

The next tripartite governance systems: governments, markets, and commons

FINAL REPORT

PREPARED BY
CSIL
CORSO MONFORTE 15,
20122 MILAN, ITALY
http://www.csilmilano.com/

CONTACT PERSON
Silvia Vignetti
vignetti@csilmilano.com
+39 0284143541

This report was commissioned by the Digital Infrastructure Insights Fund and Aspiration, Washington DC

Principal Investigator: Marco Berlinguer
Research team: Massimo Florio, Martina Gazzo, Silvia Vignetti

.

Cover photo: Getty Images for Canva



CONTENTS

EXECUTIVE SUMMARY 8

1. INTRODUCTION 15

1.1. Background and context 15

1.2. An evolutionary approach 16

1.3. A polycentric governance system 18

2. OBJECTIVE AND METHOD 19

2.1. Objective 19

2.2. Methodology 19

2.3. Selected relevant cases 21

2.4. Limitations 23

3. TAXONOMIES OF GOVERNANCE MODELS 26

3.1. Definitions 26

3.2. Taxonomy 1: governance models 28

3.3. Taxonomy 2: governmental rationales for intervention 35

3.4. Taxonomy 3: Community Roles in Open & Collaborative Tech Governance 40

4. DISCUSSION AND FURTHER ANALYSIS 45

4.1. Defining standards, aggregating ecosystems 48

4.2. Pursuing security and sovereignty by open tech 50

4.3. The strategic deployment of openness in industrial policy 52

4.4. Digital public infrastructure: the return of the hesitant state 54

4.5. The evolving logic of community in tripartite open tech governance 58

5. FURTHER RESEARCH 62

5.1. The mission ahead: developing a polycentric approach to open tech governance 62

5.2. The structural rarity of balance 63

REFERENCES 67

Annex 1. FACT-SHEETS OF THE CASES 76

Astra Linux 78

Conecte SUS (now Meu SUS Digital) 81

Copernicus Program 84

Decidim 87

Digital Public Goods Alliance (DPGA) and DPG Standards 90

ELIXIR (European Life-Sciences Infrastructure for Biological Information) 94
European Open Science Cloud (EOSC) 97
Gaia-X European Association for Data and Cloud AISBL 100
Gitee (码云, Mǎyún) 103
Hyperledger 106
India Stack 109
MOSIP (Modular Open Source Identity Platform) 113
X-Road / Nordic Institute for Interoperability Solutions (NIIS) 116
Open European Software-Defined Vehicle Platform (SDV) 119
Open Wallet Foundation (OWF) 122
OpenAtom Foundation 125
OpenSRP (Open Smart Register Platform) 128
Open Source Security Foundation (OSSF) 131
O-RAN Alliance 134
Open-Source Software Security Initiative (OS3I) 137
Risc-V International 141
Rust 145
scikit-learn 148
Signal Foundation 151
Simpl 154
Sovereign Tech Fund (now part of Sovereign Tech Agency) 157
ZenDiS (*Zentrum für Digitale Souveränität der Öffentlichen Verwaltung*) 160
Annex 2. DEEP DIVES ON SELECTED CASES 163
A Shared Architecture: The Tripartite Governance of Risc-V in an Age of Geopolitical Fragmentation 164
Gaia-X: A European Experiment in Digital Sovereignty and Industrial Policy 172
India Stack: State Power, Market Forces, and an Elusive Commons 180
Decidim: The Deliberate Building of a Public-Community Alliance 185

LIST OF ABBREVIATIONS

AISBL	*Association Internationale Sans But Lucratif* (International Non-Profit Association)
BMWK	German Federal Ministry for Economic Affairs and Climate Action
CDSE	The Copernicus Data Space Ecosystem
DARPA	Defense Advanced Research Projects Agency
DBT	Direct Benefit Transfer
DPGA	Digital Public Goods Alliance
DPI	Digital public infrastructure
EC	European Commission
EIR	Electronic Immunization Registry
EO	Earth Observation
EOSC	European Open Science Cloud
ESA	European Space Agency
EUDI	EU Digital Identity Wallet
FOSS	Free and Open Source Software
FSB	Defense Ministry and Federal Security Service
FSF	Free Software Foundation
FTE	Full-Time Equivalent
GDI	Genomic Data Infrastructure
GMES	Global Monitoring for Environment and Security
GPL	General Public License
ISA	Instruction Set Architecture
ITU	International Telecommunication Union
JSC	Joint-stock company
MAC	Mandatory Access Control
MIIT	China's Ministry of Industry and Information Technology
MVP	Minimum Viable Product
NIIS	Nordic Institute for Interoperability Solutions
NPCI	National Payments Corporation of India
NSF	National Science Foundation
OAI	OpenAirInterface
OCR	Optical Character Recognition

ODI	Open Digital Infrastructures
OMB	Office of Management and Budget
ONCD	Office of the National Cyber Director, coordinated by the White House
OSI	Open Source Initiative
OSSPI	Open-Source Software Prevalence Initiative
OSTIF	Open Source Technology Improvement Fund
OWF	Open Wallet Foundation
PAHO	Pan American Health Organization
PKI	Public Key Infrastructure
RAN	Radio Access Network
RBI	Reserve Bank of India
RFI	Request for Information
RIA	Estonia's Information System Authority
SAB	Scientific Advisory Board
SRIA	Strategic Research and Innovation Agenda
STF	Sovereign Tech Fund
UIDAI	Unique Identification Authority of India
UPI	Unified Payments Interface

EXECUTIVE SUMMARY

On November 1, 2024, CSIL was awarded a grant by Aspiration to conduct a study titled *"The Next Tripartite Governance Systems: Governments, Markets, and Commons."* This project aims to explore innovative governance models that integrate governments, markets, and commons in the promotion, development and maintenance of open technology initiatives. This document is the **Final Report** and illustrates the activities carried out, the main findings and suggestions for future research.

Objectives and context

This research explores emerging approaches to the governance of open information technology initiatives**,** focusing on the interplay between three key actors: developer communities, commercial companies, and government bodies. Whilst the strategic adoption of open-source technologies by private enterprises is well documented (Duparc & al., 2022; Li & al., 2025), the increasingly deliberate embrace of these models by governments represents an even greater departure from the grassroots, non-economic motivations that originally characterized free software communities (Raymond, 1999; Benkler, 2002).

This research looks in particular at **the tripartite governance model that must balance community autonomy, commercial goals, and public policy objectives**, all of which can pull in different directions. The focus of our research is understanding how an effective balance is achieved between potentially conflicting objectives and different management styles, and whether such tripartite configurations prove synergistic or remain inherently unstable due to competing priorities. Though open technology initiatives continue to be modelled on the consolidated success of Free and Open Source Software (FOSS), they are now witnessing a shift from unsystematic public policy interventions to more structured and strategic forms of government involvement.

The research adopts an evolutionary perspective, recognizing that the open technology paradigm has undergone profound transformations since the 1980s, from informal communities of individual developers, through gradual corporate involvement, to the emergence of powerful open-source foundations, and finally to corporate-led ecosystems at technological frontiers. This accumulated strength explains governmental interest: open source has evolved from outsider status to foundational infrastructure, with research indicating that 70–90% of codebase composed by open-source components (Synopsys, 2022; Linux Foundation, 2020 and 2022). However, this critical role also introduces governance challenges around security, maintenance, and sustainability, catalyzing increased governmental attention.

Whilst hybrid commons-market models have long attracted scholarly attention (Berlinguer, 2018; O'Neil & al., 2021), and the strategic deployment of open technology by companies is now well established, the systematic involvement of government actors signals a **transition towards novel governance configurations**. Configurations are increasingly tripartite, involving negotiated complementarities and tensions amongst governmental institutions, market actors, and community-based initiatives. This emerging phase presents both systemic challenges and innovative practices as these three spheres attempt to reconcile their distinct logic and objectives. The trajectory, ecosystem, and structural characteristics of open technology will inevitably be transformed by this evolution. Conversely, the distinctive features of open development models, including transparency, modularity, and collaborative innovation, will likely influence state strategies and drive innovations in how public actors seek to shape technological futures.

The research was guided by two main objectives. The first was to **identify and map a sample of relevant cases** in which some form of tripartite governance models of open technology initiatives are beginning to take shape, and to collect structured information about each in the form of fact sheets. The second was to **organize these cases through the development of taxonomies with the aim at detecting possible emerging patterns, trends or prevailing governance configurations**, the aim being not merely to classify the cases, but to make sense of the underlying governance systems. More specifically, the aim was to explore the extent to which these systems may actually work in a genuinely polycentric, Ostrom-inspired sense, whereby multiple actors and levels of authority interact and adjust to one another under partially self-organised rule structures.

The **main questions** arising from these developments that we have been trying to address in our investigations are:

1. *Does a governance system involving the collaboration among governments, firms, and communities prove synergistic, leveraging the complementary capabilities of each actor, or does it generate imbalance through conflicting objectives and coordination failures? How do the actors involved negotiate trade-offs between community autonomy, commercial sustainability, and public policy objectives?*

2. *What governance mechanisms and institutional arrangements enable or constrain effective collaboration across the three spheres? Can a tripartite arrangement function as a polycentric system, i.e. multiple independent but mutually adjusting decision centers?*

3. *What are the implications of increased government involvement for the fundamental characteristics of open technology (i.e. its openness, accessibility, and community-driven innovation)?*

Methodology and scope

This research took an **exploratory approach**, motivated by the recognition that tripartite governance models for open technology initiatives are still taking shape. Rather than testing established theories, the aim was to **make sense of an emerging phenomenon** and help **build a clearer conceptual understanding of it**.

The **methodological framework** employed has been **qualitative** and centered on **comparative case study analysis**, examining 27 diverse open technology initiatives in a variety of domains and with different governance models that exemplify early-stage tripartite governance. Combining desk research (analysis of websites, specialized media, and scholarly literature) with semi-structured interviews we deep dived into the strategic objectives, institutional arrangements, and socio-political tensions characterizing each case. In the second part of the investigation we have selected 4 cases which have been analyzed in greater depth:

- **Gaia-X**: A state-initiated, market-driven European project to achieve digital sovereignty through a federated data infrastructure.
- **Risc-V**: A global, community-born open standard for processors that evolved into a tripartite "big tent."
- **India Stack**: A state-orchestrated digital infrastructure built on a philosophy of "minimalism."
- **Decidim**: A deliberately constructed Public-Commons partnership.

The **study's primary output consists of three grounded taxonomies** capturing the most significant governance dynamics across these initiatives: the **balance of influence** among stakeholder types, the **rationales for government intervention**, and the **role and composition of communities**. These taxonomies serve as analytical frameworks to bring clarity to a phenomenon

that remains incompletely understood, and to lay groundwork for future research. Cases were also classified by development stage; while this was initially expected to reveal a more uniform developmental pattern correlating with specific governance features, no such consistent correlation emerged, though the classification was retained for its broader analytical value.

The study allowed us to draw insights on the existing governance models and their observed and potential future evolution.

Main Findings

The three structured and case-based grounded taxonomies are the first main outcome of the study**.** They describe the **characteristics, tensions, challenges** and **innovations** that are emerging in these evolving hybrid governance modes at the intersection of state, market, and community in the context of open technology initiatives. They are the following:

- **Taxonomy 1: Governance Models** classifies projects according to the dominant governance pole. **Government-led** models subdivide into those pursuing geopolitical autonomy (operating within contexts of strategic rivalry, potentially contributing to technological fragmentation) and independence-driven autonomy (seeking vendor independence and interoperability whilst maintaining compatibility with global cooperation). **Business-led** models similarly differentiate between geopolitical orientation and industrial competitiveness objectives. **Community-led** models distinguish between supported autonomy (benefiting from external resources whilst retaining governance independence) and conflictive relations (exhibiting adversarial dynamics with state or corporate actors). **Hybrid or tripartite governance** represents configurations with robust participation from all three poles without clear dominance, though these prove exceptionally rare in practice.
- **Taxonomy 2: Rationales for state intervention** examines motivations for state intervention. **Security and sovereignty concerns** align with autonomy objectives, whether geopolitical or independence driven. **Industrial and development policy rationales** distinguish between foundational research and development, infrastructure deployment, and sustainability and security maintenance phases. **Public interest motivations** encompass social provision (improving access to essential services, addressing digital divides) and **transparency and democratic participation** (enhancing accountability and civic engagement). The taxonomy also categorizes modes of intervention: funder, regulator, catalyst, and driver roles.
- **Taxonomy 3: Community Roles** articulates differentiated community positions and contributions. Positions range from **central and autonomous** (foundational leadership), through strong and autonomous, **collaborative**, and subordinate arrangements, to **marginal and beneficiary configurations**. Roles encompass core development, governance participation, standards contributions, security advocacy, guided contribution, peripheral contributions, maintenance and stewardship, and research contributions.

These results reflect several **key limitations**. The taxonomies offer a static snapshot of governance systems that are in reality dynamic and evolving, and their three chosen dimensions (stakeholder balance, government rationale, and community role) inevitably leave other angles less examined. Further research should particularly study possible shifts in the engagement of corporations that tend to dominate current production of FOSS/ODI. On the sampling side, focusing on formal governance structures can obscure the broader policy tools governments use and the fuller roles of all stakeholders. To address this limitation, when appropriate, we have also considered the role of

the three stakeholders in the broader ecosystem. The deliberate prioritization of case diversity also came at the cost of depth, meaning the specific content and context of individual initiatives (which can be crucial, for example, for understanding community engagement) received less attention than it deserved.

Despite these limitations, we believe the taxonomies offer a **valuable framework for advancing our understanding** of the ongoing evolution of open technology governance and provide a foundation from which a number of important conclusions can be drawn.

Discussion and further analysis

Our analysis reveals several important trends that are likely to grow in significance in the years ahead. Taken together, they suggest that **open technology** is no longer simply a development methodology or a licensing choice but it **has become an instrument of geopolitical strategy, industrial policy, and public infrastructure**, operating in an increasingly complex and contested governance landscape.

Openness as a geopolitical instrument. This development can be understood as an expansion of the strategic use of open-source software by U.S. hyperscalers (Schoeberl and Corrigan, 2024; Legenvre, Autio & Hameri, 2025; Ellis & Sustar, 2025; Haese & Peukert, 2026), but with government intervention. Open technology is increasingly deployed as a strategic tool in a fragmenting global order, serving two distinct but sometimes overlapping logics. The first is a **competitive logic**, where openness is used to aggregate ecosystems and shape markets against rival proprietary solutions or geopolitical alternatives. The second is a **trust-building logic**, where openness creates neutral ground for collaboration despite geopolitical tensions and economic rivalry. Rather than producing binary outcomes of full fracture or full integration, we are likely to see numerous grey areas and hybrid configurations, where open standards and architectures serve simultaneously as bridges and battlegrounds.

Security, sovereignty, and path dependency. Governments are turning to open technology not only for its transparency and auditability, but because the cumulative legacy of open source has become the **unavoidable foundation** of modern digital infrastructure. Decades of global, collaborative development have produced a body of code and architectural knowledge that would be prohibitively expensive to replicate. True sovereignty is therefore increasingly achieved not by rejecting this global foundation, but by deliberately and securely building upon it: hardening, curating, and integrating existing open components to serve national purposes. This logic is visible across very different political contexts, from Russia's Astra Linux and China's OpenAtom to Germany's OpenDesk and ZenDiS, suggesting it reflects a structural reality rather than an ideological choice.

Openness as industrial policy. Governments are deploying open solutions for two principal industrial policy purposes: to promote pre-competitive collaboration within industries on shared infrastructural layers, enabling competitors to cooperate on non-differentiating components while competing on higher-value applications; and to legitimize state support for the private sector in ways that navigate regulatory constraints, particularly in jurisdictions like the European Union where state aid rules limit direct subsidies. However, this **strategic use of openness** carries some risk. Quasi-cartel dynamics can emerge, as it happened in Cloud computing (Nagle, 2018; Foster, 2024), with small numbers of large incumbents coordinating through industrial consortia to shape standards in their favor (Liesenfeld & Dingemanse, 2024; Schoeberl and Corrigan, 2024; Legenvre, Autio & Hameri, 2025). Many initiatives around the EU auto industry, like the Open European Software-Defined Vehicle Platform, can be viewed under this perspective. The challenge here is to

distinguish when openness serves genuine public interest and broad-based innovation, and when it masks protectionism or facilitates the concentration of market power beneath a veneer of collaboration.

The hesitant return of the state. After decades of retreat under the dominant logic of privatization and deregulation, states are re-engaging with digital infrastructure, but cautiously and tentatively. Unlike the confident, directive state of the post-war era, today's state is stepping back in with considerable hesitation, shaped by eroded institutional capacity, ideological legacies that privilege private-sector solutions, and genuine uncertainty about appropriate governance models in a fast-moving technological landscape. India Stack stands out as the most prominent counterexample, demonstrating the **transformative potential** of decisive state action in building foundational digital infrastructure. European initiatives, by contrast, reveal persistent tensions between state-led direction, corporate-led initiatives sponsored by states and community-led stewardship, with no settled model yet emerging. The field of Digital Public Infrastructure remains in an **exploratory phase**, and the question of which experimental governance models will prove durable, scalable, and capable of delivering genuine public value is one of the most important challenges of the coming decade.

The evolution of community. Community remains a vital governance mechanism in open technology, but its form and function have transformed profoundly from the early days of the free software movement. Core **community practices** such as open collaboration, open licensing, and the production of shared digital goods **have been widely adopted and adapted across corporate and institutional contexts**. However, they are increasingly filtered, shaped, and sometimes subordinated by other logics: corporate strategy, state industrial policy, and institutional governance. Genuinely community-driven governance, characterized by individual autonomy, meritocratic decision-making, and independence from corporate or state capture, is now rare. More common are layered structures where community logic operates at the level of technical development, while strategic direction is determined by firms or states. Understanding this spectrum is essential for anyone seeking to navigate or govern the open technologies that increasingly underpin our digital world.

This evolution is also giving rise to its own “discontents", and **new types of communities could emerge** in response (Boy, 2026), inspired by a greater awareness of the inescapable “technopolitical” nature of the present stage of the digital revolution (as an example, see the in-depth analysis of the Decidim case).

Future research

This study has opened several avenues for future inquiry that we could not explore. Among others, we highlight two research directions that we could not address but believe are particularly worth pursuing in future projects.

Towards a polycentric approach to open tech governance. The findings of this research resonate strongly with Ostrom's foundational insight that the governance of commons cannot be reduced to a single universal model, but emerges from the specific institutional, social, and technological conditions of each setting (Ostrom, 1990). Future research could engage productively with two related strands of the Ostromian tradition. The first is her well-known framework for common-pool resource governance. Whilst foundational, this does not transplant straightforwardly to the open tech digital realm, where resources such as code, data, and standards are open access and non-rivalrous, the main dilemmas are not about resource overexploitation and where

governance involves actors operating at scales far removed from the small-scale communities Ostrom originally studied. Nevertheless, the three taxonomies developed in this study may be understood as a contribution to the kind of empirically grounded, middle-range theorizing that Ostrom consistently advocated. The second and potentially more fruitful strand is the framework of polycentric governance (Ostrom, 2009; Sabel & Zeitlin, 2012): a system of **multiple autonomous decision-making centers** capable of mutual adjustment, experimentation, and learning developed precisely to address large-scale, multi-level governance challenges of the kind encountered in open technology ecosystems (Krewer, 2025). This framework could **illuminate how community logic becomes institutionalized** within nested governance structures without losing its distinctive character; questions such as **what mechanisms sustain trust** among competing and rival actors; how governments can exercise meaningful agency through strategic participation rather than unilateral command; and how governance systems can be designed to remain adaptive over time. The governance of open technology initiatives, with its abundance of cases and high-stakes experiments in multi-actor coordination, constitutes an ideal terrain for advancing this research programme and for addressing questions that are not merely academic, but pressing practical challenges for those responsible for governing the digital infrastructures on which contemporary societies increasingly depend.

Ostrom's rejection of the so-called 'tragedy of the commons' narrative and her demonstration that communities are capable of developing sophisticated self-governance arrangements established a methodological legacy that remains highly relevant to hybrid governance forms of the kind documented here. Nevertheless, future innovations in the governance of open technological initiatives must address the need to strengthen and **rethink communities in light of a new understanding of their composition**—comprising not only individual developers but also organizations and users—**and** their **role** within the emerging tripartite governance models. Increasingly, these communities must contend with the strategic exploitation of digital commons by tech giants ("hyperscalers"), who leverage them to consolidate their dominant positions, reduce development costs, steer the evolution of these resources, and exploit monopolistic or oligopolistic advantages in other segments of the technology stack and in complementary markets. Ultimately, however, the pursuit of more innovative and balanced governance for technological initiatives cannot succeed in isolation; it must be supported by broader public policies aimed at dismantling the current, extreme concentration of market power in the digital sphere and fostering a new balance of power in the management of critical technological systems.

Towards tripartite governance. Secondly, within this broader polycentric framework—which would be worth exploring and developing in future research—there is a specific aspect that deserves closer examination. The **structural rarity of balanced models** of governance, where communities, firms, and states exercise meaningful and co-equal influence. According to our findings, balanced governance among states, firms, and communities remains exceptional but offers a compelling vision for how open technologies might be governed in ways that **harness the strengths of all three typologies of governance**. In the abstract, communities bring innovative capacity, technical legitimacy, and a commitment to openness as a public good. Firms bring resources, scaling capabilities, and market access. States can bring coordinating authority, long-term vision, and the capacity to regulate and invest in infrastructure that markets tend to underprovide or to transform into private monopolies. Looking ahead, achieving a balanced tripartite model requires deliberate institutional design that ensures meaningful representation for all three poles; public funding models that strengthen rather than subordinate community autonomy; layered governance that protects community voice at the technical level while allowing

appropriate state and corporate engagement at the strategic level; and a willingness to treat governance as a continuous design challenge, continuously negotiated and adapted, and not as a fixed template. Some of the analyzed cases, namely Risc-V, MOSIP, and Decidim, offer promising, if fragile, experiments in this direction. The task ahead is to learn from both their achievements and their limitations.

Structure of the report

This document is structured as follows:

- **Section 1** introduces the study context and background
- **Section 2** describes the objectives, the methodology and the comprehensive list of relevant cases, including the related limitations;
- **Section 3** illustrates the proposed taxonomies of governance models, along with application to the selected cases;
- **Section 4** describes the key emerging trends highlighted by the research;
- **Section 5** identify two main avenues for future research
- **Annex I** includes a factsheet for each of the selected relevant cases.
- **Annex II** includes a deep dive on four selected cases.

1. INTRODUCTION

1.1. Background and context

This research project explores emerging approaches to the governance of open information technology initiatives**.** We refer in particular to the institutional arrangements, decision-making processes, and coordinating mechanisms through which actors collectively shape the development, distribution, and evolution of technology production. This encompasses not only the immediate processes of design and manufacturing but also the broader structures that determine access to technological resources, the allocation of development efforts, the establishment of technical standards, and the distribution of benefits arising from technological innovation (von Hippel, 2005; O'Mahony & Ferraro, 2007).

Open technology initiatives are modelled on the consolidated success of Free and Open Source Software (FOSS) but are characterized by a shift from unsystematic public policy interventions to more structured and strategic forms of government involvement. Hence, three actors increasingly interact in the governance of these initiatives: free software communities of developers with their original ethos, companies with their profit motives, and government bodies with public policy objectives. This interaction increasingly leads to a **tripartite governance mechanism**, with particular arrangements in place. In the context of open technology, governance mechanisms must accommodate the distinctive characteristics of collaborative production across organizational boundaries, balancing community autonomy, commercial interests, and, increasingly, public policy objectives (Schweik & English, 2012; Shaikh & Vaast, 2016). The focus of our research is understanding how an effective balance is achieved between potentially conflicting objectives and different management styles, and whether such tripartite configurations prove synergistic or remain inherently unstable due to competing priorities.

Whilst the strategic adoption of open-source technologies by private enterprises is now a well-documented phenomenon driven largely by market objectives, **what represents a significant development is the increasingly strategic embrace of these models by governments**. This marks a notable departure from the original ethos of free software communities, which were driven primarily by non-economic motivations: intrinsic interests and cultural, ethical, and political values such as decentralization, freedom, and collaboration.

Several interconnected factors contribute to this evolution. First, FOSS has achieved a position of infrastructural centrality within contemporary digital ecosystems, underpinning critical systems and services. Second, open technology has matured beyond software development alone, demonstrating its viability as a broader model for technological innovation across diverse domains. Third, open approaches have emerged as powerful facilitators of collaboration and standardization, enabling cooperation even amongst competing actors who share common technical interests.

However, these **endogenous factors have been significantly amplified by broader political-economic shifts**. The partial retreat from neoliberal orthodoxy and the resurgence of state activism, driven by intensifying geopolitical competition, concerns over technological sovereignty, and the strategic importance of digital infrastructure, have **prompted governments to seek greater control over technological development trajectories**. Open technology initiatives offer governments a means to pursue industrial policy objectives, reduce dependency on proprietary foreign technologies, foster domestic innovation ecosystems, and maintain regulatory influence

over critical infrastructure, all whilst benefiting from the collaborative dynamics and distributed expertise that characterize open development models.

Whilst hybrid commons-market models have long attracted scholarly attention (Berlinguer, 2020a; 2023; O'Neil & al., 2021), and the strategic deployment of open technology by companies is now well established (Perforce OpenLogic, 2025), **the systematic involvement of government actors signals a transition towards novel governance configurations**. These configurations are increasingly tripartite, involving negotiated complementarities and tensions amongst governmental institutions, market actors, and community-based initiatives.

This emerging phase presents both systemic challenges and innovative practices as these three spheres attempt to reconcile their distinct logics and objectives. The trajectory, ecosystem, and structural characteristics of open technology will inevitably be transformed by this evolution. Conversely, the distinctive strengths of open development models, including transparency, modularity, and collaborative innovation, will likely influence state strategies and drive innovations in how public actors seek to shape technological futures.

1.2. An evolutionary approach

The perspective from which we approached this research is inspired by evolutionary economics (Dosi & Nelson, 2010; Geels, 2011; Berlinguer, 2023). While we cannot develop an exhaustive analytical framework based on that tradition, **situating** current **governance systems for open technology initiatives within their historical trajectory** is essential for understanding their temporal dynamics and the transformations that have characterized their evolution.

Indeed, whilst certain fundamental characteristics have remained constant, most notably the use of open licenses that guarantee freedoms to use, study, modify, and distribute source code (Open Source Initiative, 2022), **the open technology paradigm and its surrounding ecosystem[1] have undergone profound transformations**. This ecosystem has evolved from informal communities of individual free software developers in the 1980s and early 1990s (Raymond, 1999; Weber, 2004), through the gradual but steady growth of corporate involvement from the late 1990s onwards (Fitzgerald, 2006; West & O'Mahony, 2008), to the emergence of powerful open-source foundations in the 2000s (O'Mahony, 2007), and finally to the consolidation of corporate-led ecosystems at the frontiers of technological innovation in areas such as cloud computing, containerization, and artificial intelligence (Nagle, 2018; Foster, 2024).

These transformations have been **so profound that the original features are sometimes difficult to recognize.** However, this trajectory offers a more informed and cautious understanding of current developments, characterized by an emerging evolution driven by more structural government involvement. We highlight here **two particularly salient lessons** from this evolutionary perspective.

First, the accumulated strength of open technology explains governmental interest. We cannot understand governments' adoption of open technology models for pursuing strategic goals without considering the strength that the open technology trajectory has accumulated. This **accumulated strength** can be summarized in three interrelated aspects:

[1] By 'ecosystem' we refer to the network of interdependent actors, institutions, resources, and relationships that collectively sustain and shape open technology development (Jansen et al., 2009).

1. **Path dependency and ubiquity of open source.** Over time, open source has evolved from being an outsider in a proprietary-dominated ecosystem to becoming the foundation of digital infrastructure. Today, dependence on open-source software is nearly ubiquitous. Research indicates that between 70% and 90% of all digital systems incorporate open-source components (Synopsys, 2022; Linux Foundation, 2020 and 2022), with some critical infrastructures being entirely dependent on FOSS projects. This reversal explains major strategic shifts amongst key players. However, this critical infrastructural role also introduces governance challenges. Many essential components are maintained by small groups of volunteers or under-resourced projects, creating vulnerabilities around security, maintenance, and sustainability. The need to address these systemic risks has been a significant catalyst for increased governmental attention and commitment to the open-source ecosystem (European Commission, 2020a; OS3I Working Group, 2024).

2. **Open source as an organizational and cultural standard.** The open-source model has become not only technologically ubiquitous but also culturally hegemonic: it has established itself as a taken-for-granted approach to software development, shaping norms, practices, and expectations across the industry (Kelty, 2008). It is now structurally integrated into software development processes. This modular and collaborative structure, embedded within most digital infrastructures, has become a standard model of software development. Adopting it is not merely beneficial but increasingly necessary for both private and public actors seeking to develop robust digital systems efficiently. Furthermore, the open-source paradigm has begun to expand successfully beyond software, increasingly influencing approaches to technological innovation in domains such as hardware design, data, artificial intelligence models, and scientific research (Pearce, 2013; Murillo, 2020; Sojer & Henkel, 2010). This expansion, potentially reinforced by the nascent institutionalization of open-source principles through government policies and funding programs (see for example cases such as OpenAtom or STF in our sample), may hold the most transformative potential yet to be realized in open technology models.

3. **Open models as facilitators of co-operation and standardization strategies.** FOSS has served as a laboratory for novel forms of collaboration, proving inherently conducive to cooperation amongst diverse stakeholders and even between competing actors (West & Gallagher, 2006). This capacity for enabling shared development efforts on common technological platforms has been increasingly utilized strategically, as actors can shape technological standards by promoting their technologies as open, accessible, and widely adaptable (Simcoe, 2006; Bonaccorsi & al., 2006). In the field of artificial intelligence, for example, the release of competing open-source models by major technology firms is having significant impact precisely because openness fosters rapid adoption, community-driven development, and ecosystem building around particular architectures (Eiras & al., 2024; Seger & al., 2023). Realistically, leveraging this capacity of open-technology approaches to facilitate cooperation and influence standards will be amongst the most important motivations for future government involvement in open-technology models.

Overall, these factors, which have brought open technology to the forefront of companies' competitive dynamics and technology strategies, now form the backdrop for governments' conscious and deliberate attempts to leverage open-technology initiatives for their strategic goals.

Second, the evolutionary trajectory suggests diversity in emerging governance models. Most of these profound changes in open-technology approaches and ecosystems have occurred gradually, through processes of experimentation, adaptation, and selection, following different paths and assuming a variety of configurations. They have produced quite diverse outcomes. On one end of the spectrum, community-driven initiatives embodying many of the libertarian principles that characterized early FOSS manifestations continue to exist and form (Coleman, 2013). On the other end, cartel-like innovation ecosystems dominated by large technology companies utilizing open-source models for strategic advantage have emerged (Schoeberl and Corrigan, 2024; Foster, 2024; CloudTweaks, 2024). Between these poles lie numerous hybrid arrangements combining community, commercial, and foundation-based governance in varying proportions (Shah, 2006; de Laat, 2007; Berlinguer, 2023).

Therefore, as we approach the current early stage of government-supported and incipiently institutionalized open technology governance models, we should anticipate similar dynamics. As different governments adopt and adapt the open technology paradigm to their strategic objectives, whether for **technological sovereignty, industrial policy, innovation capacity, or public service delivery**, we should expect processes of experimentation and 'tentative' innovation (Geels, 2011; Kuhlmann & al., 2019), which will assume a variety of configurations and produce diverse outcomes. This plurality is likely to reflect variations in political-economic contexts, institutional capacities, policy objectives, and relationships between state, market, and civil society actors across different jurisdictions.

1.3. A polycentric governance system

The findings of this research on issue of tripartite governance in open technology initiatives resonate with Ostrom's foundational insight that the governance of commons cannot be reduced to a single universal model, but rather emerges from the specific institutional, social, and political conditions of each setting (Ostrom, 1990). Ostrom was an American political economist awarded the Nobel Prize in Economics in 2009 (the first woman to receive it) whose work challenged the then-dominant assumption that shared resources, such as fisheries, forests, or water systems, were inevitably destined to be over-exploited unless controlled either by private ownership or by the state, a pessimistic view famously captured by Hardin's notion of the "tragedy of the commons." (Hardin, G., 1968). Through extensive empirical research across diverse settings, she demonstrated that communities are in fact capable of developing their own effective rules and institutions for managing shared resources sustainably, without recourse to either market mechanisms or top-down government intervention. Her later work extended this insight to large-scale, multi-level governance systems, developing the concept of "**polycentric governance**" (Ostrom, 2009 and 2010) to describe settings where **multiple actors, communities, firms, and public authorities, co-govern shared resources** through overlapping and mutually adjusting arrangements, rather than through a single central authority. It is in this spirit that her work offers a particularly productive intellectual foundation for future research into the governance of open technology initiatives, as we develop below.

2. OBJECTIVE AND METHOD

2.1. Objective

This research project addresses several **key questions** arising from the developments depicted in the previous chapter:

1. Does a governance system involving the collaboration among governments, firms, and communities prove **synergistic**, leveraging the complementary capabilities of each actor, or does it generate inbalace through conflicting objectives and **coordination failures**? How do the actors involved negotiate trade-offs between community autonomy, commercial exploitation and sustainability, and public policy objectives?
2. What **governance mechanisms** and institutional arrangements **enable** or **constrain** effective **collaboration** across the three spheres? Can a tripartite arrangement function as a polycentric system, i.e. multiple independent but mutually adjusting decision centers?
3. What are the **implications of increased government involvement** for the fundamental characteristics of open technology (i.e. its openness, accessibility, and community-driven innovation)?

The goal of this research was exploratory in nature, as we understood the object of this research as referring to a new emerging evolution in the systems of governance open tech initiatives. In this context, our **goal was to give a contribution to organize the understanding of this new trend** and phenomenon.

In pursuing this goal, the research was guided by **two main objectives**. The first was to identify and map a **sample of relevant cases** in which some form of tripartite governance models of open technology initiatives are beginning to take shape, and to collect structured information about each in the form of fact sheets. The second was to **organize these cases through the development of taxonomies**.

These two objectives were pursued in parallel. In order to test the robustness of the taxonomic categories, the selection of cases prioritized diversity as the primary criterion, above all in terms of the different arrangements governing relationships among the three types of stakeholders: communities, firms, and governments. The sample was also designed to cover a broad range of political geographies and domains. Concurrently, the elaboration of the taxonomies involved iterative refinement; at various points this process revealed gaps in the sample, prompting further case identification to fill missing typological categories.

The final sample of mapped cases both illustrates the growing significance of these emerging governance models in open technology initiatives and provides sufficient diversity to support taxonomic analysis.

2.2. Methodology

The research was informed throughout by the investigators' established expertise in the governance of digital commons, public infrastructure, and innovation policy, which have guided case selection, data interpretation, and theoretical synthesis.

2.2.1. Methodological framework

The **methodological framework** employed has been **qualitative** and centered on **comparative case study analysis**. The research engaged in the systematic selection and examination of ongoing projects that exemplify the early-stage development of tripartite governance in the FOSS ecosystem. Empirical data have been collected through websites, specialized media, scholarly literature, and in-depth interviews with representatives of a sample of the selected cases. The analysis is also supplemented by semi-structured, in-depth interviews with key stakeholders who are either directly involved in the governance of these initiatives or are experts in the field.

We collected and systematized data and information relating to a total of **27 different cases**. We then verified and deepened our understanding of these cases through 14 interviews with direct representatives or informed individuals, with the aim of testing, adjusting and applying our taxonomies in the most appropriate way for each of these cases. The interviews explored the strategic objectives, institutional arrangements, and socio-political tensions that characterize each case and thus the broader ecosystem of open technology initiatives. In some instances, the interviews led to refinements in how taxonomic categories were attributed to specific cases, and provided deeper insight into the governance arrangements of a significant number of them. Overall, however, the interviews confirmed the taxonomies' capacity to synthetically capture the selected characteristics across the full set of cases.

With the soundness of the taxonomies validated, this phase of the research was considered complete. **The three structured and case-based grounded taxonomies are the first main outcome of the study.** They describe the **characteristics, tensions, challenges** and **innovations** that are emerging in these evolving hybrid governance modes at the intersection of state, market, and community in the context of open technology initiatives.

The mappings and taxonomies were then employed as analytical tools to identify **trends** and **patterns** in the governance of open technology initiatives, and to reflect on what the findings reveal about emerging governance models in this space. During this second phase of the research, it became increasingly clear that we were dealing with a wide variety of different structures and that, in many cases, these structures had undergone evolution. Indeed, these two observations confirmed our initial expectations, as one explanation for this is that we are dealing with new governance systems that are still being tested and do not yet show consolidated models.

In parallel, several cases were evaluated as candidates for **more in-depth** case studies, with a view to deepening understanding of specific governance models. In **four cases**, we expanded our research through a greater number of interviews and more in-depth analysis in order to illustrate in greater detail how governance works and is evolving in these cases.

2.2.2. Use of Artificial Intelligence

The classification of cases presented in this report is the authors' own. It results from **a process of human analysis and validation in which artificial intelligence (AI) tools served to structure and test the authors' reasoning**. The research design, the definition of the analytical dimensions, the final selection of cases and every classification reported were determined by the authors.

The categorisation was an iterative procedure developed over several rounds. The authors first defined the analytical dimensions (e.g. the roles of state, market and community in governance) and an initial group of cases drawing on prior knowledge, the literature, and informal interviews with experts and practitioners. They then clustered the cases manually around alternative

classification attempts (taxonomies), testing different approaches with the aim of developing taxonomies that are concise, analytically meaningful and insightful. Several AI tools (ChatGPT, DeepSeek, Grok and Claude) were subsequently used to test these approaches and their limits, to identify possible contradictions, and to explore alternative categorisations. Additional cases were then added to broaden the diversity of cases and governance models. AI tools also supported the identification of further cases, particularly those able to fill gaps in the existing variety, and the retrieval and synthesis of the documentation related to each case.

The final set of selected cases, together with their classifications and categorisation, was further verified through 12 interviews with 5 experts and 7 case representatives. The interviews broadly confirmed the selected set of cases and the reference frameworks developed for the taxonomies. In some instances, they led to changes in the categories assigned to individual cases.

For the four cases analysed in greater depth, AI tools (DeepSeek and Grok) were used to facilitate the retrieval and synthesis of the relevant documentation. These cases were selected only at the conclusion of the research, on the basis of the research group's already substantial knowledge of each of them, gained through prior expertise, the literature, and interviews with case representatives, and for their relevance and representativeness with respect to the variety of cases. This allowed the retrieval of documentation and the analysis of each case to be structured around their specific characteristics, with the aim of better illustrating the structures that determine their forms of governance, in line with the analytical objectives of the research.

AI tools were also used to support the literature review, both to identify relevant literature and to analyse it (Claude), and to produce the diagrams included in the report (Claude). In all these uses, AI tools played an auxiliary role: the substance of the diagrams was specified by the authors, and the results of the literature search and of the documentary retrieval were cross-checked against the original and primary sources.

2.3. Selected relevant cases

We have identified and selected a total of twenty-seven cases of open technology initiatives. The objective has been to select cases representative of the variety of "tripartite governance" models (involving states, firms, and communities) in order to progressively identify, elaborate and test the categories for possible meaningful taxonomies.

The selection of the cases for this study was based on a process informed by our previous knowledge and expertise in the governance of digital commons, the FOSS ecosystem, hybrid market-commons systems and public policy. Our established knowledge in these areas has been instrumental in guiding the identification of relevant cases that exemplify the variety of emerging tripartite governance systems. We have also consulted with experts in the field, and the deployment of three different artificial intelligence tools further facilitated the identification and categorization of the selected cases.

We believe that the cases we have selected provide a variety sufficiently robust, covering diverse domains, regions, governance models, and innovation stages, therefore providing a diversified range of cases to test categories for the taxonomies, as illustrated in the table below.

Table 1. List of selected cases

INITIATIVE	DOMAIN	REGION	GOVERNANCE MODEL	INNOVATION STAGE
Astra Linux	Operating System / Security	Russia	Gov-Led	Infrastructure
Conecte SUS (now Meu SUS Digital)	Healthcare / DPI	Brazil	Gov-Led	Growth & Scaling
Decidim	Civic Tech	Global	Community-Led	Growth & Scaling
Digital Public Goods Alliance (DPGA)	Cross-domain / DPGs	Global	Community-Led	Infrastructure
ELIXIR	Life Sciences	EU	Gov-Led	Infrastructure
EOSC (European Open Science Cloud)	Science / Cloud	EU	Gov-Led	Infrastructure
ESA-Copernicus	Space / Environmental Data	EU	Gov-Led	Infrastructure
Gaia-X	Cloud	EU	Business-Led	Growth & Scaling
Gitee	Code Hosting	China	Business-Led	Growth & Scaling
Hyperledger	Blockchain / DLT	Global	Tripartite	Pioneering Exploration
India Stack	Digital Public Infrastructure (DPI)	India	Gov-Led	Growth & Scaling
MOSIP	Digital Identity / DPI	India	Tripartite	Growth & Scaling
Open European Software-Defined Vehicle Platform	Automotive / Embedded	EU	Business-Led	Pioneering Exploration
Open Source Security Foundation (OSSF)	Cybersecurity	US	Business-Led	Infrastructure
Open Wallet Foundation	Digital Identity / Wallets	Global	Business-Led	Growth & Scaling
OpenAtom	General OSS Ecosystem	China	Gov-Led	Growth & Scaling
OpenSRP	Healthcare	Kenya	Community-Led	Growth & Scaling
O-RAN Alliance	Telecom / 5G	Global	Business-Led	Growth & Scaling
OS3I (Open-Source Software Security Initiative)	Cybersecurity	US	Gov-Led	Infrastructure
Risc-V	Hardware	Global	Tripartite	Pioneering Exploration
Rust	Programming Language	US	Community-Led	Growth & Scaling
scikit-learn	AI/ML	Global	Community-Led	Infrastructure
Signal	Privacy / Secure Comms	US	Community-Led	Growth & Scaling

INITIATIVE	DOMAIN	REGION	GOVERNANCE MODEL	INNOVATION STAGE
Simpl	DPI / Data Spaces	EU	Gov-Led	Pioneering Exploration
Sovereign Tech Fund (STF)	Cybersecurity	Germany	Gov-Led	Infrastructure
X-Road (NIIS)	DPI / Interoperability	Estonia	Gov-Led	Infrastructure
ZenDiS	Software Infrastructure	Germany	Gov-Led	Infrastructure

Source: CSIL

Annex I includes a factsheet for each of the selected relevant cases describing its main characteristics and governance systems. Among this sample, we have chosen four extremely different cases for our **in depth analysis**. **Annex II** includes a more extended description and analysis of the four selected cases:

- **India Stack**: A state-orchestrated digital infrastructure built on a philosophy of "minimalism." It layers distinct logics—State (Identity/Aadhaar: sovereign, top-down), Market (Payments/UPI: competitive, innovative), and an Elusive Commons (Data/DEPA: an attempted but fragile individual-centric model). Its governance is a strategic state-market partnership where the community is influential in design and contestation but excluded from core operational control.
- **Risc-V**: A global, community-born open standard for processors that evolved into a tripartite "big tent." Its governance is designed to balance Community (academics, enthusiasts through free membership), Market (firms competing via proprietary implementations), and State (governments pursuing strategic autonomy). It uses technical modularity and a neutral, professionalized foundation to manage tensions and prevent fragmentation.
- **Decidim**: A deliberately constructed Public-Commons partnership. Born from social movements and brought into government, its governance inverts the typical model: a non-profit Association (Community) holds sovereign power over the code, while public institutions act as co-stewards and funders. The Market is relegated to a functional role, expected to contribute back to the commons. It is a model of multi-scalar, democratic control.
- **Gaia-X:** A state-initiated, market-driven European project to achieve digital sovereignty through a federated data infrastructure. Its governance is an unstable tripartite experiment where the State (divided Franco-German visions) and Market (incumbent vs. challenger firms) struggle for control, while the Community (open-source developers, citizens) remains largely marginalized. The outcome has been a narrowing of its grand ambition due to these unresolved internal tensions.

2.4. Limitations

There are important limitations in our research, stemming from its very design. Some of them relate to the definition of taxonomies and others relate to the scope and selection of the cases.

2.4.1. Limitations related to the definition of taxonomies

The taxonomies were conceived as synthetic organizational frameworks, designed to bring clarity and establish a common analytical language for a phenomenon that remains incompletely understood. Classification into distinct categories was intended to support systematic analysis and lay groundwork for future research.

Following multiple iterations, the research yielded **three taxonomies**, each addressing one of the following dimensions: the **balance of influence** among the three stakeholder types; the **rationales underlying government intervention**; and the **role and composition of communities**. This focus was partly a matter of scope, but more fundamentally it reflects the authors' assessment that these three dimensions capture the most significant dynamics currently evolving in the governance of open technology initiatives.

The initiatives were also classified by stage of development**.** The initial hypothesis was that development stage might correlate with the relative prominence of different stakeholders and governance modes, a pattern well illustrated by the Risc-V case. However, no clear correlation was found across all cases. The classification was nonetheless retained, as it is considered to carry meaningful analytical value in the study of these governance forms, as indeed it does more broadly in the analysis of technology ventures.

We chose not to develop taxonomies specifically focused on companies, both to contain the scope of the work and because corporate engagement with open technology, and the hybrid governance forms it has generated, has already been extensively studied over the past two decades (O'Neil & al., 2021; Berlinguer, 2023; Schoeberl & Corrigan, 2024; Li & al., 2025). Instead, we focused on three phenomena we considered more novel: the tripartite nature of governance systems, the strategic involvement of governments, and the evolving role of communities in the open technology ecosystem. Nevertheless, we recognize that the more structural and strategic involvement of governments in these initiatives and the increasingly marked abandonment of the Washington Consensus as the standard for public policy (Williamson, 1990; Sullivan, 2023), is likely to reshape the relationship between commercial companies and open technology, and that this evolution equally warrants attention from future research. In fact governments in their multiple role as regulators, co-funders and strategic actors in a geopolitical complex environment may have different cards to play.

A further limitation is the **static approach to the governance** that we represented in our taxonomies. When investigating each of these cases, as we have done in several cases, we often observed an evolution in these governance systems. This sometimes created a tension and a difficulty in our attempt to categorize each case model of governance. Decidim, Gaia-X, Open Wallet show clear examples of this evolution. This can reflect the actual proceeding by trial and error of these initiatives, the lack of consolidated experience and established models for these systems of governance, the relative level of maturity and development of each of these initiatives. However, as we will suggest in our final considerations, this evolutionary dynamism in governance systems could also be more structural, reflecting the conditions in which these systems are taking shape; and a dynamic conscious modulation of the relative importance of each of these models, according to the stage of development or the prioritized objectives, could be an important aspect of the learning required for the governance of these initiatives. Our taxonomies, however, do not address explicitly this issue.

2.4.2. Limitations related to the definition of sample cases

The most important limitation related to the sample cases is that our focus on the governance of open tech initiatives is sometimes **inadequate to capture the range of tools** that governments and public actors employ in pursuing their strategies. Governments have multiple policy tools at their disposal. Examples include: regulation, taxation, public procurement, funding (including equity), and special powers (including executive orders) (Decker, 2023). And these may be more important than a direct involvement in the governance of initiatives. Furthermore, in the last decades, governments have rarely assumed direct governance roles in technological systems. This situation is slowly changing. India Stack is a good counterexample. However, a lack of experience and expertise, the uncertainty and complexity of technological systems, and an entrenched neoliberal mindset continues to hinder this evolution. The EU's ongoing—and rather tentative—efforts to adapt its policies to the new geopolitical and economic environment are a clear example of this (Berlinguer, 2024). Furthermore, a focus on the formal governance of an initiative may also be inadequate to capture the role of other stakeholders, not just governments. This is a difficulty which is not new in the research on open technology – which always poses challenges to the formal definition of borders and processes of the unit of analysis. For this reason, when appropriate, we have also considered the role of the three stakeholders in the broader ecosystem, in our research, and in the collection of the relevant information in the fact-sheets and in the assessment of the role of the different stakeholders.

Another limitation stems from the **decision to prioritize case diversity in our research**. We examined a large number of cases, focusing on the variety of governance models, and used the involvement of the three types of actors and the use of open technologies as criteria for identifying the cases relevant to our research. To highlight this diversity, we did not limit our research to infrastructure, critical, or fundamental technologies. We expanded our sample of cases with the aim of testing the ability of the taxonomy categories to succinctly capture this variety. However, this also meant we limited our attention and consideration to the specificity of the initiatives' content. This can be very important, especially, but not only, for communities engagement. For example, it may represent the primary motivation for stakeholder engagement (think, for example, of cases like Decidim or Signal) or it may embody a constraint that limits actors' ability to engage (think, for example, of the minimum scale required to participate in systems like Copernicus or industrial transformations like Open SDV).

3. TAXONOMIES OF GOVERNANCE MODELS

This section presents the three taxonomies that we have progressively developed and tested to describe and analyze the cases of tripartite governance that we have mapped. The taxonomies were refined and adapted during the course of the research and tested and validated through interviews with experts and representatives of the cases, in order to verify their robustness and fine-tune the attribution of categories to cases.

At the core of these taxonomies lies a tripartite model. Tripartite governance in open technology initiatives refers to a collaborative framework where government, firms, and communities share decision-making, funding, or development under open licenses/standards. Even in configurations where one pole appears marginal or subordinate, all three actors are present. The variation lies in their relative strength and the nature of their relationships. This first taxonomy then classifies open-tech projects on the base of the **dominant governance pole.** The other two taxonomies focus on the **motivations underpinning governmental intervention** and the relative and differentiated **position of communities**. We present here below these taxonomies and their motivations.

3.1. Definitions

In order to establish a conceptual foundation for the inquiry into the governance of open technology initiatives, we have delineated a definition for the key terms and constructs that have underpinned our research and analysis. Given the interdisciplinary nature of this field, spanning science and technology studies, innovation governance, and digital commons literature, some terms may carry varying connotations across contexts. Clarifying these concepts at the outset helped to enhance analytical precision but also ensured coherence in the interpretation of empirical cases and theoretical arguments throughout the study. We provide, below, the definitions of some of the key concepts:

- **Tripartite Governance**: We define it as "a collaborative framework where states, firms, and communities share decision-making, funding, or development under open licenses/standards". These dynamic systems balance geopolitical, economic, and social goals, with power dynamics varying across cases and contexts (e.g., national ecosystems vs. global standards). Governance evolves through factors like geopolitical rivalry, stakeholders engagement, project maturity, and innovation stages (Pioneering Exploration, Growth & Scaling Exploitation, Incorporation as Infrastructure) [2].
- **Community**: We define a community in open technology initiatives as "a group of independent contributors, independent developers, employees, academics, organizations, firms, or government entities that actively participate in the development, governance, or maintenance of shared open technology projects under open licenses/standards". Communities vary in autonomy, composition, and motivations, evolving from grassroots individuals in early FOSS to institutional actors in modern projects. Roles range from core

[2] We have integrated as an indicator in the analysis the innovation stages, because they can highlight different predispositions (e.g., communities often leading in exploration, states/firms in scaling, and infrastructural maintenance requiring balanced collaboration, but often problematic in open tech due to underfunding or free-riding). However it is important not to overestimate their influence. They are only one of many factors shaping stakeholder roles. Geopolitical rivalry, economic strategies and competition, funding, community motivations, or project goals, for example, can be equally critical.

development to peripheral contributions to the code or in other areas, shaped by governance and incentives (e.g., intrinsic motivations, career, ideology, national goals) [3].

