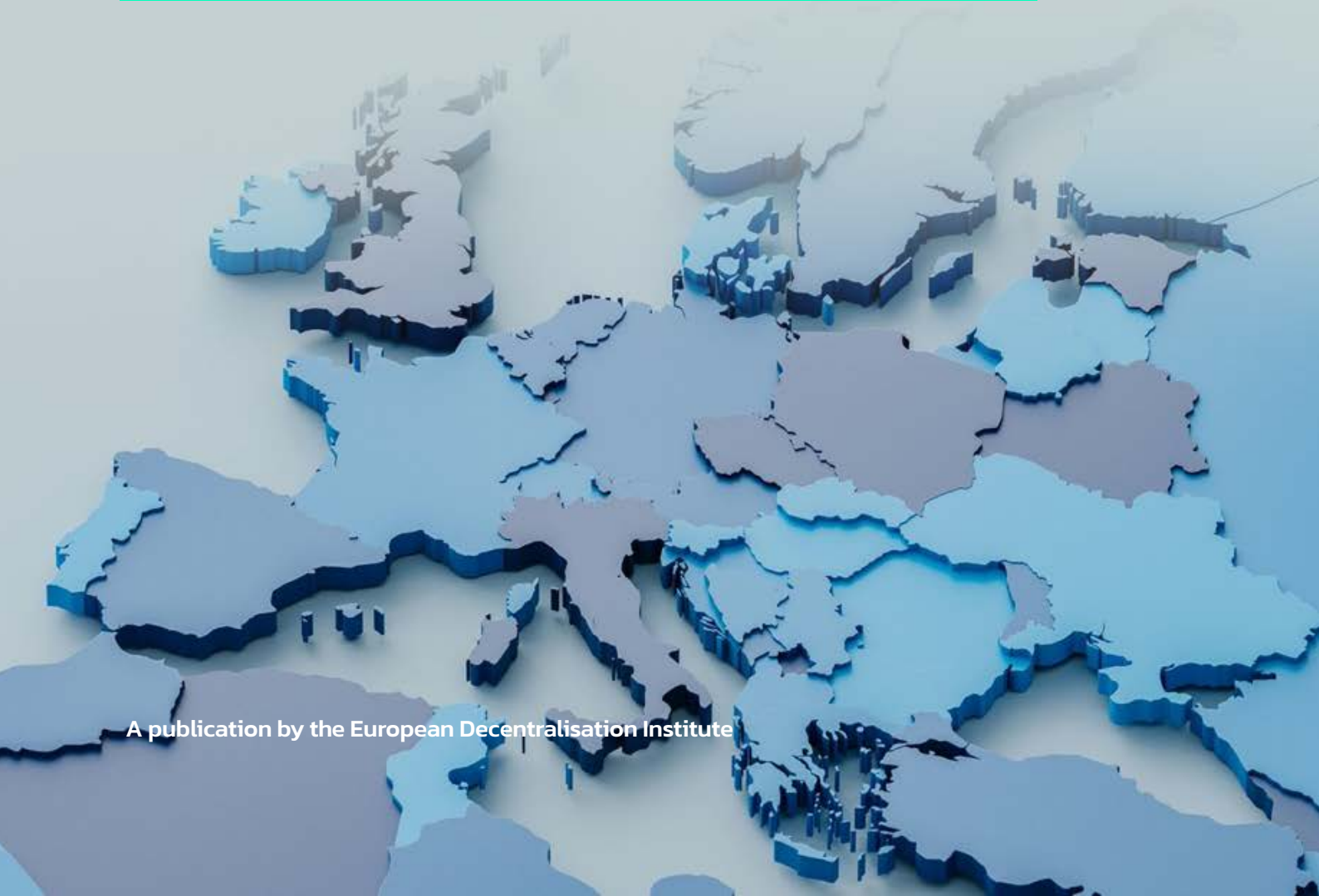




Rebalancing Europe's Digital Power

Decentralisation as a practical route to Digital Sovereignty.



November 2025

A publication by the European Decentralisation Institute



01. Abstract

Europe excels at writing digital rules, yet much of its backbone (cloud, payments, identity, AI) runs on non-European, highly centralised infrastructure. This dependency limits Europe's ability to enforce its own norms and act under stress, creating a sovereignty gap: policy ambition in Brussels depends on systems Europe neither owns nor can fully steer.

