From Digital Dependency to Distributed Sovereignty: A Hybrid Architecture for Individual Control

Dmitrii Milorava[1] Theodor Neunzerling[1]

[1]https://web3home.info
hello@web3home.info

Abstract: Contemporary digital infrastructure creates systemic vulnerabilities through centralized control that commoditizes personal data via surveillance-based business models. This research presents the Sovereignty Grid, a distributed hybrid architecture that transforms personal computing devices into collaborative networks delivering human-centric digital sovereignty across five interdependent domains: communication, computational, data, financial, and identity sovereignty. The architecture implements community-based trust mechanisms through small clusters of 3-4 participants deploying standardized hardware configurations, establishing shared infrastructure services while maintaining dedicated computational resources for individual workloads.

The Sovereignty Grid eliminates the conventional trade-off between individual control and network effects through distributed ownership models, community-based redundancy, open-source foundations, aligned economic incentives via computational resource sharing, and privacy-by-design architecture. Implementation analysis demonstrates practical feasibility through standardized deployment protocols and sustainable computational exchange models. However, systemic constraints including infrastructure gatekeepers and hardware supply chain dependencies indicate that complete digital independence remains limited by factors beyond software solutions. The Sovereignty Grid constitutes a significant advancement toward digital autonomy, providing a viable pathway from centralized infrastructure dependency toward community-driven distributed sovereignty.

Keywords: digital sovereignty; distributed computing; decentralized infrastructure; privacy-by-design; open-source

1 Problem Statement

Centralized digital infrastructure has created pervasive dependency that affects virtually every aspect of contemporary digital life. This dependency operates through extractive business models that transform personal data into commodities, often traded without meaningful consent from originators (Bradford, 2023; Staab et al., 2023). Centralized architectures amplify systemic risk by creating single points of failure that can disrupt services for millions simultaneously (Zuo et al., 2023). The proliferation of subscription-based models has generated consumer fatigue while diminishing competitive incentives, even as AI service revenues expand by an order of magnitude and personal devices with significant computational capacity remain largely underutilized (Edge, 2025; Paula Cobzaru and Alexandru Tugui, 2024).

This centralized model exhibits systematic vulnerabilities across five critical domains that collectively constitute digital sovereignty: communication faces extensive metadata collection through server architectures processing billions of daily interactions (Sharon and Gellert, 2024); computational access requires exposing sensitive data to major corporations for AI inference capabilities (Teubner et al., 2023); data control has been systematically undermined through non-negotiable terms of service that transform personal information into corporate assets (Staab et al., 2023); financial transactions remain subject to arbitrary restrictions and high remittance costs affecting 1.7 billion excluded adults (Adrian, 2022; Edwards and Mishkin, 1995); and identity verification creates single points of failure where breaches simultaneously affect access across financial, communication, healthcare, and government services (Choi, 2021; Zhang et al., 2022).

The interconnected nature of these vulnerabilities creates cascading dependencies where compromise in any domain propagates across the entire digital ecosystem, fundamentally undermining individual autonomy while concentrating control within centralized authorities (Chen et al., 2021; Zhao et al., 2025; Zhou et al., 2021).

1.1 Technological Convergence and the Opportunity for Comprehensive Transformation

Three critical technological thresholds have converged to enable viable alternatives addressing digital dependency across all five domains simultaneously:

Hardware accessibility: Semiconductor advances now provide consumer-grade systems with enterprise-level capabilities. Personal infrastructure can support high-availability communication networks, intensive computational workloads including large language models, secure encrypted data storage, cryptocurrency processing, and decentralized identity verification previously requiring dedicated data center resources (Kempny et al., 2025; Patwari et al., 2025; Xia et al., 2024).

Software maturation: Open-source ecosystems have achieved production-grade reliability across communication protocols, distributed computing frameworks, cryptographic protection systems, decentralized financial infrastructure, and identity verification mechanisms. Containerization technologies have democratized complex distributed system deployment while maintaining security isolation (Cheng, 2014; Koziolek and Eskandani, 2023; La Cava et al., 2021; Nakamoto, 2009; Wei and Tyson, 2024).

Regulatory alignment: Digital rights frameworks support distributed sovereignty principles. With 46% of consumers unable to protect personal data and legislation including GDPR, CCPA, and China's PIPL codifying data sovereignty principles, regulatory developments align with distributed architectures. Despite low awareness, 60% view privacy laws positively while 56% express concern about ethical AI implementation (Calzada, 2022; Cisco, 2021).

This convergence creates a unique opportunity to address centralized infrastructure vulnerabilities through distributed architectures that preserve network effects while eliminating single points of failure. The fundamental design challenge lies in constructing integrated distributed systems delivering the reliability, accessibility, and network effects of centralized platforms while simultaneously restoring individual control.