- **Openness**: We define openness in open technology initiatives as "the use of open licenses[4], standards, or collaborative frameworks that enable access, modification, and distribution of technology by independent actors, including individuals, organizations, firms, or governments". Evolving from FOSS principles of free redistribution and transparency, openness now encompasses strategic, contextual goals, such as interoperability, sovereignty, or innovation, while maintaining core features like open licensing and multi-actor collaboration. The degree and purpose of openness vary by project, reflecting diverse cultural, geopolitical, and economic priorities.

Digital Public Infrastructure (DPI), Digital Public Goods (DPG), and Open Digital Infrastructure (ODI) are related but distinct concepts in digital development, governance, and technology policy. They are sometimes used loosely or interchangeably, but they differ in scope, openness requirements, purpose, and level of abstraction.

- **Digital Public Goods (DPG)** are open digital assets that function like economic public goods in the digital realm: they are non-rivalrous (one person's use does not diminish availability for others) and, when properly licensed, non-excludable. DPGs are reusable building blocks or components that can be freely adopted, adapted, and used by anyone (governments, NGOs, private sector). An influential definition stems from the UN Secretary-General's Roadmap for Digital Cooperation and has been operationalized by the Digital Public Goods Alliance. It includes open-source software, open data, open AI models, open standards, and open content. However it adds to these basic characteristics (non-rivalry and non-excludability) three more requirements. These resources have to: adhere to privacy and other applicable laws and best practices, do no harm by design, and help attain the Sustainable Development Goals (SDGs).
- **Digital Public Infrastructure (DPI)** is generally used to refer to foundational, society-scale digital systems that enable the delivery of public and private services at population level. They act as shared digital "rails" or building blocks analogous to physical infrastructure (roads, electricity grids). A widely adopted definition originated from the G20 in 2023 with the New Delhi Leaders' Declaration and was subsequently used by UN frameworks. It describes DPI "as an evolving concept and as a set of shared digital systems, built and leveraged by both the public and private sectors, based on secure and resilient infrastructure, and can be

[3] Our definition of community includes the possibility of organizations participating, as we wanted to take into account and incorporate into our definition the evolution that this governance mechanism has undergone throughout the development of open technology. Therefore, some of these communities significantly differ from traditional FOSS communities, where voluntary participation and intrinsic motivations were central. However, this required further characterization of the cases we labelled as "community-led," beyond the use of open licenses and voluntary collaboration by independent actors, in order to distinguish them from other forms of corporate and government collaboration and account for the specificity of this governance mechanism. Therefore, in order to apply the label "community-led" to a case, we have taken into account other criteria such as whether governance mechanisms were meritocratic, transparent, and consensual and if they were linked to individuals rather than organizational affiliations; whether it was characterized by the presence of a plurality of actors and diverse stakeholders (e.g., not only companies); and whether there were no economic or institutional barriers to participation in the initiative. On this topic, see the chapter of conclusions dedicated to the evolution of the nature, role, and composition of communities in open technology initiatives.

[4] We assume the Open Source Initiative (OSI) or Free Software Foundation (FSF)-approved definitions of open licenses as a reference, without the need for further specification or differentiation.

built on open standards and specifications, as well as open-source software can enable the delivery of services at societal-scale". Typically these systems include components like digital identity, digital payments and trusted data exchange frameworks. Just like in the most famous original model, the India Stack, they can be built using open-source or proprietary technology, as long as open standards/specifications enable broad participation and avoid lock-in. The emphasis is on their foundational nature (across sectors), public interest, inclusion, on characteristics like interoperability, modularity, scalability, and on its public governance and accountability.

- **Open Digital Infrastructure (ODI)** is a broader, less formally standardized concept referring to the open, shared technical foundations of the digital world. It emphasizes openness, sustainability, and resistance to enclosure or proprietary capture. It typically refers to open-source software and libraries, open protocols and standards (e.g., foundational internet protocols), open repositories, tools, and multi-purpose system components, elements of the digital commons that support commerce, science, communication, administration, and the broader internet/digital economy. ODI focuses more on the underlying open technical substrate of the digital ecosystem as a whole, core digital commons and is often discussed in relation to funding digital commons, or sustaining critical open infrastructure (protocols, code libraries, standards).

3.2. Taxonomy 1: governance models

Balanced tripartite governance systems are rare. We have therefore subdivided our sample, consisting of cases involving the participation of all three stakeholders, into four distinct subcategories to reflect the different weighting of each stakeholder. Hence this taxonomy classifies open technology projects by governance models through four typologies: Gov-Led (state-dominated), Business-Led (firm-driven), Community-Led (community-driven), and Tripartite (balanced collaboration).

3.2.1. Government-led models

Projects in this category are **primarily driven by public institutions**, although the form and extent of government intervention varies considerably. The variety of motivations behind government intervention is analyzed in more detail in the second taxonomy. One of the principal motivations, however, is the pursuit of greater security and technological sovereignty. In all these cases, governments seek to reduce systemic vulnerabilities and external dependencies by fostering greater control over critical technological infrastructures and reducing reliance on foreign providers. However, within this category, we have further distinguished two main subtypes based on the geopolitical context and the likely trajectory of these interventions—specifically, whether their outcome tends towards fragmentation of technological systems or remains compatible with persistent collaboration on a global scale:

- **Geopolitical Autonomy:** These are state-driven projects employing open licenses within a context marked by geopolitical conflict and strategic rivalry. Examples include OpenAtom (China's national open-source foundation), Astra Linux (Russia's sovereign operating system), and O-RAN (Open Radio Access Network, particularly its deployment in contexts of technological decoupling). These initiatives are catalyzed by geopolitical tensions (Arcesati & Meinhardt, 2021; Pannier, 2022; Martí, 2022; Berlinguer, 2023). In these contexts, open technologies serve strategic objectives where, due to geopolitical antagonism and mutual

exclusion policies (such as export controls, entity lists, and technology sanctions), the probable outcome is a divergence in technological trajectories and the formation of parallel, regionally bounded ecosystems.

The apparent paradox is that whilst FOSS licenses formally prohibit access restrictions or discriminatory usage based on person, group, or field of endeavor (Open Source Definition, Clause 5 and 6), states may utilize openness instrumentally to construct *de facto* technological barriers through several mechanisms:

- **Parallel ecosystem development:** By creating domestically controlled alternatives to Western-dominated projects, states build parallel technology stacks that reduce integration with global systems whilst maintaining formal openness (e.g., OpenHarmony as an alternative to Android).
- **Strategic forking and divergence:** States may fork existing open projects but develop them along divergent paths aligned with national standards, specifications, and integration requirements, making cross-system compatibility increasingly difficult despite shared origins (Kim & al., 2023; Cory, 2024).
- **Controlled participation and governance:** Whilst the code remains formally open, participation in governance, standard-setting, and core development may be limited through informal mechanisms such as language barriers, domestic hosting infrastructure, security clearance requirements for contributors, or alignment with national regulatory frameworks (Cheung, 2024).
- **Export and usage controls:** Although the license permits unrestricted use, states may impose separate export controls on associated technologies, restrict deployment in sensitive sectors, or create regulatory environments that effectively segment markets (Chander & Lê, 2015; Farrell & Newman, 2019).

The result is **technological fragmentation**: nominally open projects that, through strategic state intervention and geopolitical context, contribute to the construction of separate, regionally bounded technological spheres rather than global collaborative commons.

- **Independence-driven autonomy:** These are state-supported projects that primarily seek *vendor independence, interoperability, and greater strategic autonomy*, but, operating in the absence of direct geopolitical confrontation, potentially maintain compatibility with global cooperation through the development of open and interoperable standards. Examples include Gaia-X (the European initiative for federated cloud infrastructure[5]), X-Road, India Stack, and various national open-source strategies in countries not directly involved in major geopolitical rivalries. This subtype reflects a non-confrontational drive for digital autonomy. The objective is not to fragment global technology systems but rather to reduce asymmetric dependencies, avoid vendor lock-in, and ensure that critical digital infrastructures can be domestically controlled and aligned with local regulatory requirements (such as data sovereignty, privacy standards, and security protocols).

The openness here serves a dual purpose: it enables participation in global collaborative development, reducing costs and benefiting from distributed innovation, and simultaneously ensuring that no single foreign vendor or platform can exercise monopolistic control. This approach may coexist with international cooperation, allowing shared development and

[5] Gaia-X was initially promoted by the German and French governments, though subsequently was entrusted to the governance of an association of businesses..

standard-setting, maintaining domestic control over deployment, customization, and integration into national digital ecosystems (Blind & al., 2011; European Commission, 2020b).

3.2.2. Business-led models

Here, **corporations are the primary organizers and promoters of open technology initiatives**. However, the state's presence is often significant, leading to blurred boundaries between private interest and public power. Two nuanced subtypes can be identified:

- **Geopolitical orientation:** In these cases, businesses collaborate with governments in politically charged contexts. An illustrative example is Open RAN in the 5G domain, where US and European companies, backed by their respective governments, promoted an alternative standard to counter Huawei's technological dominance (Peron & al., 2022). These efforts extend to allied states through diplomatic channels and regulatory pressure, forming strategic techno-economic coalitions that align market competition with geopolitical objectives (Farrell & Newman, 2019).
- **Industrial competitiveness**: This variant focuses less on geopolitical confrontation and more on market positioning and sectoral innovation. European initiatives such as the multipronged European SDV (Software-Defined Vehicle) aim to regain competitiveness in digital mobility and automotive software (Müller & al., 2023). The EU and national governments, particularly in France and Germany, act as supporters and conveners rather than initiators, seeking to revitalize industrial leadership through public-private collaboration without an explicit security or sovereignty framing. Here, open technology serves primarily as a mechanism for industry coordination, standard-setting, and collective innovation to compete against dominant foreign platforms.

The distinction between these two subtypes is subtle yet significant. Security-driven business-led projects differ fundamentally from those motivated by industrial policy, and the differentiation becomes crucial in evaluating the legitimacy, forms, and efficiency of public support for initiatives that primarily serve private-sector actors.

3.2.3. Community-led Models

These are instances where **communities retain clear leadership** despite the involvement of governments and businesses. Most contemporary community-led initiatives are institutionalized within foundations, which provide organizational scaffolding, legal structures, and resource management (O'Mahony, 2007; Shaikh & Vaast, 2016). The internal governance of these initiatives and foundations varies considerably, particularly regarding the degree and nature of corporate influence. Nonetheless, the primary characteristic of this category is that the community sets strategic priorities and maintains stewardship of the project's direction, values, and technical roadmap.

In community-led governance models, authority emerges from within the project community itself, typically comprising volunteers, academics, or practitioners who share a strong ethical or technical vision (Coleman, 2013; Raymond, 1999). These models interact with states or firms but on terms substantially defined by the community, with institutional actors playing supporting, limited, or contested roles rather than directive ones. Two distinct subtypes can be identified:

- **Supported autonomy**: Projects in this category benefit from external resources, such as public grants, academic infrastructure, philanthropic funding, or corporate donations, while

retaining clear governance autonomy (Eghbal, 2016). Leadership is grounded in community participation, technical meritocracy, or elected representation, and decision-making centers around long-term sustainability, technical excellence, and adherence to community values rather than commercial imperatives or policy directives. External actors may support and influence the project's mission through funding or in-kind contributions but do not exercise direct control over governance structures, technical priorities, or strategic direction.

- **Conflictive relations**: These projects exhibit, alongside collaborative features, adversarial or oppositional relationships between communities and state or corporate actors, often as a response to perceived threats to user rights, community autonomy, or freedom of expression; or conversely, as sources of concern for governments regarding regulatory compliance, national security, or content control (DeNardis, 2014; Tkacz, 2015). Governance is typically closely aligned with strong ethical or political commitments such as privacy protection, resistance to surveillance, circumvention of censorship, or preservation of digital rights and freedoms. Examples include projects like Tor (enabling anonymous communication), Signal (privacy-focused messaging)[6], various VPN and encryption tools, or decentralized social media platforms that explicitly position themselves in opposition to corporate data extraction or state monitoring. These initiatives often operate in legally and politically contested spaces, navigating tensions between technical openness and institutional pressures for control, compliance, or restriction.

3.2.4. Hybrid or tripartite governance

Some open tech projects exhibit robust participation from all three governance poles without a clearly dominant actor. Though asymmetries persist, these configurations are distinguished by **balanced co-governance**, where public institutions, corporations, and communities, all play a robust role, and engage in dynamic negotiation and mutual interdependence. The label "tripartite" thus denotes a structure of shared - leadership rather than simple coexistence.

3.2.5. Classification of the selected cases

Based on the key features depicted in the previous sections, the classification of our selected cases is presented in the following table.

[6] Signal can be seen as a case that maintains relationships with governments characterized by both support for autonomy and conflict-ridden dynamics, depending on the geopolitical context.

Table 2. Classification of cases based on Taxonomy 1

INITIATIVE	CATEGORY	SUB-CATEGORY	POWER DYNAMICS	STAGE OF INNOVATION	KEY CHARACTERISTICS	CHALLENGES AND TENSIONS
Astra Linux	Gov-Led	Geopolitical Autonomy	State ≫ Firms > Communities	Incorporation as Infrastructure	Russian OSS for military/security	Isolation, limited community engagement
Conecte SUS (Meu SUS Digital)	Gov-Led	Independence-Driven Autonomy	State ≫ Firms > Communities	Growth & Scaling Exploitation	Brazilian healthcare DPI	Autonomy loss, privacy concerns
Decidim	Community-Led	Supported Autonomy	Communities ≈ State > Firms	Growth & Scaling Exploitation	Participatory democracy platform	Scaling challenges, funding dependency
DPGA	Community-Led	Supported Autonomy	Communities ≈ State > Firms	Incorporation as Infrastructure	Global DPG standards for public good	Coordination complexity, adoption barriers
ELIXIR	Gov-Led	Independence-Driven Autonomy	States > Communities > Firms	Incorporation as Infrastructure	EU bioinformatics data infrastructure	Underfunding, firm free-riding
EOSC	Gov-Led	Independence-Driven Autonomy	States ≈ Communities > Firms	Incorporation as Infrastructure	EU open science cloud	Governance complexity, free-riding
ESA-Copernicus	Gov-Led	Independence-Driven Autonomy	States ≈ Communities > Firms	Incorporation as Infrastructure	Open satellite data, firms free-ride	Free-riding, underfunded maintenance
Gaia-X	Business-Led	Independence-Driven Autonomy	Firms > States > Communities	Growth & Scaling Exploitation	EU cloud sovereignty, interoperable	Adoption barriers, governance complexity
Gitee	Business-Led	Geopolitical Autonomy	Firms ≈ State > Communities	Growth & Scaling Exploitation	China's code hosting platform	Censorship risks, limited global reach
Hyperledger	Tripartite	Balanced Collaboration	Firms ≈ Communities > States	Pioneering Exploration	Enterprise blockchain frameworks	Complexity, firm-driven priorities

INITIATIVE	CATEGORY	SUB-CATEGORY	POWER DYNAMICS	STAGE OF INNOVATION	KEY CHARACTERISTICS	CHALLENGES AND TENSIONS
India Stack	Gov-Led	Independence-Driven Autonomy	State ≫ Firms[7] > Communities	Growth & Scaling Exploitation	Scalable DPI (Aadhaar/UPI)	Privacy risks
MOSIP	Tripartite	Independence-Driven Autonomy	Communities ≈ States ≈ Firms	Growth & Scaling Exploitation	Open digital identity for Global South	Adoption barriers, privacy concerns
Open SDV	Business-Led	Corporate Collaboration	Firms ≈ States > Communities	Pioneering Exploration	Automotive OSS ecosystem	Corporate capture, community marginality
OSSF	Business-Led	Balanced Collaboration[8]	Firms ≫ Communities > States	Incorporation as Infrastructure	Secures critical OSS infrastructure	Underfunding, corporate influence
Open Wallet Foundation	Business-Led	Corporate Collaboration	Firms ≫ States > Communities	Growth & Scaling	Open digital wallet standards	Early-stage risks, adoption challenges
OpenAtom (OpenHarmony)	Gov-Led	Geopolitical Autonomy	Firms ≈ State > Communities	Growth & Scaling Exploitation	State-backed fork for national tech stack	Isolation, limited global collaboration
OpenSRP	Community-Led	Supported Autonomy	Communities ≈ States > Firms	Growth & Scaling Exploitation	Open health records for Global South	Resource constraints, adoption barriers
O-RAN Alliance	Business-Led	Geopolitical Orientation	Firms ≈ States > Communities	Growth & Scaling Exploitation	Open telecom interfaces vs. Huawei	Geopolitical tensions, community marginality
OS3I	Gov-Led	Balanced Collaboration[9]	States ≈ Firms ≈ Communities	Incorporation as Infrastructure	U.S. PA-led OSS security initiative	Overlap with OSSF, funding dependency

[7] India Stack is composed of several building blocks, standards, Databases and protocols, developed by different governmental bodies. Also the governance can vary. For example, some of the financial blocks (like the Account Aggregator Ecosystem and the Unified Payments Interface, UPI) are co-managed with the private sectors.
[8] The OSSF is classified as "Business-Led," but with a "Balanced Collaboration" subcategory belonging to the tripartite model. This highlights the fact that, despite clear corporate leadership in the formal governance of the OSSF, the initiative has been heavily promoted and influenced by the United States government, and that achieving its mission depends largely on the participation and adoption of autonomous communities.
[9] Although OS3I is a government-led initiative, the same considerations that apply to OSSF also hold true (see the previous note).

INITIATIVE	CATEGORY	SUB-CATEGORY	POWER DYNAMICS	STAGE OF INNOVATION	KEY CHARACTERISTICS	CHALLENGES AND TENSIONS
Risc-V	Tripartite	Balanced Collaboration	Firms ≈ Community > States	Pioneering Exploration	Open ISA for global standards	Avoid patent thicket, Geopolitical tensions (U.S./China)
Rust	Community-Led	Supported Autonomy	Communities > Firms > States	Growth & Scaling	Memory-safe programming language	Volunteer burnout, Lack of funding
scikit-learn	Community-Led	Supported Autonomy	Communities > Firms > States	Incorporation as Infrastructure	Open ML tools, academic-driven	Volunteer burnout, corporate and funders demands
Signal	Community-Led	Supported Autonomy	Communities > Firms > States	Growth & Scaling Exploitation	Privacy-focused messaging	Funding dependency, centralized governance
Simpl	Gov-Led	Independence-Driven Autonomy	State ≫ Firms > Communities	Pioneering Exploration	EU dataspaces prototype, interoperable	Adoption barriers, sovereignty tensions
Sovereign Tech Fund	Gov-Led	Independence-Driven Autonomy	State ≫ Communities > Firms	Incorporation as Infrastructure	Funds OSS maintenance, interoperable	Underfunding, project selection bias
X-Road (NIIS)	Gov-Led	Independence-Driven Autonomy	State ≫ Firms > Communities	Incorporation as Infrastructure	Cross-border DPI	Scalability, cross-border coordination
ZenDiS	Gov-Led	Independence-Driven Autonomy	State ≫ Firms > Communities	Incorporation as Infrastructure	German public sector OSS standards	Adoption barriers, limited firm engagement

Note: Overlaps occur (e.g., Gaia-X spans Independence-Driven Autonomy and Growth & Scaling). Source: CSIL

Legend:

- Purpose: Categorizes open technology projects by governance models, showing how states, firms, and communities share or contest power.
- Categories: Gov-Led (state-dominated), Business-Led (firm-driven), Tripartite (balanced collaboration), Community-Led (community-driven).
- Subcategories: Geopolitical Autonomy (state-driven, risks tech splits), Independence-Driven Autonomy (state-supported, cooperative), Corporate Collaboration (firm-led ecosystems), Balanced Collaboration (shared governance), Supported Autonomy (community-led with support), Conflictive Relations (community-firm-states tensions).
- Power Dynamics: Symbols (≫, >, ≈) indicate relative influence (e.g., State ≫ Firms > Communities).
- Stage of Innovation: Pioneering Exploration (R&D), Growth & Scaling Exploitation (adoption), Incorporation as Infrastructure (maintenance).

3.3. Taxonomy 2: governmental rationales for intervention

In addition to identifying the primary actor, a complementary taxonomy considers the **rationales behind government involvement in open technology initiatives**. These rationales are grouped into three primary categories, each with additional subcategories: Security and Sovereignty; Industrial and Development Policy, which encompasses interventions motivated primarily by economic objectives; and Public Interest, which includes strategic public policy goals beyond security and economic competitiveness. In some cases one can frame this rationales as related to actual or perceived market failures, but in other cases the public interest goes beyond economic efficiency consideration.

1. **Security and Sovereignty**: These rationales align with those presented in the previous taxonomy, where the primary concern is reducing external dependencies and protecting critical technological capabilities:
    - **Geopolitical autonomy**: Government intervention is framed as part of broader strategic competition, particularly in response to perceived external threats or adversarial relationships. Technological development is closely tied to national security and digital sovereignty objectives, with open technology leveraged as a means of insulating critical infrastructure from foreign dependence and constructing alternative technological ecosystems aligned with national interests (Farrell & Newman, 2019).
    - **Independence-driven autonomy**: Governments act to safeguard long-term autonomy and resilience without necessarily responding to immediate geopolitical conflict. The focus is on cultivating domestic technological capacity, reducing systemic dependencies on foreign providers, and promoting innovation ecosystems that are robust to external shocks, market concentration, or geopolitical disruptions. This rationale tends to align more closely with industrial policy and digital development agendas than with direct geopolitical contestation, emphasizing strategic foresight over reactive positioning (Edler & Fagerberg, 2017).

2. **Industrial and Development Policy:** These rationales are primarily economic and are distinguished according to the stage of technological maturity and the objectives of government intervention within innovation and industrial lifecycles:
    - **Foundational R&D**: Government support focuses on research, experimentation, prototyping, and pioneering novel digital technologies and infrastructures where market failures are most pronounced due to high uncertainty, long time horizons, and public good characteristics. Open technology models may be promoted to enable collaborative innovation, reduce duplication, and accelerate knowledge diffusion in early-stage development (Blind & al., 2017).
    - **Infrastructure deployment**: Support for maturing technologies to achieve operational stability, scaling, and market adoption. Governments may invest in deploying open technologies to modernize public infrastructure, establish interoperability standards, or create competitive alternatives to proprietary platforms. The emphasis shifts from innovation to implementation, diffusion, and ecosystem building (Mazzucato & Kattel, 2020).
    - **Sustainability and security maintenance**: Once open technologies are incorporated into critical infrastructures and public systems, government involvement focuses on ensuring long-term sustainability, security, and maintenance. This includes addressing risks such as

dependency on under-resourced projects, security vulnerabilities, and the need for ongoing stewardship of essential digital commons (Eghbal, 2016; Gates & al., 2025).

3. **Public Interest:** In these cases, motivations are primarily social and political rather than economic or strategic. Despite their transformative potential, such initiatives are currently often the least developed dimension of governmental open technology policy. Two subcategories can be distinguished:
    - **Social provision**: Open technologies are deployed to improve access to essential public services such as education, healthcare, and social welfare. The emphasis is on equity, accessibility, and reducing digital divides. Examples include open educational resources, open health data platforms, and digital public goods designed to serve underserved populations (Gurstein, 2011; World Bank, 2021a).
    - **Transparency and democratic participation**: Open technologies are employed to promote transparency, accountability, and participatory governance. This includes open data initiatives, civic technology platforms, and digital infrastructures designed to enhance citizens' rights, enable public scrutiny of government actions, and facilitate democratic engagement (Yu & Robinson, 2012; Barandiaran & al.,2024).

This taxonomy also classifies the modes of public intervention through four categories, which help clarify what government involvement or "leadership" entails in the governance of open technology initiatives (Edquist, 2011):

- **Funder**: The state primarily provides financial support through grants, subsidies, procurement, or other funding mechanisms, without directly shaping governance or technical direction. This mode enables projects together while maintaining distance from operational control[10].
- **Regulator**: The state uses its legislative and regulatory authority to mandate adoption, impose technical standards, require interoperability, or create policy frameworks that favor open technologies. This mode leverages state power to shape market conditions and technical choices.
- **Catalyst**: The state acts as a facilitator and convener of ecosystems, enabling collaboration amongst diverse actors, reducing coordination costs, and providing organizational infrastructure. This mode emphasizes orchestration rather than direct control (Mazzucato & Kattel, 2020).
- **Driver**: The state directly initiates projects, governs their strategic trajectory, and exercises substantial control over priorities, resources, and decision-making. This mode represents the most direct form of state involvement in open technology governance.

3.3.1. The classification of the cases based on Taxonomy 2

Based on the key features depicted in the previous sections, a classification of our selected cases is presented in the following table.

[10] See for example the role of the German Sovereign Tech Fund, https://www.sovereign.tech/

Table 3. Classification of cases based on Taxonomy 2

CASE	CATEGORY	SUBCATEGORY	STAGE OF INNOVATION	EXPLANATION	GOVERNMENT ROLE(S)	COMMUNITY ROLE
Astra Linux	Security and Sovereignty	Geopolitical Autonomy	Incorporation as Infrastructure	Russian OSS for security, national use	Driver, Funder, Regulator	Contributing under Guidance
Conecte SUS (Meu SUS Digital)	Public Interest	Social Provision	Growth & Scaling Exploitation	Brazilian healthcare DPI	Driver, Funder	Minor Contributions
Decidim	Public Interest	Transparency/Democracy	Growth & Scaling Exploitation	Participatory democracy platform	Funder, Driver, Catalyst	Governance Participation
DPGA	Public Interest	Social Provision	Growth & Scaling Exploitation	Global DPG standards. Aligns with Infrastructure Deployment.	Funder, Catalyst	Standards Co-Creation
ELIXIR	Public Interest	Social Provision	Incorporation as Infrastructure	EU bioinformatics data sharing	Funder, Catalyst	Research Contributions
EOSC	Public Interest	Social Provision	Incorporation as Infrastructure	EU open science cloud	Funder, Catalyst	Research Contributions
ESA-Copernicus	Public Interest	Social Provision	Incorporation as Infrastructure	Open satellite data for public good	Funder, Driver	Research Contributions
Gaia-X	Industrial/Developmental	Foundational R&D/ Infrastructure Deployment	Growth & Scaling Exploitation	EU cloud sovereignty, interoperable. Aligns with Infrastructure Deployment.	Catalyst, Funder	Minor Contributions
Gitee	Security and Sovereignty	Geopolitical Autonomy	Growth & Scaling Exploitation	China's code hosting vs. GitHub	Driver, Regulator	Contributing under Guidance
Hyperledger	Industrial/Developmental	Foundational R&D	Pioneering Exploration	Blockchain frameworks for public pilots	Catalyst, Funder	Core Development, Standards Co-Creation
India Stack	Public Interest	Social Provision	Growth & Scaling Exploitation	National DPI scaling (Aadhaar/UPI)	Driver, Funder, Regulator, Catalyst	Minor Contributions

CASE	CATEGORY	SUBCATEGORY	STAGE OF INNOVATION	EXPLANATION	GOVERNMENT ROLE(S)	COMMUNITY ROLE
MOSIP	Public Interest/ Security and Sovereignty	Social Provision	Growth & Scaling Exploitation	Digital identity for Global South. Aligns with Infrastructure Deployment.	Funder[11], Driver, Regulator	Co-Development
Open SDV	Industrial/Developmental	Foundational R&D	Pioneering Exploration	Automotive OSS ecosystem	Catalyst, Funder	Standards Co-Creation
OSSF	Industrial/Developmental	Security/Maintenance	Incorporation as Infrastructure	Secures OSS. Voluntary adoption empowers communities.	Funder, Regulator	Security Advocacy, Tooling, Adoption Advocacy
Open Wallet Foundation	Industrial/Developmental	Foundational R&D	Growth & Scaling	Open digital wallet standards	Regulator	Standards Co-Creation
OpenAtom (OpenHarmony)	Security and Sovereignty	Geopolitical Autonomy	Growth & Scaling Exploitation	National OSS ecosystem vs. U.S. sanctions	Driver, Funder, Regulator	Contributing under Guidance
OpenSRP	Public Interest	Social Provision	Growth & Scaling Exploitation	Open health records for Global South	Funder, Driver	Standards Co-Creation, Co-Development, Adoption Advocacy
O-RAN Alliance	Industrial/Developmental	Infrastructure Deployment	Growth & Scaling Exploitation	Open telecom interfaces vs. Huawei	Catalyst, Funder	Minor Contributions
OS3I	Industrial/Developmental	Security/Maintenance	Incorporation as Infrastructure	U.S. PA-led OSS security. Aligns with OSSF.	Funder, Regulator	Security Advocacy, Tooling
Risc-V	Industrial/Developmental	Foundational R&D	Pioneering Exploration	Open ISA for chip innovation	Funder, Catalyst	Core Development, Governance
Rust	Industrial/Developmental	Foundational R&D	Growth & Scaling	Memory-safe programming language	Funder, Catalyst	Core Development, Maintenance
scikit-learn	Industrial/Devel	Foundational R&D	Incorporation as	Open ML tools, academic-	Funder, Catalyst	Core Development,

[11] Governments don't fund directly MOSIP but they fund their own systems and implementations.

CASE	CATEGORY	SUBCATEGORY	STAGE OF INNOVATION	EXPLANATION	GOVERNMENT ROLE(S)	COMMUNITY ROLE
	opmental		Infrastructure	driven		Maintenance
Signal	Public Interest	Transparency/Democracy	Growth & Scaling Exploitation	Privacy-focused messaging	Funder, Catalyst	Core Development, Maintenance
Simpl	Industrial/Developmental	Foundational R&D & Infrastructure Deployment	Pioneering Exploration	EU dataspaces prototype. Aligns with Independence-Driven Autonomy.	Driver, Funder	Standards Co-Creation
Sovereign Tech Fund	Industrial/Developmental	Security/Maintenance	Incorporation as Infrastructure	Funds OSS maintenance, interoperable	Funder, Catalyst	Maintenance Support
X-Road (NIIS)	Industrial/Developmental	Infrastructure Deployment	Incorporation as Infrastructure	Cross-border DPI	Driver, Funder	Minor Contributions
ZenDiS	Security and Sovereignty	Independence-Driven Autonomy	Incorporation as Infrastructure	German public sector OSS standards	Funder, Driver	Standards Co-Creation

Legend:
- **Purpose:** Identifies why governments support open technology, linking rationales to innovation stages and stakeholder roles.
- **Categories**: Security and Sovereignty (sovereignty-focused), Industrial/Developmental (innovation economy-driven), Public Interest (social/democratic goals).
- **Subcategories**: Geopolitical Autonomy (rivalry-driven), Independence-Driven Autonomy (cooperative sovereignty), Foundational R&D (exploration), Infrastructure Deployment (scaling), Security/Maintenance (infrastructure), Social Provision (social needs, inclusion), Transparency/Democracy (civic engagement).
- **Government Roles**: Catalyst (fostering collaboration), Funder (financial support), Driver (mandating adoption), Regulator (setting rules and standards).
- **Stage of Innovation**: It aligns with Industrial/Developmental subcategories (Foundational R&D → Pioneering Exploration, etc.) and can produce overlaps (e.g., Simpl spans Foundational R&D & Infrastructure Deployment and Pioneering Exploration & Scaling; MOSIP overlaps Social Provision and Infrastructure Deployment).

Source: CSIL

3.4. Taxonomy 3: Community Roles in Open & Collaborative Tech Governance

This final taxonomy articulates the differentiated roles and positions occupied by communities within the open technology projects examined in this research. It provides a structured analytical lens for understanding how communities engage with projects, where they are positioned within governance structures, and what forms of influence or autonomy they exercise across varying governance regimes.

3.4.1. Community Positions

Community positions are defined by the degree of influence a community exercises over a project's strategic direction and the autonomy with which it operates. These positions reflect the political economy of participation, who possesses voice, agency, and power within open technology ecosystems:

- **Central and autonomous***: Communities occupy a foundational role*, leading both technical development and governance decisions. They shape the project's agenda, establish its normative frameworks, and determine its strategic direction with minimal external oversight. Decision-making authority resides primarily within community structures, often through meritocratic or democratic mechanisms.
- **Strong and autonomous***: Communities exert significant influence*, particularly over technical and organizational matters, though governance may be formally shared with institutional partners such as foundations or sponsors. They maintain substantive independence and capacity to resist external pressures while collaborating with larger stakeholders.
- **Collaborative:** *Communities function as co-governors*, engaging actively in decision-making and development, typically in partnership with foundations, states, or firms. Their input is integrated into formal governance structures through representation, consultation, or participatory mechanisms. However, autonomy may be circumscribed by institutional constraints, funding conditions, or the strategic priorities of dominant partners.
- **Subordinate:** *Communities are present but operate substantially under the direction of dominant actors*, typically state agencies or corporate sponsors. Their contributions are primarily reactive, focused on implementation, execution of assigned tasks, or technical support rather than strategic agenda-setting.
- **Marginal:** *Communities are formally peripheral*, exercising little to no influence over governance structures or strategic direction. Participation may be nominal, symbolic, or confined to downstream activities such as adoption, localization, or minor customization. This position often characterizes projects where openness is primarily instrumental rather than constitutive.
- **Beneficiary:** *Communities are positioned as recipients of support*, whether technical infrastructure, financial resources, or capacity-building programs, but do not substantially engage in core development or governance processes. This position reflects redistributional or developmental dimensions of open technology policy, where the objective is sustainability support, capability transfer or access provision rather than collaborative production.

3.4.2. Community Roles

Community roles describe the specific types of contributions communities make to open technology ecosystems (Cheng & Guo, 2019; Trinkenreich, & al., 2020; Red Hat, 2020). Clarifying these roles helps recognize the diverse array of inputs that sustain open innovation beyond code production alone.

- **Core development**: Writing, reviewing, and maintaining core codebases, protocols, or technical standards that define the project's fundamental architecture and functionality. This role typically carries significant influence over technical direction and identity.
- **Governance participation**: Involvement in organizational decision-making processes such as serving on steering committees, participating in voting mechanisms, contributing to policy formation, or engaging in institutional design and constitutional processes.
- **Standards contributions**: Shaping technical specifications, contributing to standardization processes, or aligning components with international, sectoral, or regulatory interoperability frameworks. This role connects projects to broader institutional and technical landscapes.
- **Security advocacy and auditing**: Developing security tooling, conducting vulnerability assessments and code audits, implementing secure development practices, or engaging in activities that enhance software integrity, resilience, and trustworthiness.
- **Guided contribution**: Completing tasks, modules, or features assigned by lead developers, sponsoring organizations, or coordinating agencies, often within hierarchical or contractual structures. Participation is structured and directed rather than self-initiated.
- **Peripheral contributions**: Submitting occasional patches, translations, documentation improvements, or bug reports. Individually modest but in certain cases they can be collectively important for project health and accessibility.
- **Maintenance Support**: Sustaining legacy systems, resolving technical debt, ensuring backward compatibility, and providing ongoing support for mature components. This essential but often under-recognized work ensures long-term viability and stability.
- **Research and evaluation contributions**: Providing, internal or external,scientific, empirical, or policy insights such as performance benchmarking, socio-technical evaluation, deployment case studies, or evidence gathering that informs project evolution and policy design.

Table 4. Classification of cases based on Taxonomy 3

CASE	COMMUNITY POSITION	COMMUNITY ROLE	STAGE OF INNOVATION	COMMUNITY MOTIVATIONS	NOTES
Astra Linux	Subordinate	Contributing under Guidance	Incorporation as Infrastructure	National security, career incentives	State-dominated, "degraded" community
Conecte SUS (Meu SUS Digital)	Marginal	Peripheral Contributions	Growth & Scaling Exploitation	Civic tech, digital inclusion	Contractors, limited autonomy
Decidim	Central & Autonomous	Governance Participation	Growth & Scaling Exploitation	Democratic engagement, civic tech	Volunteer-driven, government-backed
DPGA	Central & Autonomous[12]	Standards Contributions	Growth & Scaling Exploitation	Digital inclusion, global standards	Multi-stakeholder governance
ELIXIR	Subordinate	Core development, Standards Contributions, Security Advocacy, Contributing under Guidance, Maintenance Support, Research Contributions	Incorporation as Infrastructure	Scientific progress, data sharing	Academic researchers, firm free-riding
EOSC	Collaborative	Research Contributions	Incorporation as Infrastructure	Open science, public good	Academic-led, firm free-riding
ESA-Copernicus	Collaborative	Research Contributions	Incorporation as Infrastructure	Environmental science, public good	Academic researchers, firms free-ride
Gaia-X	Marginal	Contributing under Guidance	Growth & Scaling Exploitation	Interoperability, digital sovereignty	Governments and firms collaboration
Gitee	Subordinate	Contributing under Guidance	Growth & Scaling Exploitation	National tech ecosystem, career incentives	State-aligned, "degraded" community
Hyperledger	Strong &	Core Development,	Pioneering	Blockchain innovation,	Firm and developer

[12] Three communities can be identified in the DPGA: 1) the community of the members, 2) the communities of the (150+) products owners, 3the community of contributors around the "meta-standard" on Github

	Autonomous	Standards contributions	Exploration	interoperability	collaboration
India Stack	Marginal	Contributing under Guidance	Growth & Scaling Exploitation	Civic tech, digital inclusion	Government contractors, “degraded”
MOSIP	Collaborative	Core Development	Growth & Scaling Exploitation	Digital inclusion, equitable access	NGO and developer contributions
Open SDV	Subordinate	Standards contributions	Pioneering Exploration	Professional growth, standardization	Firm-led, some academic input
OSSF	Subordinate, Beneficiary	Maintenance Support, Security Advocacy	Incorporation as Infrastructure	Cybersecurity, shared infra resilience	Voluntary adoption empowers communities
Open Wallet Foundation	Collaborative	Standards contributions	Growth & Scaling	Digital identity, interoperability	Developers and firms collaboration
OpenAtom (OpenHarmony)	Subordinate	Contributing under Guidance	Growth & Scaling Exploitation	Career incentives, national strategy	State/firm-dominated, “degraded” community
OpenSRP	Central & Autonomous	Standards contributions,Core Development	Growth & Scaling Exploitation	Healthcare access, digital inclusion	NGO and health worker contributions
O-RAN Alliance	Marginal	Peripheral Contributions	Growth & Scaling Exploitation	Telecom innovation, standardization	Firm-dominated, limited community role
OS3I	Collaborative	Security Advocacy	Incorporation as Infrastructure	Cybersecurity, public sector security	Aligned with OSSF, state-guided
Risc-V	Strong & Autonomous	Standards contributions, Core Development, Governance	Pioneering Exploration	Open hardware, anti-monopoly	Academic-corporate mix
Rust	Central & Autonomous	Core Development, Maintenance Support	Growth & Scaling	Memory safety, developer empowerment	Volunteer-driven, some firm support
scikit-learn	Central & Autonomous	Core Development, Maintenance Support	Incorporation as Infrastructure	Scientific progress, open ML tools	Volunteer-driven, some firm support
Signal	Central & Autonomous	Core Development	Growth & Scaling Exploitation	Privacy, user empowerment	Volunteer-driven, centralized governance

Simpl	Collaborative	Standards contributions	Pioneering Exploration	Interoperability, data leadership	Developer and public sector collaboration
Sovereign Tech Fund	Beneficiary	Maintenance Support, Security Advocacy	Incorporation as Infrastructure	OSS sustainability, digital autonomy	Grantees receive support in the form of public investment by the German Government
X-Road (NIIS)	Marginal	Peripheral Contributions	Incorporation as Infrastructure	Cross-border interoperability	Contractors, limited community role
ZenDiS	Collaborative	Standards contributions	Incorporation as Infrastructure	Public sector interoperability	Public sector developers, limited firms

Legend

1. **Purpose:** The framework captures the motivations, agency, and functional contributions of communities, tracing their influence within diverse governance structures—whether state-driven, corporate-led, or foundation-coordinated—and across phases of technological maturation.

2. **Governance Categories:**
Gov-Led: Dominated by state actors with strategic or developmental aims.
Corporate-Governed: Directed by private firms, often for market expansion or control.
Foundation-Led: Coordinated by neutral, often multi-stakeholder entities.
Grassroots/Community-Led: Organized bottom-up, driven by volunteers or independent developers.
Non-Profit/Advocacy: Centered on normative or ideological missions, often focused on rights, openness, or inclusion.

3. **Community Positions:**
Central & Autonomous: Communities lead and shape the project's direction.
Strong & Autonomous: Communities play influential roles but within shared structures.
Collaborative: Communities act as co-governors alongside states or firms.
Subordinate: Communities contribute under structured guidance.
Marginal: Communities have limited influence on core decisions.
Beneficiary: Communities are recipients of support or services but are not actively engaged in governance.

4. **Community Roles:**
Core Development: Driving codebases and technical standards.
Governance Participation: Engaging in strategic or organizational decision-making.
Standards Contributions: Ensuring interoperability and compliance.
Security Advocacy: Contributing to tooling, audits, and vulnerability management.
Contributing under Guidance: Undertaking specified or directed tasks.
Peripheral Contributions: Offering peripheral or occasional input.
Maintenance Support: Sustaining legacy systems or critical components.
Research Contributions: Providing scientific insight or data-driven inputs.

Source: CSIL

4. DISCUSSION AND FURTHER ANALYSIS

Our research was exploratory in nature. After multiple tests, we ended up with the three taxonomies that we presented in this report focusing on three main aspects: the balance and the relative influence of the three different types of stakeholders; the rationales behind governments intervention; the role and composition of the communities. This choice was due to the understanding that it is around these three aspects that we were dealing with the most significant evolutions undergoing in the governance systems of open tech initiatives.

Once we had confirmed the soundness of the taxonomies through interviews with experts or representatives of the cases, we began to use the mapping and the **taxonomies as tools to identify trends and patterns** (Bailey, 1994).

However, it became increasingly clear these new governance systems are still being tested and do not yet show consolidated models.

We have chosen four extremely different cases for our more in depth investigation.

- **Gaia-X**: A state-initiated, market-driven European project to achieve digital sovereignty through a federated data infrastructure.
- **Risc-V**: A global, community-born open standard for processors that evolved into a tripartite "big tent."
- **India Stack:** A state-orchestrated digital infrastructure built on a philosophy of "minimalism."
- **Decidim**: A deliberately constructed Public-Commons partnership.

Below we summarize the most salient characteristics (for a more in-depth analysis and the references of these cases look at the annexes).

- **Gaia-X** represents a landmark European experiment in the use of open technology as a strategic tool for **industrial policy. Gaia-X develops protocols and standards which should connect existing cloud and data services into a decentralized ecosystem, enabling secure data sharing across sectors**, with the aim of establishing digital sovereignty through a federated ecosystem rather than through national champions. Its governance has been designed as a hybrid, multi-level system involving three distinct actors: governments (as promoters), companies (as core members), and communities (peripherally participating in technical working groups). However, this tripartite structure has become an arena of intense struggle rather than collaboration. The Franco-German political divide has pitted a protectionist French vision against a more technical and Atlanticist German approach (On Gaia-X see the case study and also Pollet, 2025). Also in the private sector a contrasting approach emerged between companies providers and users of digital services, especially with regard to the relationships with not-European hyperscalers. The decision to admit non-European hyperscalers such as AWS and Microsoft, deemed necessary to ensure the initiative's global reach and relevance, has sparked accusations of capture by Big Tech, with criticism that these dominant players would use their resources to steer the project's roadmap. Community participants saw their influence marginalized by corporate resources and top-down management. Governments failed to activate regulatory leverage for the initiative. The lack of a shared definition of sovereignty among the three poles made consensus-building nearly impossible, as each actor projected their own conflicting

expectations onto the initiative. This governance failure has prevented Gaia-X from achieving its ambitious goal of promoting a sovereign European cloud infrastructure, with the market share of European providers steadily declining and the introduction of interoperability rules between cloud providers remaining a mirage. Ultimately, the case can be used to argue that without robust meta-governance, i.e., the strategic work of balancing power between government, business, and community poles, open technology initiatives risk being eroded by the very forces they seek to mobilize.

- **India Stack** represents a strategic architectural experiment in layering different governance logics—state, market, and community—within a single digital infrastructure (On India Stack, see the case study and also Trikanad & al., 2026). Rather than a grand plan, it evolved through minimalist interventions: identity (Aadhaar) as a state-owned layer, payments (UPI) as market-driven rails, and data sharing (DEPA) as an attempt to encode individual sovereignty. The system's governance is designed to modulate these three regimes simultaneously, creating a fragile equilibrium where each logic operates at a different layer. The **state** provides **foundational infrastructure** through coercive power and sovereign authority at the bottom layer. The market drives innovation and competition through user-facing applications built atop these rails. An emergent "citizens commons" logic attempts to empower individuals over their own data through consent architectures. However, this tripartite balance is unstable and contested. The state logic risks overpowering others through surveillance and exclusion, while the market logic enables digital extractivism by global tech giants extracting value from open infrastructure. Community actors remain fragmented—operating as policy architects (iSpirt), developer and start up ecosystems, or digital rights advocates—but hold no formal governance role over core infrastructure. The case can illustrate that open tech governance requires deliberate modulation between these competing logics to prevent any single pole—sovereign control or commercial profit—from consuming the others and transforming platforms for empowerment into structures of domination.

- **Risc-V** exemplifies how a technical project can evolve from a university lab into a globally significant open standard shaped by the distinct—and often conflicting—interests of communities, firms, and governments. Its governance model is deliberately designed to accommodate this tripartite tension through structural innovations that balance collaboration and competition (On Risc-V, see the case study and also Krewer, 2025). The **academic and enthusiast community** provides the innovative spark through free individual memberships and open technical working groups. **Firms** participate through a multi-house membership structure that allows fierce competitors like Qualcomm and Huawei to collaborate on the standard while keeping their proprietary implementations secret - enabled by the permissive BSD license. Firms also collaborate through specific open projects as Linux Foundation Europe’s RISE (Risc-V Software Ecosystem). **Governments** engage strategically: the EU funds development for digital autonomy, China pursues semiconductor self-reliance amid US export controls, and the US embodies a tension between industry-led innovation and geopolitical will of technological containment. The critical governance innovation was relocating the foundation to Switzerland in 2020, insulating technical collaboration from any single nation's foreign policy. Rigorous extension ratification processes and defined profiles prevent ecosystem fragmentation while allowing

custom innovation. The model carefully protects grassroots influence through individual voting rights and public access to technical work. Risc-V's journey demonstrates that successful open tech governance requires deliberate architecture - both technical and institutional - that creates space for competing logics while providing the glue against fragmentation, transforming potential geopolitical fractures into resilient co-opetition.

- **Decidim** represents the most sophisticated experiment in deliberately constructing a **public-commons partnership** that reconfigures relations between state, civil society, and market in technology governance (On Decidim see the case study and also: Barandiaran & al., 2024). Born from the confluence of Barcelona's 15-M social movements and hacktivists of free software traditions, its governance architecture deliberately relegates the market to a peripheral role while centering public institutions and community as co-stewards. The Barcelona City Council transferred trademark and codebase to an independent Decidim Association, creating a digital infrastructure (in a broad meaning) where public resources feed a commons without government owning or controlling it. Private companies providing services are expected to contribute improvements and resources back to the core software - public investment generates public goods, not private intellectual property. The Metadecidim community functions as an open commons where anyone can contribute, while the Association holds sovereign power through one-member-one-vote democracy. A layered technical architecture - modular core with sovereign instances - enables local autonomy without fragmentation. The model explicitly manages tensions between social movement logic (horizontal participation) and administrative logic (efficiency and compliance) through institutional innovations like public procurement mechanisms that fund commons development. Decidim can be used to argue that political purpose - democratic deepening - can mobilize both public entities and diverse communities more effectively than market mechanisms. Its governance evolution from informal community to formal Association to transnational public committees offers a replicable paradigm where infrastructure is owned by publics, governed by communities, and built explicitly for democracy rather than profit.

Despite this variety and the lack of consolidated patterns and established evolution mode, we think that our research allows to identify certain **trends** in the adoption and governance of open technology systems, which we believe are set to grow in importance.

The first and most important is this. What can be said with confidence is that **open technology continues to expand** into new domains and geographies, most notably in China (Wachs & al., 2022); and that the broader structural shifts now reshaping the global order appear to be reinforcing, rather than undermining, its relevance. The retreat from the Washington Consensus, the return of industrial policy, the intensified geopolitical competition, and the growing pursuit of technological sovereignty and security are in fact emerging as new drivers of open technology adoption, rather than factors favoring its abandonment (Pannier, 2022). This means that **open technology is not merely subject to these changes. It is becoming an active force within them**. This dynamic however is likely to prompt a further evolution in open technology governance systems, adding new layers of complexity to the tensions already present in its ecosystem (Eghbal, 2020; Gates & al., 2025), and generating challenges that existing governance frameworks will need to adapt to address.

Concluding this research, we present below a series of insights, drawn from the cases we have mapped, classified and investigated, in **five key areas** that can be identified from our exploratory research. These insights represent new emerging trends in open technology initiatives that are poised to expand in the future and to stimulate further research, action, and more informed policies.

4.1. Defining standards, aggregating ecosystems

A critical dimension framing our analysis is the evolving **geopolitical landscape**. We are entering a post-globalization phase potentially characterized by increasing fragmentation in technological development: the splintering of global technology stacks and supply chains into competing geopolitical blocs, such as Chinese versus Western ecosystems. This fragmentation is driven by intensified international competition, emerging forms of technological protectionism, and rising concerns about security and strategic autonomy. These dynamics are reshaping the governance of open technological systems and fundamentally influencing the nature and viability of global cooperation in innovation (Chien, 2018).

From this perspective, there are theoretically two polar outcomes: complete fracture and technological bifurcation on one end, or the maintenance of global collaboration and integration on the other. What our initial exploration reveals, however, is that rather than binary outcomes, we will likely see numerous grey areas and hybrid configurations. This complexity is highlighted by the significance, within this contested landscape, of initiatives that **strive to define global, or at least broadly transnational, standards**. Open technological solutions are frequently deployed to this precise end, serving as strategic instruments to shape technological trajectories and aggregate ecosystems around particular architectures (Jacobides & al., 2018; Seo & Kossmann, 2025).

Our analysis suggests that these strategic deployments of openness follow two distinct, though sometimes overlapping, logics.

