



QuantumLink

PRODUCT WHITEPAPER

Privacy-First. Open-Source. Future-Proof.

QuantumLink is a product of Dytallix, Inc. Please visit www.dytallix.com for more information.

The promise in one page

QuantumLink is a private-connectivity substrate for people and teams that want direct reachability without placing a conventional VPN operator in the middle of every session.

DOCUMENT STATUS

This paper reflects the current status of QuantumLink as of August 2026. The general architecture is expected to remain consistent, but implementation details may change before or after beta testing. Consult github.com/exocognosis/QuantumLink for the latest implementation status.

Identity on-chain. Traffic off-chain.

Peers prove who they are before joining a public mesh. Packet data, routes, DNS, endpoints, and session keys remain outside the blockchain and flow over encrypted direct or relay-assisted paths.

WHAT CHANGES

FROM

- Provider accounts
- Central gateway
- Opaque trust

TO

- Local key identity
- Direct mesh paths
- Inspectable protocol

RESULT

- Less concentrated trust
- Fewer stored records
- Clearer peer assurance

INSIDE THIS PAPER

01 The trust problem

03 How a connection works

05 Value by audience

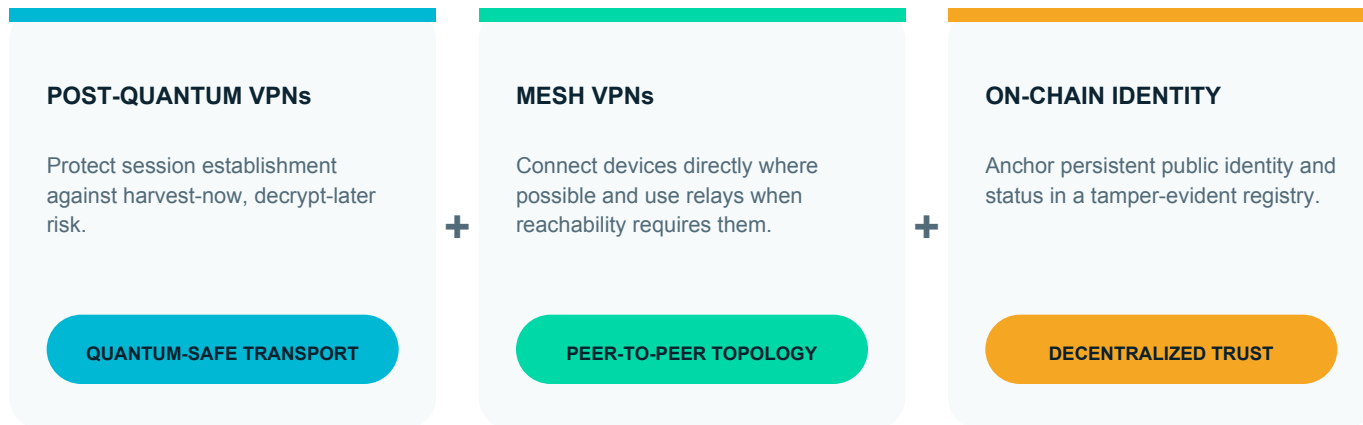
02 The product model

04 Privacy by design

06 Platforms & operations

The opportunity is at the intersection

The VPN market already contains post-quantum protection and peer-to-peer mesh products. QuantumLink's differentiation is to combine both with a decentralized identity layer that stays separate from the traffic path.



QUANTUMLINK CATEGORY

PQC-native mesh VPN

with on-chain identity; traffic kept off-chain

The registry answers “is this peer authorized and active?” The mesh answers “how do we reach it?” The encrypted session answers “how do we protect traffic?” Keeping those responsibilities separate prevents blockchain identity from becoming blockchain surveillance.