2 Theoretical Framework

The transition from surveillance-based business models necessitates alternative frameworks that reconceptualize the relationship between individual agency and collective capability (Lipartito, 2025). This work challenges the structural argument that network effects inherently require centralized coordination, proposing instead that distributed architectures can generate superior collective capabilities while preserving individual sovereignty.

2.1 Distributed Sovereignty Architecture

The theoretical model operationalizes distributed sovereignty through systematic transformation of personal computing infrastructure into collaborative networks. Standardized hardware configurations operate as interdependent nodes within hybrid systems that strategically combine shared resource allocation for infrastructure services with dedicated computational capacity for individual workloads.

Unlike centralized models that extract value through data commoditization, distributed sovereignty creates value through computational resource sharing and collaborative service provisioning that strengthens individual autonomy. This establishes positive feedback loops wherein increased participation generates enhanced computational resources and sophisticated collective services, while maintaining strict boundaries around individual data control (Figure 1).

2.2 The Five Domains of Digital Sovereignty (CCDFI)

The theoretical framework (Figure 2) identifies five interdependent domains constituting comprehensive digital autonomy. These domains function as mutually reinforcing components where enhanced capability in any domain strengthens security and functionality across all others.

Communication Sovereignty enables privacy-preserving, censorship-resistant interpersonal communication through distributed messaging architectures that eliminate metadata collection and surveillance capabilities from system design (La Cava et al., 2021; Wei and Tyson, 2024).

Computational Sovereignty provides autonomous access to processing capabilities, including AI inference and complex workloads, without external dependencies that necessitate data exposure or generate vendor lock-in (Marcondes et al., 2025; Nikolakopoulos et al., 2025).

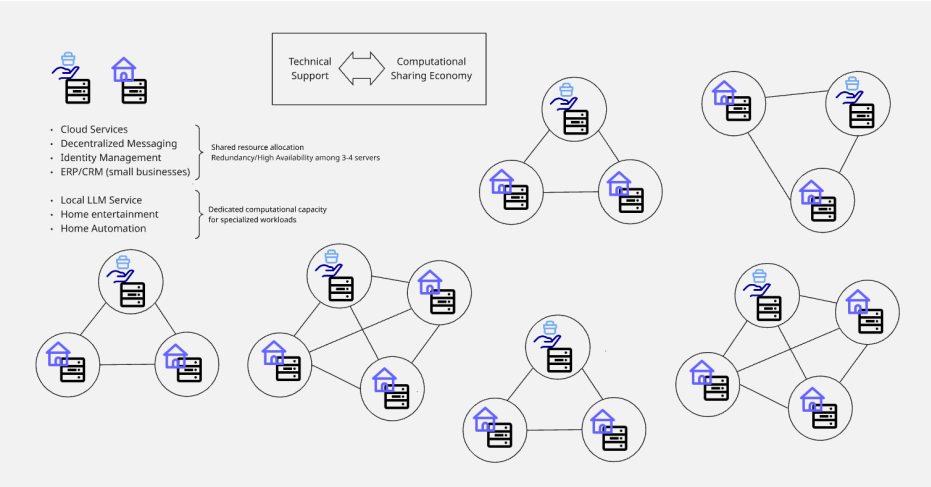

Figure 1: The Sovereignty Grid

Data Sovereignty establishes comprehensive individual control over personal information lifecycles through distributed storage and processing, encompassing data generation, storage protocols, processing methodologies, and sharing permissions without centralized cloud dependencies (Hildmann and Kao, 2014; Trautwein et al., 2022).

Financial Sovereignty encompasses autonomous economic transaction capabilities operating independently of traditional banking intermediaries and centralized payment processors (Misra, 2022).

Identity Sovereignty establishes decentralized verification mechanisms eliminating centralized identity repositories while providing universal access independent of documentation or geographic constraints (Dib and Rababah, 2020; Stockburger et al., 2021).

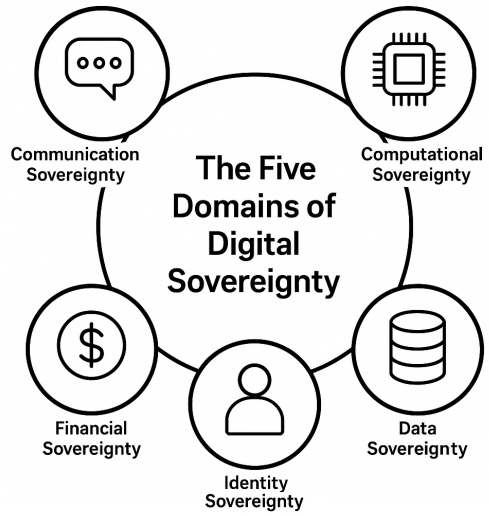

Figure 2: Theoretical Framework

2.3 Addressing Cascading Failures Through Distributed Architecture

Drawing from cascading failure research in interdependent networks (Buldyrev et al., 2010; Gao et al., 2012), distributed sovereignty architecture must address interdependence across digital domains, where compromise within any domain can propagate vulnerabilities across interconnected systems.

