Europe and the Future Web: from Findings to Opportunities

WEB4HUB: 'A SPACE FOR THE METAVERSE – VIRTUAL WORLD AND THE TRANSITION TO WEB 4.0'

Final synthesis workshop: discussion summary – 17 September, 2026

European Commission

PPMi
Part of the Verian Group

TNO

WEB4HUB

CONTENTS

Context 3

Session 1: Infrastructure and connectivity 3

Session 2: Architecture and trust 5

Open technologies and digital commons as infrastructure 5

Privacy-preserving AI: keeping European data useful without centralising it 6

Decentralisation: apply it selectively, but make the default explicit 7

Session 3: Sovereignty and competitiveness 8

Regulation needs to translate into architecture and technical requirements 9

Public-demand should bridge the gap between European innovation and adoption 9

International cooperation should focus on compatible alternatives rather than isolation 10

Conclusion **11**

Context

On **17 September 2026**, the European Commission and PPMI (part of the Verian Group) organised the final synthesis workshop of the project, entitled **"Europe and the Future Web: from Findings to Opportunities"**, within the initiative **WEB4HUB – A Space for the Metaverse: Virtual Worlds and the Transition to Web 4.0**.

The closed online workshop brought together **38 participants from 16 countries**, including policymakers from DG CNECT and other Commission services and experts in agentic AI, decentralised technologies, trust and security, internet infrastructure and internet governance. The project team presented the consolidated findings of the project[1] in three thematic sessions (infrastructure and connectivity, architecture and trust, and sovereignty and competitiveness), each followed by planned expert interventions and a moderated discussion. The workshop closed with an expert panel, which characterised Web 4.0 by the fusion of the physical and digital realms, its data intensity and potential for hyperpersonalisation, the growing presence of non-human actors and, beyond AI, emerging technologies that interface directly with the human body, and asked how the web can remain humane as these develop. Discussions during the roundtables were held under the **Chatham House Rule**.

The opening remarks placed the workshop in the context of live Commission work, including the negotiation of the Cloud and AI Development Act[2], the implementation of the open-source strategy and work on the future of the internet and internet governance. Participants were invited to consider whether regulation remains the primary instrument for tilting the web towards a more open, interoperable and decentralised architecture, or whether other levers are now needed. Overall, the workshop supported the project's cross-cutting conclusion that Web 4.0 will not be shaped by any single technology or policy intervention. Participants repeatedly returned to the interaction between infrastructure, architecture, market structure and governance, and to the need to act while agent discovery, identity, provenance and decentralised coordination remain open to influence.

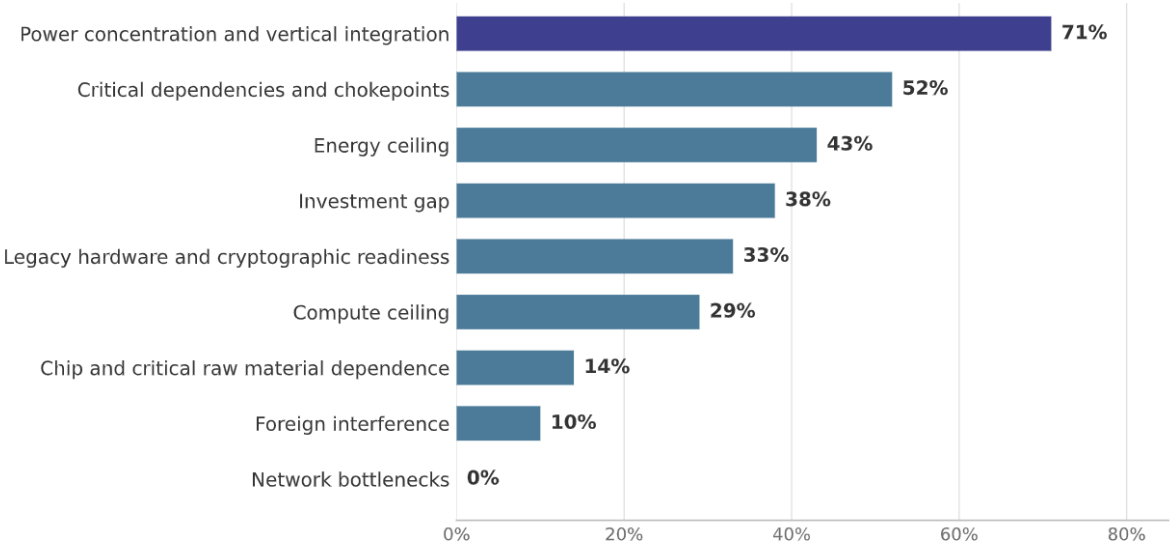
Session 1: Infrastructure and connectivity

