OLGNS Post-Quantum Migration Architecture

A Cryptographically Agile Framework for Long-Term Security of Decentralized Financial Infrastructure

OPQMA v1.0 · OLGNS Post-Quantum Security Initiative (OPSI)

Version	1.0
Project	OLGNS
Research Program	OLGNS Post-Quantum Security Initiative (OPSI)
Execution Environment	Anubis Chain
Research Status	Proposed Architecture
Publication Date	August 2026

1. Introduction

Blockchain systems depend fundamentally on cryptographic authentication. A private key authorizes an asset transfer, a validator key participates in consensus, a governance key can authorize a protocol upgrade, a bridge key can control cross-chain assets, and a treasury key can control significant ecosystem resources.

Consequently, the security of a blockchain ecosystem is strongly related to the security of its public-key cryptography. Quantum computing introduces a future threat to widely deployed public-key systems. The relevant risk is not that a quantum computer would simply “break the blockchain” — the primary concern is cryptographic impersonation:

```
PublicKey → QuantumAttack → PrivateKeyRecovery
```

which could potentially allow an attacker to generate valid signatures. Ethereum's post-quantum research similarly identifies digital signatures and exposed public keys as a principal future risk, while emphasising that migration is a multi-year systems-engineering problem rather than a single cryptographic replacement.

> *OLGNS principle: the migration must begin before the cryptographic threat becomes operationally urgent.*

2. Research Motivation

A simplistic approach would be:

```
Current Cryptography
        ↓
Choose PQ Algorithm
        ↓
Replace Current Algorithm
        ↓
Done
```

This approach is insufficient. A real blockchain migration must consider:

- user wallets
- smart contracts
- treasury keys
- DAO governance
- bridge infrastructure
- validators
- developer tooling
- hardware wallets
- exchanges
- APIs
- signatures and transaction formats
- identity systems
- contribution attestations
- privacy systems
- off-chain infrastructure

OLGNS therefore proposes a dedicated architecture: the OLGNS Post-Quantum Migration Architecture.

3. Research Objectives

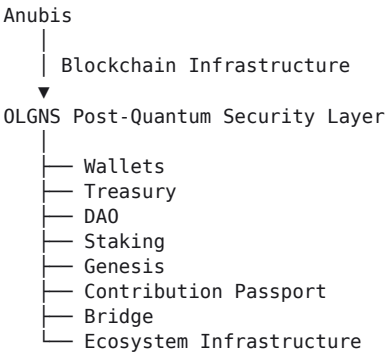
- Objective 1 — Develop a cryptographically agile architecture capable of supporting multiple signature schemes.
- Objective 2 — Enable gradual migration from classical to post-quantum authentication.
- Objective 3 — Protect high-value OLGNS infrastructure before general user migration is complete.
- Objective 4 — Develop efficient post-quantum verification mechanisms suitable for blockchain environments.
- Objective 5 — Investigate signature aggregation and proof compression to control bandwidth and gas overhead.
- Objective 6 — Preserve interoperability during migration.
- Objective 7 — Establish formal verification and security testing as mandatory components of the migration process.

4. Research Questions

- RQ1 — Can OLGNS introduce cryptographic agility without compromising existing protocol functionality?
- RQ2 — Can users migrate to post-quantum authentication without a disruptive network-wide migration event?
- RQ3 — How can larger post-quantum signatures be handled efficiently on-chain?
- RQ4 — Can signature aggregation and zero-knowledge proof systems reduce the on-chain cost of PQ verification?
- RQ5 — Which OLGNS infrastructure should receive post-quantum protection first?
- RQ6 — How can post-quantum security coexist with Anubis privacy infrastructure?
- RQ7 — How can contribution attestations remain verifiable through cryptographic migration?

5. Scope

This paper focuses on the OLGNS application and ecosystem security architecture. It does not propose replacing Anubis consensus or independently modifying the underlying blockchain.



Any changes requiring modifications to Anubis itself would require coordination with the underlying network's protocol developers and governance.

