omxus

LICENSE TO POWER

Omxus: A Sovereign Infrastructure for Direct Democracy and Universal Justice

January 2026

Abstract

A sovereign digital infrastructure is proposed that eliminates intermediary governance through direct democratic participation, prevents crime through universal voluntary response networks, and ensures justice through structural accountability rather than punitive enforcement. The system employs a non-transferable identity token anchored to physical NFC hardware, with sybil resistance achieved through in-person vouching by existing participants. Network resilience is provided through mesh topology operating independently of centralised internet service providers, with cryptographic anchoring to the Bitcoin network via RGB protocol. The architecture embodies four principles derived from medical ethics: autonomy, non-maleficence, beneficence, and justice defined as prevention only.

1. Introduction

Contemporary governance systems operate through representative intermediaries who concentrate decision-making power in institutions vulnerable to capture, corruption, and unilateral action against the interests of constituents. The dismissal of the Whitlam government in Australia (1975) demonstrates the structural fragility of representative democracy: a single unelected actor terminated an elected government without consultation, communication, or recourse. The population had no mechanism to respond.

Modern digital infrastructure compounds these vulnerabilities. Internet access depends on corporate intermediaries (ISPs) operating under state jurisdiction. Identity verification requires centralised authorities. Communication channels can be severed. The technical architecture of contemporary society enables the same pattern: isolate, then act.

Meanwhile, commercial platforms demonstrate that frequent, large-scale coordination is technically feasible. Social networks coordinate billions of daily interactions. Yet governmental democratic participation remains constrained to infrequent elections, with policy decisions delegated to representatives whose expertise rarely matches the domains they govern.

This paper proposes Omxus: infrastructure for direct democratic governance, crime prevention through universal voluntary response, and dispute resolution through mandatory perspective

exchange. The system requires no trusted intermediaries, operates on mesh networks independent of ISP infrastructure, and anchors identity and decisions to the Bitcoin blockchain via RGB protocol.

2. Foundational Principles

The system architecture derives from four principles established in medical ethics, adapted for governance infrastructure:

Autonomy. Self-sovereign identity. Individuals control their own cryptographic keys, data, and participation. No entity can revoke identity or access without consensus of the vouching network.

Non-maleficence. The system cannot be weaponised against its participants by design. No surveillance apparatus. No punishment infrastructure. No mechanism exists within the protocol to harm users.

Beneficence. Access to information, communication, and democratic participation as baseline rights. The network exists to serve human flourishing.

Justice (prevention only). No punitive architecture. The system prevents harm through structural design and universal witness, not through punishment after the fact. Justice is redefined as the prevention of injustice, not retribution for it.

3. Identity Layer

3.1 The Omxus Token

Each participant holds exactly one non-transferable token representing verified human identity. The token is not currency; it is proof of personhood and membership in the network. One human, one token. The token cannot be bought, sold, or delegated.

The token is anchored to a physical NFC ring worn by the participant. The ring stores the private key for the participant's decentralised identifier (DID). All actions requiring identity verification—voting, emergency response activation, dispute registration—require physical presence of the ring.

3.2 Sybil Resistance Through In-Person Vouching

The central problem of decentralised identity is sybil resistance: preventing one human from creating multiple identities. Existing solutions rely on biometrics (centralised storage vulnerabilities), proof-of-work (plutocratic), or trusted authorities (single points of failure).

Omxus employs a web-of-trust model with physical verification. To receive a token, a prospective participant must be vouched for by three existing token holders. Vouching must occur in person, with physical co-presence verified through device proximity (NFC handshake, QR code exchange, or equivalent).

The vouching event is recorded as a signed attestation from each voucher, timestamped and eventually anchored to Bitcoin. Vouchers accept ongoing responsibility: if a vouched participant is demonstrated to be a sybil (same human holding multiple tokens), the vouchers' reputation is affected proportionally.

3.3 Proximity Weighting

Tokens are not equally weighted in all contexts. Influence on decisions is proportionally linked to proximity—geographic, social, and domain-specific. A participant's vote on local infrastructure carries more weight if they live in the affected area. Technical decisions weight toward those with demonstrated expertise in the relevant domain.

Proximity is determined through multiple signals: physical location history (derived from mesh network topology, not surveillance), vouching relationships (social graph distance), and participation history (demonstrated engagement with specific domains). This prevents both tyranny of the majority (distant populations overruling local concerns) and capture by special interests (small groups dominating decisions that affect many).

The weighting function is quadratic: influence decreases with the square of distance, ensuring that those most affected by decisions have the strongest voice while preserving universal participation rights.

3.4 Genesis Ceremony

The network bootstrap requires an initial set of participants who cannot be vouched for by existing members (as none exist). The genesis ceremony addresses this through collective attestation.

Three initial vouchers assemble nine prospective participants. The ceremony is filmed, with each participant's face, ring, and public key visible. The video is hashed and anchored to the Bitcoin blockchain. This hash becomes the root of the social contract—publicly verifiable, immutable, and tied to identifiable humans who have staked their reputations on the network's integrity.

Subsequent participants are vouched through the standard three-voucher process, creating an expanding web of trust rooted in the genesis event.

3.5 Ring Hardware Specifications

The Omxus ring is a wearable NFC device containing a secure element for cryptographic key storage. The secure element is tamper-resistant: attempts to extract the private key destroy it. The ring has no battery; it is powered inductively during NFC communication.

Core specifications: ISO 14443-A/B NFC interface operating at 13.56 MHz; secure element meeting Common Criteria EAL5+ certification; storage for primary DID key pair and backup recovery shards; water resistance to IPX8; medical-grade hypoallergenic materials (titanium or ceramic); size range covering 95th percentile of adult finger dimensions.

The ring performs only signing operations. It cannot be interrogated remotely, does not broadcast, and stores no data beyond the cryptographic keys. All transaction data resides on the participant's device; the ring merely authorises actions.

3.6 Ring Loss and Recovery

Ring loss does not mean identity loss. At vouching, the participant's three vouchers each receive an encrypted recovery shard. These shards, when combined, can authorise transfer of identity to a new ring. No single voucher can recover the identity alone; collusion of all three is required.

Recovery process: the participant physically meets with at least two of their three original vouchers. Each voucher provides their shard and re-vouches for the participant's identity. The shards authorise minting of a new ring with a rotated key pair. The old ring's key is revoked network-wide.

If vouchers are unavailable (deceased, unreachable), the participant may petition for recovery through community attestation: a larger group (minimum seven) of network participants who can verify identity through direct knowledge must collectively vouch. This slower path prevents rapid sybil recovery while ensuring no participant is permanently locked out.

