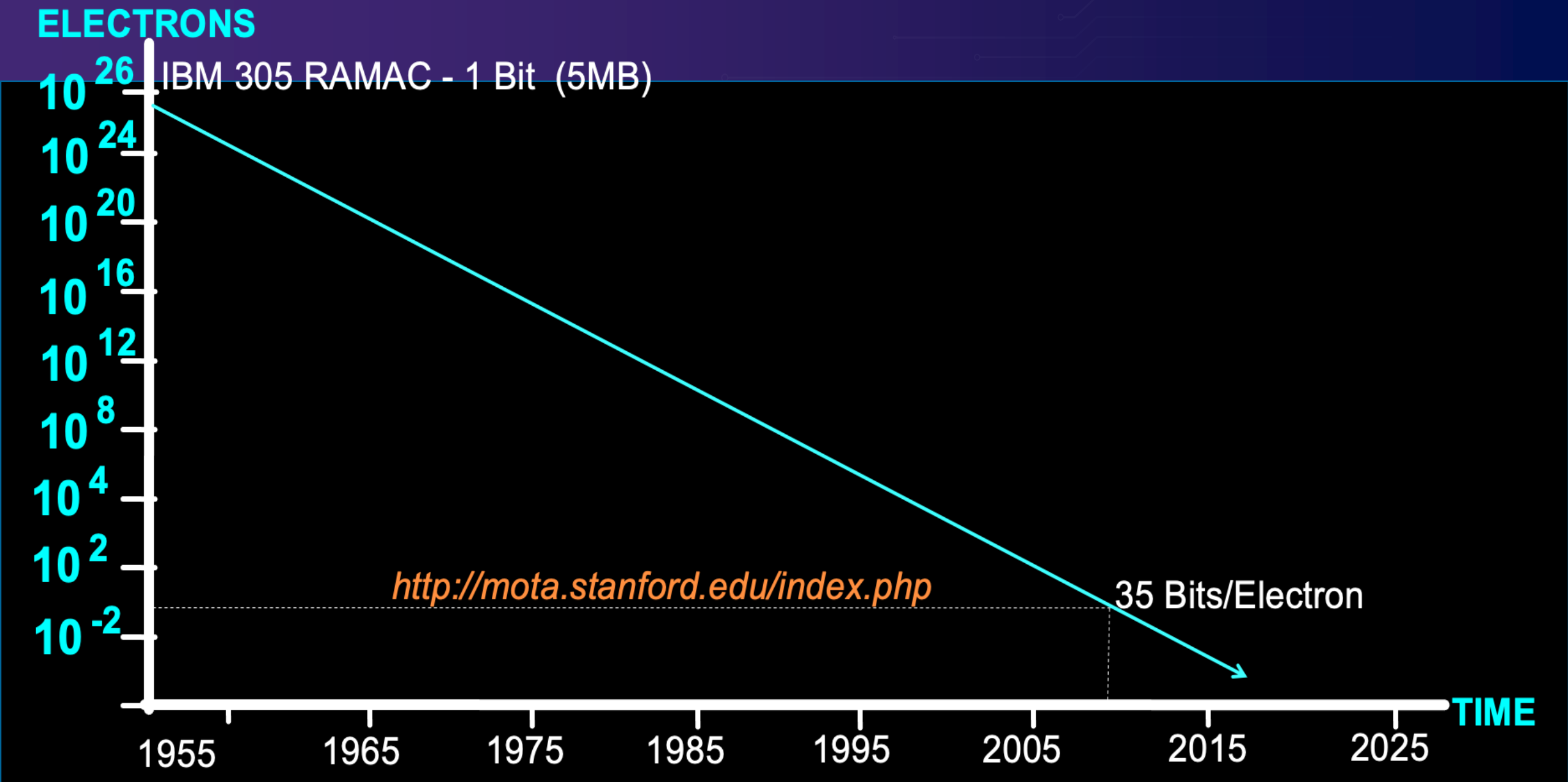
Permion

Security, Integrity, and Trust in HPC Artificial Intelligence

Bits / Electron → Future Devices → Bigger, Better, Faster Analytics



Assumption

Modern Analytics needs AI

Analytics: Data at Rest, Data in Transit, Data in Use

ANALYTICS

Data Poisoning

Data at Rest

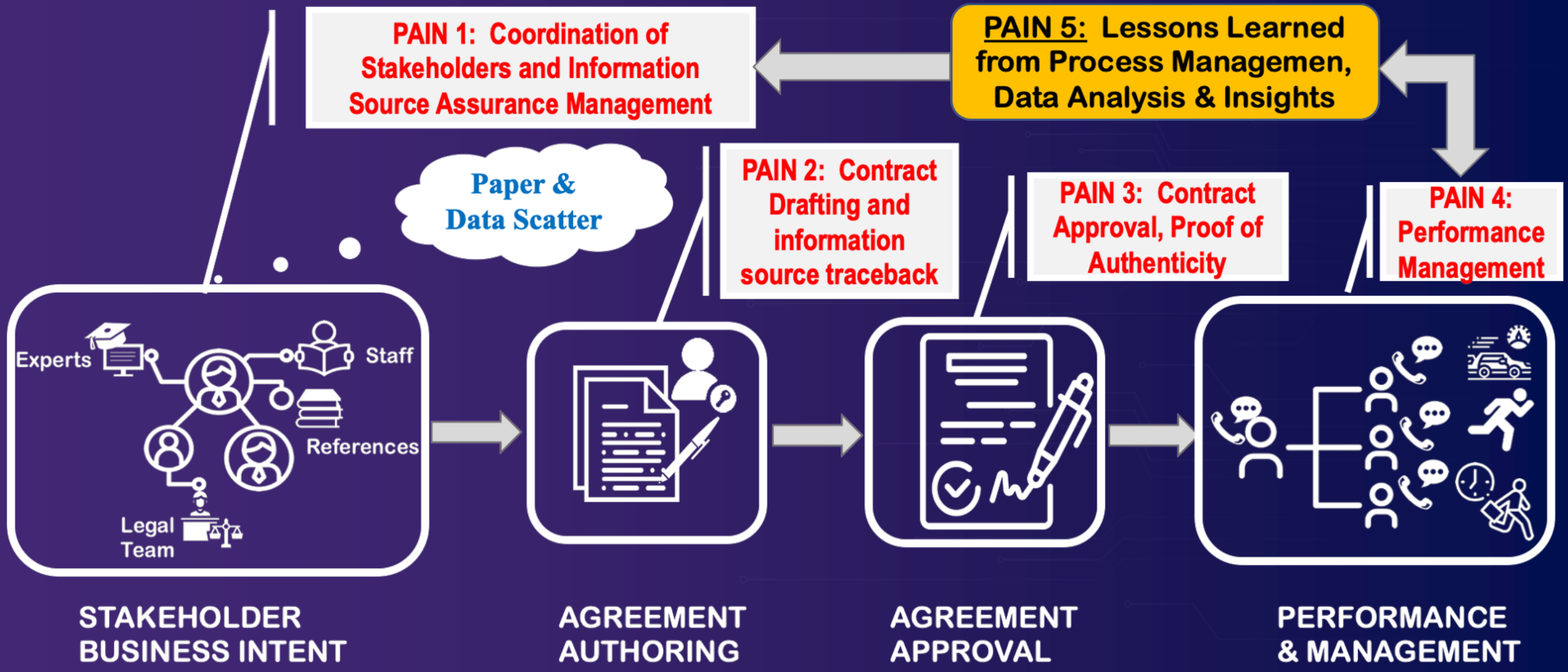
Data Corruption

Data in Transit

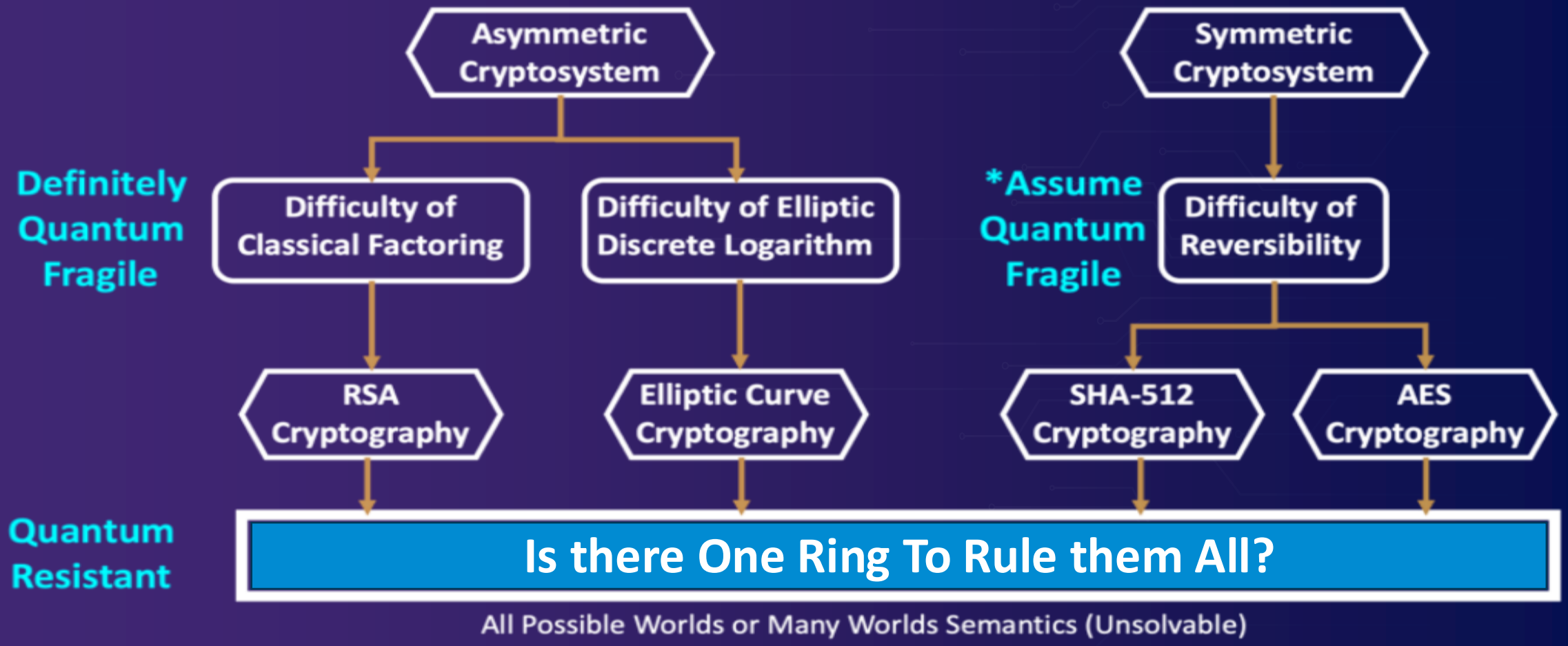
Fake Data

Data in Use

Example of a Legal Process – Risks from the Processes

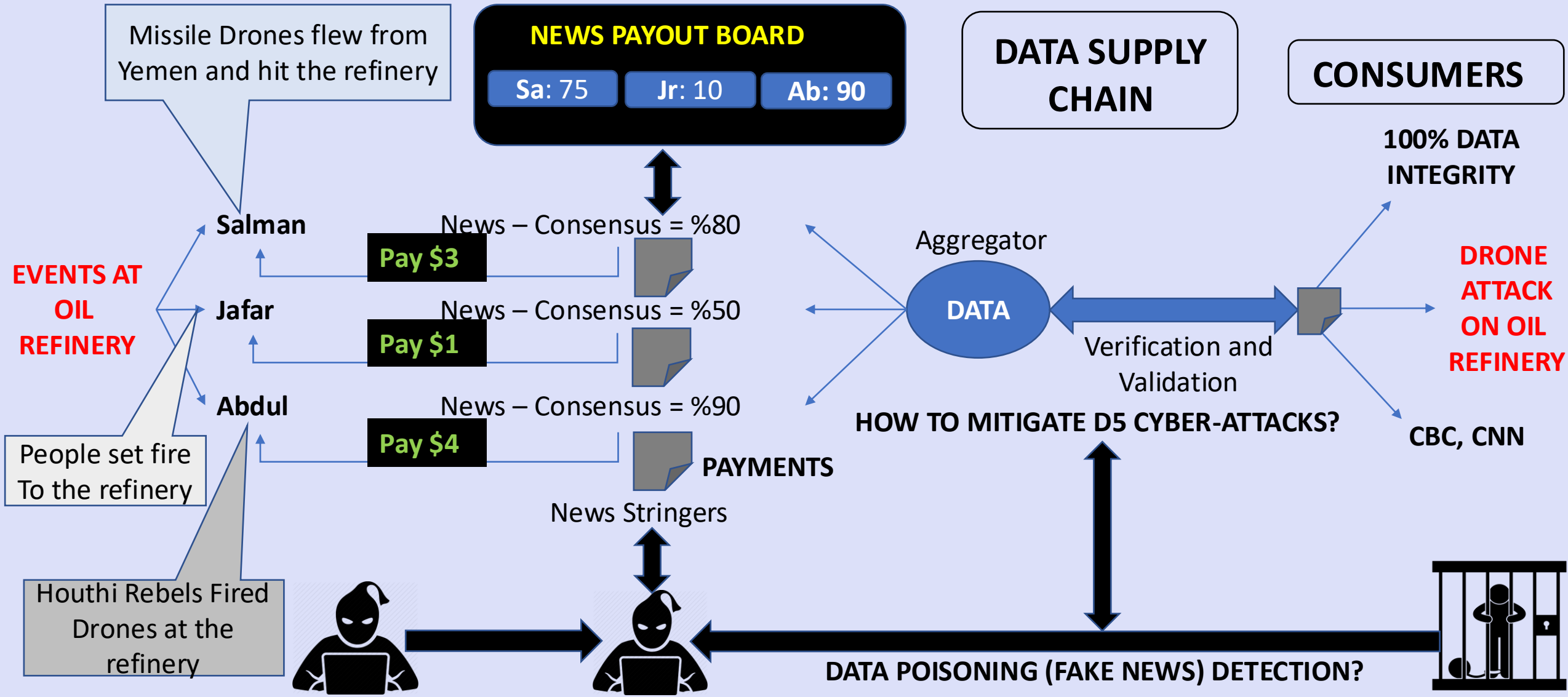


Security of Data at Rest, In Motion and In Use – Risks in Confidentiality



*If multi-entanglement in multiple-degrees of freedom is technologically scalable then the search space of solutions is reduced by orders of magnitude speedup in Grover's Search and the one-way hash becomes vulnerable. **Else the hash is quantum resistant.