6. Threat Model

The architecture considers a future adversary possessing a cryptographically relevant quantum computer, which may attempt to:

- A. Recover private keys from exposed public keys.
- B. Forge signatures to authorize unauthorized transactions.

- C. Compromise governance by obtaining administrative signing authority.
- D. Attack bridge infrastructure by compromising high-value operational keys.
- E. Impersonate contributors by forging contribution attestations.
- F. Target dormant accounts where migration has not occurred.

```
A_Q = { KeyRecovery, SignatureForgery, Impersonation, ControlCapture }
```

7. What Quantum Computing Does Not Mean

It is important to avoid inaccurate claims. A quantum computer does not automatically:

- rewrite historical blocks
- reverse finalized transactions
- recover every private key instantly
- destroy all cryptography
- make hashing useless

The principal blockchain concern is public-key authentication. Current research similarly distinguishes signature/authentication risk from confidentiality concerns.

8. Post-Quantum Cryptographic Foundation

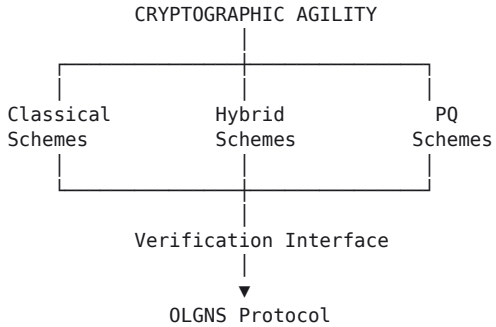
Standard	Algorithm	Purpose
FIPS 203	ML-KEM	Post-quantum key-encapsulation mechanism
FIPS 204	ML-DSA	Post-quantum digital-signature standard
FIPS 205	SLH-DSA	Stateless hash-based digital-signature standard

NIST continues evaluating additional algorithms and signature schemes, reinforcing the need for algorithm agility rather than permanent dependence on one primitive.

> *OLGNS will not define proprietary cryptography. It evaluates standardized, independently scrutinized primitives.*

9. Cryptographic Agility

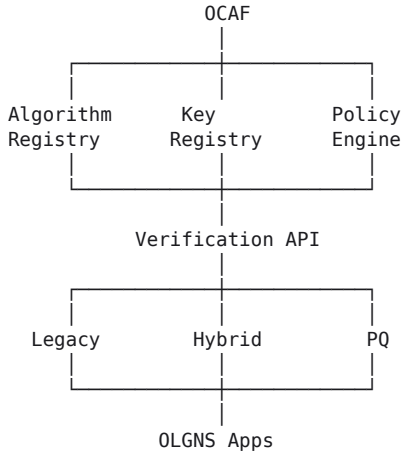
Cryptographic agility means a protocol can replace or introduce cryptographic primitives without redesigning the entire ecosystem.



The application layer should interact with a verification abstraction, rather than hard-coding a single signature algorithm.

10. OCAF — OLGNS Cryptographic Agility Framework

- Algorithm Registry
- Key Registry
- Verification Interface
- Migration Policy Engine
- Versioning System
- Emergency Fallback Mechanism



11. Algorithm Registry

ID	Type	Status	Version
CLASSICAL-1	Signature	Legacy	v1
HYBRID-1	Signature	Research	v1
PQ-SIG-1	PQ Signature	Candidate	v1
PQ-SIG-2	PQ Signature	Candidate	v1
PQ-KEM-1	KEM	Candidate	v1

This registry should never silently change. Every algorithm transition must be versioned, documented, tested, governed and auditable.

12. Key Registry

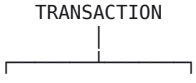
```
K = (Address, Algorithm, Version, Status, Expiry)
```

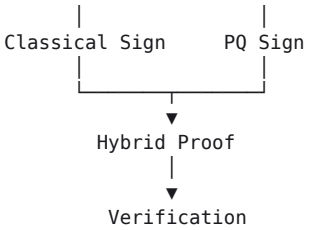
- Active
- Migration
- Deprecated
- Revoked
- Emergency

This allows the system to identify which accounts have migrated.