In a world of geopolitical tension, asymmetric cyber threats, and AI-driven disruption, that gap directly constrains economic security, crisis response, and democratic resilience. We define digital sovereignty as the ability of citizens, organisations and governments alike to act independently, predictably, and legitimately in the digital realm when vital functions are at stake. Regulation is not enough. Sovereignty requires that control over keys, code, and control planes is distributed to the lowest competent level (subsidiarity in digital form) across citizens, organisations, nations, and supra-national bodies: digital subsidiarity.

We argue that decentralisation is the practical route to embed sovereignty into infrastructure. By distributing control across verifiable, accountable networks of citizens, organisations and governments, decentralisation reduces single points of failure, improves auditability and recovery, and aligns with Europe's principles of shared governance. It is not an ideology to deploy everywhere, but a design choice where it raises resilience, privacy, agency, and accountability and where it can grow a distinct European industry for digital infrastructure and services.

We propose four priorities for the next 36 months:

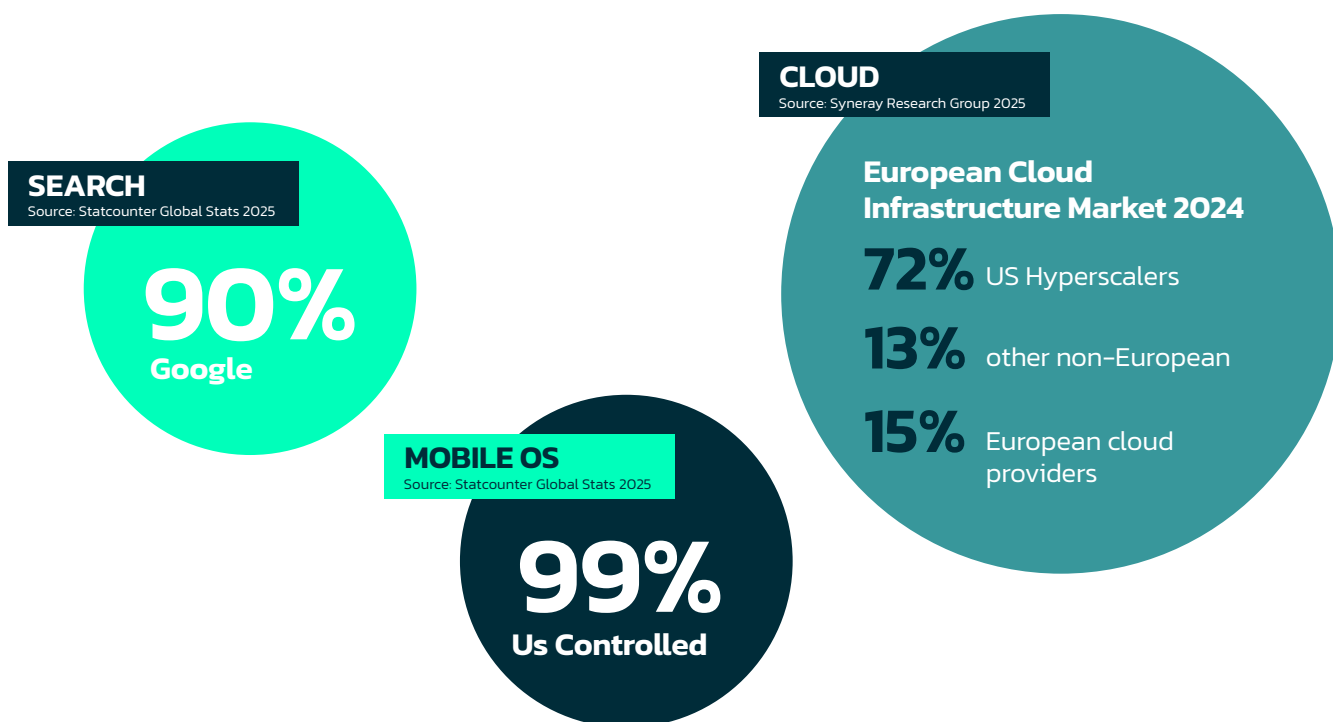
- 1. Adopt a Decentralisation for Digital Sovereignty Framework (DDS Framework)**
Operationalise through expedited amendments to existing regulations like eIDAS2, NIS2, MiCA and DORA.
- 2. Redefine the EU Digital Infrastructure Fund**
Back open protocols tied to interoperability standards and independent test suites. Leverage blended finance to crowd-in industry.
- 3. Move to governance-first regulation**
Make protection of digital sovereignty an enforceable requirement in any new regulation.
- 4. Introduce a "Total Cost of Centralisation" scorecard**
Track dependence, resilience and auditability across all government-procured systems.

