Modern Powerhouses of AI

Part 2: Case Studies & Collecting Data

What We'll Cover

- Case Study: The Evolution of Game-Playing AI
- Case Study: AlphaFold, Solving a 50 Year Old Problem
- Case Study: AI in Policing, Promise & Peril
- From Examples to Infrastructure, Data, Training & Deployment

Case Study: Game-Playing AI

Why Games Matter

- Games and game playing is a perfect testbed for AI
- They have:
  - Clearly-defined rules
  - Easily-measurable performance and success (win/lose)
  - Easy to compare to human performance
- Can a machine beat the very best human game players?

Image from: https://www.scientificamerican.com/article/20-years-after-deep-blue-how-ai-has-advanced-since-conquering-chess/

Chess Computers

Chess computers in the 1990s effectively brute-forced millions of possible combinations of moves

Trees of possible moves, and then search algorithms to find the next best move

IBM's Deep Blue computer could evaluate 200 million moves per second

In 1996, Deep Blue beat Garry Kasparov in their first game, before ultimately losing that match

In 1997, with upgraded hardware (2x as fast), Deep Blue beat Kasparov

How Deep Blue Worked

Deep Blue simulated the next possible moves for each player, and then for each of those moves all of the possible subsequent moves, and so on

This is a "game tree"

A search algorithm then evaluated the best moves, with moves that resulted in pieces being captured being penalised

It did this *really* fast

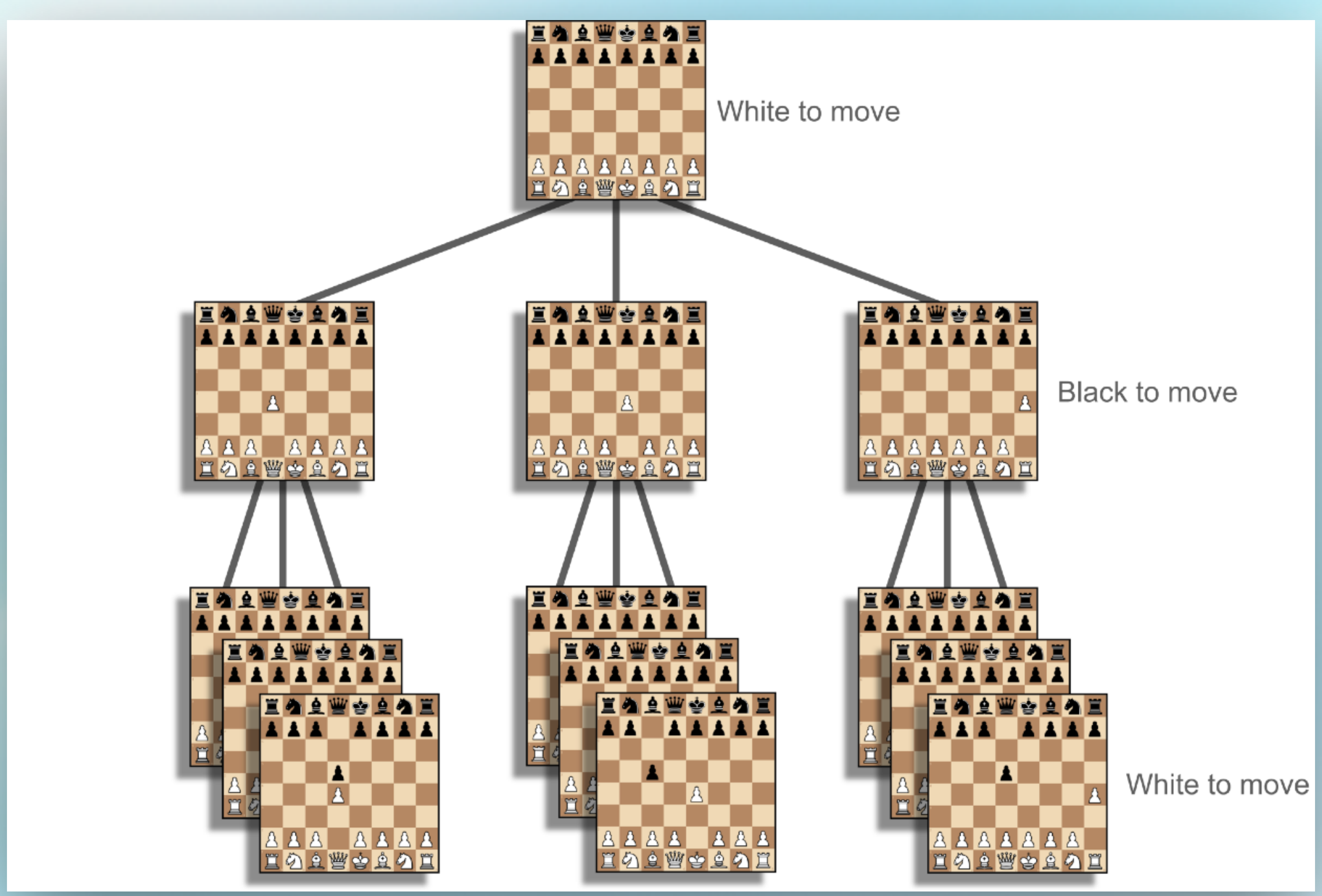


Image from https://roshan818.github.io/projects/chess/

Question:

Why is the game of Go a harder challenge?

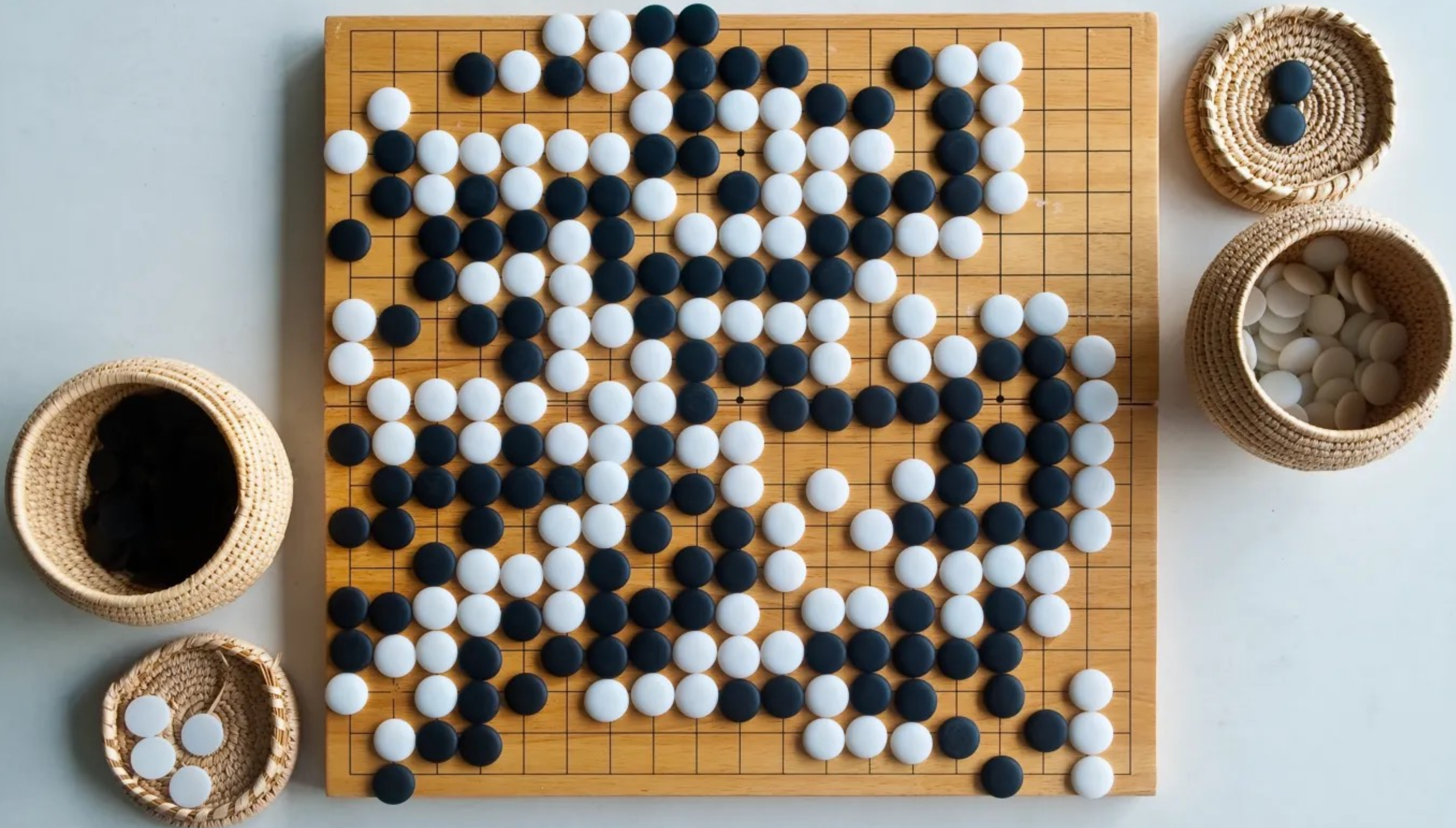


Image from https://fortune.com/2016/01/27/google-deepmind-chinese-go/

The Game of Go

An ancient Chinese game, played on a 19x19 grid, with black and white pieces

The larger board, and less constrained moves, means that there are more possible board arrangements than atoms in the universe!

