Module 8 Summary: The Future of Digital Finance

Prof. Dr. Joerg Osterrieder

Digital Finance — BSc Course

Module 8: Prerequisites

Theme: Future (digital identity, quantum, climate finance, synthesis) **From prior modules:**

- **All M1-M7:** course-to-date is the prerequisite
- **M3L1:** cryptographic-foundations bridge to quantum threat
- **M5L3:** limits of prediction for climate-finance modelling

External knowledge assumed:

- None new; the module is integrative.
- Optional: skim of one self-sovereign-identity primer if available.

Will be introduced this module: We introduce digital identity (Swiss e-ID, eIDAS 2.0), the quantum threat to current cryptography, climate finance and ESG measurement debates, and the course-wide synthesis.

Prerequisites are advisory; lessons remain self-contained where feasible. Forward references inside lessons flag any concept used before its canonical introduction.

Key Concepts by Lesson

L1: Digital Identity

- Centralized vs. federated vs. self-sovereign identity (SSI)
- SSI: user-controlled credentials, no central authority
- Zero-Knowledge Proofs (ZKP): prove a claim without revealing data
- 1.4 billion people lack formal identity documents

L2: Quantum Computing

- Qubits: superposition enables parallel exploration
- Shor's algorithm breaks RSA and elliptic-curve cryptography
- Post-quantum cryptography: lattice, hash-based, code-based
- Four-phase migration: inventory $\rightarrow$ plan $\rightarrow$ test $\rightarrow$ deploy

L3: Climate Finance

- ESG: Environmental, Social, Governance factors
- Carbon markets: compliance (cap-and-trade) vs. voluntary
- ESG AUM exceeded USD 35 trillion (2024)
- Greenwashing risk and rating divergence

L4: Future Synthesis

- Four scenarios: FinTech Supernova, Regulated Renaissance, Slow Burn, Digital Fortress
- CBDCs, programmable money, biometric payments
- Weak signals vs. strong trends
- Career paths across all 8 modules

Module 8 answers: What emerging technologies will reshape finance — and how should you prepare?

Key Formulas and Definitions

Self-Sovereign Identity (SSI)

SSI is an identity model where the individual controls their own credentials (stored in a digital wallet) and selectively discloses attributes to verifiers — without contacting the original issuer. Enabled by decentralized identifiers (DIDs) and verifiable credentials (VCs).

Zero-Knowledge Proof (ZKP)

A ZKP allows a prover to convince a verifier that a statement is true **without revealing any information beyond the truth of the statement**. Example: prove "I am over 18" without revealing your date of birth.

Quantum Threat to Cryptography

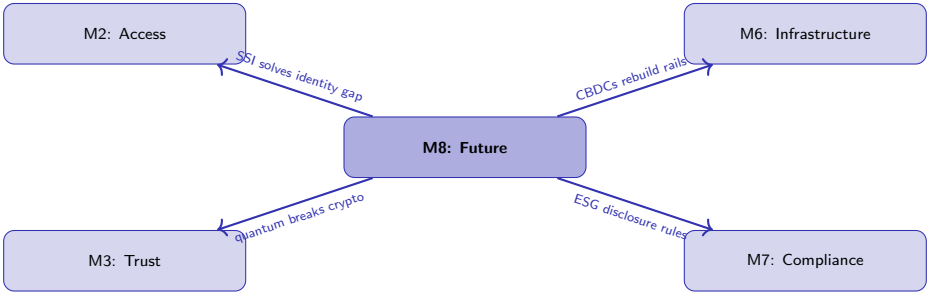
Shor's algorithm factors large integers in polynomial time, breaking RSA and ECC. **Grover's algorithm** speeds up brute-force search quadratically, weakening symmetric ciphers (AES-128 $\rightarrow$ effectively AES-64). NIST selected three families of post-quantum algorithms (2024): lattice-based, hash-based, code-based.

Four-Scenario Framework

Two axes: **Regulation** (permissive $\leftrightarrow$ restrictive) $\times$ **Technology** (rapid $\leftrightarrow$ gradual). Each combination yields a distinct future for digital finance.

The future is not a single prediction — it is a portfolio of scenarios, each requiring different preparation.

Connections to Other Modules



- **Future → Access (M2):** Self-sovereign identity gives the 1.4 billion unbanked verifiable credentials without centralized gatekeepers
- **Future → Trust (M3):** Quantum computers running Shor's algorithm could break the elliptic-curve cryptography underlying all blockchains
- **Future → Infrastructure (M6):** CBDCs may replace retail payment rails; tokenization may replace securities settlement
- **Future → Compliance (M7):** ESG disclosure mandates (TCFD, CSRD) and AI governance (EU AI Act) create new compliance obligations

Module 8 is where every thread converges: cost, access, trust, risk, automation, infrastructure, and compliance all shape the future.

Module 8: Integrative Questions

Two questions that need more than one lesson to answer:

1. The course argues digital finance is reshaping trust (M1-M7). Pick one M8 lesson (digital identity, quantum, climate, synthesis) and explain how it forces revision of an earlier-module claim.
2. Combine M8L1 (identity) + M8L2 (quantum) to design a credential scheme that survives a quantum-capable adversary while remaining usable for M2L2 thin-file credit signals.

Use these as study prompts before the module exam; each integrates concepts that span lessons.

Module 8: Worked Multi-Lesson Example

Worked example walks a Swiss retail bank launching a 2027 tokenised savings product across M3L1 (cryptographic primitives), M3L4 (stablecoin peg), M6L4 (SDX-style delivery-versus-payment), M7L3 (FINMA DLT Act licence), M8L1 (Swiss e-ID for customer onboarding), M8L4 (synthesis with course-wide closing arc). **Pedagogical pattern:** the example is intentionally end-to-end. Solve it lesson-by-lesson, then step back and identify the lesson whose assumption was the binding constraint.

The exam-style version of this example appears in extttv4/exam_prep/exam_bank.tex for module 8.

Module 8: Forward-Pointing Dependency Map

Concepts from Module 8 that later modules will use:

- **None (M8 closes the course):** Forward-pointers terminate; the cross-module map turns reflective
- **M3L1 + M3L2:** Quantum readiness (M8L2) is the trigger for re-deriving cryptographic-foundations assumptions in M3L1 + M3L2
- **M4L4 + M7L3:** Climate finance (M8L3) extends M4L4 new-risk landscape and M7L3 regulating-the-new in parallel

---

Forward-pointing dependencies; concepts not in this map are local to Module 8.