Chimera: An Autonomic, Intent-Centric Architecture for Verifiable Decentralized Intelligence

Version 1.0

Abstract

Current decentralized architectures, while powerful, operate in silos. Intent-centric protocols solve for user expression but create trust assumptions for off-chain solvers.[1] Verifiable computation markets address this trust but lack a native framework for complex, goal-oriented coordination.[2] Formal verification methods provide security for individual components but struggle with the emergent complexity of their composition.[3] This paper introduces Chimera, a novel protocol architecture that unifies these disparate paradigms. Chimera integrates **generalized intent-centricity**, a **decentralized market for verifiable AI agents (zk-Agents)**, and **autonomic governance** inspired by closed-loop control theory, all within a framework of **provable composability**. We argue that by treating all network actions—from swaps to governance—as intents fulfilled by verifiable AI agents, and by governing the system with an autonomic management layer that monitors and adapts its own parameters, Chimera enables a new class of self-organizing, intelligent, and provably secure decentralized applications. We present the full architectural design and demonstrate its power through case studies in verifiable AI-driven finance and autonomic public goods funding.

---

1. Introduction: The Fragmentation of Decentralized Paradigms

This section will establish the fundamental problem: the current landscape of decentralized protocols consists of powerful, yet fragmented, solutions. Each addresses a piece of the puzzle, but their integration reveals deeper challenges, creating the need for a new, unified architecture.

1.1 The Expressivity Gap: From Imperative Transactions to Declarative Intents

Traditional blockchain architectures, such as Bitcoin and Ethereum, are transaction-centric.[4] Users must specify the exact, imperative steps for a state change. This limits expressivity and forces users to manage complex execution paths, often without fully understanding the risks.[6]

The Anoma whitepaper introduces a paradigm shift to **intent-centricity**.[1] Intents are declarative, signed messages that express a user's desired end state (e.g., "I want to trade X for Y"), not the execution path. This approach decouples user goals from execution, simplifying the user experience and enabling more complex interactions like multi-party swaps.[6]

This shift, however, outsources the "how" to a network of off-chain actors called **solvers**. This creates a new trust bottleneck. How can a user be sure a solver executed the *best* path, or even a *correct* path, without revealing private information or re-centralizing the system around a trusted solver? Anoma acknowledges this challenge, particularly in the context of private counterparty discovery.[1]

1.2 The Trust Gap: The Rise of Verifiable Off-Chain Computation

The solver problem is a specific instance of a broader challenge in Web3: the need for trustless off-chain computation. As noted in the Boundless whitepaper, on-chain computation is a scarce and expensive resource that "prices-out" all but the highest-margin requests.[2]

The Boundless protocol directly addresses this trust gap by proposing the **financialization of verifiable compute**.[2] It treats zero-knowledge proofs (ZKPs) as a tradable commodity. Its core mechanism, **Proof of Verifiable Work (PoVW)**, provides a fraud-resistant way to measure the computational effort required for a ZKP. This enables a decentralized spot market where "requestors" can pay "provers" for ZKPs, with payment settled trustlessly upon on-chain verification of the proof.[2]

Boundless provides the "how" for verifiable execution but lacks a native framework for expressing the "what." It is a market for a raw resource (ZK proofs), not a system for satisfying high-level user goals. It provides the building blocks for verifiable solvers but does not specify the overarching architecture in which they operate.

1.3 The Guarantee Gap: The Challenge of Provably Secure Composition

Composing these complex systems—an intent layer (Anoma) with a verifiable compute layer (Boundless)—creates enormous security challenges. As the C4 paper highlights, verifying systems that mix classical concurrent objects with transactional logic is notoriously difficult.[3] Unforeseen interactions between components are a primary source of exploits in DeFi.[7]

The C4 framework provides a solution through **formal verification** for concurrent, composable systems.[3] Its key innovation is unifying linearizability and serializability by modeling transactions as higher-order methods on linearizable objects. It uses **interaction trees** to represent and syntactically instrument programs, enabling modular proofs of correctness for complex patterns like transactional predication.[3]

C4 provides the tools to build a *static* system that is secure and correct. However, it does not address how such a system should govern itself, adapt to changing conditions, or evolve over time. This is a problem of governance and system dynamics, not just static verification.

