

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

First Edition — 2025

SEVEN LIONS EDITIONS

Post-Quantum Settlement Infrastructure: Securing Financial Markets Against the Quantum Threat

Copyright © 2025 Seven Lions Editions.

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, without the prior written permission of the author, except in the case of brief quotations embodied in critical reviews and certain other non-commercial uses permitted by copyright law.

First Edition

ISBN : 979-8-19-536472-4

This is Volume II of *Blockchain for Financial Markets*. Familiarity with Volume I is helpful but not required; this volume is designed to stand alone.

The companion website (financial-blockchain-project.com) provides interactive diagrams, full source code, and updated regulatory guidance freely available to all readers.

The opinions expressed in this work are those of the author and do not necessarily represent the views of any institution or regulatory body.

*To those who build the infrastructure of trust —
and to those who will rebuild it
before the key is found.*

Contents

Preface	xiii
I The Quantum Threat	1
1 The Quantum Computer: Intuition Before Equations	3
1.1 The Bit and the Qubit	3
1.2 Entanglement: Correlations That Defy Distance	5
1.3 How Quantum Computers Actually Compute	5
1.3.1 Quantum Gates	5
1.3.2 The Role of Interference	6
1.4 The Central Obstacle: Decoherence	6
1.5 Physical Qubits Versus Logical Qubits	7
1.6 A Brief Map of Quantum Hardware	8
1.7 What This Means for Financial Market Infrastructure	9
1.8 From Intuition to Action	10
2 Shor’s Algorithm: Why ECDSA Is Doomed	13
2.1 What ECDSA Actually Does	13
2.1.1 The Problem It Solves	13
2.1.2 The Geometry of Elliptic Curves	14
2.1.3 How a Signature Is Created and Verified	15
2.2 The Hidden Structure That Shor Exploits	15
2.2.1 From Discrete Logarithm to Period Finding	15
2.2.2 The Intuition of the Quantum Fourier Transform	16
2.3 How Many Qubits Does It Actually Take?	17
2.4 The Specific Vulnerability of Blockchain Settlement	17
2.5 What Shor’s Algorithm Cannot Do	19

2.6	The Chapter in One Sentence	20
3	Grover’s Algorithm: The Partial Threat	21
3.1	How Grover’s Algorithm Works	22
3.1.1	The Oracle and the Amplitude Amplification	22
3.1.2	Why the Speedup Is Quadratic, Not Exponential	23
3.2	The Effect on Hash Functions	23
3.2.1	What Hash Functions Do in a Settlement Blockchain	23
3.2.2	Grover’s Effect on SHA-256	24
3.3	The Effect on Symmetric Encryption	25
3.4	The Effect on Proof of Work	26
3.5	The Effect on Hash-Based Commitments in Smart Contracts	27
3.6	A Comparative Map of the Quantum Threat	27
3.7	What This Means Concretely for Settlement Platforms	29
3.8	The Chapter in One Sentence	30
4	The CRQC Timeline: When to Plan the Migration	31
4.1	The Mosca Inequality: The Framework for Urgency	32
4.2	The State of Quantum Hardware in 2025	33
4.2.1	IBM’s Superconducting Programme	33
4.2.2	Google’s Willow Processor	33
4.2.3	Trapped Ion Systems: IonQ and Quantinuum	34
4.2.4	The Consensus on Timing	34
4.3	Why “Q-Day” Is a Misleading Concept	35
4.4	The Error Correction Gap and Its Rate of Closure	36
4.5	What the Regulatory Timeline Implies	37
4.6	Translating the Timeline into a Migration Plan	39
5	Harvest Now, Decrypt Later: The Silent Attack	41
5.1	The Mechanics of the Attack	41
5.1.1	Why No Intrusion Is Required	42
5.1.2	The Three Layers of Exposure	42
5.2	Who Is Harvesting?	43
5.3	What Has Already Happened Cannot Be Undone	44
5.4	The Forward-Looking Mitigations	45
5.4.1	Migrate to Post-Quantum Signatures Immediately for New Transactions	45
5.4.2	Migrate to Post-Quantum Key Exchange in All Network Communications	46

