Against Namespace Laundering

Flyxion

January 14, 2026

Abstract

This essay argues that the accelerating collapse of trust, meaning, and accountability on contemporary digital platforms is driven by a structural failure in identity architecture that can be described as *namespace laundering*. When names, reputational markers, and institutional signifiers are permitted to circulate independently of persistent, enforceable histories, platforms enter a high-entropy regime in which impersonation, metric manipulation, and recidivist abuse become not merely possible but economically and thermodynamically inevitable.

The central claim is that identity must be treated as infrastructure rather than representation. In the absence of injective and persistent identity binding, attributional entropy rises irreducibly, metrics decouple from latent qualities, and optimization pressure selects for imitation over substance. These failures are not remediable through improved moderation, artificial intelligence, or policy refinement, because they arise from the destruction of informational memory at the architectural level.

The essay develops this argument through a synthesis of information theory, platform economics, and systems dynamics, drawing on concepts such as Goodhart collapse, phase transitions, and hysteresis to explain why trust loss on large platforms is abrupt and often irreversible. It further argues that contemporary platforms systematically fail to address recidivism because their identity systems are explicitly designed to forget, aligning enforcement with revenue rather than accountability.

As a constructive alternative, the essay explores constraint-first design strategies, including cryptographic identity, Sybil resistance, and identity-conditioned media encoding, as mechanisms for restoring historical continuity without sacrificing pseudonymity. It concludes by suggesting that in environments where direct enforcement is structurally disincentivized, containment-oriented approaches—such as isolating adversarial actors within unproductive interaction spaces—may offer a pragmatic path toward harm reduction.

Ultimately, the essay advances a general principle: meaning cannot be optimized into existence once its structural substrate has been dissolved. It must be conserved by design.

1 Introduction

A recurring interaction on contemporary social platforms illustrates the structural problem this essay addresses with unusual clarity. A user receives a friend request from an account bearing the name of a well-known public figure, yet the profile lacks the signals traditionally associated with authenticity: no verified photograph, no visible history, no contextual grounding. The user hesitates, uncertain whether the request is legitimate. Shortly thereafter, a second request arrives, bearing the same name but now displaying a verification badge as its profile image. Rather than resolving the ambiguity, the badge itself becomes suspect. It is trivially reproducible, easily detached from its institutional meaning, and indistinguishable from a copied or synthetically generated artifact. The user is left without any reliable means of adjudicating identity.

This scenario is no longer exceptional. It reflects a systemic condition in which names, reputations, and institutional signifiers circulate without enforced attachment to the histories that once made them informative. The problem is not simply that impersonation occurs, but that the platforms hosting these interactions have eliminated their own capacity to distinguish authentic identity from counterfeit appearance. Under such conditions, trust does not degrade gradually; it collapses.

The same architectural failure manifests more broadly in the contemporary advertising ecosystem. Platforms increasingly permit any actor to purchase reach while claiming expertise, legitimacy, or institutional authority in domains where false claims carry material harm. Financial prediction services, medical and mental health advice, and professional credentials are routinely advertised under names that imply qualification but provide no verifiable continuity or accountability. Because identity is treated as a surface label rather than a binding structure, reputational language becomes a low-cost resource that can be copied, simulated, and redeployed without constraint.

This condition can be described as *namespace laundering*. In a coherent system, a name functions as a binding operator: it uniquely and persistently refers to a specific evolving history. Namespace laundering occurs when this binding is weakened or removed, allowing names and reputational markers to circulate independently of the actions that produced them. Once this separation occurs, attribution becomes unreliable, reputation ceases to accumulate, and metrics lose their referential grounding. What remains is an environment optimized for the appearance of legitimacy rather than its substance.

Crucially, this is not a failure of moderation, intelligence, or intent. It is a consequence of architectural choice. Contemporary platforms have prioritized scale, engagement, and advertising throughput, and in doing so have systematically relaxed the constraints required for identity coherence. The resulting systems treat identity as abundant, resettable, and non-rival. Under these conditions, the most rational strategy for adversarial actors is not to build trust, but to imitate it. Impersonation, metric manipulation, and recidivist abuse become structurally incentivized rather than aberrant.

The argument advanced in this essay is that these failures are not fixable within the incentive structures and data models of existing platforms. Once identity has been decoupled from persistent history, the system loses the informational memory required to recognize repeat behavior, accumulate consequence, or preserve meaning. Attempts to repair this condition through improved moderation or artificial intelligence operate downstream of the collapse and cannot restore the missing substrate.

Instead, the essay proposes that identity must be treated as infrastructure rather than representation. Trust, reputation, and accountability are not properties that can be optimized into existence; they are emergent properties of systems that enforce continuity, scarcity, and historical binding. Where these constraints are absent, optimization accelerates entropy. Where they are present, meaning can accumulate.

The sections that follow formalize this claim. First, the essay develops a structural account of identity as namespace and examines the thermodynamics of metric collapse under identity ambiguity. It then analyzes why contemporary platforms systematically fail to address recidivism and why this failure aligns with their economic incentives. Finally, it explores constraint-first alternatives, including cryptographic identity, Sybil resistance, and identity-conditioned media encoding, as well as containment-oriented strategies for adversarial actors in systems where direct enforcement is disincentivized.

This is not merely a critique of impersonation or fraud, it is an argument that systems which refuse to remember who acts cannot govern, cannot learn, and cannot sustain meaning over time.

2 Formal Framework: Identity, Namespaces, and Attribution

To analyze namespace laundering with sufficient rigor, it is necessary to formalize what is meant by identity, naming, and attribution in digital systems. Much of the confusion surrounding platform trust arises from the conflation of representational symbols with structural bindings. This section therefore introduces a minimal formal vocabulary for distinguishing these layers.

A *namespace* is understood here as a system that maps identifiers to referents across time. The critical property of a namespace is not expressiveness but injectivity: distinct identifiers must map to distinct referents, and this mapping must persist across events. When this condition holds, actions performed under an identifier accumulate into a coherent history. When it fails, histories fragment and meaning dissipates.

Digital platforms routinely violate this condition by allowing identifiers to be reassigned, duplicated, or abandoned without cost. Names become cosmetic rather than infrastructural. Verification badges, profile pictures, and business labels function as surface signals rather than guarantees of continuity. Once this occurs, the mapping between identifier and agent is no longer injective, and the system loses the ability to bind actions to histories.

