# Mem-Coin: A Hybrid Architectural Framework for Decentralized AI and Bitcoin Integration

## Preamble: Executive Summary & Strategic Vision

The convergence of artificial intelligence and blockchain technology represents a paradigm shift, promising the creation of decentralized, transparent, and secure ecosystems for intelligent applications. The Mem-Coin protocol is designed to be at the forefront of this revolution, with a foundational mission to build a productive, sustainable, and decentralized AI ecosystem. Its core purpose is to transform the computationally intensive process of securing a blockchain from a "wasteful" expenditure of energy into a "useful" one, where the work performed directly contributes to the generation of valuable AI models and computational results.

However, a fundamental challenge has persistently hindered this vision: the prohibitive cost and complexity of verifying computationally intensive AI tasks on-chain. The original architectural blueprint for Mem-Coin, while visionary in its scope, relied monolithically on Zero-Knowledge Machine Learning (ZKML) for all verification. This approach, while offering unparalleled cryptographic security and privacy, imposes an unsustainable computational and economic burden known as the "prover's burden." This burden threatens the protocol's scalability, its decentralization, and its core value proposition by making participation accessible only to a small cadre of highly capitalized entities with specialized hardware.[1]

This document presents a definitive technical and strategic blueprint for a re-architected Mem-Coin protocol. It details a strategic pivot to a multi-layered, hybrid architecture that is cost-efficient, environmentally friendly, and eminently practical to implement. This new blueprint moves away from the rigid, ZKP-only model, replacing mandatory ZKML with a more pragmatic, crypto-economically secured Optimistic Proof-of-Useful-Work (PoUW) layer as the network's default mechanism. This shift dramatically reduces costs and energy consumption, democratizing participation.

The report further details a suite of synergistic innovations designed to create a robust, secure, and market-aware platform. These include a high-assurance governance and arbitration body secured by a collusion-resistant MPC-HSM committee, an autonomous AI Sentinel for proactive network security, and a formal framework for deep integration with the Bitcoin ecosystem via Drivechain technology. The document culminates in a complete specification for the protocol's immutable gRPC API, providing a robust and performant contract for all developer interactions. This comprehensive framework positions Mem-Coin not as a theoretical curiosity, but as a practical and sustainable foundation for the future of decentralized AI.

## Section 1: The Mem-Coin Hybrid Verification Architecture

This section details the core computational and verification layers of the Mem-Coin protocol. It provides a comprehensive justification for the strategic pivot to a hybrid model, deconstructing the original architecture's limitations and elaborating on the mechanics, security, and benefits of each tier in the new, more flexible design.

### 1.1. The Strategic Imperative: Mitigating the ZKP Prover's Burden

The most significant and potentially fatal bottleneck within the original Mem-Coin architecture is the immense cost and complexity associated with generating Zero-Knowledge Proofs (ZKPs) for AI computations. This "prover's burden" refers to the extreme computational overhead, time, and energy consumption required for a network participant (a "Miner") to generate the ZKP that cryptographically validates their useful AI work.[1] The protocol's own foundational documents concede this critical weakness, stating that ZKP generation "can be thousands of times more computationally expensive than the original computation itself".[1]

This burden is not merely a technical inconvenience; it is a powerful centralizing force that runs directly counter to the protocol's foundational goal of decentralization. The workloads being proven are not simple transaction batches, as in a typical ZK-rollup, but large-scale AI model training or inference tasks involving potentially trillions of operations and complex, non-linear architectures. The process of converting such a computation into a verifiable arithmetic circuit, known as arithmetization, leads to a combinatorial explosion in complexity and cost.[1]

While future research into specialized hardware like Application-Specific Integrated Circuits (ASICs) or Field-Programmable Gate Arrays (FPGAs) might eventually mitigate these costs, this path risks recreating the very centralizing dynamics seen in Bitcoin mining. The high capital expenditure for specialized ZK-acceleration hardware, combined with the exorbitant operational costs for power, would inevitably marginalize smaller participants. The ecosystem would become dominated by a few large, well-capitalized entities, destroying the network's decentralization and creating an economic paradox. If the cost to *prove* the work far exceeds the value of the work itself (the block reward plus the model's utility), the incentive structure for honest participation collapses.[1]

Therefore, addressing the prover's burden is not an incremental improvement but an absolute prerequisite for the protocol's success. The proposed hybrid model represents a strategic realignment of crypto-economic incentives. It shifts the network's default mode of operation away from a mandatory, high-cost cryptographic proof model to a more accessible, economically secured optimistic model, thereby resolving this fundamental architectural challenge.

### 1.2. Tier 1 (Default Efficiency Layer): Optimistic Proof-of-Useful-Work (PoUW)

To address the profound challenge of the prover's burden, the re-architected Mem-Coin protocol adopts an optimistic verification model as its default, baseline mechanism. This approach, heavily inspired by the design of mature and battle-tested Layer 2 optimistic rollups on Ethereum like the OP Stack and Arbitrum Orbit, fundamentally realigns the cost structure of the network.[1] It strategically trades the extreme, upfront computational expense of ZKP generation for a system of verifiable economic accountability, making network participation vastly more accessible and efficient.

The modified core protocol loop for Mem-Coin's Proof-of-Useful-Work (PoUW) operates as follows [1]:

1. **Computation:** A Miner performs the designated PoUW task, such as training a machine learning model on a specific Verifiable Data Object (VDO). This

computation is performed in a native environment, optimized for speed, potentially using standard GPU hardware.[3]

2. **Bonded Submission:** Instead of generating a ZKP, the Miner submits the results of their work to the Mem-Coin blockchain. This submission typically consists of the Content Identifier (CID) of the output data (e.g., the trained model) stored on a decentralized network like IPFS. Crucially, this submission is accompanied by a substantial economic bond—a large stake of MEM tokens that is locked as collateral. This bond serves as a powerful signal of the Miner's confidence in the correctness of their work and acts as a financial guarantee of their honesty.[1]
3. **Optimistic Acceptance & Challenge Period:** The network "optimistically" accepts the submission as provisionally valid, assuming it is correct by default.[2] This allows the result of the useful work to be recognized and integrated into the network's state quickly, without the significant latency associated with generating and verifying a complex proof. Following this provisional acceptance, a predefined "challenge period" commences. This window, typically lasting around seven days as is standard in established optimistic rollups, provides an opportunity for any other network participant to dispute the Miner's submission if they believe it to be fraudulent.[1]

This paradigm shift fundamentally alters the network's cost dynamics. The immense, universal, and mandatory computational burden of ZKP generation is eliminated for the vast majority of cases. The intensive verification work is now performed only by the original Miner and any independent Challengers who voluntarily choose to re-execute the computation, rather than being a mandatory cost imposed on every single block production cycle.

