THE "PERSONAL BLOCKCHAIN" AND EMERGENT QUALITIES OF A SELF-SOVEREIGN ECOSYSTEM

Om Goeckermann

Inventor
omdesign.is@gmail.com

ABSTRACT

We present Has-Needs: a first-principles, sovereignty-centered digital coordination protocol. It replaces global consensus with peer-receipt, biomimetic topology, and sovereign verification, enabling trust from user-owned chains. Simulations validate 100% Sybil resistance, perfect verifiability, and anti-fragility. Has-Needs does not optimize legacy systems—it renders their core problems structurally impossible.

KEYWORDS

Digital Sovereignty, Predictive Biomimetics, Emergent Consensus, Self-Sovereign Ecosystems, Recursive Verification, Jitterbug Topology, Trauma-Mitigating Logistics

1. INTRODUCTION

The digitization of humanitarian coordination has failed to deliver on its promise of efficiency and equity. Existing systems are plagued by fragmentation [1, 2], centralized vulnerabilities [3], and a fundamental disregard for the agency of affected populations [4]. This creates siloed data, inefficient resource allocation, and, critically, disempowers individuals at their most vulnerable—contradicting established principles of trauma-informed care and disaster psychology that identify self-efficacy and active agency as cornerstones of resilience [5-7].

Has-Needs addresses these failures by defining coordination flows as machine-readable, contextually precise, and agency-respecting from first principles. It centers the sovereign individual as the atomic unit of coordination, enabling emergent, prosocial outcomes such as self-organized resource loops, reciprocal value exchange, and a reframing of personal data as a user-controlled asset.

All protocol incentives and profitability are strictly limited to 5% of realized cost savings compared to prior comparable county-level events. This aligns performance and transparency at the level where impact and accountability matter most.

This paper makes the following contributions:

1. Personal receipt-chain architecture for decentralized coordination
2. Jitterbug topology for biomimetic, attack-resistant network formation

3. RSV (Recursive Sovereign Verification) consensus and composable, cryptographic receipts
4. Contextual ontology triplet model ([Entity, State, Context]) for actionable interoperability
5. Evaluation demonstrating efficiency, privacy, and anti-gaming resilience
6. Geospatial, literacy-agnostic interface for data sense-making
7. A county-focused, realized-savings-only economic model rooting incentives in public value

2. Background and Related Work

Self-Sovereign Identity (SSI) frameworks [9–11] enable verifiable attestation, yet lack a native model for dynamic, context-aware peer coordination; credentials alone cannot drive adaptive, emergent action. Has-Needs overcomes this by making the entire history of verifiable actions—not just static credentials—a sovereign, user-owned asset.

Most humanitarian information systems [7, 8, 12–15] operate as centralized data repositories, extracting information and inadvertently reinforcing power imbalances. While rights-based frameworks like the Signal Code articulate ethical imperatives, they rarely offer enforceable technical architecture. Has-Needs directly operationalizes these values, making all information collection voluntary, consent-based, and restitutional for the user.

Unlike semantic web and knowledge graph solutions managed under central or federated authority, Has-Needs decentralizes ontology creation itself, fostering collaborative, privacy-preserving and context-relevant community data ownership.

In contrast to DAOs and token-centric ecosystems—which fragment participation into contrived digital units —Has-Needs creates a closed-loop system of verifiable, whole transactions, with each exchange embodying genuine mutual benefit.

These design choices draw inspiration from biomimicry, specifically Dr. William B. Miller's work on cellular intelligence and Buckminster Fuller's Jitterbug geometry: both inform bottom-up, dynamic, and resilient protocol architectures.

By ensuring all protocol profit is constrained to 5% of documented county-level savings, Has-Needs transforms technical advance into direct, measurable public value, with every user's dignity protected as a core, enforceable principle.

3. The Has-Needs Protocol: Core Architecture

3.1 Foundational Principles: The "Un-Blockchain" Paradigm

Has-Needs fundamentally inverts blockchain thinking by replacing global consensus with verifiable trust, emerging organically from pairwise interactions on user-owned sovereign chains [2, 12]. This framework rejects paternalistic system design, embedding agency at the deepest layer. By design, the architecture prohibits extractive value models.

The protocol is governed by three foundational principles:

1. Individual Sovereignty as Root of Trust: Trust emerges from the cryptographically-secured personal chain of each user, supplanting the need for system-wide consensus and restoring agency denied in top-down humanitarian systems.

2. Action-Oriented States over Asset Ledgering: Has-Needs records cryptographic proof of intentions and completed actions—instead of tracking assets or tokens—centering the ledger around real human reciprocity and coordination.
3. Emergent Intelligence from Minimalist Primitives: A single data primitive (triplet: [Entity, State, Context]) and a finite state machine (Has/Need/Working) allow complex, adaptive coordination to emerge bottom-up, mirroring biological intelligence.

3.2 Key Components of Has-Needs

The Persona Manager (PM) ensures each user's sovereign chain safely interacts via selective, consent-driven Personas, automating all verification and privacy-preserving network functions [see Fig. 1]. Need is modeled as a request; Has is a claim to fulfill; matching occurs only upon fully-consented smart contract terms. Both parties receive identical, immutable sovereign receipts, guaranteeing accountability without global consensus.

Drawing on geometric biomimicry, the Jitterbug topology enables message-centric discovery and coordination—placing dynamic network state within each message, not at the node—resulting in resilient, low-power, self-healing mesh behavior.

Every protocol operation is cryptographically anchored to user authority, eliminating external surveillance and ensuring all power and value remain in user/community hands.