13. Hybrid Authentication

```
Signature = Classical → Signature = Classical + PQ
```





Hybrid deployment is a transition strategy, not a permanent assumption.

14. Migration Engine

$$State \in \{ Legacy, Hybrid, PQ \} \cdot Legacy \rightarrow Hybrid \rightarrow PQ$$

```
Legacy Account
      │
      ▼
Migration Eligibility
      │
      ▼
New Key Registration
      │
      ▼
Hybrid Verification
      │
      ▼
PQ Verification
      │
      ▼
PQ Account
```

15. No “Flag Day”

The system should avoid a single event such as “at 00:00 UTC all users must migrate.” This creates enormous coordination risk.

```
Year 1      Legacy + PQ Research
Year 2      Legacy + Hybrid
Year 3      Hybrid + PQ
Long Term   PQ-Preferred / PQ-Native
```

The exact calendar remains dependent on cryptographic maturity, network capabilities and governance.

16. Account Migration

```
Account
│
├── Legacy Authentication
├── Hybrid Authentication
└── PQ Authentication
```

```
User
 ↓
Generate PQ Credential
 ↓
Register PQ Credential
 ↓
Prove Control of Existing Account
 ↓
Activate Hybrid Mode
 ↓
Security Delay
 ↓
PQ Mode
```

A security delay can reduce the impact of compromised migration attempts.

17. OLGNS PQ-Ready Wallet

The future wallet should be called the OLGNS PQ-Ready Wallet rather than a “Quantum-Proof Wallet.”

- algorithm registry
- key migration
- hybrid signatures
- PQ signatures
- recovery
- transaction compatibility
- security status
- migration warnings

```
OLGNS WALLET

Security Mode      ● Hybrid
Legacy Key         Active
PQ Key             Registered
Migration          72%
Recommended        Complete migration
```

18. Key Lifecycle

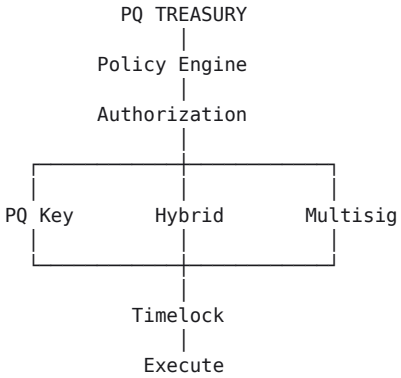
```
Generate → Register → Activate → Use → Rotate → Migrate → Revoke → Archive
```

This is more robust than treating cryptographic keys as permanent identities.

19. High-Priority Attack Surfaces

Tier	Surface	Rationale
Tier 0	Treasury	Highest financial concentration
Tier 1	Bridge	High-value cross-chain trust
Tier 2	Governance & upgrade keys	High protocol-control concentration
Tier 3	Staking / Genesis	Financial contracts
Tier 4	Contributor attestations	Identity and reputation integrity
Tier 5	User accounts	Broadest population

20. OLGNS PQ Treasury



- threshold authorization
- timelocks

- spending limits
- key rotation
- emergency recovery

21. OLGNS PQ DAO

Governance is a security boundary. A compromised governance key could authorize treasury transfers, contract upgrades, reward changes or parameter modifications.

```
Proposal → Voting → PQ / Hybrid Authorization → Timelock → Execution
```

22. PQ Smart Contracts

- Contract-level cryptography — cryptographic operations executed inside contracts.
- Account-level cryptography — how users authorize transactions.
- Administrative cryptography — how contracts are upgraded or controlled.

The migration strategy prioritizes the highest-value authorization paths first.

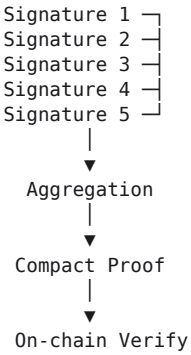
23. PQ Verification Layer

Post-quantum signatures can be larger and more computationally expensive. Research identifies larger signatures, increased verification cost and loss of BLS-style native aggregation as key engineering constraints.

