Trust Everything, Everywhere was one of ARIA's original opportunity spaces. Following an evolution of our research portfolio in August 2026, it now sits within the updated Trust Everything, Everywhere opportunity space. The beliefs and observations that defined the original opportunity space still hold, and its remit continues in full within with respect to both future programmes and seed funding. No active funding was affected by this change.

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 further funding opportunities within 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 this opportunity space:

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.

ARIA | Copyright 2025

OBSERVATIONS

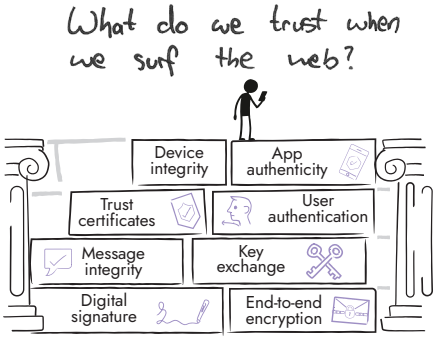
Some signposts as to why we see this area as important, under-explored, and ripe.

Digital trust building blocks such as encryption and cryptographic signatures made communication over the internet secure enough to enable trillion pound industries and our digital civilization.

e-commerce
private messaging
digital payments

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.

Lower "trust overhead"



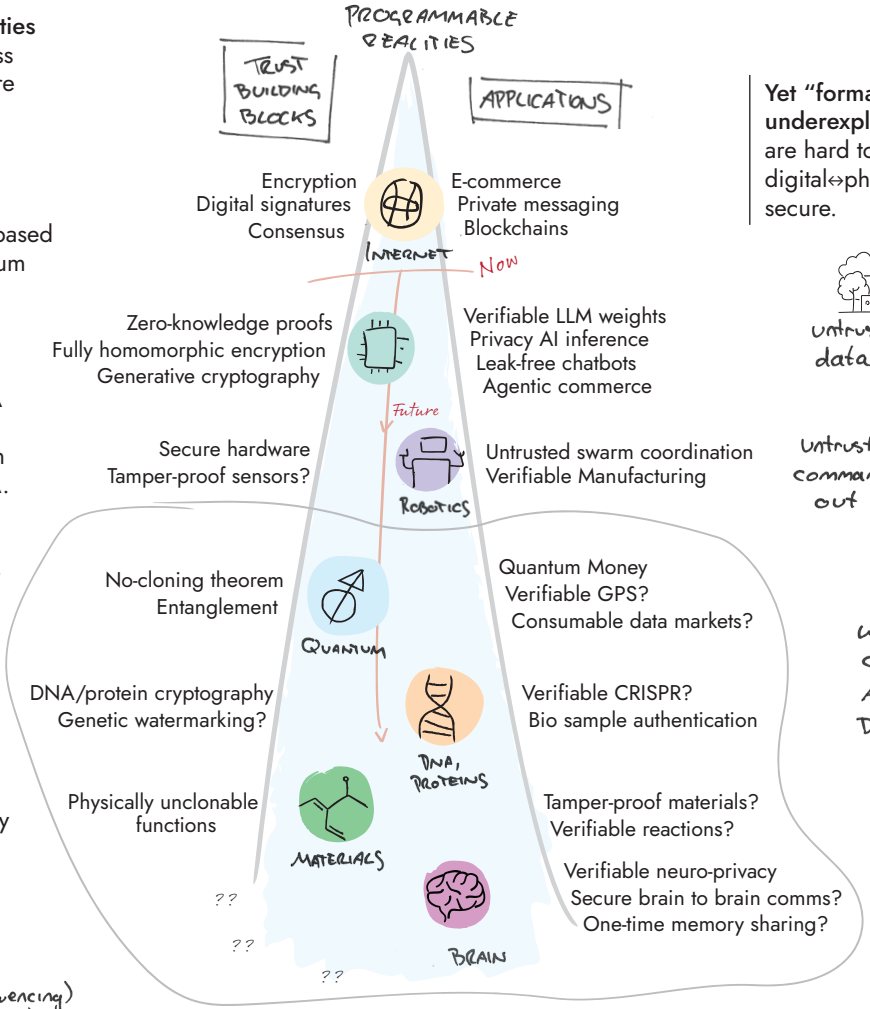
WHAT CAN WE UNLOCK WITH CYBER-PHYSICAL TRUST BUILDING BLOCKS?