1.4 Thesis: The Need for an Autonomic, Unified Architecture

The analysis of the expressivity, trust, and guarantee gaps reveals that current paradigms, while powerful, are incomplete on their own. The whitepapers for Anoma, Boundless, and C4 are not competitors; they are complements, describing the "what" (Anoma), the "how" (Boundless), and the "how to build it correctly" (C4). A direct synthesis of these three ideas represents the next logical step in protocol design. Anoma's intents create a demand for off-chain solvers.[1] These solvers must be trustless to maintain decentralization, creating the need for verifiable computation. The Boundless market for ZK proofs provides a mechanism for this verifiable computation.[2] The composition of these layers (intent gossip, solver markets, on-chain settlement) is complex and requires rigorous security guarantees, which the C4 formal verification framework can provide.[3]

However, even a system perfectly synthesized from these three ideas is fundamentally *static*. Its parameters (fees, security thresholds, etc.) are either set at genesis or changed via slow, contentious, and often low-participation human-driven governance.[8] This static nature makes it brittle and unable to adapt to dynamic market conditions or emergent threats.

Drawing inspiration from autonomic computing [10] and control theory [12], it is possible to conceive of a system that governs

itself. Therefore, the truly innovative leap is to introduce a fourth pillar: **Autonomic Governance**. This layer would use the system's own verifiable computation and intent mechanisms to monitor, analyze, and adapt its own rules, creating an intelligent, self-organizing, and resilient system. This is the core thesis of the Chimera protocol.

---

2. The Four Pillars of the Chimera Architecture

This section will detail the foundational principles of the Chimera protocol, explicitly building upon and extending the concepts from the source materials.

2.1 Pillar 1: Generalized Intent-Centricity

Chimera adopts the intent-centric model of Anoma [1] but generalizes it. In Chimera,

all state transitions are initiated as intents, not just commercial swaps. This includes governance actions, computational tasks, and data provisioning.

Formally, an intent is a set of constraints on a future state transition, signed by a user, that defines a utility function over the possible outcomes.[14] This declarative model [1] abstracts away the complexity of execution. The generalization extends beyond Anoma's scope in two primary ways:

1. **Governance Intents:** A user can express an intent such as: "I wish to change parameter X to Y, and I am willing for the DAO treasury to pay a fee F if on-chain metric M improves by Z% over the next N blocks." This reframes DAO governance [16] as an intent-driven process.

2. **Computational Intents:** A user can express an intent such as: "I desire the output of running this private ML model on my private data, and I am willing to pay up to C for a verifiable proof of the inference." This directly sets the stage for the zk-Agent market.

2.2 Pillar 2: Verifiable Resolution with zk-Agents

In Chimera, solvers are not simple scripts; they are **zk-Agents**: potentially complex, off-chain AI/ML models whose computations are made verifiable on-chain using Zero-Knowledge Machine Learning (ZKML).

This pillar directly implements and extends the vision of Boundless.[2] zk-Agents compete in a decentralized marketplace (a reverse Dutch auction, as in [2]) to fulfill user intents. The "work" they perform is not just a ZKP of a simple computation, but a ZKP of a complex AI/ML inference.

ZKML allows a prover to demonstrate that a specific ML model produced a given output from a given input, without revealing the model's weights or the input data.[8] This is crucial for both privacy and protecting the zk-Agent's model IP. The technical feasibility of this approach is grounded in the current state of ZKML frameworks like Risc Zero [20], Ezkl [22], and Succinct's SP1.[24]

Chimera's architecture represents a natural evolution of the solver market. Anoma's intents create a demand for off-chain solvers, and the Boundless market for verifiable compute provides a mechanism for it.[1] However, the most valuable "solving" tasks—such as optimal swap routing, risk analysis, and public goods impact assessment—are not simple calculations but complex optimization and prediction problems well-suited for AI/ML. ZKML provides the cryptographic primitive to make AI inference verifiable and trustless.[26] Consequently, the solver market naturally evolves from a market for raw computation (Boundless) to a decentralized, verifiable market for applied intelligence: Chimera's zk-Agent market. This creates a powerful incentive for developers to build and deploy sophisticated, specialized AI agents that can generate revenue by fulfilling complex user intents.

2.3 Pillar 3: Autonomic Governance via Closed-Loop Control

This pillar constitutes Chimera's primary innovation. The protocol governs itself through an **Autonomic Management Layer (AML)**, which functions as a closed-loop control system. This concept is adapted from autonomic computing, which defines systems with four key properties: self-configuration, self-optimization, self-healing, and self-protection.[10]

The AML operates on a **Monitor-Analyze-Plan-Execute over a shared Knowledge base (MAPE-K)** cycle [29]:

- **Monitor:** A network of oracles and indexers [30] continuously collects on-chain data representing the system's state (e.g., transaction fees, solver competition levels, token liquidity, governance participation rates).
- **Analyze:** A specialized, high-security zk-Agent, the **Constitutional AI**, analyzes this data. It compares the current state against a set of desired outcomes and constraints defined in an on-chain, human-ratified **DAO Constitution**.[31]
- **Plan:** If the system deviates from its constitutional principles (e.g., if MEV exceeds a certain threshold, or solver competition wanes), the Constitutional AI formulates a corrective action as a high-priority "governance intent."
- **Execute:** This governance intent is broadcast to the zk-Agent market, where other agents compete to find and execute the optimal state transition to fulfill it (e.g., by adjusting a fee parameter, deploying a new auction mechanism).