“

Rebalance, not retreat. This playbook moves Europe from intent to capacity, builds the rails we can steer in a crisis, and turns our laws into operational power.

02 Sovereignty on Borrowed Infrastructure

Digital infrastructure has become the backbone of our lives, economic competitiveness, public administration, and security in Europe. But most of that backbone is non-European, and in the hands of a few. International commercial platform providers as well as foreign state-backed tech giants control identity services, cloud infrastructure, payment rails, and AI models that determine citizens' ability to enjoy their Fundamental Rights and Freedoms.¹



Europe's dependence on external infrastructures means that its digital and physical futures are increasingly shaped elsewhere. **We are no longer independent.** Or as ECB President Christine Lagarde said in a recent speech: *"Independence has always been guaranteed by balance. Countries built systems of strategic balance to prevent the strong from dominating the weak. Today, it rests on system power: the ability to manage the dependencies created by the infrastructures and technologies that bind us together."*²

¹ Under the European Convention on Human Rights and the European Charter of Fundamental Rights and Freedom
² https://www.ecb.europa.eu/press/key/date/2025/html/ecb.sp250915_1-9d3e96b972.en.html

The sovereignty gap

The answer within Europe thus far has been to regulate. And while Europe excels at writing rules, its backbone runs on infrastructure or protocols it does not control. **That gap between policy ambition and infrastructure control is what we call the sovereignty gap.** It manifests in weak enforceability, delayed recovery, loss of confidence and heightened strategic vulnerability when the levers of our digital society and economy are controlled by others.

“

Europe’s problem is not overregulation, it is the lack of digitalisation.

Exceptional situations are the stress test: especially during geopolitical tensions, such as cyber-attacks, asymmetric digital warfare, military campaigns, or AI/intelligence supply shocks, the sovereignty gap limits governments from acting. Decisions only matter if underlying rails can be steered, audited, and, in emergencies, lawfully overridden.

The call for digital sovereignty is growing ever louder

Digital sovereignty is the ability to act independently, predictably, and legitimately in the digital dimension when vital functions are at stake. It includes the lawful right to declare exceptions and to steer infrastructure in emergency situations without undue dependence on external actors or foreign technologies.

Digital sovereignty matters at different levels. It matters for citizens, who need the capacity to exercise their fundamental rights such as freedom of expression and individual privacy. It also matters for organisations in industry and civil society, which depend on the ability to be economically competitive and free from external influence. Finally, it matters for states and supra-national bodies, which must remain independent from foreign interference in exercising their core tasks of providing security, stability, and welfare for their citizens.

In practical terms, achieving digital sovereignty requires aligning the governance of digital infrastructures with European values, norms and institutions. The controls that matter – keys, code, control planes – must be within reach of European citizens, organisations, states and supra-national bodies, both in times of peace and in times of crisis.

The call for digital sovereignty across Europe is growing louder

December '22

"Der Bundesrat wird beauftragt, Bericht zu erstatten, wie er "Digitale Souveränität" für die Schweiz definiert; wie er den Stand der digitalen Souveränität unseres Landes beurteilt; welche übergeordnete, umfassende Strategie zur Stärkung der staatspolitisch, wirtschaftlich und gesellschaftlich als von höchster Bedeutung einzuordnende digitale Souveränität unseres Landes er zu ergreifen gedenkt."

[Motion 22.4411 Swiss Parliament](#)

March '25

"Europe needs to recover the initiative, and become more technologically independent across all layers of its critical digital infrastructure."

