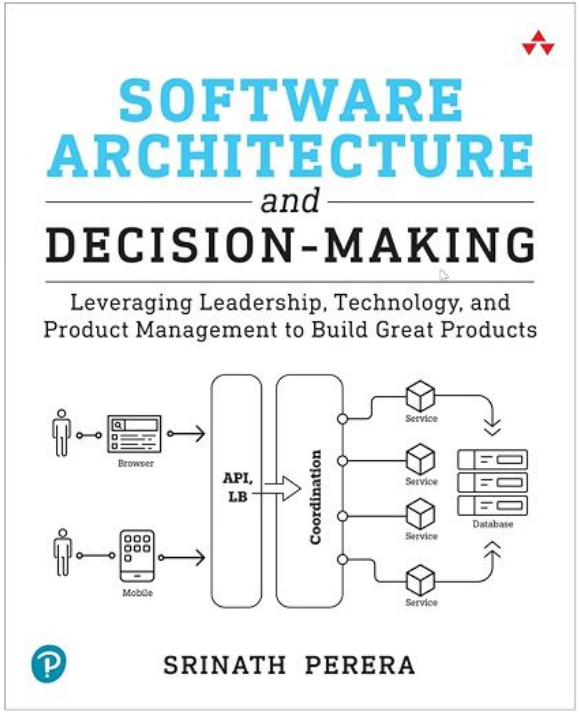
Trust, Control, and Digital Sovereignty with Open Source

Srinath Perera,
Head of Research,
WSO2

WSO2

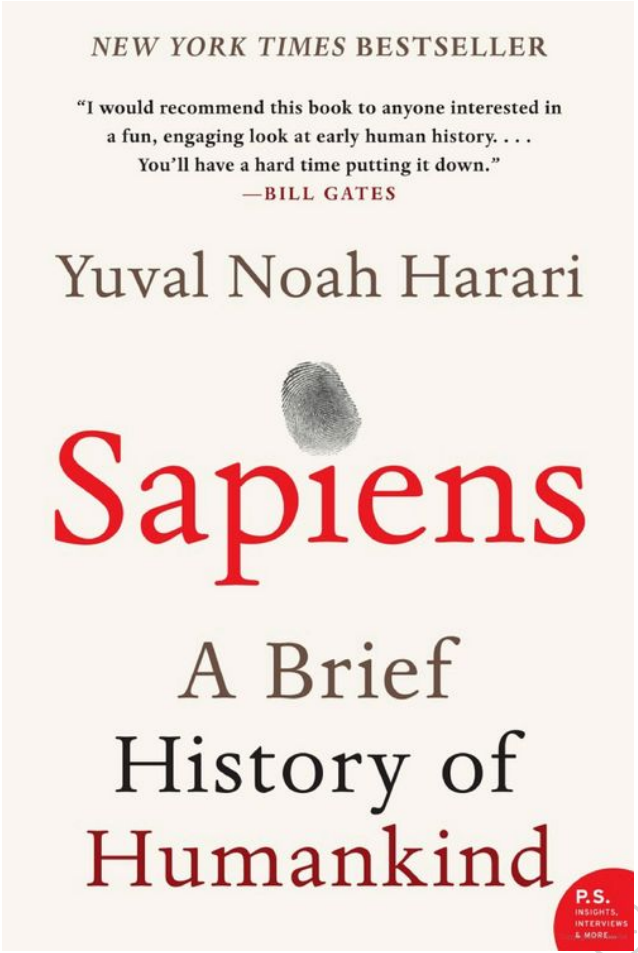
Who am I?

- Long term (20+y) Open Source Contributor
  - Apache Member, one of the people who started Apache Axis2
- Author of the book “Software Architecture and Decision-Making” (Pearson, 2024)
- Researcher working on AI + Systems
  - (e.g., we had agent reliability paper at ACM CAIS), has 1500+ citations, 40+ peer reviewed papers
- Other
  - Did my Ph.D. in US, came back and live in Sri Lanka
  - Enjoys reading and photography
  - Opinionated guy but believe in continual dialog