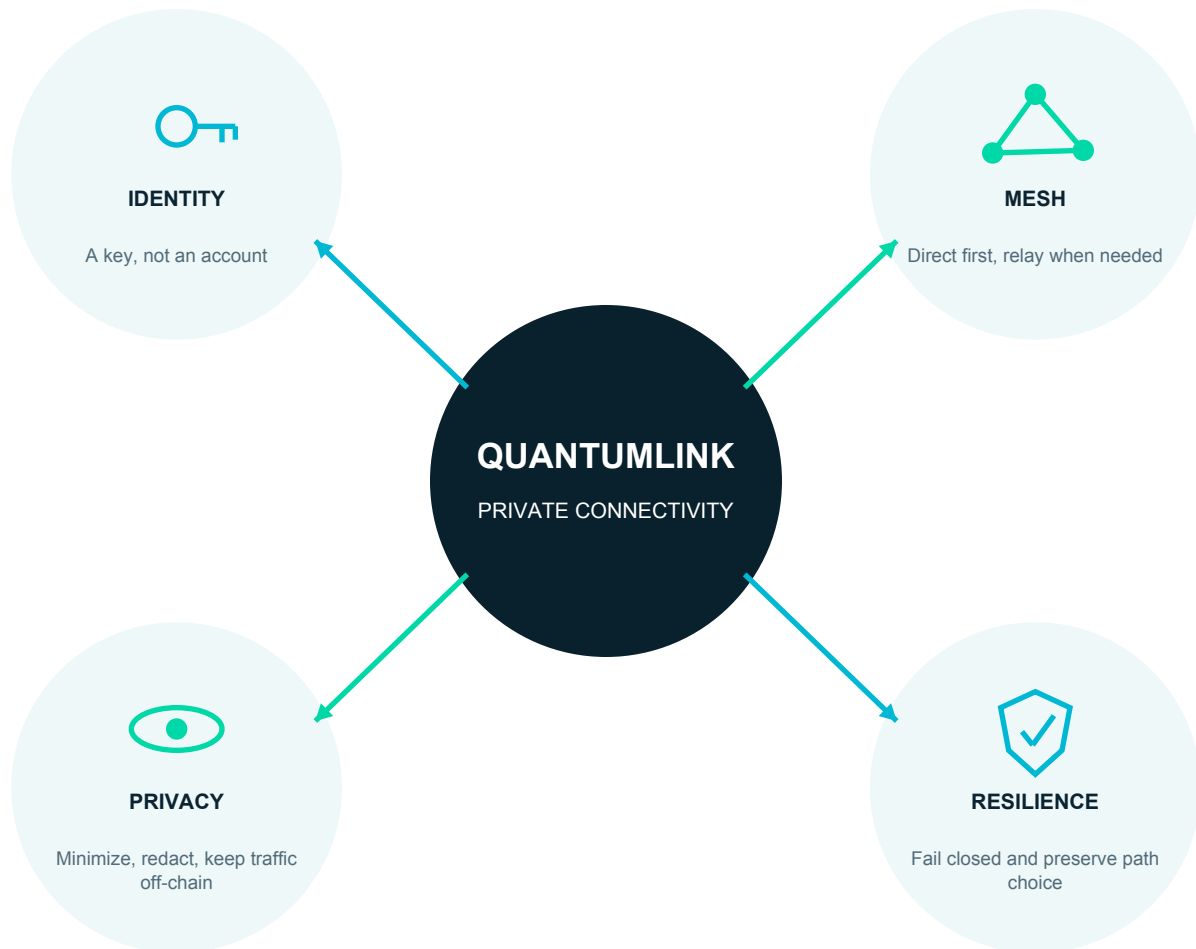
CATEGORY EVIDENCE

Official product materials demonstrate the adjacent categories: NordVPN describes post-quantum encryption across its VPN applications; Tailscale describes a peer-to-peer mesh VPN with direct and relayed connections. QuantumLink's website positions the product at the combined intersection with a distinct Dytallix identity layer.

Market examples: Nord Security, “NordVPN launches post-quantum encryption across all its applications” (2025); Tailscale, “Understanding Mesh VPNs” (accessed August 2026). Category statement: QuantumLinkVPN.com.

