Proof of Travel (PoT)

Abstract

Proof of Travel (PoT) is a neutral, blockchain-based verification protocol designed to cryptographically record the issuance of real-world travel events.

The protocol operates alongside existing travel infrastructure—including travel agencies, consolidators, Global Distribution Systems (GDSs), airlines, and settlement frameworks—without altering booking, ticketing, or settlement workflows. PoT introduces an independent and tamper-resistant audit layer that enables verifiable confirmation that a travel event has occurred, based on post-issuance and post-reconciliation signals rather than speculative or pre-transaction claims.

PoT is intentionally designed as infrastructure rather than a consumer-facing product. It does not replace existing travel systems, act as a booking platform, or introduce passenger-facing financial instruments. Instead, it provides a cryptographic proof mechanism that can be referenced by participating systems, auditors, and third parties requiring reliable verification of travel activity.

The protocol supports a phased deployment model, beginning with controlled pilot integrations and expanding through conservative governance and clearly defined operational boundaries. A protocol-native utility mechanism may be used to account for verified participation within the network; however, PoT explicitly avoids speculative design assumptions and prioritizes operational correctness, regulatory awareness, and long-term system integrity.

Proof of Travel aims to establish a foundational verification layer for travel events, enabling greater transparency, auditability, and interoperability across the global travel ecosystem.

1. Problem Statement

Global travel infrastructure processes billions of travel events each year through a complex network of travel agencies, consolidators, Global Distribution Systems (GDSs), airlines, and settlement frameworks. While these systems are highly effective at booking, ticketing, and financial reconciliation, they are not designed to produce a neutral, cryptographically verifiable record that a specific real-world travel event has occurred.

Verification of travel activity today relies on fragmented data sources, proprietary system logs, and post hoc reconciliation processes. Confirmation that a travel event has been issued, reconciled, or flown typically requires access to internal systems, bilateral data sharing agreements, or manual audits. As a result, there is no independent, tamper-resistant mechanism that can be referenced across systems to verify travel events without relying on trust in a single party.

This limitation becomes increasingly significant as travel data is reused beyond its original transactional purpose. Auditors, insurers, corporate travel platforms, loyalty systems, compliance frameworks, and emerging digital services often require confirmation that a travel event occurred, yet they must rely on indirect attestations or delayed reporting. These verification gaps introduce operational friction, increase reconciliation costs, and limit interoperability between systems.

Existing blockchain applications in travel have largely focused on pre-transaction concepts, such as tokenized bookings, NFTs issued at purchase time, or consumer-facing loyalty instruments. These approaches introduce speculative assumptions and operational risk, as they attempt to represent future or contingent events rather than confirmed outcomes. In practice, travel infrastructure is conservative by necessity, and solutions that require changes to booking flows, settlement processes, or regulatory treatment face significant adoption barriers.

What is missing is a neutral verification layer that operates *after* a travel event has been issued and reconciled, integrates with existing systems without disruption, and produces a cryptographic proof that can be independently validated. Such a layer must avoid consumer-facing financialization, respect regulatory constraints, and align with the operational realities of global travel infrastructure.

Proof of Travel is designed to address this gap. By introducing a post-issuance, post-reconciliation verification mechanism, PoT enables reliable confirmation of real-world travel events without altering how travel is sold, settled, or delivered. The protocol focuses on verifiability rather than speculation, providing an infrastructure-level foundation that can be adopted incrementally and referenced across the travel ecosystem.

2. System Overview

Proof of Travel (PoT) is designed as a lightweight verification layer that operates alongside existing travel infrastructure rather than replacing or restructuring it. The protocol introduces a post-issuance, post-reconciliation mechanism for producing cryptographic proofs that a real-world travel event has occurred.

At a high level, PoT follows three core principles:

1. **Non-disruption** — Existing booking, ticketing, and settlement workflows remain unchanged.
2. **Post-event verification** — Proofs are generated only after verifiable operational signals exist.
3. **Separation of concerns** — Operational travel systems remain off-chain, while verification artifacts are anchored on-chain.

2.1 Actors and Roles

PoT interacts with established participants in the travel ecosystem without altering their responsibilities.