Not tractable to brute-force possible moves, like Deep Blue did with chess

How could a computer beat a human player?

Deep learning was the answer!

AlphaGo

AlphaGo from Google DeepMind beat Lee Sedol, a 9-dan Go player, 4-1 in 2016

AlphaGo used deep neural networks and reinforcement learning to estimate the win probability of each move

Trained on data from millions of human and computer games

Image from https://www.theguardian.com/technology/2016/mar/15/alphago-what-does-google-advanced-software-go-next

AlphaGo Zero

Rather than being trained on real game data, AlphaGo Zero in 2017, started from scratch simulating games itself to learn the best strategies

In 40 days, it became better than any previous version of AlphaGo

It was able to find strategies never used by humans

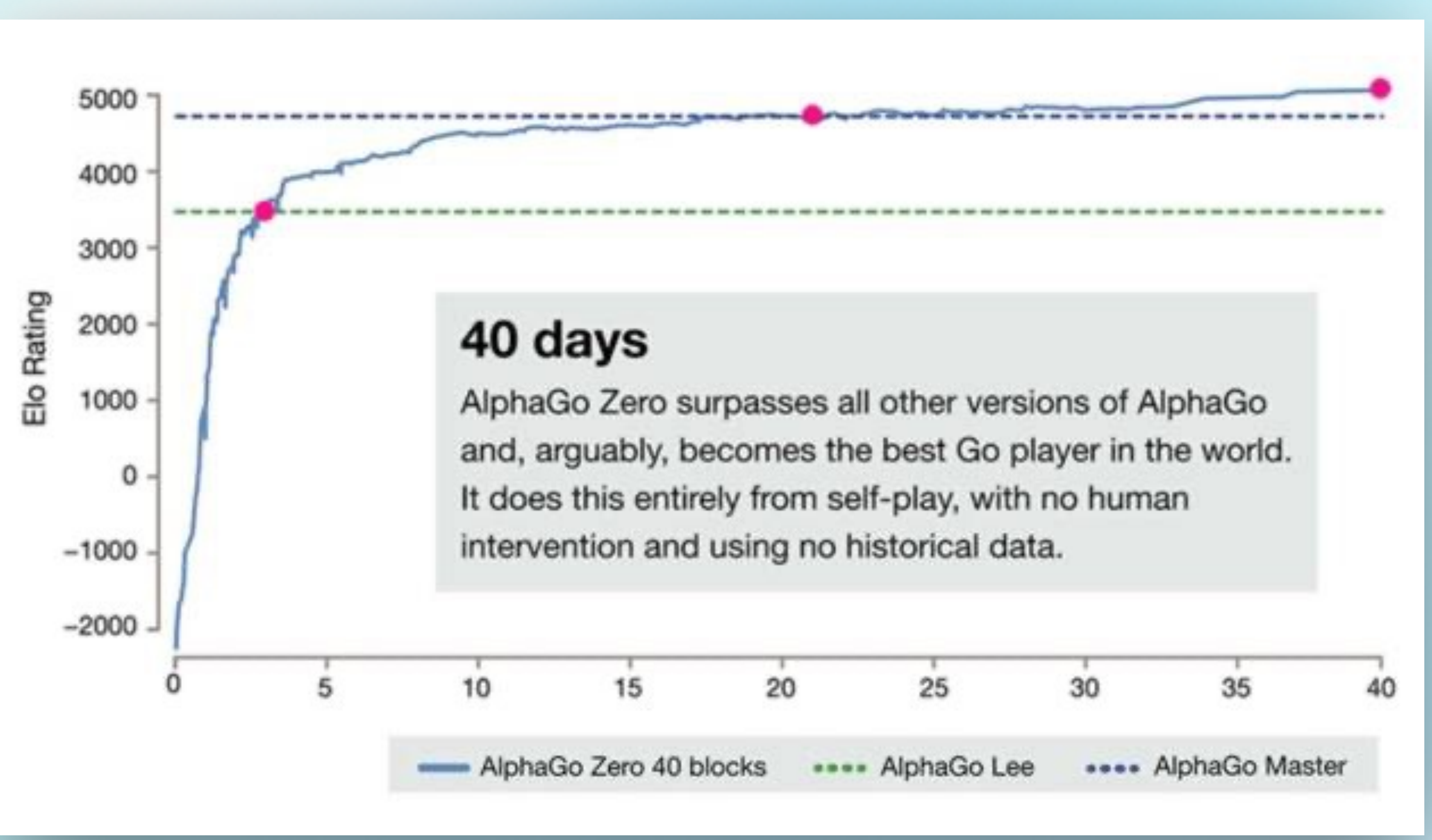


Image from https://www.i-programmer.info/news/105-artificial-intelligence/11228-alphago-zero-from-nought-to-top-in-40-days-.html

From AlphaGo to AlphaZero

The same strategy used for AlphaGo Zero (learning from scratch) was used to make AlphaZero in 2017

AlphaZero* could play Go and also chess and Shogi

After only a few hours of training, it could beat the leading computer Go, chess, and Shogi engines

