Towards a Decentralized Internet: The Interplay of Novel Architectures, Protocols, and Community-Driven Development

Piotr PORZUCZEK

Department of Business Informatics, University of Gdansk, Sopot, Poland
piotr.porzuczek@ug.edu.pl

Abstract

Platform monopolies have turned the contemporary internet into digital feudalism, extracting profit from human connection while enabling surveillance and censorship. Iran's 2019 near-blackout, which cut connectivity to 5 %, exposed how centralized architectures become authoritarian chokepoints. Yet scholarship remains fragmented: most studies isolate protocols instead of synthesizing how technical design and political economy co-evolve. We compare federated systems such as ReP2P Matrix, Nostr's peer-to-peer networks, Bluesky's AT Protocol, blockchain communication hybrids, and Named Data Networking. Our multi-method study of decentralized internet alternatives blends traffic analytics of 4 million Nostr users on 600 relays, performance benchmarks, economic sustainability modeling, and architectural case studies. We ask whether these designs can fulfil the promise of a truly decentralized internet. The evidence is mixed. SendingNetwork scales group messaging linearly, and Waku proves spam-resistant peer-to-peer networks with <300 ms proof generation; however, no single protocol reconciles censorship resistance, usability, and economic sustainability. Nostr delivers uncompromising censorship resistance yet consumes 35 × the resources of centralized systems. Bluesky's growth leaves 98.9 % of identities non-portable. Community mesh networks invite new hierarchies of technical privilege. Accepting irreducible trade-offs must guide emerging web3 governance. Communities will choose architectures aligned with their values, but meaningful decentralization will remain aspirational until funding models and accessibility gaps are resolved.

Keywords: Decentralized internet, distributed architectures, federated systems, peer-to-peer networks

Introduction

Something went terribly wrong. The internet—that defiant rejection of centralized control—calcified into precisely what its architects feared. We were promised resilience through distribution. Instead? Facebook. Surveillance dressed as connection, extraction masquerading as community. Early RFCs weren't just technical—they were ideological. Networks surviving nuclear war, protocols assuming no trust. Beautiful. Yet entire nations vanish with government decrees. Iran, November 2019: connectivity throttled to 5%, violence unfolding in digital darkness while our "resilient" network stood impotent. The technical substrate reveals visceral betrayal. We're running on decisions from when computers filled rooms. IPv4 exhaustion forces billions behind NAT boxes—digital tenements where peer-to-peer becomes architecturally impossible. Client-server thinking shapes every interaction. Path dependency? Sure. But also cowardice. Every architectural choice is political. Did we sleepwalk here, or were we pushed?

Against this landscape, something stirs. Not naive optimism—but genuine breakthroughs. SendingNetwork cracked the impossible: O(N) scaling for decentralized group messaging where we assumed $O(N^2)$ was inevitable. Their consensus mechanism breathes elegance—vertical chains submitting horizontally, trust emerging mathematically. ReP2P Matrix takes different tack, making federation actually work. Not perfect—what is?—but deployable today. Then NDN asks the fundamental question: Why address data by location? Ma's work suggests we've thought backwards for fifty years. Data should be self-authenticating, semantic, location-agnostic. Nostr embraces inefficiency as feature—messages replicated across dozens of relays, burning bandwidth for censorship resistance. Wasteful? Absolutely. Effective? Disturbingly.

These innovations encode radically different power visions. ActivityPub recreates hierarchies while claiming dismantlement—server admins become digital feudal lords. The mastodon.social concentration surprises nobody studying network effects. Bluesky promises portable identity while controlling relays. Each protocol makes explicit choices about who decides, moderates, owns. Technology cannot solve social problems—a lesson we keep forgetting. Infrastructure questions loom largest. Who pays for freedom? Relay operators subsidize Nostr

from pockets, Mastodon survives on donations. Cryptocurrency promises sustainability but brings speculation, inequality. Infrastructure gravity pulls toward consolidation.

