1	8.5	8.6	8.2	1.2 (6.2)

V1: z − 0.05. V2: activation energies −20 %. V3: no active-temperature field. V4: calendar rate +25 %. V1–V5 at year 6.

The A8b column is the honest limit of the method. An attacker who controls the firmware and falsifies throughput and temperature consistently obtained a median SoH inflation of 6.6–14.1 points at year 6, and the screen flagged at most 1.2 % of such packs, which is no better than its false-alarm rate. Signed data cannot defend against a signer that lies coherently. The countermeasures lie outside the log: producer code-signing keys held in hardware security modules, firmware measurement checked against the type-approved build (the fw field in Table 3), and independent cross-checks such as charger-side energy metering or a signed reference capacity test at service.

F. Overheads

Fig. 6(a) gives log size against retention. With k = 1 the measured six-year log is 312.4 KiB and the ten-year projection is 521 KiB, which fits in a typical on-chip flash budget; three records per day for high-duty fleets need about 1.5 MiB and an external SPI NOR device. Fig. 6(b) shows the trade-off in k: raising k to 16 saves 41 % of storage but leaves up to 15 records unsigned at any readout, and those records can be rewritten by a flash attacker before the next signature covers them. With one record per day, a signature per record costs 64 bytes a day, so we recommend k = 1 and reserve k > 1 for high-rate event logs.

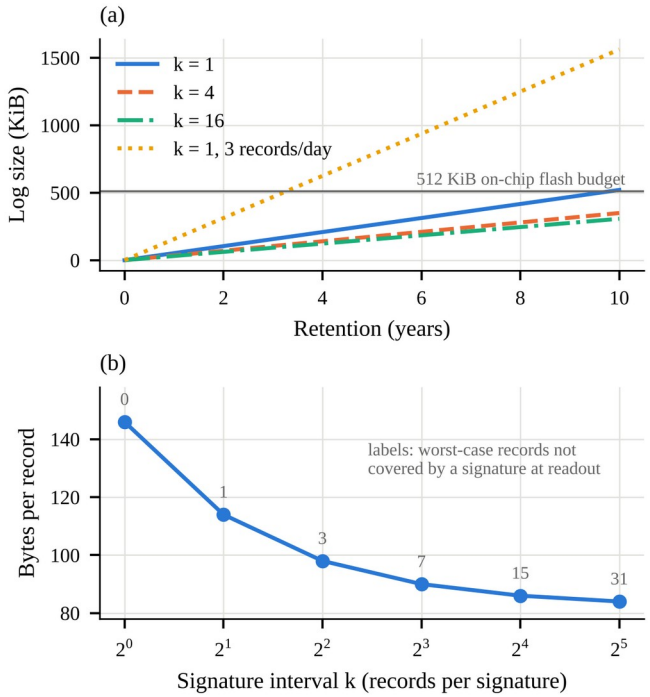


Fig. 6. (a) Log size against retention for signature intervals k and for three records per day. (b) Bytes per record against k; labels give the worst-case number of records not yet covered by a signature at readout.

Table 7 collects the remaining costs. Flash wear is irrelevant at this rate: a 2 MiB log region is filled to 25.4 % in ten years, so each sector is erased at most once. Signing energy, over the whole plausible range of signing time (20–400 ms at 60 mW, an assumption spanning a hardware SE and software ECDSA on a small Cortex-M class core), is 1.2–24 mJ per day, about 10^{-10}–10^{-9} of a 3 kWh pack's daily throughput. Reading the full ten-year log takes about 40 s over classic CAN at half bus load or 27 s over BLE at a conservative 20 kB/s; one year takes 4.0 s. The SE itself costs well under one euro in volume [32].