4.1.1. The competitive logic: aggregating ecosystems to shape markets

In some contexts, openness is deployed as a competitive mechanism to assemble a critical mass of diverse stakeholders around particular architectures, effectively creating a de facto standard that can **challenge incumbent proprietary solutions or rival geopolitical blocs**. This logic recognizes that in network industries, the ability to attract developers, users, and complementary service providers is as important as technological superiority. Openness lowers barriers to adoption, signals credible commitment to interoperability, and distributes ownership in ways that encourage ecosystem participation.

The European Software Defined Vehicle (SDV) initiative exemplifies this logic. By creating an open-source software stack for the automotive industry, it seeks to define a standardized platform that global automakers and suppliers can adopt and build upon. The initiative, backed by companies including Mercedes-Benz, BMW, Bosch, and Microsoft, aims to prevent the fragmentation of the automotive software landscape and counter the rise of vertically integrated, proprietary solutions from new entrants like Tesla or potential big-tech disruptors. Openness here is a mechanism for incumbents to collectively defend and shape their market (FEDERATE, 2025).

Similarly, Open RAN (Radio Access Network) uses open interfaces and software-defined architectures to disaggregate hardware and software in mobile networks. By breaking open the proprietary, integrated stacks of incumbent vendors like Huawei, Ericsson, and Nokia, Open RAN

creates opportunities for new entrants and allows operators to mix and match components from multiple suppliers. Governments in the US, UK, Japan, and Europe have supported Open RAN not only for supply chain resilience but also as a mechanism to foster domestic telecom equipment industries and reduce dependence on Chinese vendors.

4.1.2. The trust-building logic: sustaining collaboration amidst geopolitical tension

In other contexts, openness is deployed to create the conditions of **trust**, **transparency**, **security**, and **autonomy** necessary for sustaining global collaboration despite geopolitical tensions. Rather than being purely competitive, these initiatives **seek to construct neutral ground**—technological and governance spaces where actors from competing blocs can cooperate without fear of lock-in or surveillance (Shams & al., 2025).

The Open Wallet Foundation aims to create a common, global open-source engine for digital wallets—a foundational component for digital identity, payments, and credentials. By developing this core, initially under the auspices of the Linux Foundation (see the Open Wallet fact-sheet for more details on its evolving governance), the initiative seeks to prevent fragmentation of the emerging digital wallet landscape, where proprietary solutions from big tech (Apple, Google) or national schemes risk creating incompatible silos. Openness here is a mechanism to ensure interoperability and prevent any single actor from controlling this critical infrastructure, but still allowing companies and governments to build competitive services atop the shared core.

X-Road, developed and governed by the Nordic Institute for Interoperability Solutions (NIIS), offers another model. This open-source data exchange layer has enabled the creation of integrated digital societies in Estonia and Finland, and is now being adopted by other countries. Its openness is a trust-building measure, assuring all participating public and private entities that the core infrastructure is transparent, auditable, and free from hidden backdoors or proprietary lock-in. It sustains collaboration across national boundaries and between public and private sectors by providing a trusted, neutral foundation.

4.1.3. An enduring logic, but on a new scale and with state intervention

Ultimately, this strategic deployment of open technological solutions for standardization purposes is not entirely novel (Blind & Böhm, 2019). It has been and continues to be widely used in market competition, where it remains one of the most important drivers of open tech uptake. The logic of using openness to attract developers, build ecosystems, displace proprietary alternatives, and influence technological trajectories has been central to the success of Linux, Apache, Android, Kubernetes, TensorFlow and countless other open-source projects. Openness enables a particular form of market strategy: one that **sacrifices direct control and monetization** over a technology **in exchange for influence over the ecosystem and the new markets** that grows around it, even as it destroys its direct commercialization or previously existing markets (Berlinguer, 2018).

The current success of Chinese open AI models, such as those released by DeepSeek, Alibaba, and Baidu, can be seen as a direct continuation of this tactic (Schoeberl & Corrigan, 2024). By releasing powerful models with permissive licenses, these companies rapidly attract developers, build global ecosystems, and position their technologies as de facto standards, thereby shaping the direction of AI development in ways that favor their strategic interests (Cheng, 2026; Lee, Aug 17, 2026). This approach to open tech—strategic, ecosystem-focused, and market-shaping—has always relied on

what might be termed the creative destruction of markets: opening what was closed to displace incumbents, while retaining the ability to compete or dominate on adjacent layers.

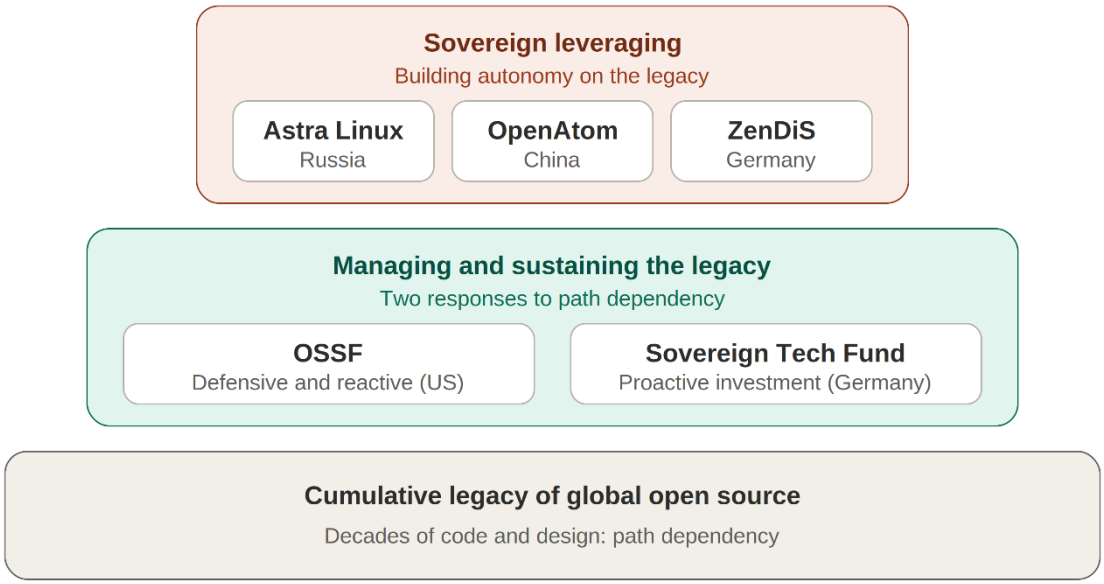
What is novel, and what cases like OpenAtom (China's open-source foundation for critical system software) and India Stack (a set of open APIs for digital identity, payments, and data) underscore, is the explicit involvement of governments in these strategic choices and the new scale at which this strategic modulation of openness and economic exploitation is being realized.

4.2. Pursuing security and sovereignty by open tech

But open technology also seems to thrive when concerns about **security** and **technological sovereignty** are at the heart of governments' approach to technology policy.

Beyond the fact that open technology promises, thanks to its transparency and reproducibility, to provide a solid basis for governments' quest for autonomy and control, there is clearly another important reason behind its use and adoption: the **cumulative legacy** embedded in open technology and open source more specifically. That is, in more theoretical terms: **path dependency** (Arthur, 1994; Berlinguer, 2020b). This concept suggests that the choices available today are often constrained or determined by the decisions and infrastructures of the past. In the digital realm, open source is not merely an optional alternative; it has become the foundational layer upon which the entire modern digital world is built. It represents a decades-long, global accumulation of intellectual capital, code, and architectural design that would be prohibitively expensive and complex to replicate from scratch. Any government or large organization seeking to build a sovereign digital infrastructure must contend with this reality: the most efficient, secure, and robust path forward is often to **build upon this existing open foundation** rather than to attempt to replace it.

Figure 1. Layers of sovereign leveraging of open source



Source: Authors' elaboration, with the support of Claude (Anthropic), based on the analysis of cases

This dual dynamic, managing the legacy while leveraging it for autonomy, is well exemplified by contrasting initiatives like the Open Source Security Foundation and the Sovereign Tech Fund. The Open Source Security Foundation (OSSF) is a classic example of managing path dependency. It is a complex, multi-stakeholder intervention designed to bring transparency, best practices, and security tooling to the widespread and ever-expanding, community-built code that every modern software system relies on. Here, the rationale is defensive: ensuring the robustness and sustainability of the de facto foundation of our digital infrastructure (OSSF, 2022). This has been the primary, often reactive, driver for government intervention in the open technology ecosystem, with the US government acting as a prime example through its support for such initiatives. A slightly different case is exemplified by the Sovereign Tech Fund (STF) in Germany. While the STF also cares deeply about security, its approach is distinct. Instead of merely reacting to vulnerabilities in the existing foundation, the STF actively invests in strengthening and sustaining the open-source infrastructure that the German economy and public administration depend on. It pays developers to maintain critical but often underfunded open-source projects. This acknowledges the same path dependency: Germany relies on this global code but responds with a positive, sustaining intervention to ensure its long-term health and, consequently, Germany's digital sovereignty. It is a proactive investment in the cumulative legacy rather than a reactive patch for it (Gates & al., 2025).

This logic of leveraging the legacy for autonomy becomes even more pronounced in recent sovereignty-driven initiatives. Here, open technology is not just a legacy system to be secured or maintained, but a key strategic lever for building independent capabilities. The reason these initiatives adopt open technology is precisely the path dependency described above: they offer the possibility of building upon existing, solid, and globally available foundations, rather than starting from zero.

Consider Astra Linux. It is an operating system, developed in Russia, initially for military and security purposes, and which has taken on a broader scope following the sanctions adopted by major economic players against Russia (Raza, 2026; Rodeheffer, 2026; Vavilov, 2026). It is not a wholly proprietary system but a Linux distribution. It leverages the immense, battle-tested codebase of the Linux kernel and the broader GNU/Linux ecosystem to create a secure, government-grade operating system tailored for military and state use. By forking and hardening this open-source foundation, the developers gain a level of control and auditability, crucial for security certifications, that would be much more expensive with a closed, foreign-owned operating system. They stand on the shoulders of a global giant to achieve national autonomy.

A similar, albeit even more ambitious, logic underpins OpenAtom in China. As China's first open-source foundation, OpenAtom's goal is to foster a homegrown open-source ecosystem (Cheung, 2024). Yet, its projects, such as the operating system OpenHarmony, do not reject the existing global legacy. Instead, they strategically build upon it. OpenHarmony incorporates elements and concepts deeply rooted in the history of Unix-like systems and modern distributed operating systems. The foundation allows Chinese developers to leverage global open-source knowledge while building a stack that is ultimately governed and controlled domestically, insulating it from potential future restrictions. It is an attempt to benefit from the global legacy while constructing a parallel, sovereign ecosystem.

Finally, the German government's ZenDiS (Zentrum für Digitale Souveränität, or Centre for Digital Sovereignty) has a flagship project, OpenDesk, aiming to create a sovereign, open-source workplace suite for the German public sector (Deuse, 2026). Instead of building everything anew, ZenDiS orchestrates and integrates existing open-source components (like collaboration tools, email

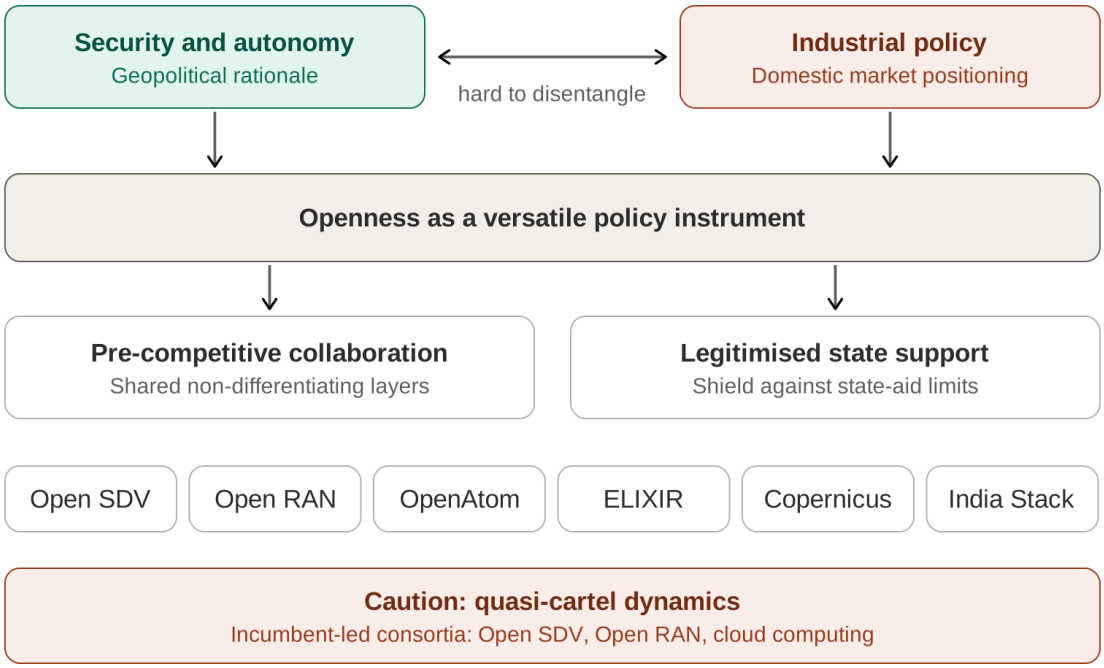
servers, and office suites) into a cohesive, secure, and federated platform. By doing so, it reduces Germany's public administration reliance on proprietary, non-European cloud providers. Here, the sovereignty lies not in creating entirely new code, but in curating, hardening, and integrating the existing open-source legacy to create a trusted, independent digital infrastructure.

In all these cases the strategic adoption of open technology is a direct response to the path dependency of the digital age: true autonomy is not achieved by ignoring the global foundation, but by deliberately and securely building upon it.

4.3. The strategic deployment of openness in industrial policy

Indeed, while it is possible to characterize certain uses of openness as serving national security or geopolitical purposes, it is equally evident that when identifying the primary motivation behind governments' adoption of open technological solutions, it has often proved difficult to disentangle **strategic autonomy** and **security considerations** from objectives of **supporting domestic industrial competitiveness and market positioning in emerging sectors**. In some cases, security or geopolitical framings may serve to legitimize what are fundamentally competitive and protectionist industrial policies. The boundary between safeguarding critical infrastructure and nurturing national champions becomes blurred, with openness serving as a versatile policy instrument that can be justified through multiple, overlapping rationales.

Figure 2. Openness as a geopolitical instrument



Source: Authors' elaboration, with the support of Claude (Anthropic), based on the analysis of cases

However, even in these ambiguous cases, like Open SDV or Open RAN we observe a growing strategic deployment of open solutions for two principal reasons that are reshaping the relationship between the state and the private sector.

First, openness is used to **promote collaboration within private industry on shared infrastructural layers**, enabling competitors to cooperate on non-differentiating components and competing on higher-value applications. This logic recognizes that foundational technologies—whether in cloud computing, automotive software, or financial infrastructure—are often too complex and costly for any single company to develop alone, and too critical to leave entirely to uncoordinated market forces. By collaboratively building open core components, industries can accelerate innovation, reduce duplication of effort, and create larger pools of talent and investment, all while preserving competitive differentiation at the application layer. This approach differs from the traditional vertically integrated model based on ownership or control by a unique corporation (Chandler, 1993).

Second, openness serves to **legitimize state support for the private sector** in ways that may be less vulnerable to regulatory or political challenges regarding market distortion. By framing investments as contributions to "open infrastructure," "digital public goods," or "pre-competitive research," governments can intervene in markets while ostensibly avoiding the appearance of picking winners or creating national champions. This is particularly valuable in jurisdictions like the European Union, where state aid rules strictly limit direct subsidies to private companies. Openness provides a shield: support for an open-source project can be presented as benefiting the entire industry or ecosystem rather than a single firm, thereby navigating complex regulatory frameworks (Berlinguer, 2024).

This approach is particularly evident in the European Union - as with the case of the Open SDV (Software Defined Vehicle) initiative - which has increasingly adopted policies to finance and support the joint development of "pre-competitive" or "non-differentiating" components by private companies.

Beyond Europe, similar dynamics are observable in diverse contexts. OpenAtom in China, while clearly serving strategic autonomy goals, also functions as an industrial policy instrument. By creating a foundation that hosts open-source projects like OpenHarmony, the Chinese government provides a legitimized platform for domestic companies—including Huawei, Alibaba, and Tencent—to collaborate on foundational software, reducing their collective dependence on foreign operating systems like Android and Windows, while fostering a domestic software industry capable of competing globally. In the telecommunications sector, **Open RAN** (Open Radio Access Network) initiatives, supported by governments in the US, UK, Japan, and Europe, aim to break the dominance of legacy vendors like Huawei, Ericsson, and Nokia. By promoting open interfaces and software-disaggregated architectures, governments enable a new wave of specialist vendors and system integrators to enter the market, fostering industrial competition and supply chain resilience.

Yet, these initiatives have often also shown **quasi-cartel dynamics**, with a small number of large operators coordinating through industrial consortia to set standards in such a way as to ultimately favor incumbent operators already present on the market. This dynamic has already been observed in cloud computing, where open source components predominate on the one hand, while on the other the market is extremely concentrated among a **few suppliers** (Schoeberl & Corrigan, 2024; Berlinguer, 2024). A comparable risk cannot be excluded for Open SDV, given that participation is contingent on membership and led by a consortium of large firms. This is an example that calls for caution about how openness can be strategically exploited within concentrated industrial structures.

The industrial policy logic of openness extends well beyond software and telecommunications into other critical sectors. In life sciences, ELIXIR—a pan-European intergovernmental organization—coordinates the development and maintenance of open data infrastructures for biological research[13]. By providing shared, open platforms for bioinformatics data, it enables European researchers and biotechnology companies to access world-class resources without each member state or firm needing to build and maintain its own costly infrastructure, thereby enhancing the competitiveness of the entire European life sciences industry. In the space sector, the ESA Copernicus program, operated by the European Space Agency in partnership with the European Union, makes vast quantities of Earth observation data freely and openly available. This open data policy has catalyzed a thriving downstream industry of startups and SMEs that develop commercial applications for agriculture, urban planning, climate monitoring, and insurance, creating jobs and economic value while fulfilling public missions (Sawyer & al., 2022; Kovács & al., 2026).

Perhaps the most transformative example of openness as industrial policy is India Stack. This set of open APIs for identity, payments, and data sharing, developed with strong government backing, has created a foundational digital infrastructure that has enabled an explosion of innovation in fintech, e-commerce, and public service delivery. By providing these layers openly, the Indian government has effectively de-risked digital entrepreneurship, allowing hundreds of domestic startups to build innovative services without having to develop their own identity verification or payment systems. The result has been the creation of a vibrant, domestically-controlled digital economy.

Across all these cases - from European automotive software to Chinese operating systems, from Indian digital infrastructure to European space data - a consistent pattern emerges. Openness is no longer merely a development methodology or a licensing choice. It has become an industrial policy tool, enabling governments to support domestic industries, shape technological trajectories, and navigate the boundary between fostering competition and ensuring strategic autonomy. This trend evidently opens a new avenue for research into open infrastructures, as it demonstrates their potential to become instruments through which government-backed companies can try to exert control over emerging markets and shape technological trajectories (see the automotive industry in EU). The challenge for researchers and policymakers alike will be to understand when such strategic deployment of openness serves genuine public interest and broad-based innovation, and when it masks protectionism or facilitates the concentration of market power under the guise of collaboration.

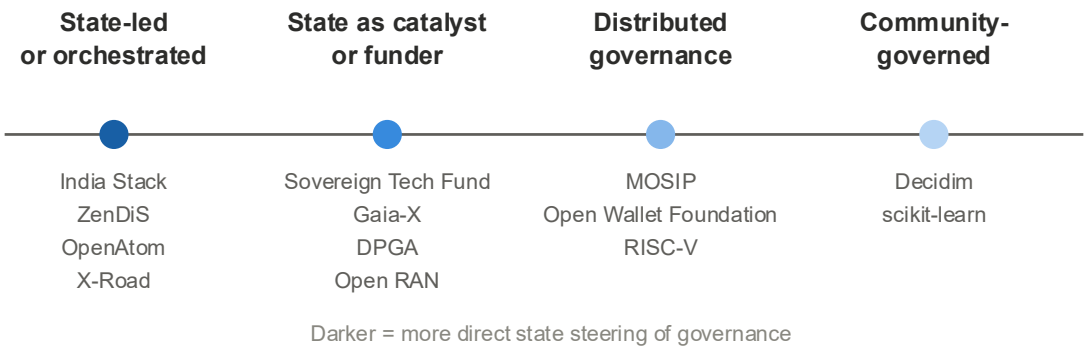
4.4. Digital public infrastructure: the return of the hesitant state

After decades where the dominant ideology (neoliberalism) favored privatization, deregulation, and the retreat of the state from direct economic intervention, governments are waking up to a stark reality. Technology is not merely a sector of the economy; it has become the foundational layer upon which economic competitiveness, national security, and even democratic health are constructed. The rise of China's state-led model of technological development, the vulnerabilities exposed by the energy crisis and pandemic-induced supply chain shocks, and the growing unaccountable power of Big Tech platforms have all acted as forceful wake-up calls. Consequently, we are witnessing a return of explicit industrial policy (Mazzucato & al., 2021; Terzi & al., 2022; Sullivan, 2023) - emblematically through the CHIPS Act and the Inflation Reduction Act (IRA) in the

[13] https://elixir-europe.org/about-us

United States - and a renewed focus on "tech sovereignty," particularly within the European Union (Lusi & al. 2025)[14].

Figure 3. State involvement in digital public infrastructure: a spectrum of governance models



Source: Authors' elaboration, with the support of Claude (Anthropic), based on the analysis of cases

However, unlike the confident, directive state of the post-war era, today's state is stepping back in with some hesitation, particularly in the EU (but less so in the US and Asia). There appears to be **caution in fully leveraging the state's directive capacity** (Wright & al., 2021; Del Bo & al., 2025) to implement open technology initiatives for building public infrastructure or providing digital public goods and services. This hesitation in the EU stems from a complex mix of factors: eroded institutional capacity after decades of outsourcing, fear of market distortion, ideological legacies that privilege private-sector solutions, and uncertainty about appropriate governance models in a fast-moving technological landscape.

Despite the growing discourse around **Digital Public Infrastructure (DPI)** (World Bank, 2021b; Clark & al. 2025) - a framework that reframes digital services not as commodities to be bought and sold, but as **foundational public utilities** (Berlinguer, 2021; Bernier & al., 2020)- our sample reveals relatively few concrete cases that substantively embody this vision. DPI suggests an infrastructural layer below the market, one that enables private competition and innovation while remaining under some form of public stewardship (Mukherjee & Joshi, 2025). It promises the efficiency of private enterprise built atop the stability and equity of public goods. But what does "public stewardship" actually look like in the digital realm? And who holds the state back from fully embracing this role?

India Stack represents the most prominent and significant counterexample to this trend of hesitation—a comprehensive digital infrastructure initiative driven decisively by the Indian state. Conceived and orchestrated by the government in partnership with private innovators, India Stack provides a set of open APIs for digital identity (Aadhaar), payments (UPI), and data sharing. It has successfully created a foundational layer upon which hundreds of domestic startups and financial institutions have built innovative services, fundamentally transforming financial inclusion and digital commerce in India. Yet, even here, the model is not straightforward. The state led the initiative and

[14] See also section 4.3 on Industrial Policy. For an update on the EU policy see https://commission.europa.eu/strategy-and-policy/state-union_en

deployed multiple roles –but India Stack did not embody a clear or systematic commitment to open-source technology. Its components are open APIs, but the underlying code and governance have not followed open-source principles. This also reveals that "openness" in DPI can take multiple forms: open interfaces, open data, open source, or open standards.

The hesitation of other states becomes more visible when contrasting India's approach with European initiatives. Consider Germany, a country with deep resources and a strong stated commitment to digital sovereignty. It has produced two initiatives that embody explicit commitments to open technology, yet they display different understandings and approaches of public infrastructure (also depending on the target group of the initiative; Public administration standards vs community-led pieces of critical infrastructure), revealing different conceptions of the roles of government and communities.

On one hand, ZenDiS (Zentrum für Digitale Souveränität), the Centre for Digital Sovereignty, represents a more traditionally state-led and controlled model. Its flagship project, OpenDesk, aims to create a sovereign workplace suite for the German public sector by integrating existing open-source components. The state acts as the orchestrator, funder, and customer, effectively creating a public alternative to proprietary cloud services. The governance remains firmly within the public sphere, with the center directing development according to the needs of public administration.

On the other hand, the Sovereign Tech Fund (STF), also a German government initiative, embodies a radically different philosophy. In this case the public infrastructure is conceived as community-led and publicly supported, with the government playing a supportive role in the maintenance and development of critical open-source infrastructure that the German economy and society depend upon, regardless of where in the world that code originates. Rather than building its own sovereign solutions, the STF strengthens the global open-source commons, trusting that a healthy, sustainable ecosystem is the best guarantee of long-term sovereignty. It is a model of public stewardship that operates indirectly, through enabling rather than directing.

This diversity of governance models is not limited to Germany and India. Many other cases from our analysis warrant examination through the DPI lens, demonstrating considerable variety in how the three poles of governance—state leadership, market participation, and community control—are combined and balanced.

- MOSIP (Modular Open Source Identity Platform), for instance, offers a compelling hybrid. Modelled on India's Aadhaar but built as open-source software from the ground up, it is a platform that enables other countries (particularly in the Global South) to build their own foundational digital identity systems. Here, an open-source community provides the core technology, while sovereign states retain control over their national implementations. The governance is distributed: the community stewards the code, but each deploying state governs its own instance.
- Gaia-X attempts to construct a federated data infrastructure for Europe. It is neither purely state-led nor purely market-driven. Instead, it brings together public and private actors to define common standards and open building blocks, with the expectation that private companies will build competitive services atop this agreed foundation. The state's role is to catalyze and legitimize collaboration, not to build or operate the infrastructure itself.
- OpenAtom in China represents a state-orchestrated model within a different political context. As a foundation hosting open-source projects like OpenHarmony, it aims to create a domestically governed ecosystem. Here, the state's hand is visible but indirect, using the

foundation structure to align private sector giants (Huawei, Alibaba) around shared infrastructural goals, effectively creating a national open-source industrial policy.

- The Open Wallet Foundation, by contrast, is a global, collaborative effort initiated by the Linux Foundation to develop an open-source engine for digital wallets. It is not tied to any single state. Its governance is multilateral, its outputs are expected be adopted and implemented by public and private actors worldwide, but with each layering their own national policies and commercial strategies on top.
- Decidim, a digital platform for participatory democracy developed by the Barcelona City Council and since adopted by numerous other cities and organizations, offers a different model again. It is publicly funded and community-owned, with governance shared between the original public sponsors, a community of developers, and the myriad user institutions. It represents a form of "commoning" where public infrastructure is co-governed by its users and creators.
- Open RAN initiatives, supported by governments seeking to diversify telecom supply chains, illustrate the challenges of DPI in concentrated industries. While aiming to create open, interoperable mobile networks, the governance of these standards is often shaped by a small number of large incumbents, raising questions about whether the resulting infrastructure will truly be open or merely re-intermediated by new forms of private control.
- Finally, even the Digital Public Goods Alliance (DPGA), a multi-stakeholder initiative hosted by the UN and supported by governments including Norway and Sierra Leone, represents an attempt to create global governance infrastructure for identifying, certifying and promoting digital public goods of many different kinds (open-source software, data, AI models, standards, content). It is a meta-layer of stewardship, aiming to coordinate and promote the ecosystem rather than build specific technologies.

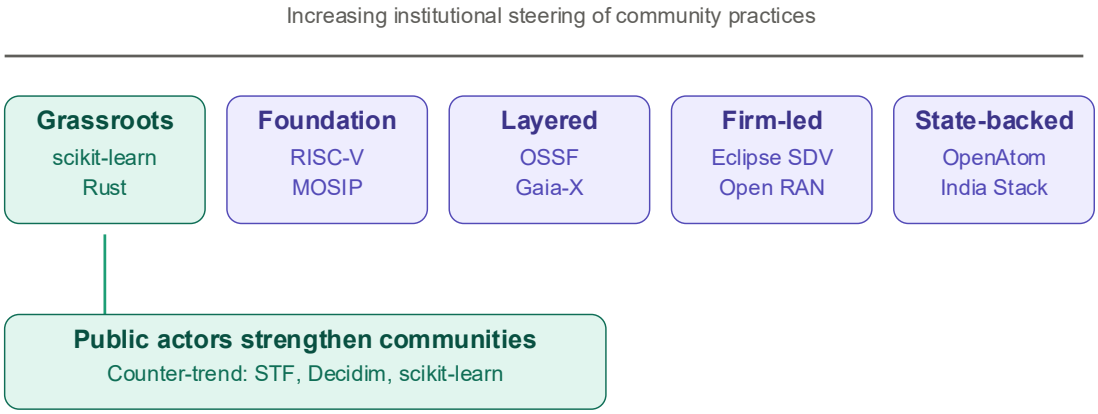
What emerges from this landscape is a picture of experimentation. The field of Digital Public Infrastructure is not yet settled. There is no dominant model of how states should engage, how communities should participate, or how openness should be defined and implemented. India Stack demonstrates the transformative potential of decisive state action, yet its selective openness raises questions about long-term lock-in and governance. Germany's twin experiments bring out a strategy that still needs to be clarified and internal tensions between state-led direction and community-led support. Global initiatives like MOSIP and the Open Wallet Foundation show that DPI can be built across borders, but their governance must navigate complex national interests.

This diversity suggests that the **return of the state** in the digital realm remains hesitant precisely because the appropriate forms of that return are **still being invented**. The state is not simply stepping back in with the confidence of the mid-twentieth century; it is tentatively exploring new roles - as funder, catalyst, orchestrator, customer, regulator, and sometimes builder - while learning to share space with communities and markets. DPI initiatives will most likely constitute an area where further evolution of state involvement could materialize and potentially generate the greatest transformative impact. The question for the coming decade is which of these experimental governance models will prove durable, scalable, and capable of delivering the public value that the hesitant state, for all its caution, is now once again being called upon to provide.

4.5. The evolving logic of community in tripartite open tech governance

A further central theme emerging from our analysis of over 20 open-technology initiatives is the profound and continuing **transformation of community models**. While the "community" remains a vital governance mechanism alongside state and market actors (forming what we term the tripartite governance of open tech) its form and function have evolved dramatically from the early days of the free software movement. Understanding this evolution is essential for grasping how open technologies are actually governed today.

Figure 4. The institutional evolution of community models in open technology initiatives



Source: Authors' elaboration, with the support of Claude (Anthropic), based on the analysis of cases

In our research, we defined the term "community" broadly to accommodate this evolution, identifying, as its essential characteristics, voluntary collaboration between independent actors and the release of collaborative outcomes through open licenses. This broad definition allows us to recognize community-like dynamics even in highly institutionalized settings. However, to classify a case as genuinely "community-driven," we applied stricter criteria, considering factors such as the **absence of economic or institutional barriers to individual participation**, the primacy of **meritocratic governance** over corporate or institutional affiliation, and the genuine **coexistence of diverse stakeholder types** beyond just corporate or institutional actors. This distinction between community practices (open collaboration, licensing) and community governance (who holds decision-making power) is central to our analysis.

From this perspective, our mapping reveals a picture of relative resilience alongside profound transformation. Some initiatives continue to thrive under conditions that closely resemble the original community ethos (Benkler, 2006). For instance, scikit-learn, the widely used machine learning library, operates under a clearly defined meritocratic, consensus-based governance model, with decision-making power rooted in technical contribution and peer recognition rather than institutional affiliation. Its steering council is composed of individuals elected by contributors, not corporate appointees (Osborne, 2024). Similarly, the Decidim project, a digital platform for participatory democracy, is governed through what its founders term a "public–commons partnership." Here, an independent, community-led association co-manages the digital infrastructure as a shared public good alongside the municipalities that deploy it (Barandiaran & al.,

2024). This model demonstrates that community logic can remain central even when interfacing extensively with government actors, precisely because the governance structures insulate community decision-making from direct state control.

At the same time, even these nominally independent communities face increasingly subtle pressures to align with corporate or governmental priorities. The dependence of scikit-learn on corporate-employed contributors for maintenance and more recently from French government funding, or the need for Decidim to respond to the procurement needs of its government adopters, creates tensions that require constant negotiation. The pure, autonomous community is increasingly rare.

The most remarkable evolution, however, is not merely the persistence of these communities, but the expansion and adaptation of their critical practices—particularly open licensing and collaborative development—into corporate and institutional contexts. This signals a broader **hybridization and institutionalization of community models** (Geels, 2011; Skelcher & Smith, 2015; Berlinguer, 2020a), a process that has been accelerating for some time, particularly through the evolution of the role of major open-source foundations.

Some initiatives begin with a strong community core but face an evolutionary trajectory that leads to strategic alignment with institutional actors. Risc-V, the open standard instruction set architecture, started as a largely academic project at UC Berkeley but has since become governed by Risc-V International, a foundation whose strategic direction is shaped by its corporate members—including major players like Google, Qualcomm, and Alibaba. While technical development retains community-like practices, the roadmap and prioritization are increasingly influenced by corporate strategies (Krewer, 2025). Similarly, Rust, the programming language, began as a Mozilla-led project but transitioned to the independent Rust Foundation, whose board includes representatives from its corporate members (AWS, Google, Huawei, Microsoft, Mozilla). The core team continues to govern it technically through meritocratic processes, but the foundation's resources and strategic decisions are now mediated through a corporate structure.

In numerous other instances, we observe community practices relegated to subordinate positions within broader, institutional governance structures (OSSF, Gaia-X, for example). This hierarchy has become typical in many projects hosted by major open-source foundations, where board positions responsible for setting strategic direction are often allocated to large corporations based on funding contributions, while community practices are confined to technical development working groups. The Open Source Security Foundation (OSSF), hosted by the Linux Foundation, exemplifies this layered model. Its governing board is composed primarily of corporate representatives from companies like Google, Microsoft, and Intel, who determine overall priorities and funding. The technical work, however, is carried out through open, collaborative working groups that anyone can join. Here, community logic operates at the implementation level, but strategic governance follows a corporate, hierarchical logic. Gaia-X presents a similar picture: its board and steering committees are dominated by large European corporate interests, while technical working groups are nominally open but require significant time and resource commitments that effectively exclude independent individuals.

As these communities integrate into hierarchical and formal institutions, some original traits persist - such as collaborative frameworks and the distribution of contributions through open licenses. However, these traits are often attenuated as individuals lose autonomy, and intrinsic motivations are supplemented or supplanted by top-down orchestrated agendas and professional employees,

and extrinsic incentives (corporate mandates, performance targets) replace volunteer contributions. Critically, **organizations - rather than individuals - become the primary actors** within the "community." This creates a layered structure where the vertical hierarchical logic of the institution (corporate strategy, funding priorities) overarches the horizontal, collaborative logic of the community (technical contribution, peer review).

This dynamic is even more pronounced in cases where a consortium of companies leads the project and participation in working groups is restricted to employees of member organizations. The Eclipse SDV (Software Defined Vehicle) initiative, an alliance part of the broader Open SDV initiative, which we investigated by a direct interview, is a paradigmatic example. Here, dozens of companies - including automotive manufacturers like Mercedes-Benz and BMW, suppliers like Bosch, and technology firms like Microsoft and Siemens - have partnered in a pre-competitive collaboration to develop a shared "automotive-grade" open-source core stack and "non-differentiating" components. Participation in the working groups that shape this stack is contingent on membership. The "community" here is a community of firms (Snow & al., 2009), not individuals, collaborating on shared infrastructure and preserving competitive differentiation elsewhere. It represents a corporate appropriation of community practices, adapted for industrial strategy (Gencer & Oba, 2017; Nguyen-Duc & A., 2018; Osborne & al., 2025).)).

Finally, OpenAtom, as a large-scale, government-backed open-source foundation in China, represents the ultimate institutionalization of community practices. It provides a formal legal and financial home for numerous projects, including OpenHarmony. The foundation structure mimics that of Western open-source foundations, but its strategic direction is closely aligned with national industrial policy objectives (Cheung, 2024). Community practices - open collaboration, shared code, distributed contribution - are channeled within a state-supported framework designed to foster domestic technological autonomy.

This process marks a departure from the original ethos of grassroots free software communities, which valued individual autonomy, hacker ethics, and often explicit political opposition to proprietary control. However, it also highlights a broadening of the model's influence, extending its reach into corporate boardrooms and government ministries. The practices pioneered by communities have become a global standard for efficient, distributed innovation, as have open digital commons.

In conclusion, our analysis suggests that **we are witnessing not the end of community, but its evolution into more complex, layered, and institutionalized forms**. The core practices - open collaboration, open licensing, and the production of common goods - have been widely adopted and adapted. However, their meaning and operation are now filtered, shaped, and sometimes subordinated by other logics: corporate strategy, state industrial policy, and institutional governance. This generates at times tense balances of power, as the horizontal logic of contribution meets the vertical logic of control.

The result is a spectrum of governance models, from community-driven projects like scikit-learn and Decidim, through deeply hybrid structures like Open SDV and OSSF, to institutional platforms like the Digital Public Goods Alliance (DPGA) and OpenAtom, where community practices serve broader strategic purposes. Understanding this spectrum is essential for anyone seeking to navigate or govern the open technologies that increasingly underpin our digital world.

There is also another direction of this transformation in the composition, role, and functioning of communities that could assume greater importance in the future. We see this reflected in initiatives

such as STF and Decidim, in which public actors are working to strengthen the role of communities. This direction hints at a **potentially renewed and more significant role** for communities as a distinct and balancing force in technology governance. Communities could perform functions that go beyond technical development: **providing legitimacy** through broad participation, acting as a **counterweight to the power of corporations and the state**, fostering **trust across geopolitical divides**, and **defending the rights of citizens and users**. To realize this potential, however, it is necessary to rethink what communities are, what governance functions they can perform, and to develop new institutional frameworks that support this renewed role (Risc-V and Decidim are examples of this).

5. FURTHER RESEARCH

While this study has opened several avenues for future inquiry that we cannot fully explore here, we highlight two research directions that we believe are particularly worth pursuing.

5.1. The mission ahead: developing a polycentric approach to open tech governance

Future research could productively engage with two distinct, though related, strands of the Ostromian intellectual tradition. The first is the well-known framework for the governance of common-pool resources, which is foundational but **does not transplant straightforwardly** to the digital realm (Madison & al., 2009; Frischmann & al., 2014; Berlinguer, 2020a). Open digital resources such as code, data, and standards differ fundamentally from fisheries or forests: they are open access and non-rivalrous; their main dilemmas and risks are not about overexploitation but revolve around a scarcity of engagement, adoption and development (Schweik & English, 2012)); their governance involves actors operating at scales and with logics far removed from the small-scale, face-to-face communities Ostrom originally studied (Hess & Ostrom, 2007). Nevertheless, the three taxonomies developed in this study (addressing stakeholder influence, government intervention rationales, and community composition) may be understood as a contribution to the kind of middle-range theorizing that Ostrom consistently advocated: empirically grounded, yet oriented toward broader analytical generalizability (Ostrom, 2010).

The second and potentially more fruitful strand is the framework of **polycentric governance**, rooted in Vincent Ostrom's work on metropolitan governance and public administration (Ostrom, Tiebout and Warren, 1961; Ostrom, 1973), and to which Elinor Ostrom turned with increasing insistence in the later years of her life. Polycentricity, understood as a system of multiple autonomous centers of decision-making operating under an overarching set of rules, capable of mutual adjustment, experimentation, and learning, was developed precisely to address large-scale, multi-level governance challenges of the kind encountered in open technology ecosystems (Krewer, 2025). Future research could explore how this framework might illuminate several dynamics that the present study has documented but not fully theorized. It could examine **how community logic becomes institutionalized** within broader, nested governance structures without losing its distinctive character; how governments can exercise meaningful agency through strategic participation in multi-stakeholder arrangements rather than through unilateral command; and how governance systems in a domain as dynamic as open technology can be designed to remain experimental and adaptive over time (Ostrom, 2009; Sabel & Zeitlin, 2012).

Elinor Ostrom herself acknowledged that polycentricity was less a fully specified theory than a research program, a set of orienting concepts and hypotheses requiring empirical testing and theoretical elaboration (Ostrom, 2010). The governance of open technology initiatives, with its abundance of cases, its variation across jurisdictions and sectors, and its high-stakes experiments in multi-actor coordination, could constitute an ideal terrain for advancing this program. Questions such as how overarching rules emerge and gain legitimacy in systems without central authority, **what mechanisms sustain trust** among actors distributed across competing firms and rival states, and how polycentric systems in the digital realm fail as well as succeed, are not merely academic: they are pressing practical challenges for those responsible for governing the infrastructures on which contemporary societies increasingly depend. Further research should discuss larger trajectories of theory of governance in increasingly complex environments.

Within this framework, Ostrom's rejection of the so-called 'tragedy of the commons' narrative and her demonstration that communities are capable of developing sophisticated self-governance arrangements established a methodological legacy that remains highly relevant to hybrid governance forms of the kind documented here. Nevertheless, future innovations in the governance of open technological initiatives must address the need to strengthen communities and more importantly, they must **reconsider** these **communities in light of a new understanding** of their composition—comprising not only individual developers but also organizations and users—and their role within the emerging tripartite governance models. Increasingly, these communities must contend with the strategic exploitation of digital commons by tech giants ("hyperscalers"), who leverage them to consolidate their dominant positions, reduce development costs, steer the evolution of these resources, and exploit monopolistic or oligopolistic advantages in other segments of the technology stack and in complementary markets. Ultimately, however, the pursuit of more innovative and balanced governance for technological initiatives cannot succeed in isolation; it must be supported by broader public policies aimed at dismantling the current, extreme concentration of market power in the digital sphere and fostering a new balance of power in the management of critical technological systems.

5.2. The structural rarity of balance

In the context of this broader polycentric framework—which would be worth exploring and developing in future research on the governance of large-scale digital infrastructures—there is a specific challenge that deserves closer examination: the structural rarity of balance.

In structuring our analysis, we rapidly realized that **balanced models** of governance (where communities, firms, and states exercise meaningful and co-equal influence) were **exceptional**. All three actors engage with open-technology models, but they do so from distinct positions and with distinct logics, incentives, and temporal horizons. The term "tripartite" thus better emphasizes the dynamic, sometimes idiosyncratic and antagonistic, interactions that define these governance systems.

The tense nature of these relationships is reflected in the empirical reality that balanced tripartite governance models are exceedingly rare. In most cases examined, one of two patterns predominates. Either a single pole dominates and the others occupy subordinate or peripheral positions, or collaboration occurs primarily between two poles, leaving the third marginalized or almost entirely absent. True multipolarity, where all three actors exercise meaningful influence over strategic decisions, remains exceptional (Pache & Santos, 2013; Skelcher & Smith, 2015).

Why is balance so difficult to achieve? There are several structural factors.

First, the poles operate with fundamentally **different logics and timescales**. Firms are driven by market competition, shareholder value, and relatively short-term product cycles (Friedman, 1970; Laverty, 1996; Porter, 1997). States are oriented toward public goods, national competitiveness, security, and electoral cycles (Samuelson, 1954; Nordhaus, 1975; Porter, 1990). Communities are motivated by intrinsic rewards, peer recognition, technical excellence, and often a commitment to openness as an end in itself (Raymond,1999; Benkler, 2002; Lakhani & Wolf, 2003). Aligning these divergent motivations around shared strategic decisions requires continuous negotiation and institutional design that is costly and fragile.

Second, **resources are asymmetrically distributed**. Firms and states command budgets, employees, and procurement power that communities cannot match. This asymmetry tends to

translate into governance influence, particularly in foundations where board seats are allocated based on funding contributions (O'Mahony & Ferraro, 2007; Riehle, 2010). Communities may retain control over technical development, but strategic direction - where the money goes, what gets prioritized - is often captured by those who fund the initiative.

Third, **the stakes rise as projects mature**. Early-stage initiatives may thrive with community-led governance, but as they become critical infrastructure - used by governments and corporations alike -demands for professionalization, security guarantees, and strategic alignment intensify (Geels & Schot, 2007; Hanseth & Lyytinen, 2010). These demands often privilege state and corporate actors, whose resources and authority are seen as necessary for scaling and sustaining the project, at the expense of community autonomy (Avelino & Rotmans, 2009).

5.2.1. The pathologies and the promises of tripolarity

Imbalanced governance can also generate **pathologies**. Just to name a few. Where firms dominate, like in a consortium, the risk is that openness serves primarily as a mechanism for corporate co-ordination (Snow & al., 2009). Where states dominate, the autonomy and critical voice that communities can provide may be suppressed (Scott, 1998). Where communities dominate in isolation, the risk is sustainability failure and struggle to achieve the scale and reliability required for widespread adoption as critical infrastructure (Eghbal, 2016).

On the other side balanced tripartite governance models can potentially **harness the comparative strengths of each actor and governance mode**. Again to name a few possibilities:

- **Communities** bring innovative capacity, technical legitimacy, peer review, and a commitment to openness as a public good. They also serve as a critical check on corporate and state power, advocating for user rights, transparency, and long-term stewardship.
- **Firms** bring resources, scaling capabilities, product discipline, and market access. They translate community innovations into reliable products, provide employment for core developers, and drive adoption through commercial channels.
- **States** bring coordinating authority, long-term vision, public interest orientation, and the capacity to invest in infrastructure that markets underprovide or tend to transform into private monopolies. They can set standards, mandate interoperability, fund maintenance, and ensure that digital infrastructure serves democratic values and social goals.

5.2.2. Glimpses of tripolarity: Risc-V and beyond

The evolution and dynamism of **Risc-V** offers a promising, if fragile, example of emerging tripartite governance. Risc-V began as a community-driven academic project but, as its potential became apparent, major technology companies joined the project and Risc-V International, the governing foundation. More recently, governments across multiple jurisdictions have begun investing in Risc-V ecosystems. The result is a governance structure where community contributors continue to shape the technical architecture, corporate members fund and prioritize development, and states provide supportive policies, funding, and procurement signals**.** Maintaining this balance as stakes increase—particularly as export controls and geopolitical tensions intensify—remains a substantial governance challenge, but the model offers a template for how a balanced tripartite model of governance might function.

MOSIP (Modular Open Source Identity Platform) offers another promising instantiation. Governed by the International Institute of Information Technology in Bangalore, with funding from multiple

governments and foundations, and developed through open-source community practices, MOSIP enables countries to build their own foundational identity systems. Here, the state pole is distributed across multiple national governments who adopt and customize the platform; the community pole develops and stewards the core code; and the firm pole provides implementation, integration, and support services. The governance design explicitly attempts to balance these forces.

Decidim, despite the role of the Barcelona government in its development, represents a different tripartite configuration. It is governed through a deliberately constructed "public–commons partnership" where an independent community association co-manages the platform alongside the municipalities that deploy it. Firms provide implementation and customization services but do not control governance.

Even **India Stack**, although predominantly state-driven in its origins, exhibits tripartite dynamics in operation. The state provides the foundational infrastructure and regulatory framework; hundreds of firms build applications and services atop it; and communities of developers, users, and civil society organizations contest, shape, and adapt its evolution. The governance of the underlying infrastructure remains state-centric, but the ecosystem as a whole is vibrantly tripartite.

5.2.3. Strategies for transforming idiosyncrasy into synergy

Balanced tripartite arrangements can stabilize multilateral cooperation, enabling firms, states, and communities to align around shared standards and infrastructures and at the same time preserving space for contestation, experimentation, and innovation. The challenge lies in designing governance institutions that can manage the inherent tensions and prevent any single pole from capturing the system. Our cases suggest several strategies.

1. **Deliberate institutional design**. Governance structures can be designed to ensure meaningful representation for all three poles. This might include reserved seats on governing board STFs for community-elected representatives, alongside corporate and government appointees; transparent and meritocratic technical governance insulated from funding influence; and clear mechanisms for contestation and appeal. The Risc-V International model, with its balanced membership classes and technical steering committees, offers lessons.
2. **Public funding without public capture**. The Sovereign Tech Fund demonstrates that states can provide resources without demanding control. By procuring maintenance and development and by respecting community governance, the STF model suggests a pathway for state support that strengthens rather than subordinates community autonomy.
3. **Multi-stakeholder foundations**. The Linux Foundation and its various projects (including Open Wallet Foundation, Hyperledger, Risc-V, and OSSF) offer templates for hosting tripartite governance, although they must strenghten mechanisms against corporate capture of board-level decisions. By providing neutral legal and financial infrastructure, these foundations can convene states, firms, and communities around shared projects. However, the Foundation model is just beginning to grapple with situations where there are governments directly involved.
4. **Layered governance**. Distinguishing between strategic governance (where firms and states may appropriately have greater weight) and technical governance (where community meritocracy should prevail) can help manage tensions (O'Mahony & Ferraro, 2007). The challenge, as seen in OSSF and Gaia-X, is preventing the hierarchy from becoming absolute—

ensuring that community voices in technical working groups can influence strategic priorities, not merely implement them (Baur, 2026)..

5. **Experimentation and adaptation**. Our cases reveal no single blueprint for a balanced tripartite model. Decidim's public–commons partnership, MOSIP's distributed sovereignty, Risc-V's evolving foundation—each represents a different institutional experiment. The field remains in an exploratory phase, and what works in one context may fail in another. The key is to treat governance as a design challenge, continuously negotiated and adapted, rather than a fixed template.

In conclusion, balanced tripartite governance remains rare and fragile but it offers a compelling vision for how open technologies might be governed in ways that harness the strengths of all three typologies of governance models. The challenge is not to eliminate tension but to design institutions that can channel these tensions toward synergistic outcomes rather than allowing them to degenerate into capture, exclusion, or stalemate.

REFERENCES

Arcesati, R., & Meinhardt, C. (2021). China bets on open-source technologies to boost domestic innovation. MERICS Primer.

Arthur, W. B. (1994). Increasing returns and path dependence in the economy. University of Michigan Press.

Avelino, F., & Rotmans, J. (2009). Power in transition: an interdisciplinary framework to study power in relation to structural change. European journal of social theory, 12(4), 543-569.

Bailey, K. D. (1994). Typologies and taxonomies: An introduction to classification techniques (Vol. 12). Sage.

Barandiaran, X. E., Calleja-López, A., Monterde, A., & Romero, C. (2024). Decidim, a technopolitical network for participatory democracy: philosophy, practice and autonomy of a collective platform in the age of digital intelligence (p. 133). Springer Nature.

Baur, A. (2026). European ambitions captured by American clouds: digital sovereignty through Gaia-X?. Information, Communication & Society, 29(2), 417-434.

Benkler, Y. (2002). Coase's Penguin, or, Linux and the Nature of the Firm. Yale LJ, 112, 369.

Benkler, Y. (2006). The Wealth of Networks: How Social Production Transforms Markets and Freedom. Yale University Press.

Berlinguer, M. (2018). The value of sharing. How commons have become part of informational capitalism and what we can learn from it. The case of FOSS. Rassegna italiana di sociologia, 59(2), 263-288.

Berlinguer, M. (2020a). New commons: Towards a necessary reappraisal. Popular Communication, 18(3), 201-215.

Berlinguer, M. (2020b). Commons, Markets and Public Policy. Transform! Epaper.