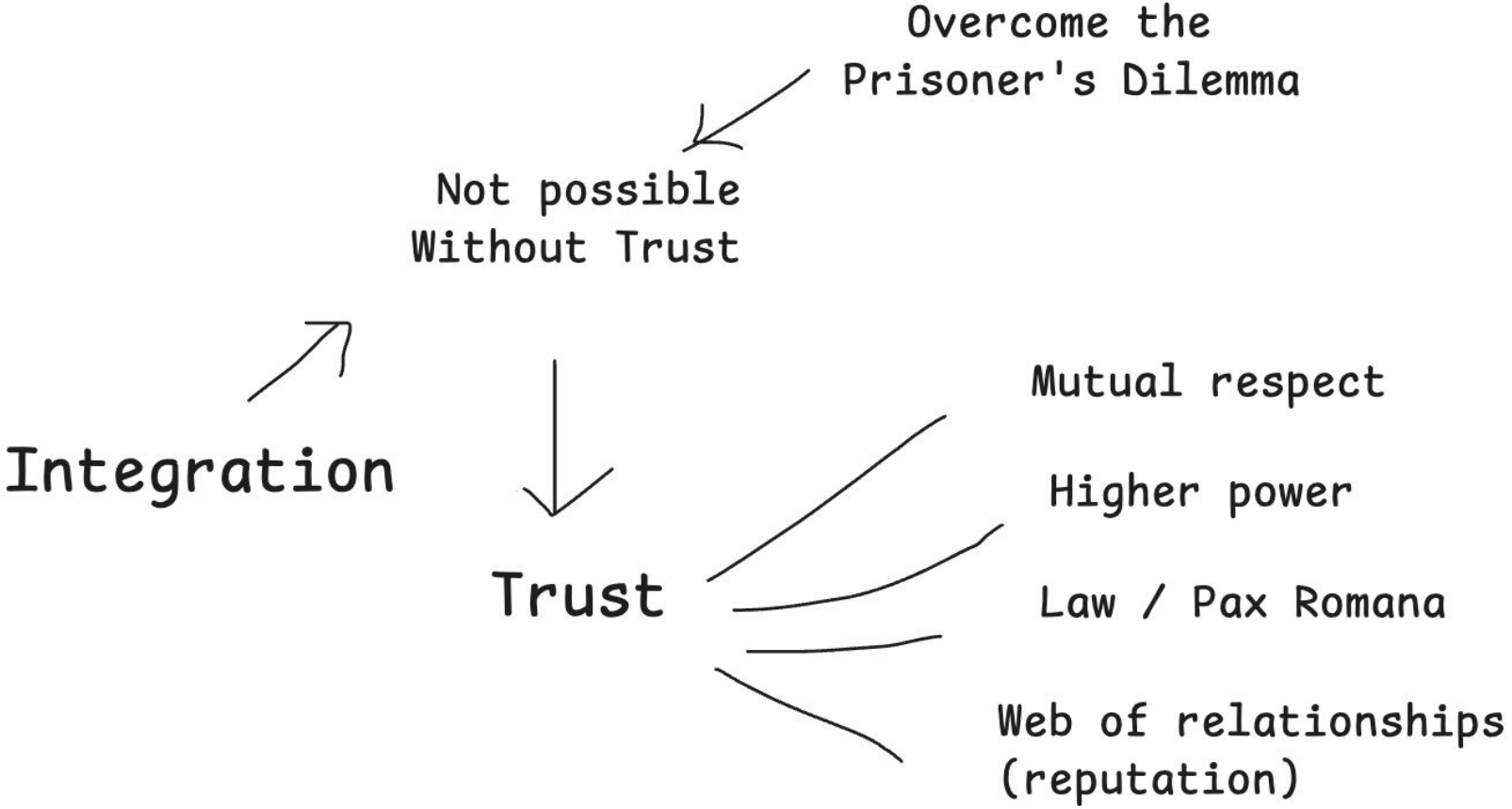


A Story of Two Trends

- Sovereignty vs. Integration
- History is a story of how we moved from groups → cities → countries, etc.
- Integration under one story has helped us.
  - Trade has been a key driver.
- But we need to be careful: those who could not protect Sovereignty are erased from history!



Trust Fuels Integration



Classical Sovereignty → Digital Sovereignty

The state has supreme power over its territory and is independent of others.
key aspects (e.g., food, energy).

Classical Sovereignty

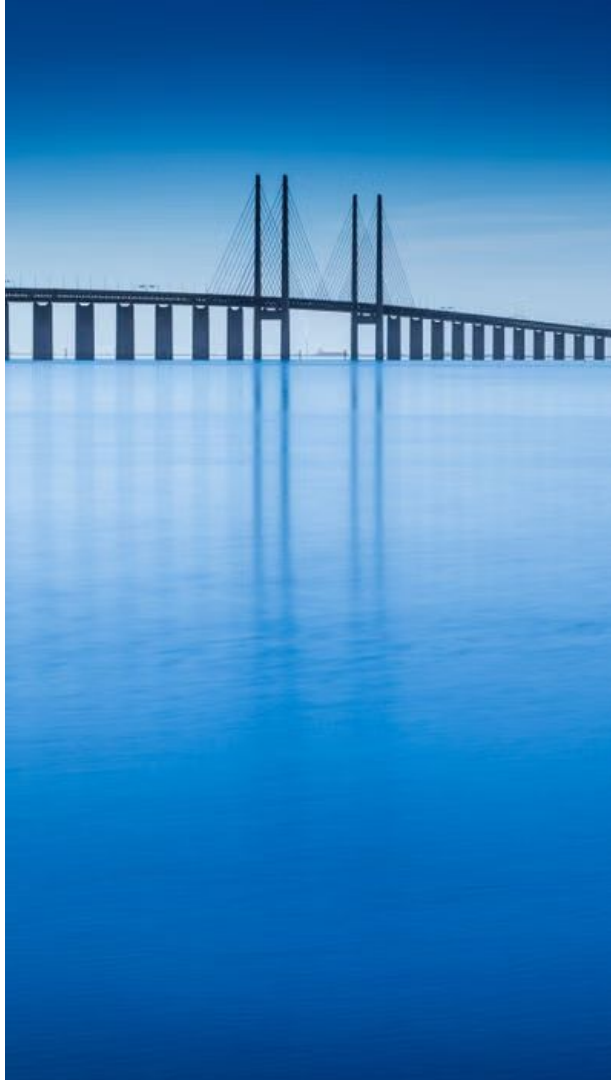
Control via gatekeepers at borders

The digital world makes territory fluid.