The primary actors include:

- **Travel Agency**
  Issues travel bookings and tickets using standard industry systems.
- **Consolidator / Operator**
  Aggregates ticketing activity, performs reconciliation, and maintains operational oversight. In pilot deployments, this role may also act as the initial protocol operator.
- **Global Distribution System (GDS)**
  Provides authoritative booking and ticketing records used as one of the verification signals.
- **Airline**
  Issues and fulfils travel services and participates indirectly through existing settlement and reporting frameworks.
- **Settlement Frameworks (e.g., BSP)**
  Provide post-issuance reconciliation data that confirms financial and operational validity of issued tickets.
- **Proof of Travel Protocol**
  Consumes verification signals and produces a cryptographic proof representing the confirmed occurrence of a travel event.

Importantly, no single actor is required to trust the protocol blindly. PoT is designed to rely on corroborating signals from established systems rather than self-attested claims.

2.2 Verification Flow (Conceptual)

A typical Proof of Travel verification flow proceeds as follows:

1. A travel event is issued through standard industry processes (e.g., ticket issuance by an agency via a GDS).
2. The event progresses through normal operational and settlement workflows.
3. One or more independent verification signals become available (e.g., post-issuance confirmation, settlement reconciliation, system-level matches).
4. These signals are evaluated according to predefined verification rules.
5. Once verification conditions are met, a Proof of Travel record is generated.
6. A cryptographic representation of this record is anchored to a blockchain network.

The protocol does not assert or predict future outcomes. It records verifiable facts derived from completed operational processes.

2.3 On-Chain and Off-Chain Separation

PoT deliberately separates operational data handling from cryptographic anchoring.

- **Off-chain components** handle:
    - Travel booking data
    - Ticket identifiers
    - Reconciliation signals
    - Verification logic
- **On-chain components** handle:
    - Immutable proof anchoring
    - Timestamping
    - Verification reference hashes
    - Protocol-level accounting mechanisms

This separation ensures that sensitive travel data remains within existing systems and regulatory boundaries, while the blockchain is used strictly for integrity, immutability, and independent verification.

2.4 Protocol Utility Mechanism (High-Level)

PoT may employ a protocol-native utility mechanism to account for verified participation within the network. This mechanism is designed to reflect confirmed verification activity rather than speculative or pre-transaction behaviour.

Any such mechanism operates at the protocol level and is not exposed to passengers or required for participation by travel agencies. Its purpose is to support protocol operations, governance, and accounting, rather than to introduce consumer-facing financial instruments.

Details of this mechanism are intentionally constrained during early deployments and may evolve through conservative governance processes as the protocol matures.

2.5 Deployment Model

Proof of Travel follows a phased deployment approach:

- **Pilot Phase**
  Limited integrations with selected operators, controlled verification rules, and conservative issuance parameters.
- **Expansion Phase**
  Additional participants, broader verification criteria, and increased interoperability.
- **Mature Phase**
  Independent validation, standardized verification references, and wider ecosystem adoption.

At each stage, protocol changes are governed to prioritize correctness, regulatory awareness, and operational stability over speed of expansion.

---

3. Trust and Verification Model

Proof of Travel (PoT) is built on the principle that verification of real-world travel events should not depend on trust in a single system, organisation, or data source. Instead, the protocol relies on corroboration across independent operational signals that already exist within the global travel ecosystem.

The PoT trust model is designed to minimise new trust assumptions while maximising verifiability. It does not seek to replace existing authorities, but to reference them in a structured and transparent manner.

3.1 Design Principles

The verification model of PoT is guided by the following principles:

- **No single point of trust**
  No individual actor or system can unilaterally assert that a travel event has occurred.

- **Post-event confirmation**
  Verification is based on completed operational processes rather than future intent or provisional states.
- **Independent corroboration**
  Proofs are derived from multiple signals that originate from distinct systems with different incentives and failure modes.
- **Auditability over prediction**
  The protocol prioritises verifiable historical accuracy over real-time or speculative claims.

3.2 Verification Signals

A *verification signal* is an objective data point generated by an established travel system that indicates a travel event has progressed through a recognised operational stage.