Current DAO governance is slow, inefficient, and suffers from low participation and voter apathy [8], making protocols vulnerable and slow to adapt. Control theory [12] provides robust models for systems that maintain stability by sensing their environment and adjusting their parameters in a feedback loop. Autonomic computing [10] offers an architectural blueprint (MAPE-K) for building such self-managing systems. Chimera's other pillars provide the necessary tools: intents are the control language, and zk-Agents are the actuators.

It is therefore possible to transform DAO governance from a slow social process into a fast, autonomous, and verifiable computational one. The AML is not just "AI in governance"; it is a fundamental re-architecting of the protocol to be a homeostatic, self-stabilizing system.

2.4 Pillar 4: Provable Composability and Security

Chimera's security is grounded in the principles of formal verification outlined in the C4 paper.[3] Each component (intent gossip, zk-Agent market, AML, settlement layer) is defined as a linearizable object with a clear sequential specification.

The verification strategy is hierarchical:

- The composition of these objects is verified to ensure their interactions do not introduce emergent vulnerabilities.
- The use of interaction trees [3] is proposed as the formal language for specifying the behavior of zk-Agents and their interactions with the AML, enabling syntactic analysis and instrumentation.
- The on-chain DAO Constitution itself is a formally specified artifact, ensuring the goals the AML is optimizing for are unambiguous.

This approach creates a hierarchy of proofs. At the lowest level, ZKPs verify the correctness of individual zk-Agent actions, as demonstrated by Boundless.[2] At the highest level, formal methods (in the style of C4) verify the correctness of the composition of all system components and the logic of the AML itself. This results in a system that is not only verifiable in its parts but provably secure in its whole.

3. Architectural Design of Chimera

This section will provide a technical breakdown of the protocol's layers and how they interact, referencing specific implementations where possible.

3.1 The Intent Layer: Expression and Gossip

- **User Interaction:** Users create intents using a high-level Domain-Specific Language (DSL) designed for expressivity and verifiability.[33] This DSL compiles to a standardized, signed data structure.
- **Intent Gossip Network:** Intents are broadcast over a sparse overlay network, as in Anoma.[1] This network is incentivized via settlement-conditional fees [1] to ensure data availability for zk-Agents. This layer is responsible for counterparty

discovery.

- **Privacy:** The protocol addresses the trade-offs between public intents for maximum solver competition and private intents for user privacy. This is done by referencing Anoma's use of threshold decryption (Ferveo) and the open research problem of fully private counterparty discovery.[1]

3.2 The Resolution Layer: The zk-Agent Market

- **zk-Agents as Solvers:** Any entity can operate a zk-Agent. These agents listen to the intent gossip network, specializing in certain types of intents (e.g., DeFi, governance, gaming).
- **Auction Mechanism:** When a zk-Agent identifies a set of intents it can solve, it participates in an auction. This will be a detailed design mechanism, inspired by the reverse Dutch auction of Boundless [2], but also considering more advanced auction theory to ensure fairness and mitigate MEV (Maximal Extractable Value).[35] The goal of the auction is to select the solver that offers the best execution *and* a valid ZK proof of its computation.
- **Verifiable Computation:** The winning zk-Agent performs the computation off-chain and generates a ZK proof using a supported zkVM (e.g., RISC Zero [20], SP1 [25]). The proof attests to the integrity of the computation (e.g., "I ran this specific AI model to find the optimal swap route"). The proof and the resulting transaction are submitted to the settlement layer.

