Digital Finance Glossary

Key Terms Across All 8 Modules

Prof. Dr. Joerg Osterrieder

Digital Finance — BSc Course

Module 1: The Cost Problem (1/2)

- **Acquirer** — The merchant's bank that processes card payments and settles funds to the merchant's account.
- **BNPL** — Buy Now Pay Later — short-term installment financing where the merchant pays the MDR and the consumer pays zero interest.
- **CAC** — Customer Acquisition Cost — total spend to acquire one new customer. Viable fintechs target LTV/CAC $> 3\times$.
- **Card Network** — Organization (Visa, Mastercard) that sets interchange rates, routes transactions, and enforces rules across issuers and acquirers.
- **Card-Not-Present (CNP)** — A transaction where the card is not physically present (e.g., online purchase). Typically carries higher interchange.
- **Chariot Payments** — Charitable giving via donor-advised funds integrated into payment checkouts.
- **Cross-Border Payment** — A payment where payer and payee are in different countries, typically involving currency conversion and correspondent banking.
- **Durbin Amendment** — US regulation (2010) capping debit card interchange fees for banks with assets above $10 billion.
- **EU IFR** — Interchange Fee Regulation — EU law capping consumer debit interchange at 0.2% and credit at 0.3%.
- **Five-Party Model** — The standard card payment model: cardholder, merchant, issuer, acquirer, card network.

Module 1: The Cost Problem (2/2)

- **Gateway Fee** — Fee charged by the payment gateway for routing the transaction from merchant to processor.
- **Interchange Fee** — Fee paid by the acquirer to the issuer on each card transaction. Largest component of MDR (60–70%).
- **Issuer** — The cardholder's bank that issues the payment card and extends credit or provides account access.
- **LTV** — Lifetime Value — total net revenue a customer generates over their relationship with the firm.
- **MDR** — Merchant Discount Rate — total percentage fee a merchant pays per card transaction. Sum of interchange + network + processor + acquirer + gateway fees.
- **Network Assessment Fee** — Small fee paid by the acquirer to the card network (Visa/Mastercard) for each transaction processed.
- **P2P Lending** — Peer-to-peer lending — platforms connecting individual borrowers and lenders, bypassing traditional bank intermediation.
- **Platform Economics** — Business models where value is created by facilitating interactions between two or more user groups (two-sided markets).
- **Processor Fee** — Fee charged by the payment processor for authorizing, clearing, and settling the transaction.
- **Two-Sided Market** — A market where a platform serves two interdependent user groups (e.g., cardholders and merchants) and must balance pricing to attract both sides.
- **Unit Economics** — Per-customer profitability analysis: revenue streams minus variable costs, expressed as LTV/CAC ratio.

Module 2: The Access Problem (1/2)

- **Algorithmic Fairness** — Ensuring automated decision-making systems do not produce systematically biased outcomes across protected groups.
- **Alternative Data** — Non-traditional data sources (mobile usage, utility payments, social media) used to assess creditworthiness of thin-file borrowers.
- **Credit Invisible** — An individual with no credit history at traditional bureaus, making them unscorable by conventional models.
- **Demographic Parity** — Fairness criterion requiring equal approval rates across groups: $P(\hat{Y} = 1|A = 0) = P(\hat{Y} = 1|A = 1)$.
- **Disparate Impact** — When a facially neutral policy produces disproportionately adverse outcomes for a protected group, even without discriminatory intent.
- **Disparate Treatment** — Intentionally treating individuals differently based on a protected characteristic (e.g., race, gender).
- **Equalized Odds** — Fairness criterion requiring equal true positive and false positive rates across groups.
- **Financial Exclusion** — The state of lacking access to affordable, appropriate financial services from regulated providers.

