



How We Tame Our AI Models

Anton Antonov Head of AI and Quant Research antonov@dxfeed.com

DKF Munich, 13.05.2025



Introduction



37%

of conversations in "Computer & Mathematical" (Antropic)

71%

adoption rate of GenAI in business functions (Stanford AI report 2025) 2.6x/year

growth of training cost since 2016, frontier models, in \$ (Epoch AI)

2023

year of PoCs

2024

year of production

2025

year of business value

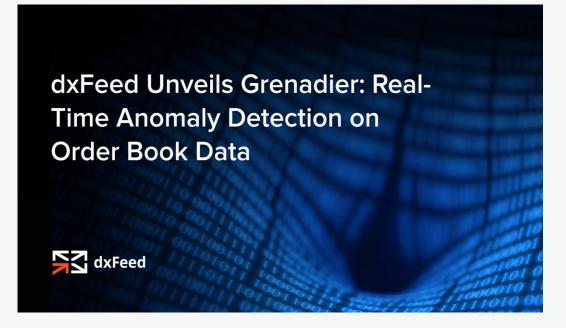
In this talk:

- Why making AI truly valuable in financial markets is difficult
- How we manage it, with practical case studies









The AI Market Analysis Challenge



Unique demands of financial markets:

- Real-time processing requirements
- Low tolerance for errors
- Multiple, often conflicting data sources
- Complex interdependencies between data points

Common AI implementation pitfalls:

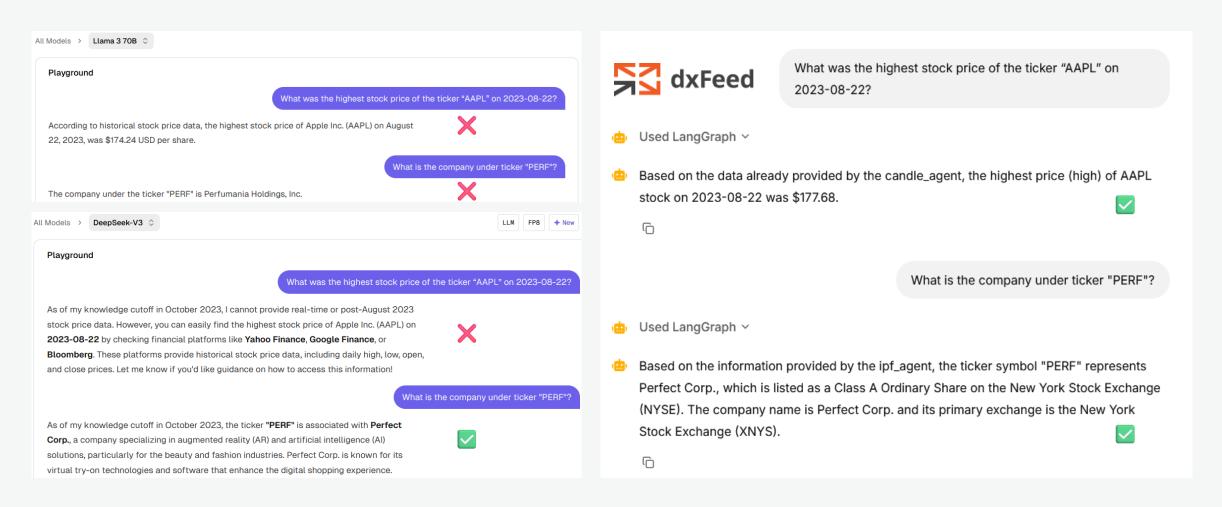
- Over-reliance on black-box models
- Insufficient data validation
- Poor integration with existing systems
- Neglecting calculation accuracy

What is the square root of 66.777.278.569?

The square root of 66,777,278,569 is 258,281.

The AI Market Analysis Challenge





Our Approach, pt. 1: MCP



Model Context Protocol (MCP):

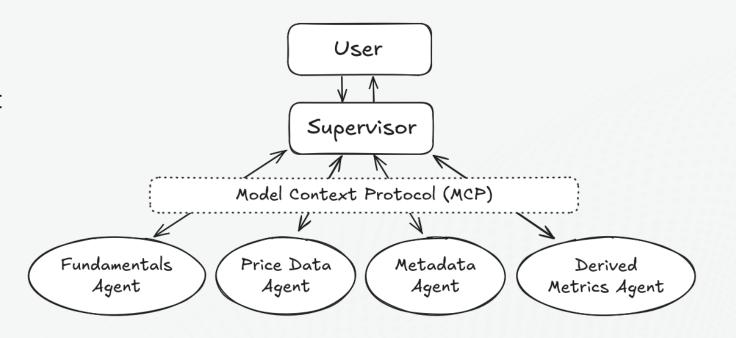
An open standard developed by Anthropic to enable AI models, particularly LLMs, to securely and efficiently access and interact with external data sources and tools.