** For recent developments that may produce hash vulnerability, see: https://www.nature.com/articles/ncomms13514

Supply Chain – Multi-Source – Risks in Integrity



AI is Revolutionizing Analytics, but . . .

Permion

But tools such as ChatGPT threaten transparent science; here are our ground rules for their use – "*Nature*"

GPT and LLMs (Large Language Models) Fabricate Information – "American Chemical Society" (ChatGPT and Environmental Research)

untrustworthy, insecure and impractical

Three Representative Cases

These are of course all interconnected

DoD/IC

Security of the Analytic

The analytic model is corrupted, causing false positives, false negatives, spills and leaks.

Corporates

Security by the Analytic

Misclassifying data samples, failure to verify facts. Countering-hallucinations and confabulations.

HR & Banking

Security for the Analytic

Loss of integrity in parts of the data causing error in results, Lack of transparence, command and control, Automation Surprise

Permion

SECURITY:

01 Privacy

02 Integrity

03 Measurability

04 Confidence

05 Trust

Safe, Secure & Trustworthy AI

OCTOBER 30, 2023

FACT SHEET:

President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence

BRIEFING ROOM ▸ STATEMENTS AND RELEASES

https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence

SECURITY:

Permion

01 Privacy

02 Integrity

03 Measurability

04 Confidence

05 Trust

What's in the new Executive Order?

1. Ensure developers of AI , especially of dual-use foundation models , to conduct AI red- teaming tests to enable deployment of safe , secure , and trustworthy systems .