an evolving concept

Digital Sovereignty

Enterprises need to adapt



A Balancing Act

High Sovereignty

Low integration

Low Sovereignty

High integration

irrelevance

lost Identity
and/or agency

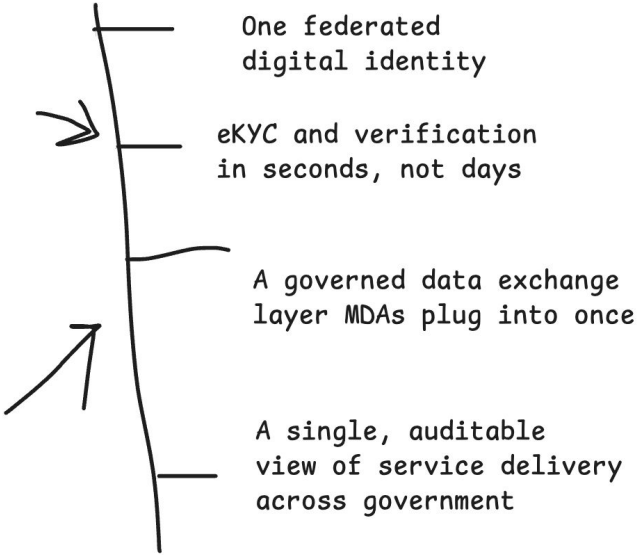
“A ship is safe in harbor, but that's not what ships are for.”
— John A. Shedd

Digital is a Key Driver of Integration

- Digital technologies have made the world seem smaller and more efficient.
- For example, Enterprise Integration and API management let different systems work together.
- Standards (ISO 20022, FDX, SWIFT, PSD2, FAPI, India’s UPI, …)
- Regulations (e.g., Open Banking, PSD2, Data Exchange Platforms)

The African Union Digital Transformation Strategy for Africa

AfCFTA (African Continental Free Trade Area)