3.3 The Settlement Layer: Verification and State Update

- **Fractal Instantiation:** Chimera adopts Anoma's model of "homogeneous architecture, heterogeneous security".[1] The protocol can be instantiated as multiple sovereign chains (fractal instances), each with its own security model (PoS, PoA, etc.), but all sharing the same core architecture.
- **Validity Predicates:** State transitions are guarded by **Validity Predicates (VPs)**, as described in Anoma.[1] A transaction is valid only if it satisfies the VPs of all state objects it touches. This includes verifying the ZK proof submitted by the zk-Agent.
- **Composable Security:** The architecture allows for atomic settlement across different fractal instances, enabling complex cross-domain applications.[1]

3.4 The Autonomic Management Layer (AML): The System's Brain

- **The Constitution:** A set of high-level principles and target metrics for the protocol, encoded as a formally specified smart contract. This is inspired by the concept of "Constitutional AI" [40] and digital constitutionalism for DAOs.[31] Example principles: "Solver revenue shall not fall below X% of total transaction fees," "Governance participation must remain above Y%."
- **The Constitutional AI (zk-Agent):** A specialized, high-security zk-Agent tasked with monitoring network health against the Constitution. It periodically queries on-chain data, performs analysis (e.g., time-series forecasting, anomaly detection), and generates a "State of the Network" report with a ZKML proof of its analysis.[18]
- **The Feedback Loop:** If the analysis reveals a deviation from constitutional parameters, the AML automatically generates a "governance intent" to correct it. For example: "Intent: Adjust the min_solver_bond parameter to increase the cost of auction spam." This intent is then fulfilled by the general zk-Agent market, creating a closed-loop, self-correcting system.[12]
- **Dynamic Tokenomics:** A key function of the AML is to manage the protocol's tokenomics dynamically.[42] Based on network health metrics, it can autonomously adjust parameters like staking rewards, token burn rates, or fee structures to maintain economic stability and incentivize desired behaviors.[44]

4. Applications and Case Studies

This section will move from the abstract architecture to concrete examples that demonstrate Chimera's unique capabilities.

4.1 Use Case 1: The Verifiably Optimal and Fair DEX

- **Scenario:** A user submits an intent: "Swap 100 ETH for the maximum possible amount of USDC, with a maximum slippage of 0.5%."

- **Chimera in Action:**
  1. Multiple zk-Agents, each with proprietary pathfinding algorithms (some potentially using ML), analyze liquidity across dozens of on-chain and off-chain pools.
  2. They compete in an auction to fulfill the intent. The winning bid is not just the best price, but the best price *with a ZK proof* demonstrating that no better path was available at the time of computation. This leverages verifiable inference.[26]
  3. Settlement is MEV-resistant because the transaction is only executed after the optimal path has been determined and privately proven. This builds on ideas from CoW Protocol [46] and Flashbots.[47]

4.2 Use Case 2: Autonomic Public Goods Funding

- **Scenario:** A DAO for funding open-source software wishes to allocate its treasury optimally.
- **Chimera in Action:**
  1. The DAO's constitution specifies its goal: "Maximize long-term developer activity on funded projects."
  2. The AML's Constitutional AI periodically performs an analysis. It ingests on-chain data (e.g., Gitcoin donation contributions [48]) and verifiable off-chain data (e.g., a zk-Agent proves "there were N commits to this GitHub repository [49] in the last month"). This is analogous to a verifiable, automated version of Optimism's RetroPGF.[40]
  3. Based on this verified impact data, the AML generates intents to adjust the parameters of the next funding round (e.g., increase the matching pool for the "developer tooling" category).
  4. This creates a self-optimizing funding ecosystem that transparently and verifiably directs resources where they create the most impact.

4.3 Use Case 3: A Self-Healing, Autonomic Protocol

- **Scenario:** A sudden market crash causes extreme network congestion and high volatility, threatening the solvency of the protocol's lending markets.

- **Chimera in Action:**
    1. The AML's monitoring function detects anomalous spikes in transaction failures and oracle price volatility.
    2. The Constitutional AI analyzes this as a critical threat, violating the "protocol solvency" principle in its constitution.
    3. It immediately generates a high-priority "self-healing" intent [51]: "Temporarily increase liquidation bonuses to 10% and raise the loan-to-value limit parameter to 5% to disincentivize new leverage."
    4. This intent is executed by the system in seconds, far faster than any human-in-the-loop governance vote could manage, stabilizing the protocol and preventing cascading liquidations. This demonstrates the "self-healing" and "self-protection" properties of an autonomic system.[28]

4.4 AI Security and Alignment in Chimera: Formal Verification vs. ZKML

- **The Challenge:** How do we ensure that zk-Agents, especially the powerful Constitutional AI, are safe and aligned with community values?
- **Formal Verification of Agent Logic:** We can use the C4 framework [3] and tools like Certora [52] to formally verify the *source code* of the zk-Agent's core logic. We can prove properties like: "The Constitutional AI will never propose a parameter change that allows the treasury to be drained." This provides strong guarantees about the agent's *possible behaviors*.
- **ZKML for Inference Integrity:** We use ZKML [8] to verify the *actual execution* of the agent's model. This proves that for a given input, the agent ran the *correct model* and produced the *correct output*, without tampering. This prevents a malicious agent operator from substituting a cheaper/malicious model for the approved one.