Network effects feel insurmountable. Decades of social capital locked in proprietary platforms. Switching costs aren't technical—they're emotional, deeply human. Telling someone to abandon Twitter is like asking them to leave home. Yet I'm unexpectedly hopeful. Not cheap optimism—something harder-won. SendingNetwork's scaling suggests we've accepted false constraints. Economic experiments fascinate—social tokens, on-chain graphs, surveillance-free funding models. Most will fail. Some won't. The emerging spectrum isn't singular but ecosystem. ReP2P Matrix for pragmatists. Nostr for censorship-resistance absolutists. Bluesky threading usability-agency needles. This diversity feels honest.

Most troubling: implementation betrayals. Protocols trumpet decentralization while requiring institutional infrastructure. Radical principles, conservative implementations. Decentralization theater for audiences who've given up. We're at an inflection point. Technical foundations exist. Economic models emerge. Social need peaks. We lack synthesis—making alternatives not just possible but inevitable. The internet we lost isn't returning. What we build next? Gloriously undetermined.

Challenges of Today's Centralised Internet

Contemporary social media platforms have evolved into 'walled gardens'—closed digital ecosystems where platform operators exercise near-total control over information flow and user interactions. While these services present themselves as free and open spaces for connection, users pay for these ostensibly free services with comprehensive surveillance of their digital identities, relationships, and creative expressions. These platforms have developed increasingly sophisticated mechanisms to monetize human connection through data extraction practices that would have seemed dystopian mere decades ago.

Platform control extends far beyond simple content moderation. Operators determine algorithmic visibility, regulate social connections, and create formidable barriers to data portability. When users attempt to export their data, they receive files in formats that prove practically unusable for reconstruction elsewhere. Social connections remain trapped within platform boundaries. Years of carefully curated digital identity become effectively non-transferable. This systematic lock-in serves a singular purpose: extracting profit from human social interaction. The infrastructure has evolved not to facilitate communication but to intermediate and monetize it. Platforms deploy attention-harvesting mechanisms with remarkable precision, implement behavioral manipulation through carefully designed patterns, and transform authentic social relationships into revenue streams. The primary beneficiaries? Platform shareholders, not the users who generate the value. (Surve, et al., 2024)

The situation deteriorates further when we consider political implications.

These monopolistic digital infrastructures have become powerful tools for authoritarian control. Singh and colleagues present compelling evidence that centralized architectures create critical vulnerabilities—digital chokepoints enabling comprehensive censorship and surveillance. Researchers documented 81 internet shutdowns across 19 countries between 2015-2016, resulting in economic damages exceeding $2.4 billion in lost GDP. Yet these economic figures fail to capture the human rights implications.

The Iranian internet shutdown of November 2019 provides a particularly stark example. During fuel price protests, connectivity dropped to just 5% of normal levels. In this enforced digital blackout, state violence proceeded without documentation, international oversight became impossible. This represents not an aberration but the logical outcome of building networks with centralized control points that invite exploitation. Corporate consolidation amplifies these vulnerabilities. A handful of technology companies control the infrastructure through which global information flows. When faced with government pressure, democratic principles often yield to business imperatives. The same architectural features enabling platform lock-in thus become instruments of political control—creating a troubling convergence of corporate profit motives and authoritarian governance objectives. (Singh, et al., 2020)

The censorship is just the tip of the iceberg.

We're dealing with surveillance machines that make Orwell look unimaginative. These platforms don't just watch us—they extract, analyze, and weaponize our data while simultaneously turning our feeds into toxic waste dumps. Huang nailed it when he showed these algorithms aren't broken; they're working exactly as designed. Truth doesn't pay. Outrage does. Think about what we've normalized. Algorithms with more influence than Cronkite ever dreamed of, except they're optimized for ad revenue, not public good. They feed on division like parasites. Every "dark pattern" is carefully engineered to squeeze out one more click, one more second of attention, one more data

point to sell.

The attention economy has created perverse incentives throughout the ecosystem. Research indicates misinformation spreads at six times the rate of accurate news. Data collection extends far beyond conscious interactions—location tracking, purchase histories, communication patterns, and relationship networks combine to create psychological profiles of extraordinary detail. These profiles serve dual purposes: enabling hyper-targeted behavioral manipulation and creating platform dependencies so personalized that departure feels psychologically impossible. (Huang, 2024)

This comprehensive surveillance represents merely a symptom of deeper architectural problems.