The project team presented three trends shaping the infrastructure layer: the changing character of internet traffic, critical fault lines in connectivity and the compute and energy ceiling. Participants were asked through a live poll which challenges to building the infrastructure Web 4.0 will run on they considered most pressing.

[1] More information and the projects' thematic papers are available at: https://www.veriangroup.com/en-be/news-and-insights/web4hub-thematic-papers-web-4-0

[2] European Commission. (n.d.). Cloud and AI Development Act. Shaping Europe's digital future. Available at: https://digital-strategy.ec.europa.eu/en/policies/cloud-and-ai-development-act

Figure 1. Most pressing challenges for building the infrastructure Web 4.0 will run on



Notes: Share of respondents selecting each option. Respondents could select up to three options (n=21).

The poll reinforced **power concentration and vertical integration** as the most pressing infrastructure concern, selected by 71% of respondents, followed by critical dependencies and chokepoints (52%), the energy ceiling (43%), the investment gap (38%) and legacy hardware and cryptographic readiness (33%). This supported the project's finding that increasing European capacity is important, but that **capacity alone is not sufficient if it remains dependent on the same suppliers or coordination layers**.

Participants suggested that European infrastructure investment could be designed around **multi-provider access, interoperability, portability and exit options**, rather than treating the geographic location of infrastructure as a sufficient proxy for sovereignty. Funding and procurement could assess not only performance and capacity, but also whether infrastructure gives European users and authorities practical control over switching, auditability, data location, identity and security. Participants also linked **European capacity to regulatory enforceability**: local infrastructure can make the enforcement of European rules less dependent on the cooperation of external providers. Values cannot simply be embedded in technology, and Europe needs architectures over which it has sufficient practical control to exercise governance.

The discussion supported **managed interdependence**[3] **rather than technological self-sufficiency**, distinguishing dependencies according to the likelihood that access could be restricted or weaponised. Two qualifications were added. Although dependencies on politically aligned third countries were seen by some as lower risk, others cautioned that **political alignment is not permanent**, that large technology firms have become geopolitical actors in their own right, and that replacing a non-European supplier with an equally concentrated European one does not by itself reduce structural dependence. Dependency assessments should therefore consider **corporate concentration alongside jurisdiction** and be revisited periodically.

Participants further pointed to dependencies between physical infrastructure and services. **Middleware** was described as under-mapped: real-time engines, 3D tooling and comparable components are largely

[3] The study's use of managed interdependence is based on the JRC's concept of "modular resilience", which accepts that some interdependencies are unavoidable while reducing those that are feasible and strategically important to reduce, and on the approach of the European Technological Sovereignty Package. See Fratini, S., Pohle, J., Di Marco, D., Thabit Gonzalez, S., & Sgueo, G. (2026). Digital sovereignty as a geopolitical strategy: Navigating dependencies, power, and democratic resilience in a changing global order (JRC146878). European Commission, Joint Research Centre. Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC146878; European Commission. (2026). European Technological Sovereignty Package (COM(2026) 503 final).

non-European, which constrains interoperability and the integration of AI into Web 4.0 services. **Data was framed as infrastructure**, with a large gap noted in European developers' access to public data for model training, including domain-specific and multilingual data. This connects to the emphasis in the State of the Union address[4], delivered the day before the workshop, on specialised models built on European data. The discussion implies extending the mapping of dependencies beyond compute, connectivity and energy to middleware and training data.