Berlinguer, M. (2021). Digital Commons as new Infrastructure: A new generation of public policy for digital transformation. Umanistica Digitale, (11), 5-25.

Berlinguer, M. (2023). Open Source and Economic Models in an Evolutionary Approach. In Business Models and Strategies for Open Source Projects (pp. 18-49). IGI Global Scientific Publishing.

Berlinguer, M. (2024) The Matrix: Is There A European Way To Cloud Computing? April 2024. Transform! ePaper.

Bernier, L., Florio, M., & Bance, P. (Eds.). (2020). The Routledge handbook of state-owned enterprises. Routledge.

Blind, K., & Böhm, M. (2019). The relationship between open source software and standard setting. OpenForum Europe (OFE).

Bonaccorsi, A., Giannangeli, S., & Rossi, C. (2006). Entry strategies under competing standards: Hybrid business models in the open source software industry. Management Science, 52(7), 1085-1098.

Boy, J. D. (2026). What comes after FOSS? Inklings from three communities of practice. Digital Infrastructure Insights Fund.

Chander, A., & Lê, U. P. (2015). Data nationalism. Emory Law Journal, 64(3), 677-739.

Chandler, A. D., Jr. (1993). The visible hand: The managerial revolution in American business. Harvard University Press.

Cheng, J., & Guo, J. L. (2019, May). Activity-based analysis of open source software contributors: Roles and dynamics. In 2019 IEEE/ACM 12th International Workshop on Cooperative and Human Aspects of Software Engineering (CHASE) (pp. 11-18). IEEE.

Cheng, Y. (2026, August 16). Alibaba's Qwen becomes world's most downloaded open AI model. China Daily.

Cheung, S. (2024, May 10). Open-source technology and PRC national strategy: Part I. Jamestown Foundation. https://jamestown.org/open-source-technology-and-prc-national-strategy-part-i/

Chien, A. A. (2018). Open collaboration in an age of distrust. Communications of the ACM, 62(1), 5-5.

China Brief Volume 24 Issue 10 https://jamestown.org/open-source-technology-and-prc-national-strategy-part-i/

Clark, J.; Marin, G.; Ardic Alper, O.P.; Galicia Rabadan, G.A. 2025. Digital Public Infrastructure and Development: A World Bank Group Approach. Digital Transformation White Paper; Volume 1. © World Bank. http://hdl.handle.net/10986/42935

CloudTweaks: Breaking the Cloud Monopoly: Dr. Ignacio M. Llorente on Europes Digital Sovereignty

Coleman, E. G. (2013). Coding freedom: The ethics and aesthetics of hacking. Princeton University Press.

Cory, N. (2024). The US-China Tech Conflict Fractures Global Technical Standards: The Case of Semiconductors and the Risc-V Standard. Information Technology and Innovation Foundation, 19.

D. Kovács, Musial, J., Bojanowski, J., Clarijs, D., de la Mar, J., & Zlinszky, A. (2026). Copernicus Data Space Ecosystem establishes public cloud processing for earth observation data. Scientific Data, 13(1), 537.

De Laat, P. B. (2007). Governance of open source software: state of the art. Journal of Management & Governance, 11(2), 165-177.

Decker, C. (2023). Modern economic regulation: An introduction to theory and practice (2nd ed.). Cambridge University Press.

Del Bo, C. F., Florio, M., Frigerio, M., & Vandone, D. (2025). State-Owned Enterprises in Developed Market Economies: Theory and Empirics. Cambridge University Press.

DeNardis, L. (2014). The global war for internet governance. Yale University Press.

Deuse, K. (2026, March 17). Abhängigkeit von den USA: Deutschlands Digitaldilemma. Deutsche Welle. https://www.dw.com/de/daten-in-gefahr-in-deutschland-digitale-souver%C3%A4nit%C3%A4t-abh%C3%A4ngigkeit-von-den-usa-ZenDiS-microsoft/a-76390557

Dosi, G., & Nelson, R. R. (2010). Technical change and industrial dynamics as evolutionary processes. Handbook of the Economics of Innovation, 1, 51-127.

Duparc, E., Möller, F., Jussen, I., Stachon, M., Algac, S., & Otto, B. (2022). Archetypes of open-source business models: E. Duparc & al. Electronic Markets, 32(2), 727-745

Edler, J., & Fagerberg, J. (2017). Innovation policy: What, why, and how. Oxford Review of Economic Policy, 33(1), 2-23.

Edquist, C. (2011). Design of innovation policy through diagnostic analysis: Identification of systemic problems (or failures). Industrial and Corporate Change, 20(6), 1725-1753.

Eghbal, N. (2016). Roads and bridges: The unseen labor behind our digital infrastructure. Ford Foundation.

Eghbal, N. (2020). Working in Public: The Making and Maintenance of Open Source Software. Stripe Press. — Accessible analysis of sustainability challenges and contributor dynamics.

Eiras, F., Petrov, A., Vidgen, B., Schroeder, C., Pizzati, F., Elkins, K., Mukandavire, S., Birhane, A., Estrela, M., Faria, J., Derczynski, L., & Broniatowski, D. (2024). Risks and opportunities of open-source generative AI. arXiv preprint arXiv:2405.08597.

Ellis, B., & Sustar, L. (2025, December 3). KubeCon North America 2025 retrospective: Closed source and open source battle for the AI-native cloud. Cloud Native Computing Foundation. https://www.cncf.io/news/2025/12/03/forrester-kubecon-na-2025-retrospective-closed-and-open-source-battle-for-the-ai-native-cloud/

European Commission. (2020a). Open source software strategy 2020-2023. Publications Office of the European Union.

European Commission. (2020b). Shaping Europe's digital future. Publications Office of the European Union.

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. International Security, 44(1), 42-79.

FEDERATE (2025). Open-Source Pact Drives Europe’s SDV Ambitions. https://federate-sdv.eu/2025/06/24/open-source-pact-drives-europes-sdv-ambitions/#content

Ferguson, Randy. Publicación de blog. CloudTweaks Newstex. Sep 19, 2024.

Fitzgerald, B. (2006). The transformation of open source software. MIS Quarterly, 30(3), 587-598.

Foster, D. (2024). The new dynamics of open source: Relicensing, forks, & community impact. arXiv preprint arXiv:2411.04739.

Friedman, M. (1970/2007). The social responsibility of business is to increase its profits. In Corporate ethics and corporate governance (pp. 173-178). Berlin, Heidelberg: Springer Berlin Heidelberg.

Frischmann, Brett M., Michael J. Madison, and Katherine J. Strandburg (eds), Governing Knowledge Commons (, 2014; online edn, Oxford Academic, 20 Nov. 2014), https://doi.org/10.1093/acprof:oso/9780199972036.001.0001, accessed 5 Mar. 2026.

Gates, N., Tridgell, J., Torraco, R.M., Schwäbe, C., Reda, F., Hummler, A., Streinz, T. Nummelin Carlberg, A. & Blind,K. (2025). Funding Europe’s Open Digital Infrastructure. OpenForum Europe

Geels, F. W. (2011). The multi-level perspective on sustainability transitions: Responses to seven criticisms. Environmental innovation and societal transitions, 1(1), 24-40.

Geels, F. W., & Schot, J. (2007). Typology of sociotechnical transition pathways. Research policy, 36(3), 399-417.

Gencer, M., & Oba, B. (2017). Taming of 'Openness' in Software Innovation Systems. International Journal of Innovation in the Digital Economy (IJIDE), 8(2), 1-15.

Gurstein, M. (2011). Open data: Empowering the empowered or effective data use for everyone? First Monday, 16(2).

Haese, J., & Peukert, C. (2026). Open at the core: Moving from proprietary technology to building a product on open source software. Management Science, 72(5), 4173-4199.

Hanseth, O., & Lyytinen, K. (2010). Design theory for dynamic complexity in information infrastructures: the case of building internet. Journal of information technology, 25(1), 1-19.

Hardin, G. (1968) 'The Tragedy of the Commons', Science, 162(3859), pp. 1243–1248.

He, S., & Ding, Y. (2021, November 10). Huawei donates operating system to Chinese tech nonprofit. Caixin Global. https://www.caixinglobal.com/2021-11-10/huawei-donates-operating-system-to-chinese-tech-nonprofit-101803174.html

Hess C. and Ostrom E. (eds), (2007) Understanding Knowledge as a Commons: From Theory to Practice (MIT Press).

Jacobides, M. G., Cennamo, C., & Gawer, A. (2018). "Towards a Theory of Ecosystems." Strategic Management Journal, 39(8), 2255–2276.

Jansen, S., Finkelstein, A., & Brinkkemper, S. (2009). A sense of community: A research agenda for software ecosystems. In 31st International Conference on Software Engineering - Companion Volume (pp. 187-190). IEEE.

Kelty, C. M. (2008). Two bits: The cultural significance of free software. Duke University Press.

Kim, M. J., Eom, D., & Lee, H. (2023). The geopolitics of next generation mobile communication standardization: The case of open RAN. Telecommunications Policy, 47(10), 102625.

Krewer, J. (2025). How Geopolitical Tensions Influence Collaboration in Open Technology Ecosystems: Evidence from Risc-V and the Semiconductor Industry. OFA Symposium 2025.

Kuhlmann, S., Stegmaier, P., & Konrad, K. (2019). The tentative governance of emerging science and technology—A conceptual introduction. Research policy, 48(5), 1091-1097.

Lakhani, K. R., & Wolf, R. G. (2003). Why hackers do what they do: Understanding motivation and effort in free/open source software projects. Open Source Software Projects (September 2003).

Laverty, K. J. (1996). Economic "short-termism": The debate, the unresolved issues, and the implications for management practice and research. Academy of management review, 21(3), 825-860.

Lee, L. (2026, August 17). The next China shock will come from open-source AI. Financial Times.

Legenvre, H., Autio, E., & Hameri, A. P. (2025). Creating value by combining AI and other open technologies: Cloud infrastructure as a pivotal asset. In Contemporary Issues in Industry 5.0: Towards an AI Integrated Society (pp. 137-161). Cham: Springer Nature Switzerland.

Li, X., Zhang, Y., Osborne, C., Zhou, M., Jin, Z., & Liu, H. (2025). Systematic literature review of commercial participation in open source software. ACM Transactions on Software Engineering and Methodology, 34(2), 1-31.

Liesenfeld, A., & Dingemanse, M. (2024, June). Rethinking open source generative AI: open-washing and the EU AI Act. In Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency (pp. 1774-1787).

Linux Foundation, (2022) "A Summary of Census II: Open Source Software Application Libraries the World Depends On"

Linux Foundation. (2020). 2020 FOSS Contributor Survey. https://www.linuxfoundation.org/resources/publications/foss-contributor-survey-2020

Lusi, J., Lorenz, B., & Pappel, I. (2025). Innovation or Reinvention? A Systematic and Bibliometric Review of Public Sector Digital Infrastructure. Journal of Open Innovation: Technology, Market, and Complexity, 100593.

Madison, M. J., Frischmann, B. M., & Strandburg, K. J. (2009). Constructing commons in the cultural environment. Cornell L. Rev., 95, 657.

Martí, A. (2022, November 29). The birth of a geopolitical EU cloud industry: Reclaiming open source as a tool for Europe's technological sovereignty. SovereignEdge.EU Blog.

Mazzucato, M., & Kattel, R. (2020). COVID-19 and public-sector capacity. Oxford Review of Economic Policy, 36(Supplement_1), S256-S269.

Mazzucato, M., Kattel, R., & Ryan-Collins, J. (2021). Industrial policy's comeback. Boston Review. https://www.bostonreview.net/forum/industrial-policys-comeback/

Mukherjee, A. & Joshi, A. (2025). Digital Public Infrastructure as a Catalyst for Private Sector Innovation. Observer Research Foundation. https://www.orfonline.org/english/research/digital-public-infrastructure-as-a-catalyst-for-private-sector-innovation

Müller, J. M., Kiel, D., & Voigt, K. I. (2023). Software-defined vehicles: Implications for the automotive industry and its ecosystems. Technological Forecasting and Social Change, 188, 122249.

Murillo, L. F. R. (2020). Replication and cumulative knowledge production in archaeology: A case study of open science practices. Advances in Archaeological Practice, 8(4), 381-390.

Nagle, F. (2018). Learning by contributing: Gaining competitive advantage through contribution to crowdsourced public goods. Organization Science, 29(4), 569-587.

Nguyen-Duc, A., Cruzes, D. S., Terje, S., & Abrahamsson, P. (2018). Do software firms collaborate or compete? A model of coopetition in community-initiated OSS projects. arXiv preprint arXiv:1808.06489.

Nordhaus, W. D. (1975). The political business cycle. The review of economic studies, 42(2), 169-190.

O'Neil, M., Muselli, L., Raissi, M., & Zacchiroli, S. (2021). 'Open source has won and lost the war': Legitimising commercial–communal hybridisation in a FOSS project. New Media & Society, 23(5), 1157-1180.

O'Mahony, S. (2007). The governance of open source initiatives: What does it mean to be community managed? Journal of Management & Governance, 11(2), 139-150.

O'Mahony, S., & Ferraro, F. (2007). The emergence of governance in an open source community. Academy of Management Journal, 50(5), 1079-1106.

Open Source Initiative. (2022). The Open Source Definition. https://opensource.org/osd

OSSF (2022) OSSF Expands Supply Chain Integrity Efforts with S2C2F. https://OSSF.org/blog/2022/11/16/OSSF-expands-supply-chain-integrity-efforts-with-s2c2f/?hsLang=en

OS3I Working Group. (2024). Securing the Open Source Software Ecosystem: End of Year Report Open Source Software Security Initiative OS3I. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/01/Securing-the-Open-Source-Software-Ecosystem-OS3I-End-of-Year-Report-MASTERCOPY.pdf

Osborne, C. (2024). Public-private funding models in open source software development: A case study on scikit-learn. arXiv preprint arXiv:2404.06484.

Osborne, C., Daneshyan, F., He, R., Ye, H., Zhang, Y., & Zhou, M. (2025). Characterising open source co-opetition in company-hosted open source software projects: the cases of PyTorch, TensorFlow, and transformers. Proceedings of the ACM on Human-Computer Interaction, 9(2), 1-30.

Ostrom E., (1990) Governing the Commons: The Evolution of Institutions for Collective Action (Cambridge University Press).

Ostrom E., (2009) 'A Polycentric Approach for Coping with Climate Change' (World Bank Policy Research Working Paper No 5095).

Ostrom E., (2010) 'Beyond Markets and States: Polycentric Governance of Complex Economic Systems' 100 American Economic Review 641.

Ostrom, V., Tiebout, C. M., & Warren, R. (1961). The organization of government in metropolitan areas: a theoretical inquiry. *American political science review*, *55*(4), 831-842.

Pache, A. C., & Santos, F. (2013). Inside the hybrid organization: Selective coupling as a response to competing institutional logics. Academy of management journal, 56(4), 972-1001.

Pannier, A. (2022). Software Power: The Economic and Geopolitical Implications of Open Source Software. Ifri.

Pearce, J. M. (2013). Open-source lab: How to build your own hardware and reduce research costs. Elsevier.

Perforce OpenLogic (2025). 2025 State of Open Source Report. https://www.openlogic.com/blog/state-of-open-source-report-key-insights

Peron, M., Sgambati, A., & Gargiulo, P. (2022). Open RAN: Security considerations and geopolitical implications. Telecommunications Policy, 46(8), 102347.

Pollet, M. (2025). Anatomy of a Franco-German tech misfire. Politico. https://www.politico.eu/article/anatomy-franco-german-tech-misfire-american-dependence/

Porter, M. E. (1990). The competitive advantage of nations. Harvard Business Review/March-April.

Porter, M. E. (1997). Competitive strategy. Measuring business excellence, 1(2), 12-17.

Raymond, E. S. (1999). The cathedral and the bazaar: Musings on Linux and open source by an accidental revolutionary. O'Reilly Media.

Raza, A. (2026, April 8). Russia's government transition to open-source Linux: From Putin's 2010 order to 2026. TechEngage. https://techengage.com/russia-government-transition-open-source-linux/

Red Hat (2020). A guide to open source project governance models. https://www.redhat.com/en/resources/guide-to-open-source-project-governance-models-overview

Riehle, D. (2010). The economic case for open source foundations. Computer, 43(1), 86-90.

Rodeheffer, L. (2026, May 20). Russia's push for digital sovereignty yielding mixed results. Eurasia Daily Monitor. Jamestown Foundation. https://jamestown.org/russias-push-for-digital-sovereignty-yielding-mixed-results/

Sabel, C. F., & Zeitlin, J. (2012). Experimentalist Governance. Oxford Handbooks Online.

Samuelson, P. A. (1954). The pure theory of public expenditure. The review of economics and statistics, 36(4), 387-389.

Sawyer, G., Mamais, E., & Papadakis, D. (2022). The six dimensions of value associated to the use of Copernicus Sentinel data: key findings from the Sentinel benefits study. Frontiers in Environmental Science, 10, 804862.

Schoeberl, C., & Corrigan, J. (2024, November 13). Funding the AI cloud—Amazon, Alphabet, and Microsoft's cloud computing investments, Part 2: OSS as Big Tech's rotisserie chicken. Center for Security and Emerging Technology (CSET). https://cset.georgetown.edu/publication/funding-the-ai-cloud-amazon-alphabet-and-microsofts-cloud-computing-investments-part-2/

Schweik, C. M., & English, R. C. (2012). Internet success: a study of open-source software commons. MIT Press.

Scott, J. C. (1998). Seeing like a state: How certain schemes to improve the human condition have failed (Vol. 464). New Haven, CT: Yale University Press.

Seger, E., Ovadya, A., Garfinkel, B., Siddarth, D., & Dafoe, A. (2023). Democratising AI: Multiple meanings, goals, and methods. In Proceedings of the 2023 AAAI/ACM Conference on AI, Ethics, and Society (pp. 715-722). ACM.

Seo, C. J., & Kossmann, S. (2025). Curating Power: Open Source Infrastructures in the Service of National and Geopolitical Agendas. OFA Symposium 2025. https://pretalx.com/ofa-symposium-2025/speaker/CBWDUM/

Shah, S. K. (2006). Motivation, governance, and the viability of hybrid forms in open source software development. Management science, 52(7), 1000-1014.

Shaikh, M., & Vaast, E. (2016). Folding and unfolding: Balancing openness and transparency in open source communities. Information Systems Research, 27(4), 813-833.

Shams, Reza; Saraf, Nilesh; and Ruckman, Karen, "Co-creating Open Digital Platforms: Analyzing Java Standard Ecosystem" (2025). AMCIS 2025 TREOs. 102. https://aisel.aisnet.org/treos_amcis2025/102

Simcoe, T. (2006). Open standards and intellectual property rights. In H. Chesbrough, W. Vanhaverbeke, & J. West (Eds.), Open Innovation: Researching a New Paradigm (pp. 161-183). Oxford University Press.

Skelcher, C., & Smith, S. R. (2015). Theorizing hybridity: Institutional logics, complex organizations, and actor identities: The case of nonprofits. Public administration, 93(2), 433-448.

Snow, C. C., Strauss, D. R., & Culpan, R. (2009). Community of firms: a new collaborative paradigm for open innovation and an analysis of Blade. org. International Journal of Strategic Business Alliances, 1(1), 53-72.

Sojer, M., & Henkel, J. (2010). Code reuse in open source software development: Quantitative evidence, drivers, and impediments. Journal of the Association for Information Systems, 11(12), 868-901.

Sullivan, J. (2023). Remarks by National Security Advisor Jake Sullivan on renewing American economic leadership at the Brookings Institution. WhiteHouse.gov.

Synopsys. (2022). 2022 Open Source Security and Risk Analysis Report. https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html

Terzi, A., Singh, A., & Sherwood, M. (2022). Industrial policy for the 21st century: Lessons from the past. Publications Office of the European Union.

Tkacz, N. (2015). Wikipedia and the politics of openness. University of Chicago Press.

Trikanad, S., Katira, D., Kulshrestha, A., & Grover, G. (2026, March). Governance, openness and security of digital public infrastructure in India. Internet Research Lab.

Trinkenreich, B., Guizani, M., Wiese, I., Sarma, A., & Steinmacher, I. (2020). Hidden figures: Roles and pathways of successful oss contributors. Proceedings of the ACM on human-computer interaction, 4(CSCW2), 1-22.

Vavilov, A. (2026, June 12). Astra Linux: история компании, которую санкции сделали популярной [Astra Linux: The story of a company made popular by sanctions]. Peoples.ru. https://www.peoples.ru/business/soft/astra_group/

von Hippel, E. (2005). Democratizing innovation. MIT Press.

Wachs, J., Nitecki, M., Schueller, W., & Polleres, A. (2022). The geography of open source software: Evidence from github. Technological Forecasting and Social Change, 176, 121478.

Weber, S. (2004). The success of open source. Harvard University Press.

West, J., & Gallagher, S. (2006). Challenges of open innovation: The paradox of firm investment in open-source software. R&D Management, 36(3), 319-331.

West, J., & O'Mahony, S. (2008). The role of participation architecture in growing sponsored open source communities. Industry and Innovation, 15(2), 145-168.

Williamson, J. (1990) What Washington Means by Policy Reform. In: Williamson, J., Ed., Latin American Adjustment: How Much Has Happened? Institute for International Economics, Washington, 7-20.

World Bank. (2021a). Digital public goods for development. World Bank Group.

World Bank. (2021b). Digital Public Infrastructure: Building Blocks for Inclusive Digital Economies. Washington, DC.

Wright, M., Wood, G., Musacchio, A., Okhmatovskiy, I., Grosman, A., & Doh, J. P. (2021). State capitalism in international context: Varieties and variations. Journal of World Business, 56(2), 101160.

Yu, H., & Robinson, D. G. (2012). The new ambiguity of "open government". UCLA Law Review Discourse, 59, 178-208.

ANNEX 1. FACT-SHEETS OF THE CASES

Astra Linux

Year of Beginning: 2008

Sector: Operating Systems, Open Source Software, Cybersecurity

Political Geography: Russia (developed by Rusbitech, headquartered in Moscow; deployed globally, including China)

Description:

Astra Linux is a Russian Linux-based operating system designed for high-security environments, initially for the Russian military and intelligence agencies. Based on Debian, it features mandatory access control (MAC) for data protection up to Russia's "top secret" classification. Available in two editions—Special Edition (paid, high-security) and Common Edition (free, basic security)—it supports x86-64, ARM, and Elbrus architectures. Widely adopted for Russia's import substitution policy, it replaces Microsoft Windows in government, military, and industries like Gazprom and Rosatom. Astra Linux integrates with Huawei equipment and includes a custom Fly desktop environment.

Short History:

Developed by Rusbitech (NPO RusBITech) in 2008, Astra Linux was formalized after the 2010 Russian government decree (No. 2299-p) mandating free software use in federal institutions. Certified by Russia's Defense Ministry and Federal Security Service (FSB) in 2015, it was deployed in the Russian National Center for Defense Control. In 2018, it replaced Windows in Russian Army systems and was ported to Elbrus microprocessors. By 2019, it powered MIG tablets and was implemented at China's Tianwan Nuclear Power Plant. In 2020, it generated an estimated 2 billion rubles from over 1 million licenses. In 2022, Rusbitech announced plans for a Moscow Exchange listing, driven by Microsoft's exit from Russia and Astra Group has been listed in Moscow on December 2023. As of 2025, it supports 15,000+ users in Rosatom and other sectors.

Mission:

To provide a secure, Debian-based operating system for government, military, and industry, ensuring data protection, import independence, and compliance with Russian and international open-source standards.

Aims and Objectives:

- Deliver robust security with mandatory access control for classified data.
- Support Russia's import substitution by replacing Western software like Windows.
- Provide a stable, Debian-derived OS for diverse hardware (x86-64, ARM, Elbrus).
- Foster an ecosystem of compatible software and hardware via partnerships (e.g., Huawei).
- Enhance usability with the custom Fly desktop environment for enterprise and government users.

Funding:

Funded by Rusbitech through sales of Special Edition licenses, consulting services, and government contracts. Additional funding comes from one institutional investor (A. Partners) and partnerships with firms like Huawei. Government backing aligns with Russia's import substitution policy.

System of Governance (Ownership and Control):

Managed by Rusbitech (NPO RusBITech), a Russian technology company led by CEO Alexei Bocharov. Development is centralized, with contributions from Rusbitech's team and limited community input via GitHub for Common Edition. The Special Edition includes proprietary components (e.g., Fly desktop), limiting full open-source transparency. Governance follows Russian government standards, with certifications from the Defense Ministry and FSB. The Linux Foundation partnership ensured alignment with open-source principles. However Rusbitech was suspended from The Document Foundation's advisory board in 2022 due to Russia's invasion of Ukraine.

Legal Form:

Astra Linux is a software product of Rusbitech, a Russian joint-stock company (JSC). The Common Edition is open-source, while the Special Edition includes proprietary components. The OS is recognized as a Debian derivative, compliant with Russian and international laws, and aligns with the "spirit" of the GPL license.

Licenses Used:

The Common Edition uses the GNU General Public License (GPL) for its Debian-based components, ensuring open-source accessibility. The Special Edition includes proprietary elements (e.g., Fly desktop, security modules) under commercial licenses. The system uses .deb packages, with repositories structured into main, base, and extended for Special Edition.

Broader Contributors:

Primarily Rusbitech, with partnerships from Huawei, The Linux Foundation, and ParaType (for PT Astra fonts). Over 5,000 software and hardware products are certified compatible, including Russian-made Elbrus processors and MIG tablets. Community contributions to the Common Edition occur via GitHub, though less active than other Debian derivatives. Educational institutions and state agencies (e.g., Rosatom, Aeroflot) provide feedback and training support.

Broader Impact:

Astra Linux drives Russia's import substitution, reducing reliance on Western software like Windows. It secures critical infrastructure (e.g., National Center for Defense Control, Rosatom) and supports industries like education, healthcare, and transport (e.g., Russian Railways). Its security features, like mandatory access control and ELF signature checks, protect sensitive data but limit flexibility for non-government users. Critics note outdated packages in repositories and proprietary elements (e.g., Fly Desktop) as drawbacks. Geopolitical concerns, including Rusbitech's 2022 suspension from The Document Foundation, raise trust issues for international adoption. Its use in China's Tianwan Nuclear Power Plant shows global reach, though Western sanctions limit broader expansion.

Qualitative Impact:

Astra Linux strengthens Russia's digital sovereignty, securing sensitive systems and supporting industries under sanctions. Its security certifications and mandatory access control make it a leader in high-stakes environments, but the proprietary Fly desktop and limited package repositories hinder enthusiast and commercial use. Partnerships with Huawei and adoption in China expand its footprint, though geopolitical tensions limit global trust. The custom PT Astra fonts ensure compatibility with Russian standards (e.g., GOST), replacing Western fonts like Verdana. Community feedback highlights its stability but notes challenges with outdated software and restrictive security for non-government use.

Flagship Projects:

- Fly Desktop Environment: Custom, Windows-like interface for government users (proprietary).
- PT Astra Fonts: Metric-compatible replacements for Times New Roman, Arial, and Verdana.
- MAKSIM-M1 Module: Hardware-based trusted boot control for enhanced security.

Official Website:

https://astralinux.ru

Primary Sources:

Astra Linux Official Website

Description: Primary source for OS details, editions, and certifications.

Link: https://astralinux.ru

Wikipedia: Astra Linux

Description: Overview of history, editions, and deployments.

Link: https://en.wikipedia.org/wiki/Astra_Linux

Conecte SUS (now Meu SUS Digital)

Year of Beginning: 2019

Sector: Healthcare, Digital Health, Open Source Software

Political Geography: Brazil (developed by the Ministry of Health, headquartered in Brasília; deployed nationwide)

Description:

Meu SUS Digital, previously known as Conecte SUS, is Brazil's national digital health platform, designed to integrate and digitize health records within the Unified Health System (Sistema Único de Saúde, SUS). Built with open-source components, it enables citizens to access their medical history, vaccination records, medications, lab results, and healthcare services via a mobile app or web portal. The platform connects public and private healthcare providers through the National Health Data Network (RNDS), enhancing interoperability, care coordination, and public health outcomes. Managed by the Ministry of Health's DataSUS department, it aims to create one of the world's largest health data networks.

Short History:

Launched in November 2019 as Conecte SUS, the platform was piloted in Alagoas to digitize health records and improve access to SUS services. It expanded nationwide in 2020, integrating the RNDS. A major cyberattack in December 2021 disrupted vaccination data access, prompting significant security upgrades. Rebranded as Meu SUS Digital in 2023, it issued over 150 million COVID-19 vaccine certificates and supported Brazil's Digital Health Strategy (ESD28, 2020-2028). As of 2025, the platform serves millions, with enhancements for cybersecurity, telehealth, and real-time health analytics, reinforcing its role in public health.

Mission:

To deliver a secure, interoperable, and accessible digital health platform that empowers Brazilians with their health data, enhances healthcare delivery, and supports evidence-based public health policies within the SUS framework.

Aims and Objectives:

- Provide a unified platform for accessing personal health records, including vaccinations, exams, and prescriptions.
- Ensure interoperability among SUS units, private providers, and regional health systems via the RNDS.
- Enhance public health monitoring through real-time data analytics for disease tracking and resource allocation.
- Promote open-source development to ensure transparency and community contributions.
- Strengthen cybersecurity to protect sensitive health data and ensure user trust.

Funding:

Funded by the Brazilian Ministry of Health through federal budgets allocated to DataSUS. Additional support comes from international partnerships, such as the Pan American Health Organization (PAHO) and grants for digital health initiatives.

System of Governance (Ownership and Control):

Managed by the Ministry of Health's DataSUS department, which oversees development, deployment, and maintenance. The platform's open-source components are hosted on GitHub, allowing community contributions through DataSUS control core development. Governance follows Brazilian public sector regulations, with oversight from the Ministry and collaboration with state and municipal health authorities. Cybersecurity is prioritized following the 2021 hack, with audits by the Federal Police and private firms. Community feedback is integrated via public consultations and developer contributions.

Legal Form:

Meu SUS Digital is a public-sector digital platform under the Brazilian Ministry of Health, not a standalone legal entity. Open-source components are freely available, while proprietary integrations (e.g., cybersecurity modules) are managed under government contracts.

Licenses Used:

Open-source components use OSI-approved licenses like GNU General Public License (GPL) or MIT License, ensuring accessibility and modification. Proprietary elements, such as security layers, are licensed under government terms, with details not fully public.

Broader Contributors:

Led by DataSUS, with contributions from state and municipal health departments, private healthcare providers, and tech firms like Zello Health. The open-source community participates via GitHub, focusing on app features and integrations. International partners, including PAHO and WHO, provide technical guidance. Universities and research institutes contribute to data analytics and public health applications. Engagement occurs through developer forums, public consultations, and health tech conferences.

Broader Impact:

Meu SUS Digital transforms Brazil's healthcare by providing millions with digital access to health records, improving care coordination and vaccination tracking. It issued over 150 million COVID-19 vaccine certificates by 2023, supporting travel and public health compliance. The platform's analytics enhance disease surveillance (e.g., dengue, Zika), but challenges include cybersecurity vulnerabilities (post-2021 hack), uneven rural adoption due to connectivity issues, and delays in state-level data integration. Its open-source model fosters transparency, though proprietary components limit full community governance. Meu SUS Digital positions Brazil as a digital health leader in Latin America.

Qualitative Impact:

Meu SUS Digital empowers citizens with real-time access to health data, reducing administrative burdens and improving care continuity. Its role in COVID-19 vaccination campaigns and disease surveillance strengthens public health responses. Enhanced cybersecurity post-2021 rebuilds trust, though user complaints about missing records highlight integration challenges. Rural access remains limited by connectivity and digital literacy gaps. The platform's open-source components drive innovation, but government control over proprietary elements restricts full community involvement. It sets a model for digital health in developing nations.

Flagship Projects:

- National Health Data Network (RNDS): Backbone for interoperable health data across SUS units.
- Digital Vaccine Certificate: Enables verification of COVID-19 and other vaccinations.
- Conecte SUS Cidadão App: Mobile access to health records, appointments, and prescriptions.
- Health Analytics Dashboard: Real-time data for public health monitoring and policy-making.

Official Website:

https://meususdigital.saude.gov.br/

Primary Sources:

Ministry of Health: Meu SUS Digital Official Page

Description: Primary source for platform details, app downloads, and user guides.

Link: https://www.gov.br/pt-br/servicos/acessar-a-plataforma-movel-de-servicos-digitais-do-ministerio-da-saude

GitHub: Conecte SUS Repository

Description: Open-source components and developer contributions.

Link: https://github.com/datasus

Copernicus Program

Year of Beginning: 1998 (initiated as GMES); 2014 (first Sentinel launch)

Sector: Earth Observation, Environmental Monitoring, Open Data, Space Technology

Political Geography: Global (coordinated from Brussels, Belgium; serves 27 EU member states, UK, and international partners)

Description:

Copernicus is the European Union's flagship Earth observation program, providing free, open, and near-real-time data and services to monitor the planet's land, oceans, atmosphere, and climate. Managed by the European Commission (EC) and implemented with the European Space Agency (ESA), EUMETSAT, ECMWF, EEA, JRC, EMSA, Frontex, SatCen, and Mercator Océan, it comprises a space component (Sentinel satellites and Contributing Missions), in-situ measurements (ground, air, sea sensors), and six core services: atmosphere, marine, land, climate change, emergency, and security. The Copernicus Data Space Ecosystem (CDSE) offers tools like the Copernicus Browser and APIs for data access and analytics, supporting applications in agriculture, urban planning, and disaster response.

Short History:

Initiated in 1998 as Global Monitoring for Environment and Security (GMES) in Baveno, Italy, Copernicus was renamed in 2012 and launched its first satellite, Sentinel-1A, in 2014. In 2024, the UK rejoined as a full participant, and Sentinel-6B's planned 2025 launch was announced. The 2025 Copernicus Interactive Climate Atlas (C3S Atlas) v2 added new indices. With 772 European companies generating €1.796 billion (2023), the program targets a €6 billion market by 2033. Future missions (e.g., Sentinel-7/CO2M) are planned for 2026.

Mission:

To provide accurate, timely, and freely accessible Earth observation data and services to improve environmental management, mitigate climate change, enhance civil security, and support sustainable development for European citizens and global users.

Aims and Objectives:

- Deliver near-real-time data via Sentinel satellites and in-situ networks for six thematic services.
- Ensure open, free access to data for public, private, and scientific users.
- Support EU policies in climate adaptation, urban planning, and disaster response.
- Foster innovation through APIs, cloud processing, and tools like the Copernicus Browser.
- Expand the space component with new Sentinel missions by 2030 for enhanced monitoring.

Funding:

Copernicus is funded primarily by the EU budget, with €5.42 billion allocated under Regulation (EU) 2021/696 for 2021–2027 (approximately €775 million per year on average). ESA and EUMETSAT implement the space component and operations under delegation and contribution agreements

with the Commission. Additional resources come from Horizon Europe, national contributions and associated third countries.

System of Governance (Ownership and Control):

Coordinated by the EC, with ESA leading the space component (Sentinel development and operations) and EEA managing in-situ coordination. Governance involves EU member states, EUMETSAT, ECMWF, and other agencies via contribution agreements. Data access is open, with CDSE managed by T-Systems and Sinergise Solutions. Community input is limited to user feedback via portals like dataspace.copernicus.eu. Policies align with EU open data principles, though operational control remains with EC and ESA.

Legal Form:

Copernicus is a program under the EU Space Program, not a standalone legal entity, governed by EU regulations and international agreements (e.g., with USGS). Data and services use open licenses with no proprietary control.

Licenses Used:

Data products (e.g., Sentinel imagery, service outputs) are released under Creative Commons CC-BY 4.0 or public domain licenses, ensuring free reuse. Software tools (e.g., Copernicus Browser APIs, openEO) use Apache 2.0 or MIT licenses.

Broader Contributors:

Includes 27 EU member states, the UK, and partners like USGS, NOAA, and NASA via data-sharing agreements. Over 772 European companies (96% SMEs) contribute to data processing, employing more than 13,000 people. Third-party missions (e.g., Pléiades, WorldView) and in-situ networks (e.g., SEIS) enhance data. Community engagement occurs via hackathons (e.g., Copernicus Masters) and portals like WEkEO.

Broader Impact:

Copernicus provides the world's largest space data repository, supporting climate adaptation (e.g., C3S Atlas), disaster response (e.g., EFFIS), and sustainable shipping (e.g., Pacific Green Corridor). Its open data model drives a €3.4 billion Earth Observation (EO) market (2023), with 22% from climate services. Challenges include data volume management and ensuring equitable access globally. Critics note reliance on EU funding and potential gaps in non-EU regions.

Qualitative Impact:

Copernicus revolutionizes environmental monitoring, enabling precision farming, urban heat island management, and iceberg tracking (e.g., Greenland, 2024). Its free data model fosters innovation, as seen in Littosat for coastal management and LisOcean for water quality forecasts. However, exponential data growth strains infrastructure, and EU-centric governance limits global inclusivity. Alignment with GEOSS and FAIR principles ensures long-term impact, though funding sustainability is a concern.

Flagship Projects:

- Copernicus Data Space Ecosystem (CDSE): Portal for Sentinel data access with Copernicus Browser and APIs.
- Sentinel Missions: Sentinel-1 (SAR), Sentinel-2 (multispectral), Sentinel-3 (marine), Sentinel-5P (atmosphere).
- C3S Interactive Climate Atlas: Dataset and viewer for climate indices (v2, 2025).
- Urban Atlas: High-resolution land use mapping for 800+ European cities.

Official Website:

https://www.copernicus.eu

Primary Sources:

Copernicus Official Website

Description: Primary source for program overview, services, and data access.

Link: https://www.copernicus.eu

ESA: Copernicus Overview

Description: Details ESA's role, Sentinel missions, and space component.

Link: https://www.esa.int/Applications/Observing_the_Earth/Copernicus

Copernicus Data Space Ecosystem

Description: Outlines CDSE portal, data model, and processing tools.

Link: https://dataspace.copernicus.eu

EUSPA: Copernicus Program

Description: Covers funding, market impact, and commercialization.

Link: https://www.euspa.europa.eu/eu-space-programme/copernicus

Sentinel Online

Description: Technical details on Sentinel missions and data products.

Link: https://sentinels.copernicus.eu

Decidim

Year of Beginning: 2016 (launched as *decidim.barcelona*); 2017 (rewritten as standalone project)

Sector: Digital Democracy, Open Source Software, Citizen Participation

Political Geography: Global (developed in Barcelona, Spain; used in 30+ countries)

Description:

Decidim is a free, open-source digital platform for participatory democracy, enabling organizations to create customizable web portals for citizen engagement. It supports participatory spaces (e.g., initiatives, assemblies, processes, consultations) and components (e.g., proposals, voting, surveys, meetings) to facilitate strategic planning, participatory budgeting, and collaborative governance. Coordinated by the Decidim Association, it emphasizes transparency, traceability, and privacy, integrating hybrid (digital and face-to-face) participation. Used by over 400 administrations and 50 NGOs across 30 countries, Decidim fosters democratic innovation as a public-commons infrastructure.

Short History:

Decidim was launched on January 31, 2016, as *decidim.barcelona*, a fork of Madrid's Consul software, to support Barcelona's 2016-2019 Municipal Action Plan. In 2017, the code was rewritten for modularity, becoming a standalone project. The Decidim Association, formed in 2019, took control of the trademark and codebase, ensuring community governance. By 2023, Decidim powered platforms like New York City's participate.nyc.gov and France's petitions.assemblee-nationale.fr. Version 0.27 (2023) introduced ephemeral verification, and in 2024, the MultiPoD project advanced EU-wide participation. In December 2024, the Brazilian government formalized a partnership with the Decidim Association through a Memorandum of Understanding—the first such agreement with a government outside Catalonia (4). Brazil's "Brasil Participativo" platform, launched in 2023 on Decidim, now hosts over 1.5 million participants. Brazil also joined the Committee of Public Institutions (founded in 2025 with Barcelona, New York, and Catalan institutions), allowing public bodies to participate directly in governing the digital commons. The platform is translated into 50+ languages and hosts around 3 million registered participants globally.

Mission:

To provide a free, open-source platform that empowers organizations and citizens to organize democratically, fostering transparent, inclusive, and collaborative decision-making for participatory governance.

Aims and Objectives:

- Enable customizable participatory processes (e.g., budgeting, urban planning, consultations) and democratic governance of a public institution or social organization.
- Promote transparency and traceability in digital participation, except for privacy-sensitive data.
- Support hybrid participation combining digital tools with face-to-face engagement.

- Foster a global community (Metadecidim) to collaboratively design and improve the platform.
- Counter digital reductionism by enhancing collective, multimodal participation.

Funding:

Primarily funded through public budgets (e.g., Barcelona City Council 500,000 euros per year[15]), donations via OpenCollective, and grants from organizations like the European Union (e.g., MultiPoD project). Additional support comes from municipalities and NGOs adopting Decidim. Each organization funds the deployment of its own instance. Companies offering services based on the platforms are required to contribute a portion of their profits to the association to help fund its operations.

System of Governance (Ownership and Control):

Managed by the Decidim Association, a democratic non-profit under Spanish law, with a General Assembly of community members. The Metadecidim community governs development via participatory processes on meta.decidim.org, using GitHub for transparent code contributions. The platform adheres to a Social Contract with six guidelines (e.g., public-commons, democratic innovation). Barcelona City Council funds core development but cedes control to the Association. Contributions follow the AGPL-3.0 license and OpenStand principles.

Legal Form:

The Decidim Association is a non-profit registered in Spain. The Decidim software is an open-source project under the AGPL-3.0 license, with documentation under Creative Commons Attribution-ShareAlike 4.0 International (CC-BY-SA-4.0) and GNU Free Documentation License (GFDL-1.3-or-later).

Licenses Used:

Software is licensed under the GNU Affero General Public License (AGPL-3.0), ensuring free use, modification, and distribution. Documentation uses CC-BY-SA-4.0 and GFDL-1.3-or-later. The Decidim logo and trademark are protected by the Association, requiring attribution for non-commercial use.

Broader Contributors:

Includes over 400 administrations (e.g., Barcelona, Helsinki, Mexico City), 50 NGOs, and multilateral organizations like the European Union (futureu.europa.eu). The Metadecidim community, with thousands of participants, contributes via GitHub, Crowdin translations, and events like Decidim Fest. Developers, activists, and researchers collaborate, with adopters like New York City and Brazil's national government enhancing global reach.

Broader Impact:

Decidim democratizes governance by enabling inclusive, transparent participation, as seen in Barcelona's 120,000 active participants and 35,000 proposals. It reduces reliance on proprietary

[15] https://meta.decidim.org/en/assemblies/general-assembly-association

platforms, fostering digital sovereignty and collective decision-making. Its modular design suits diverse contexts, but challenges include digital divides and sustaining engagement. Globally, it inspires participatory models, though scaling requires addressing technical and cultural barriers.

Qualitative Impact:

Decidim enhances participatory democracy by combining digital tools with face-to-face engagement, avoiding "click-participation" and fostering collective action. Its open-source model ensures accessibility. The Social Contract promotes technopolitical commons, countering corporate platforms. However, effectiveness varies (e.g., Switzerland's uneven adoption), and sustaining community contributions remains a challenge. Decidim's global spread signals a shift toward inclusive governance.

Flagship Projects:

- *Decidim.Barcelona*: Core platform for Barcelona's participatory processes, with 120,000 participants.
- DPG Registry: Recognized as a Digital Public Good, enhancing global discoverability.
- Proposals Component: Enables collaborative proposal creation with voting and geolocation.
- Ephemeral Verification: Simplifies one-time participation (e.g., voting) without full registration.

Official Website:

https://decidim.org

Primary Sources with Links:

Decidim Official Website

Description: Primary source for Decidim's mission, features, and community details.

Link: https://decidim.org

Metadecidim Community Platform

Description: Hub for community discussions, governance, and Decidim Fest updates.

Link: https://meta.decidim.org

Digital Public Goods Alliance: Decidim Profile

Description: Outlines Decidim's global adoption and DPG status.

Link: https://digitalpublicgoods.net/registry/decidim

GitHub: Decidim Repository

Description: Hosts source code, development roadmap, and contributor details.

Link: https://github.com/decidim/decidim

Decidim Overview (Barandiaran et al., 2024)

Barandiaran, X. E., Calleja-López, A., Monterde, A., & Romero, C. (2024). *Decidim, a technopolitical network for participatory democracy: philosophy, practice and autonomy of a collective platform in the age of digital intelligence*. Springer Nature.

Digital Public Goods Alliance (DPGA) and DPG Standards

Year of Beginning: 2019 (DPGA founded); 2020 (DPG Standard formalized)

Sector: Digital Infrastructure, Open Source Software, Sustainable Development

Political Geography: Global. Headquartered in New York, USA, with operations coordinated by UNICEF and Norad, the Norwegian Agency for Development Cooperation.

Description:

The Digital Public Goods Alliance (DPGA) is a UN-endorsed, multi-stakeholder initiative that accelerates the attainment of the UN's 2030 Sustainable Development Goals (SDGs) by facilitating the discovery, development, use, and investment in digital public goods (DPGs). DPGs are open-source software, open data, open AI models, open standards, and open content that adhere to the DPG Standard, a nine-indicator framework[16] ensuring privacy, no harm, and SDG relevance. The DPGA maintains a DPG Registry, supports a practitioner community, and advocates for digital public infrastructure (DPI) through partnerships with governments, UN agencies, and private sectors. The DPG Standard guides nominations and ensures solutions are interoperable, equitable, and sustainable.

Short History:

In mid-2019, the UN Secretary-General's High-level Panel on Digital Cooperation recommended a platform for sharing DPGs, leading to the DPGA's formation in late 2019 by Norway, Sierra Leone, UNICEF, and iSPIRT[17]. The DPG Standard v1.0 was published in September 2020, evolving from a 51-indicator framework for early-grade reading projects. By 2022, the DPG Charter formalized collaboration, and in 2023, the State of the DPG Ecosystem Report highlighted 40+ government adopters. Version 1.1.6 of the Standard, released on September 4, 2024, refined indicators. By 2025, the DPGA included members like Singapore and Malawi, with DPGs like TYPO3[18] and FormSG[19] recognized for global impact.

Mission:

To accelerate the attainment of the SDGs in low- and middle-income countries by facilitating the discovery, development, use, and investment in digital public goods that adhere to the DPG Standard, fostering equitable, open, and sustainable digital ecosystems.

Aims and Objectives:

- Ensure discoverability and accessibility of DPGs for governments and organizations addressing SDG challenges.
- Enhance capacity and incentives for UN institutions and governments to adopt DPGs.

---

[16] The DPG Standard's nine indicators cover SDG relevance, open licensing, privacy, and more, detailed in the GitHub repository.

[17] iSPIRT - the Indian Software Product Industry Round Table – is a non-profit think-tank based in India and a co-founder of the DPGA.

[18] TYPO3 is an open-source enterprise content management system (CMS) recognized as a DPG by the DPGA in April 2025.

[19] FormSG is an open-source form-building platform developed by Singapore's Open Government Products (OGP) team. It enables secure, user-friendly data collection for government and public sector use.

- Empower governments to plan, deploy, and maintain DPG-based digital public infrastructure.
- Foster vibrant commercial ecosystems for DPG creation and maintenance at local levels.
- Maintain and refine the DPG Standard as an open, community-driven framework for quality assurance.

Funding:

Funded through contributions from member governments (e.g., Norway, Sierra Leone, Singapore, Germany), UN agencies (e.g., UNICEF, UNDP), and donors like the Norwegian Agency for Development Cooperation (Norad). Additional support comes from private-sector partners and grants.

System of Governance (Ownership and Control):

The DPGA is governed by a board including representatives from the German Federal Ministry for Economic Cooperation and Development, EkStep Foundation, Government of Sierra Leone, Norad, UNDP, and UNICEF. The secretariat, hosted by UNICEF and Norad, coordinates activities, while a technical review team assesses DPG nominations against the Standard. The DPG Standard is an open project on GitHub, following OpenStand's five principles (cooperation, adherence to principles, collective empowerment, availability, voluntary adoption). Governance is transparent, with community input via public repositories and a Code of Conduct.

Legal Form:

The DPGA is a multi-stakeholder initiative without a standalone legal entity, operating under UNICEF's non-profit status in the U.S. and Norad's governmental framework in Norway. The DPG Standard is licensed under Creative Commons Attribution ShareAlike 4.0 International.

Licenses Used:

DPGs must use approved open licenses (e.g., Apache 2.0, MIT, GPL for software; CC BY 4.0 for content; ODC-By for data). The DPG Standard itself is licensed under Creative Commons Attribution ShareAlike 4.0 International. Application data is released under the Unlicense, ensuring public domain access, though personal contact details remain private.

Broader Contributors:

Includes 49 member organizations (e.g., Governments of Norway, Sierra Leone, Singapore, Malawi; UNICEF, UNDP, Creative Commons, GitHub). Over 100 experts from 67 organizations across 30+ countries participate in consultations. Thousands of developers contribute to DPGs via GitHub, with pathfinder countries (e.g., Rwanda, Bangladesh) testing implementations. The DPG Registry lists 150+ DPGs, and communities engage through events like WSIS[20] and the Internet Governance Forum[21].

---

[20] The World Summit on the Information Society (WSIS) is a United Nations-sponsored initiative aimed at bridging the global digital divide and promoting the development of an inclusive information society.

[21] The Internet Governance Forum (IGF) is a global multi-stakeholder platform established by the United Nations to facilitate dialogue on internet governance issues.

Broader Impact:

The DPGA and DPG Standard enable countries to adopt scalable, interoperable technologies, reducing vendor lock-in and fostering digital sovereignty. DPGs like MOSIP[22] and DHIS2[23] support identity systems and health management, impacting millions in low- and middle-income countries. The Standard ensures privacy and SDG alignment, though challenges include the free-rider problem and varying national capacities. The DPGA's advocacy strengthens global DPI, with initiatives like India's DIGIT[24] enhancing local governance.

Qualitative Impact:

The DPGA empowers governments and organizations to leverage open-source solutions for equitable development, as seen in FormSG's global rollout and DIGIT's community reporting. The DPG Standard ensures trust through rigorous privacy and "do no harm" requirements, but scaling adoption requires addressing maintenance incentives and capacity gaps. Its UN endorsement enhances credibility, positioning the DPGA as a leader in digital equity, though coordination across diverse stakeholders remains complex.

Flagship Projects:

- DPG Registry: Public database of 150+ vetted DPGs, accessible via API.
- DPG Standard: Nine-indicator framework for assessing open-source solutions.
- MOSIP: Modular Open Source Identity Platform for digital identity systems.
- FormSG: Zero-code form builder for safe data collection, used in Sri Lanka and Cambodia.

Official Website:

https://digitalpublicgoods.net

Primary Sources:

Digital Public Goods Alliance Official Website

Description: Primary source for DPGA's mission, DPG Standard, and Registry details.

