BLACKRIDGE · PRIVATE INVESTOR RESEARCH

Artificial Intelligence in Quant Trading

A plain-language guide to the different kinds of AI, what each one actually does, and how they are combined inside an investment system.

NO TECHNICAL BACKGROUND REQUIRED | INVESTOR QUESTIONS INCLUDED

PUBLICATION
1 September 2026

EDITION
English

FORMAT
18-page guide

EVIDENCE
17 direct sources

Quant trading means making investment decisions with data, mathematical rules and software. AI can improve parts of that process, but it is not a crystal ball and it is never a substitute for risk control.

01

THE MAIN IDEA

There is no single “best AI”. Different tools solve different problems.

Think of an investment firm as a team. One specialist studies history, another reads documents, another checks causes, and another enforces the risk budget.

Prediction estimates what may happen. Generation turns information into text, code or scenarios. Pattern-finding notices unusual behavior. Cause analysis asks why. Reward learning chooses a sequence of actions. Optimization keeps the final portfolio within rules.

75%	17%	2%	6
of surveyed UK financial firms already used AI BOE / FCA [03]	of reported uses involved general-purpose models trained on enormous datasets, including language models BOE / FCA [03]	were described as fully autonomous BOE / FCA [03]	jobs this guide uses to group AI tools, a simplification rather than an industry standard BLACKRIDGE FRAMEWORK

FOR THE INVESTOR

A credible manager should be able to say which tool performs each job, what can go wrong, and which rule stops the system when it is uncertain.

02

PREDICTION SYSTEMS

Useful when the answer can later be checked: up or down, high or low, likely or unlikely.

These systems learn from labelled examples. A label is simply the outcome we want the model to estimate, such as how strongly prices will fluctuate next month.

01

What it is

A forecasting model studies many past examples and learns which combinations were followed by a particular result.

02

Simple analogy

Like an experienced doctor comparing a new case with thousands of earlier cases, but using numbers rather than intuition.

03

Quant use

Estimate price direction; volatility, meaning how strongly prices fluctuate; default risk, meaning the chance a borrower will not repay; liquidity, meaning how easily an asset can be traded without moving its price; or the chance that an order will be filled.

04

Investor question

Was the model tested on data it had genuinely never seen, after fees and trading costs?

What is XGBoost?

It is a popular method that builds many small decision trees. Each tree asks simple questions, such as “Was volatility high?” The trees correct one another and combine their answers. It is often effective when the data look like a spreadsheet with many different columns. [04]

Why investors should care

Research in asset pricing has found that tree-based models and neural networks — systems made from many simple computing units that learn together — can capture relationships missed by simple straight-line formulas. [05] But this does not guarantee profit: costs, competition and changing market conditions still matter.

03

SEQUENCE SYSTEMS

Useful when the order of events matters, not only the latest number.

A market is a story unfolding through time. Yesterday, this morning and the last five trades may mean something different together than separately.

01	02	03	04	05
Observe	**Remember**	**Compare**	**Forecast**	**Act**
Prices, trades, news and economic releases arrive in sequence.	The model keeps useful information from earlier steps.	It decides which past moments deserve more attention.	It estimates the next step or several future horizons.	The forecast period must match how long the investment will actually be held.

Two terms in plain language

Recurrent network means a model with a working memory: each new observation is processed together with what it retained from earlier observations. A **Transformer** uses “attention” to compare many earlier moments directly and decide which are most relevant. [07]

Where it is used

Order-book changes — changes in the live list of buy and sell orders — volatility, economic releases and forecasts over several horizons. The Temporal Fusion Transformer is a specialized Transformer designed to combine different time-based data and show which moments and features mattered most. [06]

INVESTOR QUESTION

Does the model remember a genuine market pattern, or has it merely memorized dates and noise from the backtest (a test on historical data)?

04

PATTERN-FINDING SYSTEMS

Useful when nobody has labelled the answer and the system must first explore.

These models do not begin with “predict tomorrow’s return”. They look for groups, unusual observations and hidden market states.

A

Grouping

Assets or market days with similar behavior are placed together. The groups help researchers organize a complex market.

B

Anomaly detection

An anomaly is something unusually different: a broken data feed, an abnormal order or a price move that does not fit recent history. Isolation Forest is one method for spotting such cases. [15]

C

Compression

Thousands of related data points are summarized into a smaller set of useful signals.

D

Market regimes

A regime is a broad market condition, such as calm growth or stressed liquidity. A Hidden Markov Model estimates an unobserved state from visible data. [16]

INVESTOR QUESTION

Does the manager treat discovered groups as flexible clues, or as permanent laws with reassuring names?

05

GENERATIVE AI

Useful when new material must be created: a summary, code, explanation or scenario.

Generative AI learns the structure of existing material and produces a new version. A language model predicts the next pieces of text; other generators can create data or market scenarios.