Session 2: Architecture and trust

The project team presented three trends shaping the architecture and trust layer: the trust architecture needed for autonomous agents, collective intelligence under pressure and decentralisation reshaping the architecture of the future web. Participants were also asked to position Europe on the project's four-scenario framework, first where current trends are likely to lead by 2035 and then where Europe should seek to be (see section below).

Open technologies and digital commons as infrastructure

One of the clearest additions from the workshop was the call to treat **open-source software and digital commons as infrastructure rather than as a sequence of innovation projects**. Rather than using public funding primarily to correct market failures, participants proposed using it to **deliver the public functions of digital ecosystems that markets do not provide**. Public service broadcasting was the reference model: a deliberate institutional architecture, with dedicated funding, that sustains services of public value without relying on market incentives. Participants asked what equivalent **institutional architectures for stewardship** of the digital commons would look like. Europe was described as already funding substantial open-source experimentation, but with support insufficiently connected to adoption, maintenance and the needs of public institutions. The proposed direction was to connect research funding with **public procurement, deployment and long-term stewardship**. The table below records the follow-up actions raised.

Table 1. Possible follow-up actions on open technologies and the digital commons

Area	Possible follow-up action emerging from the workshop
Funding	Provide more multi-year support for maintenance, security and governance of critical open-source and open-knowledge resources, rather than primarily financing new development.
Procurement	Use public institutions as anchor users of viable open and interoperable technologies, giving them reference deployments and predictable demand.
Scaling	Link Horizon/RDI-funded experimentation more explicitly to adoption pathways, including integration, testing, procurement readiness and sustained operation.
Stewardship	Recognise that public institutions can help steward technological ecosystems, not only purchase finished products. Explore dedicated institutional architectures and funding frameworks for stewardship of the digital commons, drawing on the public service broadcasting model.
Commons beyond code	Extend support to knowledge bases, datasets, human-created content and other collective-intelligence resources on which AI systems increasingly depend.

[4] European Commission. (2026, September 16). State of the Union 2026. https://commission.europa.eu/strategy-and-policy/state-union_en

Participants also highlighted a societal dimension of the commons. Openness was described as the internet's historic strength but also as the condition that allowed today's concentrations to form, so the task is to sustain openness in ways that do not lead back to concentration. Generative AI was seen as straining the social contract that has sustained the creativity of the online environment and the people who maintain it. Asked where Europe could become a frontrunner, participants pointed to **reliable and trustworthy content for citizens and their agents**, human-generated content and open digital infrastructure, and argued that a freer web depends on **content quality and pluralism**, not only on decentralised technologies. A possible avenue would be to explore how **public-service broadcasters, independent media, cultural institutions and universities** could contribute machine-readable, provenance-rich and appropriately licensed content to open or federated knowledge infrastructures. Measures mentioned included common provenance and attribution standards, controlled access mechanisms for trustworthy content, licensing and compensation models for automated reuse, and keeping public-interest content discoverable by agents.

Finally, participants cautioned against framing the digital ecosystem as a choice between **state and market**. Community organisations, foundations, open-source maintainers and knowledge communities were described as **infrastructure maintainers and governance institutions** in their own right, not only as stakeholders to be consulted. Possible follow-up actions include support for civil-society participation in standards processes and meaningful governance roles for non-commercial stakeholders in EU-funded digital infrastructures.

Privacy-preserving AI: keeping European data useful without centralising it

A concrete proposal concerned **keeping sensitive or commercially valuable European data local while allowing AI systems to use it**, by moving AI processing to the data rather than transferring data to an external AI provider. Confidential-computing environments were suggested as one way for one organisation's model to perform inference over another organisation's data without either party accessing the other's underlying information. This was not treated as settled. Some participants pointed to the limitations of trusted execution environments and argued for continued research into **fully homomorphic encryption (FHE)**, while others favoured a dual track: deploying confidential computing where appropriate now while investing in FHE and other approaches that may offer stronger guarantees later.

