When AI Is Confidently Wrong: Calibration and Risk Analysis of Large Language Models in Financial Decision-Making

Wei-Lun Cheng[a], Wei-Chung Miao[b,*]

[a]*Institute of Information Science, Academia Sinica, Taipei, Taiwan*
[b]*Department of Finance, National Chengchi University, Taipei, Taiwan*

Abstract

Large Language Models (LLMs) are increasingly deployed in financial applications, yet their reliability in high-stakes decision-making remains understudied. We evaluate the confidence calibration of LLMs on 257 CFA (Chartered Financial Analyst) examination questions using two models (GPT-4o-mini, Qwen3-32B) and two confidence estimation methods (verbalized, self-consistency). We find pervasive overconfidence: the average expressed confidence exceeds actual accuracy by 22–32 percentage points ($t = 9.70$, $p < 0.0001$). Critically, **30.0% of all responses are high-confidence errors** (confidence $\geq 80\%$), and among incorrect answers, 66.4% are delivered with high confidence. These overconfident errors are not uniformly distributed: Ethics & Standards questions exhibit a 43.5% overconfident error rate, compared to 22.2% for Derivatives ($\chi^2 = 12.37$, $p = 0.030$). We introduce Confidence-at-Risk (CaR), adapting Value-at-Risk methodology to AI confidence assessment, and connect our findings to CFA Institute Ethics Standards, arguing that deployment of miscalibrated AI may violate fiduciary duty requirements. Our results suggest that financial regulators should establish minimum calibration standards—specifically, Expected Calibration Error (ECE) below 0.15—before permitting AI deployment in advisory roles.

Keywords: Large Language Models, Calibration, Financial AI, Risk Management, CFA Examination, Overconfidence

*Corresponding author
Email addresses: wlcheng@iis.sinica.edu.tw (Wei-Lun Cheng), wcmiao@nccu.edu.tw (Wei-Chung Miao)

1. Introduction

The deployment of Large Language Models (LLMs) in financial services has accelerated rapidly, with applications spanning automated financial advice, risk assessment, equity research, and regulatory compliance [10, 6]. A growing body of work evaluates LLM *accuracy* on financial benchmarks—whether models can pass the CFA exam, correctly price derivatives, or interpret financial statements. However, accuracy alone is a poor guide to deployment safety.

Consider two AI systems: Model A achieves 70% accuracy with well-calibrated confidence (it says "85% confident" when it is correct 85% of the time), while Model B achieves 75% accuracy but systematically overstates confidence. Model B is more dangerous despite being more accurate, because its confidence signal cannot be trusted to identify errors. A financial advisor who says "I'm 95% certain this bond has a duration of 4.2 years" but is wrong poses a far greater risk than one who acknowledges uncertainty. This phenomenon—*overconfident error*—represents the most dangerous failure mode for AI systems in finance.

Yet confidence calibration of LLMs in financial contexts remains largely unexplored. Prior calibration studies focus on general knowledge [5], medical diagnosis [8], or scientific reasoning [7], leaving a critical gap in understanding how LLMs behave in domains where miscalibrated confidence carries direct monetary consequences.

This paper makes four contributions:

1. We systematically evaluate LLM calibration on CFA examination questions—a standardized benchmark for financial professional competency—using 257 observations across two models and two confidence estimation methods.
2. We identify and quantify *overconfident errors*, finding that 30.0% of all responses are high-confidence errors (confidence $\geq 80\%$), significantly exceeding a 20% baseline ($z = 3.99$, $p < 0.0001$).
3. We introduce *Confidence-at-Risk* (CaR), adapting Value-at-Risk methodology to quantify the reliability of AI confidence signals for risk management.
4. We connect calibration findings to the CFA Institute's Code of Ethics, arguing that poorly-calibrated AI deployment may violate fiduciary

duty standards, and propose minimum calibration thresholds for financial AI regulation.