### 1.3. The Challenge-Response Protocol: Securing PoUW with Game Theory

The security of the optimistic model is not based on pure cryptography but on a robust challenge-response protocol. This protocol functions as a crypto-economic game meticulously designed to make fraud unprofitable, ensuring that while anyone can make a claim, only the truthful claim will ultimately be finalized by the network.[3] The mechanics of this game are critical to its success and are heavily influenced by the fraud-proof systems of optimistic rollups and frameworks like

opML.[1]

The process unfolds as follows:

- **Permissionless Challenge Initiation:** The security of the network is decentralized and permissionless. Any participant in the network, having independently executed the same PoUW task and detected a discrepancy in the Miner's submitted result, can act as a "Challenger" and initiate a dispute. To prevent spam or frivolous challenges that could disrupt the network, the Challenger must also post an economic bond. If the challenge is ultimately proven to be baseless, the Challenger forfeits their bond, creating a strong disincentive against malicious or careless challenges.[1] This model relies on the "any-trust assumption," which posits that the system remains secure as long as there is at least one honest and vigilant actor in the network willing to challenge fraudulent claims.[3] This is a far lower and more realistic security assumption than requiring a majority of the network's computational power to be honest, as in traditional Proof-of-Work systems.
- **The Interactive Bisection Game:** Re-executing an entire AI training process on-chain to resolve a dispute would be prohibitively expensive and would defeat the purpose of the optimistic model. Instead, the protocol employs an **interactive bisection game**, a technique pioneered by optimistic rollups like Arbitrum and adapted for machine learning in frameworks like opML.[1] In this game, the Miner (the original claimant) and the Challenger engage in an off-chain, peer-to-peer protocol where they recursively narrow down their point of disagreement. They start by dividing the entire computational trace of the AI task in half and agreeing on the machine's state at the midpoint. They continue this bisection process, repeatedly halving the disputed segment, until they have isolated the single, specific computational instruction where their results first diverge.[1]
- **On-Chain Arbitration:** Once the dispute has been narrowed down to a single instruction—for example, a single matrix multiplication or even a single floating-point operation—that one step is submitted as a "one-step proof" to a smart contract on the Mem-Coin chain. This single computational step is computationally trivial for the blockchain's virtual machine to execute and verify. However, it serves as a definitive and impartial arbiter, cryptographically proving which party's computation was correct at the precise point of divergence.[1]
- **The Crypto-Economic Loop:** The system is secured by a powerful incentive and punishment mechanism known as **slashing**. If the on-chain arbitration determines that the original Miner's submission was fraudulent, their entire staked bond is "slashed"—confiscated by the protocol's smart contract. The magnitude of this bond is carefully calibrated by network governance to be substantially larger than any profit a Miner could possibly extract from having a fraudulent state

temporarily accepted. To complete the incentive loop, a significant portion of the slashed bond is awarded to the successful Challenger.[1] This creates a powerful "bounty hunter" dynamic, where network participants are financially motivated to actively seek out, verify, and prove fraud, making the network effectively self-policing. A rational, profit-seeking Miner will not attempt to cheat if the expected value of doing so is demonstrably less than the guaranteed loss they will incur from being caught.

### 1.4. Addressing a Critical Challenge: Non-Determinism in AI Computations

A critical and non-trivial challenge arises when applying fraud proofs to AI and ML computations: non-determinism. Standard ML execution environments can produce slightly different results across different hardware or even on the same hardware during different runs. This can be due to factors like parallel GPU thread scheduling, the order of floating-point arithmetic operations, or differences in underlying libraries.[1] This non-determinism would break the interactive bisection game, which fundamentally relies on the ability of two honest parties to execute the exact same computation and arrive at the exact same bit-for-bit result. Any discrepancy, no matter how small, would be indistinguishable from fraud.

Fortunately, this is a recognized problem with a known and practical solution path. The existence and open-source nature of projects like opML (Optimistic Machine Learning on Blockchain) dramatically de-risk and accelerate the implementation of this critical component for Mem-Coin.[2] Instead of undertaking a massive research project to build a deterministic fraud-proof system for ML from scratch, the protocol can adapt an existing, robust framework.

The opML academic paper and its associated implementation directly address the non-determinism issue by enforcing deterministic execution.[2] The proposed solution involves two key techniques:

1. **Fixed-Point Arithmetic:** Standard floating-point arithmetic is replaced with fixed-point arithmetic (quantization). This removes the potential for minute variations in how floating-point numbers are handled across different processor architectures.
2. **Software-Based Floating-Point Libraries:** For operations that still require floating-point precision, software-based libraries (like softfloat) are utilized.

These libraries implement floating-point standards in software, guaranteeing that calculations are performed identically regardless of the underlying hardware.

By adopting these techniques, the ML execution process becomes perfectly reproducible and consistent across different machines. This makes it fully compatible with a fraud-proof system, as any two honest actors running the computation will now be guaranteed to produce identical outputs, allowing the bisection game to function correctly. This transformation of a complex research problem into a more manageable engineering task is a crucial enabler for the entire optimistic PoUW layer.

### 1.5. Tier 2 (Premium Privacy Layer): On-Demand ZKML PoUW

A complete abandonment of Zero-Knowledge Machine Learning is not the recommended course of action. The privacy guarantees afforded by ZKPs—the ability to prove computational correctness without revealing the underlying data or the proprietary model architecture—are an exceptionally valuable feature. This is particularly true for enterprise and commercial applications that deal with sensitive information such as medical records, financial data, or high-value, proprietary AI models.[1] A protocol that can attract and securely handle these high-value workloads will possess a significant and durable competitive advantage.

Therefore, the hybrid architecture retains ZKML not as a discarded technology, but as a specialized, optional, and premium feature. This creates a flexible marketplace for verification, reframing the "Optimistic vs. ZK" debate from a mutually exclusive choice into a tiered service offering that caters to diverse user needs. This is a mature design pattern that acknowledges that not all users have the same priorities or budget, allowing the protocol to capture a much wider market than a rigid, one-size-fits-all solution.

The workflow for this premium privacy layer is as follows [1]:

- **User Specification:** A user, DAO, or corporation seeking to perform a computation on sensitive data or with a valuable proprietary model can specify that their PoUW task is "ZK-required."
- **Premium Fee:** To compensate the network for the immense cost of ZKP generation, the user pays a premium network fee.
- **Specialized Miner:** This fee is used to incentivize a specialized Miner, likely one with the necessary ZK-acceleration hardware, to undertake the additional

computational burden of generating the ZKP.
- **Cryptographic Verification:** The Miner submits the result along with the ZKP. Network validators then perform a fast and cheap verification of the proof, providing a pure, unbreakable cryptographic guarantee of the work's integrity and privacy.

