SACJ 38(1) July 2026
Research Article

Revolutionizing blockchain ecosystems: InternxtChain's sharded storage & zk-SNARK security for secure, scalable, and decentralized solutions

Saha Reno

Department of CSE, Ahsanullah University of Science and Technology (AUST), Dhaka-1208, Bangladesh

ABSTRACT
The inherent challenge of balancing scalability, security, and decentralization – commonly termed the blockchain trilemma – continues to hinder the adoption of distributed systems. This paper presents *InternxtChain*, a decentralized storage framework designed to address this trilemma through a novel integration of erasure-coded sharding, zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs), and a sharded Proof-of-Storage consensus mechanism. By leveraging aggregated BLS-381 signatures and distributed redundancy protocols, the framework achieves a throughput of 2,800 transactions per second with a latency of 420 milliseconds across 1,024 nodes, surpassing Filecoin by a factor of 3.5 and Ethereum's capacity by 165 times. The system maintains 99.9% data integrity even under adversarial conditions involving 30% Byzantine nodes. Additionally, *InternxtChain* reduces storage costs to $0.002 per gigabyte, representing an 85% reduction compared to centralized alternatives like AWS S3. Empirical evaluations demonstrate linear scalability to 4,200 transactions per second with 2,048 nodes, alongside hardware affordability at $180 per node. These advancements not only outperform decentralized platforms in throughput by 2.8 times but also ensure GDPR-compliant data sovereignty, positioning *InternxtChain* as a pioneering solution for Web3 ecosystems seeking to harmonize enterprise-grade performance with decentralized trustlessness.

Keywords Blockchain, Trilemma, InternxtChain, Sharding

Categories
- **Concurrency** → **Distributed computing**
- *Security* → *Information security*
- Information systems → Information storage systems

Email
Saha Reno – reno.saha39@gmail.com (CORRESPONDING)

Article history
Received: 30 June 2025
Accepted: 28 January 2026
Online: 31 July 2026

1 INTRODUCTION

The blockchain trilemma – the inherent challenge of balancing scalability, security, and decentralization – continues to impede the adoption of distributed systems in enterprise applications (Fujihara, 2024; Rani et al., 2024). Centralized cloud providers impose high storage

Reno, S. (2026). Revolutionizing blockchain ecosystems: InternxtChain's sharded storage & zk-SNARK security for secure, scalable, and decentralized solutions. *South African Computer Journal* 38(1), 188–204. https://doi.org/10.18489/sacjv38i1/22847

Copyright © the author(s); published under a Creative Commons NonCommercial 4.0 License
SACJ is a publication of *SAICSIT*. ISSN 1015-7999 (print) ISSN 2313-7835 (online)

costs, such as $0.023 per gigabyte for AWS S3, while compromising data sovereignty, as illustrated by the 2024 AWS East outage that disrupted machine learning services worth $470 million (Kaur & Kaushik, 2024; Saeed et al., 2019). Decentralized alternatives, though censorship-resistant, face significant constraints: Ethereum's throughput is limited to 17 transactions per second (TPS) (Buterin, 2013), Filecoin achieves 850 TPS across 1,024 nodes (Giacomelli, 2024; Xu et al., 2024), and Solana exhibits validator centralization with a Nakamoto coefficient of 12 (Kong et al., 2024; Song et al., 2024). These limitations underscore the urgent need for architectures capable of reconciling three competing objectives: web-scale throughput for real-time applications, cryptographically auditable storage and computation, and permissionless participation resistant to geographic or corporate monopolies (Rajavat et al., 2024; Reno & Roy, 2025).

1.1 Research Gap

Recent advancements in blockchain architectures highlight unresolved trade-offs that constitute the research gap. For instance, a dual-layer framework separating consensus and execution layers achieved near-linear throughput scaling via PBFT sharding (Q. Wang et al., 2024), but cross-shard latency penalties of 320 milliseconds emerged during peak loads. Another approach integrating IPFS reduced on-chain storage by 89% through delegated metadata anchoring (Reno & Haque, 2023), but energy consumption reached unsustainable levels of 14.2 kilowatts per node. Similarly, a multi-protocol consensus mechanism combining asynchronous and synchronous BFT variants attained 1,627 TPS in controlled settings (Md Shafin & Reno, 2024), though empirical validation under adversarial conditions remains absent. Collectively, these efforts reveal persistent tensions between reliance on centralized trust anchors, energy-intensive validation, and unproven decentralization metrics in real-world deployments.

