

SCDO Laboratory · TECH PR · UNIT 07

Automated Contract Ledgers for AI Agents · Next-Gen Smart Payments

Decentralized Social: Identity Graphs

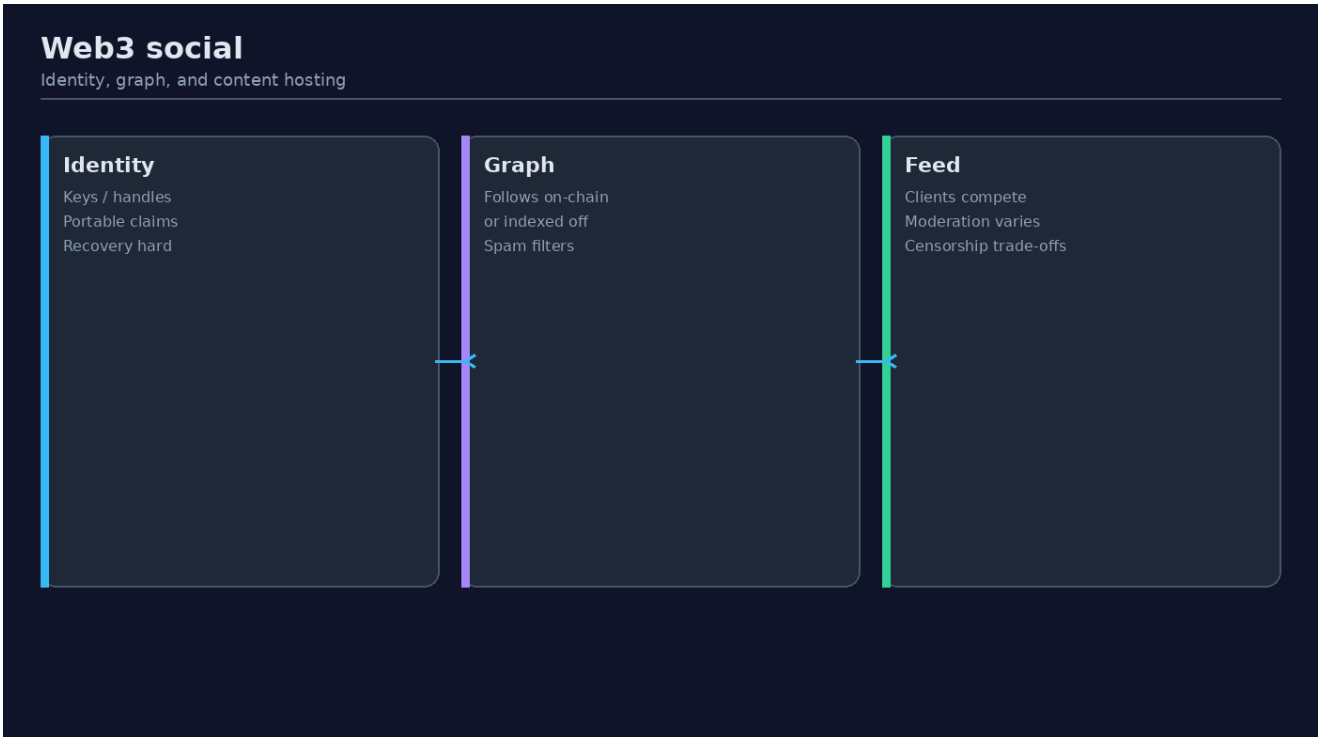
DIDs, graphs, and content sovereignty · Ying Willam Zhang · 2026

> Disclaimer: This primer is for education only — not investment, legal, or tax advice.

7. Decentralized social

SCDO Lab · Web3 Primer for Newcomers v2 · English edition
When social wants to “go protocol,” the fight is not another App skin—it is **whether relationships and content are portable, who can ban you, where data lives**.
Compresses the old two long essays; clarifies **federation ≠ fully decentralized**.
Not investment advice.

What is Web3 social?



Web2 social: accounts live on platforms; fans and posts mostly lock to platforms; companies change rules.
Web3 social tries to put some identity, follow graphs, and content indexes on **open protocols or user-controllable storage**, so apps become replaceable “clients.”