Two technical points were raised. First, participants noted that confidential-computing capability for AI accelerators is currently available primarily from a single vendor[5], so that an architecture built on trusted execution environments **reintroduces the hardware concentration risk discussed under infrastructure**, whereas FHE does not require trusted hardware. The choice between the two tracks was therefore described as a dependency choice as much as a question of maturity. Second, it was noted that remote attestation verifies the integrity of the server software but not where the data is sent, and that binding attestation evidence to the TLS session, while used in some production deployments, is still being standardised at the IETF[6]. Any Commission support for confidential computing should therefore specify **attested, standards-based deployments**. Taken together, this points to a possible RDI direction: **privacy-preserving AI inference and data-sharing architectures**, with a focus on interoperability, assurance and reduced dependence on single hardware or cloud providers. Confidential computing for decentralised AI and privacy-preserving protocols in the agentic web were also among the areas participants named where Europe could lead.

[5] GPU-based confidential computing for AI workloads was introduced with NVIDIA's Hopper (H100) architecture, described by the vendor as the first GPU with a hardware-anchored trusted execution environment. See NVIDIA (2023). Confidential computing on H100 GPUs for secure and trustworthy AI. Available at: https://developer.nvidia.com/blog/confidential-computing-on-h100-gpus-for-secure-and-trustworthy-ai/. CPU-based trusted execution environments are available from several vendors.

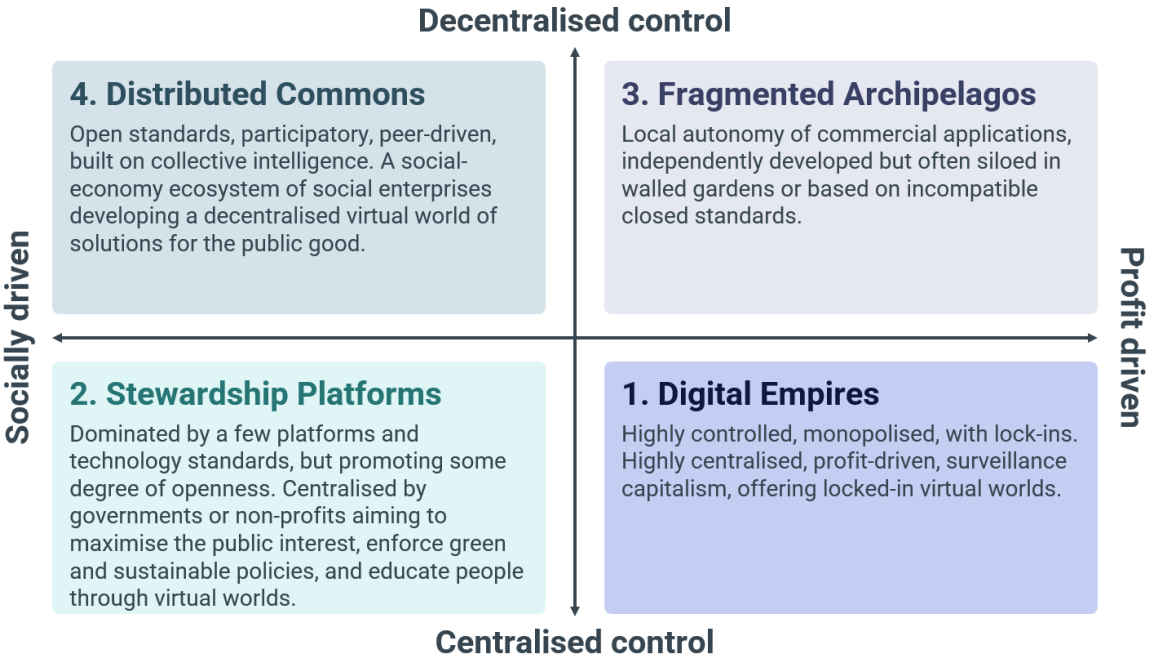
[6] IETF (2026). Attestation in TLS/DTLS, Internet-Draft draft-fossati-seat-early-attestation-05 (work in progress). Available at: https://datatracker.ietf.org/doc/draft-fossati-seat-early-attestation/.