Ninety smaller European technology firms and lobby groups have urged European Commission President Ursula von der Leyen to create a sovereign infrastructure fund to ramp up public investments in cutting edge technologies, [according to Reuters](#).

August '25

"In light of the global economy's evolution, one thing is now clear: no country which aspires to prosperity and sovereignty can allow itself to be left out of the race for critical technologies. The United States and China openly use their control of strategic resources and technology to obtain concessions in other areas; any excessive dependence thereby becomes incompatible with a future in which we are sovereign."

[Mario Draghi in Groupe d'études géopolitique](#)

September '25

"I want us in Europe, not just us in Germany, but we in Europe as a whole, to become more independent."

[Friedrich Merz on digital sovereignty](#) while addressing the audience at the Schwarz Ecosystem Summit in Berlin.

It's a root cause

The **sovereignty gap** is the root cause of almost everything and not "yet another topic" on the policymaker's desk. This sovereignty gap is a systems problem: security, AI provenance, industrial competitiveness, data protection, identity, payments, energy, logistics: they all depend on who governs the rails beneath them. Fix the rails once; reduce firefighting across files. Many of today's challenges hinge on who governs the digital infrastructure beneath them: the security and continuity of critical services, the safety and provenance of AI models, industrial competitiveness, and data protection, as well as the foundational systems for payments, identity, energy, and logistics.

“

If Europe cannot control the rails, every downstream policy becomes a best-efforts exercise.

And decentralisation is the answer

The way out of this is by redeveloping the capability and gaining back the capacity to govern rights and strategic digital infrastructures autonomously, under sovereign authority, within decentralized systems, at all levels: the design of the architecture, the protocols, the lines of code.

Decentralisation disperses power, reduces systemic dependency, and strengthens resilience by eliminating single points of failure. Rather than shifting dominance from one actor to another, decentralisation embeds balance within governance and architecture itself. It aligns autonomy with accountability, thereby ensuring that no single entity can unilaterally dictate the rules.

“

By distributing authority across networks, decentralisation transforms digital infrastructure from a site of dependency into an enabler of sovereignty.

03 Decentralisation to rebalance control over infrastructure

Why decentralisation matters

Decentralisation means that agency in a system is distributed to independent entities capable of managing their own resources best, thereby prioritising the agency of the parts over that of the whole. As a principle of governance, decentralisation resonates with the subsidiarity principle, one of the core principles of European governance.

Technological advances over the past decades have made this possible by levelling the information playing field and enabling coordination among parties that need neither prior familiarity nor mutual trust.

Decentralisation enables citizens to exercise their fundamental rights independently, e.g., through privacy-by-design architectures that embed autonomy and protection into the system itself. It helps organisations to make use of standardised trusted infrastructures for payments, communications, and other vital functions, for instance through blockchain-based standards. It also strengthens the capacity of states to rely on resilient digital infrastructures that resist hostile capture, for instance through decentralised network security architectures.

As a governance strategy, decentralisation redistributes power within digital infrastructure from a single center to a network of accountable stakeholders. It solves the 'system power' challenge put forward by Ms. Lagarde as it rebalances dependencies in our digital society. It also allows to propagate –even embed– norms and values that a sovereign citizen, community, society, state or group of states hold dear. Privacy, for example. Or democracy. Or self-determination.

“

Therefore decentralisation is an enabler of true digital sovereignty. Without it we just replace one central chokepoint with another.

Alternative paths to digital sovereignty

The Adapter Strategy

Vendor “sovereignty packages” from companies like AWS, Microsoft and Google can reduce risk, yet they usually keep a central core that cannot be controlled decentrally. Europe should favour decentralised governance planes: these include custody of critical keys under European control, code that is open to independent conformance testing, clear shutdown and exit rights, and verifiable governance for rule changes. That is how infrastructure carries our laws and values, not just our workloads.

• **Reduces risk, does not eliminate dependency.**

Federated Systems

Federated architectures like GAIA-X attempted sovereignty through coordination layers atop existing infrastructure. This failed because federation without foundation is decoration. True sovereign design requires: (1) Root control of consensus mechanisms, (2) Absence of non-EU dominant control, (3) Cryptographic proof of computation location, (4) Hard-coded compliance primitives that cannot be overridden by external actors. Decentralisation for Digital Sovereignty offers sovereign-by-design, not federated-by-hope.