The theoretical model proposes distributed infrastructure enabling community-powered networks to deliver the

reliability and accessibility of centralized platforms while preserving individual autonomy. This approach transforms the traditional trade-off between individual control and network effects by demonstrating that distributed architectures can generate superior collective capabilities while strengthening individual sovereignty.

3 Design Principles

The Sovereignty Grid operationalizes distributed sovereignty through five foundational design principles that counter structural vulnerabilities in centralized infrastructure:

Distributed Ownership replaces centralized service dependencies with individual infrastructure control. Participants own, operate, and maintain computational nodes, eliminating external gatekeepers while preserving network connectivity and resource sharing.

Community-Based Redundancy transforms high availability from a centralized engineering challenge into distributed social architecture leveraging peer relationships for system resilience. Small clusters create mutual backup relationships and shared infrastructure services, shifting trust from corporate entities to peer networks.

Open-Source Foundation ensures architectural transparency and prevents proprietary lock-in mechanisms. All system components operate on open-source technologies, enabling community-driven evolution, comprehensive security auditing, and protection against vendor dependency.

Aligned Economic Incentives establish sustainable resource sharing through computational exchange markets creating positive-sum economic relationships. Participants contribute excess processing capacity for technical support, software development, and infrastructure maintenance, creating self-reinforcing loops that strengthen network effects.

Privacy by Design embeds data sovereignty directly into system architecture rather than treating privacy as a policy overlay. Through local-first computation, end-to-end encryption, and user-controlled data flows, this principle eliminates surveillance capitalism models that commoditize personal information.

4 Comparative Analysis

Current digital sovereignty solutions operate within mutually exclusive paradigms forcing users to choose between computational capability and digital autonomy. Individual devices typically lack computational capacity for modern workloads, while centralized platforms achieve scale through surveillance-based models that contradict sovereignty principles (Table 1).

Table 1: Overview of market players in the field of digital sovereignty

Market players	**Description**	**Constraints**
Sovereign computing / personal server providers (Umbrel, Start9, ZimaSpace)	Sovereign computing services enable individuals to host their own cloud services without relying on centralized players.	Convenience; network for high availability; defined user-centric use case.
Hardware solutions for digital sovereignty (Synology, QNAP)	Hardware for self-hosting of digital services.	Vendor lock-in and limited solutions for decentralized networking.
Cloud platforms (AWS, Google Cloud, Microsoft Azure)	Traditional commercial cloud platforms that offer scalability and convenience.	Centralization, dependence, and pervasive data mining.

4.1 Limitations of Existing Solutions

Personal server platforms address privacy concerns through local deployment but cannot overcome fundamental hardware constraints. Individual devices typically possess limited RAM (8-32GB) and insufficient bandwidth to

support resource-intensive applications requiring 70GB+ VRAM configurations. Technical complexity barriers exclude non-expert users from successful deployment and maintenance.

Consumer NAS solutions provide reliable local storage but remain constrained by single-device architectures that cannot aggregate computational resources across multiple units, severely limiting AI inference capabilities while maintaining vendor dependencies through proprietary software stacks.

Centralized cloud platforms deliver computational scale and convenience but operate through data extraction models that systematically commoditize personal information. Users exchange digital autonomy for computational capability, creating privacy violations and external dependencies that directly contradict sovereignty objectives.

4.2 The Sovereignty Grid's Architectural Innovation

The Sovereignty Grid transcends these limitations through hybrid distributed architecture that strategically combines shared resource allocation for community services with dedicated computational capacity for personal workloads. This resolves the false trade-off between computational capability and digital autonomy by enabling both through distributed coordination rather than centralized extraction.

Standardized hardware configurations operate as interdependent nodes where infrastructure services achieve redundancy and high availability across community networks. Simultaneously, resource-intensive applications operate on dedicated owner-controlled infrastructure preserving individual sovereignty. Automated deployment systems eliminate technical barriers while peer-redundancy networks provide enterprise-grade availability without centralized dependencies.

5 Implementation

The Sovereignty Grid deployment strategy addresses practical challenges of transitioning from centralized to distributed infrastructure through a structured approach targeting early adopters and gradually expanding to mainstream adoption.