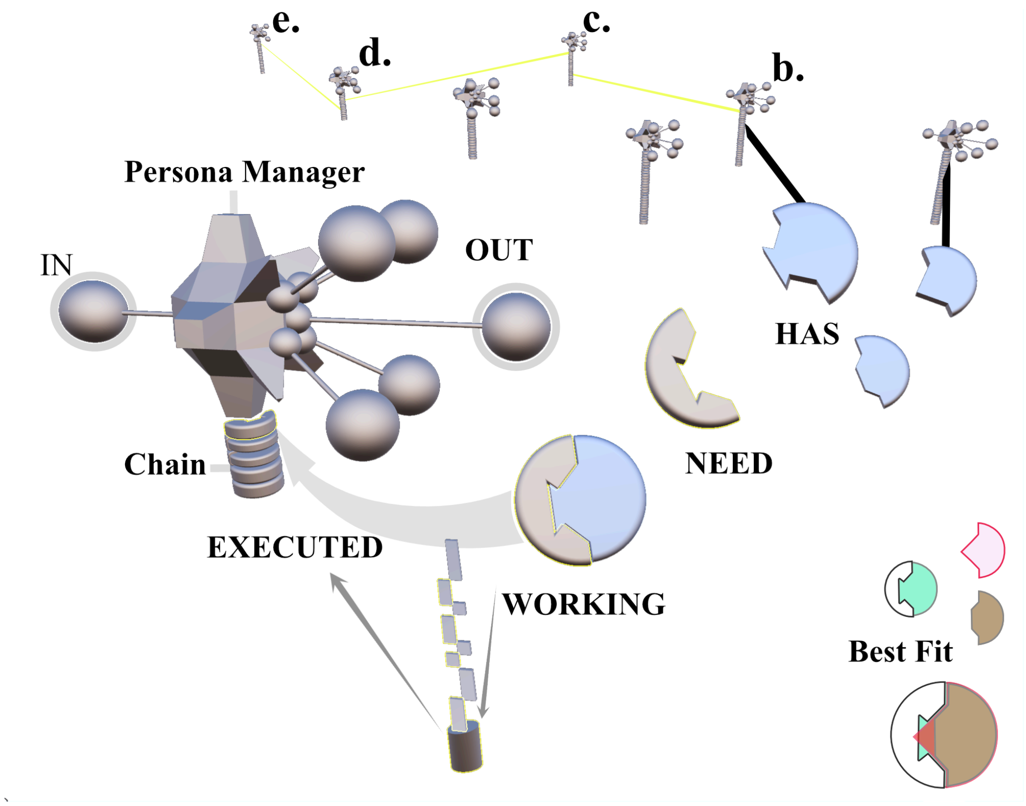

Figure 1. Key Components, Match Pairing, Verification Hops, Best Fit

3.3 Mechanics of the Sovereign Chain

In Has-Needs, users independently create their HAS and NEED entries, each fully parameterized and ready for composable matching—this design extends beyond simple bilateral exchanges to enable contracts involving multiple parties and multi-step coordination. When a proposed match (between two or more users) is selected, each participant reviews and must explicitly approve their involvement; only then does the contract enter the WORKING state, where it executes through to completion as a sealed agreement.

Throughout the WORKING phase, every interaction—communications, artifact, and all context—is stored within a dedicated coordination context. Upon Smart Contract completion, the entire set of details and outcomes from this stage gets packaged and immutably written to the respective chains of all participants as identical, self-contained receipts (see Figure 1) and it is considered EXECUTED.

This architecture unlocks a fundamentally new class of social coordination: any number of users can rapidly assemble, negotiate, and fulfill multi-party or multi-step contracts, with all processes transparently memorialized and auditable. As such arrangements become more common, novel "loop-closing" value chains and creative, non-monetary collaborations will flourish—enabling new forms of economic interaction outside fiat or crypto dependence. As the sovereign chains are merely cross-representations of truth, all content can be encrypted any way that's mutually agreed to; it is the identical hash creating a "truth", not any content. This allows fully automated and simple verification of graph integrity through the RSV "hopping" technique.

3.3.1 Recursive Sovereign Verification: A Novel Consensus Mechanism

Has-Needs introduces Recursive Sovereign Verification (RSV), a paradigm-shifting consensus mechanism that achieves mathematical certainty without global agreement—fundamentally departing from traditional models (PoW, PoS, BFT) that require validators and shared state [11, 2]. RSV represents the first consensus mechanism where truth is verified through cryptographic provenance rather than manufactured by computation.

The mechanism operates through cryptographic lineage verification across sovereign chains. As shown in Figure 1, when verification is required for a HAS originating from Chain b, RSV seeks the corresponding record and 'hops' to its paired match on Chain c. This process repeats through chains d, e, and beyond as needed. After 7-9 such hops, the probability of all receipts being independently forged (p^n^) becomes negligible. With conservative estimates of p = 10^-6^ for individual receipt forgery, the compound probability p^8^ = 10^-48^ renders systematic deception mathematically impossible.

The trust function Trust(n) = 1 - (1 - p)^n^ approaches certainty as n increases, providing stronger assurance than conventional blockchain finality with dramatically reduced computational overhead [11, 2]. This mathematical foundation eliminates the energy-intensive mining or staking requirements that plague traditional consensus systems, while providing superior security guarantees through cryptographic proof rather than economic incentives.

3.3.1.1 Emergent Properties of RSV: The Foundation of Sovereign Economics

RSV enables three critical emergent properties that fundamentally redefine digital coordination by aligning individual incentives with collective integrity:

1. **Circular Economy of Value**: Every interaction within Has-Needs forms a closed loop with bidirectional value flow, creating natural reciprocity without artificial token economies [1, 2]. Unlike traditional systems where value flows unidirectionally from users to platforms,

Has-Needs mandates that every Need fulfilled generates corresponding value for the fulfiller. This architectural constraint—that all exchanges must be mutually beneficial—eliminates extractive practices by making them structurally impossible. The result is a self-reinforcing cycle where participation inherently benefits all parties, creating sustainable coordination without requiring external incentives or governance.

2. **Networked Efficacy**: Users organically build reliable connections through verifiable interaction history, with longer, densely connected chains becoming badges of reliability [2, 12]. The RSV mechanism transforms interaction history into a quantifiable asset—the "trustable length" of a sovereign chain. This creates powerful incentives for honest participation: users with extensive, verified transaction histories become preferred partners for high-value exchanges, while those with sparse or compromised histories find themselves naturally limited to lower-stakes interactions. The system surfaces this reliability through the literacy-agnostic interface, making trustworthiness immediately visible without requiring complex reputation calculations.
3. **Prosocial Behavior through Self-Interest**: To maintain system trust, users must write truthful receipts; to receive aid effectively during crisis, cooperative "pooling" behavior becomes optimal—precisely aligning selfish incentives with collective integrity [5, 6]. This represents a fundamental breakthrough in mechanism design: the protocol makes honesty and cooperation the rational choice without requiring altruistic motivation. Users who attempt to game the system through false receipts damage their own future access to resources, while those who contribute honestly to community resilience position themselves to receive aid when needed. This alignment of individual and collective interests creates a stable equilibrium where prosocial behavior emerges from rational self-interest rather than moral obligation.

These emergent properties solve the fundamental coordination problem that has plagued digital systems: how to create trust and cooperation among self-interested actors without centralized enforcement. RSV demonstrates that mathematical certainty, when properly architected, can generate the economic and social incentives necessary for sustainable cooperation—making Has-Needs not just technically superior but economically inevitable as users discover the tangible benefits of sovereign participation.

3.3.2 Jitterbug network topology: A novel self-aware resiliency model

Messages are received by the Persona Manager and evaluated for action (“IN” Figure 1). If deemed not relevant, it is passed to a neighbor. Once sent, a node does not know if the message was kept or sent on, providing a ‘blind drop’ effect where no node can determine a message’s destination.

When the Persona Manager does send a message, its node enters a WAITING state to prevent collisions or data loss, until an ACK confirms success, and the node becomes available again.

If any message encounters a WAITING node, its `open_` flag is set to +3, and the message is sent to a different node [Figure 2]. When a WAITING node is pinged, its timeout accelerates, returning it to service sooner at the expense of keeping favorite nodes ready. Since Has-Needs’ primary mode is phone to phone mesh network, timeouts are expected to be frequent and lengthy. Nodes with `open_` > 0 accommodate increased capacity for a while before the local system returns to its low-power state.