Table 7 Per-pack overheads (k = 1, one record per day)

Item	Value	Basis
Record / signature	82 B / 64 B	Table 3, raw rls
Log, 6 years (measured)	312.4 KiB	S1 logs
Log, 10 years	521 KiB	Eq. 13
Flash erases per sector, 10 y	1	2 MiB region
Signing energy per day	1.2–24 mJ	assumed 20–400 ms, 60 mW
Readout, 10 y log, CAN	40 s	500 kbit/s, 50 % load
Readout, 10 y log, BLE	27 s	assumed 20 kB/s
Append incl. software sign	35 µs	x86-64 host
Verify 2190 records	190 ms	x86-64 host
SE unit price	≈ EUR 0.66–0.86	distributor listing [32]

G. Fleet-scale anchoring

Fig. 7(a) shows the write rate needed if every pack's daily record were anchored individually on a ledger, as per-pack NFT designs imply. Ten million packs produce 116 writes per second, several times the order of 15–30 transactions per second commonly cited for a public layer-1 chain (shaded, approximate). At 43,612 gas per anchor (Eq. 16) a pack costs 15.9 million gas per year, which at 1 gwei is 0.016 ETH per pack-year, a cost denominated in a volatile token. Batching removes both problems: one Merkle root per day is one write regardless of *N*. We note this honestly because it weakens a common argument against blockchains: once batched, ledger anchoring is cheap. But a batched ledger anchor is a timestamp on a Merkle root, which is exactly what the witnessed registry log already provides. Fig. 7(b) confirms that verification on the buyer side scales linearly and stays well under a second for six years of history on the evaluation host; a phone will be slower by a constant factor that we did not measure.

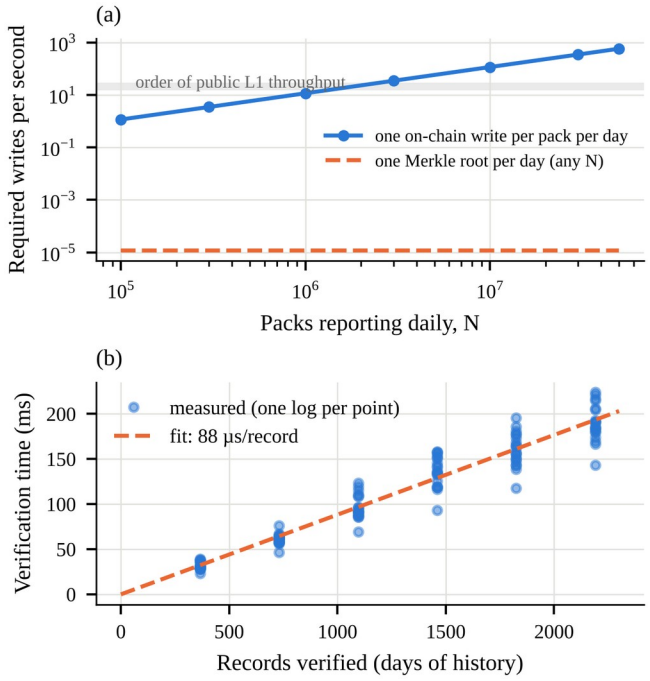


Fig. 7. (a) Required write rate against fleet size for per-record and batched anchoring. (b) Measured verification time against log length with a linear fit.

H. Threats to validity

All results are from simulation; no physical BMS, SE or vehicle was tested, and the SE was emulated in software. Signing latency and energy were bracketed by assumption rather than measured on a target MCU. The ageing model is representative, not fitted to Indian packs, and the verifier's model belongs to the same family as the simulator's; V1–V4 probe mis-specification but cannot fully replace field data, so the plausibility thresholds should be read as optimistic. Duty-cycle parameters are engineering estimates. The cryptographic results, by contrast, hold by construction under assumptions T1–T4 and do not depend on the battery model.

IX. Comparative Analysis

Table 8 compares TEHL with representative passport designs on the dimensions that matter for BDD in India. The entries for other works use only what those works report; "not reported" marks a dimension they do not address. TEHL is the only design in the set that authenticates the origin of use-phase data. It is also the only one that reports its own failure modes quantitatively. It does not address material provenance or

carbon-footprint data, where the blockchain designs and commercial services have more to offer.