This self-learning approach was a crucial moment

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

Case Study: AlphaFold

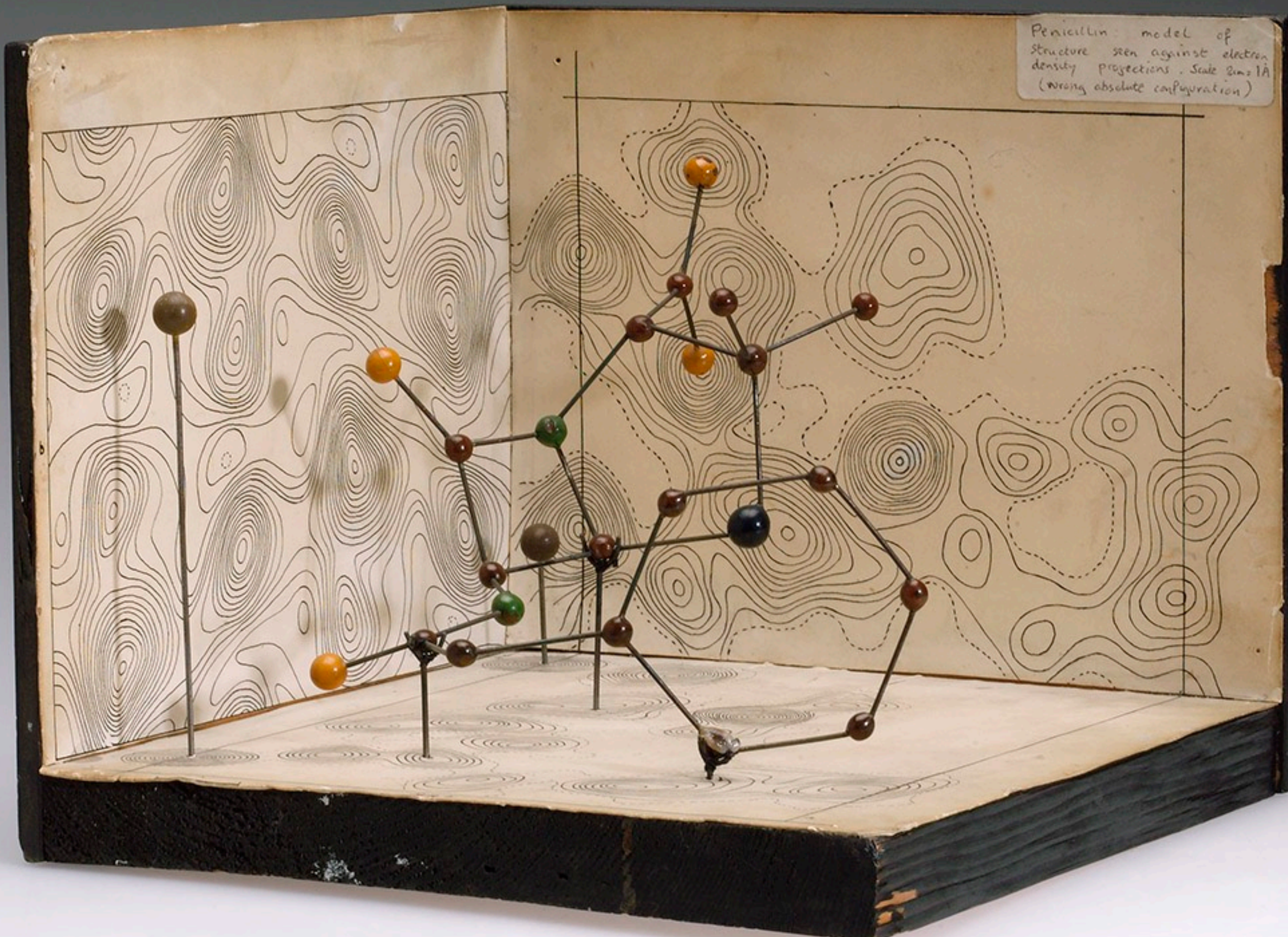


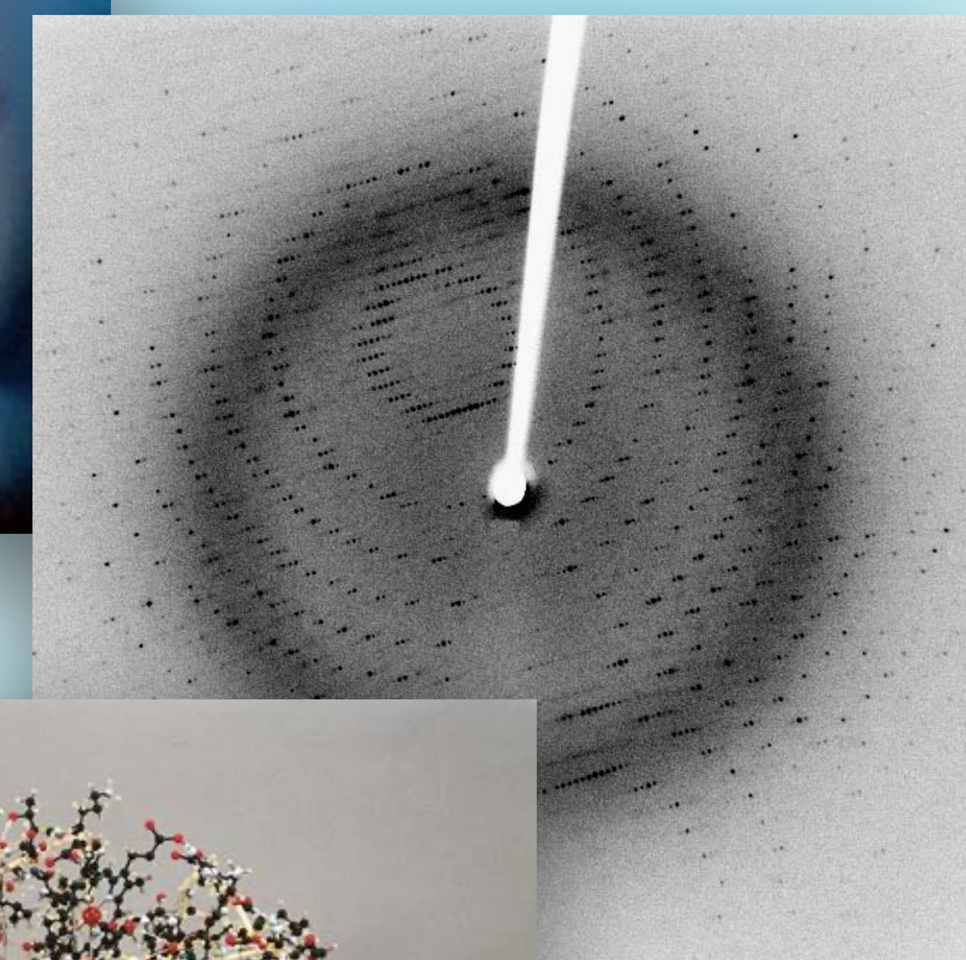
Image from https://en.wikipedia.org/wiki/Dorothy_Hodgkin

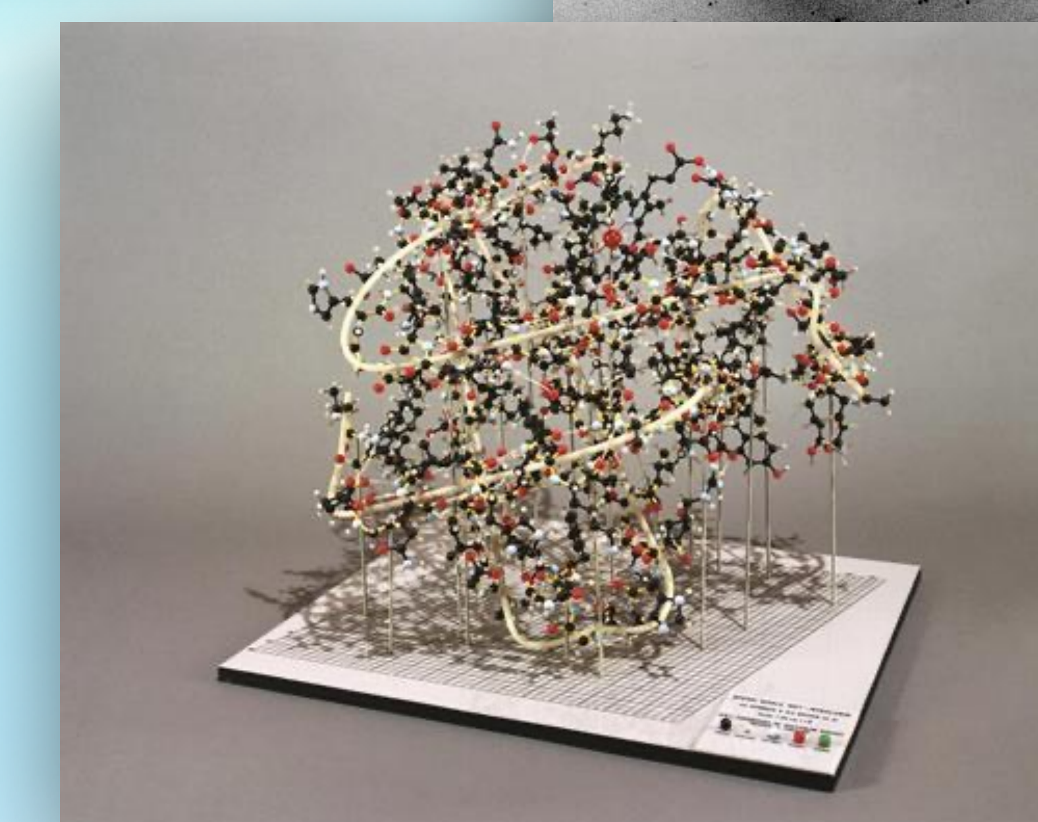
The First Molecular Structures

From 1937 to 1969, Dorothy Hodgkin pioneered the use of **X-ray crystallography** to solve the structures of cholesterol, penicillin, vitamin B12, and insulin