Ma's dissertation illuminates the fundamental issue: architectural lock-in so comprehensive it renders genuine competition impossible. These systems don't merely collect user data—they imprison it within proprietary architectures where interoperability is not just absent but actively prevented. The implications are profound. Secure communication becomes impossible without corporate intermediaries who monitor, analyze, and monetize every interaction. This arrangement represents not a technical limitation but a deliberate business model. The technical dependencies creating this situation read like a blueprint for digital authoritarianism. IPv4 address scarcity forces most users behind Network Address Translation systems, preventing direct peer-to-peer connections. The client-server architecture creates systematic dependencies on corporate authentication systems. Contemporary collaborative tools intermediate all activity, creating comprehensive records. The result? Changing platforms requires users to abandon not just an application but their entire digital existence. (Ma, 2024)

The promise of decentralized alternatives has proven more complex than early advocates anticipated.

Wei and Tyson's comprehensive analysis of the Nostr ecosystem reveals the challenging realities. While attracting four million users across 600 relays, the system exhibits severe inefficiencies. Posts replicate across an average of 34.6 relays, with 98% of retrievals being redundant—a massive duplication challenging system sustainability.

The irony strikes hard: while decentralized architectures successfully prevent surveillance and censorship, they introduce coordination challenges significantly impacting usability. Infrastructure reliability presents serious concerns—20% of relays experience downtime exceeding 40% of operational time. Despite Bitcoin integration attempts, 95% of free relays operate at a financial loss. The economic model suffers from classic tragedy of the commons dynamics. Individual node operators bear infrastructure costs while benefits diffuse network-wide. These systemic failures don't merely inconvenience users—they actively reinforce centralized monopolies' dominance by making alternatives seem impractical. (Wei & Tyson, 2024)

Technological Innovations in Decentralised Architectures

SendingNetwork represents a significant architectural advancement in decentralized messaging systems. Rather than iterating on existing approaches, Yeung's team has fundamentally reconceptualized how decentralized messaging should function. Their three-tier architecture demonstrates elegant simplicity while addressing complex technical challenges. The system comprises an access layer enabling direct peer-to-peer connections without corporate intermediaries, a relay layer where nodes route messages without data retention, and a consensus layer dividing responsibilities between "Proof of Availability" and "Proof of Relay" mechanisms.

This architectural solution addresses several long-standing challenges with remarkable effectiveness. Identity fragmentation is resolved through unified identity management. The Double Ratchet encryption protocol extends to support large group communications. Most notably, the Delegation scheme achieves linear O(N) scaling for group messaging—a significant improvement over the $O(N^2)$ complexity plaguing conventional systems. The dual consensus mechanism design merits particular attention. Vertical chains continuously submit to horizontal layers, creating a trust framework operating without central authority. This represents algorithmic elegance—a self-sustaining system maintaining coherence and security through mathematical principles rather than institutional control. (Yeung, 2024)

Singh's DWeb framework proposes fundamental reimagining of internet infrastructure. Rather than attempting to repair existing systems, DWeb envisions replacing them entirely with architecture combining mesh networking and blockchain technology innovatively. Community-owned routers form the physical layer while blockchain provides persistent, tamper-resistant memory. The result is infrastructure designed to resist both corporate capture and government censorship at the architectural level.

Technical design choices demonstrate careful consideration. Blockchain maintains immutable indexes of

cryptographically hashed references while actual content flows through mesh networks. The reputation system shows particular sophistication—community routers accumulate trust scores based on demonstrated reliability, with consensus mechanisms revoking malicious nodes. The economic argument proves compelling. The documented 2015-2016 shutdowns caused $2.4 billion in damages. DWeb's architecture would render such shutdowns both technically infeasible and economically pointless. Communities maintain sovereignty over infrastructure while participating in global networks—achieving local control with worldwide connectivity through elegant engineering. (Singh, et al., 2020)

ReP2P Matrix addresses one of peer-to-peer systems' most persistent challenges: reliable message delivery.

Schichtholz and colleagues developed decentralized relays buffering messages for offline recipients while carefully avoiding creation of new centralization points. The design philosophy emphasizes architectural minimalism to maximize security. Relay nodes store only minimal authorization DAGs—just enough for resynchronization validation. The "forgetful relay" concept deserves particular attention: events automatically expire after configured retention periods, implementing "weak post-compromise security."