Four design commitments

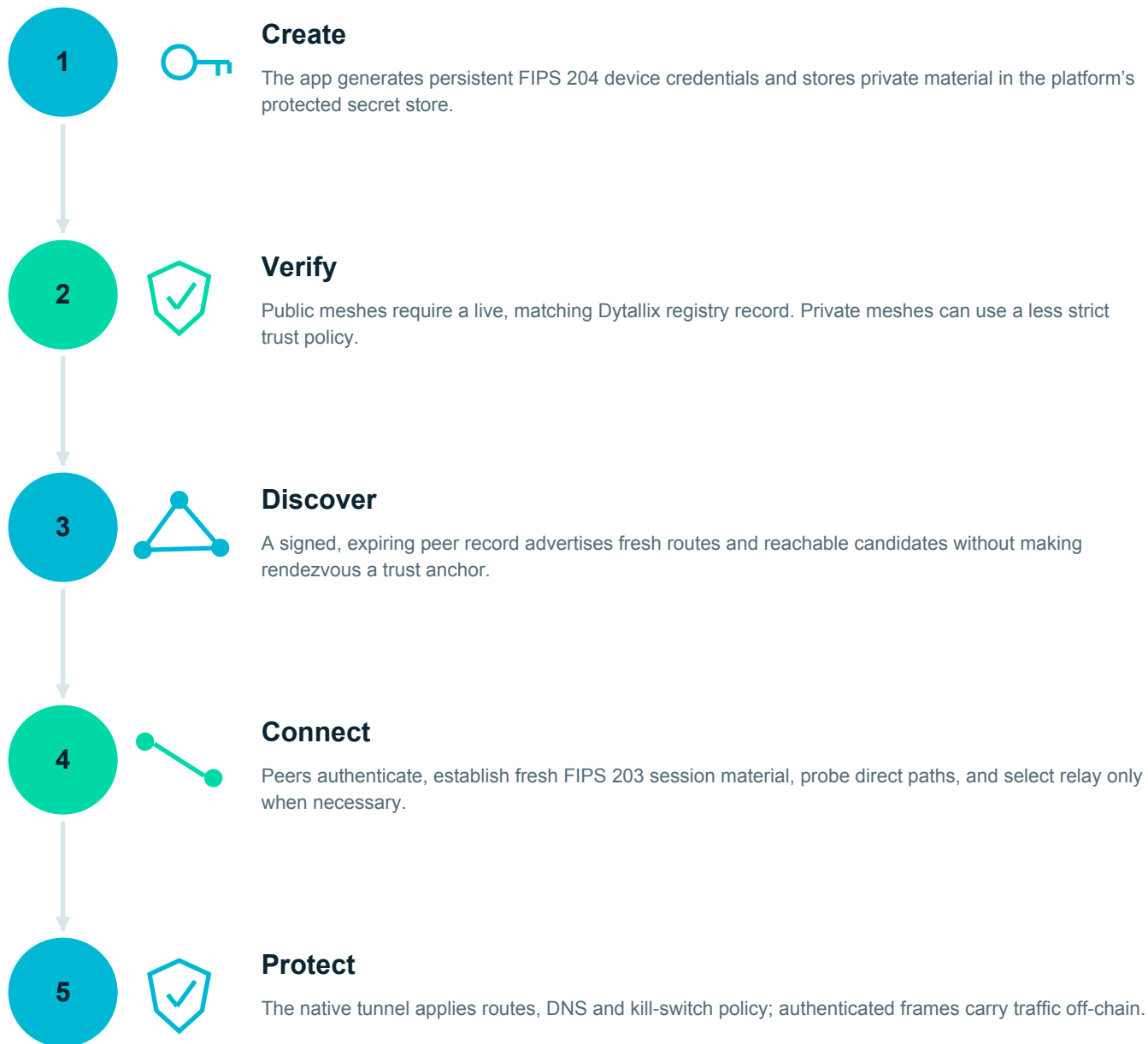
QuantumLink combines cryptographic identity, a server-minimized mesh, post-quantum session establishment, and native operating-system controls into one coherent product.



A single shared Rust protocol core owns session cryptography, signed peer records, packet framing, replay protection, trust decisions, discovery, relay coordination, metrics, and tracing. Native applications add the tunnel, user experience, platform security, privileges, and release mechanics.

From first launch to private path

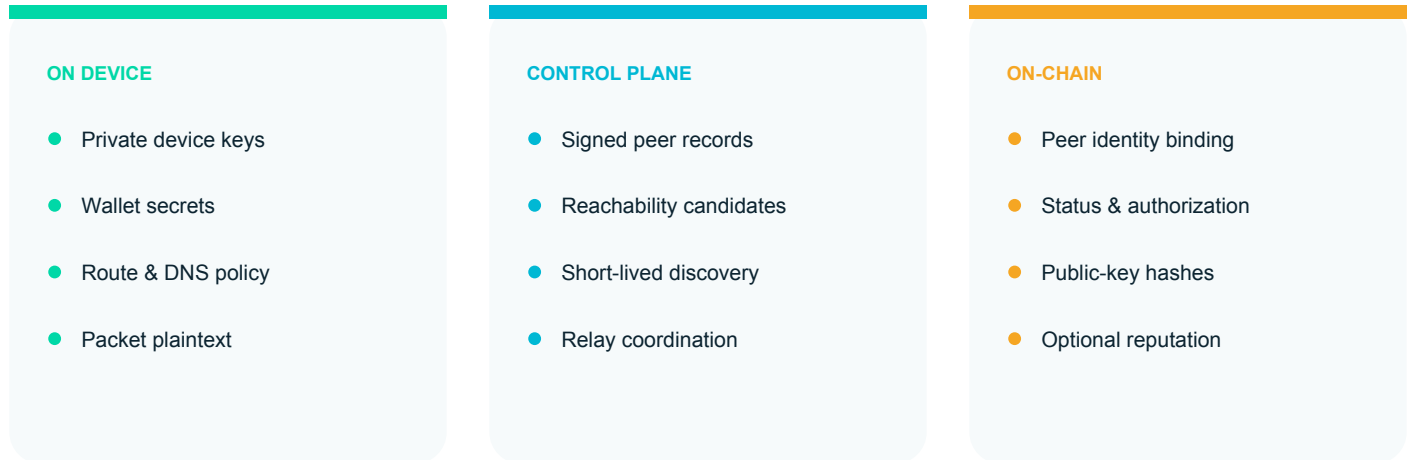
The connection journey separates identity, discovery, session establishment, and traffic so each layer has one clear responsibility.