Decentralisation: apply it selectively, but make the default explicit

Participants broadly supported the project's argument that technical decentralisation does not automatically decentralise control. Some proposed a stronger starting principle than the project currently uses: "**decentralised unless**", grounded in subsidiarity. Functions would be performed at the lowest feasible level, with federation or more centralised coordination introduced only where there is a clear functional reason. Without such an explicit default, it was argued, cost and complexity repeatedly push systems back towards centralisation, and some federated projects have already been captured by concentrated actors. The EUDI Wallet was cited as an example of subsidiarity in practice: users hold their own credentials, but these are issued by qualified providers.

The scenario exercise illustrated this concern. Throughout the project, four Web 4.0 scenarios have been used to think about how technology, markets and governance could evolve. They are organised along two axes: whether control over the functions that others depend on (identity, discovery, provenance, access to knowledge, payments) becomes more concentrated or more distributed, and whether these systems are shaped around commercial value capture or around social and public-interest objectives. The scenarios are not forecasts and are not mutually exclusive.

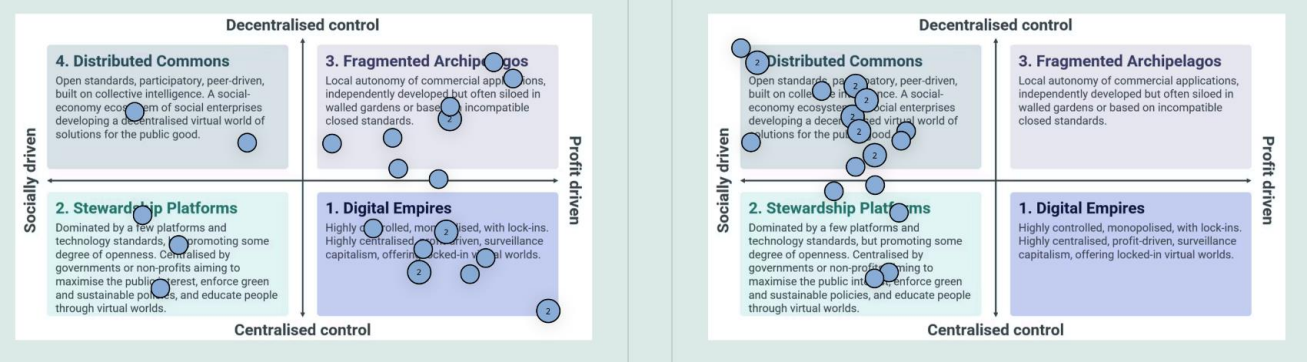
Figure 2. The four Web 4.0 scenarios used in the project[7]



Participants were asked to position Europe on this framework twice, and the two answers differed sharply. Expectations concentrated on the profit-driven side: of 24 responses, 11 placed Europe in Digital Empires and 8 in Fragmented Archipelagos, with only 3 in Stewardship Platforms and 2 in Distributed Commons. Asked about the desired direction, all 23 responses fell on the socially driven side, 18 in Distributed Commons and 5 in Stewardship Platforms, with a visible cluster along the boundary between the two.

[7] More information about the scenarios is available at: https://www.veriangroup.com/hubfs/BE/EUMI%20(LT)/Decentralised%20data%20and%20architectures_vfinal_draft.pdf

Figure 3. Expected scenario if current trends continue (left) and desired scenario for Europe (right)



Notes: Each dot represents one response placed by a participant on the scenario framework (n=24 for the expected scenario, n=23 for the desired scenario).