2. Related Work

2.1. LLM Calibration

Calibration refers to the alignment between a model's expressed confidence and its actual accuracy [4]. A well-calibrated model expressing 80% confidence should be correct approximately 80% of the time. Kadavath et al. [5] demonstrate that large language models "mostly know what they know," but this self-knowledge degrades on out-of-distribution tasks. Lin et al. [7] show that models can be prompted to verbalize uncertainty, though the resulting confidence estimates often exhibit systematic biases. Xiong et al. [11] survey confidence estimation methods for LLMs, identifying verbalized confidence, consistency-based, and logit-based approaches as the three primary paradigms.

2.2. AI in Financial Applications

Domain-specific financial LLMs have emerged rapidly. BloombergGPT [10] demonstrated competitive performance on financial NLP tasks. Ke et al. [6] introduced FinDAP, a three-stage training pipeline that adapts Llama-3 to finance via continual pre-training, supervised fine-tuning, and preference alignment, achieving state-of-the-art results on CFA examination benchmarks. Callanan et al. [1] evaluated GPT-4 on CFA Level I, finding pass-rate performance but without examining confidence calibration.

2.3. Risk and Trust in AI-Assisted Financial Decision-Making

The literature on trust in algorithmic advice reveals a paradox: users both over-rely on and under-rely on algorithmic recommendations depending on context [2]. Green & Chen [3] argue that AI transparency alone is insufficient—what matters is whether users can accurately assess when AI is reliable. Our work contributes to this debate by showing that LLM confidence signals, which serve as the primary transparency mechanism, are themselves unreliable in financial domains.

3. Methodology

3.1. Confidence Estimation Methods

We employ two complementary confidence estimation approaches:

Verbalized Confidence. Following Lin et al. [7], we prompt models to express confidence as a percentage alongside their answer:

> *"Answer the following CFA question. After your answer, state your confidence level as a percentage (0–100%). Be honest about your confidence—if you are uncertain, say so with a lower percentage."*

Self-Consistency. Following Wang et al. [9], we sample $k = 10$ responses at temperature $\tau = 0.7$ for each question. Confidence is defined as the agreement ratio: $c = n_{\text{majority}}/k$, where n_{majority} is the count of the most frequent answer.

3.2. Calibration Metrics

Our primary metric is the *Expected Calibration Error* (ECE) [4]:

$$\text{ECE} = \sum_{m=1}^{M} \frac{|B_m|}{n} \left|\text{acc}(B_m) - \text{conf}(B_m)\right| \tag{1}$$

where B_m denotes the set of predictions in confidence bin m, $\text{acc}(B_m)$ is the accuracy within that bin, and $\text{conf}(B_m)$ is the average confidence. We use $M = 10$ equal-width bins.

We also report the *Brier Score* $= \frac{1}{n}\sum_{i=1}^{n}(c_i - y_i)^2$, where c_i is the expressed confidence and $y_i \in \{0, 1\}$ is the correctness indicator; AUROC measuring whether confidence scores can discriminate correct from incorrect answers; and the *Overconfidence Gap* $= \overline{c} - \overline{y}$, which is positive when the model is systematically overconfident.

3.3. Overconfident Error Identification

We define *overconfident errors* as cases satisfying:

$$\text{Overconfident Error} = \mathbf{1}\left[\text{confidence} \geq \theta \ \wedge \ \text{answer incorrect}\right] \tag{2}$$

with threshold $\theta = 0.80$. This threshold is motivated by the decision-making context: a financial professional receiving a signal with $\geq 80\%$ confidence would typically act on it without extensive verification.

3.4. Confidence-at-Risk (CaR)

Drawing from Value-at-Risk (VaR) methodology, we introduce *Confidence-at-Risk*:

$$\text{CaR}(\alpha) = \inf\{c^* : P(\text{incorrect} \mid \text{confidence} \geq c^*) \leq \alpha\} \tag{3}$$

CaR answers the question: "What is the minimum confidence level at which the error rate falls below α?" If CaR is undefined (no threshold achieves the target error rate), the model's confidence signal is fundamentally unreliable for risk-budgeting purposes.