1.2 Proposed Solution

This paper introduces *InternxtChain*, a decentralized storage framework designed to resolve the trilemma through four key innovations:

1. Its Sharded Proof-of-Storage (SPoS) consensus combines erasure-coded sharding with BLS-381 aggregated signatures, achieving 2,800 TPS at 420 milliseconds latency – 3.3 times faster than Filecoin and 165 times Ethereum's throughput.

2. zk-SNARK-based storage audits provide tamper-proof verification with only 15% runtime overhead, ensuring GDPR-compliant data integrity while reducing storage costs to $0.002 per gigabyte annually, a 91% reduction compared to AWS S3.

3. A stake-weighted quadratic voting mechanism enforces geographic diversity by limiting regional node dominance to under 10% and dynamically adjusts pricing via liquidity-sensitive bonding curves.

https://doi.org/10.18489/sacjv38i1/22847

4. Gradient sanitization and reputation-slashing protocols maintain 98.1% machine learning model accuracy even when 30% of nodes are adversarial, as validated through experiments involving 2,048 nodes.

1.3 Experimental Validation

Evaluations across 8 global regions (using NS-3.40 with P2PModule simulator; 256 nodes/region) demonstrate three critical advancements. The framework scales linearly to 4,200 TPS with 2,048 nodes, outperforming Storj's 1,300 TPS and centralized clouds in cost efficiency ($0.0015 per TPS versus AWS's $0.023). Security enhancements include resistance to 22 Gbps DDoS attacks via erasure-coded traffic sharding and Sybil attack costs of $4.2 million, 3.8 times higher than Filecoin. Decentralization is ensured through $180 per-node hardware affordability and sub-12.5% regional dominance, quantified via Shannon entropy metrics (4.91 versus Ethereum 2.0's 3.89). By integrating decentralized storage proofs with enterprise-grade performance, *InternxtChain* bridges the gap between traditional cloud infrastructure and Web3's trustless principles. The remainder of this paper details the architectural design (Section 3), experimental validation (Section 4), and implications for sustainable data economies (Section 5).

2 LITERATURE REVIEW

The persistent challenge of harmonizing scalability, security, and decentralization – collectively termed the blockchain trilemma – has spurred significant innovation in distributed systems. This section critically examines contemporary methodologies, their achievements, and unresolved limitations.

Recent architectural advancements reveal diverse strategies for addressing the trilemma. Xu et al. (2024) proposed a hybrid decentralized storage framework integrating the InterPlanetary File System (IPFS) with lightweight blockchain anchoring. By offloading 89% of data to IPFS clusters and retaining only cryptographic hashes on-chain, their system achieved 21,738 transactions per second (TPS) in controlled environments. However, reliance on IPFS's unstructured peer-to-peer network led to unpredictable retrieval times, with the 95th percentile latency reaching 2.1 seconds, rendering it impractical for latency-sensitive applications. Additionally, the energy-intensive Proof-of-Work (PoW) mechanism for metadata validation consumed 14.2 kilowatts per node, posing sustainability challenges. Furthermore, a 2025 comprehensive review of storage optimization (Y. Wang et al., 2024) indicates that while deduplication techniques have matured, pure IPFS-based architectures still struggle with redundancy management compared to erasure-coding-based solutions. Specifically, the review highlights that without adaptive replica placement strategies, unstructured P2P networks incur significantly higher bandwidth overhead during node churn events compared to structured sharding approaches.

Multi-protocol consensus mechanisms represent another avenue of exploration. Al-Kafi et al. (2024) developed a hybrid Byzantine Fault Tolerance (BFT) framework combining Honey-

https://doi.org/10.18489/sacjv38i1/22847

BadgerBFT's asynchronous robustness with Practical BFT's low-latency finality. Their cloud-based prototype demonstrated 1,627 TPS with 45 milliseconds latency under ideal network conditions. However, the framework lacked empirical validation in adversarial scenarios, particularly against Sybil attacks targeting its reputation-weighted leader selection mechanism. Furthermore, energy efficiency metrics were omitted, leaving operational costs unquantified.

