Risk, Regulation, and the Future of Digital Finance

Day 5 of 5

Prof. Jörg Osterrieder

BSc Seminar: Digital Finance

Spring 2026

PhD Seminar Series: Digital Finance Research

The Week So Far

Day 1: Crypto Fundamentals

- What crypto is, why it matters
- Exchanges, wallets, on-chain vs. off-chain

Day 2: DeFi and AMMs

- Uniswap, liquidity pools
- Impermanent loss, yield farming

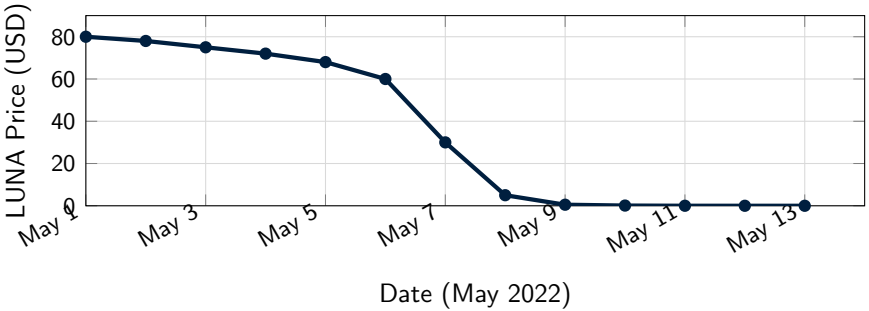
Day 3: Blockchain Economics

- PoW vs. PoS, EIP-1559, MEV
- Stablecoins, CBDCs

Day 4: AI & Crypto

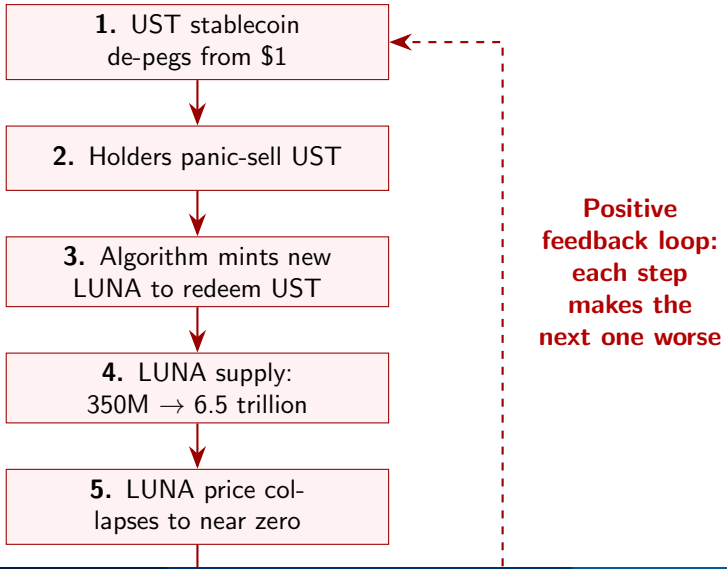
- ML basics, overfitting
- Random forests, SHAP
- Predicting BTC returns

The $40 Billion Crash: Terra/Luna



From $80 to $0.0001 in less than two weeks.
The largest crypto collapse in history.

The Death Spiral Explained



Could This Have Been Prevented?

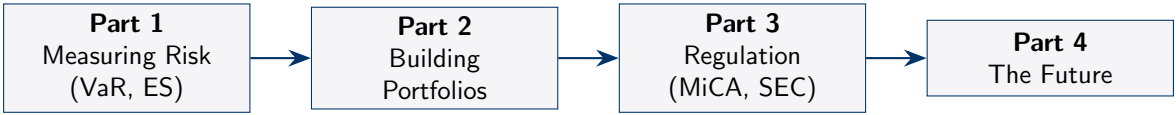
The Human Cost

- Thousands of people lost their life savings
- Many had been told UST was “safe” (it’s a stablecoin, right?)
- Suicide hotline numbers were pinned on crypto forums
- Do Kwon (founder) later arrested, charged with fraud

Key questions for today:

1. How do we *measure* the risk of crypto investments?
2. How should we *build portfolios* to limit catastrophic losses?
3. What *regulations* could prevent events like this?

Today: Risk, Portfolios, and Regulation



Outline

Risk $\neq$ Volatility

Volatility (standard deviation of returns) tells you how much prices bounce around on average. But it misses the big question:

What Really Matters

How bad can it get? Not on an average day — on the *worst* days.

