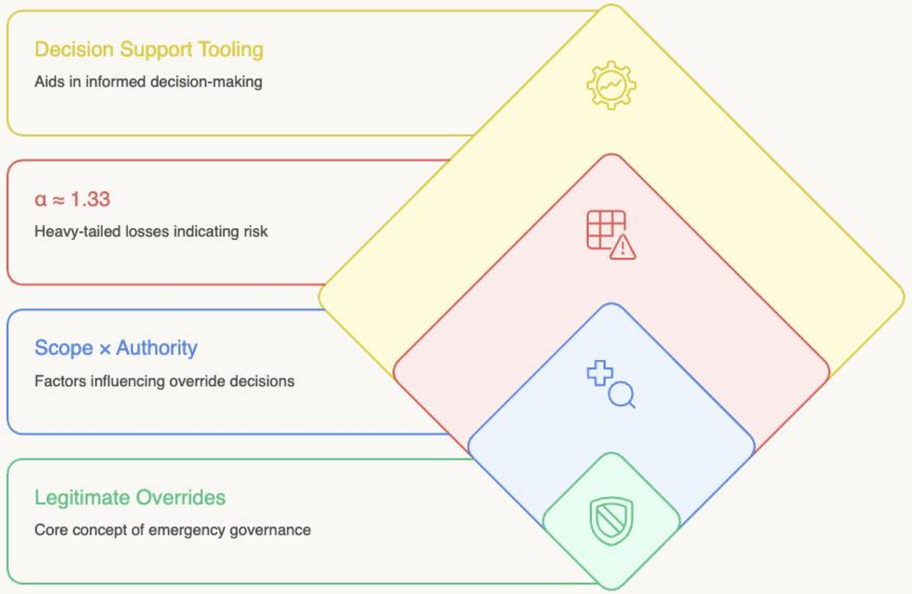
Legitimate Overrides in Decentralized Protocols

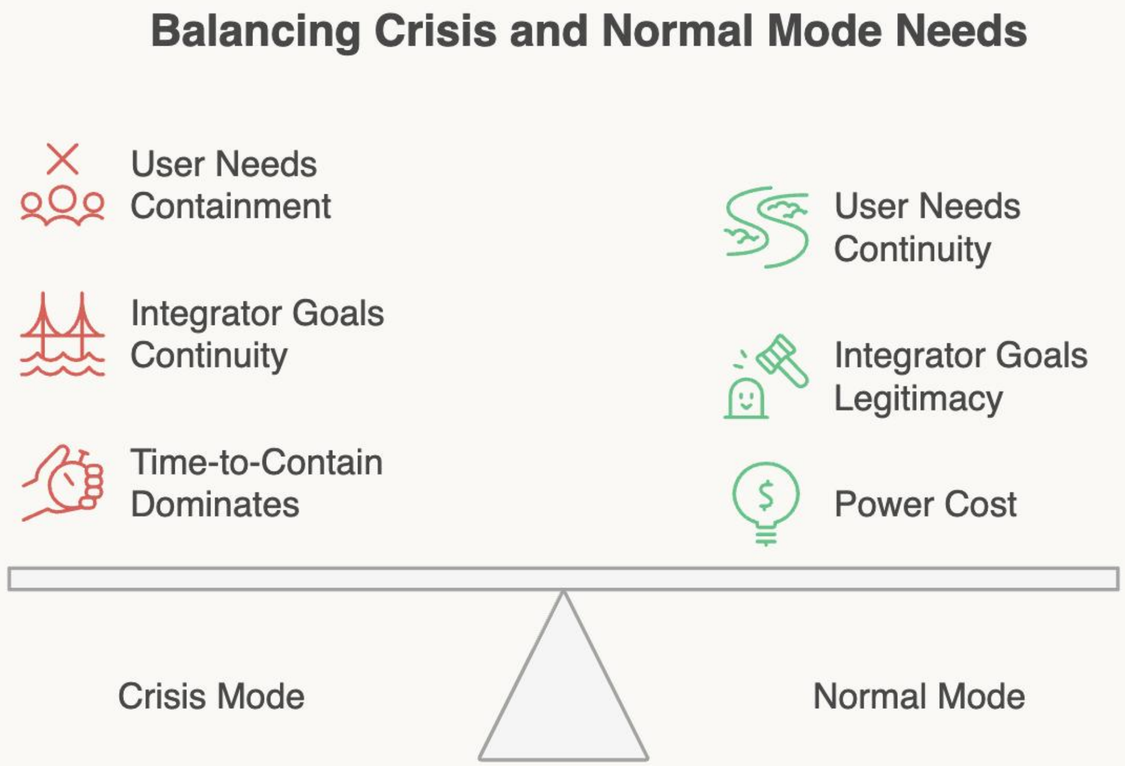
Engineering emergency governance under time pressure



TERSE 2026 · Elem Oghenekaro · Dr. Nimrod Talmon

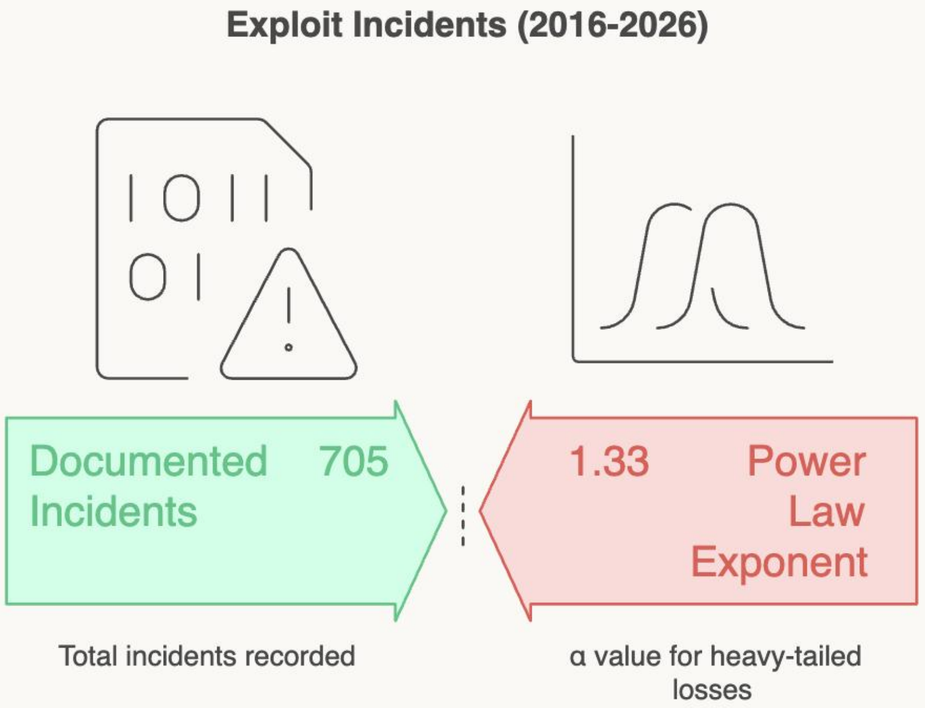
THE PARADOX

In crises, communities demand intervention. Outside crises, override capability reduces trust.



EVIDENCE

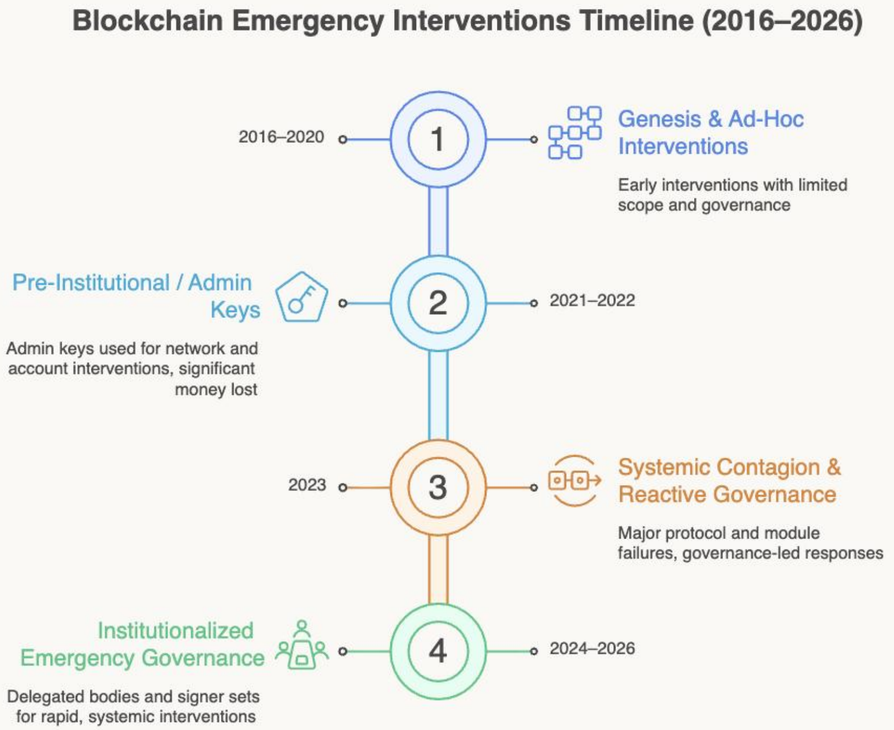
Dataset and scope



Interpreting the Power Law Exponent ($\alpha = 1.33$):

- Because $1 < \alpha < 2$, the distribution has a defined mean but *infinite variance*.
- This means standard deviation and traditional risk models fail; expected risk is heavily skewed by rare, catastrophic outliers (super-hacks).