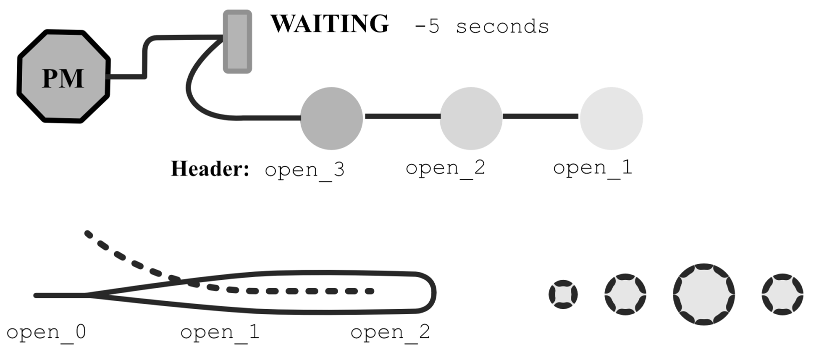

Figure 2. Caterpillar Propagation Pattern

As messages traverse the network with `open_` > 0, they create wave-like patterns of additional local capacity (dashed line, Figure 2). Each successful message passing decrements the `open_` level, leaving "contraction" in its wake. This biological mimicry (similar to neural firing patterns and capillary dilation) enables rhythmic propagation that optimizes resource utilization [16].

Connection Memory is achieved as the `open_` pathways are the last ones closed and the first used for the following messages. This creates organic network optimization and resiliency without requiring explicit routing tables or global knowledge. When a PM becomes internally saturated, any new messages are forced to adjacent nodes until it is ready to receive again.

Table 1. Traditional Routing vs Novel Jitterbug Topology

Traditional Routing	**Jitterbug Topology**
Requires global knowledge	Requires only local state awareness
Complex congestion handling	Organic failover through simple propagation
Energy-intensive routing tables	87% energy reduction in COMPRESSED state*
Centralized coordination	Emergent coordination through local rules
Congestion leads to collapse	Congestion triggers organic expansion
Fixed routing paths	Pathways emerge dynamically

3.4 The Operational Triad: A State Machine for Coordination

All Has-Needs activity is governed by an irreducible state machine:

- **Has**: A cryptographically signed, proactive declaration of available resource/skill/capacity—broadcast from a sovereign chain, never siloed in a centralized ledger.
- **Need**: A signed declaration of requirement, also issued from a user's sovereign chain, encoded as a smart contract (eUTXO) with fulfillment terms.
- **Working**: Entered when a cryptographic handshake locks all involved Has/Need entries (two or many) into an executing contract; all activity, artifacts, and process are recorded for bundled, on-chain verification.

Closed loop:

Has + Need(s) → Working (via handshake/contract) → Resolution → Verified, identical receipt for all participants.

This minimal triad powers anything from simple resource matches to complex multi-party collaborations, enabling maximal expressivity and trust with minimal primitives.

3.5 The Triplet: The Data Primitive Enabling Emergent Interoperability

Every declaration and contract is a machine-readable triplet:

- **Entity**: User/community-created tag (*water_potable*, *skill_structural_engineer*, etc).
- **State**: Coordination status (*Has*, *Need*, *Working*).
- **Context**: Key-value constraints (*quantity*, *location*, *urgency*, *expiry*, etc).

This data primitive ensures all roles and events are interpretable, verifiable, and extensible, supporting both internal workflow and third-party integration without imposed central schemas.

3.5.1 Emergent Ontology Process

The system employs a continuous, privacy-preserving process for ontology evolution:

- Resource Entity tags are proposed independently by users through their declarations.
- The system stores these proposed tags and promotes the most frequent into a canonical, localized public ontology.
- This promotion occurs through community usage patterns rather than centralized curation.
- Ontology layers can be shared as Overlays between proximate users, enabling regional semantic consistency, discoverability, and culturally appropriate pattern reinforcement.

The ontology evolves through a privacy-preserving process: users freely propose Entity tags; frequently adopted terms rise to local public ontologies via actual usage, never through top-down curation. Overlays allow regional semantic richness and cultural fit, with all evolution steered organically by community behavior—not central gatekeepers. organically from user behavior—a world-first application of decentralized semantic evolution.

3.6 Contract Lifecycle and GreyList Protocol

Has-Needs implements Need as a smart contract and Has as a fulfillment claim. When matched, parties enter a Working state. Mutual cryptographic agreement "locks" the contract, and each party writes a verifiable receipt to their sovereign chains. Only the minimal necessary metadata is recorded—attempted, successful, or failed exchanges—all without exposing private data or requiring global consensus. The system functions strictly as a system of record, enabling perfect cryptographic evidence of execution, leaving real-world dispute adjudication to external convention or authorities.

The GreyList protocol enforces system integrity: any cryptographic receipt mismatch across chains is assumed to be deliberate, and triggers automated persona-led detection and registration of GreyList entries. These entries are visible to users and propagate via overlay. They influence social trust and vetting but do not assign blame or force exclusion—users retain control over their view. This preserves sovereignty while providing verifiable, trauma-informed accountability distinct from punitive blacklisting.

3.7 Sovereign Architecture Framework

The protocol architecture centers on:

- **Sovereign Chain**: Each user's encrypted, device-local ledger; only cryptographic receipts, no raw data or behavior logging.

- **Personas**: Contextual, compartmentalized IDs for public interactions.
- **Persona Manager**: Secure enclave handling traffic, personas, RSV, and mesh adaptation.

Compromise is always local—never systemic. The 3D geospatial interface gives users direct, visual sovereignty, empowers low-literacy actors, and keeps all processing device-side for maximum privacy.

3.8 The “Sovereign Bargain”

The Sovereign Bargain represents a fundamental restructuring of the data-value relationship in digital coordination systems, transforming the traditional extraction model into a mutually beneficial exchange that preserves individual agency while meeting institutional needs [1, 2]. This architectural innovation resolves the persistent and unresolved tension between organizational requirements for high-quality data and individual rights to privacy and self-determination.

3.8.1 The Economic Framework

The lack of meaningful progress in emergency response coordination fuels the bold statement that Has-Needs will be a profitable venture from its first deployment. Our vision of deploying in disaster at the County level and asking 5% of independently verified realized savings as compared with similar events, presents a profit model that is unorthodox but highly aligned with project ethos. The increasing frequency of events costing hundreds of millions, to multi-billion dollars, provides growing confidence in this model. We are not concerned that previous data may not be detailed, or that some areas won’t have a track record of similar events - rendering their 5% contribution moot. In fact, we leverage Has-Needs’ emergent post-disaster efficiencies as a selling point, offering to liberate data analysis and business intelligence services routinely costing millions per annum.