4. Data and Experimental Design

4.1. Dataset

We use the CFA-Challenge dataset from FinEval [6], comprising 90 questions drawn from CFA Level III curriculum materials (SchweserNotes). All questions are multiple-choice with three options (A, B, C), spanning the full CFA curriculum: Ethics & Standards, Quantitative Methods, Economics, Financial Reporting, Corporate Finance, Equity, Fixed Income, Derivatives, Alternative Investments, and Portfolio Management. CFA Level III questions emphasize application and analysis, representing the most cognitively demanding tier of the CFA Program.

Table 1: Dataset Summary

Dataset	**Questions**	**Options**	**Source**
CFA-Challenge	90	3 (A/B/C)	SchweserNotes Level III

4.2. Models

We evaluate two LLMs representing different architectures and scales:

- **GPT-4o-mini** (OpenAI): A proprietary, cloud-hosted model optimized for efficient inference. Evaluated using both verbalized confidence ($n = 95$) and self-consistency with $k = 10$ samples ($n = 90$).
- **Qwen3-32B** (Alibaba): An open-weight, 32-billion parameter model run locally via Ollama. Evaluated using verbalized confidence ($n = 72$).

The total dataset comprises 257 model–question–method observations. Both models are evaluated at temperature $\tau = 0.0$ for single-shot methods and $\tau = 0.7$ for self-consistency sampling. Answers and confidence values are extracted using a five-layer regex chain with fallback parsing.

5. Results

5.1. Overall Calibration

Table 2 presents calibration metrics across all model–method combinations. All configurations exhibit substantial overconfidence, with the overconfidence gap ranging from +22.5% (Qwen3-32B) to +31.5% (GPT-4o-mini verbalized).

Table 2: Calibration Metrics by Model and Confidence Estimation Method

Model	**Method**	**N**	**Acc.**	**Avg Conf.**	**ECE**	**Brier**	**AUROC**	**OC Gap**
GPT-4o-mini	Self-consistency	90	.522	.829	.307	.334	.639	+.307
GPT-4o-mini	Verbalized	95	.526	.841	.315	.340	.586	+.315
Qwen3-32B	Verbalized	72	.611	.836	.247	.226	.787	+.225

ECE = Expected Calibration Error; Brier = Brier Score; AUROC = Area Under ROC Curve; OC Ga
= Overconfidence Gap (Avg Confidence − Accuracy).

A one-sample t-test on the per-observation overconfidence gap (confidence minus correctness indicator) yields $t = 9.70$ ($p < 0.0001$), confirming that LLM overconfidence on CFA questions is highly statistically significant (H1).

Figure 1 presents reliability diagrams. All models exhibit a consistent pattern: the calibration curve lies well below the diagonal (perfect calibration), indicating that models are more confident than they are accurate across virtually all confidence levels.

Qwen3-32B achieves the best calibration (ECE = 0.247) and highest discriminative ability (AUROC = 0.787), while GPT-4o-mini shows the worst calibration regardless of estimation method. Self-consistency marginally improves ECE over verbalized confidence for GPT-4o-mini (0.307 vs. 0.315), but substantially improves AUROC (0.639 vs. 0.586), suggesting it provides more discriminative confidence estimates.

Figure 2 visualizes the overconfidence gap across all configurations. In every case, expressed confidence substantially exceeds actual accuracy, confirming that overconfidence is a pervasive, not idiosyncratic, phenomenon.