Four eras of blockchain intervention

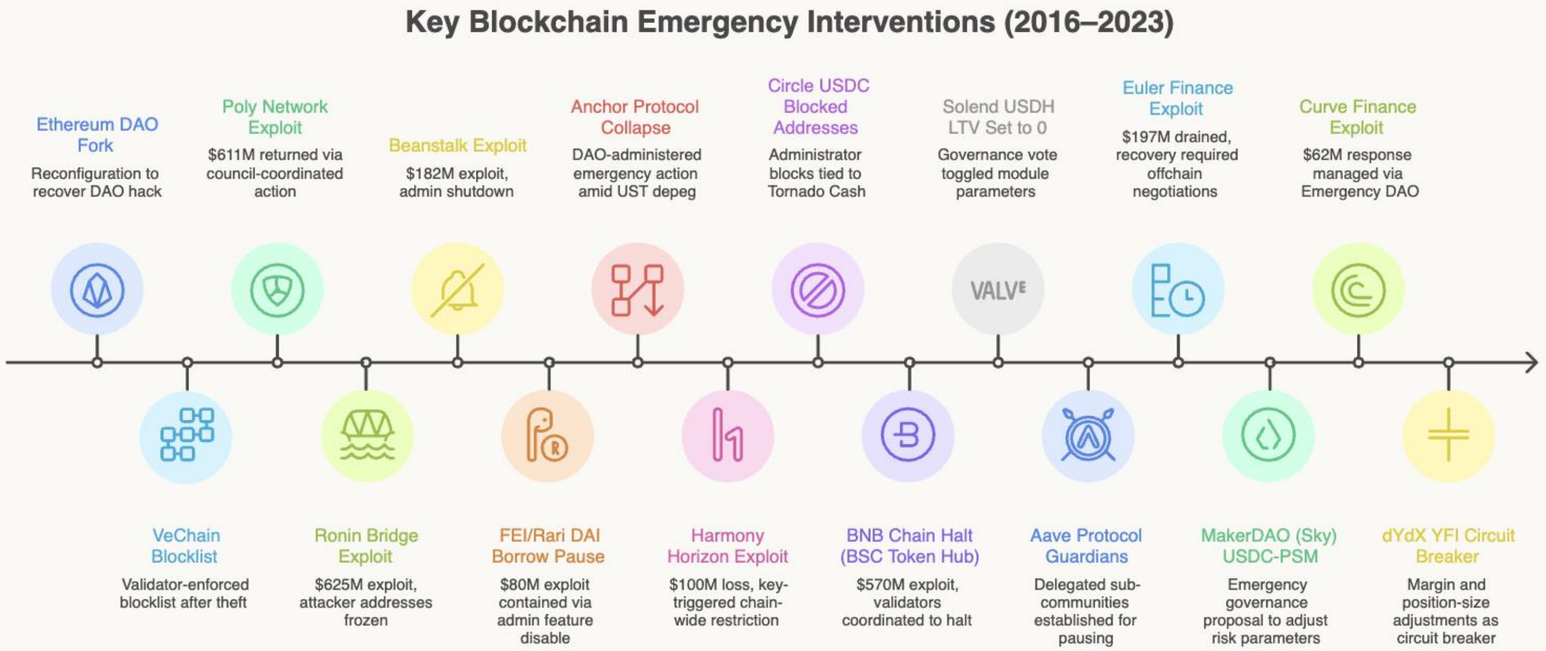


1) What

While systemic market failures (e.g., Terra, FTX) account for vast losses, a persistent ~$10B strata consists of technical exploits that are *addressable* by onchain emergency mechanisms. We synthesized some major incidents to map this evolution.

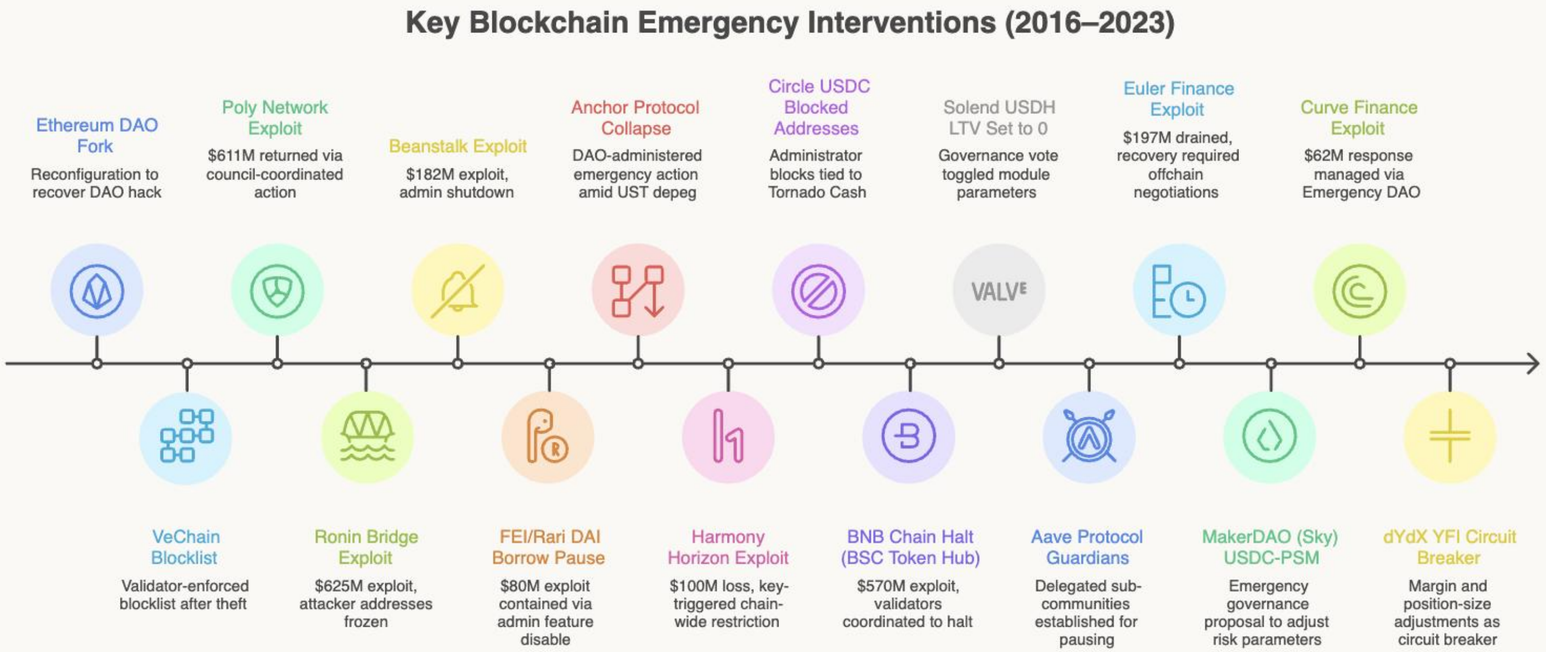
CASE STUDIES

Early interventions (Eras 1-3)



- **Era 1 – Genesis (2016–2020):** Ad-hoc forks and manual blocklists. No formal guardrails.
- **Era 2 – Admin Keys (2021–2022):** "God Mode" keys to freeze assets; validator collusion to halt networks.
- **Era 3 – Reactive Governance (2023):** Circuit breakers, delegated risk parameters, off-chain war rooms.