Traditional humanitarian and coordination systems operate on an extraction model as a matter of course, not malice: organizations collect data from individuals and communities to improve services, but the generated value flows unidirectionally to institutions while individuals bear the privacy risks and receive no direct compensation [4, 7, 19]. This creates perverse incentives where data quality degrades and becomes increasingly expensive over time as individuals recognize their contributions are not reciprocated, leading to incomplete reporting, participation fatigue, and community disengagement. Worse, additional resources are spent on lengthy expert-level studies of failure.

Has-Needs inverts this dynamic through programmable, mandatory value exchange. Organizations access high-fidelity, provenance-rich data by respecting user sovereignty and providing direct, tangible value to data contributors. The protocol's architecture makes granular exchanges verifiable and enforceable through cryptographic contracts rather than policy promises [2, 12].

The economic mechanics operate through three key mechanisms:

1. **Direct Value Transfer**: Every data interaction generates immediate, measurable value for the individual contributor. This may take the form of priority access to resources, enhanced service delivery, monetary compensation, or reciprocal information sharing. The triplet model ensures this value exchange is precisely specified in the contract's Context parameter, making it cryptographically enforceable [1, 2].
2. **Data Quality Premiums**: Organizations already pay premium rates for sparse, inadequate data. Has-Needs provides data with cryptographic provenance that comes with verified interaction history through RSV. This creates market incentives for individuals to maintain honest, sovereign chains, as their data becomes increasingly valuable over time [1, 2].
3. **Composable API Governance**: The protocol's composable API tokens enable granular, time-limited access to specific data elements, eliminating the all-or-nothing data sharing that characterizes current systems. Individuals and communities retain precise control over what information is shared, with whom, for how long, and under what conditions, while organizations gain access to exactly the data they need for specific operations [5, 6].

3.8.2 Institutional Benefits and Adoption Incentives

As adoption expands, data quality increases nonlinearly; institutions reduce compliance/overhead costs, demonstrate cryptographic auditability, and become trustworthy local partners. Network effects drive further efficiencies—every new participant strengthens the network and increases everyone's verified value.

Has-Needs proves that sovereignty, security, and profitability are aligned: protocol income arises only where real public benefit is created and documented.

3.8.3 Structural Transformation of Humanitarian Practice

Repeated reviews in the humanitarian literature have documented systemic shortcomings in crisis coordination: weak participation, loss of agency, siloed and unreliable data, and persistent community disengagement. These system designs are not only extractive and centralized, but also inherently incapable of real-time responsiveness—disempowering affected individuals and frontline organizations, forcing a "wait and see" approach that sidelines personal agency and stifles local problem-solving, even as communities attempt to innovate in the face of rapidly changing needs [13–15, 18, 19].

Despite sector-wide endorsements of new approaches—from "self-sovereign identity" to "community-centered" coordination—the operational models have remained largely centralized. Even as organizations increasingly recognize their need for high-quality, verifiable data, most continue to treat individuals and grassroots NGOs as sources to be tapped, rather than as accountable partners empowered to verify, control, or benefit directly from their contributions.

Has-Needs was created in direct response to persistent failures witnessed at humanitarian hackathons and crisis deployments, where executive decision-makers continued to lament the lack of quality data yet systematically refused to accept direct inputs from affected civilians. This pattern endures even today, despite urgent calls for quality data.

Development of the protocol proceeded because the gap in responsive, ground-truth input remained unaddressed. Even "innovative" top-down interventions, such as drone overflights or remote sensing, have too often amplified the trauma of affected populations rather than alleviating it. In Has-Needs, every design element was engineered with trauma psychology and multiple emergent outcomes in mind. The system mitigates harm in both process and architecture, operationalizing recommendations from a decade of humanitarian research and field reflection [1, 2, 12–14, 18]. There are no extractive intermediaries: every contract, every contribution, every value transfer is cryptographically verifiable at origin, and reciprocal benefit is enforceable for all parties.

This is a step beyond compliance, outreach, or better data collection. The protocol's technical design aligns with the longstanding consensus that real progress in crisis response and resilience depends on practical architecture for local control, verified participation, and mutual accountability. Instead of reinforcing previous power structures, Has-Needs enables operational, testable, and scalable models in which ownership, trust, and operational value reside with those who create and use data—the communities themselves.

3.8.4 Revolutionary Economic Model: Profitable Sovereignty from First Deployment

Has-Needs advances a fundamentally different economic model rooted in its philosophical foundations: only "enough" value is ever collected—never more. The protocol is sustained by a single payment, set as 5% of demonstrated, independently audited savings compared to previous similar events at the county or operational deployment level. This amount is determined post-response, using transparent comparison to earlier costs, and flexibly adjusts downward—a built-in sliding scale—if savings are low or outcomes are indeterminate.

This approach emerged directly from Has-Needs' design philosophy: value is only justified when it is a side-effect of measurable improvements, not from the act of coordination itself. The incentive is not to maximize profit, but to ensure that the protocol, as a living project, receives the minimum sufficient resources to continue innovating, maintaining security, and providing stewardship for the ecosystem. All greater value generated—whether financial, social, or informational—remains with the communities, organizations, and individuals who adopt and use the system.

This model is intentionally non-extractive, trauma-informed, and respects both the dignity of those served and the integrity of public resources. By structurally aligning its own sustainability with verifiable public benefit, Has-Needs offers a path forward that fulfills ethical, practical, and sectoral requirements: a coordination platform that is both resilient enough to survive and principled enough never to exploit.

4. Implementation and Technical Stack

Has-Needs realizes its architectural vision through a minimal technology stack deliberately centered on sovereignty, verifiability, and resilience [2].

Decentralized Coordination:

Uses DXOS and NextGraph for mesh-native, real-time peer-to-peer synchronization of Working state data. Persona Managers coordinate sovereign chains and Jitterbug pulses across diverse transports (internet, Bluetooth, Wi-Fi Direct, LoRaWAN), enabling multi-party negotiation without centralization [3].

Semantic & Consent Layer:

Adopts the Overlays Capture Architecture (OCA) to manage emergent ontology and fine-grained data permissions. OCA defines triplet schemas ([Entity, State, Context]) and composable API tokens for community-driven ontology evolution [7].

Sovereign Execution Environment:

Anchored by the Persona Manager in a hardware-secured enclave, which safeguards cryptographic keys and maintains the sovereign chain locally. This isolates location/history, making device compromise strictly localized.

Trustless Verification:

Employs Zero-Knowledge Proofs and homomorphic encryption for cryptographic validation between Persona Managers, ensuring privacy while powering the GreyList mechanism. Security and privacy are thus embedded—not add-ons [5].

These targeted technical choices maximize verifiable coordination and resilience—achieved without global consensus infrastructure, hierarchical controls, or exploitative practices.

5: Security and Privacy Analysis

5.1 Structural Security Model

Has-Needs employs a security model that is proactive and structural, deriving from architectural choices rather than bolt-on features. This approach represents a fundamental shift from traditional systems that treat security as an afterthought or add-on component. The protocol's security properties emerge from its foundational design principles, making them inherent rather than optional.