Examples of verification signals include, but are not limited to:

- Ticket issuance records generated through a Global Distribution System (GDS)
- Post-issuance status confirmations within agency or consolidator systems
- Settlement and reconciliation data from frameworks such as BSP
- System-level consistency checks across independent operational databases

Verification signals are consumed off-chain and evaluated according to predefined rules. Sensitive or personally identifiable data is not published on-chain as part of the verification process.

3.3 Multi-Signal Verification Thresholds

PoT does not treat any single verification signal as sufficient proof. Instead, the protocol applies configurable *verification thresholds* that require agreement across multiple independent signals.

A typical threshold may require confirmation from at least two distinct sources, for example:

- Settlement reconciliation **and**
- GDS issuance consistency

These thresholds are intentionally conservative and may vary depending on deployment phase, participant maturity, and regulatory context.

The use of multi-signal thresholds reduces the risk of false positives, unilateral assertions, or manipulation by any single participant.

3.4 Neutrality and Independence

PoT is designed to remain neutral with respect to commercial relationships, transaction flows, and commercial incentives.

The protocol does not privilege:

- a specific GDS,
- a specific airline,
- a specific agency,
- or a specific operator.

Verification outcomes are derived from corroboration across systems rather than endorsement by a single authority. This neutrality is essential to enable broad adoption and to prevent the protocol from becoming an extension of any one commercial platform.

3.5 Failure Modes and Non-Verification

The absence of a Proof of Travel record does not imply that a travel event did not occur. It simply indicates that the verification thresholds required by the protocol were not met.

Reasons for non-verification may include:

- incomplete reconciliation data,
- delayed settlement cycles,
- unavailable verification signals,
- or conservative threshold configurations.

PoT explicitly avoids producing probabilistic or speculative proofs. When sufficient verification signals are not present, the protocol produces no proof rather than an unreliable one.

3.6 Trust Minimisation

By anchoring verification outcomes to cryptographic proofs rather than institutional trust alone, PoT reduces reliance on opaque attestations and bilateral trust agreements.

Participants can independently validate that:

- a verification record exists,
- it was produced according to defined rules,
- and it has not been altered after publication.

This approach supports transparency and auditability without requiring participants to disclose sensitive operational data or relinquish control of their systems.

4. Protocol Architecture

Proof of Travel (PoT) is architected as a layered verification system that separates operational travel processes from cryptographic proof anchoring. This design ensures that existing travel infrastructure remains unchanged, while the protocol provides an independent, immutable verification reference.

The architecture is intentionally minimal, focusing on integrity, traceability, and auditability rather than transaction execution or data storage.

4.1 Architectural Overview

At a high level, PoT consists of three primary architectural layers:

1. **Operational Layer (Off-Chain)**
   Existing travel systems where bookings, ticket issuance, and reconciliation occur.
2. **Verification Layer (Off-Chain)**
   Logic that evaluates verification signals and determines whether proof conditions are met.
3. **Anchoring Layer (On-Chain)**
   A blockchain-based layer that records immutable references to verified travel events.

This separation allows PoT to integrate with conservative, regulated travel systems while leveraging blockchain strictly for its strengths: immutability, timestamping, and independent verification.

4.2 Operational Layer (Off-Chain)

The operational layer includes all existing systems involved in travel issuance and settlement, such as:

- travel agency and consolidator systems,
- Global Distribution Systems (GDSs),
- airline reporting and fulfilment systems,
- settlement and reconciliation frameworks.

PoT does not ingest or store full operational records on-chain. Instead, it consumes derived verification signals produced by these systems after standard operational processes have completed.

All sensitive, personally identifiable, or commercially confidential data remains within existing operational environments and under existing regulatory controls.

4.3 Verification Layer (Off-Chain)

The verification layer is responsible for:

- collecting verification signals from independent sources,
- evaluating those signals against predefined verification rules,
- determining whether a Proof of Travel record may be generated.

Verification logic is executed off-chain to allow flexibility, configurability, and compliance with operational constraints. This layer may be operated by a designated protocol operator during early deployments and expanded to additional validators as the protocol matures.

Verification rules are deterministic and auditable, ensuring that identical inputs produce identical verification outcomes.

4.4 Proof Object Structure

When verification thresholds are met, PoT produces a *proof object* representing the confirmed occurrence of a travel event.