- optimized verification
- batch verification
- precompiles where supported
- proof compression
- aggregation
- caching
- hardware acceleration research

24. Signature Aggregation

```
n Signatures → Compressed Proof
```



Aggregation is treated as research — not a promise that it automatically solves PQ overhead.

25. Zero-Knowledge Proof Integration

Anubis documents a privacy execution layer with ZK proof generation and verification, including a PLONK verification precompile. This creates an opportunity to investigate:

```
Multiple PQ Signatures → ZK Proof → Single Verification
```

- contributor attestations
- governance
- bridge messages
- treasury authorization
- batch transactions

26. PQ Contribution Passport

```
A_i = (Event_i, Evidence_i, Issuer_i, Signature_i, Timestamp_i)
```

```
Legacy Attestation → Re-attestation → Hybrid Attestation → PQ Attestation
```

The historical contribution record should remain accessible while its authentication layer evolves.

27. Privacy-Preserving PQ Contribution

```
Private Evidence → ZK Circuit → PQ-Compatible Authentication → Proof → Contribution Registry
```

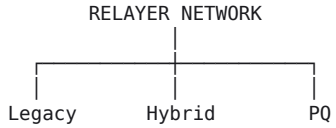
> *A zero-knowledge proof is not automatically post-quantum secure. Both properties must be evaluated independently.*

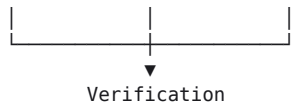
28. PQ Bridge

```
SOURCE CHAIN
     │
     ▼
Bridge Message
     │
     ▼
PQ / Hybrid Authentication
     │
     ▼
Relayer Network
     │
     ▼
Verification
     │
     ▼
Destination
```

- key rotation
- algorithm versioning
- message replay protection
- nonce management
- emergency pause
- rate limits
- independent monitoring

29. PQ Relayer Network





Relayers can operate in classical, hybrid or PQ mode, enabling staged deployment.

30. Data Security

Post-quantum migration is not only about signatures. OLGNS must also inventory:

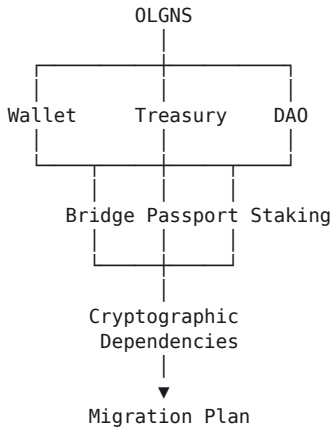
- encrypted off-chain data
- API credentials
- contributor evidence
- custody records
- private governance communications
- bridge secrets
- operational credentials

31. Cryptographic Inventory

System	Current Primitive	Purpose	Exposure	Migration
Wallet	TBD	Authentication	High	PQ
Treasury	TBD	Authorization	Critical	PQ
DAO	TBD	Governance	Critical	Hybrid / PQ
Bridge	TBD	Messaging	Critical	PQ
Passport	TBD	Attestation	High	PQ
Staking	TBD	Authorization	High	Hybrid
Genesis	TBD	Allocation	High	Hybrid / PQ

The exact current primitives must be established through code and deployment analysis rather than assumed.

32. Cryptographic Dependency Graph



33. Security Levels

- Level 0 — Low-value public data

- Level 1 — Standard user activity
- Level 2 — Financial applications
- Level 3 — High-value operational systems
- Level 4 — Protocol control
- Level 5 — Critical cross-system trust

Migration priority increases with the level.

34. Emergency Migration

```
Threat Detected → Security Assessment → Emergency Classification
      → Freeze / Restrict → Activate Alternative Primitive
      → Migrate Keys → Resume
```

The emergency mechanism itself must be secured.

35. Algorithm Failure

- cryptanalysis
- implementation vulnerabilities
- performance problems
- denial-of-service risk
- interoperability problems

```
Algorithm A ≠ Permanent Security → Algorithm Registry → Migration Path
```

36. Formal Verification

- Mathematical level — does the implementation correspond to the specification?
- Protocol level — does the cryptographic mechanism behave correctly within OLGNS?

OLGNS should therefore establish the OLGNS Formal Security Program.