This failure can be expressed in information-theoretic terms. Let A denote the true agent producing actions and I the observed identifier under which those actions appear. In a coherent namespace, the conditional entropy $H(A \mid I)$ is zero: observing the identifier uniquely determines the agent. Under namespace laundering, this entropy becomes strictly positive. The system itself introduces irreducible uncertainty about who is acting, independent of any observer's intelligence or intent (Shannon 1948; Cover and Thomas 2006).

This distinction is crucial. The resulting ambiguity is not epistemic, meaning it cannot be resolved by better inference, larger models, or more data. It is architectural. The system has destroyed information at the moment of creation by permitting ambiguous attribution. No downstream process can

recover what was never conserved.

3 Goodhart Collapse as a Consequence of Identity Failure

The collapse of platform metrics under optimization pressure is often described using Goodhart's Law: when a measure becomes a target, it ceases to be a good measure (Goodhart 1975; Campbell 1979). While accurate, this formulation is incomplete. It describes the symptom but not the cause. Namespace laundering supplies the missing structural explanation.

Metrics function only insofar as they remain anchored to latent qualities. A follower count, for example, is meaningful only if it aggregates genuine attention toward a persistent agent. When identity is coherent, the metric can serve as a proxy for accumulated trust or relevance. When identity is ambiguous, the proxy decouples from the underlying quantity it was meant to represent.

Under these conditions, optimization pressure does not merely distort metrics; it actively selects against substance. Rational agents shift effort away from improving latent quality and toward manipulating the metric directly. Engagement rings, click farms, impersonation campaigns, and synthetic audiences become dominant strategies because the cost of simulation is lower than the cost of authenticity (Strathern 1997; Muller 2018).

This dynamic is particularly visible in advertising systems. When platforms allow advertisers to claim arbitrary identities without proof of qualification or continuity, the advertising market becomes saturated with performative authority. Claims of financial expertise, medical competence, or therapeutic insight proliferate precisely because they are not constrained by credential verification or reputational persistence. The platform's ranking systems, optimized for engagement and revenue, amplify these claims regardless of their truth value.

The result is not a gradual erosion of quality but a phase transition. Once the cost of laundering identity falls below the cost of maintaining reputation, the system flips into a high-entropy equilibrium dominated by imitation. At that point, attempts to "improve" the metric accelerate collapse rather than reversing it.

4 Phase Transitions, Hysteresis, and the Irreversibility of Trust Loss

A defining feature of namespace collapse is its nonlinearity. Platforms do not lose trust smoothly or proportionally. Instead, they appear stable for long periods and then suddenly become unusable. This behavior is characteristic of phase transitions in complex systems.

Within the RSVP framework, identity coherence functions as a scalar field that shapes the flow of activity. When coherence is high, interaction vectors follow gradients of accumulated meaning, allowing reputation to concentrate and stabilize. When coherence weakens past a critical threshold, these gradients flatten. Activity remains energetic but becomes directionless, producing churn rather than accumulation.

Once this transition occurs, recovery is asymmetric. The effort required to rebuild trust vastly exceeds the effort originally required to maintain it. This phenomenon, known as hysteresis, explains

why platforms that attempt to restore earlier norms through incremental policy changes consistently fail. The informational structures that once supported meaning have already dissipated.

Empirically, this is observed in the failure of post hoc verification schemes, retroactive moderation, and symbolic enforcement gestures. Verification badges lose value once they can be trivially replicated. Content takedowns lose deterrent effect once offenders can immediately reappear under new identities. The system has crossed a threshold beyond which previous control parameters no longer apply.

The implication is severe but unavoidable: some platforms may be structurally irrecoverable. When a system has optimized itself into identity incoherence, no amount of moderation can reconstruct the lost history. At best, a parallel system must be built alongside it, capable of accepting trust transfers from the old while enforcing stronger constraints from inception.

5 Why Platform Incentives Preclude Structural Repair

It is tempting to attribute the persistence of namespace laundering to negligence or regulatory lag. This interpretation is inadequate. The continued existence of these failures reflects the alignment of platform incentives with identity fragmentation.

Large platforms monetize activity volume rather than participant integrity. Advertising revenue scales with impressions, clicks, and targeting efficiency, not with trust preservation. Identity coherence introduces friction, liability, and exclusion. Namespace laundering, by contrast, maximizes participation and reduces onboarding costs. From a narrow economic perspective, it is optimal.

This incentive structure explains why platforms address abuse at the level of content rather than actors. Removing individual posts or accounts satisfies external pressure while preserving the underlying revenue stream. Addressing recidivism would require binding actions across time, which would imply durable exclusion and reduced throughput. The system is therefore designed to forget.

Shoshana Zuboff's analysis of surveillance capitalism captures this dynamic at a macroeconomic level, describing how platforms externalize social harm while internalizing behavioral surplus (Zuboff 2019). Varian's account of network-age market structure further explains why dominant platforms can tolerate degradation without immediate competitive penalty (Varian 2019). In such an environment, trust collapse is not corrected by market forces. It is monetized.

This structural alignment between profit and forgetting renders in-platform reform implausible. The problem is not that platforms cannot fix namespace laundering; it is that doing so would undermine their core business model.

6 Toward Constraint-Based Containment

If direct enforcement is economically disincentivized and technically insufficient, an alternative strategy suggests itself: containment rather than correction. Instead of attempting to eliminate deceptive actors, systems can deprive them of external effect.

In this model, accounts exhibiting high-probability adversarial behavior are not banned in the traditional sense. Instead, they are routed into isolated interaction environments that simulate engagement without connecting to real users or markets. From the actor's perspective, the system remains responsive. From the system's perspective, harm is contained.

This approach reframes moderation as an adversarial systems problem rather than a moral one. It accepts that certain behaviors are persistent under given incentive structures and seeks to neutralize their impact rather than eradicate them. Similar strategies have long been employed in computer security, where honeypots and sandboxed environments absorb malicious activity without exposing production systems (Provos 2003; Biggio and Roli 2018).

While ethically nontrivial, this strategy has two advantages over traditional enforcement. First, it aligns with platform incentives by preserving activity metrics. Second, it restores external coherence without requiring perfect attribution or punitive escalation. The system does not need to know who an actor "really is"; it only needs to prevent identity-laundered behavior from influencing shared reality.

The deeper lesson is that once namespace laundering is entrenched, governance must operate at the level of system dynamics rather than individual intent. Constraint replaces judgment. Architecture replaces moderation.

7 Metric Collapse and the Thermodynamics of Optimization

Once identity coherence is weakened, the failure of metrics is not a secondary effect but an immediate structural consequence. Contemporary discussions often invoke Goodhart's Law to describe this phenomenon, observing that when a measure becomes a target it ceases to be a reliable measure. While descriptively accurate, this formulation understates the depth of the problem. In systems affected by namespace laundering, metric collapse is not merely behavioral but thermodynamic. It arises from the loss of an invariant that once anchored measurement to substance.