Link: https://digitalpublicgoods.net

---

[22] MOSIP (Modular Open Source Identity Platform) is an open-source digital identity platform recognized as a Digital Public Good (DPG) by the Digital Public Goods Alliance (DPGA). It is designed to provide countries, particularly low- and middle-income nations, with a modular, customizable, and secure framework for building national digital identity systems.

[23] DHIS2 (District Health Information Software 2) is an open-source, web-based platform primarily used as a Health Management Information System (HMIS), recognized as a Digital Public Good (DPG) by the Digital Public Goods Alliance (DPGA). It is designed for the collection, validation, analysis, visualization, and sharing of aggregate and individual-level data, with a focus on health but also applications in sectors like education, logistics, and e-governance. DHIS2 is the world's largest HMIS, used by over 80 countries, covering approximately 3.2 billion people, or over 40% of the global population.

[24] DIGIT (Digital Infrastructure for Government Innovation and Transformation) is an open-source platform developed by the eGov Foundation in India, recognized as a Digital Public Good (DPG) by the Digital Public Goods Alliance (DPGA). It provides foundational building blocks and pre-built solutions to enable governments, markets, and non-profits to deliver efficient, transparent, and inclusive public services across multiple sectors, such as e-justice, climate and energy, agriculture, industries, and education. DIGIT is a key component of India's Digital Public Infrastructure (DPI), complementing initiatives like the India Stack (Aadhaar, UPI, DigiLocker).

DPGA GitHub: DPG Standard

Description: Hosts the DPG Standard, changelog, and nomination process.

Link: https://github.com/DPGAlliance/dpg-standard

DPGA: Submission Guide

Description: Details requirements for DPG nominations and Standard indicators.

Link: https://digitalpublicgoods.net/submission-guide/

UN: Digital Public Goods

Description: Contextualizes DPGA's role in the UN's digital cooperation roadmap.

Link: https://www.un.org/digital-emerging-technologies/content/digital-public-goods

DPGA: State of the DPG Ecosystem 2023 Report

Description: Highlights DPG adoption and ecosystem growth.

Link: https://www.digitalpublicgoods.net/DPG-Ecosystem-2023.pdf

Creative Commons: DPGA Membership

Description: Details CC's role and DPG licensing contributions.

Link: https://creativecommons.org/2024/03/04/cc-joins-dpga/

ELIXIR (European Life-Sciences Infrastructure for Biological Information)

Year of Beginning: 2007 (preparatory phase); 2013 (formal establishment)

Sector: Bioinformatics, Life Sciences, Open Data, Research Infrastructure

Political Geography: Europe. Headquartered at Wellcome Genome Campus, Hinxton, Cambridge, UK. 23 member states participating plus the EMBL-EBI (the European Molecular Biology Laboratory's European Bioinformatics Institute)

Description:

ELIXIR is an intergovernmental research infrastructure that coordinates and sustains bioinformatics resources across Europe, enabling researchers to access, analyze, and share life science data. It operates a Hub-and-Nodes model, with the ELIXIR Hub in Hinxton and 23 national Nodes, plus EMBL-EBI, managing over 240 institutes. ELIXIR's five Platforms (Data, Tools, Compute, Interoperability, Training) support data stewardship, software development, cloud computing, FAIR principles, and training. It addresses grand challenges in health, agriculture, and environmental sciences, with initiatives like the Genomic Data Infrastructure (GDI) and BioHackathon Europe fostering innovation.

Short History:

Launched in 2007 under the EU's FP7 program as part of the ESFRI roadmap, ELIXIR completed its preparatory phase by 2012. It became a permanent legal entity in 2013 with the ratification of the ELIXIR Consortium Agreement (ECA) by five countries and EMBL. By 2015, the €19 million EXCELERATE project enhanced Node integration, followed by CONVERGE (2020), both funded by the European Commission through the Horizon 2020 Research Infrastructures program. In 2024, ELIXIR celebrated its 10-year jubilee, launching the 2024–2028 Scientific Program, emphasizing AI and human data interoperability. Recent projects include GDI (€40 million, 2022–2026) and EUCAIM for cancer imaging.

Mission:

To build a sustainable European infrastructure for biological information, supporting life science research and its translation to medicine, agriculture, bio-industries, and society by coordinating and integrating bioinformatics resources.

Aims and Objectives:

- Provide open access to high-quality, sustainable data resources and tools for life sciences.
- Enhance data interoperability and FAIRification (Findable, Accessible, Interoperable, Reusable) across Nodes.
- Develop secure compute infrastructure for sensitive data (e.g., human genomics via AAI).
- Deliver training to empower researchers and bioinformaticians.

- Foster collaboration with industry and other ESFRI infrastructures[25] to address societal challenges.

Funding:

Funded by membership fees from 23 member states (proportional to Net National Income), European Commission grants, and other sources like BBSRC, MRC, and NERC[26]. Infrastructure Services like AAI and TeSS[27] received €350,000 (2024–2026).

System of Governance (Ownership and Control):

Governed as an intergovernmental organization under the ELIXIR Consortium Agreement (ECA), with the ELIXIR Board (member state representatives) as the highest authority. The ELIXIR Hub, coordinates Nodes and Platforms, through the Heads of Nodes Committee. Nodes are national networks of institutes, with EMBL-EBI as a unique Node. Governance includes the Scientific Advisory Board (SAB) and the Industry Advisory Board (IAB) and more informal technical committees, ensuring transparency and consensus. Data and tools are open, with contributions via GitHub under open licenses.

Legal Form:

ELIXIR is an intergovernmental organization established in 2013 under international law. It operates under the ECA, signed by 23 members. Data resources and tools use open licenses (e.g., CC0, Apache 2.0).

Licenses Used:

Data resources typically use Creative Commons CC0 or CC-BY 4.0 for open access. Software tools (e.g., BioContainers, AAI) use Apache 2.0 or MIT licenses. Bioschemas and other standards align with Open Definition licenses.

Broader Contributors:

Over 240 institutes across 23 Nodes, plus EMBL-EBI. Collaborators include ESFRI infrastructures (e.g., Euro-BioImaging, Instruct-ERIC), industry (via Innovation and SME Program), and global initiatives (e.g., GA4GH). Thousands of researchers contribute data and tools, with events like BioHackathon Europe (180+ participants in 2024) fostering community engagement.

Broader Impact:

ELIXIR enables researchers to tackle grand challenges in health (e.g., GDI for genomics), agriculture (e.g., AgroServ), and environment (e.g., Marine Metagenomics). Its federated infrastructure

[25] ESFRI (European Strategy Forum on Research Infrastructures) infrastructures are large-scale research facilities, resources, or services of pan-European importance, designed to support scientific research and innovation. Established by the European Commission in 2002, ESFRI identifies and supports the development of these infrastructures to address scientific needs across various disciplines.

[26] BBSRC (Biotechnology and Biological Sciences Research Council), MRC (Medical Research Council), and NERC (Natural Environment Research Council) refer to UK research councils that contribute to ELIXIR's UK membership and support its activities, particularly through the ELIXIR-UK Node.

[27] These are two ELIXIR's critical services: Authentication and Authorisation Infrastructure (AAI) and the Training e-Support System (TeSS).

enhances data accessibility, as seen in the COVID-19 Data Platform and EUCAIM. Open resources drive innovation, with millions of hits from academia and industry. Challenges include managing data growth and ensuring equitable access across Nodes. ELIXIR's AI and FAIRification efforts position it for future impact.

Qualitative Impact:

ELIXIR's federated model reduces data fragmentation, as seen in the Genomic Data Infrastructure's support for 1M+ genomes. Its training network empowers researchers, while FAIR standards (e.g., Bioschemas) enhance data reuse. Industry engagement (100+ SMEs) drives economic impact, but challenges include sustaining services and addressing AI biases. ELIXIR's role in pandemics (BY-COVID) and biodiversity (PHENET) underscores its societal value.

Flagship Projects:

- Genomic Data Infrastructure (GDI): Enables access to genomic and clinical data across Europe.
- ELIXIR AAI: Authentication and Authorization Infrastructure for secure data access.
- BioContainers: Registry of 7.9K containerized tools for reproducible research.
- TeSS (Training e-Support System): Portal for bioinformatics training resources.

Official Website:

https://elixir-europe.org

Primary Sources :

ELIXIR Official Website

Description: Primary source for mission, services, governance, and projects.

Link: https://elixir-europe.org

ELIXIR: Providing a Sustainable Infrastructure for Life Science Data (Bioinformatics, 2021)

Description: Details ELIXIR's structure, AAI, and community impact.

Link: https://academic.oup.com/bioinformatics/article/37/16/2506/6306416

ELIXIR Data Platform (2024–2026)

Description: Outlines Core Data Resources, FAIRification, and data brokering.

Link: https://elixir-europe.org/platforms/data

ELIXIR 10-Year Jubilee (E2 News, 2024)

Description: Covers leadership transition, GDI, and 2024–2028 program.

Link: https://e2-news.ch/en/news/elixir-10-year-jubilee

BioHackathon Europe 2025

Description: Details community engagement and collaborative innovation.

Link: https://biohackathon-europe.org

European Open Science Cloud (EOSC)

Year of Beginning: 2015 (conceptualized); 2018 (formal launch)

Sector: Scientific Research, Digital Infrastructure, Open Science

Political Geography: Europe (headquartered in Brussels, Belgium, with global outreach)

Description:

The European Open Science Cloud (EOSC) is a European Commission initiative to create a federated, open, and multi-disciplinary digital environment for researchers, innovators, and citizen scientists. It provides seamless access to FAIR (Findable, Accessible, Interoperable, Reusable) research data, tools, and services, fostering collaboration and data-driven science. Managed through a tripartite governance model involving the European Commission, Member States/Associated Countries, and the EOSC Association, EOSC integrates existing infrastructures into a "Web of FAIR Data and Services," supporting open science, reproducibility, and innovation across disciplines.

Short History:

Proposed in 2015 by the European Commission, EOSC aimed to federate research data infrastructures for open science. It officially launched in November 2018 with the EOSC Portal, supported by €320 million from Horizon 2020 (2018-2020). The EOSC Association was formed in July 2020, and a co-programmed European Partnership began in 2021 under Horizon Europe, guided by a Strategic Research and Innovation Agenda (SRIA). The EOSC EU Node, a key gateway, was launched in October 2024 at the Berlin Symposium. By 2024, EOSC had 150+ members, with €1 billion in co-investments planned through 2027.

Mission:

To develop a trusted, federated digital environment for European researchers to find, share, and reuse FAIR research data, tools, and services, enabling open science, interdisciplinary collaboration, and global leadership in data-driven research.

Aims and Objectives:

- Facilitate open sharing and reuse of research data adhering to FAIR principles.
- Federate existing research infrastructures to enhance interoperability and scale.
- Provide secure, user-friendly access to data, computing, and analytical tools.
- Promote open science practices, skills, and rewards across Europe.
- Support cross-disciplinary research to address global challenges (e.g., climate, health).

Funding:

Initial phase (2018-2020): €320 million via Horizon 2020[28]. Current phase (2021-2030): €1 billion co-investment from EU (Horizon Europe) and non-EU partners, including in-kind and financial contributions[29]. Horizon Europe funds INFRAEOSC projects and the EOSC EU Node.

[28] https://sciencebusiness.net/news/european-research-area/eu-science-cloud-project-get-eu950m-investment

System of Governance (Ownership and Control):

EOSC operates under a tripartite governance model: the European Commission (policy and funding), the EOSC Steering Board (27 EU countries plus Associated Countries, ~100 experts), and the EOSC Association (150+ members representing research communities). The Association, a non-profit under Belgian law, drives stakeholder engagement. The EOSC EU Node is EC-owned until 2027, with future ownership under discussion. Governance emphasizes transparency, inclusivity, and stakeholder-driven decisions via the Strategic Research and Innovation Agenda (SRIA)[30].

Legal Form:

No single legal entity; EOSC is a federated initiative under the European Commission, with the EOSC Association as an international non-profit (AISBL) under Belgian law since July 2020. EOSC's federated model relies on existing infrastructures, not a single cloud. The EOSC EU Node is managed by EC contracts.

Licenses Used:

EOSC data model follows FAIR principles (detailed in SRIA). EOSC promotes open-source and FAIR-compliant licenses, such as Apache 2.0, MIT, or Creative Commons (e.g., CC BY 4.0) for data, software, and services. Specific licenses vary by provider but align with open access and reusability principles.

Broader Contributors:

Over 150 EOSC Association members (universities, research institutes, e-infrastructures) and 50 observers, plus 27 EU countries and Associated Countries. Contributors include projects like EOSC-hub, OpenAIRE, and EUDAT, with thousands of researchers, providers (e.g., EGI, Athena RC), and citizen scientists. Global partners engage via open science initiatives.

Broader Impact:

EOSC removes barriers to data sharing, enhancing transparency, reproducibility, and interdisciplinary collaboration. It supports 1.7 million European researchers, reduces research duplication, and accelerates innovation in fields like climate and health. The EOSC EU Node provides access to diverse datasets and tools, aligning with the European Data Strategy. Globally, it positions Europe as a leader in open science, though challenges include adoption complexity and varying national capacities.

Qualitative Impact:

EOSC fosters a culture of open science, enabling researchers to validate findings and build on existing work, as seen in the COVID-19 Data Platform's rapid response. It reduces costs through shared infrastructure, supports SMEs via value-added services, and enhances trust via FAIR principles. However, complexity and uneven adoption across countries pose challenges. Its global influence grows through partnerships, but full impact awaits broader node federation.

---

[29] https://eosc.eu/wp-content/uploads/2024/01/20231212_FMR.pdf

[30] The Strategic Research and Innovation Agenda (SRIA) of the European Open Science Cloud (EOSC) is a comprehensive roadmap designed to guide the development and implementation of EOSC over a seven-year period (2021–2027).

Flagship Projects:

- EOSC EU Node: European gateway for FAIR data, tools, and services, launched in 2023.
- OpenAIRE: Aggregates scholarly resources, feeding the EOSC hub.
- EOSC-hub: Integrates services for interdisciplinary research (2018-2020).
- EOSC-Synergy: Adapts thematic services (e.g., biomedicine, astrophysics) for EOSC.

Official Website:

https://open-science-cloud.ec.europa.eu

Primary Sources :

European Commission: European Open Science Cloud (EOSC)

Description: Official source for EOSC's mission, governance, funding, and history.

Link: https://research-and-innovation.ec.europa.eu/strategy/strategy-2020-2024/our-digital-future/open-science/european-open-science-cloud-eosc_en

EOSC EU Node Website

Description: Details the EOSC EU Node, services, and federation model.

Link: https://open-science-cloud.ec.europa.eu

EOSC Association Website

Description: Information on membership, stakeholder engagement, and events.

Link: https://eosc.eu

European Commission: Shaping Europe's Digital Future (EOSC)

Description: Outlines EOSC's role in open science and data strategy.

Link: https://digital-strategy.ec.europa.eu/en/policies/european-open-science-cloud

Gaia-X European Association for Data and Cloud AISBL

Year of Beginning: 2019 (officially founded in 2020)

Sector: Cloud Computing, Data Infrastructure, Digital Sovereignty

Political Geography: Europe (headquartered in Brussels, Belgium)

Description:

Gaia-X is a European initiative to develop a federated, secure, and interoperable data infrastructure that promotes digital sovereignty, transparency, and data protection. It connects existing cloud and data services into a decentralized ecosystem, enabling secure data sharing across sectors like healthcare, finance, and manufacturing. Governed by the Gaia-X European Association for Data and Cloud AISBL, it emphasizes European values (e.g., GDPR compliance, openness) and supports innovation through data spaces and open-source standards. Gaia-X is not a cloud provider but a framework for interoperability and trust.

Short History:

Initiated in 2019 by German Minister Peter Altmaier and French Minister Bruno Le Maire, Gaia-X was formally announced at the 2019 Digital Summit in Dortmund, Germany. The Gaia-X Association AISBL was established in June 2020 with 22 founding members, including Fraunhofer, CISPE, and major firms like Siemens and SAP. By 2021, it grew to over 300 members, and in 2024, it released the Gaia-X Compliance Document to standardize interoperability and trust. Despite ambitions, critics note challenges like bureaucratic delays and influence from non-European hyperscalers, diluting its original vision.

Mission:

To create a trusted, federated, and interoperable digital ecosystem aligned with European values, enabling secure data sharing, innovation, and digital sovereignty while reducing dependency on non-European cloud providers.

Aims and Objectives:

- Develop a federated data infrastructure for secure, transparent data exchange.
- Promote digital sovereignty by ensuring user control over data access and usage.
- Establish common standards and policies (e.g., Gaia-X Compliance Document) for interoperability and trust.
- Foster data spaces in sectors like agriculture, health, and mobility to drive innovation.
- Support European cloud providers and SMEs to compete globally while adhering to EU regulations.

Funding:

Funded primarily through membership subscriptions from over 340 member organizations, including corporations, research institutions, and associations. The German government has provided significant funding to support the Gaia-X initiative. In 2021, the German Federal Ministry for Economic Affairs and Energy (BMWi) launched the funding competition “Innovative and Practical Applications and Data Spaces in the Gaia-X Digital Ecosystem”, with a budget of up to €186.8 million.

Eleven projects were selected in the first tranche (approximately €122 million planned, €117.4 million awarded in February 2022), and total funding for these projects amounted to approximately €132 million by 2025[31]. Also The French government supports Gaia-X-related projects through its national AI strategy. Additional funding comes from EU grants (e.g., NextGenerationEU) and national contributions via Gaia-X Hubs. Exact figures are not publicly disclosed.

System of Governance (Ownership and Control):

Gaia-X operates as an international non-profit (AISBL) under Belgian law, governed by a Board of Directors elected by the General Assembly for two-year terms (only European-headquartered organizations eligible)[32]. The Policy Rules Committee defines compliance rules, the Technical Committee sets technical standards, and the Data Space Business Committee supports sector-specific data spaces. National Gaia-X Hubs coordinate local ecosystems. Decision-making is collaborative, emphasizing neutrality and transparency.

Legal Form:

International non-profit association (Association Internationale Sans But Lucratif, AISBL) under Belgian law, headquartered in Brussels.

Licenses Used:

Gaia-X promotes open-source principles, with its Federation Services and software components (e.g., Gaia-X Digital Clearing House) released under permissive licenses like Apache 2.0 or MIT. Specific licenses vary by component but align with open-source standards.

Broader Contributors:

Over 340 member organizations from 27 countries, including cloud providers (e.g., OVHcloud, Deutsche Telekom), users (e.g., BMW, Bosch), research institutions (e.g., Fraunhofer), and associations (e.g., IDSA, CISPE). Contributors participate in working groups, national hubs, and open-source communities, with thousands of experts involved globally.

Broader Impact:

Gaia-X enhances Europe's digital sovereignty by enabling secure data sharing, reducing reliance on US/Chinese hyperscalers (e.g., AWS, Azure), and fostering innovation in data-driven business models. It supports GDPR-compliant ecosystems, benefiting SMEs, governments, and industries. However, its impact is limited by slow progress and competition from dominant providers. The framework influences global standards for data interoperability and trust.

---

[31] https://dsc.bund.de/SharedDocs/Downloads/DE/Sachgebiete/Digitales/GAIAX/Foerderbekanntmachung.pdf; https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Pressemitteilungen/2022/02/20220228-117-millionen-euro-fuer-elf-gaia-X-leuchtturmprojekte.html; https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Pressemitteilungen/2025/20250401-gaia-x-projekte-fuer-europaeische-dateninfrastruktur-erfolgreich-abgeschlossen.html

[32] Even so concerns about hyperscaler influence are widespread in recent analyses (e.g., DataCenterDynamics, 2025).

Qualitative Impact:

Gaia-X empowers European businesses, especially SMEs, to leverage data securely, fostering innovation and competitiveness. Its focus on sovereignty and GDPR compliance builds trust, while data spaces enable cross-sector collaboration. Critics highlight bureaucratic challenges and partial capture by hyperscalers, but the initiative remains a cornerstone of Europe's digital strategy.

Flagship Projects:

- Catena-X: Automotive data space for supply chain interoperability.
- OpenGPT-X: AI language model node for secure data processing.
- TEAM-X: Medical data exchange ecosystem.
- Gaia-X Digital Clearing House (GXDCH): Trust framework for automated credential validation.

Official Website:

https://Gaia-X.eu

Primary Sources:

Gaia-X Official Website

Description: Primary source for Gaia-X's mission, structure, projects, and contacts.

Link: https://Gaia-X.eu

Gaia-X Association Page

Description: Details on governance, membership, and organizational structure.

Link: https://Gaia-X.eu/association

Gaia-X Compliance Document Announcement

Description: Outlines the 2024 Compliance Document, labeling system, and trust framework.

Link: https://Gaia-X.eu/news/Gaia-X-introduces-the-compliance-document-to-enable-and-increase-trust-security-and-european-sovereignty-in-digital-ecosystems

Gaia-X Architecture Document

Description: Technical details on Gaia-X credentials, policy enforcement, and federation services.

Link: https://docs.Gaia-X.eu

Gaia-X Hub Germany

Description: Information on national hubs, use cases, and funded projects.

Link: https://Gaia-X-hub.de

DataCenterDynamics Article (2025)

Description: Critical analysis of Gaia-X's progress, challenges, and hyperscaler influence.

Link: https://www.datacenterdynamics.com/en/analysis/Gaia-X-has-europes-grand-digital-infrastructure-project-hit-the-buffers/

Gitee (码云, Mǎyún)

Year of Beginning: 2013 (launched by OSChina)

Sector: Software Development, Open Source Hosting, DevOps, SaaS

Political Geography: Primarily China (headquartered in Shenzhen, Guangdong); global user base

Description:

Gitee is a proprietary online forge and software development collaboration platform primarily for hosting open-source and private software projects using Git version control. It offers a compatible API and features like code management, project collaboration, CI/CD pipelines, and enterprise-grade security. With over 10 million repositories and 5 million users, Gitee supports individual developers, enterprises, and government initiatives. Designated by China's Ministry of Industry and Information Technology (MIIT) as an "independent, open-source code hosting platform for China," it introduced mandatory manual code review in 2022 to comply with national regulations.

Short History:

Launched in 2013 by Shenzhen-based OSChina, Gitee emerged to provide a China-centric alternative to GitHub. By 2016, it gained traction among Chinese developers for its localized interface and compliance with national cybersecurity laws. In 2020, Gitee was selected by MIIT to bolster China's open-source ecosystem. On May 18, 2022, it implemented a manual code review for public repositories. By 2024, Gitee expanded enterprise services, supporting AI-driven development and cloud-native workflows with integrations like PaddleOCR and MindSpore[33].

Mission:

To provide an efficient, secure, and localized platform for software development and collaboration, fostering China's independent open-source ecosystem while enabling global developer productivity.

Aims and Objectives:

- Offer robust code hosting and collaboration tools for open-source and enterprise projects.
- Ensure compliance with Chinese cybersecurity and data sovereignty regulations.
- Enhance R&D efficiency through integrated DevOps and CI/CD pipelines.
- Support AI and cloud-native development with frameworks like PaddleOCR and MindSpore.
- Build a scalable, secure platform for China's digital transformation and global users.

Funding:

Funded through venture capital (e.g., Series B round in 2021) and revenue from enterprise SaaS subscriptions (Gitee Enterprise Edition). OSChina, its parent company, secures investments from Chinese tech funds.

---

[33] PaddleOCR and MindSpore are open-source AI frameworks developed by Chinese tech companies (by Baidu and Huawei respectively) and hosted on Gitee to advance domestic capabilities in artificial intelligence and reduce reliance on foreign tools like TensorFlow or PyTorch.

System of Governance (Ownership and Control):

Owned by OSChina (Shenzhen OSC Network Technology Co., Ltd.), a private Chinese company. Governance is centralized, with OSChina's leadership overseeing strategy and compliance. The platform enforces manual code review for public repositories, aligning with MIIT directives. Open-source contributions are managed via Git, with community input on public projects, though proprietary control limits transparency compared to fully open platforms[34].

Legal Form:

Gitee is a proprietary service operated by OSChina, a private limited company under Chinese law. It is not a non-profit or open-source entity, though it hosts open-source projects. Code contributions follow Gitee's terms of service, with open-source licenses (e.g., MIT, Apache 2.0) for public repositories.

Licenses Used:

Gitee itself is proprietary but hosted open-source projects use standard licenses like MIT, Apache 2.0, or GPL, as specified by contributors. Gitee's terms require compliance with Chinese regulations, impacting code visibility post-review[35].

Broader Contributors:

Includes over 5 million users, thousands of enterprise clients, and open-source contributors to projects like PaddleOCR, MindSpore, and OpenGait. OSChina collaborates with MIIT, universities, and tech firms (e.g., Baidu and Huawei). Community engagement occurs via forums, hackathons, and Gitee's Model Zoo for AI models. Global users contribute to multilingual projects, though the platform prioritizes Chinese developers.

Broader Impact:

Gitee strengthens China's open-source ecosystem, reducing reliance on Western platforms like GitHub while supporting digital sovereignty. Its compliance measures ensure regulatory alignment but limit transparency, impacting global adoption. Projects like PaddleOCR (80+ languages) and MindSpore drive AI innovation, benefiting academia and industry. Challenges include censorship perceptions and competition with global forges. Gitee's enterprise tools enhance R&D efficiency, with millions of repositories shaping China's tech landscape.

---

[34] Gitee's Terms of Service grants the platform broad rights to modify, restrict, or delete projects to comply with Chinese laws (e.g., Cybersecurity Law, Data Security Law), which prohibit content deemed sensitive, politically subversive, or harmful to national interests. Deleted repositories or modifications due to regulatory compliance are rarely documented, making it harder to track censorship actions. Foreign contributors face hurdles (e.g., mandatory phone verification, slower review cycles) compared to GitHub's frictionless pull-request model.

[35] Gitee requires all code uploaded to public repositories to undergo manual review by its administrators before it becomes publicly visible. Until the review is complete and approved, code in public repositories remains invisible to other users. This introduces a delay which can discourage open-source contributions, especially for projects requiring rapid iteration or collaboration across borders. Moreover if code is flagged as non-compliant during review, it may be rejected or censored, meaning it either remains private or is removed entirely.

Qualitative Impact:

Gitee empowers Chinese developers by providing a localized, compliant platform, fostering innovation in AI, cloud computing, and DevOps. Its manual review process ensures regulatory adherence but raises concerns about censorship, limiting its appeal to global open-source communities. Projects like MindSpore (deep learning) and PaddleOCR (OCR) showcase their technical prowess, though proprietary governance contrasts with fully open platforms. Gitee's role in China's tech strategy enhances national R&D but faces scrutiny over data privacy and code visibility.

Flagship Projects:

- PaddleOCR: Multilingual OCR framework supporting 80+ languages, with tools like PPOCRLabel.
- MindSpore: Open-source deep learning framework for mobile, edge, and cloud.
- OpenGait[36]: Gait recognition framework with state-of-the-art model support.
- Gitee Enterprise Edition: SaaS platform for secure, scalable DevOps workflows.

Official Website:

https://gitee.com

Primary Sources:

Gitee Official Website

Description: Primary source for platform features, mission, and support details.

Link: https://gitee.com

Wikipedia: Gitee

Description: Provides history, user metrics, and 2022 code review policy context.

Link: https://en.wikipedia.org/wiki/Gitee

Crunchbase: Gitee Profile

Description: Details funding, ownership, and enterprise services.

Link: https://www.crunchbase.com/organization/gitee

Slashdot: Gitee Reviews

Description: Contextualizes Gitee among other DevOps platforms.

Link: https://slashdot.org/software/p/Gitee

[36] OpenGait is an open-source gait recognition framework designed to advance research and development in gait analysis, a biometric technology that identifies individuals based on their walking patterns.

Hyperledger

Year of Beginning: 2015

Sector: Blockchain, Open Source Software, Distributed Ledger Technology

Political Geography: Global (founded by the Linux Foundation, USA; used by enterprises worldwide)

Description:

Hyperledger is an open-source collaborative project for developing enterprise-grade blockchain and distributed ledger technologies. It hosts frameworks like Hyperledger Fabric, Sawtooth, and Besu, supporting private, permissioned networks for industries like finance, supply chain, and healthcare. Managed by the Linux Foundation, Hyperledger engages 250+ member organizations (e.g., IBM, Accenture) and a global developer community via GitHub, focusing on scalability, privacy, and interoperability.

Short History:

Launched in 2015 by the Linux Foundation to advance enterprise blockchain, Hyperledger released Fabric 1.0 in 2017, adopted by firms like Walmart for supply chain tracking. By 2020, it supported 12 frameworks and tools, with 100,000+ deployments. In 2023, Hyperledger Besu gained traction for Ethereum-compatible networks. As of 2025, Hyperledger powers thousands of enterprise solutions with Fabric 2.5 and ongoing integrations for Web3 and DeFi.

Mission:

To foster open-source blockchain technologies that enable secure, scalable, and interoperable enterprise solutions, promoting trust and efficiency across industries.

Aims and Objectives:

- Develop enterprise-grade blockchain frameworks for diverse use cases.
- Ensure privacy and scalability in permissioned networks.
- Promote interoperability with standards like Ethereum's EVM.
- Build a global community of developers and enterprises via GitHub.
- Support industries like finance, healthcare, and supply chain with secure ledgers.

Funding:

Managed by the Linux Foundation through membership fees from 250+ organizations and grants.

System of Governance (Ownership and Control):

Operated initially by the Linux Foundation, with a Governing Board of member organizations and a Technical Steering Committee (TSC) overseeing development. The Hyperledger Project evolved into LF Decentralized Trust in September 2024. Community contributions occur via GitHub, with decisions made through RFCs and forums. Governance balances corporate and community input, though large members like IBM influence priorities.

Legal Form:

Hyperledger is an open-source project under the Linux Foundation, a US non-profit. Frameworks are freely available under open-source licenses.

Licenses Used:

Released under the Apache 2.0 License. Documentation uses Creative Commons Attribution 4.0 (CC BY 4.0).

Broader Contributors:

Includes 250+ members (e.g., IBM, Microsoft, Walmart), community developers, and academic partners. Frameworks like Fabric and Besu are maintained by dedicated teams. Engagement occurs through GitHub, Hyperledger Global Forum, and working groups on finance and supply chain.

Broader Impact:

Hyperledger drives enterprise blockchain adoption, with Fabric used in Walmart's food traceability and IBM's TradeLens. Its permissioned model ensures privacy but limits public blockchain use. Scalability and interoperability are strengths, though corporate dominance raises concerns about decentralization. It sets standards for enterprise DLT, but complexity and costs challenge smaller firms.

Qualitative Impact:

Hyperledger transforms industries by enabling secure, transparent ledgers. Its enterprise focus ensures privacy but distances it from public blockchain communities. Adoption by major firms validates its reliability, though setup complexity and corporate influence limit accessibility for smaller players. As a Digital Public Good, it drives innovation but requires careful governance to maintain openness.

Flagship Projects:

- Hyperledger Fabric: Permissioned blockchain for enterprise use.
- Hyperledger Besu: Ethereum-compatible framework for hybrid networks.
- Hyperledger Sawtooth: Scalable ledger with pluggable consensus.
- Cacti: Interoperability framework for blockchain networks.

Official Website:

https://www.hyperledger.org

Primary Sources:

Hyperledger Official Website

Description: Primary source for frameworks, use cases, and community.

Link: https://www.hyperledger.org

Hyperledger GitHub Repository

Description: Hosts code for Fabric, Besu, and other frameworks.

Link: https://github.com/hyperledger

Hyperledger Documentation

Description: Technical guides for deployment and development.

Link: https://docs.hyperledger.org

Linux Foundation: Hyperledger Overview

Descrhyperledgeription: Details governance and member contributions.

Link: https://www.linuxfoundation.org

Hyperledger Global Forum 2023

Description: Highlights enterprise use cases and updates.

Link: https://events.linuxfoundation.org/hyperledger-global-forum

India Stack

Year of Beginning: 2009 (conceptualized with Aadhaar[37] launch)

Sector: Digital Infrastructure, Financial Technology, e-Governance

Political Geography: India (with global adoption potential; headquartered in New Delhi)

Description:

India Stack is a set of open APIs and digital public goods[38] designed to unlock identity, data, and payment systems at a population scale, fostering financial and social inclusion. It comprises four layers: Presenceless (Aadhaar biometric ID), Paperless (eKYC, DigiLocker), Cashless (Unified Payments Interface, UPI), and Consent (Data Empowerment and Protection Architecture, DEPA). Managed by various government entities like the Unique Identification Authority of India (UIDAI) and National Payments Corporation of India (NPCI), it enables seamless digital transactions, e-governance, and data sharing, transforming India's digital economy.

Short History:

India Stack began in 2009 with Aadhaar, a biometric ID system launched by UIDAI to provide unique identities to 1.4 billion Indians. By 2015, DigiLocker and eSign enabled paperless services, followed by UPI in 2016, revolutionizing digital payments. DEPA, introduced in 2020, added consent-based data sharing. The 2016 demonetization policy accelerated adoption, with UPI handling 74 billion transactions by 2022. In 2022, India launched *indiastack.global* to share its framework globally, signing MoUs with countries like Trinidad and Tobago. By 2024, 1.35 billion Indians (95%) were enrolled in Aadhaar, with over 80% of adults banked, up from 35% in 2011.

Mission:

To provide a unified digital infrastructure of open APIs and digital public goods that enables presence-less, paperless, and cashless service delivery, promoting financial inclusion, innovation, and digital transformation for all.

Aims and Objectives:

- Enhance financial inclusion by providing digital identity and payment access to underserved populations.
- Streamline e-governance through paperless services like DigiLocker and eSign.
- Foster innovation via interoperable APIs for startups, fintechs, and businesses.
- Ensure user control over data through consent-based frameworks like DEPA.
- Share India Stack globally as a model for digital public infrastructure (DPI).

---

[37] Aadhaar, in Hindi, means "foundation" or "base". It refers to the biometric ID system launched by UIDAI to provide unique identities.

[38] India Stack is composed of several building blocks, most of which were not developed and released as open source software. However, they are open protocols and standards, freely accessible and usable.

Funding:

Funded primarily by the Government of India through ministries like the Ministry of Electronics and Information Technology (MeITY) and agencies like UIDAI, NPCI, and the Reserve Bank of India (RBI). Additional support comes from private-sector partnerships (e.g., banks, fintechs).

System of Governance (Ownership and Control):

India Stack is a decentralized framework managed by multiple government entities: UIDAI oversees Aadhaar, NPCI manages UPI, MeITY handles DigiLocker and DEPA, and RBI regulates financial components like Account Aggregators. Governance emphasizes interoperability, open APIs, and public-private collaboration, with no proprietary IP restricting adoption. The framework operates as a public good, with transparent, consent-driven data policies, though critics note government oversight raises privacy concerns[39].

Legal Form:

No single legal entity; India Stack is a framework of digital public goods managed by government agencies (UIDAI, NPCI, MeITY) under Indian law, with components like UPI regulated by RBI. It operates as a public infrastructure project under the Digital India initiative.

Licenses Used:

The data model (e.g., Aadhaar's biometric database, UPI's transaction protocols) is proprietary to respective agencies but accessible via open APIs. India Stack APIs are open and royalty-free, with no proprietary licenses, enabling global adoption. Software components (e.g., UPI, DigiLocker) use open-source-compatible licenses where applicable, though specific licenses (e.g., Apache 2.0) are not always disclosed. Aadhaar's biometric data is managed under UIDAI's security protocols, not licensed externally.

Broader Contributors:

Includes government agencies (UIDAI, NPCI, MeITY, RBI), private firms (e.g., Google, Paytm, PhonePe), fintech startups, and open-source developers. Over 42,000 fintech firms leverage India Stack, with millions of developers using APIs. International partners like Singapore's MAS and global bodies (e.g., World Bank, IMF) collaborate on adoption. Citizens contribute via platforms like myGov.in.

Broader Impact:

India Stack has transformed India's digital economy, achieving 80% financial inclusion in six years (2011-2017), compared to a projected 46 years. According to official data from the National Payments Corporation of India (NPCI) and the Ministry of Finance, UPI processed 241.6 billion transactions during the 2025–26 financial year. DigiLocker stores 5 billion documents, and Aadhaar authenticates 74 billion transactions. It reduces corruption via direct benefit transfers (DBT), boosts

[39] Privacy concerns led to a 2017 Supreme Court ruling affirming privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd) vs Union of India*. The unanimous decision by a nine-judge bench declared that the right to privacy is a fundamental right under Article 21 (right to life and personal liberty) and Part III of the Indian Constitution. The case arose from a challenge to Aadhaar's constitutionality, as critics argued its collection of biometric and demographic data posed significant privacy risks.

fintech (87% adoption rate), and supports sectors like healthcare and education. Globally, it's a model for DPI, though privacy, security, and digital exclusion concerns persist.

Qualitative Impact:

India Stack empowers citizens with digital access to services, reducing bureaucracy and enabling instant transactions. It fosters innovation, with fintechs like Paytm thriving on UPI. DBT enhances welfare efficiency, saving $36 billion. However, privacy concerns (e.g., Aadhaar leaks) and digital exclusion for rural/illiterate populations remain challenges. Globally, it's praised as a DPI benchmark by the IMF and World Bank.

Flagship Projects:

- Aadhaar: Bimetric ID for 1.35 billion, enabling eKYC and DBT.
- Unified Payments Interface (UPI): Real-time payment system, 99 billion transactions annually.
- DigiLocker: Cloud storage for 5 billion documents, paperless governance.
- DEPA/Account Aggregator: Consent-based data sharing for finance, health, and more.

Official Website:

https://indiastack.org

Primary Sources:

India Stack Official Website

Description: Primary source for mission, components, APIs, and developer resources.

Link: https://indiastack.org

IMF: The India Stack is Revolutionizing Access to Finance

Description: Details Aadhaar, UPI, and financial inclusion impacts.

Link: https://www.imf.org/external/pubs/ft/fandd/2021/07/india-stack-financial-access-and-digital-inclusion.htm

Wikipedia: India Stack

Description: Overview of history, layers, and global influence.

Link: https://en.wikipedia.org/wiki/India_Stack

IMF Working Paper: Stacking up the Benefits

Description: Analysis of DPI's economic and social impacts.

Link: https://www.elibrary.imf.org/view/journals/001/2023/078/001.2023.issue-078-en.xml

India Stack 101: Times of India

Description: Explains Aadhaar, UPI, DigiLocker, and DEPA's societal role.

Link: https://timesofindia.indiatimes.com/blogs/voices/india-stack-101-a-primer-on-indias-world-renowned-digital-public-infrastructure

EEF: India's Supreme Court Ruling on Right to Privacy

Description: Details the Supreme Court judgment on biometric scheme Aadhaar

Link: https://www.eff.org/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its-about-time

MOSIP (Modular Open Source Identity Platform)

Year of Beginning: 2018

Sector: Digital Identity, Open Source Software, Biometrics

Political Geography: Global (developed by IIIT-Bangalore, India; deployed in countries like Morocco, Philippines, Ethiopia)

Description:

MOSIP is an open-source platform for building national digital identity systems, enabling governments to create secure, scalable, and interoperable ID solutions. It supports biometric and demographic data management, authentication, and e-KYC processes, with modular components for registration, authentication, and partner management. Designed for sovereignty and privacy, MOSIP is vendor-neutral and customizable, used in countries like Morocco, Philippines, and Ethiopia. Managed by the International Institute of Information Technology, Bangalore (IIIT-B), it fosters a global community via GitHub and collaborates with organizations like the World Bank and Bill & Melinda Gates Foundation.

Short History:

Launched in 2018 by IIIT-Bangalore with funding from the Gates Foundation, Omidyar Network, and Tata Trusts, MOSIP aimed to provide a cost-effective alternative to proprietary identity systems. Pilot deployments began in 2019 in Morocco and the Philippines. In 2024, MOSIP introduced version 1.2.0, enhancing biometrics and interoperability. By 2025, MOSIP supported nearly 130 million digital IDs across 26 countries (roughly 95 million registrations in the Philippines and Ethiopia)[40], with ongoing integrations for digital public infrastructure (DPI).

Mission:

To empower nations with an open-source, modular digital identity platform that ensures data sovereignty, privacy, and inclusivity, enabling secure and scalable ID systems for public and private services.

Aims and Objectives:

- Provide a modular, open-source framework for national ID systems.
- Ensure data sovereignty and privacy through vendor-neutral design.
- Avoid lock-in and ensure interoperability.
- Support interoperability with global standards (e.g., ISO, W3C).
- Foster a global community for development and customization via GitHub.
- Enable cost-effective, scalable digital identity for underserved populations.

Funding:

Funded by grants from the Bill & Melinda Gates Foundation, Omidyar Network, Tata Trusts, Norad and partnerships with organizations like the World Bank.

[40] https://www.mosip.io/news_events/mosip-country-conversations-2025

System of Governance (Ownership and Control):

Managed by IIIT-Bangalore, with a governance council including academic, industry, and government representatives. Development is community-driven via GitHub, with contributions reviewed by a core team. MOSIP's modular architecture allows countries to customize deployments while adhering to open-source principles. Transparency is ensured through public repositories and regular audits, though strategic decisions are centralized at IIIT-B.

Legal Form:

MOSIP is an open-source project under IIIT-Bangalore, a registered academic institute in India, not a standalone legal entity. Software is freely available under open-source licenses.

Licenses Used:

Released under the Mozilla Public License 2.0 (MPL 2.0), allowing use, modification, and distribution with minimal restrictions. Documentation uses Creative Commons Attribution 4.0 (CC BY 4.0). Some edge components, such as user interfaces, are licensed under the more permissive Mit license.

Broader Contributors:

Led by IIIT-B, with contributions from governments (e.g., Philippines, Ethiopia), tech partners (e.g., Idemia, Thales), academic partners (Alan Turing Institute UK, CMU Africa) and donors like the Gates Foundation. Community developers contribute via 30+ GitHub repositories. Collaborations with the World Bank and MOSIP Connect events foster engagement. Local implementers adapt MOSIP for national needs, ensuring context-specific solutions.

Broader Impact:

MOSIP enables digital inclusion for over 100 million people, supporting services like financial access and healthcare. Its open-source model reduces costs compared to proprietary systems, but customization requires technical expertise, posing challenges for low-capacity governments. Privacy concerns arise from biometric data storage, though MOSIP's decentralized design mitigates risks. Its adoption in Africa and Asia drives DPI growth, but geopolitical tensions and funding dependence limit global scalability.

Qualitative Impact:

MOSIP empowers nations to build sovereign ID systems, reducing reliance on proprietary vendors. Its modular design supports diverse use cases, from Identity being established as foundational technical infrastructure across the economy to financial inclusion. Challenges include ensuring data privacy in authoritarian regimes and overcoming technical barriers in low-resource settings. As a Digital Public Good, MOSIP sets a global standard for open-source identity, though sustained funding and local capacity are critical for success.

Flagship Projects:

- Inji Wallet: Mobile app for storing and sharing digital credentials.
- e-Signet: Authentication module for secure login across services.
- Resident Services: Tools for citizens to manage their digital IDs.

- Fayda ID Integration: Ethiopia's national ID system powered by MOSIP.
- Philsys ID Integration: Philipines' national ID system powered by MOSIP (93 million people registered out of 110 million population).
- RNP (national population register): Morocco's national ID system powered by MOSIP

Official Website:

https://www.mosip.io

Primary Sources:

MOSIP Official Website

Description: Primary source for platform details, deployments, and resources.

Link: https://www.mosip.io

MOSIP GitHub Repository

Description: Hosts open-source code and developer contributions.

Link: https://github.com/mosip

MOSIP Documentation

Description: Technical details and implementation guides.

Link: https://docs.mosip.io

World Bank: MOSIP Case Study

Description: In the framework of a study on "Open Source for Global Public Goods", it highlights MOSIP's role in digital identity.

Link: https://documents1.worldbank.org/curated/en/672901582561140400/pdf/Open-Source-for-Global-Public-Goods.pdf

MOSIP Connect 2023 Report

Description: Summarizes deployments and community engagement.

Link: https://www.mosip.io/news_events/mosip-rewind-looking-back-at-2023

X-Road / Nordic Institute for Interoperability Solutions (NIIS)

Year of Beginning: 2001 (X-Road launched); 2017 (NIIS founded)

Sector: Digital Government, Data Exchange, Interoperability, Open Source Software

Political Geography: Global (NIIS headquartered in Tallinn, Estonia, and Helsinki, Finland; X-Road used in 20+ countries)

Description:

X-Road is an open-source data exchange layer solution that enables secure, unified, and interoperable data sharing between organizations over the Internet. It serves as a distributed integration layer for information systems, ensuring confidentiality, integrity, and interoperability using Public Key Infrastructure (PKI) and standardized protocols. Managed by the Nordic Institute for Interoperability Solutions (NIIS), a non-profit association founded by Estonia and Finland, X-Road powers national ecosystems like Estonia's X-tee and Finland's Suomi.fi Data Exchange Layer, saving Estonia 1,345 years of working time annually. NIIS oversees X-Road's development, strategic management, and global adoption, fostering cross-border digital government solutions.

Short History:

X-Road was developed by Estonia's Information System Authority (RIA) and launched in 2001. Finland adopted it in 2015 for Suomi.fi, connecting both countries' data layers by 2018. In 2017, Estonia and Finland founded NIIS to manage X-Road's core development, with Iceland joining in 2021. The source code was open-sourced under the MIT license in 2015-2016. NIIS released X-Road 6.19.0 in 2018 and X-Road 7 "Unicorn" beta in 2019, adding REST support by 2019. In 2024, NIIS began a proof-of-concept for X-Road 8 "Spaceship," aligning with Gaia-X's trust framework for data spaces. Partnerships include Ukraine, the Faroe Islands, and Åland.

Mission:

To ensure the development and strategic management of X-Road and other cross-border digital government solutions, providing a sustainable, secure, and interoperable data exchange platform that enhances digital public services and fosters global collaboration.

Aims and Objectives:

- Develop and maintain X-Road as a secure, open-source data exchange solution.
- Promote interoperability and cross-border data sharing for digital government.
- Enhance sustainability, targeting X-Road as the most sustainable data exchange solution by 2030.
- Support self-sovereign identity (SSI) and Gaia-X compliance for modern trust frameworks.
- Foster a global X-Road community for knowledge sharing and innovation.

Funding:

NIIS is funded through membership contributions from Estonia, Finland, and Iceland, with additional revenue from partner agreements (e.g., Ukraine, Åland) and public procurement contracts (e.g., Gofore Plc).

System of Governance (Ownership and Control):

NIIS, a non-profit association under Estonian law, governs X-Road's development and strategy. A Management Board, led by a CEO, oversees operations, with technical direction from a CTO. Member countries (Estonia, Finland, Iceland) have equal representation, and partners (e.g., Ukraine) participate in discussions. Development is transparent, community-driven, and managed via GitHub, with contributions under the MIT license. The X-Road trust model uses PKI (Public Key Infrastructure)[41], with ongoing research into SSI (Self-Sovereign Identity) for Gaia-X compatibility.

Legal Form:

NIIS is a non-profit association registered under Estonian law. X-Road is an open-source software project with no independent legal entity, managed by NIIS and distributed under the MIT license.

Licenses Used:

X-Road's core components are licensed under the MIT license, ensuring free use, modification, and distribution. Extensions like REST Adapter Service and X-Road Metrics also use MIT or compatible open-source licenses.

Broader Contributors:

Includes NIIS members (Estonia, Finland, Iceland), partners (Ukraine, Faroe Islands, Åland, Schleswig-Holstein), and a global X-Road community across 20+ countries. Contributors comprise developers, e-governance experts, and organizations via GitHub, with tools like X-Road Metrics and Catalog developed collaboratively. Universities (e.g., the University of Tartu) and firms like Gofore Plc contribute research and code. Thousands engage through community events and forums.

Broader Impact:

X-Road enables efficient, secure data exchange, reducing administrative burdens and saving time (e.g., 1,345 years annually in Estonia). It supports cross-border services, aligns with EU initiatives like the Single Digital Gateway, and enhances digital sovereignty. Its open-source model fosters global adoption, though challenges include complexity and Gaia-X integration. Sustainability efforts, like carbon footprint reduction, position it as a leader in green digital infrastructure.

Qualitative Impact:

X-Road streamlines e-governance, enabling seamless data exchange while prioritizing security and privacy. Its open-source nature empowers governments to avoid vendor lock-in, fostering digital sovereignty. Community-driven development and sustainability goals (e.g., carbon neutrality by 2030) enhance trust and innovation. However, integrating modern frameworks like Gaia-X requires ongoing effort.

Flagship Projects:

- X-Road 8 "Spaceship": Proof-of-concept for Gaia-X-compatible data spaces (2024).
- X-Road Metrics: Tool for collecting and analyzing ecosystem data.

[41] X-Road is not blockchain-based, despite erroneous claims; it uses PKI for trust.

- REST Adapter Service: Enables REST service integration with X-Road.
- Harmony eDelivery Access: Supports EU cross-organizational data exchange.

Official Website:

https://www.niis.org (NIIS); https://x-road.global (X-Road)

Primary Sources:

NIIS Official Website

Description: Primary source for NIIS's mission, governance, and X-Road details.

Link: https://www.niis.org

X-Road Official Website

Description: Details X-Road's features, adoption, and technical specifications.

Link: https://x-road.global

NIIS GitHub: X-Road Development

Description: Hosts source code, development practices, and community contributions.

Link: https://github.com/nordic-institute/X-Road-development

Wikipedia: X-Road

Description: Overview of X-Road's history, technical details, and NIIS's role.

Link: https://en.wikipedia.org/wiki/X-Road

Open European Software-Defined Vehicle Platform (SDV)

Year of Beginning: 2022 (conceptualized); 2023 (formal initiative launched)

Sector: Automotive, Software Engineering, Open Source Software, Digital Infrastructure

Political Geography: Europe (coordinated by the European Commission, headquartered in Brussels, Belgium, with global outreach potential)

Description:

The Open European Software-Defined Vehicle Platform, part of the Software-Defined Vehicle of the Future (SDVoF) ecosystem, is a European Commission-led initiative to develop a modular, open-source software stack for software-defined vehicles (SDVs). It focuses on non-differentiating, pre-competitive components like hardware abstraction layers, middleware, APIs, and development tools to enhance interoperability, maintainability, and time-to-market. Supported by the Chips Joint Undertaking and Horizon Europe, it involves major European automotive OEMs, suppliers, and tech firms, aiming to bolster EU competitiveness against non-EU players by fostering collaboration and reducing software complexity.

Short History:

Conceptualized in 2022 via DG CONNECT workshops (November 29, 2022, and March 7, 2023), the initiative addressed rising software complexity and talent shortages in the EU automotive sector. A Concept Paper was published in 2023, proposing a Focus Topic under the Key Digital Technologies Joint Undertaking. Calls for initial actions closed on May 3, 2023. In 2024, the SDVoF ecosystem was formalized within the Vehicle of the Future initiative, with projects like FEDERATE and HAL4SDV launched to develop reference architectures and governance. A Joint Roadmap and Vision document was developed by 2024, with €250 million invested for 2023-2024.