The blockchain verifies identity. It never carries VPN traffic.

A precise boundary: what goes where

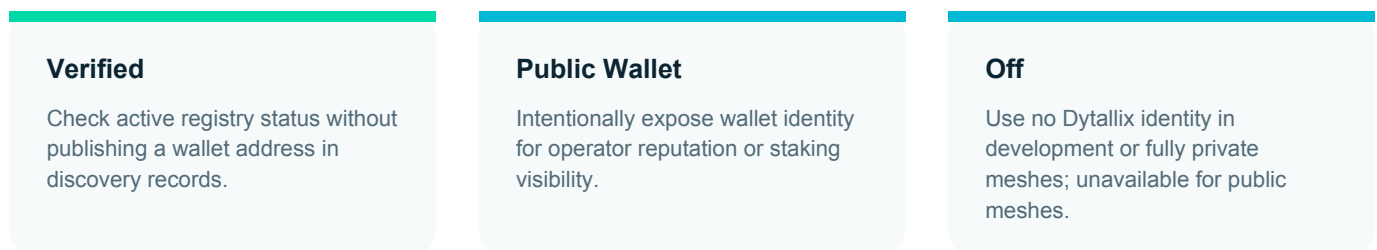
Privacy comes from limiting each system to the minimum information it needs, not from asking one system to hold everything.



NEVER PLACED ON-CHAIN



PRIVACY MODES



Value is different for every audience

The same architecture supports personal privacy, team connectivity, operational control, and game-aware networking without changing the shared protocol.

1

Technical individuals

Reach laptops, home labs, NAS devices, workstations, and private services without operating a gateway VPN.

DIRECT PRIVATE ACCESS

2

Security-conscious teams

Connect people and devices with identity-bound policy, redacted diagnostics, and fewer broad credentials.

VERIFIABLE TRUST

3

Managed environments

Apply per-app VPN, MDM defaults, device policy, signed artifacts, and native platform controls.

OPERATIONAL CONTROL

4

Gamers & streamers

Create trusted peer paths while preserving Steam store, wallet, checkout, and account-security bypass policy.

