# BUS5001 – Cloud Platforms and Analytics

## Week 12 – The End of a Journey

Centre for Data Analytics and Cognition
La Trobe University, Australia

# It was a pleasure

"Learning is the only thing the mind never exhausts, never fears, and never regrets."

- It has been a pleasure being your guides on this journey through Cloud Platforms and Analytics
- You have been an engaged and enthusiastic class and we thank you for your patience, diligence and cooperation
- Cloud platforms have democratised to a great extent technology and analytics however there is an element of technical knowledge and application that is required and we hope we have exposed you to that in this class
- Cloud platforms also make up a broad topic and this course has focused on giving you a foundation to continue your exploration and adoption of these platforms in your work
- Focus on extending your knowledge
- Important to be hands on and you keep up to date
- Find people that you can follow on social media or blogs that you can follow to keep you up to date

# A Non-Exhaustive Recap

- Core concepts of cloud computing, its advantages, and various deployment models
- IaaS, SaaS, PaaS
- What enables the cloud and a look behind the scenes
- Virtualisation / Containerisation
- How to navigate major cloud platforms such (Azure and GCP) and key services
- Cloud adoption and governance
- Devops / DevSecOps / AIOps / MLOps / Version Control
  - Kubernetes / Git / Github  / Github Actions
- Cloud boundaries / security / threats

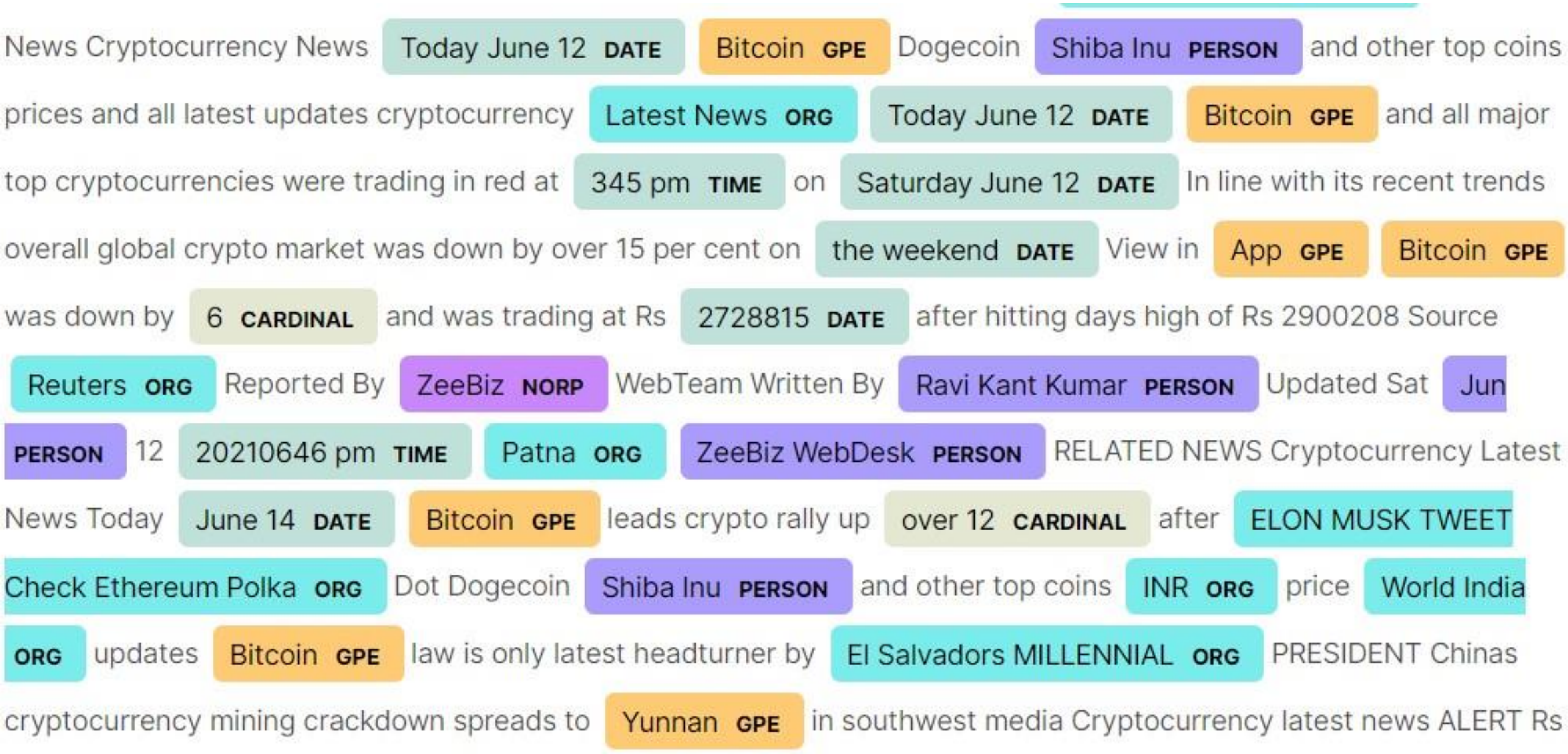
# A Non-Exhaustive Recap

- Code in the Cloud
  - Google Colab
- Serverless
  - Google Cloud Functions
- The spectrum of data storage to Big Data and Streaming Data use cases
  - Azure Blob Storage / Data Factory / Cosmos DB / Google Big Table / Big Query / Dataflow / Looker
- Databases to Date Lakes
  - Azure SQL / Databricks

# A Non-Exhaustive Recap

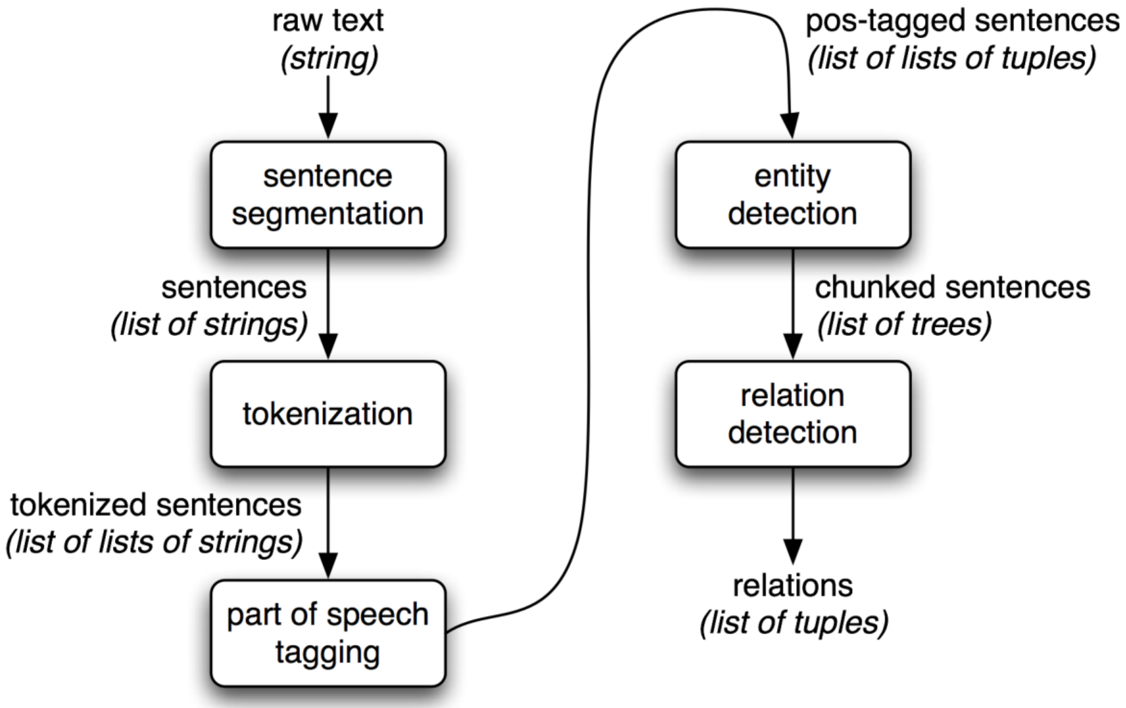
- Robotic Process Automation
  - Logic Apps / Conversational Agents / Google Dialogflow
- AI in the Cloud
  - Azure Cognitive Services / Hugging Face / Google Colab / OpenAI
- Data Ethics

# Language Semantics



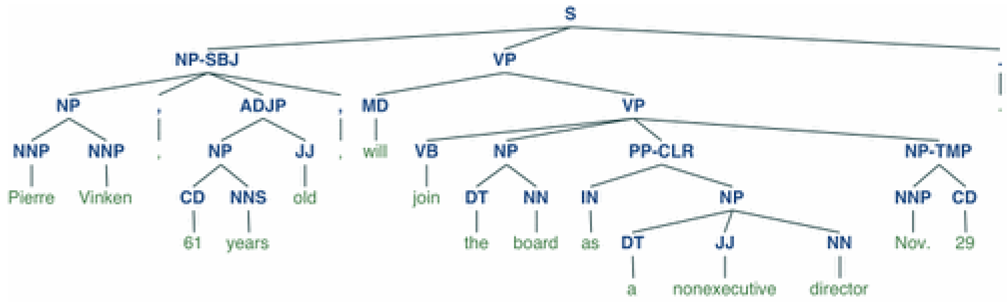
News Cryptocurrency News Today June 12 DATE Bitcoin GPE Dogecoin Shiba Inu PERSON and other top coins prices and all latest updates cryptocurrency Latest News ORG Today June 12 DATE Bitcoin GPE and all major top cryptocurrencies were trading in red at 345 pm TIME on Saturday June 12 DATE In line with its recent trends overall global crypto market was down by over 15 per cent on the weekend DATE View in App GPE Bitcoin GPE was down by 6 CARDINAL and was trading at Rs 2728815 DATE after hitting days high of Rs 2900208 Source Reuters ORG Reported By ZeeBiz NORP WebTeam Written By Ravi Kant Kumar PERSON Updated Sat Jun PERSON 12 20210646 pm TIME Patna ORG ZeeBiz WebDesk PERSON RELATED NEWS Cryptocurrency Latest News Today June 14 DATE Bitcoin GPE leads crypto rally up over 12 CARDINAL after ELON MUSK TWEET Check Ethereum Polka ORG Dot Dogecoin Shiba Inu PERSON and other top coins INR ORG price World India ORG updates Bitcoin GPE law is only latest headturner by El Salvadors MILLENNIAL ORG PRESIDENT Chinas cryptocurrency mining crackdown spreads to Yunnan GPE in southwest media Cryptocurrency latest news ALERT Rs

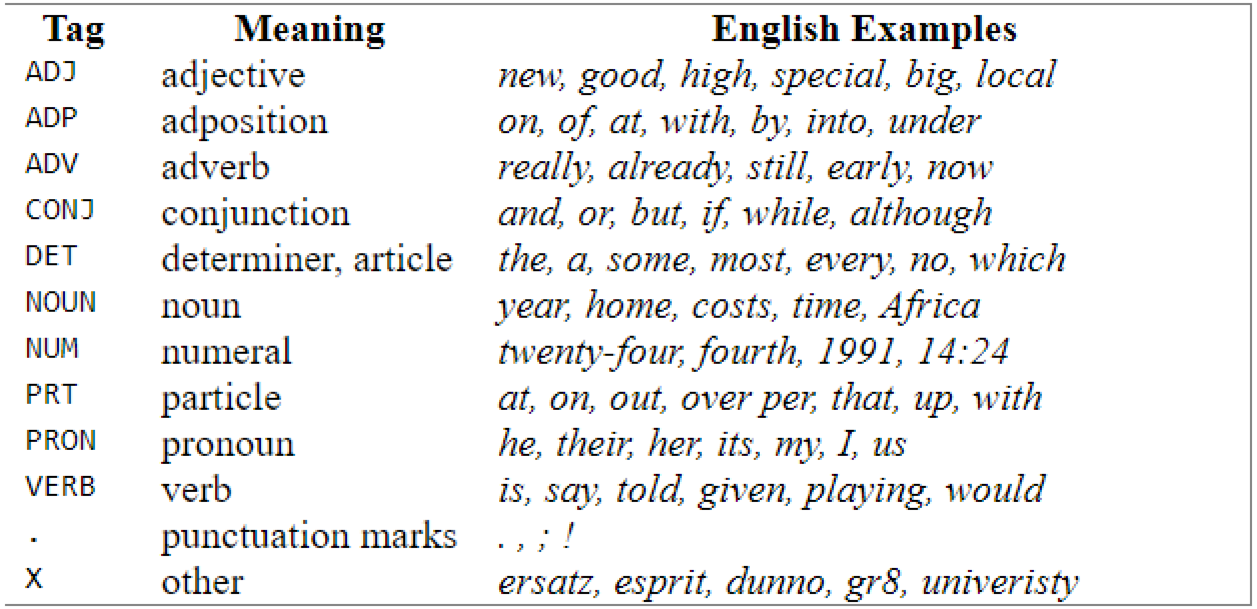
# The Process


raw text
(string)
sentence segmentation
sentences
(list of strings)
tokenization
tokenized sentences
(list of lists of strings)
part of speech tagging
pos-tagged sentences
(list of lists of tuples)
entity detection
chunked sentences
(list of trees)
relation detection
relations
(list of tuples)

# Language Parsing

"Pierre Vinken, 61 years old, will join the board as a nonexecutive director Nov. 29."





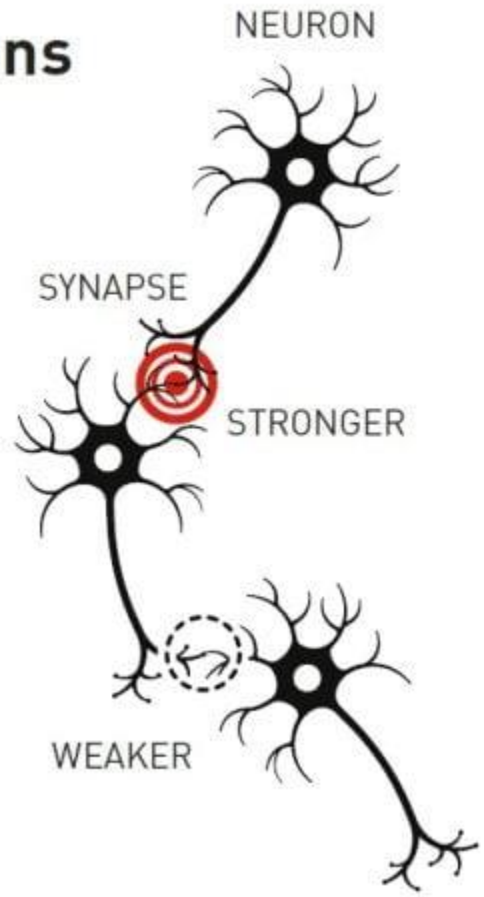
| Tag | Meaning | English Examples |
|---|---|---|
| ADJ | adjective | *new, good, high, special, big, local* |
| ADP | adposition | *on, of, at, with, by, into, under* |
| ADV | adverb | *really, already, still, early, now* |
| CONJ | conjunction | *and, or, but, if, while, although* |
| DET | determiner, article | *the, a, some, most, every, no, which* |
| NOUN | noun | *year, home, costs, time, Africa* |
| NUM | numeral | *twenty-four, fourth, 1991, 14:24* |
| PRT | particle | *at, on, out, over per, that, up, with* |
| PRON | pronoun | *he, their, her, its, my, I, us* |
| VERB | verb | *is, say, told, given, playing, would* |
| . | punctuation marks | *. , ; !* |
| X | other | *ersatz, esprit, dunno, gr8, univeristy* |

# Parts of Speech Tagging

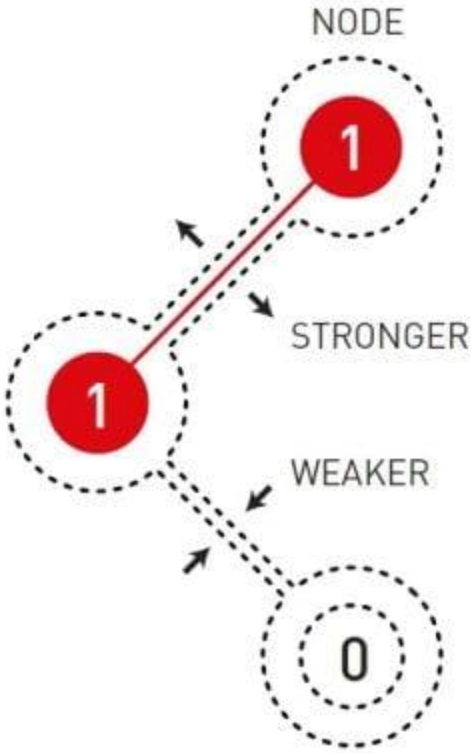
- The tree starts with the sentence as a whole and breaks it down into its constituents (subject, verb, object, etc.)
- Within the constituents, it breaks down further into phrases (noun phrases, verb phrases, etc.) and finally into individual words with their corresponding syntactic roles (e.g., nouns, verbs, prepositions).