• **Without root control, sovereignty is cosmetic.**

Legal Sovereignty

The Bretton Woods collapse (1971) proved that legal agreements without infrastructure control are suggestions. Despite binding treaties, the U.S. unilaterally ended dollar-gold convertibility because it controlled the infrastructure (Federal Reserve). Similarly, SWIFT’s 2022 Russia exclusion demonstrated that payment sovereignty resides with infrastructure operators, not law writers. History shows: control the rails or become cargo.

• **Law without enforcement power is theatre.**

Decentralise only what matters: strategic infrastructure

Digital sovereignty especially matters when dealing with strategic infrastructure. Infrastructure is strategic when it underpins core public, economic, or democratic functions and if its failure disrupts society. Think identity services and payments, public registries, energy balancing, and core data or compute capacity.

Strategic infrastructure impacts different levels of decision-making. For political institutions, it is crucial that they are able to execute their mandate and take full accountability for the decisions they take – without being pressured by external forces. Economic actors, such as SMEs, need to be able to trust the infrastructure of rules, standards, and interfaces without fearing to be dependent on powerful centralised organisations. Governments, corporations, and citizens require access to technical architectures that guarantee their basic rights and capacities.

Decentralisation as a strategy to guarantee digital sovereignty needs to be responsive to these levels of decision-making. Although it is concerned with strategic infrastructure, decentralisation is not a purely technical matter but **needs to align political, administrative, and architectural concerns:**

1. **Political decentralisation** implies that the capacity to make decisions and implement rules is distributed amongst capable stakeholders, in line with the subsidiarity principle.
2. **Administrative decentralisation** relies, somewhat counterintuitively, on strengthening logical coherence and interoperability between systems; ensuring common standards, rules, and interfaces that make behaviours predictable.
3. **Architectural decentralisation** implies that digital infrastructures are run by a polycentric network of nodes, for instance computational validators, without any centralised single point of failure.

In so doing, power is shifting to auditable protocols and replaceable institutions, not just new intermediaries.

These levels of decentralisation interact: governance cannot authorise what the architecture cannot enforce; logic must be verifiable against both. Design tests follow from this system's view: no single actor should be able to veto or secretly override a vital function; upgrades follow timed, observable processes; users have real exit paths across implementations. In short, decentralised governance is preferable to reliance on a single hub. Power shifts to protocols and institutions that are observable, auditable, and replaceable, not just to new intermediaries with different logos.

“

Decentralisation should be applied deliberately and selectively where it improves resilience, privacy, agency and accountability, and not as a universal ideology.

It allows Europe to strengthen and grow its digital startups and scale-ups into a distinctive and competitive industry.

04. Four policy priorities for the next 36 months

Decentralisation to achieve digital sovereignty is not only feasible, it is also necessary. The traditional view that 'law remains national' (Bindseil & Senner 2025) fundamentally misunderstands digital reality: **when the rules run on foreign infrastructure, the sovereignty is contingent on someone else's discretion.** Europe can and should invert that logic: build sovereign, decentralised infrastructure first. By distributing control across audited protocols and accountable institutions, we remove single choke points, create real exit paths, and embed European rules into the rails themselves. This cuts the hidden 'trust tax' of dependency and turns enforcement of regulation from ex-post paperwork into ex-ante capability³. In so doing, Europe actively responds to today's critical policy challenges:

- **Artificial Intelligence:** enforceable model provenance and auditable accountability.
- **Data protection:** selective disclosure built into design, not post-hoc promises.
- **Competition and SME growth:** interoperability by default, avoiding platform lock-ins.
- **Payments and energy resilience:** decentralised architectures that cannot be "switched off."
- **Government Continuity:** infrastructures that remain operational in times of crisis.

1 – Adopt a Decentralisation for Digital Sovereignty Framework (DDS Framework)

To make it actionable, Europe should adopt a Decentralisation for Digital Sovereignty Framework (DDS Framework) – not another strategy document but binding legislation with teeth – that mandates decentralised governance across –to begin with– four pillars: 1. digital identity, 2. financial sovereignty, 3. energy resilience, and 4. AI autonomy. Link regulators, infrastructure providers, and innovators; name owners and timelines; publish results.