2. Create robust , reliable , repeatable , and standardized evaluations of AI to provide measurably secure systems.

3. Provide mechanisms to test , understand , and mitigate risks from these systems before they are put to use.

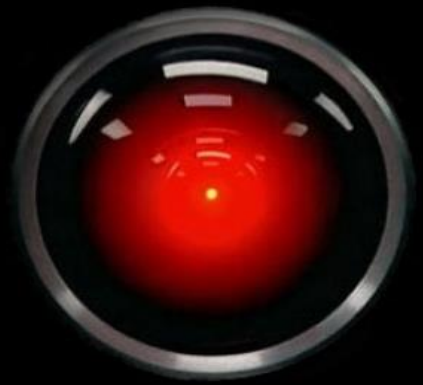
4. Ensure compliance with record-keeping , cybersecurity , confidentiality , privacy , and data protection requirements

5. Develop model guardrails and protect the integrity and trustworthiness models.

6. Install differential-privacy safeguards and prohibit leaks, spills and exposure of PII.

7. Secretary of Commerce , via the Director of NIST, with the Director of OMB and the Director of OSTP , shall develop guidelines , tools , and practices to implement Artificial Intelligence risk-management

Security of the Analytic, by the Analytic and for the Analytic



HAL, please open the door, for my pod … HAL, please open the door.