In 1958, John Kendrew solved the first protein structure, myoglobin

Both Hodgkin and Kendrew won Nobel prizes in chemistry





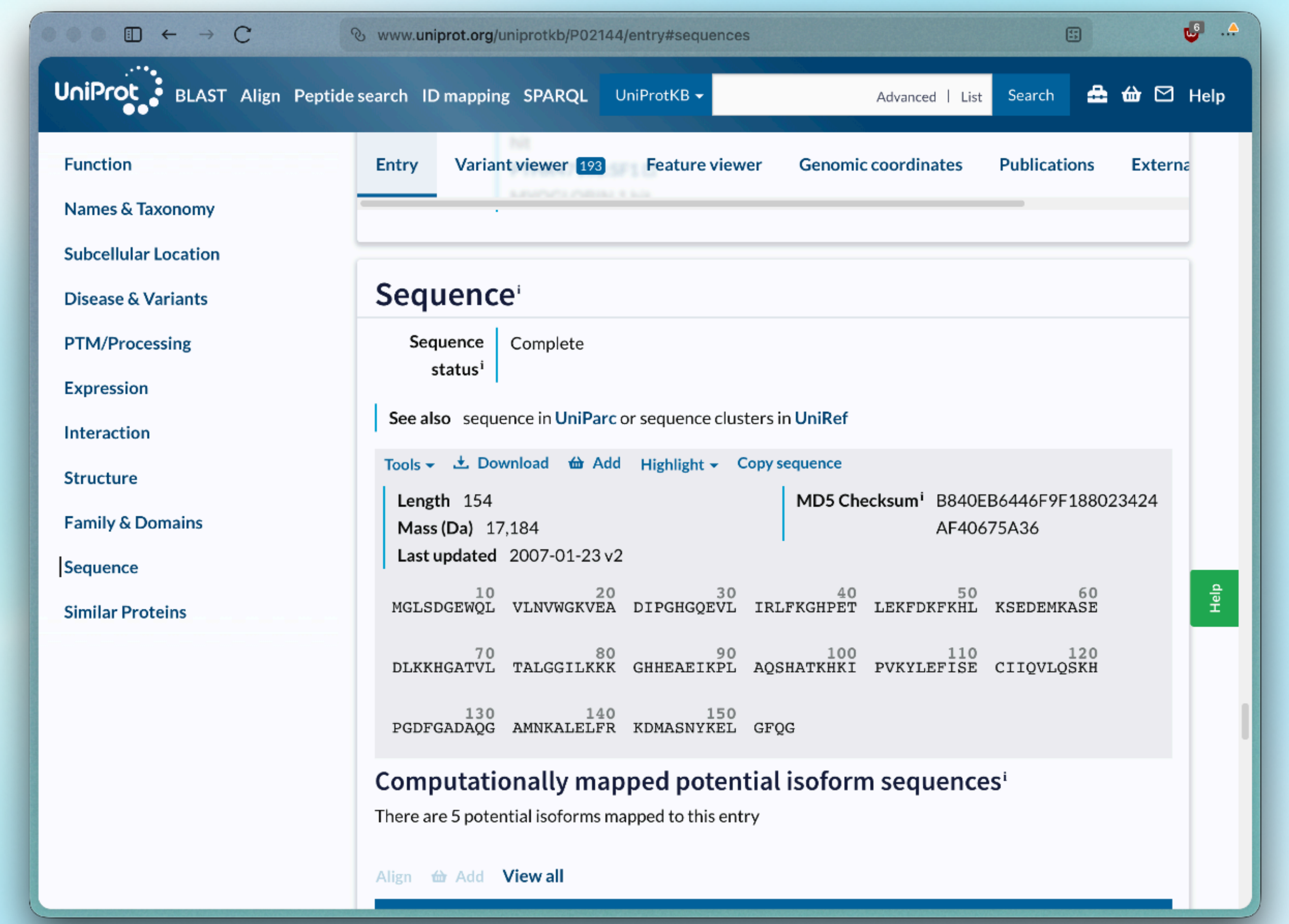
https://en.wikipedia.org/wiki/X-ray_crystallography

The Protein Folding Problem

How do we go from a sequence of amino acids to a folded, 3D protein structure?

Until recently, the only was by X-ray crystallography or cryo-EM and a huge amount of work to solve the structure

These were deposited in the Protein Data Bank (PDB), 100s of thousands of them



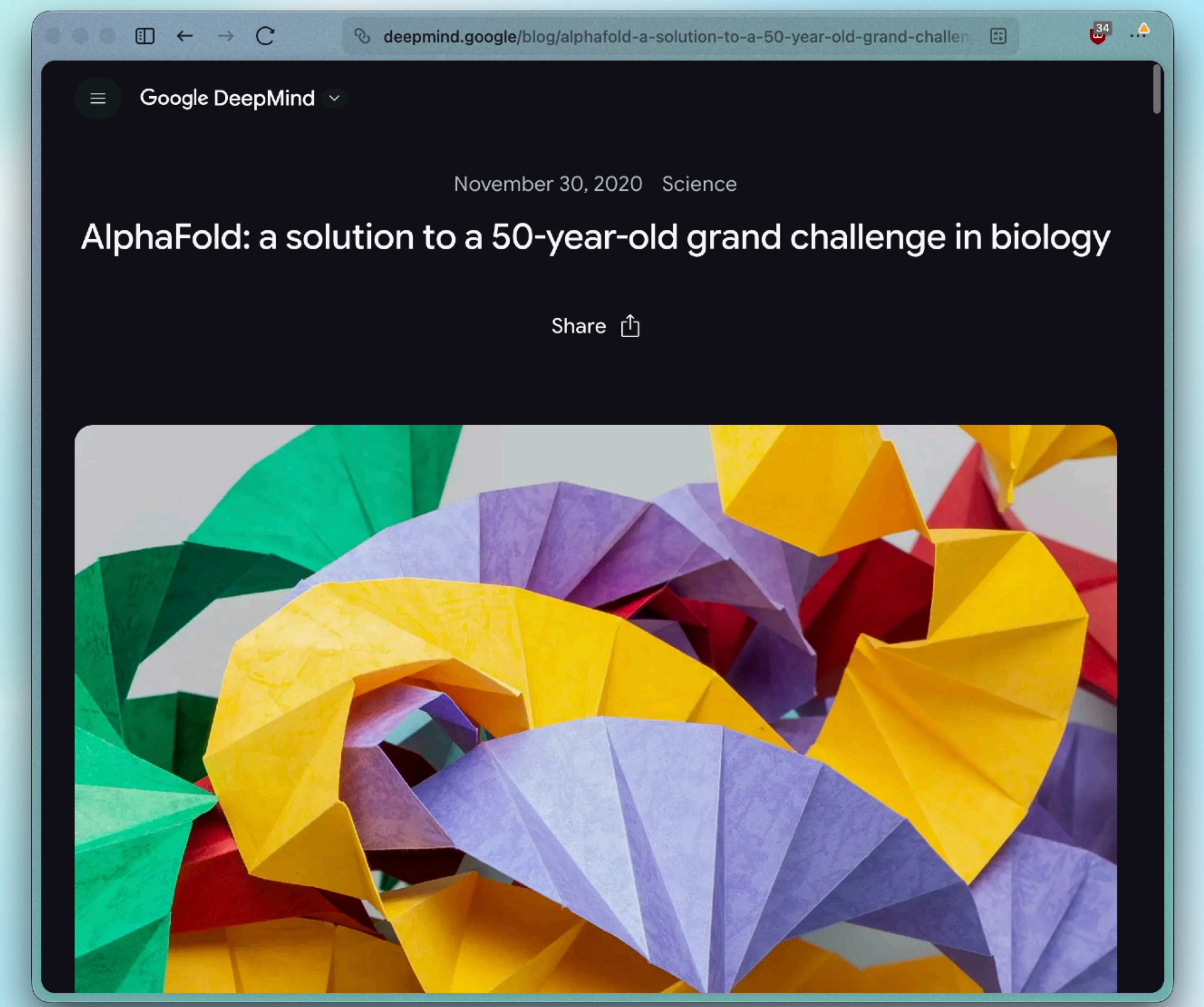
https://en.wikipedia.org/wiki/X-ray_crystallography

AlphaFold

AlphaFold2 won the 2020 CASP14 competition

It was able to predict structures, from their sequence alone, with comparable accuracy to X-ray crystallography structures