This tiered model transforms Mem-Coin into a powerful and market-aware platform, capable of serving the broad market that prioritizes cost and efficiency while simultaneously catering to the high-value niche that demands absolute privacy and confidentiality.

### 1.6. Foundational Data Layer: Verifiable Data Objects (VDOs)

Underpinning the entire verification architecture is the protocol's foundational data layer, centered on the Verifiable Data Object (VDO). The VDO is the atomic unit of data within the Mem-Coin ecosystem, designed to be both highly compressed and cryptographically verifiable.[1]

The VDO structure is derived from the memvid library and employs a novel technique for data storage and compression. It stores text and its corresponding semantic vector embeddings as a sequence of QR codes within a standard MP4 video file. This unconventional approach reportedly achieves remarkable compression ratios, 50-100 times greater than conventional vector databases, making the storage and transmission of large datasets more efficient.

The lifecycle of a VDO is as follows:

1. A memvid artifact is created.
2. This artifact is stored on a decentralized storage network, such as the InterPlanetary File System (IPFS).
3. The unique Content Identifier (CID) generated by IPFS for that artifact is then recorded on the Mem-Coin blockchain.

This final step elevates the file from a simple off-chain object to a canonical, content-addressable, and immutable VDO. It serves as the verifiable and tamper-proof input for all subsequent PoUW tasks on the network.[1] To address the critical data availability problem inherent in off-chain storage (i.e., ensuring the data pointed to by the CID is actually accessible), the protocol integrates Data Availability

Sampling (DAS). This technique allows network participants, including low-powered light clients, to probabilistically verify that the complete off-chain data is available by sampling only a few small pieces of it. This dramatically lowers the hardware burden and cost of network participation and verification, preventing the state bloat that can lead to centralization.[1] This synergistic design ensures that the verification layers have reliable access to the large, verifiable datasets they require to function.

## Section 2: High-Assurance Governance and Arbitration

While the PoUW layers handle the high-frequency task of block-by-block verification, a decentralized protocol requires an ultimate root of trust for low-frequency, high-stakes decisions like protocol upgrades and the resolution of catastrophic disputes. This section details the protocol's governance and arbitration layer, explaining why the proposed MPC-HSM model is a cryptographically and philosophically superior choice compared to more common but fundamentally flawed federated approaches.

### 2.1. The Fallacy of Federated Trust: Deconstructing the Collusion Attack Vector

A common architectural pattern for high-security functions in enterprise systems and cross-chain bridges is a federated model, which could be conceptualized for Mem-Coin as a "Distributed HSM Verification Ledger" (DHVL). In such a system, a consortium of known, trusted organizations would each operate a Hardware Security Module (HSM) to hold a private key. A high-stakes action would require a threshold M-of-N of these members to sign the transaction with their HSM-secured keys.[1]

However, this model suffers from a critical and fundamental weakness: the risk of **federation collusion**. While an HSM provides excellent physical and logical protection against the *theft* of a private key from its hardware enclosure, it provides no protection against the *misuse* of that key by its legitimate, authorized operator.[1] The security of the entire federated system collapses from a cryptographic problem to a human one, resting on the fragile, trust-based assumption that a sufficient number of the human operators or organizations will remain honest, independent, and uncoerced at all times.

This creates a dangerous attack surface that targets the human layer, not the technology [1]:

- **Coercion and Bribery:** An attacker does not need to break FIPS-certified cryptography. Instead, they can bribe, blackmail, or legally compel a threshold of M federation members. These compromised operators can then use their perfectly secure HSMs to sign a fraudulent transaction. The HSM will dutifully perform the signing operation, having no concept of the operator's malicious intent.
- **Centralization of Trust:** This model inherently centralizes trust in a small, identifiable, and therefore easily attackable group of entities. If M members form a cartel, they can unilaterally control the protocol, censor transactions, or steal funds, destroying the network's core properties of decentralization and censorship resistance.

This vulnerability is fundamental to any system based on a simple multi-signature scheme, even one where each key is hardware-backed. The model replaces a trustless cryptographic system with a far weaker trust-based one, creating an unacceptable security risk for a foundational protocol like Mem-Coin. The choice to reject this model is a fundamental statement of the protocol's philosophy: it is a choice to "verify math" rather than "trust reputations," a core tenet of the Web3 ethos.

### 2.2. Tier 3: The MPC-HSM Committee as a Cryptographically Secure Root of Trust

To provide a maximally secure root of trust, the Mem-Coin architecture implements a committee based on a synergistic combination of Secure Multi-Party Computation (MPC) and Hardware Security Modules (HSMs). This MPC-HSM architecture represents the current gold standard for institutional-grade digital asset security and directly mitigates the collusion risks inherent in federated models.

The mechanism provides two powerful, independent, and complementary layers of security:

1. **Cryptographic Security via MPC:**
    - **Mechanism:** A committee of N independent entities (who do not need to trust

each other) collaboratively generates a single logical private key. This key, however, is never assembled in its entirety in any single location. It is created and immediately split into encrypted mathematical "shards" or "shares." Each of the N participating parties receives and holds only one of these shards.

   - **Distributed Signing:** To generate a signature for a governance action, a threshold t-of-N of the members must engage in an interactive, multi-round cryptographic protocol. Each party uses its unique key shard to perform a series of calculations and exchange intermediate, encrypted cryptographic data with the other participants. At the end of this protocol, a single, valid digital signature is produced. Crucially, no single party ever had access to any other party's key shard, nor was the complete private key ever reconstructed in any single location, not even in memory.[1]
   - **Collusion Resistance:** This property provides a monumental security advantage. An attacker who compromises t-1 parties gains absolutely nothing of value; they cannot combine the shards offline to forge a signature. To create a fraudulent signature, an attacker must compromise a threshold of t parties *simultaneously* and force them all to participate in the live, interactive signing protocol at the exact same time. This dramatically raises the difficulty, coordination complexity, and cost of a successful attack compared to the much simpler task of collecting M independent signatures in a federated model. This protects against **internal collusion**.
2. **Hardware Security via HSMs:**
   - **Mechanism:** The cryptographic security of MPC is further hardened by combining it with the physical security of HSMs. Each of the N participating entities operates their own HSM (on-premises or cloud-based). The MPC key generation protocol is executed such that each party's unique key shard is generated directly inside their HSM's secure cryptographic boundary and configured to be non-exportable.
   - **Hardened Security:** When a signature is required, the interactive MPC protocol takes place between the HSMs. Each HSM performs its part of the computation internally using its protected key shard. This protects each individual key shard from theft, extraction, or malware, even if a participant's host server, network, and entire software stack are completely compromised. This protects against **external hacking** of individual committee members.