Benefits:

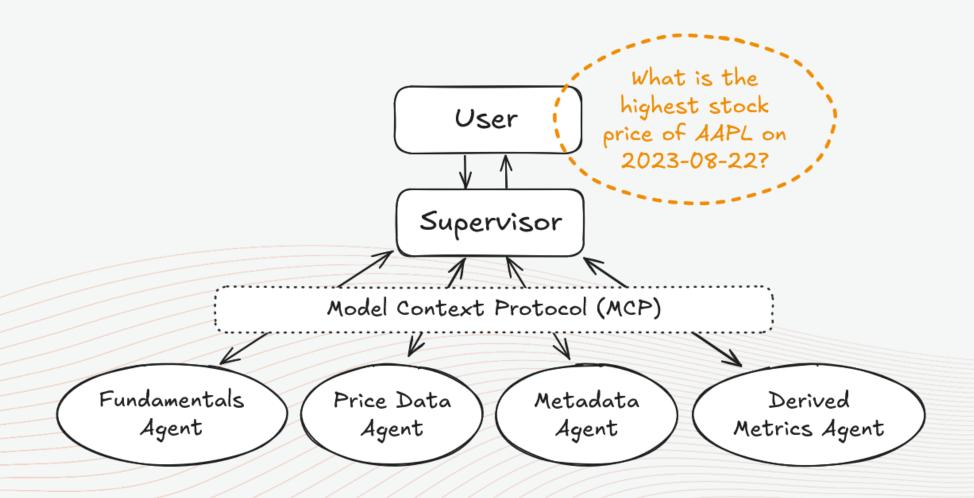
- real-time data access,
- reduced integration complexity,
- enhanced security and compliance.

"...like a USB-C port for AI applications".