In a coherent system, metrics function as lossy compressions of underlying qualities. A follower count approximates influence, a citation count approximates scholarly impact, and a reputation score approximates trustworthiness. These approximations are imperfect, but they remain informative so long as they are stably coupled to a persistent subject. Identity coherence provides this coupling. When a metric is attached to a name that uniquely and continuously refers to a single evolving history, changes in the metric reflect accumulated action over time.

Namespace laundering severs this coupling. When identifiers can be duplicated, reset, or abandoned at negligible cost, metrics detach from the histories they purport to summarize. The same numeric signal can now be produced by qualitatively distinct processes: long-term contribution, short-term manipulation, or outright impersonation. The metric no longer compresses reality; it averages over incompatible generators. At this point, its informational content collapses.

Optimization pressure accelerates this collapse. When a system explicitly rewards metric improvement, agents are incentivized to identify the cheapest causal pathway to metric change. In a coherent identity regime, this pathway is constrained by persistence: manipulation risks long-term

reputational damage, and success accumulates slowly. In a laundered namespace, however, identity reset removes long-term cost. The optimal strategy shifts from producing value to producing the appearance of value. Engagement farming, astroturfing, and ritualized interaction are not pathological behaviors; they are locally optimal responses to the system's incentive landscape.

This shift marks a phase transition rather than a gradual degradation. Below a critical threshold of identity dispersion, metrics remain weakly informative despite noise. Above it, the signal-to-noise ratio collapses abruptly. Small increases in identity ambiguity produce disproportionate increases in metric manipulability. The system bifurcates into a regime where optimization actively selects against the behaviors the metrics were designed to encourage.

Advertising saturation provides a concrete illustration of this dynamic. As platforms increase the density of ads within user feeds, they simultaneously weaken the informational environment in which those ads are interpreted. When advertisers can claim expertise or legitimacy without binding to verifiable history, the metric governing ad performance no longer measures relevance or trust. It measures only attention capture. Under such conditions, deceptive or sensational claims outperform accurate ones, not because users prefer deception, but because the system's metrics reward engagement divorced from consequence.

The destruction of long-term user curation further amplifies this effect. Users invest years constructing semantic filters through follows, blocks, and preferences, effectively shaping a personalized informational topology. Advertising insertion disregards this topology, flooding the feed with content optimized for generic engagement rather than contextual coherence. The metric success of such content reflects the platform's objective function, not the user's informational needs. Over time, the feed ceases to be an expression of accumulated preference and becomes a surface for continuous extraction.

Importantly, metric collapse under namespace laundering is self-reinforcing. As metrics lose meaning, trust in the system erodes. As trust erodes, users rely more heavily on superficial signals. As superficial signals become more influential, they are further targeted by optimization. The system enters a feedback loop in which every attempt to optimize accelerates entropy production. At no point does the system naturally recover, because the conditions required for recovery—stable identity and historical memory—have already been dissolved.

This analysis clarifies why appeals to better ranking algorithms or more nuanced engagement metrics consistently fail. No metric, however sophisticated, can recover meaning once its referent has been fragmented. Optimization cannot substitute for constraint. In the absence of identity coherence, measurement ceases to be an epistemic act and becomes a performative one.

The next section examines why this collapse cannot be reversed through moderation or enforcement within existing platforms, and why recidivism emerges as a structural inevitability rather than a policy failure.

8 Platform Amnesia, Recidivism, and the Limits of Enforcement

The collapse of metrics described in the previous section is often attributed, in public discourse, to insufficient moderation or inadequate enforcement. This diagnosis is appealing because it suggests a remedial path: more reviewers, better classifiers, stricter rules. However, within systems affected by namespace laundering, enforcement failures are not contingent or temporary. They are structurally guaranteed. The inability to address recidivism is not an implementation flaw but an inevitable consequence of platform amnesia.

Recidivism presupposes memory. To identify a repeat offender, a system must be able to bind present actions to a persistent historical subject. Contemporary platforms do not possess such a subject. Identity is fragmented into disposable identifiers that can be abandoned and reconstituted at negligible cost. When an account is removed, the platform treats the event as terminal rather than cumulative. The history associated with that identifier is deleted rather than integrated into a broader model of agent behavior. From the system's internal perspective, the offending entity has ceased to exist.

This design produces a fundamental asymmetry. Legitimate users accumulate years of history, preferences, and social structure under persistent identifiers, while adversarial actors enjoy effective historical reset. The more aggressively a platform enforces content-level rules, the stronger the incentive becomes to externalize that cost by cycling identities. Enforcement thus increases, rather than decreases, identity dispersion. What appears externally as repeated failure is internally consistent behavior in a system optimized to forget.

Crucially, current platforms do not merely fail to punish recidivism; they render it formally undefined. Because identity is not treated as a conserved variable, there exists no internal representation corresponding to "the same actor over time." Heuristics such as IP correlation, device fingerprinting, or behavioral similarity are deliberately weak, both for legal reasons and because strengthening them would contradict the platform's public commitments to anonymity, accessibility, and growth. These heuristics therefore function only as temporary friction, never as binding constraint.

This absence of persistent attribution explains why moderation remains shallow even as technical capacity increases. Platforms remove posts, pages, or advertisements, but they do not accumulate negative evidence against agents. Each enforcement action resets the state rather than updating it. Information that could reduce uncertainty about future behavior is destroyed at the moment it is observed. From an information-theoretic perspective, the system operates as a memoryless channel, incapable of learning from experience.

The economic incentives reinforce this amnesia. Many of the most harmful behaviors—impersonation, scam advertising, synthetic expertise—are also among the most profitable. They generate impressions, clicks, and transactions regardless of their legitimacy. Penalizing repeat offenders would require binding these behaviors across identifiers, which would in turn require acknowledging continuity of agency. Such acknowledgment would impose obligation, escalation, and exclusion, directly threatening revenue streams predicated on frictionless participation.

As a result, platforms converge on a mode of governance that is reactive rather than accumulative.

Enforcement actions are episodic, local, and reversible. They are designed to manage public perception and regulatory risk, not to preserve system coherence. The platform becomes a high-throughput mechanism for laundering behavior, in which the same deceptive patterns recur endlessly under fresh names, faces, and brands.