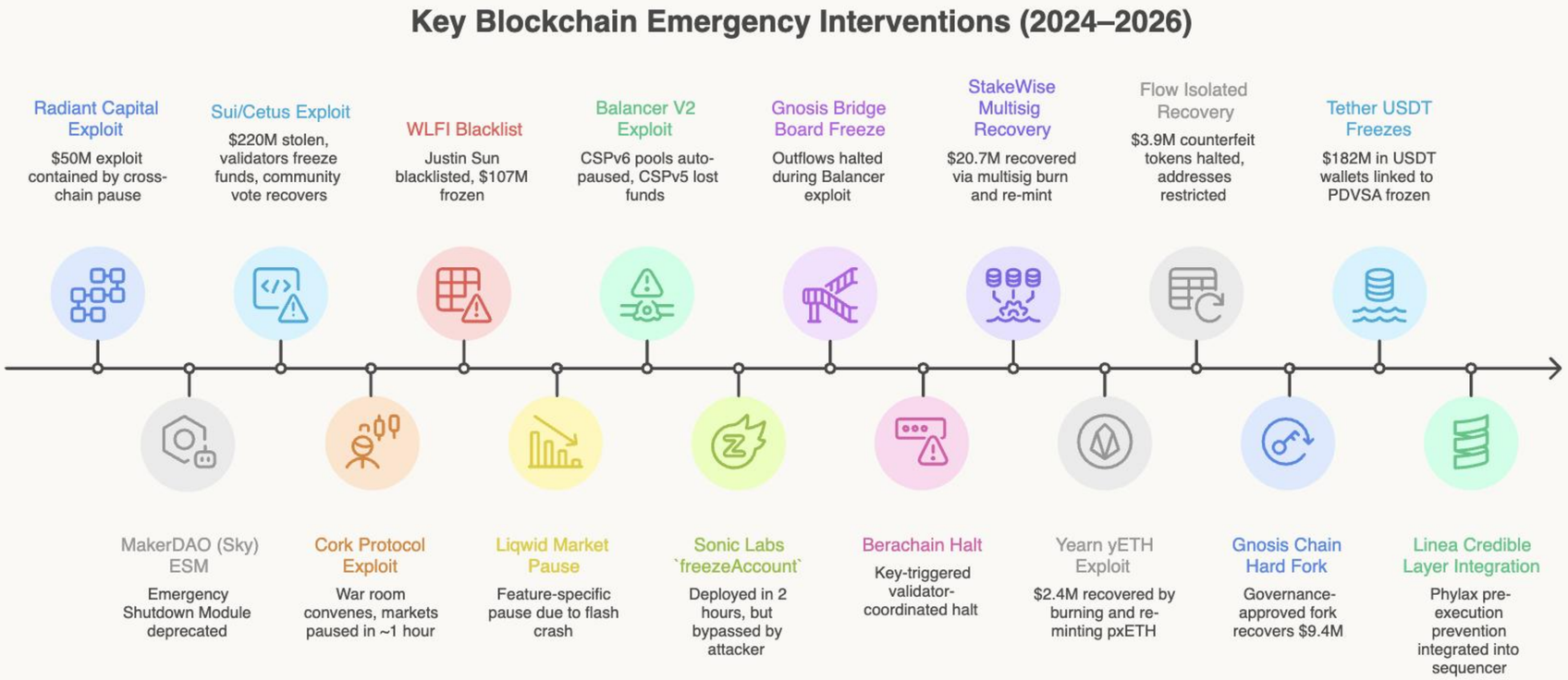
Early interventions (Eras 1-3)



- **Era 1 – Genesis (2016–2020):** Ad-hoc forks and manual blocklists. No formal guardrails.
- **Era 2 – Admin Keys (2021–2022):** "God Mode" keys to freeze assets; validator collusion to halt networks.
- **Era 3 – Reactive Governance (2023):** Circuit breakers, delegated risk parameters, off-chain war rooms.

CASE STUDIES

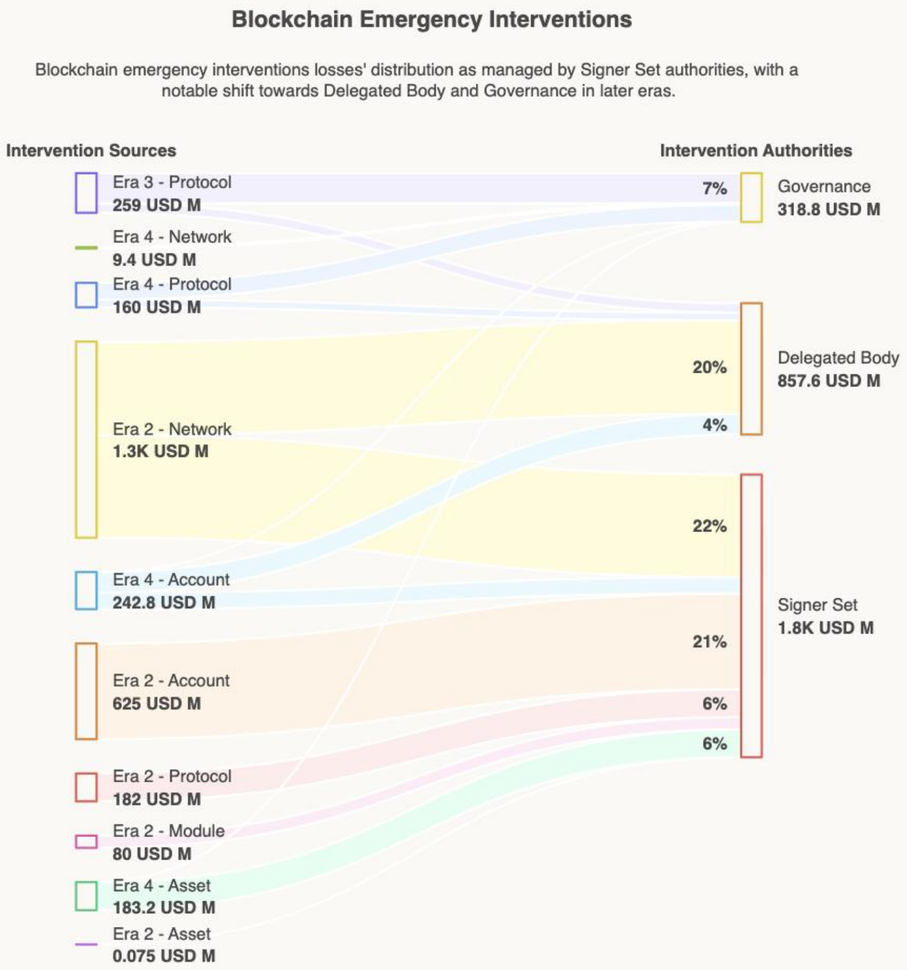
Modern interventions (Era 4)



– **Era 4 – Institutionalization (2024–2026):** Emergency capabilities transition into formalized, mathematically constrained engineering – Security Councils, SEAL911 war-rooms, scoped subDAOs, and verifiable credible layers.

AUTHORITY DISTRIBUTION

Who makes the decision?

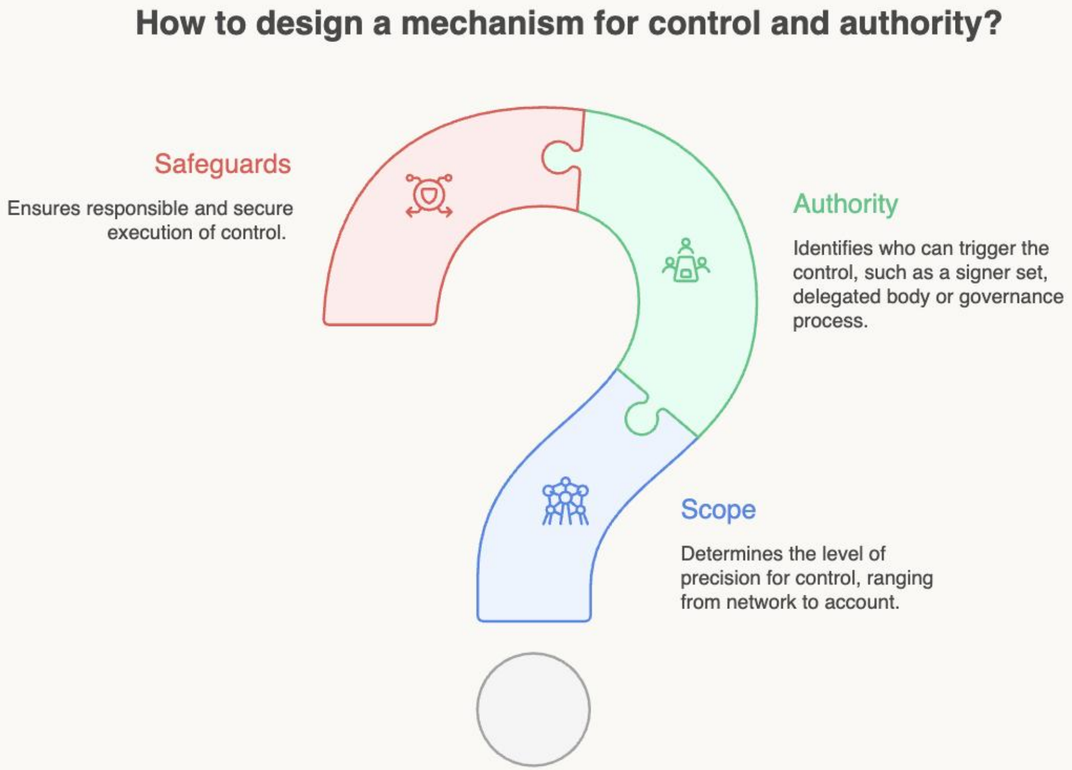


Super-hacks dominate the risk

Key insight: ~80% of cumulative losses are concentrated in a small number of incidents. In heavy-tailed systems, *one* governance failure can dominate years of safe operation.

DESIGN SPACE

Scope × Authority taxonomy



Scope (Precision) × Authority (Trigger Holder)

Reframes the "centralized vs decentralized" debate into mechanism design: what scope, triggered by whom, under what safeguards.