The combination of these two approaches creates a symbiotic security model. Formal verification protects the agent's *design*, while ZKML protects its *execution*. Neither is sufficient on its own. A formally verified agent could be run incorrectly (or not at all, with a faked output). A verifiably correct inference could come from a model with flawed logic. Therefore, Chimera proposes a security model where the DAO constitution requires any registered zk-Agent to have its core safety logic formally verified, *and* for all its outputs to be accompanied by a ZKML proof of inference. This provides end-to-end, provable security and alignment.

5. Comparative Analysis and Future Work

5.1 Chimera in the Landscape of Decentralized Architectures

- **vs. Ethereum:** Ethereum pioneered general-purpose on-chain computation, but its transaction-centric model and monolithic architecture created scalability and user experience bottlenecks.[4] Chimera builds upon Ethereum as a potential settlement layer but abstracts execution and user expression to a higher, more efficient level.
- **vs. Anoma:** Anoma introduced the intent-centric paradigm, a foundational innovation that Chimera adopts and generalizes.[1] However, Anoma leaves the solver problem as a trust issue. Chimera resolves this explicitly by requiring solvers (zk-Agents) to provide zero-knowledge proofs of their computation.
- **vs. Cosmos & Polkadot:** These protocols pioneered interoperability and application-specific chain sovereignty.[54] Chimera shares the vision of a multi-chain ecosystem but focuses on unifying the *user experience* and *governance logic* across these chains through a shared intent and autonomic management layer.
- **vs. EigenLayer:** EigenLayer introduces restaking for shared security, allowing new services to rent security from Ethereum.[59] Chimera's Autonomic Management Layer could be implemented as an Actively Validated Service (AVS) on EigenLayer, leveraging Ethereum's security to govern the Chimera ecosystem.

In short, Chimera does not reinvent the wheel; it assembles the existing wheels, chassis, and engine into a new type of vehicle and adds an autopilot system.

5.2 Open Research and Future Directions

- **Private Counterparty Discovery:** Building on Anoma's work [1], exploring advanced cryptographic techniques like Fully Homomorphic Encryption (FHE) or multi-party computation (MPC) to allow zk-Agents to find solutions over encrypted intents without a trusted decryptor.

- **Ethical Algorithmic Governance:** The AML automates governance, but this raises profound ethical questions.[62] Who is responsible if the Constitutional AI makes a harmful but verifiably correct decision? How can the constitution be safely amended? This section will frame these as open problems in digital constitutionalism [31] and value alignment.[65]
- **Scalability and Hardware Acceleration:** Acknowledging the high computational cost of ZKML.[67] Discussing the trajectory of hardware acceleration (GPUs, FPGAs, ASICs) for ZKPs and how this makes the zk-Agent model increasingly viable.

---

6. Conclusion

The Chimera architecture is proposed as a necessary evolutionary step in the decentralized protocol space. Existing solutions, while innovative, remain fragmented, addressing the challenges of user expressivity, verifiable computation, and compositional security in isolation. Chimera transcends this fragmentation by unifying these elements under a new paradigm of autonomic governance.

By integrating **intent-centricity** for expressivity, **verifiable AI** for trustless execution, **formal methods** for security, and **autonomic principles** for adaptive governance, Chimera provides a blueprint for building truly decentralized, intelligent, and resilient systems. This synthesis allows the protocol to self-organize, self-optimize, and self-heal, moving beyond simple transactions into a world of coordinated, verifiable intelligence capable of tackling complex, real-world problems with an unprecedented degree of autonomy and robustness.

References

[1] Goes, C., Sun Yin, A., & Brink, A. (2022).

Anoma: a unified architecture for full-stack decentralised applications. Pre-release.

[2] The RISC Zero Team. (n.d.).

The Boundless Protocol.

[3] Lesani, M., Xia, L., Kaseorg, A., Bell, C. J., Chlipala, A., Pierce, B. C., & Zdancewic, S. (2022). C4: Verified Transactional Objects.

Proc. ACM Program. Lang., 6(OOPSLA1), Article 80. https://doi.org/10.1145/3527324

Note: Additional numbered references correspond to the research material provided and are available upon request.