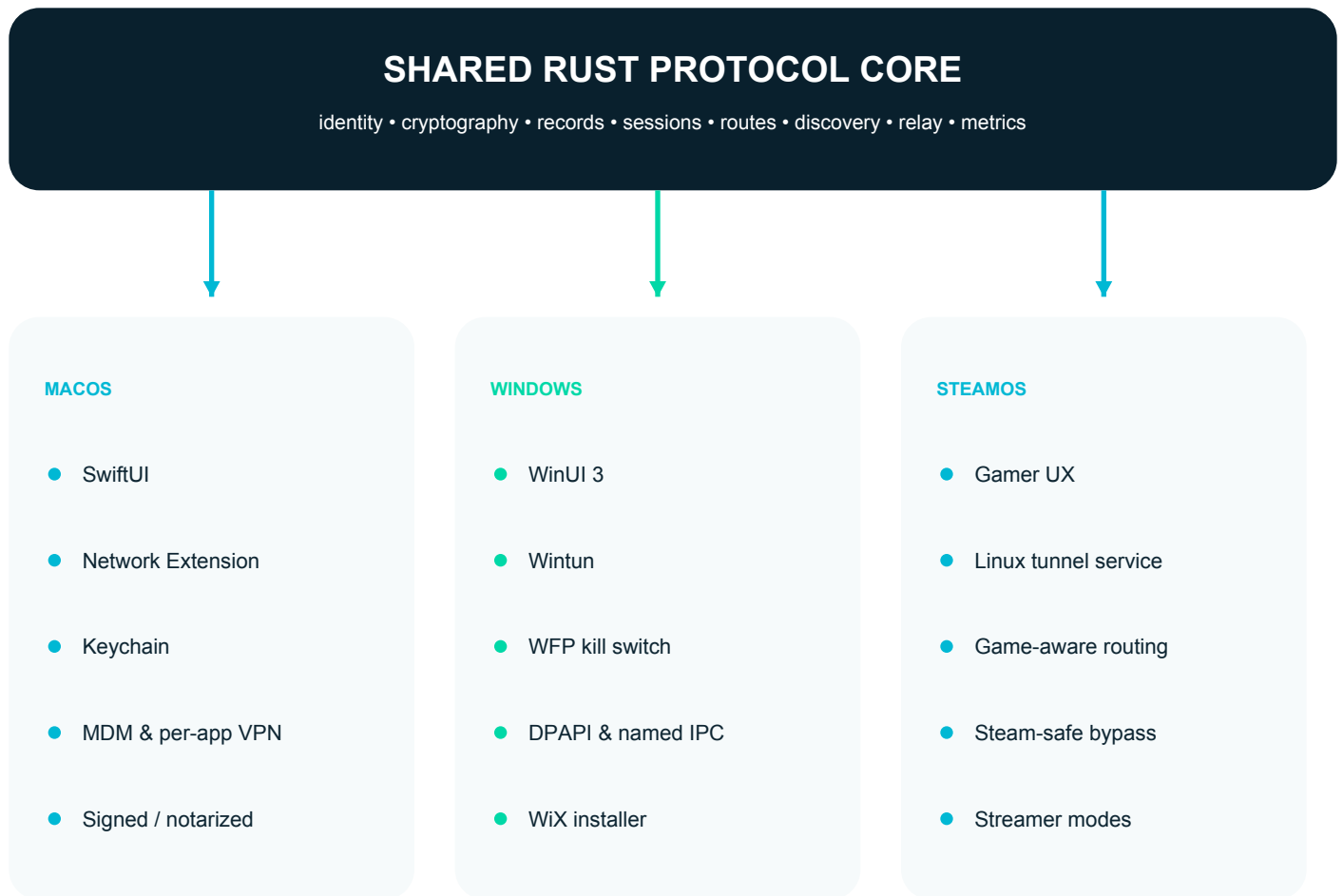
LATENCY-AWARE PRIVACY

DELIBERATE NON-GOALS

QuantumLink is not positioned as an anonymity network, consumer geo-evasion service, traffic-laundering system, or full enterprise ZTNA/SD-WAN replacement. Its core job is authenticated private reachability.

One shared core. Three native experiences.

The protocol does not fork by operating system. Each platform wraps the same core with the tunnel, privilege, security storage, interface, and packaging expected by that OS.



WHY THIS MATTERS

Shared protocol ownership keeps cryptographic and identity behavior consistent. Native silos preserve the security and usability properties that only the operating system can provide.

Defense in layers, with visible failure

QuantumLink treats trust as a sequence of checks. A peer must satisfy identity, record, session, route, and platform policy before protected traffic can flow.