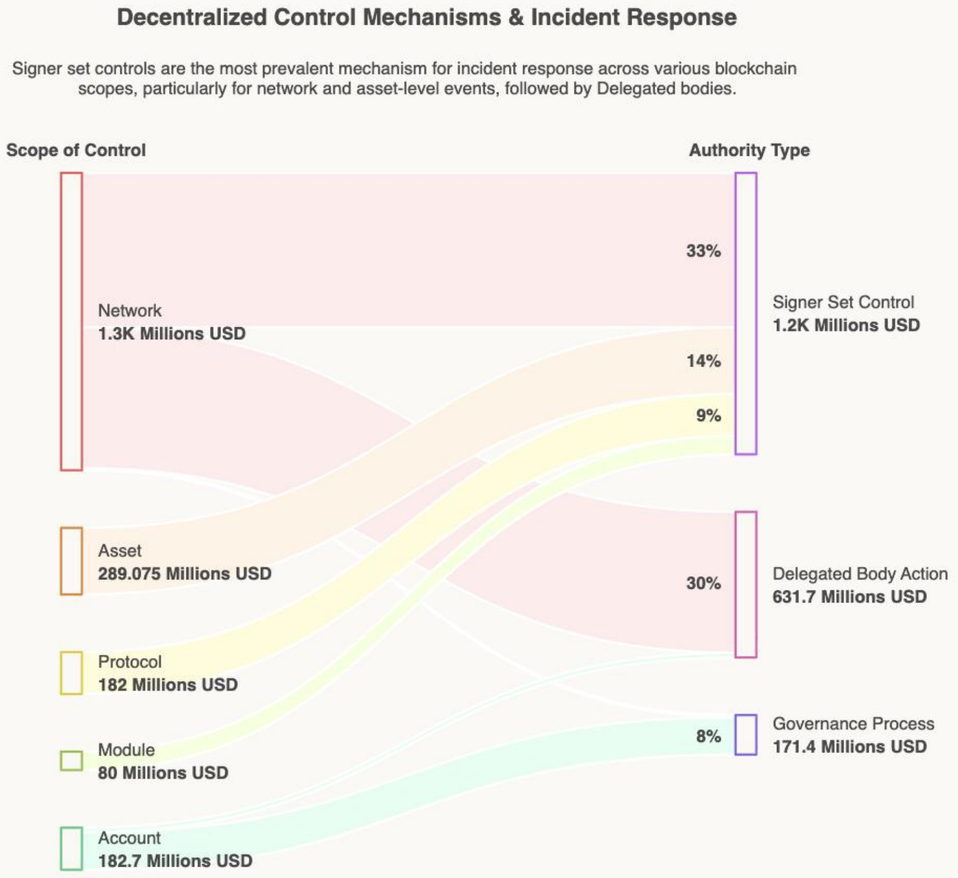
TAXONOMY EXAMPLES

Defining Scope and Authority

Scope / Authority

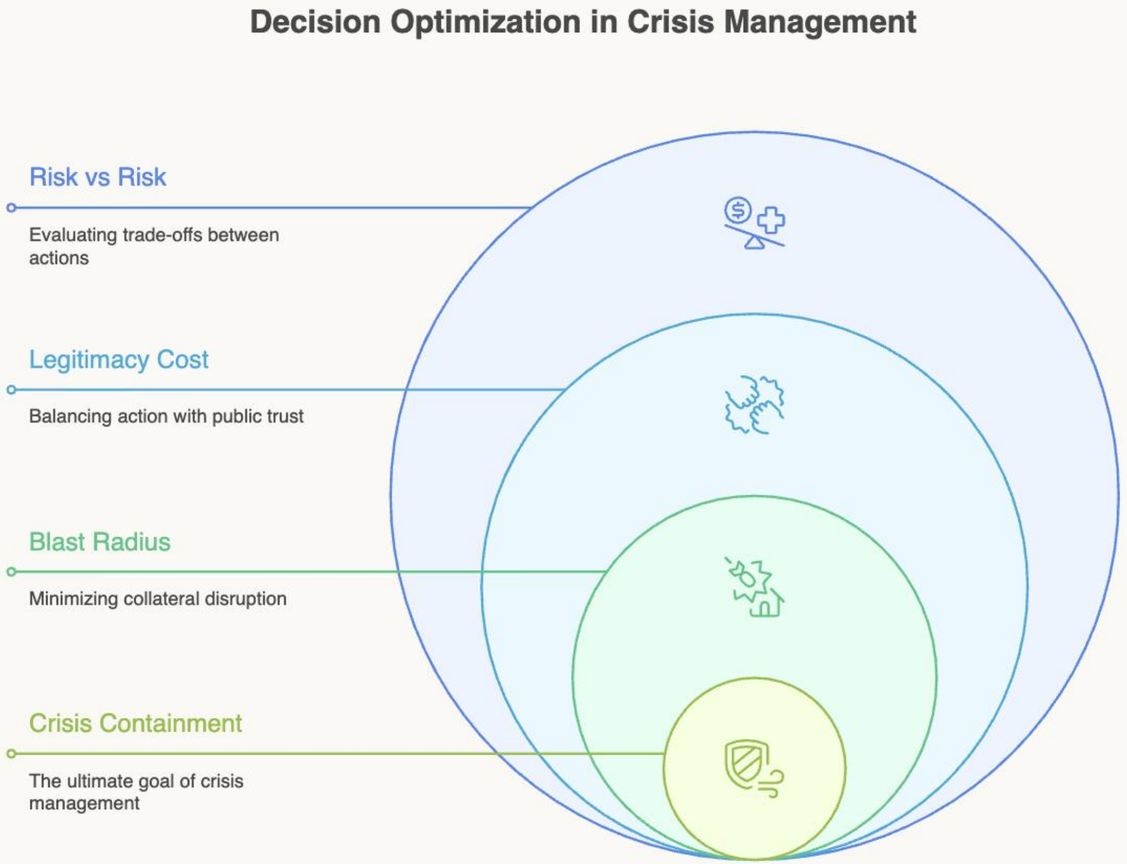
- Examples: Harmony Horizon (Jun 2022, $100M); BNB Chain halt (Oct 2022, $570M); Berachain halt (Nov 2025)
- Examples: Tether USDT freezes (PDVSA $182M); Circle USDC blocked addresses (Tornado Cash $75K); WLFI blacklist of Justin Sun ($107M)
- Examples: Balancer CSPv6 auto-pause (Nov 2025); Liqwid Kill Switch; Beanstalk shutdown (Apr 2022, $182M); Superfluid agreement halt (Feb 2022)
- Examples: Compound price oracle pauses (2021); FEI/Rari DAI borrow pause (Apr 2022, $80M); Elephant Money TRUNK minting pause (Apr 2022)
- Examples: Tether/Circle address blacklists; Sonic freezeAccount (Nov 2025); Ronin attacker freeze

Decentralized control in practice



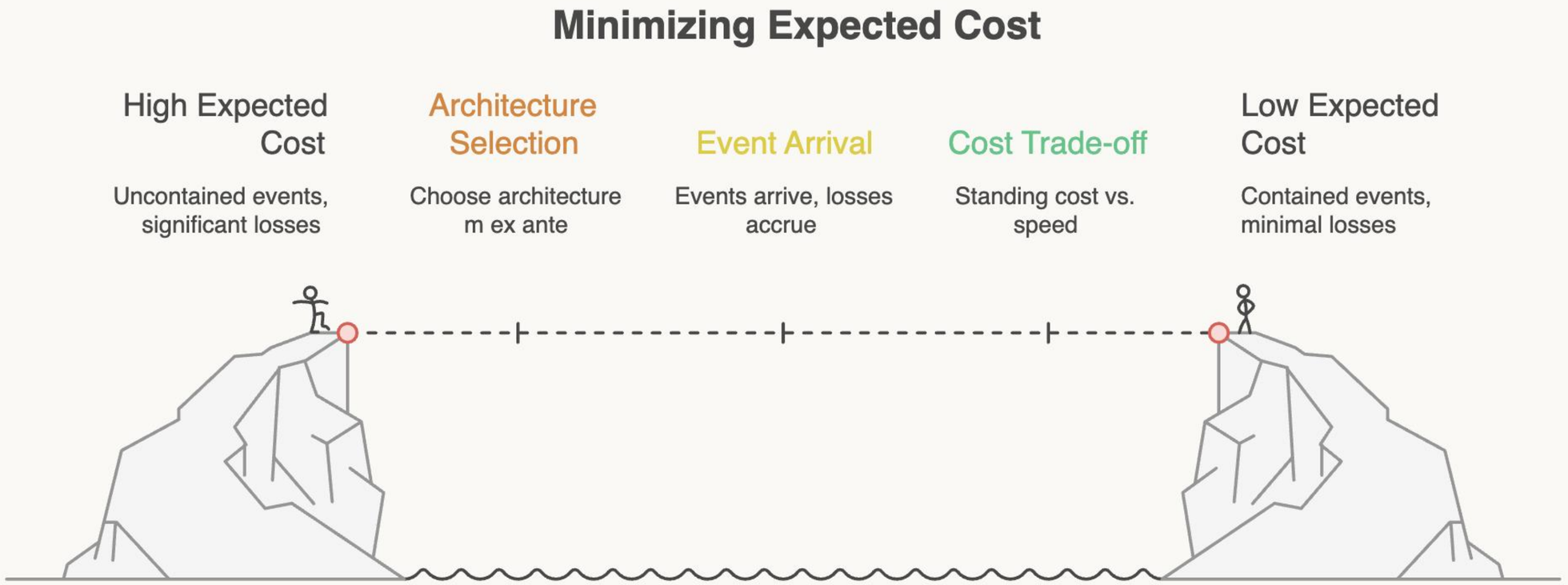
OBJECTIVE

What are we optimizing?