Module 2: The Access Problem (2/2)

- **Fractional Shares** — Ownership of less than one full share of a security, enabling investment with as little as $1.
- **Gamification** — Use of game-design elements (streaks, leaderboards, confetti) in non-game contexts like trading apps. Can encourage overtrading.
- **Impossibility Theorem** — Result (Chouldechova, 2017) showing that when base rates differ across groups, equal FPR, FNR, and predictive values cannot all hold simultaneously.
- **M-Pesa** — Mobile money service launched in Kenya (2007) enabling financial transactions via SMS on basic phones. A leapfrog technology for financial inclusion.
- **Microfinance** — Provision of small loans, savings, and insurance to low-income individuals who lack access to traditional banking.
- **Neobank** — A digital-only bank with no physical branches, offering accounts, payments, and lending via a mobile app.
- **Open Banking** — Regulatory framework (e.g., PSD2 in EU) requiring banks to share customer data with authorized third parties via APIs, with customer consent.
- **PSD2** — Payment Services Directive 2 — EU regulation mandating Strong Customer Authentication (SCA) and open access to payment accounts via APIs.
- **Robo-Advisor** — Algorithm-driven platform providing automated portfolio management (asset allocation, rebalancing, tax-loss harvesting) at low cost.
- **Thin File** — A credit file with too few data points for a reliable traditional credit score, common among young adults and immigrants.
- **Unbanked** — An adult without an account at a formal financial institution. Approximately 1.4 billion globally.
- **Underbanked** — An adult with a bank account who still relies on alternative financial services (payday lenders, check cashers).

Module 3: The Trust Problem (1/2)

- **AMM** — Automated Market Maker — a smart contract that uses a mathematical formula (e.g., $x \cdot y = k$) to set token prices without an order book.
- **Avalanche Effect** — A property of cryptographic hash functions where a single-bit input change produces a drastically different output.
- **BFT** — Byzantine Fault Tolerance — ability of a distributed system to function correctly even when up to f of n nodes are malicious. Requires $n \geq 3f + 1$.
- **Block Reward** — Cryptocurrency awarded to miners/validators for successfully proposing a new block. Incentivizes honest participation.
- **Blockchain Trilemma** — The observation that blockchain systems can optimize at most two of three properties: security, decentralization, and scalability.
- **Consensus Mechanism** — Protocol by which distributed nodes agree on the current state of the ledger (e.g., PoW, PoS, PBFT).
- **Constant Product Formula** — AMM invariant $x \cdot y = k$ where x and y are token reserves. Larger trades cause greater price slippage.
- **DeFi** — Decentralized Finance — financial services (lending, trading, insurance) built on smart contracts without intermediaries.
- **Digital Signature** — Cryptographic proof that a message was created by the holder of a specific private key, providing authentication and non-repudiation.

Module 3: The Trust Problem (2/2)

- **ERC-20** — Ethereum token standard for fungible tokens (currencies, stablecoins, governance tokens).
- **ERC-721** — Ethereum token standard for non-fungible tokens (NFTs) — each token is unique.
- **EVM** — Ethereum Virtual Machine — the runtime environment executing smart contracts deterministically on every node.
- **Flash Loan** — An uncollateralized loan that must be borrowed and repaid within a single blockchain transaction. Used in arbitrage and exploits.
- **Gas** — Unit measuring computational effort on Ethereum. Users pay gas fees (in gwei) to compensate validators for execution.
- **Hash Function** — A function mapping arbitrary-length input to fixed-length output. Must be deterministic, one-way, and collision-resistant.
- **Impermanent Loss** — Loss incurred by AMM liquidity providers when token prices diverge from the ratio at deposit time.
- **Merkle Tree** — A binary tree of hashes enabling efficient transaction verification in $O(\log n)$ via inclusion proofs.
- **Oracle** — A service providing external data (prices, events) to smart contracts. Oracle manipulation is a major DeFi attack vector.
- **PoS** — Proof of Stake — consensus where validators lock capital as collateral. Malicious behavior is punished by slashing (losing staked funds).
- **PoW** — Proof of Work — consensus where miners compete to solve computational puzzles. Converts electricity into security.
- **Reentrancy Attack** — A smart contract exploit where a malicious contract recursively calls back into the victim contract before state is updated.
- **Rollup** — Layer-2 scaling solution that executes transactions off-chain and posts compressed data to L1 for security. Types: optimistic, zero-knowledge.
- **SHA-256** — Secure Hash Algorithm producing a 256-bit output. The most widely used hash in blockchain and financial cryptography.
- **Slippage** — The difference between expected and actual execution price in an AMM trade, caused by limited liquidity.
- **Smart Contract** — Self-executing code deployed on a blockchain that automatically enforces the terms of an agreement.
- **Stablecoin** — A cryptocurrency designed to maintain a stable value relative to a reference asset. Three types: fiat-backed, crypto-collateralized, algorithmic.
- **TVL** — Total Value Locked — the total amount of assets deposited in a DeFi protocol. Used as a measure of protocol adoption.

