arm

From Cloak of Invisibility, to Chain of Custody, to Personal Oracle

A brief overview of digital identity

Michael Lu, Director Strategy (Security & Privacy)

September 3, 2020

arm

The Architects of Global Possibilities

The global leader in the development of licensable technology

- R&D outsourcing for semiconductor companies

Focused on freedom and flexibility to innovate

- Technology reused across multiple applications

With a partnership based culture & business model

- Licensees take advantage of learnings from a uniquely collaborative ecosystem

1,690+
licenses, growing by 100+ every year

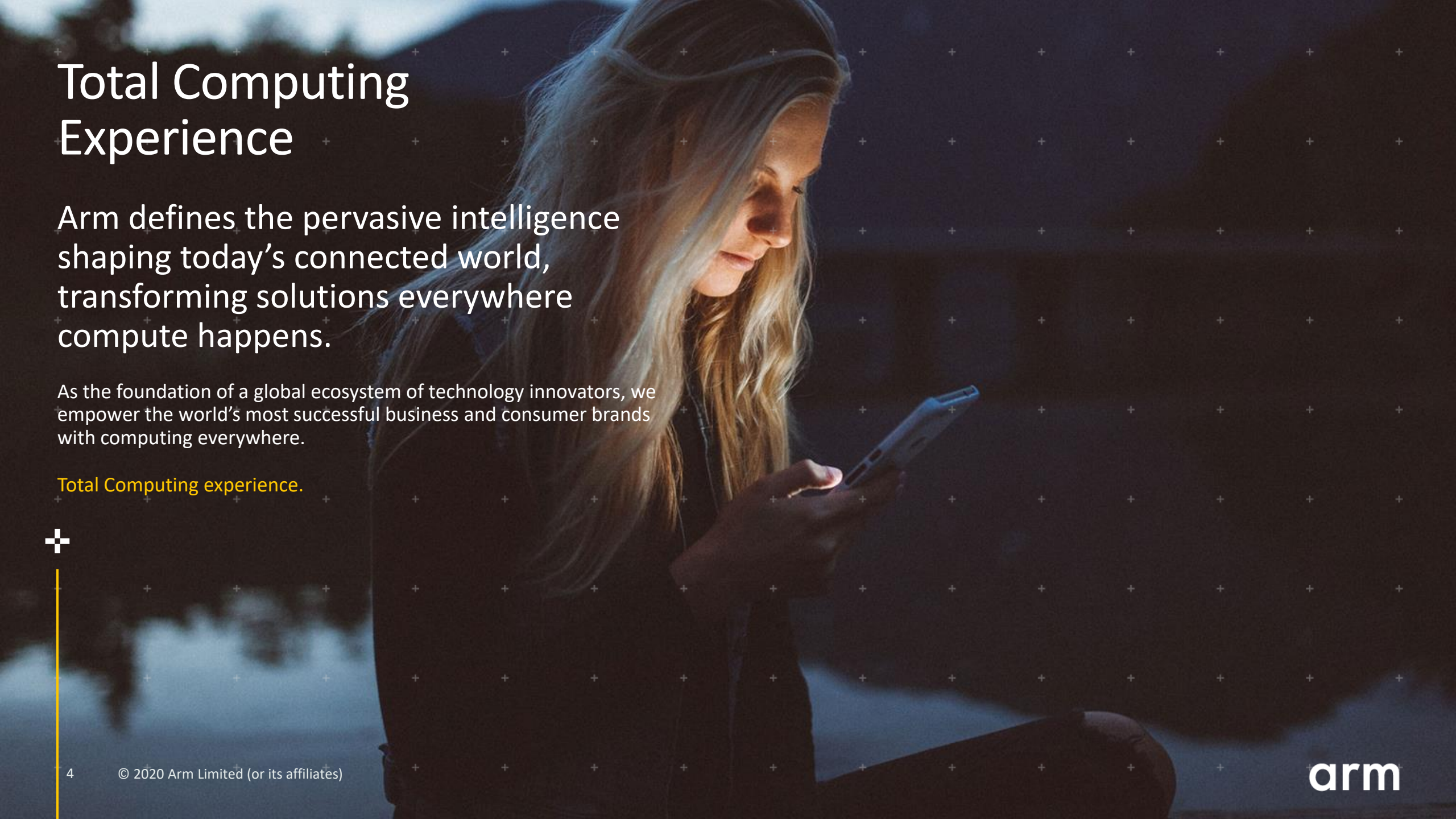
500 licensees
Industry leaders and high-growth start-ups; chip companies and OEMs

155+bn
Arm-based chips shipped to-date

25+bn
Arm-based chips shipped in 2019

arm

Total Computing Experience



Arm defines the pervasive intelligence shaping today's connected world, transforming solutions everywhere compute happens.