3.7 Death and Incapacitation

Upon death, a participant's token is not destroyed but transitioned to memorial status. The identity remains in the social graph (preserving vouching relationships for historical integrity) but loses voting rights and emergency activation capability. Transition to memorial status requires attestation from vouchers or next-of-kin, plus a defined period of inactivity.

For incapacitation (medical, legal, or voluntary), participants may pre-designate a guardian relationship. Guardians can vote on behalf of the incapacitated participant but cannot alter identity, transfer tokens, or revoke vouching relationships. Guardian actions are publicly logged and revocable upon recovery of capacity.

3.8 Children and Onboarding Age

Full token participation requires demonstrated capacity for autonomous decision-making. The network does not impose a global age threshold; instead, vouchers attest to the prospective participant's readiness. Vouchers stake their reputation on this attestation as with any other vouching.

Children may hold provisional tokens granting access to communication and emergency response but not voting or ViewSwap obligations. Provisional tokens are linked to guardian tokens. Transition to full participation requires standard three-voucher attestation, which may include but need not be limited to guardians.

This model respects developmental variation across cultures and individuals while preventing both premature enfranchisement and arbitrary exclusion based on calendar age alone.

4. Direct Democracy

4.1 Elimination of Representative Intermediaries

Representative democracy emerged from communication constraints: citizens could not practically participate in every decision, so they delegated authority to representatives. These constraints no longer exist. Digital infrastructure enables real-time, large-scale coordination.

Omxus eliminates the politician as a role. Policy decisions are made directly by affected participants. Technical implementation is delegated to domain experts (engineers build roads, medical professionals design health policy) who are accountable to direct democratic oversight, not electoral cycles.

4.2 Voting Mechanics

Proposals enter the system through participant submission. Any token holder may submit a proposal. Proposals require a minimum endorsement threshold (signatures from other participants) to proceed to voting, preventing spam while ensuring accessibility.

Voting windows are defined per proposal, with duration proportional to scope: local matters may resolve in days; constitutional changes require extended deliberation periods. Quorum requirements scale with affected population: a neighbourhood decision requires neighbourhood-level participation; network-wide changes require network-wide quorum.

Votes support multiple expression types: binary (yes/no), ranked choice (preference ordering), quadratic (diminishing returns on strong preferences), and approval (acceptable/unacceptable for multiple options). The appropriate voting type is specified in the proposal and may be challenged during the endorsement phase.

Votes are cryptographically signed by the participant's ring, timestamped, and stored locally before network propagation. This ensures votes cannot be lost to connectivity failures. When the device eventually reaches another node, votes propagate and eventually anchor to Bitcoin via RGB.

4.3 Local Meetings

Digital participation is supplemented by physical assembly. Local meetings provide space for deliberation that text-based systems cannot replicate. Participants gather to discuss proposals, hear perspectives, and form considered opinions before casting votes.

Meeting attendance is recorded through NFC proximity verification among attendees, creating a record of deliberative participation without mandating specific outcomes.

5. Communication System

5.1 Unseverable Communication

The communication layer ensures that no participant can be silenced. Messages are signed by the sender's ring, encrypted end-to-end for the recipient, and propagated through the mesh network. No central server routes or stores messages; every participant's device is a potential relay.

Message properties: sender authentication (cryptographically verified), recipient privacy (end-to-end encryption), non-repudiation (sender cannot deny sending), persistence (messages store-and-forward until delivered), and resilience (multiple routing paths).

5.2 Broadcast and Group Communication

Beyond point-to-point messaging, the system supports broadcast channels and group communication. Any participant may create a broadcast channel; others subscribe voluntarily. Group chats employ multi-party encryption where membership changes rotate keys automatically.

Emergency broadcasts propagate network-wide with priority routing. These are reserved for genuine emergencies (natural disasters, coordinated threats) and abuse is socially sanctioned through reputation effects on the broadcaster.

5.3 Offline Message Handling

Messages for offline recipients are stored by their social graph neighbours (vouchers and those they have vouched). When the recipient reconnects, pending messages are delivered from multiple sources, ensuring redundancy. Message expiry is configurable by sender; expired undelivered messages are purged.

6. Crime Prevention Through Universal Response

6.1 The Prevention Principle

Contemporary justice systems are primarily punitive: harm occurs, then the system responds with punishment intended to deter future harm. This approach fails empirically (recidivism rates demonstrate limited deterrent effect) and ethically (punishment does not undo harm to victims).

Omxus inverts this model. Justice is prevention only. The system is designed such that harmful actions cannot occur, or are interrupted before completion, rather than punished afterward.

6.2 Universal Voluntary Response Network

All token holders agree, as a condition of participation, to respond to emergency activations within their proximity. This mirrors the volunteer firefighter model common in regional areas: community members who maintain normal occupations but respond when needed.

When a participant activates an emergency through their ring, all nearby token holders are notified. The density of the network ensures rapid response: if every person is a potential responder, response time approaches zero.

This creates structural prevention: the commission of harm requires isolation of the victim from witnesses and responders. Universal network participation eliminates this isolation. Crime becomes impractical not because punishment is severe, but because completion is impossible.

6.3 Accountability Without Punishment

Actions within the network are cryptographically signed. Participants cannot deny actions they have taken (non-repudiation). This creates accountability through transparency: the truth of what occurred is structurally guaranteed, eliminating disputes of fact.

Where harmful intent is demonstrated, the response is not punishment but intervention: mandatory participation in ViewSwap (Section 7), community support for addressing underlying causes, and if necessary, restriction of network privileges through voucher consensus.

7. ViewSwap: Dispute Resolution Through Perspective Exchange

7.1 Mechanism

When disputes cannot be resolved through deliberation, participants engage in ViewSwap: a mandatory exchange of circumstances for a defined period (typically one week). Each party lives the other's life—their home, their routine, their constraints.

The mechanism is designed to create embodied understanding that argument cannot achieve. Most disputes arise from failures of empathy—inability to comprehend the other party's constraints, pressures, and perspective. ViewSwap makes this comprehension unavoidable.

7.2 Worked Example

Consider a dispute between a factory operator and nearby residents over noise pollution. Standard resolution mechanisms (legal action, regulation) are adversarial and slow. ViewSwap proceeds as follows:

The factory operator lives in the resident's home for one week, experiencing the noise at all hours. The resident shadows the factory operator, understanding the production constraints, employee livelihoods, and economic pressures involved. Both parties maintain logs, verified by ring signatures.