A proof object typically includes:

- a unique proof identifier,
- cryptographic hashes derived from verification inputs,
- a timestamp indicating proof creation,
- references to the verification rule set applied.

The proof object does not contain raw travel data. Instead, it provides a cryptographic fingerprint that can be independently validated without exposing underlying operational information.

4.5 Anchoring Layer (On-Chain)

The anchoring layer records proof object references on a blockchain network. Its responsibilities include:

- immutably recording proof hashes,
- providing public timestamping,
- enabling independent verification of proof existence and integrity.

The blockchain is not used to execute travel logic, store travel records, or mediate commercial transactions. Its role is strictly limited to anchoring and verification.

By keeping on-chain interactions minimal, PoT reduces operational costs, limits attack surface, and avoids unnecessary complexity.

4.6 Protocol Accounting (High-Level)

PoT may incorporate a protocol-level accounting mechanism to track verified activity within the network. This mechanism is logically separate from proof generation and does not affect verification outcomes.

Protocol accounting may support:

- operational cost allocation,
- governance processes,
- and long-term protocol sustainability.

Details of this mechanism are intentionally abstracted in early phases and subject to conservative governance controls.

4.7 Extensibility and Evolution

The architecture of PoT is designed to evolve incrementally without disrupting existing integrations.

Future extensions may include:

- additional verification signal sources,
- independent verification operators,
- enhanced governance structures,
- interoperability with external systems that consume proof references.

All extensions are intended to preserve the core architectural principles of non-disruption, neutrality, and verifiability.

---

5. Security and Integrity Considerations

Proof of Travel (PoT) is designed with a security model that reflects the realities of real-world travel infrastructure. The protocol does not attempt to eliminate all risk, nor does it assume adversarial behaviour beyond what is realistic for established industry participants. Instead, PoT focuses on integrity, auditability, and resistance to tampering through layered verification and conservative architectural choices.

5.1 Threat Model

The PoT security model considers the following classes of risk:

- **Data manipulation or unilateral assertion**
  Attempts by a single participant to falsely assert that a travel event has occurred.
- **Post-hoc alteration of records**
  Modification of verification records after a travel event has been issued or reconciled.

- **System inconsistencies or operational errors**
  Divergent data states across operational systems due to delays, reconciliation cycles, or system faults.
- **Misinterpretation of verification results**
  Incorrect assumptions about what a proof represents or guarantees.

PoT explicitly does not attempt to defend against hypothetical nation-state adversaries or systemic compromise of multiple independent travel systems simultaneously.

5.2 Integrity Through Corroboration

The primary security property of PoT arises from corroboration across independent verification signals.

By requiring agreement between multiple systems with different incentives and operational controls, PoT reduces the likelihood that false or manipulated data can produce a valid proof. This approach mirrors established audit and reconciliation practices within the travel industry, augmented with cryptographic anchoring.

No single verification signal is treated as authoritative in isolation.

5.3 Cryptographic Anchoring and Immutability

Once a proof object is generated, its cryptographic representation is anchored to a blockchain network. This provides:

- an immutable timestamped record,
- resistance to post-publication modification,
- independent verifiability without reliance on the protocol operator.

The blockchain is used strictly as an integrity layer. The protocol does not depend on smart contract execution for security-critical decision-making, reducing exposure to common blockchain-specific attack vectors.

5.4 Off-Chain Security Considerations

Because verification logic and signal evaluation occur off-chain, PoT places emphasis on operational security practices, including:

- access controls on verification systems,
- audit logging of verification decisions,
- separation of duties within operator environments,
- retention of verification inputs for post-event audit.

These measures align with standard enterprise security practices and can be adapted to jurisdictional and organisational requirements.

5.5 Failure Handling and Conservative Defaults

PoT is intentionally biased toward non-verification rather than false verification.

If verification signals are incomplete, inconsistent, or delayed, the protocol produces no proof rather than a partial or probabilistic result. This conservative default reduces the risk of incorrect assertions and reinforces trust in verified outcomes.

The absence of a proof must not be interpreted as evidence that a travel event did not occur.