I'm sorry Dave, I can't open the door

Probabilistic Computing

- In a probabilistic computing, the heavy lifting is done by an **inference rule** — the algorithm that readjusts probabilities on the basis of new training data – *cannot* abstract to unknowns

Quantum Information

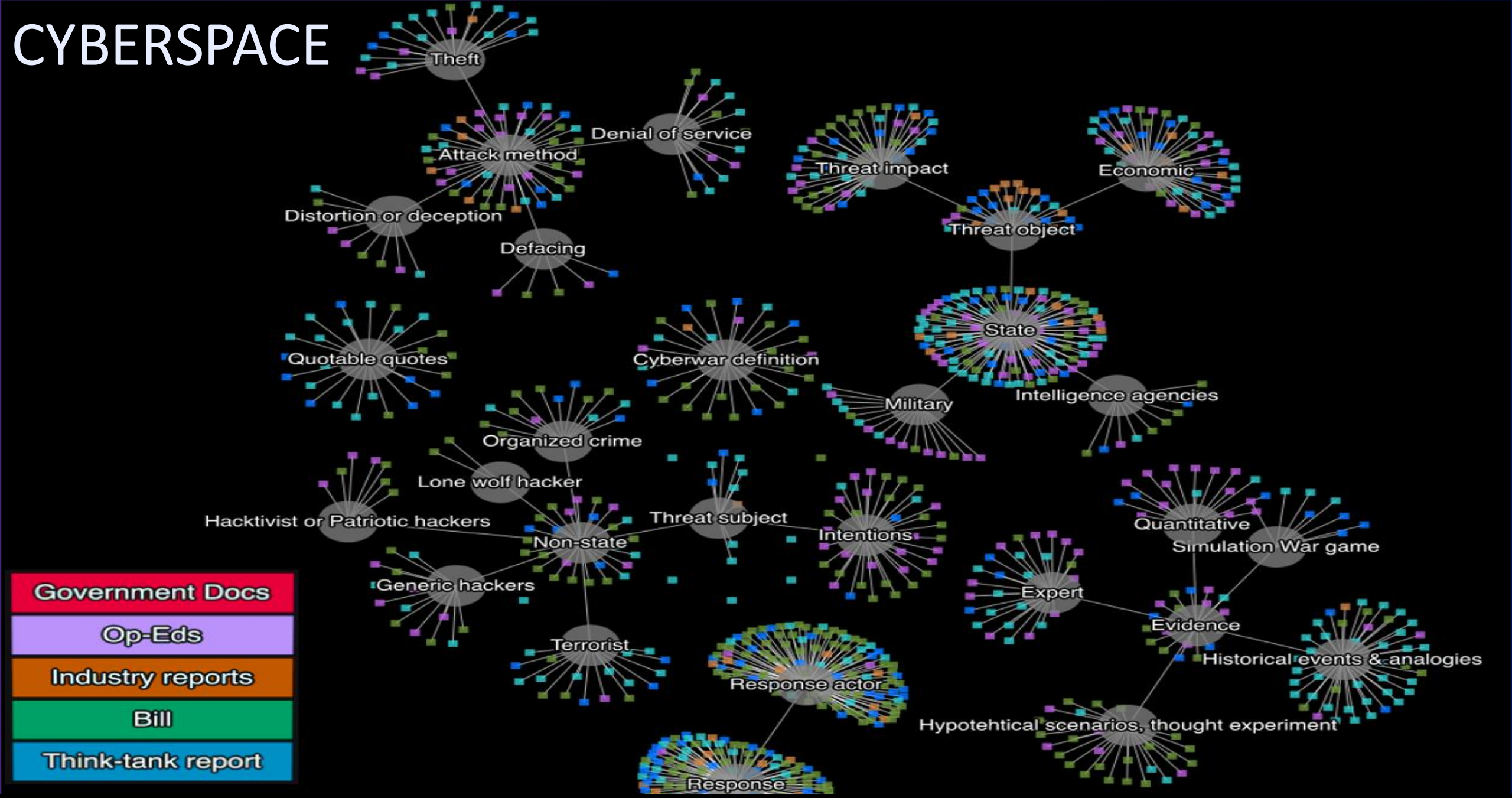
- In Quantum information, the heavy lifting is done by **transition-functions** — models for movement over probabilistic state representations on the basis of new distributions of outcomes given data inputs – *can* abstract to unknowns

Large language models (LLM)

- Combine the aspects of both classical Probability models and Quantum models, the heavy lifting is done by **tensorial network interactions** — models transforming between distributions of activations and given data inputs and outputs – *expresses emergent behaviors not originally designed*