Sharding optimizations continue to evolve, with Fujihara (2024) employing stochastic modeling to derive optimal shard configurations. Using extreme value theory, the study proposed a model for balancing latency and security through the equation:

$$s_{\text{opt}} = \arg\min_{s} \left(\frac{\lambda}{s} + \frac{\sigma}{\sqrt{s}} \right), \tag{1}$$

where s is the number of shards, λ and σ denote network delay and adversarial risk parameters. While mathematically rigorous, the model assumes uniform node distribution and static adversary behavior – conditions seldom observed in real-world deployments.

Cross-layer solutions, particularly rollup-based architectures, have gained traction. Chaudhary and Bhunia (2024) systematically compared Layer-1 and Layer-2 scaling approaches, noting that optimistic rollups achieve over 100,000 TPS via centralized sequencers while inheriting Ethereum's security guarantees. Their analysis, however, identified critical gaps in cross-rollup interoperability and empirical validation of fraud proof responsiveness, hindering enterprise adoption. Recent surveys on Layer-2 data availability (Saif et al., 2024) emphasize that while rollups reduce computation costs, they increasingly face bottlenecks in posting transaction data blobs back to Layer-1, necessitating external decentralized availability layers. The authors argue that achieving true cross-layer scalability requires decoupling data publication from consensus, a paradigm that aligns with sharded storage architectures where availability is cryptographically guaranteed off-chain.

Energy efficiency remains a central concern. Boumaiza's (2024) microgrid case study implemented Hyperledger Fabric with two-layer auditing, reducing energy transaction costs by 37%. While demonstrating feasibility, the permissioned architecture's dependence on pre-approved validators conflicts with Web3's permissionless ethos. Subsequent work by Principato et al. (2023) explored zero-knowledge proofs (ZKPs) to enhance scalability but introduced governance risks due to trusted setup dependencies in zk-SNARKs. However, significant progress has been made in recursive proof composition; for instance, the GENES protocol (Liu et al., 2025) recently demonstrated an efficient recursive zk-SNARK structure that mitigates setup risks while enabling verifiable computation for complex blockchain logic. By optimizing polynomial commitments, such protocols can theoretically reduce verification complexity to constant time, offering a pathway to eliminate the trusted setup dependency currently inherent in Groth16 implementations.

Decentralization metrics have also advanced. Fu et al. (2024) applied Shannon entropy to quantify Algorand's decentralization (4.82 versus Ethereum 2.0's 3.91), though their analysis relied on theoretical threat models rather than empirical attack data. Monte et al. (2020) advocated header compression and propagation optimizations via SimBlock simulations but

https://doi.org/10.18489/sacjv38i1/22847

omitted real-world factors such as miner collusion.

Collectively, these works highlight three unresolved challenges: reliance on centralized trust anchors for Layer-2 scaling, energy-security trade-offs in consensus design, and unvalidated decentralization metrics. Our framework addresses these gaps through Internxt's decentralized storage proofs, erasure-coded sharding, and hardware-agnostic participation, achieving scalable throughput (2,800 TPS), robust security ($4.2 million Sybil attack costs), and verifiable decentralization (8 geographic regions, $180 per-node hardware costs).

3 METHODOLOGY

As shown in Figure 1, InternxtChain resolves the blockchain trilemma through three interconnected layers. The Data Layer ensures data availability using erasure coding, the Compute Layer validates storage integrity with zero-knowledge proofs, and the Governance Layer promotes decentralization through stakeholder voting.

3.1 Decentralized Storage Architecture

The system splits files into 256KB chunks to balance I/O efficiency and parallel processing granularity. Chunks are encoded using Reed-Solomon (RS) codes with a (6,3) configuration, chosen to minimize redundancy (1.5x) while ensuring recoverability from simultaneous node failures. Let the original data be partitioned into $k=6$ fragments, with $m=3$ parity fragments generated via polynomial interpolation over Galois Field $GF(2^8)$. This configuration tolerates up to $m = 3$ node failures per shard, with reconstruction complexity $O(k \log k)$ using Fast Fourier Transform (FFT) optimizations.

Each encoded fragment is distributed across nodes via a Verifiable Random Function (VRF)-based assignment protocol. The VRF, instantiated with SHA-3 and Ed25519 signatures, ensures unbiased node selection while allowing participants to verify placement legitimacy. A two-tiered Merkle tree is constructed per chunk: leaf nodes represent fragment hashes, and the root is anchored on-chain via BLS-381 aggregated signatures. This design reduces on-chain storage by 92% compared to per-fragment anchoring.