Empirical validation demonstrates substantial improvements. Message delivery success rates increase by 28 percentage points, while sub-two-second delivery rates jump from 26% to 76%. These improvements create meaningful impact on real-world usability—the difference between a system feeling responsive versus broken. By reusing existing Matrix authentication mechanisms, the system avoids compatibility problems typically plaguing protocol extensions. (Schichtholz, et al., 2024)

Waku's integration of Rate Limiting Nullifiers represents a breakthrough in addressing spam. The challenge of maintaining open networks while preventing abuse has plagued decentralized systems since inception. Revuelta's team achieved what many considered impossible: spam prevention that preserves privacy. The technical architecture elegantly combines established and novel components. GossipSub provides the underlying gossip protocol, while RLN adds cryptographic rate limiting. Publishers register on-chain with privacy-preserving commitments. Relay nodes verify zkSNARK proofs confirming rate limit compliance through mathematical verification rather than tracking users. Performance metrics exceed expectations. Proof generation completes in under 300 milliseconds. Total latency overhead remains between 10-50%. The incentive design demonstrates particular cleverness—rate limit violators face automatic disconnection as reputation scores plummet. Waku demonstrates anonymous, spam-resistant messaging at scale has moved from theoretical possibility to operational reality. (Revuelta, et al., 2024)

Named Data Networking challenges fundamental assumptions about network architecture. Ma's NDN Workspace questions the basic premise guiding internet development for fifty years: that data resides at specific network locations. This host-centric model may represent not optimal design but historical artifact we've unnecessarily preserved. NDN inverts traditional networking principles entirely. Data becomes self-authenticating through cryptographic signatures. Content receives semantic names like "/alice/dissertation/chapter3.pdf" rather than location-based addresses. These names function universally across network changes, device migrations, even infrastructure failures. Performance benchmarks prove encouraging—NDN matches centralized speeds while providing vastly superior resilience. Ma raises profound questions about technological path dependence. By focusing on data semantics rather than temporary location, NDN opens genuinely new possibilities for resilient, sovereign communication architectures. (Ma, 2024)

Communities & Moderation in Decentralised Networks

The Bluesky platform's public launch on February 6, 2024, provides valuable empirical data on decentralized platform dynamics. Within 24 hours, the platform experienced six-fold user increase—1.5 million new registrations generating 71 million trackable actions. Particularly noteworthy is toxicity metrics' stability despite massive influx. Traditional platform theory predicts rapid growth correlates with increased toxic behavior, yet Sahneh's comprehensive data analysis reveals remarkably stable toxicity levels throughout.

An intriguing linguistic shift occurred during expansion. Japanese-language content increased from 14% to 44% of total platform activity, temporarily displacing English as dominant language. This organic shift—occurring without algorithmic intervention—represents significant departure from typical platform dynamics. Analysis reveals highly concentrated malicious activity patterns. Approximately 62% of low-credibility links originated from just ten accounts existing before public opening. However, unlike traditional platforms, these malicious actors faced swift moderation through transparent community mechanisms rather than opaque algorithmic enforcement. The data suggests counterintuitive finding: decentralized moderation structures may maintain

community standards more effectively than centralized systems during rapid growth phases. Transparency of enforcement mechanisms appears crucial. (Sahneh, et al., 2024)

Bono's comprehensive analysis of 3.2 million block events provides unprecedented insights into decentralized moderation dynamics. The public availability of Bluesky's blocking data transforms traditionally opaque platform behaviors into observable phenomena. Rather than serving purely defensive functions, blocks appear to operate as sophisticated boundary-setting mechanisms actively shaping community spaces. A particularly striking finding concerns high-activity users attracting disproportionate blocking despite exhibiting no increased toxicity. This suggests visibility itself triggers blocking responses—users employ blocking as curatorial tool for managing social environment. Machine learning analysis yields remarkable results. Models achieve high accuracy predicting blocks, yet just three variables—reply frequency, mention patterns, and network centrality—capture majority of predictive power. This simplicity suggests communities develop consistent heuristics for problematic behavior.