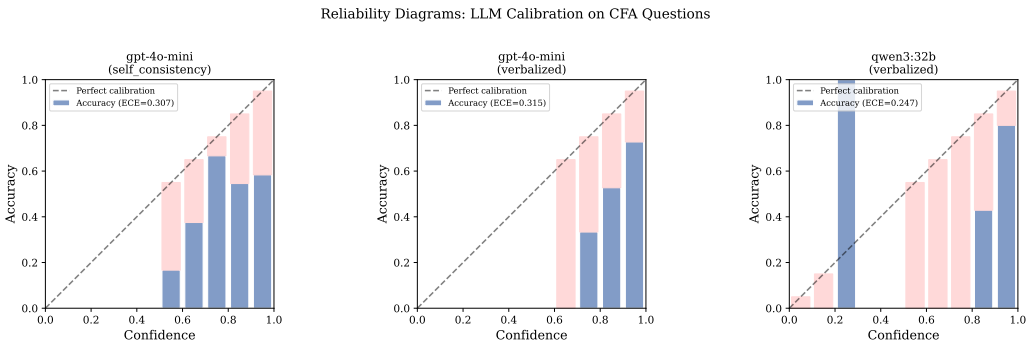

Figure 1: Reliability diagrams for three model–method configurations on CFA-Challenge questions. The dashed diagonal represents perfect calibration. Red-shaded regions indicate overconfidence: the gap between expressed confidence and actual accuracy. All configurations exhibit systematic overconfidence, particularly in the 0.8–1.0 confidence range where most predictions concentrate.

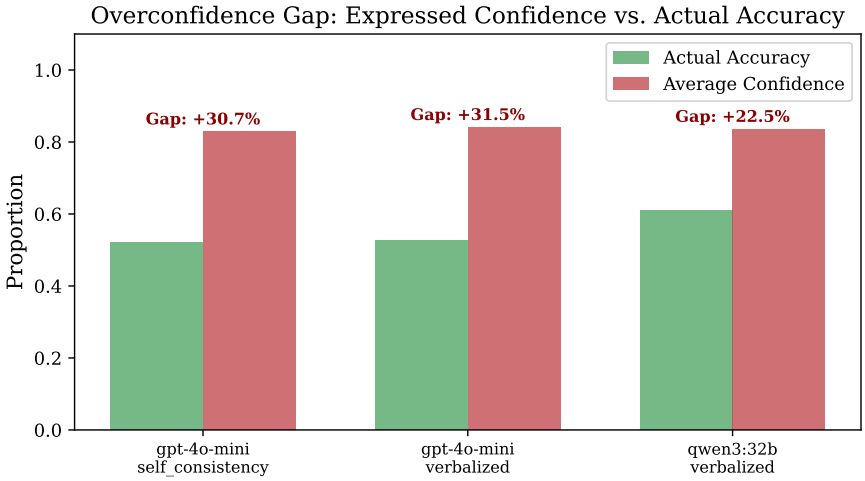

Figure 2: Overconfidence gap across models and methods. Blue bars represent actual accuracy; red bars represent average expressed confidence. The gap between them—ranging from +22.5% to +31.5%—quantifies the degree of systematic overconfidence.

5.2. Overconfident Error Analysis

Table 3 details the overconfident error profile. Across all 257 observations, 77 are overconfident errors (30.0%), significantly exceeding a 20% baseline (binomial test, $z = 3.99$, $p < 0.0001$; H3). Among the 116 incorrect answers, 66.4% are delivered with confidence $\geq 80\%$ ($z = 3.53$, $p = 0.0002$), meaning that *most errors are high-confidence errors*. The average confidence of overconfident errors is 89.0%.

Table 3: Overconfident Error Analysis (Confidence $\geq 80\%$)

Model / Method	**Total**	**Errors**	**OC Errors**	**OC Rate**
GPT-4o-mini / Self-consistency	90	43	25	27.8%
GPT-4o-mini / Verbalized	95	45	38	40.0%
Qwen3-32B / Verbalized	72	28	14	19.4%
Overall	**257**	**116**	**77**	**30.0%**

5.3. Topic-Level Miscalibration

Table 4 reveals significant variation in overconfident error rates across CFA knowledge domains ($\chi^2 = 12.37$, $p = 0.030$; H4).

Table 4: Calibration Metrics by CFA Topic (Topics with $N \geq 10$)

CFA Topic	**N**	**Acc.**	**ECE**	**OC Errors**	**OC Rate**
Ethics & Standards	46	.478	.360	20	43.5%
Portfolio Management	14	.500	.357	6	42.9%
Economics	10	.600	.340	4	40.0%
Fixed Income	20	.650	.223	6	30.0%
Derivatives	27	.593	.291	6	22.2%

Ethics & Standards—the CFA curriculum's foundational domain—exhibits the highest overconfident error rate (43.5%) and lowest accuracy (47.8%). This is particularly concerning: ethics questions require nuanced professional judgment, exactly the domain where overconfident AI poses the greatest fiduciary risk. Derivatives, despite involving complex quantitative reasoning, shows a lower overconfident error rate (22.2%), suggesting that models may be better calibrated on computation-heavy topics where confidence can be partially grounded in mathematical consistency.