# Natural and artificial neurons

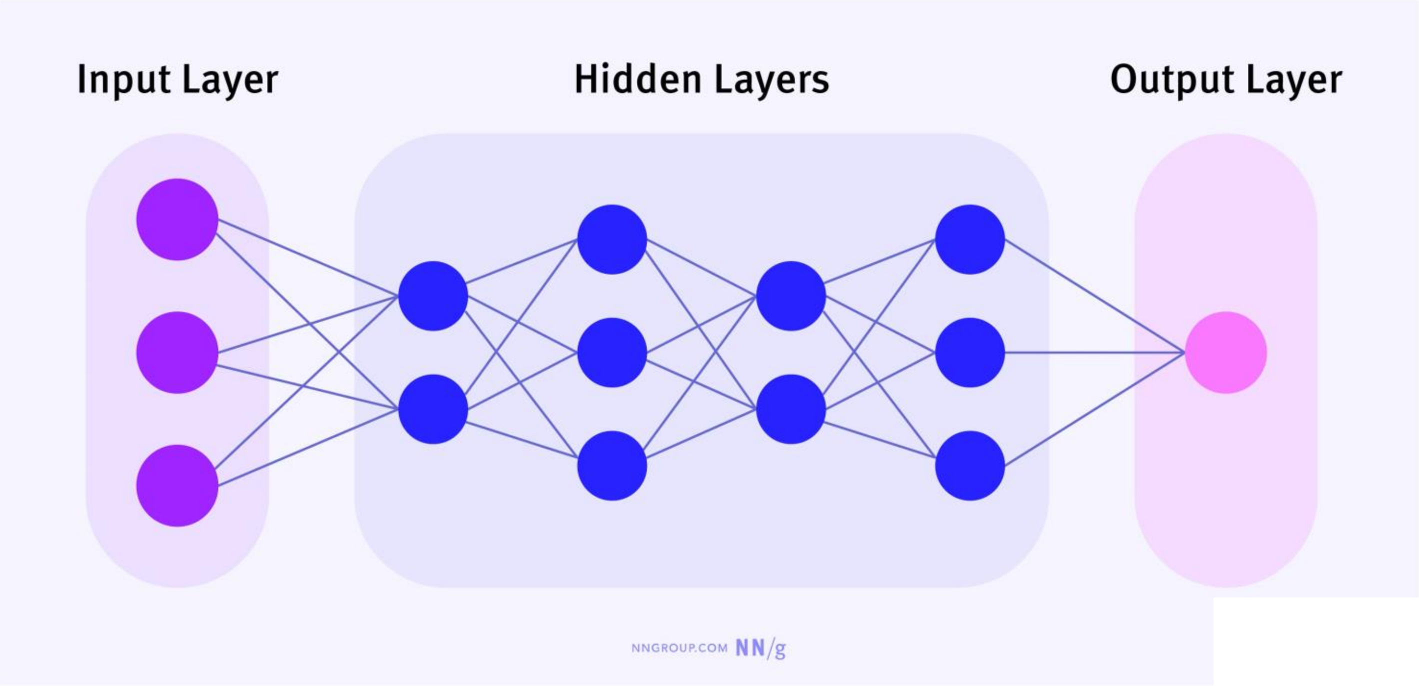
The brain's neural network is built from living cells, neurons, with advanced internal machinery. They can send signals to each other through the synapses. When we learn things, the connections between some neurons get stronger, while others get weaker.



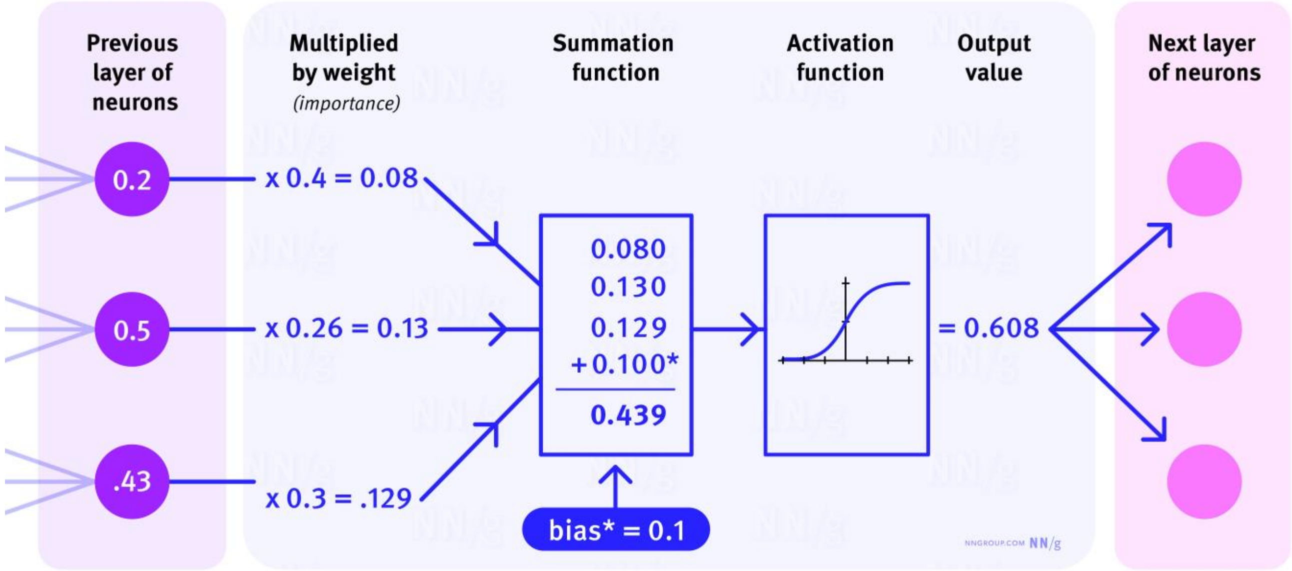
Artificial neural networks are built from nodes that are coded with a value. The nodes are connected to each other and, when the network is trained, the connections between nodes that are active at the same time get stronger, otherwise they get weaker.



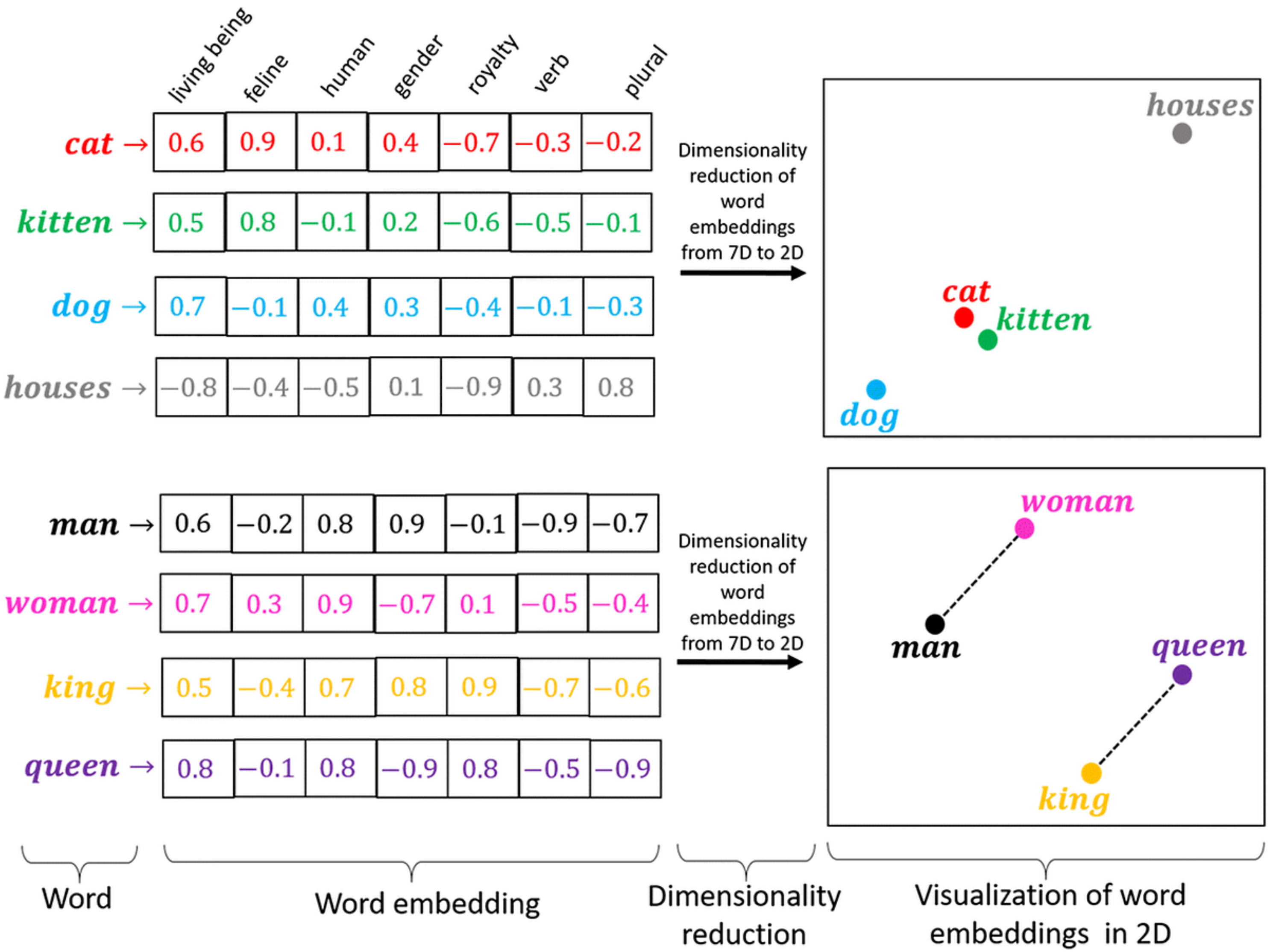
# Neural Network Diagram



# How a Single Artificial Neuron Works



# Word Embeddings

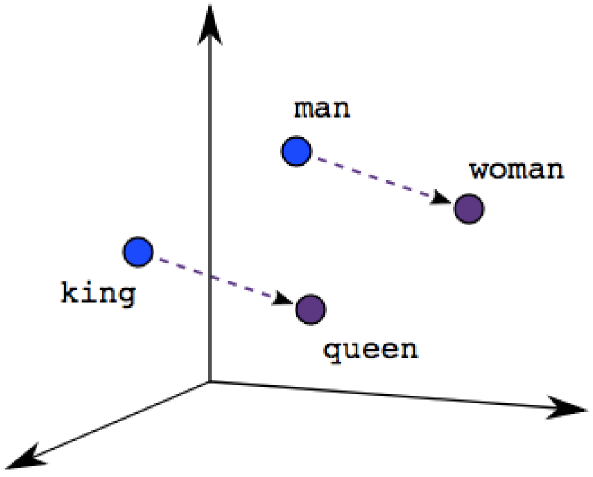


| | living being | feline | human | gender | royalty | verb | plural |
|---|---|---|---|---|---|---|---|
| *cat* → | 0.6 | 0.9 | 0.1 | 0.4 | −0.7 | −0.3 | −0.2 |
| *kitten* → | 0.5 | 0.8 | −0.1 | 0.2 | −0.6 | −0.5 | −0.1 |
| *dog* → | 0.7 | −0.1 | 0.4 | 0.3 | −0.4 | −0.1 | −0.3 |
| *houses* → | −0.8 | −0.4 | −0.5 | 0.1 | −0.9 | 0.3 | 0.8 |

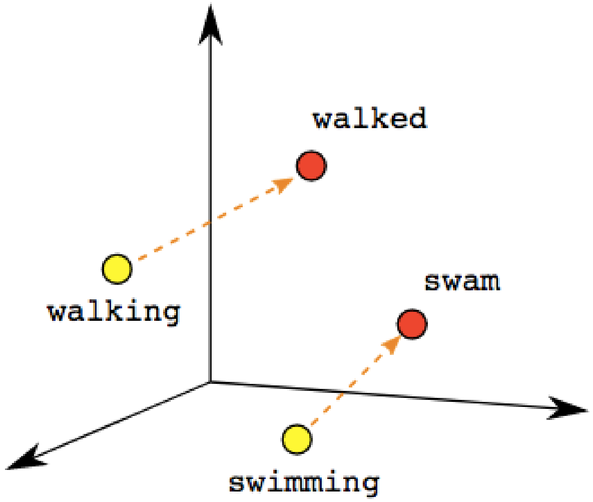
| | | | | | | | |
|---|---|---|---|---|---|---|---|
| *man* → | 0.6 | −0.2 | 0.8 | 0.9 | −0.1 | −0.9 | −0.7 |
| *woman* → | 0.7 | 0.3 | 0.9 | −0.7 | 0.1 | −0.5 | −0.4 |
| *king* → | 0.5 | −0.4 | 0.7 | 0.8 | 0.9 | −0.7 | −0.6 |
| *queen* → | 0.8 | −0.1 | 0.8 | −0.9 | 0.8 | −0.5 | −0.9 |

Dimensionality reduction of word embeddings from 7D to 2D
houses
cat
kitten
dog
Dimensionality reduction of word embeddings from 7D to 2D
woman
man
queen
king
Word
Word embedding
Dimensionality reduction
Visualization of word embeddings in 2D