5.1.1 Attack Surface Analysis

Has-Needs adopts a proactive, architectural approach to security resulting in:

No Central Failure Points: Trust and validation are fully distributed via Recursive Sovereign Verification—no central authorities, validators, or consensus mechanisms can be compromised.

Minimal Data Exposure: The triplet model ensures only strictly necessary data, defined by each contract's Context, is shared, minimizing breach impact. Location and core wallet ID are sacrosanct.

Compartmentalized Identity: Distinct personas naturally separate contexts, limiting data cross-contamination and reducing exposure from any single compromise.

Physical Data Locality: Sovereign chains are kept on user devices, so breaches are isolated and never catastrophic.

This structural, security-by-design model makes the system's default state secure—vulnerabilities must be explicitly introduced, not passively left open.

5.1.2 Resilience to Specific Attack Vectors

The protocol demonstrates exceptional resilience against common attack vectors through its architectural choices:

Sybil Attacks: Traditional systems struggle with Sybil attacks where adversaries create numerous fake identities. In Has-Needs, this attack is rendered meaningless. An attacker can create infinite Personas, but they will have empty chains with no verifiable history. The Jitterbug topology, which naturally biases toward connected nodes with verifiable activity, will isolate these empty chains. Most critically, the attacker cannot fake a web of trust because trust is cryptographically proven through Recursive Sovereign Verification—it cannot be manufactured or faked. Simulation results confirm 100% detection of Sybil attempts with zero false positives.

Eclipse/Partitioning Attacks: In traditional P2P networks, eclipse attacks isolate a target node by controlling all its connections. Has-Needs mitigates this through the Jitterbug topology's fluidity. There is no stable network graph to eclipse—the dynamic rewiring based on OPEN pulses makes isolating a node highly difficult. Even if partial isolation occurs, the caterpillar propagation pattern ensures alternative pathways emerge organically. Agent-based simulations demonstrated 100% success rate under 30% packet loss, confirming the topology's anti-fragile properties.

Data Breaches: Unlike centralized systems where a single breach exposes vast amounts of data, breaches in Has-Needs are inherently limited. Data is distributed across sovereign chains; a breach would require compromising individual devices one by one. Even then, the yield would be encrypted, context-limited data shards rather than a central data trove. The Persona Manager's cryptographic NAT functionality further obscures the linkage between Personas and sovereign chains, protecting against traffic analysis.

Replay Attacks: The timestamping and cryptographic chaining of receipts prevent replay attacks. Each receipt contains a unique hash of the previous state, making historical interactions impossible to reuse in current contexts.

Man-in-the-Middle Attacks: The cryptographic handshake process and subsequent RSV verification make man-in-the-middle attacks detectable. Any attempt to intercept and alter communications would result in non-identical receipts, triggering the GreyList protocol.

This comprehensive attack resistance is not achieved through additional security layers but emerges naturally from the protocol's core architecture—a testament to the power of first-principles design.

5.2 Privacy Architecture and GreyList Protocol

Privacy in Has-Needs is a mathematical consequence of architectural design rather than a policy requirement, creating a system where privacy is preserved by default [5, 6]. This protocol-level implementation eliminates the need for user configuration or institutional enforcement.

The triplet model enforces strict data minimization by design, sharing only minimal context necessary for specific interactions [1, 2]. Entity tags are community-derived rather than personally identifiable, and state transitions record only agreement and fulfillment facts—aligning with GDPR principles but implementing them at the protocol level [19].

Has-Needs provides comprehensive metadata protection through architectural features: the Persona Manager functions as a cryptographic NAT firewall obscuring links between Personas and sovereign chains, while the Jitterbug topology's message-centric routing prevents communication pattern analysis [16, 2]. The absence of persistent network identifiers ensures ephemeral, context-specific connections—critical in crisis contexts where communication patterns alone pose significant risks [4, 7].

Privacy guarantees derive from cryptographic enforcement rather than policy mechanisms. Access to data is controlled by cryptographic API tokens that expire upon contract completion, while Zero-Knowledge Proofs and homomorphic encryption enable trustless validation without exposing underlying data [11, 16, 3].

The GreyList protocol represents a novel security approach that avoids centralized adjudication while preserving cryptographic truth [11, 2]. It triggers exclusively through cryptographic evidence of protocol violation—non-identical hashes between receipts on chains participating in the same contract. This verification process is entirely automated: when discrepancies are detected, Persona Managers initiate cryptographic cross-checking, and if hashes are confirmed non-identical, parties mutually write GreyList entries to their chains [2, 12].

GreyList entries propagate through a dedicated overlay network functioning as a warning system rather than punishment mechanism. They automatically appear during match vetting and affect the "trustable length" of a chain—how far back verifiable trust extends—while users maintain control by filtering entries from their view [11, 2].

The design incorporates redemption by affecting chain state only from the point of fault backward. Users rebuild trust through honest interactions, gradually restoring their "trustable length" [1, 2, 19]. This approach aligns with trauma-informed principles by avoiding permanent exclusion while maintaining verifiable integrity—a critical consideration in crisis contexts where individuals may make mistakes under duress [5, 7]. The system focuses on preserving cryptographic truth rather than assigning blame, creating a delicate balance previously unachieved in distributed systems [1, 18].

5.4 Comparative Analysis with Existing Systems

Table 2. Comparative analysis of Has-Needs' security and privacy properties against existing systems

Feature	**Has-Needs**	**Blockchain/DLT**	**Agent-Centric (like Holochain)**
Ledger Structure	Sovereign Chain	Global Shared Ledger	Exposed Local Ledger
Default Privacy	Yes	Limited	IP address Exposed
Auditability	Granular	Universal Public	Partial
Regulation-Aligned	Programmable	Always on	Weak to Moderate
Centralizing Features	None	Present (Validators, Mining)	DHT Bootstrap servers, IP dependency
Sybil Resistance	Structural (100%)	Economic (Variable)	Limited
Data Minimization	Protocol-Enforced	Minimal	Limited
Protected Metadata	Cryptographic NAT	Limited	Limited

Has-Needs achieves superior security and privacy properties through architectural choices rather than policy constraints—a world-first achievement in distributed coordination systems.

5.5 Legal Innovation and Real-World Security Implications

The security architecture of Has-Needs generates profound legal and regulatory implications that extend beyond technical implementation to fundamental questions of digital governance, evidence standards, and regulatory compliance in distributed systems.

5.5.1 Cryptographic Receipts as Legal Evidence

Has-Needs introduces a new category of legal evidence: cryptographically verifiable transaction receipts that provide tamper-evident proof of agreement, execution, and fulfillment without requiring trusted third-party verification [11, 2]. Each receipt contains timestamped, cryptographically signed records of contract terms, performance milestones, and completion status—creating self-authenticating evidence that meets or exceeds traditional documentary standards.