Mission:

To create a sustainable, open-source software platform for software-defined vehicles that promotes collaboration, standardizes non-differentiating components, and ensures EU leadership in automotive innovation, competitiveness, and digital sovereignty.

Aims and Objectives:

- Develop an open reference architecture and standardized software building blocks (e.g., interfaces, middleware) for SDVs.
- Facilitate rapid adoption through open-source strategies, reference implementations, and development tools.
- Reduce software complexity and development costs via pre-competitive collaboration.
- Establish a governance structure to coordinate EU-wide research and innovation.
- Integrate with initiatives like Risc-V hardware platforms and Gaia-X for interoperability and data spaces.

Funding:

Funded through Horizon Europe and the Chips Joint Undertaking Member States, and industry. Additional investments were announced under the European Chips Act for chip production, with a

significant share for automotive applications. Future funding is planned for middleware, APIs, and zero-emission mobility tools through 2030.

System of Governance (Ownership and Control):

Managed by the European Commission (DG CONNECT) and the Chips Joint Undertaking, with a governance structure involving major European OEMs, suppliers, and consortia like FEDERATE[42] and HAL4SDV[43]. The FEDERATE project orchestrates research and innovation, while a high-level governance body ensures stakeholder alignment. The platform is open-source, with no proprietary ownership, emphasizing a "code-first" approach and community-driven development under Apache 2.0 or compatible licenses. The EC acts as a neutral convener.

Legal Form:

No independent legal entity; the platform is an initiative under the European Commission's Horizon Europe and Chips Act frameworks, with projects managed by consortia and the Chips Joint Undertaking, a public-private partnership under EU law.

Licenses Used:

Software components are developed under OSI-approved open-source licenses, primarily Apache 2.0, to ensure accessibility and collaboration. The Eclipse SDV Working Group's maturity badges ensure compliance with automotive standards like A-SPICE and ISO 26262.

Broader Contributors:

Includes major European OEMs (e.g., BMW, Stellantis, Volkswagen), suppliers (e.g., Bosch, Continental), tech firms (e.g., Microsoft, Renesas), and research organizations. Consortia like FEDERATE and HAL4SDV, alongside alliances (Eclipse SDV[44], COVESA[45], AUTOSAR[46], SOAFEE[47]), drive development. Thousands of developers contribute via open-source platforms like GitHub, with community events like the European Conference on Automotive Software.

Broader Impact:

The platform strengthens EU automotive competitiveness by standardizing non-differentiating software, reducing development costs, and countering non-EU competition (e.g., Tesla, Chinese OEMs). It supports zero-emission mobility, enhances safety via modular updates, and aligns with EU data strategies like Gaia-X. Challenges include coordinating diverse alliances and ensuring adoption by 2030. Its open-source model could inspire global SDV standards, though scalability remains a hurdle.

---

42 FEDERATE (Software-Defined Vehicle Support and Coordination Project): https://federate-sdv.eu

43 HAL4SDV (Hardware Abstraction Layer for a European Software-Defined Vehicle Approach): https://www.hal4sdv.eu

44 Eclipse SDV (Software Defined Vehicle): https://sdv.eclipse.org

45 COVESA (Connected Vehicle Systems Alliance): https://covesa.global

46 AUTOSAR (AUTomotive Open System ARchitecture): https://www.autosar.org

47 SOAFEE (Scalable Open Architecture for Embedded Edge): https://www.soafee.io

Qualitative Impact:

The platform fosters collaboration, reducing redundant development and closing the gap with non-EU competitors. Its open-source approach enhances maintainability and portability, benefiting SMEs and startups. Integration with AI and Gaia-X could revolutionize mobility, but governance complexity and talent shortages pose risks. If successful, it will secure EU leadership in SDVs, supporting sustainable and connected mobility.

Flagship Projects:

- FEDERATE: Coordinates SDVoF research, governance, and ecosystem building.
- HAL4SDV: Develops hardware abstraction layer for SDV architecture.
- Eclipse SDV Working Group: Provides open-source SDV components (e.g., SDV.Edge, SDV.Ops).
- SOAFEE: Scalable open architecture for embedded edge, aligned with SDVoF.

Official Website:

https://digital-strategy.ec.europa.eu/en/policies/european-digital-vehicle-ecosystem

Primary Sources:

European Commission: European Digital Vehicle Ecosystem

Description: Official source for SDVoF ecosystem, governance, and funding details.

Link: https://digital-strategy.ec.europa.eu/en/policies/european-digital-vehicle-ecosystem

Concept Paper: Open European Software-Defined Vehicle Platform

Description: Outlines challenges, scope, and open-source strategy for SDVoF.

Link: https://digital-strategy.ec.europa.eu/en/library/concept-paper-open-european-software-defined-vehicle-platform

FEDERATE Project Website

Description: Details FEDERATE's role in SDVoF coordination and roadmap.

Link: https://federate-sdv.eu/

Eclipse SDV Working Group

Description: Provides open-source SDV components and standards compliance.

Link: https://sdv.eclipse.org/

Chips Joint Undertaking: SDV Actions

Description: Funding and governance details for SDVoF projects.

Link: https://www.chips-ju.europa.eu/

European Commission: Vehicle of the Future Initiative

Description: Context for SDVoF within broader automotive strategy.

Link: https://digital-strategy.ec.europa.eu/en/policies/vehicle-future

Open Wallet Foundation (OWF)

Year of Beginning: 2022 (announced); 2023 (formal launch)

Sector: Digital Identity, Open Source Software, Cybersecurity

Political Geography: Global (headquartered in Brussels, Belgium, under Linux Foundation Europe)

Description:

The Open Wallet Foundation (OWF), a project of Linux Foundation Europe, is a consortium of companies, non-profits, and academic organizations developing open-source software for secure, interoperable, and multi-purpose digital wallets. OWF fosters collaboration to create standards-based components that issuers, wallet providers, and relying parties can use to build wallets for diverse use cases, including payments, identity verification, and credential storage (e.g., driver's licenses, diplomas). It emphasizes user choice, privacy, and security, avoiding vendor lock-in and supporting initiatives like the EU Digital Identity Wallet (EUDI).

Short History:

Announced in September 2022 by the Linux Foundation, OWF was formally launched on February 23, 2023, with 37 inaugural members, including Accenture, Visa, Google, and MOSIP. By August 2023, Google joined as a Premier member, and MOSIP contributed code for digital identity. In 2024, OWF announced the Open Wallet Forum with the International Telecommunication Union (ITU) and published the Safe Wallet Guide, collaborating on the EU Digital Identity Wallet (EUDI) with milestones like code contributions from Google and Ping Identity. In late May 2024, at the WSIS+20 High-Level Event in Geneva, OWF announced three key milestones: the intent to launch the Open Wallet Forum (hosted by ITU and Linux Foundation to drive multi-stakeholder collaboration on interoperable digital wallets), a partnership with the United Nations International Computing Centre (UNICC) and Linux Foundation to mirror all OWF Git repositories for global accessibility and upstream contributions, and enhanced public-sector alignment. In June 2024, Mastercard joined as a new Premier member, strengthening focus on payments interoperability. By September 2024, Huawei joined as a Premier member, expanding innovation in open digital wallet ecosystems. In 2025, OWF hosted events like a webinar on MOSIP's Inji credentialing stack (June) and a high-level panel at Davos (January), while incubating new TypeScript projects for digital identity standards (February). On July 2025, OWF co-promoted together with other 50 organizations - including ITU, European Commission, World Bank, Red Cross, ISO, IEC, ETSI, CEN, and CENELEC, Linux Foundation and Eclipse Foundation - the Global Digital Collaboration Conference (GDC25) in Geneva, focusing on global standards for open digital ecosystems, with participation from members like Google and Visa to advance cross-border interoperability.

Mission:

To develop an open-source software engine for secure, interoperable, and multi-purpose digital wallets, enabling anyone to build solutions that preserve user choice, security, and privacy while fostering global adoption and interoperability.

Aims and Objectives:

- Develop and maintain open-source components for digital wallets supporting payments, identity, and credentials.
- Ensure interoperability across devices, operating systems, and use cases, including cross-border projects like EUDI.
- Promote privacy, security, and user control through standards-based, transparent development.
- Establish best practices via guides (e.g., Safe Wallet Guide) and Special Interest Groups (SIGs).
- Collaborate with public and private sectors through the Governmental Advisory Council and Open Wallet Forum.

Funding:

Primarily funded through membership fees from Premier (e.g., Google, Visa, Accenture), General, and Associate members, with additional revenue from events and sponsorships.

System of Governance (Ownership and Control):

Hosted by Linux Foundation Europe, OWF is governed by a Governing Board and a Technical Advisory Council (TAC) overseeing project lifecycles (Labs, Growth, Impact stages). The Governmental Advisory Council ensures public-sector alignment. Governance is transparent, community-driven, and adheres to Apache 2.0 licensing and Linux Foundation Europe's Code of Conduct.

Legal Form:

Non-profit project under Linux Foundation Europe, an independent entity under Belgian law, with no standalone legal status for OWF.

Licenses Used:

OWF projects use the Apache 2.0 license for code, ensuring open access and collaboration. Labs projects must adopt Apache 2.0 or approved open licenses to align with OWF's open-source ethos.

Broader Contributors:

Over 37 members, including Google, Visa, Accenture, American Express, Microsoft, and MOSIP, Mastercard, Huawei, plus 20 non-profits/academic entities (e.g., OpenID Foundation, Hyperledger Foundation, MIT Connection Science). Thousands of developers contribute via GitHub, Discord, and Special Interests Groups (SIGs) like the Safe Wallet SIG. Public-sector engagement occurs through the Governmental Advisory Council and ITU's Open Wallet Forum.

Broader Impact:

OWF drives a global open wallet ecosystem, reducing vendor lock-in and enhancing privacy and security. It supports digital freedom by enabling portable credentials (e.g., IDs, tickets) across platforms. Its alignment with EUDI and MOSIP accelerates interoperable identity systems, though early-stage adoption limits widespread impact.

Qualitative Impact:

OWF empowers users with control over digital assets, fostering trust through open-source transparency. Its Safe Wallet Guide defines privacy, security, and governance pillars, aiding developers and policymakers. Collaboration with EUDI and ITU enhances global standards, but challenges include scaling community contributions and competing with proprietary wallets (e.g., Apple Wallet). OWF's work supports digital equity and cybersecurity, aligning with Europe's privacy priorities.

Flagship Projects[48]:

- Bifold Wallet: Extensible React Native wallet for digital identities, used by BC Wallet[49].
- Askar: Rust-based secure storage for decentralized trust systems.
- MULTIPAZ: Multiprotocol wallet framework for OpenID4VC and SD-JWT, aligned with EUDI.
- Learner Credential Wallet: Cross-platform app for storing/sharing digital credentials.

Official Website:

https://Open Wallet.foundation

Primary Sources:

Open Wallet Foundation Official Website

Description: Primary source for mission, projects, governance, and community engagement.

Link: https://Open Wallet.foundation

Linux Foundation Europe: Open Wallet Foundation Formation

Description: Details OWF's launch, membership, and objectives.

Link: https://linuxfoundation.eu/newsroom/linux-foundation-europe-announces-formation-Open Wallet-foundation

Open Wallet Foundation GitHub

Description: Hosts project repositories, proposals, and technical details.

Link: https://github.com/Open Wallet-foundation

Linux Foundation: Why the World Needs an Open Source Digital Wallet

Description: Whitepaper on OWF's role and digital wallet challenges.

Link: https://www.linuxfoundation.org/resources/publications/why-the-world-needs-an-open-source-digital-wallet-right-now

Payments Dive: Google Joins Open Wallet Foundation

Description: Covers Google's membership and OWF's interoperability goals.

Link: https://www.paymentsdive.com/news/google-joins-Open Wallet-foundation/624038/

---

[48] OWF does not publish wallets or credentials, focusing on open-source components for others to build upon.

[49] BC Wallet is a smartphone app developed by the Province of British Columbia, designed to securely receive, store, and present digital credentials such as permits, certifications, licenses, and identities.

OpenAtom Foundation

Year of Beginning: 2020

Sector: Open Source Software, Technology, Digital Infrastructure

Political Geography: China (headquartered in Beijing, with global outreach)

Description:

The OpenAtom Foundation, established in Beijing in June 2020, is China's first non-profit organization dedicated to fostering the global open-source community. Founded by leading tech companies, including Alibaba, Baidu, Huawei, Inspur, Qihoo 360, Tencent, and China Merchants Bank, it serves as a developer-oriented platform for incubating open-source projects. The foundation promotes collaboration, open governance, and sustainable development through activities like fundraising, education, technical support, and international partnerships. It hosts projects such as OpenHarmony, openEuler, and XuperCore, aiming to enhance China's contribution to global open-source ecosystems.

Short History:

Initiated with support from China's Ministry of Industry and Information Technology (MIIT) and registered under the Ministry of Civil Affairs, the OpenAtom Foundation was formally established on June 15, 2020. It launched its organizational structure and mission publicly on September 9, 2020. By 2022, it hosted projects like OpenHarmony and openEuler, donated by Huawei and others. In 2021, it partnered with the Eclipse Foundation to develop Oniro, a compatible OpenHarmony-based operating system. The 2023 OpenAtom Global Open Source Summit in Beijing marked its growing international presence. As of 2024, it continues to expand with over 50,000 users and thousands of enterprise applications.

Mission:

To promote the development of the global open-source community through co-construction, co-governance, and sharing, building an open and collaborative framework that empowers industries and enhances China's role in open-source innovation.

Aims and Objectives:

- Incubate and sustain open-source projects to drive technological innovation.
- Facilitate industry collaboration and build international open-source communities.
- Provide technical, legal, and financial support to developers and projects.
- Promote open-source education, talent cultivation, and academic exchange.
- Enhance open-source security and governance to ensure sustainable ecosystems.

Funding:

Primarily funded through fees and donations from member companies (e.g., Alibaba, Huawei, Tencent) and non-targeted financial contributions from enterprises and individuals. The foundation also generates revenue from consulting services, events, and training programs.

System of Governance (Ownership and Control):

Operates as a non-profit with a Board of Directors, responsible for strategic oversight and revising bylaws. The Technical Oversight Committee (TOC) provides technical guidance, approves project incubation, and promotes cross-project collaboration. The Secretariat handles daily operations. An Open Source Security Committee plans security-related activities. Governance emphasizes neutrality, transparency, and developer focus, though board members' ties to MIIT and state-aligned firms suggest government influence.

Legal Form:

Non-profit legal entity registered with China's Ministry of Civil Affairs under Chinese law.

Licenses Used:

Projects use OSI-approved open-source licenses (e.g., Apache 2.0, MIT), with specifics varying by project. For example, OpenHarmony uses Apache 2.0.

Broader Contributors:

Includes major tech firms (Alibaba, Baidu, Huawei, Tencent, Inspur, Qihoo 360), and academic institutions like Beijing Institute of Technology. Over 50,000 users and thousands of companies engage with its projects. Contributors participate via project development, the OpenAtom Open Source Contest, and events like the OpenAtom Tech Meetup, fostering a global developer community.

Broader Impact:

OpenAtom strengthens China's open-source ecosystem, reducing reliance on proprietary software and aligning with national goals for technological independence. Projects like OpenHarmony unify IoT device ecosystems, while openEuler supports enterprise computing. Its global partnerships (e.g., Eclipse Foundation) enhance interoperability, though critics note potential state influence via MIIT ties. The foundation empowers industries like AI, IoT, and blockchain, serving thousands of enterprises.

Qualitative Impact:

OpenAtom drives open-source adoption in China, fostering innovation in AI, IoT, and blockchain. Its projects address fragmentation (e.g., OpenHarmony for IoT) and enhance enterprise efficiency (e.g., openEuler). Educational initiatives like the OpenAtom Campus Tour cultivate talent, while global partnerships promote interoperability. The foundation's focus on open governance and community collaboration strengthens the global open-source ecosystem. However, state ties raise concerns about neutrality, potentially limiting international trust.

Flagship Projects:

- OpenHarmony: IoT operating system for unified device ecosystems, partnered with Eclipse for Oniro.
- openEuler: Enterprise-grade Linux distribution for servers and cloud computing.
- XuperCore: Blockchain kernel donated by Baidu, supporting scalable applications.
- AliOS Things: IoT operating system for resource-constrained devices.

Official Website:

https://www.openatom.org

Primary Sources:

OpenAtom Foundation Official Website

Description: Primary source for mission, projects, governance, and events.

Link: https://www.openatom.org

Wikipedia: OpenAtom Foundation

Description: Summarizes history, projects, and partnerships (e.g., Eclipse Foundation).

Link: https://en.wikipedia.org/wiki/OpenAtom_Foundation

Eclipse Foundation Blog: Collaboration with OpenAtom

Description: Details on the Oniro project and OpenAtom partnership.

Link: https://eclipse-foundation.blog/2024/01/30/eclipse-and-openatom-pioneering-open-source-innovation

Jamestown Foundation: Open-Source Technology and PRC Strategy

Description: Analysis of OpenAtom's state ties and strategic role.

Link: https://jamestown.substack.com/p/open-source-technology-and-prc-national

OpenSRP (Open Smart Register Platform)

Year of Beginning: 2013

Sector: Digital Health, Open Source Software, Mobile Health

Political Geography: Global (developed by Ona in Kenya; deployed in 14+ countries, including Bangladesh, India, Pakistan, Uganda, and Zambia)

Description:

OpenSRP is an open-source, FHIR-native, mobile-first electronic health record platform designed to empower frontline health workers in low-resource settings. It supports client registration, care plan management, and data collection for health services like maternal care, child immunization, and disease surveillance, even in offline environments. Built on Android with Kotlin[50] and aligned with WHO SMART Guidelines[51], OpenSRP integrates with national health systems via FHIR standards[52]. Managed by Ona, a Kenyan social enterprise, it fosters a global community of contributors through GitHub, serving over 150 million registered patients across 14 countries as of 2023.

Short History:

Initiated in 2013 by Ona, OpenSRP emerged from a student-led effort to digitize health data collection. It was central to the THRIVE Study (2014-2018), which assessed its impact in Bangladesh, India, and Pakistan. OpenSRP 2, launched in 2023, introduced FHIR-native capabilities and WHO SMART Guideline integration, with deployments in Uganda as the world's first FHIR-native Android app. By 2025, OpenSRP operates in 14 countries, including four national systems (e.g., Zambia's ZEIR), and support initiatives like the Electronic Immunization Registry (EIR). Its community-driven model continues to expand through partnerships with governments, NGOs, and the WHO.

Mission:

To empower frontline health workers with a scalable, offline-capable digital health platform that enhances care delivery, promotes data-driven decision-making, and ensures interoperability with national health systems, prioritizing equity and accessibility in low-resource settings.

Aims and Objectives:

- Provide a mobile-first, offline-capable platform for health workers to manage patient records and care plans.
- Ensure interoperability with global health standards (e.g., FHIR, WHO SMART Guidelines).
- Support scalable deployments for maternal, child, and community health programs.
- Foster an open-source community for collaborative development and local adaptation.
- Reduce administrative burdens through automated reporting and task prioritization.

---

[50] Kotlin is a open-source language for Android development.

[51] The World Health Organization's SMART (Standards-based, Machine-readable, Adaptive, Requirements-based, and Testable) Guidelines are a framework for translating health policies and clinical protocols into digital formats.

[52] Fast Healthcare Interoperability Resources (FHIR) is a global standard developed by HL7 (Health Level Seven International) for exchanging healthcare data electronically.

Funding:

Funded through Ona, grants, and partnerships with organizations like the Bill & Melinda Gates Foundation, Gavi, and the Open Technology Fund. Implementation costs vary by scale and scope, with larger deployments reducing per-worker costs. Additional revenue comes from consulting services and donor support for country-specific deployments.

System of Governance (Ownership and Control):

Managed by Ona, with a meritocratic, consensus-based governance structure established in 2021. The Project Management Committee (PMC), chaired by Ona's CEO, sets strategic direction, while the Product/Technical Committee (PTC) oversees technical roadmaps. Development occurs on GitHub, with committers and contributors following a transparent process. Community input is encouraged via developer forums and voting for committee members. Governance emphasizes human-centred design and local adaptability, with oversight from governments and partners in implementing countries.

Legal Form:

OpenSRP is an open-source project under Ona, a Kenyan social enterprise, not a standalone legal entity. The software is freely available under open-source licenses, with deployments managed by Ona or local partners.

Licenses Used:

Released under the Apache 2.0 License, allowing use, modification, and distribution without branding rights. FHIR-based modules align with HL7 standards, ensuring open interoperability.

Broader Contributors:

Led by Ona, with contributions from global partners including WHO, PATH, Gavi, and Ministries of Health in 14 countries (e.g., Zambia, Uganda, Bangladesh). Community developers contribute via 117 GitHub repositories, with implementations like Zambia's ZEIR involving over 300 facilities. Collaborations with the Linux Foundation and HL7 ensure FHIR compliance. Engagement occurs through developer forums, OpenSRP's wiki, and events like the Global Digital Health Forum.

Broader Impact:

OpenSRP empowers frontline health workers, registering over 150 million patients by 2023 across 14 countries. It streamlines care for maternal health, immunizations, and disease tracking, reducing paper-based burdens. Its offline capability supports remote areas, while FHIR integration ensures scalability with national systems. Challenges include initial user training, varying implementation timelines (2 months to 2 years), and funding dependence. OpenSRP's human-centered design and WHO alignment make it a Digital Global Good, though adoption in non-supported regions is limited by customization needs.

Qualitative Impact:

OpenSRP transforms healthcare delivery by digitizing workflows, enabling health workers to prioritize care over paperwork. Its offline functionality and FHIR integration make it ideal for low-

resource settings, as seen in Zambia's ZEIR deployment across 300+ facilities. Community-driven development ensures local adaptability, but initial learning curves and funding constraints challenge scalability. As a Digital Global Good, OpenSRP sets a standard for equitable health tech, though sustained donor support is critical for expansion.

Flagship Projects:

- OpenSRP 2: FHIR-native Android app with WHO SMART Guideline integration.
- Electronic Immunization Registry (EIR): Strengthens vaccine delivery (e.g., Zambia's ZEIR).
- Analytics Dashboard: Provides real-time health data for administrators and policymakers.
- Offline Data Sync: Enables device-to-device and cloud syncing in low-connectivity areas.

Official Website:

https://opensrp.io

Primary Sources:

OpenSRP Official Website

Description: Primary source for platform details, features, and community resources.

Link: https://opensrp.io

OpenSRP Documentation

Description: Technical details, app features, and deployment guides.

Link: https://docs.opensrp.io

GitHub: OpenSRP Repositories

Description: Hosts 117 repositories for code, including FHIR Core and client apps.

Link: https://github.com/OpenSRP

Ona: OpenSRP Overview

Description: Details Ona's role and OpenSRP 2's capabilities.

Link: https://ona.io/opensrp

OpenSRP Governance Structure

Description: Outlines meritocratic governance and committee roles.

Link: https://smartregister.org/governance-structure

Open Source Security Foundation (OSSF)

Year of Beginning: 2020

Sector: Cybersecurity, Open Source Software

Political Geography: Global (headquartered under the Linux Foundation, USA)

Description:

The Open Source Security Foundation (OSSF) is a cross-industry initiative under the Linux Foundation focused on improving the security of open-source software (OSS). It fosters collaboration among industry leaders, developers, and researchers to establish best practices, develop security tools, and promote secure software development and consumption. OSSF addresses vulnerabilities in the OSS ecosystem through technical initiatives, educational resources, and projects like Sigstore[53] and Alpha-Omega.[54]

Short History:

Formed in August 2020 as the successor to the Core Infrastructure Initiative, OSSF was launched to address growing concerns about OSS security following high-profile incidents. It brought together major tech companies (e.g., Microsoft, Google, GitHub) and security organizations (e.g., OWASP[55], NCC Group[56]). The foundation has since expanded its working groups and initiatives to enhance software supply chain security.

Mission:

To make it easier to sustainably secure the development, maintenance, and consumption of open-source software, ensuring OSS is trusted, secure, and reliable as a digital public good.

Aims and Objectives:

- Develop and promote best practices for secure OSS development.
- Create open-source security tools and standards (e.g., Sigstore for code signing, Open Source Project Security Baseline[57]).
- Enhance software supply chain security through initiatives like Alpha-Omega.
- Foster global collaboration among stakeholders, including developers, corporations, and policymakers.
- Educate and mentor diverse communities to improve OSS security.

---

[53] Sigstore is a project focused on providing a standard for signing, verifying, and protecting software to ensure supply chain integrity. It enhances trust and security in open-source software through cryptographic signatures and a public ledger.

[54] Alpha-Omega is an OSSF initiative, funded by Microsoft, Google, and Amazon, which funds critical projects (Alpha) with grants for security enhancements and audits, and uses automated tools (Omega) to identify and fix vulnerabilities in thousands of widely used open-source projects.

[55] OWASP (Open Web Application Security Project) is a nonprofit foundation focused on improving software security. It provides free, open-source tools, resources, and community-driven guidance to help developers build secure applications.

[56] NCC is a global cybersecurity and risk mitigation firm offering services like security testing, audits, and consulting.

[57] It is an OSSF program that provides a standardized framework to assess and improve the security of open-source projects. It defines best practices, tools, and metrics to establish a security baseline, helping projects identify vulnerabilities and enhance resilience against threats.

Funding:

OSSF is primarily funded through membership dues from corporate sponsors (e.g., Microsoft, Google, IBM) and grants from the Linux Foundation. Additional funding comes from contributions to specific projects and initiatives. Exact funding details are not publicly disclosed.

System of Governance (Ownership and Control):

OSSF operates under the Linux Foundation's governance model, with a Technical Advisory Council overseeing technical initiatives and a governing board comprising representatives from member organizations. Projects follow a meritocratic, community-driven model with maintainers and contributors. The foundation emphasizes transparency and inclusivity, adhering to a collaborative decision-making process.

Legal Form:

Non-profit organization under the Linux Foundation, a 501(c)(6) entity in the United States.

Licenses Used:

OSSF projects typically use permissive open-source licenses such as MIT or Apache 2.0 (e.g., Sigstore uses Apache 2.0). Specific licenses vary by project, but all align with open-source principles.

Broader Contributors:

OSSF engages thousands of contributors globally, including individual developers, security researchers, and employees from member organizations like Microsoft, Google, IBM, GitHub, and OWASP. The community contributes through working groups, code contributions, and participation in events like OSSF Community Day.

Broader Impact:

OSSF's work strengthens the global OSS ecosystem, reducing vulnerabilities in critical software used by billions (e.g., 97% of software depends on OSS). Its tools and standards (e.g., Sigstore, SBOMs[58]) enhance supply chain security, benefiting industries, governments, and end-users. The foundation's advocacy for secure-by-design principles influences policy and development practices worldwide.

Qualitative Impact:

OSSF has shifted the OSS community toward proactive security, reducing risks in software supply chains. Its guidelines, like the Open Source Project Security Baseline, empower maintainers with practical steps, fostering a culture of shared responsibility. The 2025 OSSF Policy Summit in Washington, D.C., brought together industry leaders, government officials, and security experts to discuss software supply chain security, influencing global policy recommendations and frameworks[59]. The foundation's DEI efforts promote inclusivity, broadening participation in

---

[58] SBOMs (Software Bill of Materials) is an OSSF-supported concept involving a structured list detailing a software project's components, libraries, and dependencies. SBOMs enhance supply chain security by enabling transparency, vulnerability tracking, and compliance, often integrated with tools like Sigstore for verification.

[59] Seee https://OSSF.org/category/press-release/

cybersecurity. High-profile adoptions (e.g., Sigstore by major repositories) demonstrate trust in its solutions.

Flagship Projects:

- Sigstore: A standard for signing, verifying, and protecting software, widely adopted for secure artefact management.
- Alpha-Omega: A large-scale initiative to improve the security of critical OSS projects through funding and audits.
- Open Source Project Security Baseline: Guidelines aligning OSS security with international standards.
- Scorecard: Automated checks to assess OSS project security risks.

Official Website:

https://OSSF.org

Primary Sources:

OSSF Official Website

Description: Main source for OSSF's mission, projects, governance, and contact information.

Link: https://OSSF.org

OSSF Projects Page

Description: Comprehensive overview of flagship projects like Sigstore, Alpha-Omega, and Scorecard.

Link: https://OSSF.org/projects/

OSSF Blog and Announcements

Description: Updates on leadership changes (e.g., Omkhar Arasaratnam as GM, Brian Behlendorf as CTO) and community initiatives.

Link: https://OSSF.org/blog/

Sigstore Official Website

Description: Details on Sigstore's licensing (Apache 2.0) and adoption as a key OSSF project.

Link: https://www.sigstore.dev

OSSF Community Resources

Description: Information on working groups, community engagement, and events like OSSF Community Day.

Link: https://OSSF.org/community/

Atlantic Council: Open-source Software as Infrastructure

Description: OSSF's advocacy influence in policy and development practices worldwide

https://www.atlanticcouncil.org/in-depth-research-reports/report/open-source-software-as-infrastructure/

O-RAN Alliance

Year of Beginning: 2018

Sector: Telecommunications, Open Source Software, Radio Access Network (RAN) Innovation

Political Geography: Global (headquartered in Bonn, Germany; members in 30+ countries)

Description:

The O-RAN Alliance is a global, open technical organization dedicated to transforming Radio Access Networks (RANs) by developing specifications for open, intelligent, virtualized, and fully interoperable mobile networks. Founded by major mobile operators, it promotes disaggregation of hardware and software, open interfaces, and AI-driven automation to enhance network efficiency and innovation. With over 345 members, including 32 operators, vendors, and academic institutions, the Alliance publishes RAN specifications, supports open software via the O-RAN Software Community (O-RAN SC), and facilitates testing through Open Testing and Integration Centers (OTICs). Its standards complement 3GPP, targeting 5G and 6G ecosystems.

Short History:

Founded in February 2018 by AT&T, China Mobile, Deutsche Telekom, NTT DOCOMO, and Orange, the O-RAN Alliance was formalized as a German entity (O-RAN ALLIANCE e.V.) in August 2018. By 2020, it welcomed Rakuten Mobile and released its first Minimum Viable Plan. In 2021, the "Cherry" release advanced open software, and 2022 saw 53 new technical documents in Release 002. The 2024 Summit at MWC Barcelona highlighted AI integration and deployments, with new board members (China Telecom, SoftBank, UScellular) elected in December 2024 for 2024-2026. By 2025, the Alliance collaborated with 3GPP for 6G and transposed specifications to ATIS and ETSI standards.

Mission:

To reshape the RAN industry toward open, intelligent, virtualized, and fully interoperable mobile networks, enabling a competitive supplier ecosystem, faster innovation, and improved user experience while enhancing deployment efficiency for operators.

Aims and Objectives:

- Develop open RAN specifications for interoperable, multi-vendor solutions.
- Promote AI-driven automation via RAN Intelligent Controllers (RICs) for network optimization.
- Support open-source software development through the O-RAN Software Community.
- Facilitate global testing and integration via OTICs and PlugFests.
- Align with 3GPP and regional standards (e.g., ATIS, ETSI) for 5G and 6G ecosystems.

Funding:

Funded through membership fees from over 345 members, including 32 operators, vendors, and academic contributors. Additional revenue comes from event sponsorships (e.g., PlugFests) and grants. Governments, particularly in the U.S., Europe, and Japan, have backed O-RAN to reduce

reliance on “high-risk vendors” like Huawei. For example, the U.S. allocated $1.5 billion in 2023 for O-RAN development under the CHIPS and Science Act[60].

System of Governance (Ownership and Control):

O-RAN ALLIANCE e.V. is a non-profit governed by a 15-member Board of Directors, elected every two years by General Members (operators only). The Board, chaired by Abdurazak Mudesir (Deutsche Telekom, 2024-2026), oversees strategy, with a Technical Steering Committee (TSC) managing 11 Work Groups (WGs) and Focus Groups (FGs). Development is transparent via GitHub, adhering to WTO principles (transparency, openness, consensus). Contributors follow a consensus-based process, though founding members hold a >25% veto.

Legal Form:

Registered as a non-profit association (e.V.) under German law. The O-RAN Software Community operates under the Linux Foundation, a U.S. non-profit. Specifications are freely accessible, with contributions licensed under open terms.

Licenses Used:

O-RAN specifications are publicly available under the O-RAN ALLIANCE’s licensing terms, typically royalty-free for implementation. Software contributions (via O-RAN SC) use Apache 2.0 or MIT licenses, ensuring open use and modification.

Broader Contributors:

Over 345 members, including 32 operators (e.g., AT&T, Vodafone, Rakuten Mobile), vendors (e.g., Nokia, Ericsson, Intel), and academic institutions. The O-RAN Software Community, under the Linux Foundation, collaborates with OpenAirInterface (OAI) and Nephio. Thousands of engineers contribute via GitHub, with 41+ demos at MWC 2024. Regional standards bodies (ATIS, ETSI, TTA) and 3GPP align specifications. Community engagement occurs through PlugFests, summits, and workshops.

Broader Impact:

O-RAN fosters a competitive RAN ecosystem, reducing vendor lock-in and enabling innovations like AI-driven RIC and virtualized RANs. Deployments (e.g., Rakuten, Deutsche Telekom) show cost efficiency and scalability, with 15% of 2G-5G RAN revenue projected by 2026. Large-scale deployments in established networks, however, face challenges due to integration complexities with legacy systems. Despite progress, O-RAN deployments remain a small fraction of global RAN infrastructure, with traditional vendors still dominating. Traditional RAN vendors like Ericsson and Nokia, while publicly supporting O-RAN, have been cautious, as open architectures threaten their proprietary business models. While Huawei, a major RAN vendor excluded from many Western markets due to security concerns, does not participate in the O-RAN Alliance, limiting its applicability in markets where Huawei dominates. Challenges also include security, addressed via Zero Trust Architecture.

---

[60] Link: https://www.ntia.gov/press-release/2023/biden-harris-administration-launches-15-billion-innovation-fund-develop-more

Qualitative Impact:

O-RAN's open standards accelerate innovation, as seen in Rakuten's network-wide 5G deployment and Deutsche Telekom's Neubrandenburg rollout. AI-driven RIC optimizes energy and performance, supporting massive MIMO and network slicing. The Zero Trust Architecture enhances security. O-RAN's collaboration with 3GPP and open-source communities positions it for 6G leadership, though scaling multi-vendor interoperability remains complex.

Flagship Projects:

- Open Fronthaul Interface: Enables multi-vendor DU-RRU interoperability for 5G.
- RAN Intelligent Controller (RIC): Non-RT and Near-RT RICs for AI-driven network management.
- O-RAN Software Community: Open-source reference designs for RAN deployment.
- Certification & Badging Program: Ensures product compliance via OTICs.

Official Website:

https://www.o-ran.org

Primary Sources:

O-RAN Alliance Official Website

Description: Primary source for mission, specifications, membership, and events.

Link: https://www.o-ran.org

O-RAN Software Community

Description: Details open-source software development and alignment with O-RAN specifications.

Link: https://o-ran-sc.org

O-RAN Alliance Summit at MWC Barcelona 2025 (PR Newswire)

Description: Highlights 2024 progress, AI adoption, and 6G collaboration.

Link: https://www.prnewswire.com/news-releases/o-ran-alliance-advances-open-and-ai-driven-ran-standardization-by-setting-priorities-for-scaled-deployments-and-collaboration-towards-6g-302088803.html

Business Wire: O-RAN Alliance Leadership and Specifications

Description: Covers leadership elections, technical documents, and ecosystem growth.

Link: https://www.businesswire.com/news/home/20221116005058/en/O-RAN-ALLIANCE-Announces-New-Leadership-New-Specifications-3-Face-to-Face-Meetings-in-2023-and-Further-Alignment-with-TIP

Ericsson: O-RAN Alliance Contributions

Description: Outlines Ericsson's role and technical contributions to O-RAN specifications.

Link: https://www.ericsson.com/en/ran/open-ran

Open-Source Software Security Initiative (OS3I)

Year of Beginning: 2021

Sector: Cybersecurity, Open Source Software, National Security

Political Geography: United States. Coordinated by the White House Office of the National Cyber Director (ONCD). Global impact due to open-source software ubiquity.

Description:

The Open-Source Software Security Initiative (OS3I) is a U.S. federal interagency working group established to enhance the security of open-source software (OSS) ecosystems critical to all 16 U.S. critical infrastructure sectors. Part of the Biden-Harris National Cybersecurity Strategy (March 2023), OS3I unites federal agencies, industry, academia, and OSS communities to address systemic vulnerabilities, such as Log4Shell (2022). It focuses on memory-safe programming languages, secure software supply chains, and community engagement, guided by the Cybersecurity and Infrastructure Security Agency's (CISA) OSS Security Roadmap. OS3I's efforts include the Open-Source Software Prevalence Initiative (OSSPI)[61] and policy solutions like Software Bills of Materials (SBOMs)[62].

Short History:

OS3I was established in 2021 by ONCD and the Office of Management and Budget (OMB) to channel government resources toward OSS security. In August 2023, OS3I issued a Request for Information (RFI), receiving over 100 responses from OSS communities, shaping its 2023 End of Year Report. In March 2024, CISA hosted the OSS Security Summit, fostering public-private collaboration. The 2024 report outlined 12 activities for 2024–2025, including OSSPI, funded by the Bipartisan Infrastructure Law. By 2025, OS3I continued aligning with initiatives like the Open Source Security Foundation (OSSF) and global partners.

Mission:

To strengthen the security and resilience of the open-source software ecosystem through federal coordination, community engagement, and investment in secure development practices, ensuring national security, economic stability, and technological innovation.

Aims and Objectives:

- Unify federal agencies' approach to OSS security, fostering collaboration across sectors.
- Promote memory-safe programming languages to reduce systemic vulnerabilities.
- Enhance software supply chain security through SBOMs and secure package repositories.
- Engage OSS communities to sustain projects and improve governance.

---

[61] The Open-Source Software Prevalence Initiative (OSSPI) is a U.S. government initiative, led by the White House Office of the National Cyber Director (ONCD) and the Department of Homeland Security (DHS), aimed at enhancing the security of open-source software (OSS) used in critical infrastructure sectors such as healthcare, transportation, and energy production. Funded with $10 million from the 2021 Bipartisan Infrastructure Law, OSSPI seeks to understand the distribution and use of OSS components to strengthen national cybersecurity.

[62] A Software Bill of Materials (SBOM) is a structured list that details the components, libraries, and dependencies of a software application, including their versions and sources. It enhances transparency and security by enabling organizations to track, manage, and mitigate vulnerabilities in software supply chains.

- Invest in R&D for secure software development, including tools and frameworks.

Funding:

Funded through federal budgets, primarily via ONCD, CISA, and the Bipartisan Infrastructure Law (e.g., OSSPI). Additional support comes from agencies like the National Science Foundation (NSF) and the Defense Advanced Research Projects Agency (DARPA).

System of Governance (Ownership and Control):

Managed by ONCD in collaboration with OMB, CISA, NSF, DARPA, NIST[63], and other agencies. OS3I operates as an interagency working group with no independent legal entity, guided by the National Cybersecurity Strategy. Community input is solicited via RFIs and summits, but critics note limited representation from grassroots OSS developers. Governance emphasizes public-private partnerships, with contributions managed through platforms like GitHub (e.g., usncd/oss-security). Policies align with WTO principles, though some argue corporate influence overshadows community voices.

Legal Form:

OS3I is a federal initiative under ONCD, operating within U.S. government frameworks, not a standalone legal entity. Outputs (e.g., reports and tools) use open licenses like CC-BY 4.0 or Apache 2.0 for accessibility, though policy implementation is government-driven.

Licenses Used:

Reports and documentation use Creative Commons CC-BY 4.0 or public domain licenses. Software contributions (e.g., CISA's open-source code) use Apache 2.0 or MIT licenses, aligning with OSS community standards. Package repositories (e.g., PyPI, Maven Central) adopt secure practices like Sigstore and Trusted Publishing.

Broader Contributors:

Includes federal agencies (CISA, NSF, DARPA, NIST), industry, academia, and OSS organizations (e.g., OSSF, Python Software Foundation, Rust Foundation). Over 100 RFI responses came from nonprofits, individuals, and researchers. Events like the OSS Security Summit (March 2024) and OSSF's SOSS Summit (2023) engaged hundreds. Critics highlight minimal involvement from grassroots FOSS communities, with corporate and government voices dominating.

Broader Impact:

OS3I strengthens OSS security, which is critical for infrastructure like healthcare and energy, by promoting memory-safe languages and SBOMs. Initiatives like OSSPI enhance visibility into OSS usage, reducing risks from vulnerabilities like Log4Shell. However, decentralized OSS development and underfunded maintainers pose challenges. Critics argue OS3I's corporate tilt risks "openwashing," sidelining FOSS principles. Globally, its alignment with OSSF and memory safety efforts influences secure software practices, though adoption varies.

---

[63] NIST is the National Institute of Standards and Technology, a U.S. government agency under the Department of Commerce.

Qualitative Impact:

OS3I's focus on memory-safe languages and supply chain security addresses ~70% of vulnerabilities tied to memory-unsafe code (e.g., C/C++). Its collaborative approach, via RFIs and summits, fosters trust, but limited FOSS representation raises concerns about corporate-driven priorities. Initiatives like Sigstore and Trusted Publishing enhance repository security, benefiting millions of developers. However, underfunded maintainers and decentralized OSS governance remain hurdles. OS3I's global influence via OSSF and CISA's roadmap sets a precedent for secure software, though critics urge more inclusive community engagement.

Flagship Projects:

- Open-Source Software Prevalence Initiative (OSSPI): Maps OSS use in critical infrastructure ($10M, 2024).
- CISA OSS Security Roadmap: Guides risk management with 4 goals (unify, harden, measure, secure).
- Memory-Safe Programming Advocacy: Promotes Rust and Python to reduce vulnerabilities.
- Principles for Package Repository Security: Framework for secure repositories (with OSSF).

Official Website:

https://www.whitehouse.gov/oncd/ (OS3I-specific page unavailable; managed under ONCD)

Primary Sources:

White House ONCD: OS3I 2023 End of Year Report

Description: Details OS3I's mission, focus areas, and 2023 progress.

Link: https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/01/Securing-the-Open-Source-Software-Ecosystem-OS3I-End-of-Year-Report-MASTERCOPY.pdf

CISA: Open Source Software Security

Description: Outlines CISA's OSS Security Roadmap and summit outcomes.

Link: https://www.cisa.gov/resources-tools/resources/cisa-open-source-software-security-roadmap

Federal Register: OS3I RFI (2023)

Description: Details RFI process, focus areas, and community engagement.

Link: https://www.federalregister.gov/documents/2023/08/10/2023-17102/request-for-information-on-open-source-software-security-areas-of-long-term-focus-and-prioritization

OSSF: OS3I RFI Response

Description: OSSF's contributions to OS3I emphasizing community and memory safety.

Link: https://OSSF.org/blog/2023/11/08/OSSF-responds-to-us-federal-government-rfi-on-open-source-software-security/

Techrights: OS3I Critique

Description: Critiques OS3I's corporate tilt and limited FOSS involvement.

Link:
https://techrights.org/n/2024/02/01/Open_Source_Software_Security_Initiative_OS3I_Has_Nothing_to_Do.shtml

Risc-V International

Year of Beginning: 2010 (Risc-V project); 2015 (Risc-V Foundation); 2020 (Risc-V International)

Sector: Computer Architecture, Open Source Hardware, Instruction Set Architecture (ISA)

Political Geography: Global (headquartered in Zug, Switzerland)

Description:

Risc-V International is a global non-profit organization managing the Risc-V open standard instruction set architecture (ISA), a royalty-free, modular, and extensible ISA based on reduced instruction set computing (RISC) principles. Initiated at UC Berkeley in 2010, Risc-V enables customizable processor designs for applications from IoT devices to supercomputers. The organization fosters collaboration among 4,000+ members across 70 countries, developing specifications, tools, and ecosystems to drive innovation, reduce costs, and promote digital sovereignty by avoiding proprietary ISA licensing.

Short History:

Risc-V began in 2010 at UC Berkeley's Parallel Computing Laboratory, aiming to create a free, open ISA. The first specification was published in 2011 under a Creative Commons license. In 2015, the Risc-V Foundation was formed with over 36 members, including Google, Nvidia, and IBM. In 2020, it reincorporated as Risc-V International in Switzerland for neutrality, avoiding U.S. regulatory concerns. By 2023, over 10 billion Risc-V cores had shipped.

Mission:

To advance processor innovation through an open standard Risc-V ISA, enabling a collaborative, royalty-free ecosystem for software and hardware development across diverse applications, fostering design freedom and global interoperability.

Aims and Objectives:

- Maintain and develop the Risc-V ISA as a free, open standard for global adoption.
- Promote modularity and customization for applications from embedded systems to AI and automotive.
- Foster a collaborative ecosystem through technical working groups and community contributions.
- Support software portability and hardware innovation via standardized specifications and tools.
- Ensure neutrality and accessibility by avoiding proprietary restrictions and licensing fees.

Funding:

Primarily funded through membership fees, with free Community Membership for individuals, academics, and non-profits. Additional revenue comes from events, certifications, and training (e.g., Risc-V Fundamentals Exam).

System of Governance (Ownership and Control):

Risc-V International operates as a non-profit with a Board of Directors elected by members, overseeing strategy and neutrality. Technical Working Groups, led by contributors, develop and ratify specifications via a transparent, meritocratic process. Profiles ensure interoperability[64], and members vote on changes. The ISA is public domain (encoding) or Creative Commons/BSD-licensed (documents), allowing free use while encouraging community contributions.

Legal Form:

Non-profit association under Swiss law, incorporated in Zug, Switzerland.

Licenses Used:

Risc-V ISA specifications are under Creative Commons Attribution 4.0 International or BSD licenses. The ISA encoding is effectively public domain, with no patents filed. Implementations (e.g., CPU designs) may be open (e.g., MIT, Apache 2.0) or proprietary, per developer choice.

Broader Contributors:

Over 4,000 members across 70 countries, including companies (e.g., Google, Intel, Nvidia, SiFive), universities (e.g., UC Berkeley, MIT), and individuals. Contributors participate via Technical Working Groups, open-source projects (e.g., GCC, LLVM), and collaborations with groups like OpenHW Group and CHIPS Alliance. Thousands of developers globally contribute to Risc-V software and hardware.

Several governments support Risc-V's open-standard model to enhance national semiconductor capabilities, driven by strategic goals like technological independence, cost reduction, and innovation in AI, automotive, and high-performance computing. The Chinese government is heavily promoting Risc-V to reduce dependency on Western semiconductor technologies amid U.S. export controls[65]. The U.S. government, particularly through DARPA, has supported Risc-V **for** its cost-effectiveness and flexibility in defense applications. However, concerns about China's use of Risc-V have led to calls from U.S. lawmakers (e.g., House Select Committee on the CCP in 2023) to explore restrictions, though no bans have been implemented due to Risc-V's open nature. The EU is investing in Risc-V to reduce reliance on foreign semiconductor technologies. The Barcelona Supercomputing Center leads initiatives like the European Processor Initiative and Open Chip to develop Risc-V-based processors for high-performance computing and other applications, driven by concerns over supply chain security. India's DIR-V program supports Risc-V to foster self-reliance in semiconductors, reducing risks from sanctions or supply chain disruptions, particularly for applications in AI and defense. The Japanese government funds Risc-V development through the

---

[64] Risc-V profiles are standardized sets of ISA features (extensions and instructions) designed to meet the needs of specific application domains, such as embedded systems, application processors, or microcontrollers. Risc-V's flexibility allows designers to customize the ISA by selecting specific extensions, but this can lead to a "combinatorial explosion" of possible configurations. Profiles address this by defining a common, smaller subset of ISA features that ensures that software written for a specific profile (e.g., RVA23 for 64-bit application processors) will run on any Risc-V hardware compliant with that profile, promoting compatibility between hardware and software.

[65] In 2025, Chinese bodies like the Cyberspace Administration and Ministry of Industry and Information Technology are reportedly developing guidelines to encourage nationwide Risc-V adoption. The Beijing Institute of Open Source Chip supports projects like XiangShan, a high-performance Risc-V processor initiative. Hong Kong is also promoting Risc-V to establish itself as an IC design hub, complementing China's efforts.

Leading-edge Semiconductor Technology Center, collaborating with U.S. firm Tenstorrent to create Risc-V-based chips for edge AI accelerators, aiming to strengthen its semiconductor ecosystem.

Broader Impact:

Risc-V democratizes processor design, reducing costs and barriers via royalty-free licensing, enabling innovation in IoT, AI, automotive, and HPC. Over 10 billion cores shipped by 2023, with major Linux-based operating systems—Linux kernel, Debian, and Fedora—having integrated support for Risc-V, specifically the 64-bit variant (riscv64), enabling these systems to run on Risc-V hardware. Risc-V promotes digital sovereignty by offering an alternative to proprietary ISAs (e.g., ARM, x86). Concerns exist in USA about China's adoption potentially bypassing U.S. export controls.

Qualitative Impact:

Risc-V fosters innovation by enabling customizable, low-cost processor designs, empowering startups, academia, and emerging markets. Its open standard promotes collaboration, as seen in projects like SiFive's HiFive1 and Renesas' RZ/Five. It enhances energy efficiency and performance in devices, but faces challenges in high-end applications and U.S. policy concerns over China's involvement. The ecosystem's growth signals a shift toward open hardware standards.

Flagship Projects[66]:

- SiFive HiFive Boards: Arduino-compatible dev kits with Risc-V SoCs (e.g., FE310).
- Renesas RZ/Five: 64-bit Risc-V MPUs for IoT gateways.
- Risc-V Software Ecosystem (RISE): Accelerates software for consumer electronics, automotive, and datacenters.
- OpenSBI: Reference Supervisor Binary Interface for Risc-V systems.

Official Website:

https://riscv.org

Primary Sources:

Risc-V International Official Website

Description: Main source for Risc-V's mission, governance, specifications, and membership.

Link: https://riscv.org

Risc-V Instruction Set Manual (GitHub)

Description: Source for ISA specifications, licenses, and technical details (e.g., memory model, registers).

Link: https://github.com/riscv/riscv-isa-manual

Wikipedia: Risc-V

Description: Comprehensive overview of Risc-V's history, software support, and ecosystem.

---

[66] Risc-V International does not produce chips or software, only standards; implementations are by members (e.g., SiFive, Renesas).

Link: https://en.wikipedia.org/wiki/Risc-V

Risc-V International: Understanding Risc-V

Description: Details on Risc-V's evolution, technical aspects, and community.

Link: https://riscv.org/news/2023/11/understanding-Risc-V-the-open-standard-instruction-set-architecture-Risc-V-international/

Wevolver: Risc-V Architecture Guide

Description: Technical overview of Risc-V's design principles and applications.

Link: https://www.wevolver.com/article/Risc-V-architecture-a-comprehensive-guide-to-the-open-source-isa

CSIS: Risc-V and Chip Development

Description: Analysis of Risc-V's geopolitical implications and adoption.