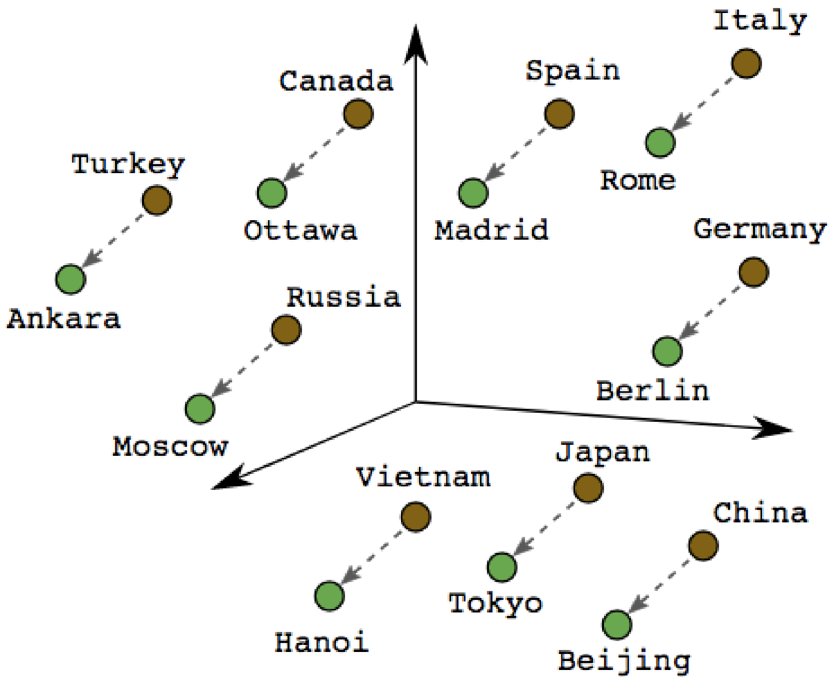
# Similarities



Male-Female

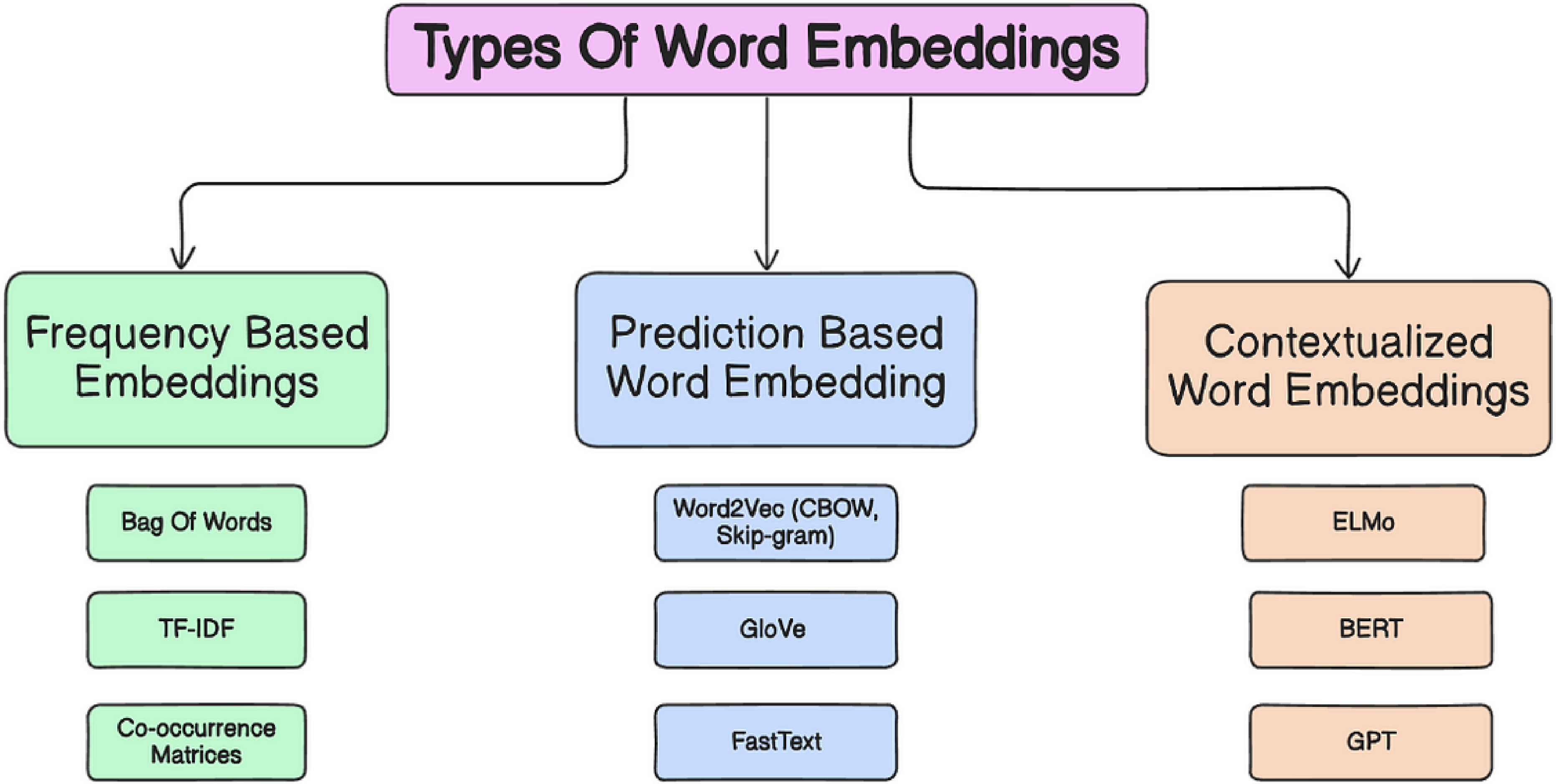


Verb Tense

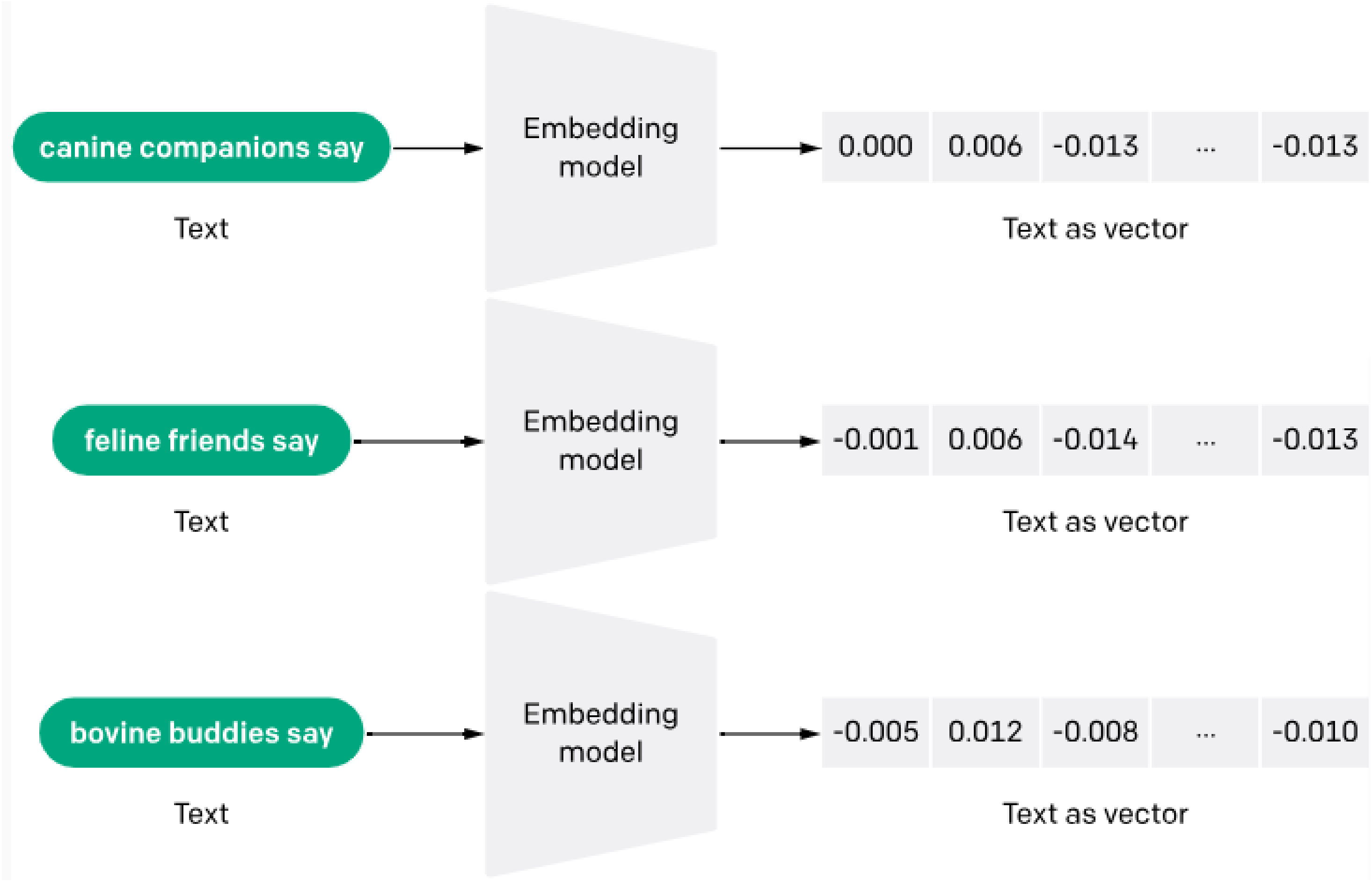


Country-Capital

# Types of Word Embeddings


Types Of Word Embeddings
Frequency Based Embeddings
Prediction Based Word Embedding
Contextualized Word Embeddings
Bag Of Words
TF-IDF
Co-occurrence Matrices
Word2Vec (CBOW, Skip-gram)
GloVe
FastText
ELMo
BERT
GPT

# Creating and Embedding



canine companions say → Embedding model → 0.000 | 0.006 | -0.013 | ... | -0.013

Text — Text as vector

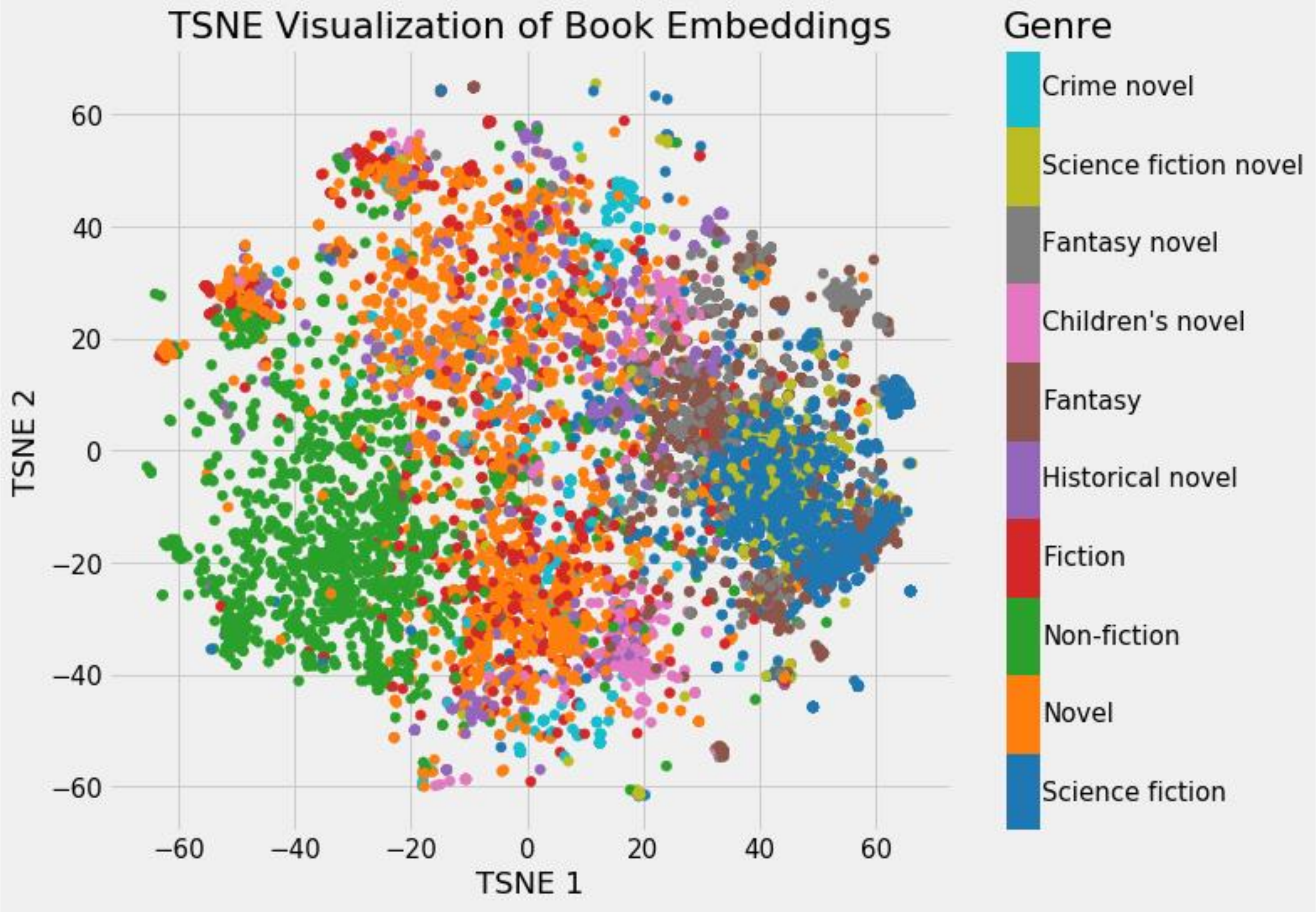
feline friends say → Embedding model → -0.001 | 0.006 | -0.014 | ... | -0.013

Text — Text as vector

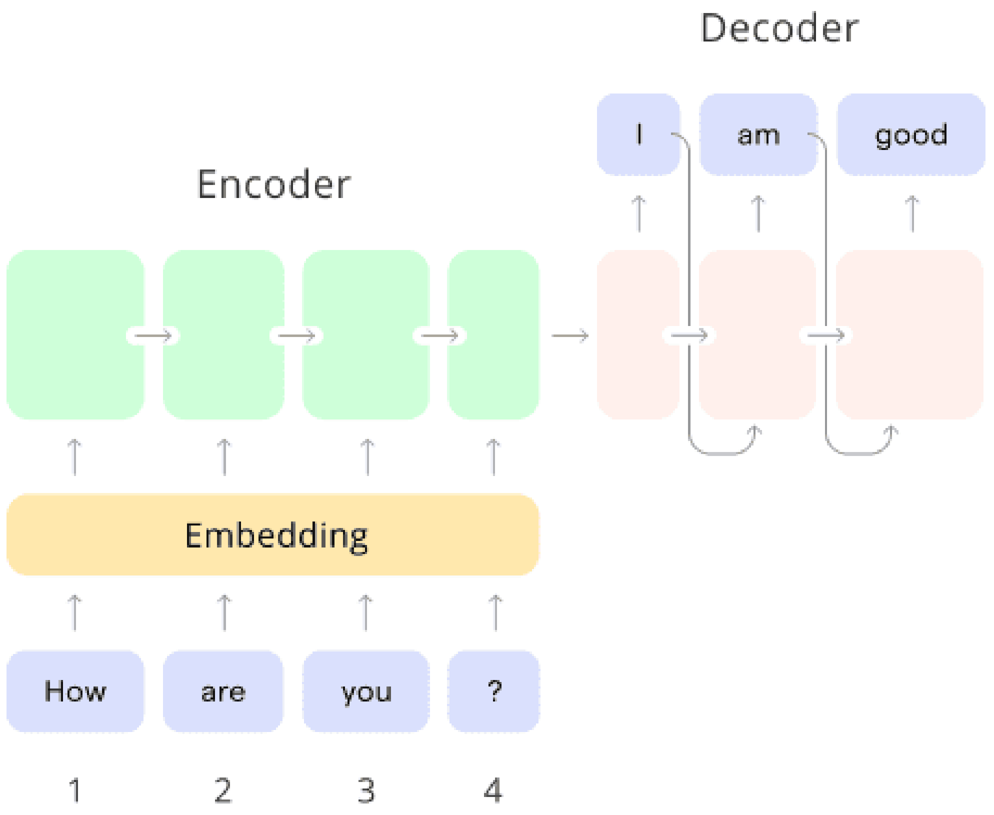
bovine buddies say → Embedding model → -0.005 | 0.012 | -0.008 | ... | -0.010