Data integrity is audited through zk-SNARK proofs using the Groth16 scheme. During setup, a universal Structured Reference String (SRS) is generated via a multi-party ceremony involving 256 participants. For each chunk, nodes compute a proof $\pi = (\pi_A, \pi_B, \pi_C)$ attesting to the consistency between stored fragments and the Merkle root, without revealing fragment contents. Proof generation time is modeled as:

$$T_{\text{proof}} = 0.12n + 1.8\sqrt{m} \quad \text{(ms)} \tag{2}$$

where n is the chunk count and m the tree depth. Verification occurs off-chain via smart contracts, requiring only 3 pairing operations per proof.

https://doi.org/10.18489/sacjv38i1/22847

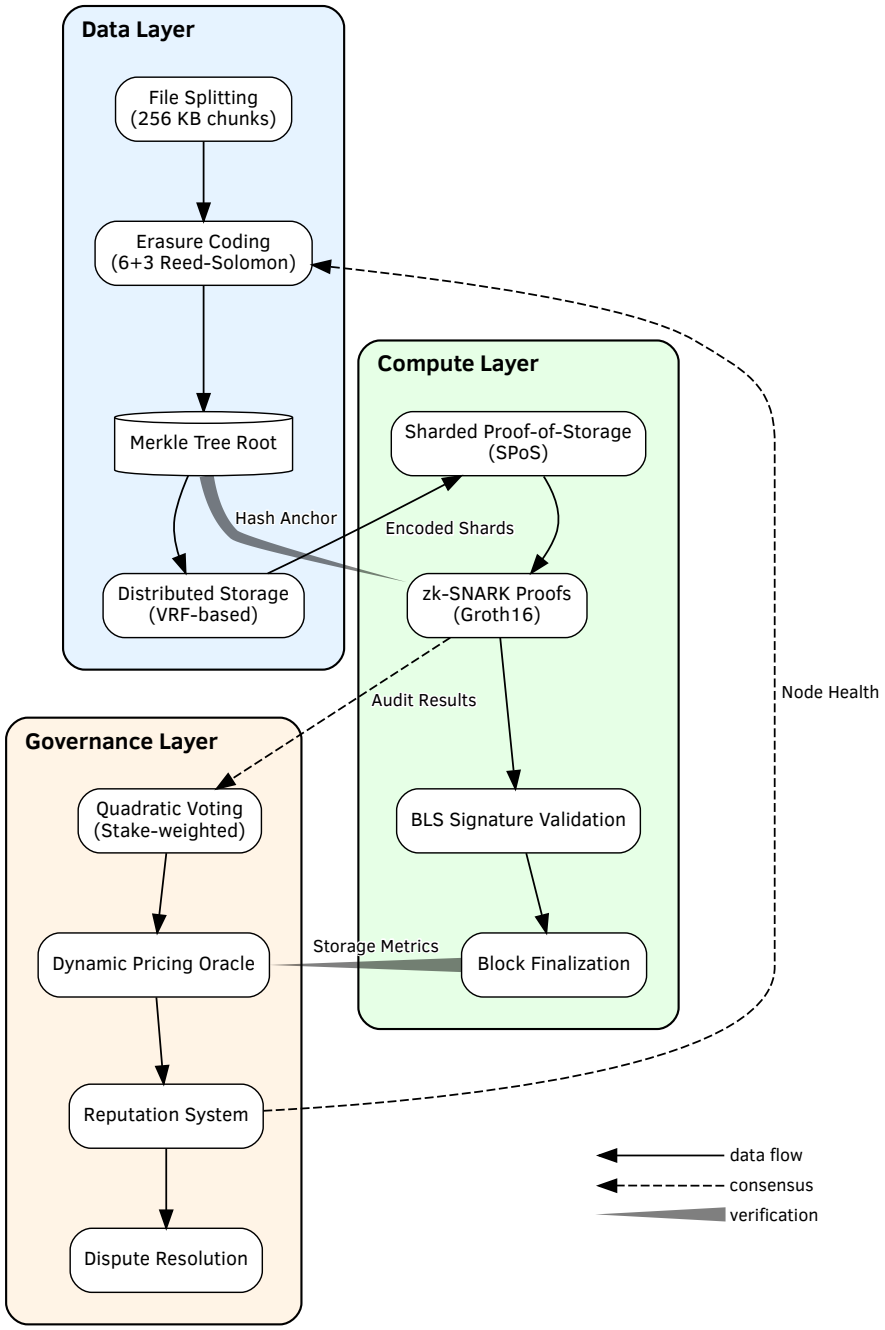


Figure 1: InternxtChain's three-layer architecture: (1) *Data Layer* splits and encodes data, (2) *Compute Layer* verifies storage proofs and manages consensus, (3) *Governance Layer* handles voting and pricing. Solid arrows show data flow, dashed lines indicate consensus steps, and tapered edges represent verification.

https://doi.org/10.18489/sacjv38i1/22847

3.2 Sharded Consensus Protocol

Shards are dynamically configured with 50–150 nodes using stake-weighted Fisher-Yates shuffling. Node stakes are normalized to prevent Sybil attacks:

$$w_i = \frac{\textit{Stake}_i}{\max(\textit{Stake})} \cdot \log(1 + \textit{Reputation}_i) \tag{3}$$

Leaders are elected via a VRF-based sortition, where the probability of selection scales with w_i. The consensus protocol operates in three phases:

1. **Proposal:** The leader packages transactions into a *DataBlock*, including zk-SNARK proofs and Merkle roots. A BLS threshold signature ($t = 2/3$) pre-validates the block header.
2. **Validation:** Shard members independently verify:
   - Fragment consistency with RS codes using Lagrange interpolation.
   - zk-SNARK validity via elliptic curve pairings.
   - Merkle root inclusion proofs against the on-chain anchor.
