BEFORE Q-DAY

What to Expect While We’re Expecting



Douglas B.

Before Q-Day

What to Expect While We're Expecting

How to Prepare Your Bitcoin and Crypto for the Quantum Change: What's Settled, What's Coming, and What to Do in the Meantime

Douglas J. Brownfield

Before Q-Day

Copyright © 2026 Douglas J. Brownfield

All rights reserved. No part of this book may be reproduced, stored, or transmitted in any form or by any means — electronic, mechanical, photocopying, recording, or otherwise — without the prior written permission of the author, except for brief quotations used in reviews.

This book was written with the assistance of AI tools, working from the author's own practice, questions, and editorial direction, and from a research record built for this book from primary sources. Facts are stated as of 2026; where the record is unfinished or disputed, the book says so rather than guess.

The art in this book is the author's own painting, photographed at four stages of its making and reproduced with cleanup only — nothing added, nothing painted over. Art by Douglas John Brownfield.

Introduction

This is a book about a change that has already been scheduled.

Somewhere in the next decade, the mathematics that proves you own your coins is going to be replaced. Not patched — replaced. The signatures your wallet makes today belong to a family of problems that a large enough quantum computer can solve backwards, working from a public key to the private key it was supposed to protect. No such computer exists yet. That sentence is true as this book is written, in November 2026, and this book will keep returning to it, because everything honest about this subject hangs on knowing exactly which parts are settled and which parts are still guesses.

Here is what is settled.

The replacement signatures exist. In August 2024, after an eight-year public competition, the United States National Institute of Standards and Technology published the finished standards: ML-DSA and SLH-DSA for signatures, built to survive the machine that breaks the old ones. The deadlines exist too. The same institute has set the dates after which the old algorithms are deprecated (2030) and then disallowed (2035) in the systems it governs, and governments and standards bodies on several continents have published timelines in the same window. And the cost of the change is known, because it can be measured in bytes: a signature that takes about 64 bytes today will take roughly 2,400 to 4,600 bytes in its standard replacement, and nearly 50,000 in the most conservative one. The future, in this case, is not mysterious. It is merely large.

Here is what is not settled. Nobody knows when a quantum computer capable of breaking today's signatures will be built. The honest estimates from the people building them range across years to decades, and this book will show you those estimates with their sources rather than pick one and pretend. Nobody has chosen the post-quantum signature scheme for Bitcoin; there are drafts, and drafts are all they are. And nobody — no foundation, no wallet maker, no standards body — has yet written the instructions you will one day follow to move your coins, because the address type you will move them to does not exist yet.

A book that hid those gaps would be selling you something. This one takes the other road, and it is worth saying plainly what that road gives you:

For everything you need to do **now**, this book contains complete solutions. The practices that keep a holder safe in the meantime — how addresses expose their keys and when, how to keep a seed the way it deserves to be kept, how to sign without your keys ever touching the internet, how to change devices without changing wallets, and how to change wallets when a device is in doubt — are finished, documented, and testable today. Nothing in that half of the book depends on a roadmap.

For the change itself, this book contains the complete map as it stands: the standards, the deadlines, the exposure — how much coin sits where a future machine could reach it, counted several ways by several counters — and the state of each major chain, including one that has already made the crossing and can be visited today. Where the map runs out, it says so, in a chapter of unknowns that is part of the book and not an apology appended

to it.

You will not find quantum physics here beyond the one idea the whole thing turns on: a signature is a proof made from a secret, and a new kind of computer threatens the hiding of that secret. This is not a book about the machine. It is a book about a transition — written for the people who will have to make it, holding what they hold, with the tools that exist today.

It is dated, deliberately. November 2026. When the facts move, the facts that were true on that date will still be the record of what a careful holder knew, and when.

— The Author



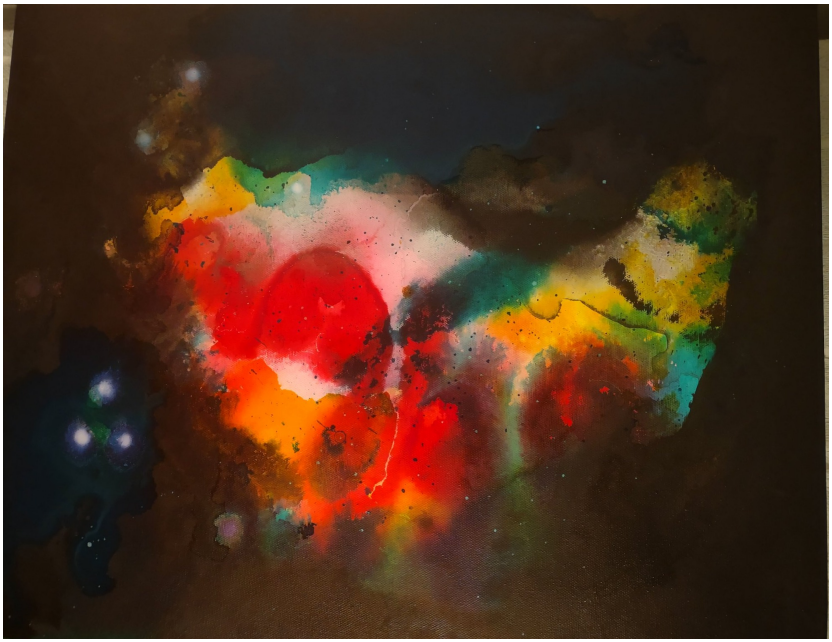
Stage 0 — the first washes. Art by Douglas John Brownfield.



Stage 1 — the full colour nebula. Art by Douglas John Brownfield.



Stage 2 — the starfield. Art by Douglas John Brownfield.



Stage 3 — the deep field. Art by Douglas John Brownfield.

Part One — The Change That Is Coming

Chapter 1 — What a Signature Is, and What a Quantum Computer Breaks

Every coin you hold is controlled by a pair of keys. The private key is a secret number. The public key is derived from it by a one-way piece of mathematics: easy to compute going forward, hopeless to reverse. When you spend, your wallet uses the private key to produce a *signature* — a proof that the holder of

the secret approved this transaction, which anyone can check against the public key without learning the secret.

The whole of self-custody rests on that one-way street. And the one-way street rests on a problem: given a public key, finding the private key means solving the discrete logarithm problem, which for a classical computer takes longer than the age of the universe at the sizes wallets use.

A quantum computer changes the problem, not by trying harder but by working differently. Shor's algorithm, published in 1994, solves exactly this family of problems efficiently. A sufficiently large, error-corrected quantum computer — the field's term is a *cryptographically relevant quantum computer* — could take a public key and compute the private key from it. Not guess it. Derive it.

