Module 8 Summary: The Future of Digital Finance

Prof. Dr. Joerg Osterrieder

Digital Finance — BSc Course

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

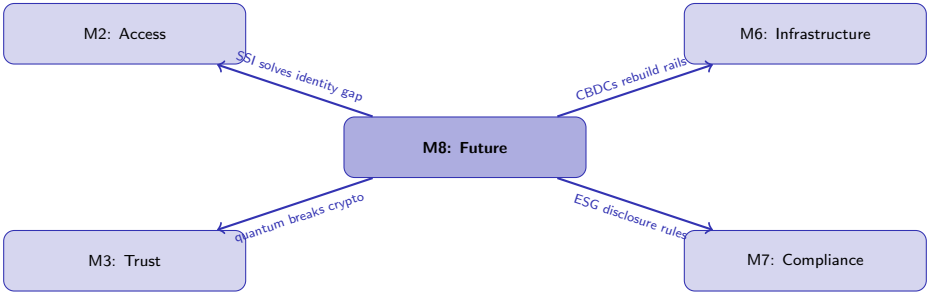
Shor's algorithm factors large integers in polynomial time, breaking RSA and ECC. **Grover's algorithm** speeds up brute-force search quadratically, weakening symmetric ciphers (AES-128 $\rightarrow$ effectively AES-64). NIST selected three families of post-quantum algorithms (2024): lattice-based, hash-based,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