BTC daily returns:

- Average: $+0.15\%$
- Std. deviation: $\sim 4\%$
- Worst day (2020): -37%
- Worst week ever: -50%

S&P 500 daily returns:

- Average: $+0.04\%$
- Std. deviation: $\sim 1.2\%$
- Worst day (2020): -12%
- Worst week ever: -18%

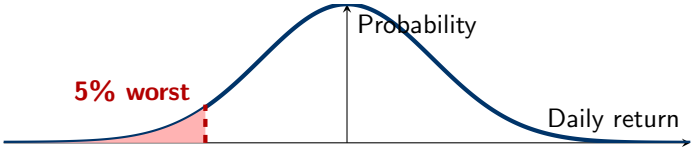
Crypto has ~ 3–$4\times$ the volatility of stocks, but the **tail losses** are far worse than that ratio suggests.

Value at Risk (VaR): Quantifying the Worst Case

Definition

VaR at confidence level α answers:

"With α% probability, I will **not lose more than** \$X in one day."



The red area = the 5% worst outcomes. VaR is the boundary.

Calculating VaR: The Simple Formula

Parametric VaR (assuming normal returns)

$$\text{VaR}_{95\%} = \text{Portfolio Value} \times z_{0.95} \times \sigma_{\text{daily}}$$

where $z_{0.95} = 1.65$ (from the normal distribution).

Step-by-step:

1. Portfolio value: \$10,000
2. Daily volatility: $\sigma = 4\%$ (typical for BTC)
3. z-score at 95%: $z = 1.65$
4. $\text{VaR}_{95\%} = \$10{,}000 \times 1.65 \times 0.04 = \mathbf{\$660}$

Interpretation: On 95% of days, you will lose at most \$660. But on the other 5% of days, losses could be *much* larger.

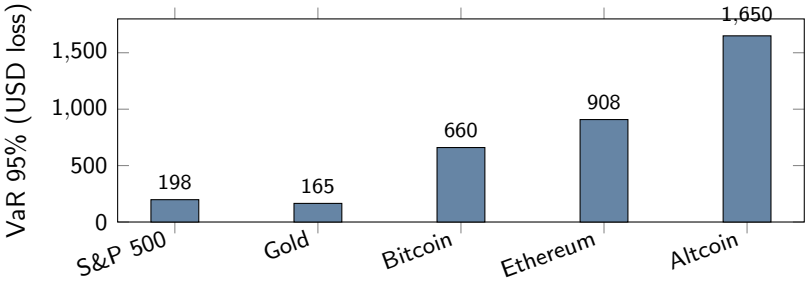
VaR Comparison: Stocks vs. Crypto

Same portfolio value ($10,000), different assets:

Asset	Daily Vol	VaR(95%)	Meaning
S&P 500 index	1.2%	$198	Lose up to $198 on bad day
Gold	1.0%	$165	Lose up to $165 on bad day
Bitcoin	4.0%	$660	Lose up to $660 on bad day
Ethereum	5.5%	$908	Lose up to $908 on bad day
Small altcoin	10%	$1,650	Lose up to $1,650 on bad day

Crypto is 3–8× riskier than traditional assets by this measure. This is why position sizing matters enormously.

Visual: $10,000 at Risk — Stocks vs. Crypto



Same $10,000 invested. Very different risk profiles.

Expected Shortfall: When Things Go Really Bad

Definition

Expected Shortfall (ES) = the average loss in the worst $\alpha\%$ of cases.

$$\text{ES}_\alpha = \mathbb{E}\big[-R \;\big|\; R \leq -\text{VaR}_\alpha\big] \times \text{Portfolio Value}$$

VaR says: "The boundary of the worst 5%"
ES says: "If you're in the worst 5%, how bad is it *on average*?"

Example (BTC, $10,000 portfolio)

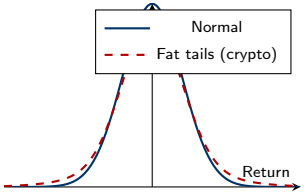
- VaR(95%) = \$660 ("you probably won't lose more than this")
- ES(95%) = \$950 ("but if you do, expect to lose about this much")

ES is the preferred risk measure for regulators (Basel III/IV) because it captures **tail risk** — the stuff VaR misses.