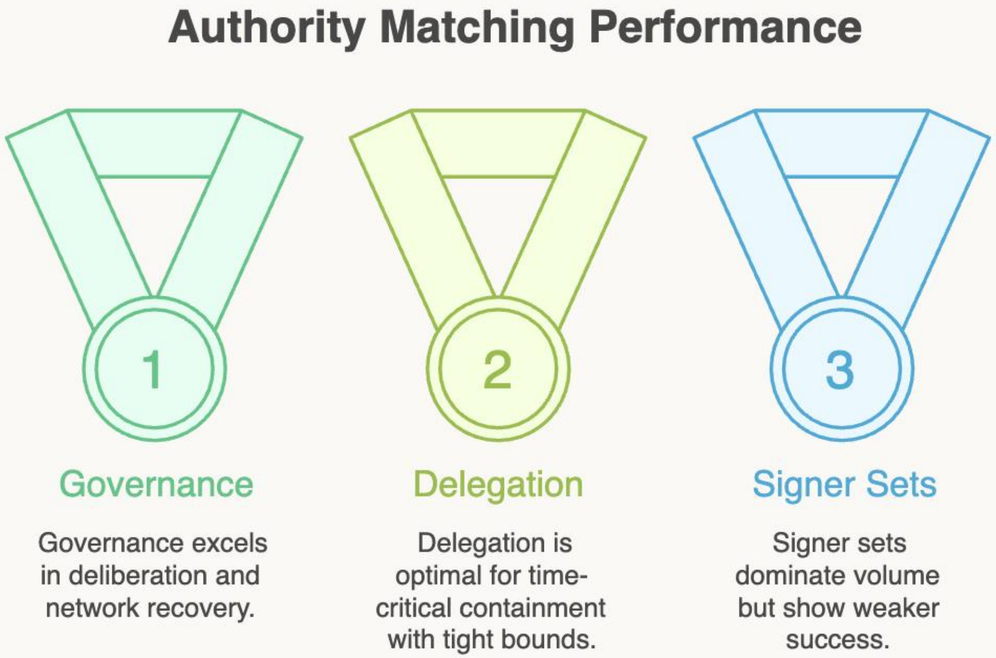
Risk vs. risk: Most real decisions aren't risk vs. safety — they're *action risk vs. inaction risk*, where the baseline is not neutral.

Expected cost framing (intuition)




```
ExpectedCost(m) = CentralizationCost(m) + Σ Pr[h] · ( Time(m) · DamageRate(h) + BlastRate(m) )
```

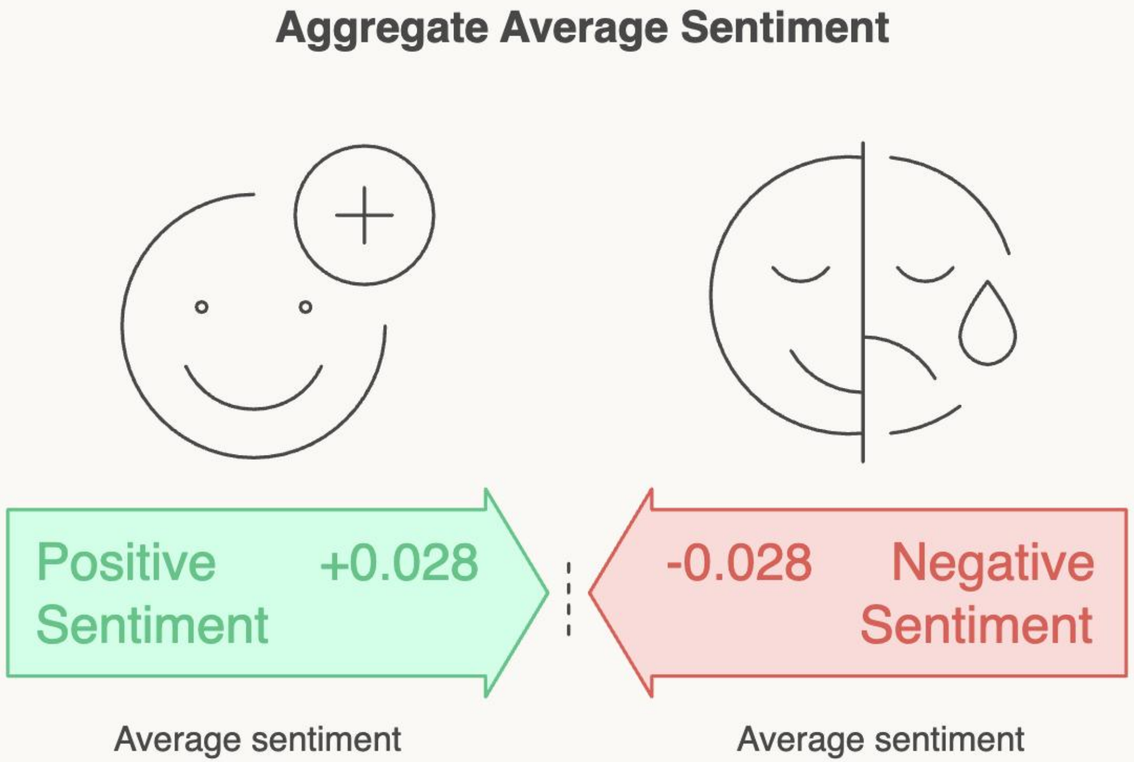
Scope–Authority matching



- **Signer Set (Oligarchy):** High speed (~30 min), low success (39%), high volume (71%).
- **Delegated (Representative):** Medium speed (60-90 min), medium success (48%).
- **Governance (Direct):** Low speed (days), high success (73%), low volume (11%).