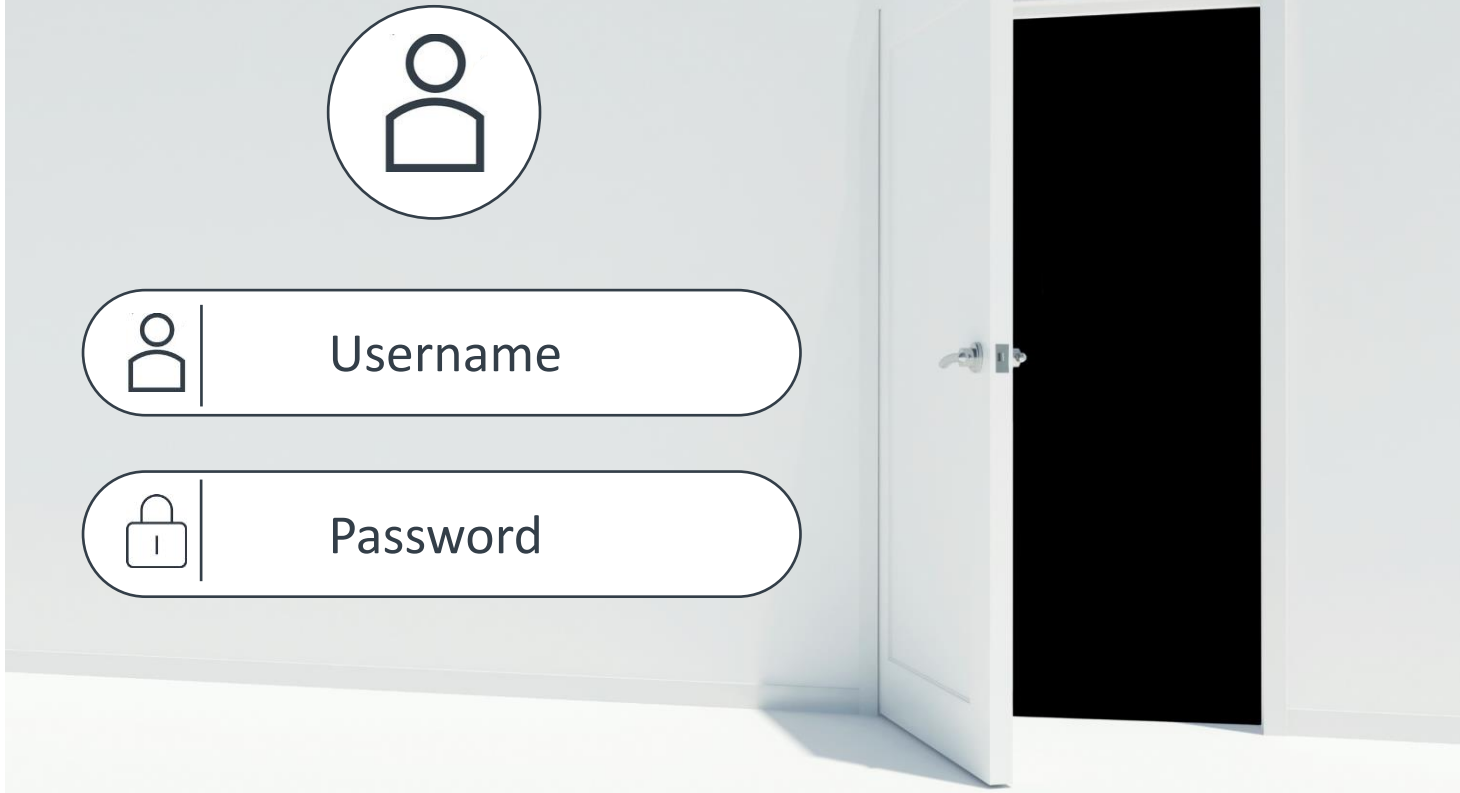
As the foundation of a global ecosystem of technology innovators, we empower the world's most successful business and consumer brands with computing everywhere.