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

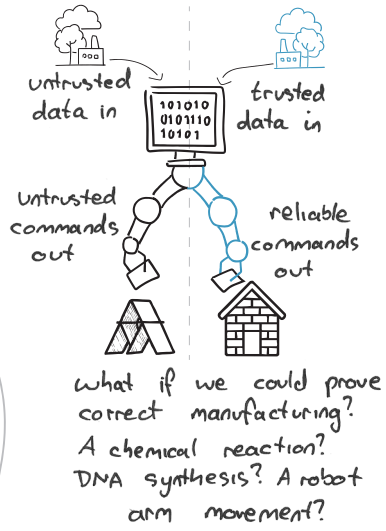
New Assumptions
Eg. No-cloning theorem: building secure systems based on unclonability of quantum state (like Quantum Key Distribution).

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.

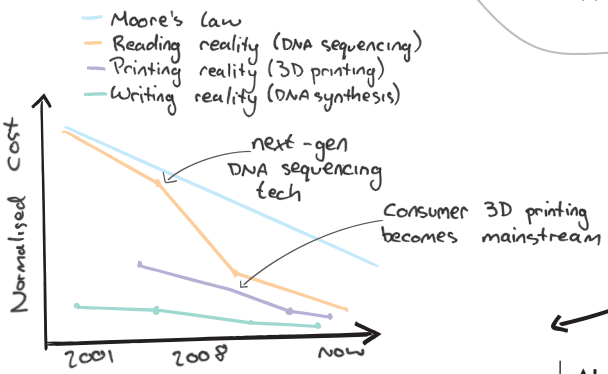
New Applications
Eg. Physical one-way functions for chip authentication: Unique physical imperfections in a silicon chip create a "fingerprint" that uniquely authenticate the chip and guard against physical tampering.



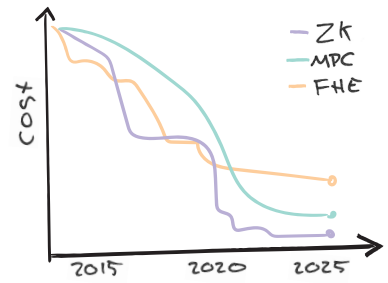
Yet "formal security" is largely underexplored: physical systems are hard to formalise and the digital↔physical link is hard to secure.



Nature Cryptography?



WHAT'S ENABLING THIS?



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).

ARIA | Copyright 2025

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

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

Nature cryptography?

8. Physical One-Way Functions – Pappu et al.
9. A New Approach to Nuclear Warhead Verification Using a Zero-Knowledge Protoco – Glaser et al.
10. Quantum Cryptography: Uncertainty in the Service of Privacy – Charles Bennett
11. Consumable Data via Quantum Communication – Gilboa et al.
12. Conjugate Coding – Stephen Wiesner
13. Unclonable Polymers and Their Cryptographic Applications – Almashaqbeh et al.
14. Building Unclonable Cryptography: A Tale of Two No-cloning Paradigms – Almashaqbeh et al.
15. An Introduction to Protein Cryptography – Tirmazi et al.
16. Cryptography in the DNA of living cells enabled by multi-site base editing – Volf et al.
17. Hidden Messages in DNA Could Reduce Biosecurity Risks – Danielle Gerhard
18. Neuroscience needs network science – Barabási et al.
19. A New Age of Computing and the Brain – Golland et al.
20. Mosquito-derived ingested DNA as a tool for monitoring terrestrial vertebrates within a peri-urban environment – Chivas et al.
21. Molecules that Generate Fingerprints: A New Class of Fluorescent Sensors for Chemical Biology, Medical Diagnosis, and Cryptography – Motiei et al.

Programmable Reality

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

Programmable cryptography, secure systems, and trust

38. Programmable Cryptography – 0xParc
39. Transparency has value – Dionna Amalie Glaze
40. In Machines We Trust – Zarinah Agnew
41. Formal Methods for Secure Cyber-Physical Systems Workshop: Report on the First Edition – Wright et al.
42. Formal Techniques for Verification and Testing of Cyber-Physical Systems – Deshmukh et al.
43. Building a Zero-Trust Security Model for Autonomous Systems
44. SSITH: System Security Integration Through Hardware and Firmware | DARPA
45. AISS: Automatic Implementation of Secure Silicon | DARPA
46. QuANET: Quantum-augmented network | DARPA
47. COMPASS: Critical Orientation of Mathematics to Produce Advancements in Science and Security | DARPA
48. PROVERS: Pipelined Reasoning of Verifiers Enabling Robust Systems | DARPA
49. Cyber-physical problems - NCSC.GOV.UK
50. zkPi: Proving Lean Theorems in Zero-Knowledge – Laufer et al.
51. Verified Value Chains, Innovation and Competition – Weber et al.
52. IRIS (Infra-Red, in situ) Project Updates – Bunnie:studios
53. SecureDNA – A system capable of verifiably and privately screening global DNA synthesis – Baum et. al
54. Eight Reasons to Prioritize Brain-Computer Interface Cybersecurity – Bernal et al.
55. 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.

ARIA | Copyright 2025