The emerging system resembles distributed sensing network for community health. This transparency creates novel dynamics enabling organic moderation emergence. (Bono, et al., 2025)

Surve's architectural analysis reveals fundamental shifts in user-platform power dynamics. The AT protocol implements user sovereignty through cryptographic guarantees rather than policy promises. Users maintain complete control over repositories containing comprehensive social graph. This enables genuine seamless migration between service providers without data loss or social capital erosion. The "pick-your-moderator" service model introduces unprecedented governance flexibility. Different communities can select moderation approaches precisely aligned with specific values. Religious communities might emphasize content standards reflecting beliefs, academic groups prioritize factual accuracy, while artistic communities maximize expressive freedom.However, increased user agency demands substantially greater engagement and technical sophistication. Platform participation requires conscious community construction. This raises important accessibility questions about potential digital inequality. (Surve, et al., 2024)

Huang's analysis exposes fundamental tensions in decentralized platform design. The core insight proves sobering: technology alone cannot resolve deeply rooted social problems. Decentralized architectures must navigate irreducible trade-offs between knowledge production, democratic discourse, and individual autonomy. Attempting to optimize all three simultaneously proves mathematically impossible. Without institutional gatekeepers, information environments risk devolving into unanchored discourse. Communities may develop fundamentally incompatible epistemological frameworks, inhibiting cross-pollination essential for democratic debate. Technical accessibility creates substantial barriers. Key management requirements and protocol selection transform theoretical freedoms into practical exclusions. Every design decision embeds normative assumptions—shared blocklists encode collective values, federation flexibility negotiates autonomy versus coherence. Seeking absolute solutions fundamentally misunderstands the challenge. Sustainable systems must enable adaptive navigation rather than static solutions. (Huang, 2024)

Vergne's contribution fundamentally reframes platform limitations through rigorous theoretical analysis. The platform trilemma presents mathematical constraint: free speech, free usage, and safe usage cannot be simultaneously optimized. This isn't merely difficult but structurally impossible. Attempts to maximize all three inevitably result in unstable compromises. This necessitates "ecosystem pluralism"—different platforms specializing in different value configurations. Vergne's observation reframes democracy: "social media primarily document political democracy's decline while spurring organizational democracy's revival." Platforms mirror pre-existing legitimacy problems while enabling novel collective organization beyond nation-state frameworks. Mandatory interoperability through "unified multihoming" leverages existing standards but requires regulatory frameworks. Democracy always involved negotiating irreconcilable values. Decentralized architectures simply make these negotiations visible and continuous. (Vergne, 2025)

Diversity of Decentralised Protocols

Jeong's taxonomical analysis brings much-needed structure to the diverse landscape of decentralized architectures. Four primary architectural approaches emerge, each embodying distinct ideological commitments. Federated systems like Mastodon create digital fiefdoms—server administrators exercise considerable control while participating network-wide. Server selection becomes critical: smaller servers risk sustainability, larger ones replicate centralization.

Pure peer-to-peer systems eliminate servers entirely, achieving theoretical censorship resistance through infrastructure absence. However, message delivery becomes unreliable—dependent on individual device

availability. Blockchain-based platforms introduce immutability, creating permanent records. While ensuring transparency, every communication becomes permanently etched. "Immutable social media" reveals profound implications: content remains forever accessible, creating new digital liability.

Hybrid approaches balance competing priorities through architectural compromise. Bluesky maintains decentralized identity with centralized infrastructure. These reflect pragmatic decisions raising questions about meaningful decentralization. Decentralization exists on a spectrum rather than binary state. Each system makes specific trade-offs. Successful systems must balance ideological purity with practical functionality. (Jeong, et al., 2018)

Oshinowo's analysis reveals how protocol design encodes implicit political philosophies. "Decentralization is not fixed end state but consequential design decisions" illuminates fundamental truth. Every technical choice embodies governance assumptions with profound implications. ActivityPub inadvertently recreates hierarchical structures. Instance administrators wield authority—users select digital sovereigns hoping for benevolence. AT Protocol's "modular liberation" unbundles platform functions promising user choice, yet Bluesky maintains control over essential infrastructure. Nostr embodies cryptographic anarchism purely, predictably enabling spam and scams.