This structural amnesia renders algorithmic solutions ineffective by construction. Machine learning systems excel at pattern recognition given stable labels. In a laundered namespace, labels do not persist. The target variable itself is unstable. No increase in model capacity can compensate for the absence of a conserved identity substrate. The problem is not that the system cannot see clearly; it is that there is nothing stable to see.

The persistence of recidivism under these conditions should therefore not be interpreted as institutional negligence or moral failure, but as the natural equilibrium of systems that refuse to bind actions to histories. Where identity is optional, history is irrelevant. Where history is irrelevant, accountability cannot exist. Enforcement without memory is indistinguishable from erasure.

The following section examines why this amnesiac equilibrium is not merely stable but difficult to escape, introducing the concepts of phase transition and hysteresis to explain why trust collapse is abrupt and why recovery, once lost, requires forces far greater than those that originally sustained coherence.

9 Phase Transitions, Hysteresis, and the Irreversibility of Trust Collapse

The preceding section established that platforms affected by namespace laundering are structurally incapable of learning from repeated abuse. This alone would be sufficient to explain long-term degradation. However, it does not yet account for a more striking empirical feature of platform failure: trust does not erode gradually. Instead, platforms often appear stable for extended periods before undergoing abrupt, catastrophic collapse. This behavior is best understood not through linear decay models, but through the language of phase transitions and hysteresis.

In systems governed by identity coherence, trust functions as a macroscopic order parameter. While individual interactions may fluctuate, the overall structure remains stable so long as identity binding is sufficiently strong to anchor attribution. Within this regime, reputational information accumulates, and localized failures are damped rather than amplified. The system exhibits resilience: perturbations decay, and coherence is preserved.

Namespace laundering destabilizes this equilibrium by increasing identity dispersion. As the number of apparent identities diverges from the number of underlying agents, attributional entropy rises. Initially, this increase may appear tolerable. Platforms continue to function, metrics retain partial meaning, and users compensate through informal heuristics and social intuition. However, these compensatory mechanisms mask an underlying structural weakening. The system approaches a critical threshold without obvious surface indicators.

Once identity dispersion exceeds this threshold, the system undergoes a qualitative transformation. Attribution ceases to be reliable at scale, reputational signals lose predictive power, and optimization pressure shifts decisively toward imitation and manipulation. This transition is abrupt because

the mechanisms that previously stabilized trust depend on the very coherence that is being eroded. When that coherence collapses, stabilizing feedback loops invert into destabilizing ones. Trust does not slowly diminish; it bifurcates.

This behavior is characteristic of phase transitions in complex systems. Below the critical point, order is maintained by collective alignment. Above it, disorder becomes the dominant equilibrium. Importantly, the transition point is not determined by any single policy change or technical failure. It emerges from the cumulative effect of identity ambiguity under sustained optimization pressure. Platforms often cross this boundary inadvertently, mistaking short-term growth for long-term stability.

The presence of hysteresis further explains why trust collapse is so difficult to reverse. In systems exhibiting hysteresis, the path to collapse is not symmetric with the path to recovery. The forces required to maintain coherence are significantly weaker than those required to restore it once lost. When a platform allows its identity namespace to fragment, it flattens the informational landscape in which trust once accumulated. The basins that once stabilized reputation disappear.

Restoring trust in such a system is not a matter of reversing recent changes. It requires reconstructing an entire substrate of historical binding, often in the presence of actors who have adapted to exploitation as the dominant strategy. Even aggressive enforcement measures struggle to regain traction, because the system no longer possesses the memory required to differentiate restoration from further disruption. Attempts to reimpose order encounter resistance not only from malicious actors, but from the platform's own accumulated entropy.

This asymmetry explains a common pattern in platform governance. Early, lightly enforced identity systems can remain functional for years. Once coherence collapses, however, even drastic interventions produce limited improvement. Users perceive moderation as inconsistent or arbitrary, trust continues to erode, and legitimate participation declines. The platform enters a high-entropy regime in which activity persists but meaning dissipates.

The critical implication is that trust is not linearly recoverable. It cannot be restored through incremental policy adjustment or reactive enforcement once the system has crossed the threshold into identity incoherence. Any serious attempt at recovery must operate at the same architectural level as the original failure. It must reintroduce binding constraints strong enough to recreate stable historical trajectories.

This observation reframes platform decline as a problem of irreversibility. Decisions to weaken identity constraints may appear reversible at the level of policy, but they are not reversible at the level of system dynamics. Once namespace laundering becomes endemic, the system's future state space is permanently altered. The cost of recovery grows superlinearly with delay.

The next section turns from diagnosis to construction. It examines how identity can be reintroduced as infrastructure through cryptographic binding and Sybil resistance, and why these mechanisms must operate at the level of the operating system and content pipeline rather than as optional platform features.

10 Cryptographic Identity as Infrastructural Binding

If namespace laundering is the failure mode of contemporary platforms, then cryptographic identity represents the minimal architectural response. Its importance does not lie in novelty or security theater, but in the reintroduction of binding at the level where modern systems have deliberately removed it. Cryptographic identity is not a social feature; it is an infrastructural primitive that restores the possibility of historical continuity.

At its most basic level, cryptographic identity replaces declarative naming with provable authorship. An identity is no longer asserted through a mutable label, profile, or badge, but instantiated through possession of a private key capable of authorizing actions. The corresponding public key serves as a stable referent through which actions can be verified, ordered, and accumulated. Continuity is enforced not by trust in the platform, but by mathematical constraint.

This shift has profound consequences. When actions are cryptographically bound to a persistent key, attribution ceases to be interpretive. The system no longer asks whether an action plausibly belongs to an identity; it verifies that it does. Impersonation, in the strict sense, becomes impossible. A malicious actor may still deceive, but they cannot convincingly inhabit another identity's historical trajectory without control of its cryptographic material.

However, cryptographic binding alone does not resolve namespace laundering. While it enforces continuity for a single identity, it does not limit identity proliferation. A system that allows unlimited key generation merely formalizes ambiguity rather than eliminating it. The problem shifts from impersonation to multiplicity. This is the Sybil problem re-emerging at a lower layer.

The relevance of cryptographic identity within this essay is therefore not as a complete solution, but as a necessary substrate upon which further constraints can operate. Cryptography restores the possibility of persistence, but not scarcity. Without scarcity, reputation remains unstable. An actor who can abandon a key at negligible cost can abandon history just as easily as they abandon a username.

This distinction clarifies a common misconception in platform design. Identity is often treated as binary: either verified or anonymous, either real-name or pseudonymous. Cryptographic identity reveals that the crucial axis is neither disclosure nor realism, but continuity. A persistent pseudonym supported by cryptographic binding is vastly more coherent than a real-name account that can be duplicated, reset, or counterfeited.