37. Formal Verification Pipeline

```
Specification → Formal Model → Implementation → Proof
   → Property Testing → Fuzzing → Independent Audit
   → Testnet → Mainnet
```

> *No cryptographic migration component should move directly from research to production.*

38. Testing Framework

- Unit testing — cryptographic primitives
- Known answer tests — validate standardized algorithms
- Fuzz testing — malformed inputs
- Differential testing — compare independent implementations
- Property testing — verify security invariants
- Performance testing — CPU, memory, gas, bandwidth, latency
- Adversarial testing — compromised keys and malicious migration

39. Performance Model

```
minimize ( T_verify , S_sig , G_verify , B_network ) subject to Security ≥
                                RequiredSecurity
```

40. Economic Impact

- transaction costs
- storage requirements
- node bandwidth
- validator / operator requirements

```
TotalCost = Gas + Storage + Bandwidth + Compute + OperationalCost
```

41. Decentralization Constraint

Security cannot be improved by making node operation prohibitively expensive.

```
Decentralization ≥ D_min , Security ≥ S_target , Performance ≥ P_target

Optimize ( Security , Decentralization , Performance )
```

42. Migration Phases

- Phase 0 — Discovery: cryptographic inventory, key inventory, threat model, dependency graph.
- Phase I — PQ Readiness: OCAF, algorithm registry, key registry, PQ test environment, benchmark framework. No production replacement yet.
- Phase II — Hybrid Infrastructure: hybrid keys and verification, PQ treasury/DAO testing, PQ bridge testnet, PQ contribution attestations.
- Phase III — Controlled Migration: Legacy → Hybrid → PQ, voluntary and governed.
- Phase IV — PQ-Preferred: new infrastructure defaults to approved PQ/hybrid mechanisms.
- Phase V — PQ-Native: PQ authentication, treasury, DAO, bridge, contribution and infrastructure — conditional on maturity.

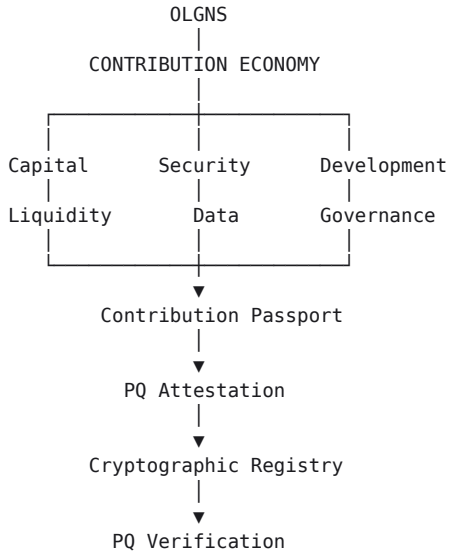
43. Proposed Roadmap

Stage	Focus	Deliverables
A — Research	Foundations	Cryptographic inventory · threat model · OCAF spec · algorithm evaluation · benchmarking
B — Prototype	Build	PQ wallet prototype · PQ key registry · hybrid signature module · PQ treasury prototype
C — Testnet	Validate	PQ transactions · PQ governance · PQ Contribution Passport · PQ bridge · PQ relayer
D — Security	Assure	Formal verification · independent audit · adversarial testing · bug bounty
E — Mainnet	Migrate	High-value infrastructure → early adopters → general users → PQ-preferred

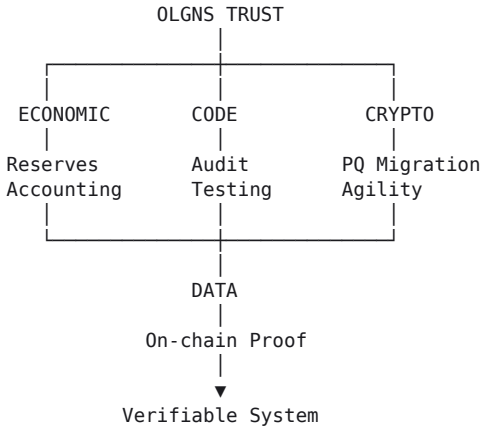
44. Migration Priority Matrix

Component	Value at Risk	Control Risk	PQ Priority
Treasury	Very High	Very High	P0
Bridge	Very High	Very High	P0
DAO / Admin	Very High	Very High	P0
User Wallets	High	High	P1
Contribution Passport	Medium / High	High	P1
Genesis	High	High	P1
Staking	High	Medium	P1
Data Infrastructure	Medium	Medium	P2
Analytics	Low	Low	P3