Two clarifications separate this book from the noise around it.

First: what breaks is **signatures** (and key exchange), not hashes. Bitcoin's addresses and mining rest on hash functions; a quantum computer speeds up hash attacks only modestly (Grover's algorithm), and modestly is survivable. The exposed half of the design is the signature.

Second: for signatures, there is no "harvest now, decrypt later." That danger belongs to encryption — an adversary records encrypted traffic today and decrypts it when the machine arrives. Public keys on a blockchain are not intercepted secrets; they are *published*, permanently, by design. The signature danger is better named **record now, forge later**: every exposed public key is already in the adversary's hands, waiting only for the machine. Chapter 14 will show you exactly which of your

keys are exposed, and when they became so.

Chapter 2 — The State of the Machine

Measured facts first. As of November 2026:

has broken RSA or any elliptic-curve key. None is close in the only currency that counts — error-corrected *logical* qubits — which the world's best laboratories currently field in the dozens.

fast-moving research frontier.

- **No cryptographically relevant quantum computer exists.** None
- What exists are noisy physical qubits in the thousands and a

Now the projections, which is all anyone has — the resource estimates researchers publish for what the attack would take:

estimated in 2017 at roughly **2,330 logical qubits** — far beyond today's dozens, and a measure of the gap.

qubits running 8 hours**. By May 2025 the same lead author had cut that to** under 1 million qubits and under a week** — the target is not moving, but the estimate of the machine needed to hit it fell twenty-fold in six years.

elliptic-curve keys specifically: **fewer than 1,200 logical qubits, under 500,000 physical qubits** on their architecture, with key recovery in *minutes* — and, notably, they withheld the circuits themselves, publishing a zero-knowledge proof that the work is real. Google has set its own post-quantum migration target at 2029.

- Breaking a 256-bit elliptic-curve key (Bitcoin's size) was

- For RSA-2048, the famous 2019 estimate was **20 million noisy
- In March 2026, Google's quantum team published estimates for

Read those three items together and you have the honest picture: the gap between today's machines and the attack is large; the estimates of the machine required keep shrinking; and the people closest to the work behave as if the arrival is a matter of when, not if — while stating, as NIST does, that the timing is unknown and plausibly years to decades away. This book proceeds on exactly that footing. Anyone who gives you a date is guessing. Anyone who tells you there is nothing to prepare for is guessing the other way.

Chapter 3 — The Standards Are Finished

On **13 August 2024**, NIST published the first three finished post-quantum standards, ending an eight-year public competition that began with 82 submissions from around the world:

a shared secret. (Not a signature standard — the distinction matters and the next chapter of the wider world's story, in Chapter 7, turns on it.)

lattice-based scheme (Module-Lattice Digital Signature Algorithm), standardised at three strengths.

stateless hash-based scheme (SPHINCS+), whose security rests on hash functions alone — the most conservative assumptions in the field, paid for in size, as the next chapter shows.

- **FIPS 203 — ML-KEM.** Key establishment: how two parties agree
- **FIPS 204 — ML-DSA.** The primary signature standard: a
- **FIPS 205 — SLH-DSA.** The conservative signature standard: a

Two more facts complete the picture. A fourth signature standard, **FN-DSA** (based on Falcon), is in preparation as FIPS 206 — prized because its signatures are the smallest of the new family — but as of this writing it is **not final**, and no public draft could be confirmed on NIST's own pages. And NIST's work continues: a backup key-establishment algorithm (HQC) was selected in March 2025, and nine additional signature candidates — designs unlike the lattice family, kept as insurance — advanced to a third round in May 2026.

The significance for a holder is not the alphabet. It is that the question "what will replace today's signatures?" now has official answers, with names, parameters, and finished specifications that any wallet maker on Earth can build to. The standards phase of this transition is *over*. What remains is adoption — and adoption, as Chapter 5's deadlines and Chapter 9's history will show, is the slow part.

Chapter 4 — The Size Jump

Here is the transition reduced to one table — public key and signature sizes, in bytes, for what you use today and what replaces it:

Scheme	Public key	Signature
ECDSA (secp256k1, Bitcoin today)	33	~64–71
Ed25519 (Solana, Algorand standard)	32	64
RSA-2048 (for contrast)	256	256
ML-DSA-44	1,312	2,420
ML-DSA-65	1,952	3,309
ML-DSA-87	2,592	4,627
SLH-DSA (range across parameters)	32–64	7,856 – 49,856
Falcon-512 (FN-DSA, not yet final)	897	~666

A signature grows by a factor of roughly **40 to 700**. On a blockchain, signatures are not an abstraction — they are block space, the scarcest resource the system has. The published modelling of what that means (Blockstream's, the most concrete to date) holds Bitcoin's throughput at the current block weight roughly as follows: today's Schnorr signatures sustain about **6.5 transactions per second**; ML-DSA at mid-strength, about **0.5**; SLH-DSA, about **0.36**; a compact hash-based design (SHRINCS, from the draft literature) recovers about **3**. And the migration itself must fit through the same pipe: Chaincode's research estimates that moving every one of Bitcoin's ~190 million unspent outputs would take **76 days if it had the entire block space to itself** — 305 to 568 days at a realistic quarter share, and roughly **seven years** for a comprehensive migration (five at best, fifteen at worst).

What no one has published, as of this writing, is honest modelling of the *fees* a holder would pay to migrate in a crowded market. That number does not exist yet, and this book will not invent it. What the arithmetic already proves is the strategic fact: **the migration cannot be done in a hurry, by everyone, at the last minute.** Which is why it is being scheduled a decade out — the subject of the next chapter.

Chapter 5 — The Deadlines

Governments have begun converting "someday" into dates. They are not all the same kind of date, and this chapter grades them as it goes: **binding** (a mandate on the systems named) versus **guidance** (official direction others are expected to follow).

for the algorithms themselves: quantum-vulnerable public-key algorithms are **deprecated after 2030 and disallowed after 2035** in the federal standards framework.

phases the change by use: software and firmware signing prefers the new algorithms from 2025 and requires them exclusively by **2030**; web and cloud services by **2033**; from **1 January 2027**, new equipment purchases for national-security use must support the new standards — and for signatures, only the strongest parameter sets qualify (ML-DSA-87).

inventories and migration plans were due in autumn 2026, with key establishment for high-value assets to complete by **31 December 2030** and signatures by **31 December 2031**.

2025): begin by end of **2026**, high-risk systems migrated by end of **2030**, everything feasible by end of **2035**.

2028, priority migrations by **2031**, completion by **2035**.

and elliptic-curve cryptography by **end of 2030** — among the earliest hard dates in the world.