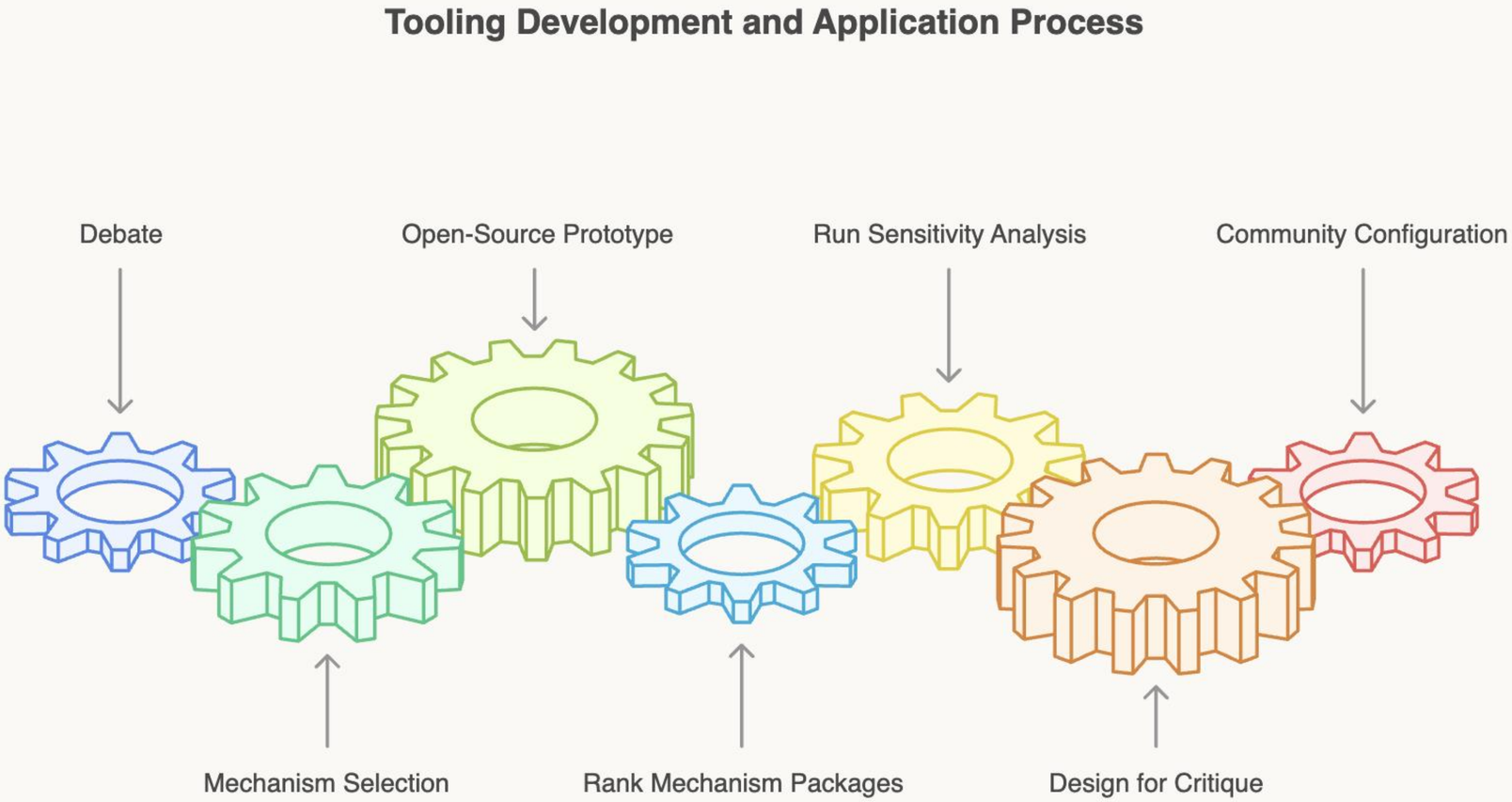
SENTIMENT

Legitimacy cost is not fixed

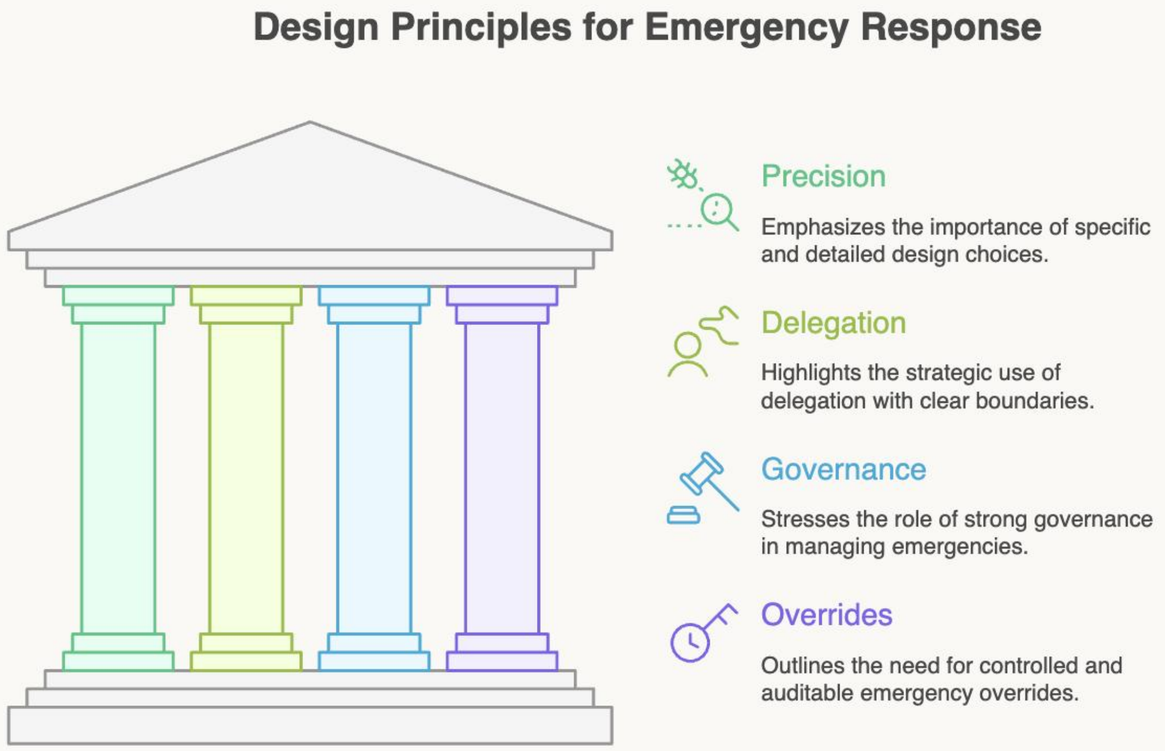


Empirical finding: Aggregate sentiment across 271 verified incident posts is slightly positive (+0.028), but highly variable. Positive sentiment *reduces* the effective centralization cost of an override mechanism.

From debate to mechanism selection

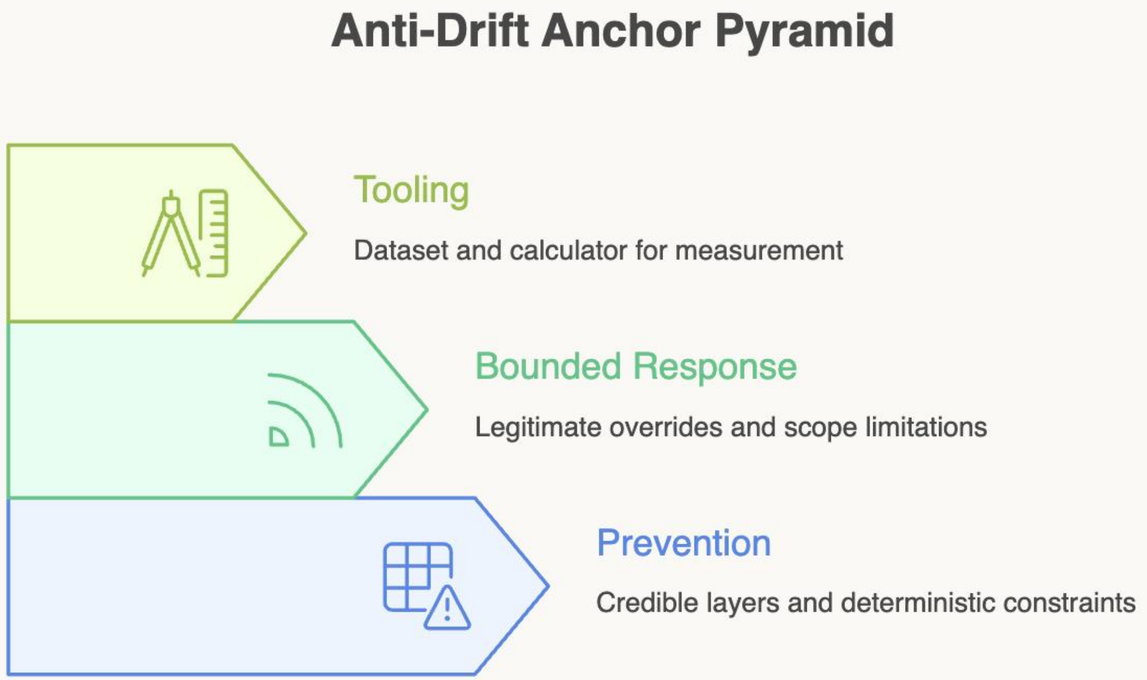


Actionable design takeaways



The Delegation Sweet Spot: Pure governance is too slow for containment. Signer sets impose too high a trust tax. Bounded delegated councils (Emergency subDAOs) occupy the empirical sweet spot.

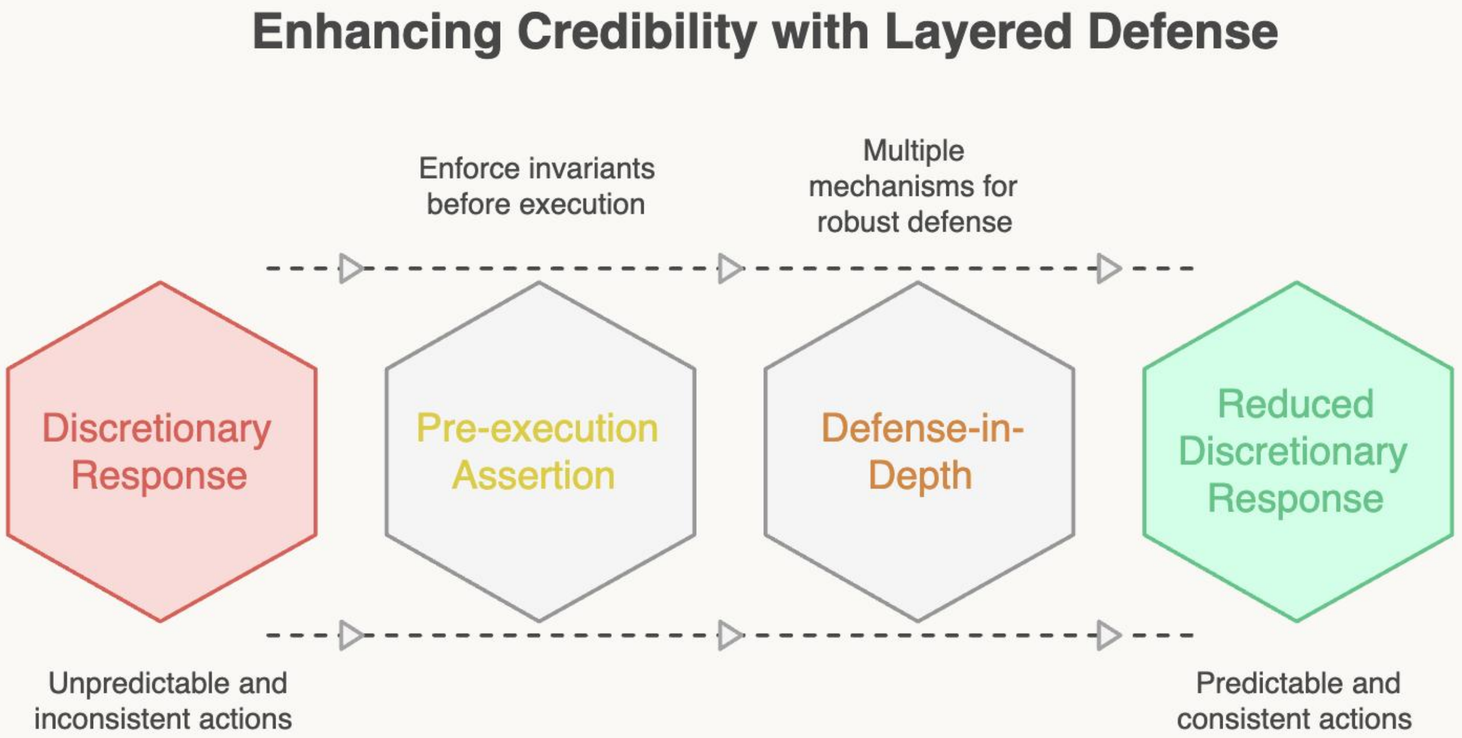
Layered stack: prevention, bounded response, tooling



