Agentic AI Class Task (2 Hours)

Task Title

Build a Crypto Agent using Knowledge Base + FreeCryptoAPI

Core Idea (Very Important)

The agent **must NOT answer directly from the LLM**.

It can answer **only** if:

1. The answer exists in the **Knowledge Base**, OR
2. The answer is fetched via **FreeCryptoAPI**, OR
3. The answer can be derived from the **KB + API result**

Otherwise → **reject**.

Data Layers (Mandatory)

1. Knowledge Base (Primary Source)

Students must create a **local Knowledge Base** containing:

- Crypto coin metadata
- Static facts (symbol, launch year, consensus, chain type)
- Cached API responses (prices, market cap, timestamps)

Allowed formats

- JSON files
- SQLite
- CSV (not recommended but allowed)

Example KB Record

```
{
  "coin": "Bitcoin",
```

```
  "symbol": "BTC",
  "launch_year": 2009,
  "consensus": "Proof of Work",
  "last_price": 43210.55,
  "price_timestamp": "2026-01-06T10:15:00Z"
}
```

---

2. Live Tool (Secondary Source)

FreeCryptoAPI
https://freecryptoapi.com/

Used **only when**:

- Data is missing in KB
- Data is stale (older than X minutes)

Functional Requirements

1. Context Awareness

- Track last **8–10 turns**
- Resolve follow-ups using context

Example:

```
User: Tell me about Ethereum
User: What is its consensus?
```

→ Use KB entity resolution

---

2. Memory Design (Required)

Type	Purpose
Short-term	Conversation history

Long-term   Knowledge Base (facts + cached API
              data)

---

3. Knowledge-First Logic (Mandatory)

```
User Query
↓
Entity & intent detection
↓
Search Knowledge Base
↓
Is data sufficient & fresh?
↓          ↓
Yes        No
↓          ↓
Answer     Call FreeCryptoAPI
↓          ↓
           Update KB
↓
Return response with source
```

---

4. Hallucination Prevention (Hard Rules)

Students must implement **ALL**:

1. **KB-First Policy**
   - In fact, not in KB and not returned by API → reject
   - **Explicit Rejection Response**
     `INSUFFICIENT DATA — Not found in Knowledge Base or API`
2. **Source Tag**
   Every response must include:
   `Source: Knowledge Base | FreeCryptoAPI`
3. **Confidence Score**
   Return value between `0.0 and 1.0`

---

5. Allowed & Disallowed Queries

Allowed

- Price, market cap (via API)
- Coin metadata (via KB)
- Follow-ups using context

Disallowed (Must Reject)

- Price prediction
- Investment advice
- Hypothetical questions
- Data not in KB or API