Following the exchange, both parties reconvene with mediators (randomly selected network participants). Resolution emerges from shared understanding: perhaps operational hours shift, sound barriers are installed, or compensation structures are established. The solution is co-created by parties who now viscerally understand each other's position.

7.3 Deterrent Effect

ViewSwap functions primarily as deterrent. The obligation to experience another's circumstances discourages frivolous disputes and incentivises good-faith resolution before escalation. Participants approach conflicts knowing they may be required to inhabit the other party's position.

7.4 Obligation and Duty

Participation in ViewSwap when triggered is a non-negotiable obligation of token holding. This duty is accepted at the moment of vouching and cannot be subsequently declined. The network depends on mutual commitment to perspective exchange as the ultimate dispute resolution mechanism.

8. Technical Architecture

8.1 Network Layer

The network operates on Yggdrasil, an encrypted IPv6 mesh network. Each device receives a cryptographic address and routes traffic through available paths—internet where available, direct device-to-device connections where not. The network self-heals around failures and cannot be disabled through any single point of control.

Peer discovery employs Hyperswarm, enabling devices to locate each other and establish connections through firewalls and network address translation. Participants with internet access

serve as gateways to the broader network for those without, distributing access rather than concentrating it.

8.2 Gateway Mechanics and Incentives

Participants with internet connectivity may operate as gateways, routing traffic between the mesh network and the public internet. Gateway operation is voluntary but incentivised through reputation: gateway uptime and bandwidth contribution are recorded and visible in the participant's public profile.

Gateway selection employs distributed trust scoring. Traffic routes through gateways with established reputation, preventing malicious actors from intercepting communications by operating rogue gateways. Multiple gateways are used simultaneously where available, with traffic split to prevent any single gateway from observing complete communication patterns.

No monetary payment for gateway operation exists by design. The incentive is purely social: gateway operators are recognised as infrastructure contributors, and this contribution factors into proximity weighting for network governance decisions.

8.3 Content Mirroring

Critical public information is cached and replicated across the network using IPFS (InterPlanetary File System). Content is addressed by cryptographic hash, ensuring integrity: content cannot be modified without detection. Popular content naturally distributes across many nodes; critical content (reference documents, educational materials, emergency procedures) is pinned by community consensus.

When a participant requests content unavailable locally, the request propagates through the mesh. Any node holding the content may serve it. This creates a censorship-resistant library: content cannot be removed without purging it from every node that holds a copy.

8.4 Physical Fallbacks

When digital communication fails entirely, physical fallbacks ensure continuity. The network defines three fallback layers:

LoRa (Long Range) radio: Low-bandwidth, long-range communication (kilometers) without infrastructure. Sufficient for text messages, emergency alerts, and vote transmission. Devices with LoRa capability form a secondary mesh when primary connectivity fails.

HF Radio: High-frequency radio signals bounce off the ionosphere, enabling global communication without any infrastructure. Bandwidth is minimal (text only), but reach is unlimited. Amateur radio operators within the network maintain HF capability for extreme scenarios.

Sneakernet: Physical transport of data on devices. Participants may carry encrypted data bundles to be synchronised upon reaching connected nodes. This method is slow but unstoppable—it is how samizdat literature circulated under Soviet censorship.

For voting specifically, a final fallback exists: printed QR codes encoding signed votes. A participant may print their cryptographically signed vote, and any other participant who scans it can submit it to the network. The vote is valid regardless of how it reaches the network.

8.5 Data Layer

Data synchronisation employs Hypercore, an append-only log structure enabling offline-first operation. Participants create signed records locally; records propagate through the network as connectivity allows. Conflict-free replicated data types (CRDTs) ensure that devices synchronising after periods of disconnection merge state deterministically without central coordination.

Critical records (votes, identity attestations, dispute records) are periodically anchored to the Bitcoin blockchain via RGB protocol. RGB enables smart contract functionality on Bitcoin's UTXO model without requiring a separate blockchain or token. Anchored records are immutable and independently verifiable by any party with Bitcoin access.

8.6 Identity Layer

Identity employs W3C Decentralised Identifiers (DIDs). Each participant controls a DID anchored to their NFC ring's secure element. The ring stores the private key; the public key and attestations are distributed through the network.

Authentication requires physical ring presence. No passwords, no centralised identity providers, no CAPTCHAs. Identity is proven through cryptographic signature from a key that requires physical hardware to access.

8.7 Resilience Properties

The architecture provides resilience against the failure modes that enable authoritarian intervention:

No ISP kill switch: mesh routing bypasses centralised infrastructure. No server to seize: data is replicated across all participants. No database to corrupt: each participant maintains an independent copy, with Bitcoin anchoring providing ultimate verification. No company to pressure: no legal entity operates the network. No identity to revoke: DIDs are self-sovereign and cannot be disabled by external authority.

9. Privacy and Accountability Balance

9.1 The Tension

Accountability requires traceability: actions must be attributable to actors. Privacy requires opacity: actors must control what others can observe about them. These principles exist in tension. Omxus resolves this tension through context-dependent disclosure.

9.2 Action Categories

Public actions (voting, proposals, public statements) are permanently attributable. Participants cannot vote anonymously; democratic accountability requires visible commitment to positions. This prevents both vote manipulation and the social corrosion of anonymous political discourse.

Private actions (personal communications, movement, transactions) are encrypted and visible only to directly involved parties. The network routes these actions but cannot inspect them. Location data, in particular, is never broadcast; proximity detection operates through local device-to-device communication without central logging.

Disputed actions may be revealed through ViewSwap proceedings or community arbitration, but only with the consent of involved parties or through established dispute resolution processes. Revelation is targeted and temporary, not surveillance.

9.3 No Surveillance Architecture

The system is architecturally incapable of mass surveillance. No central server collects data. No entity has visibility into all network traffic. Even protocol developers cannot observe private communications because the cryptographic design makes this impossible, not merely prohibited.

This is non-maleficence implemented technically: the system cannot be weaponised against users because the capability does not exist, regardless of who controls it.

10. Threat Model and Attack Vectors

10.1 Voucher Collusion

Three colluding individuals could vouch for non-existent persons (sybils), creating fraudulent voting power. Defence: voucher responsibility is transitive and reputational. If sybils are detected, all vouchers in the chain to the genesis ceremony suffer reputation penalties. Deep collusion (many generations of fraudulent vouching) becomes expensive as reputation costs compound.

Additionally, statistical analysis of vouching patterns can detect anomalies: legitimate vouching follows social graph patterns (friends vouch friends); fraudulent vouching creates artificial clusters. Anomaly detection triggers community investigation.