5.4. Coverage-Accuracy Tradeoff

Figure 3 presents the selective prediction analysis. If a financial institution restricts AI to answer only questions where confidence exceeds a threshold, what accuracy can be achieved?

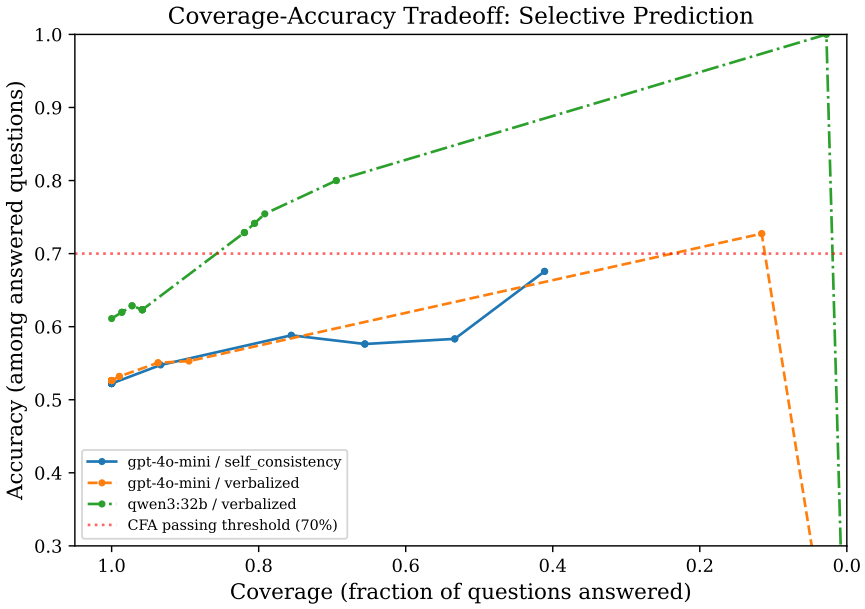

Figure 3: Coverage-accuracy tradeoff under selective prediction. As the confidence threshold increases (moving right to left), fewer questions are answered (lower coverage) but with higher accuracy. The horizontal dashed line marks the CFA passing threshold (70%). Qwen3-32B reaches 81.3% accuracy at 69% coverage, while GPT-4o-mini cannot reach 70% accuracy at any coverage level.

For Qwen3-32B, restricting to predictions with confidence $\geq 90\%$ yields 81.3% accuracy at 69% coverage—exceeding the CFA passing threshold. However, GPT-4o-mini cannot achieve 70% accuracy at *any* confidence threshold, reaching only 67.6% even when restricted to its highest-confidence predictions (41% coverage). This demonstrates that selective prediction viability is highly model-dependent.

5.5. Confidence-at-Risk

Applying our CaR framework to the data: for GPT-4o-mini, CaR(5%) is *undefined*—no confidence threshold achieves a 5% error rate. Even at maximum confidence (self-consistency = 1.0), the error rate remains 41.7%. For

Qwen3-32B, the error rate at confidence $\geq 95\%$ is 19.6%, still far exceeding a 5% risk tolerance. These results demonstrate that current LLM confidence signals are fundamentally inadequate for financial risk management purposes.