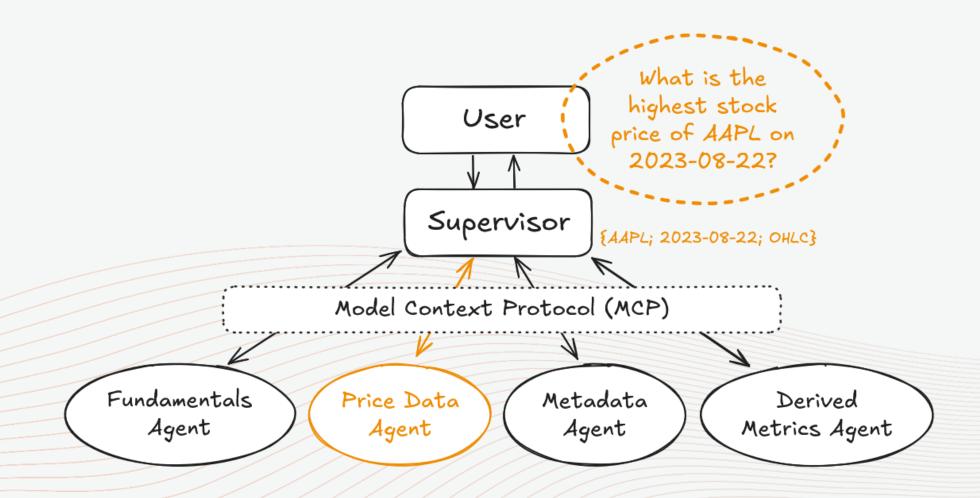
https://modelcontextprotocol.io



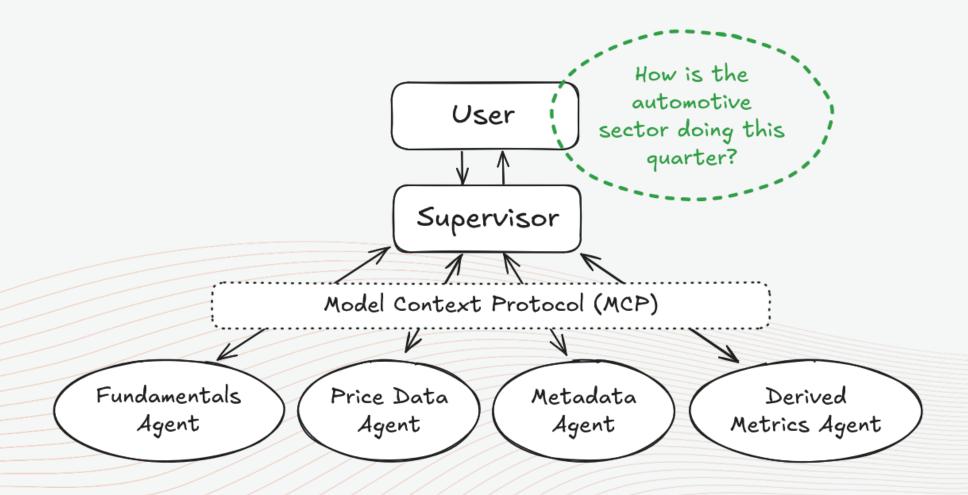




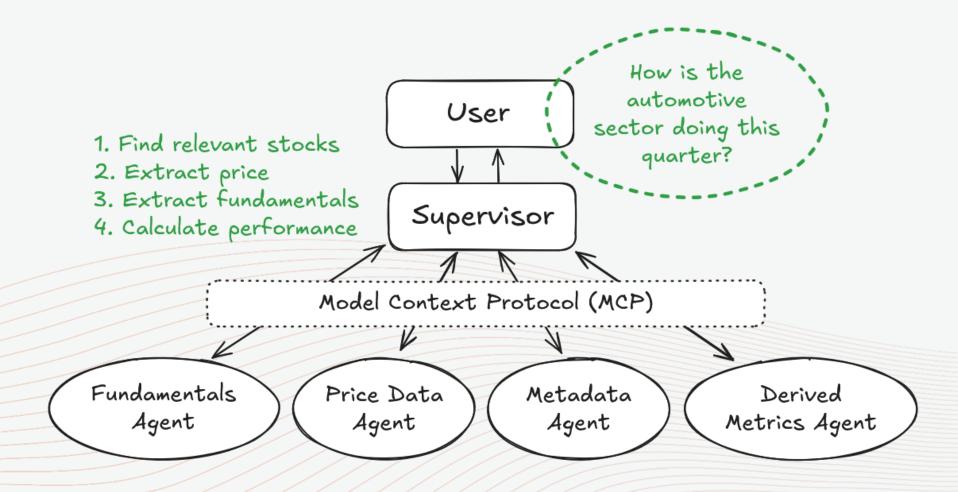




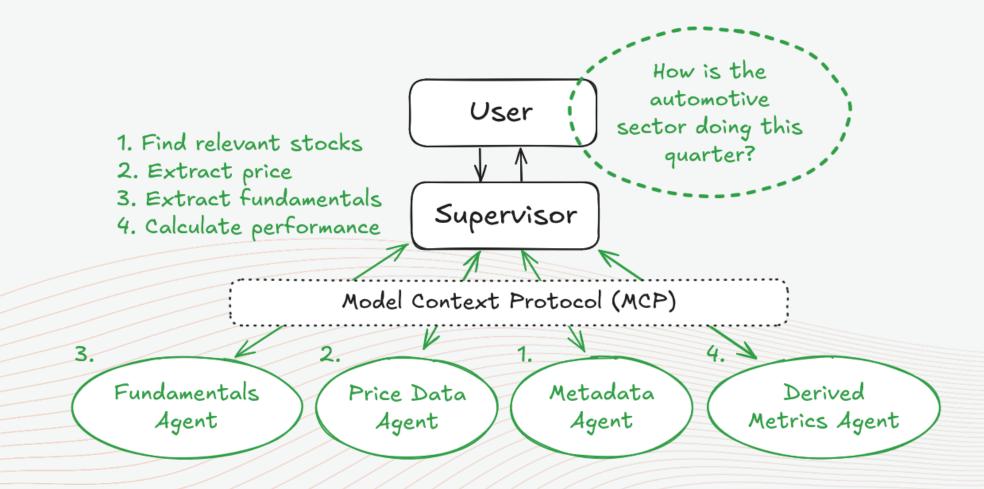










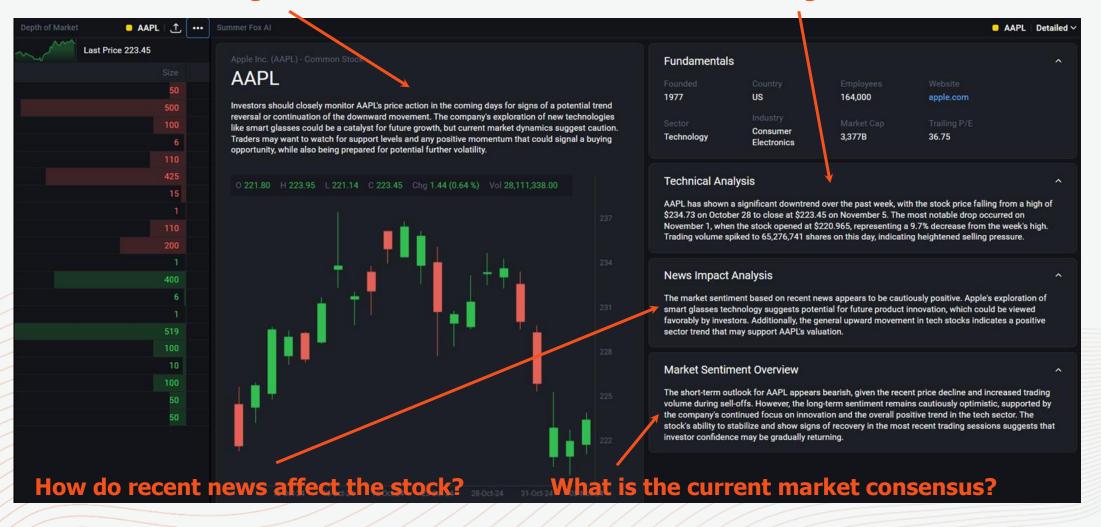


dxFeed SummerFox in Action



What is the the high-level outlook?

What data-driven insights are there?



Our Approach, pt. 3: Implementation



Prompt engineering techniques:

- Be specific
- Provide few-shot response examples
- Establish specific guardrails
- Make sure that the LLM does not do what it's not good at (zero-shot reasoning, derived calculations)

Performance and audit:

- Enable prompt and response caching
- Implement tracing (e.g., via <u>Langsmith</u>)
- Have multiple independent LLM vendors

Quality control through **Deepeval**