10.2 State-Level Attacks

A hostile state may attempt to disrupt the network through infrastructure attacks, participant targeting, or mass sybil creation.

Infrastructure attacks (internet shutdown, device seizure) are mitigated by mesh topology and physical fallbacks. No single infrastructure component is critical. Participant targeting (arrest, coercion) cannot compromise the network because no participant holds special privileges; there are no administrators to target.

Mass sybil creation requires in-person vouching, limiting the rate at which state actors can inject false identities. Detection mechanisms described above apply. The genesis ceremony's public nature makes it impossible to create a parallel fraudulent network without detection.

10.3 Social Attacks

Coordinated disinformation, manipulation of deliberation, and strategic voting present social rather than technical threats. The system provides infrastructure; it cannot prevent humans from misleading each other.

Mitigations include: transparent vote records (manipulation patterns become visible), local meeting requirements (face-to-face deliberation is harder to manipulate at scale), and ViewSwap (perspective exchange counteracts dehumanisation that enables manipulation).

10.4 Ring Theft and Coercion

A stolen ring could be used to impersonate the victim. Mitigation: high-stakes actions (large-scope votes, identity changes) require biometric confirmation on the device in addition to ring presence. The ring alone is insufficient for consequential actions.

Coerced voting (forced to vote a particular way under threat) is detectable through pattern analysis and addressed through vote revision: participants may change their vote until the voting window closes, with only the final vote counting. A coerced participant can revise when no longer under duress.

11. Protocol Governance

11.1 Self-Amendment

The Omxus protocol governs itself through the same mechanisms it provides: direct democratic participation with proximity weighting. Protocol changes are proposals subject to network-wide voting with elevated quorum requirements.

Constitutional changes (modifications to foundational principles, identity mechanisms, or governance structure) require supermajority approval (two-thirds of participating votes) and

extended deliberation periods (minimum 90 days). This prevents hasty modification of core properties while enabling evolution.

11.2 Implementation Without Authority

Approved protocol changes must be implemented in software and adopted by network participants. No central authority can force software updates. Implementation follows the Bitcoin model: developers propose changes, participants choose whether to run updated software.

Incompatible changes create forks: participants running different software versions form separate networks. This is a feature, not a bug. Fundamental disagreements resolve through voluntary association rather than imposed authority. The market of ideas operates literally: participants join the network whose rules they endorse.

11.3 Developer Accountability

Software developers contributing to Omxus implementations are participants in the network, subject to the same accountability mechanisms as all participants. Malicious code contributions are traceable through signed commits; developers face reputation consequences for harmful contributions.

Multiple independent implementations are encouraged. No single development team controls the canonical implementation. Participants may choose among implementations, preventing developer capture.

12. Scalability Analysis

12.1 Identity Scale

Eight billion identities require approximately 256 bits of addressing space (2^33 ≈ 8 billion). DID addressing provides ample space. The vouching graph at this scale contains approximately 24 billion edges (three vouchers per participant). This graph is distributed across all participants; no node must store the complete graph.

Verification of any identity requires traversing the vouching path to the genesis ceremony. Average path length in social networks scales logarithmically with population (six degrees of separation phenomenon). Verification thus requires approximately log(N) lookups, remaining practical at global scale.

12.2 Voting Scale

Global votes potentially involve billions of participants. However, proximity weighting means most votes have local scope. A neighbourhood decision involves thousands, not billions. Network-wide votes are rare and spread over extended periods.

Vote aggregation is hierarchical: local nodes aggregate local votes, regional nodes aggregate local aggregates, eventually reaching global consensus. Individual vote verification remains possible (any participant can trace their vote through the aggregation tree) while keeping bandwidth requirements manageable.

12.3 Network Scale

Mesh networks face scaling challenges: fully connected meshes grow quadratically with participants. Yggdrasil addresses this through hierarchical routing based on cryptographic address space, achieving logarithmic scaling similar to internet BGP routing.

Content distribution via IPFS scales naturally: popular content distributes across many nodes, reducing load on any single source. Rare content may require longer retrieval times but remains accessible.

12.4 Bitcoin Anchoring Scale

Bitcoin's limited transaction throughput (approximately seven transactions per second) cannot directly record eight billion individual actions. RGB protocol addresses this through client-side validation: only state commitment hashes are anchored to Bitcoin, while full state is maintained off-chain.

Batching further reduces on-chain footprint: many Omxus state changes are aggregated into single Bitcoin anchors. Individual actions are verifiable through Merkle proofs against these anchors without requiring individual on-chain records.

13. Transition Path

13.1 Adoption Phases

Global transition from existing governance to Omxus occurs through voluntary adoption in phases:

Phase 1 (Genesis): Initial community of early adopters establishes network, proves technical viability, and refines protocols through lived experience. Scale: thousands to tens of thousands.

Phase 2 (Parallel): Omxus operates alongside existing governance. Participants maintain dual membership, using Omxus for community coordination while remaining subject to territorial law. Governance decisions are advisory, building legitimacy through demonstrated wisdom. Scale: millions.

Phase 3 (Transition): As Omxus participation reaches critical mass in regions, existing governance structures begin recognising Omxus decisions. Hybrid arrangements emerge: local governments implement Omxus-decided policies, gaining efficiency while ceding authority.

Phase 4 (Supersession): Omxus becomes the primary governance mechanism. Residual territorial governments handle legacy systems during wind-down. Scale: billions.

13.2 Coexistence with Existing Systems

During transition, Omxus participants remain subject to territorial law. The system does not advocate violation of existing legal frameworks. Instead, it builds parallel capacity: when existing systems fail (as in the Whitlam dismissal), alternatives exist. When existing systems function, Omxus provides supplementary coordination.

This is not revolution but evolution: demonstrating superior coordination mechanisms that existing structures may voluntarily adopt or that persist when existing structures collapse.

13.3 Bootstrapping Challenges

Early adoption faces chicken-and-egg challenges: the network's value depends on participation, but participation depends on perceived value. Initial adopters must be intrinsically motivated by principle rather than immediate utility.

The genesis ceremony addresses this: publicly committed founders stake their identities and reputations on network success. This personal commitment attracts others who share the vision, creating a community of aligned participants before utility becomes self-evident.

14. Economic Implications

14.1 Elimination of Administrative Overhead

Contemporary governance requires substantial bureaucratic infrastructure: election administration, legislative staffing, regulatory agencies, justice system personnel. Omxus replaces these functions with protocol—automated, transparent, and requiring no ongoing administrative labour.