Text — Text as vector

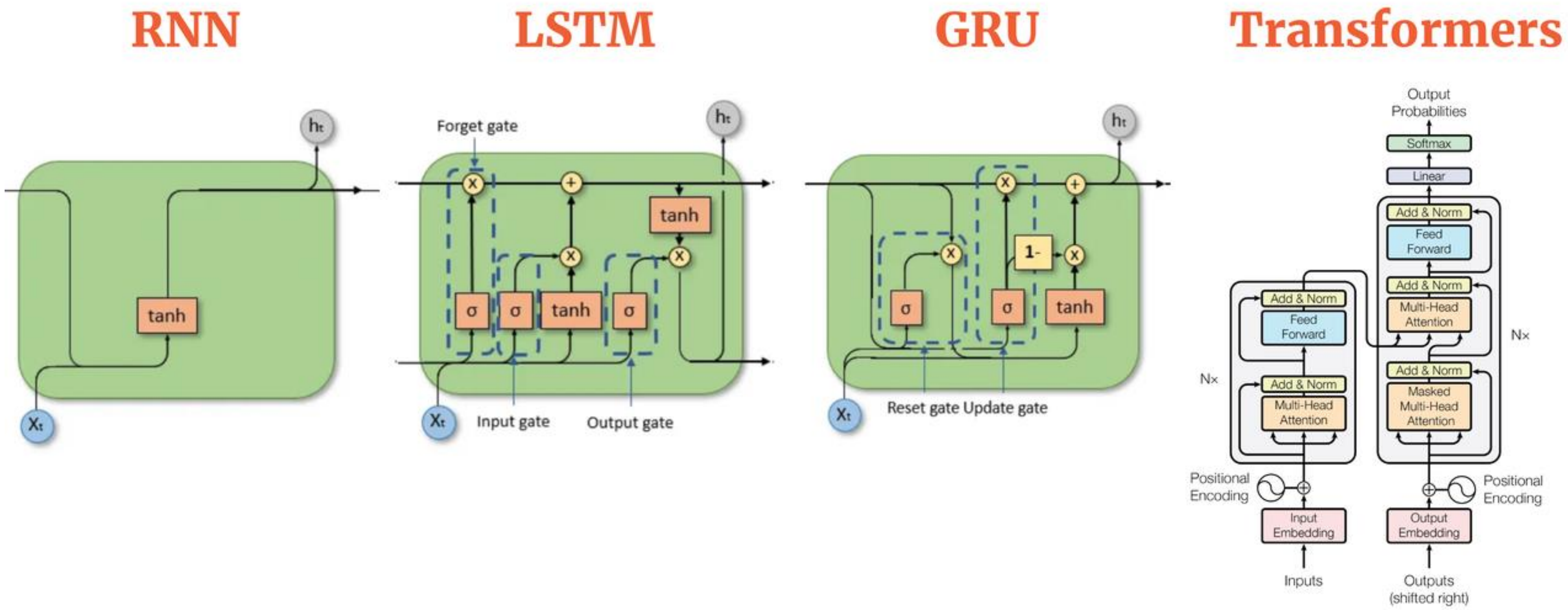
# Language Representation



# Sequence Modeling

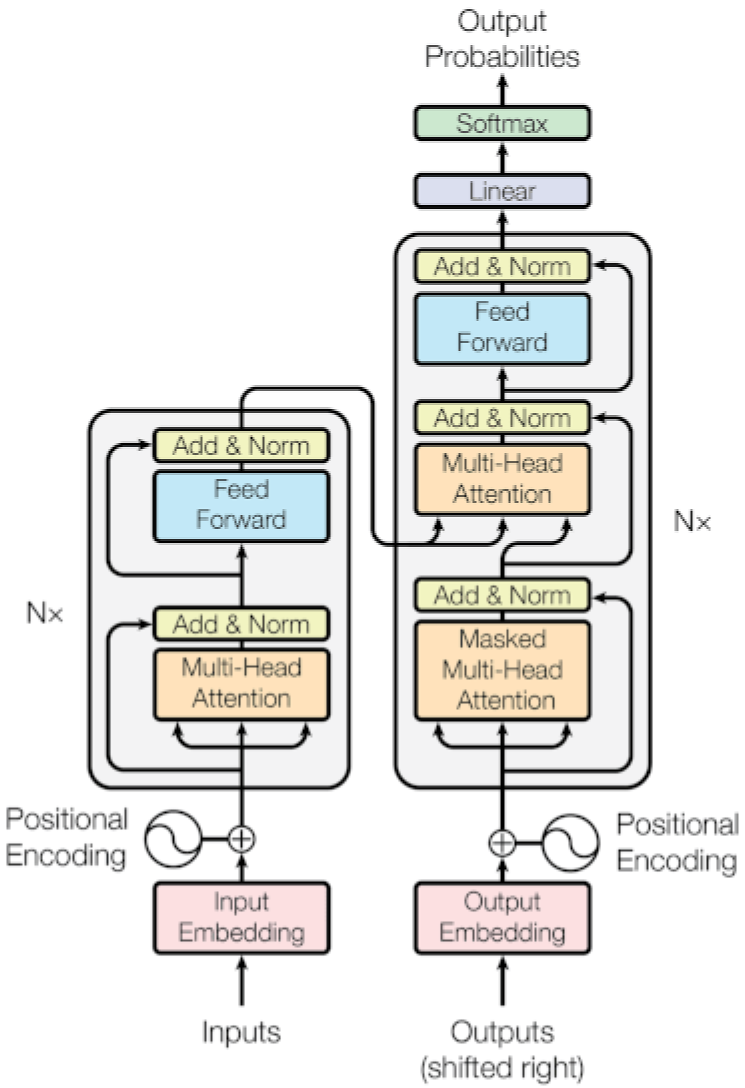


# RNN – LSTM – Transformers

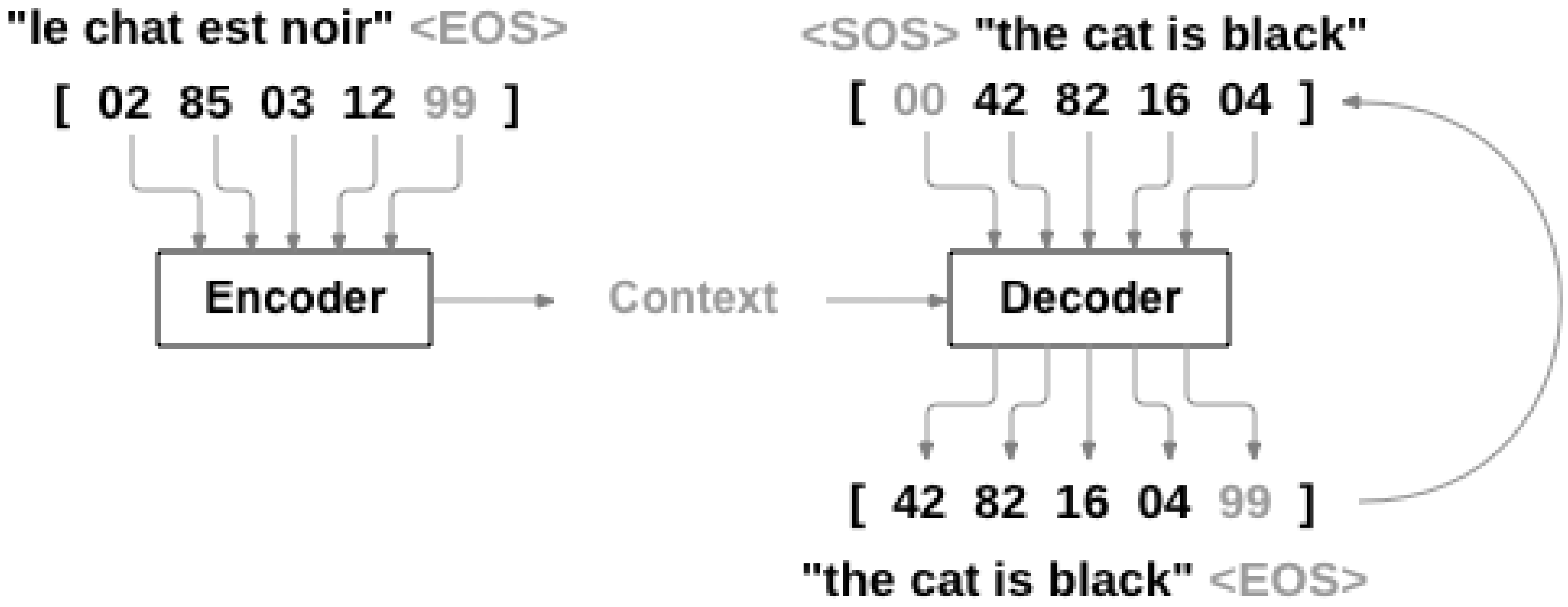


# BERT

# Bidirectional Encoder Representations from Transformers

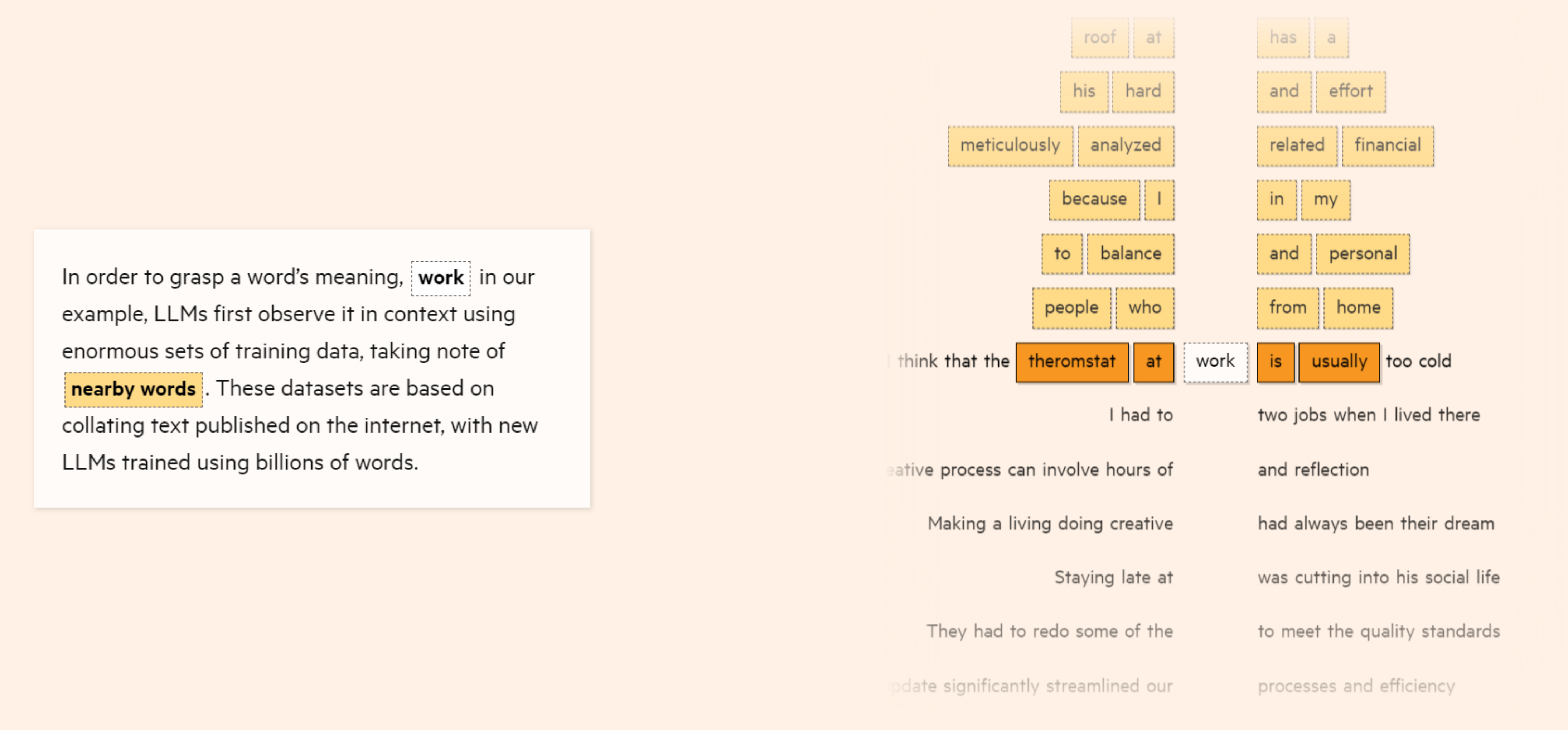


# Machine Translation



# Gen AI - Visualise

https://ig.ft.com/generative-ai/



In order to grasp a word’s meaning, **work** in our example, LLMs first observe it in context using enormous sets of training data, taking note of **nearby words**. These datasets are based on collating text published on the internet, with new LLMs trained using billions of words.

think that the theromstat at work is usually too cold

I had to two jobs when I lived there

eative process can involve hours of and reflection

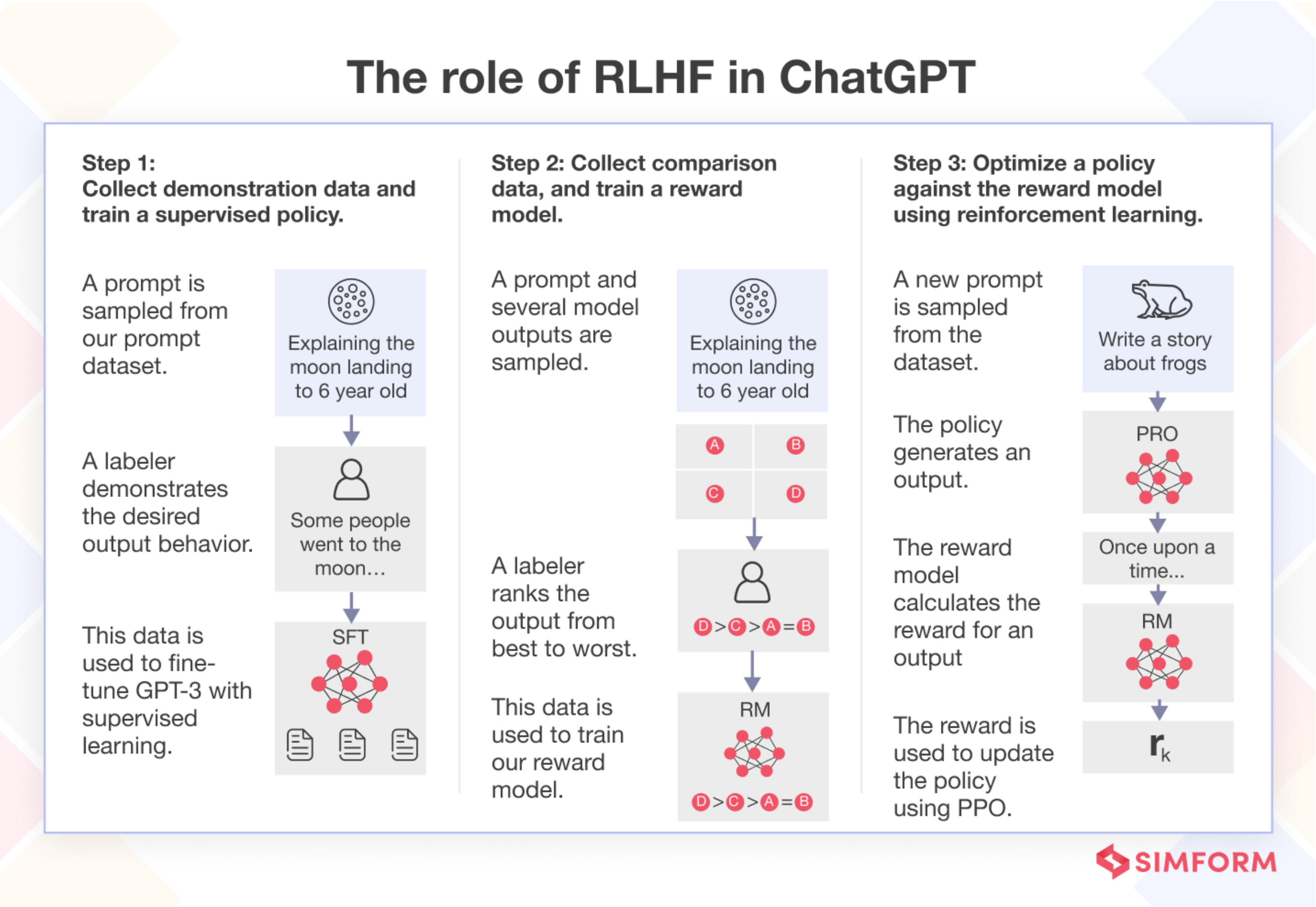
Making a living doing creative had always been their dream

Staying late at was cutting into his social life

They had to redo some of the to meet the quality standards

pdate significantly streamlined our processes and efficiency

# RLHF: Reinforcement Learning from Human Feedback



## The role of RLHF in ChatGPT

**Step 1:
Collect demonstration data and train a supervised policy.**

A prompt is sampled from our prompt dataset.

A labeler demonstrates the desired output behavior.

This data is used to fine-tune GPT-3 with supervised learning.

**Step 2: Collect comparison data, and train a reward model.**

A prompt and several model outputs are sampled.

A labeler ranks the output from best to worst.

This data is used to train our reward model.

**Step 3: Optimize a policy against the reward model using reinforcement learning.**

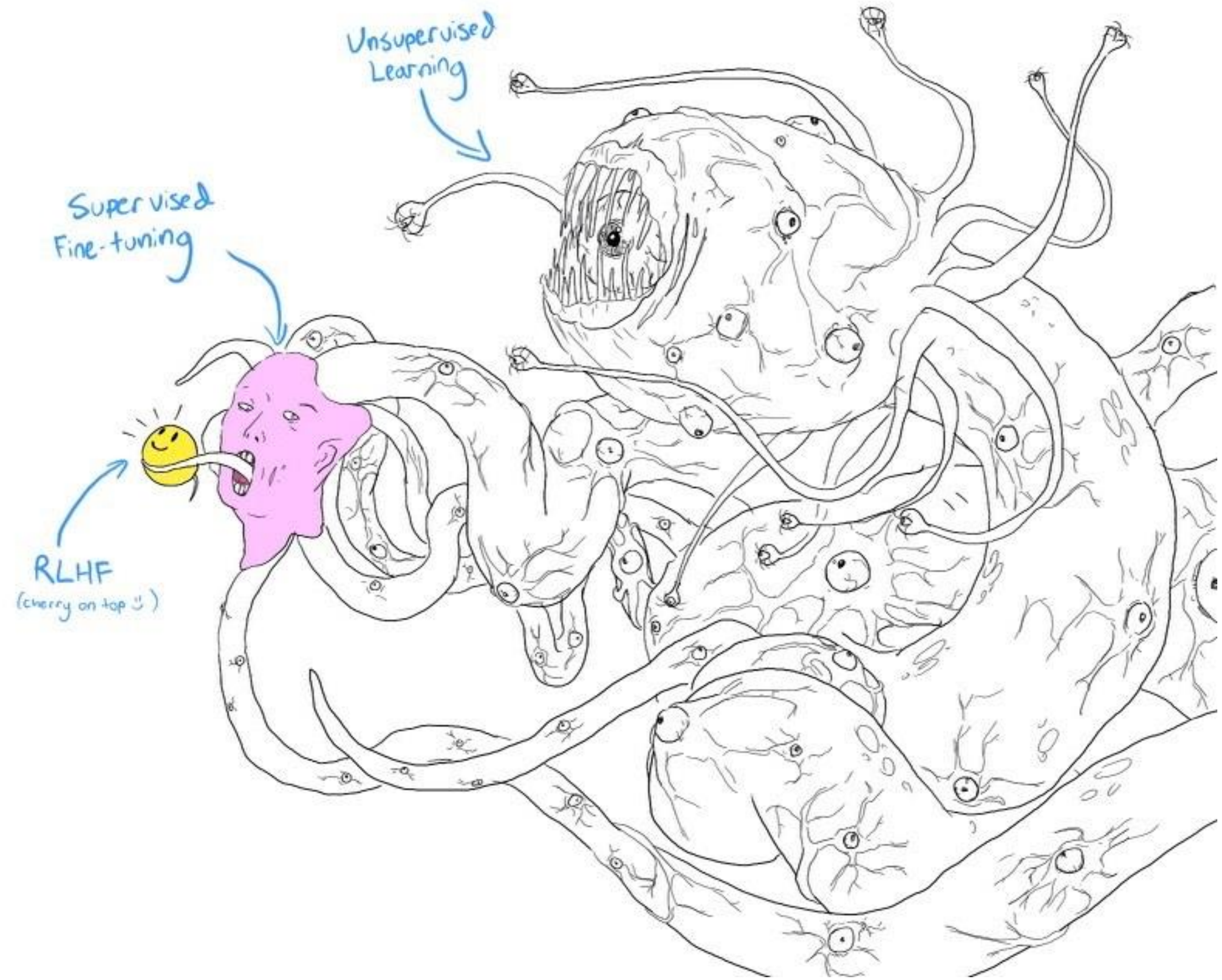
A new prompt is sampled from the dataset.

The policy generates an output.