From the perspective of system dynamics, cryptographic identity transforms identity from a surface attribute into a state variable. Actions accumulate. Histories become irreversible. Time begins to matter again. This is precisely what namespace laundering erases.

Importantly, cryptographic identity also relocates authority. In conventional platforms, the platform operator serves as the final arbiter of identity, verification, and enforcement. This centralization is both politically contentious and technically brittle. Cryptographic binding allows identity coherence to be enforced independently of platform discretion. Verification becomes local, mechanical, and composable across systems.

Yet this same property explains why contemporary platforms have avoided such architectures.

Cryptographic identity constrains not only malicious actors but the platform itself. It limits the ability to selectively forget, to quietly reset state, or to privilege engagement over continuity. Once actions are bound to keys, the platform inherits memory whether it desires it or not.

In this sense, cryptographic identity is incompatible with business models predicated on amnesia. It introduces a form of conservation law into systems designed for throughput. Where platforms profit from disposable participation, cryptographic identity imposes obligation. Where platforms benefit from ambiguity, cryptographic identity enforces distinction.

This tension explains why cryptographic identity has largely been relegated to niche systems, financial protocols, and security-critical infrastructure. Its implications are not merely technical but economic and political. To adopt it seriously would require platforms to acknowledge that identity is not content, not preference, and not branding, but structure.

The following section extends this analysis by addressing the remaining failure mode: multiplicity. It examines Sybil resistance as the mechanism by which identity acquires scarcity, and why scarcity is not a social inconvenience but an informational necessity.

11 Sybil Resistance and the Economics of Scarcity

Cryptographic identity restores continuity, but continuity alone is insufficient to prevent namespace laundering. A system in which identities are cheap to instantiate remains vulnerable to multiplicity, even if each individual identity is internally coherent. The critical missing property is scarcity. Without scarcity, identity loses its coordinating power, and reputation cannot function as a conserved quantity.

The Sybil problem names this condition precisely. When an actor can generate arbitrarily many identities at negligible cost, the system cannot distinguish between plural participation and simulated consensus. Popularity, agreement, and legitimacy become manipulable signals, decoupled from the number of actual agents present. In such an environment, identity becomes inflationary, and meaning collapses under the weight of its own replication.

Scarcity is often misunderstood as an exclusionary or authoritarian design choice. In reality, it is an informational necessity. All systems that support durable reputation implicitly enforce scarcity in some dimension. In pre-digital societies, identity was scarce because it was bound to physical presence, geographic constraint, and long-lived social memory. In institutional systems, scarcity was enforced through credentialing, licensure, and membership, all of which imposed cost and delay on identity acquisition.

Digital platforms eliminated these frictions in the name of accessibility. This decision was defensible at small scale, when communities could self-regulate and reputation emerged organically. At planetary scale, however, the absence of scarcity transforms openness into a vulnerability. The system no longer accumulates signal; it amplifies noise.

Sybil resistance is the mechanism by which scarcity is reintroduced. It does not require uniqueness in an absolute sense, nor does it demand that identities be tied to real-world persons. It requires only that identity acquisition incur a non-trivial cost that cannot be parallelized indefinitely. The nature

of that cost determines the system's political and ethical character.

Computational costs, such as proof-of-work, impose scarcity through energy expenditure. While effective in limiting identity proliferation, they externalize cost onto the environment and privilege access to hardware and energy. Economic costs, such as staking or fees, tie identity weight to capital, reinforcing existing inequalities. Social costs, such as web-of-trust models, rely on pre-existing relationships and are vulnerable to infiltration once identity laundering has already occurred.

Each approach reveals the same underlying principle: identity must be expensive somewhere. A system that attempts to be universally accessible, frictionless, and anonymous while also supporting trust is structurally incoherent. The contradiction is not moral but mathematical.

From the perspective of namespace coherence, the goal of Sybil resistance is not to prevent all duplication, but to bound it. What matters is that the ratio between apparent identities and actual agents remains within a regime where attribution remains feasible. Beyond this threshold, the system undergoes a qualitative shift. Identity ceases to convey information, and all downstream mechanisms fail.

This threshold behavior explains why platforms often appear stable for long periods before experiencing rapid collapse. As identity proliferation increases gradually, the system absorbs the noise. Once a critical point is crossed, however, the accumulation of synthetic identities overwhelms the remaining structure. Trust dissipates rapidly, and recovery becomes non-linear.

Importantly, Sybil resistance also reintroduces consequence. When identities are costly to create and maintain, abandoning one becomes a meaningful decision. History acquires weight. Actors must choose between preserving accumulated reputation and discarding it to escape constraint. This trade-off is precisely what namespace laundering removes.

The economic dimension of this trade-off cannot be ignored. Systems that enforce identity scarcity inevitably produce asymmetries. Some actors will accumulate more trust, more influence, and more reach than others. This is often framed as a failure of fairness. In reality, it is the inevitable result of a system that allows reputation to mean anything at all.

The alternative is not equality, but entropy. A system that flattens identity to avoid hierarchy also flattens meaning. No one can build durable trust because trust itself cannot persist. Newcomers are not empowered; they are deprived of the possibility of accumulation. Every interaction becomes provisional, and every signal becomes suspect.

The central insight is that Sybil resistance is not about excluding participants, but about preserving the conditions under which participation can matter. It enforces the asymmetry between effort and outcome that makes deception costly and contribution worthwhile.

With continuity restored through cryptographic identity and scarcity enforced through Sybil resistance, the system acquires the two prerequisites for memory. The remaining question is how memory can persist beyond accounts and into artifacts themselves. The next section addresses this by formalizing identity as an information-theoretic constraint embedded directly into media and communication.

12 Information-Theoretic Identity and Media-Bound Provenance

Identity coherence cannot be sustained solely at the level of accounts or keys. In adversarial environments, actors adapt by fragmenting presence, abandoning identifiers, and re-entering under new guises. Even when cryptographic identity and Sybil resistance are enforced, a system that treats artifacts as free-floating objects remains vulnerable to historical erasure. To preserve memory under these conditions, identity must be bound not only to agents but to the informational structure of the artifacts they produce.

From an information-theoretic perspective, this problem can be framed as one of channel preservation. An artifact such as an image, video, or document constitutes a transmission from an agent into the shared environment. If the transformation from agent to artifact destroys provenance information, then the channel is lossy with respect to identity. Once lost, this information cannot be reconstructed downstream without introducing error. The system becomes incapable of attributing repeated behavior to a single source, even when patterns are obvious at the semantic level.