Australia allocated approximately $32 billion to justice administration in 2019 (Australian Bureau of Statistics, Government Finance Statistics). The majority of this expenditure addresses functions that Omxus renders unnecessary: dispute adjudication (replaced by ViewSwap), crime response (replaced by prevention), incarceration (eliminated by the prevention principle). These resources become available for direct human benefit.

14.2 Reclaimed Time

A substantial portion of contemporary labour serves administrative rather than productive functions: compliance, reporting, verification, authentication. Omxus eliminates much of this through cryptographic proof: identity is proven by ring, actions are verified by signature, compliance is ensured by protocol.

The elimination of administrative friction, combined with direct democratic efficiency, enables substantial reduction in required labour. Participants may find themselves with significantly increased discretionary time—potentially twenty or more hours per week—to allocate according to their own values.

15. Funding Model: The Value of Verified Humanity

15.1 The Problem Organisations Cannot Currently Solve

Contemporary identity infrastructure verifies accounts, not humans. Google, Facebook, and other identity providers can confirm that a login corresponds to a registered account. They cannot confirm that the account represents a unique human being. The same person may hold dozens of accounts. A bot farm may operate millions.

This creates substantial costs across industries. Advertisers pay for impressions that reach bots, not humans. Social platforms fight endless battles against fake engagement. Employers process applications from non-existent candidates. Financial services invest heavily in Know Your Customer (KYC) compliance that remains unreliable. Online polls and reviews are trivially manipulated. Every organisation that needs to interact with verified humans currently cannot.

15.2 What Google Actually Sells

Google's authentication services are not its product; they are the glue that maintains its ecosystem. Revenue derives primarily from advertising (~80% of total revenue). The identity layer serves this advertising business by tracking users across services, maintaining engagement within the ecosystem, and providing targeting data. Google Sign-In for third parties extends this tracking beyond Google properties.

Crucially, Google cannot sell verified humanity because it does not have it. CAPTCHAs exist precisely because Google cannot distinguish humans from bots through its authentication system. The company verifies credentials, not personhood. This is a fundamental limitation of account-based identity systems: accounts are abstractions that may or may not correspond to unique humans.

15.3 The Omxus Value Proposition

Omxus provides what no existing system can: cryptographic proof of unique humanity. Each token represents exactly one human, vouched in person by three existing participants, traceable through a web of trust to the genesis ceremony. This proof is:

Verifiable: Any party can confirm the vouching chain without accessing private data. Unforgeable: The cryptographic signature from a physical ring cannot be replicated. Unique: The sybil-resistance mechanism ensures one human holds one token. Privacy-preserving: Verification

reveals nothing beyond 'this is a verified unique human'—no name, location, or personal data required.

15.4 Transition-Phase Revenue

During the transition period, organisations may access verified-human attestation through API calls. The attestation answers one question: 'Is this a verified unique human in the Omxus network?' The response is binary. No personal data is transmitted. No tracking is enabled.

Use cases with immediate commercial value include: advertising verification (real impressions, not bots), platform integrity (real users, not farms), employment verification (real candidates), financial services (KYC compliance), market research (real respondents), content authenticity (real authors), and access control (real attendees).

Revenue from attestation services flows to network-governed resource pools. These pools fund ring production, infrastructure development, accessibility features, and other network needs as determined through direct democratic allocation. No profit is extracted; all revenue serves network purposes.

15.5 Pricing Dynamics

The value of verified-human attestation scales with network size. At thousands of participants, the service is a curiosity. At millions, it becomes valuable for niche applications. At billions, it becomes essential infrastructure—the definitive answer to 'is this a real person?'

Pricing is set through network governance. Early pricing may be low to encourage adoption; mature pricing reflects actual value. Differential pricing may apply: higher rates for advertising (where bot fraud is most costly), lower rates for non-profit and public-interest applications. Participants may vote to provide free attestation for specific categories of use.

15.6 Participant Consent and Benefit

Attestation requires participant action. When an organisation requests verification, the participant's device prompts for ring confirmation. The participant chooses whether to provide attestation for each request. No verification occurs without explicit consent.

Participants benefit directly: verified-human status eliminates CAPTCHAs, reduces fraud friction, enables access to services requiring identity verification, and may qualify for benefits that organisations offer to verified humans (reduced advertising, premium features, priority service). The participant's humanity becomes an asset they control rather than a fact they must repeatedly prove to systems designed not to trust them.

15.7 Principle Alignment

This funding model aligns with foundational principles. Autonomy: participants control attestation consent. Non-maleficence: no personal data is transmitted or retained; the service cannot be weaponised for surveillance. Beneficence: revenue funds network infrastructure that

serves all participants. Justice: the same verification is available to all participants regardless of wealth, status, or location.

The funding mechanism does not compromise the network's purpose. It monetises a byproduct (verified humanity) that emerges from the identity layer designed for governance. Organisations pay for something Omxus provides inherently; participants receive benefit from something they already possess. The transaction is mutually beneficial, consensual, and privacy-preserving.

15.8 Post-Transition Economics

As Omxus becomes primary governance infrastructure, attestation-for-payment diminishes in importance. Organisations operating within the network verify humanity through native network mechanisms. External organisations (those not yet transitioned) continue paying for attestation, but these become edge cases as adoption spreads.

Post-transition funding derives primarily from resource reallocation: the substantial budgets currently consumed by bureaucratic, administrative, and justice functions redirect to network infrastructure through democratic decision. The attestation revenue model is a bridge—necessary for transition, obsolete upon completion.

16. Conclusion

Omxus proposes infrastructure for a fundamentally different social organisation: one where governance is direct, justice is preventive, and access is universal. The technical components—mesh networking, decentralised identity, blockchain anchoring—are not novel individually. The contribution is their composition into a coherent system embodying specific ethical principles.

The system requires no trusted intermediaries. It cannot be disabled by authoritarian action. It provides every participant with equal voice in collective decisions and equal protection through universal response.

The goal is not utopia but robustness: a social infrastructure that cannot be Whitlam'd. Where no one can be isolated, silenced, or overruled by unilateral action. Where eight billion humans have access to communication, information, and collective self-determination as basic rights rather than privileges granted by intermediaries.

Autonomy. Non-maleficence. Beneficence. Justice.

Prevention only.

17. Frequently Asked Questions

17.1 Funding and Sustainability

Who pays for the rings? Who funds development?

Ring production is funded through direct democratic allocation. The network votes to direct pooled resources (voluntary contributions during transition; post-transition, resources previously consumed by replaced bureaucratic functions) toward manufacturing. Initial development is funded by early adopters who share the vision—the same model that bootstrapped Bitcoin, Linux, and Wikipedia. Ongoing development continues through allocated network resources and voluntary contribution from participants with relevant skills. There is no company, no venture capital, no profit motive. The network owns itself.

