

Decentralized Platforms: Comprehensive Comparative Analysis

Section 11 – Final Index, Master Comparison Tables & Architectural Decision Guidance
Version 3.0 | 16 August 2026 | Segment 11 of 11 (Final)

11.1 Complete Document Index

#	Segment	File
01	Executive Summary	01_Executive_Summary
02	Scope, Methodology & Conceptual Landscape	02_Scope_Methodology_Landscape
03	Nostr Deep Profile	03_Nostr_Deep_Profile
04	Peergos Deep Profile	04_Peergos_Deep_Profile
05	Solid (Data Pods) Deep Profile	05_Solid_Deep_Profile
06	IPFS Deep Profile	06_IPFS_Deep_Profile
07	Secure Scuttlebutt (SSB) Deep Profile	07_SSB_Deep_Profile
08	Syncthing Deep Profile	08_Syncthing_Deep_Profile
09	Matrix Deep Profile	09_Matrix_Deep_Profile
10	ActivityPub / Fediverse Deep Profile	10_ActivityPub_Deep_Profile
11	Final Index, Comparison & Guidance	11_Final_Index_Comparison_Guidance

All segments: /home/workdir/artifacts/decentralized-comparison/segments/

11.2 Platforms at a Glance

Platform	One-line characterization	Best-fit use
Nostr	Minimal event protocol + keypair + relays	Censorship-resistant social / notes
Peergos	Vertical encrypted FS + social + sandboxed apps	Private quantum-resistant storage & sharing
Solid	User-owned Pods + WebID + WAC/ACP	Personal data ownership & app interop
IPFS	Content-addressed blocks + DHT + gateways	Verifiable distribution & permanent links
SSB	Local-first signed feeds + gossip	Offline-capable social graphs
Syncthing	Continuous block-level folder sync	Multi-device file consistency
Matrix	Federated rooms + events + Olm/Megolm	Secure team & community messaging
ActivityPub	W3C federated social activities (Fediverse)	Open public social web across many apps

11.3 Master Feature Comparison

Legend: ✓ = strong/native · ~ = partial/optional · – = weak or absent

Feature	Nostr	Peergos	Solid	IPFS	SSB	Syncthing	Matrix	AP
Crypto user identity	✓	✓	~	–	✓	–	~	–
Domain/server identity	–	–	–	–	–	–	✓	✓
Device identity	–	–	–	–	–	✓	✓	–
Default E2EE content	–	✓	–	–	~	~	✓	–
PQ sharing deployed	–	✓	–	–	–	–	–	–
Strong metadata protect.	–	✓	–	–	~	–	–	–
Content addressing	–	~	–	✓	–	–	–	–
Append-only history	✓	–	–	–	✓	–	~	–
Continuous file sync	–	–	–	–	–	✓	–	–
Federated servers	–	~	–	–	–	–	✓	✓
Relay/gossip model	✓	–	–	–	✓	–	–	–
Sandboxed apps	–	✓	~	–	–	–	–	–
Rich multi-client	✓	–	–	✓	~	✓	✓	✓
Offline/local-first	~	~	~	~	✓	✓	–	–
Public social network	✓	–	–	–	~	–	~	✓
Self-hostable	✓	✓	✓	✓	✓	✓	✓	✓

11.4 Benefits & Downsides (Condensed)

Nostr: Simple, diverse clients, hard to censor · Key UX, spam, no private storage. **Peergos:** Strongest privacy, PQ sharing, capabilities · Almost no 3rd-party clients. **Solid:** Clean data ownership · Immature apps, weaker default encryption. **IPFS:** Content addressing, large ecosystem · Public by default, pinning required. **SSB:** Offline strength, unforgeable feeds · Multi-device hard, modest scale. **Syncthing:** Reliable continuous sync, no cloud · Files only, not social. **Matrix:** Production messaging, E2EE, bridges · Homeserver trust, complexity. **ActivityPub:** Largest open social multi-app network · Domain identity, instance moderation, E2EE emerging.

11.5 Architectural Decision Guidance

Primary data shape: Public notes → Nostr/AP · Real-time chat → Matrix · Private files → Peergos · Continuous folders → Syncthing · Personal structured data → Solid · Verifiable content → IPFS · Offline social → SSB.

Confidentiality: Max content+metadata → Peergos · Strong messaging E2EE → Matrix · Transit+device trust → Syncthing · Public by design → Nostr/AP/IPFS.

Client diversity: Highest → Nostr, AP, Matrix, IPFS, Syncthing · Lowest → Peergos.

Identity preference: User keypair → Nostr/SSB/Peergos · Domain → Matrix/AP · Device cert → Syncthing · WebID → Solid.

Offline strength: SSB, Syncthing strongest; Matrix/AP/Solid more server-dependent for live use.

Common hybrids: Private files + public social (Peergos/Syncthing + Nostr/AP) · Team chat + file sync (Matrix + Syncthing) · Content + social (IPFS + AP/Nostr) · Max resilience (SSB/Nostr social + Syncthing files + self-hosted Matrix).

11.6 Consolidated Official Links

- Nostr: nostr.com · github.com/nostr-protocol/nips
- Peergos: peergos.org · book.peergos.org · github.com/Peergos
- Solid: solidproject.org · solidproject.org/TR · github.com/solid/specification

- IPFS: ipfs.tech · docs.ipfs.tech · specs.ipfs.tech · github.com/ipfs
- SSB: scuttlebutt.nz · ssbc.github.io/scuttlebutt-protocol-guide · github.com/ssbc
- Syncthing: syncthing.net · docs.syncthing.net · github.com/syncthing/syncthing
- Matrix: matrix.org · spec.matrix.org · element.io
- ActivityPub: w3.org/TR/activitypub · activitypub.rocks · codeberg.org/fediverse/fep

11.7 Validation Notes & Next Steps

Sections built from primary docs, specs, GitHub and 2025–2026 project status. Network stats are approximate. Re-verify audits and threat models for production. Series is an architectural reference, not a substitute for primary specs.

Suggested next steps: (1) Map requirements to the decision tables. (2) Prototype top 1–2 candidates with realistic volumes. (3) Review audits, key management and recovery for sensitive data. (4) Consider hybrids early. (5) Re-compose these modular segments into internal design docs or runbooks.