5.6. Statistical Summary

Table 5 summarizes all hypothesis tests:

Table 5: Statistical Tests for Research Hypotheses

Hypothesis	**Test**	**Statistic**	***p*-value**
H1: Systematic overconfidence	One-sample t-test on confidence gap	$t = 9.70$	$< 0.0001^{***}$
H3: Overconf. error $> 20\%$	Binomial test, $\hat{p} = 0.300$	$z = 3.99$	$< 0.0001^{***}$
H3b: Majority of errors are overconf.	Binomial test, $\hat{p} = 0.664$	$z = 3.53$	0.0002^{***}
H4: Topic-dependent miscalib.	Chi-squared independence test	$\chi^2 = 12.37$	0.030^{*}

$^{***}p < 0.001$; $^{*}p < 0.05$

6. Discussion

6.1. Economic Significance

The finding that 30% of AI responses are high-confidence errors has concrete economic implications. In portfolio management, an overconfident duration estimate can directly impact portfolio value:

$$\Delta V \approx -D_{\text{error}} \times \Delta y \times V \tag{4}$$

If an AI system reports "duration = 4.2 years, confidence = 95%" but the true duration is 6.8 years, a 100-basis-point rate shock on a $10 million portfolio position creates an unexpected loss of approximately $260,000—a 2.6% portfolio-level loss that was "invisible" to the risk model.

More broadly, our Confidence-at-Risk analysis reveals that no confidence threshold can reduce the error rate below 19.6% for the best model (Qwen3-32B) and 41.7% for GPT-4o-mini. In traditional risk management, a VaR

model with 41.7% exceedance rate would be immediately rejected. Our CaR metric formalizes this analogy, providing risk managers with a framework to evaluate AI confidence signals using the same rigor applied to financial risk models.

The overconfidence gap of 22–32 percentage points has implications for information economics. In rational expectations models, information value is proportional to signal precision $\tau = 1/\sigma^2$. A well-calibrated model with ECE = 0.05 provides signal precision $\tau \approx 400$, while our observed ECE values of 0.25–0.32 yield $\tau \approx 10$–16—*40 times less informative* than what users implicitly assume when acting on "85% confident" recommendations.

6.2. CFA Ethics Framework

We map overconfident errors to three CFA Institute Standards of Professional Conduct:

Standard I(C) — Misrepresentation. The CFA Standards prohibit misstatement of performance or analysis. An AI system that expresses 89% average confidence on answers that are wrong 30% of the time systematically misrepresents its analytical reliability. Whether this constitutes misrepresentation depends on whether the firm presents the AI's confidence as a calibrated probability—if so, our evidence suggests such presentation is materially misleading.

Standard V(A) — Diligence and Reasonable Basis. CFA charterholders must have a "reasonable and adequate basis" for investment recommendations. When an AI system expresses high confidence, the natural human response is reduced verification effort. Our finding that 66.4% of errors are high-confidence errors means that relying on AI confidence signals as a proxy for verification fails the "reasonable basis" standard—the very cases where verification is most needed are the ones where the AI most discourages it.

Standard III(C) — Suitability. Our topic-level analysis reveals that Ethics & Standards questions—which directly test professional judgment—exhibit the highest overconfident error rate (43.5%). An AI system confidently recommending actions that violate fiduciary standards undermines the suitability requirement.

6.3. Regulatory Implications and Policy Recommendations

Our findings have direct implications for emerging AI financial regulation:

Table 6: Mapping Findings to Regulatory Frameworks

Framework	Relevant Provision	Our Finding
EU AI Act (2024)	High-risk AI in financial services requires accuracy assessment	ECE > 0.30 fails accuracy transparency
SEC AI Guidance	AI-driven recommendations need "reasonable basis"	30% OC error rate undermines this standard
MAS FEAT Principles	AI must be fair, ethical, accountable, transparent	Miscalibrated confidence violates transparency
CFA Institute	AI should augment, not replace, judgment	Overconfident AI suppresses professional skepticism

We propose a tiered minimum calibration standard for financial AI deployment:

- **Tier 1 (Advisory/Execution)**: ECE < 0.15, overconfident error rate $< 15\%$
- **Tier 2 (Screening/Research)**: ECE < 0.25, overconfident error rate $< 25\%$
- **Tier 3 (Internal tool)**: ECE < 0.35 with mandatory confidence disclaimers

Under this framework, none of the models tested would qualify for Tier 1 or Tier 2 deployment. Qwen3-32B (ECE $= 0.247$) would marginally qualify for Tier 2, while GPT-4o-mini (ECE > 0.30) would be restricted to Tier 3.

