KnectIQ

WHITEPAPER

The Future of Money Must be Sovereign, Programmable, and Quantum-Safe

SelectiveTRUST®

For decades, we've relied on the strength of our cryptographic foundations to secure digital transactions and build trust in our financial systems. Digital assets, stablecoins, and programmable money are now deeply embedded in global commerce. But those foundations were never designed with quantum computing in mind, and the clock is ticking.

A quantum-capable adversary doesn't need to break the system. It only needs to extract one exposed public key. From there, it can derive the private key using Shor's algorithm to forge transactions, corrupt ledgers, and collapse trust.

The Stablecoin Ecosystem Is Not Ready

What started as a curiosity has become a cornerstone of cross-border commerce. Yet most stablecoins and the infrastructure that supports them depend on public key encryption, particularly ECDSA, which will not withstand the arrival of practical quantum computing.

Public keys are exposed during routine blockchain operations. Once those keys are visible, a sufficiently advanced quantum system can derive the private key. Every asset, contract, and transaction becomes vulnerable. It's a visibility problem—and the exposure has already happened.

Trust Without Exposure

We don't need to burn down existing protocols or hard-fork entire ecosystems. We need a better trust layer, one that enforces control and access without persistent secrets, foreign-controlled certificate authorities, or exposed public key infrastructure.

SelectiveTRUST® from KnectIQ delivers precisely that. It creates sovereign, ephemeral trust environments between endpoints, establishing dynamic access to cryptographic functions without ever transmitting or storing keys.

- No key is stored
- No secret is reused
- No public key is exposed

SelectiveTRUST® supports ML-KEM Levels 3 and 5, aligning with the U.S. National Institute of Standards and Technology (NIST) post-quantum cryptographic standards. It is Kubernetes-native, scalable across public, private, and classified cloud environments.

Policy, Compliance & Global Standards

The GENIUS Act, passed by the U.S. Congress, reinforces the imperative that programmable money must be secure, sovereign, and quantum-safe. SelectiveTRUST® satisfies these mandates by delivering:

- Quantum-safe infrastructure without rewriting existing protocols
- GENIUS Act alignment with sovereign cryptographic control
- Support for zero-trust architecture principles (NIST SP 800-207, SP 800-208)
- Cross-jurisdictional enforcement of national boundaries in cryptographic operations

Globally, SelectiveTRUST® aligns with security and governance principles set forth by the Bank for International Settlements (BIS), the Financial Stability Board (FSB), the International Monetary Fund (IMF), and the European Union's Markets in Crypto-Assets (MiCA) framework, ensuring that both private issuers and central banks can meet regulatory obligations without compromising flexibility or performance.

The Future of Digital Money Must be Sovereign

As the world shifts to programmable value, trust must evolve with it. If a monetary system depends on foreign root keys, centralized certificate authorities, or static secrets stored on vendor hardware, it is neither sovereign nor safe.

SelectiveTRUST® ensures that cryptographic control stays in the hands of the issuing authority. It enables secure, policy-driven collaboration across chains, currencies, and jurisdictions, while preserving national digital sovereignty

For central banks, stablecoin issuers, payment providers, regulators, and financial institutions, the choice is clear. Modernize your trust layer by integrating foundational, next-generation trust for digital sovereignty and quantum-safe readiness with SelectiveTRUST®. Make programmable money your competitive force multiplier.

T: +1.651.447.4264 | E: secure@knectiq.com | www.KnectIQ.com | 724 Bielenberg Drive, St. Paul, Minnesota 55125