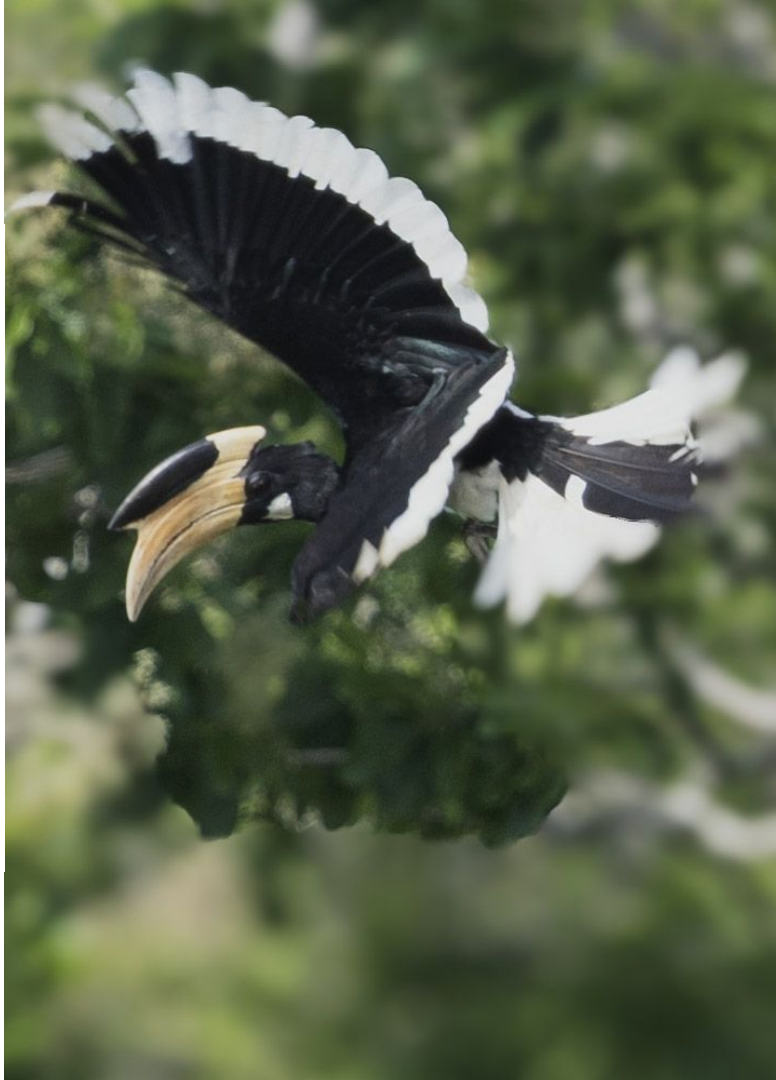
One federated digital identity

eKYC and verification in seconds, not days

A governed data exchange layer MDAs plug into once

A single, auditable view of service delivery across government

e.g., NITA Uganda



MM.DD.YYYY

Old Safeguards are not Enough

WSO2

Digital Sovereignty: Historical Triggers

Snowden revelations

↘

focus on privacy

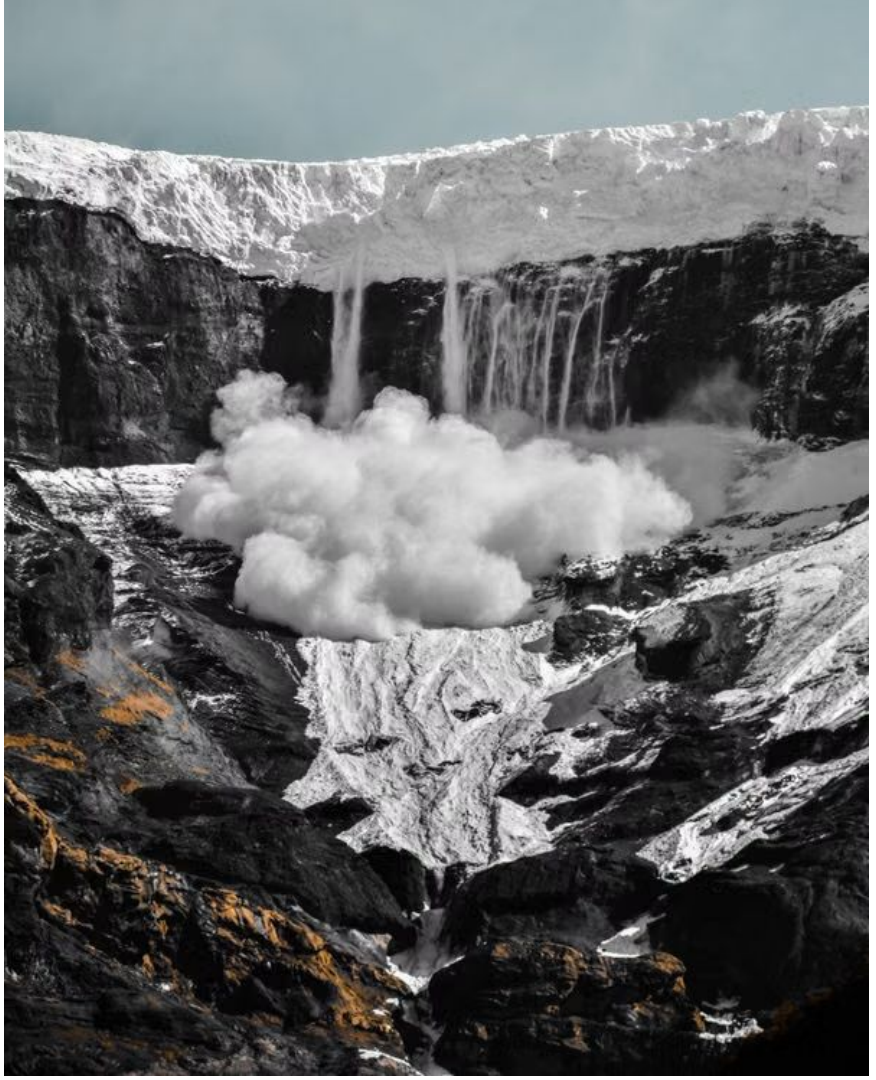
↓

GDPR — give users control over their data

CLOUD Act — letting the US ask any US-based tech company to hand over data regardless of where they are stored

↑

US asked a US tech giant to provide details about a suspect stored in Ireland, and when a legal battle ensued



Core pillars of Digital Sovereignty

- Data Control
  - Ensuring that personal and business data stays within local legal borders and follows regional privacy rules.
- Administrative Control
  - Operational Rules: Keeping administrative access and security responses inside trusted local teams and laws.
- Technical Independence
  - Building open software and hardware systems to avoid getting trapped by a single foreign supplier.
- Legal Compliance
  - Ensuring compliance to laws and regulations covering the above three

More dimensions

- Scopes
  - Country
  - Enterprise
  - Personal
- Three "layers" of the digital sphere [1]:
  - the physical layer (infrastructure, hardware),
  - the code layer (standards, software, system design)
  - the data/information layer (content, data flows, ownership)

[1] by Yochai Benkler.