Short term actions under the DDS Framework entail several regulatory amendments:

- **eIDAS 2:** Add Article 12a mandating DID support
- **MiCA:** New Chapter VII on permissionless settlement layers
- **NIS2:** Expand Article 21 to cover decentralized infrastructure resilience testing
- **DORA:** Article 17 amendment for public blockchain dependency management

³ Without infrastructure control, any Regulatory Act becomes theater: de jure sovereignty (laws) without de facto sovereignty (execution) is performative.

2 - Redefine the EU Digital Infrastructure Fund

Create an EU Digital Infrastructure Fund. Co-finance open protocols and shared services tied to interoperability standards and independent test suites. Leverage blended finance to crowd in industry.

3 - Move to governance-first regulation

Start shaping requirements for protocol governance, constitutional change controls, dispute processes, transparency and audit, similar in spirit to how ICANN governs rule changes. Focus on how digital institutions change their rules, not only on policing conduct after the fact. Make protection of digital sovereignty an enforceable requirement in any new regulation.

4 - Measure what matters

Track resilience under exercise, independence from single vendors, enforceability by design, and adoption across borders. Add a simple Total Cost of Centralisation scorecard to make hidden risks visible in every procurement. Here's what the Total Cost of Centralisation scorecard could measure:

- a. Exit costs and switching time
- b. Key custody and operational control
- c. Auditability of processes and data flows
- d. Systemic concentration risk across providers and regions
- e. Emergency steering rights under European law

Track progress

Independence: Within 24 months, $\geq 30\%$ of all Tier-1 digital services must operate on infrastructures that allow verifiable exit and migration paths, with all cryptographic keys and access controls held under EU jurisdiction.

Enforceability: $\geq 50\%$ of new rules enforceable by design (protocol/standard) within 18 months.

Resilience: Mean time to recover under attack, continuity results in civil and military tabletop exercises.

Independence: Concentration and lock-in indices, share of services with real exit paths and European key custody.

Enforceability: Share of rules that are enforceable by design through code and standards, not only ex post through supervision.

Adoption: Number of services procured on open, auditable standards, number of cross-border pilots live and evaluated.

“

Rebalance, not retreat. This playbook moves Europe from intent to capacity, builds the rails we can steer in a crisis, and turns our laws into operational power.

Closing thought

Can Europe afford to do nothing?

Geopolitical pressure is unprecedented and accelerating. The U.S. CHIPS and Science Act⁴ mobilizes \$280 billion to lock in semiconductor dominance, while China's Blockchain Service Network (BSN)⁵ creates parallel infrastructure explicitly designed to bypass Western protocols. As the President of the German Federal Office for Information Security (BSI) Claudia Plattner warned, 'We are years behind. Not in regulation, but in actual digital capability'.⁶ Meanwhile, U.S. and Chinese firms are consolidating dominance in AI, cloud, and platform services, with Europe's productivity gains in high-tech sectors lagging far behind the U.S.⁷ At the same time, BRICS are launching alternative payment systems such as BRICS Pay and expanding their Digital Silk Road infrastructure, establishing standards that risk bypassing European influence.⁸ European efforts to close the innovation gap have seen only limited success, with just 11.2 % of the 2024 innovation strategy recommendations fully adopted to date.⁹ This combination of foreign acceleration and domestic delay heightens the risk of technological lock-in. If global platforms, protocols, and compliance regimes harden around non-European rules, they will be costly and difficult to dislodge later. To safeguard Europe's autonomy, a coherent digital sovereignty strategy must be developed now, building decentralized European open protocols that reflect the democratic values and ensure competitiveness before the window closes.