Each protocol reveals creators' assumptions about human nature and social organization. (Oshinowo, et al., 2026)

Wei and Tyson provide sobering Nostr empirical data. 17.8 million posts across 712 relays achieve uncensorable communication. However, broadcasting to 34.6 relays average creates massive redundancy—98.2% of retrievals redundant, consuming 35 times centralized resources. Geographic distribution appears impressive—no country controls 25%. Yet 20% of relays experience 40% downtime. Despite Bitcoin integration, 95% operate at financial loss. Identity through public keys provides security but no recovery. Key loss means permanent identity loss—ideological purity over user experience. Nostr succeeds at its goal but struggles with spam, economics, usability. (Wei & Tyson, 2024)

Balduf examines Bluesky's sophisticated architecture complexities.

40,000 Feed Generators and 62 Labelers supposedly democratize curation. However, all depend on Bluesky PBC's infrastructure—distributed control illusion while maintaining dependencies. Only 1.1% utilize portable identity—striking given users joined escaping Big Tech. GDPR conflicts expose contradictions. Data persists indefinitely despite deletion requests. Users own data but depend on Bluesky's systems entirely. Bluesky represents particular decentralization interpretation prioritizing developer flexibility while maintaining operational control. (Balduf, et al., 2024)

Kocaoğullar challenges blockchain decentralization assumptions profoundly.

Counterintuitively, 1980s DNS achieves more meaningful decentralization than blockchain-based ENS. This illuminates architecture versus power distribution distinctions. ENS governance requires purchasing tokens—digital plutocracy. DNS employs multi-stakeholder governance achieving broader representation. Every ENS update requires gas fees creating barriers. DNS updates involve no direct costs. Sometimes boring committees create more meaningful distribution than elegant cryptography. (Kocaoğullar, et al., 2024)

Open Standards & Interoperability

Portable digital identity represents fundamental shift in platform power dynamics. Surve's DID and PDS analysis reveals identity transformation from platform-controlled to user-sovereign resource. Globally unique identifiers secured through cryptographic verification operate independently, creating genuine portability. PDS architecture enables true data portability without information loss. When switching costs approach zero, platforms must compete on service quality rather than lock-in. However, only 1.1% utilize these features despite joining to escape traditional constraints. Complexity creates accessibility challenges. Gap between capability and usability represents current limitation and future opportunity. (Surve, et al., 2024)

Vergne's unified multihoming framework addresses fragmentation elegantly. "Social media document political democracy's decline while spurring organizational democracy's revival" reframes the challenge. Platform fragmentation obstructs meaningful decentralization more than diversity itself. This enables productive specialization. Expression-focused platforms minimize moderation, safety-oriented platforms implement

comprehensive protection. Users navigate with portable identities choosing appropriate contexts. Government mandates could transform dynamics. Telecommunications precedent suggests regulatory frameworks could mandate genuine portability, transforming winner-take-all into competitive markets. (Vergne, 2025)

SendingNetwork bridges blockchain's critical communication gap. Yeung identifies fundamental limitation: blockchain lacks native real-time communication. This forces applications toward centralized messaging, undermining decentralization principles. Three-layer architecture addresses comprehensively. Double Ratchet provides forward secrecy through continuous key rotation. Delegation achieves linear O(N) scaling. Universal addressing eliminates traditional communication silos. SendingNetwork bridges Web2/Web3 paradigms enabling value transfer across incompatible systems. (Yeung, 2024)

Bluesky's Firehose tests radical transparency limits profoundly. Balduf documents unprecedented openness: 30GB daily streams to anyone without gatekeeping. This catalyzed remarkable ecosystem development—40,000 Feed Generators emerged. However, processing requires substantial computational resources. Infrastructure requirements shift gatekeeping from access to capacity. Privacy tensions prove most challenging—deleted content remains permanently accessible to archivists. Does meaningful decentralization require radical transparency? The experiment provides valuable empirical data. (Balduf, et al., 2024)

Ma's NDN reconceptualizes network architecture fundamentally. Challenging five decades' assumptions, NDN proposes addressing data by content not location. Data incorporates cryptographic signatures proving authenticity without authorities. Semantic names replace addresses, decoupling information from infrastructure entirely. Whether representing networking's future or important thought experiment, NDN demonstrates questioning fundamental assumptions' value. (Ma, 2024)

