

Contents

- 1 Introduction 2
- 2 The Non-DeFi Transaction Archetype 2
 - 2.1 Security Integration Points for Data-in-Transit Protection..... 3
- 3 The DeFi Transaction Archetype..... 4
 - 3.1 Security Integration Points for Data-in-Transit Protection..... 5
- 4 Conclusion 6

Strengthening Cryptocurrency Transaction Security Through Post-Quantum-Safe Data-in-Transit Protection

1 Introduction

Cryptocurrency ecosystems depend on a chain of off-chain services, intermediaries, and network participants to move a transaction from a user's wallet to the blockchain and ultimately to the intended recipient. While the cryptographic signatures that authorize transactions represent a post-quantum vulnerability, this paper focuses on the *transport paths* that carry these transactions, and the sensitive metadata surrounding them, that remain exposed to architectural weaknesses fundamental to the client-server architecture of the internet and classical cryptographic protocols that will not withstand the post-quantum transition.

As quantum-capable adversaries emerge, the confidentiality and integrity of data in transit become critical. Attackers do not need to break wallet-level signing to cause harm; they can exploit weaknesses in RPC communication, exchange integrations, and off-chain data flows to intercept, manipulate, correlate, or replay sensitive information. These risks are amplified by the long-term threat of "harvest-now, decrypt-later" attacks against today's classical encryption.

This paper describes how PortalSIX, which is focused on securing data in transit, can provide post-quantum-resistant communication channels and architectural hardening across the full lifecycle of a Non-DeFi cryptocurrency transaction.

SIX3RO's technology represents a revolution in information exchange tools. Combining an innovative decentralized architecture, blockchain, and post-quantum cryptography, the SIX3RO platform represents the vanguard of a new secure information exchange paradigm. For a full description of this decentralized, post-quantum, refer to the SIX3RO white paper, which can be found here: <https://six3ro.com/whitepaper/>

2 The Non-DeFi Transaction Archetype

In the Non-DeFi model, a transaction moves through a predictable sequence of off-chain and on-chain steps:

1. Wallet to RPC Provider

The user's wallet application or browser extension constructs and signs a transaction locally, then transmits it to an RPC provider. While the signature protects the transaction's authenticity, the *transport path* remains vulnerable to interception, metadata leakage, and downgrade attacks.

2. **RPC Provider to Full Nodes**

The RPC provider announces the transaction to one or more full blockchain nodes. This propagation step often relies on classical TLS or unencrypted peer-to-peer protocols.

3. **Full Nodes to Network**

Nodes replicate and propagate the transaction across the blockchain network. Although the transaction itself is public, the surrounding metadata, including timing, origin, and network topology, can be sensitive.

4. **Exchange Monitors Network**

Exchanges continuously ingest blockchain data to detect inbound transactions. Their ingestion pipelines often include internal APIs, message buses, and monitoring services that rely on legacy transport protections.

5. **Exchange to Network**

Exchanges generate outbound transactions (withdrawals, settlements, internal transfers) and broadcast them to the network. Again, signing protects the transaction, but the transport path remains a point of exposure.

6. **Recipient Wallet Updates**

The recipient's wallet monitors the blockchain and updates its state. Wallet-to-node communication frequently traverses third-party RPC providers or light-client services, creating additional transport-layer risk.

In addition to these on-chain flows, exchanges maintain two critical off-chain integrations:

- **Exchange → Internal Systems (KYC, AML, risk engines)**
- **Exchange → External Payment Processors**

These systems handle identity, compliance, and fiat-settlement data, information that is far more sensitive than the blockchain transactions themselves.

2.1 Security Integration Points for Data-in-Transit Protection

Across this architecture, there are four locations where PortalSIX can deliver meaningful benefit by securing data in transit with post-quantum-resistant mechanisms:

1. **Wallet → RPC Provider**

This is one of the most exposed boundaries in the ecosystem, where PQC-safe secure channels can prevent interception, metadata leakage, and downgrade attacks without altering the wallet's signing logic. Both the wallet provider and the RPC provider must adopt the SIX3RO capability to achieve the benefit.

2. Exchange → Internal Systems

Exchanges can deploy PortalSIX to protect sensitive KYC, AML, and compliance data flows. These internal APIs and message buses often rely on classical TLS or unencrypted channels, making them prime targets for harvest-now, decrypt-later attacks.

3. Exchange → External Payment Processor

These integrations frequently use legacy financial protocols that were never designed with post-quantum threats in mind. In this scenario, both parties must adopt the capability to secure fiat-settlement communications.

4. Exchange-Originated Blockchain Interactions

While the transaction signatures remain unchanged, the communication paths used to prepare, stage, and broadcast transactions can be protected with PQC-resistant secure channels, reducing the risk of manipulation or surveillance.

By focusing exclusively on data-in-transit protection, PortalSIX strengthens the architectural fabric of the cryptocurrency ecosystem without altering existing signing workflows or blockchain-level cryptographic primitives.

3 The DeFi Transaction Archetype

Decentralized Finance (DeFi) introduces additional architectural complexity compared to traditional exchange-mediated cryptocurrency flows. As with the non-DeFi archetype, while the underlying cryptographic signatures remain the responsibility of wallets and smart contracts, the *transport paths* that carry transactions, contract calls, state updates, and off-chain coordination traffic are significantly more diverse, and often more exposed.