5.4.3	Segment Data by Sensitivity and Shelf Life	46
5.5	The Special Case of Smart Contract Logic	47
5.6	The Urgency Calculus Revisited	48
5.7	Part I in Retrospect	49
II	The Post-Quantum Arsenal	51
6	The NIST 2024 Standards: A Map of the Territory	53
6.1	The Logic of the Competition	54
6.1.1	Why a Competition Rather Than a Committee	54
6.1.2	The Four Rounds of Evaluation	54
6.2	The Four Standardised Algorithms	55
6.2.1	ML-KEM: Key Encapsulation (FIPS 203)	55
6.2.2	ML-DSA: Digital Signatures (FIPS 204)	56
6.2.3	SLH-DSA: Hash-Based Signatures (FIPS 205)	56
6.2.4	FN-DSA: Falcon (In Progress)	57
6.3	The Diversity Principle	57
6.4	The Numbers That Matter for Settlement Infrastructure	58
6.5	Choosing the Right Algorithm for Each Use Case	60
6.6	The Standards as a Starting Point, Not an Endpoint	61
7	Lattice Cryptography: The Mathematics of Hard Geometry	63
7.1	Why Lattices?	63
7.2	What Is a Lattice?	64
7.2.1	The Geometry of Hard Lattices	65
7.3	Learning With Errors: The Foundation	65
7.3.1	The Intuition: A Noisy System of Equations	66
7.3.2	The Formal LWE Definition	67
7.3.3	Module LWE: Scaling Up Efficiently	67
7.4	How ML-KEM (Kyber) Works	68
7.4.1	The Mental Model: A Noisy Padlock	68
7.4.2	Key Generation	68
7.4.3	Encapsulation	68
7.4.4	Decapsulation	69
7.5	How ML-DSA (Dilithium) Works	70
7.5.1	The Mental Model: A Commitment That Cannot Be Faked	70

7.5.2	The Fiat-Shamir Transform	70
7.5.3	Key Generation	70
7.5.4	Signing	70
7.5.5	Verification	71
7.6	Performance: The Good News	71
7.7	The Rejection Sampling Gap	72
7.8	Implications for Settlement Infrastructure	72
7.8.1	Transaction Signing at Scale	73
7.8.2	TLS Handshakes for Settlement Messaging	73
7.8.3	Smart Contract and On-Chain Signature Verification	73
7.8.4	Key Lifecycle and Agility	74
7.9	What the Next Chapter Covers	75
8	Hash-Based Signatures: SPHINCS+ and the Minimal Assumption	77
8.1	One-Time Signatures: The Starting Point	78
8.1.1	The Lamport Signature	78
8.1.2	Winternitz One-Time Signatures	79
8.2	Merkle Trees: Signing Many Messages with One Key	79
8.2.1	Building the Tree	79
8.3	XMSS and Its Statefulness Challenge	80
8.4	SLH-DSA (SPHINCS+): Stateless Hash-Based Signatures	81
8.4.1	The Hypertree Architecture	81
8.4.2	Stateless Operation Through Pseudorandomness	81
8.4.3	FORS: The Few-Time Signature	82
8.5	Concrete Parameters and Sizes	82
8.6	When to Use SLH-DSA	83
8.6.1	Root Certificates and Long-Lived Identity Keys	83
8.6.2	Regulatory Records with Decade-Long Retention Obligations	84
8.6.3	Governance and Smart Contract Administration	84
8.7	Grover's Algorithm and Hash-Based Security	85
8.8	Implementation Considerations for Settlement Infrastructure	85
8.9	The Diversity Principle in Practice	87
9	Quantum Key Distribution: Security from Physics	89
9.1	The BB84 Protocol: The First Quantum Key Exchange	90
9.1.1	The Intuition: Measuring Disturbs	90
9.1.2	The Protocol Step by Step	91

9.1.3	Why This Is Unconditionally Secure	91
9.2	E91 and Device-Independent QKD	92
9.3	The Practical Limitations of QKD	93
9.3.1	Distance Limitations	93
9.3.2	Key Rate Limitations	93
9.3.3	Authentication Requirement	94
9.4	Current QKD Deployments in Financial Infrastructure	95
9.5	Satellite QKD: Extending the Range	96
9.6	The Honest Assessment: QKD's Role in Settlement Infrastructure	97
9.7	Looking Ahead: Quantum Networks and the Quantum Internet	98
10	Quantum Random Numbers: True Randomness for Cryptography	101
10.1	Why Classical Pseudorandomness Is Not Enough	102
10.1.1	The Debian OpenSSL Catastrophe	102
10.1.2	The Android Bitcoin Wallet Vulnerability	102
10.1.3	The General Problem: Entropy Starvation	103
10.2	How Quantum Random Number Generators Work	103
10.2.1	Photon Path Splitting	103
10.2.2	Vacuum Fluctuations	104
10.2.3	Photon Arrival Time Jitter	104
10.3	Randomness Extraction and Certification	105
10.4	Integration with Settlement Infrastructure	105
10.4.1	HSM Integration	105
10.4.2	Transaction Nonce Generation	106
10.4.3	TLS Session Key Material	106
10.5	QRNG and the Regulatory Landscape	107
10.6	The Seed of Trust	108
10.7	Closing Part II	109
III	Migration and Applications	111
11	Why Migrating a Blockchain Is Different	113
11.1	The Seven Structural Challenges	114
11.1.1	Immutability as a Feature That Becomes a Liability	114
11.1.2	No Single Owner, No Single Migration Decision	115
11.1.3	Consensus Protocol Integrity During Transition	115