Won the 2024 Nobel prize for chemistry



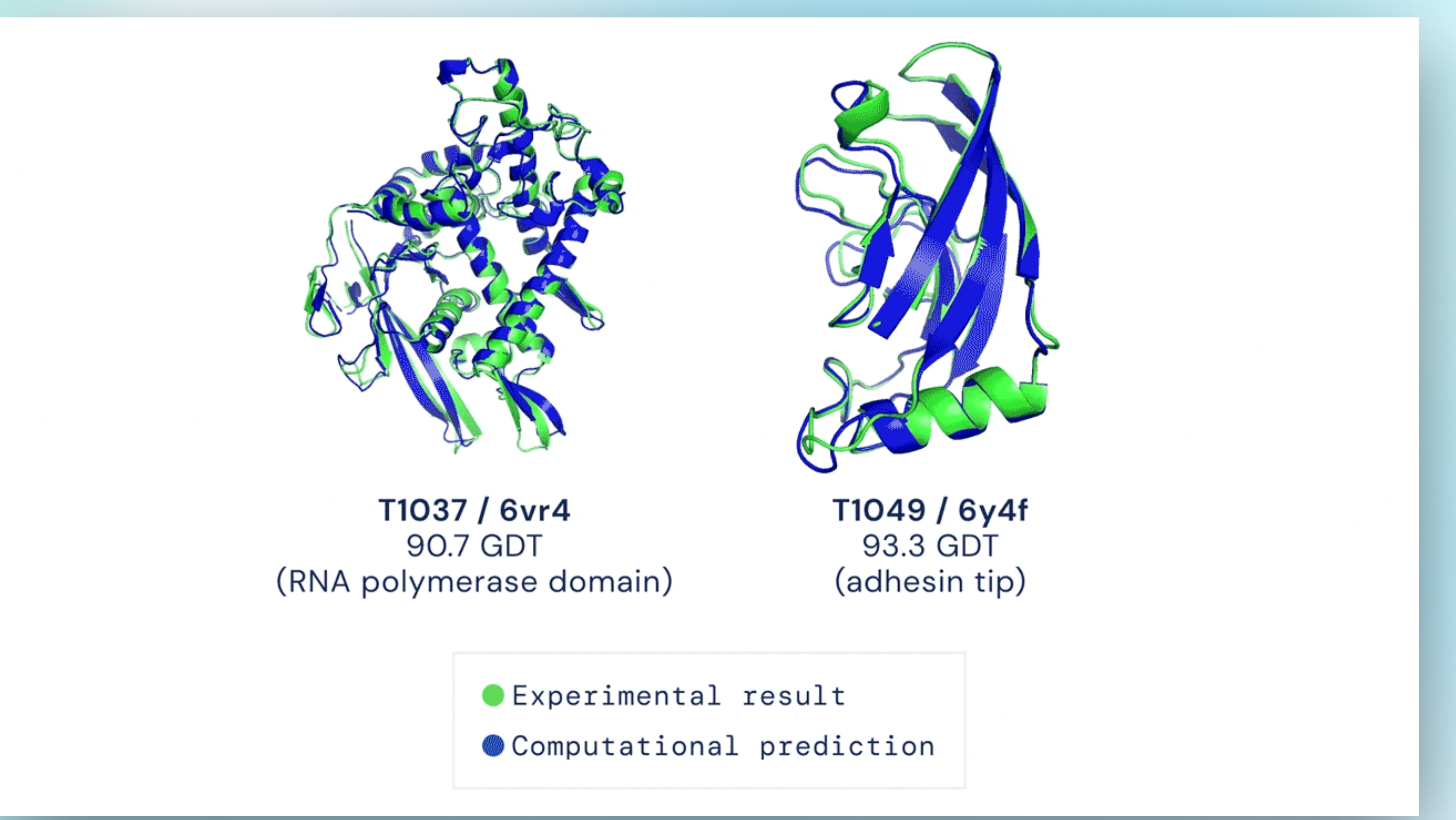
https://deepmind.google/blog/alphafold-a-solution-to-a-50-year-old-grand-challenge-in-biology/

AlphaFold

They used the ~170,000 protein structures in PDB to train AlphaFold

It uses a transformer-based deep neural network similar to LLMs to learn the relationships between amino acid sequence and 3D structure

It learned the "grammar" of proteins



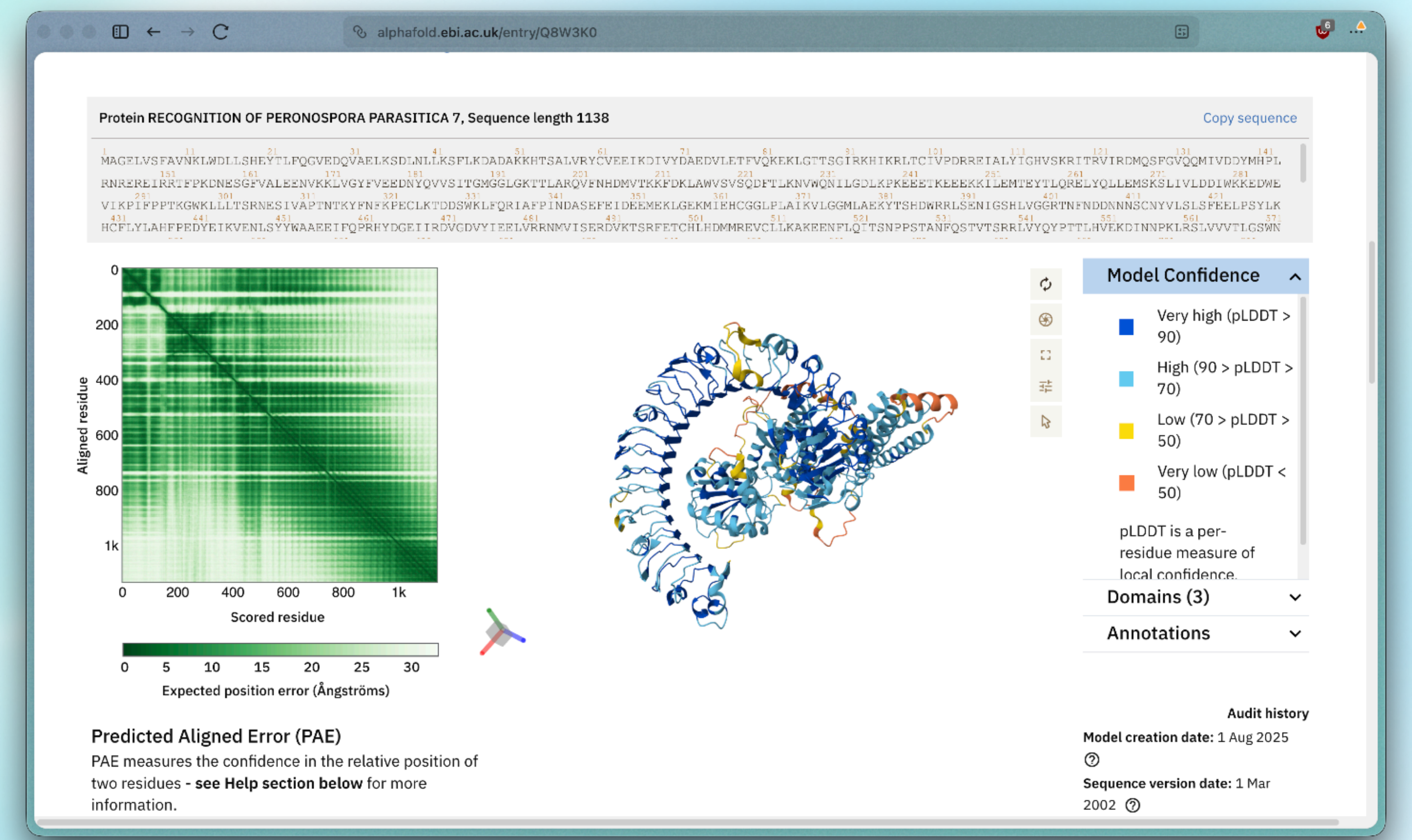
https://deepmind.google/blog/alphafold-a-solution-to-a-50-year-old-grand-challenge-in-biology/