The existence of this high-assurance arbitration body provides the entire network with the confidence to operate optimistically by default. The community can tolerate the risks of a 7-day challenge period because it knows there is a robust, collusion-resistant "court of last resort" to handle worst-case scenarios. The security layers are not independent; they are mutually reinforcing. The strength of the MPC-HSM committee enables the efficiency of the optimistic layer.

The role of this committee is strictly limited to low-frequency, high-stakes events, ensuring it does not become a bottleneck for routine network operations. Its functions include:

- Serving as a final arbiter for highly contentious fraud proof disputes.
- Authorizing critical protocol upgrades as a hardware-secured backstop to the on-chain DAO.
- Governing the release of funds from the network's treasury.

## Section 3: RFC-MEM-001: A Drivechain Framework for Bitcoin Stack Integration

This section is presented as a formal Request for Comments (RFC) information paper. It provides a complete technical specification for a standardized framework to make Mem-Coin's resources available to the Bitcoin ecosystem, positioning Mem-Coin as a symbiotic computational layer for Bitcoin.

---

**RFC:** MEM-001

**Title:** A Drivechain Framework for Bitcoin Stack Integration

**Author(s):** Mem-Coin Protocol Architects

**Status:** Informational

**Date:** August 2, 2025

### 3.1. Abstract & Motivation

This document specifies a framework for establishing a trust-minimized, two-way peg between the Bitcoin blockchain and the Mem-Coin sidechain. The proposed mechanism is a direct implementation of Drivechain technology, as detailed in Bitcoin Improvement Proposals (BIP) 300 and 301.

The primary motivation for this framework is twofold. First, it aims to provide the Bitcoin ecosystem with access to advanced, productive computational capabilities, specifically large-scale AI/ML model training and inference, without altering Bitcoin's core protocol.[7] Second, it seeks to create a new, sustainable source of transaction fee revenue for Bitcoin miners through a process known as Blind Merged Mining. This enhances Bitcoin's long-term security budget, which is a critical concern as the block subsidy diminishes over time.[9] This framework positions Mem-Coin as a symbiotic Layer 2 solution that extends Bitcoin's utility, rather than a competitive Layer 1 platform.[11]

### 3.2. Specification: A Two-Way Peg via Hashrate Escrow and Blind Merged Mining

The framework is built upon the two core components of Drivechain technology.[7]

- **Sidechain Security (Blind Merged Mining - BIP 301):** Bitcoin miners secure the Mem-Coin sidechain by including a cryptographic commitment to Mem-Coin blocks within the Bitcoin blocks they mine. This process is "blind" because it does not require Bitcoin miners to run a full Mem-Coin node or validate the sidechain's transactions. They are incentivized to do so by earning transaction fees from the Mem-Coin network, paid in Bitcoin.[7] This mechanism allows the Mem-Coin sidechain to inherit the full security of Bitcoin's massive hashrate.
- **Two-Way Peg Mechanism:**
    - **Peg-In (Bitcoin to Mem-Coin):** A user transfers assets to the sidechain by sending BTC to a special OP_DRIVECHAIN output script on the Bitcoin mainchain. This transaction effectively locks the BTC. The Mem-Coin sidechain's consensus rules recognize this mainchain transaction after a confirmation period, and an equivalent amount of a representative token (e.g., memBTC) is minted on the Mem-Coin network.[11]
    - **Peg-Out (Mem-Coin to Bitcoin) via Hashrate Escrow (BIP 300):** A user initiates a withdrawal on the Mem-Coin sidechain. This withdrawal request is aggregated with others into a "bundle." For this bundle to be considered valid and for the locked BTC to be released on the mainchain, it must be approved by a supermajority of Bitcoin miners' hashrate. This voting process is extended over a very long period, typically 3-6 months (e.g., 13,150 blocks).[7]

> This extreme delay serves as the core security feature. It makes a theft attack by a rogue miner majority incredibly difficult to execute, prohibitively expensive to sustain, and transparently auditable by the entire community, giving honest users ample time to react socially or economically.

There is a profound architectural resonance between the security models of Drivechain and Mem-Coin's Optimistic PoUW. Both rely on a long delay period as a core security feature—months for Drivechain withdrawals, days for PoUW challenges. This shared philosophy of "security through verifiable delay and social consensus" makes the two systems a natural and coherent fit. Both systems convert a potential brute-force attack into a slow, observable, and socially contestable process, demonstrating a consistent end-to-end security philosophy for the entire integrated stack.

### 3.3. Protocol Messages and State Transitions

The Drivechain mechanism, as defined in BIP 300, introduces six new blockchain messages to manage the sidechain lifecycle, from creation to withdrawal processing. Any Bitcoin client or stack wishing to support this RFC MUST be able to parse, validate, and interpret these messages. The following table summarizes these messages.[7]

| Message ID | Message Name | Purpose | Key Parameters |
|---|---|---|---|
| M1 | Propose New Sidechain | A transaction that proposes the creation of a new sidechain slot on the Bitcoin blockchain. | nSidechain (slot number), sidechainTitle, sidechainDescription |
| M2 | ACK Sidechain Proposal | A miner signal within a coinbase transaction that acknowledges (votes for or against) a pending sidechain proposal. | nSidechain, vote (upvote/downvote) |

| | | | |
|---|---|---|---|
| M3 | Propose Bundle | A transaction that proposes a bundle of withdrawal transactions from a specific sidechain for miner approval. | nSidechain, hashBundle (hash of withdrawal data) |
| M4 | ACK Bundle | A miner signal within a coinbase transaction that acknowledges (votes for or against) a pending withdrawal bundle. | nSidechain, hashBundle, vote (upvote/downvote) |
| M5 | Deposit | A standard Bitcoin transaction that sends BTC to the sidechain's OP_DRIVECHAIN UTXO, acting as a peg-in. | OP_DRIVECHAIN output, amount |
| M6 | Withdrawal | A transaction that spends the sidechain's OP_DRIVECHAIN UTXO to release BTC back to the mainchain after a bundle has been approved by miners. | CTIP (Critical Transaction Input Pointer), withdrawal outputs |

### 3.4. Security Considerations and Miner Incentives

The primary security concern raised by critics of the Drivechain model is the "miners-can-steal" vector, where a 51% hashrate majority could collude to approve a fraudulent withdrawal bundle and steal the funds locked in a sidechain's UTXO.[14] The primary mitigation for this risk is the Hashrate Escrow mechanism itself. The 3-6 month voting period makes such an attack extremely transparent and slow. The

Bitcoin community would have ample time to observe the malicious voting, identify the participating mining pools, and orchestrate a social or technical response, such as a user-activated soft fork (UASF) to invalidate the theft. The attack is therefore not just a technical problem but a socio-political one, with a prohibitively high cost in terms of reputation and potential disruption to the mainchain itself.[18]

The framework is sustained by clear miner incentives. Blind Merged Mining provides a direct financial incentive for Bitcoin miners to secure the Mem-Coin sidechain. They earn additional transaction fees, paid in BTC, for including Mem-Coin's block commitments in their mined blocks.[10] This aligns their economic self-interest with the health and security of the sidechain, creating a symbiotic relationship that strengthens both networks.

