



Permion

**Security, Integrity,
and Trust in HPC
Artificial Intelligence**

CLSAC 2023 - Security of the Analytic, by the Analytic and for the Analytic

Bits / Electron $\rightarrow$ Future Devices $\rightarrow$ Bigger, Better, Faster Analytics

ELECTRONS

10²⁶ IBM 305 RAMAC - 1 Bit (5MB)

10²⁴

10²⁰

10¹⁶

10¹²

10⁸

10⁴

10²

10⁻²

<http://mota.stanford.edu/index.php>

35 Bits/Electron

1955

1965

1975

1985

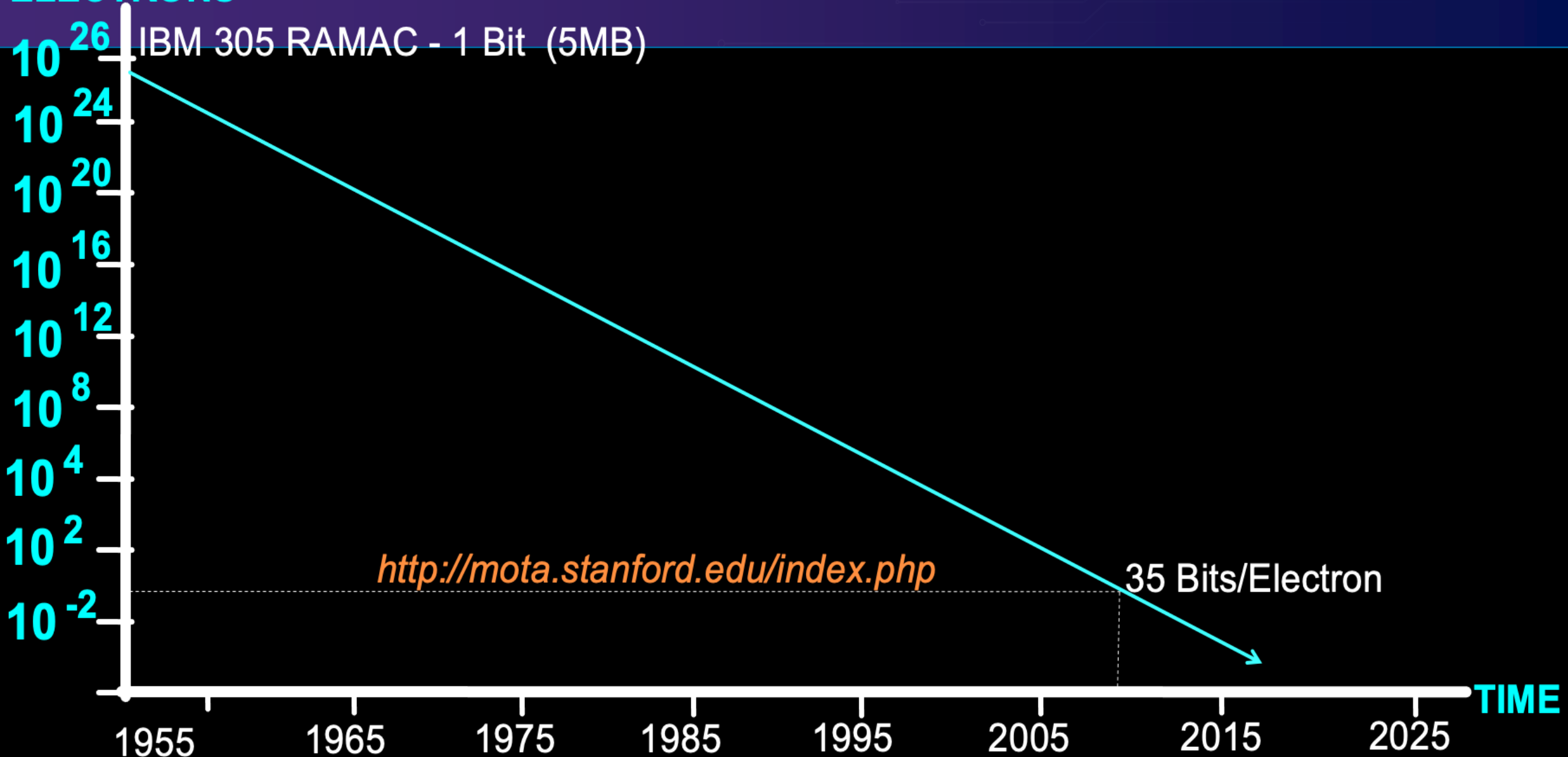
1995

2005

2015

2025

TIME



Assumption

Modern Analytics needs AI

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