TOOL	PLAIN-LANGUAGE MEANING	QUANT USE	MAIN DANGER
Large language model	A powerful text-completion system trained on enormous collections of language	Read filings, organize news, explain code, search research	Confidently invented facts
GAN	One model creates examples while a second tries to detect fakes; both improve through competition [08]	Create additional scenarios for testing	Repeating only a narrow part of reality
Diffusion model	Starts with noise and gradually shapes it into a plausible example [09]	Generate conditional paths or scenarios of sharp adverse moves	Plausible does not mean probable

THE SAFE ROLE

Generative AI can prepare and explain information. NIST's Generative AI Profile treats invented facts ("confabulation"), information integrity and human oversight as core generative-AI risks. [02] In our view, that means numbers should be calculated by dedicated services, sources should remain visible, and a separate rule should approve any action.

INVESTOR QUESTION

Can every important statement be traced to a source, and can the system refuse to answer when evidence is missing?

06

CAUSE VERSUS COINCIDENCE

Useful when the real question is “what changed because of this?” rather than “what happened next?”

Prices often move together without one causing the other. Causal analysis tries to separate a genuine mechanism from coincidence.

01	02	03	04	05
Question	**Alternative**	**Other causes**	**Evidence**	**Honesty**
What action or event are we studying?	What might have happened without it?	Which outside factors affected both sides?	Is there a natural experiment or comparison group?	Which assumptions cannot be proved? [10]

Quant use

Measure whether a policy decision, fund flow, new trading rule or hedge — a position intended to reduce another risk — actually changed returns, liquidity or costs.

Simple example

Open umbrellas and wet pavement appear together, but umbrellas do not wet the pavement; rain causes both. Markets contain many similar traps.

INVESTOR QUESTION

Does the manager say “caused” when the evidence only shows that two things moved together?

07

LEARNING THROUGH REWARD

Useful when today's action changes tomorrow's choices and success is measured over a sequence.

Reinforcement learning trains an agent by reward and penalty. The agent tries actions, observes the result and gradually develops a policy — a rule for what to do in each situation.

S	A	R	F	P
Situation	**Action**	**Reward**	**Feedback**	**Policy**
What do the market and the portfolio look like now?	Buy, sell, wait, split an order or hedge.	Profit after costs, risk and penalties.	How did the market and portfolio change?	The learned rule for the next action. [11]

Where it can help

Splitting large orders, dynamic hedging — using one position to reduce the risk of another — and adjusting positions while costs and risk change. Deep Hedging applies this idea to hedging with transaction costs and limits. [12]

The simulation trap

The system may become excellent at exploiting mistakes in its training simulator rather than trading the real market. Research with interacting learning agents has also shown that AI traders can learn to collude without communicating. [13]

INVESTOR QUESTION

Was the system first run in observation mode with strict action limits, or was it given capital because the simulation looked impressive?

08

OPTIMIZATION

Useful when the forecasts are ready and the portfolio must obey real-world limits.

Optimization is the portfolio’s rulebook. It chooses the best combination it can find while respecting limits set by the manager.

Inputs	Expected return, risk, relationships between assets, liquidity and costs.	ESTIMATES
Goal	Seek return without taking more risk than the mandate allows.	DECLARED
Limits	Maximum position, sector exposure, leverage, turnover and liquidity.	BINDING
Solver	A calculation method searches for the best permitted combination. [17]	AUDITABLE
Final check	Independent rules confirm prices, data freshness and risk limits.	FAIL SAFE

SIMPLE ANALOGY

A forecast is a shopping wish list. Optimization is the budget, the size of the basket and the rule that prevents one item from filling the entire cart.

INVESTOR QUESTION

Can the manager show which limits constrained the portfolio and what happens if the forecasts are slightly wrong?

09

CHOOSING THE ARCHITECTURE

Begin with the investment question, not with the fashionable model.

A clear task can be written in ordinary language before any technology is selected.

01	02	03	04	05
Decision	**Information**	**Success**	**Limits**	**Feedback**
What exactly must be decided?	What was genuinely known at that moment?	Which result matters after costs and risk?	What is the system never allowed to do?	When will we know whether it worked?

IF THE QUESTION IS…	USE FIRST	EXPECTED ANSWER	SAFE FALLBACK
What may happen?	Prediction	Probability or range	Simple historical baseline
What does this document say?	Generative language AI	Summary with sources	Read the original
Did this event cause the move?	Causal analysis	Effect with assumptions	Say “not proven”
What should we do next?	Reward learning	Bounded action	Fixed rule
How large should positions be?	Optimization	Permitted portfolio	Previous safe portfolio

10

A COMPLETE SYSTEM

Professional firms combine several tools, then separate their powers.

The safest design does not give one all-purpose AI permission to read, predict, size and trade by itself.

