📈 Autonomous Probabilistic Trading Agent (AI Trader)

Probabilistic Autonomous Trading Agent

Project Title	Autonomous Probabilistic Trading Agent (AI Trader)
Prepared For	Owner (Self-Deployment with Seed Capital)
Version	1.0 (Based on Current Architecture Review)
Date	October 30, 2025

---

1. Executive Summary and Project Goals

The objective of this project is to evolve the existing modular trading framework into a **Probabilistic Multi-Agent Collective** capable of achieving sustainable financial growth. The system will leverage specialized AI agents and advanced statistical filters to navigate the complex, non-stationary market environment.

Primary Project Goals	**Architectural Mandate**
Financial Goal: Grow **$500 seed capital** to generate **$50/week net passive profit** with continued capital growth [Conversation History].	Implement a **Hybrid Reactive-Deliberative Architecture**.
Risk Goal: Ensure robust defense of seed capital by explicitly quantifying and managing uncertainty.	Implement the **RiskManagementAgent** using the **Fractional Kelly Criterion** and **uncertainty propagation** via the Kalman filter's *P* matrix.
Technical Goal: Transition from basic indicators to **adaptive, probabilistic reasoning**.	Formalize the **Data Abstraction Layer (DAL)** and integrate the **Probabilistic Core** (Kalman Filter, HMMs).
Interface Goal: Develop a **mobile-friendly Web Application** for observability and structured input [Conversation History].	Leverage existing **FastAPI orchestration** and **Streamlit** for front-end development [Conversation History].

---

2. Project Scope and Organization

2.1 Project Architecture (Modular Agent Collective)

The system is defined as a **multi-agent collective**, where specialized agents communicate via a message bus or orchestration layer. The agents are:

- **SignalFilteringAgent:** Applies filters (e.g., **Kalman Filter**, Butterworth) to generate cleaned signals and probabilistic estimates, including the **error covariance matrix (*P*)**.
- **RegimeAnalysisAgent:** Employs **Hidden Markov Models (HMMs)** or GARCH models to classify the market regime (e.g., Low-Vol vs. High-Vol).
- **StrategySelectionAgent (Reasoning Agent):** The central decision-maker, potentially powered by **LangChain/LangGraph**. It dynamically selects, parameterizes, and deploys strategies ("tools") based on signals and regimes.
- **RiskManagementAgent: CRITICAL** for the $500 seed capital. It ingests *P* and portfolio updates, uses the **Kelly Criterion** for optimal sizing, and can **veto or modify** proposed trades.
- **ExecutionAgent:** Responsible for API interaction and handling the order lifecycle; operates on a highly **reactive** timescale.

2.2 In-Scope Activities (Deliverables)

Area	Deliverables to be Produced
Data & Resilience	Formalized **Data Abstraction Layer (DAL)**; Integration of **Marketstack** and **Tiingo** APIs.
Probabilistic Core	Implementation of **Kalman Filter** and **HMM** logic; Propagation of **Uncertainty Matrix (*P*)**.
Orchestration & Control	**LangGraph** model defining the agent workflow; Risk module updated to use **Fractional Kelly Criterion**.
Validation	Implementation of **Purged and Embargoed K-Fold Cross-Validation**; Successful **Paper Trading** validation [Conversation History].
Interface	Functional **Telegram** notification interface; Initial build of **Streamlit** mobile-friendly **Web**

	App [Conversation History].

2.3 Out-of-Scope Activities (Anti-Patterns and Exclusions)

Area	Exclusion / Rationale	Source Support
Data Sourcing	**Exclusion of Finviz**. Web scraping is **inherently unreliable** and an anti-pattern for production systems.	
Filtering	**Exclusion of Hodrick-Prescott (HP) Filter**. The standard two-sided filter is **non-causal** and causes the "repainting" anti-pattern, making it unsuitable for real-time signal generation.	
Backtesting	**Exclusion of Vectorized Backtesting** for agent validation. The system requires an **Event-Driven Architecture** for realism and fidelity.	

---

3. Work Breakdown Structure (WBS) and Schedule

The plan follows the P0-P4 priority levels defined in the project status, grouping related technical activities into four main phases.

Phase 1: Foundational Hardening & Data Resilience (P0)

Objective: Secure data feeds and eliminate architectural vulnerabilities.

ID	Task	Effort (Est.)	Dependency
1.1	**Formalize Data Abstraction Layer (DAL)**	High	None

1.2	**Implement Cost-Optimized Hybrid Data Stack** (Marketstack/Tiingo adapters)	Medium	1.1
1.3	**REMOVE** Finviz and update `app/sources/` (Eliminate scraping)	Low	None
1.4	Finalize **P0 Filter Implementation** (Volatility, Range, Butterworth)	Medium	None
1.5	Configure **Telegram** for event notifications (Auditing interface)	Low	1.4

Phase 2: Probabilistic Core Integration (P1)

Objective: Implement the mathematical foundation for adaptive, risk-aware reasoning.