ANALYTICS

**Data
Poisoning**



Data at Rest

**Data
Corruption**



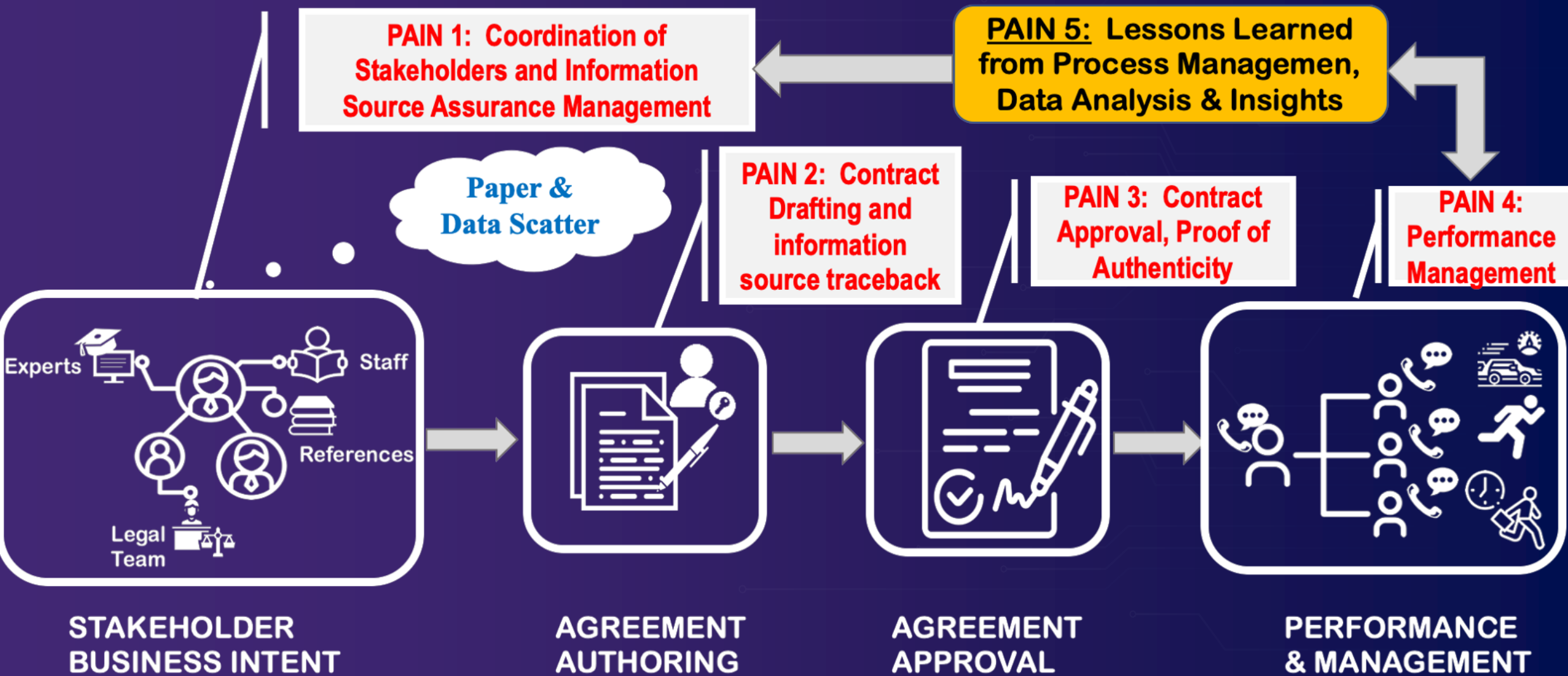
Data in Transit

**Fake
Data**

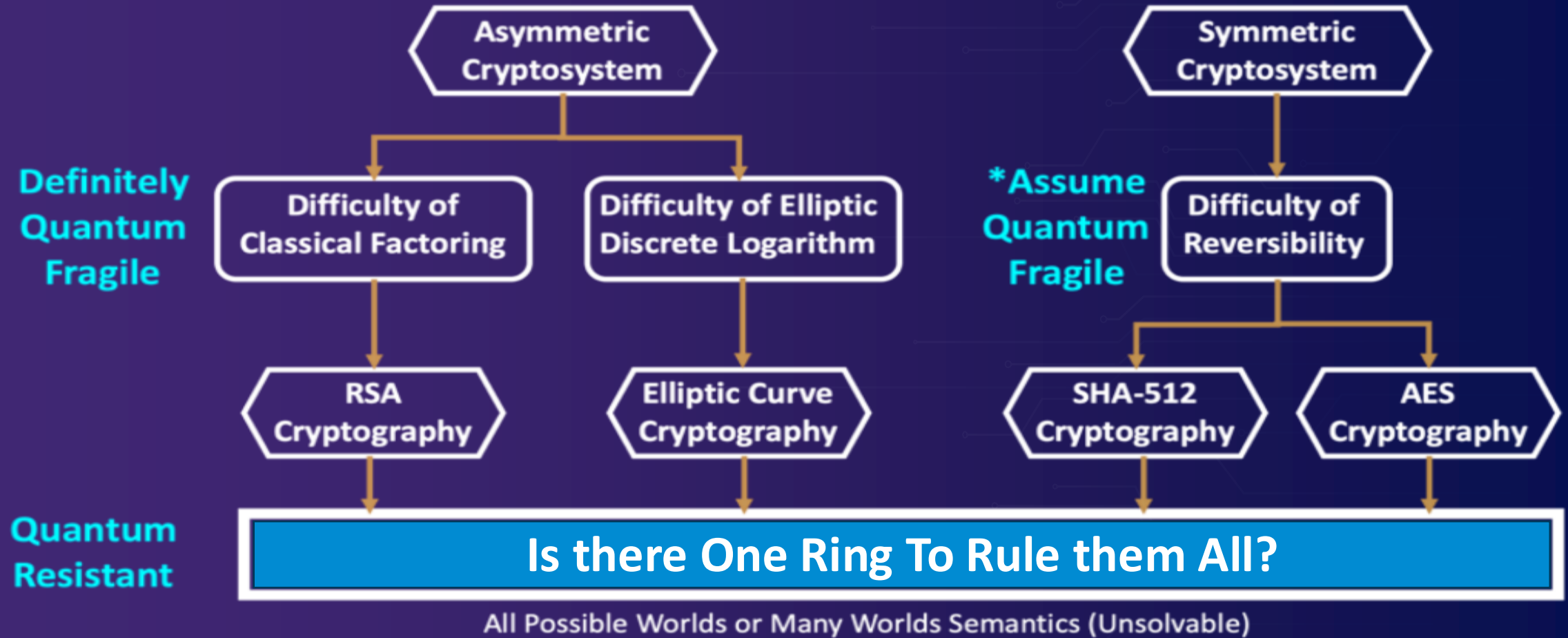


Data in Use

Example of a Legal Process – Risks from the Processes

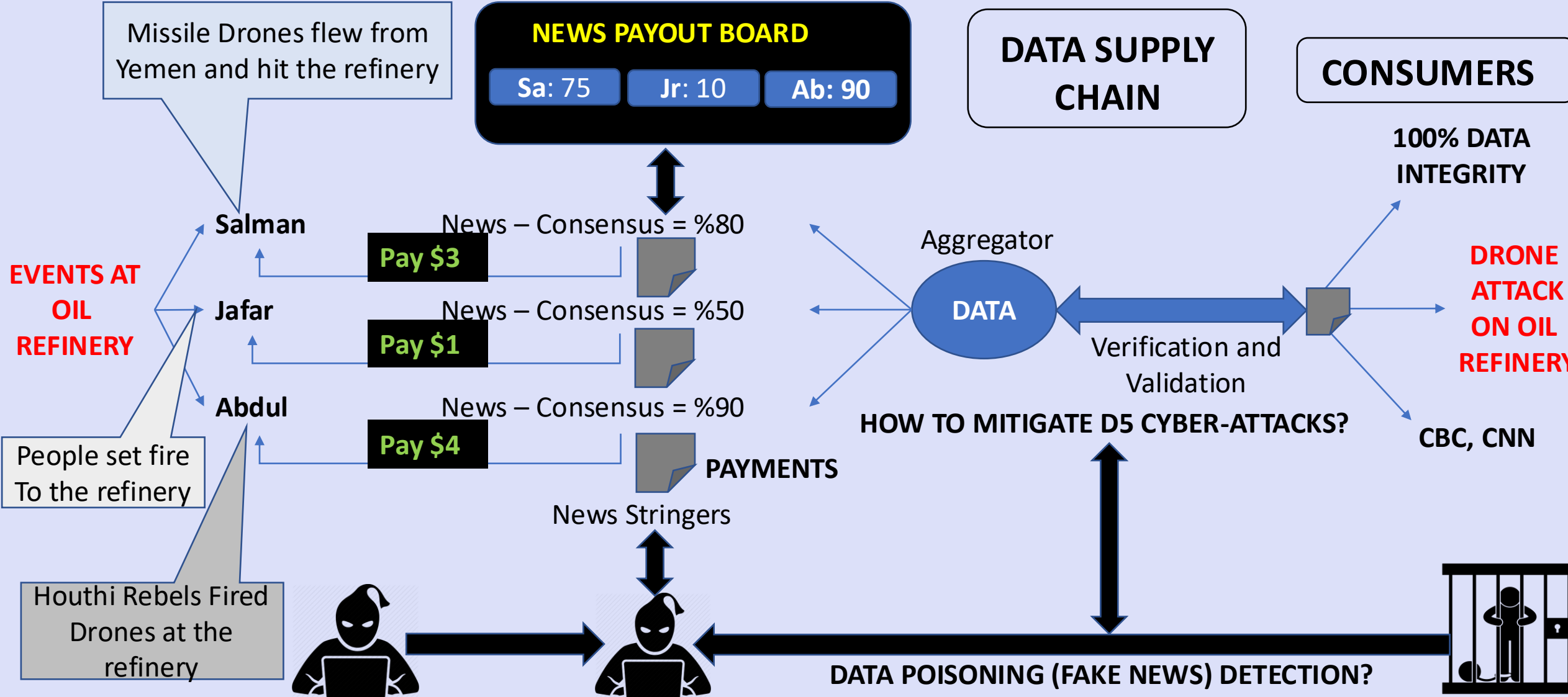