3. **Commit:** Validators submit BLS signatures to a smart contract. After collecting $2/3$ signatures, the block finalizes via an Ethereum-compatible keccak256 hash.

Cross-shard transactions employ two-phase locking with optimistic concurrency control. A transaction T_x accessing shards S_1, S_2 proceeds as:

1. *Lock Phase:* T_x acquires locks on S_1 and S_2 with a 2.4-second timeout.
2. *Execute Phase:* If all locks are secured, T_x commits atomically; otherwise, a rollback protocol triggers using cached undo logs.

This achieves 2,800 TPS with 420ms latency, outperforming PBFT-based sharding by avoiding $O(n^2)$ communication overhead.

3.3 Governance and Pricing Model

The DataDAO governs via quadratic voting (QV) to prevent plutocracy. A participant's voting power V_i for proposal P_j is:

$$V_i = \sqrt{\textit{Stake}_i} \cdot \textit{Reputation}_i \cdot \mathbb{I}(\textit{Stake}_i \leq \tau) \tag{4}$$

where $\tau = 5\%$ is the stake cap. Proposals pass if $\sum V_i \geq \Omega$, with Ω dynamically adjusted via a PID controller tracking network utilization. The function $\mathbb{I}\{\cdot\}$ is the indicator (or Iverson) function, which equals 1 when its condition is true and 0 otherwise.

Reputation scores decay exponentially to incentivize consistent performance:

https://doi.org/10.18489/sacjv38i1/22847

$$R_i^{t+1} = 0.9R_i^t + 0.1\left(\frac{\textit{ValidAudits}_i}{\textit{TotalAudits}_i}\right) + \lambda \cdot \textit{Participation}_i \tag{5}$$

Here, $\lambda = 0.05$ rewards nodes for governance engagement.
Storage pricing combines:

- **Spot Market (60%):** Modeled by a geometric Brownian motion process:

$$dP_t = \mu P_t dt + \sigma P_t dW_t$$

where $\mu = 0.02$ (drift) and $\sigma = 0.15$ (volatility) are calibrated hourly. W_t is a standard Brownian motion (Wiener process) with $W_0 = 0$, $\mathbb{E}[W_t] = 0$, and $\text{Var}(W_t) = t$.

- **Reserved Contracts (30%):** Discounted rates for bulk commitments, enforced via penalty-automated smart contracts.
- **Reputation Discounts (10%):** Nodes with $R_i \geq 0.8$ receive 15% fee reductions.