The Goal

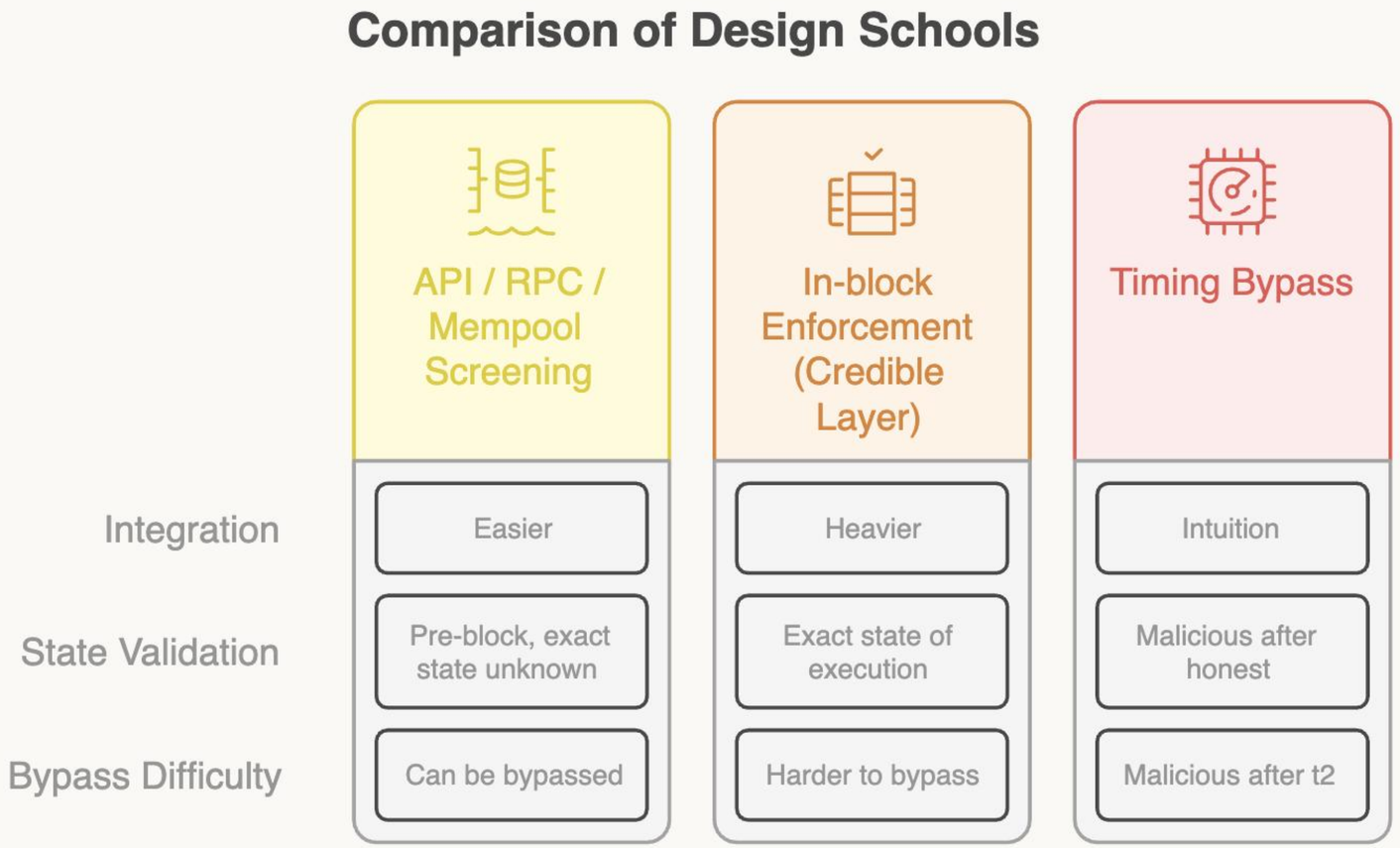
A layered stack prevents permanent damage from novel exploits while explicitly minimizing the shadow centralization of the response mechanisms themselves.

Where they fit (and what they don't solve)

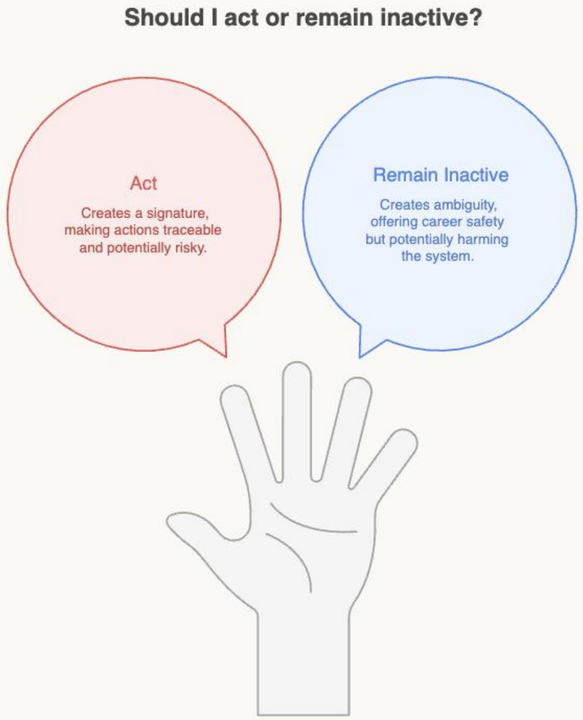


COMPARISON

Design schools in the market



"Do nothing" is an equilibrium



- **Acting** creates a signature – you're on record.
- **Inaction** creates ambiguity – plausible deniability.
- Ambiguity can be *career-safe* even when systemically harmful.