1. **Phase 1: Foundation**
   Establishes core technical infrastructure and initial market validation:
   - **Hardware R&D:** Establish standardized reference architectures optimizing price-performance ratios while ensuring compatibility with distributed resource sharing. Develop supply chain partnerships enabling cost-effective procurement.
   - **Software Development:** Deploy minimum viable product encompassing core sovereignty services including encrypted messaging, distributed storage, local AI inference, and decentralized identity management with automated deployment capabilities. The complete technical architecture and containerized service stack are detailed in Appendix A.
   - **Market Entry:** Engage privacy-conscious professionals and small businesses through targeted marketing emphasizing digital sovereignty benefits while establishing pilot communities for technical validation.
2. **Phase 2: Optimization**
   Refines technical architecture based on deployment experience while expanding market reach:
   - **Hardware Advancement:** Develop enhanced configurations incorporating improved AI inference capabilities and simplified installation processes based on Phase 1 feedback.
   - **Software Maturation:** Integrate advanced services including enhanced local language models and collaborative tools leveraging distributed architecture capabilities while refining user experience and security protocols.
   - **Market Expansion:** Scale deployment to broader small business adoption through channel partnerships and community certification programs with comprehensive training and support systems.
3. **Phase 3: Scale**
   Transitions from specialized solution to mainstream alternative:
   - **Platform Consolidation:** Achieve enterprise-grade reliability through systematic optimization, comprehensive regulatory compliance automation, and advanced governance frameworks.
   - **Market Acceleration:** Enable mainstream adoption through simplified onboarding experiences and comprehensive support systems making digital sovereignty accessible without technical expertise.
   - **Economic Sustainability:** Complete transition to self-sustaining economic model through mature computational exchange markets and community-driven development programs.

6 Validation Methods

The Sovereignty Grid's viability requires systematic validation across multiple dimensions establishing both technical feasibility and sustainable deployment. The validation framework encompasses four interdependent dimensions:

Technical validation measures system performance through rigorous testing of distributed system capabilities including synchronization latency, system resilience under device failures, conflict resolution efficiency, network partition simulations, and automated failover testing.

Security validation employs continuous assessment including penetration testing, vulnerability scanning, and cryptographic protocol verification ensuring privacy-preserving architectures maintain security guarantees under adversarial conditions through regular independent audits.

Economic validation tests sustainability assumptions underlying computational exchange models by comparing resource contribution rates against operational costs across different adoption scenarios while testing incentive alignment mechanisms preventing system gaming.

Regulatory validation ensures continuous compliance with evolving data protection frameworks including GDPR and CCPA while establishing appropriate open-source licensing structures and governance frameworks that mitigate liability risks while maintaining decentralized ownership.

7 Risks and Limitations

While the Sovereignty Grid represents significant advancement toward digital independence, complete digital autonomy remains constrained by systemic infrastructure dependencies extending beyond software solutions. Understanding these limitations establishes realistic expectations and appropriate mitigation strategies.

Infrastructure Dependencies create persistent bottlenecks beyond distributed architecture control. Internet Service Providers retain fundamental control over connectivity through bandwidth throttling and service termination (Ohm, 2008). Domain name resolution depends on ICANN's centralized structures vulnerable to manipulation and political interference (Zalnieriute and Schneider, 2014). Physical internet infrastructure remains under telecommunications corporations and nation-state control (Deibert et al., 2010).

Hardware Supply Chain Vulnerabilities introduce dependencies through concentrated semiconductor supply chains with proprietary designs incorporating opaque components and closed-source firmware (Skorobogatov and Woods, 2012). Embedded management systems operate below operating system levels with unverifiable functionality potentially compromising system security (Wu, 2019).

Client Device Attack Vectors represent critical vulnerability points where user endpoint devices operating proprietary systems can compromise distributed architectures. Complete sovereignty requires migration to privacy-focused operating systems creating significant user education requirements and technical adaptation barriers limiting mainstream adoption (Bailey and Labovitz, 2011; Bostoen and Mândrescu, 2020).

Distributed Architecture Risks emerge from design characteristics including network partitioning events isolating community clusters and peer-to-peer connectivity dependence meaning geographical disruptions can have greater impact than centralized systems with redundant data center locations.

7.1 Mitigation Strategies

Infrastructure dependencies can be partially mitigated through multiple ISP relationships, mesh networking technologies, and satellite connectivity, though complete elimination remains impractical. Hardware vulnerabilities can be addressed through diversified sourcing, open hardware initiatives, and comprehensive security testing. Client device risks require user education programs, secure operating system recommendations, and architectural designs minimizing individual compromise impact.

These constraints demonstrate that distributed architectures can substantially reduce centralized platform dependence while remaining subject to infrastructure gatekeepers and hardware dependencies extending beyond software solutions. The Sovereignty Grid represents significant advancement toward digital autonomy rather than complete independence, and implementation planning must acknowledge these fundamental limitations while maximizing achievable benefits.

8 Results and Discussion

The convergence of centralized infrastructure dependency with data commoditization practices has created systemic vulnerabilities that compromise individual autonomy while concentrating control within dominant platforms (Misra et al., 2025). This research demonstrates that the Sovereignty Grid addresses these challenges through distributed hybrid architectures eliminating the conventional trade-off between digital sovereignty and computational capability.