5.6 Scope and Limitations

PoT provides cryptographic verification that a defined set of conditions were met at a specific point in time. It does not guarantee:

- that a passenger travelled,
- that services were fully consumed,
- or that downstream obligations were fulfilled.

The protocol verifies *issuance and reconciliation conditions*, not physical movement or passenger behaviour. These limitations are explicit and intentional, and they preserve clarity about what PoT does and does not represent.

---

6. Governance and Control Model

Proof of Travel (PoT) adopts a conservative governance model that prioritises operational correctness, accountability, and regulatory awareness over premature decentralisation. The protocol is designed to evolve through clearly defined governance stages, with explicit control boundaries at each phase.

Governance within PoT determines how verification rules are defined, how protocol parameters may change, and who is authorised to operate verification and anchoring components.

6.1 Governance Principles

PoT governance is guided by the following principles:

- **Accountability over anonymity**
  Protocol operation and rule changes are attributable to identifiable entities.
- **Stability over rapid change**
  Verification logic and thresholds are modified conservatively to preserve trust and continuity.

- **Transparency over opacity**
  Governance decisions and rule definitions are documented and auditable.
- **Incremental decentralisation**
  Control may be distributed over time, but only where it enhances resilience without compromising operational integrity.

6.2 Operator-Led Governance (Early Phases)

During initial deployments, PoT operates under an **operator-led governance model**.

Under this model:

- A designated protocol operator manages verification infrastructure.
- Verification rules and thresholds are defined and maintained centrally.
- On-chain anchoring keys and operational credentials are controlled by the operator.
- Governance decisions are documented and published alongside protocol documentation.

This approach reflects the realities of integrating with regulated travel infrastructure and allows the protocol to mature in a controlled environment.

6.3 Verification Rule Management

Verification rules define:

- acceptable verification signals,
- required thresholds,
- and conditions under which proofs may be generated.

Changes to verification rules are:

- versioned,
- documented,
- and applied prospectively rather than retroactively.

Historical proofs remain valid under the rule sets that were active at the time of their creation, preserving auditability and preventing reinterpretation of past records.

6.4 Governance Evolution

As the protocol matures, governance may evolve to include:

- multiple independent verification operators,
- shared control over verification thresholds,
- advisory input from industry participants.

Any transition toward broader governance is intended to be gradual and opt-in, based on demonstrated operational stability and ecosystem demand. PoT explicitly avoids assuming that decentralisation is inherently beneficial in early phases.

6.5 Separation of Governance and Verification Outcomes

Governance authority does not grant the ability to retroactively alter verification outcomes.

Once a proof has been generated and anchored, it cannot be modified or revoked through governance actions. Governance influences future protocol behaviour only, not historical records.

This separation protects the integrity of the verification layer from administrative or political interference.

6.6 Governance Transparency

Governance policies, rule definitions, and material changes are made publicly available through protocol documentation. This transparency allows participants and third parties to understand:

- how proofs are generated,
- under what conditions they are valid,
- and how protocol behaviour may evolve.

Transparency is essential to establishing PoT as a neutral and trustworthy verification layer.

7. Protocol Lifecycle and Deployment Phases

Proof of Travel (PoT) is designed to evolve through clearly defined lifecycle phases that prioritise correctness, stability, and real-world integration over speed or speculative growth. Each phase introduces additional capabilities only after operational assumptions have been validated.

The protocol lifecycle reflects the conservative requirements of global travel infrastructure and acknowledges that trust is earned through demonstrated reliability rather than early scale.

7.1 Phase One: Pilot Deployment

The pilot phase focuses on validating core protocol assumptions in a controlled environment.

Key characteristics of this phase include:

- integration with a limited number of operators,
- conservative verification thresholds,
- manual or semi-automated verification oversight,
- and minimal protocol-level accounting activity.

During this phase, PoT is used to generate proofs for selected batches of travel events following post-issuance and post-reconciliation confirmation. Proof generation frequency, thresholds, and operational processes are intentionally constrained to reduce risk and enable detailed review.

The objective of the pilot phase is not scale, but correctness.

7.2 Phase Two: Controlled Expansion

Following successful pilot validation, PoT may enter a controlled expansion phase.