Why ES > VaR Matters: Fat Tails

Normal distribution (bell curve) assumes extreme events are very rare. **Crypto reality:** extreme events happen **much more often** than the bell curve predicts. This is called **fat tails**.

- Normal: >3% daily move is a "1 in 100" event
- BTC actual: happens **every week**
- Normal: >10% daily move is "once in 10,000 years"
- BTC actual: happens **several times per year**



The red curve has fatter tails:
more probability of extreme events.

Outline

Markowitz: The Power of Diversification

Key Insight [ ]

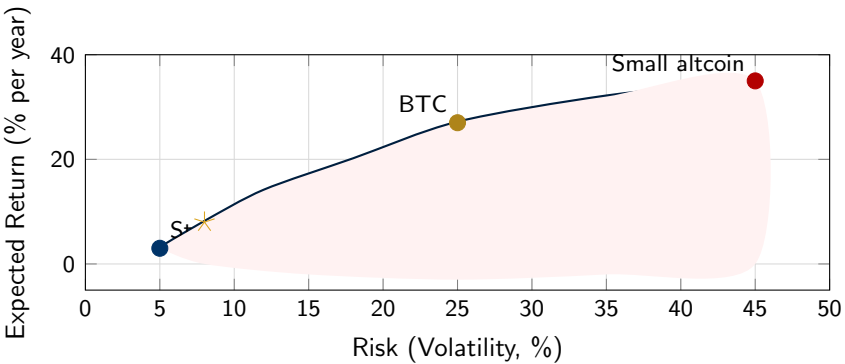
Don't put all your eggs in one basket. By combining assets that don't move perfectly together, you can **reduce risk without sacrificing expected return**.

The math (for 2 assets):

$$\sigma^2_{\text{portfolio}} = w_1^2\sigma_1^2 + w_2^2\sigma_2^2 + 2w_1w_2\rho_{12}\sigma_1\sigma_2$$

- w_1, w_2 = portfolio weights (how much in each asset)
- σ_1, σ_2 = volatilities of each asset
- ρ_{12} = correlation between assets
- If $\rho_{12} < 1$: portfolio risk $<$ weighted average of individual risks

The Efficient Frontier



The curve shows the **best possible risk-return tradeoff**. Points below the curve are inefficient — you could do better.

Adding Crypto to a Traditional Portfolio

Research finding: a small crypto allocation (5–10%) can improve the risk-return profile of a traditional portfolio.

Portfolio	Ann. Return	Ann. Vol	Sharpe Ratio
60/40 Stocks/Bonds	7.2%	9.5%	0.54
55/35/10 Stocks/Bonds/BTC	9.8%	11.2%	0.70
55/35/5/5 Stocks/Bonds/BTC/ETH	10.5%	11.8%	0.72

Sharpe ratio = return per unit of risk (higher is better).

Caveat

This works in "normal" times. During major crises (2022 crypto winter), crypto correlations with stocks **spike to 0.6–0.8**, and diversification benefits disappear exactly when you need them most.

The Correlation Problem in Crypto

Within crypto:

	BTC	ETH	SOL
BTC	1.0	0.80	0.70
ETH	0.80	1.0	0.75
SOL	0.70	0.75	1.0

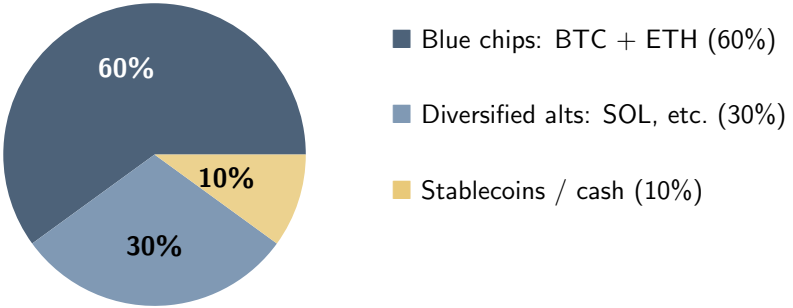
Correlations of 0.7–0.8 mean crypto assets **move together**. Diversifying across cryptos alone doesn't help much.

During crashes:

- Normal times: BTC-S&P 500 correlation ≈ 0.2
- During crashes: correlation jumps to 0.6–0.8
- "Everything goes down together"
- This is called **correlation breakdown**

True diversification requires assets outside crypto: bonds, commodities, real estate.

