Advanced Research + Invention Agency ARIA

Trust Everything, Everywhere

Opportunity space

v1.0

CONTEXT

This document describes an early opportunity space from which we believe one or more funding programmes can emerge. We've sketched out some of our early thinking to spark your interest, and invite you to imagine relevant potential programmes with us, or suggest new directions. We'll publish updated versions of this document as our thinking evolves. Sign up **here** to receive those updates and learn about any funding opportunities that emerge from this opportunity space.

An ARIA opportunity space should be:

+ important if true (i.e. could lead to a significant new capability for society);
+ under-explored relative to its potential impact; and
+ ripe for new talent, perspectives, or resources to change what's possible.

SUMMARY

Software is transcending digital screens to shape the physical world, connecting cyber instructions to real-world outcomes. We are entering a new cyber-physical age that can bring great benefits for humanity: interactions like bioprinting medicines from an online file, tasking an embodied AI agent to run errands for us, or outsourcing an experiment to a self-driving lab are nearly within reach.

Yet, without the right trust infrastructure, we risk every interaction to incur a steep 'trust overhead', making it slower, costlier, and less certain or worse, not happen at all.

The solution is a new trust infrastructure that extends formal security reasoning into the physical world. This will unlock trillion-pound cyber-physical markets and a society free to trust everything, everywhere.

BELIEFS

The core beliefs that underpin/bound this area of opportunity.

1. *Creating a new trust infrastructure will unlock the cyber-physical economy.* The trust building blocks that enabled today's £24-trillion digital economy, like encryption and cryptographic signatures, do not extend to the physical world.
2. *Formal security reasoning is key to designing new cyber-physical trust building blocks:* rooted in different assumptions (e.g. quantum physics instead of computational hardness), and living in alternative informational substrates (e.g. DNA instead of bits).
3. *AI will make secure cyber-physical interactions accessible to everyone.* The next generation of trust infrastructure will allow AI systems to generate customised, on-demand protocols in situ for any given cyber-physical interaction, spanning atoms, molecules, waves, and bits.

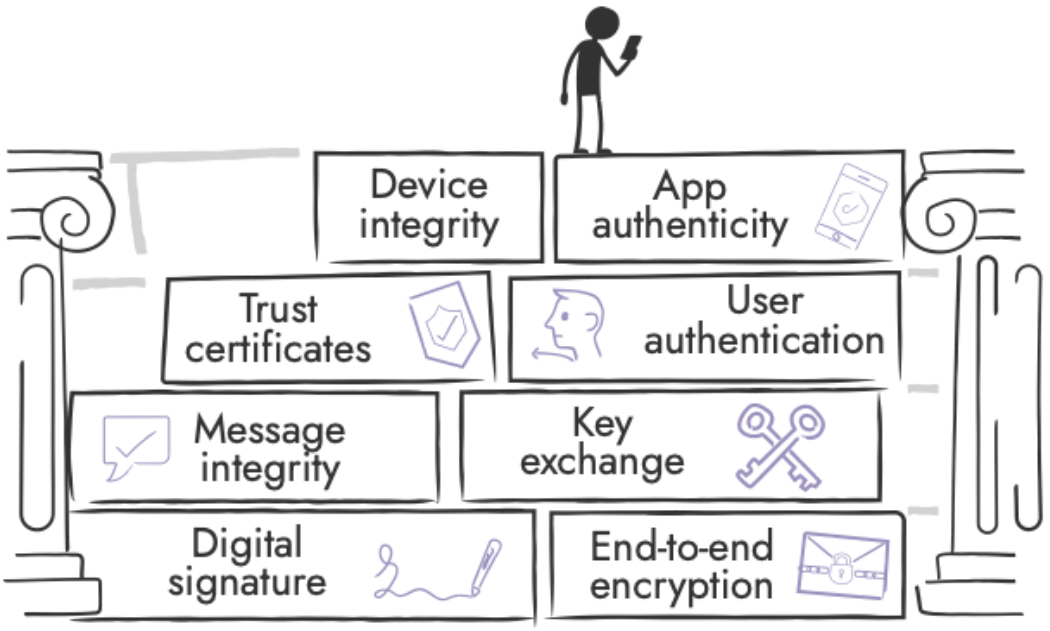
OBSERVATIONS

Some signposts as to why we see this area as important, underserved, and ripe.