Three readings follow. Participants expect that, without intervention, **the dynamics of the current web** (vertical integration, network effects and dependence on a small number of providers) **will reproduce themselves in Web 4.0**, as renewed concentration or as fragmentation. The preferred direction clusters between Stewardship Platforms and Distributed Commons, matching the view that both have a place: distribution alone can produce fragmentation or new chokepoints, so some trusted coordination remains necessary, and the question is who provides it and under what conditions. The gap between the two positions is the space where EU action is required, and it points towards structural measures that change who controls coordination functions rather than safeguards applied to a structure otherwise left to develop on its own.

Participants also gave examples of why a blanket decentralisation principle would be inappropriate. Healthcare data illustrated cases where transferring full control to individuals could remove protections associated with trusted institutions, for example by taking data outside patient confidentiality rules and exposing patients to pressure from insurers, so that **hybrid and federated models may sometimes protect rights better than maximal decentralisation**. Commercial data offered a related point: people may benefit from maintaining separate contexts or "personas" rather than having all behavioural data merged centrally. Social media was raised as a case where decentralisation alone is insufficient, since federated platforms do not change the **commercial incentive structures that shape content**, and the same polarisation dynamics could be reproduced on a different architecture. Reference was made to the European Parliament's recently adopted report on the European democracy shield[8], which recognises both the infrastructures and the commercial logics behind these harms. Participants also acknowledged that users cannot be made to adopt decentralised platforms artificially, and that these need to become credible alternatives in their own right. The practical implication is that European programmes could require project promoters to justify **where coordination needs to be centralised and where functions can be distributed**, rather than treating either model as intrinsically preferable.

Session 3: Sovereignty and competitiveness

The project team presented three trends, European frontier AI competitiveness, power concentration, and dependencies and sovereignty, together with the four priority areas proposed by the project. Participants were asked to rate the four priority areas by the effort required and the urgency of action (see the conclusion).

[8] Bentzen, N. (2026, September 7). Findings and recommendations of the Special Committee on the European Democracy Shield. European Parliamentary Research Service. https://eprs.europarl.europa.eu/contents/publications/EPRS/2026/09/EPRS_ATA(2026)791474.html

Regulation needs to translate into architecture and technical requirements

A strong theme was that **legal rules alone will not necessarily deliver European values if the underlying technical architecture makes those rules difficult to enforce**. Existing European principles, for example on workplace monitoring and algorithmic management, were seen as already providing a basis for Web 4.0 governance. The challenge is increasingly how these principles are translated into standards and system design, and into architectures that people actually choose to use, since a well-designed rule that is inconvenient for users will not be adopted in the market. Participants argued that restrictions on paper may be ineffective unless organisations operating in Europe are also subject to **design requirements**. The case was put by analogy: bridges are built to safety specifications as a matter of course, and digital architectures should not be exempt from equivalent requirements. Architectures capable of implementing rights and governance requirements were described as a potential European competitive proposition and an exportable model, while acknowledging that acting on this runs against a widespread preference to leave technology to the market and requires political will.

Enforcement of existing rules, including the **Digital Markets Act** (DMA) and the GDPR, was described as **demanding in practice** where the infrastructure sits with providers outside Europe. Building European capacity was seen as a way to make enforcement less dependent on external providers and to let public authorities implement governance requirements directly at the technical level. Participants also distinguished two issues that should not be conflated: whether a technology is aligned with European values, and **who controls the infrastructure on which it operates**. A system could comply with European safeguards while still increasing structural dependence. This aligns with the project's recommendation to **adapt existing frameworks rather than automatically create new legislation**, while using standards, codes of practice, procurement conditions and pre-standardisation work to turn principles into implementable requirements.

Public-demand should bridge the gap between European innovation and adoption

Participants reinforced the project's demand-side sovereignty recommendation. Europe already funds strong technological experimentation but does not always connect it to **deployment, adoption and market formation**. Public procurement was suggested as a source of early customers for open, interoperable and European alternatives, particularly in public administration, education, health and research. Procurement could move beyond European-origin criteria to requirements such as **interoperability, portability, open interfaces, data control, switching arrangements and transparent governance**, so that public demand shapes the market structure of Web 4.0 rather than purchasing capacity after markets have consolidated.