Referências citadas

1. What Are Modular Blockchains? A Deep Dive into the Future of ..., acessado em julho 15, 2025, https://www.lcx.com/what-are-modular-blockchains-a-deep-dive-into-the-future-of-scaling/
2. Modular blockchains: why 2025 is the year of scalable layer 2 innovation? | CodrinBA on Binance Square, acessado em julho 15, 2025, https://www.binance.com/en/square/post/23933546410889
3. What Is Eclipse Crypto? Complete Guide To The Layer-2 Blockchain ..., acessado em julho 15, 2025, https://blog.mexc.com/what-is-es-eclipse/
4. I Read Ethereum's Whitepaper So That You Don't Have To - Flipster, acessado em julho 15, 2025, https://flipster.io/en/blog/ethereum-whitepaper-explained
5. Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform (Ethereum Whitepaper) - Global Alliance for ICT and Development | GAID, acessado em julho 15, 2025, https://gaid.org/publications/blockchain-and-cryptocurrency/ethereum-a-next-generation-smart-contract-and-decentralized-application-platform-ethereum-whitepaper
6. acessado em dezembro 31, 1969,
7. FailSafe Web3 Security Report 2025, acessado em julho 15, 2025, https://getfailsafe.com/failsafe-web3-security-report-2025/
8. Why Futarchy Matters: A Clearer North Star to Guide Fledgling Crypto Projects - Galaxy, acessado em julho 15, 2025, https://www.galaxy.com/insights/research/why-futarchy-matters

9. Governance as Conflict: Constitution of Shared Values Defining Future Margins of Disagreement - MIT Computational Law Report, acessado em julho 15, 2025, https://law.mit.edu/pub/governanceasconflict
10. Internet of Smart Things - IoST: Using Blockchain and CLIPS to Make Things Autonomous, acessado em julho 15, 2025, https://www.researchgate.net/publication/319637395_Internet_of_Smart_Things_-_IoST_Using_Blockchain_and_CLIPS_to_Make_Things_Autonomous
11. [MIT IAP 2023] Modern Zero Knowledge Cryptography, acessado em julho 15, 2025, https://zkiap.com/
12. Discover the Top 5 Best Modular Blockchain Projects of 2025 - CryptoNinjas, acessado em julho 15, 2025, https://www.cryptoninjas.net/crypto/best-modular-blockchains/
13. governance/docs/constitution/pyth-dao-constitution.md at main - GitHub, acessado em julho 15, 2025, https://github.com/pyth-network/governance/blob/main/docs/constitution/pyth-dao-constitution.md
14. Top 5 Web3 Market Trends to Look Out For in 2025, acessado em julho 15, 2025, https://rocknblock.io/blog/web3-market-trends-to-look-out-for
15. Top Web3 Trends to Watch in 2024 for 2025 Success - Web3Auth Blog, acessado em julho 15, 2025, https://blog.web3auth.io/top-web3-trends-to-watch-in-2024-for-2025-success/
16. FOAM Map: Overview of the TCR Design and Incentives | by Ryan ..., acessado em julho 15, 2025, https://blog.foam.space/foam-map-overview-of-the-tcr-design-and-incentives-3a26603d3bab
17. MakerDAO | An Unbiased Global Financial System, acessado em julho 15, 2025, https://makerdao.com/
18. Some thoughts on token governance and curation — a look into a possible future for KnownOrigin | by James Morgan | Medium, acessado em julho 15, 2025, https://medium.com/@james.morgan/some-thoughts-on-token-governance-and-curation-a-look-into-a-possible-future-for-knownorigin-41ac900f8a79
19. A Survey on the Applications of Zero-Knowledge Proofs - arXiv, acessado em julho 15, 2025, https://arxiv.org/html/2408.00243v1
20. Position: The Right to AI - arXiv, acessado em julho 15, 2025, https://arxiv.org/html/2501.17899v2
21. The DeFi Revolution: An In-Depth Look Into The MakerDAO Protocol - Medium, acessado em julho 15, 2025, https://medium.com/coinmonks/the-defi-revolution-an-in-depth-look-into-makerdao-58e8e9bd4fbf
22. Overlord: Centralized Control in Highly Decentralized Systems - ASC, acessado em julho 15, 2025, https://asc.di.fct.unl.pt/~jleitao/prepdocs/TomasGabrielPrep.pdf
23. Economic DAO Governance: A Contestable Control Approach - arXiv, acessado em julho 15, 2025, https://arxiv.org/html/2403.16980v3
24. Bitcoin Hyper and the Rise of Layer 2 Tokens in the 2025 Crypto Market -

Techpoint Africa, acessado em julho 15, 2025, https://techpoint.africa/cryptoexplorer/2025/07/08/how-layer-2-solutions-are-supercharging-bitcoins-next-bull-run/

