Quantum Resilience Explained
Bazaars ORC-55

How ORC-55 Achieves Quantum Resilience

The multi-chain architecture means all host chains must be compromised simultaneously to destroy the asset. Since BZR is deployed on 10 different blockchains (Ethereum, BNB Chain, Base, Polygon, Arbitrum, Avalanche, zkSync Era, Cronos, Mantle, and Optimism), a quantum attack would need to breach all networks at once.

Diverse Consensus Protection

The diverse consensus mechanisms across chains provide resistance against quantum computing threats that might impact a single network's cryptography. Different blockchains use different cryptographic implementations and consensus algorithms, so a quantum breakthrough that compromises one chain wouldn't necessarily affect the others immediately.

Additional Security Layers

Beyond quantum considerations, the ORC-55 standard enhances security through immutable code that eliminates governance or proxy attack vectors, and maintains a minimal attack surface with no external calls in token logic. This means even if quantum computers eventually break the cryptography of one blockchain, the token continues to exist authentically on the remaining chains without losing its identity or value.

Essentially, ORC-55's quantum resilience is about survival through distribution — by existing on multiple independent blockchains simultaneously, BZR can withstand catastrophic failures of individual networks, whether from quantum threats or other security compromises.