Module 4: The Risk Problem (1/2)

- **Basel III** — International regulatory framework (2010–2019) requiring higher capital ratios, liquidity rules (LCR, NSFR), and a leverage ratio for banks.
- **Basel III.1 / "IV"** — Updated standards (2023+) introducing an output floor, revised standardized approaches, and reduced reliance on internal models.
- **Black-Scholes Model** — Option pricing formula deriving the theoretical price of European options from five inputs: stock price, strike, time, risk-free rate, volatility.
- **Call Option** — A contract giving the holder the right (not obligation) to buy an asset at a specified price (strike) before a specified date.
- **CET1 Ratio** — Common Equity Tier 1 capital divided by risk-weighted assets. Basel III minimum: 4.5%.
- **CVaR / ES** — Conditional Value-at-Risk / Expected Shortfall — the average loss in the tail beyond VaR. Always $\geq$ VaR.
- **Cyber Risk** — Risk of financial loss from cyberattacks. Violates stationarity assumptions underlying traditional risk models.
- **Delta (Δ)** — Option price change per \$1 move in the underlying. Measures stock-equivalent exposure.

Module 4: The Risk Problem (2/2)

- **Flash Crash** — Extremely rapid market decline and recovery (minutes), often triggered by algorithmic trading cascades.
- **Gamma (Γ)** — Rate of change of Delta. High Gamma means Delta changes rapidly — important near expiration.
- **Greeks** — Sensitivity measures for option prices: Delta, Gamma, Vega, Theta, Rho. Used for risk management, not pricing.
- **Historical Simulation** — VaR method using actual past returns. No distributional assumptions, but depends on history being representative.
- **LCR** — Liquidity Coverage Ratio — high-quality liquid assets divided by 30-day net cash outflows. Basel III minimum: 100%.
- **Leverage Ratio** — Tier 1 capital divided by total exposure (including off-balance-sheet). A non-risk-weighted backstop to capital ratios.
- **Monte Carlo Simulation** — VaR method generating thousands of random return scenarios from a statistical model. Flexible but computationally expensive.
- **NSFR** — Net Stable Funding Ratio — available stable funding divided by required stable funding. Addresses long-term liquidity risk.
- **Put Option** — A contract giving the holder the right (not obligation) to sell an asset at a specified price (strike) before a specified date.
- **Risk-Weighted Assets (RWA)** — Assets weighted by credit risk. Cash = 0%, government bonds = 0–20%, corporate loans = 100%, equities = up to 250%.
- **Theta (Θ)** — Time decay — how much an option loses per day, all else equal. Always negative for long options.
- **VaR** — Value-at-Risk — the maximum loss expected at a given confidence level over a specified time horizon.
- **Variance-Covariance** — VaR method assuming returns are normally distributed. Fast but underestimates tail risk.
- **Vega** — Option price sensitivity to a 1 percentage-point change in implied volatility.
- **Volatility** — Standard deviation of returns. Measures the magnitude of price fluctuations, regardless of direction.