Total Computing experience.

arm

1993

My first digital identity



arm

Authentication

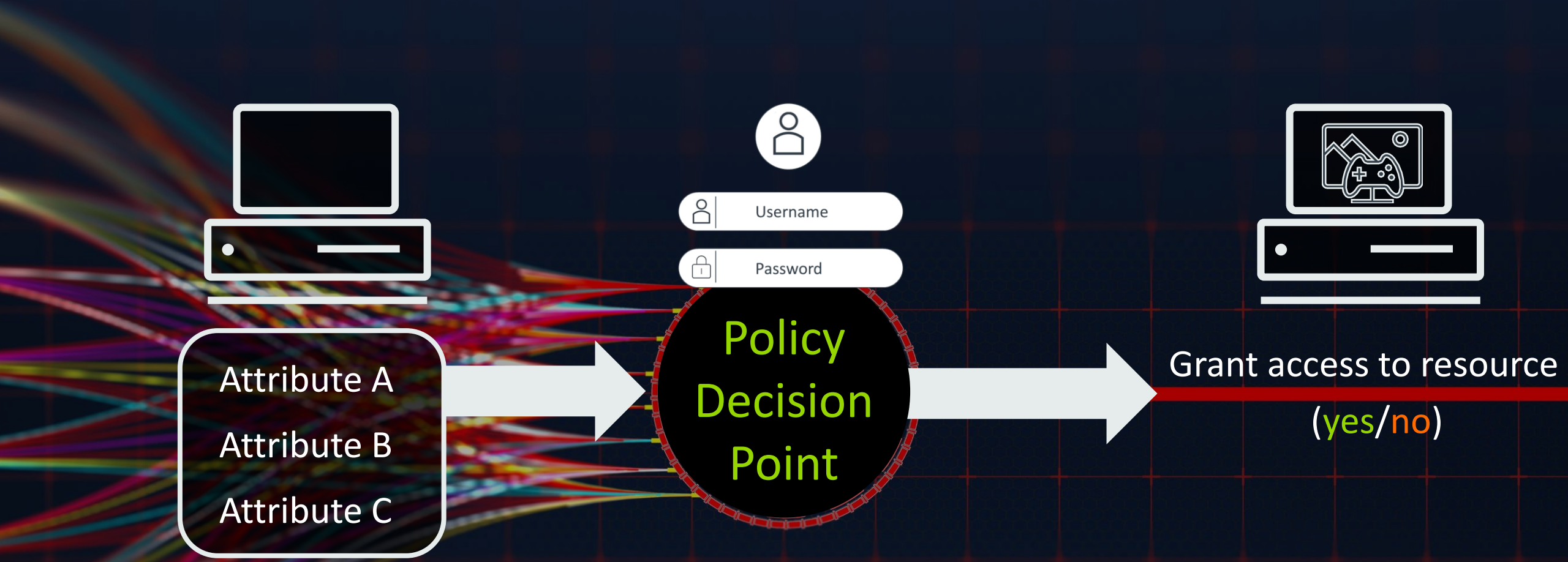
arm

Why?