Observation 1

Digital trust building blocks such as encryption and cryptographic signatures made communication over the internet secure enough to enable trillion pound industries (such as e-commerce, private messaging, and digital payments) and our digital civilisation.

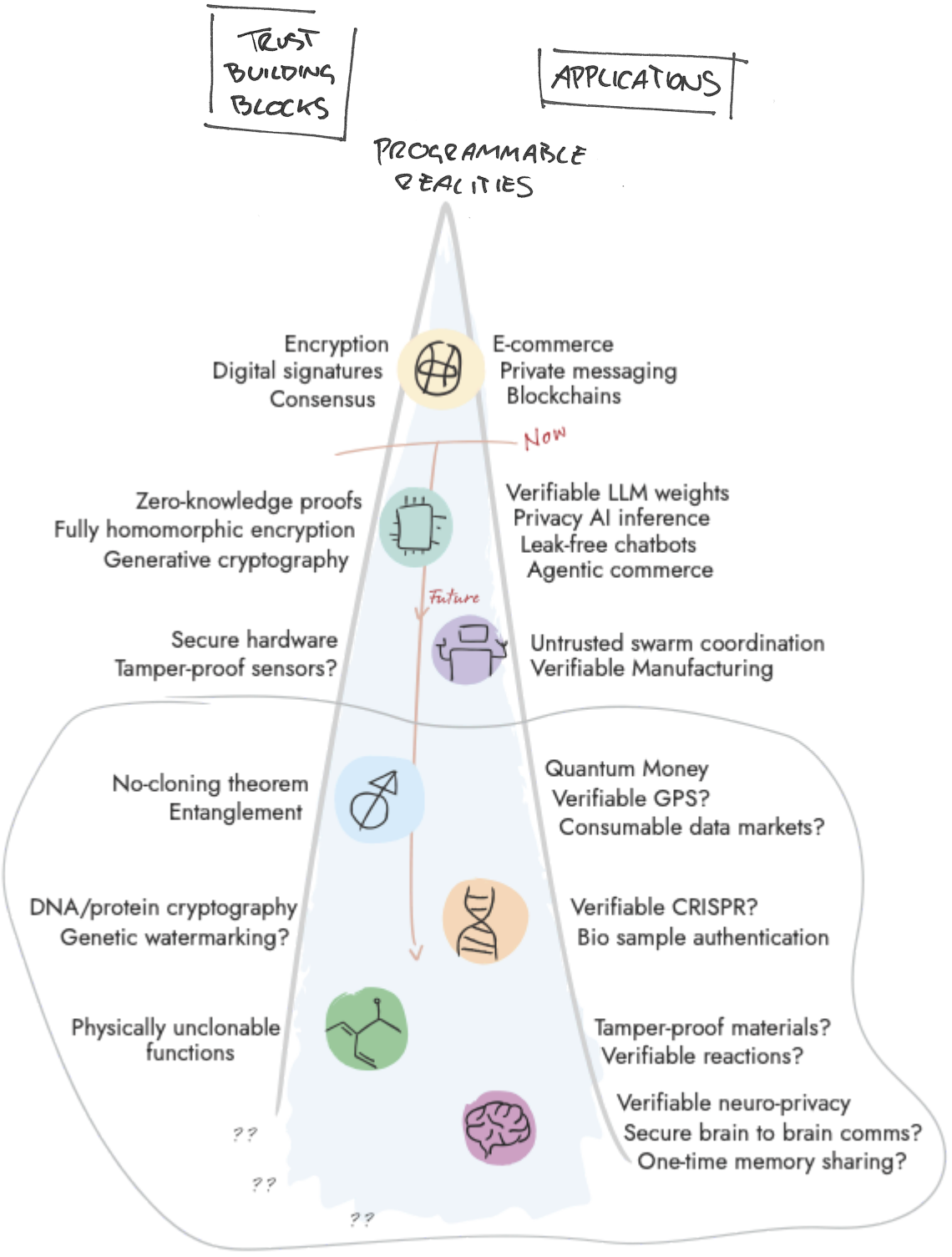
Secure by design: Formal security helps us make digital systems secure by design such that no actors can deceive, steal or abuse the system. This in turn enables cooperation amongst untrusted parties and increases competition (i.e. lower "trust overhead".)