The analysis reveals that three critical technological thresholds have been simultaneously achieved, creating conditions for practical distributed sovereignty implementation. The Sovereignty Grid's hybrid approach successfully resolves fundamental limitations preventing existing solutions from achieving comprehensive digital sovereignty through community-based trust mechanisms that deliver both individual control and collective resilience.

Implementation feasibility has been demonstrated through standardized hardware architectures, automated deployment protocols, and sustainable computational exchange models aligning individual benefit with collective network strength. This creates a foundation for scalable digital sovereignty transforming value generation from surveillance-based data commoditization to computational resource sharing.

The Sovereignty Grid represents a fundamental architectural paradigm shift toward distributed digital autonomy that challenges basic assumptions underlying contemporary digital infrastructure. Where centralized platforms extract value through surveillance models compromising user privacy, distributed networks generate value through computational exchange mechanisms strengthening individual agency while providing superior collective services.

8.1 Policy and Future Research Implications

The demonstrated viability of distributed sovereignty architectures suggests regulatory frameworks should actively support alternatives to centralized platform dependency rather than simply regulating existing systems. Policy makers should consider incentives for distributed architecture development, interoperability standards, and legal frameworks supporting community-based governance models.

Future research directions include investigation of alternative network infrastructure models, development of open hardware supply chains, and creation of regulatory frameworks specifically designed to support distributed sovereignty architectures. Long-term sustainability of computational exchange markets and governance mechanisms for distributed communities require ongoing research and empirical validation.

The Sovereignty Grid demonstrates that distributed digital autonomy is not only theoretically possible but practically achievable within current technological and regulatory constraints. While complete independence from all external dependencies remains elusive, the substantial reduction in centralized platform dependence and elimination of systematic data commoditization represents transformative advancement toward digital sovereignty meriting continued research, development, and policy support.

References

Adrian, T. (2022, November 18). *A cross-border payments, exchange, and contracting platform for the 21st century* [IMF]. Retrieved April 1, 2023, from https://www.imf.org/en/News/Articles/2022/11/18/sp-cross-border-payments-exchange-contracting-platform-21st-century (cit. on p. 1).

Bailey, M., & Labovitz, C. (2011). Censorship and Co-option of the Internet Infrastructure. *Ann Arbor*, *1001*, 48104. Retrieved September 21, 2025, from http://nsrg.ece.illinois.edu/publications/CSE-TR-572-11.pdf (cit. on p. 6).

Bostoen, F., & Mândrescu, D. (2020). Assessing abuse of dominance in the platform economy: A case study of app stores. *European Competition Journal*, *16*(2-3), 431–491 (cit. on p. 6).

Bradford, A. (2023, September). *Digital Empires: The Global Battle to Regulate Technology* (1st ed.). Oxford University PressNew York. https://doi.org/10.1093/oso/9780197649268.001.0001 (cit. on p. 1).

Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., & Havlin, S. (2010). Catastrophic cascade of failures in interdependent networks. *Nature*, *464*(7291), 1025–1028. https://doi.org/10.1038/nature08932 (cit. on p. 3).

Calzada, I. (2022). Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL). *Smart Cities*, *5*(3), 1129–1150. https://doi.org/10.3390/smartcities5030057 (cit. on p. 2).

Chen, Y., Richter, J. I., & Patel, P. C. (2021). Decentralized governance of digital platforms. *Journal of Management*, *47*(5), 1305–1337 (cit. on p. 1).

Cheng, S. M. C. (2014). *Proxmox high availability: Introduce, design, and implement high availability clusters using Proxmox*. Packt Publishing. (Cit. on p. 2).

Choi, Y. B. (2021). Organizational Cyber Data Breach Analysis of Facebook, Equifax, and Uber Cases: *International Journal of Cyber Research and Education*, *3*(1), 58–64. https://doi.org/10.4018/IJCRE.2021010106 (cit. on p. 1).

Cisco. (2021). *Cisco 2021 Consumer Privacy Survey* (tech. rep.). Cisco Systems, Inc. https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-cybersecurity-series-2021-cps.pdf (cit. on p. 2).

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. L. (Eds.). (2010, April). *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. The MIT Press. https://doi.org/10.7551/mitpress/8551.001.0001 (cit. on p. 6).

Dib, O., & Rababah, B. (2020). Decentralized identity systems: Architecture, challenges, solutions and future directions. *Annals of Emerging Technologies in Computing (AETiC)*, *4*(5), 19–40 (cit. on p. 3).

Edge, C. (2025). AI Goes Mainstream: The Consumer Spend Boom of 2025. *Consumer Edge*. Retrieved September 19, 2025, from https://www.consumeredge.com/resources/ai-goes-mainstream-the-consumer-spend-boom-of-2025/ (cit. on p. 1).