Table 8 Comparative analysis for BPAN dynamic data

Criterion	BPAN draft [4]	NFT passport [10]	BlockBaRT [11]	Volvo/Circulor [9]	TEHL (this work)
Use-phase record origin authenticated	No	No	No	Not disclosed	Yes (SE in BMS)
Rollback / truncation detection	No	Ledger order only	Ledger order only	Not disclosed	Yes with live challenge or anchors
Offline verification at point of sale	QR static data only	No (chain access)	No (web app)	QR to service	Yes (CAN/BLE + nonce)
Per-update cost	Server write	Gas per update	Chain tx per record	≈ USD 10 per car (reported)	One 64 B signature; daily root
Writes at 10 M packs/day	Server	116 tx/s unbatched	116 tx/s unbatched	Not disclosed	1 root/day
Infrastructure	Central server	Ethereum + L2 + storage	Algorand + BaaS	Vendor platform	SE + central log + witnesses
Quantified failure modes	n/a	Partial	No	No	Yes (Tables 5, 6)
Material provenance, carbon data	Yes (static)	Yes	Partial	Yes	Out of scope

X. Key Outcomes

- **Origin over ledger.** For BPAN dynamic data, the integrity question is decided where SoH is measured. Hardware signing in the BMS fixes the origin; a witnessed registry log fixes storage without a blockchain.
- **Live challenge is mandatory.** Exported passport files cannot reveal rollback; a nonce answered by the SE counter can. Buyer and financier apps should be required to challenge the pack.
- **Plausibility has a floor.** At 1 % false alarms, physics screening reaches 90 % detection only for inflations of about 5–14 points, better for NMC than LFP, and fails against a consistent firmware-level liar.
- **Low cost.** One 82-byte record and one 64-byte signature per day, ≈ 520 KiB in ten years, negligible energy and wear, and a sub-euro SE.
- **Regulatory fit.** The record maps onto BDD fields and the stress factors named in the draft, so the scheme can be specified through the AIS route the draft proposes [4], and anchored heads can be exported to EU passport schemas.

XI. Conclusion

This paper set out to test whether a battery passport for Indian two- and three-wheeler packs needs a blockchain to be trustworthy. For dynamic health data the answer from our implementation is no, provided the root of trust sits in the BMS. A secure element that signs and numbers each daily record turned every cryptographic manipulation in our suite into a rejected log, a fresh attestation exposed rollback that no file-based check can see, and a witnessed Merkle registry made insider edits visible. The same experiments marked the boundaries: exported files cannot prove completeness, physics screening only bounds large SoH inflations, and a firmware-level attacker who falsifies stress counters coherently is not caught by any log-side check.

Future work will move the design onto a production BMS and SE to measure signing time, energy and readout on real hardware, fit the ageing prior to field data from Indian fleets, add charger-side energy metering as an independent cross-check, and work with the AIS process on a record schema and challenge protocol for the BPAN dynamic layer.

Acknowledgment

The authors thank the Research and Development Division of Tekstein Solutions Private Limited for computing support. [Funding statement to be confirmed by the authors.]

Data Availability

All code, configuration, generated data summaries, result logs and figure scripts are provided in the accompanying reproducibility bundle (global seed 20261023).

References

[1] S. Ojha, “India registered 2.55 million EV sales in FY2025-26, says IESA,” *EV Infrastructure News*, 2026 (reporting IESA, *India's Mobility Report FY2025-2026*).

[2] Rocky Mountain Institute, “India's used EV battery market needs trust,” RMI, 2026.

[3] European Parliament and Council, “Regulation (EU) 2023/1542 concerning batteries and waste batteries,” *Off. J. Eur. Union*, L 191, Jul. 2023, Art. 77 and Annex XIII.

[4] Ministry of Road Transport and Highways, Govt. of India, “Guidelines for implementation of Battery Pack Aadhaar system (draft),” New Delhi, Dec. 2025.

[5] Ministry of Environment, Forest and Climate Change, Govt. of India, “Battery Waste Management Rules, 2022,” Aug. 2022.

[6] Office of the Principal Scientific Adviser to the Govt. of India, “e-Mobility R&D roadmap for India,” 2024.

[7] European Commission, “Guidance document: Digital batteries passport – data points by category,” ver. 2.0, Aug. 2026.

[8] Battery Pass Consortium, “Battery passport content guidance,” ver. 1.0, Apr. 2023.

[9] N. Carey, “Volvo to issue world's first EV battery passport ahead of EU rules,” Reuters, Jun. 2024.

[10] H. R. Hasan, K. Salah, A. Mayyas, A. Musamih, I. Yaqoob, M. Omar, and R. Jayaraman, “Using composable NFTs and blockchain for the creation of EV battery digital passports with sustainability and traceability features,” *Sustainable Futures*, vol. 10, Art. no. 100847, Dec. 2025, doi: 10.1016/j.sftr.2025.100847.