A Sensible Crypto Portfolio: The "60/30/10" Rule



- **60% BTC/ETH**: battle-tested, most liquid, lowest relative risk
- **30% alts**: higher growth potential but higher risk
- **10% stablecoins**: "dry powder" for buying dips, earning yield

Staking Yield: Additional Return Component

What is staking?

Lock your tokens to help secure the network. In return, earn **staking rewards** — like interest on a savings account.

Asset	Staking Yield (APY)	Lock-up
Ethereum (ETH)	3.0–4.5%	Variable (days to weeks)
Solana (SOL)	5.0–7.0%	$\sim$2 days unstaking
Cosmos (ATOM)	15–20%	21 days unstaking
Polkadot (DOT)	12–15%	28 days unstaking

Caution: High yields often come with higher token risk. A 20% yield is meaningless if the token drops 60%.

Outline

Why Regulate Crypto?

Without regulation:

- Terra/Luna collapse: $40B lost, no recourse
- FTX fraud: $8B customer funds misused
- Rug pulls: new token launched, creators disappear with funds
- Money laundering through mixers
- No deposit insurance

Goals of regulation:

1. **Investor protection**: disclosure, audits, insurance
2. **Financial stability**: prevent systemic risk
3. **AML/KYC**: prevent money laundering and terrorist financing
4. **Fair markets**: prevent manipulation
5. **Innovation**: don't kill useful technology

The challenge: regulate enough to protect people, but not so much that innovation moves offshore.

EU MiCA: The World's First Comprehensive Crypto Law

Markets in Crypto-Assets Regulation [ ]

Enacted 2023, fully effective since Dec. 2024. Covers all 27 EU member states.

Key provisions:

- **Stablecoin issuers**: must hold 1:1 reserves, regular audits
- **Exchanges**: must be licensed, segregate customer funds
- **Token issuers**: white paper requirements (like a prospectus)
- **Market abuse**: insider trading and manipulation prohibited
- **Consumer protection**: clear risk warnings required

Impact: If MiCA had existed in 2021, Terra/UST likely could not have operated in the EU without proving adequate reserves.

US: The Fragmented Approach

The big question: Is a token a security? The **Howey Test** (from a 1946 Supreme Court case):

1. Investment of money
2. In a common enterprise
3. With expectation of profits
4. From the efforts of others

If yes ⇒ it's a **security** ⇒ SEC regulates it.
If no ⇒ it might be a **commodity** ⇒ CFTC regulates it.

Agency	Claims
SEC	Most tokens are securities
CFTC	BTC and ETH are commodities
FinCEN	AML/KYC compliance
IRS	Crypto is taxable property

Result: confusion, regulation by enforcement, and uncertainty for businesses.

Global Landscape: Asia-Pacific

Country	Approach	Status
Japan	Progressive, licensed exchanges	Clear framework since 2017
South Korea	Regulated, investor protections	Real-name trading since 2018
Singapore	Licensing regime (MAS)	Innovation-friendly but strict
Hong Kong	Re-opening to crypto	Licensed retail trading since 2023
China	**Complete ban** on trading & mining	Since 2021 (but CBDC active)
India	30% crypto tax, uncertain rules	Discouraging but not banned

Pattern: Most countries are moving from "ignore" or "ban" toward structured regulation. The question is *how strict*.

The Unsolved Problem: How Do You Regulate DeFi?

The Challenge

Traditional regulation requires a **responsible entity**: a company, a CEO, a compliance officer. DeFi protocols are...

DeFi characteristics:

- Run by smart contracts (code)
- No CEO, no headquarters
- Governed by token holders (DAOs)
- Accessible globally, 24/7
- Pseudonymous users

Regulatory approaches:

- Regulate the **front-ends** (websites)
- Regulate the **developers** who wrote the code
- Regulate the **token holders** who govern
- Regulate the **on/off ramps** (fiat $\leftrightarrow$ crypto)
- Accept that some DeFi is **unregulable**

No country has fully solved this yet. It's the frontier of financial regulation.

Outline

Tokenization: Putting Real Assets on Blockchain

What is Tokenization?

Representing ownership of real-world assets (real estate, bonds, art) as tokens on a blockchain. Enables fractional ownership and 24/7 trading.