April 2026, high-priority systems by end of **2031**, the rest by end of **2035**. Germany's BSI and France's ANSSI run comparable programmes in the same window, with hybrid (classical + post-quantum together) required or expected in the early phases.

- **NIST IR 8547** (finalised October 2026) sets the anchor dates
- **NSA's CNSA 2.0** (binding on US national-security systems)
- **US federal orders (2026)** make it operational: cryptographic
- **The European Union's** coordinated roadmap (guidance, June
- **The United Kingdom's NCSC** (guidance, "indicative"): plans by
- **Australia's ASD** (official recommendation): stop using RSA
- **Canada's CCCS roadmap** (policy-backed): migration plans by

Stand back and the pattern is unmistakable: independent institutions, on several continents, none of them selling anything, have converged on the same decade — **the work of the late 2020s, the deadlines of the early 2030s, completion by 2035.** Your wallet's signature scheme is a tiny part of what they are moving. But it is being moved on their schedule, not the

market's — and the chains in Part Two will have to fit inside it.

Chapter 6 — Exposure — How Much, and Whose

Chapter 1 named the mechanism; this chapter counts it. A coin is exposed if its public key is visible on the chain — either because it always was (the earliest format, P2PK; and Taproot outputs, whose key is visible at rest), or because the address was spent from once and then reused, which publishes the key at the spend.

The counters do not agree, because they do not count the same thing the same way. Here are the published totals for Bitcoin, with their counters and dates, in the open:

million BTC, roughly 25%** of supply.

walk): **7,126,359 BTC — 35.4% of supply** — split into 1,934,735 BTC always exposed and 5,191,624 BTC exposed by reuse. Its own revisions moved its headline from 25.3% to 35.4% within months as its method was corrected — the counters themselves will tell you the figure is methodology, all the way down.

near **6.7 million BTC** on its method.

- **Deloitte** (the earliest widely cited study): **over 4
- **Chaincode** (2025): **6.26 million BTC.**
- **Glassnode** (May 2026): **6.04 million BTC, roughly 30%.**
- **ARK Invest / Unchained** (March 2026): **34.6%.**

- **ChainQuery** (snapshot 1 November 2026, weekly full-chain
- **Project Eleven's Risq List** tracks the same ground and lands

Inside every total sits the most famous slice: roughly **1.1 million BTC** in the earliest P2PK format, attributed to Bitcoin's creator — keys public since 2009, unmoved since, and (Chapter 22 will argue the point properly) possibly the world's most-watched tripwire.

For Ethereum's externally owned accounts, **no sourced aggregate figure exists** as of this writing — the exposure there runs through a different mechanism (an account's key is revealed by its first outgoing transaction, and active accounts have all made one), and nobody has published the count. This book notes the absence rather than filling it.

What a holder should take from this chapter is not a percentage. It is that the exposed share is measured in **millions of coins and a third of the supply** on every serious count — large enough that the question of Part Four, what happens to coins that never move, is not a corner case. It is a third of the system.

Part Two — Where Each Chain Stands

Chapter 7 — The Ones Who Already Crossed

Before judging the chains for slowness, look at the industries that have already done this — because they show both that the crossing is possible and which half of it is hard.

Messaging went first. Signal — whose protocol also underlies WhatsApp — added post-quantum key agreement in September 2023 (PQXDH: the classical X25519 exchange and Kyber-1024, run together, so an attacker must break both), and followed in October 2025 with a full post-quantum ratchet (SPQR), so the protection renews with every message, not just the first. Apple announced iMessage PQ3 in February 2024 and shipped it that spring: hybrid key establishment plus *periodic post-quantum rekeying* — a design Apple rated above every other deployed messaging protocol. **The tools you already use** crossed too: OpenSSH has defaulted to a post-quantum hybrid key exchange since version 9.0 in April 2022 (and to the ML-KEM hybrid since 10.0 in 2025); Chrome turned on hybrid post-quantum key exchange in 2023 and standardised it in November 2024; Cloudflare has offered it since October 2022, and by late October 2025 **more than half of all human-initiated traffic across Cloudflare's network was already post-quantum protected.** OpenSSL, Go, and Firefox carry the same default. You have probably used post-quantum cryptography today. You just weren't told, which is what a finished migration looks like.

Now the nuance this book exists to carry: **almost everything above is key exchange, not signatures.** Those systems migrated the *confidentiality* half — agreeing keys a quantum computer can't later unwrap. The *authenticity* half — signatures — lags everywhere: OpenSSH states plainly that post-quantum signatures are **not yet supported**; Signal's and Apple's user authentication remains classical. The world has crossed the river you can cross with KEMs. The signature crossing — the one your wallet needs — has been completed at scale by no one. The chains in this part are not behind the world on the hard half. The

world is with them, unfinished, on the same half.

Chapter 8 — Bitcoin — Drafts, Not Decisions

Bitcoin's post-quantum state, as of November 2026, fits in one paragraph — and then deserves three pages of context, because the paragraph is easy to misread as inaction.

Nothing is activated. No post-quantum scheme is chosen. What exists is drafts. BIP-360 (merged as a draft in February 2026) proposes P2MR — essentially Taproot with the key-path spend removed, so no public key sits exposed in the output. It contains **no post-quantum signature at all**; it is groundwork, not the crossing. BIP-361 (April 2026) proposes the hard part as policy: some years after a post-quantum address type activates, stop deposits to quantum-vulnerable types, and some years after that, make coins in them unspendable by the old signatures — with a zero-knowledge proof-of-seed path by which a living owner could still recover. Its lead author, Jameson Lopp, argues the case bluntly: coins recovered by a quantum attacker "only make everyone else's coins worth less — think of it as a theft from everyone." A third draft family, SHRINCS, works on shrinking hash-based signatures toward practicality (a 48-byte public key; signatures from a few hundred bytes upward, depending on the version of the draft you read — its reviewers note the security proof is still a TODO). And in January 2026 a company launched a public test network implementing BIP-360 with ML-DSA signatures, so the mechanics can be exercised even while the proposals are undecided.

Context, then. The unresolved question is not the cryptography — several buildable candidates exist. It is the question of

Chapter 6's third-of-the-supply: what does the network do about coins whose owners never move them — the lost, the dead, and the patient, including the creator's own million? Freeze them by consensus, and Bitcoin breaks a promise it has kept since 2009 (that valid coins remain spendable). Leave them, and the first cryptographically relevant quantum computer inherits them. That is a genuinely hard question wearing a technical costume, and it is being argued in the open, in drafts, by named people — which is where Bitcoin makes all its hard decisions. The counter-arguments get their own full hearing in Chapter 22. For the map, the state is: **the debate is the work, and the debate is underway.**

Chapter 9 — A Short History of Bitcoin

Twelve dates carry the holder's version of the story — and notice, as you read, that it is mostly a history of *addresses and signatures*:

Electronic Cash System," posted by Satoshi Nakamoto.

newspaper headline: *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."* Its output is P2PK — the raw public key, exposed from day one. ECDSA signs everything.