The Future of the Decentralised Web

Transformation from singular Internet to plurality of interconnected networks has already begun. Singh presents compelling vision: infrastructure reflecting human community structures rather than corporate models. IEEE 802.11s enables communities constructing their own networks. Trust emerges through behavioral verification rather than certification. Challenges require serious acknowledgment. Deployment demands technical expertise and social cohesion. Without accessibility attention, requirements risk deepening digital divides. Infrastructure embodying democratic principles presents compelling alternative. Discourse evolved from questioning feasibility to determining optimal implementation strategies. (Singh, et al., 2020)

Profound democratic participation shifts occur through decentralized channels. Vergne illuminates striking paradox: only 8% experience traditional democracy while millions participate in DAOs. These function as experimental laboratories for collective decision-making accessible regardless of political system. Taiwan's Polis achieves 80% implementation rate—remarkable by any democratic standard. Like maritime communities pioneering governance while monarchies ruled, DAOs operate at power structure margins developing practices where institutions cannot reach. Innovation velocity is extraordinary. Traditional systems required centuries; DAOs compress to months. We witness democracy's next evolutionary phase—supplementing traditional institutions with new forms. (Vergne, 2025)

NFT markets transform into creator empowerment infrastructure fundamentally. Miller traces evolution from speculation to foundational economic infrastructure. Social tokens establish unprecedented creator-audience alignment. Supporters transition from passive consumers to active stakeholders. DeFi integration amplifies possibilities dramatically. Lens Protocol exemplifies paradigm shift—cryptographic audience ownership portable across platforms. However, digital inequalities threaten replicating existing hierarchies. Historical precedent suggests technologies exacerbate inequality before democratizing. Realizing potential requires prioritizing broad accessibility. (Miller, et al., 2025)

Traditional corporate structures confront fundamental transformation. Murray documents enterprise navigation comprehensively. Companies must "collaborate directly, share decision-making, develop novel revenue streams." Customer relationships evolve to participatory partnerships. DAOs demonstrate radically alternative structures. Geographic constraints become irrelevant, hierarchies optional. Web 3.0's compressed timeline dramatically accelerates adaptation. Organizations navigating successfully discover substantial advantages; others face potential obsolescence. (Murray, et al., 2022)

Civ Kit converges technologies into unified marketplace architecture remarkably. Gregory synthesizes Bitcoin security, Lightning efficiency, Nostr communication enabling "global trade without intermediaries." Web-of-

Stakes transforms reputation into concrete economic risk. Traditional infrastructure systematically excludes billions. Civ Kit's minimal requirements democratize participation dramatically. "Markets without masters" progressed from theoretical manifesto to practical implementation. (Gregory, et al., 2023)

Conclusions

The architectural diversity emerging across decentralized protocols reveals something beyond simple opposition to centralization—it's fundamental rethinking of how infrastructure mediates human interaction. SendingNetwork's O(N) messaging breakthrough through delegation schemes isn't clever engineering; it's conceptual revolution. Dual consensus—vertical chains submitting horizontally—creates trust without authority. NDN challenges fifty years of assumptions. Ma's right: we've been solving the wrong problem, routing between endpoints when we should route content itself. What's striking is how protocols navigate ideological purity versus sustainability. Nostr's radical simplicity—your public key is your identity, period—borders on nihilism. Yet it works. The 98% redundancy isn't inefficiency; it's the price of genuine censorship resistance. Meanwhile, Bluesky's "modular liberation" maintains just enough centralization for usability while enabling exits 98.9% won't exercise. This spectrum isn't weakness—it's recognition that communities require different trade-offs.

Economic models merit scrutiny. Vergne's trilemma captures why no architecture optimizes speech, usage, and safety simultaneously. But deeper: DAOs aren't just funding mechanisms; they're governance laboratories bypassing institutional ossification. Taiwan achieves 80% implementation through Polis while democracies struggle with basic consensus. We're witnessing alternative decision-making pathways emerge. DAO iteration cycles—decades compressed to months—suggest Cambrian explosion of institutional forms. Persistent patterns reveal fundamental constraints. Trust must be computationally verifiable or socially constructed—no middle ground. Identity portability demands cryptographic sovereignty users find burdensome. Spam resistance requires economic stakes or exclusion. These aren't bugs but trade-offs. Civ Kit's Web-of-Stakes binds reputation to economic risk. Waku's RLN achieves similar through zero-knowledge—300 milliseconds generating proof enables anonymous participation without abuse.