A typical DeFi transaction follows this sequence:

1. Wallet to RPC Provider

The user's wallet constructs and signs a transaction or contract call locally, then transmits it to an RPC provider. As in the Non-DeFi model, the signature protects the transaction itself, but the transport path remains vulnerable to interception, metadata leakage, and downgrade attacks.

2. RPC Provider to Full Ethereum Nodes

The RPC provider announces the transaction to one or more full Ethereum nodes (or nodes on another chain, though Ethereum is the dominant platform for DeFi). This propagation step often relies on classical TLS or unencrypted peer-to-peer protocols.

3. **Full Nodes to Ethereum Network / Contract Execution**

Nodes replicate the transaction across the Ethereum network and, if applicable, execute the associated smart-contract call. While the contract logic is public, the surrounding metadata — timing, origin, and network topology — can reveal sensitive behavioral patterns.

4. **Exchange Monitors Network**

If an exchange is involved (e.g., for settlement, liquidity routing, or hybrid CeFi/DeFi operations), it monitors the Ethereum network for relevant events.

5. **Recipient Wallet Monitors Network**

Alternatively, the recipient's wallet directly observes the network and updates its state based on contract events or token transfers.

6. **Exchange Posts New Transactions**

Exchanges may generate outbound transactions or contract calls and broadcast them to the network.

7. **Recipient Wallet Updates**

The recipient's wallet identifies relevant on-chain activity and updates accordingly.

In addition to these flows, DeFi introduces several off-chain or cross-system interactions that are essential to the functioning of exchanges, liquidity providers, and smart-contract platforms:

- **Exchange → Smart Contract Provider** (the entity that develops, deploys, or maintains the contract)
- **Exchange → RPC Provider**
- **Exchange → Internal Systems (KYC, AML, risk engines)**
- **Exchange → External Payment Processor**

These interactions often involve sensitive operational data, proprietary algorithms, or identity-linked information — all of which are vulnerable to harvest-now, decrypt-later attacks if protected only by classical cryptography.

3.1 Security Integration Points for Data-in-Transit Protection

Across the DeFi architecture, there are six locations where PortalSIX can provide meaningful post-quantum-safe data-in-transit protection:

1. **Wallet → RPC Provider**

This boundary is one of the most exposed in the DeFi ecosystem, and PQC-resistant

secure channels can prevent interception, metadata leakage, and traffic correlation without altering signing workflows. In this scenario, both the wallet provider and the RPC provider must adopt the PortalSIX capability.

2. Exchange → Internal Systems (KYC, AML, risk engines)

Exchanges can deploy PortalSIX to secure internal APIs, message buses, and data pipelines that handle identity, compliance, and risk-scoring information. These systems often rely on legacy transport protections that are vulnerable to quantum-enabled adversaries.

3. Exchange → Smart Contract Provider

Many exchanges interact directly with the organizations that develop or maintain smart contracts, for audits, upgrades, oracle coordination, or operational support. Securing these communications requires both parties to adopt PortalSIX, ensuring that proprietary or sensitive operational data is protected in transit.

4. Exchange → RPC Provider

Exchanges frequently rely on third-party RPC providers for high-volume contract calls, transaction broadcasting, and state queries. PQC-safe secure channels prevent interception or manipulation of these high-value data flows.

5. Exchange → External Payment Processor

Fiat settlement, off-chain reconciliation, and compliance reporting often traverse legacy financial protocols. Both the exchange and the payment processor must adopt PortalSIX to ensure post-quantum-safe protection of these sensitive data flows.

6. Exchange-Originated Blockchain Interactions

While the transaction signatures remain unchanged, the communication paths used to prepare, stage, and broadcast DeFi-related transactions or contract calls can be protected with PQC-resistant secure channels. This reduces the risk of surveillance, manipulation, or targeted disruption.

By focusing exclusively on data-in-transit protection, PortalSIX strengthens the architectural fabric of DeFi ecosystems without modifying smart-contract logic, wallet signing behavior, or blockchain-level cryptographic primitives.

4 Conclusion

The analysis of both Non DeFi and DeFi transaction flows illustrate that the most significant vulnerabilities in today's cryptocurrency infrastructure arise not from the signing algorithms that authorize transactions, which can be upgraded in a relatively

straightforward manner, but from the transport paths that carry those transactions and the sensitive metadata surrounding them. These paths rely on classical cryptography and legacy client server architectures that cannot withstand the arrival of quantum capable adversaries. As discussed, every stage of the transaction lifecycle contains communication channels that remain exposed to interception, correlation, manipulation, or long-term decryption. These weaknesses exist across wallet to RPC communication, exchange integrations, smart contract coordination, and the off-chain systems that support compliance and fiat settlement.

PortalSIX provides a practical and forward-compatible solution to this systemic problem by delivering post-quantum safe protection for data in transit without requiring any changes to wallet signing logic, smart contract code, or blockchain-level cryptographic primitives. Its value lies in strengthening the connective infrastructure that underpins every cryptocurrency transaction, whether simple or highly composable. By securing these communication paths with quantum resistant mechanisms, PortalSIX gives exchanges, wallet providers, RPC operators, and smart contract developers a clear path to long-term resilience. Integrating PortalSIX now allows the ecosystem to harden its architecture before quantum threats materialize, ensuring that both current operations and long-lived data remain protected. In a rapidly evolving threat landscape, adopting PortalSIX is a strategic investment in the integrity and durability of digital asset systems.