Finney, 10 BTC.

"1…" form. Keys hidden until spent. (Chapter 14's rule is born here.)

pizzas.

One seed, many keys.

24-word phrases every holder now knows.

addresses. Still ECDSA.

change of signature scheme in Bitcoin's history — Schnorr signatures for P2TR outputs, "bc1p" — and, per Chapter 14, keys visible at rest.

- **31 Oct 2008** — The whitepaper, "Bitcoin: A Peer-to-Peer
- **3 Jan 2009** — The genesis block. Its coinbase carries a
- **12 Jan 2009** — First transfer between people: Satoshi to Hal
- **Jan 2009** — P2PKH appears: the hashed address, the familiar
- **22 May 2010** — First known purchase: 10,000 BTC for two
- **11 Feb 2012** — BIP-32: hierarchical deterministic wallets.
- **1 Apr 2012** — P2SH activates ("3…" addresses).
- **28 Nov 2012** — First halving: the block reward falls 50 → 25.
- **10 Sep 2013** — BIP-39: the seed becomes words — the 12- and
- **24 Aug 2017** — SegWit activates; P2WPKH gives the "bc1q"
- **14 Nov 2021** — Taproot activates (BIPs 340–342): the first

Seventeen years, three address eras, one signature change. The next change of signature scheme — the post-quantum one — will be the second in the system's life, and the first that holders *didn't* choose one wallet at a time, but must complete against a deadline set outside the system entirely.

Chapter 10 — Ethereum — The Account Route

Ethereum's problem is shaped differently, and so is its answer. An Ethereum account's public key is revealed by its first outgoing transaction — which is to say, essentially every active account has already revealed it. There is no hash hiding to preserve, and Chapter 6 recorded that nobody has even published the aggregate count.

The foundation's programme, organised openly since January 2026, counts four vulnerable layers across the stack and takes the route only Ethereum can take: **account abstraction.** Because an Ethereum account can be a small program rather than a fixed key, its signature scheme can become a *choice* — upgraded per account, opt-in, without a network-wide flag day. The vehicle is EIP-8141, targeted at the Hegotá upgrade; on the consensus side, researchers are building post-quantum signature aggregation (leanXMSS, inside the leanVM research track) with a planning horizon around 2029. The official guidance to users today is exactly one sentence long, in substance: **do nothing now** — nothing post-quantum runs in production, and when the time comes, the upgrade is designed to arrive account by account.

For the map: Ethereum has a *mechanism* Bitcoin lacks (programmable accounts) and the same present tense (nothing shipped). Its holders' migration, when it comes, should be the gentlest of any major chain's — a setting changed, not a fortune moved.

Chapter 11 — Solana and the Rest

layer. What it has is the experiment: an opt-in **Winternitz Vault** (January 2025) — a hash-based, one-time-signature vault where

each transfer burns a fresh key, exactly the discipline one-time signatures demand — plus a public post-quantum testnet running since December 2025, and reported (not officially confirmed) convergence among its client teams on Falcon. The active lab is active; its production chain is classical.

phased, with ML-DSA signatures planned for its Devnet in the second half of 2026 and a full transition targeted at **2028** by validator amendment. Its own audit figure is a useful contrast to Bitcoin's: **0.03%** of XRP sits in vulnerable dormant accounts.

Falcon-based event signing once the Falcon standard exists; a post-quantum user key type targeted at 2027). Nothing shipped.

(June 2026) and a dedicated post-quantum experimental network (September 2026). Mainnet: classical, no date.

shipped; its founder has publicly cautioned that premature post-quantum cryptography could slow the chain roughly tenfold.

began with hash-based one-time signatures (Winternitz), then **replaced them with Ed25519 in 2021** for practicality — and has not been quantum-resistant since, despite two official Europol reports in October 2026 still describing it as post-quantum. Check the chain, not the summaries.

(XMSS) since 2018 — the existence proof that a classical-era chain *can* run post-quantum signatures from birth, at the cost of managing stateful keys — and is testing ML-DSA for its 2.0.

- **Solana** signs with Ed25519 and has not changed its base
- **The XRP Ledger** has an official programme (April 2026):
- **Hedera** has announced its direction (hybrid Ed25519 +

- **Tezos** has ML-DSA-44 accounts live behind a testnet flag
- **Cardano** has a research programme dating to 2018 and nothing
- **Cosmos**: a forum concept. Recorded as such.
- **IOTA** is the cautionary tale in the other direction: it
- **QRL** has signed every transaction with a hash-based scheme

Chapter 12 — Case Study — Algorand, the Destination Already Running

One major chain has made the crossing, in stages a holder can inspect:

Algorand's ledger state is compressed into a certificate signed with **Falcon** by the network's node runners — post-quantum signatures doing production work, proving the chain's history to the outside world.

user account (through a logic-signature account): a person, not the protocol, signing post-quantum on mainnet.

release, any holder can generate a Falcon-1024 account from the familiar 25-word mnemonic, in the standard SDKs and the Pera wallet — and, the detail that matters most for Part Four, an existing account can be **rekeyed** to a Falcon key *while keeping its address*. The migration, on Algorand, turned out to be a key change, not a move.

- **7 September 2022 — State Proofs.** Every 256 rounds,
- **3 November 2025 — the first Falcon-signed transaction** by a

- **August 2026 — native Falcon-1024 accounts.** With the v5.0.0

Algorand states its own limits as plainly as its milestones, and this book repeats them in the same breath: the Falcon accounts are **opt-in, not the default** — standard accounts still sign Ed25519; the consensus layer and its VRF still run on classical signatures; and the foundation's own target for *broad* quantum resilience is **end of 2027**. The destination exists. It is a district, not yet the whole city.

Why this chain earns a chapter in a book whose worked example is Bitcoin: because every other chapter in this part describes intentions, drafts, and programmes — and holders, reasonably, discount intentions. Algorand is where the book can stop saying "one day, a holder will" and say "since August 2026, a holder can." The shape of its migration — rekey, keep the address — may or may not be the shape of yours. It is the first working sample of the thing itself.

Chapter 13 — A Short History of Algorand

verifiable random functions (1999) — the tool his chain's consensus would later be built on. In 2012 he shared the ACM Turing Award, computing's highest honour, with Shafi Goldwasser, *"for transformative work that laid the complexity-theoretic foundations for the science of cryptography."* Algorand is a cryptographer's chain in the literal sense.