To play Doom

Source: Doom® - Bethesda.net

The Point of Identity Systems is to Manage Resources



arm

2019 – New World of Apps

8.9

Million Apps in App Stores Worldwide in 2019

source: RiskIQ

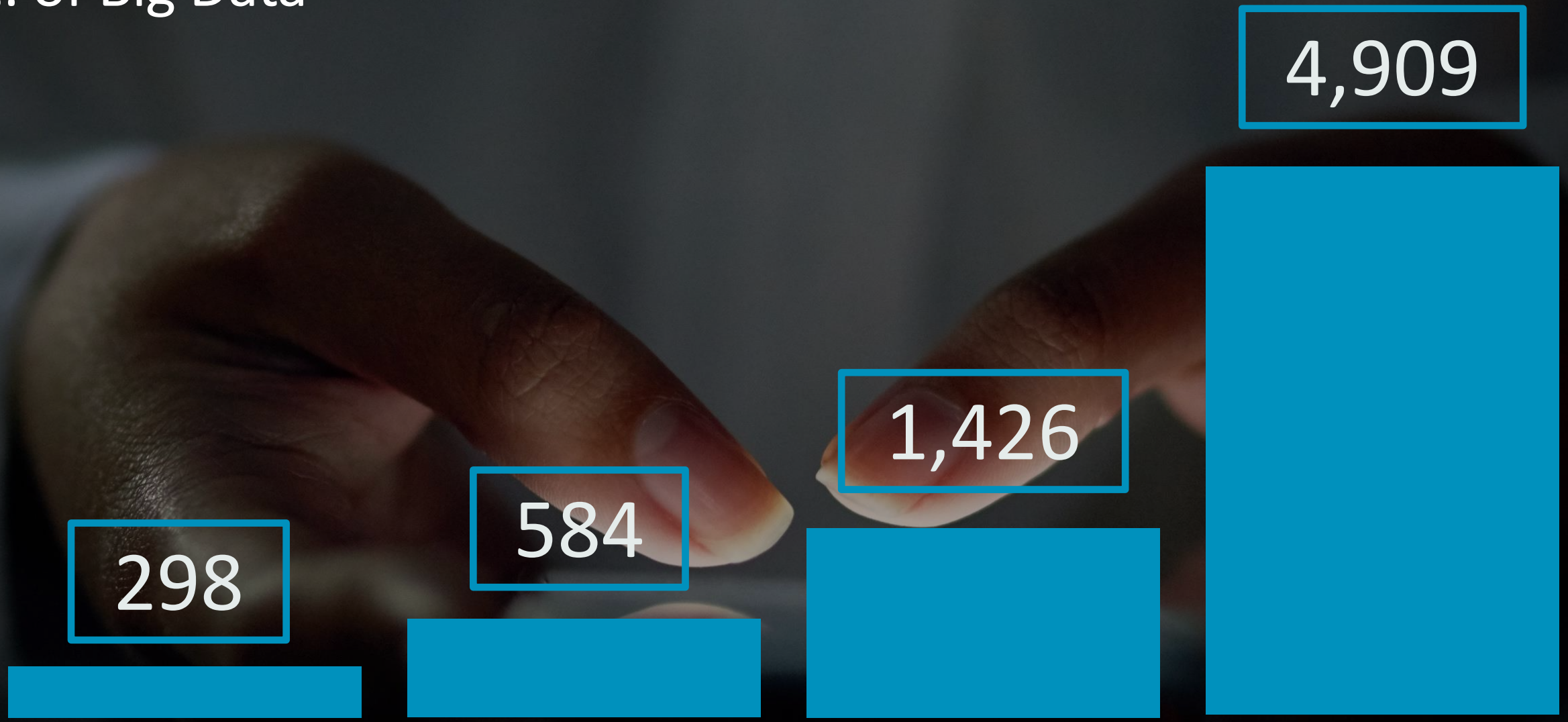
204

Billion App Downloads in 2019

source: App Annie State of Mobile 2020

arm

… of Big Data



** Data Age 2025: The Digitization of the World. IDC and Seagate Dec. 2018 https://www.seagate.com/our-story/data-age-2025/*

arm

…and Data Trails, of Ourselves, Across All the Apps We Use

SECURITY/USABILITY ISSUES

- Honey pots of passwords
- Surveillance

DATA TRAILS

- Correlation, identification
- Secondary storage and usage
- Behavioural Nudging