Participants also identified a limit to this approach. If the public sector shifts to open alternatives while citizens and businesses remain with incumbent providers, the overall market structure does not change. The project's reference to citizen engagement was noted as lacking corresponding actions. The demand-side recommendation should therefore also address the **private side**, making switching possible and attractive for users and firms and supporting decentralised platforms to scale. Two regulatory suggestions followed. First, the **Data Act** contains provisions on cloud switching and access to data that are relevant to agentic AI, but its evaluation is not due until September 2028[9]. Participants suggested bringing forward an assessment of whether these provisions are fit for purpose in an agentic environment, or issuing guidance on how the Data Act applies to AI agents. Second, a comparable fitness check was proposed for the DMA, so that emerging agent gateways are covered before positions become entrenched. A further suggestion

[9]Regulation (EU) 2023/2854 (Data Act), Article 49, requires the Commission to evaluate the Regulation by 12 September 2028.

linked demand-side action to the announced measures on children's access to social media: rather than relying on restrictions alone, participants proposed developing **curated European alternatives** for younger users, and encouraging young people towards study and careers outside the large incumbents.

International cooperation should focus on compatible alternatives rather than isolation

The discussion supported the framing of sovereignty as **managed interdependence**[10]. European sovereignty should not be framed only as competition with US or Chinese providers, and cooperation with countries sharing similar goals can expand Europe's room to act. European goals around privacy, participation and civil-society involvement were described as a strategic strength in themselves. A practical implication would be to prioritise international cooperation around **interoperability, privacy-preserving protocols, agent identity and safety, open standards, evaluation and mutual recognition**, while using trusted partnerships to diversify dependencies that cannot realistically be eliminated.

[10] The study's use of managed interdependence is based on the JRC's concept of "modular resilience", which accepts that some interdependencies are unavoidable while reducing those that are feasible and strategically important to reduce, and on the approach of the European Technological Sovereignty Package. See Fratini, S., Pohle, J., Di Marco, D., Thabit Gonzalez, S., & Sgueo, G. (2026). Digital sovereignty as a geopolitical strategy: Navigating dependencies, power, and democratic resilience in a changing global order (JRC146878). European Commission, Joint Research Centre. Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC146878; European Commission. (2026). European Technological Sovereignty Package (COM(2026) 503 final).

Conclusion

Participants were asked to rate the project's **four priority areas by effort and urgency**. All four were seen as requiring substantial effort and relatively early action. Inclusive global governance was rated most urgent (7.6 on a 10-point scale), followed by decentralised and federated architectures (7.4) and demand-side sovereignty (7.1), with the latter two also rated as the most demanding. Open Web 4.0 and collective intelligence scored somewhat lower on both urgency (5.9) and effort (6.6). Given how strongly the discussion emphasised the commons and trustworthy information, this probably reflects the more diffuse nature of that priority rather than lower importance.