AlphaFold's Impact

AlphaFold has now predicted more than 200 million protein structures

Software is open-source, and free to use

Huge impacts on drug design, understanding of disease, and protein engineering



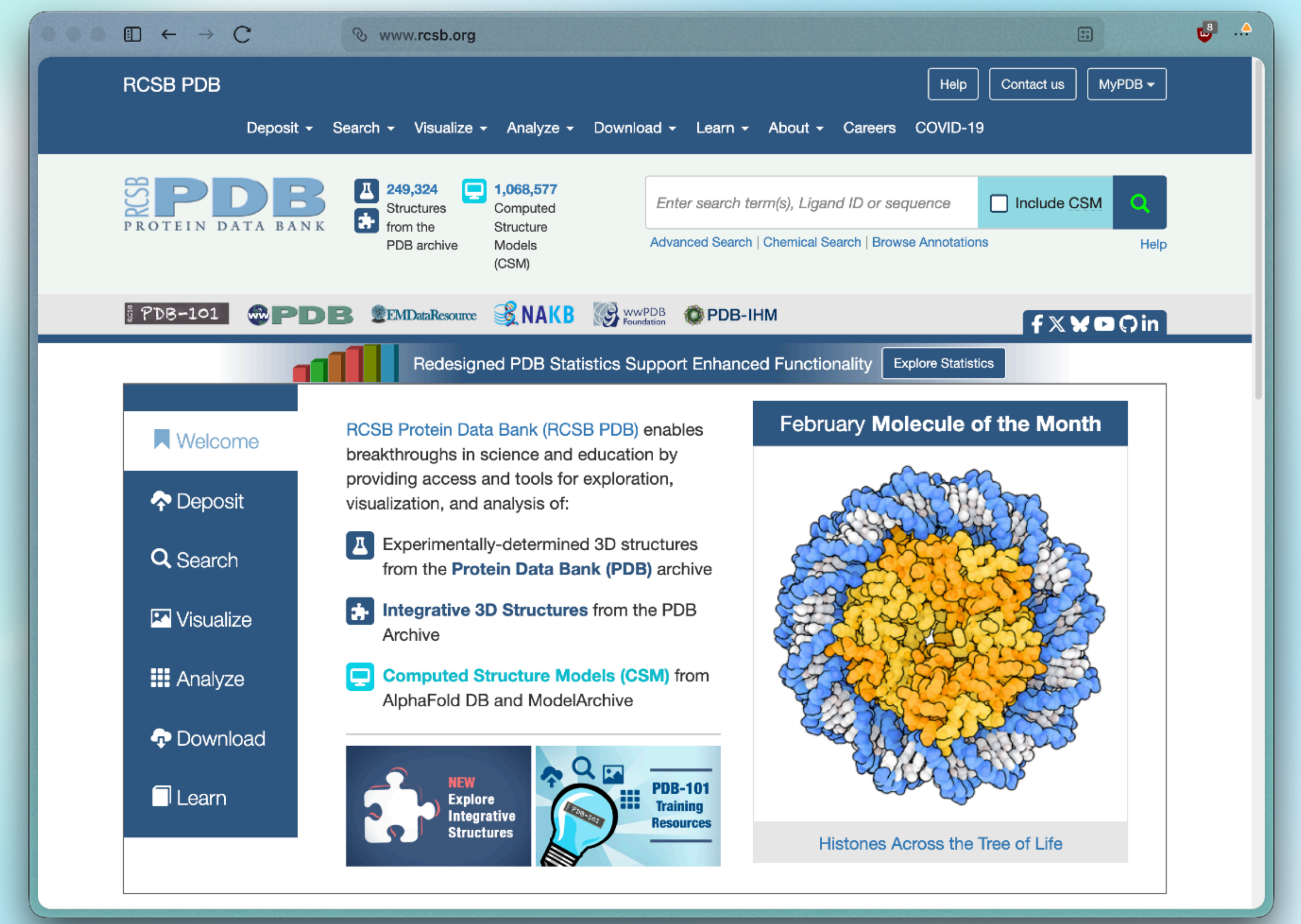
https://alphafold.ebi.ac.uk/

Impossible Without PDB

AlphaFold built on a legacy of 50 years of painstaking work by researchers solving protein structures in PDB, and sequencing of DNA and proteins

A prime example of deep learning training data needing to be both vast and very high quality

More on that later...



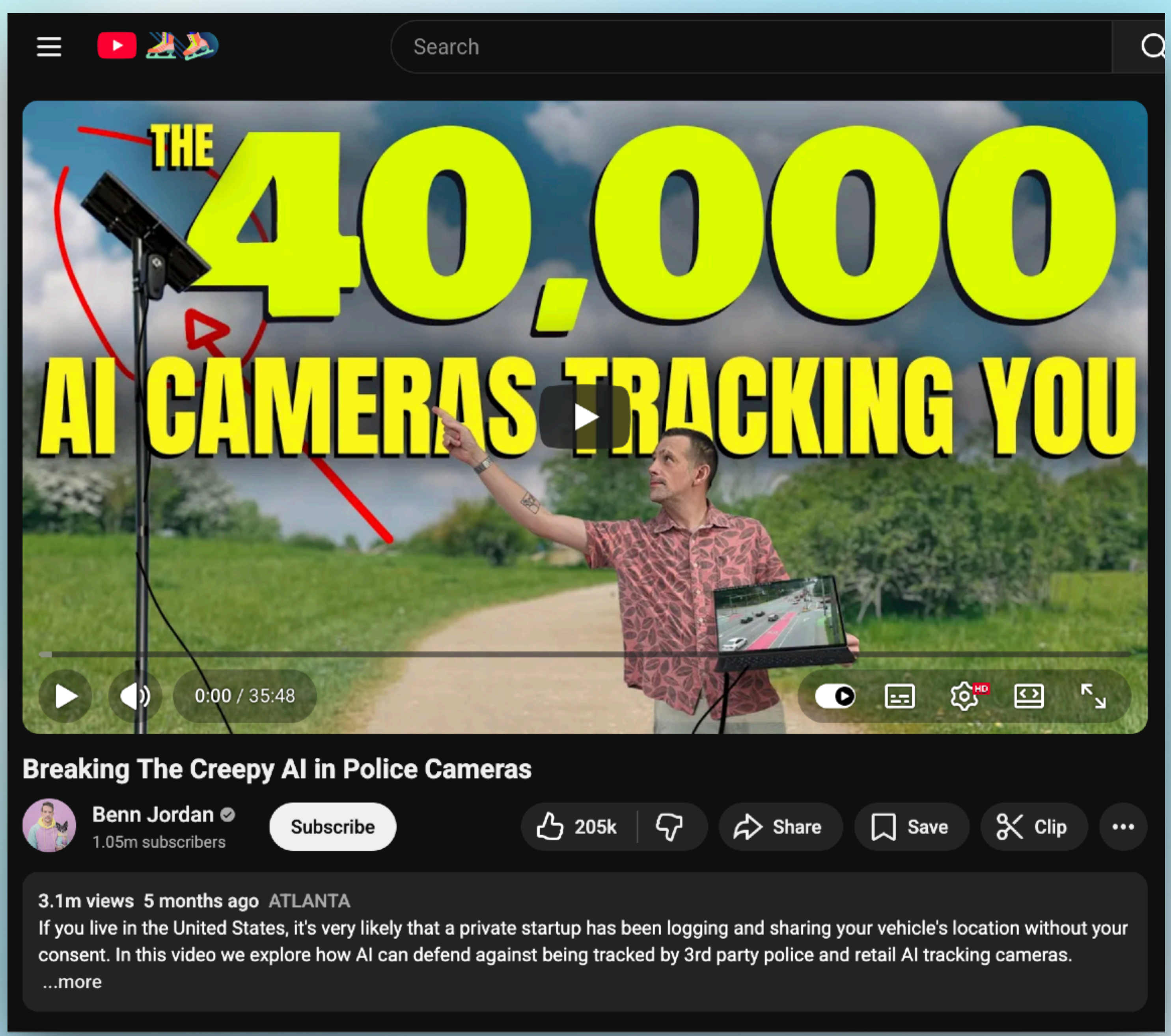
Case Study: AI in Policing

AI in Policing

AI is increasingly being used in policing

One of its most controversial uses, with significant concerns around privacy

Predictive policing, facial recognition, and ANPR are key areas



* https://www.youtube.com/watch?v=Pp9MwZkHiMQ

Predictive Policing

PredPol, now called Geolitica, is a predictive policing company out of LAPD

Uses historic data on crime and other factors to direct policing to certain areas

Concerns that this will lead to over-policing and to more arrests in those areas, i.e. a positive feedback loop

Concerns over effectiveness also


www.wired.com/story/plainfield-geolitica-crime-predictions/

WIRED

NEWSLETTERS SUBSCRIBE

AARON SANKIN SURYA MATTU SECURITY OCT 2, 2023 10:00 AM

Predictive Policing Software Terrible at Predicting Crimes

A software company sold a New Jersey police department an algorithm that was right less than 1 percent of the time.