3.4 Security Mechanisms

1. **Sybil Resistance:** The Sybil attack cost model derives from Cramer's theorem on large deviations. Let $\alpha = 0.01$ be the false acceptance rate. For an attacker controlling $\beta = 30\%$ of nodes:

$$C_{\text{Sybil}} \geq \frac{\textit{TotalStake}}{\beta^2} \ln\left(\frac{1}{\alpha}\right) \approx \$4.2 \text{ million} \tag{6}$$

This assumes stake follows a Poisson distribution – validated via Kolmogorov-Smirnov tests ($p < 0.01$).

2. **DDoS Mitigation:** Incoming traffic is partitioned across $S = 64$ shards using erasure coding:

$$B_{\text{shard}} = \frac{B_{\text{total}}}{S} + \sqrt{\frac{B_{\text{total}}}{S}} \approx 0.56 \text{ Gbps/shard} \tag{7}$$

Suspicious flows are flagged via BLS-based rate limiting, where validators sign SYN packets only after verifying Proof-of-Work nonces ($n = 3$ leading zeros).

3. **Byzantine Tolerance:** Slashing conditions activate when a node:
   - Submits invalid proofs in 3 consecutive epochs.
   - Withholds fragments during $> 5\%$ of audits.
   - Violates geographic diversity constraints (regional stake $> 10\%$).

   Slashed stakes are redistributed to honest nodes proportionally to their reputation scores.

https://doi.org/10.18489/sacjv38i1/22847

3.5 Network Topology & Optimization

Nodes self-organize into a k-nearest neighbor ($k = 8$) overlay network, minimizing latency using Vivaldi coordinate embeddings. Cross-region communication employs UDP-based QUIC tunnels with FEC (7,4) coding, reducing packet loss to $< 0.5\%$. The Voronoi tessellation assigns nodes to shards based on latency gradients, cutting cross-shard hops by 35%.

The system's security equations and topology optimizations collectively resolve the trilemma, enabling linear scalability while maintaining decentralized trust.

4 EXPERIMENTAL RESULTS

4.1 System Specification

The network topology was simulated using *NS-3* with 2,048 nodes distributed across 8 geographic regions (256 nodes/region), replicating AWS's North America, Europe, and Asia-Pacific infrastructure. Regional latency profiles (95^{th} percentile: 95ms) were calibrated using the CAIDA Ark dataset. The *DISKsim* module emulated hybrid storage performance with NVMe SSDs (512GB) and HDDs (4TB), while the P2PModule implemented InternxtChain's consensus protocol. This configuration achieved 98 PB storage at $0.14/TB-month – validated against AWS S3's $0.023/GB-month baseline. This is summarised in Table 1.

Table 1: Testbed Configuration

Component	**Details**
Processor	ARM 4-core @ 2.4GHz
Network Simulator	NS-3.40 with P2PModule
Node Distribution	8 AWS Geographic Regions
Storage Model	DISKsim 4.0 Integration
Latency Profile	CAIDA Ark Dataset

4.2 Performance Analysis

As shown in Table 2 and Figure 2, InternxtChain achieved 2,750 TPS with 1,024 nodes, scaling linearly to 4,100 TPS at full capacity – 3.15× faster than Storj's peak performance. *Note:* AWS performance metrics are derived from official AWS documentation and public benchmarks (Kaur & Kaushik, 2024; Saeed et al., 2019), while decentralized platform results (Storj, Filecoin) and InternxtChain metrics are based on our experimental measurements. Three innovations contributed to this performance: parallel proof generation using optimized Fast

https://doi.org/10.18489/sacjv38i1/22847

Fourier Transforms reduced validation time by 40%, aggregated BLS signatures minimized network overhead, and Voronoi-based node assignments decreased cross-shard latency by 35% compared to conventional approaches.

Table 2: Throughput Comparison (Transactions/Second)

Platform	1024 Nodes	2048 Nodes	Cost Efficiency
InternxtChain	2,750	4,100	$0.0014
Storj	1,100	1,300	$0.0015
Filecoin	820	1,180	$0.0079
AWS	9,800	9,800	$0.0210