This phase may include:

- onboarding of additional operators or consolidators,
- broader verification signal coverage,
- increased automation of verification workflows,
- refinement of protocol accounting mechanisms.

Expansion is incremental and conditional. New participants are introduced only when operational stability and verification accuracy have been demonstrated under existing conditions.

At no stage is rapid growth prioritised over integrity or auditability.

7.3 Phase Three: Mature Operation

In the mature phase, PoT operates as a stable verification layer referenced by multiple independent participants.

Characteristics of this phase include:

- standardised verification rulesets,
- multiple verification operators,
- transparent governance processes,
- and broader ecosystem interoperability.

Even at maturity, PoT remains intentionally limited in scope. The protocol continues to focus on verification and integrity rather than transaction execution, settlement, or consumer-facing functionality.

7.4 Change Management and Backward Compatibility

Protocol changes are managed through versioned documentation and prospective application.

Key principles include:

- no retroactive alteration of existing proofs,
- clear documentation of rule changes,
- advance notice for material protocol updates,
- preservation of historical verification semantics.

These principles ensure that proofs generated under earlier protocol versions remain interpretable and auditable over time.

7.5 Exit and Deactivation Considerations

PoT explicitly recognises that protocol participation may change over time.

Operators may:

- suspend proof generation,
- reduce verification scope,
- or withdraw from protocol operation.

Such changes do not invalidate previously generated proofs. Historical verification records remain accessible and verifiable independent of ongoing protocol activity.

This approach reinforces PoT's role as a verification record rather than an ongoing service dependency.

---

8. Legal and Regulatory Considerations

Proof of Travel (PoT) is designed as a technical verification protocol rather than a consumer-facing service, financial product, or booking platform. The protocol's scope and functionality are intentionally constrained to reduce regulatory exposure and to align with existing legal and operational frameworks within the global travel industry.

This section outlines key legal and regulatory considerations relevant to the protocol's design and deployment. It does not constitute legal advice.

8.1 Non-Financial Nature of the Protocol

PoT does not provide financial services, facilitate payments, or act as an intermediary for the sale of travel services. The protocol does not set prices, process transactions, or interact directly with passengers.

Any protocol-native utility mechanism is designed solely for operational accounting, governance, or protocol sustainability purposes. It is not intended to function as an investment product, security, or store of value.

8.2 Data Protection and Privacy

PoT is architected to minimise data exposure and privacy risk.

- No personally identifiable travel data is recorded on-chain.
- Sensitive operational data remains within existing travel systems and under existing regulatory controls.
- On-chain records consist only of cryptographic references and metadata that cannot be reverse-engineered to reveal personal information.

This design supports compliance with data protection frameworks such as GDPR and other jurisdiction-specific privacy regulations.

8.3 Jurisdictional Deployment Considerations

PoT may be operated and referenced across multiple jurisdictions. The protocol is designed to be jurisdiction-agnostic at the technical level while allowing operational controls to be adapted locally.

Participation by entities in jurisdictions with restrictions on digital assets or token usage does not require direct interaction with protocol-native utility mechanisms. Such entities may consume verification outputs without holding, transacting, or promoting digital tokens.

8.4 No Solicitation or Offering

PoT documentation, software, and protocol outputs are provided for informational and operational purposes only.

Nothing within the protocol or its documentation constitutes:

- an offer or solicitation of investment,
- a recommendation to purchase or sell digital assets,
- or a promise of economic return.

Any participation in protocol-related mechanisms is voluntary and subject to applicable laws and internal compliance requirements of participating entities.

8.5 Regulatory Engagement and Evolution

PoT acknowledges that regulatory frameworks governing digital systems and blockchain technologies continue to evolve.

The protocol's governance model allows for adaptation in response to regulatory guidance, legal requirements, or industry standards. Where necessary, protocol features may be constrained, modified, or suspended to maintain compliance without compromising historical verification records.

---

9. Conclusion

Proof of Travel (PoT) is designed as a foundational verification protocol for real-world travel events. By introducing a neutral, cryptographically anchored proof mechanism that operates alongside existing travel infrastructure, PoT addresses a longstanding gap in the ability to independently verify travel activity without disrupting established systems or workflows.