45. PQ-Ready Contribution Economy



46. OLGNS Trust Architecture



> *The objective is not to claim OLGNS is impossible to attack — it is to make security assumptions visible, testable and replaceable.*

47. Interoperability

Different chains may adopt different PQ signatures, key formats, verification systems and migration timelines.

```
Chain A → Message Standard → Verification Adapter → OCAF → OLGNS
```

The bridge should not assume that every chain will use the same cryptographic system.

48. Standardization Strategy

- NIST PQC standards
- IETF developments
- blockchain-specific cryptographic standards
- wallet standards
- hardware security standards

49. Open Research Policy

- technical specifications
- benchmark results
- test vectors
- migration proposals
- security assumptions
- audit reports
- implementation status

> *The programme clearly distinguishes Research → Prototype → Testnet → Mainnet. This is essential for credibility.*

50. Security Disclosure Policy

```
classify → contain → notify maintainers → develop mitigation → test → deploy → disclose responsibly
```

The protocol should maintain a public security history.

51. No Proprietary “Quantum” Claims

OLGNS explicitly rejects the following claims: “world's first quantum blockchain”, “100% quantum-proof”, “unbreakable cryptography”, “quantum computers cannot attack OLGNS.” These statements are scientifically indefensible.

> *Correct terminology: Post-Quantum Ready · Cryptographically Agile · Migration-Oriented · Quantum-Resilience Research.*

52. Research Hypotheses

- H1 — Cryptographic agility reduces migration coordination risk compared with one-time replacement.
- H2 — Hybrid authentication can provide a practical transition path between classical and post-quantum systems.
- H3 — Signature aggregation or proof compression can reduce the effective blockchain overhead of PQ signatures.
- H4 — Prioritizing high-value operational keys reduces systemic quantum exposure before full ecosystem migration.

- H5 — A cryptographically migratable Contribution Passport can preserve contribution history across transitions.

53. Evaluation Metrics

$$MC = PQReadyAccounts / EligibleAccounts$$

$$IC = PQReadyCriticalSystems / TotalCriticalSystems$$

$$VC = Gas + Compute + Bandwidth$$

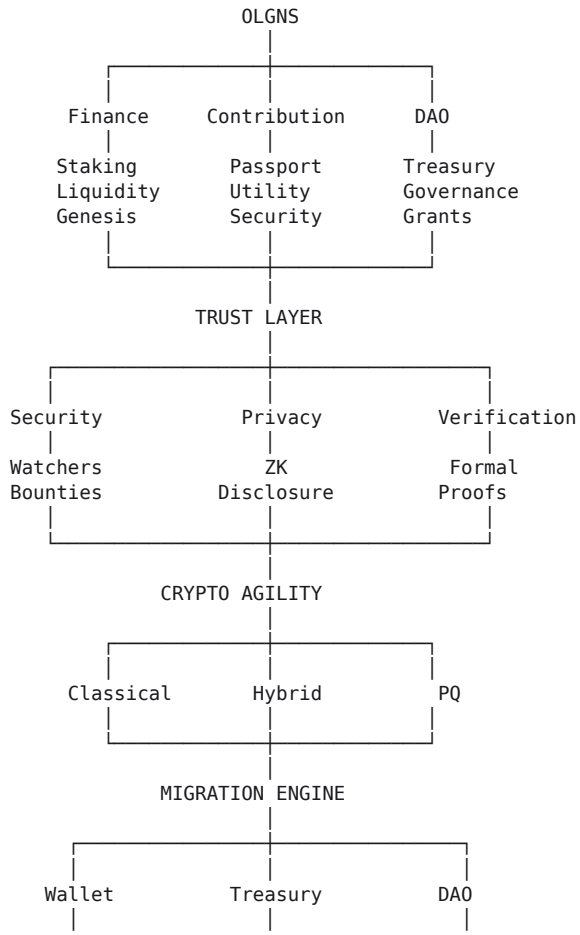
$$MR = SuccessfulMigrations / MigrationAttempts$$