By choosing the Drivechain model, Mem-Coin makes a specific and strategic alignment with a particular vision for Bitcoin's future. This is not merely a technical choice but also a social one that positions Mem-Coin to be a flagship application if and when BIP 300 and 301 are adopted by the Bitcoin community. While this ties the protocol's integration path to the outcome of the ongoing Drivechain debate, it represents a strong bet on a future where Bitcoin embraces layered innovation.[8]

## Section 4: The Mem-Coin gRPC API Specification

This section provides a formal and detailed specification for the gRPC (gRPC Remote Procedure Call) API, which serves as the primary programmatic interface for all interactions with the Mem-Coin protocol. The design is guided by principles of high performance, strong typing, resource-orientation, and a novel interpretation of immutability that aligns with blockchain's core properties.

### 4.1. Design Principles: Resource-Orientation and Immutability

The choice of gRPC over alternatives like REST is a deliberate one, signaling that the protocol is designed for high-performance, system-to-system integration (e.g., microservices, backend clients, other blockchains) rather than direct browser interaction. In a decentralized context where all participants must operate on a non-ambiguous and verifiable contract, the tight coupling and strict schema enforcement of gRPC is a critical feature, not a bug.[20] It prioritizes performance, type safety, and contractual rigidity, which are paramount for a deterministic distributed system.

The API design is governed by the following core principles:

- **Resource-Orientation:** The API is structured around resources, which are the fundamental nouns of the system. This approach, heavily influenced by Google's API Improvement Proposals (AIPs), provides a consistent and predictable structure for developers.[22] Core resources include
  VDO, PoUWTask, Challenge, GovernanceProposal, etc.
- **Protocol Buffers (Protobufs):** The API surface, including all services, methods, and message structures, is defined using Protocol Buffers (version 3). This provides an efficient binary serialization format, a strongly-typed contract, and language-agnostic code generation, which is essential for a polyglot ecosystem.[20]
- **Immutability:** This is a novel design principle for the API, inspired by immutable infrastructure patterns and the append-only nature of blockchains.[25] Instead of methods that mutate resources in-place (e.g.,
  UpdateTask), the API favors append-only and create-on-change patterns. For example, to challenge a task, a client does not update the PoUWTask resource; instead, it calls a method that creates a new Challenge resource that is immutably linked to the task. This approach produces a clear, auditable history of state changes, simplifies client-side state management, and drastically reduces the potential for state-related bugs and race conditions.[27] It forces developers to think in terms of event sourcing, which is philosophically consistent with the underlying blockchain.

### 4.2. Service Definitions (Protocol Buffers)

The following tables and code blocks define the primary services and message structures of the Mem-Coin API.

| Service | Method | Request Message | Response Message | Streaming Type | Description |
|---|---|---|---|---|---|
| PoUWServic | SubmitPoUW | SubmitPoUW | SubmitPoUW | Unary | Submits a |

| | | | | | |
|---|---|---|---|---|---|
| e | Task | TaskRequest | TaskResponse | | new PoUW task for execution and optimistic verification. |
| PoUWService | GetPoUWTask | GetPoUWTaskRequest | PoUWTask | Unary | Retrieves the current state of a specific PoUW task. |
| PoUWService | WatchPoUWTask | WatchPoUWTaskRequest | stream PoUWTask | Server-Streaming | Subscribes to real-time state updates for a specific PoUW task. |
| PoUWService | ChallengeTask | ChallengeTaskRequest | ChallengeTaskResponse | Unary | Initiates a challenge against a submitted PoUW task result. |
| PoUWService | ExecuteBisectionGame | stream BisectionStep | stream BisectionStep | Bidirectional | Conducts the real-time interactive bisection game for dispute resolution. |
| Governance Service | SubmitProposal | SubmitProposalRequest | Governance Proposal | Unary | Submits a new proposal for the MPC-HSM committee to vote on. |
| Governance Service | GetProposal | GetProposalRequest | Governance Proposal | Unary | Retrieves the state and |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | vote tally of a governance proposal. |
| BitcoinBridgeService | InitiatePegIn | InitiatePegInRequest | PegInStatus | Unary | Provides proof of a Bitcoin deposit to mint memBTC on the sidechain. |
| BitcoinBridgeService | ProposePegOutBundle | ProposePegOutBundleRequest | PegOutBundle | Unary | Submits a withdrawal request to be included in the next peg-out bundle. |
| SentinelService | StreamAlerts | StreamAlertsRequest | stream SentinelAlert | Server-Streaming | Subscribes to a real-time feed of security alerts from the AI Sentinel. |

Below are example Protobuf definitions for some of the core message types.

Protocol Buffers

```
// File: memcoin/api/v1alpha/pouw.proto
syntax = "proto3";

package memcoin.api.v1alpha;
```

```
import "google/protobuf/timestamp.proto";

// Represents a single Proof-of-Useful-Work task in the system.
// This resource is immutable; its state is defined by the events
// that reference it, such as submissions and challenges.
message PoUWTask {
  string name = 1; // Resource name, e.g., "pouwTasks/12345"
  string vdo_cid = 2; // IPFS CID of the input Verifiable Data Object.
  string task_definition = 3; // Describes the AI computation to be performed.
  google.protobuf.Timestamp create_time = 4;
  TaskStatus status = 5;
  string current_submission_id = 6; // ID of the latest submission for this task.
}

enum TaskStatus {
  TASK_STATUS_UNSPECIFIED = 0;
  PENDING_SUBMISSION = 1;
  CHALLENGE_PERIOD = 2;
  FINALIZED = 3;
  IN_DISPUTE = 4;
}

// Represents a Miner's submission of results for a PoUW task.
message Submission {
  string name = 1; // Resource name, e.g., "pouwTasks/12345/submissions/abcde"
  string miner_address = 2;
  string result_cid = 3; // IPFS CID of the computed result (e.g., trained model).
  string bond_amount = 4; // The amount of MEM tokens staked as a bond.
  google.protobuf.Timestamp submission_time = 5;
}

// Represents a challenge initiated against a submission.
message Challenge {
  string name = 1; // Resource name, e.g., "submissions/abcde/challenges/fghij"
  string challenger_address = 2;
  string bond_amount = 3; // The amount of MEM tokens staked by the challenger.
  google.protobuf.Timestamp challenge_time = 4;
}

// Request to submit a new PoUW task.
```

```
message SubmitPoUWTaskRequest {
 string vdo_cid = 1;
 string task_definition = 2;
}

// Response after submitting a new PoUW task.
message SubmitPoUWTaskResponse {
 PoUWTask task = 1;
}
```