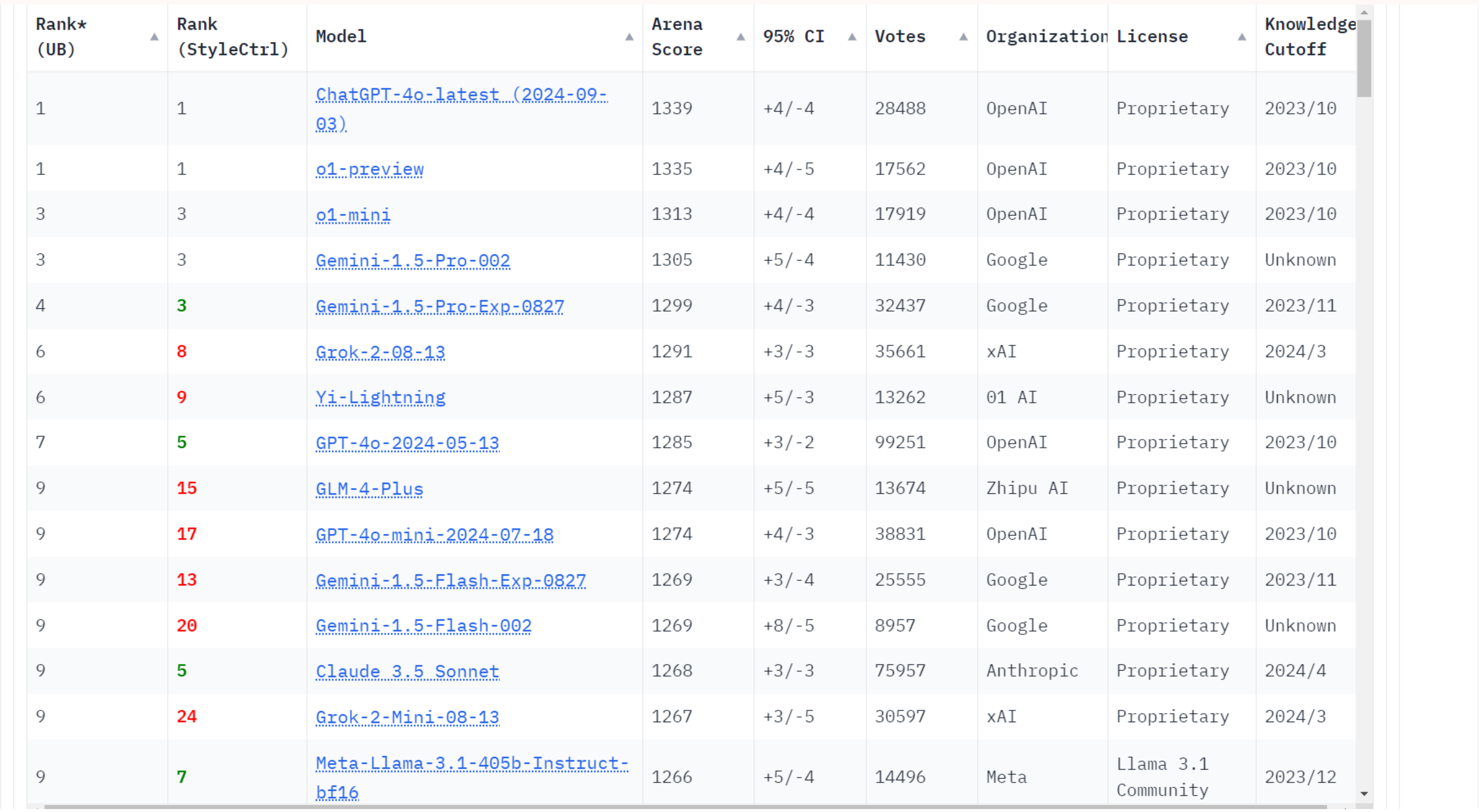
The reward model calculates the reward for an output

The reward is used to update the policy using PPO.

Explaining the moon landing to 6 year old
Some people went to the moon...
SFT
Explaining the moon landing to 6 year old
A
B
C
D
D > C > A = B
RM
D > C > A = B
Write a story about frogs
PRO
Once upon a time...
RM
$r_k$
SIMFORM

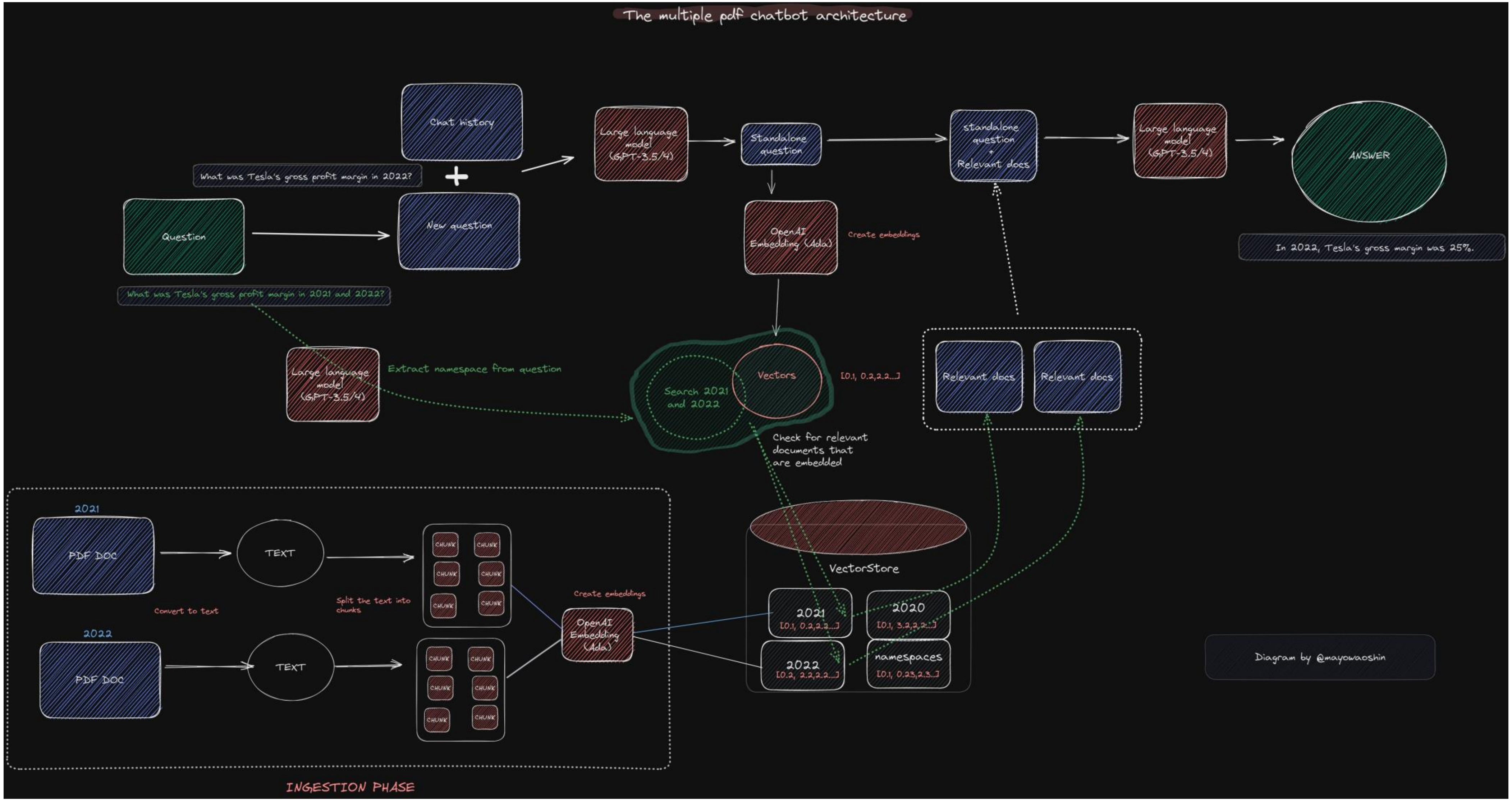

Unsupervised Learning
Supervised Fine-tuning
RLHF
(cherry on top ☺)

# Large Language Models

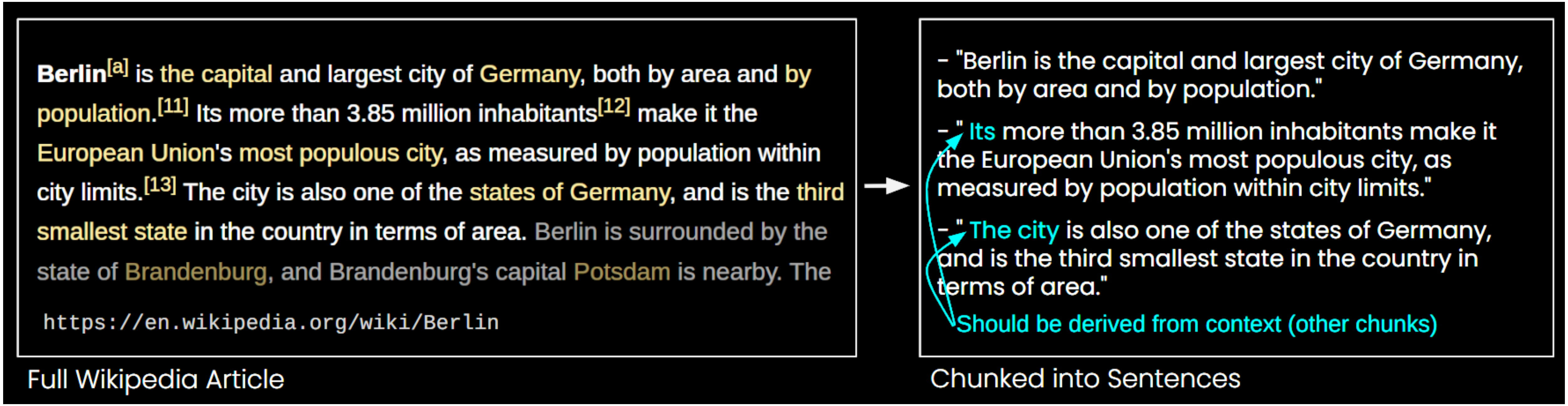


| Rank* (UB) | Rank (StyleCtrl) | Model | Arena Score | 95% CI | Votes | Organization | License | Knowledge Cutoff |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | ChatGPT-4o-latest (2024-09-03) | 1339 | +4/-4 | 28488 | OpenAI | Proprietary | 2023/10 |
| 1 | 1 | o1-preview | 1335 | +4/-5 | 17562 | OpenAI | Proprietary | 2023/10 |
| 3 | 3 | o1-mini | 1313 | +4/-4 | 17919 | OpenAI | Proprietary | 2023/10 |
| 3 | 3 | Gemini-1.5-Pro-002 | 1305 | +5/-4 | 11430 | Google | Proprietary | Unknown |
| 4 | 3 | Gemini-1.5-Pro-Exp-0827 | 1299 | +4/-3 | 32437 | Google | Proprietary | 2023/11 |
| 6 | 8 | Grok-2-08-13 | 1291 | +3/-3 | 35661 | xAI | Proprietary | 2024/3 |
| 6 | 9 | Yi-Lightning | 1287 | +5/-3 | 13262 | 01 AI | Proprietary | Unknown |
| 7 | 5 | GPT-4o-2024-05-13 | 1285 | +3/-2 | 99251 | OpenAI | Proprietary | 2023/10 |
| 9 | 15 | GLM-4-Plus | 1274 | +5/-5 | 13674 | Zhipu AI | Proprietary | Unknown |
| 9 | 17 | GPT-4o-mini-2024-07-18 | 1274 | +4/-3 | 38831 | OpenAI | Proprietary | 2023/10 |
| 9 | 13 | Gemini-1.5-Flash-Exp-0827 | 1269 | +3/-4 | 25555 | Google | Proprietary | 2023/11 |
| 9 | 20 | Gemini-1.5-Flash-002 | 1269 | +8/-5 | 8957 | Google | Proprietary | Unknown |
| 9 | 5 | Claude 3.5 Sonnet | 1268 | +3/-3 | 75957 | Anthropic | Proprietary | 2024/4 |
| 9 | 24 | Grok-2-Mini-08-13 | 1267 | +3/-5 | 30597 | xAI | Proprietary | 2024/3 |
| 9 | 7 | Meta-Llama-3.1-405b-Instruct-bf16 | 1266 | +5/-4 | 14496 | Meta | Llama 3.1 Community | 2023/12 |

# Chat over PDF



# Chunking



**Berlin**[a] is the capital and largest city of Germany, both by area and by population.[11] Its more than 3.85 million inhabitants[12] make it the European Union's most populous city, as measured by population within city limits.[13] The city is also one of the states of Germany, and is the third smallest state in the country in terms of area. Berlin is surrounded by the state of Brandenburg, and Brandenburg's capital Potsdam is nearby. The

https://en.wikipedia.org/wiki/Berlin

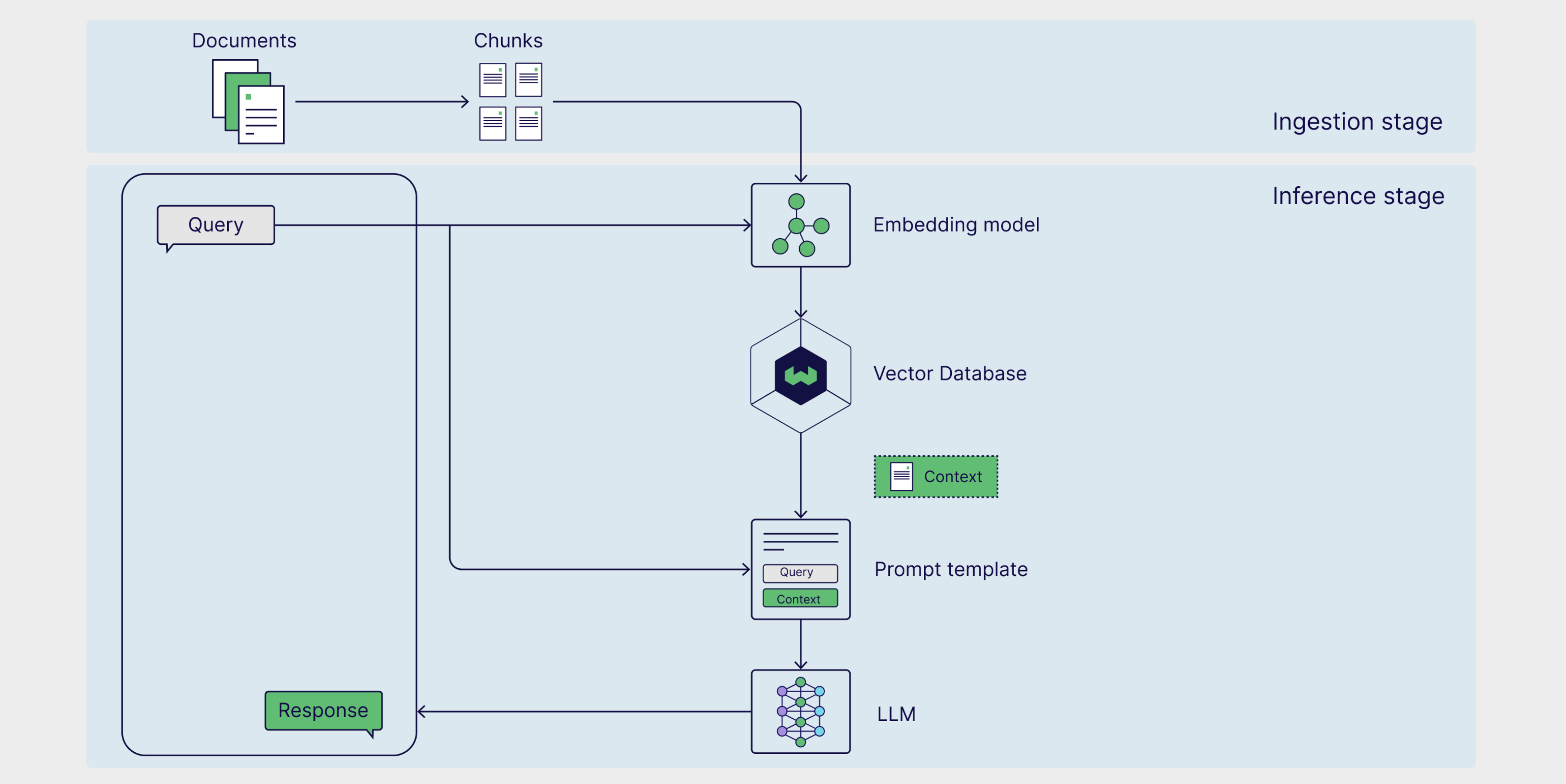
Full Wikipedia Article

- "Berlin is the capital and largest city of Germany, both by area and by population."
- " Its more than 3.85 million inhabitants make it the European Union's most populous city, as measured by population within city limits."
- " The city is also one of the states of Germany, and is the third smallest state in the country in terms of area."