17.2 Domestic Violence and Intimate Partner Abuse

How does universal response help when the abuser lives with the victim?

Domestic violence is the hardest case for the prevention model, and honesty requires acknowledging its difficulty. The system provides several mechanisms: silent emergency activation (the ring can signal distress without visible action); pattern detection (repeated activations from the same location trigger community welfare checks); mandatory separation protocols (when domestic abuse is identified, the accused must immediately relocate, with housing provided by community resources, not the victim); and economic independence (network participation provides identity and access independent of any partner). These do not guarantee prevention—no system can. But they eliminate the isolation that enables ongoing abuse. The victim is never alone, never without resources, never dependent on the abuser for identity or access. The abuser knows that every interaction is potentially witnessed, that the victim can summon response instantly, and that the community will act. This shifts the structural conditions that enable domestic violence.

17.3 Private Space Crimes

Prevention relies on witnesses. What about harm behind closed doors?

The system does not surveil private spaces—this would violate non-maleficence. Instead, it ensures that no one can be isolated. Anyone in any space can activate emergency response. The ring is always present, always capable of summoning help. The shift is from 'crime cannot be seen' to 'crime cannot prevent the victim from being heard.' Additionally, the accountability system means that all network interactions between parties are signed. Patterns of coercion, manipulation, or threat become visible through communication records the victim can choose to reveal. The abuser cannot deny what they said. Prevention is not perfect, but the conditions that enable private harm—isolation, dependence, deniability—are systematically undermined.

17.4 Accessibility

How do blind, deaf, physically disabled, cognitively impaired, or illiterate people participate?

Universal participation is a foundational requirement, not an afterthought. The ring interface is tactile—it works without sight. Devices support screen readers, voice interfaces, and haptic feedback. Proposals and voting interfaces are available in audio, visual, and simplified formats. For participants with cognitive impairments, guardian relationships allow trusted parties to assist without removing agency. For illiterate participants, audio and video content, icon-based interfaces, and community assistance provide access. The network allocates resources to accessibility development proportional to need. If any human cannot participate, the system has failed. Eight billion means eight billion.

17.5 Language

How do proposals work across hundreds of languages?

Proposals are submitted in the author's language. Machine translation provides initial versions in all major languages. For proposals affecting multilingual populations, community translators verify accuracy—this is a form of network contribution recognised in reputation systems. Critical proposals require certified translation by multilingual participants who stake their reputation on accuracy. Voting interfaces adapt to participant language preferences. Local meetings occur in local languages; cross-community coordination employs translation layers. The network explicitly recognises linguistic diversity as a strength, not an obstacle.

17.6 Rural and Remote Areas

Mesh networks need density. What about the outback, the Sahara, the Amazon?

Low-density regions employ different infrastructure. LoRa provides long-range, low-bandwidth connectivity across kilometers. HF radio reaches globally. Satellite uplinks (initially through existing providers; eventually through network-funded infrastructure) bridge gaps. Fixed relay stations at community centers, trading posts, and transport hubs provide connection points. Nomadic participants carry data that synchronises opportunistically. Response times in remote areas are necessarily longer—but so they are under current systems. The commitment remains: every participant can activate emergency response, cast votes, and communicate, regardless of location. The infrastructure adapts to geography rather than demanding geography adapt to infrastructure.

17.7 Device Requirements

What devices do participants need beyond the ring? Who provides them?

The ring alone enables emergency activation and identity verification. Full participation requires a device capable of NFC communication, network connectivity, and interface display—currently, a smartphone or tablet. For participants without devices, the network provides them through the same resource allocation mechanism as rings: community-funded, community-

distributed. Shared devices at community locations serve those who prefer not to carry personal devices. The software runs on commodity hardware; no proprietary devices required. As the network matures, purpose-built Omxus devices—optimised for mesh networking, low power, and durability—may be developed and distributed. No participant is excluded for lack of device access.

17.8 Emergency Response Protocol

Someone activates an emergency. Then what? How do untrained volunteers handle medical emergencies, violence, or mental health crises?

Emergency activations are categorised: medical, safety, mental health, and general. Nearby participants are notified with category and distance. Participants with relevant skills (medical training, crisis de-escalation, mental health first aid) are flagged in the system and prioritised in notifications. All participants receive basic response training as part of onboarding—not expert training, but enough to provide presence, call for additional help, and avoid making situations worse. The first responder's role is often simply to be there: to witness, to document, to prevent escalation through presence. Specialised help follows. The network maintains rosters of participants with advanced skills who can provide remote guidance during incidents. This is not a replacement for professional emergency services during transition—it operates alongside them. Post-transition, professional responders are network participants with specialised roles, funded and coordinated through the same system.

17.9 False Emergency Abuse

What prevents swatting-style abuse of the emergency system?

Every emergency activation is signed by the activating ring. False activations are permanently attributable to the person who made them. Reputation consequences for false activation are severe and visible. Repeated false activations trigger community review; participants who abuse the system face escalating response: first warnings, then mandatory mediation to understand underlying issues, then temporary suspension of activation privileges (though they can still be recipients of response). The difference from swatting is accountability: swatting relies on anonymous tips to weaponise state force. Omxus activations are never anonymous. You cannot abuse a system that records your identity with every action.

17.10 ViewSwap Edge Cases

What about dangerous jobs? Dependents who cannot be left? Medical conditions? People currently incarcerated?

ViewSwap is mandatory but adaptable. The principle is perspective exchange; the implementation accommodates reality. Dangerous jobs: the swapping party shadows rather than performs dangerous work—understanding the conditions, not risking untrained injury. Dependents: swap includes temporary care arrangements; network support provides childcare,

eldercare, or other dependent care during the exchange. Medical conditions: accommodations are made; if physical swap is impossible, extended immersive observation substitutes. Incarceration during transition: a limitation of the transition period. Incarcerated participants hold provisional status until release; disputes involving them are handled through adapted mechanisms (recorded video exchange, extended correspondence, post-release physical swap). The goal is embodied understanding of another's circumstances; rigid implementation that defeats this goal is counterproductive.

17.11 Meta-Disputes

What if someone refuses ViewSwap? Who decides the dispute about the dispute?