Module 5: The Automation Problem (1/2)

- **Attention Mechanism** — Neural network component that learns which parts of the input are most relevant for each output token. Core of the transformer.
- **Bias (Statistical)** — Systematic error from overly simplistic model assumptions. High bias = underfitting.
- **Bias-Variance Trade-off** — Fundamental ML tension: simpler models have high bias (underfit), complex models have high variance (overfit).
- **Classification** — ML task predicting a category label (e.g., default/no default, fraud/legitimate).
- **Concept Drift** — Change in the relationship between input features and target variable: $P(Y|X)$ shifts over time.
- **Covariate Shift** — Change in input distribution $P(X)$ while $P(Y|X)$ remains stable.
- **Cross-Validation** — Technique splitting data into k folds, training on $k-1$ and testing on the held-out fold, rotating to reduce variance of performance estimates.
- **Data Drift** — Change in input feature distributions: $P(X)$ shifts, potentially degrading model performance.
- **Data Snooping** — Using test data or future information during model development, leading to inflated performance estimates.

Module 5: The Automation Problem (2/2)

- **Feature Engineering** — Creating informative input variables from raw data (e.g., moving averages, volatility ratios, lagged returns).
- **GenAI** — Generative AI — models that create new content (text, code, images) rather than classify or predict.
- **Hallucination** — When an LLM generates plausible-sounding but factually incorrect output. Critical risk in financial applications.
- **LLM** — Large Language Model — a neural network with billions of parameters trained to predict the next token. Does not "understand" finance.
- **Look-Ahead Bias** — Using information that was not available at the time of the decision (e.g., restated earnings in a backtest).
- **MLOps** — Machine Learning Operations — DevOps principles (automation, monitoring, versioning, governance) applied to the ML lifecycle.
- **Overfitting** — Model memorizes training data noise, performing well on training data but poorly on unseen data.
- **RAG** — Retrieval-Augmented Generation — combining LLM generation with retrieval from a curated document corpus to reduce hallucinations.
- **Regime Change** — Structural break in market behavior where statistical properties (mean, variance, correlations) shift abruptly.
- **Regression** — ML task predicting a continuous numerical value (e.g., stock return, credit spread).
- **Stationarity** — Property of a time series whose mean, variance, and autocorrelation do not change over time. Financial data rarely satisfies this.
- **Survivorship Bias** — Backtesting only on entities that still exist, excluding bankruptcies and delistings, leading to overly optimistic results.
- **Transformer** — Neural network architecture using self-attention to process sequences in parallel. Foundation of GPT, BERT, and modern LLMs.
- **Underfitting** — Model is too simple to capture the underlying pattern. Both training and test errors are high.
- **Variance (Statistical)** — Sensitivity of the model to the specific training data used. High variance = overfitting.

Module 6: The Infrastructure Problem (1/2)

- **ACH** — Automated Clearing House — US batch payment system for payroll, bill pay, and direct debit. Uses deferred net settlement.
- **API** — Application Programming Interface — a contract defining how two software systems communicate. The connective tissue of digital finance.
- **API Gateway** — Central entry point that routes, authenticates, rate-limits, and logs all API calls. The control plane of modern banking.
- **BaaS** — Banking-as-a-Service — a model where licensed banks provide banking infrastructure (accounts, cards, payments) to fintechs via APIs.
- **CBDC** — Central Bank Digital Currency — digital form of central bank money. Retail (public) or wholesale (interbank).
- **COBOL** — Legacy programming language (1959) still running many core banking systems. Declining developer workforce creates maintenance risk.
- **Core Banking System** — The central IT system processing a bank's daily transactions: accounts, payments, loans, interest. The "operating system" of a bank.
- **Correspondent Banking** — A network of bilateral agreements where banks hold accounts at other banks to facilitate cross-border payments.