The protocol's design reflects the operational realities of the global travel industry. It prioritises post-issuance and post-reconciliation verification, conservative trust assumptions, and clear separation between operational data and cryptographic integrity. PoT does not seek to replace booking, settlement, or fulfilment systems, nor does it introduce consumer-facing financial instruments or speculative mechanisms.

Through a phased deployment model, explicit governance boundaries, and an intentionally constrained scope, PoT aims to earn trust through demonstrated correctness rather than rapid expansion. Its role is to provide an auditable, tamper-resistant reference layer that can be adopted incrementally and referenced by participating systems, auditors, and third parties requiring reliable confirmation of travel events.

As global travel infrastructure continues to evolve and travel data is increasingly reused beyond its original transactional context, the need for neutral verification mechanisms becomes more pronounced. Proof of Travel is positioned to serve as such a mechanism—quietly, conservatively, and in alignment with the regulatory and operational frameworks that underpin the travel ecosystem.

Appendix A

Protocol Utility and Accounting Mechanism (v1.0)

This appendix describes the protocol-native utility and accounting mechanism used within Proof of Travel (PoT). The purpose of this section is to document operational mechanics relevant to protocol operation and governance, without introducing speculative assumptions or economic guarantees.

The mechanism described here is intentionally constrained and may evolve through conservative governance processes as the protocol matures.

A.1 Purpose and Scope

The Proof of Travel protocol may employ a protocol-native utility unit to support internal accounting, operational coordination, and governance processes.

This utility mechanism is designed to:

- represent verified participation within the protocol,
- support operational cost allocation and sustainability,
- enable governance-related functions where appropriate.

The mechanism is **not** designed to function as a consumer-facing instrument, payment method, investment product, or store of value.

A.2 Relationship to Verification

The generation of Proof of Travel records is independent of the protocol utility mechanism.

Verification outcomes are determined solely by the evaluation of verification signals and defined thresholds. The presence or absence of protocol utility units does not influence whether a proof is generated.

This separation ensures that verification integrity is preserved regardless of accounting or governance considerations.

A.3 Issuance Principles

Protocol utility units may be issued in response to verified protocol activity.

Issuance principles include:

- **Event linkage**
  Issuance may be associated with confirmed verification outcomes rather than speculative or pre-transaction events.
- **Conservative parameters**
  Issuance quantities and frequency are intentionally constrained during early deployment phases.
- **Operator control (early phases)**
  During pilot deployments, issuance is managed by the designated protocol operator under documented governance rules.

The protocol does not require issuance to occur for every verified event, and issuance may be suspended or adjusted without affecting verification functionality.

A.4 Distribution and Access

Protocol utility units are intended for use by protocol operators and participants interacting with the verification layer.

They are not required for:

- travel agencies issuing tickets,
- airlines fulfilling travel services,
- passengers,
- or entities consuming verification outputs in a read-only capacity.

Entities operating in jurisdictions with restrictions on digital assets may participate in PoT without holding or transacting protocol utility units.

A.5 Governance and Accounting Use

The protocol utility mechanism may support governance and accounting functions, including:

- tracking verified protocol activity,
- allocating operational costs,
- supporting governance decisions where applicable.

Governance authority does not permit retroactive modification of verification records, and accounting mechanisms do not affect historical proofs.

A.6 Supply Characteristics (v1.0)

During early protocol phases:

- total supply parameters are intentionally flexible,
- issuance is event-linked and operator-governed,
- long-term economic characteristics are explicitly undefined.

This approach avoids premature optimisation and allows protocol parameters to be informed by real operational data rather than theoretical assumptions.

A.7 Non-Goals and Explicit Exclusions

The protocol utility mechanism is explicitly **not** intended to:

- provide financial returns,

- enable yield, staking, or profit-sharing schemes,
- act as a medium of exchange for consumer transactions,
- replace existing settlement or payment systems,
- or incentivise speculative behaviour.

Any future changes to the scope or function of the mechanism would be subject to documented governance processes and regulatory considerations.

A.8 Evolution and Amendments

This appendix may be amended in future protocol versions to reflect:

- operational learnings,
- regulatory guidance,
- governance evolution,
- or changes in protocol maturity.

Amendments apply prospectively and do not alter the interpretation of historical verification records.