4 CHIPS and Science Act, Public Law 117-167, August 2022, allocating \$52.7 billion for semiconductor manufacturing and \$200 billion for research. <https://www.congress.gov/crs-product/R47523>

5 China's BSN launched 2020, now operating 130+ nodes globally as 'new internet' infrastructure.

<https://digichina.stanford.edu/work/knowledge-base-blockchain-based-service-network-bsn-%E5%8C%BA%E5%9D%97%E9%93%BE%E6%9C%8D%E5%8A%A1%E7%BD%91%E7%BB%9C/>

6 Plattner, C. (2024). Interview with Heise, emphasizing Europe's digital infrastructure deficit

<https://www.heise.de/news/BSI-Praesidentin-Digitale-Souveraenitaet-fuer-Deutschland-vorerst-unerreichbar-10517756.html>

7 Consultancy.eu, "Europe Behind US in AI Arms Race, Accenture Report," <https://www.consultancy.eu/news/12083/europe-behind-us-in-ai-arms-race-accenture-report>

8 Wikipedia, "BRICS Pay," https://en.wikipedia.org/wiki/BRICS_Pay; BRICS Today, "The Digital Silk Road: Cybersecurity and Tech Alliances in the BRICS Bloc,"

<https://bricstoday.com/the-digital-silk-road-cybersecurity-and-tech-alliances-in-the-brics-bloc/>

9 Business Insider, "Europe Risks Losing Innovation Race as Draghi Report Shows Limited Progress," September 2025

<https://www.businessinsider.com/europe-innovation-deutsche-bank-report-draghi-us-china-2025-9>

About the European Decentralisation Institute

The European Decentralisation Institute (EDI) is an independent, non-profit think tank dedicated to advancing decentralisation as a strategic foundation for Europe's digital economy and society. We engage in dialogue with senior policymakers, elected officials and industry executives on policy topics where decentralisation makes a difference. We make policy recommendations based on thorough research and our deep expertise and experience in decentralisation across public and private organisations.

Authors of this policy brief



Prof. Dr. Christoph Kreiterling – lead author Christoph Kreiterling is professor of Tech-Impact & Sustainability at the University of Applied Sciences Trier. His research focuses on exploring how emerging technologies are reshaping markets, regulation, and innovation. Before entering academia, he served as a Senior Adviser at BaFin.



Dr. Michael Zargham Michael Zargham is the Founder of BlockScience, a systems engineering firm that designs and analyses digital public infrastructure. His work combines rigorous mathematics with real-world governance challenges, engineering systems that are transparent, resilient, and adaptive.



Dr. Wessel Reijers Wessel Reijers is a Postdoctoral Researcher in Media Studies at Paderborn University. He received his PhD in technology ethics from Dublin City University and was Research Associate in the ERC-funded BlockchainGov project led by Dr. Primavera De Filippi.



Prof. Dr. Dr. h.c. Roman Beck Roman Beck is Chester B. Slade professor at the Computer Information Systems Department at Bentley University in Boston. As blockchain economist, his research focuses on the changing nature of economic transactions due to blockchain.

Reviewers

Prof. Dr. Sebastian Kortmann – University of Amsterdam

Igor Mikhalev – EY-Parthenon

Arno Laeven – European Decentralisation Institute

We would like to thank the following organisations and people for their input, review and support: the Ethereum Foundation, the Lisbon Council, the Directorate-General for Communications Networks, Content and Technology (DG CNECT) of the European Commission, Anja von Rosenstiel, Andrea Halmos, Brendan Devlin, Hubert Romaniec, Erwin Voloder, Quirijn Mohr, Alex Borg, Tomasso Astazi, Bert Streng, Pierre Marro, Jan Bellens, Julien Blanchez, Alberto di Felice, Mike McCabe, Johan Pouwelse, Salvatore Furnari, Joachim Schwerin, Theo Beutel, Alessandro Malventano, Stefano Mazzocchi, Joeri Toet, Jacopo Nuti, Jeroen Schouten, Dimitrios Thomas, Kelly Roegies

APPENDIX

The Decentralisation for Digital Sovereignty Framework: Legislative Architecture

The DDS Framework isn't aspirational, it's prescriptive policy requiring amendments to existing regulations:

Overview of Required Regulatory Amendments:

- **eIDAS 2:** Add Article 12a mandating DID support
- **MiCA:** New Chapter VII on permissionless settlement layers
- **NIS2:** Expand Article 21 to cover decentralized infrastructure resilience testing
- **DORA:** Article 17 amendment for public blockchain dependency management