Ideal: change frontend, keep your social graph.
Reality: UX, moderation, discovery, and anti-spam remain hard; many products are still “Web2 with wallet login.”

Tiny history

From forums and blogs to giant feeds, centralization brought growth and lock-in/censorship fights. After blockchains heated up, “on-chain social” experiments appeared: follow graphs on-chain, NFTs as tickets, tokens for posting—some shipped products; some only shipped charts. In 2026 the calm read separates protocol layers (graphs, relays) from app layers.

How to enter (low risk)

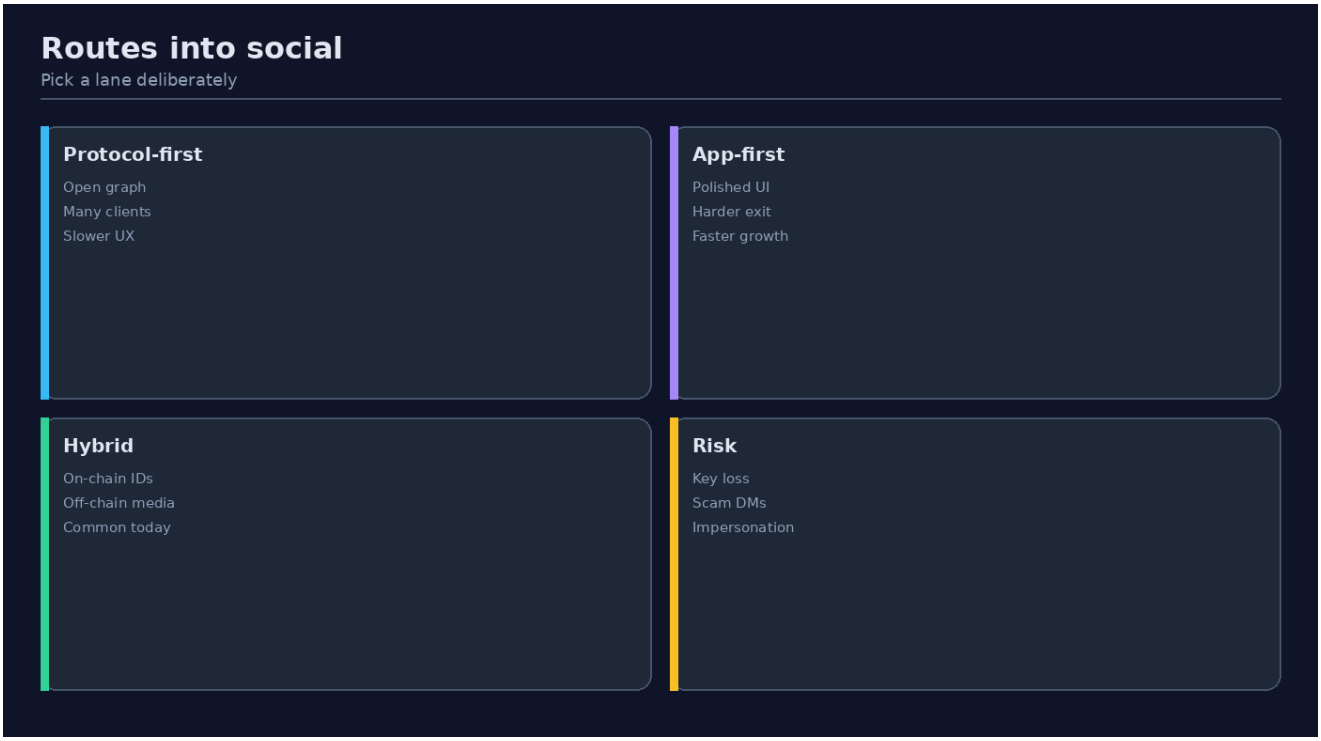
1. Start as a reader: which protocol does this product use?
2. Experiment with tiny funds or empty accounts; do not bind your main wallet’s large assets first.
3. Separate **on-chain writes** (costly, slow, permanent) vs **off-chain storage** + **on-chain pointers**.
4. Assume exits, shutdowns, and protocol migrations can happen—test portability.