Security of Data at Rest, In Motion and In Use – Risks in Confidentiality



*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

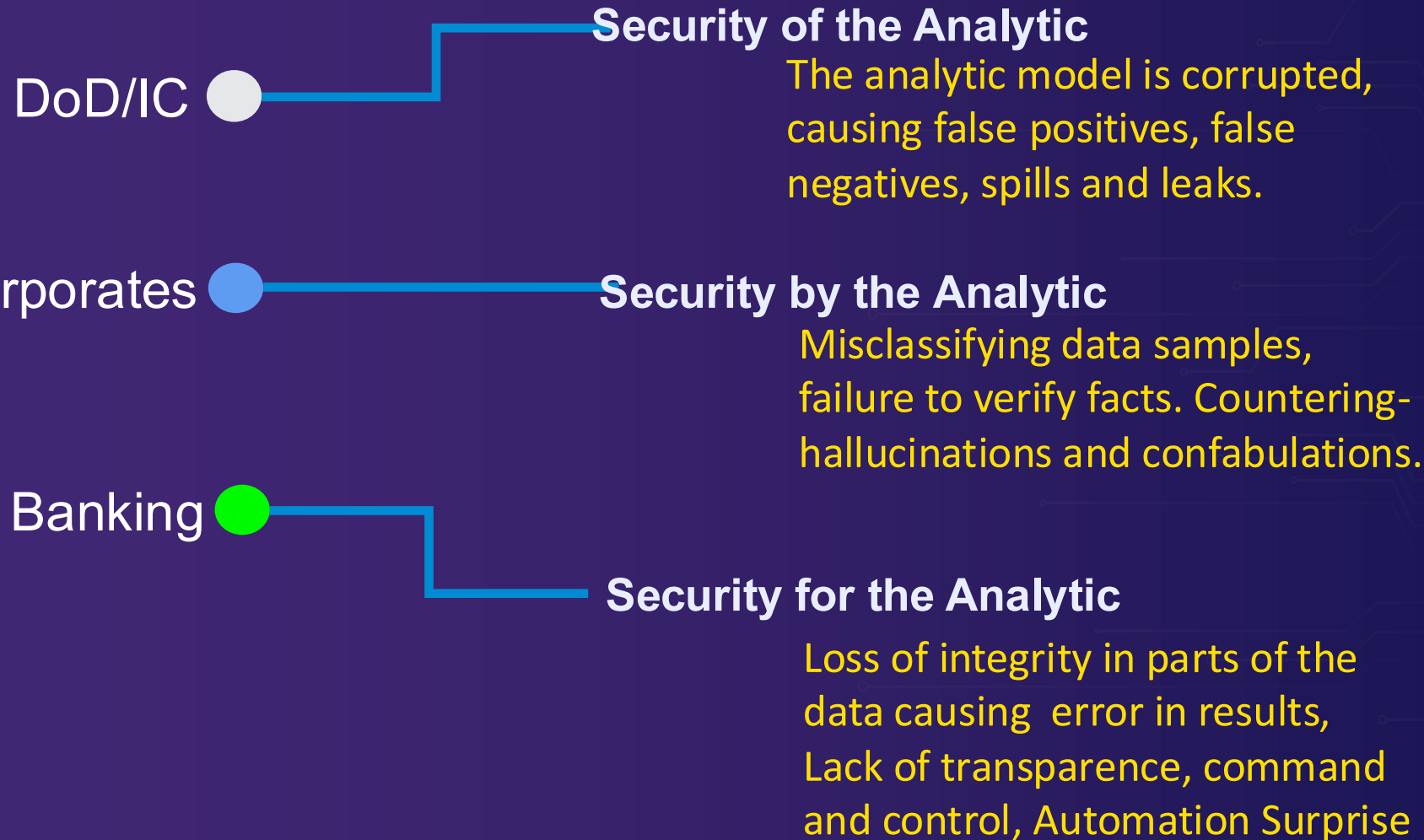
But tools such as ChatGPT threaten transparent science; here are our ground rules for their use –
“Nature”

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



Permission

SECURITY:

01 Privacy

02 Integrity

03 Measurability

04 Confidence

05 Trust

Safe, Secure & Trustworthy AI

Permion

SECURITY:

01 Privacy

02 Integrity

03 Measurability

04 Confidence

05 Trust

OCTOBER 30, 2023

FACT SHEET:

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



BRIEFING ROOM



STATEMENTS AND RELEASES

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*

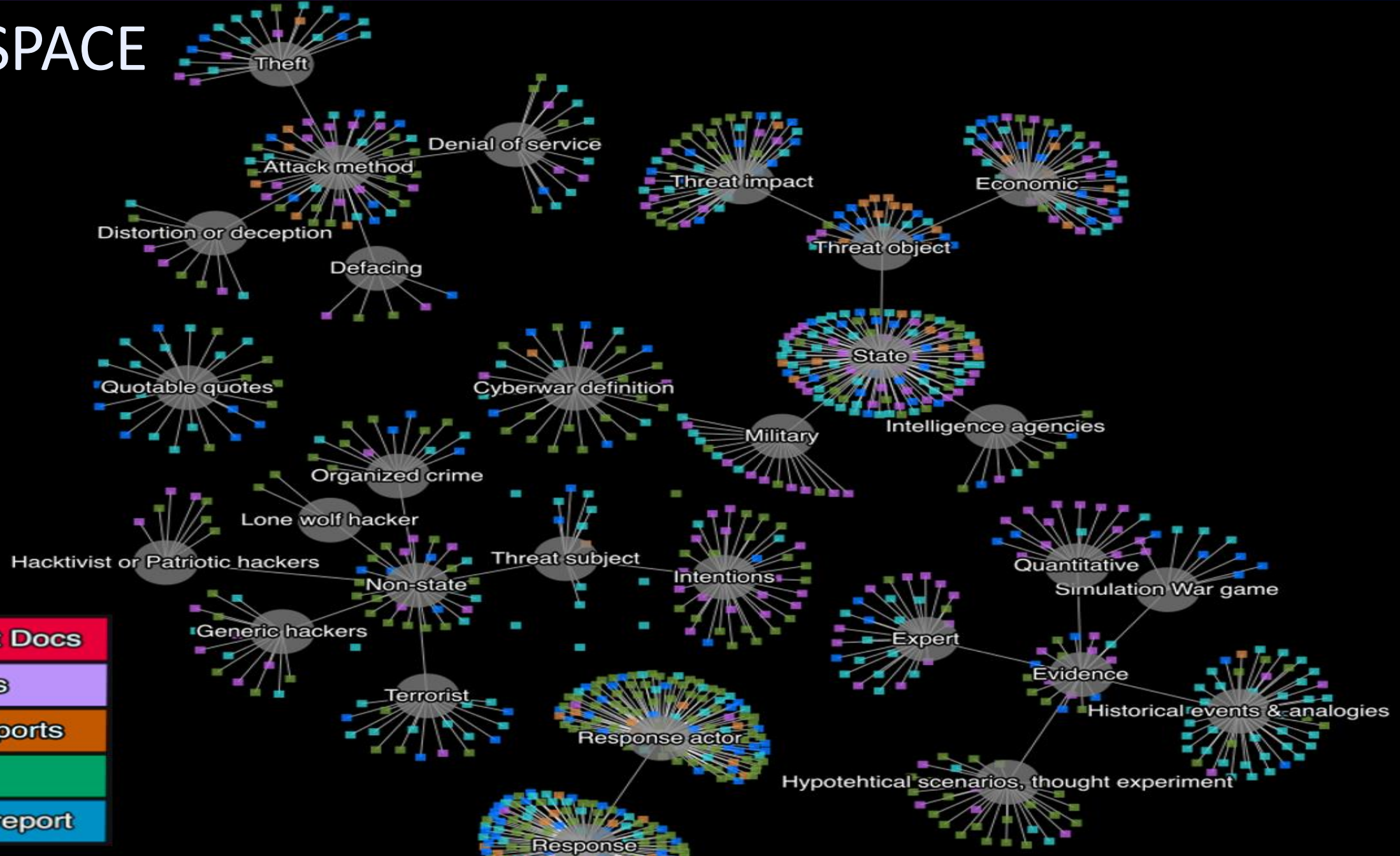
Quantum Information

- ▣ 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)

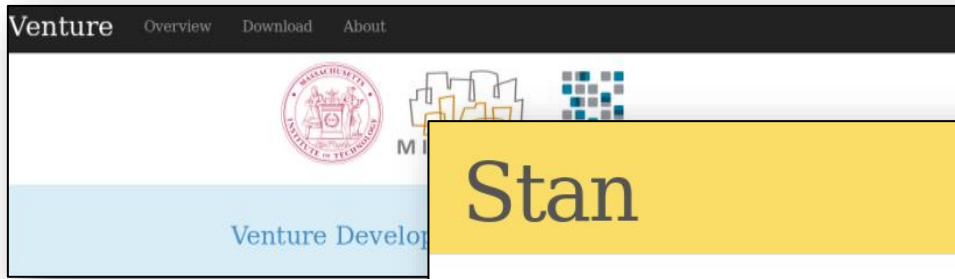
- ▣ Combine the aspects of both classical Probability models and Quantum models, the heavy lifting is done by **tensorial network interactions** – models transforming between distributions of activations and given data inputs and outputs – *expresses emergent behaviors not originally designed*
- ▣ The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



Stan

Stan is a probabilistic programming language implementing full Bayesian statistical inference with

- MCMC sampling (NUTS, HMC)

gamalon

Probabilistic programming at scale.

[Learn more about Gamalon »](#)

charles river analytics

FIGARO/ An open-source probabilistic programming language

[BLOG](#) [Documentation](#) [Download](#) [Contributors](#)

Hakaru

An embedded probabilistic programming language for Haskell.