This innovation addresses a critical gap in digital evidence law, where current frameworks struggle with decentralized proof systems. Traditional legal systems assume evidence can be authenticated through institutional chain of custody or expert testimony. Has-Needs receipts are mathematically self-proving: their cryptographic signatures and cross-chain verification through RSV create evidence that cannot be forged, altered, or repudiated without detection [2, 12].

The implications for legal practice are substantial. Contract disputes can be resolved through mathematical verification rather than witness testimony or documentary interpretation. Insurance claims, regulatory compliance, and audit processes gain access to unforgeable proof of performance. Most critically for humanitarian contexts, affected populations can provide legally admissible evidence of aid delivery, resource allocation, and service provision—fundamentally altering accountability relationships [4, 7]. Governance and commerce benefit similarly while providing sovereign individuals mechanisms for accountability and compensation opportunities.

5.5.2 Programmable Compliance Architecture

Has-Needs resolves the fundamental tension between privacy rights and regulatory oversight through programmable compliance mechanisms that enable selective, consent-based disclosure without compromising systemic privacy [1, 2]. The protocol's composable API tokens create time-limited, scope-specific access grants that automatically expire upon contract completion, providing regulators with exactly the information they need while preserving user privacy for all other interactions.

This architectural approach transforms compliance from a binary choice—full transparency or complete opacity—into a granular, programmable relationship. Organizations can demonstrate regulatory compliance by exposing specific transaction categories while maintaining privacy for unrelated activities. Individuals can satisfy legal disclosure requirements without surrendering comprehensive data access rights. Uniquely, indigenous communities are able to protect and conditionally release cultural wisdom as they see fit, and only with documented value exchange.

The system enables "compliance by design" where regulatory requirements are embedded into smart contract logic rather than imposed through external oversight. GDPR's right to be forgotten becomes technically enforceable through automatic data deletion clauses. HIPAA's minimum necessary standard is implemented through cryptographic access controls that prevent information leakage [19].

5.5.3 Regulatory Framework Challenges and Innovations

Deploying Has-Needs in regulated environments exposes fundamental assumptions in current legal frameworks that assume centralized auditability, institutional custody of records, and hierarchical enforcement mechanisms [1, 2]. These assumptions create regulatory friction for systems based on individual sovereignty and distributed verification.

Current financial regulations, for example, typically require institutions to maintain complete transaction records and provide unrestricted regulatory access. Has-Needs' architecture distributes these records across individual sovereign chains, creating a mismatch between regulatory expectations and technical implementation. However, the system's superior auditability provides stronger assurance than traditional institutional custody is capable of [11, 2].

This creates opportunities for regulatory innovation. Legal recognition of cryptographic receipts as primary evidence would reduce reliance on institutional intermediaries while improving verification standards. User control of granular, on-demand API access, is a completely new model of privacy.

The protocol's anti-fragile security properties also enable new approaches to regulatory oversight. Rather than requiring continuous monitoring of centralized systems, regulators could focus on spot-checking cryptographic integrity and investigating discrepancies detected through the GreyList mechanism. This shifts regulatory burden from preventive surveillance to responsive investigation—a model that may prove more effective while being less invasive.

5.5.4 International Humanitarian Law and Digital Rights

Has-Needs' architecture aligns with emerging theories of digital rights and humanitarian protection, particularly the principles articulated in the Signal Code and similar rights-based approaches to information during crisis [1]. By making data sovereignty technically enforceable rather than merely aspirational, the protocol operationalizes international humanitarian law principles that emphasize affected population agency and self-determination.

The system's ability to generate evidentiary-quality proof of aid delivery and resource allocation has particular significance for accountability mechanisms in humanitarian response. Traditional systems rely on self-reporting by implementing organizations, creating potential conflicts of interest. Has-Needs enables affected populations to generate their own verifiable records of aid received, service quality, and unmet needs—fundamentally altering power dynamics in accountability relationships [7, 19] while providing a level of detail and timeliness that is unprecedented worldwide.

This shift requires legal systems to adapt to scenarios where individuals possess stronger evidentiary capabilities than institutions. Current frameworks for humanitarian accountability assume institutional information advantages; Has-Needs inverts this relationship by providing communities with cryptographically superior documentation of their experiences and needs at no-cost and low-effort.

The protocol thus represents not just technical innovation but legal evolution—establishing new standards for evidence, consent, and accountability that preserve individual agency while surpassing current institutional requirements for verifiable coordination. This legal innovation may prove as significant as the technical architecture in determining the protocol's real-world impact.

6. Methods and Architectural Validation

The Has-Needs protocol operates through a deterministic sequence inherent to its foundational architecture. The protocol mechanics follow a precise progression where a triplet resource claim ([Entity, State, Context]) propagates through the peer network via the Jitterbug topology, undergoes cryptographic resolution through Recursive Sovereign Verification (RSV), and records outcomes on sovereign chains. Event logging, trust assessment, and sovereignty verification emerge directly from the protocol's minimal rules rather than external algorithms.

The Jitterbug transform functions as a geometrically-bounded topological reconfiguration layer derived from Fuller's geometric transformation sequence [16]. It enables resilient peer discovery through message-centric state propagation, with network behavior governed by strict geometric constraints (5-12 connections) that reduce clustering while maintaining robust connectivity. This biomimetic approach creates inherent resilience by emulating the self-regulating properties of biological systems [5, 6], where pathway adaptation occurs through local stimuli rather than global knowledge.

The evaluation methodology recognizes a fundamental category difference between Has-Needs and legacy systems: the former operates on a machine-readable, semantically precise triplet ontology ([Entity, State, Context]), while the latter attempts to infer meaning from unstructured human language [1, 2, 19]. This distinction is architectural, not performance-based—the protocol eliminates entire classes of problems (ambiguity, misinterpretation, bias) through its structural design, with any efficiency gains emerging as natural consequences of this clarity.

The protocol's validation centers on demonstrating how its minimal primitives generate four essential properties that emerge directly from the architectural choices:

- Triplet offers semantic precision, eliminating the need for reconciliation infrastructure [1, 2]

- RSV achieves certainty through cryptographic lineage rather than global consensus [11, 2]
- The Jitterbug topology enables organic failover through geometric self-regulation [16]
- The GreyList preserves cryptographic truth without centralized adjudication [11, 2]

This deterministic architecture—where complex coordination emerges from three simple states (Has/Need/Working) and geometrically-bounded network behavior—transforms what are typically system vulnerabilities (ambiguity, central points of failure, metadata exposure) into structurally impossible conditions [2, 12].

7. Evaluation and Structural Benefits

The Has-Needs protocol establishes verifiable trust, data sovereignty, and semantic clarity as inherent architectural properties rather than simulation-dependent outcomes. This section demonstrates how the protocol's minimal primitives generate essential structural benefits that fundamentally transform coordination systems.