25. IEEE DASC 2025: The 23rd IEEE International Conference on Dependable, Autonomic and Secure Computing - CFP, acessado em julho 15, 2025, https://easychair.org/cfp/IEEEDASC2025
26. Zero-Knowledge Machine Learning (zkML) - Ledger, acessado em julho 15, 2025, https://www.ledger.com/academy/glossary/zero-knowledge-machine-learning-zkml
27. GG23 OSS Program Quadratic Funding Results - #20 by debuggingfuture - Gitcoin Grants, acessado em julho 15, 2025, https://gov.gitcoin.co/t/gg23-oss-program-quadratic-funding-results/20334/20
28. Zero Knowledge Machine Learning (zkML) Explained: What is zkML? - DroomDroom, acessado em julho 15, 2025, https://droomdroom.com/zero-knowledge-machine-learning-zkml-explained/
29. Five Web3 Trends To Watch In 2025: AI, DePINs, RWAs And Beyond, acessado em julho 15, 2025, https://www.forbes.com/councils/forbesbusinesscouncil/2025/01/15/five-web3-trends-to-watch-in-2025-ai-depins-rwas-and-beyond/
30. SoK: Understanding zk-SNARKs: The Gap Between Research and Practice, acessado em julho 15, 2025, https://eprint.iacr.org/2025/172.pdf
31. DAOs, Procedural Perversity and the Metaverse | Insights - Holland & Knight, acessado em julho 15, 2025, https://www.hklaw.com/en/insights/publications/2023/01/daos-procedural-perversity-and-the-metaverse
32. White - Amber Group, acessado em julho 15, 2025, https://ambergroup.io/pdf/white.pdf
33. SuperEx丨12 Web3 Trends to Watch in 2025. - Medium, acessado em julho 15, 2025, https://superex.medium.com/superex%E4%B8%A812-web3-trends-to-watch-in-2025-55191a4d8264
34. Futarchy: A Better Form of Governance - Tanishq's Blog, acessado em julho 15, 2025, https://tutorials.hashnode.dev/futarchy-a-better-form-of-governance
35. Decentralized Physical Infrastructure Networks (DePIN) - LCX, acessado em julho 15, 2025, https://www.lcx.com/decentralized-physical-infrastructure-networks-depin/
36. Ultimate Guide to DAO Tokenomics: Strategies, Models, Future Trends - Rapid Innovation, acessado em julho 15, 2025, https://www.rapidinnovation.io/post/comprehensive-guide-dao-tokenomics-key-strategies-best-practices-effective-incentive-structures
37. Eco-Tokenomics → Term - Sustainability Directory, acessado em julho 15, 2025, https://sustainability-directory.com/term/eco-tokenomics/
38. Zero knowledge proofs | Everything I Know, acessado em julho 15, 2025, https://wiki.nikiv.dev/security/cryptography/zero-knowledge-proofs
39. DePIN Infrastructure Networks Grow as Edge Computing Demand Surges -

AInvest, acessado em julho 15, 2025, https://www.ainvest.com/news/depin-infrastructure-networks-grow-edge-computing-demand-surges-2507/

40. Decentralized Physical Infrastructure Networks: Understanding The Basics - Calibraint, acessado em julho 15, 2025, https://www.calibraint.com/blog/decentralized-physical-infrastructure-networks
41. Regulating under Uncertainty: Governance Options for Generative AI, acessado em julho 15, 2025, https://www.alejandrobarros.com/wp-content/uploads/2024/08/11.pdf
42. Blockchain technology and real-time auditing: Transforming financial transparency and fraud detection in the Fintech industry - FE Gulf Publishers, acessado em julho 15, 2025, https://www.fegulf.com/index.php/gjabr/article/download/88/94
43. Autonomic Computing and Networking, acessado em julho 15, 2025, http://ndl.ethernet.edu.et/bitstream/123456789/58544/1/3.pdf
44. Plurality philosophy in an incredibly oversized nutshell - Vitalik Buterin's website, acessado em julho 15, 2025, https://vitalik.eth.limo/general/2024/08/21/plurality.html
45. (PDF) Autonomic Resilience in Cybersecurity: Designing the Self-Healing Network Protocol for Next-Generation Software-Defined Networking - ResearchGate, acessado em julho 15, 2025, https://www.researchgate.net/publication/386267410_Autonomic_Resilience_in_Cybersecurity_Designing_the_Self-Healing_Network_Protocol_for_Next-Generation_Software-Defined_Networking
46. Congressional AI: A Framework for Task Generalization and Alignment with Expert Language Models - University of Pennsylvania, acessado em julho 15, 2025, https://repository.upenn.edu/bitstreams/a59dd461-ad0b-4c43-8336-18f834b81b0f/download
47. data-centric ai governance: addressing the limitations of model-focused policies - arXiv, acessado em julho 15, 2025, https://arxiv.org/pdf/2409.17216?
48. Top Trends Shaping the Web3 Space in 2025 | Zypto, acessado em julho 15, 2025, https://zypto.com/blog/blockchain-industry/top-web3-trends-in-web3-in-2025/
49. DAOstack - Peer Production on the Crypto Commons, acessado em julho 15, 2025, https://cryptocommons.cc/daos/daostack/
50. Optimism's Retroactive Public Goods Funding (RPGF): The Perfect Hack for Ecosystem Growth | by Samuel Eric | Medium, acessado em julho 15, 2025, https://medium.com/@samykoke/optimisms-retroactive-public-goods-funding-rpgf-the-perfect-hack-for-ecosystem-growth-fc18898047c8
51. Requirements Engineering And Analysis of existing Mechanisms for, acessado em julho 15, 2025, https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/387085/R%C3%B6ssnerDappFach2018-ProspectsofDLTSystems-FinalETHZ.pdf?sequence=1&isAllowed=y
52. GG23 OSS Program Quadratic Funding Results - Gitcoin Grants ..., acessado em julho 15, 2025,