ID	Task	Effort (Est.)	Dependency
2.1	Implement **Kalman Filter** logic (Outputting state *x^* and **uncertainty** *P*)	High	Python 3.11+
2.2	Implement **HMM/GARCH** for Regime Analysis	High	2.1
2.3	Refactor **SignalFilteringAgent** to publish *P*	Medium	2.1
2.4	Develop probabilistic strategies ("tools")	Medium	2.2

Phase 3: Orchestration & Risk Control (P2/P3)

Objective: Integrate specialized agents and finalize the protective risk framework.

ID	Task	Effort (Est.)	Dependency
3.1	Upgrade **RiskManagementAgent** to ingest *P* and use **Fractional Kelly Criterion**	High	2.3, 3.2
3.2	Implement **StrategySelectionAgent** using **LangChain/LangGraph**	High	2.4
3.3	Model Agent Workflow Graph (`app/wiring/`)	Medium	3.2
3.4	Implement **Time Series Cross-Validation** (Purged & Embargoed CV) (P2)	High	4.1
3.5	Begin **Streamlit Web App** development (Visualization of *P*, Grafana embedding)	Medium	1.5, Grafana

Phase 4: Final Validation and Scaling (P4)

Objective: Confirm real-world performance, meet regulatory readiness, and deploy live.

ID	Task Description	Effort (Est.)	Dependency
4.1	**Advanced Backtesting** and	High	3.4

	Analytics Extension (Fidelity modeling)		
4.2	**Paper Trading Validation** via Alpaca	Medium	3.1, 3.3
4.3	Final **Docker Hardening** and CI/CD Review (P4)	Low	GitHub/Azure
4.4	**LIVE DEPLOYMENT** to Azure App Service	Low	4.2 (Success Criteria Met)

---

4. Resource Plan

Category	Component	Status	Rationale / Strategic Use
Orchestration / Reasoning	**LangChain/LangGraph, FastAPI**	KEEP	LangGraph defines the **stateful, cyclical agent workflow**. FastAPI is the confirmed orchestration layer.
Probabilistic Modeling	**PyMC, pgmpy, Kalman/HMM Logic**	ADD	Essential for **Bayesian filtering** and modeling complex dependencies with **Probabilistic Graphical Models (PGMs)**.
Execution	**Alpaca**	KEEP	Brokerage API for the **ExecutionAgent**.
Observability	**Grafana, Sentry**	KEEP	**Mandatory** for auditing the complex multi-agent system and ensuring

			decisions are **auditable and debuggable**.
Historical Data (Cold)	**Marketstack**	ADD	**Cost-effective** ($9.99/mo) source for deep **EOD coverage** for historical backtesting.
AI Signal Data (Hot)	**Tiingo**	ADD	Provides **proprietary NLP-tagged News API** and real-time IEX data, crucial for generating AI context signals.
User Interface	**Streamlit** (Web App), **Telegram**	KEEP/GROW	Streamlit provides the foundation for the long-term, **mobile-friendly Web App** interface for **deliberative input** [Conversation History].

---

5. Risk Management Plan

The following table identifies the primary high-impact risks specific to AI trading and outlines the mitigation strategies required by the sources.

Risk ID	Risk Description	Impact	Probability	Mitigation Strategy	Source Support
R-1	**Overfitting** due to Lookahead Bias or Data Snooping.	High (Fatal to goal)	High	Use **Time Series Cross-Validation** and implement	

				Purged and Embargoed K-Fold CV. Backtesting should be treated as validation, not research.	
R-2	**Catastrophic Loss of Seed Capital** due to single large trade.	High (Ends project)	Medium	**RiskManagementAgent** must use **Fractional Kelly Criterion** for optimal sizing, combined with **uncertainty propagation** (*P*) to dynamically reduce exposure during volatility.	
R-3	**Data Vendor Failure** (e.g., IEX Cloud Shutdown).	High (Forced migration)	Medium	**Build a Data Abstraction Layer (DAL)**. Avoid unstable models and brittle anti-patterns like **Finviz web scraping**.	

R-4	**Repainting Signal** from Non-Causal Filter.	High (Deceptive profitability)	Low	**Strictly enforce causal filtering logic**. Explicitly reject non-causal filters like the standard two-sided **Hodrick-Prescott (HP) Filter**.	
R-5	**Unrealistic Backtest Friction Modeling** (Slippage/Commissions).	Medium (Failure to achieve net profit goal)	High	Must use **Event-Driven Backtesting** and model realistic market costs, including **slippage** and **liquidity constraints** (capping order size relative to volume).	