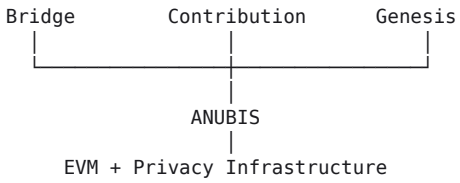
$$ER = f (MC , IC , VC , MR)$$

54. Research Limitations

- Cryptographic uncertainty — future algorithms may change.
- Implementation risk — even standardized algorithms can be implemented incorrectly.
- Performance — PQ signatures can be larger and more computationally demanding.
- Migration complexity — users cannot be assumed to migrate simultaneously.
- Interoperability — different chains may adopt different standards.
- Governance — migration policies require legitimate decision-making.
- Hardware — wallet and HSM environments may require substantial adaptation.
- Economic cost — migration may increase transaction and infrastructure costs.

55. Long-Term Architecture





56. OLGNS Post-Quantum Security Model

```
DISCOVER → INVENTORY → MODEL THREATS → DESIGN CRYPTO-AGILITY
   → TEST PQ ALGORITHMS → BUILD HYBRID SYSTEM → FORMALLY VERIFY
   → AUDIT → TESTNET → MIGRATE HIGH-VALUE SYSTEMS → MIGRATE USERS
   → PQ-PREFERRED → CONTINUOUS CRYPTOGRAPHIC REVIEW
```

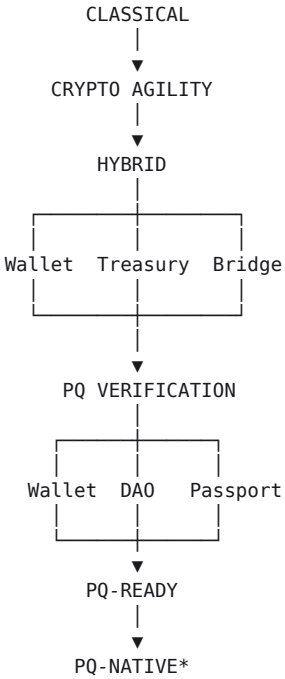
This is the core of OPQMA.

57. Research Position

OLGNS does not position this work as “we invented post-quantum cryptography.” It is positioned as: OLGNS proposes a cryptographically agile migration architecture for decentralized financial infrastructure, integrating post-quantum authentication, key migration, verification, privacy, contribution attestations and high-value operational security.

58. Conclusion

Quantum computing represents a long-term change to the security assumptions underlying public-key cryptography. The correct response is not panic and not marketing — it is preparation. OPQMA therefore treats quantum resilience as a systems-engineering problem, combining cryptographic agility, key migration, hybrid authentication, PQ verification, signature aggregation, formal verification, privacy preservation, operational security and cross-chain security into one migration framework.



**Subject to cryptographic maturity, standards, testing, governance and network capabilities.*

OLGNS should not wait for the quantum threat to become urgent before beginning migration. Design for cryptographic change before cryptographic change becomes an emergency.

Selected References

1. Ethereum Foundation — Post-Quantum Ethereum: research architecture, migration strategy, execution/consensus/data layers, cryptographic agility and attack-surface analysis.
2. NIST — FIPS 203 / FIPS 204 / FIPS 205: finalized standards for ML-KEM, ML-DSA and SLH-DSA.
3. NIST IR 8545 — Status of the fourth round of post-quantum cryptography standardization.
4. Anubis Network — System Architecture: three-layer architecture, hybrid state model, EVM extensions, privacy execution, note system and ZK verification.
5. NIST CSRC — Post-Quantum Cryptography: Additional Digital Signature Schemes.