Asset Class	**Example**	**Market Size**
US Treasuries	Tokenized T-bills on Ethereum	\$2B+
Real estate	Fractional property ownership	\$1B+
Private credit	On-chain lending to businesses	\$4B+
Art & collectibles	Fractional Picasso ownership	\$500M+
Total tokenized	(excl. stablecoins)	**\$10B+**

BlackRock, JPMorgan, Goldman Sachs are all building tokenization platforms. This is where TradFi and crypto converge.

AI + DeFi: Autonomous Financial Agents

What if AI agents could manage money on DeFi protocols autonomously?

Already Happening

- AI agents that rebalance liquidity positions
- Automated yield optimization across protocols
- Smart order routing using ML predictions
- AI-powered risk monitoring

Open Questions

- Who is liable if an AI agent causes losses?
- Can AI agents be regulated?
- What happens when AI agents trade with each other?
- Could this create new systemic risks?

This is where Days 3 and 4 converge: blockchain economics + ML in a single autonomous system.

Zero-Knowledge Proofs: Privacy Meets Compliance

The Concept (no math, just intuition)

A **zero-knowledge proof** lets you prove something is true **without revealing the underlying information**.

Examples:

- Prove you're over 18 **without showing your ID**
- Prove you have enough funds **without revealing your balance**
- Prove you're not on a sanctions list **without revealing your identity**
- Prove a transaction is valid **without showing the amounts**

Why it matters: ZK proofs could solve the privacy vs. regulation tension. You get compliance *and* privacy. Projects like zkSync and Polygon zkEVM are building this today.

Risks on the Horizon

Risk	Timeline	Impact
Quantum computing	10–20 years	Could break current encryption. Post-quantum cryptography is being developed now.
ESG concerns	Ongoing	PoW energy use is controversial. PoS helps, but e-waste and energy from data centers remain.
Regulatory crackdown	1–5 years	Overly strict rules could push innovation to less regulated jurisdictions.
AI-driven manipulation	Now	Deepfakes, fake news, and AI-driven pump-and-dump schemes are emerging threats.

Outline

Hands-On Exercise

Building and Evaluating a Crypto Portfolio

Python / Jupyter Notebook

Exercise: Build a Crypto Portfolio

Goal: Apply portfolio theory and risk measurement to real crypto data.

Given data (pre-loaded)

- Daily returns for BTC, ETH, SOL, and a stablecoin (USDC yield)
- 2 years of data (2024–2026)
- Pre-computed correlation matrix

Your tasks:

1. Compute means, volatilities, and correlations
2. Calculate VaR(95%) for a 100% BTC portfolio
3. Calculate VaR(95%) for a diversified portfolio
4. Plot the efficient frontier (BTC + stablecoin)
5. Find the minimum-variance portfolio

Step 1: Compute Descriptive Statistics

Asset	Ann. Return	Ann. Volatility	Sharpe Ratio
BTC	45%	60%	0.67
ETH	35%	75%	0.40
SOL	80%	95%	0.79
Stablecoin	5%	0.5%	–

Your code:

```
annual_return = df[assets].mean() * 252
annual_vol = df[assets].std() * np.sqrt(252)
sharpe = annual_return / annual_vol
```

Note: We multiply daily stats by $\sqrt{252}$ (for vol) and 252 (for returns) to annualize. $252 =$ trading days per year.

Step 2: Examine the Correlation Matrix

	BTC	ETH	SOL	Stablecoin
BTC	1.00	0.78	0.68	0.02
ETH	0.78	1.00	0.75	0.01
SOL	0.68	0.75	1.00	0.03
Stablecoin	0.02	0.01	0.03	1.00

Key observations:

- Crypto assets are highly correlated (0.68–0.78)
- Stablecoins are nearly uncorrelated with everything (≈ 0)
- **This means:** mixing crypto with stablecoins provides the best diversification within a crypto-only portfolio