Observation 2

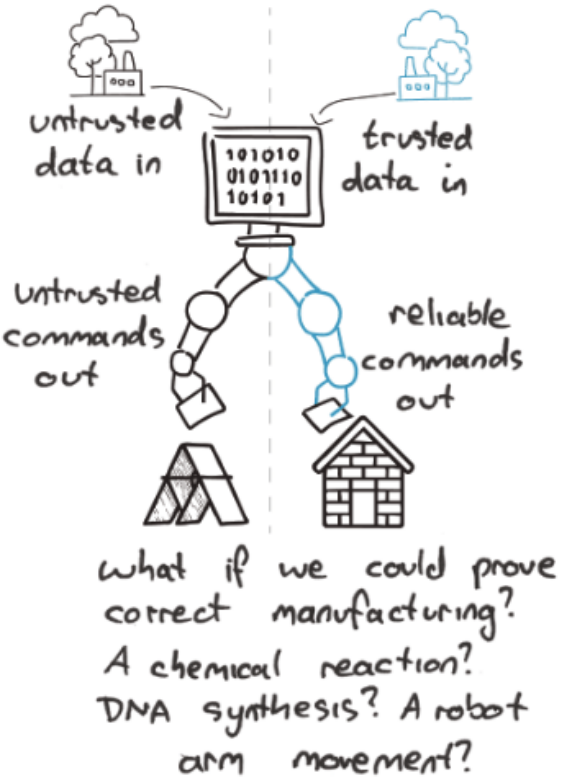
Nature offers unique properties we can harness for a new class of trust building blocks that are native to the physical world:

- **New Assumptions:** *Eg. No-cloning theorem*: building secure systems based on unclonability of quantum state (like Quantum Key Distribution).
- **New Media**: *Eg. DNA cryptography*: A message is encoded into a DNA strand and hidden with other irrelevant DNA. An attacker without the right information must brute-sequence the entire mixture.
- **New Applications**: *Eg. Physical one-way functions for chip authentication:* Unique physical imperfections in a silicon chip create a "fingerprint" that uniquely authenticate the chip and guard against physical tampering.


TRUST BUILDING BLOCKS
APPLICATIONS
PROGRAMMABLE REALITIES
Encryption
Digital signatures
Consensus
E-commerce
Private messaging
Blockchains
Now
Zero-knowledge proofs
Fully homomorphic encryption
Generative cryptography
Verifiable LLM weights
Privacy AI inference
Leak-free chatbots
Agentic commerce
Future
Secure hardware
Tamper-proof sensors?
Untrusted swarm coordination
Verifiable Manufacturing
No-cloning theorem
Entanglement
Quantum Money
Verifiable GPS?
Consumable data markets?
DNA/protein cryptography
Genetic watermarking?
Verifiable CRISPR?
Bio sample authentication
Physically unclonable functions
Tamper-proof materials?
Verifiable reactions?
Verifiable neuro-privacy
Secure brain to brain comms?
One-time memory sharing?
??
??
??
Nature Cryptography?