WALKTHROUGH

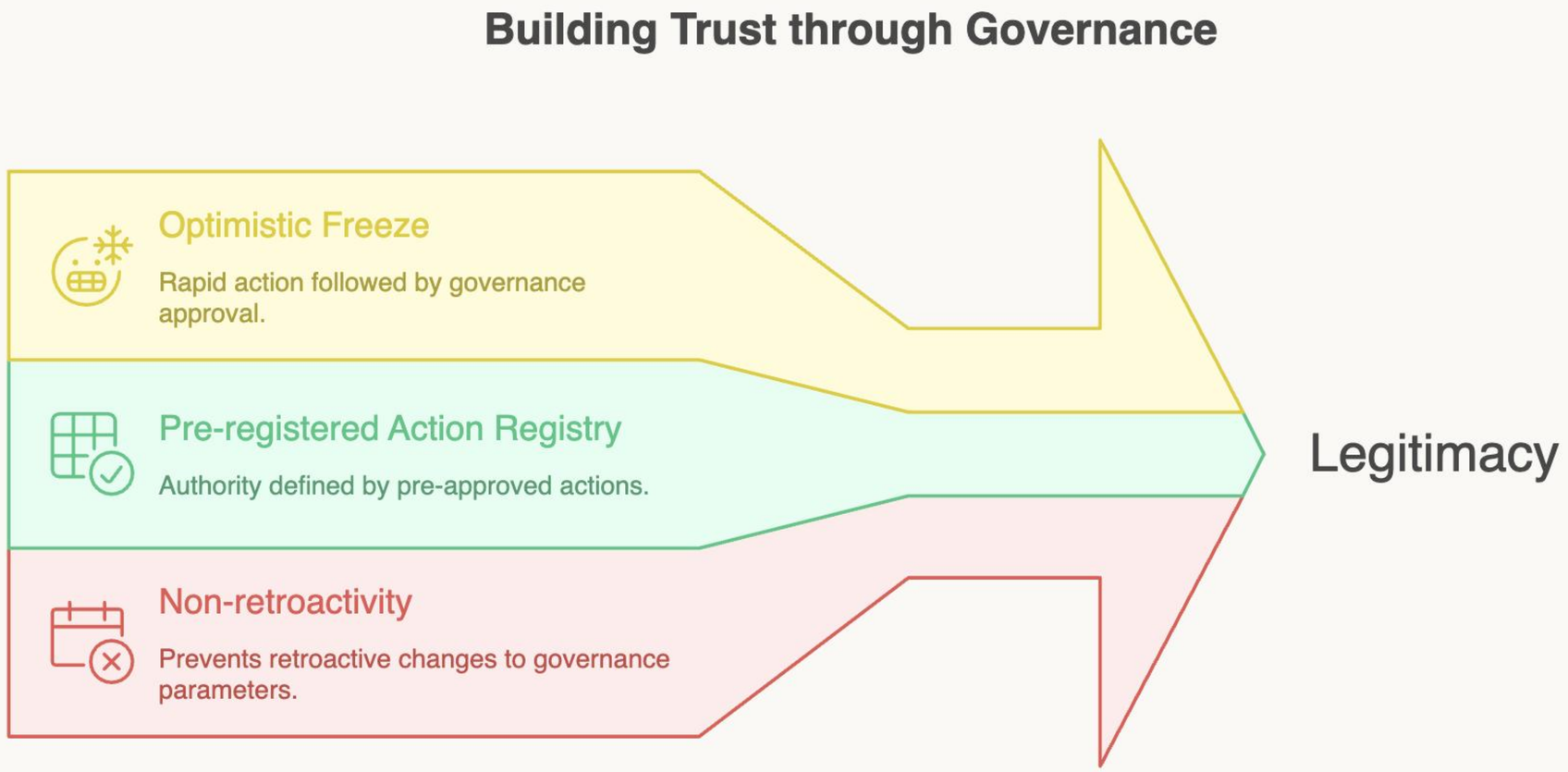
A single incident, mapped to the taxonomy

Scope vs. Authority Comparison

Scope / Authority	Signer Set	Delegated Body	Governance Process
Network	Key-triggered chain-wide restriction	Council-coordinated network action	Governance-led chain reconfiguration
Asset	Issuer/admin asset controls	Delegated asset committee	Governance changes asset rules
Protocol	Admin pause / shutdown	Security-council pause	DAO-administered emergency action
Module	Admin disables a feature	Delegated feature-specific pauses	Governance toggles module parameters
Account	Key-based targeted restriction	Delegated targeted remediation	Governance-authorized targeted action

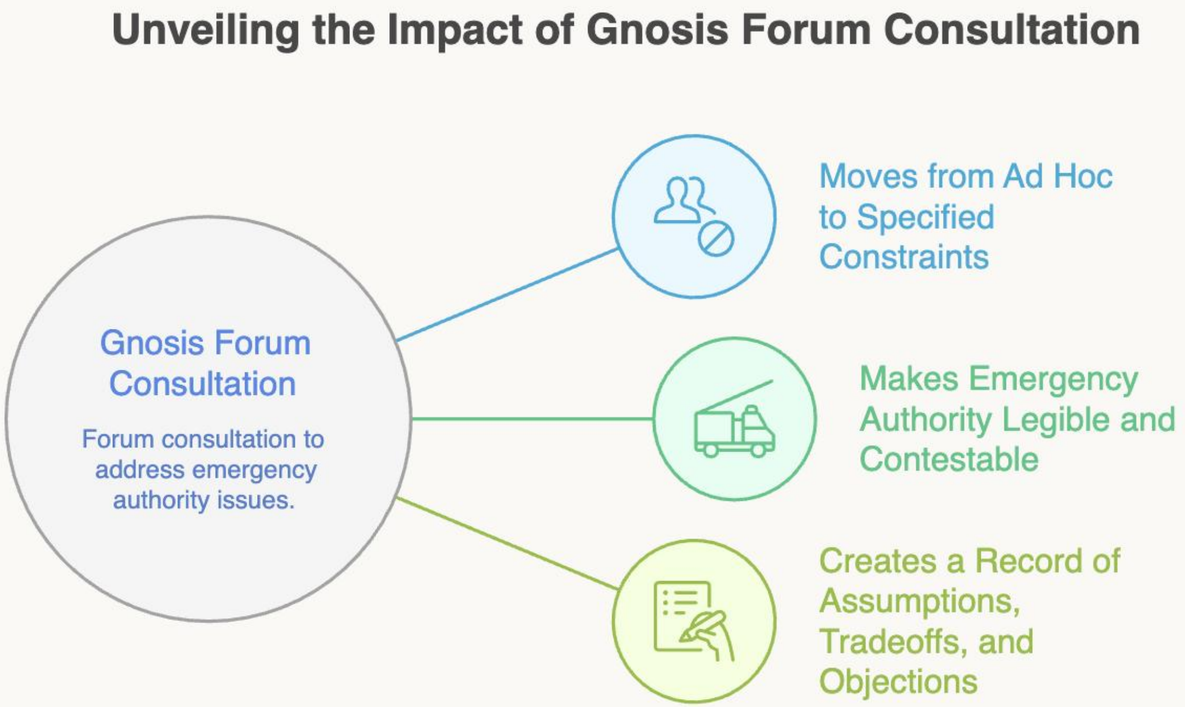
IMPLEMENTATION

Patterns (how to embed legitimacy)



CASE NOTE

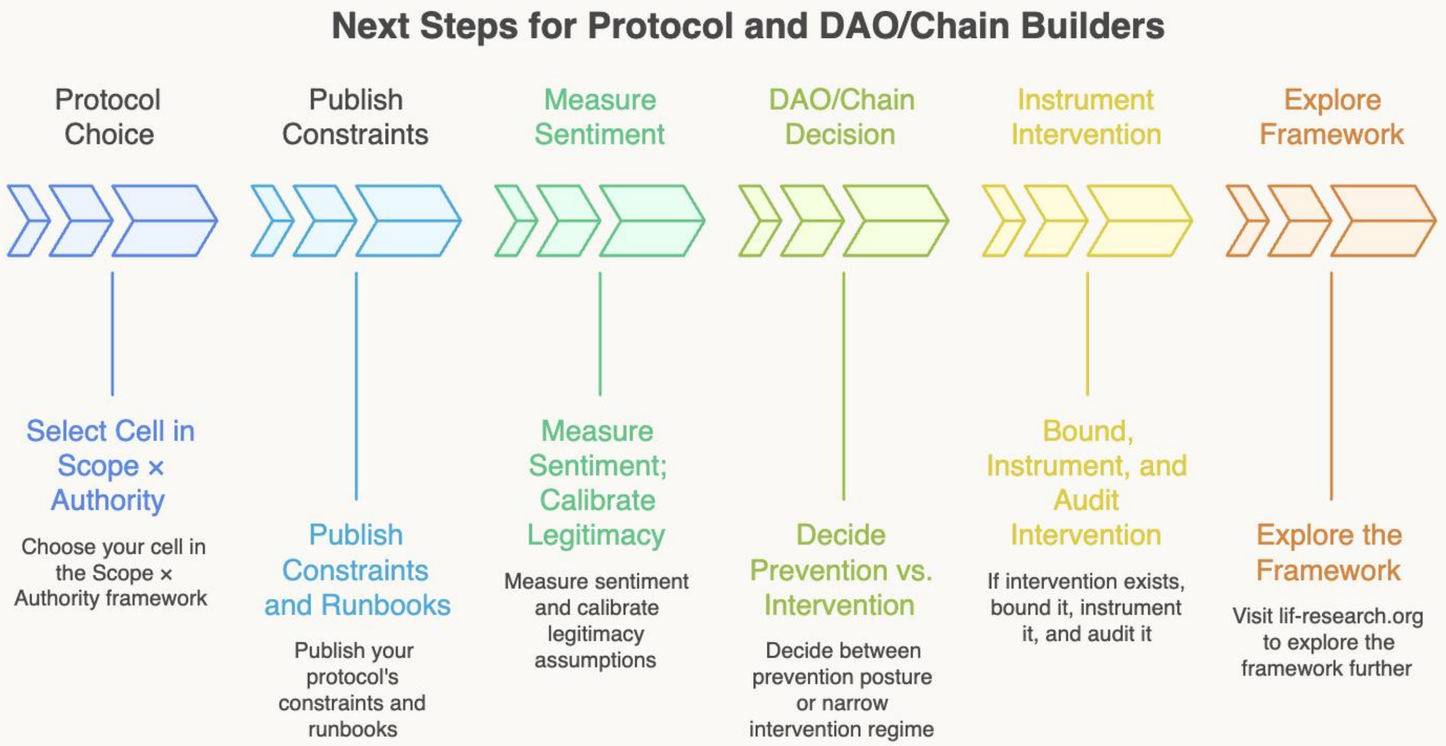
Gnosis: forum consultation



Read the forum consultation thread ↗

Questions?

What to do next



Explore the framework: lif-research.org ↓ PDF