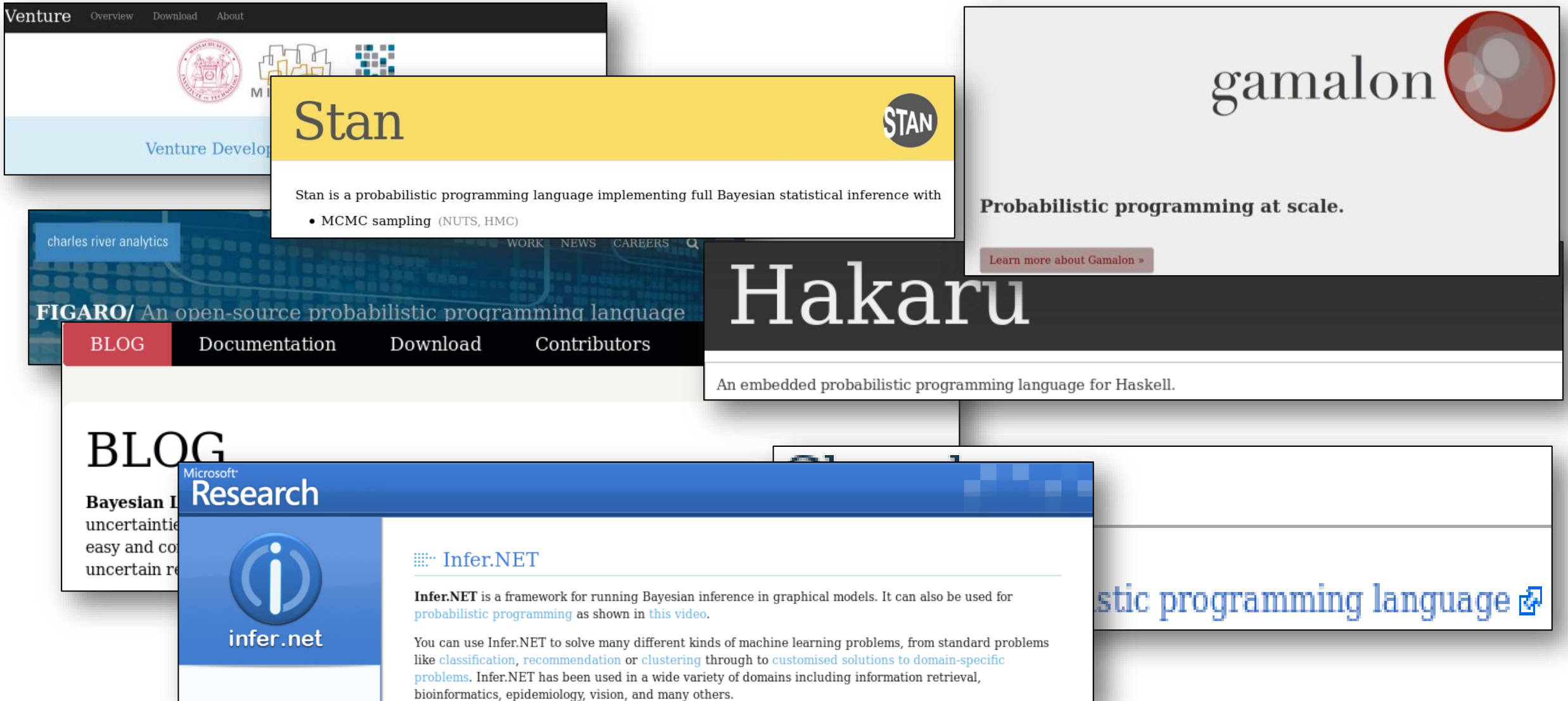
- The underlying tensorial structure resembles the quantum many-body wave function - hence LLMs/GPT possess quantum-like properties!