arm

Technology Response

DISSOCIATE SENSITIVE DATA FROM ONLINE ACTIVITIES

Sign in with …

Self-sovereign Identities

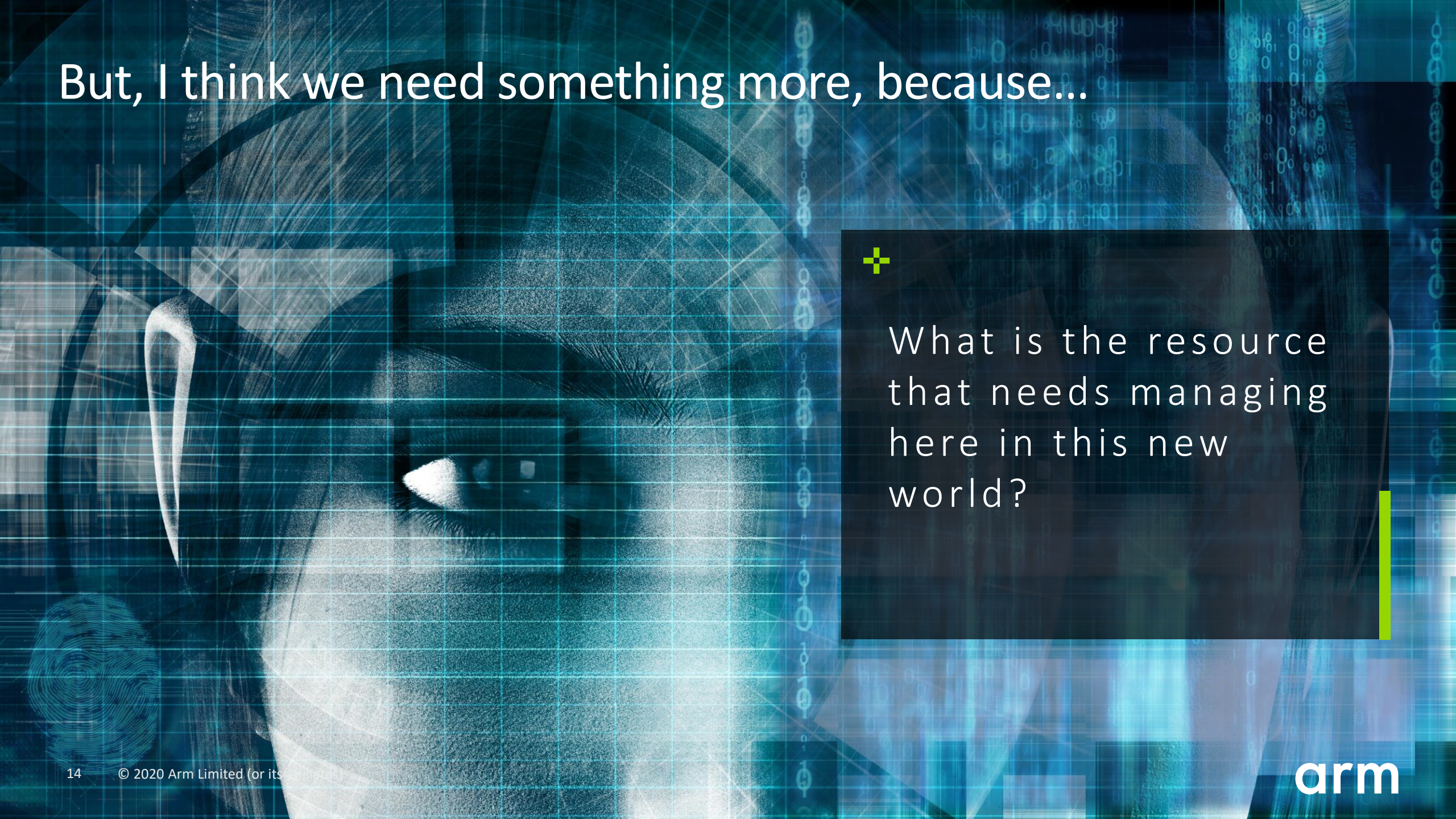
Platform COVID Bluetooth APIs

Cloak of Invisibility

Policy Response – Chain of Custody

arm

But, I think we need something more, because…



What is the resource that needs managing here in this new world?

Fundamental Change in Nature of Computing

Direction
Manipulation

arm

Fundamental Change in Nature of Computing

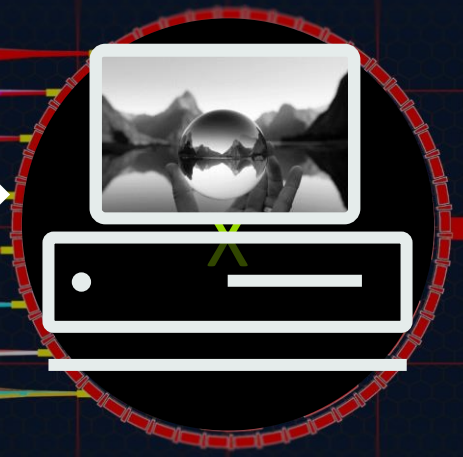
Intention Driven, needs Context and Data

arm

Economic Issue
The valuable resource now is our spending, our relationships

$ value

External/3rd party oracle



Wouldn't it be good to have a personal oracle to navigate the new digital landscape ?