Challenges to Digital Sovereignty

- Data
  - Mass surveillance and privacy erosion
  - Lost control over data
- Administrative
  - Erosion of state capacity to regulate and govern
  - Economic/competitive disadvantage and "digital colonialism."
- Technical Independence
  - Vendor lock-in in public administration
  - Structural dependence on a handful of foreign providers
  - National-security risk from foreign hardware/software
- Legal Compliance: Making sure that all digital actions answer to local courts and national laws instead of foreign regulations.
  - Extraterritorial legal exposure

	Data	Administrative	Technical Independence	Legal Compliance
Country	- Losing control of data - Mass surveillance - Privacy erosion	- Erosion of state capacity to regulate and govern - Economic/competitive disadvantage - Vendor lock-in in public administration	Structural dependence on a handful of foreign providers National-security risk from foreign hardware/software	
Enterprise	Covered under Legal Compliance	Covered under Legal Compliance	Vendor lock-in	- Extraterritorial legal exposure (dominant providers are US- or China-based)
Personal	- Losing control of data and how it is used - Mass surveillance - Privacy erosion			

	Data	Administrative	Technical Independence	Legal Compliance
Country	- Losing control of data - Mass surveillance - Privacy erosion	- Erosion of state capacity to regulate and govern - Economic/competitive disadvantage - Vendor lock-in in public administration	Structural dependence on a handful of foreign providers National-security risk from foreign hardware/software	
Enterprise	Covered under Legal Compliance	Covered under Legal Compliance	Vendor lock-in	- Extraterritorial legal exposure (dominant providers are US- or China-based)
Personal	- Losing control of data and how it is used - Mass surveillance - Privacy erosion			

Solutions

- Data
  - Rights-based regulation
    - Data localization / data residency laws
- Technical Independence
  - Interoperability and open standards as an alternative to full ownership
  - Free and open-source software (FOSS) mandates or preference
  - Procurement reforms favouring SMEs, domestic and open-source suppliers
  - Sovereign cloud infrastructure

Solutions (long term)

- Increase capability
  - Industrial policy and public investment in domestic capability
  - The European Chips Act (target: 20% of global semiconductor market by 2030)
- Capacity-building and digital literacy investment
- Education reform, research funding, and South-South knowledge exchange.
- Multilateral/international cooperation

Broad List of Laws and Compliance needs

- Can be understood in terms of tension between the US and other countries
- Right to access data
  - [US] Foreign Intelligence Surveillance Act (FISA, 2008) -
    - US can access data held by US-owned companies, including data about non-US persons stored abroad.
  - [US] CLOUD Act - 2018
    - US can access data held by US companies worldwide and other countries may obtain reciprocal access via bilateral agreements.
  - [China] Cybersecurity Law (CSL) and follow up Statutes
- Right to cut off services
  - International Emergency Economic Powers Act (IEEPA) - 1977
    - US can declare a national emergency and order US companies to cease business with sanctioned individuals, organisations or states

Broad List of Laws and Compliance needs [Safeguards]

- Protect data - by giving citizens control over the personal data
  - [EU] General Data Protection Regulation (GDPR, 2016)
  - [China] Personal Information Protection Law (PIPL, 2021)
  - EU-US Data Privacy Framework - Executive agreement / adequacy decision 2023, following Schrems II (2020) to provide a lawful basis for EU-to-US personal data transfers
- Reduce dependence
  - China "3-5-2" directive (2017) - Ordered Chinese government bodies and public institutions to phase out foreign computer hardware and software over three years
  - Free/open-source-software mandates (Global South and India) - e.g., Policy on Adoption of Open Source Software for Government of India (2015)
- Protect the market
  - Digital Services Act (DSA,2022) - To regulate content moderation and platform accountability obligations across the EU digital single market.
  - Digital Markets Act (DMA, 2022) - To constrain the market power of large "gatekeeper" platforms and guarantee competition and market access in the EU digital economy.

Challenges associated with Solutions

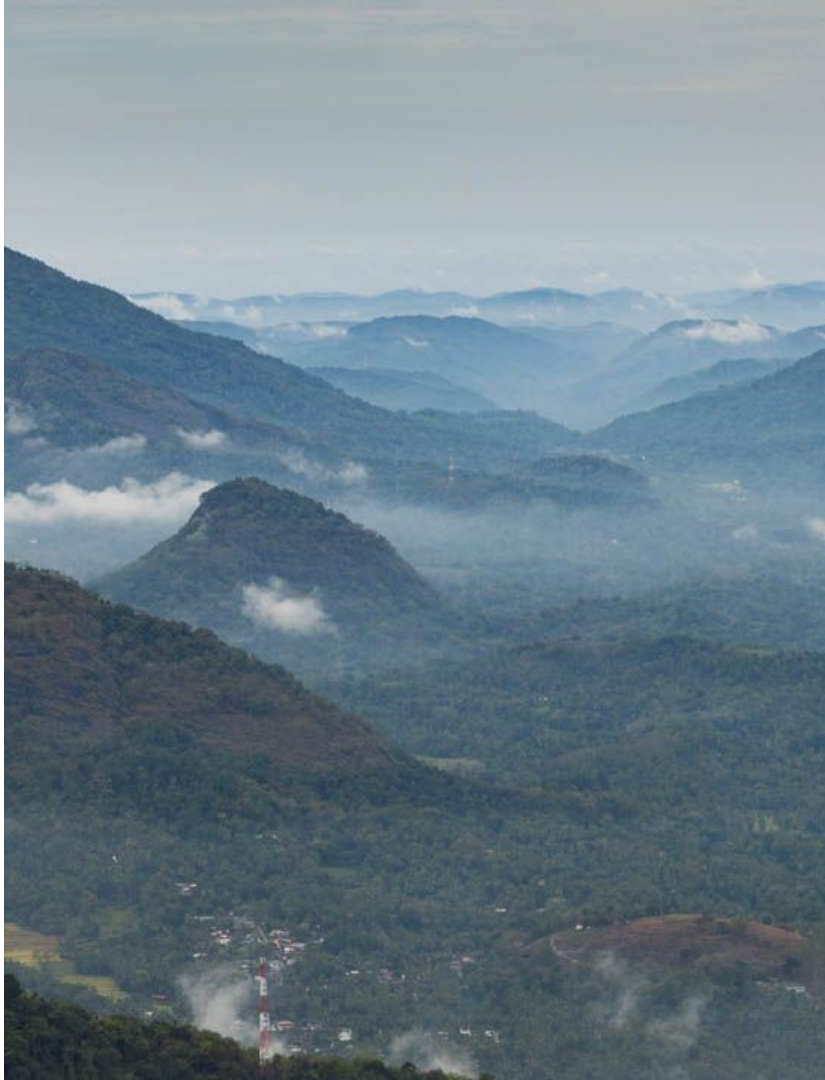
- Too slow for a fast-changing IT world
  - Rights-based regulation (GDPR, DSA, DMA, AI Act). Comprehensive regulation requires extended debate and accountability, which can slow responsiveness to fast-moving technology
- Higher costs
- Lack of skills & Funds
  - Lack of people with skills to maintain open systems at scale
  - Lack of funding for projects (e.g., migration projects)
  - Lack of funding for open source projects
- Lack of solutions
  - E.g. The EU's flagship "sovereign cloud" project admitted the American and Chinese providers