### 4.3. Streaming Patterns for Real-Time Interaction

A key advantage of gRPC is its native support for persistent, bidirectional streaming over HTTP/2, which is leveraged for several critical, real-time interactions within the protocol.[28]

- **Server-Streaming:** This pattern is ideal for use cases where a client needs to receive a continuous stream of updates from the server. The WatchPoUWTask RPC, for example, allows a client to subscribe to a task and receive real-time PoUWTask messages as its status changes (e.g., from PENDING_SUBMISSION to CHALLENGE_PERIOD to FINALIZED). Similarly, the SentinelService.StreamAlerts RPC provides a live feed of security alerts, pushing them to subscribers as they are generated.[29] This is far more efficient than traditional polling.
- **Bidirectional-Streaming:** This pattern is essential for complex, interactive protocols. The ExecuteBisectionGame RPC uses a bidirectional stream to facilitate the off-chain dispute resolution process. The Miner and Challenger can exchange a sequence of state proofs and intermediate machine states over a single, long-lived gRPC connection. The streams operate independently, allowing for efficient, low-latency, back-and-forth communication until the single point of disagreement is isolated.[29]

### 4.4. Error Handling, Versioning, and Backward Compatibility

To ensure a robust and developer-friendly experience, the API adheres to established best practices for error handling and evolution.

- **Error Handling:** The API adopts Google's standard error model, which uses a canonical set of error codes (e.g., NOT_FOUND, INVALID_ARGUMENT, PERMISSION_DENIED). This provides clients with a consistent and predictable way to handle errors across all services.[22] More detailed, domain-specific error information can be attached via error details metadata.
- **Versioning and Compatibility:** API evolution is managed carefully to prevent breaking changes for clients.
    - The API version is clearly indicated in the Protobuf package name (e.g., memcoin.api.v1alpha).[22]
    - Strict backward-compatibility rules are enforced for all changes to .proto files. For example, field numbers must never be changed or reused, and new fields must be added as optional. Fields are never removed; they are marked as deprecated instead. This ensures that older clients can continue to communicate with newer server versions without failing to parse messages.[22]

## Section 5: The AI Sentinel and Hybrid Monetary Model

This section details the final two pillars of the Mem-Coin architecture: an autonomous AI agent for proactive security and a pragmatic monetary framework designed for regulatory compliance and integration with the traditional financial system.

### 5.1. The AI Sentinel: Autonomous Security and Network Intelligence

While the protocol's structural and crypto-economic layers provide robust static defenses, a dynamic and intelligent system is required for real-time threat detection and adaptive response. The **AI Sentinel** is an autonomous, generative AI agent designed to function as the continuous security and intelligence immune system for the entire Mem-Coin ecosystem.

The Sentinel's architecture consists of three core components [1]:

1. **Data Ingestion Layer:** The agent is designed to be omniscient with respect to network activity, continuously ingesting real-time data streams from all protocol

layers. This includes on-chain transaction graphs, PoUW submissions and challenges, NFT minting events, and user behavior patterns.

2. **Analytical Core:** This is the Sentinel's "brain," powered by generative AI models (e.g., Generative Adversarial Networks or autoencoders). Its primary function is advanced **anomaly detection**. Instead of relying on static rules that only catch known attacks, the Sentinel is trained on vast datasets of legitimate network activity to build a highly nuanced, evolving baseline of "normal" behavior. It then identifies any activity that deviates significantly from this baseline as a potential threat.[1] This approach allows it to flag novel and unforeseen types of fraud (e.g., sophisticated Sybil attacks, market manipulation) as suspicious outliers without needing to be explicitly reprogrammed.
3. **Action and Reporting Layer:** When an anomaly exceeds a predefined risk threshold, the Sentinel takes automated action. This primarily involves generating real-time, detailed alerts routed to the relevant parties (e.g., the MPC-HSM committee, a bank's compliance department, or smart contract developers). For critical threats, it could be granted limited authority to take defensive measures, like temporarily quarantining a suspicious transaction pending human review.

This design creates a unique and powerful "reflexive security" property. The network's primary economic activity—the Proof-of-Useful-Work—involves generating vast quantities of structured AI/ML computational traces. This very output becomes the perfect, high-quality training data for the Sentinel's own security models. The more the network is used for its intended purpose, the richer the dataset becomes, and the smarter and more effective the Sentinel's AI becomes. This creates a positive feedback loop where economic activity directly fuels and enhances network security, a synergy not present in other blockchains where the security mechanism is divorced from application-layer activity.[1]

A cornerstone of the Sentinel's design is the **Immutable Audit Dashboard**. Every piece of data ingested, every analysis performed, and every alert generated by the Sentinel is cryptographically hashed and committed to a dedicated, immutable ledger on the Mem-Coin chain itself. This creates a permanent, tamper-proof, and fully auditable log of all security monitoring activities, providing unprecedented transparency for regulators, participants, and the public.

### 5.2. The Hybrid Monetary Model: A Bridge to Traditional Finance

To achieve widespread adoption and integrate with the global financial system, a protocol must operate within existing regulatory and monetary structures. The Mem-Coin protocol overlays a regulated, **two-tier hybrid monetary model** onto its core decentralized architecture. This model is a pragmatic strategic choice, designed as a "Trojan horse" for mainstream adoption by building a bridge to the existing financial world rather than attempting to replace it entirely.[1] It sacrifices a degree of permissionlessness at the currency issuance layer to gain massive potential benefits in liquidity, user trust, and regulatory compliance.