Should be derived from context (other chunks)

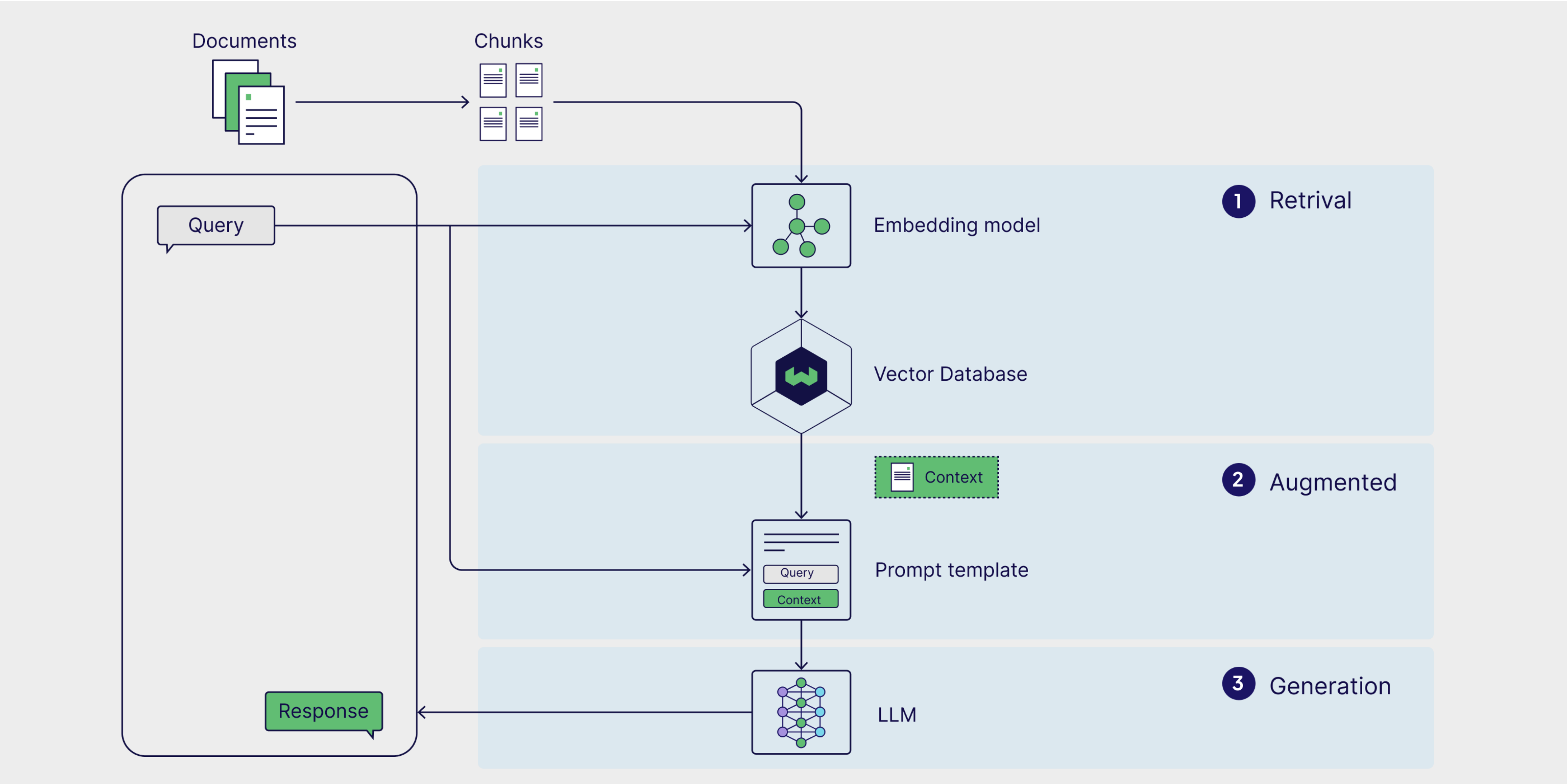
Chunked into Sentences

# Retrieval Augmented Generation (RAG) - Ingestion



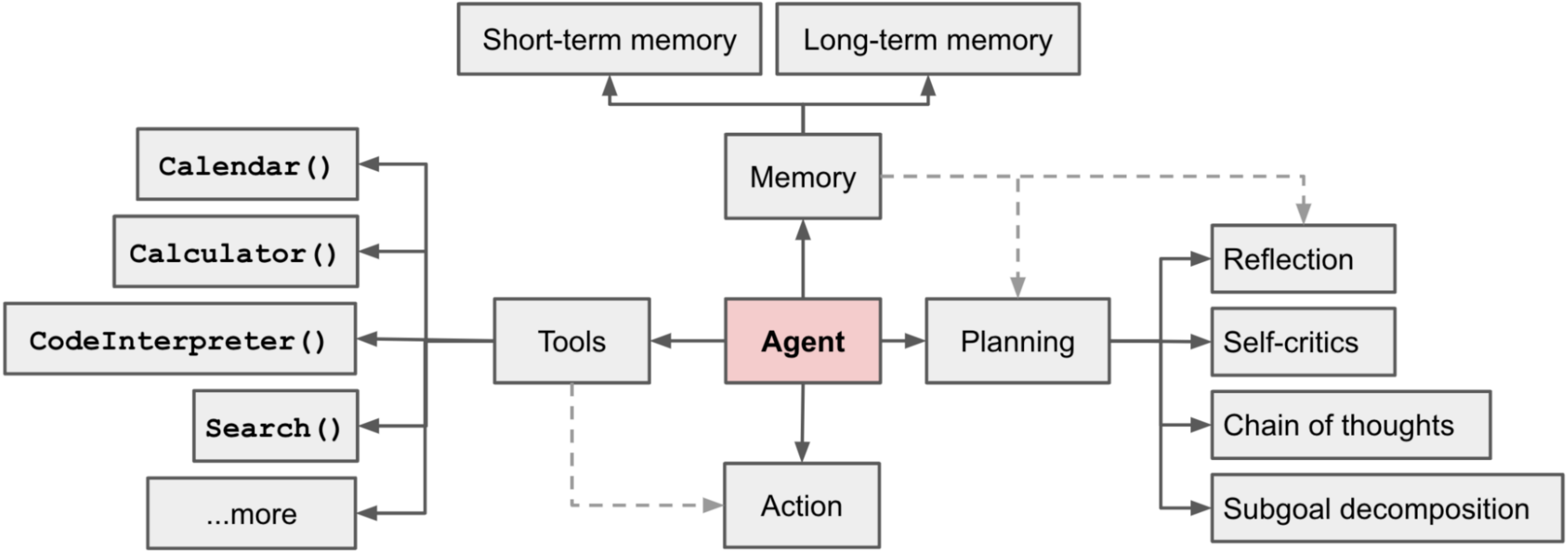
https://weaviate.io/blog/introduction-to-rag

# RAG - Inference

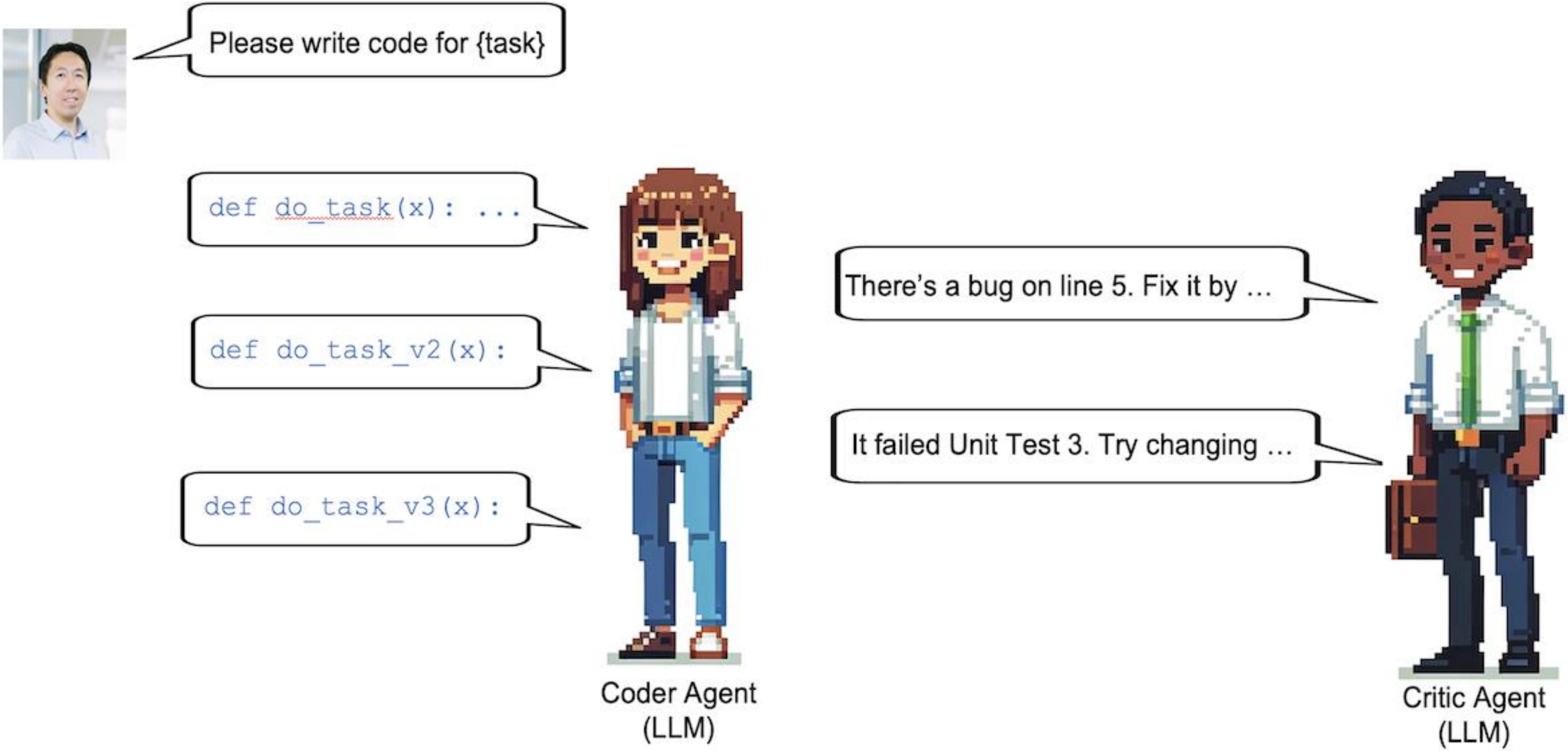


https://weaviate.io/blog/introduction-to-rag

# Agents


Short-term memory
Long-term memory
Memory
Calendar()
Calculator()
CodeInterpreter()
Search()
...more
Tools
Agent
Planning
Action
Reflection
Self-critics
Chain of thoughts
Subgoal decomposition

# Agentic Design Patterns: Reflection



Please write code for {task}

```
def do_task(x): ...
```

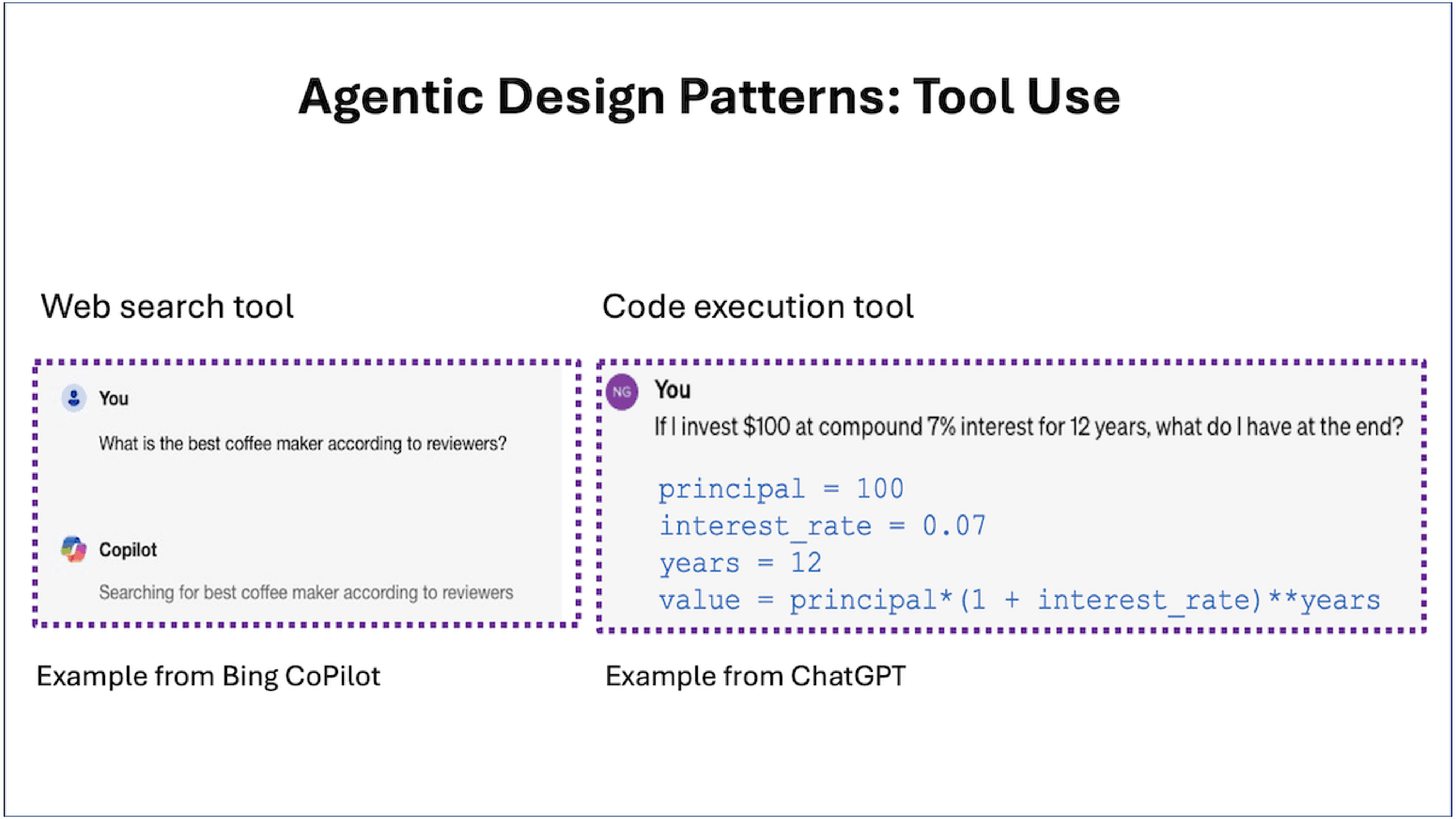
```
def do_task_v2(x):
```

```
def do_task_v3(x):
```

There’s a bug on line 5. Fix it by …

It failed Unit Test 3. Try changing …

# Tool Use



## Agentic Design Patterns: Tool Use

Web search tool

You

What is the best coffee maker according to reviewers?

Copilot

Searching for best coffee maker according to reviewers

Example from Bing CoPilot

Code execution tool

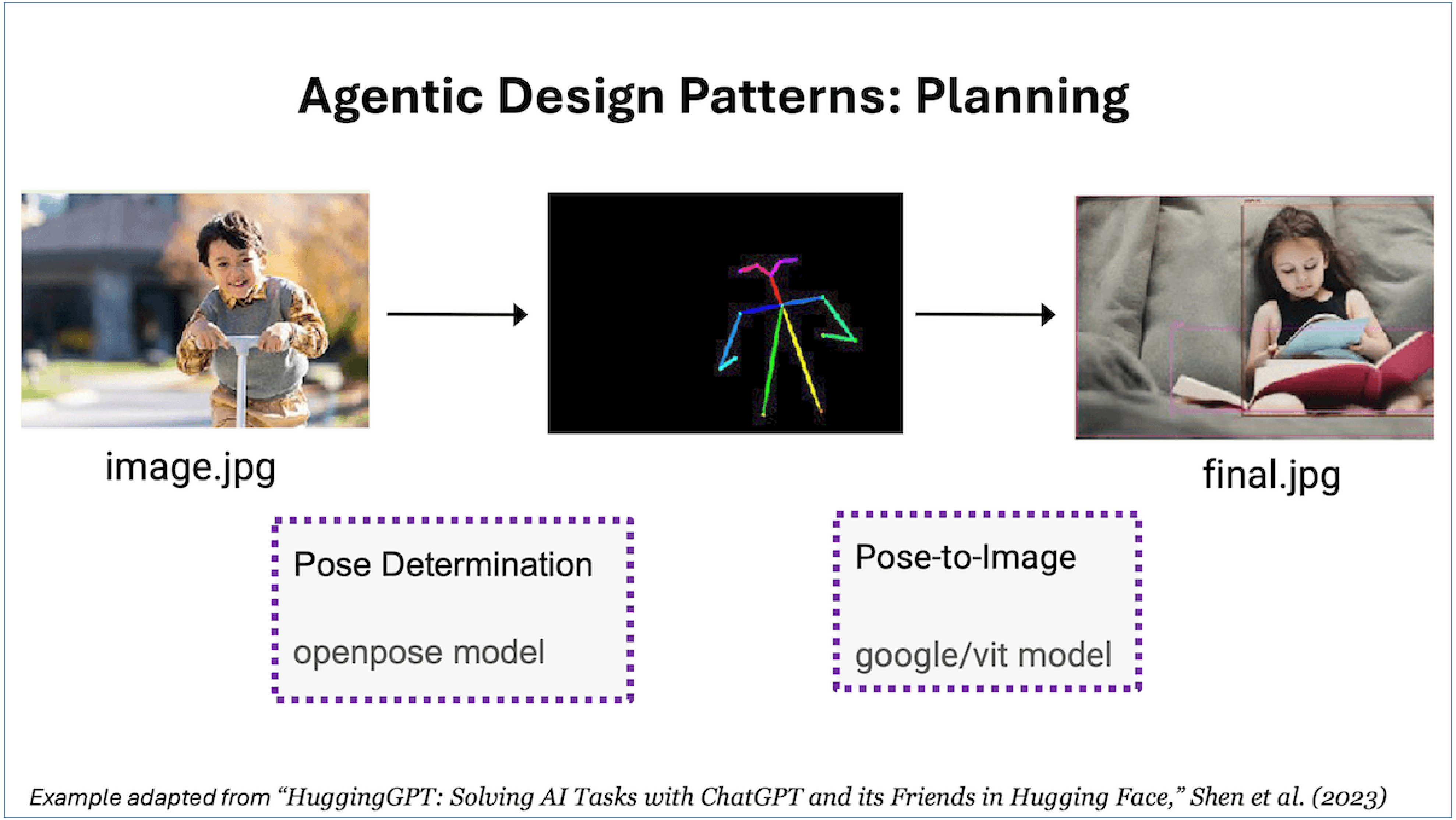
You

If I invest $100 at compound 7% interest for 12 years, what do I have at the end?

```
principal = 100
interest_rate = 0.07
years = 12
value = principal*(1 + interest_rate)**years
```