01

Research assistant

Reads documents, finds passages and prepares summaries. It cannot approve a trade.

02

Forecasting engine

Turns cleaned data into estimates with uncertainty.

03

Market-state monitor

Looks for unusual conditions and reduces confidence when the environment changes.

04

Portfolio builder

Combines many forecasts while spreading money across different risks and respecting loss limits.

05

Execution system

Turns a desired position into smaller orders and tracks real costs.

06

Independent control

Can block a model, reduce risk or return to a simple fallback.

INVESTOR QUESTION

Which parts are independent, and who has the authority to stop the system?

11

CREATING A SIGNAL

A signal is not a magic instruction. It is a measured clue with an expiry date.

A trading signal is evidence suggesting that an asset may behave differently from what is already reflected in its price.

01 · Collect

Prices, company information, news and other data.

02 · Time-stamp

Record exactly what was known at each past moment.

03 · Clean

Remove errors and define comparable information.

04 · Test

Compare the idea with simple alternatives.

05 · Price

Include fees, the price movement caused by the trade itself, and the maximum amount the strategy can trade without losing quality.

06 · Retire

Stop when the evidence or economics disappear.

Point-in-time data

This means rebuilding the past using only information that was available then. Using a later revision in an earlier test is like answering an exam with the answer sheet.

Overfitting

This happens when a model learns the accidents of the historical sample so precisely that it fails on new data. Publicly known predictors can also weaken after discovery and competition. [14]

INVESTOR QUESTION

How many ideas were tested and rejected before the manager selected the strategy being shown?

12

FROM FORECAST TO TRADE

A forecast, a portfolio and an order are three different decisions.

Many impressive models fail because these decisions are connected poorly.

Forecast	What may happen, over what period, and with what uncertainty?	ESTIMATE
Position	How much can be owned after diversification, liquidity and loss limits?	PORTFOLIO
Order	How should the position be built without paying away the expected advantage?	EXECUTION
Risk control	Which conditions reduce or stop the trade?	INDEPENDENT
Review	Was profit or loss caused by the forecast, sizing or execution?	LEARNING

SIMPLE EXAMPLE

A model may correctly expect a share to rise, yet the strategy can still lose if the position is too large or the order pushes the price against itself.

INVESTOR QUESTION

Does performance attribution separate the idea, position size and trading cost?

13

A DAY IN THE SYSTEM

One event can activate several kinds of AI, each with a narrow role.

Imagine a central-bank decision arriving during a volatile trading day.

Language AI	Prediction	Pattern monitor	Cause check	Optimizer	Execution (reward learning)
Reads the statement and highlights changes from the previous meeting.	Updates expected moves in rates, currencies and volatility.	Recognizes that liquidity is unusually thin.	Separates the policy surprise from unrelated market moves.	Reduces position sizes because uncertainty increased.	Trades gradually and stops if costs exceed the limit.

WHY THE COMBINATION MATTERS

No single component needs to understand the entire market. Each produces a limited output that the next component can verify and constrain.

INVESTOR QUESTION

Can the firm replay this chain and show what each component knew and decided at every moment?

14

INVESTOR DUE DILIGENCE

The most useful questions are about process, not the number of internal adjustable values.

A private investor does not need to reproduce the mathematics. The goal is to test whether the manager understands and controls the system.

01 **Purpose.** What exact decision does each model make, and what does it never decide?

02 **Evidence.** How was the result tested on unseen periods, including fees, impact and failed ideas?

03 **Change.** Which market conditions make the model less reliable?

04 **Limits.** What automatically reduces positions or stops trading?

05 **Responsibility.** Who can override the system, and who independently reviews that decision?

06 **Attribution.** Can the manager separate returns from forecasting, sizing and execution?

A GOOD ANSWER

Specific, measured and clear enough to be proven wrong. “Our proprietary AI finds a hidden edge” is a slogan, not an operating explanation.

15

WARNING SIGNS

Sophisticated language can hide a very ordinary lack of control.

AI adds new tools, but the oldest investment risks remain: weak data, borrowed money, concentration, difficulty selling positions and overconfidence.

01 **No clear job description.** The manager cannot explain what the model decides in one sentence.

02 **Backtest without a graveyard.** Only successful historical tests are shown; rejected models and trials have disappeared.

03 **Autonomy as a selling point.** Full automation is presented as proof of quality, although only 2% of AI use cases at surveyed UK financial firms were fully autonomous in 2024. [03]

04 **Hidden dependence.** One outside provider supplies the model, cloud and data, with no tested alternative. Third-party concentration was a material finding in the Bank of England and Financial Conduct Authority survey. [03]

05 **No failure plan.** The system has no simple fallback, no way to return to a previous safe version and no tested stop condition.