Stack layers: infrastructure / middleware / apps / tools

Layer	Role	How newcomers touch it
Infrastructure	Public chains/L2s, identity, storage, availability	Usually indirect
Middleware	Social-graph protocols, indexing, notifications, permissions	Decides “can I move”
Apps	Clients and creator studios you open daily	The thing you swipe
Tools	Analytics, anti-phishing, cross-client import	Safety and migration

Choose products backwards: is the app nice? → is middleware open? → is infrastructure costly, where are censorship points?

Three routes: Lens / Mastodon / Nostr



Lens-class: on-chain social graph protocols

- **Idea:** follow/post relations as protocolized as possible so many clients share a graph.
- **Feel:** often wallet signatures; on/near-chain ops affect fees and pace.
- **Watch:** open protocol ≠ one frontend is decentralized; NFT/token incentives can inject speculative noise.

Mastodon: the Fediverse

- **Idea:** many independent servers (instances) interoperate with shared protocols—like email domains.
- **Critical clarification: federation ≠ no admins**. Each server still has people setting rules, bans, and storing your data. You "change post offices," not "abolish post offices."
- **Fit:** people who dislike one global corporate moderator and will choose a community server.
- **Cost:** discovery is fragmented; server risk (admin malice or shutdown).

Nostr: key identity + relays

- **Idea:** identity ≈ key pair; messages to multiple relays; diverse clients.
- **Feel:** more "crypto-native"; spam and discovery depend on clients and relay quality.
- **Watch:** lost private key ≈ lost identity; relays can refuse service—censorship resistance is a degree question.

Contrast table

	Lens-class	Mastodon federation	Nostr
Identity	Often wallet / profile NFT	Server account	Public/private keys
Moving	Depends on protocol + clients	Server export / interoperability	Clients easier; maintain your relay list
Decentralization point	Chain and governance assumptions	Many servers, not zero admin	Many relays, not automatic permanence
Main friction	Signatures, fees, complexity	Server choice and fragmentation	Spam and key security

Farcaster and similar "sufficiently decentralized + strong product" routes mix on-chain identity with off-chain messages—when reading docs, grab **data availability and censorship points**.

Trends and boundaries (2026)



Worth watching: verifiable credentials in social (attendance, contribution, weak anti-Sybil signals); client competition; better wallet-signing UX.
Do not fantasize: full replacement of super-apps next year; an unmoderated high-quality global square appearing automatically; token incentives alone growing healthy public discourse.

Security: "support" DMs, signature approvals, fake airdrops are dense in social scenes—Chapter 9 generalizes.

SCDO, lightly: if social graphs serve real communities, they need auditable permissions and anti-abuse—not only points. Agent auto-posting needs budgets and logs even more.

Anti-spam and Sybils: the tax of open protocols

Open write invites spam and farming. Web2 uses central algorithms and humans; Web3 social often uses stake, invites, CAPTCHAs, client filters, reputation scores. Each introduces new centers or new discrimination. **A fully unmoderated global square** and **high-quality conversation** rarely coexist—products must choose explicitly.

Content storage strategies

- Full text on-chain: expensive, permanent, hard to delete (a feature in some cases).
- Off-chain storage + on-chain hash: cheaper; depends on storage networks or companies.
- Relay-only: faster; durability follows relay policy.

Creators should ask: which copy is the “canonical” one you care about?

Honest creator economics

Token tips, fan tokens, content NFTs all tell stories. Sustainable creator income still mostly comes from sponsorships, memberships, ads, live events—on-chain tools are amplifiers, not automatic financial freedom. Locking fans into one speculative coin collapses communities when the coin collapses.

Privacy

Pseudonymous addresses can still be clustered. On-chain social graphs make follows more transparent—and easier to surveil. When you need privacy: separate identity addresses, reduce on-chain social binding, learn advanced ZK/mixnet tools (learning cost applies).

Product selection flow

1. Do I want “anti-giant” or “a more fun feed”?
2. Can I export or recreate relationships in a second client?
3. If keys are lost, is social recovery possible?
4. In moderation fights, where do I stand—choose servers/protocols that match values.
5. Did I connect my main wallet to a high-risk experimental client?

Crossings with news / governance

DAO votes, forums, Snapshot-class tools often link social identity. Watch **vote buying, farming, concentrated delegation**. On-chain governance is not automatic democracy—only a countable rule set.