Challenges associated with Solutions (Contd.)

- Sovereignty-washing
  - a persistent, well-documented gap between sovereignty rhetoric and actual implementation
- Fragmentation + Centralisation
  - Pushes against open market model (you do what you are good at and depend on other for what they are good at)
  - Does this push us towards fragmented regions?

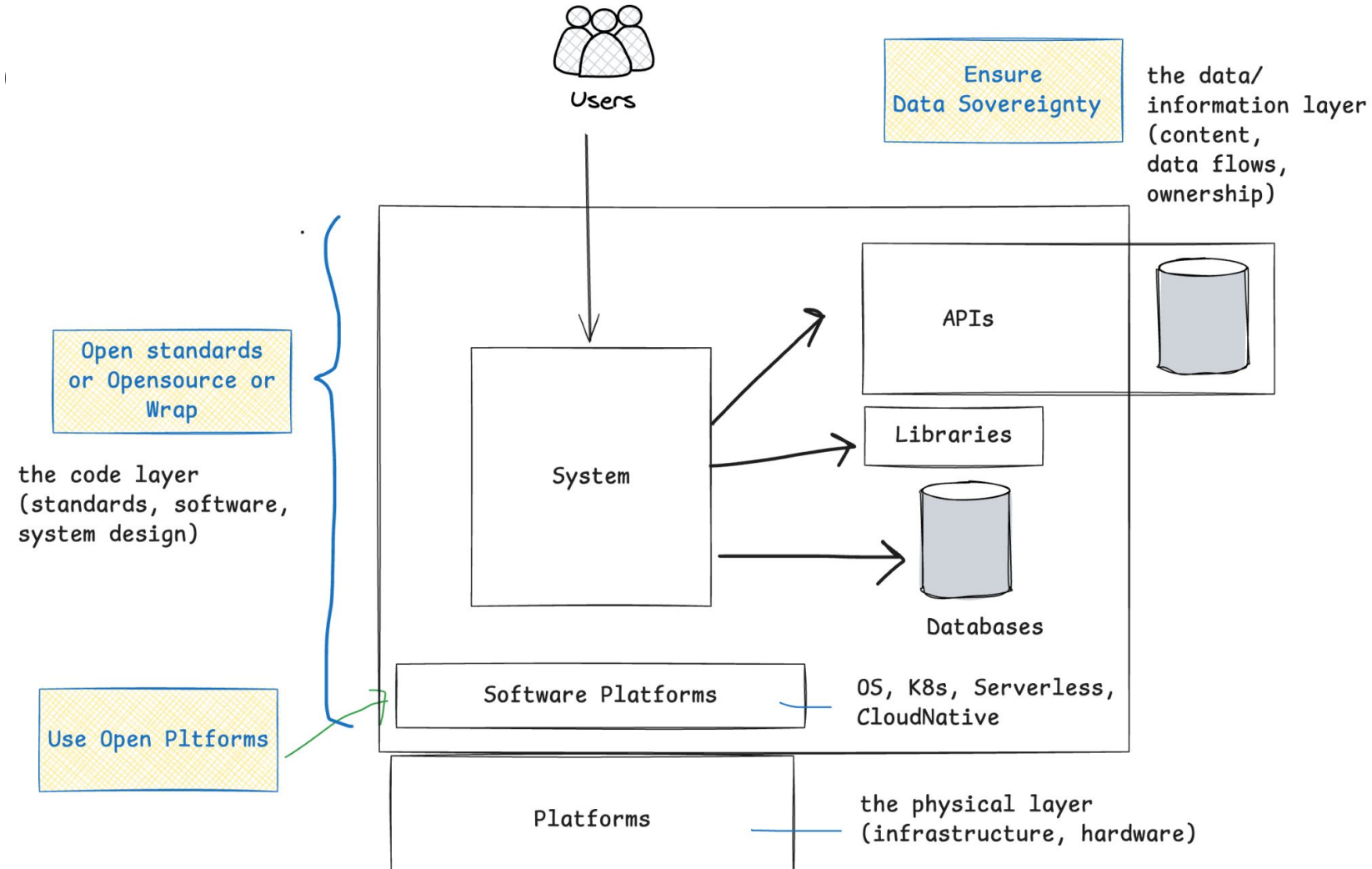
What This Means for Software?