Zeldovich) and the company's founding.

proof-of-stake* — every round, a block proposer and voting committees are chosen by VRF-based cryptographic sortition, privately, in proportion to stake; blocks are certified and final, with forks designed out. All **10 billion ALGO** were minted at genesis.

transfers, and Layer-1 smart contracts.

platform for the World Cup.

Chapter 12: State Proofs, the first Falcon transaction, native Falcon accounts.

- **The founder.** Silvio Micali, MIT professor, co-inventor of
- **2017** — The Algorand paper (Gilad, Hemo, Micali, Vlachos,
- **June 2019** — Mainnet launch. The design: *pure
- **21 Nov 2019** — Algorand 2.0: standard assets, atomic
- **Oct 2021** — Community governance begins.
- **May 2022** — FIFA names Algorand its official blockchain
- **Sep 2022 → Aug 2026** — The post-quantum sequence of

The middle years hold few holder-level milestones, and this sidebar does not invent any. Algorand's story, for this book's purpose, is a strong beginning, a quiet middle, and then — alone among the majors — the ending arriving early.

Part Three — The Meantime

Everything in this part can be done today, with tools that exist today, and none of it depends on a roadmap. These are the complete solutions the Introduction promised.

Chapter 14 — Address Hygiene — Exposure Begins at First Spend

A Bitcoin address is not a public key. For most address types, it is a *hash* of a public key — a fingerprint that hides the key itself. That distinction is the whole of this chapter, because a quantum attacker needs the public key. What is hidden behind a hash is, for now, hidden from the machine as well.

So exposure has a precise moment: **the first spend.**

the start. Coins sitting in it — including the roughly 1.1 million early coins attributed to Bitcoin's creator — have had their keys public for over a decade.

public key only when you spend. Receive all you like; the key stays hidden. Spend once, and the key is on the chain forever.

visible in the output itself, so Taproot addresses are exposed at rest even before any spend.

attached to every later payment to that address. This is why the oldest advice in Bitcoin — a fresh address for every receipt, which the whitepaper itself recommends in its privacy section — turns out to be quantum advice too.

- The oldest format, P2PK, put the raw public key on the chain from
- The hashed formats (P2PKH, and the SegWit P2WPKH) reveal the
- Taproot (P2TR) is the exception to keep straight: its key is
- Reusing an address after spending from it leaves the revealed key

The practice is simple to state: receive at fresh addresses; treat any address you have spent from as retired for long-term storage; and know which of your addresses are which. Tools now exist that will tell you — public datasets walk the whole chain weekly and will show a holder exactly which of their addresses have a revealed key, and the spend that revealed it. The counters disagree on the global total (their methods differ, and the totals move when the methods are revised), but for a single address the answer is a fact, not an estimate.

Chapter 15 — The Offline Device — Offline Before the Words Go In

A seed phrase is only as safe as the machine that first held it. If the words are generated on, typed into, or restored to a device that is connected to the internet — or ever will be again — then the holder is trusting every network that device has met.

The documented practice of the air-gapped wallet makers is a rule with a strict order of operations:

maker shipped it to be trusted in. AirGap's own FAQ recommends the factory reset before a phone is used as an offline vault, and allows exactly one brief connection — to fetch the app — or none at all, loading the app from an SD card instead.

"usually offline." Offline as a property of the device, the way a safe is heavy as a property of the safe.

device, never shown to any other screen.

1. The device is prepared first: factory reset, in the state the

2. Then the device goes offline. Airplane mode, permanently. Not
3. Only then are the words generated — on the device, by the

Other makers arrive at the same place by different roads: the Coldcard generates and keeps its seed inside a device that has no radio at all; the SeedSigner holds the seed in memory only, for the session only, and forgets it at power-off — stateless by design. The details differ. The principle is one: **the words are born offline and live offline.** A device is not made trustworthy by the seed it holds; the seed is made trustworthy by the device never having been anywhere else.

Chapter 16 — Signing by QR — The Keys Never Touch the Internet

If the signing device never connects, how does anything get signed? By light.

The flow, which is standardised (the transaction format is BIP-174, the Partially Signed Bitcoin Transaction, extended by BIP-370) and shipped interoperably by the major air-gapped makers and the coordinator software holders already use:

your addresses and balances — through your public keys — but it cannot sign. It has nothing to steal.

code — animated, in frames, when it is large (the UR standard exists for exactly this).

the address, the amount, the fee. You check it on the device that holds the keys — the one screen in the flow that cannot be lying to you on behalf of a network.

own.

it. The keys never left the offline device. No cable, no Bluetooth pairing with a connected machine, no moment in which the seed and the internet were in the same room.

1. An online, watch-only wallet builds the transaction. It can see
2. The unsigned transaction travels to the offline device as a QR
3. The offline device shows you the transaction on its own screen:
4. You approve. The device signs and answers with a QR code of its
5. The online wallet scans the signed transaction and broadcasts

This is not a proposal. It is the daily practice of holders using Coldcard with Sparrow, SeedSigner, Keystone, and AirGap, and it is the same shape on other chains wherever an offline signer and an online companion are paired.

Chapter 17 — Restore and Sweep — Two Different Ways to Change Devices

Devices die, get lost, get sold, get doubted. The seed phrase makes the device replaceable — but there are two different moves, and using the wrong one is the most common quiet mistake in self-custody. The definitions here follow the wallet documentation holders have used for years (Electrum's FAQ states them plainly):

Restore recreates the same wallet from the seed. You enter the words on the new device — offline first, per the previous chapter — and the wallet reappears: same keys, same addresses, same history. Nothing moves on the chain, because nothing needs to. Restore is the answer to a *device* problem: the hardware failed, but the seed was never in doubt.

Sweep moves the money. You create a *brand-new* seed on the new device, and then send all the funds from the old wallet to the new wallet's addresses in an ordinary transaction. The old seed is retired — not restored, not kept as a spare, retired. Sweep is the answer to a *seed* problem: the old device was lost or sold, the words may have been seen, the generation of the old seed is in doubt for any reason. A new device restored from a doubtful seed is a doubtful wallet in a clean box; sweeping is what actually closes the question. (A swept key does not join the new wallet — the funds land on keys derived from the new seed only.)

Rule of thumb, stated once: **device in doubt → restore is not enough if the seed shared the doubt; seed in doubt → sweep.** And note what the sweep is, because Part Four will return to it: a move of funds from old keys to new keys, in one ordinary transaction, costing one ordinary fee. Hold that shape in mind.