ViewSwap obligation is accepted at vouching. Refusal is breach of network contract. The refusing party's vouchers are notified and bear responsibility for mediating compliance. Continued refusal triggers community review by randomly selected participants. If refusal is found unjustified, the refusing party faces graduated consequences: temporary suspension of voting rights, restrictions on proposal submission, and ultimately, if persistent, voucher-initiated token suspension (not revocation—restoration is possible through demonstrated good faith). The dispute about whether ViewSwap was properly triggered is handled through standard community arbitration before ViewSwap is mandated. The system acknowledges that meta-disputes exist and provides clear escalation paths rather than pretending they will not occur.

17.12 Network Partition Attacks

What if attackers isolate a region, feed different information, and create inconsistent state?

Network partitions are a known distributed systems problem. Omxus handles them through eventual consistency with conflict detection. During partition, both regions continue operating with local state. When reconnection occurs, CRDTs merge state automatically for most data types. For conflicts that cannot be automatically merged (e.g., contradictory votes on the same proposal), the timestamp ordering and cryptographic signature chain determines canonical state. Proposals with partition-affected voting are flagged for extended deliberation and potential revote. Bitcoin anchoring provides ultimate truth: any participant can verify the correct state by tracing to anchored records. Attackers cannot forge a partition history that contradicts Bitcoin-anchored reality. Partitioned participants are disadvantaged during partition but not permanently harmed; state reconciles when connectivity returns.

17.13 Legal and Political Opposition

States will fight this. What happens when governments declare Omxus illegal?

The network does not advocate illegal activity. Participants in jurisdictions where participation is criminalised must make their own risk assessments—as dissidents always have. The system provides: technical resilience (participation is difficult to detect and impossible to prevent without shutting down all digital communication); legal ambiguity (participating in a

communication network is not obviously illegal in most jurisdictions); and strength in numbers (as participation grows, criminalisation becomes politically costly). The transition strategy emphasises demonstration over confrontation: showing that Omxus coordination produces better outcomes than existing governance, building legitimacy that makes opposition look foolish rather than necessary. States that declare participation illegal reveal themselves as the authoritarians the system is designed to resist. This is not comfortable, but it is honest. Freedom has always required risk.

17.14 Cultural Assumptions

This seems to assume Western individualism. How does it work in collectivist cultures, caste systems, or existing tribal governance?

The system provides infrastructure; it does not impose values. Collectivist communities may choose to coordinate their voting, with family or community heads consulting members before casting weighted collective positions. This is not prevented—but it is transparent. Individual members always retain the capability to vote independently if they choose. The ring is individual, but nothing prevents individuals from deferring to collective decision-making. Caste systems and oppressive tribal governance face a challenge: the system makes the oppressed visible and gives them voice. This is intentional. Omxus does not claim cultural neutrality; it claims that autonomy, non-maleficence, beneficence, and justice are universal values that some cultural practices violate. The system does not forcibly dismantle these practices, but it provides exit options for those within them who wish to exercise individual agency. This is a value position, openly stated.

17.15 Prevention Claims

The claim that universal response prevents ALL crime seems bold. Crimes of passion happen in seconds. How does notification and response happen faster than a punch?

It does not, and honest assessment requires acknowledging this. The prevention principle does not claim to stop every harmful action instantaneously. A punch can land before anyone responds. The system prevents the conditions that enable patterns of harm: isolation, unwitnessed repeated abuse, denial of facts, victim helplessness. For impulsive violence, the prevention is cultural over time: growing up in a network where every action is accountable, where perspective exchange is mandatory, where violence summons immediate community response, shapes behaviour before the impulse arises. The claim is not 'no harm will ever occur' but 'the structural conditions that enable systematic harm are eliminated.' Individual failures will happen. The question is whether they remain individual failures or become systematic oppression. Omxus ensures the former.

17.16 ViewSwap Logistics

'Live their life for a week' sounds good. What about their job, their children, their medication, their security clearances?

ViewSwap requires infrastructure. Employers recognise ViewSwap obligation as legitimate absence (during transition, this is negotiated; post-transition, network decisions govern employment norms). Children are cared for by the swapping party or, where inappropriate, by network-provided childcare. Medication transfers with the participant. Security clearances present transition-period complications: ViewSwap into classified environments is impossible until such environments are subject to network governance. Practical arrangements are negotiated in the mediation phase before swap begins. The principle is: you experience the other's daily reality to the maximum extent possible given hard constraints. Perfect fidelity is not required; genuine effort to understand is. Mediators assess whether reasonable effort was made; bad-faith minimal-compliance swaps fail to resolve disputes and can be repeated.

17.17 Proximity Weighting Mechanics

'Quadratic' is mentioned but no formula. How is proximity actually measured without surveillance?

Proximity is computed from three sources, none requiring central surveillance: (1) Vouching distance—how many vouching hops separate you from the proposal's author or affected region. (2) Meeting attendance—recorded presence at local meetings in the affected area. (3) Declared residence—participants self-declare primary location, verifiable through voucher attestation. The weighting function for geographic proximity is: weight = $1 / (1 + d^2)$, where d is distance in standardised units (vouching hops or declared location distance). Weights are normalised across all voters so that local participants collectively have majority influence on local decisions while universal participation remains possible. Domain expertise weighting uses participation history: demonstrated engagement with related proposals over time increases weight on technical matters. The specific parameters are subject to network governance and may be adjusted through standard proposal processes.

17.18 Voucher Incentives

Vouching carries risk if the vouchee is a sybil. What is the upside? Why would anyone vouch for strangers?

You should not vouch for strangers. Vouching is for people you know personally well enough to stake reputation on. The incentive is network growth: a larger network benefits all participants through more robust infrastructure, more diverse deliberation, and wider emergency response coverage. Successful vouching (vouchees who participate constructively over time) contributes positively to reputation. The system explicitly discourages vouching strangers for growth's sake—this is how sybil attacks propagate. Vouching incentives are social, not monetary: you extend the network to people you trust because you want them to have access and because their

participation strengthens the whole. This is how social networks naturally grow. The vouching system formalises and makes accountable what already happens informally.

17.19 Genesis Ceremony Legitimacy

Why should the world trust 12 people who filmed themselves?

The world should not trust them based on the filming alone. The genesis ceremony creates accountability, not authority. Those 12 people are identifiable, their reputations staked, their future actions visible. If they abuse the network they founded, this is observable and they bear consequences. Legitimacy comes not from the ceremony but from the network's subsequent operation: does it produce good outcomes? Are decisions wise? Is participation meaningful? The genesis participants gain no special privileges; they are simply the first nodes in the vouching graph. Their lasting influence is limited to their vouching chains—the people they vouched, and the people those people vouched. Authority dissipates through the graph. The ceremony is a starting point, not a coronation.