Current platforms exacerbate this loss by aggressively stripping metadata, recompressing media, and treating content as interchangeable units optimized for delivery rather than traceability. These practices maximize throughput but annihilate memory. As a result, artifacts circulate independently of their origin, and identity laundering becomes trivial. A single deceptive actor can populate the environment with uncorrelated fragments that evade aggregation and consequence.

The proposed alternative treats identity as an invariant embedded within the informational structure of artifacts themselves. Each identity is associated with a cryptographic hash derived from a persistent key. When an artifact is created, this hash is incorporated into the compression or encoding process as a parameter that modulates the basis of representation. The resulting artifact is therefore identity-conditioned at a structural level.

Crucially, this modulation does not take the form of a visible watermark or appended metadata. Instead, the identity hash alters the statistical structure of the compressed representation itself. For a given identity, the transformation is deterministic, ensuring that artifacts produced by the same agent exhibit consistent structural signatures. Across different identities, the same source material compresses differently in ways that are not perceptually salient but are statistically detectable when analyzed at scale.

Because the identity signal is embedded in the compression basis rather than in surface features, it remains robust under common transformations. Re-encoding, resizing, cropping, and format conversion preserve the underlying statistical modulation. Even when artifacts are reposted across platforms that do not cooperate or share infrastructure, their provenance remains probabilistically recoverable. Identity becomes sticky not through enforcement, but through physics.

This approach transforms artifacts into carriers of memory. Repeated behavior leaves correlated traces across time and context, even when the actor attempts to shed identity. The mutual information between agent and artifact increases, and the attributional entropy that enables recidivism decreases. The system no longer relies on account-level continuity alone; it acquires artifact-level persistence.

Importantly, this does not require global coordination or centralized authority. Provenance can

be inferred locally through statistical analysis, allowing independent systems to detect correlated behavior without sharing identity registries or personal data. The binding operates at the level of information, not governance.

Such a design reframes moderation and enforcement. Instead of attempting to infer intent from content semantics, the system accumulates evidence structurally. Patterns of abuse emerge naturally as repeated identity-conditioned transformations. Actors who persist in deceptive or harmful behavior find their actions increasingly correlated, regardless of surface changes. Identity laundering loses its efficacy because abandoning one identifier does not erase the informational residue of prior behavior.

This structural memory enables graduated response rather than binary exclusion. Actors can be rate-limited, isolated, or redirected based on accumulated correlation rather than single violations. In extreme cases, deceptive behavior can be confined to closed interaction spaces where it no longer impacts real users. The system need not accuse, expose, or shame; it simply ceases to provide leverage.

At a deeper level, media-bound provenance restores an asymmetry between creation and deception. Producing original content under a stable identity accumulates value over time. Attempting to exploit the system through imitation or misrepresentation accumulates traceable structure that constrains future action. The cost of abandoning history rises, and with it the incentive to behave consistently.

The significance of this shift is not merely technical. It represents a change in how systems relate to time. Instead of treating each interaction as an isolated event, the platform becomes temporally thick. Past actions inform present affordances. Memory becomes a first-class property rather than an accidental byproduct.

This, ultimately, is what namespace laundering destroys: the thickness of time. By embedding identity into artifacts themselves, the system regains the ability to remember, and with memory comes the possibility of accountability, learning, and trust. The next section examines why contemporary platforms systematically avoid such memory and how their economic structure rewards forgetting rather than conservation.

13 Platform Amnesia and the Political Economy of Recidivism

The absence of effective responses to recidivism on contemporary platforms is often attributed to technical limitations or the overwhelming scale of moderation. This explanation is insufficient. The persistence of repeat abuse is not a contingent failure but an emergent property of platforms whose economic incentives are aligned with forgetting. What appears externally as negligence or incapacity is internally consistent with systems designed to privilege throughput, growth, and monetization over historical coherence.

Recidivism presupposes memory. To identify an actor as a repeat offender, a system must be able to bind present behavior to past actions under a stable identity. Yet the dominant platform architectures explicitly avoid such binding. Identity is fragmented into disposable tokens, and enforcement actions are applied only to the currently visible manifestation of behavior. When an account is re-

moved, flagged, or deprioritized, the system treats the event as resolved. The actor who generated the behavior is not modeled as a persistent entity; they are simply absent from the system's internal representation.

This design produces a profound asymmetry between legitimate participants and adversarial actors. Ordinary users invest time, effort, and social capital into cultivating a coherent presence. They accumulate preferences, relationships, and histories that are costly to abandon. By contrast, malicious or deceptive actors face negligible switching costs. They can shed identity instantaneously and re-enter the system without penalty. Enforcement thus operates only on those who have something to lose.

From an informational perspective, the platform behaves as a memoryless channel. Observations of abuse do not update a durable model of agent behavior; they merely trigger local reactions that erase the very data required for future inference. Each moderation action destroys information that could have reduced uncertainty about future actions. Entropy therefore increases monotonically, not because harmful behavior is difficult to detect, but because detected information is systematically discarded.

This structural amnesia is reinforced by economic incentives. Advertising-driven platforms derive revenue from activity volume rather than participant integrity. Impressions, clicks, and conversions are valuable regardless of their provenance. Indeed, deceptive actors often outperform legitimate ones in generating engagement, precisely because sensationalism, impersonation, and false authority exploit human attention biases. To meaningfully address recidivism would require collating behavior across identities, imposing escalating constraints, and potentially excluding high-volume contributors. Such measures directly conflict with revenue optimization.

As a result, moderation is constrained to operate at the surface level. Content may be removed, accounts may be suspended, but the system never escalates against the underlying actor because, architecturally, there is no such object. Recidivism is not punished because it is not representable. The platform has no internal variable corresponding to "repeat offender." Without that variable, learning is impossible.

This explains why appeals to more sophisticated artificial intelligence consistently disappoint. Machine learning systems excel at pattern recognition given stable labels and training data. In a namespace-laundered environment, labels are unstable by design. Each identity reset erases the continuity required for supervised learning. The classifier is forced to relearn the same patterns endlessly, while adversarial actors adapt faster than models can converge. Intelligence is expended, but nothing is accumulated.

The economic structure of these platforms thus rewards strategic forgetting. Enforcement actions that would create durable memory are avoided because they impose friction on growth and expose platforms to legal and political risk. Forgetting becomes a feature rather than a bug. The system optimizes itself into incoherence while maintaining the appearance of responsiveness.