Chapter 18 — How We Do It

This book's method is not theoretical. It is the practice of the author's own setup, kept small on purpose, and it is offered as a worked example — one holder's arrangement, every part of it rehearsed, rather than a product to buy.

fresh, inexpensive Android phone, factory-reset, taken permanently offline before anything else happened to it. The vault app went on during one brief connection (it can also be loaded by card, with no connection at all). The seed was created on that phone, after it went offline, and has never existed on any other device.

connected machine, never photographed, never spoken to an assistant, never entered anywhere except the offline device and its successor. The author's rule for everyone who helps him — human or otherwise — is absolute: helpers may build anything *around* the wallet; the signing itself is never delegated. No helper ever sees a key. Signing is the holder's act, done on the holder's hardware, at the holder's prompt.

wallet builds; the offline phone scans, shows, signs, answers in light; the online wallet broadcasts.

seed restored if the old seed is sound; a new seed and a sweep the moment it isn't.

nothing parked long-term in an address already spent from.

first signing this setup ever did was a small test transaction, on a test network, whose only job was to prove the flow worked before anything real rode on it. The rule generalises: recovery, too, is rehearsed before it is needed, because the day it is needed is the wrong day to learn it.

hardware was evaluated for this setup, the questions were asked in a fixed order: Where was it made, and by whom? Is it truly air-gapped, or does it merely sign offline between connections? (One well-known candidate, for all its quality, is not air-gapped at all.) Is the chain support you need *named* by the maker, or

hidden inside the phrase "all EVM chains"? What do the maker's own pages say today — not the reviews, not the memory of last year's model? The cheapest option on the table turned out to be the phone above; the vetting is what made it a decision instead of a guess.

- **The signer is a phone that will never be a phone again.** A
- **The words live on paper and nowhere else.** Never typed into a
- **The daily flow is the QR flow of Chapter 16.** The online
- **Changes of device follow Chapter 17.** A new phone gets the
- **Addresses follow Chapter 14.** Fresh address for every receipt;
- **New arrangements are rehearsed before they are trusted.** The
- **Signers are vetted before they are believed.** When dedicated

None of this required wealth, expertise, or exotic equipment. It required deciding that the device is replaceable and the words are the wallet — and then behaving that way on ordinary days, so that the behaviour is already there on the extraordinary ones.

Part Four — The Move, When It Comes

Chapter 19 — What the Migration Will Actually Be

Strip away the whitepapers and the migration, for a holder, is one of the two moves you already know from Chapter 17 — chosen by the chain, not by you:

post-quantum address type exists and your wallet supports it, you will send your coins from your old addresses to your new ones, in an ordinary transaction, signed by your old keys. That signature is the last classical signature the migration asks of you, and it must be made while classical signatures are still trustworthy — which is the entire reason the work is scheduled years ahead of any plausible machine. Your seed does not change its nature: the same words that restore your wallet today will derive your new keys then, in whatever wallet you trust at the time. Nothing about the move requires new hardware, a new system, or a new you. It requires a *destination*, which does not exist yet, and time inside the window, which Chapter 4's arithmetic (76 days at total block capacity; years at a realistic share) shows is scarcer than it sounds.

(Chapter 12): the account keeps its address and history, and its controlling key is exchanged for a Falcon key. The move took the form of a setting, not a journey.

program; its signature scheme becomes one of its settings, changed per account, opt-in (Chapter 10).

- **On Bitcoin's shape (UTXO chains): a sweep.** When a
- **On Algorand's shape: a rekey.** Already demonstrated
- **On Ethereum's shape: an account upgrade.** The account is a

Around those three shapes sit the questions nobody has answered, and this book leaves them where it found them: the

coins of the lost and the dead (Chapter 8's debate; Chapter 21's list); the fees a crowded migration window will charge (unmodelled, Chapter 4); and whether hybrid signatures — classical and post-quantum side by side, the pattern the web's migration used and one hardware maker already uses for its own firmware — will be offered to chain accounts at all. No chain has shipped them for holders as of this writing.

What can be said whole: the migration is a **move, not a rebuild**. Every practice in Part Three — fresh addresses, an offline seed, a rehearsed recovery, a wallet you chose on purpose — is precisely the posture from which the move is one transaction instead of a crisis. The meantime was the preparation. That is not a slogan; it is the mechanics.

Chapter 20 — Lightning and the Layers Above

This chapter is short because the record is short, and the book prints it anyway, because a holder with Lightning channels deserves to know the shape of what is *not* known.

The plain finding first: as of November 2026, **none of the Lightning Network's principal development firms — Lightning Labs, ACINQ, Blockstream — has published an assessment of Lightning's quantum exposure.** No roadmap, no mitigation programme, no official word. What exists around that silence:

channel funds sit in hashed (P2WSH) outputs while a channel is open — keys hidden, per Chapter 14's rule. Lightning's contracts (HTLCs) are hash-based. The exposure concentrates in the unhappy path: a *force-close* puts scripts and keys on chain and starts a clock — the standard delay is roughly 144 blocks, about

a day — inside which a quantum adversary with the revealed keys would have to beat the honest party's claim. Shorter contract windows run to roughly 40 blocks — six or seven hours. Transport between nodes uses classical key exchange, which carries the harvest-now-decrypt-later exposure of Chapter 1 — for channel gossip, not for coins.

prototypes a hybrid post-quantum Lightning — ML-DSA and ML-KEM through the gossip, transport, invoice, and onion layers — at a measured cost (gossip traffic grows about tenfold) and with an explicit limit stated by its authors: it does **not** protect the on-chain funds in the channels themselves. Those wait, as everything in this chapter waits, on the base layer's own migration (Chapter 8).

(April 2026) that Lightning is "helplessly broken" against a quantum adversary, and a published rebuttal walking through the windows above. That is the whole of the record.

- **The structure, from the protocol's public specifications:**
- **The one research artifact:** a September 2026 preprint (PQLN)
- **The public argument so far** consists of a prominent claim

Verdict, stated as the book states all of them: Lightning's exposure is real but mostly *windowed* — measured in hours inside adversarial edge cases, rather than the standing, permanent exposure of Chapter 6 — and its defence cannot be built until Bitcoin's is. If your holdings ride Lightning, the meantime practices of Part Three apply unchanged; the layer above them is an open file, and this book will not pretend otherwise.

Chapter 21 — The Unknowns, Stated

A chapter of questions, kept on purpose. As of November 2026, the public record does not answer:

cryptographically relevant quantum computer will exist. Every date in circulation is a projection (Chapter 2).

what final parameters.

the choice survives its own governance.

will ever make un-migrated coins unspendable (Chapter 8).

a third of the supply's fate is an open question, not a detail.

never been published (Chapter 6).

well** — the secure elements inside today's hardware wallets were not sized for signatures of 2,400 bytes and up; the industry's answer is not yet public. (One maker already uses ML-DSA for device attestation; that is not the same as signing your transactions with it.)

model exists (Chapter 4).

written until the destination exists (Chapter 19).