BLOG

Microsoft Research

Bayesian Inference
uncertainty
easy and compact
uncertain results


infer.net

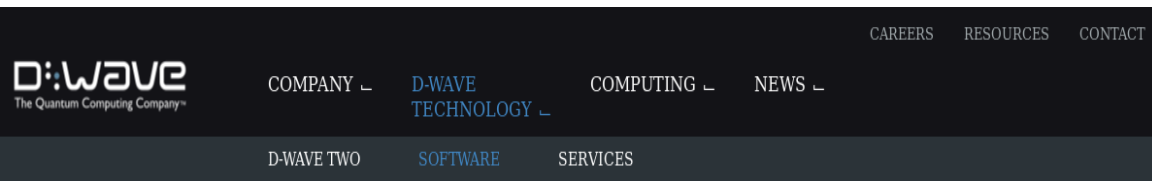
Infer.NET

Infer.NET is a framework for running Bayesian inference in graphical models. It can also be used for probabilistic programming as shown in [this video](#).

You can use Infer.NET to solve many different kinds of machine learning problems, from standard problems like [classification](#), [recommendation](#) or [clustering](#) through to [customised solutions to domain-specific problems](#). Infer.NET has been used in a wide variety of domains including information retrieval, bioinformatics, epidemiology, vision, and many others.

probabilistic programming language [↗](#)

Quantum Programming



Software

Just as the classical development, quantum layers of "system software" system and exploit

The

The Quipper System

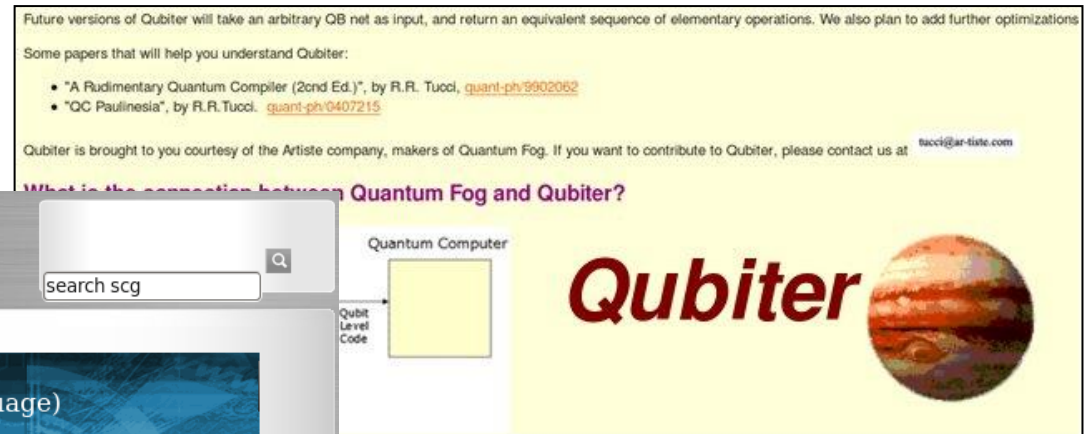
This is the Quipper System, an embedded functional programming language for quantum computation. You can browse the source code and documentation from here.

[LanQ – a quantum imperative programming language](#)

[About](#) [Download](#) [Documentation](#) [Contact](#)

About

LanQ is a research project in the field of quantum computer science - a quantum programming language designed to support execution of multiple processes in parallel. Its syntax is similar to the C language.



Prompt Design or Engineering?



**PROMPT
ENGINEERING**



**Awesome ChatGPT
Prompts**



Popular Design Patterns in Prompt Engineering



Uplimit

INSTRUCTIONAL DESIGN

**PROMPT
ENGINEERING**

GUIDE TO CORPORATE
TRAINING & GENERATIVE AI

Prompt Design & Building AI Products

Autonomous AI Poisoning



**FAKES
CONFUSIONS
BREAKDOWNS**

**Probability
Distributions of
Original Content
Disappear**



**THROW AWAY
DIGITAL CONFABULATIONS**



**MACHINE GENERATED
CONTENT**



**MODEL COLLAPSE
DEGENERATION
BIAS**

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!