The intersection of technology, power, and culture. START FREE TRIAL

* https://www.wired.com/story/plainfield-geolitica-crime-predictions/

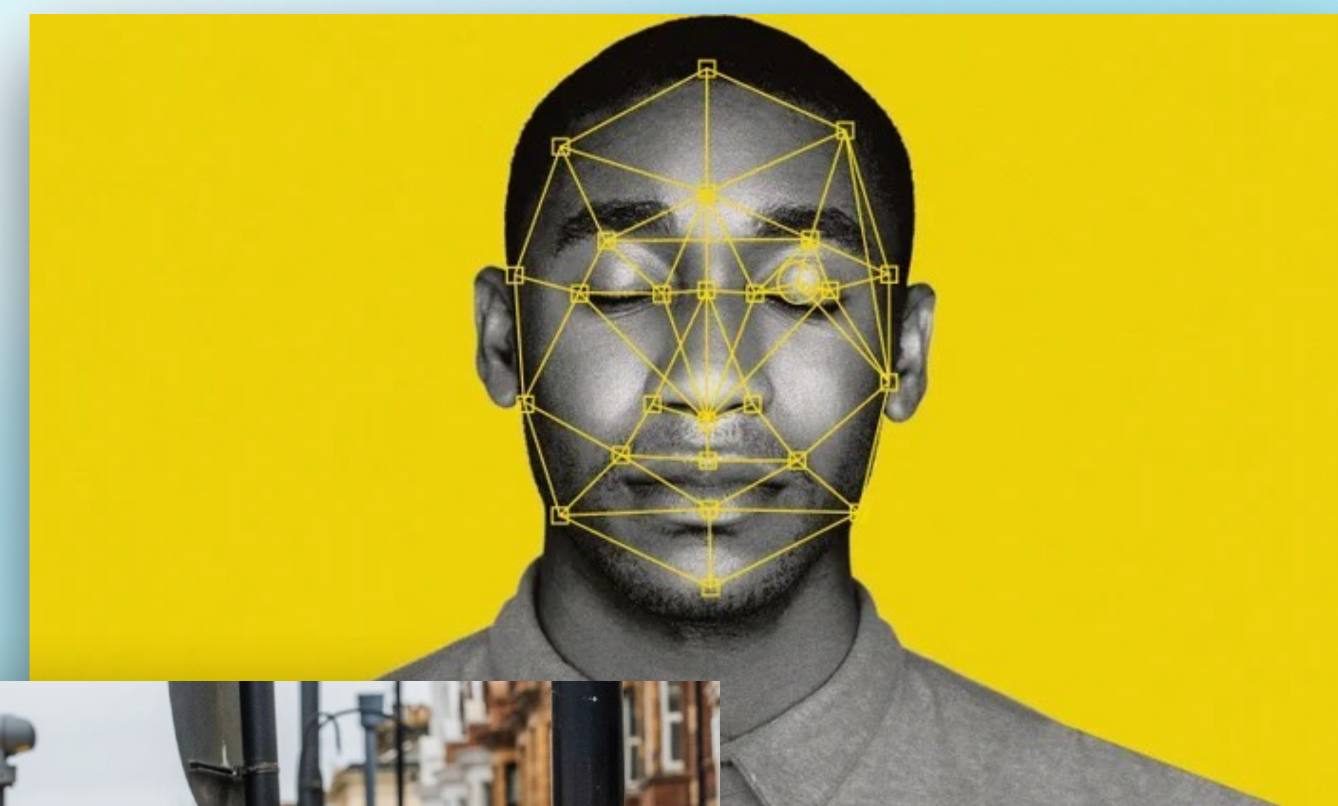
Facial Recognition

AI picks out key facial features and then matches against databases to identify suspects

Increasingly used for live facial recognition at events and protests

Concerns around what happens with collected data, and the scale of it

Proven to be less accurate at matching darker skin tones due to training biases



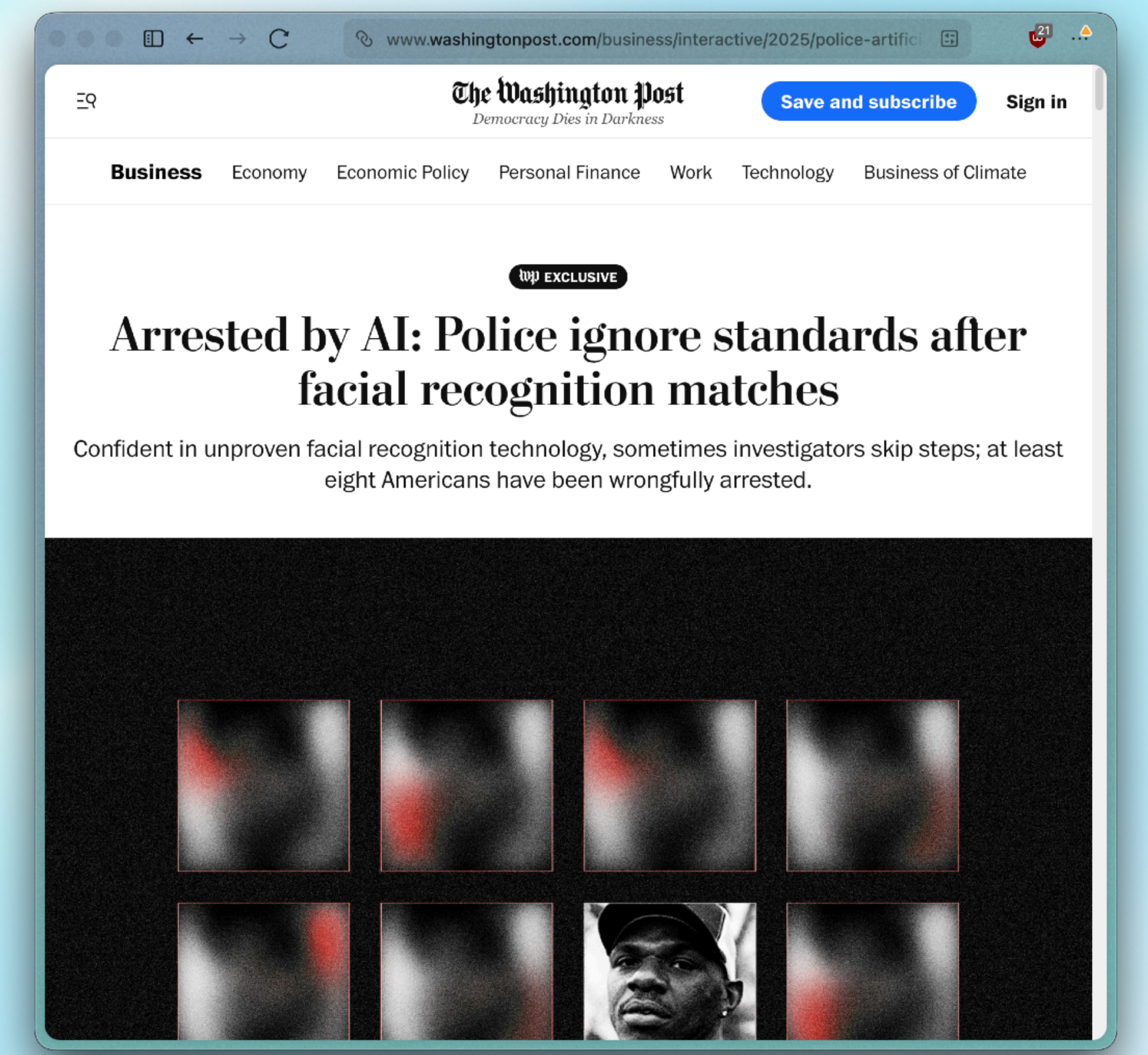
* https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it

Real World Impacts

Met. Police say facial recognition led to 1,300 arrests over two years

In South Wales, a criminal who was recalled to prison was identified by CCTV after walking past officers unnoticed

However, federal studies showed that Black and Asian people are 100x more likely to be misidentified than white people



* https://www.gov.uk/government/news/government-pledges-to-ramp-up-facial-recognition-and-biometrics
https://www.nec.com/en/press/201707/global_20170711_01.html
https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition/

Question:

Should police be allowed to use AI facial recognition? What safeguards would you want?

Bias and Ethical Concerns

Training data for AI-based policing reflects historic biases in human policing, whether that is towards deprived areas or towards specific races

The vast scale of surveillance data that is being collected raises concerns around civil liberties, e.g. Ed Bridges' case against South Wales Police and their resulting pause on live surveillance before improving (and indeed proving) its effectiveness

Is the data collected sufficiently secure and adhering to e.g. GDPR?

From Examples to Infrastructure, Data, Training & Deployment

Question:

Thinking about the examples we've seen, what determines how data is stored, and the level of data security?

Basic Model Training Process

1. Data collected
2. Data cleaned and labelled
3. Model trained (billions of parameters to minimise errors)
4. Model performance evaluated and tuned

This is the compute, time, energy-consuming part. Models like AlphaFold, AlphaGo, and the major LLM platforms took massive compute and months to train.

Where does the data come from?

With Deep Blue and AlphaGo, this was relatively easy: collect data from games

For AlphaFold, there was the benefit having large amounts of standardised, high quality data in databases like PDB and UniProt, and NCBI's databases

LLMs like ChatGPT and Claude use data scraped from the web. Issues with quality, reliability (trusted sources?), and bias of data.

With historical crime and policing data, bias is a particular issue

Where does the model run?

Where the model runs determines where inference data must be sent

Models can be **local**, **edge**, or **cloud-based**

A **local model** runs on a machine your own network (we'll see this in Coding Exercise 3), e.g. TinyLlama or Qwen running with Ollama. **Inference data stays local**.