Module 6: The Infrastructure Problem (2/2)

- **DNS** — Deferred Net Settlement — payments accumulated over a period and settled as net positions. Lower liquidity cost but settlement risk during the window.
- **Embedded Finance** — Integrating financial services (payments, lending, insurance) into non-financial platforms (e-commerce, ride-sharing, SaaS).
- **General Ledger** — The foundational accounting record in a core banking system. Every transaction ultimately posts to the general ledger.
- **GraphQL** — API query language allowing clients to request exactly the data fields they need. Alternative to REST for complex data relationships.
- **mTLS** — Mutual Transport Layer Security — both client and server authenticate each other via certificates. Stronger than one-way TLS.
- **OAuth 2.0** — Authorization framework allowing third-party applications to access user resources with scoped permissions and without sharing passwords.
- **Programmable Money** — Digital currency with embedded rules (e.g., spending restrictions, expiry dates). Enabled by CBDCs and smart contracts.
- **REST** — Representational State Transfer — the dominant API architectural style, using HTTP methods (GET, POST, PUT, DELETE) on resource URLs.
- **RTGS** — Real-Time Gross Settlement — each payment settled individually in real time. Zero counterparty risk. Examples: Fedwire (US), TARGET2 (EU).
- **RWA Tokenization** — Representing ownership rights to real-world assets (bonds, equities, real estate) as digital tokens on a distributed ledger.
- **SEPA** — Single Euro Payments Area — EU payment integration scheme enabling euro transfers across 36 countries under uniform rules.
- **SWIFT** — Society for Worldwide Interbank Financial Telecommunication — a messaging network for cross-border payment instructions. Not a settlement system.
- **TARGET2** — Trans-European Automated Real-time Gross Settlement Express Transfer — the eurozone RTGS system operated by the Eurosystem.
- **Webhook** — Server-to-server push notification triggered by an event (e.g., payment received). Replaces polling with real-time updates.

Module 7: The Compliance Problem (1/2)

- **AML** — Anti-Money Laundering — laws, regulations, and procedures to prevent criminals from disguising illegally obtained funds as legitimate income.
- **ART** — Asset-Referenced Token (MiCA) — a crypto-asset referencing multiple assets or currencies. Subject to strict reserve and governance requirements.
- **CDD** — Customer Due Diligence — standard identity verification and risk assessment performed at customer onboarding.
- **DORA** — Digital Operational Resilience Act — EU regulation requiring financial entities to ensure ICT risk management and operational resilience.
- **EDD** — Enhanced Due Diligence — deeper scrutiny applied to high-risk customers: PEPs, high-risk jurisdictions, complex structures.
- **EMT** — E-Money Token (MiCA) — a crypto-asset referencing a single fiat currency. Regulated similarly to e-money.
- **EU AI Act** — EU regulation classifying AI systems by risk level. Credit scoring and insurance pricing are "high risk," requiring human oversight and explainability.
- **FATF** — Financial Action Task Force — intergovernmental body setting global AML/CFT standards via the 40 Recommendations.

Module 7: The Compliance Problem (2/2)