(Chapter 20).

key that must never be reused, and must survive restores without rewinding — **get solved for ordinary holders**, or whether the stateless and lattice families simply carry the field.

1. **When** — or, strictly, whether on any plannable horizon — a
2. **When FN-DSA (Falcon) becomes a finished standard**, and with

3. **Which post-quantum scheme Bitcoin will choose**, or whether
4. **Whether the freeze happens** — whether Bitcoin's consensus
5. **What becomes of the lost and dead coins** if it doesn't —
6. **How much Ethereum is exposed, in aggregate** — the count has
7. **Whether mainstream hardware signers can run the new schemes
8. **What the migration will cost a holder in fees** — no honest
9. **What the migration instructions will say** — they cannot be
10. **What Lightning's builders intend** — unpublished
11. **Whether stateful hash-based schemes' hazards** — a signing

This list is the book's promise kept in the other direction: the same standard that made the certain chapters certain makes this one a list of questions. When any of them is answered, the answer will be dated, and this list will shrink by one.

Chapter 22 — The Counter-Case, Fairly

The strongest version of "you are preparing for nothing" deserves its own chapter, in its proponents' own terms.

Adam Back — cryptographer, inventor of Hashcash (the proof-of-work Bitcoin adopted), CEO of Blockstream — puts the timeline at **"probably not for 20–40 years, if then,"** and

the preparedness case in the same breath: preparation is "the prudent thing to do," and Bitcoin has "a decade in which to migrate" and can "be quantum ready, long before cryptographically relevant quantum computers arrive." Read whole, his position is not denial; it is *scheduling*: the threat is real, distant, and slower than the fix.

The Bernstein research note (April 2026) tells its investor readers the quantum question is **"neither existential, nor novel"** — a "medium to long term system upgrade cycle," with three to five years needed to prepare against an expert-consensus machine timeline of roughly ten — and locates the genuine risk narrowly, in about **1.7 million** early-format coins.

Charles Hoskinson adds the engineer's caution from the other side: done prematurely, post-quantum cryptography could slow a chain roughly **tenfold** — the migration itself has a cost, and paying it too early is also a way to be wrong.

And then there is the **canary** question — how would we *know*? Three forms of it circulate, and they do not agree:

sizes and watch who breaks them. Nic Carter's warning gives the argument its title — *"If the Quantum Canary Sings, It's Too Late"*: small breaks prove nothing (classical machines can fake them), and because Shor's algorithm scales smoothly, the first *unambiguous* break may arrive only months before the real one.

park a bounty behind a calibrated challenge — a spend from it would *prove* the capability exists, publicly and undeniably, and could trigger a pre-agreed defensive fork.

in some 30,000 identical lots of 50 BTC, keys exposed since 2009 — the most attractive target in the system and, on this

argument, a slow one: weeks of machine time per key at the projected rates, so the theft of the creator's era would be noticed long before it finished — *if* the field accepts those coins falling as the price of the warning.

- **The challenge ladder:** cryptographers publish keys of rising
- **The canary fund:** a published proposal (BitMEX Research) to
- **Satoshi's shield:** the roughly 1.7 million earliest coins sit

Now weigh both cases against the same scale. The preparation case says: the standards are finished, the deadlines are set by institutions with no product to sell, the exposed third of the supply is measured, and the estimates of the machine keep shrinking. The counter-case says: the machine is decades out if ever, the migration has its own real costs, and the system has a decade in hand. **Notice what they agree on.** Not one voice in this chapter — not one — argues against the meantime: fresh addresses, an offline seed, knowing which of your keys are exposed, understanding that your wallet is your words. The argument between the camps is entirely about a date. The practices cost nothing under either timeline, and pay under both.

That is where this book leaves it: prepared for the early date, unharmed by the late one, and honest about which parts of the future are still unwritten.

Back Matter

The State of This Book

Written November 2026. Facts are stated as of that date; the chapters that will age first are 2 (the machine), 8 and 11 (the drafts and programmes), and 21 (the unknowns) — by design, in that order. Standards, deadlines, sizes, and counts are cited to their sources in the research record kept with this book's files.

Sources

Primary records consulted include: NIST FIPS 203/204/205 and IR 8547; NSA CNSA 2.0; the EU PQC roadmap; UK NCSC migration guidance; ASD (Australia) and CCCS (Canada) roadmaps; BIPs 16, 32, 39, 141, 173, 174, 340–342, 360, 361 (drafts as marked); Chaincode's post-quantum research report; Blockstream's and Blockstream-adjacent throughput modelling; ChainQuery's and Project Eleven's exposure datasets; Algorand's official post-quantum documentation; Signal's and Apple's engineering blogs; OpenSSH's post-quantum page; Cloudflare's 2025 state-of-the-post-quantum-internet report; and the wallet documentation of Electrum, AirGap, Coldcard, and SeedSigner. The full dated research record — three feasibility reports and the appendix verification log — is kept with this book's project files.

Appendix — Go Deeper

For enthusiasts and scholars. Everything below was free at the time of writing (November 2026). Links age; the institutions behind them are the durable part.

Learn — free courses and texts

(8.370x).** Quantum foundations, protocols and algorithms — including Shor's — with all materials usable without enrolling. Beginner-to-intermediate. https://ocw.mit.edu/courses/8-370x-quantum-information-science-i-spring-2018/

Shor's own graduate course: the factoring algorithm, error correction, quantum cryptography. Lecture notes and problem sets included. Intermediate-to-advanced. https://ocw.mit.edu/courses/18-435j-quantum-computation-fall-2003/download/

built on Qiskit, from *Basics of Quantum Information* up to graduate-level series by John Watrous. Free to all. https://quantum.cloud.ibm.com/learning

The dedicated course on this book's subject — lectures plus hands-on labs with ML-KEM and ML-DSA. Free to audit; UMBC's open teaching module carries the slides, syllabus and exercises. https://est.umbc.edu/teaching/pqc-teaching-module/

for Everyone (edX).** A true-novice start; basic algebra is enough. Free to audit. https://www.edx.org/learn/quantum-computing/university-of-chicago-introduction-to-quantum-computing-for-everyone

quantum basics to the quantum internet. Free to audit. https://www.edx.org/school/delftx

- **MIT OpenCourseWare — Quantum Information Science I
- **MIT OpenCourseWare — Quantum Computation (18.435J).** Peter
- **IBM Quantum Learning.** Ten-plus courses and guided paths
- **UMBC — Introduction to Post-Quantum Cryptography (edX).**
- **University of Chicago — Introduction to Quantum Computing
- **TU Delft (DelftX) — Quantum 101 and 201 (edX).** From