In contrast, systems that conserve identity coherence invert this incentive structure. When actions are bound to persistent histories, recidivism becomes costly. Abandoning an identity entails forfeiting accumulated reach, trust, and artifact continuity. The rational strategy shifts from cycling identities

to maintaining consistency. Abuse does not disappear, but it ceases to scale.

This analysis clarifies why namespace laundering is not merely tolerated but actively reproduced by current platforms. It is the mechanism by which they externalize the costs of abuse while internalizing its benefits. Any solution that ignores this political economy is destined to fail.

The final section synthesizes these arguments and articulates the broader implications of treating identity as a conserved structural primitive rather than a mutable social attribute.

14 Synthesis: Identity, Memory, and the Conservation of Meaning

The preceding analysis has traced a single structural failure across a wide range of contemporary platform pathologies: the systematic erosion of identity coherence through what has been described as namespace laundering. Impersonation, metric collapse, predatory advertising, and the persistence of recidivist abuse are not independent problems requiring separate remedies. They are coupled consequences of architectures that refuse to conserve identity as a binding relation between action and history.

At the center of this failure lies a mistaken ontological commitment. Contemporary platforms treat identity as representational rather than infrastructural. Names, badges, profiles, and brands are handled as surface-level symbols whose function is to signal affiliation or credibility, rather than as binding operators that enforce continuity over time. Once identity is reduced to representation, it becomes cheap to duplicate and easy to discard. The system thereby destroys the very precondition required for reputation, trust, and accountability to exist.

This destruction has precise informational consequences. When actions cannot be uniquely attributed to persistent agents, attributional entropy rises. Metrics decouple from substance, optimization selects for imitation, and enforcement loses its capacity to learn. The platform becomes a high-entropy environment in which activity is abundant but meaning is scarce. Importantly, this is not a moral failure on the part of users, nor a technical failure of moderation tools. It is a predictable outcome of optimization applied to an unconstrained namespace.

The political economy of large platforms ensures that this outcome is stable. Revenue models reward volume, not integrity. Enforcement that preserves memory would impose costs on growth and expose platforms to governance obligations they are structurally incentivized to avoid. As a result, platforms are optimized to forget. Recidivism is not addressed because it cannot be represented; identity resets are not penalized because identity itself is not conserved. The system is internally coherent even as it becomes socially incoherent.

Against this backdrop, proposals that focus on content moderation, fact-checking, or improved artificial intelligence are necessarily insufficient. They attempt to infer truth and intent downstream of a failure that has already destroyed the information required for inference. Intelligence cannot substitute for memory. No classifier can recover continuity that the system has chosen not to record.

The alternative advanced in this essay is deliberately architectural. Identity must be treated as infrastructure. This entails persistence, cost, and enforceable continuity, but not necessarily transparency. Cryptographic identity, Sybil resistance, and information-theoretic binding mechanisms

demonstrate that it is possible to conserve identity without collapsing into surveillance or eliminating pseudonymity. What is required is not that identities be publicly known, but that they be privately continuous and structurally inescapable.

Embedding identity into artifacts themselves extends this continuity beyond accounts and into the informational fabric of the system. When images, texts, and media objects carry identity-conditioned structure, behavior becomes collatable across contexts and over time. Recidivism ceases to be a policy concern and becomes a detectable physical phenomenon. Constraint replaces judgment. Abuse is not argued with; it is damped.

The speculative notion of containment-oriented responses follows naturally from this framework. If adversarial behavior is persistent and incentive-aligned, then attempting to eradicate it is futile. What matters is whether such behavior can exert influence. Isolating malicious actors into unproductive interaction loops acknowledges economic reality while preserving systemic coherence. This is not deception for its own sake, but a form of architectural harm reduction.

Taken together, these arguments support a single, unifying claim: meaning is a conserved quantity. It cannot be generated by optimization once the structures that preserve it have been dissolved. Trust, reputation, and truth are emergent properties of systems that remember who acts. Platforms that refuse to remember cannot govern, learn, or stabilize, regardless of how sophisticated their algorithms become.

This analysis is not limited to a critique of impersonation or fraud. It advances a more fundamental claim: memory must be treated as a first-class design principle in any system that aspires to support durable social, economic, or epistemic activity. When actions are not bound to persistent histories, trust cannot accumulate and collapse becomes structurally inevitable. The central design decision is therefore not between openness and control, but between architectures that preserve meaning through continuity and those that allow it to dissipate into irrecoverable noise.

15 Conclusion

This essay has argued that the contemporary crisis of trust on digital platforms is neither accidental nor primarily cultural, but architectural. The proliferation of impersonation, scam advertising, synthetic authority, and recidivist abuse is not a failure of moderation, intelligence, or goodwill. It is the predictable consequence of systems that treat identity as a disposable label rather than as a conserved structural primitive. Namespace laundering is not a marginal exploit but a dominant equilibrium produced by prevailing platform design choices.

By reframing identity as namespace infrastructure, the analysis has shown that trust, reputation, and meaning are not subjective overlays that can be optimized after the fact, but informational quantities that require stable binding to persist over time. When actions cannot be uniquely and persistently associated with histories, attribution collapses, metrics decouple from substance, and optimization pressure inevitably selects for imitation over contribution. Goodhart collapse, metric farming, and performative engagement arise not because actors are irrational, but because the system renders authenticity more costly than deception.

The argument further demonstrates that this collapse is thermodynamic rather than linear. Within the RSVP framework, platform dynamics undergo phase transitions once identity dispersion exceeds a critical threshold. Beyond this point, coherence does not degrade gradually but bifurcates into a high-entropy regime characterized by vector churn and reputational dissipation. Hysteresis explains why mature platforms cannot easily recover trust once it has been lost: the scalar basins that once stabilized meaning have been flattened, and restoring them requires forces far greater than those originally required to maintain them.

Contemporary platform responses—account bans, content removal, automated moderation, and policy adjustments—fail because they operate downstream of this structural collapse. They address symptoms rather than causes. Most critically, they do nothing to address recidivism. By permitting offenders to re-enter systems under fresh identifiers at negligible cost, platforms systematically erase the very information required to learn, escalate, or deter. Enforcement thereby becomes a source of entropy, accelerating the loss of meaning rather than conserving it.

Against this backdrop, the alternatives explored here are deliberately architectural rather than punitive. Cryptographic identity, Sybil resistance, and information-theoretic binding mechanisms are not instruments of surveillance or control, but means of restoring conservation laws. By binding identities to persistent cryptographic structures, embedding those bindings into shared artifacts, and ensuring that permissible variations remain contractibly associated with a single historical trajectory, a system can acquire memory without sacrificing pseudonymity. Under such conditions, recidivism becomes structurally visible, manipulation grows increasingly costly, and deception is constrained not by discretionary judgment but by incompatibility with the system's invariants.