- **FIU** — Financial Intelligence Unit — national agency receiving, analyzing, and disseminating SARs to law enforcement.
- **GDPR** — General Data Protection Regulation — EU data privacy law. The "right to explanation" constrains opaque algorithmic decisions.
- **KYC** — Know Your Customer — the process of verifying a customer's identity and assessing their risk profile before establishing a business relationship.
- **MiCA** — Markets in Crypto-Assets — EU regulation (2023) creating a comprehensive framework for crypto-asset issuers and service providers.
- **Model Risk** — The potential for adverse consequences from decisions based on incorrect or misused model outputs (SR 11-7 definition).
- **PEP** — Politically Exposed Person — an individual holding a prominent public function, subject to enhanced due diligence.
- **PRA SS1/23** — UK Prudential Regulation Authority supervisory statement on model risk management, effective 2024. UK equivalent of SR 11-7.
- **RegTech** — Regulatory Technology — technology solutions that help financial institutions comply with regulations more efficiently and accurately.
- **SAR** — Suspicious Activity Report — mandatory filing when a financial institution detects transactions that may involve money laundering or terrorist financing.
- **SR 11-7** — US Federal Reserve/OCC guidance (2011) establishing the framework for model risk management. Three pillars: development, validation, governance.
- **Sanctions Screening** — Automated checking of customers and transactions against government sanctions lists (OFAC, EU, UN).
- **Three Lines of Defense** — Governance model: 1st line (business units), 2nd line (risk management/compliance), 3rd line (internal audit).
- **Transaction Monitoring** — Automated surveillance of transactions to detect patterns indicative of money laundering, fraud, or sanctions violations.

Module 8: The Future of Digital Finance (1/2)

- **Biometric Payment** — Authentication using biological characteristics (fingerprint, face, iris) instead of PINs or passwords.
- **Cap-and-Trade** — Emissions trading system where regulators set an overall cap; firms buy/sell allowances. Price signal incentivizes emission reduction.
- **Carbon Credit** — A tradable certificate representing one tonne of CO_2 equivalent removed or avoided. Compliance vs. voluntary markets.
- **CSRD** — Corporate Sustainability Reporting Directive — EU regulation requiring large companies to disclose ESG data under European Sustainability Reporting Standards.
- **DID** — Decentralized Identifier — a globally unique identifier controlled by the subject (not a central authority). Foundation of SSI.
- **ESG** — Environmental, Social, Governance — three categories of non-financial factors used to evaluate companies alongside traditional financial metrics.
- **Federated Identity** — Identity model where a trusted third party (e.g., Google, government) vouches for the user's identity across multiple services.
- **Greenwashing** — Misleading claims about the environmental benefits of a product, service, or investment strategy.

Module 8: The Future of Digital Finance (2/2)

- **Grover's Algorithm** — Quantum algorithm that speeds up brute-force search quadratically. Weakens symmetric ciphers: AES-128 effectively becomes AES-64.
- **Lattice-Based Cryptography** — Post-quantum cryptographic schemes based on hard problems in lattice mathematics. NIST primary selection for key exchange.
- **Post-Quantum Cryptography (PQC)** — Cryptographic algorithms resistant to both classical and quantum computers. Three NIST families: lattice, hash-based, code-based.
- **Qubit** — Fundamental unit of quantum information. Unlike a classical bit, a qubit exists in superposition of 0 and 1 until measured.
- **Scenario Planning** — Strategic method exploring multiple plausible futures along key dimensions of uncertainty (e.g., regulation $\times$ technology pace).
- **Shor's Algorithm** — Quantum algorithm that factors large integers in polynomial time, breaking RSA and elliptic-curve cryptography.
- **SSI** — Self-Sovereign Identity — identity model where individuals control their own credentials in a digital wallet, selectively disclosing attributes to verifiers.
- **Superposition** — Quantum property where a qubit exists in a combination of 0 and 1 states simultaneously, until measurement collapses it to a definite value.
- **TCFD** — Task Force on Climate-related Financial Disclosures — framework for reporting climate risks and opportunities. Now incorporated into ISSB standards.
- **Verifiable Credential (VC)** — A tamper-evident digital credential issued by a trusted authority, held in a wallet, and presented to verifiers. Core of SSI.
- **Voluntary Carbon Market** — Market where companies and individuals buy carbon credits voluntarily to offset emissions, outside of regulatory mandates.
- **Weak Signal** — An early indicator of a potentially important future trend that is not yet mainstream. Requires monitoring without overcommitting.
- **ZKP** — Zero-Knowledge Proof — cryptographic method allowing one party to prove a statement is true without revealing any information beyond the statement's validity.