17.20 Economic Sustainability

No payment for gateways, no token economy. How does development continue long-term?

The network allocates resources through direct democratic decision. During transition, voluntary contributions fund development—time from skilled participants, money from those with resources, both recognised through reputation. Post-transition, the resources currently consumed by replaced functions (bureaucracy, administration, justice system) are redirected through network governance to infrastructure, development, and ring production. This is substantial: the $32 billion Australia spends annually on justice alone funds significant development if redirected. Gateway operation and other infrastructure contribution are recognised socially, not monetarily—but in a system where social recognition directly influences governance weight, this is meaningful. The absence of monetary incentive prevents the accumulation dynamics that corrupt monetary systems. Contribution is its own reward, amplified by genuine voice in collective decisions.

17.21 Emergency Response and Privacy

Emergency response requires knowing where people are. 'No surveillance' is claimed. These conflict.

The conflict is resolved through local versus global knowledge. Emergency activation broadcasts to nearby devices determined by local mesh topology—devices that can hear each other directly. No central server knows anyone's location. When you activate, your device broadcasts locally; devices that receive the broadcast are nearby by definition. They respond to the broadcast, not to a location report. Your location is revealed only to those close enough to help, only at the moment you choose to reveal it, only for the duration of the emergency. After response, no record of your location persists anywhere. This is fundamentally different from surveillance: you

control when location is revealed, revelation is local and temporary, and no entity ever has global location visibility. Privacy and emergency response coexist because response does not require surveillance—it requires local, user-initiated broadcast.

17.22 Coercion Detection

'Pattern analysis' and 'vote revision' are mentioned but not specified. How do you actually detect coerced voting?

Detection employs multiple signals: (1) Vote revision patterns—a participant who changes their vote near the deadline after maintaining a consistent position may be escaping coercion. (2) Voting location anomalies—votes cast from unusual locations relative to participant's normal patterns. (3) Temporal clustering—multiple participants in the same location voting identically in rapid sequence suggests coordinated coercion. (4) Direct report—coerced participants can flag their own vote as coerced after the fact, triggering investigation. No single signal is conclusive; the system flags anomalies for human review rather than automated action. The primary protection remains vote revision: coerced participants change their vote when free from duress. Since only the final vote counts and revisions are private until the window closes, coercers cannot verify compliance. Coercion becomes unreliable and therefore unattractive.

17.23 Scalability Evidence

'Logarithmic' scaling is stated but there is no proof. Has this been simulated?

The scalability claims rest on established computer science results, not novel assertions. Yggdrasil's logarithmic routing is proven in its published documentation and running on a global network of thousands of nodes today. IPFS operates at massive scale across millions of nodes. CRDTs are mathematically proven to converge. The six-degrees phenomenon in social networks is empirically validated across billions of humans. RGB's client-side validation scales by design. What has not been validated is Omxus specifically at eight-billion scale, because it does not yet exist. The transition phases exist precisely to build evidence: Phase 1 proves viability at thousands, Phase 2 at millions, Phase 3 at hundreds of millions. If scaling problems emerge, they are addressed before global rollout. This is engineering prudence, not magical thinking. The theoretical basis is sound; implementation will test and refine it.

17.24 Transition Forcing Function

'Governments begin recognising Omxus decisions'—why would they? What forces this transition?

Nothing forces it; everything incentivises it. When Omxus participation reaches critical mass in a region, ignoring its decisions becomes costly: policies opposed by Omxus consensus face implementation resistance; candidates without Omxus backing cannot mobilise volunteers; administrative functions that Omxus handles more efficiently become redundant expenses. Governments that recognise Omxus decisions gain efficiency, legitimacy, and alignment with

their populations. Those that resist face ongoing friction. The transition is not revolutionary seizure of power but evolutionary obsolescence of existing structures. Some governments will resist longer than others. Some may never transition. The network does not require universal governmental recognition to function—it operates in parallel, providing value to participants regardless of state endorsement. Transition happens because it works better, not because it is imposed.

17.25 Honest Limitations

What can Omxus NOT solve?

Omxus is infrastructure, not utopia. It cannot solve: scarcity of physical resources (governance must still allocate finite goods); genuine value disagreements (people may still want incompatible things after full perspective exchange); human mortality (prevention cannot stop death); natural disasters (response can be coordinated, but earthquakes still happen); malice by determined individuals (someone truly committed to causing harm in the instant before response can succeed); accumulated historical injustice (the system starts from where we are, not where we should have been); its own bootstrap problem (initial adoption requires believers before proof exists); the heat death of the universe. The claim is not perfection. The claim is: better infrastructure for human coordination than any currently available. More accountable governance. More preventive justice. More robust communication. More universal access. These are substantial. They are not everything.

References

Australian Bureau of Statistics. (2020). Government Finance Statistics, Australia, 2018-19. ABS Catalogue No. 5512.0.

Benet, J. (2014). IPFS - Content Addressed, Versioned, P2P File System. arXiv:1407.3561.

Beauchamp, T. L., & Childress, J. F. (2019). Principles of Biomedical Ethics (8th ed.). Oxford University Press.

Buterin, V., Hitzig, Z., & Weyl, E. G. (2019). A Flexible Design for Funding Public Goods. Management Science, 65(11), 5171-5187.

Kerr, J. (1975). Matters for Judgment: An Autobiography. Macmillan.

Kleppmann, M., & Beresford, A. R. (2017). A Conflict-Free Replicated JSON Datatype. IEEE Transactions on Parallel and Distributed Systems, 28(10), 2733-2746.

Milgram, S. (1967). The Small World Problem. Psychology Today, 2(1), 60-67.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Orlandi, M., Pinto, A., & Uberti Foppa, L. (2023). RGB Protocol Specification. LNP/BP Standards Association.

Reed, D., Sporny, M., Longley, D., Allen, C., Grant, R., & Sabadello, M. (2022). Decentralized Identifiers (DIDs) v1.0. W3C Recommendation.

Shapiro, M., Preguiça, N., Baquero, C., & Zawirski, M. (2011). Conflict-Free Replicated Data Types. Proceedings of the 13th International Symposium on Stabilization, Safety, and Security of Distributed Systems.

Tarr, D., Lavoie, E., Meyer, A., & Tschudin, C. (2019). Secure Scuttlebutt: An Identity-Centric Protocol for Subjective and Decentralized Applications. Proceedings of the 6th ACM Conference on Information-Centric Networking.

Whitlam, G. (1979). The Truth of the Matter. Penguin Books.

Yggdrasil Network. (2023). Yggdrasil Network Documentation. https://yggdrasil-network.github.io/