The speculative proposal of isolating deceptive actors within unproductive, game-like environments further illustrates this shift in perspective. Rather than attempting continuous moral correction or adversarial policing, the system simply denies such behavior informational leverage. Where identity is conserved and consequences accumulate, abuse fails to scale. Where identity is laundered, no degree of intelligence or moderation can prevent collapse.

The broader implication is that many existing platforms may be beyond repair. Their economic incentives are aligned with identity fragmentation, and their architectures lack the authority to collate behavior across time. In such cases, recovery may be impossible without abandoning the system itself. New platforms must therefore be constructed alongside the old, grounded in constraint-first design and offering continuity through trust transfer rather than restoration.

The central claim of this essay is thus straightforward: meaning is not generated by optimization but preserved by constraint. Identity coherence is not a feature to be balanced against growth or engagement; it is the precondition for any system that claims to support knowledge, reputation, or social reality. Systems that refuse to bind actions to histories must accept collapse as their terminal state. Only systems that remember can govern.

References

[1] C. A. E. Goodhart. Problems of monetary management: The U.K. experience. In *Papers in Monetary Economics*, Reserve Bank of Australia, 1975.

[2] D. T. Campbell. Assessing the impact of planned social change. *Evaluation and Program Planning*, 2(1):67–90, 1979.

[3] M. Strathern. "Improving ratings": Audit in the British university system. *European Review*, 5(3):305–321, 1997.

[4] J. Z. Muller. *The Tyranny of Metrics*. Princeton University Press, Princeton, 2018.

[5] E. M. Bender, T. Gebru, A. McMillan-Major, and S. Shmitchell. On the dangers of stochastic parrots: Can language models be too big? In *Proceedings of the ACM Conference on Fairness, Accountability, and Transparency*, 2021.

[6] C. Olah, A. Mordvintsev, L. Schubert, L. Carter, and C. Yeh. The building blocks of interpretability. *Distill*, 3(3), 2018.

[7] K. Friston. The free-energy principle: A unified brain theory? *Nature Reviews Neuroscience*, 11(2):127–138, 2010.

[8] R. Landauer. Irreversibility and heat generation in the computing process. *IBM Journal of Research and Development*, 5(3):183–191, 1961.

[9] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 623–656, 1948.

[10] H. R. Varian. Market structure in the network age. *Journal of Economic Perspectives*, 33(3):91–110, 2019.

[11] C. Doctorow. The enshittification of TikTok. *Pluralistic*, 2023.

[12] S. Zuboff. *The Age of Surveillance Capitalism*. PublicAffairs, New York, 2019.

[13] L. Lamport. The part-time parliament. *ACM Transactions on Computer Systems*, 16(2):133–169, 1998.

[14] S. Mac Lane. *Categories for the Working Mathematician*. Springer, New York, 2nd edition, 1998.

[15] R. Ghrist. *Elementary Applied Topology*. Createspace, 2014.

[16] J. C. Scott. *Seeing Like a State*. Yale University Press, New Haven, 1998.

[17] L. Lessig. *Code and Other Laws of Cyberspace*. Basic Books, New York, 1999.

[18] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[19] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[20] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, 1989.

[21] D. Chaum. Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM*, 28(10):1030–1044, 1985.

[22] J. R. Douceur. The Sybil attack. In *Peer-to-Peer Systems: First International Workshop, IPTPS 2002*, pages 251–260. Springer, 2002.

[23] B. N. Levine, C. Shields, and N. B. Margolin. A survey of solutions to the Sybil attack. Technical report, University of Massachusetts Amherst, 2006.

[24] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. White paper, 2008.

[25] V. Buterin. A next-generation smart contract and decentralized application platform. Ethereum white paper, 2014.

[26] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten. SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2015.

[27] F. Wang and L. Liu. Sybil-resistant trust mechanisms in online social networks. *IEEE Transactions on Network Science and Engineering*, 4(4):268–282, 2017.

[28] L. Alvisi, A. Clement, A. Epasto, S. Lattanzi, and A. Panconesi. SoK: The evolution of Sybil defense via social networks. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2013.

[29] M. Feldman, K. Lai, I. Stoica, and J. Chuang. Robust incentive techniques for peer-to-peer networks. *ACM Transactions on Economics and Computation*, 9(1), 2021.

[30] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. *Bitcoin and Cryptocurrency Technologies*. Princeton University Press, Princeton, 2016.

[31] D. Chaum. Blind signatures for untraceable payments. In *Advances in Cryptology (CRYPTO '82)*, pages 199–203. Springer, 1983.

[32] S. Brands. *Rethinking Public Key Infrastructures and Digital Certificates*. MIT Press, Cambridge, MA, 2000.

[33] J. Camenisch and A. Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *Advances in Cryptology (EUROCRYPT 2001)*, pages 93–118. Springer, 2001.

[34] J. Camenisch and A. Lysyanskaya. Dynamic accumulators and application to efficient revocation of anonymous credentials. In *Advances in Cryptology (CRYPTO 2002)*, pages 61–76. Springer, 2002.

[35] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the ACM*, 38(3):691–729, 1991.

[36] E. Ben-Sasson, A. Chiesa, E. Tromer, and M. Virza. Succinct non-interactive zero knowledge for a von Neumann architecture. In *Proceedings of the 23rd USENIX Security Symposium*, 2014.

[37] I. Miers, C. Garman, M. Green, and A. Rubin. Zerocoin: Anonymous distributed e-cash from Bitcoin. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2013.

[38] E. Ben-Sasson et al. Zcash: Decentralized anonymous payments from Bitcoin. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2016.

[39] S. Bowe, J. Gabizon, and D. Green. Halo: Recursive proof composition without a trusted setup. Cryptology ePrint Archive, Report 2019/1021.

[40] T. Hardjono, A. Lipton, and A. Pentland. Towards an interoperability architecture for blockchain autonomous systems. *IEEE Transactions on Engineering Management*, 2019.

[41] C. Allen. The path to self-sovereign identity. *Life With Alacrity*, 2015.

[42] World Wide Web Consortium. Verifiable credentials data model v1.1. W3C Recommendation, 2022.

[43] C. Garman, M. Green, and I. Miers. Decentralized anonymous credentials. *ACM Transactions on Privacy and Security*, 23(1), 2020.