Edwards, F., & Mishkin, F. (1995, January). *The decline of traditional banking: Implications for financial stabilityand regulatory policy* (w4993). National Bureau of Economic Research. Cambridge, MA. https://doi.org/10.3386/w4993 (cit. on p. 1).

Gao, J., Buldyrev, S. V., Stanley, H. E., & Havlin, S. (2012). Networks formed from interdependent networks. *Nature Physics*, *8*(1), 40–48. https://doi.org/10.1038/nphys2180 (cit. on p. 3).

Hildmann, T., & Kao, O. (2014). Deploying and extending on-premise cloud storage based on owncloud. *2014 IEEE 34th International Conference on Distributed Computing Systems Workshops (ICDCSW)*, 76–81. https://doi.org/10.1109/ICDCSW.2014.18 (cit. on p. 3).

Kempny, C., Annac, K., Yilmaz-Aslan, Y., & Brzoska, P. (2025, July). QualiPilot – an offline AI tool for qualitative content analysis. https://doi.org/10.21203/rs.3.rs-7122121/v1 (cit. on p. 2).

Koziolek, H., & Eskandani, N. (2023). Lightweight Kubernetes Distributions: A Performance Comparison of MicroK8s, k3s, k0s, and Microshift. *Proceedings of the 2023 ACM/SPEC International Conference on Performance Engineering*, 17–29. https://doi.org/10.1145/3578244.3583737 (cit. on p. 2).

La Cava, L., Greco, S., & Tagarelli, A. (2021). Understanding the growth of the Fediverse through the lens of Mastodon. *Applied Network Science*, *6*(1), 64. https://doi.org/10.1007/s41109-021-00392-5 (cit. on p. 2).

Lipartito, K. (2025). Surveillance capitalism: Origins, history, consequences. *Histories*, *5*(1), 2 (cit. on p. 2).

Marcondes, F. S., Gala, A., Magalhães, R., Perez de Britto, F., Durães, D., & Novais, P. (2025). Using ollama. In *Natural language analytics with generative large-language models: A practical approach with ollama and*

open-source llms (pp. 23–35). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-76631-2_3 (cit. on p. 2).

Misra, S. (2022). *Blockchain Applications in the Smart Era*. Springer International Publishing AG. (Cit. on p. 3).

Misra, S., Barik, K., & Kvalvik, P. (2025). Digital sovereignty in the era of industry 5.0: Challenges and opportunities. *Procedia Computer Science*, *254*, 108–117 (cit. on p. 7).

Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system, 9 (cit. on p. 2).

Nikolakopoulos, A., Litke, A., Psychas, A., Veroni, E., & Varvarigou, T. (2025). Exploring the potential of offline llms in data science: A study on code generation for data analysis. *IEEE Access*, *13*, 64087–64114. https://doi.org/10.1109/ACCESS.2025.3556973 (cit. on p. 2).

Ohm, P. (2008). The rise and fall of invasive isp surveillance. *University of Illinois law review*, *2009* (cit. on p. 6).

Patwari, R., Sirasao, A., & Das, D. (2025). Forecasting LLM Inference Performance via Hardware-Agnostic Analytical Modeling. https://doi.org/10.48550/ARXIV.2508.00904 (cit. on p. 2).

Paula Cobzaru & Alexandru Tugui. (2024). The Subscription Economy and Its Contribution to the Global Economy. *Management Studies*, *12*(3). https://doi.org/10.17265/2328-2185/2024.03.001 (cit. on p. 1).

Sharon, T., & Gellert, R. (2024). Regulating Big Tech expansionism? Sphere transgressions and the limits of Europe's digital regulatory strategy. *Information Communication and Society*, *27*(15), 2651–2668. https://doi.org/10.1080/1369118X.2023.2246526 (cit. on p. 1).

Skorobogatov, S., & Woods, C. (2012). Breakthrough silicon scanning discovers backdoor in military chip. In E. Prouff & P. Schaumont (Eds.), *Cryptographic hardware and embedded systems – ches 2012* (pp. 23–40). Springer Berlin Heidelberg. (Cit. on p. 6).

Staab, R., Vero, M., Balunović, M., & Vechev, M. (2023). Beyond Memorization: Violating Privacy Via Inference with Large Language Models. https://doi.org/10.48550/ARXIV.2310.07298 (cit. on p. 1).

Stockburger, L., Kokosioulis, G., Mukkamala, A., Mukkamala, R. R., & Avital, M. (2021). Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation. *Blockchain: Research and Applications*, *2*(2), 100014 (cit. on p. 3).

Teubner, T., Flath, C. M., Weinhardt, C., Van Der Aalst, W., & Hinz, O. (2023). Welcome to the Era of ChatGPT et al.: The Prospects of Large Language Models. *Business & Information Systems Engineering*, *65*(2), 95–101. https://doi.org/10.1007/s12599-023-00795-x (cit. on p. 1).