Infrastructure questions loom larger than acknowledged. Singh's mesh networks could route around control, but who maintains routers when enthusiasm wanes? Economic data sobers—$2.4 billion lost to shutdowns, yet alternative infrastructure requires uncertain investment. Technology works; incentives struggle. Free riders proliferate while providers subsidize until burnout. Yet something significant happens at margins. Creator tokens align incentives advertising never could. Lens Protocol's cryptographic audience ownership diminishes platform risk. Traditional businesses experimenting with DAOs indicates Web3 permeating beyond crypto-natives. These aren't incremental improvements but structural transformations.

Moderation reveals deepest tensions. Bluesky's radical transparency enables oversight but creates privacy concerns. Pick-your-moderator offers flexibility but risks hermetic bubbles. These aren't problems but tensions to manage. What emerges isn't roadmap to inevitable decentralization but recognition of sustained infrastructure experimentation. Technical foundations exist: mature cryptography, evolved P2P, aligned incentives. Whether experiments coalesce depends on communities finding complexity worthwhile. When stakes suffice—communities facing shutdowns—complexity becomes acceptable. The question isn't whether decentralized replaces centralized—it's which communities find them necessary. The answer varies by geography, politics, conditions—mosaic not replacement. The internet's future might resemble diverse, locally adapted systems these protocols enable.

References

- Balduf, L., Sokoto, S., et al., "Looking AT the Blue Skies of Bluesky," IMC '24, 2024.
- Bono, C., Liu, N., Russo, G., & Pierri, F., "Self-moderation in the decentralized era," arXiv:2505.01174v1, 2025.
- Gregory, N., Youssef, R., & Riard, A., "Civ Kit: A Peer-to-Peer Electronic Market System," 2023.
- Huang, T., "Decentralized social networks and the future of free speech online," Computer Law & Security Review, vol. 55, 2024.
- Jeong, U., Ng, L. H. X., et al., "Navigating Decentralized Online Social Networks," 2018.
- Kocaoğullar, Y., Osterweil, E., & Zhang, L., "Towards a Decentralized Internet Namespace," DIN '24, 2024.
- Ma, X., "Towards Decentralized Applications," Ph.D. dissertation, University of California, Los Angeles, 2024.
- Miller, R., Steve, J., & Hart, M., "From Crypto to Content: The Expanding Landscape of Digital Assets," 2025.

- Murray, A., Kim, D., & Combs, J., "The Promise of a Decentralized Internet: What is Web 3.0 and How Can Firms Prepare?" Business Horizons, forthcoming, 2022.
- Oshinowo, T., Hwang, S., et al., "Seeing the Politics of Decentralized Social Media Protocols," 2026.
- Revuelta, A., Tikhomirov, S., Challani, A., Cornelius, H., & Vivier, S. P., "Message Latency in Waku Relay with Rate Limiting Nullifiers," DLT2024 Workshop, 2024.
- Sahneh, E. S., Nogara, G., et al., "The Dawn of Decentralized Social Media: An Exploration of Bluesky's Public Opening," arXiv:2408.03146v1, 2024.
- Schichtholz, B., Bless, R., Jacob, F., Hartenstein, H., & Zitterbart, M., "RePP2P Matrix: Decentralized Relays to Improve Reliability and Performance of Peer-to-Peer Matrix," DIN '24, 2024.
- Singh, R., Donegan, A., & Tewari, H., "Framework for a Decentralized Web," arXiv preprint, vol. 2008, no. 02083, pp. 1-7, 2020.
- Surve, A., Shamraj, A., & Mehta, S., "How Decentralization Affects User Agency on Social Platforms," arXiv preprint, vol. 2406, no. 09035, pp. 1-11, 2024.
- Vergne, J.-P., "The Social Media Platform Trilemma and the Future of Democracy," 2025.
- Wei, Y., & Tyson, G., "Exploring the Nostr Ecosystem: A Study of Decentralization and Resilience," arXiv preprint, vol. 2402, no. 05709, 2024.
- Yeung, M., "SendingNetwork: Advancing the Future of Decentralized Messaging Networks," arXiv preprint arXiv:2401.09102v2, 2024.