The system is structured as follows [1]:

- **Tier 1: The Central Monetary Authority:** At the apex is a governing body, analogous to a central bank. This authority sets overall monetary policy, manages systemic risk, and—most importantly—licenses and regulates the participants in the second tier. It does not interact directly with the public.
- **Tier 2: Licensed Intermediaries and Producers:** This tier consists of all entities granted the right to mint or distribute Mem-Coin. This includes both traditional financial institutions and individual network participants.
  - **Licensed Financial Institutions:** Regulated entities like commercial banks can be licensed to mint Mem-Coin, for example, by issuing it as loans or in exchange for fiat deposits, subject to capital adequacy and other rules.
  - **Licensed Individual Producers:** Citizens who participate in the PoUW consensus mechanism are also considered licensed producers. The block rewards they earn are recognized as newly issued, legitimate Mem-Coin.

A core innovation of this model is the use of Non-Fungible Tokens (NFTs) to manage minting rights and provide a verifiable, immutable record of provenance for every unit of currency.[1]

- **Minting License NFTs:** The Tier 1 authority issues "Minting License NFTs" to all approved Tier 2 participants. The protocol's minting smart contracts are programmed to only execute for wallets holding a valid license NFT.
- **Branded Insignia NFTs:** Each time a new block of Mem-Coin is minted, the transaction also generates a unique "Insignia NFT" that is immutably linked to that block of coins. This NFT contains metadata identifying its origin, creating a transparent "brand library" for the entire money supply (e.g., "JPMorgan-Chase-Mem-Coin-Series-B" or "Citizen-Miner-XYZ-PoUW-Reward-Block-12345"). This provides a level of transparency and auditability that financial regulators currently can only dream of.

This structure provides seamless and compliant on-ramps and off-ramps. A citizen who mints a Mem-Coin via PoUW can deposit it at their commercial bank. The bank verifies the coin's authenticity via its Insignia NFT and credits the citizen's standard bank account with the equivalent fiat value. The citizen gains immediate access to the global financial system, and the bank holds the Mem-Coin as a Tier 1 digital asset on its balance sheet.[1] This creates a powerful economic flywheel where computational contribution is directly and seamlessly convertible into real-world purchasing power.

## Section 6: Strategic Analysis and Conclusion

This final section provides a series of comparative analyses to strategically position the Mem-Coin hybrid architecture within the broader market landscape. It synthesizes the report's findings and culminates in a clear and unequivocal recommendation for the protocol's future trajectory.

### 6.1. Comparative Analysis: Positioning Mem-Coin in the Ecosystem

To fully appreciate the strategic advantages of the proposed pivot, it is essential to compare the hybrid architecture against both its original monolithic design and the incumbent leaders of the blockchain market. The following tables provide a clear, evidence-based assessment of these comparisons.

The first table highlights the internal benefits of moving from the ZKML-only model to the proposed hybrid architecture. It demonstrates a clear superiority across nearly every key metric related to cost, accessibility, and practicality, directly addressing the core challenges that motivated the redesign.[1]

| Metric | Original Mem-Coin (ZKML-Only) | Proposed Hybrid Architecture | Justification/Analysis |
|---|---|---|---|
| **Default Verification Cost** | Very High | Very Low | The hybrid model eliminates mandatory ZKP generation, replacing it with a |

| | | | |
|---|---|---|---|
| | | | low-cost bonded submission. Intensive computation is only required in the rare event of a challenge.[1] |
| **Power Consumption** | Very High | Very Low | Removing the energy-intensive ZKP generation from the standard workflow dramatically reduces the network's overall energy footprint.[1] |
| **Privacy Guarantees** | Always On (Mandatory) | On-Demand (Premium) | The hybrid model makes privacy an optional, paid feature, better aligning cost with specific user needs and expanding the addressable market.[1] |
| **Miner Hardware** | Specialized (ZK ASICs/FPGAs) | Standard (Commercial GPUs) | Optimistic verification lowers the barrier to entry for Miners, promoting greater decentralization of network producers.[1] |
| **Miner Capital** | Low (Computational Cost) | High (Staked Bonds) | The security model shifts from a high operational expenditure (energy) to a high capital expenditure (locked tokens), which is non-consumptive.[1] |
| **Resistance to Cheating** | Cryptographic (Unbreakable) | Crypto-economic (Rational Deterrence) | ZKPs offer absolute mathematical proof. The optimistic model makes cheating an economically irrational act through the threat of large, |

| | | | |
|---|---|---|---|
| | | | slashable bonds.[1] |
| **Transaction Finality** | Fast (ZKP verification time) | Slow (7-day challenge window) | This is the primary trade-off. The optimistic model requires a delay for challenges, which is deemed an acceptable compromise for the AI use case.[1] |
| **Architectural Complexity** | Uniformly High | Tiered (Simple Default) | The default path for participation is vastly simpler. Complexity is strategically isolated in optional or low-frequency layers.[1] |

The second table positions the Mem-Coin hybrid architecture within the broader market, comparing it against the two leading incumbent protocols, Bitcoin and Ethereum. This analysis demonstrates how Mem-Coin's unique features create a distinct and compelling value proposition.[1]

| **Metric** | **Bitcoin** | **Ethereum** | **Mem-Coin (Hybrid)** |
|---|---|---|---|
| **Energy Efficiency** | Extremely Low (Proof-of-Work) | High (Proof-of-Stake) | **Very High (Productive & Efficient)** |
| | Inherently "wasteful" energy use on arbitrary puzzles.[1] | Low energy footprint, but non-productive.[1] | Low-energy default layer; optional high-energy layer is directed toward valuable AI computation, avoiding waste.[1] |
| **Scalability & Adoption** | High (Store of Value), Low (Transactions) | Very High (Smart Contracts), relies on L2s | **High (Designed for Practicality)** |

| | | | |
|---|---|---|---|
| | Centralized mining, limited programmability.[11] | Base layer congestion is a known issue.[30] | Low entry barriers, built-in L2 design, and a pragmatic bridge to traditional finance promote broad adoption.[1] |
| **Security Model** | High (Brute Force Hashrate) | High (Economic Stake) | **Very High (Defense-in-Depth)** |
| | Secured by immense computational power.[1] | Secured by the economic value of staked ETH.[1] | Employs a layered security model: Crypto-economic (bonds), Cryptographic (ZKPs), Hardware-backed (MPC-HSM), and AI-driven (Sentinel).[1] |

### 6.2. Conclusion and Final Recommendation

This report has conducted an exhaustive evaluation of the Mem-Coin architectural blueprint, confirming that a pivot to a hybrid model is not merely an improvement but a strategic necessity for the protocol's long-term viability. The analysis concludes with two unequivocal findings: the original ZKML-only architecture's "prover's burden" is an unsustainable and centralizing force, and any governance model based on federated trust represents a fundamental security anti-pattern for a decentralized system.[1]

The proposed tiered hybrid verification and monetary architecture directly and comprehensively addresses these challenges, positioning Mem-Coin for success and widespread adoption.