Trautwein, D., Raman, A., Tyson, G., Castro, I., Scott, W., Schubotz, M., Gipp, B., & Psaras, Y. (2022). Design and evaluation of IPFS: A storage layer for the decentralized web. *Proceedings of the ACM SIGCOMM 2022 Conference*, 739–752. https://doi.org/10.1145/3544216.3544232 (cit. on p. 3).

Wei, Y., & Tyson, G. (2024). Exploring the Nostr Ecosystem: A Study of Decentralization and Resilience. https://doi.org/10.48550/ARXIV.2402.05709 (cit. on p. 2).

Wu, J. (2019). Security risks from vulnerabilities and backdoors. In *Cyberspace mimic defense: Generalized robust control and endogenous security* (pp. 3–38). Springer. (Cit. on p. 6).

Xia, H., Zheng, Z., Wu, X., Chen, S., Yao, Z., Youn, S., Bakhtiari, A., Wyatt, M., Zhuang, D., Zhou, Z., Ruwase, O., He, Y., & Song, S. L. (2024). Quant-LLM: Accelerating the serving of large language models via FP6-Centric Algorithm-System Co-Design on modern GPUs. *2024 USENIX Annual Technical Conference (USENIX ATC 24)*, 699–713. https://www.usenix.org/conference/atc24/presentation/xia (cit. on p. 2).

Zalnieriute, M., & Schneider, T. (2014). Icann's procedures and policies in the light of human rights, fundamental freedoms and democratic values. *Council of Europe, DGI (2014)*, *12* (cit. on p. 6).

Zhang, X., Yadollahi, M. M., Dadkhah, S., Isah, H., Le, D. P., & Ghorbani, A. A. (2022). Data breach: Analysis, countermeasures and challenges. *International Journal of Information and Computer Security*, *19*(3/4), 402. https://doi.org/10.1504/IJICS.2022.127169 (cit. on p. 1).

Zhao, Y., Cai, B., Cozzani, V., & Liu, Y. (2025). Failure dependence and cascading failures: A literature review and research opportunities. *Reliability Engineering & System Safety*, *256*, 110766. https://doi.org/10.1016/j.ress.2024.110766 (cit. on p. 1).

Zhou, J., Coit, D. W., Felder, F. A., & Wang, D. (2021). Resiliency-based restoration optimization for dependent network systems against cascading failures. *Reliability Engineering & System Safety*, *207*, 107383. https://doi.org/10.1016/j.ress.2020.107383 (cit. on p. 1).

Zuo, T., Sherman, J., Hamin, M., & Scott, S. (2023). *Critical infrastructure and the cloud: Policy for emerging risk* (tech. rep.). Retrieved September 19, 2025, from https://www.atlanticcouncil.org/in-depth-research-reports/report/critical-infrastructure-and-the-cloud-policy-for-emerging-risk/ (cit. on p. 1).

A MVP: Digital Sovereignty Platform

A.1 Objective

The Digital Sovereignty Platform MVP delivers individual control across five core domains: data, communication, computational, and identity sovereignty, with optional financial services. The design supports two operational modes (Table 2):

- **Standalone Mode:** a complete sovereignty solution on a single node, without any external dependency.
- **Collaborative Mode:** optional peer-to-peer federation with trusted nodes, adding redundancy, disaster recovery, and community-building features.

Dimension	Standalone Mode	Collaborative Mode
Availability	Services run only on the local node; if the node fails, downtime occurs until recovery	Near-automatic failover using Patroni (async), DNS updates, and client fallback mechanisms
Resilience	Local backups only; recovery from hardware failure requires reinstall/restore	Distributed redundancy: Syncthing, Restic, and async database replicas ensure disaster recovery across peers
Performance	Full system resources dedicated to a single user/family	Slight overhead from replication and backup traffic; resilience gained at cost of bandwidth
Complexity	Simple to deploy and manage; minimal networking configuration	Requires WireGuard mesh, DNS failover, and optional admin intervention for finalizing failover
Community Aspect	Individual sovereignty only	Collective resilience; encourages trust networks (family, friends, communities) and organic growth of the grid
Security Surface	Single-node attack surface	Multi-node: higher redundancy but larger attack surface; mitigated by VPN-only peering and Tor fallback

Table 2: Comparison of Standalone vs Collaborative Mode in the MVP

A.2 Hardware Specifications

Component	Specification
APU	AMD Strix Halo (16 cores/32 threads + 40 RDNA 3.5 GPU cores)
Memory	128GB LPDDR5x unified (70GB allocatable for AI inference)
Storage	4TB NVMe Gen4 SSD primary + 2TB NVMe backup
Network	500 Mbps upload / 100 Mbps download minimum
Power	120W TDP with UPS backup recommended