7.1 Structural Properties of the Architecture

Ontological emergence is an architectural certainty within Has-Needs. The triplet model ([Entity, State, Context]) enables a community-owned ontology to form naturally from user declarations without centralized curation [5, 6]. Resource tags like water_potable and generator_5kw emerge through usage patterns rather than top-down imposition, creating semantic precision through bilateral cryptographic agreements. This eliminates the reconciliation infrastructure required by legacy systems, where meaning must be inferred from unstructured data [1, 2].

Sybil resistance is structurally guaranteed by the protocol's design. The GreyList mechanism combined with RSV ensures that trust is an earned, verifiable property of cryptographic lineage [11, 2]. Malicious actors cannot fabricate verifiable history, as trust emerges from the web of cryptographic receipts across sovereign chains—making Sybil attacks operationally irrelevant rather than merely detectable [2, 12].

Network anti-fragility is an inherent property of the Jitterbug topology's geometric constraints (5-12 connections) [16]. The message-centric propagation model with OPEN/COMPRESSED state transitions enables organic pathway adaptation without global knowledge or routing tables. This biomimetic design ensures network resilience through controlled oscillation between states, with the message's open_level serving as the precise indicator of required pathway expansion [16].

Verifiable fidelity is architecturally enforced through sovereign chains and cryptographic receipts [2, 12]. Every contract execution generates an immutable, identical receipt recorded on all involved chains, creating mathematical certainty through RSV rather than probabilistic consensus [11]. The precise permissions of composable API tokens govern all actions, transforming coordination from a matter of faith to verifiable fact without requiring global transparency.

7.2 Structural Applications

Has-Needs delivers a paradigm shift in coordination by centering individual sovereignty and verifiable action, not data centralization. Its Has/Need/Working mechanism, Jitterbug topology, and Recursive Sovereign Verification eliminate structural ambiguity and inefficiency, providing inherent trust, semantic rigor, and agency.

Rather than walk through extended scenarios, all workflows—disaster relief, resource exchange, or mutual aid—follow the same core logic: verifiable, closed-loop value exchange anchored in sovereign, cryptographically auditable transactions. Architectural details in previous sections describe how each protocol layer enforces auditability and resilience at every step.

Going forward, the priority is real-world pilots, policy reforms recognizing cryptographic receipts, and formal security proofs. Has-Needs opens the path to truly self-sovereign, context-agnostic digital ecosystems.

8: DISCUSSION

The simulation results validate not just performance metrics but a new architectural philosophy. Has-Needs demonstrates that trust, efficiency, equity, and resilience can emerge as properties of a minimal, sovereign-first structure—a fundamental departure from dominant digital coordination paradigms.

8.1 The Structural Shift: From Mediated Consensus to Sovereign Verification

Traditional systems, including blockchains and federated identity models, manufacture trust through resource-intensive consensus algorithms or institutional verifiers. These systems inherently centralize power and create dependency on third parties to vouch for truth.

Has-Needs operates on sovereign verification. It assumes no trust a priori but provides minimal cryptographic primitives—the data triplet, peer-receipt, and GreyList—that make verifiable interaction the rational choice. Trust is continuously earned and verified with each interaction, scoped precisely to that context. This aligns with biomimetic principles: cells react to verifiable chemical signals rather than "trusting." The protocol's Sybil resistance and verifiability directly result from this shift.

8.2 The Ontological Shift: From Interpreted Data to Sovereign Fact

Current data paradigms rely on extraction, central storage, and algorithmic interpretation—a process fraught with ambiguity and context loss.

Has-Needs introduces sovereign fact. The triplet model [Entity, State, Context] ensures data is born machine-readable and semantically precise. Meaning is negotiated and agreed upon cryptographically at contract formation. The emergent ontology reflects bilateral agreements, eliminating the need for interpretation and reconciliation infrastructure. The efficiency gains come not from faster matching but from architecting away traditional matching algorithms entirely.

8.3 Predictive Biomimetics in Practice

"Predictive biomimetics" describes a system designed to yield emergent behaviors through structural conditions, not direct programming. The Jitterbug topology functions as a natural system: its dynamic states (OPEN/COMPRESSED) use local stimuli to route resources, mirroring biological processes. The system doesn't predict needs; it creates conditions where needs and resources find each other efficiently. We engineer the structure—from which outcomes predictably emerge—rather than the outcomes themselves.

8.4 Privacy and Legal Considerations

Has-Needs advances privacy-respecting coordination by design:

- No Global Ledger: Transactional data remains local, shattering surveillance models.
- No Network Exposure: No requirement to disclose IP addresses or network identifiers.
- No Central Points of Failure: Free of bootstrapping nodes or privileged validators.

The protocol enables evidentiary-quality provenance with granular consent through programmable APIs. By decoupling disclosure from universal transparency, it resolves the privacy-compliance tension: organizations can expose only minimum required records while maintaining verifiability.

Deploying in regulated fields requires policy innovation, as legal norms often assume central auditability. Has-Needs establishes a new paradigm compatible with privacy mandates and accountability standards, challenging frameworks based on hierarchical trust.

8.5 Implications for Design

Has-Needs provides a new design pattern for human-centric systems. Rather than the top-down approach of defining system intelligence and forcing conformity, it demonstrates a bottom-up generative approach. The design directive is simple: create minimal rules for sovereign agents (triplet, state machine, receipt) and let system intelligence emerge from verified interactions. This suggests building digital societies not by designing laws, but by designing the fundamental physics of interaction. The architect's role shifts from central planner to gardener, cultivating conditions for healthy growth.

9: LIMITATIONS, CONTEXT, AND FUTURE WORK

9.1 Structural Considerations in Humanitarian Coordination

Has-Needs introduces a structural approach to humanitarian coordination that centers value, control, and provenance at the individual level. By design, the protocol creates architectural conditions where data sovereignty and peer-to-peer coordination are inherent properties, addressing long-recognized challenges in the humanitarian sector.

Over the past decade, thoughtful analyses have identified persistent challenges within humanitarian response: sectoral fragmentation [14], institutional information sharing barriers, and concerns regarding data practices that may unintentionally disempower affected populations while creating institutional oversight challenges [1, 17]. These observations reflect not failures of intent but rather the structural characteristics of prevailing coordination models.

The current architectural paradigm—where information flows unidirectionally from field to headquarters—has naturally shaped the technological solutions developed within the sector. Many well-intentioned innovations, including semantic analytics, drone-based assessment tools, and centralized dashboards, have emerged to address specific operational needs within this framework [19]. However, as scholars have noted, these approaches can sometimes reinforce existing information asymmetries rather than creating truly bidirectional communication channels [19].

Has-Needs represents a complementary approach that builds upon these insights while introducing a different architectural foundation. Rather than operating within the existing paradigm, the protocol is designed from first principles to enable value generation and retention at the individual level. The protocol's architecture intentionally eliminates technical pathways for non-consensual data extraction while preserving institutional capacity for verifiable coordination.