- By establishing **Optimistic PoUW** as the default, low-cost, and energy-efficient layer, the protocol becomes an accessible and economically competitive platform for decentralized AI.[1]
- By retaining **ZKML PoUW** as a premium privacy layer, it secures a critical competitive advantage in high-value commercial markets.[1]
- By instituting an **MPC-HSM Committee** for governance, it establishes a

maximally secure, collusion-resistant root of trust.[1]

- By implementing a **Drivechain framework (RFC-MEM-001)**, it creates a symbiotic bridge to the Bitcoin ecosystem, enhancing Bitcoin's utility and security budget.[7]
- By specifying an **immutable gRPC API**, it provides a robust, performant, and safe contract for developers.
- By deploying an **AI Sentinel** and a **Regulated Monetary Model**, it builds in proactive security and a pragmatic path to mainstream financial integration.[1]

This report concludes with a strong and unequivocal recommendation to adopt the proposed tiered hybrid verification and monetary architecture. This path offers the most viable, secure, and strategically sound route for Mem-Coin to achieve its goals. It effectively resolves the complexities and risks identified in the initial query by mitigating ZKP prover costs, solving the federation collusion problem, and lowering overall processing requirements and power consumption. By embracing this hybrid model, Mem-Coin can evolve from a theoretical blueprint into a practical, scalable, and economically sustainable foundation for the future of the decentralized AI ecosystem.

#### Works cited

1. Mem-Coin Hybrid Architecture Feasibility
2. opML - ORA, accessed August 2, 2025, https://docs.ora.io/doc/onchain-ai-oracle-oao/fraud-proof-virtual-machine-fpvm-and-frameworks/opml
3. opML: Optimistic Machine Learning on Blockchain - arXiv, accessed August 2, 2025, https://arxiv.org/html/2401.17555v1
4. [Literature Review] opML: Optimistic Machine Learning on Blockchain, accessed August 2, 2025, https://www.themoonlight.io/en/review/opml-optimistic-machine-learning-on-blockchain
5. opML: Optimistic Machine Learning on Blockchain - arXiv, accessed August 2, 2025, https://arxiv.org/pdf/2401.17555
6. ora-io/opml - OPtimistic Machine Learning on Blockchain - GitHub, accessed August 2, 2025, https://github.com/ora-io/opml
7. What Are Bitcoin Drivechains? A Beginner's Guide - Samara Asset Group, accessed August 2, 2025, https://www.samara-ag.com/market-insights/bitcoin-drivechains
8. Drivechains: The Future of Bitcoin's Scalability and Sustainability | Nasdaq, accessed August 2, 2025, https://www.nasdaq.com/articles/drivechains:-the-future-of-bitcoins-scalability-and-sustainability
9. Drivechains: The Future Of Bitcoin's Scalability And Sustainability - Bitcoin

Magazine, accessed August 2, 2025, https://bitcoinmagazine.com/technical/drivechains-the-future-of-bitcoins-scalability-and-sustainability

10. Drivechains as an alternative to Altcoins - The Bitfinex Blog, accessed August 2, 2025, https://blog.bitfinex.com/education/drivechains-as-an-alternative-to-altcoins/
11. What Are Bitcoin Sidechains and How Do They Work | Lightspark, accessed August 2, 2025, https://www.lightspark.com/glossary/sidechains
12. Bitcoin Layer 2: Sidechains, accessed August 2, 2025, https://bitcoinmagazine.com/technical/bitcoin-layer-2-sidechains
13. drivechain-project/mainchain-old - GitHub, accessed August 2, 2025, https://github.com/drivechain-project/mainchain-old
14. What Are Bitcoin Drive Chains, accessed August 2, 2025, https://thebitcoinmanual.com/blockchain/drive-chains/
15. What Are Bitcoin Drivechains? A Complete Guide - Nervos Network, accessed August 2, 2025, https://www.nervos.org/knowledge-base/What_are_bitcoin_drivechains_(explainCKBot)
16. bips/bip-0300.mediawiki at master · bitcoin/bips - GitHub, accessed August 2, 2025, https://github.com/bitcoin/bips/blob/master/bip-0300.mediawiki
17. What Is A Blockchain Sidechain? - Komodo Platform, accessed August 2, 2025, https://komodoplatform.com/en/academy/blockchain-sidechain/
18. What's a Bitcoin Drivechain and Why Are Devs At Odds Over Its Proposal? - Decrypt, accessed August 2, 2025, https://decrypt.co/154129/what-is-a-bitcoin-drivechain
19. Drivechains - Bitcoin Magazine, accessed August 2, 2025, https://bitcoinmagazine.com/tags/drivechains
20. REST or gRPC? A Guide to Efficient API Design | Zuplo Blog, accessed August 2, 2025, https://zuplo.com/blog/2025/03/24/rest-or-grpc-guide
21. gRPC vs REST - Difference Between Application Designs - AWS, accessed August 2, 2025, https://aws.amazon.com/compare/the-difference-between-grpc-and-rest/
22. API design guide - Google Cloud, accessed August 2, 2025, https://cloud.google.com/apis/design
23. Understanding gRPC Concepts, Use Cases & Best Practices - InfraCloud, accessed August 2, 2025, https://www.infracloud.io/blogs/understanding-grpc-concepts-best-practices/
24. What is gRPC? Benefits & Use Cases for Developers - Ankr, accessed August 2, 2025, https://www.ankr.com/blog/what-is-grpc/
25. REL08-BP04 Deploy using immutable infrastructure - Reliability Pillar - AWS Documentation, accessed August 2, 2025, https://docs.aws.amazon.com/wellarchitected/latest/reliability-pillar/rel_tracking_change_management_immutable_infrastructure.html
26. Immutable object - Wikipedia, accessed August 2, 2025, https://en.wikipedia.org/wiki/Immutable_object

27. API design - Azure Architecture Center - Microsoft Learn, accessed August 2, 2025, https://learn.microsoft.com/en-us/azure/architecture/microservices/design/api-design
28. gRPC Motivation and Design Principles, accessed August 2, 2025, https://grpc.io/blog/principles/
29. Core concepts, architecture and lifecycle - gRPC, accessed August 2, 2025, https://grpc.io/docs/what-is-grpc/core-concepts/
30. www.kraken.com, accessed August 2, 2025, https://www.kraken.com/learn/layer-2-solutions#:~:text=Layer%202%20scaling%20solutions%20refer,Layer%201%20blockchains%20can%20process.