Read the sources — the primary documents, free

hub: status, migration guidance, and the IR 8547 timeline. https://csrc.nist.gov/projects/post-quantum-cryptography

FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA) — with the Falcon standard (FN-DSA) in development. https://csrc.nist.gov/Projects/post-quantum-cryptography/pqc-standards

including the post-quantum drafts of Chapter 8. https://github.com/bitcoin/bips/blob/master/README.mediawiki

working reference for native Falcon accounts: generation, fees, rekeying, the algokey pq commands. https://dev.algorand.co/concepts/accounts/post-quantum/

State Proofs since 2022, native Falcon accounts since August 2026, and what remains. https://algorand.co/technology/post-quantum

- **NIST Post-Quantum Cryptography project.** The standardisation
- **NIST PQC Standards page.** The standards themselves —
- **The BIP repository.** Every Bitcoin Improvement Proposal,
- **Algorand — Post-Quantum Accounts (developer docs).** The
- **Algorand — Post-Quantum Technology overview.** The roadmap:

Join the work — scholar and research communities

cryptographers designing and attacking the schemes post here. Subscribe to post; the archive is public. https://csrc.nist.gov/projects/post-quantum-cryptography/email-list

(home of RFC 9958, *Post-Quantum Cryptography for Engineers*). Public list and archive; anyone may join the discussion or submit a draft. https://datatracker.ietf.org/group/pquip/

certificates and signed mail — including the FN-DSA drafts. https://datatracker.ietf.org/group/lamps/

reference library for the new schemes, now under the Linux Foundation's Post-Quantum Cryptography Alliance. Development is public on GitHub; the project's own warning stands: not yet for production use. https://openquantumsafe.org/

· https://github.com/open-quantum-safe/liboqs

of the new standards (mlkem-native, mldsa-native) — the living continuation of the retired PQClean project's mission. https://github.com/pq-code-package/mlkem-native

new results appear here first, free to read. Author-posted — read as work in progress. https://eprint.iacr.org/

cryptography meet. No proceedings; talk recordings are posted free. (Attending in person is a paid event.) https://realworldcrypto.iacr.org/

Quantum Resistance topic page that tracks Bitcoin's post-quantum debate proposal by proposal. https://bitcoinops.org/en/newsletters/ · https://bitcoinops.org/en/topics/quantum-resistance/

list — the post-quantum proposals are argued here first. (The list moved from its old Linux Foundation home in 2024.) https://groups.google.com/g/bitcoindev

threads included. Read freely; posting is research-grade. https://ethresear.ch/

help, the developer portal and Discord are the live doors. https://forum.algorand.org/

- **NIST pqc-forum.** The standardisation discussion list; the
- **IETF PQUIP.** The transition-engineering working group
- **IETF LAMPS.** Where the new algorithms are fitted into
- **Open Quantum Safe — liboqs.** The field's open-source
- **PQ Code Package.** Production-grade, verified implementations

- **IACR Cryptology ePrint Archive.** The field's paper commons:
- **Real World Crypto Symposium.** Where academic and deployed
- **Bitcoin Optech.** The weekly technical digest, plus a
- **bitcoin-dev (Google Groups).** Bitcoin's core technical
- **ethresear.ch.** Ethereum's research forum, post-quantum
- **Algorand Forum.** Governance and community; for developer

Touch it — hands-on, free

time on real quantum hardware — enough to run the classic demonstrations, including Shor's algorithm, yourself. https://www.ibm.com/quantum/products

the new schemes, with test vectors and benchmarks. https://github.com/open-quantum-safe/liboqs

nginx, OpenSSH, OpenVPN) and a public test server for quantum-safe connections. Partially maintained — contributors wanted, says the project itself. https://github.com/open-quantum-safe/oqs-demos

network on your own machine, and the commands to generate and sign with a real Falcon-1024 account — the account type live on mainnet today. https://dev.algorand.co/getting-started/algokit-quick-start/

- **IBM Quantum Open Plan + Qiskit.** Free account, free monthly
- **Build liboqs.** Clone it and compile the reference library:

- **OQS demos.** Post-quantum versions of familiar tools (curl,
- **AlgoKit + algokey pq.** Algorand's free toolkit: a local

Keep current — the standing trackers

the whole chain, counted in the open: on 1 November 2026 it put 7,126,359 BTC (about 35.4%) at risk, split between always-exposed and reuse-exposed. The numbers in Chapter 6 come from here and its peers; check it for the current count. http://chainquery.com/reports/quantum-exposure

address, searchable, with the reason it is vulnerable; the underlying query is open source. Its counting runs broader than ChainQuery's — the two together bracket the truth. https://projecteleven.com/bitcoin-risq-list

standards themselves; **Bitcoin Optech** (above) is the weekly digest for Bitcoin's side of the story.

- **ChainQuery — Bitcoin Quantum Exposure.** A weekly walk of
- **Project Eleven — Bitcoin Risq List.** Every vulnerable
- **NIST's project pages** (above) are the tracker for the

Compiled November 2026 from the live pages. One honest exclusion: no Coursera course appears, because no course page there could be found stating its free-audit terms plainly — rather than guess, the shelf leaves the space empty.

About the Art

The art in this book is one painting, four times.

It is an abstract work in ink on canvas by the artist — a nebula, laid down in stages. First the washes: yellow and gold and pink on white, all weather and no sky yet. Then the full colour of the nebula itself. Then the starfield, point by point. Then the deep field, the dark laid over everything until the colours burn through it.

Each stage appears in this book as itself — a photograph of the work at that moment, cleaned of its surroundings and otherwise untouched. The cover is the fourth stage. The parts of the book open on the stages in order, so the painting finishes as the book does.

That seemed only honest, and more than honest. This is a book about a change that arrives in stages while the thing changing stays itself — a holder's keys, a holder's coins, carried through a migration that replaces the mathematics around them and nothing else. Many stages. One work.

Art credit: the painting and the art throughout this book are by Douglas John Brownfield.

About the Author

Douglas J. Brownfield is an independent builder and artist based in America. He builds self-custodial software tools — programs

designed so the people who use them keep hold of their own keys, their own work, and their own decisions — and he holds his own assets the way this book describes: fresh addresses, an offline seed, signing done by hand on hardware he controls.

His artwork — from book art to ink on canvas to graphic apparel design — takes its cues from whatever he's been looking at: deep space, riverboats, and more to come. One of them, in four stages, carries the art of this book.

Before Q-Day grew out of the author's own preparation. Faced with a scheduled change to the mathematics his holdings depend on, he went looking for the book that explained it plainly — what is settled, what is not, and what to do in the meantime — and then wrote the one he had needed.