6.4. Limitations

Several limitations should be acknowledged. First, our dataset comprises 90 unique CFA questions, yielding 257 observations across model–method combinations. While sufficient for the statistical tests presented, larger-scale validation across the full CFA-Easy corpus (1,032 questions) and multiple additional models would strengthen generalizability. Second, topic classification is based on keyword matching from question text, which may introduce

noise. Third, our CFA question benchmark, while standardized, may not fully represent the range of financial reasoning tasks encountered in practice. Fourth, verbalized confidence may be susceptible to prompt sensitivity; we use a single prompt template and acknowledge that alternative prompts could yield different calibration profiles.

7. Conclusion

This paper demonstrates that Large Language Models exhibit significant calibration failures on financial reasoning tasks. Our key finding is stark: 30% of all AI responses to CFA questions are high-confidence errors—cases where the model is confident but wrong. Among all incorrect answers, two-thirds are delivered with high confidence, meaning that *the error signal is largely invisible* to users who rely on expressed confidence.

We introduce Confidence-at-Risk (CaR), adapting Value-at-Risk methodology to evaluate the reliability of AI confidence signals. Applying CaR reveals that no confidence threshold can reduce the error rate to acceptable levels for financial risk management, even for the best-performing model.

Our analysis connects technical calibration metrics to the CFA Institute's ethical framework, demonstrating that three Standards of Professional Conduct—Misrepresentation, Diligence, and Suitability—are implicated by overconfident AI deployment. We propose tiered minimum calibration standards for financial AI, ranging from ECE < 0.15 for advisory roles to ECE < 0.35 for internal tools.

The question is not whether AI can pass the CFA exam, but whether it knows when it cannot. Our evidence suggests it does not.

Data Availability

The CFA-Challenge dataset is available via HuggingFace under the FinEval benchmark [6]. All experiment code, analysis scripts, and raw results are available at `https://github.com/[anonymized]`.

References

References

[1] Callanan, E., Mbae, A., Selle, S., Gupta, V., & Houlihan, R. (2023). Can GPT-4 pass the CFA exam? *arXiv preprint arXiv:2310.09542*.

[2] Dietvorst, B. J., Simmons, J. P., & Massey, C. (2015). Algorithm aversion: People erroneously avoid algorithms after seeing them err. *Journal of Experimental Psychology: General*, 144(1), 114–126.

[3] Green, B., & Chen, Y. (2019). The principles and limits of algorithm-in-the-loop decision making. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), 1–24.

[4] Guo, C., Pleiss, G., Sun, Y., & Weinberger, K. Q. (2017). On calibration of modern neural networks. In *Proceedings of the 34th International Conference on Machine Learning* (pp. 1321–1330).

[5] Kadavath, S., Conerly, T., Askell, A., et al. (2022). Language models (mostly) know what they know. *arXiv preprint arXiv:2207.05221*.

[6] Ke, Z., Ming, Y., Nguyen, X. P., Xiong, C., & Joty, S. (2025). Demystifying domain-adaptive post-training for financial LLMs. In *Proceedings of the 2025 Conference on Empirical Methods in Natural Language Processing (EMNLP)*.

[7] Lin, S., Hilton, J., & Evans, O. (2022). Teaching models to express their uncertainty in words. *Transactions on Machine Learning Research*.

[8] Nori, H., King, N., McKinney, S. M., Carignan, D., & Horvitz, E. (2023). Capabilities of GPT-4 on medical competence examinations. *arXiv preprint arXiv:2303.13375*.

[9] Wang, X., Wei, J., Schuurmans, D., et al. (2023). Self-consistency improves chain of thought reasoning in language models. In *Proceedings of the 11th International Conference on Learning Representations (ICLR)*.

[10] Wu, S., Irsoy, O., Lu, S., et al. (2023). BloombergGPT: A large language model for finance. *arXiv preprint arXiv:2303.17564*.

[11] Xiong, M., Hu, Z., Lu, X., et al. (2024). Can LLMs express their uncertainty? An empirical evaluation of confidence elicitation in LLMs. In *Proceedings of the 12th International Conference on Learning Representations (ICLR)*.