11.1.4	Smart Contract Code as Frozen Cryptographic Logic	116
11.1.5	Key Derivation and Hierarchical Deterministic Wallets	117
11.1.6	Certificate Chains and Identity Infrastructure	117
11.1.7	Regulatory Reporting and Audit Trail Continuity	117
11.2	The Two-Phase Migration Protocol	118
11.2.1	Phase 1: Hybrid Operation	118
11.2.2	Phase 2: ECDSA Retirement	119
11.3	The Governance Framework for Migration	119
11.4	The Message Format Problem	121
11.5	The Historical Records Problem	121
11.6	What Cannot Be Fixed: Accepting Residual Risk	123
12	Hybrid Schemes: The Transition Architecture	125
12.1	The Fundamental Principle	125
12.2	Hybrid Key Encapsulation in TLS 1.3	126
12.2.1	X25519Kyber768: The Deployed Standard	127
12.2.2	IANA-Registered Hybrid Suites	128
12.3	Hybrid Digital Signatures	128
12.3.1	The Dual-Signature Construction	128
12.3.2	Composite Signatures	129
12.4	Hybrid Certificates	130
12.4.1	Dual-Algorithm Certificates	130
12.4.2	Composite Public Key Certificates	130
12.5	Hybrid Key Management in HSMs	131
12.6	Algorithm Negotiation and the Downgrade Attack	132
12.7	The Interoperability Imperative	132
12.8	Hybrid Schemes as a Permanent Feature	134
13	Quantum-Safe DLT Architecture	137
13.1	The Seven-Layer Security Model	137
13.2	Layer 1 — Entropy and Key Generation	138
13.3	Layer 2 — Key Storage and HSM	139
13.4	Layer 3 — Transport Security	140
13.5	Layer 4 — Node Authentication	141
13.6	Layer 5 — Transaction Signing	142
13.7	Layer 6 — Consensus Protocol	143
13.8	Layer 7 — Ledger and Archival	143

13.9 Cross-Cutting Concerns: Cryptographic Agility	144
13.10 The Quantum-Safe Settlement Network: An Integrated View	146
14 The Regulatory Framework	149
14.1 NIST: The Algorithmic Foundation	149
14.2 NSA and CNSA 2.0: The US National Security Mandate	150
14.3 DORA: The European Union’s Digital Resilience Framework	151
14.3.1 ICT Risk Management (Articles 5–16)	152
14.3.2 ICT Change Management (Article 8(6))	152
14.3.3 Digital Operational Resilience Testing (Articles 24–27)	153
14.3.4 ICT Third-Party Risk (Articles 28–44)	153
14.4 The European Banking Authority and ECB Guidance	154
14.5 CPMI-IOSCO: Global Principles for Financial Market Infrastructures	154
14.6 The SWIFT Community and ISO 20022	155
14.7 National Cybersecurity Agencies	156
14.8 Liability and Legal Risk	157
14.9 Building a Compliant Programme	158
15 Code: Post-Quantum Signatures on a Settlement Ledger	161
15.1 Environment Setup	161
15.2 ML-DSA Signatures: Signing a Settlement Instruction	162
15.3 The Dual-Signature Pattern	164
15.4 ML-KEM Key Encapsulation: Protecting the Settlement Bus	166
15.5 A Minimal Post-Quantum Settlement Ledger	167
15.6 Measuring the Performance Impact	172
15.7 SLH-DSA for Archival Records	173
15.8 Cryptographic Agility in Code	174
15.9 What the Code Does Not Show	176
Epilogue: The Quantum-Safe Settlement System	179
Bibliography	185

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

ALSO IN THIS SERIES

Blockchain for Financial Markets

VOLUME I

A Practitioner's Guide to Settlement, Tokenization, and Distributed Ledgers

Volume I examines why today's settlement infrastructure fails — from T+2 delays to cascade settlement failures — and builds the case for a blockchain-based alternative. It develops each component of a settlement DLT from first principles: the data structure, consensus mechanisms, smart contract automation, tokenisation of securities and cash, and the governance models required for institutional adoption. Two hands-on chapters provide working Python and Solidity implementations of a DVP settlement chain.

financial-blockchain-project.com

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.