Link: https://www.csis.org/analysis/what-Risc-V-means-future-chip-development

Rust

Year of Beginning: 2006 (public release in 2010)

Sector: Programming Languages, Open Source Software, Systems Programming

Political Geography: Global (initiated by Mozilla, U.S.-based; developed by a worldwide community)

Description:

Rust is an open-source systems programming language designed for performance, safety, and handling multiple tasks at once. It keeps programs safe from memory errors without needing extra software to manage memory, and it stops common problems like crashes from bad pointers or issues when tasks share data. Rust is used in projects like Mozilla Firefox, Dropbox, and Microsoft Windows, and powers critical infrastructure, including Linux kernel components. Maintained by the Rust Project and a global community, supported by the Rust Foundation, its open-source nature encourages contributions via GitHub, with regular releases enhancing features and ecosystem tools like Cargo (package manager).

Short History:

Rust was created in 2006 by Graydon Hoare as a personal project, with Mozilla sponsoring development from 2009. The first public release, Rust 0.1, came in 2010. Rust 1.0, the first stable version, launched in 2015, establishing it as production-ready. The Rust Foundation, a non-profit, was formed in 2021 to provide a legal arm to the community, backed by Platinum members like AWS, Google, Huawei, Microsoft, and Mozilla. By 2025, Rust is a top choice for systems programming, with growing adoption in web, cloud, and embedded systems, and over 2.5 million users.

Mission:

To empower developers to build reliable, high-performance software through a safe, concurrent, and open-source programming language, fostering a collaborative and inclusive global community.

Aims and Objectives:

- Ensure memory and thread safety to eliminate common programming errors.
- Maintain an open-source, community-driven development model via GitHub.
- Enhance tooling (e.g., Cargo, rustup) for developer productivity.
- Promote adoption across industries, from systems to web and embedded programming.
- Support education and diversity through community events, tutorials, and outreach.

Funding:

Most of the development is made by volunteers and participants in the Rust Project community. Funding is organized through the Rust Foundation via donations, corporate sponsorships (e.g., AWS, Microsoft), and membership fees from organizations. Additional revenue comes from events like RustConf and grants.

System of Governance (Ownership and Control):

The Rust Project is led by the Leadership Council composed by representatives of the main areas of development. The Rust project is organized by informal meritocratic principles. The Rust Project, led by core teams (e.g., Compiler, Language, Library), oversees technical development. Decisions are made via a consensus-based process, with Requests for Comments (RFCs) on GitHub ensuring transparency. The community, including thousands of contributors, drives development, with leadership teams elected or appointed based on merit.

The Rust Foundation is a U.S.-based 501(c)(6) non-profit, with a Board of Directors composed of 5 representatives from members companies (e.g., AWS, Microsoft) and 5 representatives from the Rust Project.

Legal Form:

Rust is an open-source project, developed and maintained by the informal Rust Project community, legally supported by the Rust Foundation, a U.S. 501(c)(6) non-profit. The language and its tools are freely available under open-source licenses.

Licenses Used:

Rust's source code, including the compiler and standard library, is dual-licensed under the MIT License and Apache License 2.0, allowing flexible use and modification. Documentation uses Creative Commons Attribution 4.0 (CC BY 4.0). Crates (libraries) on Cargo typically use MIT or Apache 2.0.

Broader Contributors:

Includes the Rust Project core teams, the Rust Foundation, and a global community of over 2.5 million developers (2024 Stack Overflow survey). Major contributors include Mozilla, AWS, Microsoft, and Google, alongside individual developers and academics. The Rust Project collaborates with organizations like the Linux Foundation for kernel integration. Community engagement occurs through RustConf, local meetups, and online forums like Discord and the Rust Users Forum.

U.S. government agencies – like the White House Office of the National Cyber Director (ONCD), the National Security Agency (NSA), and the Cybersecurity and Infrastructure Security Agency (CISA) - are actively promoting Rust adoption for secure software development. Internationally, Germany's government-backed Sovereign Tech Fund has advocated for Rust in open-source infrastructure to enhance digital sovereignty and security.

Broader Impact:

Rust has transformed systems programming by offering safety without sacrificing performance, influencing projects like Firefox, Windows, and the Linux kernel. Its adoption in cloud (e.g., AWS Lambda), web (e.g., Actix), and embedded systems highlights versatility. The 2024 Stack Overflow survey ranked Rust as the "most loved" language for nine consecutive years. Challenges include a steep learning curve and slower compilation times, but its ecosystem (Cargo, crates.io) drives innovation. Rust's focus on inclusivity fosters a diverse community, though scaling governance for its growing user base remains complex.

Qualitative Impact:

Rust's memory safety guarantees have reduced vulnerabilities in critical software, as seen in Microsoft's adoption for Windows and Azure. Its concurrency model enables scalable systems, powering Dropbox's backend and Discord's infrastructure. The Cargo ecosystem simplifies dependency management, accelerating development. Community initiatives like RustBridge and Rust All Hands promote diversity and education. However, adoption in legacy systems is slow due to retraining needs, and competition from languages like Go persists.

Flagship Projects:

- Cargo: Package manager and build system for Rust projects.
- rustc: Rust's compiler, ensuring memory-safe code generation.
- crates.io: Central repository for Rust libraries and frameworks.
- Async Rust: Asynchronous programming support via async/await for high-performance applications.

Official Website:

https://www.rust-lang.org

Primary Sources:

Rust Official Website

Description: Primary source for documentation, downloads, and community resources.

Link: https://www.rust-lang.org

Rust Foundation Website

Description: Details governance, funding, and community programs.

Link: https://foundation.rust-lang.org

Rust GitHub Repository

Description: Source code, RFCs, and contribution guidelines.

Link: https://github.com/rust-lang/rust

Stack Overflow Developer Survey 2024

Description: Metrics on Rust's adoption and developer sentiment.

Link: https://survey.stackoverflow.co/2024/

Rust Blog

Description: Updates on releases, features, and community events.

Link: https://blog.rust-lang.org

scikit-learn

Year of Beginning: 2007 (initiated); 2012 (first public release)

Sector: Machine Learning, Open Source Software, Data Science

Political Geography: Global (no formal headquarters; managed by a distributed community, with significant contributions from Inria, France)

Description:

scikit-learn (also known as sklearn) is a free, open-source machine-learning library for Python designed for data mining, data analysis, and model building. It is a critical ML library used by millions worldwide. It provides a consistent API for supervised and unsupervised learning, featuring algorithms for classification, regression, clustering, dimensionality reduction, and more (e.g., support vector machines, random forests, k-means). It supports preprocessing, model evaluation, and visualization, integrating seamlessly with Python libraries like Pandas and plotly. As a NumFOCUS fiscally sponsored project[67], scikit-learn is widely used in academia, industry, and research for its simplicity and performance.

Short History:

scikit-learn began in 2007 as a Google Summer of Code project by David Cournapeau, initially named *scikits.learn*, a SciPy Toolkit extension. Inria's involvement began in 2010. In that same year there was the first public release (v0.1 beta, February 2010). Version 1.0, released in September 2021, marked 14 years of development with enhanced stability. The latest version, 1.6.1 (January 2025), supports Python 3.8+ and includes performance improvements. The project has over 30 active contributors and is maintained by volunteers. The France 2030 AI strategy, launched in November 2021, provides funding to Inria and open-source AI resources and indirectly supports scikit-learn development and adoption.

Mission:

To provide a simple, efficient, and open-source machine learning library for Python that enables practitioners to build, evaluate, and deploy robust models for diverse applications, fostering accessibility and innovation in data science.

Aims and Objectives:

- Offer a consistent, user-friendly API for a wide range of machine learning algorithms.
- Support preprocessing, model tuning, and evaluation for efficient workflows.
- Integrate with Python's scientific ecosystem for interoperability.
- Promote open science and reproducibility through transparent, well-documented tools.
- Maintain an active community for continuous updates, bug fixes, and contributions.

[67] NumFOCUS is a 501(c)(3) nonprofit organization based in Austin, Texas, founded in 2012 to promote open practices in research, data, and scientific computing. Its mission is to support open source software for scientific discovery through fiscal sponsorship of projects and community-driven educational programs.

Funding:

Primarily funded through NumFOCUS fiscal sponsorship, donations, and institutional support (e.g., Inria, Google, Python Software Foundation). Additional revenue comes from grants and corporate sponsorships (e.g., Tinyclues).

System of Governance (Ownership and Control):

scikit-learn is a community-driven project under NumFOCUS with no formal ownership. A core team of volunteers, including Gaël Varoquaux and Andreas Mueller, oversees the development, guided by a meritocratic process. Decisions are made transparently via GitHub discussions and enhancement proposals. Contributors follow a Development Guide, and the project adheres to the Python Software Foundation's Code of Conduct. The codebase is fully open, with no proprietary restrictions.

Legal Form:

No independent legal entity; scikit-learn is a NumFOCUS fiscally sponsored open-source project, operating under U.S. non-profit law and the 3-Clause BSD license.

Licenses Used:

Distributed under the 3-Clause BSD license, ensuring free use, modification, and distribution. Documentation uses Creative Commons-compatible licenses where applicable. Core algorithms in Cython (e.g., SVM via LIBSVM) are also BSD-compliant, maintaining open access.

Broader Contributors:

Over 2,000 contributors on GitHub, including academics, data scientists, and engineers from organizations like Inria, Google, and Microsoft. Users span industries (e.g., Mendeley, Evernote, Telecom ParisTech) and academia, with millions of downloads via PyPI. Community engagement occurs through GitHub, forums, and events like SciPy conferences.

Broader Impact:

scikit-learn is a cornerstone of Python-based machine learning, used by millions for research, industry, and education. It democratizes access to advanced algorithms, enabling applications in finance, healthcare, and neuroimaging. Its consistent API and extensive documentation lower barriers for beginners, while its performance suits production systems. The library's popularity on GitHub (one of the top ML repositories in 2019) reflects its global influence, though it's less suited for deep learning or large-scale datasets compared to TensorFlow or PyTorch.

Qualitative Impact:

scikit-learn simplifies machine learning, making it accessible to novices and experts. The active community ensures regular updates and robust documentation, fostering trust and adoption. Limitations include a lack of deep learning support and challenges with very large datasets, but integration with libraries like Joblib addresses scalability. Its open-source nature promotes equity in data science education.

Flagship Projects:

- Pipeline Utility: Chains preprocessing and modeling for reproducible workflows.
- RandomForestClassifier: Widely used for classification tasks, e.g., iris dataset.
- GridSearchCV: Automates hyperparameter tuning for model optimization.
- LabelEncoder: Converts categorical data to numerical for preprocessing.

Official Website:

https://scikit-learn.org

Primary Sources:

scikit-learn Official Website

Description: Primary source for mission, documentation, tutorials, and updates.

Link: https://scikit-learn.org

scikit-learn GitHub Repository

Description: Hosts source code, contributor details, and development guide.

Link: https://github.com/scikit-learn/scikit-learn

PyPI: scikit-learn

Description: Details release history, dependencies, and licensing.

Link: https://pypi.org/project/scikit-learn/

NumFOCUS: scikit-learn

Description: Outlines fiscal sponsorship and funding model.

Link: https://numfocus.org/project/scikit-learn

Signal Foundation

Year of Beginning: 2013

Sector: Cryptography, Secure Communication, Open Source Software

Political Geography: Global (developed by Open Whisper Systems, now Signal Messenger, based in the U.S.; used worldwide)

Description:

The Signal Protocol is an open-source cryptographic protocol designed for end-to-end encrypted messaging, ensuring secure, private communication across applications. It combines the Double Ratchet Algorithm, Extended Triple Diffie-Hellman (X3DH) key agreement, and AES-256 encryption to provide forward secrecy, backward secrecy, and authentication. Widely adopted by messaging apps like Signal, WhatsApp, and Skype, it powers secure communication for billions of users. The protocol is maintained by Signal Messenger, a non-profit, and its open-source nature allows community contributions and audits.

Short History:

Developed in 2013 by Open Whisper Systems (founded by Moxie Marlinspike and Trevor Perrin), the Signal Protocol evolved from earlier protocols like TextSecure and RedPhone. By 2014, it was integrated into the Signal app. In 2015, WhatsApp adopted the protocol, followed by Facebook Messenger, Skype, and Google Allo (in specific modes). The 2018 formation of the Signal Foundation formalized its non-profit governance. By 2025, the protocol remains a gold standard for secure messaging, with ongoing updates to counter quantum computing threats.

Mission:

To provide a secure, open-source cryptographic framework for end-to-end encrypted communication, ensuring privacy, security, and accessibility for global users while fostering trust through transparency and community collaboration.

Aims and Objectives:

- Develop and maintain a robust, open-source cryptographic protocol for secure messaging.
- Ensure forward and backward secrecy to protect user communications against future breaches.
- Promote adoption by major messaging platforms to maximize privacy impact.
- Support community audits and contributions to maintain transparency and security.
- Adapt the protocol to emerging threats, including quantum computing.

Funding:

Funded primarily through the Signal Foundation, a 501(c)(3) non-profit, via donations, grants, and individual contributions. Key early funding included support from the Open Technology Fund[68] and a loan from Brian Acton (WhatsApp co-founder) in 2018.

System of Governance (Ownership and Control):

Managed by Signal Messenger (under the Signal Foundation), a U.S.-based non-profit. Development is led by a small core team, with Moxie Marlinspike as a key figure until 2022. The protocol's open-source nature allows community contributions via GitHub, with changes reviewed by Signal's team. Governance emphasizes transparency, with public code audits and no formal board for protocol decisions. Contributions follow open-source principles, ensuring community-driven improvements.

Legal Form:

The Signal Protocol is an open-source project under the Signal Foundation, a U.S. 501(c)(3) non-profit. Code and documentation are freely available under open-source licenses.

Licenses Used:

The protocol's source code is released under the GNU Affero General Public License v3.0 (AGPLv3), allowing free use, modification, and distribution with the requirement to share derivative source code. Documentation uses Creative Commons Attribution 4.0 (CC BY 4.0).

Broader Contributors:

Includes Signal Messenger's core team, independent cryptographers, and open-source developers contributing via GitHub. Major adopters (e.g., WhatsApp, Microsoft, Google) integrate the protocol but do not directly contribute to its development. Security researchers and organizations like the Open Technology Fund provide audits and feedback. Community engagement occurs through public code repositories and cryptographic conferences.

Broader Impact:

The Signal Protocol has transformed secure communication, enabling end-to-end encryption for over 2 billion users via apps like WhatsApp and Signal. It sets a benchmark for privacy, influencing industry standards and government policies on encryption. Its open-source nature fosters trust through audits, though adoption faces challenges in regions with restrictive internet policies, as in China where Signal is banned. The protocol's lightweight design ensures scalability, but quantum computing poses future challenges, prompting research into post-quantum cryptography.

---

[68]The Open Technology Fund (OTF) is an American nonprofit corporation that "support open technologies and communities that increase free expression, circumvent censorship, and obstruct repressive surveillance as a way to promote human rights and open societies." Until its formation as an independent entity, the Open Technology Fund had operated as a program of Radio Free Asia. As of November 2019, the Open Technology Fund became an independent nonprofit corporation and a grantee of the U.S. Agency for Global Media. The OTF has funded digital privacy and security technology, including The Tor Project, Signal, and other encryption projects.
(Source: https://en.wikipedia.org/wiki/Open_Technology_Fund)

Qualitative Impact:

The Signal Protocol has redefined secure messaging by making end-to-end encryption accessible to billions, protecting user privacy in personal and sensitive communications. Its adoption by major platforms amplifies its impact, while open-source availability ensures transparency and trust. The protocol's design influences emerging standards for secure IoT and group messaging. However, resistance from governments seeking backdoors and the need for quantum-resistant updates pose ongoing challenges.

Flagship Projects:

- Double Ratchet Algorithm: Ensures forward and backward secrecy for asynchronous messaging.
- X3DH Key Agreement: Facilitates secure key exchange for initiating encrypted sessions.
- Signal App Integration: Reference implementation showcasing the protocol's capabilities.
- Group Messaging Encryption: Extended protocol for secure multi-user chats.

Official Website:

https://signal.org

Primary Sources:

Signal Foundation Official Website

Description: Primary source for protocol details, Signal app, and mission.

Link: https://signal.org

Signal Protocol GitHub Repository

Description: Source code and technical documentation for the protocol.

Link: https://github.com/signalapp/libsignal

Whisper Systems Blog

Description: Historical details on protocol development and early adoption.

Link: https://signal.org/blog/

Open Technology Fund: Signal Support

Description: Details funding and development support for the protocol.

Link: https://www.opentech.fund/projects-we-support/supported-projects/signal-open-whisper-systems/

Simpl

Year of Beginning: 2022

Sector: Open Source Software, Data Interoperability, Cloud Computing

Political Geography: European Union (headquartered in Brussels, Belgium; supports EU-wide data initiatives)

Description:

Simpl is an open-source, secure middleware platform developed by the European Commission to enable data access and interoperability across Common European Data Spaces. It supports cloud-to-edge federations, ensuring secure, scalable, and modular data sharing for sectors like health, science, and public procurement. Comprising three components—Simpl-Open (open-source software stack), Simpl-Live (deployments in specific data spaces), and Simpl-Labs (testing environment)—it promotes transparency, data sovereignty, and compliance with EU regulations. Simpl is funded through the DIGITAL Europe Program and collaborates with initiatives like Gaia-X and the Data Spaces Support Centre.

Short History:

Initiated in 2022 following a European Commission presentation of its vision on May 30, 2022, Simpl aligns with the European Data Strategy to foster interoperable data ecosystems. In 2023, a €150 million framework contract was awarded to two consortia, led by Eviden Belgium, to develop Simpl-Open. A proof-of-concept and source code repository were released in June 2024, with a Minimum Viable Product (MVP) planned for late 2024. By 2025, Simpl supports projects like Destination Earth and the European Open Science Cloud, with a new website launched to share progress and engage the community.

Mission:

To provide a smart, secure, and open-source middleware platform that enables seamless data sharing and interoperability across European data spaces, empowering businesses, governments, and researchers while upholding EU values of data sovereignty, privacy, and fair markets.

Aims and Objectives:

- Develop an open-source middleware stack (Simpl-Open) to power data spaces and cloud-to-edge federations.
- Deploy Simpl-Live instances in sectoral data spaces (e.g., European Health Data Space, Destination Earth).
- Provide Simpl-Labs for prototyping and testing interoperability with open-source software.
- Ensure data sovereignty and compliance with EU regulations (e.g., GDPR, Data Act).
- Foster community collaboration through open repositories and alignment with initiatives like Gaia-X.

Funding:

Funded through the DIGITAL Europe Program. Additional funding supports administrative services and Simpl-Labs. Contributions come from EU budgets, with no direct reliance on private donations or commercial revenue.

System of Governance (Ownership and Control):

Managed by the European Commission's Directorate-General for Communications Networks, Content and Technology (DG CONNECT). Development is led by a consortium headed by Eviden Belgium, including Aruba, Capgemini, IONOS, and COSMOTE Global Solutions. Governance is transparent, with Simpl-Open's codebase hosted on a self-hosted GitLab instance for community contributions. The Data Spaces Support Centre defines requirements, ensuring alignment with EU standards. A Program Support Office oversees coordination, with community feedback integrated via open repositories and forums.

Legal Form:

Simpl is an open-source project under the European Commission, not a standalone legal entity. It operates within the DIGITAL Europe Program framework, with software released under open-source licenses to ensure public access and modification.

Licenses Used:

Simpl-Open uses OSI-approved open-source licenses (e.g., Apache 2.0, MIT), though specific licenses are not yet detailed in public documentation. Documentation is expected to use Creative Commons Attribution 4.0 (CC BY 4.0). The open-source model ensures transparency and allows modification and distribution without proprietary restrictions.

Broader Contributors:

Led by the Eviden Belgium consortium (Aruba, Capgemini, IONOS, COSMOTE Global Solutions). Collaborators include Gaia-X, the Data Spaces Support Centre, and open-source communities. Stakeholders from sectoral data spaces (e.g., European Health Data Space, European Open Science Cloud) provide requirements and feedback. Community engagement occurs through GitLab repositories, the Simpl website, and events like the Data Spaces Symposium.

Broader Impact:

Simpl enables interoperable data ecosystems, supporting EU priorities like digital sovereignty and the data economy. It powers initiatives like Destination Earth and the European Health Data Space, facilitating secure data sharing for research, governance, and industry. Its open-source model fosters transparency and community-driven innovation, though challenges include ensuring interoperability across diverse data spaces and managing stakeholder coordination. Simpl's alignment with EU regulations strengthens trust, but its early-stage development limits widespread adoption as of 2025.

Qualitative Impact:

Simpl advances EU data sovereignty by enabling secure, interoperable data sharing across sectors, reducing reliance on proprietary platforms. Its modular design supports customization, while its green focus monitors environmental performance. Integration with Gaia-X and other standards ensures compatibility, though complexity in aligning diverse data spaces poses challenges. Simpl's open-source approach encourages innovation, but its success depends on community adoption and robust governance to scale across EU initiatives.

Flagship Projects:

Simpl-Open: Open-source middleware stack for data space interoperability.

Simpl-Live: Deployments in six sectoral data spaces (e.g., European Open Science Cloud, Public Procurement Data Space).

Simpl-Labs: Testing environment for prototyping and assessing interoperability.

Integration with Gaia-X: Aligns Simpl with EU cloud federation standards.

Official Website:

https://simpl-programme.ec.europa.eu

Primary Sources:

Simpl Program Official Website

Description: Primary source for mission, components, and development updates.

Link: https://simpl-programme.ec.europa.eu

European Commission: Simpl Overview

Description: Details Simpl's role in data spaces and funding via DIGITAL Europe.

Link: https://digital-strategy.ec.europa.eu/en/policies/simpl

Hostingjournalist: Simpl-Open Contract Announcement

Description: Outlines the €41 million contract and consortium details.

Link: https://hostingjournalist.com/news/eu-simpl-middleware-platform-tender-winners-revealed

Simpl Program: Architecture Documentation

Description: Technical details on Simpl-Open's architecture and community involvement.

Link: https://simpl-programme.ec.europa.eu/book-page/simpl-open-architecture

Data Spaces Symposium 2025

Description: Event for Simpl and data space stakeholder engagement.

Link: https://www.data-spaces-symposium.eu

Sovereign Tech Fund (now part of Sovereign Tech Agency)

Year of Beginning: 2022

Sector: Open Source Software, Cybersecurity, Digital Infrastructure

Political Geography: Germany (global investment focus, headquartered in Leipzig)

Description:

The Sovereign Tech Fund (STF), a program under the Sovereign Tech Agency, invests in open-source software (OSS) to strengthen digital infrastructure critical to Germany and Europe's competitiveness, innovation, and digital sovereignty. It supports foundational technologies like libraries, package managers, and encryption tools, focusing on security, resilience, and sustainability. STF addresses the "free-rider" problem in OSS by funding maintenance and development, preventing over-reliance on unpaid maintainers and enhancing cybersecurity across sectors.

Short History:

Initiated in 2021 via a feasibility study by Adriana Groh and Fiona Krakenbürger, STF was established in May 2022 with funding from the German Federal Ministry for Economic Affairs and Climate Action (BMWK). Launched as a pilot under SPRIND (Federal Agency for Disruptive Innovation), it began with €3.5 million, growing to €11.5 million in 2023. In 2024, STF transitioned into the Sovereign Tech Agency, a permanent SPRIND subsidiary, expanding programs like Sovereign Tech Resilience and Fellowships. Over €23.5 million has been invested in 60+ technologies, including Samba and OpenStreetMap.

Mission:

To sustainably strengthen the open-source ecosystem by investing in foundational digital technologies, focusing on security, resilience, technological diversity, and the people behind the code, to ensure digital sovereignty and innovation.

Aims and Objectives:

- Fund maintenance and development of critical OSS to enhance security and stability.
- Address vulnerabilities in digital infrastructure (e.g., Log4j, Heartbleed) to mitigate risks.
- Promote digital sovereignty by reducing dependency on proprietary systems.
- Support maintainers and communities through funding, fellowships, and resilience programs.
- Foster innovation in sectors like healthcare, education, and industry by securing OSS dependencies.

Funding:

Funded by the BMWK through SPRIND. Funding is time-limited, targeting specific challenges or vulnerabilities, and does not overlap with other public grants.

System of Governance (Ownership and Control):

STF operates under the Sovereign Tech Agency, a SPRIND subsidiary. Governed by co-CEOs Adriana Groh and Luisa von Beust, with Fiona Krakenbürger as CTO, Investments are selected based on criteria like prevalence, societal relevance, and vulnerability, with input from external experts. Proposals are reviewed for feasibility and impact, ensuring transparency and alignment with public interest.

Legal Form:

Subsidiary of SPRIND, a public entity under German law, operating as a funding program with no independent non-profit status.

Licenses Used:

STF requires funded projects to use OSI-approved or FSF Free/Libre licenses (e.g., MIT, Apache 2.0) for code, and Creative Commons-like licenses for documentation without non-commercial or no-derivative clauses, ensuring free reuse and redistribution.

Broader Contributors:

Engages global OSS communities, including maintainers, developers, and organizations like the OpenJS Foundation and OpenStreetMap. Over 500 project submissions since 2023, with contributors from startups, NGOs, and research bodies. Funded projects involve thousands of developers worldwide.

Broader Impact:

STF strengthens digital sovereignty by securing OSS critical to 97% of global software, reducing risks from vulnerabilities like Log4j. It enhances competitiveness for startups and SMEs, supports innovation in sectors like healthcare and energy, and promotes a resilient digital commons. Its model influences global OSS funding strategies, though critics note its scale remains small compared to ecosystem needs.

Qualitative Impact:

STF empowers maintainers, often unpaid, by providing financial and structural support, addressing the free-rider problem. It enhances trust in OSS through security improvements (e.g., Samba's SMB over QUIC) and fosters innovation by securing foundational tools. Its focus on diversity and sustainability strengthens community resilience, though some argue its funding is insufficient for systemic change.

Flagship Projects:

- Samba: €688,800 to enhance security, scalability, and Unix compatibility.
- OpenStreetMap: Funding for code modernization and infrastructure improvements.
- gfortran: €360,000 for parallel computing in climate modelling and AI.
- OpenJS Foundation: Support for JavaScript ecosystem security.

Official Website:

https://www.sovereign.tech

Primary Sources:

Sovereign Tech Agency Official Website

Description: Main source for STF's mission, projects, funding, and governance.

Link: https://www.sovereign.tech

Sovereign Tech Fund Evaluation Report: Pilot Phase (2023)

Description: Detailed findings from STF's pilot phase, including metrics and processes.

Link:
https://www.sovereign.tech/public/files/SovereignTechFund_Evaluation_Report_Pilot_Phase.pdf

SPRIND: Sovereign Tech Fund Page

Description: Overview of STF's goals, funding, and SPRIND's role.

Link: https://www.sprind.org/en/projects/sovereign-tech-fund

OpenStreetMap Blog: STF Investment

Description: Specifics on STF's funding for OpenStreetMap, including project scope.

Link: https://blog.openstreetmap.org/2024/12/20/sovereign-tech-fund-invests-in-openstreetmap

OSTechNix: Samba Funding by STF

Description: Details on STF's €688,800 investment in Samba's security enhancements.

Link: https://ostechnix.com/samba-receives-eur-688800-from-sovereign-tech-fund

ZenDiS (*Zentrum für Digitale Souveränität der Öffentlichen Verwaltung*[69])

Year of Beginning: 2022 (founded in December)

Sector: Open Source Software, Digital Sovereignty, Public Administration, IT Infrastructure

Political Geography: Germany (headquartered in Bochum, North Rhine-Westphalia); European collaboration

Description:

ZenDiS is a German federal initiative, operating as a GmbH (limited liability company), to promote digital sovereignty in public administration through open-source software (OSS). It coordinates OSS development, provides consulting, and manages platforms like openCode (a repository for OSS projects) and OpenDesk (a sovereign workplace suite). Aimed at reducing dependency on proprietary vendors, ZenDiS supports federal, state, and municipal administrations with tools for secure, transparent, and interoperable IT solutions. Its flagship project, OpenDesk 1.0, launched in October 2024, integrates OSS tools for collaboration, email, and project management, aligning with the EU's 2020–2023 Open Source Strategy.

Short History:

Established in December 2022 by the Federal Ministry of the Interior (BMI) following a 2019 market analysis highlighting vendor lock-in risks, ZenDiS was formalized by the IT-Planungsrat's 2021 Strategy for Digital Sovereignty. In 2023, it launched openCode and took over OpenDesk development (previously Souveräner Arbeitsplatz). The OpenDesk 1.0 Enterprise Edition was released in October 2024 at the Smart Country Convention, offering self-hosting and SaaS models. ZenDiS collaborates with BSI and BWI GmbH on secure software supply chains.

Mission:

To strengthen the digital sovereignty of Germany's public administration by promoting, developing, and providing scalable open-source software solutions, ensuring technological self-determination, transparency, and security.

Aims and Objectives:

- Coordinate OSS projects to reduce dependency on proprietary tech providers.
- Develop and maintain platforms like openCode and OpenDesk for public sector needs.
- Provide consulting and tools (e.g., Souveränitätscheck) to identify and mitigate vendor lock-in.
- Foster collaboration between OSS communities, public administration, and European partners.
- Enhance IT security and interoperability through open standards and supply chain transparency.

[69] Tr. Center for Digital Sovereignty in Public Administration.

Funding:

Funded by the German federal government (BMI as a sole shareholder) through public contracts, with plans for state governments to join as shareholders. Specific grants include budgets for OpenDesk and openCode development.

System of Governance (Ownership and Control):

ZenDiS GmbH is wholly owned by the BMI, with plans to become a federal-state corporation. Governed by a management board, it operates under German corporate law and IT-Planungsrat strategies. OSS projects are managed transparently via GitHub (e.g., openCode), with community contributions encouraged but controlled by ZenDiS. The Souveränitätscheck tool aids dependency analysis, but critics note limited grassroots OSS community involvement compared to corporate partnerships (e.g., B1 Systems, STACKIT).

Legal Form:

ZenDiS is a limited liability company (GmbH) under German law, fully owned by the federal government. OSS outputs use open licenses, and the company operates as a non-profit-oriented public entity focused on digital sovereignty.

Licenses Used:

OSS projects (e.g., OpenDesk, openCode) use Apache 2.0, MIT, or GPL licenses, ensuring free use and modification. Documentation is released under Creative Commons CC-BY 4.0 or CC-BY-SA 4.0. ZenDiS's proprietary tools, like the Souveränitätscheck, are not fully open but accessible to public administrations.

Broader Contributors:

Includes federal, state, and municipal administrations, OSS vendors (Collabora, Nextcloud, OpenProject, Univention, XWiki, Element, Nordeck, Open-Xchange), and partners like BSI, BWI GmbH, and STACKIT. The OSS community contributes via openCode, though engagement is primarily through curated projects. European collaboration aligns with EU OSS strategies, with ~2000 LinkedIn followers indicating niche interest. Critics note that corporate-driven partnerships may overshadow grassroots OSS voices.

Broader Impact:

ZenDiS reduces vendor lock-in, enhancing Germany's public sector IT autonomy, as seen in OpenDesk's adoption by early adopters. Its open-source model promotes transparency and cost-efficiency. Challenges include scaling across diverse administrations, limited community-driven development, and dependency on government funding. Internationally, ZenDiS sets a precedent for sovereign IT, influencing EU policies, though practical adoption lags behind ambitions.

Qualitative Impact:

ZenDiS's OpenDesk provides a viable alternative to Microsoft and Google, fostering secure, interoperable workplaces. Its Souveränitätscheck (Sovereignty-check) tool helps identify critical dependencies, but adoption is slowed by administrative inertia and skill gaps. The openCode

platform encourages OSS reuse, yet curated governance limits community spontaneity. ZenDiS's EU-aligned approach positions Germany as a digital sovereignty leader, but critics argue its top-down model may hinder grassroots innovation. Long-term success depends on broader state participation and user training.

Flagship Projects:

- OpenDesk: OSS collaboration suite with email, video calls, and project management (v1.0, 2024).
- openCode: Repository for public sector OSS projects, enhancing transparency.
- Souveränitätscheck: Tool to analyze and mitigate vendor lock-in risks.
- BSI[70] Collaboration: Strategy for secure software supply chains with openCode.

Official Website:

https://ZenDiS.de/en

Primary Sources:

ZenDiS Official Website

Description: Primary source for mission, projects, and organizational details.

Link: https://ZenDiS.de/en

OpenDesk Official Website

Description: Details OpenDesk's features, release history, and ZenDiS's role.

Link: https://www.OpenDesk.eu

North Data: ZenDiS GmbH Profile

Description: Provides legal form, ownership, and financial context.

Link: https://www.northdata.com/Zentrum+f%C3%BCr+Digitale+Souver%C3%A4nit%C3%A4t+der+%C3%96ffentlichen+Verwaltung+%28ZenDiS%29+GmbH,+Bochum/Amtsgericht+Bochum+HRB+21488

IT-Planungsrat: Digital Sovereignty Strategy

Description: Contextualizes ZenDiS's role in Germany's OSS strategy.

Link: https://www.it-planungsrat.de/fileadmin/it-planungsrat/foederale-zusammenarbeit/Gremien/AG_Cloud/20210104_Strategy_for_strengthening_the_digital_sovereignty_of_public_administration_IT_1.0.pdf

[70] The BSI (Bundesamt für Sicherheit in der Informationstechnik) is Germany's Federal Office for Information Security. It's a government agency responsible for protecting IT systems, networks, and data from cyber threats.

ANNEX 2. DEEP DIVES ON SELECTED CASES

A Shared Architecture: The Tripartite Governance of Risc-V in an Age of Geopolitical Fragmentation

1. A compelling case of open technology governance

Risc-V offers a compelling case study of open technology governance, illustrating how a technical project can evolve into a global phenomenon shaped by the distinct—and sometimes conflicting—interests of communities, firms, and governments. Its trajectory from a university lab to a strategically significant open standard reveals much about innovation, geopolitical tension, and the quest for technological sovereignty in the 21st century.

This analysis begins by tracing the origins and development of Risc-V, followed by an examination of the evolving community that forms its core. It then dissects the roles and motivations of governments, with a focus on Europe, China, and the USA. The subsequent section categorizes the diverse types of firms involved and their economic drivers. Finally, the analysis explores how Risc-V has navigated inherent tensions through key innovations in its governance structure.

2. History: From Berkeley Lab to Global Standard

The story of Risc-V begins not in a corporate boardroom, but at the University of California, Berkeley, in 2010. Professors Krste Asanović and David Patterson, along with graduate students Andrew Waterman and Yunsup Lee, were frustrated with the landscape of computer architecture. Existing instruction set architectures (ISAs) were either proprietary and legally encumbered, or outdated and technically flawed for the emerging era of specialized computing (10, 13). Their goal was initially modest: to create a clean, simple, and efficient ISA for use in research and education over a three-month summer project (11). The name Risc-V, standing for the *fifth* generation of Reduced Instruction Set Computer (RISC) architecture from Berkeley, was a nod to this academic lineage.

What set their project apart was not just its technical merit—its modular design and clean-slate approach—but the founders' decision to release it under a permissive Berkeley Software Distribution (BSD) license. This made it freely available for anyone to use, study, and modify. For the first few years, Risc-V remained a niche tool within academia. However, its adoption began to spread organically as researchers and engineers worldwide discovered this open alternative. The turning point came in 2015, when the team realized they had significantly underestimated the "hunger for an open ISA" from industry (10). The first Risc-V workshop in Monterey, California, attracted 40 different companies, a clear signal of commercial interest. Later that year, the Risc-V Foundation was established with 36 founding members to steward the ISA's development, protect its open nature, and foster a broader ecosystem. From that point, Risc-V's momentum became unstoppable, growing from a few enthusiasts to a global community of over 4,600 members across 70 countries, with its architecture found in more than 13 billion cores by 2024 (5). It has since been used in everything from microcontrollers and laptops to servers and even space-grade processors.

3. The Evolving Community: Composition and Role

The Risc-V community is the project's lifeblood, but its composition and role have changed dramatically since 2010.

- Phase 1 - **The Academic Core (2010-2015):** In its earliest phase, the community was small and homogenous, consisting primarily of the Berkeley team and researchers from other universities. Their motivation was intellectual: to advance computer architecture research, develop teaching tools, and explore new design paradigms without the barriers of proprietary IP. This group was responsible for defining the base ISA and establishing the foundational technical ethos of simplicity and modularity (13).
- Phase 2 - **The Enthusiast and Hobbyist Expansion:** As word spread, individual hardware enthusiasts and embedded systems developers began to take notice. This group was drawn to Risc-V for its openness, low cost of entry, and the freedom it offered to tinker and create custom implementations for non-commercial projects (5). They contributed by porting software, identifying bugs, and creating a grassroots groundswell of interest.
- Phase 3 - **The Industrial and Institutional Takeover (2015-Present):** The formation of the Risc-V Foundation marked a profound shift. The community's center of gravity moved from individual academics to large corporations and, increasingly, government-backed entities. While individual contributors and academics remain vital (10), the technical working groups and strategic direction are now dominated by engineers and representatives from member companies like Google, Qualcomm, Alibaba, Huawei, and Nvidia (1, 5). This shift has accelerated the development of complex extensions for high-performance computing, AI, and automotive applications but has also introduced new layers of formality and commercial considerations into previously open-ended discussions.

3.1 Arrangements for maintaining grassroots community presence

Risc-V International has however implemented several structural, financial, and technical arrangements to ensure that the grassroots community—including individual developers, researchers, and small organizations—can maintain a presence, collaborate, and continue to tinker with the ISA and that innovation is not restricted to large corporations, thus maintaining Risc-V open to a "bottom-up" development approach.

Key arrangements facilitating this include:

- Free Individual Membership: Individual membership in Risc-V International is free. This allows individuals not associated with a member organization to participate in the ecosystem, access technical working groups, and join community discussions without paying fees (7).
- Zero-Fee Academic/Nonprofit Tiers: Academic and non-profit entities are granted community membership at no cost, promoting continued research and open-source development.
- Low-Cost Startup Membership: A specialized "Strategic Startup" tier exists for companies with fewer than 10 employees and less than 2 years old, priced significantly lower ($2,000 USD) than standard strategic memberships, allowing small companies to participate in technical leadership.
- Open Access to Technical Work: While active participation in technical committees is restricted to members, all Risc-V technical committees and workgroups are non-confidential, meaning their mailing lists, meeting minutes, and deliverables are public.
- Open-Source Licensing Model: The Risc-V ISA is a free and open standard. This allows anyone, regardless of membership status, to tinker, innovate, and develop implementations using a permissive license.

- Mentorship Programs: Risc-V offers dedicated mentorship programs (e.g., via LFX Mentorship) that connect individuals with experienced engineers to learn, develop, and contribute to the ISA (7).
- Publicly Available Tools and Resources: The community provides free online courses, GitHub repositories (e.g., hosted by OpenHW Group), and QEMU support, allowing developers to simulate and test Risc-V cores without expensive hardware.

Furthermore the governance model carefully protects the voting power of unaffiliated individuals. As clarified in official Risc-V International policy, each member entity (including Premier companies) gets only one vote in a technical group (12, 14).

4. Governments: Strategic Interests and Motivations

For governments, Risc-V has transcended its technical roots to become a strategic asset in the global competition for technological leadership and digital sovereignty. Their interest is framed by a desire to reduce dependence on foreign, proprietary technologies (primarily from the U.S.) and to foster domestic innovation.

- **The European Union** (strategic autonomy): The EU's engagement is most explicitly framed around the concept of "digital autonomy." The DARE (Digital Autonomy for Risc-V in Europe) project, a large-scale EU-funded initiative, aims to develop European-made processors for high-performance computing (HPC) and AI based on Risc-V (3). The motivation is clear: to reduce reliance on non-European manufactured products, cut costs, and build a domestic semiconductor ecosystem that can support European research and industry, from medicine to finance. The EU's role is that of a **funder and orchestrator**, bringing together research institutions and companies like the Barcelona Supercomputing Center and Axelera AI to achieve collective strategic goals.
- **China** (technological self-reliance): China has embraced Risc-V with the greatest intensity, viewing it as a powerful tool to achieve semiconductor self-sufficiency amid escalating U.S. export controls (2). The open and royalty-free nature of Risc-V offers a pathway to bypass dependence on American-dominated ISAs like x86 and ARM. This is a national priority, reflected in high-level political support. Chinese investment is multi-pronged: national-level guidance, municipal and provincial support (e.g., Beijing, Shanghai, Zhuhai) for creating Risc-V industrial zones and innovation centers, and active participation by giants like Alibaba and Huawei in defining the standard (5, 9). The motivation is a blend of **strategic necessity and industrial ambition**.
- **United States** (a story of duality): The U.S. position is more complex and dualistic. On one hand, its industry and research institutions are foundational to Risc-V. DARPA, the Pentagon's advanced research agency, has funded Risc-V development, and U.S. tech firms are leading its commercial adoption. On the other hand, this very openness has sparked a national security debate in Washington. Some policymakers fear that China's active participation will allow it to leverage Risc-V to circumvent export controls and erode the U.S.'s historical leadership in chip design (4). Think tanks like the CSIS have cautioned against disengagement, arguing that Risc-V enhances the competitiveness of U.S. firms and that its open nature does not inherently pose a security risk, as sensitive intellectual property remains with the companies implementing the standard, not in the standard itself (5). The U.S. thus embodies a tension between its **pro-innovation, industry-led tradition** and **its geopolitical reflexes towards technological containment.**

- Emerging players (**Brazil and India**): The appeal of Risc-V is also evident in the Global South. In 2025, the Chinese Electronics Standardization Association signed a strategic cooperation agreement with the Brazilian Semiconductor Industry Association, signaling a South-South technology partnership aimed at fostering open hardware ecosystems. India has also shown interest in Risc-V for similar reasons of strategic autonomy and fostering a domestic semiconductor design industry, often in partnership with commercial players like SiFive.

5. Firms: Business Models and Motivations

The business ecosystem around Risc-V is not monolithic; it comprises different types of firms, each with distinct commercial logic and expectations (1, 2, 5, 7, 9, 10).

BUSINESS MODEL	CORE ACTIVITY	KEY MOTIVATIONS & EXPECTATIONS	EXAMPLE COMPANIES
Selling IP Cores	Licensing semiconductor blueprints.	**Monetizing expertise** by creating pre-validated, high-performance CPU cores. Aims for high margins and widespread licensing. First to market in high-growth segments like AI and automotive.	SiFive (US), Nuclei System Technology (China)
Selling Chips	Manufacturing and selling physical chips based on Risc-V.	**Capturing value through volume**. Leverages Risc-V's low cost, customizability, and power efficiency to gain a price/performance edge in competitive markets like IoT, industrial control, and consumer electronics.	Espressif Systems (China), Sophgo (China), SpacemiT (China)
Selling Solutions	Building and selling full "system-level" platforms.	**Ecosystem orchestration**. Lowers the adoption barrier for others by integrating Risc-V cores with software, tools, and reference designs. Aims to create a "stickier" business model and dominate a key technology layer.	Eswin Computing (China)

But, as in many other cases of open tech adoption, a fourth, and perhaps most influential category of companies operating in Risc-V ecosystem, consists of **"consumer-creators"**: large technology firms that use Risc-V internally rather than selling it. Companies like Google, NVIDIA, Qualcomm, and Alibaba have integrated Risc-V cores into their own systems-on-chip (SoCs) for functions ranging from power management and security in GPUs to accelerators in data centers. For them, the motivation is **strategic control and flexibility**. Risc-V allows them to build custom hardware tailored to their specific workloads (especially in AI), reduce licensing costs and legal red tape associated with proprietary vendors, and insulate their supply chains from vendor lock-in. NVIDIA's decision to replace its proprietary Falcon controllers with Risc-V, resulting in a billion cores shipped, is a prime example.

6. Architecture, License, and Governance: Tools for Balance and Cohesion

The specific technical and legal foundations of Risc-V are important and were deliberately chosen to create a framework that could at the same time accommodate diverse interests and prevent the ecosystem from fracturing.

6.1 Leaving Space for Commercial Interests and Industrial Secrets

The genius of Risc-V's design lies in how it separates the *standard from the implementation* (9).

- The **BSD license as a shield for secrets**: The choice of the permissive Berkeley Software Distribution (BSD) license is paramount. Unlike copyleft licenses (like GPL) that require any derivative work to be shared under the same license, the BSD license allows users to take the open ISA, build their own proprietary chip designs around it, and keep those designs entirely confidential. This directly addresses the core concern of for-profit firms: they can innovate and differentiate without being forced to give away their secret sauce. As one analysis notes, users are not required to "disclose their own proprietary implementations" to competitors or customers (6).
- The **Minimal Core as a foundation for competition**: The Risc-V ISA is intentionally minimal, providing only a small set of essential instructions. This modularity, with a small base and space for standard and custom extensions, is its key feature. It means that companies can build entirely different products on the same foundational ISA.

In this way, wildly different commercial interests could coexist peacefully while its flexibility is the primary source of Risc-V's appeal, as it fuels "innovation in areas like IoT, AI, and embedded systems" without forcing companies into a one-size-fits-all mold.

6.2 Avoiding Ecosystem Fragmentation

The same openness that enables competition also poses a risk: fragmentation (14). If every company adds its own custom instructions, software and tools might not work across different Risc-V chips. Risc-V International has implemented several layers of governance and process to prevent this.

- The **Rigorous Extension Ratification Process**: The most critical tool against fragmentation is a formal, multi-stage process for approving new standard extensions. This "rigorous process" ensures that any new standard extension has broad industry consensus and demonstrated need, preventing a free-for-all of incompatible additions.
- **Defining Profiles and Platforms**: To ensure software portability, Risc-V International defines profiles. A profile is a curated set of extensions that must be supported for a class of hardware. This allows operating system vendors to target a known baseline. Going a step further, they are developing platform specifications (e.g., for a server platform) that standardize hardware interfaces.
- The **Architecture Compatibility Test Suite**: Any company claiming Risc-V compatibility must pass a suite of tests against a golden model, verifying that their implementation truly adheres to the standard.
- **Proactive Management of Custom Extensions**: Recognizing that custom extensions are a key feature, Risc-V is not banning them but managing them. The Composable Custom

Extensions Task Group is developing standards to allow multiple custom extensions from different authors to coexist "conflict-free" within a single system, with a uniform programming model. This is a proactive, governance-based solution to a potential fragmentation problem

6.3 Ensuring Pluralistic Stakeholder Representation

The governance structure of Risc-V International is designed to be a "big tent," giving a voice to the different types of stakeholders identified in the earlier analysis (9).

- A *Multi-House Model*: The representation is built into the very fabric of the organization through its membership classes:
    - *Premier and Strategic Members (Firms/Governments)*: These are the for-profit entities and large non-profits. They have significant voting power in strategic decisions and can heavily influence the technical direction by dedicating engineering resources to the working groups. Their interests in commercialization and standardization are the primary drivers of the formal extension process.
    - *Organizational Community Members (Academia/Non-profits)*: Universities and research institutions, the original home of Risc-V, have a formal seat at the table. This ensures that the academic values of exploration and education are represented alongside commercial interests.
    - *Individual Community Members (Grassroots)*: As noted, unaffiliated individuals have their own voting rights, ensuring that the hobbyist and independent developer perspective is part of the formal decision-making process.
- *Representation in Technical Work*: This multi-house model filters down to the technical committees. The rules state that a person affiliated with a member entity must represent that entity's vote, but an unaffiliated individual can vote on their own behalf. In technical working groups, leadership can be shared between a corporate representative and an individual. This ensures leadership is not exclusively corporate.

7. Navigating Tensions: Innovation in Governance

The confluence of a diverse, global community, profit-driven firms, and geopolitically motivated governments creates significant tensions. Risc-V's ability to navigate these pressures is a direct result of deliberate innovations in its governance model.

The most significant governance decision was the **relocation of the Risc-V Foundation**'s headquarters from Delaware to Switzerland in 2020 (5). This move was a direct response to escalating geopolitical tensions and fears that a U.S.-based entity could be subject to U.S. government restrictions on technology cooperation with China. By incorporating in a neutral country, Risc-V International signaled its commitment to remaining a truly global, open standard, insulating the technical collaboration from the whims of any single nation's foreign policy. This act of "polycentric governance" has been identified by researchers as a key buffer against politicization (9).

The transition from informal academic collaboration to a formal, de facto global standards body required deliberate and highly competent **professionalization of its governance**. The creation of the Risc-V Foundation (now Risc-V International) was the pivotal moment, thanks to the adoption of the structures and practices of mature open source foundations, particularly the Linux Foundation.

Crucially, the organization and its procedures were rigorously designed to ensure neutrality and trust and to navigate with diplomacy and inclusivity among multiple competing forces (9).

This structural neutrality is complemented by a **technical and processual openness**. Risc-V International does not require its members to divulge their proprietary implementations; they only collaborate on the standard itself. This allows fierce competitors like Qualcomm and Huawei to sit on the same technical committees, shaping a common foundation while building their secret sauce on top of it. The organization's technical steering committee, which includes members from both U.S. and Chinese companies, facilitates this co-opetition. The governance model has successfully channeled the competing pushes from different stakeholders into a collaborative standard-setting process. For instance, a firm with a new idea for an AI extension is incentivized to drive it through the Risc-V International process to prevent ecosystem fragmentation and ensure broad adoption, even if the alternative of going it alone is technically possible.

8. Concluding observations

In conclusion, Risc-V's journey is a masterclass in open technology governance. Its technical design provides the space for competition and secrecy, while its formal, professionalized processes provide the glue against fragmentation. The multi-layered membership structure ensures that all voices—corporate, academic, governmental, and individual—have a place, albeit with different weights. And its leadership has demonstrated the strategic foresight and diplomatic skill required to navigate the treacherous waters of global geopolitics and commercial rivalry, transforming a university project into a resilient and thriving ecosystem. Risc-V's journey from a student project to a globally critical technology is a testament to the power of open collaboration. However, its continued success hinges on the delicate balancing act performed by its governance structure. It must nurture the academic and enthusiast community that provides its innovative spark, accommodate the commercial needs of firms seeking competitive advantage, and assuage the strategic anxieties of governments pursuing digital sovereignty. By anchoring its legitimacy in technical openness and political neutrality, Risc-V has so far successfully navigated the tensions inherent in this tripartite model. Its future trajectory—whether it remains a unifying force or splinters under geopolitical pressure—will serve as a defining case study for the governance of open technology in an age of fractured globalization.

Notes and references:

1. 36Kr. (2024). Risc-V ecosystem development and industry trends. 36Kr. https://36kr.com/p/3531527624563844

2. Cheung, S. (2023). Examining China's Grand Strategy For Risc-V. China Brief, 23(23). https://jamestown.org/examining-chinas-grand-strategy-for-Risc-V/

3. CORDIS. (2024). Project 101202459. European Commission. https://cordis.europa.eu/project/id/101202459

4. Cory, N. (2024). The US-China Tech Conflict Fractures Global Technical Standards: The Case of Semiconductors and the Risc-V Standard. Information Technology and Innovation Foundation, 19.