- Current and future perspective
  - Requirement change: need to be able to support current and future requirements (*Context is the King!*)
  - Mandatory for some government projects
  - Even when optional, it is preferred due to service cutoff risks! (IEEPA)
  - Customers may also think the same, so optional regulations and suggestions might become deal breakers
- Data and Administrative Control
- Technical Independence



Handling Data Sovereignty

- Privacy and giving the users choice and control is the key!!
  - Give the data principal the right to decide who accesses what, for what purpose, and for how long
- How?
  - Keep the data in the region
  - GDPR vs. Cloud Act tension is unresolved
    - Customer-held keys
    - Cross-border transfer mechanisms

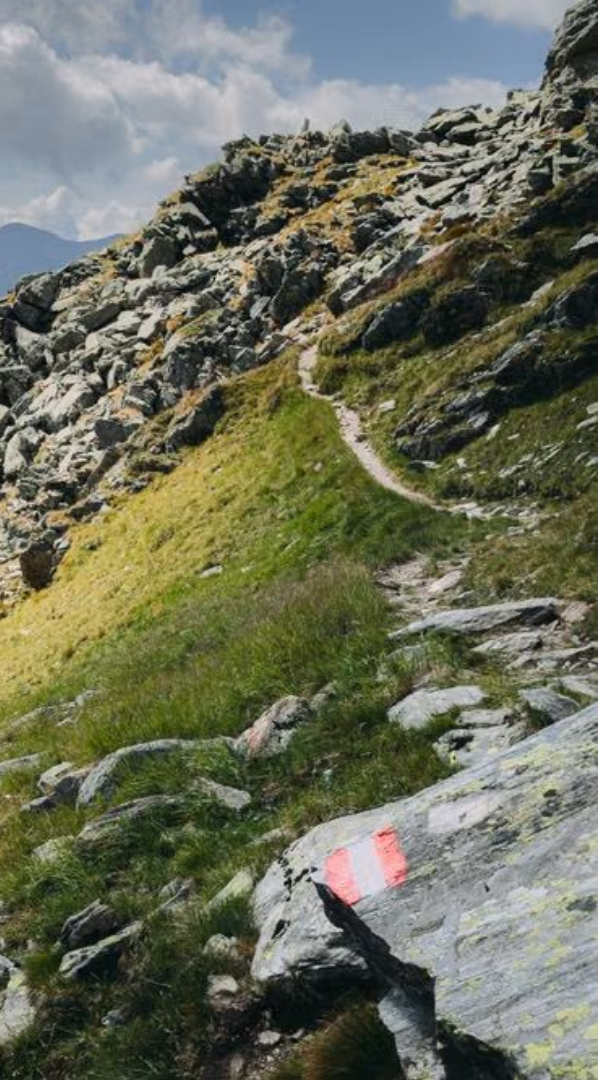

Users
Ensure
Data Sovereignty
the data/
information layer
(content,
data flows,
ownership)
APIs
Open standards
or Opensource or
Wrap
Libraries
the code layer
(standards, software,
system design)
System
Databases
Use Open Pltforms
Software Platforms
OS, K8s, Serverless,
CloudNative
Platforms
the physical layer
(infrastructure, hardware)

What This Means for Software? Independence

- Use an open platform (hard/ impossible to wrap)
- Dependencies (APIs, libraries) - use open standards, open source, or wrap
- Do not expose proprietary technologies to customers; use open messages and protocol formats and standardized configurations
- I have written extensively about best practices in
  - How to Evolve Software for Minimum Disruptions: The Architect's Two Hats