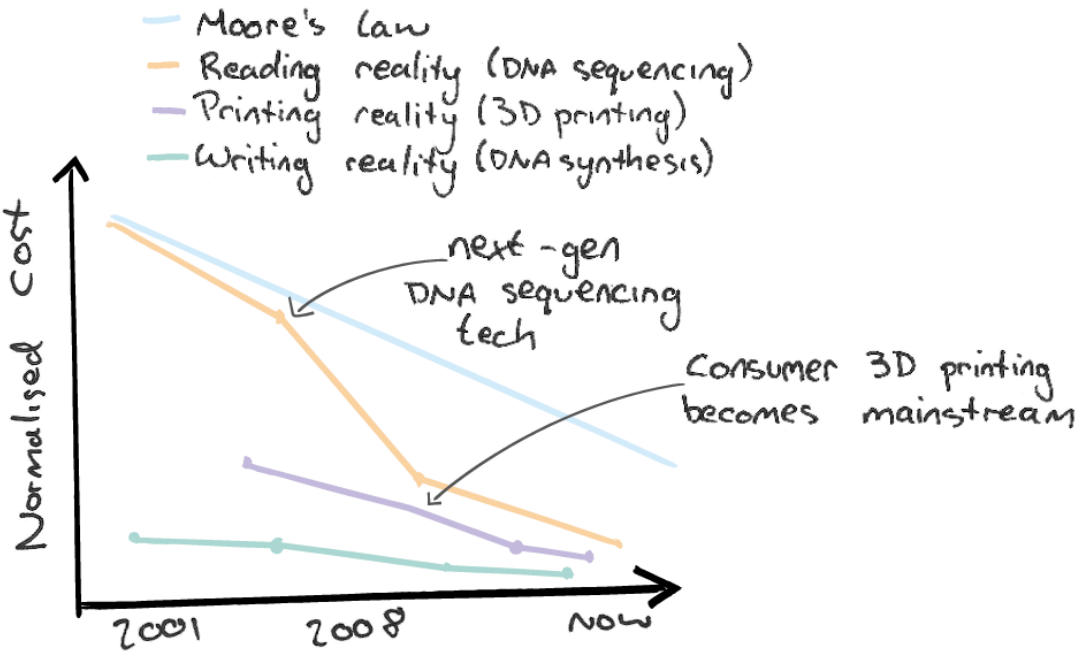
Observation 3

Yet "formal security" is largely underexplored: physical systems are hard to formalise and the digital↔physical link is hard to secure.

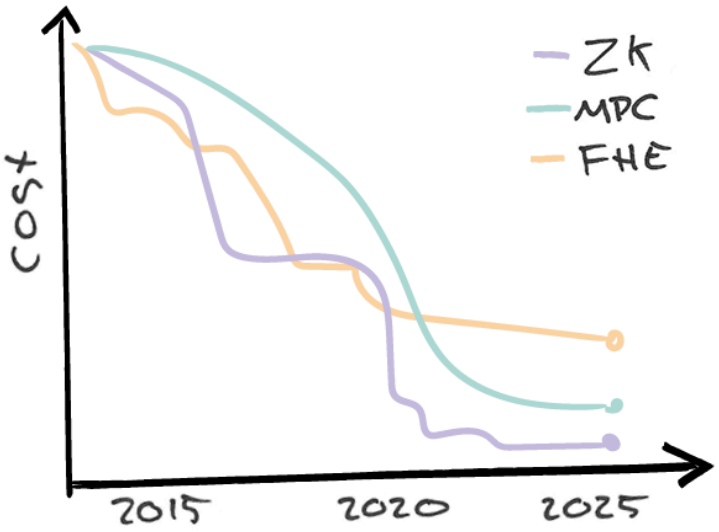


Observation 4

- **Programming reality is becoming practical**: We can program quantum states, DNA with CRISPR, soon synthetic and biological materials and patterns including plants, mitochondria,and brain signals.



- **AI as a new tool for programmability**: As cryptography and physical matter become programmable, AI could write secure cyber-physical protocols on demand. This would reduce the cost and complexity of security, therefore reduce the 'trust overhead' of cyber-physical interactions.
- **Programming cryptography is becoming practical:** There is more to encryption — we can now have programs to compute on encrypted data (FHE), over shared inputs with untrusted parties (MPC), in a verifiable way (ZK).



SOURCES

A compiled, but not exhaustive list of works helping to shape our view and frame the opportunity space (for those who want to dig deeper).

Inspiration

- Is Information the Key? – Gilles Brassard
- The Moral Character of Cryptographic Work – Phil Rogaway
- My Techno Optimism — Vitalik Buterin
- Why I Support Privacy — Vitalik Buterin
- Mechanisms too simple for humans to design – Telescopic Turnip
- The Quantum Thief – Hannu Rajaniemi
- Black-Hole Radiation Decoding is Quantum Cryptography – Zvika Brakerski

Nature cryptography?