Mandatory Sovereignty Metrics. The following metrics expose the gap between paper sovereignty and operational sovereignty that traditional legal scholarship overlooks:

- **Infrastructure Dependency Index:** Percentage of critical operations executable without foreign infrastructure (target: >60% by 2027)
- **Enforcement Latency:** Time from regulatory decision to technical implementation (target: <72 hours)
- **Jurisdictional Override Capability:** Ability to technically enforce European rules despite platform resistance (binary pass/fail)
- **Exit Velocity:** Time to migrate critical functions to alternative infrastructure (target: <30 days)

Digital Identity

The most natural starting point is the EUDI Framework, which establishes the EU Digital Identity Wallet framework. While it sets out interoperability requirements, additional work is needed to incorporate decentralised identifiers (DIDs), verifiable credentials, selective disclosure, and revocation mechanisms, so that wallets can function in permissionless or federated ecosystems without compromising trust.¹⁰ NIS2 should likewise be extended to clarify the security obligations of wallet providers and trust services operating on decentralised infrastructure, and to enable consistent cross-border incident reporting and resilience testing.¹¹ Wallets must also support front-end independence so users can interact directly with protocols, and social recovery with multi-party custody under EU law. Supervisors should run annual Exit Tests in drills where core teams disappear and services continue under European governance, with notarised timelocks and public, verifiable change logs for non-emergency upgrades.

¹⁰ <https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng>

¹¹ <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>

Financial Sovereignty

Decentralised open protocols for privacy-preserving payments must be recognised under MiCA, which should include a supervisory sandbox for zero-knowledge compliance solutions and a clear regulatory perimeter for permissionless settlement layers used by crypto-asset service providers and e-money token issuers.¹² The Instant Payments Regulation (IPR) should allow standardised on-chain interfaces to connect with SEPA SCT Inst front-ends,¹³ and DORA must be adapted to ensure operational resilience obligations are met when supervised firms rely on public blockchain infrastructure.¹⁴ Finally, PSD3/PSR and the forthcoming Financial Data Access (FiDA) framework should guarantee API rights for tokenized accounts, programmable escrow, and fraud-monitoring on smart contract-based payments.¹⁵

Energy Resilience

The ongoing Electricity Market Design reform (amending Regulations 2019/942 and 2019/943) provides an opportunity to standardise tokenized metering proofs, on-chain flexibility bids, and PPA settlements, enabling auditable and low-latency market operations.¹⁶ The recast of REMIT should explicitly cover DLT-based trading venues and registries to ensure transparency and market-abuse monitoring in tokenized energy markets.¹⁷ The Data Act and Data Governance Act, along with the forthcoming Common European Energy Data Space, must also be aligned to enable sovereign, real-time sharing of prosumer and grid data with cryptographic proofs.¹⁸

AI Autonomy

The AI Act will need operational measures to embed verifiable provenance into the digital content supply chain, using cryptographic signatures, registries, and audit logs to meet transparency requirements for deepfake disclosures.¹⁹ Similarly, the Cyber Resilience Act should treat provenance libraries and agents as “products with digital elements,” ensuring that they include software bill-of-materials (SBOMs), secure update mechanisms, and coordinated vulnerability disclosure even in decentralised deployment contexts.²⁰

The result would be a rebalancing, unlike the current retreat. Europe can move from rule-maker to power-holder by building decentralised infrastructure that enforces its norms and values. The next 12 to 36 months comprise a decisive window for Europe.

¹² <https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng>

¹³ <https://eur-lex.europa.eu/eli/reg/2024/886/oj/eng>

¹⁴ <https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng>

¹⁵ <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023PC0366>

¹⁶ <https://eur-lex.europa.eu/eli/reg/2024/1747/oj/eng>

¹⁷ <https://eur-lex.europa.eu/eli/reg/2011/1227/oj/eng>

¹⁸ <https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng>

¹⁹ <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>

²⁰ <https://eur-lex.europa.eu/eli/reg/2024/2847/2024-11-20/eng>

November 2025

EUROPEAN

DECENTRALISATION INSTITUTE

info@eudecentralisation.org
eudecentralisation.org