arm

What is a personal oracle – one perspective

Acts on our behalf and extends our control

Ensuring we are the main beneficiary

Involves us in decision making

arm

Arm's role

Key Future Challenges

- How do we address privacy concerns while still enabling analytics
- How do I convince consumers that their data does not leave their device?
- How do I control and protect data I have given someone else?
- How do we make it widely accessible to developers
- How do I prove that my system is trustworthy

What's needed

Architecture support for Secure Enclaves that are:

- **Secure** – protects data and applications in use
- **Attestable** – Providing assurance, Emphasis on HW and Firmware provenance
- **Dynamic** – flexible workloads and accessible to developers

arm

Trust Manifesto

arm AI

November 6th, 2019

Toward Trustworthy AI Development: Mechanisms for Supporting Verifiable Claims*

Miles Brundage[1†], Shahar Avin[3,2†], Jasmine Wang[4,29†‡], Haydn Belfield[3,2†], Gretchen Krueger[1†], Gillian Hadfield[1,5,30], Heidy Khlaaf[6], Jingying Yang[7], Helen Toner[8], Ruth Fong[9], Tegan Maharaj[4,28], Pang Wei Koh[10], Sara Hooker[11], Jade Leung[12], Andrew Trask[9], Emma Bluemke[9], Jonathan Lebensold[4,29], Cullen O'Keefe[1], Mark Koren[13], Théo Ryffel[14], JB Rubinovitz[15], Tamay Besiroglu[16], Federica Carugati[17], Jack Clark[1], Peter Eckersley[7], Sarah de Haas[18], Maritza Johnson[18], Ben Laurie[18], Alex Ingerman[18], Igor Krawczuk[19], Amanda Askell[1], Rosario Cammarota[20], Andrew Lohn[21], David Krueger[4,27], Charlotte Stix[22], Peter Henderson[10], Logan Graham[9], Carina Prunkl[12], Bianca Martin[1], Elizabeth Seger[16], Noa Zilberman[9], Seán Ó hÉigeartaigh[2,3], Frens Kroeger[23], Girish Sastry[1], Rebecca Kagan[8], Adrian Weller[16,24], Brian Tse[12,7], Elizabeth Barnes[1], Allan Dafoe[12,9], Paul Scharre[25], Ariel Herbert-Voss[1], Martijn Rasser[25], Shagun Sodhani[4,27], Carrick Flynn[8], Thomas Krendl Gilbert[26], Lisa Dyer[7], Saif Khan[8], Yoshua Bengio[4,27], Markus Anderljung[12]

[1]OpenAI, [2]Leverhulme Centre for the Future of Intelligence, [3]Centre for the Study of Existential Risk, [4]Mila, [5]University of Toronto, [6]Adelard, [7]Partnership on AI, [8]Center for Security and Emerging Technology, [9]University of Oxford, [10]Stanford University, [11]Google Brain, [12]Future of Humanity Institute, [13]Stanford Centre for AI Safety, [14]École Normale Supérieure (Paris), [15]Remedy.AI, [16]University of Cambridge, [17]Center for Advanced Study in the Behavioral Sciences, [18]Google Research, [19]École Polytechnique Fédérale de Lausanne, [20]Intel, [21]RAND Corporation, [22]Eindhoven University of Technology, [23]Coventry University, [24]Alan Turing Institute, [25]Center for a New American Security, [26]University of California, Berkeley, [27]University of Montreal, [28]Montreal Polytechnic, [29]McGill University, [30]Schwartz Reisman Institute for Technology and Society

April 2020

Consortium Members [August 2020]

Premier

accenture · 蚂蚁金服 ANT FINANCIAL · FACEBOOK · HUAWEI · Microsoft · ORACLE · Alibaba Cloud · arm · Google · intel · Red Hat

General

AMD · ByteDance · CYSEC · KINDITE · Anqlave · cosmian · OASIS LABS · NVIDIA · r3. · anjuna · decentriq · Fortanix · swisscom · vmware · CONFIDENTIAL COMPUTING CONSORTIUM

Looking forward

Additional Industry and Policy collaboration

Industry Collaboration

Assurance for TrustWorthy AI

Policy Research and Data Points to guide

https://www.arm.com/blogs/blueprint/arm-ai-trust-manifesto
https://confidentialcomputing.io/

arm

arm

Thank You
Danke
Merci
谢谢
ありがとう
Gracias
Kiitos
감사합니다
धन्यवाद
شكرًا
ধন্যবাদ
תודה