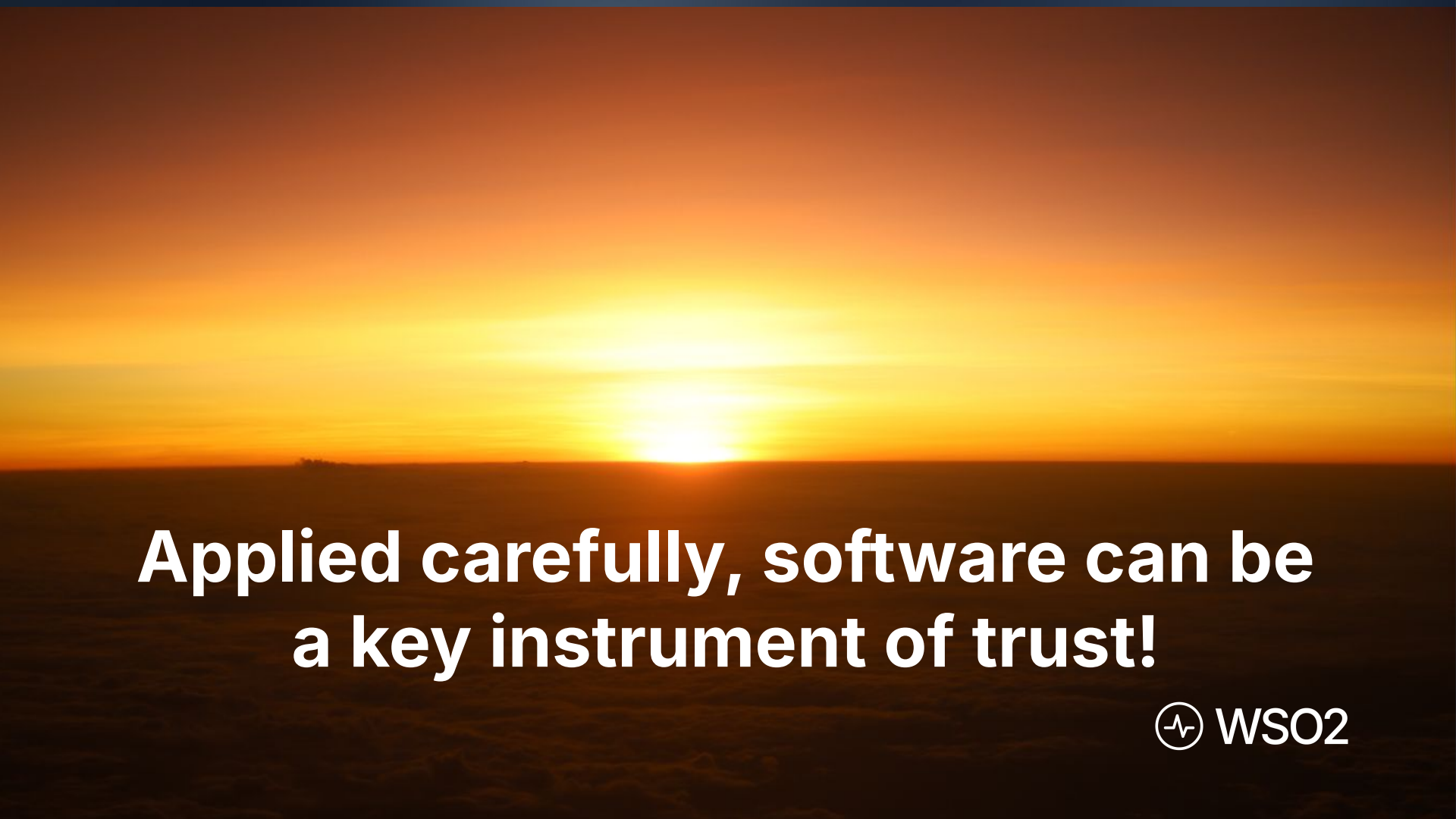
Real Life Challenges

- Open standard or open source project may not be available
  - Too slow for a fast changing IT world
  - Best solutions may be protected by IP
- Lack of skills
  - Weaker Community
  - Scarce hirable expertise
- Need to go back to key question “how much work to move away?” and do our best
- It may cost us more in the short term
- In the long term, it will create more open standards and open source projects



Challenges with Open Source

- Security and vulnerability-management responsibility shifts onto the adopter, not a vendor
- Open Source sustainability
  - Open source "does not eliminate cost, it redistributes it"
  - if the community fails
    - A small number of maintainers can become a single point of failure — and a security risk
    - Most organizations still consume far more open source than they govern or contribute back
- "Open" doesn't automatically mean "not locked in"
  - E.g., a single-vendor open-core projects


Applied carefully, software can be
a key instrument of trust!
WSO2

A Few Examples

- NITA Uganda - a data Exchange Platform for improving government efficiency and enhancing citizen interaction
- The Reserve Bank of India (RBI) is India - The ULI platform dramatically cut loan processing time from 4–6 weeks to just minutes
- POLIGRAFICO E ZECCA DELLO STATO ITALIANO - The IT Wallet has transformed digital identity verification in Italy, with 33+ million citizens onboarded, and authentication by over 60%

Conclusion

- Two competing forces: integration and sovereignty ebb and flow with time.
- Digital sovereignty is an outcome of natural power dynamics; it is a fact of life.
- We need to achieve integration while protecting sovereignty; it is a tightrope.
- From a software point of view, it is about Data and Administrative Control and Technical Independence
    - We need to take the long view, and dynamics will likely change, and we will need to adapt
    - Data and Administrative Control is much about keeping data in administrative domains.
    - Technical Independence is achieved through standards and open source

We face challenges, but our job is to get there, one step at a time if we must!!

Questions?

WSO2