- Physical One-Way Functions – Pappu et al.
- A New Approach to Nuclear Warhead Verification Using a Zero-Knowledge Protocol – Glaser et al.
- Quantum Cryptography: Uncertainty in the Service of Privacy – Charles Bennett
- Consumable Data via Quantum Communication – Gilboa et al.
- Conjugate Coding – Stephen Wiesner
- Unclonable Polymers and Their Cryptographic Applications – Almashaqbeh et al.
- Building Unclonable Cryptography: A Tale of Two No-cloning Paradigms – Almashaqbeh et al.
- An Introduction to Protein Cryptography – Tirmazi et al.
- Cryptography in the DNA of living cells enabled by multi-site base editing – Volf et al.
- Hidden Messages in DNA Could Reduce Biosecurity Risks – Danielle Gerhard
- Neuroscience needs network science – Barabási et al.
- A New Age of Computing and the Brain – Golland et al.
- Mosquito-derived ingested DNA as a tool for monitoring terrestrial vertebrates within a peri-urban environment – Chivas et al.

- Molecules that Generate Fingerprints: A New Class of Fluorescent Sensors for Chemical Biology, Medical Diagnosis, and Cryptography – Motiei et al.

Programmable reality

- Programmable Plants – ARIA
- Programmable Mitochondria – ARIA
- AlphaGenome: AI for better understanding the genome – Avsec et al.
- Zeroshot anti-body design in a 24-well plate – Chai Discovery
- Breaking bonds, breaking ground: Advancing the accuracy of computational chemistry with deep learning – van den Berg et al.
- Osmo AI — giving computers a sense of smell
- Electric Plant Company – translating plants' electric signals
- You Can Just Program Biology – Union Square Ventures
- Tissue-specific modulation of CRISPR activity by miRNA-sensing guide RNAs – Guerra et al.
- Biology has scaling laws too – Air Street Capital Press
- A Protein Printer, How to make a machine that turns bits into molecules – Englert et al.
- The Next $10 Trillion Opportunity: Why 'AI x Physical World' Is Where It's All Headed – Bilal Zuberi
- Welcome to the Era of Experience – Silver et al.
- Lila Sciences – autonomous science labs to speed up scientific experiments
- Computer-inspired Quantum Experiments – Krenn et al.
- Towards Material Abundance – Mackenzie Morehead

Programmable cryptography, secure systems, and trust

- Programmable Cryptography – 0xParc
- Transparency has value – Dionna Amalie Glaze
- In Machines We Trust – Zarinah Agnew
- Formal Methods for Secure Cyber-Physical Systems Workshop: Report on the First Edition – Wright et al.
- Formal Techniques for Verification and Testing of Cyber-Physical Systems – Deshmukh et al.
- Building a Zero Trust Security Model for Autonomous Systems - IEEE Spectrum

- SSITH: System Security Integration Through Hardware and Firmware | DARPA
- AISS: Automatic Implementation of Secure Silicon | DARPA
- QuANET: Quantum-augmented network | DARPA
- COMPASS: Critical Orientation of Mathematics to Produce Advancements in Science and Security | DARPA
- PROVERS: Pipelined Reasoning of Verifiers Enabling Robust Systems | DARPA
- Cyber-physical problems - NCSC.GOV.UK
- zkPi: Proving Lean Theorems in Zero-Knowledge — Laufer et al.
- Verified Value Chains, Innovation and Competition — Weber et al.
- IRIS (Infra-Red, in situ) Project Updates — bunnie:studios
- SecureDNA — A system capable of verifiably and privately screening global DNA synthesis — Baum et al.
- Eight Reasons to Prioritize Brain-Computer Interface Cybersecurity — Bernal et al.
- Secure and secret cooperation in robotic swarms — Ferrer et al.

ENGAGE

Our next step is to formulate a £10-100m programme within this opportunity space that will direct funding across research disciplines and institutions toward a focused objective. In order to ensure we select the right first challenge, we want to hear from you.

Complete this form to provide feedback on the opportunity space and inform the development of our programme thesis - we will read anything you send.

We'll also be organising a set of roundtables to help shape the programme. If you're interested in participating, please register your interest in the form above.