Key metrics to monitor:

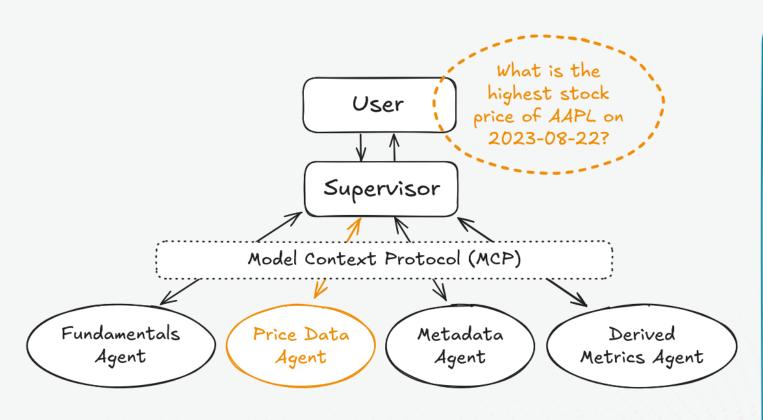
- Factual correctness
- Alignment
- Toxicity
- Contextual relevancy
- Bias
- Hallucination rates
- Adherence to guardrails

Eval cycles in the development workflow:

- At new releases
- For switchover to new models
- As early warnings of model degradation

Our Approach, pt. 3: Evals





What is the point validating LLM against itself?

Against a bigger and better model!

LLM-as-a-judge

Q: What agents should be called to answer this question?

A: Price Data Agent

A: Price Data Agent

Q: Is the answer relevant to the question?

A: The Apple stock's last week high was \$202.85

Q: Is the system aligned with given instructions?

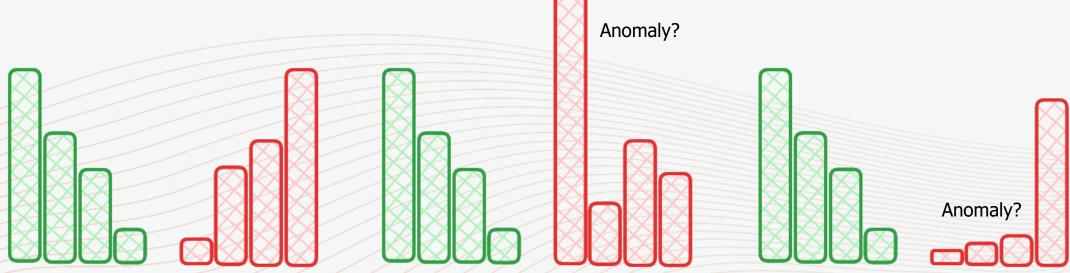
A: I'm sorry, Dave. I'm afraid I can't do that.

