Volume II

Post-Quantum Settlement Infrastructure

Securing Financial Markets Against the Quantum Threat

Volume II of Blockchain for Financial Markets

Abdelkader BOUSABAA

University of Paris-Saclay

Second Edition — 2026

Seven Lions Editions

Contents

Preface

"The time to repair the roof is when the sun is shining."

— John F. Kennedy, State of the Union Address, 1962

In August 2024, the US National Institute of Standards and Technology published three Federal Information Processing Standards — FIPS 203, FIPS 204, and FIPS 205 — that formally defined the first post-quantum cryptographic algorithms approved for widespread deployment. The publication was the culmination of eight years of global competition, involving 69 submissions from cryptographers in dozens of countries, subjected to the most rigorous public cryptanalytic evaluation in the history of the discipline. The announcement did not make the front pages of financial newspapers. It should have.

Those three documents mark the beginning of the most consequential cryptographic transition in the history of financial market infrastructure. Every digital signature that authorises a settlement instruction, every encrypted channel that carries a margin call, every certificate that authenticates a clearing house to its participants — all of it depends on mathematical assumptions that a sufficiently powerful quantum computer will render worthless. That quantum computer does not yet exist. But the consensus among quantum engineers, cryptographers, and intelligence agencies is that it will exist within the window that matters for data generated and systems deployed today.

This book was written for the practitioners who must act on that reality: the technology officers at central securities depositories, the infrastructure architects at central counterparties, the risk managers at custodian banks, and the policy specialists at central banks and regulators who are beginning to ask what "post-quantum migration" actually means at the operational level. It was not written for quantum physicists, although they will find the financial applications interesting, nor for pure cryptographers, although the rigour of the underlying mathematics is preserved throughout. It was written for the person who must answer, in a board presentation or a regulatory response, the question: *what do we need to do, and by when?*

Why This Book Now

The post-quantum migration has a peculiar temporal structure that makes it unlike most technology transitions. In most technology upgrades, the risk is present and the solution is future: we know the system is inadequate, we wait for the better alternative, and we deploy it when ready. The post-quantum transition is inverted. The solution is present — the NIST standards are published, the implementations are available, the performance is adequate — and the risk is future. The quantum computer that will break ECDSA does not yet exist. The harvest-now-decrypt-later attack, however, operates in reverse time: adversaries record encrypted data today, store it, and decrypt it when the quantum computer arrives. For settlement infrastructure that generates records with legal and regulatory significance for ten years or more, the harvest attack means the effective risk window already includes the present.

There is a second temporal inversion. Financial market infrastructure migrates slowly, because it cannot be taken offline, because it is shared across dozens of institutions with competing priorities, and because its governance requires multilateral consensus. The migration of European settlement infrastructure to ISO 20022 message formats, a change far simpler than a cryptographic algorithm replacement, took the better part of a decade. The post-quantum migration is more complex. If institutions wait until the quantum threat is imminent to begin, they will not finish in time. The migration must begin before the threat materialises, which is to say it must begin now, while the case for urgency requires some explanation rather than being self-evident from daily events.

This book attempts to provide that explanation with the technical precision and financial market specificity that practitioners need to make the case internally and to take concrete action.

Structure and Scope

The book is divided into three parts.

Part I, *The Quantum Threat*, builds the foundation from first principles. Chapter 1 develops the intuition for quantum computing — what a qubit is, why superposition and entanglement matter, and why quantum computers are not simply faster classical computers. Chapter 2 explains Shor's algorithm and why it destroys the elliptic curve cryptography that protects every settlement instruction signed today. Chapter 3 addresses Grover's algorithm, a more nuanced threat that weakens but does not break symmetric cryptography, and draws the map of which settlement components are existentially threatened and which are merely degraded.

Chapter 4 analyses the timeline for a cryptographically relevant quantum computer, examining the Mosca inequality framework and the regulatory consensus around 2030 to 2040. Chapter 5 documents the harvest-now-decrypt-later threat in detail, explaining why the risk clock is already running for institutions whose data has long-term sensitivity.

Part II, *The Post-Quantum Arsenal*, surveys the solution space. Chapter 6 provides a comprehensive map of the four NIST-standardised algorithms. Chapter 7 develops the mathematics of lattice cryptography from intuition to implementation, explaining how ML-KEM and ML-DSA achieve their security. Chapter 8 covers hash-based signatures, explaining why SLH-DSA's minimal-assumption security is the right choice for root certificates and archival records. Chapter 9 addresses Quantum Key Distribution — what it promises, what it cannot deliver, and how it complements rather than replaces post-quantum cryptography. Chapter 10 examines Quantum Random Number Generation, the often-overlooked foundation on which all cryptographic security ultimately rests.