Figure 4. The four priority areas proposed by the project

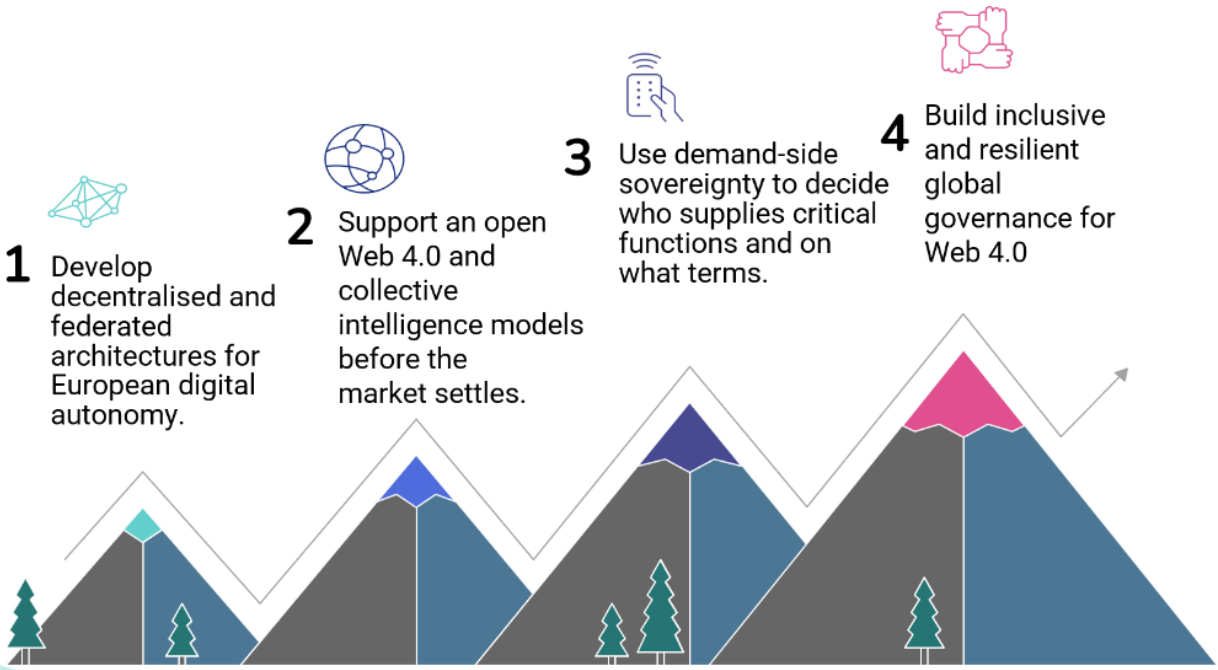


Figure 5. Effort and urgency of the four priority areas, average participant rating



Participants disagreed on how the four priority areas relate to one another. One view was that decentralised and federated architectures are the **causal first step**, so that the other three follow largely as a consequence. Another view treated the four as mutually dependent, with demand-side sovereignty (procurement conditions on source code availability, open standards and cloud portability) as the main lever for delivering federated architectures, and inclusive governance as their necessary complement, because once technical control is distributed, power asymmetries reappear in standardisation bodies and global governance structures.

Asked where Europe could become a frontrunner in Web 4.0 over the next five to ten years, participants' suggestions fell into six clusters: trusted content and human-generated knowledge; digital commons and open digital infrastructure; privacy-preserving and confidential computing for decentralised AI; open protocols and user-controlled data architectures, including the AT Protocol, where Europe was described as well positioned; rights-based regulation and rights-respecting technology exported as European alternatives; and sectoral or partnership-based routes such as Web 4.0 services for energy, domain-specific agents, age verification and cooperation with new regions.

Taken together, the workshop did not point towards a single technological route for Europe. It did suggest five messages that are largely aligned with the recommendations of the project:

1. **Public investment should shape market structure**, not merely add capacity.
2. **Open alternatives need an adoption and maintenance pathway** from RDI funding to procurement, deployment and stewardship.
3. **European values need technical implementation mechanisms** through standards, procurement specifications and system design. '

4. **Data should not automatically move to whichever actor owns the strongest AI model**, since privacy-preserving and federated approaches can allow European data to create value while reducing concentration.
5. **Trusted information and collective intelligence should be treated as strategic infrastructure**, because agents themselves will depend on the knowledge environment from which they retrieve and act.

The workshop ended on a deliberately positive note. Participants cautioned against framing Web 4.0 primarily through European weakness or technological catch-up. Web 4.0 does not only present new risks, but also opens up a plethora of opportunities for citizens and companies (e.g. democratic participation, access, opportunities to develop new services). Moreover, dominance at foundational layers does not automatically determine outcomes at every layer above them, and Europe's market size, developer base, regulatory experience and public institutions were highlighted as the assets on which such a strategy could build. The EU DLT regulatory sandbox, which brought some 60 European projects to at least technology readiness level 5 within three years, was cited as evidence that Europe can build this capacity. A more cooperative framing of sovereignty, recognising shared challenges and opportunities with like-minded partners, was seen as part of that more confident stance.