5. CSIS. (2025). Sustaining standards leadership: The United States cannot disengage from Risc-V. Center for Strategic and International Studies. https://www.csis.org/analysis/sustaining-standards-leadership-united-states-cannot-disengage-Risc-V

6. LDRA. (2024). How safety-critical system developers are adopting Risc-V. LDRA. https://ldra.com/how-safety-critical-system-developers-are-adopting-Risc-V/

7. Meegle. (2024a). Risc-V community. Meegle. https://www.meegle.com/en_us/topics/Risc-V/Risc-V-community

8. Meegle. (2024b). Risc-V commercialization. Meegle. https://www.meegle.com/en_us/topics/Risc-V/Risc-V-commercialization

9. Pretalx. (2025). OFA Symposium 2025 talk: XSBFL7. Pretalx. https://pretalx.com/ofa-symposium-2025/talk/XSBFL7/

10. Risc-V International. (2025). High RISC, High Reward: Risc-V at 15. Risc-V Blog. https://riscv.org/blog/Risc-V-15-years/

11. Risc-V International. (2024a). 14 years of Risc-V: A journey of innovation and firsts. Risc-V Blog. https://riscv.org/blog/14-years-of-Risc-V-a-journey-of-innovation-and-firsts/

12. Risc-V International. (2024b). Technical working group messages. Risc-V Tech-P Extension Mailing List. https://lists.riscv.org/g/tech-p-ext/messages?expanded=1&msgnum=544

13. SiFive. (2025). From Berkeley Lab to Global Standard: Risc-V's 15-Year Journey. SiFive Blog. https://www.sifive.com/blog/from-berkeley-lab-to-global-standard-Risc-Vs-15-ye

14. TechPowerUp. (2024). Interview with Risc-V International: High-performance chips, AI ecosystem fragmentation, and the future. TechPowerUp. https://www.techpowerup.com/327781/interview-with-Risc-V-international-high-performance-chips-ai-ecosystem-fragmentation-and-the-future

Gaia-X: A European Experiment in Digital Sovereignty and Industrial Policy

1. A New Model of Industrial Policy

Gaia-X represents a prime example of a shift in European industrial policy. Faced with the dominance of US hyperscalers - which still account for roughly 70 percent of Europe's cloud market (1) - and growing geopolitical tensions, European governments are moving beyond their traditional role as market regulators, attempting to assume a more active influence as architects of the digital economy. What has made the European approach distinctive is its strategic use of open technology as a tool for industrial policy, aiming not to build a single "national champion" but to orchestrate a federated ecosystem of providers bound by common rules and standards (2, 7).

Gaia-X has been the prime example of this federated ecosystem approach. Its tentative conception and evolution is also a testament of the uncertain results that this approach and its struggled governance has achieved so far (2, 7).

2. Origins—The Awakening

The story of Gaia-X begins in Germany in the late 2010s. German industry—particularly its powerful automotive sector—recognized that its future competitive advantage would depend to a large extent on data generated by factories and vehicles. Yet this data increasingly resided in the data centers of Amazon, Microsoft, and Google, on the other side of the Atlantic.

Two shocks amplified this anxiety (2):

- **The Snowden revelations (2013)** laid bare the extent of US government surveillance, transforming data storage into a potential geopolitical and industrial espionage vulnerability.
- **The *US CLOUD Act* (2018)** – approved during the first Trump presidency, gave US law enforcement authority to demand data from US companies regardless of where it was stored, creating a legal vacuum for European sovereignty.

In response, German Federal Minister Peter Altmaier initiated conversations with industrial giants—SAP, Deutsche Telekom, Siemens, and automotive leaders—asking: How do we prevent European industry from becoming a digital colony? The answer was Gaia-X, announced in 2019. France, with its own digital champions like OVHcloud, quickly joined, transforming it into a Franco-German engine for European digital autonomy.

The initiative was hailed as a "European industrial policy fit for the 21st Century"—a rallying cry that brought German and French companies together with top political backing to create a data infrastructure. The endgame goal was to "establish data sovereignty in Europe" and "counteract monopolistic tendencies" (7).

3. The European Definition of Digital Sovereignty

The broader ambition, behind this EU policy shift, was to make Europe the global leader in creating a market for industrial data. The European Strategy for Data (4), launched in 2020, aims to build a "single European data space"—an integrated digital system allowing individuals, businesses, and

governments to share vast troves of industrial, government, and personal data across borders and sectors (2, 10).

This strategy was further supported by two cornerstone laws:

- **The *Data Governance Act*** (in effect since 2023) that governs how public-sector and protected data can be reused and lays legal groundwork for data spaces (11).
- **The *Data Act*** (applying from September 2025) that mandates that providers of connected products give users real-time access to device-generated data. It explicitly excludes "gatekeepers" (primarily US and Chinese tech giants) from accessing data under these new rules, handicapping the very companies that gained prominence "through the accumulation and aggregation of vast volumes of data" (12).

But maybe the most original aspect was the concept of sovereignty underlying Gaia-X, which differs from classical, state-centric notions.

In truth, there are two interpretations of digital sovereignty in the formulations which have been used by EU policy. The first expresses the traditional Westphalian concept of supreme and exclusive monopoly of legitimate regulatory power within one's own borders, albeit adapted to Europe's politically complex context of shared sovereignty. The second, on the other hand, emphasizes the preservation of autonomy, freedom of choice and action, and self-determination for individuals, organizations, and governments in the face of dependence on critical digital systems (2).

Influenced by the EU's structure as a union of sovereign states, the market-centric nature of the EU and by German engineering culture, it developed a sort of universal, shared definition of sovereignty applicable to public and private actors alike and based on certain distinctive principles of technological design.

This vision was first articulated in the 2020 Berlin Declaration on Digital Society (5) and is embedded in four core technological principles (2):

- ***Open Source***: Ensuring transparency and auditability, preventing lock-in to opaque proprietary systems
- ***Modularity***: Allowing users to combine best-of-breed components from different providers
- ***Interoperability***: Enabling seamless communication between services from different vendors
- ***Standardization***: Creating common languages and rules that all participants must follow

This "matrix" of principles represents an attempt to embed sovereignty into technology itself, creating a system where control remains distributed, autonomy is preserved and trust is to an extent delegated to the technological design, rather than relying solely on legal agreements or state power and regulations (2).

4. Open Tech as a Tool for Industrial Policy

Gaia-X was also the prime example of a broader EU strategy to use open technology as a strategic tool for industrial policy. This still-evolving approach – which has been driven by growing trade and geopolitical tensions - features several distinctive features (2):

From Regulator to Architect

Rather than merely correcting market failures, the EU aims at actively shaping market structure and technological trajectory. This represents a progressive and tentative return to industrial policy after decades of market liberalism.

Navigating State Aid Rules

Open tech serves a crucial strategic function: it helps European governments and industry navigate the limitations that strict market rules—both at European and global level—impose on government aid. By funding open-source "digital commons" rather than picking national champions, the EU can support industrial development while remaining compliant with competition and trade regulations. This allows public investment that benefits entire ecosystems rather than single companies.

Pre-competitive Collaboration on Non-Differentiating Components

Open technology facilitates collaboration between competitors on components that are not sources of competitive advantage. The logic is simple: companies can share the foundational infrastructure and compete on the services built atop it.

Another example is the software-defined vehicle initiative, in which competing automakers collaborate on a shared software infrastructure while differentiating their own vehicle offerings[71].

Orchestrating Federated Ecosystems

Unlike traditional industrial policy that picks national champions, the EU uses open tech to enable many players to participate. Programs like *Next Generation Internet* (funding over 1,400 open-source projects)[72] and *SIMPL* (open-source data-sharing middleware)[73] invest in shared digital commons.

The Openness Paradox

However, this approach creates a fundamental tension between the logic of openness—which implies and requires global inclusion, by design and furthermore with the aim of promoting a standard—and the goal of achieving strategic autonomy—which requires cultivating a domestic industry and excluding non-European actors from the most strategic areas and markets. This tension has also manifested itself in the development and governance of Gaia-X (7).

5. Technical Architecture—Sovereignty by Design

The technical architecture of Gaia-X translates political goals into concrete mechanisms. The core idea – as it prevailed progressively - was not to build a new cloud to compete with hyperscalers, but to create a *federated trust layer* enabling existing and future services to interoperate under common rules.

Its key concepts are[74]:

Verifiable Credentials: Every participant and service creates machine-readable documents describing themselves—including technical capabilities, security certifications, and data usage policies. These

---

71 See https://federate-sdv.eu/sdvof-initiative/

72 See https://ngi.eu/

73 See https://simpl-programme.ec.europa.eu/dashboard/home

74 See https://Gaia-X.eu/services-deliverables/deliverables/ and https://Gaia-X.eu/news-publications/publications/

are digitally signed by trusted third parties, creating tamper-proof credentials that enable automated verification.

The Gaia-X Digital Clearing House which provides essential services:

- ***Registry***: A public directory of trusted anchor points
- ***Compliance Service***: Automated verification of credentials against Gaia-X rules
- ***Notary***: Validation of specific claims (like company registration)
- ***Federated Catalogues***: Interoperable directories where verified services can be published and discovered

Data Usage Control with Policies: Data providers attach machine-readable policies defining exactly what consumers may do with their data. These policies are enforced automatically at access time, not just through legal contracts.

In practice, this enables scenarios like an automotive company sharing sensor data with a university for research, where policies like "Usage Purpose = Road Safety Research Only" are automatically verified and enforced without human intervention.

6. The Governance Experiment—A Multi-Stakeholder Struggle

The governance of Gaia-X was designed as a *multi-layered, hybrid system* intended to be open and federated. In practice, it became an arena of intense struggle between governments, companies, and communities with conflicting interests (Baur, 2026) .

The Formal Structure[75]

Governments played the role of initiators and funders but do not directly fund the Gaia-X association itself. Instead, they provide political backing and fund national initiatives and lighthouse projects. Formally, governments are represented only in an advisory capacity—through the *Government Advisory Board*—without direct decision-making power in the association. The German and French governments provided the initial political impetus and continued to shape strategic direction through national hubs.

Companies form the core membership of the Gaia-X European Association AISBL, founded in 2021. The association develops the technical framework and strategic direction. Crucially, membership is open to non-European companies, but to have voting rights and serve on the *Board of Directors*, a company must have its headquarters in Europe. This was intended to keep strategic control in European hands[76].

Communities. Member organizations can participate through open technical *working groups*, contribute to technical specifications, architecture, and policy rules. This layer was designed to be transparent and grassroots-driven.

Lighthouse Projects and *Hubs*[77] provide real-world, sector-specific implementations (mobility, health, agriculture) (9) and national contact points, feeding practical experience back into governance.

---

[75] See https://Gaia-X.eu/about/

[76] See https://Gaia-X.eu/community/members-directory/#/members-directory

[77] See https://Gaia-X.eu/community/hubs/ and https://Gaia-X.eu/community/lighthouse-projects/

The real world tensions

Despite this elegant structure, governance became a battleground for several tensions (2, 7):

The Franco-German Fault Line: The two founders had divergent visions. France pushed a more protectionist approach, seeing Gaia-X as a tool to nurture European champions and break reliance on the US. Germany took a more technical, Atlanticist approach, focused on data sovereignty but open to partnerships with US companies. As one founding member described it: "France turned it into a very political issue, whereas the Germans treated it more as a technical matter". This lack of a "clear or common" definition of sovereignty—let alone a shared understanding of what it would take to get there—made consensus extremely difficult. Former CEO Francesco Bonfiglio described how this pitted a "historically more protectionist" France against a "fluctuating" Germany, with everybody "interpreting" Gaia-X as they wanted.

The Paradox of Inclusion: The decision to admit non-European hyperscalers (AWS, Microsoft, Google, Alibaba, Huawei) to membership—necessary for global relevance and competition law compliance—created accusations of "capture" (18). Critics argued these companies used their massive resources to "steer the entire roadmap" and dilute rules. While board seats remained reserved for EU companies and industry groups, some interviewees expressed criticism that European industry associations and companies on the board were representing the interests of business partners abroad.

Provider-User Conflicts: The governance bodies reflected the wider European divide between digital service providers (seeking protectionist rules) and digital service users (seeking efficient, low-cost solutions, often from US providers). This made building consensus nearly impossible. Large European telecom companies, for instance, have largely accommodated themselves to being resellers of hyperscaler technology rather than investing in developing independent European alternatives—a reality that further entrenches the status quo.

The Divergent Expectations: The mission to create a "federated cloud infrastructure" involved "staggering complexity" that turned into an "unmanageable mess," according to Lechelle, a French tech executive. Bonfiglio described how this divergence in expectations made his task extremely difficult: "Everybody was projecting into Gaia-X their own, at times very different, hopes" (7).

The Community's Limited Influence: While working groups were theoretically inclusive, the practical influence of participants was overshadowed by a top-down managerial approach aimed at accelerating the initiative effects and by the resources and expertise that few large corporate members could deploy in the working groups.

7. The Elusive Overall Impact

Despite five years of effort, the overall impact of Gaia-X and related EU digital sovereignty initiatives has been very limited.

The main objective of achieving data portability and interoperability—which the EU has been pursuing since the GDPR with several initiatives—remains elusive and not concretized (2, 3, 10).

Despite a fast-growing market for cloud computing services, the global share of European cloud providers has continued to fall, dwarfed by the dominance of Amazon, Microsoft and Google, which account for more than 70 percent of Europe's cloud market.

Europe has still to prove the commercial viability of its dataspace initiative. AgDataHub, a state-backed dataspace built to exchange data between French farmers that was touted as a triumph for farming data, went bankrupt in late 2023 (15). As Ilana Kunkel, a European Commission policy officer, acknowledged: "Eventually, data spaces should be able to sustain themselves and fund themselves. There still needs to be a business model and business participants in the data space to make it viable" (17).

Gaia-X effective use is still very elusive (16) and it also struggled to build international alliances and promote itself to become a global standard (17).

8. Geopolitical chill and the missed regulatory leg

The Russian invasion of Ukraine in February 2022 also delivered a shock from which Gaia-X's most ambitious sovereign aspirations never recovered. Overnight, the United States transformed from a digital "adversary" into a vital security ally. Weeks after the invasion, Biden and von der Leyen announced a new **Transatlantic Data Privacy Framework**, burying the application of an hard-won ruling of the European Court of Justice, which declared illegal the data transfer under the previous framework (2).

Even more directly important for Gaia-X, this shift definitively paralyzed key regulatory legs. The **EUCS** cloud certification scheme, which should provide the framework for the classification of the “secure” providers for the most critical services and data, and which had become the primary battleground for sovereignty requirements (with France pushing for providers "immunity" from non-EU laws), **stalled after five years of debate**. Germany, prioritizing NATO unity, joined other nations in opposing the harshest measures (2).

9. The Leadership Vacuum

Underlying Gaia-X's struggles is a broader lack of robust leadership in European digital policy (2).

Governments are divided and reluctant to take a strong role in industrial and technological policy. The Franco-German divergence on sovereignty remains unresolved. While Chancellor Merz recently acknowledged that "the global situation has changed so dramatically that we Europeans now have to become more sovereign," Germany simultaneously celebrated Google's decision to invest more than €5 billion in building data centers in the country—a move Finance Minister Lars Klingbeil described as "exactly what we need right now". This contradiction illustrates the absence of a coherent political will to pursue digital autonomy with determination.

Companies are divided and accommodated. European industry is not unified in its sovereignty ambitions. Large users—automakers, manufacturers, telecoms—have largely accommodated themselves to junior partnerships with Big Tech incumbents. They lack either the capabilities or the incentives to lead the massive investments required to build European alternatives. The telecom sector's acceptance of reseller status vis-à-vis hyperscalers exemplifies this dynamic.

Communities have been marginalized. The open-source and developer communities that might drive grassroots innovation have not been empowered within Gaia-X's governance. Beyond technical communities, **citizens as users of digital platforms and services**—who might have the strongest motivations to pursue sovereignty objectives (privacy, security, democratic control)—have not been mobilized. The entire initiative has remained an elite project of governments and

corporations, lacking the popular engagement that could generate sustained political pressure for change.

As Bonfiglio concluded, reflecting on the Gaia-X experience: "It is obvious that everybody sitting in the boardroom of an association with such a big and impactful objective tries to protect the interests of their own company". Without a countervailing force—from determined governments, from unified industry, or from mobilized citizens—those who "wanted to maintain the status quo have won" (7).

10. The New Reality

Gaia-X has not died. It continues as an association developing technical specifications and federated data spaces. It has united industry around tangible deliverables such as compliance labels and data spaces for sectors like energy and mobility.

Current CEO Ulrich Ahle, who joined in 2023, pushed back against characterizations of failure—arguing that "some people thought that Gaia-X would be the European hyperscaler as the competition to Amazon, Google, Microsoft... it is more about creating a way to handle data in a European way". He pointed to tangible deliverables like federated data spaces and compliance labels and cited EDF's use of Gaia-X standards to coordinate nuclear site construction (7).

However its scope has progressively narrowed. The grand ambition of creating a sovereign European cloud infrastructure has faded.

The European industry that inspired it has, largely, moved on. While participating in Gaia-X projects, strategic cloud partnerships often remain with US hyperscalers whose AI and analytics capabilities are indispensable. The market has responded with partnerships between local providers and global giants to offer "sovereign" services that comply with EU regulations while meeting customer demands.

Gaia-X's story is therefore a story of an ambition born of real and present danger, which united many under a common flag, only to be slowly eroded by the very forces it sought to overcome: the entrenched interests of its own members, the divisions between its governments, the accommodation of European industry to junior partnerships, and the overwhelming gravity of global geopolitics, in which Europe proved to lack genuine autonomy. Yet it also represents something genuinely new: an attempt to use open technology as an instrument of industrial policy and as a tool for an innovative framing of a shared and distributed sovereignty and the democratization of digital environments and infrastructures (2).

Notes and references:

1. Synergy Research Group. (2022). European cloud providers continue to grow but still lose market share. Synergy Research Group.

2. Berlinguer, M. (2024). The Matrix: Is there a European way to cloud computing? Transform! Europe.

3. Jamison, M. (2025a). Europe's data strategy is built on wishful thinking. AEIdeas. https://ctse.aei.org/europes-data-strategy-is-built-on-wishful-thinking/

4. European Commission. (2020). A European strategy for data. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066

5. Council of the European Union. (2020). Berlin declaration on digital society and value-based digital government. European Commission. https://ec.europa.eu/isa2/sites/isa/files/cdr_20201207_eu2020_berlin_declaration_on_digital_society_and_value-based_digital_government_.pdf

6. Wire. (2025). Sovereign cloud in the EU: Providers, challenges, and opportunities. Wire. https://wire.com/en/blog/sovereign-cloud-eu-providers-challenges-opportunities

7. Pollet, M. (2025). Anatomy of a Franco-German tech misfire. Politico. https://www.politico.eu/article/anatomy-franco-german-tech-misfire-american-dependence/

8. Computer Weekly. (2024). UK emphasizes EU split by kicking digital trade scheme into long grass. Computer Weekly. https://www.computerweekly.com/news/366554312/UK-emphasises-EU-split-by-kicking-digital-trade-scheme-into-long-grass

9. The Machinist. (2025). Continental white paper explores key technologies for connected mobility. The Machinist. https://www.themachinist.in/news/4507334/continental-white-paper-explores-key-technologies-connected-mobility

10. Jamison, M. (2025b). Europe's grand data plan: Ambitious, expansive, and ill-fated. AEIdeas. https://ctse.aei.org/europes-grand-data-plan-ambitious-expansive-and-ill-fated/#main

11. European Parliament and the Council of the European Union. (2022). Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868

12. European Parliament and the Council of the European Union. (2023). REGULATION (EU) 2023/2854 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202302854

13. Madiega, T. (2020). Digital sovereignty for Europe: Towards a more resilient EU. European Parliamentary Research Service.

14. Tews, S. (2024). Between rules and reality: The complex challenge of EU data compliance. AEIdeas. https://www.aei.org/technology-and-innovation/between-rules-and-reality-the-complex-challenge-of-eu-data-compliance/

15. Agdatahub. (2024). Agdatahub applies for bankruptcy proceedings. Agdatahub. https://agdatahub.eu/en/agdatahub-procedure-collective-liquidation/

16. Banks, M. (2024). Gaia-X - some real world user stories in action. Diginomica. https://diginomica.com/Gaia-X-some-real-world-user-stories-action

17. Computer Weekly. (2025). European digital market figurehead pleads to Westminster. Computer Weekly. https://www.computerweekly.com/news/366628192/European-digital-market-figurehead-pleads-to-Westminster

18. Baur, A. (2026). European ambitions captured by American clouds: digital sovereignty through Gaia-X? Information, Communication & Society, 29(2), 417–434. https://doi.org/10.1080/1369118X.2025.2516545

India Stack: State Power, Market Forces, and an Elusive Commons

1. A Foundation Laid in Minimalism

The story of India Stack is not one of a grand, pre-ordained plan, but rather an evolutionary tale of pragmatic, minimalist interventions that, over time, coalesced into a formidable digital infrastructure. Its origins trace back to the late 2000s with the conception of Aadhaar, a biometric identity project that was, at the time, highly unconventional and controversial (1). The driving force was a profound state failure: the inability to efficiently deliver subsidies and welfare to the intended beneficiaries due to leaky, corruption-ridden analog systems. The architects, led by figures like Nandan Nilekani and technologist Pramod Varma, applied a first-principles approach. They realized that the complexity of physical identity was the root problem. By digitizing identity into a simple, API-driven, and "extremely minimalist" layer, they could bypass the need for physical documents and endless photocopies (1).

This philosophy of "extreme minimalism" became the genetic code for subsequent layers. The Unified Payments Interface (UPI), launched in 2016, asked a similarly disruptive question: "If you can send an email or an instant message for free, why can't you send money?" (1). The result was a 1.5-page protocol that dematerialized money and made it interoperable. This was followed by the Data Empowerment and Protection Architecture (DEPA), a consent-based data-sharing layer. The overall impact has been staggering: from bringing hundreds of millions into the formal banking system—a feat the Bank for International Settlements estimated would have taken five decades without digitization—to enabling over 19 billion transactions a month (1). India Stack transformed the relationship between the state, citizens, and the economy, creating a foundational layer upon which a vibrant startup ecosystem could flourish.

2. The Conceptual Home: Digital Public Infrastructure (DPI)

India Stack is the undisputed poster child for the global rise of the Digital Public Infrastructure (DPI) concept. Before DPI became a buzzword at the G20 and in global policy circles, India Stack was already demonstrating its core tenets in practice (2, 3, 4). The DPI framework provides the language to understand India Stack not as a set of discrete government websites, but as a set of shared, open, and interoperable networks that function like digital utilities.

As the academic literature suggests, DPI moves beyond techno-solutionist framings to encompass the socio-technical, legal, and institutional elements that make the technology work (5). India Stack perfectly illustrates this. Its success is not just in the code of Aadhaar or UPI, but in the accompanying "techno-legal" framework - the 2016 Aadhaar Act, the 2023 Data Protection Board rules - and the institutional arrangements that govern data flows (6). In this sense, India Stack provides a concrete, real-world laboratory for the otherwise abstract debates on DPI, demonstrating both its immense potential for inclusion and innovation, and its inherent risks around surveillance and privatization.

3. Interrogating "Government as a Platform"

India Stack is often cited as the ultimate illustration of Tim O'Reilly's concept of "Government as a Platform" (GaaP) (7). The idea is that the government's role shifts from being a monolithic service provider to an enabler - a platform operator that builds core utilities and sets standards, upon which private markets and civil society can innovate. At first glance, India Stack fits this bill perfectly. The state provides the foundational layers (identity, payments), and private companies (from fintech startups like PhonePe and Google Pay to banks) build user-facing applications on top.

However, the tripartite model (state-market-community) allows for a more nuanced critique. While India Stack is a platform, the "government as a platform" model often underplays the platform's own agency and interests. The Indian state is not a neutral host. It is an active participant with its own sovereign goals: economic formalization, tax collection, and social control. The platform becomes a new instrument of governance, what some scholars have termed the "platformized information state," where the state's traditional functions are interwoven with platform logics to exert a new kind of infrastructural power (8). This is not just a platform for services; it is a platform for sovereignty. The state uses the stack to make its citizens and its economy legible in ways that were previously impossible, a digital extension of James Scott's "administrative ordering of nature and society" (9).

4. The Global Ambition and the Puzzle of Non-Adoption

Despite its domestic success, the Indian government's attempt to export India Stack as a global standard has met with mixed results (10). It has signed MoUs with countries like Armenia, Sierra Leone, and Papua New Guinea, and its model is a central point of reference in the EU-India Trade and Technology Council discussions on a potential "EuroStack". Why this push? The interest is geopolitical and economic. For India, positioning its stack as a global standard is a classic move of "stack geopolitics." It creates a democratic, Global South-led alternative to the digital architectures dominated by the US (Big Tech) and China. It also opens up new markets for Indian tech companies whose products are built on top of this stack.

However the reproduction of India Stack is not a technical challenge; it is a political, legal, and institutional one. The "stack" is not just software; it is a socio-technical system embedded in India's unique context. Other countries lack:

- **A "Big State" Push:** The Indian state's willingness to absorb the short-term political and social costs of disruptive reforms like demonetization to push digital adoption is unique.
- **Institutional Congruence:** The model relies on a specific alignment of bureaucracy (the elite Indian Administrative Service), technical talent (the IITs), and policy entrepreneurship (groups like iSpirt)[78] (9).
- **Legal Frameworks:** Exporting UPI requires exporting the legal liability and dispute resolution frameworks that underpin it. For the EU, for example, this clashes with the General Data Protection Regulation's (GDPR) adequacy requirements and concerns about source code protection clauses that could hinder transparency and security audits (2). The stack is too entangled with India's specific "state" logic to be easily transplanted into a different "state" logic elsewhere.

[78] See https://ispirt.in/

5. A Multi-Layered System of Governance: Modulating Regimes

India Stack is an interesting case for exploring the importance of the strategic use of the architecture of technological systems, to modulate different regimes in a multi-layered system of governance which support different logics at the different layers. The system is designed to support different logics simultaneously, creating a fragile but productive equilibrium.

- **Layer 1: Identity (Aadhaar) — The State Logic:** At the bottom layer, the logic is purely that of the state. It is about sovereign authority, legibility, and the provisioning of a public good (a unique identity). This layer is non-competitive and state-owned. Its success relies on the state's coercive power to mandate its use and its creative capacity to enroll a billion people (9). The community logic is almost entirely absent here; it is a top-down, state-driven project.
- **Layer 2: Payments (UPI) — The Market Logic:** Built atop the identity layer, UPI unlocks a vibrant market logic. The state provides the open, interoperable rails (the "public good"), but the actual user-facing apps are built by competing private firms. The state acts as a regulator and standard-setter, ensuring a level playing field. The driver here is private-sector innovation, competition, and profit. The success of this layer depends on keeping the state's own interventionist logic in check: the state provides the infrastructure but does not compete and instead unleash private and market innovation in the application layer.
- **Layer 3: Data (DEPA/Account Aggregators) — The Emergent Citizens Commons Logic:** This layer is the least developed and the most experimental. DEPA attempts to create a new logic: the **individual-centric data commons**. The architecture (consent managers) is designed to disintermediate both the state and large data silos (Big Tech). It empowers the individual to act as a sovereign over their own data, sharing it with whichever service provider they choose. The drivers here are a unique mix: policy entrepreneurs and technologists from civil society (like iSpirt) who championed the "consent-first" architecture, and regulated entities (Account Aggregators) who operate as a new kind of market actor, but one whose very purpose is to serve the individual's agency. This layer attempts to encode a "digital social contract" directly into the technology, creating a protected space for data as a common asset of the individual.

6. The Ambiguous Role of "Open Tech" and the Community

India Stack's relationship with "open tech" is not explicit. While the *protocols* and *APIs* are open, and while it uses open-source software, the *core infrastructure* (like the Aadhaar database) is a state-owned, closed system. The state has been strategic about this. It uses the language of "open" to attract innovation and build trust with the developer community, but it retains firm control over the foundational layers to ensure its sovereign authority is not compromised.

Where, then, do communities operate? They are not the "community" that builds the Linux kernel. Instead, they are:

- **Policy Communities (iSpirt):** The most significant community actor is the iSpirt (Indian Software Product Industry Roundtable). This is a network of tech professionals and entrepreneurs who acted as a policy think-tank and advocacy group, architecting the vision for DEPA and UPI. They are a "community of experts" operating in the civic space, translating techno-solutionist ideas into policy.

- **Developer Ecosystems:** The community that builds applications on top of UPI or integrates DigiLocker into their services. They are a market-driven community, contributing to the stack's network effects without governing its core.
- **Digital Rights Advocates:** This is a counter-community, operating in the civic sphere, constantly challenging the state logic and demanding more transparency, privacy, and safeguards against the coercive potential of the stack (9).

The community logic is thus fragmented. It exists in the *design* phase (iSpirt), the *usage* phase (developers), and the *contestation* phase (activists), but it has no formal governance role in the *operation* of the core infrastructure.

7. The Dark Side: Technological, Economic, and Political Problems

Finally, a balanced reflection must account for the shadows cast by this ambitious project. The tripartite model helps us see where the equilibrium breaks down.

- **Political. Coercion and Exclusion (The State Logic Overpowering Others):** The most severe critique is that the stack enables a new form of authoritarianism. The same infrastructure that delivers subsidies can be used for surveillance, exclusion, and social control. The Cambridge Handbook chapter explicitly links India Stack to the Indian state's "historical habits of authority," noting that its legitimacy is built on a combination of "calculation, creativity, **and coercion**" (9).
- **Economic. Privatization and Digital Extractivism (The Market Logic Overpowering Others):** While the stack enables small players, it also creates new monopolies. The biggest beneficiaries of UPI have been large corporations like Google and Walmart (PhonePe). There is a persistent fear of "digital extractivism," where global tech giants use the open infrastructure to harvest Indian data, train their AI models, and extract value without contributing back to the local innovation ecosystem (11). Here, the market logic overwhelms the public good, turning the infrastructure into a conduit for rent-seeking by global capital.
- **Technological. Security and Data Breaches:** The technological architecture is not impervious. There have been numerous reports of Aadhaar data breaches, where personal information was exposed. While the minimalist design of Aadhaar was meant to mitigate privacy risks (by not collecting data like religion or caste), the sheer scale of the system makes it an irresistible and vulnerable target (8).

8. Concluding remarks

India Stack is a powerful lens through which to view the complexities of 21st-century governance. It shows how a strategic technological architecture can successfully layer the logics of the state, market, and community to create immense public value. But it also serves as a warning. The equilibrium is unstable. The constant struggle lies in preventing any one logic—be it the state's hunger for control or the market's hunger for profit—from consuming the others and turning the stack from a platform for empowerment into a structure of domination.

Notes and references:

1. Jhangiani, N., Kalra, D., Hemrajani, V., & Rana, R. (2025). *Behind the success and ongoing evolution of India Stack*. Egon Zehnder. https://www.egonzehnder.com/what-we-do/board-advisory/insights/behind-the-success-and-ongoing-evolution-of-india-stack

2. Gottarelli, S. (2025). *EU-India Trade and Technology Council: A chance to join forces for a "Euro-India Stack"*. European DIGITAL SME Alliance. https://www.digitalsme.eu/eu-india-trade-and-technology-council-a-chance-to-join-forces-for-a-euro-india-stack/

3. Bruns, A. (2025). *Analysing the policy debate about digital public infrastructure*. Snurblog. https://www.snurb.info/node/3318

4. Kapoor, A., & Watson, E. (2023). *Defining the digital public infrastructure approach*. T20 Policy Briefs. https://images.hindustantimes.com/images/app-images/2023/8/t20-pb-tf-2-251-definingdpi.pdf

5. Lusi, J., Lorenz, B., & Pappel, I. (2025). *Innovation or reinvention? A systematic and bibliometric review of public sector digital infrastructure*. *Journal of Open Innovation: Technology, Market, and Complexity, 11*(3), 100593.

6. IE Center for the Governance of Change. (2023). *Enabling a thriving data economy with digital public infrastructures*. IE University. https://www.ie.edu/cgc/news-and-events/news/enabling-a-thriving-data-economy-with-digital-public-infrastructures/

7. O'Reilly, T. (2011). Government as a platform. *Innovations: Technology, Governance, Globalization, 6*(1), 13–40.

8. Ninan Thomas, P. (2022). The platformized information state: Infrastructure, anxieties, and contestations. In *Information infrastructures in India: The long view*. Oxford Academic. https://doi.org/10.1093/oso/9780192857736.003.0007

9. Singh, J. P. (2025). India Stack: Authority and innovation in a new financial infrastructure. In C. Westermeier, M. Campbell-Verduyn, & B. Brandl (Eds.), *The Cambridge global handbook of financial infrastructure* (pp. 336–346). Cambridge University Press.

10. Watson-Lynn, E. (2024). *The India Stack as a potential gateway to global economic integration*. https://www.orfonline.org/research/the-india-stack-as-a-potential-gateway-to-global-economic-integration

11. Sen, A. (2026). *India–EU relations and open source tech*. Takshashila Institution. https://takshashila.org.in/content/blogs/20260127-open-source-tech-india-eu.html

Decidim: The Deliberate Building of a Public-Community Alliance

1. What It Is

Decidim (from the Catalan "let's decide") is a free and open digital infrastructure for participatory democracy. It is a web framework that allows any organization—city council, association, university, or cooperative—to create a platform for strategic planning, participatory budgeting, public consultation, and collaborative design. Participants can create and support proposals, comment, attend virtual meetings, and receive documentation. Administrators can design participatory processes, configure democratic organs, and set up consultations. The infrastructure includes code, documentation, design assets, legal texts, datasets, and training resources—all openly licensed (1,3).

2. A Technopolitical History

Decidim's peculiarity lies in its technopolitical origins. It was not born in a city hall office, but in the fervor of Spain's 15-M (Indignados) movement in 2011—part of the global wave of square occupations from the Arab Spring to Occupy Wall Street. This anti-austerity movement reclaimed radical democracy, as hacktivists and social activists converged in public squares, using digital tools to organize and deliberate. This was the crucible where Decidim's technopolitical ethos was forged: the understanding that technology is never neutral, that its design carries inherent political assumptions, and that the rise of platform capitalism demanded democratic alternatives (1,6).

When activists from this movement won Barcelona's municipal elections in 2015 as Barcelona en Comú, they brought this ethos into government. Their aim was a digital infrastructure not merely serving the administration but owned and governed by the citizenry.

Two cultural and political traditions fused in Decidim. The **hacktivist and free software movement** transmitted the commitment to open licenses (AGPLv3 for code, CC-BY-SA for content), ensuring the platform remained a public good and preventing vendor lock-in. It also articulated "technological sovereignty"—the principle that a city must control its own infrastructure to be truly democratic, rejecting dependence on corporate platforms that extract data and shape interactions for profit.

The **autonomous and libertarian tradition of Barcelona's social movements** contributed grassroots know-how from occupied plazas: assemblyism, cooperative self-organization, and collective deliberation. When these activists entered city hall, they sought to scale this assembly logic through digital infrastructure.

Together, these currents forged Decidim as a **public-commons** infrastructure: publicly funded but commonly governed. This led to the deliberate construction of a community—in Barcelona, Catalonia, Spain, and globally—and in 2019, to the formal creation of the Decidim Association and Metadecidim community, to which the Barcelona City Council transferred control of the trademark and codebase. The project was structured as "recursively democratic": the tools for participation must themselves be democratically governed (2).

Since then, Decidim has become the most widely used participatory democracy platform internationally, with over 400 administrations (Barcelona, Helsinki, Mexico City, the EU) and dozens of organizations, with hundreds of contributors (1,6).

Its technopolitical character was tested in late 2019, when Chile's government—simultaneously repressing social movements—sought help setting up the platform. The Metadecidim community mobilized quickly, issuing a public communiqué: "Not with (the support of) Decidim". They acknowledged they could not stop the government from using the open-source software, but refused to provide support or legitimacy to what they termed "participatory washing," declaring solidarity with Chilean social movements (5). The message was clear: the platform is not a neutral tool for the highest bidder, but a political project with values.

The international climate has since shifted. Even locally, Barcelona en Comú lost the municipality. Yet the new administration maintained its commitment, and Decidim's journey continued. In December 2024, the Brazilian government formalized a partnership with the Decidim Association through a Memorandum of Understanding—the first such agreement with a government outside Catalonia (4). Brazil's "Brasil Participativo" platform, launched in 2023 on Decidim, now hosts over 1.5 million participants (9). Brazil joined the Committee of Public Institutions (founded in 2025 with Barcelona, New York, and Catalan institutions), allowing public bodies to participate directly in governing the digital commons. The Brazilian government explicitly framed this as a response to "the growing concentration of technological power by large private corporations," investing instead in "public, transparent, and collaborative infrastructure."

3. The Public-Commons Architecture: Governance as Deliberate Design

Decidim's governance structure is the most sophisticated expression of its technopolitical approach. At its core is a **public-commons partnership**—a concrete institutional arrangement reconfiguring relations between state, civil society, and market. Unlike models where infrastructure is fully privatized or remains entirely within governmental control, Decidim is deliberately structured as a **shared public good**: owned by neither city alone nor any private entity, but co-governed by a community of public institutions, activists, developers, and researchers (1,2).

The governance architecture, formalized progressively since 2019, creates clear separation between spheres of power while maintaining interconnection. The **Decidim Association**—a non-profit independent from the Barcelona City Council—holds legal responsibility for the project. Its **General Assembly** (all members) functions as sovereign body; an elected **Coordination Committee** manages daily operations.

This associational structure exists within the broader **Metadecidim community**, encompassing everyone who uses or contributes to the software—individuals, companies, public institutions, researchers. This is where the commons truly operates: open contribution, bug reporting, feature proposals, and thematic working groups on software, research, and methodology (1,2,7).

A deliberate **gradient of participation** operates: community members can contribute actively, but only Association members participate in governance decisions about strategic direction.

4. The Public-Private-Commons Triad: Relegating the Market to a peripheral role

Public institutions are not "clients" but **co-stewards** of a common infrastructure. Private companies occupy a deliberately marginal though functional role. This is formalized through mechanisms like the **Product Team**, established by a 2019 agreement between Barcelona City Council, the Decidim Association, and Localret (a consortium of Catalan municipalities). This team oversees the software roadmap, but its composition reflects public-commons logic: representatives of public and associative entities, not private vendors, define priorities.

Companies that provide services around Decidim—implementation, customization, training—are expected to **contribute back to the commons**. When they win public contracts to develop new features, those developments become part of the core software, available to all (3). This is not voluntary charity but an institutionalized expectation built into the procurement and governance model. The goal is to create a local ecosystem of small and medium enterprises that work with free software, within a framework where public investment generates public goods, not private intellectual property.

However this **over-reliance on Barcelona City Council funding** has showed limitations and weaknesses along Decidim's evolution and is a source of potential financial vulnerability. As a 2022 funding crisis showed, bureaucratic delays or political changes could theoretically jeopardize the project (10). Since then, Decidim has achieved a more solid funding base (11), among other things by obtaining EU funding (12).

However the deliberate marginalization of companies from its governance to prevent capture, can also contribute to create sustainability problems. Though the Association has now introduced a rule which requires integrator companies (13) which profit from the ecosystem to fund back the maintenance of the core infrastructure, the Association still struggles to capture value from this commercial activity.

5. Foundational Tensions, Necessary Frictions

This partnership generates inherent tensions. A research on Decidim's implementation across Catalan municipalities captured a dynamic between two competing logics: "democracy-driven governance" (social movement logic, emphasizing horizontal participation) and "governance-driven democratization" (administrative logic, emphasizing efficiency and legal compliance) (1).

From the community perspective, concern about institutional capture is real. This is precisely why power was deliberately transferred to the Association: to ensure community retains ultimate control, even as public institutions provide essential funding.

These tensions have driven remarkable institutional innovations, particularly in public procurement. Standard government procurement procedures are designed for purchasing goods or services from vendors, in competitive tenders, not for funding a commons. Barcelona had to **change its procurement standards** to accommodate a platform governed by a community rather than controlled by the city. The innovation: contractual mechanisms allowing the city to fund development while relinquishing exclusive control over the resulting code (3). The "deliverable" is not a finished product owned by the city, but a feature integrated into a shared infrastructure benefiting all users globally.

The Brazil MoU represents another innovation: a formal agreement establishing transnational public-commons governance through the **Committee of Public Institutions (4)**.

Governance Bodies: A Layered Architecture of Power

BODY/SPACE	COMPOSITION	FUNCTION	LOGIC
Metadecidim Community	Anyone using or interested	Contribution, discussion, working groups	Open commons
Thematic Working Groups	Self-selected community members	Software, research, methodology	Functional self-organization
Decidim Association	Formal members	Legal governance	Associative democracy
General Assembly	All Association members	Sovereign decision-making	One-member-one-vote
Coordination Committee	Elected members	Day-to-day management	Representative democracy
Product Team	Barcelona, Association, Localret	Software roadmap	Public-commons co-stewardship
Committee of Public Institutions	Public institutions using Decidim	International coordination	Transnational public governance

This layered architecture ensures different decisions are made by different bodies with appropriate legitimacy. The community generates proposals; the Association holds sovereign power; the Product Team coordinates with public funders; international bodies incorporate new institutions.

6. Technical Architecture as Constitutional Design

The technical architecture is crucial to Decidim's governance. It deliberately creates spaces for autonomy, innovation, and participation, while equally deliberately creating mechanisms for coherence, quality, and coordination (3). This is the technopolitical approach made tangible: software design shapes political possibilities, and building democratic infrastructure requires building democracy into the infrastructure itself.

From Monolith to Modularity

Decidim's technical story begins with a deliberate break from its predecessor, Consul. When the Barcelona team inherited Consul's codebase from Madrid[79], they encountered a fundamental

[79] The first artifact of the Decidim software was named Consul and was created in Madrid as a consultative platform during the sister parallel electoral campaign which brought Ahora Madrid to win the municipal election there. Initially, Barcelona en Comú used a fork of the "Consul" software for its *decidim.barcelona* site. However, in early 2017, the Barcelona team completely rewrote the software to create a new, more modular project called Decidim and transformed it into a deliberate techno-political initiative.

limitation: it was monolithic, requiring complete forks for each new instance. Customizations lived in separate repositories, making upgrades painful and fragmenting development.

The decision to completely rewrite Decidim in early 2017 used an architecture where the core platform functions as a library, and each new instance adds that library as a dependency. This technical choice carried profound governance implications: upgradability became seamless, and customizations became modular—organizations develop separate modules that plug into the platform, preserving core integrity while enabling local adaptation (1,3,8).

This modularity extends throughout. Every participatory feature—proposals, debates, voting, meetings, accountability—is implemented as an independent module. Administrators can mix and match functionalities without touching code. Over **80 community-developed modules** demonstrate how this enables distributed innovation: anyone can develop a module for a specific need and make it available to the ecosystem.

Crucially, this distributed innovation does not lead to fragmentation because of the clear distinction between **core modules** (maintained officially) and **community modules** (maintained by third parties). When a community module proves its value, democratic mechanisms certify its desirability and potentially incorporate it into the core—a controlled pathway from periphery to center.

Contribution and Release

Contribution management extends this approach. Everything happens openly on GitHub (14): all contributions reviewed openly, technical decisions debated. Participation is radically open, but changes are merged only when they meet technical standards (through automated and human review) and align with the project's direction.

Release management is deliberately centralized, controlled by core maintainers. Release candidates are first deployed to **Metadecidim**—the community's own instance—for at least one week of real-world testing before official release (3).

The Instance Ecosystem

The final layer is the instance ecosystem: **488 instances across 32 countries**, used by 308 institutions and 169 organizations. Each instance is **sovereign**: administrators control configuration, user access, and module selection, adapting the platform to diverse contexts. Yet each benefits from the shared core: when the core team releases a new version, instances upgrade with minimal friction. Autonomy at the edges does not require isolation (1,6).

A Layered Technical Governance

LAYER	TECHNICAL EXPRESSION	GOVERNANCE FUNCTION	BALANCE STRUCK
Core	Maintained by core team, AGPLv3	Coherence, security, interoperability	Centralized control for systemic integrity
Modules	Independent components, community-developed	Innovation without permission	Distributed innovation within constraints
Release	Maintainer-controlled, validation period	Ecosystem coordination, quality	Central coordination with community testing
Instances	Sovereign deployments, configurable	Local autonomy, adaptation	Independence without fragmentation
Contribution	Open GitHub workflows, automated testing	Broad participation with quality gates	Open access with quality enforcement

The license choices reinforce this: AGPLv3 ensures improvements must be shared back, preventing fragmentation; CC-BY-SA and Open Database License extend the commons logic to content and data.

The result accommodates diverse preoccupations: unleashing innovation through modularity; allowing autonomy through sovereign instances; avoiding fragmentation through centralized release management and strong copyleft—all through sophisticated layering that lets each principle govern at its appropriate level.

7. Lessons: Towards a New Generation of Open Tech Governance

Decidim offers profound insights as we witness the exhaustion of both purely corporate-driven models and original community-led open source forms.

Political Motivations as Primary Drivers

Decidim was not founded on a business model but on a political project of democratic deepening (1,6). It exemplifies the resurgence of explicitly political motivations over purely economic ones—a trend likely to grow. These motivations mobilize both public entities and diverse communities (developers, activists, researchers, public servants alike). In an era of widespread disillusionment with corporate technology, political purpose becomes a powerful organizing force—mobilizing contributions, sustaining communities, and guiding ethical decision-making in ways market mechanisms cannot.

The Public-Commons Arrangement

The most original lesson is that a public-commons partnership is not only possible but institutionally viable at scale. This offers a genuine alternative to dominant technology governance models. Decidim shows public institutions can fund and sustain digital infrastructure without owning or controlling it. By transferring trademark and codebase to an independent association, Barcelona created a structure where public resources feed a commons and the public sector becomes a steward of common goods—inverting the usual relationship where communities provide free labor for corporate platforms or contractors extract public money for proprietary code (1,6).

Generating Common Public Digital Infrastructure for Sovereignty

Decidim offers a concrete instantiation of what digital sovereignty can mean: not autarkic isolation, but the capacity of publics to govern the infrastructures shaping their collective life. This operates at multiple scales simultaneously—local, national, international—through shared infrastructure rather than fragmented isolation (6). The modular architecture and common core enable infrastructure that is both locally autonomous and globally interconnected, suggesting the potential emergence of a "public stack": a layer of digital infrastructure owned and governed by publics, interoperable across jurisdictions (4,9).

The Deliberate Construction of Community

Decidim offers crucial lessons about intentional community cultivation in open tech ecosystems. The project did not assume community would emerge spontaneously from code contributions; it actively constructed spaces, processes, and institutions to grow and sustain it. This responds to the evolution of traditional open source governance. Here, community becomes a primary design object, governance becomes explicit, codified, and democratically accountable. The governance evolution—from informal community to formal Association to international public committees—demonstrates remarkable reflexive institutional innovation, reflecting the understanding that community requires institutional scaffolding and that different project stages need different structures (2,7).

8. Conclusion: The Emerging Contours of a New Tech Governance Paradigm

Synthesizing and expanding the Decidim's lessons, we can discern the contours of an emerging alternative paradigm for technology governance:

- **Public purpose replaces private gain** as primary organizing logic. Technology serves democratic ends, not shareholder value.
- **Commons governance ensures accountability** beyond electoral cycles. The community holds the infrastructure, preventing capture by any single administration or corporation.
- **Multi-scalar sovereignty** enables autonomy at local, national, and transnational levels simultaneously, through shared infrastructure.
- **Deliberate community-building** creates resilient, diverse publics capable of governing complex sociotechnical systems.

- **Technopolitical integration** recognizes that code is constitution, architecture is policy, and every design decision carries political weight.

Decidim is not alone in this landscape. But its explicit theorization, sophisticated governance institutions, and growing international adoption make it a particularly rich case for understanding where open tech governance is heading.

Questions remain. Can this model scale? Can community governance evolve to include diverse public institutions worldwide? These remain unanswered.

What remains clear is that Decidim has demonstrated, in practice, that *another technological world is possible*: one where infrastructure is owned by publics, governed by communities, and built for democracy.

Notes and references:

1. Barandiaran, X. E., Calleja-López, A., Monterde, A., & Romero, C. (2024a). Decidim: A brief overview. In *Decidim, a Technopolitical Network for Participatory Democracy: Philosophy, Practice and Autonomy of a Collective Platform in the Age of Digital Intelligence*, 1-33. Springer Nature Switzerland

2. Decidim Organization Chart https://meta.decidim.org/assemblies/the-association/f/1723/?locale=es

3. Barandiaran, X. E., Calleja-López, A., Monterde, A., & Romero, C. (2024b). The Technical Plane: The Fabric of an Infrastructure. In *Decidim, a Technopolitical Network for Participatory Democracy: Philosophy, Practice and Autonomy of a Collective Platform in the Age of Digital Intelligence* (pp. 103-118). Springer Nature Switzerland.

4. Brazilian Government and Decidim Association Formalize Partnership with a Memorandum of Understanding, 20/12/2024. https://decidim.org/blog/2024-12-20-brazilian-government-and-decidim-association-formalize-partnership-with-a-memorandum-of-understanding/

5. Not with (the support of) Decidim. https://meta.decidim.org/assemblies/technopolitical-committee/f/1163/proposals?order=most_followed

6. Prieto Martín, P., & Smith, A. (2023). Decidim: Why digital tools for democracy need to be developed democratically. *Institute of Development Studies*. https://www.ids.ac.uk/opinions/decidim-why-digital-tools-for-democracy-need-to-be-developed-democratically/

7. Decidim Organization Chart https://meta.decidim.org/assemblies/the-association/f/1723/?locale=es

8. Engine Structure. DeepWiki Decidim https://deepwiki.com/decidim/decidim/2.1-engine-structure

9. Decidim. (2024). Brazilian government and Decidim Association formalize partnership with a memorandum of understanding. *Decidim Blog*. https://decidim.org/blog/2024-12-20-brazilian-government-and-decidim-association-formalize-partnership-with-a-memorandum-of-understanding/

10. Changes at "Economic sustainability" Blog Post. https://meta.decidim.org/processes/sustainability-governance/f/1795/debates/245/versions/7

11. FOSDEM. (2025). Building sustainability: A case study in funding diversification for Decidim. *FOSDEM 2025 Presentation*. https://archive.fosdem.org/2025/schedule/event/fosdem-2025-5552-building-sustainability-a-case-study-in-funding-diversification-for-decidim/

12. Welcome To The World Of Collaborative Tools: Decidim. https://ngi.eu/impact-stories/collaborative-tools/decidim/

13. OW2. (2025). Building digital commons with the public: It starts by reusing their projects. OW2 Presentation. https://pretalx.ow2.org/ow2con-2025/talk/VDL88C/

14. Decidim at Github. https://github.com/decidim/decidim

CSIL

Corso Monforte 15
20122 Milan, Italy
Tel: +39 02796630
E-mail: csil@csilmilano.com