[11] J. Kanjere, M. Ford, and M. Louw, “BlockBaRT: Towards a blockchain-based battery passport with selective disclosure of verifiable data,” in *Proc. FDCR 2025*, pp. 15–23, 2025.

[12] A. Farhani, “Digital product passports and blockchain for sustainable lithium battery and EV supply chains: A unified framework,” *Preprints*, 2025, doi: 10.20944/preprints202509.2046.v1, unpublished.

[13] Automotive Research Association of India, “AIS-156 (Rev. 1) Amendment 3: Specific requirements for L category motor vehicles with electric power train,” MoRTH, 2022.

[14] EVreporter, “AIS 156 standard – additional safety requirements: Practitioner's perspective,” 2022.

[15] K. Berger, J.-P. Schöggl, and R. J. Baumgartner, “Digital battery passports to enable circular and sustainable value chains: Conceptualization and use cases,” *J. Cleaner Prod.*, vol. 353, Art. no. 131492, 2022.

[16] C. A. Rufino Júnior, E. Riva Sanseverino, P. Gallo, D. Koch, S. Diel, G. Walter, and H. Zanin, “Towards to battery digital passport: Reviewing regulations and standards for second-life batteries,” *Batteries*, vol. 10, no. 4, Art. no. 115, 2024.

[17] A. Butera and V. Gatteschi, “EU battery regulation and the role of blockchain in creating digital battery passports,” in *Proc. 6th Conf. Blockchain Res. Appl. Innov. Netw. Serv. (BRAINS)*, Berlin, 2024, doi: 10.1109/BRAINS63024.2024.10732126.

[18] B. Schneier and J. Kelsey, “Secure audit logs to support computer forensics,” *ACM Trans. Inf. Syst. Secur.*, vol. 1, no. 3, pp. 159–176, 1999.

[19] S. A. Crosby and D. S. Wallach, “Efficient data structures for tamper-evident logging,” in *Proc. 18th USENIX Security Symp.*, 2009, pp. 317–334.

[20] B. Laurie, A. Langley, and E. Kasper, “Certificate Transparency,” IETF RFC 6962, Jun. 2013.

[21] B. Laurie, E. Messeri, and R. Stradling, “Certificate Transparency version 2.0,” IETF RFC 9162, Dec. 2021.

[22] E. Syta *et al.*, “Keeping authorities ‘honest or bust’ with decentralized witness cosigning,” in *Proc. IEEE Symp. Security Privacy*, 2016, pp. 526–545.

[23] National Institute of Standards and Technology, “Digital signature standard (DSS),” FIPS 186-5, Feb. 2023.

[24] National Institute of Standards and Technology, “Secure hash standard (SHS),” FIPS 180-4, Aug. 2015.

[25] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[26] M. Castro and B. Liskov, “Practical Byzantine fault tolerance,” in *Proc. 3rd USENIX Symp. Operating Syst. Design Implement. (OSDI)*, 1999, pp. 173–186.

[27] J. Wang *et al.*, “Cycle-life model for graphite-$LiFePO_4$ cells,” *J. Power Sources*, vol. 196, no. 8, pp. 3942–3948, 2011.

[28] J. Schmalstieg, S. Käbitz, M. Ecker, and D. U. Sauer, “A holistic aging model for $Li(NiMnCo)O_2$ based 18650 lithium-ion batteries,” *J. Power Sources*, vol. 257, pp. 325–334, 2014.

[29] G. L. Plett, *Battery Management Systems, Vol. II: Equivalent-Circuit Methods*. Norwood, MA, USA: Artech House, 2015.

[30] V. Buterin and M. Swende, “EIP-2929: Gas cost increases for state access opcodes,” Ethereum Improvement Proposals, 2020; G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” Yellow Paper.

[31] K. A. Severson *et al.*, “Data-driven prediction of battery cycle life before capacity degradation,” *Nature Energy*, vol. 4, pp. 383–391, 2019.

[32] Microchip Technology, “ATECC608C CryptoAuthentication device summary data sheet,” 2023; unit price from Farnell distributor listing for ATECC608A-MAHDA-S, accessed Oct. 2026.