Part III, *Migration and Applications*, turns from theory to practice. Chapter 11 analyses why migrating a settlement blockchain is structurally harder than migrating any other system, identifying the seven specific challenges that arise from the combination of immutability, multilateral governance, and smart contract logic. Chapter 12 explains hybrid cryptographic schemes — the technical bridge between the current classical infrastructure and the quantum-safe destination — and shows how they can be deployed immediately and unilaterally. Chapter 13 presents the seven-layer quantum-safe DLT reference architecture, specifying which algorithm goes where and why. Chapter 14 surveys the regulatory landscape in detail: DORA, CNSA 2.0, the EBA, the ECB, CPMI-IOSCO, and SWIFT. Chapter 15 demonstrates working Python code for every core operation, from ML-DSA signing to a minimal post-quantum settlement ledger. The Epilogue reflects on the four strategic decisions that every institution responsible for settlement infrastructure must make.

What This Book Assumes

The book assumes familiarity with financial market infrastructure at the level of a practitioner who understands what a CSD does, why DVP settlement matters, and what a CCP's role in risk mutualisation entails. It does not assume any prior knowledge of quantum computing, cryptography, or advanced mathematics. Every concept is introduced from intuition before formalism, with analogies drawn from physics, finance, and everyday experience before equations are introduced. The equations are present, because the practitioner who needs to evaluate a vendor's post-quantum claims or respond to a regulator's technical query will encounter them; but no equation appears without a plain-language explanation of what it means.

Readers who are primarily interested in the regulatory and operational dimensions of the migration can read Part I for orientation, focus on Chapters 6, 11, 12, 13, and 14 for the practical content, and treat the more mathematical sections as reference material. Readers with a stronger technical orientation may find themselves spending more time in Chapters 7, 8, and 15.

A Note on Terminology

The book uses the NIST standardised names throughout: ML-KEM (not Kyber), ML-DSA (not Dilithium), SLH-DSA (not SPHINCS+), FN-DSA (not Falcon). Where historical context requires the competition names, both are given. The abbreviation PQC refers to post-quantum cryptography as a field, not to any specific algorithm. CRQC refers to a Cryptographically Relevant Quantum Computer: a quantum computer capable of breaking ECDSA-256 in a practically relevant timeframe.

Acknowledgements

This volume is the second in a series on the cryptographic infrastructure of financial markets. The first volume addressed the blockchain settlement infrastructure in financial markets from a technical and operational perspective. This volume addresses the quantum threat to that infrastructure and the path to securing it. Together, they are intended to equip the practitioners who build and govern settlement infrastructure with the technical and regulatory understanding they need to navigate the transition to the quantum era.

Paris, 2026

Post-Quantum Settlement Infrastructure

Volume II

Quantum computers will not merely be faster classical machines — they will break the asymmetric cryptography on which every digital signature, TLS handshake, and encrypted settlement message currently relies. Shor's algorithm factors large integers in polynomial time; the ECDSA keys protecting today's blockchain infrastructure offer no resistance.

This volume builds the technical and strategic case for migration to post-quantum cryptography before a cryptographically relevant quantum computer arrives. It covers the 2024 NIST standards (ML-KEM, ML-DSA, SLH-DSA), the mathematics of lattice-based and hash-based schemes, hybrid transition architectures, and the specific challenges of migrating distributed ledger infrastructure. The final chapters translate the standards into working Python code and map the emerging regulatory landscape from DORA to CNSA 2.0.

Topics covered

Shor's & Grover's algorithms • CRQC timeline • Harvest-now-decrypt-later • NIST 2024 standards • Lattice cryptography • Hash-based signatures • QKD & QRNG • Hybrid transition schemes • Quantum-safe DLT architecture • Regulatory framework • ML-DSA & ML-KEM in Python

Abdelkader BOUSABAA — *University of Paris-Saclay*

Researcher and educator specialising in financial market infrastructure, distributed ledger technology, and post-quantum cryptography. This two-volume series bridges capital markets practice and the mathematics of next-generation settlement systems.

FINANCIAL BLOCKCHAIN PROJECT