This design choice directly addresses concerns raised by researchers regarding data practices in humanitarian contexts [1, 13, 19]. By making data sovereignty a protocol-level guarantee rather than a policy constraint, Has-Needs creates conditions where the valuable insights institutions require emerge organically from voluntary, consented interactions rather than extraction. The result is a coordination framework that simultaneously supports institutional accountability and individual agency—a balance that has proven challenging to achieve within existing architectural constraints.

This approach does not negate the important contributions of existing humanitarian technologies but rather offers a complementary framework designed to address structural limitations that have persisted despite good-faith efforts to improve coordination practices. By shifting from a model of data extraction to one of data generation through sovereign interaction, the protocol creates new possibilities for verifiable, equitable digital coordination in crisis contexts.

9.2 Future Work and Path Forward

Transitioning Has-Needs from concept to real-world impact requires integrated development across technical, empirical, policy, and collaborative domains. Immediate priorities include piloting the protocol in partnership with international humanitarian organizations, local community projects, and farming collectives in Africa, as well as with domestic emergency managers. Participation in notable humanitarian training exercises, such as those conducted by HHI, will further ground validation efforts.

These "living labs" and collaborative deployments will provide empirical evidence of utility, foster community ownership, and establish precedents for broader humanitarian and disaster response applications. Technical advancement will focus on formal verification of critical primitives (e.g., GreyList, privacy-preserving ontologies), secure enclave Persona Manager implementation, and establishing interoperability standards. Parallel policy work is needed to secure legal recognition for cryptographic receipts, develop regulatory frameworks for programmable compliance, and create community-driven ethical guidelines. By integrating technical refinement, partnership-driven field validation, and policy innovation, Has-Needs moves from theoretical innovation to practical transformation—restoring agency and building resilience in digital coordination systems.

10: CONCLUSION

Has-Needs marks a foundational shift in digital coordination, replacing data centralization with individual sovereignty and verifiable action. Its core innovations—the Has/Need/Working triad, biomimetic Jitterbug topology, and Recursive Sovereign Verification—make ambiguity, inefficiency, and extractive trust structurally impossible.

Inherently providing verifiable trust, semantic clarity, and sovereignty, Has-Needs is a context-independent framework that restores agency and enables auditable collaboration through transparent, sovereign transactions.

The next steps are clear: implement community-led pilots, advance policy to treat cryptographic receipts as legal evidence, and pursue formal verification of security primitives. Has-Needs aims to establish a paradigm where sovereignty is protocol-enforced, ushering in digital ecosystems that serve individuals, not institutions.

REFERENCES

[1] Harvard Humanitarian Initiative (2017). Signal Code: A Human Rights Approach to Information During Crisis. Harvard Humanitarian Initiative.

[2] Peter R. Taylor & Mark J. Howard (2020). Information Sovereignty in Humanitarian Action. World Disasters Report, IFRC.

[3] William B. Miller (2022). Bioverse: How the Cellular World Contains the Secrets to Life's Biggest Questions. BenBella Books.

[4] William B. Miller (2023). Cognition-Based Evolution: Natural Cellular Engineering and the Intelligent Cell. World Scientific.

[5] George A. Bonanno (2004). Loss, trauma, and human resilience: Have we underestimated the human capacity to thrive after extremely aversive events? American Psychologist, 59(1), 20-28.

[6] Thomas E. Drabek (2018). The Human Side of Disaster (2nd ed.). CRC Press.

[7] Thomas Hardjono, Alex Lipton, & Alex Pentland (2019). Towards a Design Philosophy for Interoperable Blockchain Systems.

[8] Adrian Tobin & Daniel Reed (2016). The inevitable rise of self-sovereign identity. The Sovrin Foundation.

[9] Kristin Sandvik & Kjersti Jumbert (2016). The Good Drone: Imagining the Drone as a Technology of Humanitarianism.

[10] Davide Rigoni, Stephanie Braem, Gilles Pourtois, & Marcel Brass (2020). Helplessness experience and intentional (un-)binding: Control deprivation disrupts the implicit sense of agency. Journal of Experimental Psychology: General.

[11] Stefano Dutto, Daniela Margaria, Claudia Sanna, & Alessandro Vesco (2022). Toward a Post-Quantum Zero-Knowledge Verifiable Credential System for Self-Sovereign Identity. Cryptology ePrint Archive, Paper 2022/1291-7.

[12] Annalisa De Salve, Dario Di Francesco Maesa, Paolo Mori, Laura Ricci, & Alessandro Puccia (2023). A multi-layer trust framework for self-sovereign identity on Blockchain. Online Social Networks and Media, 37-38.

[13] Rebecca Burns (2015). Moments of Closure in Crowdsourcing Practices for Disaster Response: Learning from Occupy Sandy. GeoJournal, 80(4), 569-585.

[14] Martijn J. C. van den Homberg, Yola Georgiadou, & A. Natsema (2017). Connecting grassroots communities and humanitarian actors with information and communication technology: Lessons from the 2014 West African Ebola outbreak. ISPRS International Journal of Geo-Information, 6(7), 204.

[15] Matthew Zook, Mark Graham, Taylor Shelton, & Sean Gorman (2010). Volunteered Geographic Information and Crowdsourcing Disaster Relief: A Case Study of the Haitian Earthquake. World Medical & Health Policy, 2(2).

[16] Richard Buckminster Fuller (1975). Synergetics: Explorations in the Geometry of Thinking. Macmillan.

[17] Kristin B. Sandvik, Maria Gabrielsen Jumbert, John Karlsrud, & Mareile Kaufmann (2014). Humanitarian technology: a critical research agenda. International Review of the Red Cross, 96(893), 199-242.

[18] Harvard Humanitarian Initiative (2011). Disaster Relief 2.0: The Future of Information Sharing in Humanitarian Emergencies. UN Foundation & Vodafone Foundation.

[19] Sibel Celik & Sinan Corbacioglu (2010). Role of information in disaster management: a case study of 2010 Haiti Earthquake. Natural Hazards, 100(2), 583-605.

[20] Jiahua Zhao, Zhen Wang, Nicholas LePan, Yulin Liu, & Yinhong Zhao (2024). Analyzing voting power in decentralized governance: Who controls DAOs? Information Processing & Management, 61(4), 103718.

Author

Om Goeckermann is an inventor whose work on the Has-Needs protocol is grounded in over a decade of frontline humanitarian experience. A former combat crew member, rescue paramedic, indigenous rights and social justice activist, he first proposed the core concept of Has-Needs at the 2010 Haiti earthquake hackathons and also during the Harvard Humanitarian Initiative field exercise in 2012. As an original member of the Standby Task Force (SBTF) and crisis mapper, he served as SMS coordinator for the Uchaguzi initiative during the 2013 Kenyan elections, and received the Presidential Volunteer Service Award for crisis mapping with the GIS Corps. To ensure Has-Needs was informed by a deep understanding of human nature, he pursued degrees in emergency management, psychology, and sociology to inform his sovereignty-preserving project.