5

PLATFORM

Native tunnel, secret store, privilege separation, signing, updates

4

ROUTE & LEAK CONTROL

Protected routes, DNS policy, kill switch, packet-drop accounting

3

SESSION

FIPS 203 establishment, transcript binding, directional keys, replay rejection

2

PEER

Signed expiring records, inbound assertions, ACLs, certificate binding

1

REGISTRY

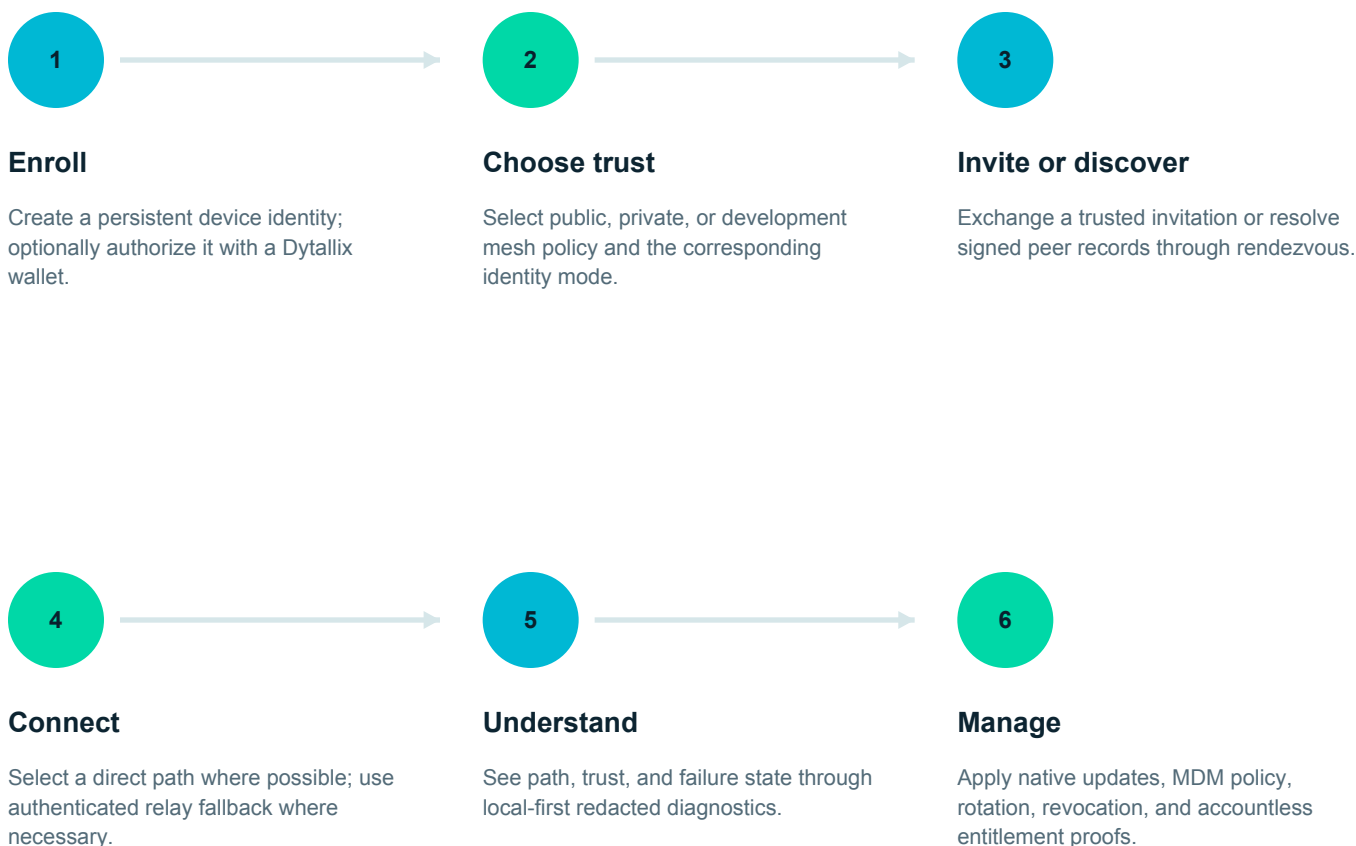
Active identity, owner authorization, status, key and record bindings

WHEN TRUST FAILS

Public-mesh policy rejects missing, revoked, suspended, mismatched, or unavailable identity state. Session and route failures drop protected traffic instead of silently bypassing the tunnel. Redacted diagnostics explain why without exposing raw identifiers by default.

A product journey designed for confidence

QuantumLink turns a complex mesh-security model into a small number of understandable moments for users and operators.



COMMERCIAL ACCESS WITHOUT ACCOUNT-CENTRIC NETWORKING

Future paid access is represented by a signed cryptographic entitlement bound to an opaque subject. Billing may issue or verify access, but it remains outside the VPN path and does not receive peer IDs, routes, DNS, packet metadata, session keys, or mesh traffic.

A smaller trust footprint

QuantumLink's product thesis is that private connectivity becomes more trustworthy when identity, transport, platform integration, and operations are separated, with each system receiving only the data it needs.

The final-release promise

IDENTITY	Verifiable before public-mesh admission
TRAFFIC	Encrypted and off-chain
ACCESS	Accountless by design
TRANSPORT	Direct-first and server-minimized

THE DECISION IN PLAIN LANGUAGE

Choose QuantumLink when the goal is authenticated, inspectable, cross-platform private reachability without routing every session through a mandatory provider concentrator. The architecture favors local keys, direct peer paths, explicit trust policy, post-quantum session establishment, redacted operations, and native leak controls.