https://gov.gitcoin.co/t/gg23-oss-program-quadratic-funding-results/20334
53. Understanding the Ethereum Whitepaper - eccuity, acessado em julho 15, 2025, https://www.eccuity.com/blog/understanding-the-ethereum-whitepaper
54. An Introduction to Polkadot - polkadot-network-web-assets, acessado em julho 15, 2025, https://assets.polkadot.network/Polkadot-lightpaper.pdf
55. About Cosmos: Building the Internet of Blockchains, acessado em julho 15, 2025, https://cosmos.network/about/
56. cosmos/WHITEPAPER.md at master - GitHub, acessado em julho 15, 2025, https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md
57. Polkadot Papers, acessado em julho 15, 2025, https://polkadot.com/papers/
58. polkadot-io/polkadot-white-paper: The technical vision paper for Polkadot, a heterogeneous extensible multi-chain. - GitHub, acessado em julho 15, 2025, https://github.com/polkadot-io/polkadot-white-paper
59. whitepaper/EIGEN_Token_Whitepaper.pdf at master - GitHub, acessado em julho 15, 2025, https://github.com/Layr-Labs/whitepaper/blob/master/EIGEN_Token_Whitepaper.pdf
60. Whitepapers | EigenCloud, acessado em julho 15, 2025, https://docs.eigencloud.xyz/products/eigenlayer/concepts/whitepaper
61. EigenLayer: The Restaking Collective - GitBook, acessado em julho 15, 2025, https://2039955362-files.gitbook.io/~/files/v0/b/gitbook-x-prod.appspot.com/o/spaces%2FPy2Kmkwju3mPSo9jrKKt%2Fuploads%2F2dCfPgItRfQbX25KriQv%2Fwhitepaper.pdf?alt=media&token=d4d94480-3f01-4e63-bc92-a0658ea37aab
62. DePIN project set to power a nation's digital infrastructure - Cointelegraph, acessado em julho 15, 2025, https://cointelegraph.com/news/depin-project-set-to-power-a-nation-s-digital-infrastructure
63. Archives | EthCC[8], acessado em julho 15, 2025, https://ethcc.io/archives?subject=all&type=all&event=EthCC[8]&search=
64. Blockchain revenue sharing Demystifying Blockchain Revenue Sharing: A Comprehensive Guide - FasterCapital, acessado em julho 15, 2025, https://fastercapital.com/content/Blockchain-revenue-sharing-Demystifying-Blockchain-Revenue-Sharing--A-Comprehensive-Guide.html
65. secure model verification and privacy preservation with zk-snarks and neural networks - Open METU, acessado em julho 15, 2025, https://open.metu.edu.tr/bitstream/handle/11511/105263/TEZ_FINAL_oylum-35.pdf
66. An Empirical Analysis of Source Code Metrics and Smart Contract Resource Consumption - Edge Hill University, acessado em julho 15, 2025, https://research.edgehill.ac.uk/files/29031796/smart_contracts_and_metrics_Journal_of_Software_Evolution_and_Process.pdf
67. DePIN Explained: What is a Decentralized Physical Infrastructure Network? - TheStreet, acessado em julho 15, 2025, https://www.thestreet.com/crypto/explained/what-is-depin
68. Ethereum's Vitalik Buterin Is Worried About Crypto's Future - Time Magazine, acessado em julho 15, 2025,

https://time.com/6158182/vitalik-buterin-ethereum-profile/