Example from ChatGPT

# Planning



## Agentic Design Patterns: Planning

image.jpg

Pose Determination

openpose model

Pose-to-Image

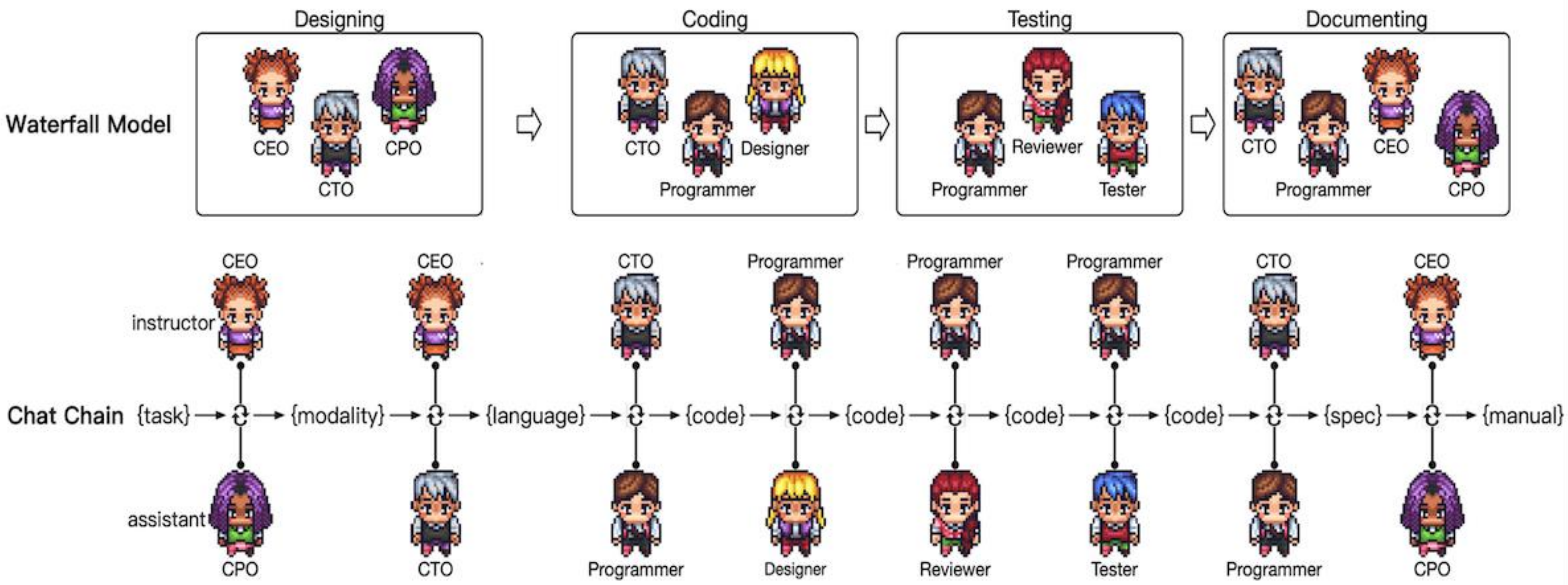
google/vit model

final.jpg

*Example adapted from "HuggingGPT: Solving AI Tasks with ChatGPT and its Friends in Hugging Face," Shen et al. (2023)*

# Multiple Agents

## Agentic Design Patterns: Multi-Agent Collaboration



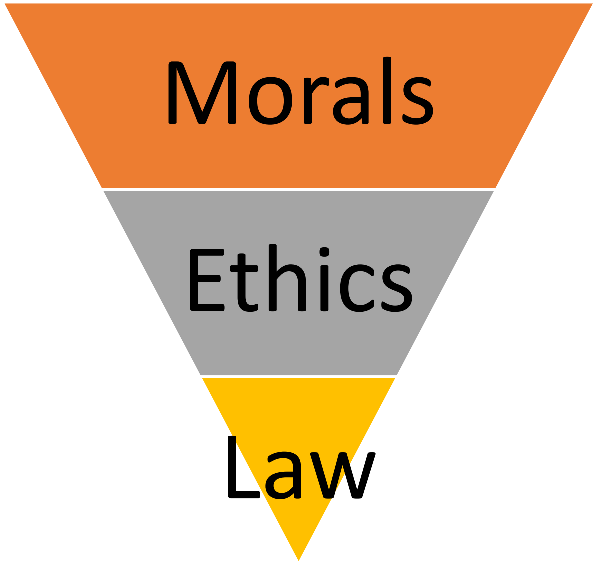
*Proposed ChatDev architecture. Image adapted from "Communicative Agents for Software Development," Qian et al. (2023).*

# Data Ethics

LA TROBE
UNIVERSITY
Centre for
Data Analytics
and Cognition

# Moral, ethical, legal

- Moral, ethical, legal
  - Morals – individual, personal beliefs, philosophical
  - Ethics – community, correct behaviour, analytical
  - Law – society/country, a basic standard that is enforced to protect morals and ethics, logical



# Defining Ethics

- Many formal definitions (‘the science of the ideal human character’)
- A branch of philosophy that can be summarised as “What should I do?” or “How should I live?”
- A critical phase in any decision-making process guided by values, principles and purpose, instead of own interests, social convention, company policy, or even rule of law.
    - Values – what is good, what we strive, desire and seek to protect.
    - Principles – what is right, in terms of achieving our values (above).
    - Purpose – in life, rationalises values and principles

# Ethics – Areas of Study

- Meta-ethics – how we understand ethics (theory and philosophy)
- Normative ethics - study of ethical action, standards for right/wrong
- Applied ethics – application to real-world settings
  - Medical ethics
  - Bioethics
  - AI ethics
  - Animal ethics
  - Business ethics etc.

# Ethics theories

- Consequentialist – an action is judged by its consequences
  - Utilitarianism – ‘greatest good for the greatest number’
  - Ethical egoism/altruism - self-centred vs selfless
- Non-consequentialist – an action is judged on properties intrinsic to the action
  - Aristotle’s virtue ethics – a character based approach of virtue through practice
  - Kant’s deontological (duty-based) ethics - rules to distinguish right from wrong
- The Dark Knight
  - Batman should kill the Joker
  - Batman should not kill the Joker
  - What kind of person would kill the Joker?

# Normative Ethics

- Sets standards for right and wrong behavior
- A business analytics firm creates a code of ethics requiring all data analysts to maintain data accuracy and honesty in reporting findings.
- A cloud service provider develops a policy stating that all user data must be encrypted both in transit and at rest to ensure privacy and security. This policy sets a standard for ethical behavior by establishing what is right (data encryption) and wrong (leaving data unencrypted).

# Applied Ethics

- Practical application of moral considerations to specific problems.

- A tech company faces a data breach. They immediately inform affected customers, offer credit monitoring, and improve their cybersecurity measures.

- A company faces a data breach where user information is exposed. Applied ethics would guide the company to take immediate action, notify affected users, offer support such as credit monitoring, and implement stronger security measures to prevent future breaches.

# Descriptive Ethics

- Studies people's beliefs about morality.

- Conducting a survey within the company to understand employees' views on data privacy and implementing policies that reflect these concerns.

- Researchers conduct a survey across different countries to understand how users perceive data privacy in cloud services. They find that users in some regions are more concerned about government surveillance, while others prioritize protection from corporate misuse of data. This understanding helps tailor ethical policies to different cultural contexts.

- Project Maven (https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html)

# Meta-Ethics

- Examines the nature and meaning of ethical principles.
- Discussing what data privacy really means for users of a cloud service, and whether users truly understand and consent to data collection practices.
- Philosophers and ethicists debate the concept of data ownership in cloud computing. They explore questions like whether users truly own their data once it is uploaded to the cloud, and what it means for a cloud provider to have ethical responsibilities regarding that data.

# Virtue Ethics

- Focuses on developing good character traits.

- Promoting a company culture where employees are recognized and rewarded for demonstrating integrity, such as reporting unethical practices.

- A cloud company fosters a corporate culture emphasizing virtues like honesty and integrity. Employees are encouraged to report any unethical practices they observe, such as improper access to user data, ensuring that the company operates transparently and ethically.

- Whistleblower programs

# Deontological Ethics

- Ethics based on rules and duties.

- Implementing a strict no-tolerance policy against using customer data for purposes other than those explicitly agreed to by the customers.

# Consequentialism

- Judges actions by their outcomes.

- Deciding to implement machine learning algorithms that improve user experience but also carefully evaluating and mitigating potential biases in the algorithms.

- A cloud company considers implementing a new AI algorithm to improve service efficiency. Before deployment, they assess the potential consequences, including benefits like faster processing times and risks like unintended biases in decision-making. They decide to proceed only if the positive outcomes outweigh the negative impacts.

# Ethics of Care

- Emphasises caring relationships and responsibilities.

- Establishing an employee assistance program that provides support for mental health, showing the company's commitment to employee well-being.

- A cloud provider implements strict rules requiring user consent before any personal data can be shared with third parties. Even if sharing data could be profitable or beneficial, the company adheres to the rule of obtaining consent, demonstrating its commitment to ethical duties.

# Environmental Ethics

- Focuses on the ethical relationship between humans and the environment.
- Implementing a company-wide initiative to reduce carbon footprint by transitioning to cloud services powered by renewable energy.
- A cloud provider invests in green energy solutions for its data centers, such as solar and wind power. By reducing its carbon footprint, the company demonstrates its commitment to environmental ethics and the broader impact of its operations on the planet.
- Google Demand Response (https://cloud.google.com/blog/products/infrastructure/using-demand-response-to-reduce-data-center-power-consumption)

# Frameworks Applied to Cloud Computing

- Deontological Ethics (Duty-Based Ethics): This framework is based on the idea that certain actions are inherently right or wrong, regardless of their outcomes. In the context of cloud computing, this could mean that certain practices (such as maintaining strong data security or respecting user privacy) should always be followed because they are the right thing to do.

- Consequentialism (Outcome-Based Ethics): This framework evaluates the morality of an action based on its consequences. In cloud computing, a consequentialist approach might involve weighing the potential benefits of a decision (such as increased efficiency or cost savings) against the potential harms (such as privacy breaches or data loss).

- Virtue Ethics: This framework focuses on the character traits that a moral individual should possess, and suggests that ethical decisions should reflect these virtues. In the context of cloud computing, virtues might include honesty (being transparent about data usage), responsibility (protecting user data), and fairness (treating all users equally).

# Frameworks Applied Continued.

- Principlism: Commonly used in bioethics, this approach involves four principles: autonomy, beneficence, non-maleficence, and justice. Applied to cloud computing, these principles might translate to respecting user control over their data (autonomy), ensuring the cloud service benefits the user (beneficence), avoiding harm to the user (non-maleficence), and treating all users fairly (justice).

- Ethics of Care: This framework emphasizes the importance of care as a value in moral decision-making. In cloud computing, an ethics of care approach might prioritize user needs and concerns, fostering trust, and building positive relationships with users.

- Professional Codes of Ethics: Many IT and computing professional organizations, such as the ACM and IEEE, have their own codes of ethics that provide guidance for ethical decision-making in the field. These codes often encompass principles from several of the above frameworks, and may have specific guidelines relevant to cloud computing.

# AI Ethics in the public interest

- Autonomous cars
  - Networks of movement, convenient, economical, efficient
  - Avoiding a road accident, saving a human life, which human?
- Automated sentencing
  - Big data-driven insights that overcome human bias, fast, informed
  - Inclusivity, completeness, quality – human bias is easily replicated in training datasets
- Personalisation and disinformation overload
  - Social beings, networks of support, emergency announcements
  - Confirmation bias, social herding, echo chambers, fake news bots
- Military and surveillance use cases
- Those who build the AI – 80% of AI academics and 70% of AI industry are male

# What are Data Ethics

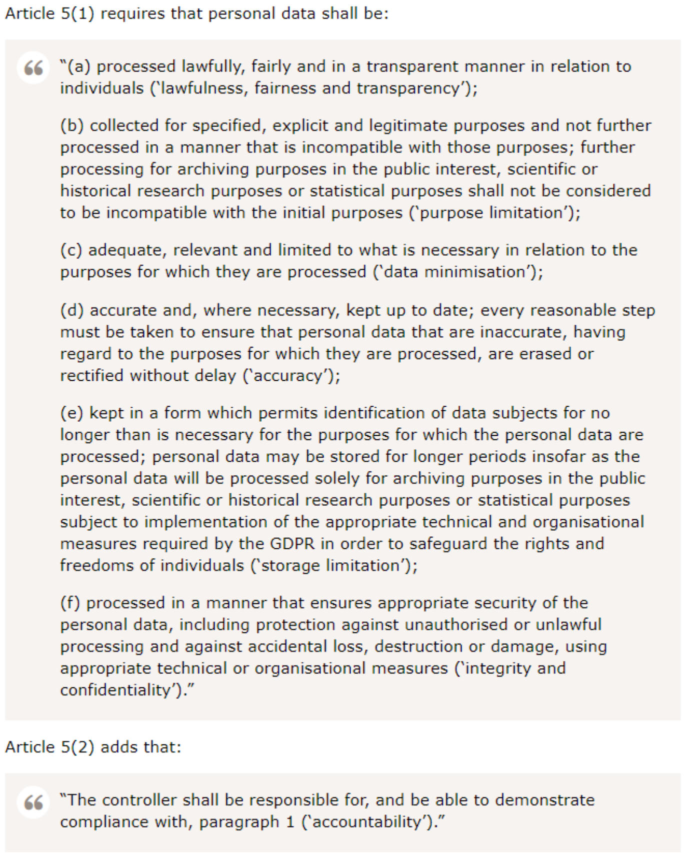
- A branch of ethics that deals with the moral problems related to data during its phases of collection, processing, curation, manipulation, dissemination

# Data - Security, Protection, Privacy

- Data security – securing data from external threats (unauthorised access to systems)
  - Confidentiality - only accessed by authorised individuals
  - Integrity - not altered without authorisation
  - Availability - reliable access to data
- Data protection - securing data from internal threats (unregulated control of data)
  - A legal construct for informational self-determination, data loss
- Data privacy – how the data gets used (unspecified processing of data)
  - Consent and notice
  - Legal right to access/delete
  - Third party access

# GDPR

- General Data Protection Regulation
  - A law on data protection and privacy in the European Union and the European Economic Area.
  - The strongest set of data protection rules in the world, implemented in May 2018
  - Gives control of personal data and simplify data access for organisations
- Seven principles:
  - Lawfulness, fairness and transparency
  - Purpose limitation
  - Data minimisation
  - Accuracy
  - Storage limitation
  - Integrity and confidentiality (security)
  - Accountability



Article 5(1) requires that personal data shall be:

> "(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
>
> (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
>
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
>
> (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Article 5(2) adds that:

> "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

# OECD Privacy Guidelines

- Organisation for Economic Co-operation and Development
  - An intergovernmental organisation with 38 member countries, founded in 1961 to stimulate economic progress and world trade.
  - Australia is a signatory
- Offers principles for privacy protection across member countries, created by the Organisation for Economic Co-operation and Development (OECD). https://www.oecd.org/digital/privacy/
- Emphasizes the protection of personal data and privacy rights.
- Encourages transparency in data collection and usage.
- Advocates for individuals' rights to access and correct their data.
- Promotes international cooperation to ensure consistent privacy standards globally.

# Health Insurance Portability and Accountability Act (HIPAA)

- A US law designed to provide privacy standards to protect patients' medical records and other health information.

- Ensures the confidentiality, integrity, and availability of protected health information (PHI).

- Requires appropriate administrative, physical, and technical safeguards to ensure the privacy of PHI.

- Establishes national standards for the protection of health information.

- Mandates covered entities to notify affected individuals, the Secretary of Health and Human Services (HHS), and, in certain circumstances, the media, of a breach of unsecured PHI.

- Applies to healthcare providers, health plans, and healthcare clearinghouses, as well as their business associates.

# In Australia..

- Most states and territories (except WA and SA) have their own data protection legislation applicable to state government agencies, and private businesses that interact with state government agencies.

- At the Federal level:
  - Privacy act 1988: https://oaic.gov.au/privacy-law/
  - Australian Privacy Principles
  - Privacy Amendment (Notifiable Data Breaches) Act 2017: https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme
  - Who – government agency, business with +3m turnover, organisations in health services

- Australian Government Information Security Manual
  - https://www.cyber.gov.au/ism

# Consumer Data Right

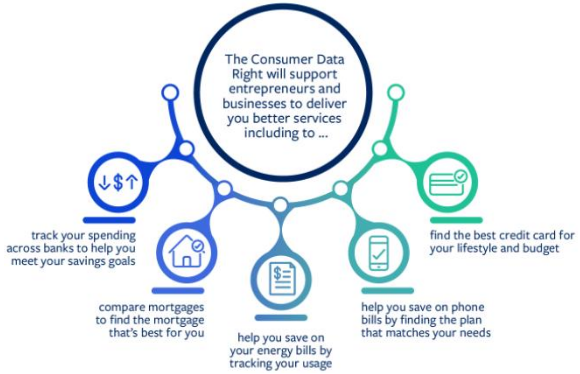
- CDR establishes the right for consumers to direct a supplier to share designated data about the consumer with another supplier or with the consumer themselves

- CDR aims to increase the bargaining power of consumers by enabling comparison and switching between products/services, while also driving competition and innovation between service providers

- Introduced into the banking sector in July 2020 (open banking), energy and telecom to follow

- It is an opt-in system, the consumer can authorise a business to access your data, with control over what data is transferred, where it is used, who it can be disclosed to, with the ability to withdraw consent at any time and delete if no longer needed

- Only ‘accredited data recipients’ accredited by the ACCC can provide services, which include requesting data with the customer’s consent, then using to provide a comparison or product/service



The Consumer Data Right will support entrepreneurs and businesses to deliver you better services including to ...

track your spending across banks to help you meet your savings goals

compare mortgages to find the mortgage that’s best for you

help you save on your energy bills by tracking your usage

help you save on phone bills by finding the plan that matches your needs

find the best credit card for your lifestyle and budget

# Responsible data collection

- Two rules of thumb – avoid harm and build trust
- Manipulation and misrepresentation
  - Manipulate consumers into revealing personal information (apps).
  - Misrepresented identity (collect survey data in the guise of student projects).
- Develop an awareness and accountability of the following ten principles
  - Informed consent – should the subject know data is being collected and agree to its collection?
  - Anonymity - should all personally identifying information be eliminated from the data? or collect only in the form of aggregates such that individuals cannot be identified?
  - Confidentiality - should sources and providers of data be protected from disclosure?
  - Security - what level of protection from intrusion, corruption, and unauthorized access?
  - Privacy - should each individual have the ability to control access to personal data about themselves?