CYBERSPACE

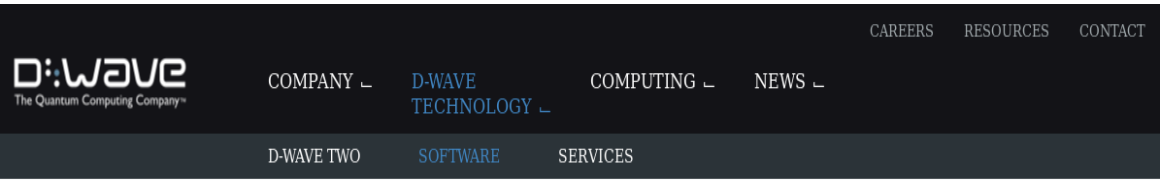


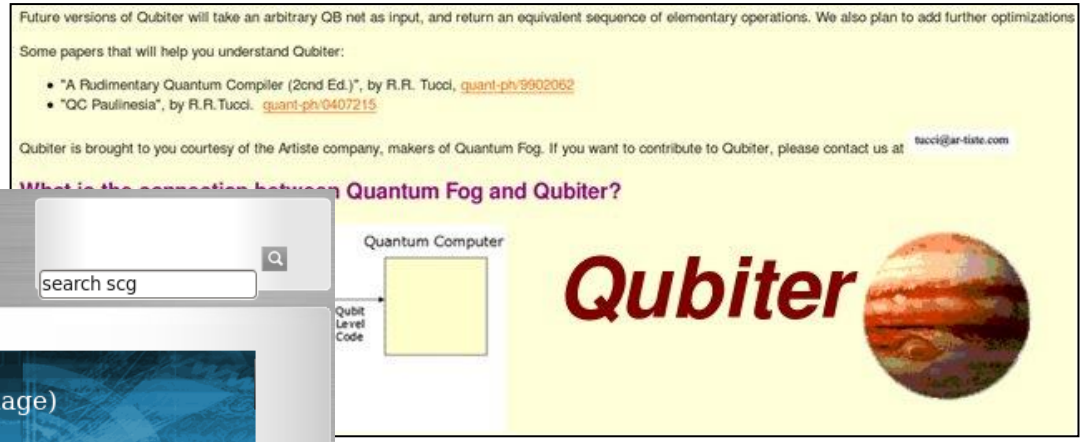
. . . AND MANY OTHER SOURCES AND COLLECTIONS

