Module 3 Summary: The Trust Problem

Prof. Dr. Joerg Osterrieder

Digital Finance — BSc Course

Key Concepts by Lesson

L1: Cryptographic Foundations

- Hash functions: deterministic, fixed-length, one-way
- SHA-256: 2^{256} possible outputs, avalanche effect
- Merkle trees: efficient transaction verification via inclusion proofs

L2: Consensus Mechanisms

- Byzantine Fault Tolerance: $n \geq 3f + 1$
- Proof of Work: SHA-256(header $\|$ nonce) $<$ target
- Proof of Stake: validators lock capital as collateral
- Blockchain trilemma: security, decentralization, scalability

L3: Smart Contracts & dApps

- EVM: deterministic execution across all nodes
- Gas model: 21,000 (transfer) to 500,000+ (DeFi)
- Token standards: ERC-20 (fungible), ERC-721 (NFT)
- Layer-2 scaling: rollups, sidechains, state channels

L4: DeFi & Stablecoins

- AMM constant product: $x \cdot y = k$
- Stablecoin types: fiat-backed, crypto-collateralized, algorithmic
- Flash loans, reentrancy attacks, oracle manipulation

Module 3 answers: How can strangers transact without a trusted intermediary?

Key Formulas and Definitions

Byzantine Fault Tolerance Threshold

$$n \geq 3f + 1 \quad \text{where } n = \text{total nodes},\ f = \text{faulty/malicious nodes}$$

Proof of Work Puzzle

$$\text{SHA-256}(\text{block\_header} \| \text{nonce}) < \text{target}$$

Miners iterate over nonce values until a valid hash is found. Difficulty adjusts to maintain constant block time.

Constant Product AMM (Uniswap)

$$x \cdot y = k \qquad \text{Price: } P = \frac{x}{y}$$

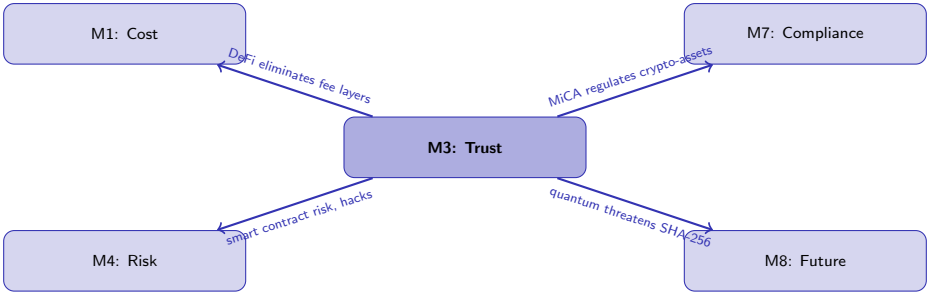
Larger trades cause greater slippage. The AMM never runs out of either token — price approaches infinity.

Merkle Tree Verification

Verify a single transaction in $O(\log n)$ hash computations (vs. $O(n)$ for a flat list). Only the **inclusion proof** (sibling hashes along the path) is needed, not the full block data.

Cryptography + consensus + smart contracts + DeFi = a complete financial system without banks.

Connections to Other Modules



- **Trust → Cost (M1):** DeFi protocols replace intermediaries with code, collapsing the MDR fee stack
- **Trust → Risk (M4):** Smart contract bugs, oracle failures, and flash loan exploits create a new category of financial risk
- **Trust → Compliance (M7):** MiCA classifies crypto-assets (EMTs, ARTs, utility tokens) and imposes reserve/disclosure requirements
- **Trust → Future (M8):** Quantum computers running Shor's algorithm could break elliptic-curve signatures underlying all blockchains

Blockchain replaced trust in institutions with trust in mathematics — but the code still needs auditing and the math faces a quantum threat.