
**Blockchain for Europe Statement on
Franco-German Joint Paper on Digital Sovereignty**

Brussels, July 2026

Blockchain for Europe welcomes the Franco-German Joint Paper on Digital Sovereignty, released in June 2026, as a significant step toward a resilient, self-determined European digital ecosystem. We strongly support its recognition that sovereignty requires both defensive protection and proactive capability-building, and its insistence that reducing dependencies must not slide into protectionism or isolation.

We endorse the paper's emphasis on partnerships with actors who respect human rights, democratic principles and the rule of law, alongside fundamental data protection standards. We share the understanding of defensive sovereignty as protection against external coercion — whether through legal means or technological restrictions — together with safeguarding strategic assets and sensitive data. This aligns closely with the needs of European institutions and citizens operating in an era of increasing digital threats.

We welcome the paper embracing open source software, open hardware and open access as means for direct technical co-creation. The recognition that sovereign technology requires modular architectures, open data standards and interoperable interfaces — enabling genuine substitutability rather than vendor lock-in — is foundational to developing trustworthy critical IT infrastructure. We support the call for the highest protection standards for sensitive data, including mandatory use of privacy-preserving technologies (such as end-to-end encryption, zero-knowledge proofs, secure multi-party computation and homomorphic encryption), and adequate safeguards against cybersecurity risks and the effects of non-EU extraterritorial legislation.

The paper rightly identifies unilateral dependencies as a core vulnerability of digital systems. Yet the most precarious risks in today's digital landscape stem from centralised architectures that concentrate power and data, creating single points of failure and control.

Decentralised, open-source infrastructure offers a structural solution. By distributing trust across networks rather than concentrating it in single entities, these systems embody the paper's requirement that *"systems' designs do not cause unilateral dependencies."* They inherently resist extraterritorial data access and technological restrictions that the paper rightly identifies as digital sovereignty risks. Where architectures are open, verifiable and substitutable by design, they deliver digital sovereignty guarantees independent of any operator's identity or location.

The paper's definition of sovereignty extends beyond EU institutions to administrations and private organisations. We believe the same logic extends to communities and individual citizens. Individual agency over one's digital environment — the ability to verify, to choose and to exit — complements and reinforces collective sovereignty. A Europe of digitally sovereign institutions is strongest when it is also a Europe of digitally empowered citizens, and the paper's goal of strengthening basic digital literacy for *"independent, self-determined and secure use"* of digital services points in exactly this direction.

Recommendations

As the paper informs the Commission's 2026 legislative agenda, including the Tech Sovereignty Package and the Cloud and AI Development Act, Blockchain for Europe offers four concrete recommendations:

1. **First, recognise distributed ledger technologies among the key digital technologies.** The paper names artificial intelligence, microelectronics, robotics, data, quantum technologies and cybersecurity — DLT belongs on this list. Europe holds a genuine first-mover position through MiCA, the world's first comprehensive regulatory framework for crypto and digital assets, and through one of the world's largest blockchain developer and research communities. Few key technologies offer Europe a comparable existing lead to build upon.
2. **Second, recognise that open, decentralised infrastructure can achieve the desired sovereignty outcomes, as defined across all building blocks of EU digital sovereignty.** Specifically, where public buyers assess sovereignty under the paper's dimensions, openly governed, verifiable and substitutable protocols should be recognised as scoring on the structural dimensions — substitutability, transparency and resilience — that the framework identifies as decisive in critical environments.
3. **Third, overtly recognise decentralization as a technique for operational resiliency.** The capabilities to “implement and enforce” and to ensure operational resilience need to be considered together. Specifically, the *“use of digital products or services from a provider whose top-holding company is headquartered in an EU Member State or in a trusted international partner state”* may not, by itself, deliver the most “adequate level of security”. It is a well established principle in operational resilience that not creating single points of failure and wide geographical distribution of infrastructure or data creates resilient infrastructure. At the same time, access rights and privileges, and specific cryptographic techniques, can still grant EU industrial users sovereign control. In DLT technologies, for example, there are multiple examples of techniques that align the seemingly divergent concepts of geographically decentralized infrastructure and user-centric control. Therefore, when considering implementation / enforcement control such techniques should be allowed to be considered at least in parallel to the geographical location of service providers.
4. **Fourth, consider open, decentralised infrastructure as offering equivalent benefits to what the paper calls “sovereign solutions” within strategic procurement frameworks,** by anchoring exit concepts and multi-vendor strategies at the technical, as well as at the contractual, level. Genuine substitutability requires user control and/or portability of data, identities and logic across providers, not only contractual switching rights. Open protocols and open standards can provide technical guarantees for exit, and should be reflected as such in the forthcoming Cloud and AI Development Act.

The Franco-German paper offers Europe a coherent and operational vision of digital sovereignty. Blockchain for Europe stands ready to contribute to the discussions it sets in motion. We are convinced that the strongest foundation for European digital sovereignty lies in supporting open, decentralised infrastructure that combines the paper's defensive protections with architectural guarantees aligning Europe's strategic interests with its founding values of openness, interoperability and human-centric digital rights.