An **edge model** runs on dedicated tensor-processing units (TPUs) or AI cores on a device like your phone. These can run *really fast!* **Inference data stays local.**

A **cloud model** runs on an unspecified cloud server in a data centre (e.g. AWS or Google Cloud). **Inference data must be sent to these servers.**

Cloud AI

LLM AI models like ChatGPT, Claude, and Gemini run in data centres, on "the cloud"

Advantages: huge compute power, always maintained and up to date, no local hardware needed

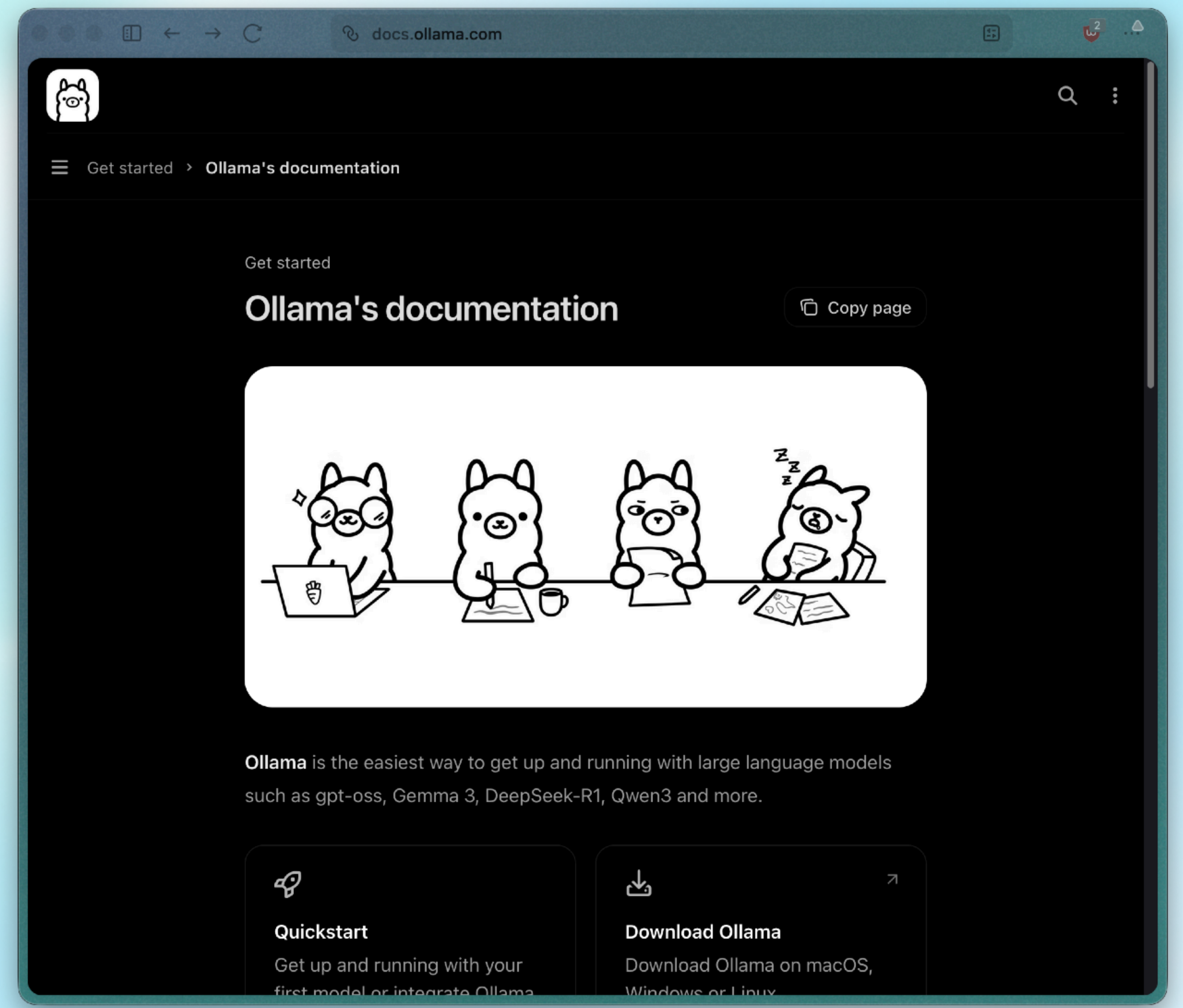
Disadvantages: data security (sent to servers), requires internet, cost

Local AI

Software like Ollama, TensorFlow/Keras, or PyTorch, can run local models

Advantages: privacy (data is kept local), free, can run offline and air-gapped

Disadvantages: hardware limitations, smaller/less capable models, ongoing maintenance needed



Edge AI

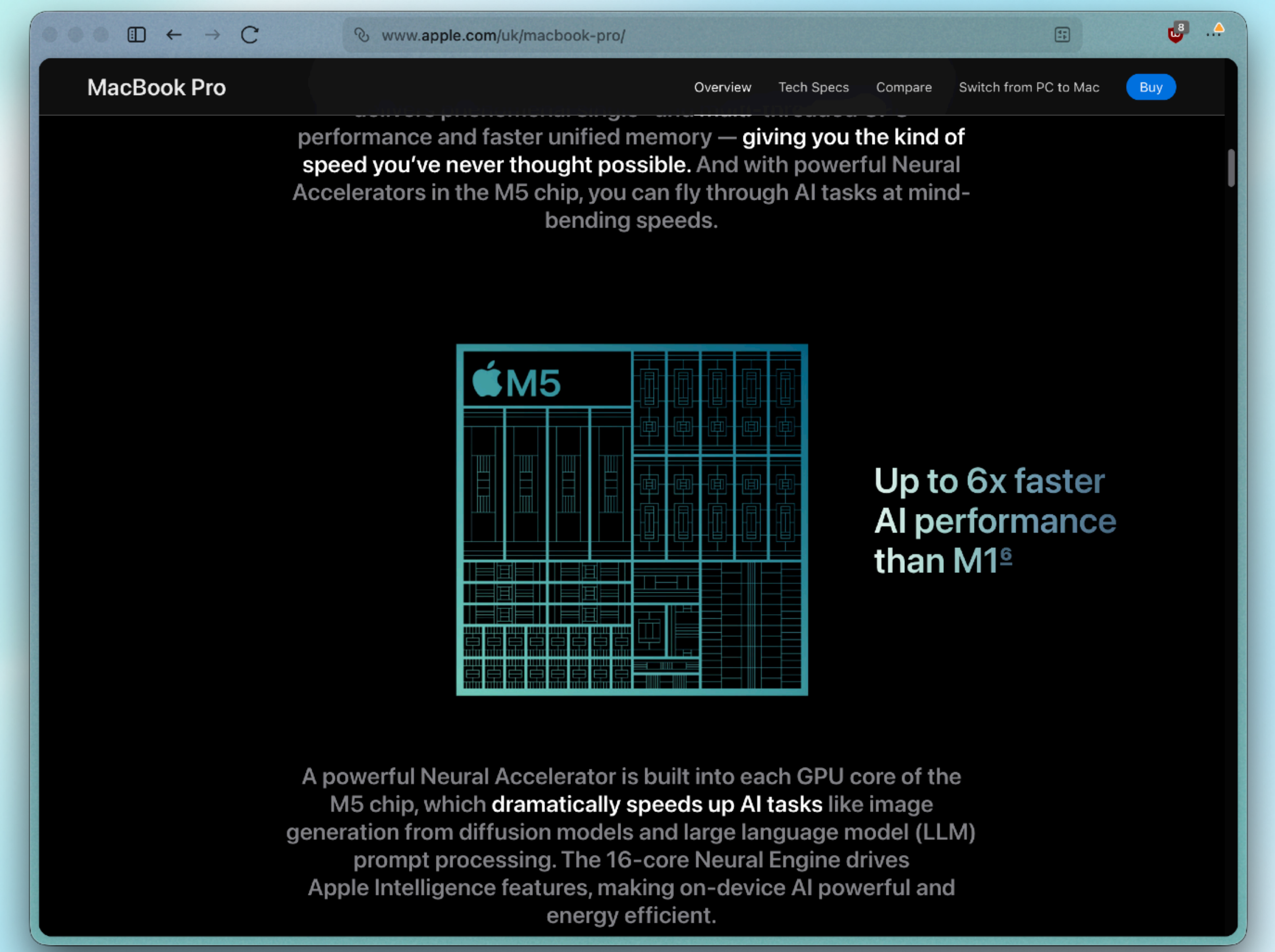
These are dedicated GPU or TPU cores, designed for running AI models on-device

Examples include: Face ID, Touch ID, AI image processing on your phone, object detection in autonomous cars

Advantages: super-fast, local and private

Disadvantages: hardware limitation, model size, usually for dedicated tasks

Also hybrid edge/cloud solutions like Apple's Private Cloud Compute



Question:

For your own research, which deployment method would you trust, especially with sensitive data?

The Big Picture

AI's power comes from training and inference data, and from compute

Where it runs determines who controls it and who has data governance

We'll think more about these ethical issues in the next Breakout Session...