Table 3: Hardware Requirements for Standalone Node

A.3 Software Architecture

A.3.1 Base Infrastructure

- **Operating System:** Ubuntu Server 24.04 LTS with hardware-optimized kernel

- **Container Platform:** Docker 24.x with Docker Compose orchestration
- **Reverse Proxy:** Traefik 3.x with automatic Let's Encrypt TLS certificates
- **Database:** PostgreSQL 16.x with automated backup scheduling

A.3.2 Security Framework

- **Authentication:** Authelia SSO with multi-factor authentication support
- **Encryption:** LUKS2 full-disk encryption with TPM integration
- **Network Security:** UFW firewall with fail2ban intrusion prevention
- **Certificate Management:** Internal CA for service-to-service authentication

A.4 Digital Sovereignty Services

A.4.1 Data Sovereignty

- **NextCloud Hub:** File synchronization, document collaboration, calendar, and contact management
- **Backup System:** Restic with encrypted incremental backups and point-in-time recovery

A.4.2 Communication Sovereignty

- **Matrix Synapse:** Self-hosted messaging server with federation capabilities
- **Mastodon:** Ruby-based ActivityPub server with media processing
- **Nostr:** Lightweight relay implementation with NIP-01 support

A.4.3 Computational Sovereignty

- **Ollama:** Local LLM inference supporting Llama 3.1 70B parameter models
- **Stable Diffusion:** Image generation with RDNA 3.5 GPU acceleration
- **Jupyter Environment:** Web-based development interface with GPU access

A.4.4 Identity Sovereignty

- **Vaultwarden:** Bitwarden-compatible password manager with encrypted vault storage
- **Certificate Authority:** Self-signed certificate generation for internal services
- **WebAuthn Support:** Hardware security key integration for passwordless authentication

A.4.5 Financial Sovereignty (Optional)

- **Bitcoin Node:** Bitcoin Core with Electrum server for wallet operations
- **Lightning Network:** Core Lightning (CLN) for micropayment channels
- **Ethereum Node:** Geth execution client for smart contract interaction
- **Privacy Options:** Monero daemon support for enhanced transaction privacy

A.5 Resource Allocation

Component	RAM Allocation	Purpose
System Services	16GB	Ubuntu, Docker, networking, monitoring
Database Layer	8GB	PostgreSQL with query caching
Application Services	8GB	NextCloud, Matrix, email, identity services
AI Inference	70GB	Large language model processing
System Buffer	26GB	File caching and peak load handling

Table 4: Memory Distribution for 128GB Configuration

A.6 Storage Architecture

A.6.1 Primary Storage (4TB NVMe)

- User data and application storage with XFS filesystem
- Database storage with optimized I/O scheduling
- AI model storage and inference cache

A.6.2 Backup Storage (2TB NVMe)

- Daily encrypted incremental backups via Restic
- System snapshots for rapid recovery
- Configuration and certificate backup storage

A.7 Network Architecture

A.7.1 Standalone Mode

- **External Access:** Traefik reverse proxy with domain-based routing
- **Port Management:** Minimal port exposure (80, 443, SSH)
- **Local Network:** Integration with existing home/office infrastructure
- **DNS:** Local DNS resolution with external domain support

A.7.2 Collaborative Mode

In Collaborative Mode, nodes retain full standalone functionality while gaining resilience through federation:

- **WireGuard Mesh:** Encrypted peer-to-peer overlay with stable private IPs
- **Data Replication:**
  - Syncthing for eventual file consistency
  - Restic for nightly encrypted snapshots
  - Patroni (asynchronous mode) for PostgreSQL replicas
- **Near-Automatic User Switching:**
  - Patroni promotes replicas if the primary fails
  - *DNS failover:* external-dns updates records with low TTL (30–60s)
  - *Client fallback:* signed peer-access file with alternate domains, Tor addresses, and VPN IPs
  - *Safe defaults:* promoted replicas may start read-only; a node owner finalizes failover via dashboard
- **Resilience Features:**
  - Multiple domains across registrars
  - Tor v3 hidden service access
  - Optional direct access via WireGuard VPN

A.8 Installation and Deployment

A.8.1 Automated Installation Process

1. Hardware detection and driver installation
2. Base OS configuration with security hardening
3. Container platform deployment with service orchestration
4. SSL certificate generation and domain configuration
5. Initial user account creation and authentication setup

A.8.2 Management Interface

- Web-based dashboard for service monitoring and configuration
- Mobile-responsive interface for remote administration
- Automated software updates with rollback capabilities
- Integrated backup management and recovery tools

A.9 Security Considerations

A.9.1 Threat Model

- Protection against unauthorized access and data exfiltration
- Resilience to hardware failures and data corruption
- Defense against network-based attacks and service disruption
- Privacy preservation for all user data and communications

A.9.2 Compliance Framework

- GDPR compliance through privacy-by-design architecture
- Automated audit logging for security event tracking
- Data retention policies with configurable deletion schedules
- Export capabilities for data portability requirements