GalacticQB Lightpaper

A Quantum-Safe Trust Infrastructure for Space, Defence and Critical Systems

Document Version: 1.0
Date: 10th March 2026
Classification: Public
Next Review: N/A

About This Lightpaper

This document is a lightpaper — a concise, accessible overview of a technology, product, or concept designed to give readers a clear top-level understanding without delving into deep technical implementation detail.

Lightpapers are intended for a broad audience, including technical and non-technical stakeholders, prospective partners, investors, and decision-makers who need to understand the strategic purpose, capabilities, and relevance of a solution. They sit between a marketing one-pager and a full technical white paper: substantive enough to convey real value, accessible enough to be read without specialist expertise.

For clients and partners requiring deeper technical documentation — including integration guides, runtime specifications, attestation protocols, and compliance frameworks — Pan Galactic provides dedicated technical materials upon request and under appropriate confidentiality agreements.

Executive Summary

Modern digital systems increasingly rely on distributed infrastructure. Satellites, ground networks, data processing platforms and autonomous systems exchange large volumes of data across multiple organisations and jurisdictions.

In these environments, trust becomes one of the most difficult problems to solve. Operators must be able to confirm that data is authentic, that software has not been tampered with and that mission systems are operating according to approved configurations.

Traditional centralised systems struggle to provide verifiable trust across distributed networks, particularly where multiple organisations are involved.

GalacticQB is Pan Galactic's quantum-safe blockchain infrastructure designed to provide a verifiable trust layer for critical systems operating in space, defence and edge environments.

Rather than focusing on cryptocurrency or speculative finance, GalacticQB is designed to support data integrity, software provenance and secure infrastructure coordination across distributed mission systems.

The Problem

Critical infrastructure increasingly operates across complex distributed networks.

Examples include:

- satellite constellations
- ground station networks
- defence communications infrastructure
- autonomous sensor networks

In these environments, organisations must share data and coordinate software systems while maintaining strong security guarantees.

Several key challenges arise.

1) Data integrity

Operators must confirm that data has not been modified or manipulated during transmission or processing.

2) Software provenance

Mission systems must verify that software components originate from trusted sources and have not been altered.

3) System coordination

Distributed systems often require multiple organisations to interact securely without relying on a single central authority.

Traditional centralised systems create a single point of failure and are often difficult to audit.

These challenges become even more significant as quantum computing threatens existing cryptographic infrastructure.

The Pan Galactic Solution

GalacticQB provides a distributed trust infrastructure designed specifically for mission-critical systems.

It uses a permissioned blockchain architecture combined with post-quantum cryptography to create tamper-resistant records of data, software and system events.

The platform enables organisations to verify:

- the origin of software and system components
- the integrity of operational data
- the execution of mission software
- the identity of participating systems

Unlike public blockchains used for financial speculation, GalacticQB is designed for high-assurance operational environments where performance, security and governance are essential.

How the Technology Works

GalacticQB operates as a permissioned distributed ledger with known and verified validator nodes.

This architecture allows the system to maintain strong security guarantees while avoiding the high energy consumption and unpredictability associated with public proof-of-work networks.

Permissioned Validator Network

Validators are trusted infrastructure operators within the network.

These may include:

- space operators
- ground infrastructure providers
- defence organisations
- trusted technology partners

Each validator maintains a copy of the distributed ledger and participates in validating transactions and records.

This creates a shared and verifiable history of system activity.

Post-Quantum Cryptographic Security

GalacticQB integrates post-quantum cryptographic algorithms through the GalacticQSL library.

This allows the network to remain secure against future quantum computing threats.

Cryptographic capabilities include:

- post-quantum key exchange mechanisms
- quantum-resistant digital signatures
- secure hashing and data integrity verification

By integrating PQC directly into the network infrastructure, GalacticQB supports the long-term security requirements of government and defence operators.

Verifiable Metadata Records

GalacticQB does not store large files or software packages directly on the blockchain.

Instead it records verifiable metadata related to system activity.

Examples include:

- software image hashes
- container deployment records
- system attestation proofs
- data integrity records
- developer identities and signing keys

These records provide a tamper-resistant audit trail for software supply chains and operational systems.

Infrastructure Coordination

The distributed ledger allows multiple organisations to coordinate secure operations without relying on a central authority.

This can support several functions:

verifying software deployment across distributed systems
coordinating data exchange between organisations
tracking system state across large infrastructure networks

This architecture is particularly valuable in multi-organisation environments such as international space missions or defence collaborations.

Standards and Compliance Alignment

GalacticQB is designed to align with emerging standards for distributed infrastructure and cryptographic security.

Relevant frameworks include:

- NIST post-quantum cryptography standards
- ISO cybersecurity and information assurance standards
- UK National Cyber Security Centre guidance
- ECSS security frameworks for space systems
- ETSI distributed ledger standards
- 3GPP telecommunications security frameworks

The platform also supports the principle of crypto-agility, allowing cryptographic algorithms to evolve as standards develop.

Deployment Environments and Use Cases

GalacticQB can support a range of operational environments.

Space Infrastructure

- satellite constellations
- orbital compute platforms
- inter-satellite communications networks

The system can provide verifiable data provenance across distributed orbital systems.

Ground Infrastructure

- ground station networks
- mission operations systems
- space data processing platforms

GalacticQB can record software deployments and system events across mission infrastructure.

Defence and Government Systems

- secure communications networks
- autonomous systems coordination
- multi-organisation mission environments

The distributed trust model allows multiple organisations to interact while maintaining verifiable records of activity.

Why It Matters

As critical infrastructure becomes more distributed and software-driven, trust must be built directly into the system architecture.

Operators need to verify not only the security of communications but also the authenticity of software and the integrity of operational data.

GalacticQB provides a distributed trust layer that enables organisations to confirm that systems are operating as expected and that critical data has not been manipulated.

By integrating post-quantum cryptography and permissioned governance, the platform is designed to support the long-term security requirements of space and defence infrastructure.

How It Fits Into the Pan Galactic Ecosystem

GalacticQB forms the trust and provenance layer of the Pan Galactic platform.

It interacts with the other components of the system stack.

GalacticQSL provides the cryptographic primitives used for identity, signatures and key exchange.

Galactic Secure Containers provide secure packaging and deployment of applications.

GalacticOS provides the secure runtime environment in which these systems operate.

Together these components create a unified architecture for building secure distributed infrastructure capable of supporting space systems, defence platforms and other mission-critical environments.

Contact

For guidance on this document:
flow@pangalactic.io