# Ten principles (continued)

- Accuracy - what level of exactness and correctness is required of the data?
- Ownership - is personal data about individuals an asset that belongs to the business or privately owned information for which the business has stewardship responsibilities?
- Honesty - to what degree should the business be forthright and visible about data collection practices?
- Responsibility - who is accountable and at what level for use and misuse of data?
- Transparency – between the two extremes of open and stealth data collection, what is the right level of transparency?

# Anonymised data

- Anonymised data is frequently used in AI projects.
- Remove/replace classification of personally identifiable information so that individuals associated with that data can remain anonymous.
- Useful for segmentation - identifying collective patterns which does not require information at individual level.
- But, the more Anonymised the less useful it becomes.
- Identity information inevitably removes contextual information.
- And pseudo-anonymised
- A pragmatic solution – be transparent and provide consumers the choice to opt-in/opt-out.

# Opt-in and Opt-out

- Seen on many websites and social networks.
- Opt-out – default settings used by the service provider most often for all data collection.
  - The user must explicitly choose to opt out of the default into custom settings.
- Opt-in – explicit permission has to be granted to collect and use information in a certain set of ways before the collection of data begins.
  - Tedious but useful as it forces end-users to consider repercussions before making a choice.
  - Less likely to be used as it's frequently ignored (need to incentivise).

# Data - other considerations

- The right to be forgotten – explicit request for removal of data.
- Individuals requesting invisibility from search engines raises questions about both privacy and freedom of speech.
- The right to data expiry - data be deleted after it fulfills a business purpose
- Data ownership – provide the end-user ownership/full control of their data
- Lessons from bioethics - medical/clinical research

# Data Privacy

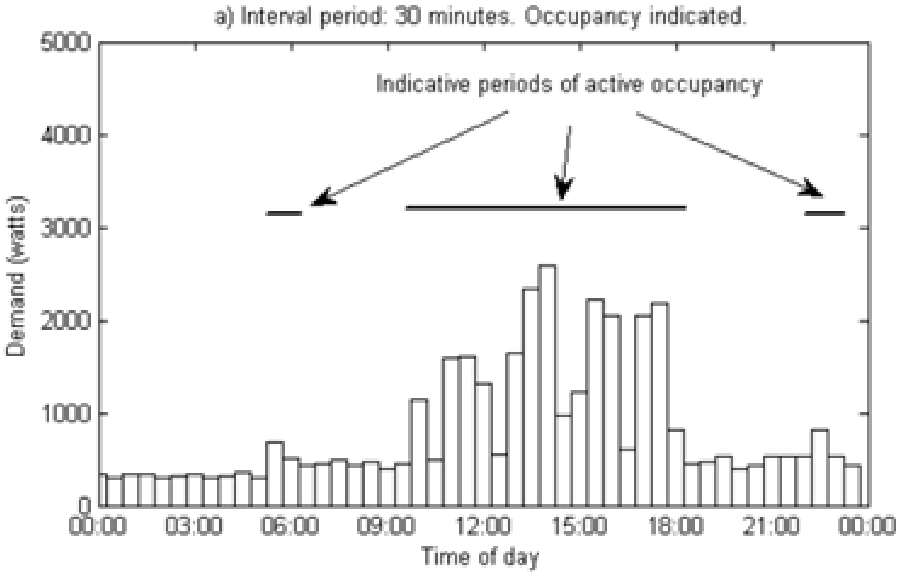
- Data privacy (or information privacy or data protection) is about access, use and collection of data, and the data subject's legal right to the data. This refers to:
  - Freedom from unauthorized access to private data
  - Inappropriate use of data
  - Accuracy and completeness when collecting data about a person or persons (corporations included) by technology
  - Availability of data content, and the data subject's legal right to access; ownership
  - The rights to inspect, update or correct these data

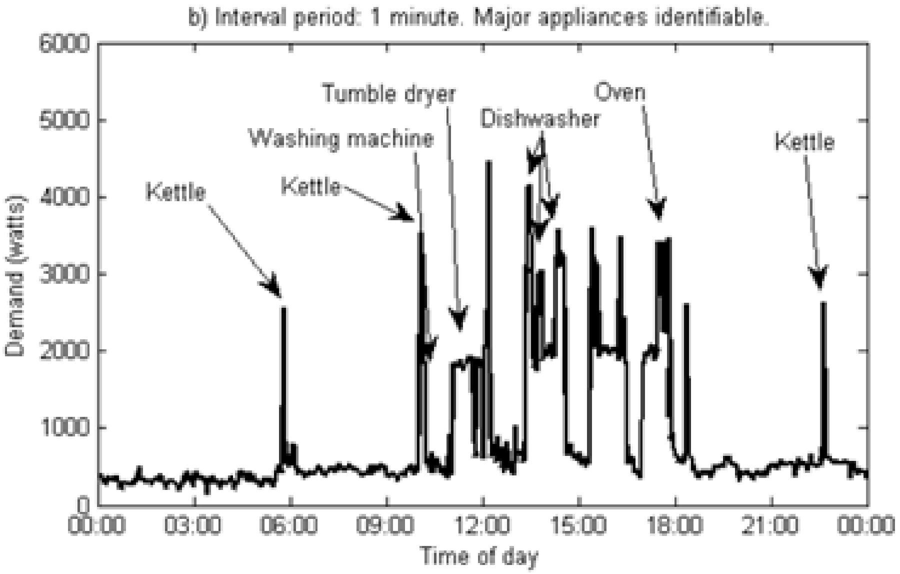
# A way forward..

- Micro-ethics - transition from guidelines to instructions
  - Left to the scientist to derive concrete technological implementations from abstract values and principles
  - Datasets - generation, recording, curation, processing, dissemination, sharing and use in training the AI
  - Designing new algorithms with ethics in place, instead of post-processing XAI components
  - Example: standardized datasheets (metadata) listing the properties of training datasets, that can be used to check fit for purpose, original intent, collection, pre-processing.
- Ethical theories – from deontology to virtue ethics
  - Deontologically inspired check-box ticking exercise to a situation-sensitive approach based on virtue ethics
- Increased visibility of ethicists in professional communities, not only the general public.
  - Collaborative public dialogue on the social value of AI

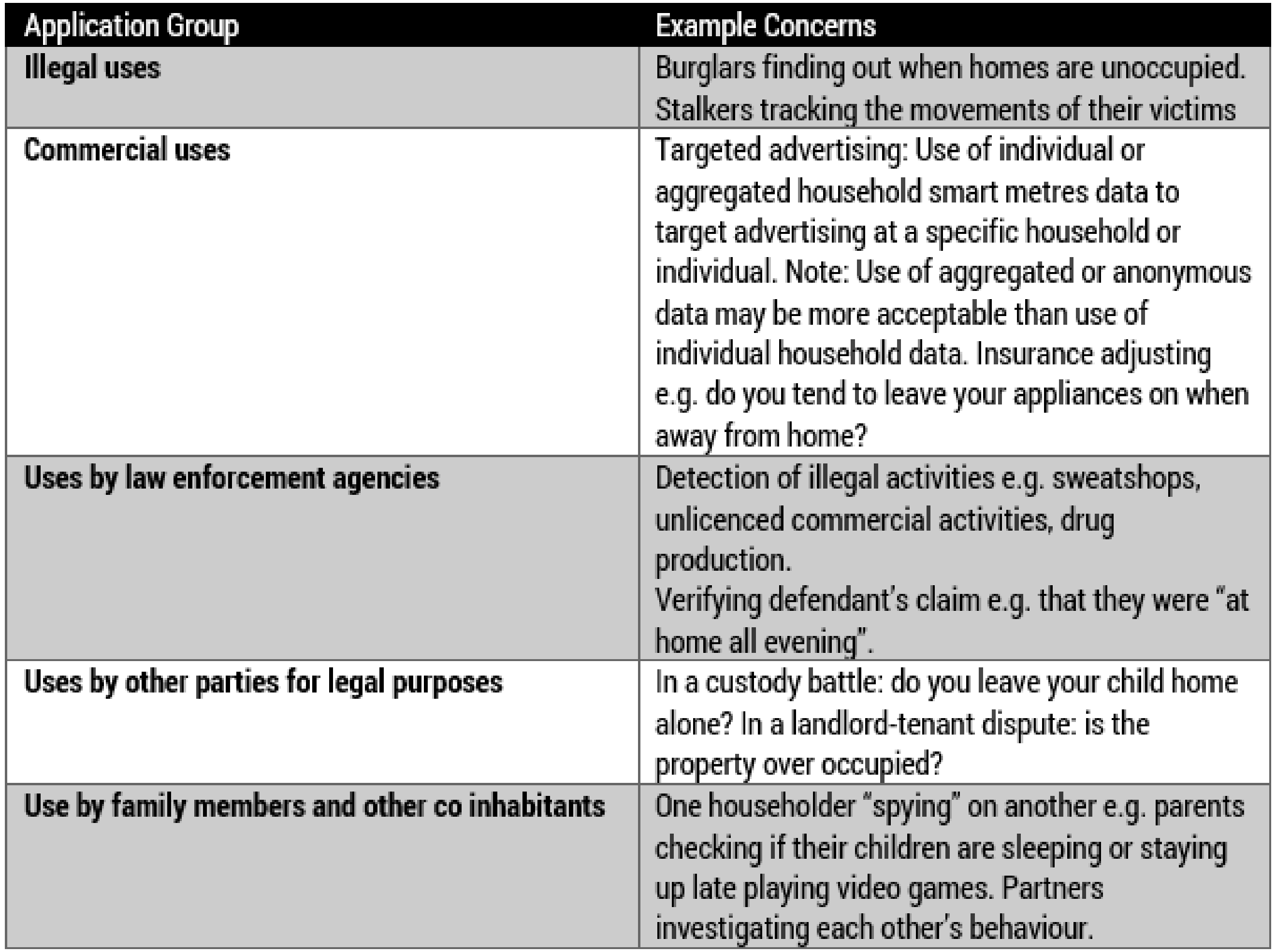
# Example – Smart meters

- Smart meters are used to measure and monitor consumption of utilities (electricity, water, natural gas, and fuel) in near real-time, and transmit a digital data stream of readings to a central node of the grid infrastructure.
- “spy in the home” - which will allow governments to monitor household behaviour
- An abundance of convenience for optimal energy grid management, supplier, distributor, retailer, consumer
- Unlike quarterly or monthly readings of cumulative energy consumption, 15 min or 30 min interval data reveal much more information about the consumers – behaviours and profiles.





# Applying Ethics



| Application Group | Example Concerns |
|---|---|
| **Illegal uses** | Burglars finding out when homes are unoccupied.<br>Stalkers tracking the movements of their victims |
| **Commercial uses** | Targeted advertising: Use of individual or aggregated household smart metres data to target advertising at a specific household or individual. Note: Use of aggregated or anonymous data may be more acceptable than use of individual household data. Insurance adjusting e.g. do you tend to leave your appliances on when away from home? |
| **Uses by law enforcement agencies** | Detection of illegal activities e.g. sweatshops, unlicenced commercial activities, drug production.<br>Verifying defendant's claim e.g. that they were "at home all evening". |
| **Uses by other parties for legal purposes** | In a custody battle: do you leave your child home alone? In a landlord-tenant dispute: is the property over occupied? |
| **Use by family members and other co inhabitants** | One householder "spying" on another e.g. parents checking if their children are sleeping or staying up late playing video games. Partners investigating each other's behaviour. |

| **EAD Principle** | **Implications for Smart Meters/ Smart Grid** |
|---|---|
| Human rights | In a prosumer setting, priorities when charging/discharging from the grid into batteries and EVs. |
| Prioritizing well-being | In peak shedding events, priority to aged and disadvantaged communities |
| Accountability | Multi-stakeholder ecosystems from supplier, distributor to retailer |
| Transparency | Providing consumers full access to their consumption data and comparative information (similar households), across national/local benchmarks |
| Misuse | Ensuring data and insights are not shared with third parties who may link across other datasets for more individualised profiles |

# Limitations in practice

- “Ethics plays the role of a bicycle brake on an intercontinental airplane” (Beck 1988)
- Purpose - economic incentive vs societal values or fundamental rights
- Budgets - significant investments in AI for commercial gain vs ethics for public relations purposes
- Staff - neither systematic education of ethical issues, nor empowered to raise ethical concerns
- Approach - voluntary and non-binding, not enforced. An “add-on” to a technical specification.
- Gender - 80% academics and 70% industry are men
- Datasets - collected/curated in the technical domain/developed world on systems/technology built for unrelated objectives

# A way forward..

- Micro-ethics - transition from guidelines to instructions
  - Left to the scientist to derive concrete technological implementations from abstract values and principles
  - Datasets - generation, recording, curation, processing, dissemination, sharing and use in training the AI
  - Designing new algorithms with ethics in place, instead of post-processing XAI components
  - Example: standardized datasheets (metadata) listing the properties of training datasets, that can be used to check fit for purpose, original intent, collection, pre-processing.
- Ethical theories – from deontology to virtue ethics
  - Deontologically inspired check-box ticking exercise to a situation-sensitive approach based on virtue ethics
- Increased visibility of ethicists in professional communities, not only the general public.
  - Collaborative public dialogue on the social value of AI

# An Ethical Approach to Data Privacy Protection

- Comply with national data protection or privacy law, national contract law, and other legal requirements or regulations relating to data privacy.
- Comply with current security standards to protect stored personal data from illegitimate or unauthorized access or from accidental access, processing, erasure, loss or use.
- Implement an easily perceptible, accessible and comprehensible privacy policy with information on who is in charge of data privacy and how this person can be individually contacted, why and which personal data are collected, how these data are used, who will receive these data, how long these data are stored, and whether and which data will be deleted or rectified upon request.
- Instruct employees to comply with such privacy policies and avoid activities that enable or facilitate illegitimate or unauthorized access in terms of IDPPs.

# International Data Privacy Principles

- Do not use or divulge any customer data (except for statistical analysis and when the customer's identity remains anonymous), unless the company is obliged to do so by law or the customer agrees to such use or circulation.
- Do not collect customer data if such collection is unnecessary or excessive.
- Use or divulge customer data in a fair way and only for a purpose related to activities of the company.
- Do not outsource customer data to third parties unless they also comply with standards comparable to these IDPPs.

# International Data Privacy Principles

- Announce data breaches relating to sensitive data.
- Do not keep personal data for longer than necessary.
- Do not transfer personal data to countries with inadequate or unknown data protection standards unless the customer is informed about these standards being inadequate or unknown and agrees to such a transfer.

# International Data Privacy Principles

- In the case of a contract between the company and the customer in which the customer commits to pay for services or goods:
    - Inform the costumer individually and as soon as reasonably possible in the event of a data breach.
    - Inform the customer upon request about which specific data are stored, and delete such data upon request unless applicable laws or regulations require the company to continue storing such data.
    - Do not use or divulge content-related personal data.
    - Do not use or divulge any other personal data without the customer's explicit, separate and individual consent.
    - Do not store, use or divulge any customer data, unless applicable laws or regulations require the company to continue storing such data.
- In the absence of a contract between the company and the customer in which the customer commits to pay for services or goods:
    - Inform the customer as soon as reasonably possible in the event of data breaches.
    - Inform the customer upon request what types of sensitive data are stored and delete such data upon request when such data are outdated, unless applicable laws or regulations require the company to continue storing such data.
    - Do not use or divulge sensitive data without the customer's explicit, separate and individual consent.

# Artificial Intelligence

- Overview of the EU AI Act
  - https://artificialintelligenceact.eu/
  - The EU AI Act is the world's first comprehensive AI legislation, focusing on protecting individual rights, democracy, and environmental sustainability.
  - It adopts a risk-based approach, categorizing AI systems as Prohibited, High-Risk, or General-Purpose AI, with increasing regulatory scrutiny for higher risks.
  - Companies operating in the EU, including Australian firms, must comply with the Act.
- Whitehouse Executive Order
  - https://ai.gov/actions/

# Implications and Compliance

- Australian companies may be affected when selling AI-related products to the EU.
- Prepare by conducting AI audits, assessing data flows, and ensuring compliance with privacy, security, and AI ethics.
- Fines for non-compliance can be severe.
- Proactive steps are essential.
- Teraflops based regulation
  - 10^25 – UK
  - 10^26 - US

# Thank you

LA TROBE UNIVERSITY

Centre for
Data Analytics
and Cognition

http

LinkedIn

Scholar