MINIMUM STANDARD

Known owner, documented purpose, visible data sources, independent limits, tested fallback and a clear reason to retire the model. This is BlackRidge's checklist; NIST's AI Risk Management Framework likewise treats documented roles and responsibilities and safe decommissioning as lifecycle governance tasks. [01]

16

SELECTED SOURCES

Evidence should remain easy to verify.

The technical papers are included for verification. The main text explains their relevance in plain language.

01 · NIST

AI Risk Management Framework 1.0

Cross-sector lifecycle and trustworthy-system framework.

02 · NIST

Generative AI Profile, NIST AI 600-1

Generative-AI-specific risks and suggested actions.

03 · BANK OF ENGLAND / FCA

Artificial intelligence in UK financial services 2024

Financial-sector adoption, autonomy and concentration survey.

04 · CHEN & GUESTRIN

XGBoost: A Scalable Tree Boosting System

Tree boosting for sparse structured data.

05 · GU, KELLY & XIU

Empirical Asset Pricing via Machine Learning

Nonlinear ML for cross-sectional risk-premium prediction.

06 · LIM ET AL.

Temporal Fusion Transformers for Interpretable Multi-horizon Time Series Forecasting

Mixed-covariate, multi-horizon sequence forecasting.

07 · VASWANI ET AL.

Attention Is All You Need

Transformer attention architecture.

08 · GOODFELLOW ET AL.

Generative Adversarial Networks

Adversarial generative modelling.

09 · HO, JAIN & ABBEEL

Denoising Diffusion Probabilistic Models

Diffusion-based generative modelling.

17

SELECTED SOURCES

Good technology should be possible to explain.

10 · YAO ET AL.
A Survey on Causal Inference
Potential-outcome causal inference and assumptions.

11 · SUTTON & BARTO
Reinforcement Learning: An Introduction
State, action, reward and policy formalism.

12 · BÜHLER ET AL.
Deep Hedging
Hedging with frictions and constraints.

13 · DOU, GOLDSTEIN & JI
AI-Powered Trading, Algorithmic Collusion, and Price Efficiency
Simulated RL traders sustain tacit collusion without communication.

14 · MCLEAN & PONTIFF
Does Academic Research Destroy Stock Return Predictability?
Post-publication return-predictor decay.

15 · LIU, TING & ZHOU
Isolation Forest
Unsupervised anomaly detection by isolation.

16 · RABINER
A Tutorial on Hidden Markov Models
Latent-state sequence modelling.

17 · BOYD & VANDENBERGHE
Convex Optimization
Constrained optimization foundations.

The strongest AI investment system is not the one with the most impressive vocabulary. It is the one whose decisions, limits and mistakes can be explained clearly.

UNDERSTAND THE JOB | TEST THE EVIDENCE | DEMAND A SAFETY NET

This publication is for research and educational purposes only. It is not investment advice, an offer, a solicitation, or a recommendation to transact in any security or strategy. Examples explain system design and do not represent live performance. Markets, data and model behavior can change materially.

ABOUT BLACKRIDGE

Independent research, introductions clearly defined.

BlackRidge is an independent research bureau introducing private investors to quantitative traders through multiple strategy providers. We publish quantitative research. Investors access strategies through PAMM accounts at the broker. We are not a fund or broker and never hold client money.

01 **Your funds stay at the broker.** The account is opened in your own name. BlackRidge never receives, holds, or has withdrawal rights over client capital.

02 **No fee on your profits.** A one-time access payment of 6.7% of the agreed trading level, paid to the selected strategy provider. No management fee, no performance fee, no profit share, in any year.

03 **You fund the risk, not the exposure.** Allocations are notionally funded: you agree a trading level and fund the margin and drawdown allowance behind it. Trading losses can exceed the deposit without applicable negative balance protection; the separate 6.7% access payment is nonrefundable.

CONTINUE READING

blckridge.com/research: published research. Notional funding and PAMM accounts explained in full, and answers to the questions this raises.

We use AI models to gather and aggregate source material and to help prepare each report. Read it with its cited sources, sample, methods and limitations, and send corrections through research methodology and corrections.

The client pays the selected strategy provider a one-time access payment of 6.7% of the agreed trading level. BlackRidge receives an introduction fee from that provider and does not receive broker compensation. About BlackRidge.

Minimum funded capital $25,000. Strategy authorship, live records, the broker, the selected strategy provider and the full commercial terms are presented on an introductory call and confirmed in writing before any payment or deposit.

This report is published for information only. It is not investment advice and does not take account of your circumstances. Trading leveraged instruments including CFDs carries substantial risk and is not suitable for all investors; you may lose the capital you fund and, depending on your broker's terms, may owe more than your deposit. Findings in this report may combine third-party evidence, historical calculations and illustrative scenarios; they are not verified live trading results of any strategy provider. Past performance does not indicate future results.