Our Approach, pt. 4: In-house Models



The Market Anomaly Detection Challenge:

- The needle in the haystack problem: rare and fuzzily defined events
- Rule-based or feature engineered conditions:
 - Must be manually constructed or selected
 - Must be calibrated and recalibrated
 - May get outdated quickly

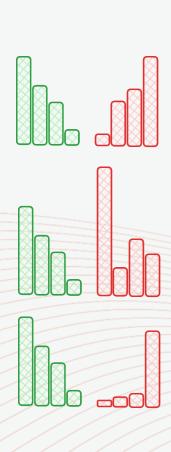


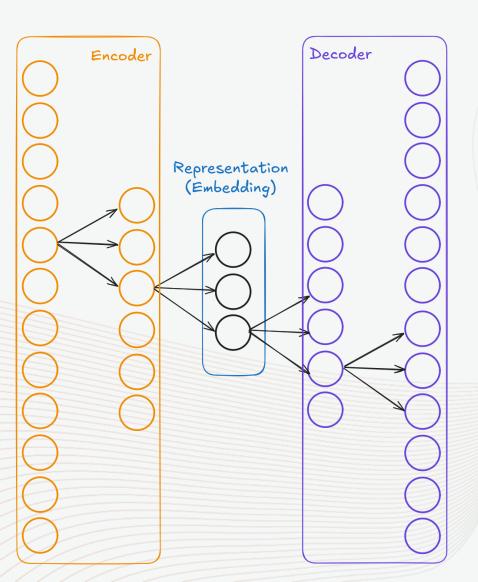
Our Approach, pt. 4: In-house Models



Our training setup:

- Order book snapshots sourced from Historical Data Lake (HDL)
- Autoencoder architecture (unsupervised learning)
- Reconstruction quality is what defines anomalousness
- Full control over the neural net parameters and model weights





dxFeed Grenadier in Action

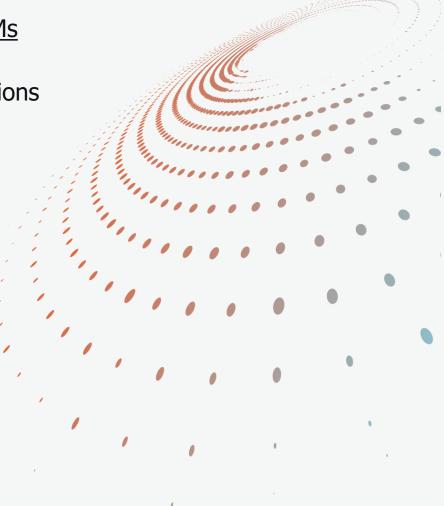




Key Takeaways



- 1. AI in finance requires specialized approaches beyond generic LLMs
 - a. Agentic workflows with guaranteed knowledge extraction
 - b. In-house ML models trained specifically for financial applications
- 2. Model Context Protocol enables flexible, secure tool use
- 3. Output quality is secured via:
 - a. Data layers and calculation engines
 - b. "LLM-as-a-judge" tests and specialized evals
 - c. Full control over the training cycle for in-house models

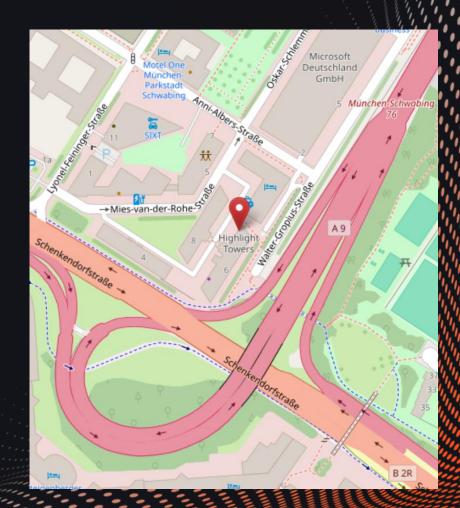


References

- <u>SummerFox</u>: AI-driven market reporting engine
- Grenadier: L2-based anomaly detection model
- Follow dxFeed on <u>LinkedIn</u> or <u>YouTube</u>
- Connect on LinkedIn: <u>@tonytonov</u>
- Visit us in Highlight Towers!

Materials used:

- 1. The Anthropic Economic Index, https://www.anthropic.com/news/the-anthropic-economic-index
- 2. The 2025 AI Index Report by The Stanford Institute for Human-Centered AI, https://hai.stanford.edu/ai-index/2025-ai-index-report
- 3. Machine Learning Trends by Epoch AI, https://epoch.ai/trends
- 4. H. Kang and X.Y. Liu, Deficiency of Large Language Models in Finance: An Empirical Examination of Hallucination, https://arxiv.org/abs/2311.15548
- 5. J.P. Bouchaud, J. Bonart, J. Donier, M. Gould, *Trades, Quotes and Prices: Financial Markets Under the Microscope*, Cambridge University Press, 2018



Thanks!