Moderation, values, and the “protocol neutrality” myth

Protocols claim neutrality; clients still filter; relays still refuse; servers still ban. Users want **predictable rules** and **migratable exits**, not abstract absolute neutrality. Joining a federated server or a client’s default blocklist is already taking a side—normal. What matters: are rules public, abusive, and can you leave with relationships?

Another reality: celebrities and institutions may still prefer more centralized, better-moderated products for brand safety. Web3 social will not auto-become the only public sphere; it will be one among many. Accept that, and debate stops being a religious war.

Builders: ship high-quality tools for small communities before “global replace.” Users: experiment on alts; bind main identity carefully.

FAQ (social)

Q: Wallet login = decentralized?
A: Only a login method; content and moderation may still be centralized.

Q: Server dies—then what?
A: In federation, backups/migration matter; choose servers carefully.

Q: Lost Nostr private key?
A: Identity is hard to recover; multi-device strategy and social recovery if the client supports it.

Q: Connect main wallet to social DApps?
A: Prefer dedicated addresses.

Q: On-chain posting too expensive?
A: Most designs put content off-chain or on L2.

Product metrics for protocol social

Do not measure Web3 social only by token price. More informative: how many daily addresses are real interaction, client-switch rates, migration success, abuse rates, creator

repeat-post rates, whether people use the identity for real-world ticket checks. Hard to measure ≠ ignorable—if you cannot measure, do not claim “already replaced.”

Governance communities that mix forums and votes must design against bribery and apathy: delegation, optimistic governance, one-address-one-vote vs one-person-one-vote each have pits. Bind social identity too tightly to voting power → bought accounts; too loosely → Sybils. No perfect formula—only revised rules with public revision logs.

For ordinary people, a practical strategy: **keep main social where you already know the network; experiment with alts and dedicated wallets**. Raise binding only after a protocol proves migration and moderation. Moving every social graph onto an experimental protocol is like putting every deposit into an experimental contract—brave, mismatched risk.

Client competition and open graphs

If graphs truly live on open protocols, clients should compete like email clients: better notifications, anti-spam, creation tools. In reality liquidity may still concentrate in one or two frontends because discovery has strong network effects. Open protocols lower the legal/technical ceiling of lock-in; they do not erase economic incentives to lock. As a user, occasionally try a second client—exercise for exit rights.

Developers worry about index cost and write cost: full-chain indexes are expensive; self-built indexes become new centers. Public community indexes, verifiable sync, light-client proofs are ongoing engineering. You need not build them—but understand when your timeline “can’t see latest” whether it is relay, index, or censorship. Misclassify the fault and you may recklessly rotate seeds or approve junk.

Finally, when social mixes with money stimuli, relationships financialize: follows become investments, replies become market moves. Sensible separation—e.g. dedicated “finance identity” vs “chat identity”—reduces personality eroded by price. Not a sermon; mental-health risk management.

Modular identity: from one giant profile to composable proofs

The likelier future is not “one decentralized Facebook wins,” but composable identity modules: login, reputation proofs, verifiable credentials, encrypted inbox from different protocols; frontends orchestrate. UX still decides winners. SCDO’s verifiable-record emphasis fits the “reputation/achievement” module—not rewriting the entire feed. Builders: pick a narrow cut and go deep. Users: avoid binding every module to one hot wallet.

Crisis comms and rumors

Decentralized social in crises is fast and messy: official and fake statements run in parallel; screenshots leave context. Projects should pre-stage multi-channel authenticity (on-chain notes, known-key signed notices, mirrors). Users should wait for verifiable statements instead of instantly forwarding spicy screenshots. That habit protects community assets better than any anti-phishing plugin.

Patch summary

Protocol social’ s decisive factors are migration cost and anti-abuse—not slogans. Alts first, binding later; second client before full migration.

Chapter wrap

1. Web3 social fights for portability and fewer single points—not another skin.
2. Read in layers: pretty apps ≠ open protocols.
3. Federation has admins; Nostr relies on keys and relays; on-chain graphs have fees and governance assumptions.
4. 2026 is still an experiment field; start with alts.
5. Next: **GameFi**—motives for on-chain game economies, failure modes, industry map—without “explosive growth” hype.

(End of Chapter 7 · v2 English edition · SCDO Lab)