Probabilistic Programming



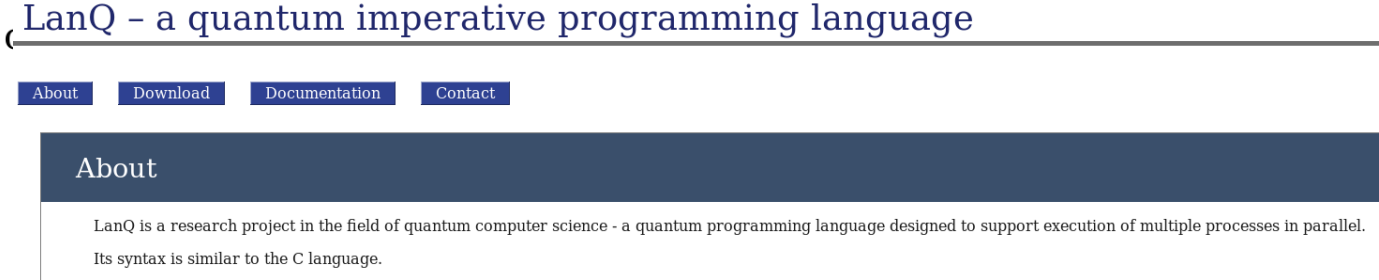
Quantum Programming



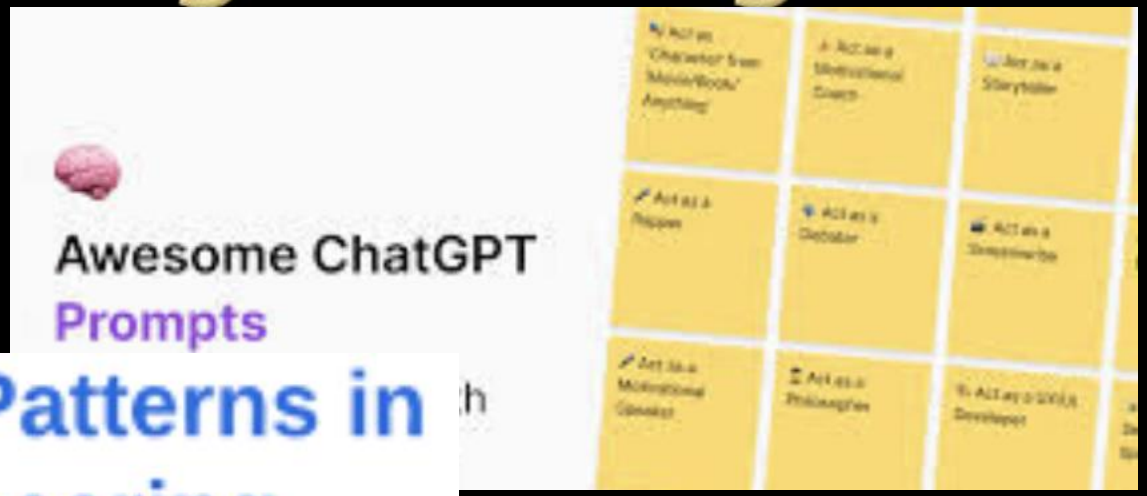


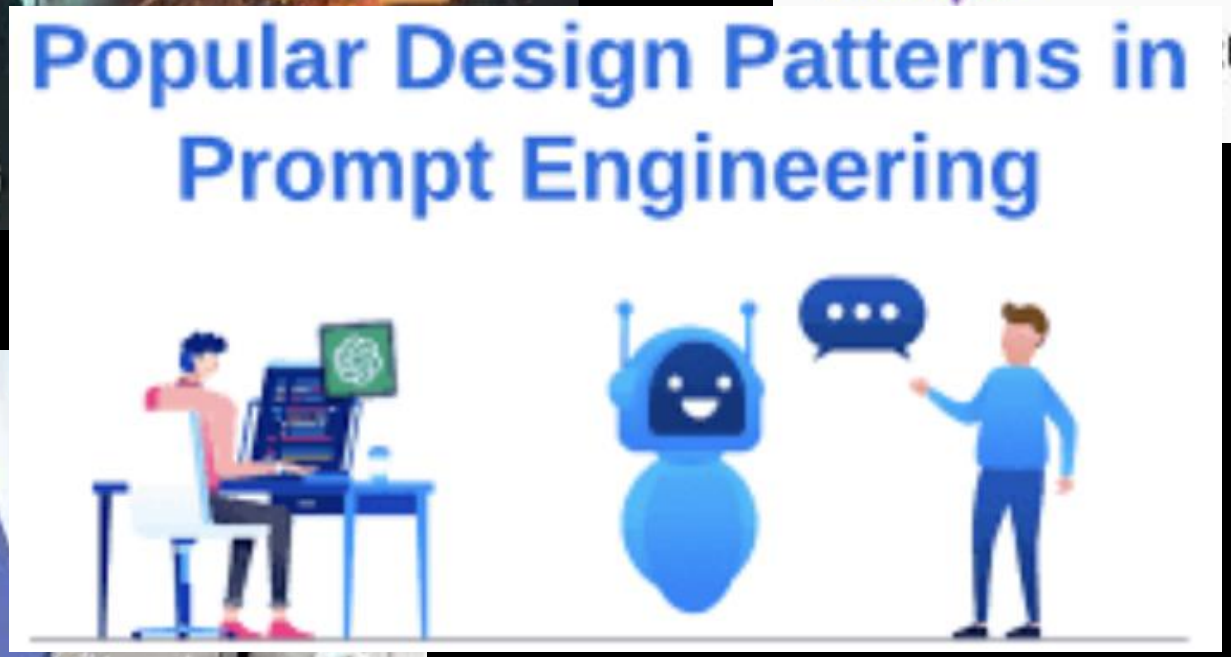
The Quipper System

This is the Quipper System, an embedded functional programming language for quantum computation. You c
browse the source code and documentation from here.



Prompt Design or Engineering?





Uplimit

Prompt Design & Building AI Products

Autonomic AI Poisoning

MACHINE GENERATED CONTENT

FAKES
CONFUSIONS
BREAKDOWNS

Probability Distributions of Original Content Disappear

MODEL COLLAPSE
DEGENERATION
BIAS

THROW AWAY
DIGITAL CONFABULATIONS

TODAY's LEGACY

348 days

average time before a 0-day is public knowledge

Vulnerabilities will always exist.

TODAY's LEGACY

100,000+

new malware samples per day

Signature-based detection is dying.

Threat TTPs are dynamic and will change.

TODAY's LEGACY

60 months

PLA Unit 61398 maintained APT access to US Orgs

Response is predicated on detection…

What do you do if you can not detect?

What do we need?

POLICY AUTOMATION
ATTESTATION
VERIFICATION
VALIDATION
PROOF

Trusted Human-like analysis

PERFORMANCE
MULTI-MODEL
DIVERSITY
PARALLELISM
SUSTAINABILITY

Supercomputer-like performance

BLOCKCHAIN
CONFIDENTIALITY
INTEGRITY
AVAILABILITY
COMPUTABILITY

Data Agnostic

PORTABILITY
RESILIENCE
TRUSTED DEVICES
SUPPLY CHAINS
MANUFACTURING

Small Footprint (↓SWAP)

Risks in Artificial Intelligence

- Deception, hacked Machine Learning, poisoned Artificial Intelligence model and Deep Fakes

- is the data which is used to make decisions trustworthy?

- Has this data been poisoned?

- Is the data that is at the source of machine learning for decision making being corrupted en-route?

- Emergent Threshold of Complexity:
  - ❖ Use the "force"
  - ❖ Flip to the "Dark Side"

Thank You!