Step 3: VaR for Concentrated vs. Diversified Portfolio

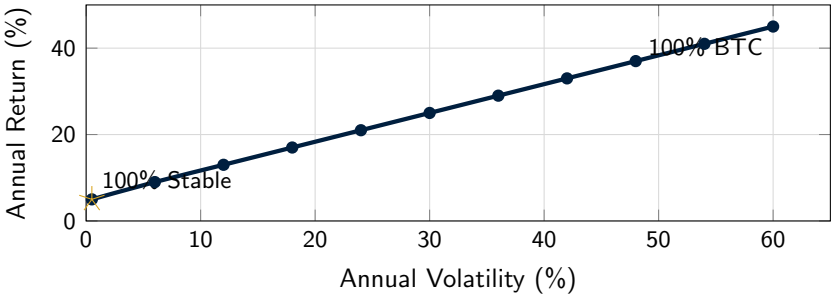
Portfolio A: 100% BTC ($10,000)
Portfolio B: 50% BTC + 30% ETH + 10% SOL + 10% Stablecoin

```
# VaR(95%) = Portfolio * z * daily_vol
var_btc_only = 10000 * 1.65 * btc_daily_vol
# For diversified:  compute portfolio volatility first
port_vol = np.sqrt(w.T @ cov_matrix @ w)
var_diversified = 10000 * 1.65 * port_vol
```

Expected Results

- 100% BTC: VaR(95%) $\approx$ $624
- Diversified: VaR(95%) $\approx$ $410
- **Diversification saves $\sim$$214 in daily risk** (34% reduction!)

Step 4: Plot the Efficient Frontier (BTC + Stablecoin)



Each point = a different mix of BTC and stablecoins. Moving right: more BTC, more return, more risk.

Step 5: Find the Minimum-Variance Portfolio

For two assets, the minimum-variance weight for asset 1 is:

$$w_1^* = \frac{\sigma_2^2 - \rho_{12}\sigma_1\sigma_2}{\sigma_1^2 + \sigma_2^2 - 2\rho_{12}\sigma_1\sigma_2}$$

With BTC ($\sigma_1 = 60\%$) and stablecoin ($\sigma_2 = 0.5\%$, $\rho \approx 0$):

$$w_{\text{BTC}}^* = \frac{0.005^2 - 0}{0.60^2 + 0.005^2 - 0} = \frac{0.000025}{0.360025} \approx 0.007\%$$

Result

The mathematically optimal "minimum risk" portfolio is almost 100% stablecoin. This makes sense: stablecoins have near-zero volatility!

In practice: investors accept more risk for higher returns. The "right" portfolio depends on your risk tolerance.

Debate: Should Crypto Be Regulated Like Traditional Finance?

FOR: Same Rules

- Same risks deserve same protections
- FTX, Terra/Luna prove self-regulation fails
- Institutional adoption needs clear rules
- Consumers don't understand the risks
- "Same activity, same regulation"

AGAINST: Different Rules

- Crypto is fundamentally different (decentralized)
- Over-regulation kills innovation
- Old rules don't fit new technology
- Users should have freedom to take risks
- "Regulate the risks, not the technology"

15-minute structured debate: divide the room in half.

What Was the Most Surprising Thing This Week?

Quick round-table (2 minutes each):

1. What concept or fact surprised you the most?
2. What changed your mind about something?
3. What question do you still have?
4. What would you want to explore in your group project?

Some prompts

- "I didn't know that validators choose transaction order..."
- "I was surprised that 54% accuracy is actually useful..."
- "I didn't realize stablecoins could collapse like that..."
- "The CBDC privacy tradeoff is more complex than I thought..."

Course Wrap-Up

What You've Learned

- Day 1: How crypto works
- Day 2: DeFi and AMMs
- Day 3: Incentives, fees, and money
- Day 4: AI for crypto markets
- Day 5: Risk, portfolios, and regulation

You now have the foundations to read crypto research, evaluate projects critically, and understand the ongoing debates.

Group Project Guidance

- Teams of 3–4 students
- Choose a topic from the project brief
- 15-minute presentation + 5-page report
- Combine concepts from multiple days
- Due: [see project brief]

Key references:
[5], [3], [1], [2]

Thank you for an excellent week!

References I

[1] Saifedean Ammous. *The Bitcoin Standard: The Decentralized Alternative to Central Banking*. Wiley, 2018.

[2] Bank for International Settlements. *Cryptocurrencies and Decentralised Finance*. BIS Annual Economic Report, Chapter III. Bank for International Settlements, 2024.

[3] Marco Di Maggio. *Blockchain, Crypto and DeFi: Bridging Finance and Technology*. Wiley, 2024.

[4] European Commission. *Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA)*. Official Journal of the European Union, L 150/52. 2023.

[5] Campbell R. Harvey, Ashwin Ramachandran, and Joey Santoro. *DeFi and the Future of Finance*. Wiley, 2021.

[6] Harry Markowitz. "Portfolio Selection". In: *Journal of Finance* 7.1 (1952), pp. 77–91.