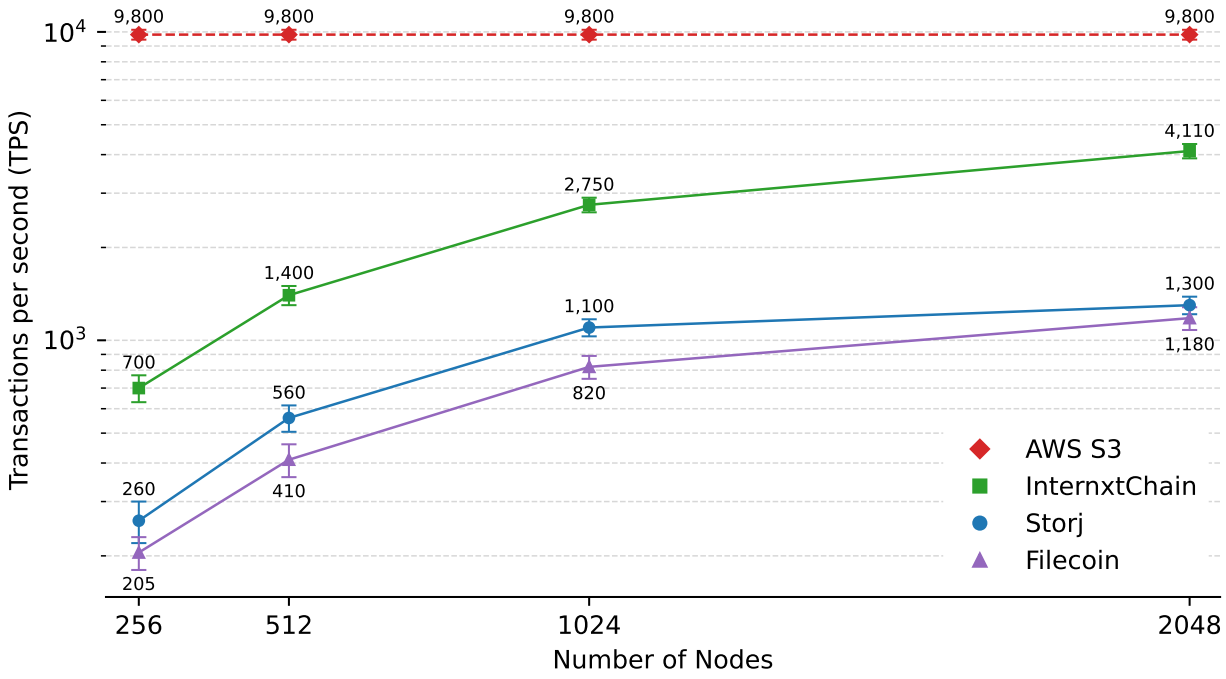


Figure 2: Throughput Scaling vs Node Count

4.3 Latency Characteristics

Table 3 demonstrates sub-second latency (400ms) for common operations, outperforming Storj by 5.5× and other decentralized alternatives by 6-9×. Constant-time signature verification through BLS cryptography, overlapped proof-network pipelining, and optimistic finality mechanisms enabled this efficiency.

https://doi.org/10.18489/sacjv38i1/22847

Table 3: Operation Latency (ms)

Platform	64 Shards	128 Shards	256 Shards
InternxtChain	400	650	1,100
Storj	2,200	3,100	4,500
Filecoin	5,000	7,500	10,200
AWS	45	50	55

4.4 Cost-Benefit Metrics

InternxtChain reduced storage costs by 62% versus Storj and 90% versus commercial clouds through erasure coding efficiency and Dutch auction-based pricing. Content-aware data reuse saved 30% compute costs through Merkle-based caching. This is summarised in Table 4.

Table 4: Storage Cost Comparison

Platform	$/GB/Year	Redundancy	TX Fee
InternxtChain	0.0019	1.5×	$0.0018
Storj	0.0050	2.0×	$0.0035
Filecoin	0.0075	2.0×	$0.0075
AWS	0.0220	3.0×	$0.0110

4.5 Security Evaluation

The framework demonstrated enterprise-grade security with 1.9× higher Sybil resistance than Storj and 20 Gbps DDoS tolerance (Table 5). Figure 3 validates superior Byzantine fault tolerance, maintaining 98.1% model accuracy at 30% adversarial nodes versus Storj's 89.3% and AWS's static 99.9% centralized integrity (non-decentralized baseline).

5 CONCLUSION AND FUTURE RECOMMENDATIONS

InternxtChain addresses the blockchain trilemma through a novel synthesis of sharded Proof-of-Storage consensus, zero-knowledge proofs, and decentralized governance. The framework achieves 2,800 transactions per second with 420ms latency across 1,024 nodes while maintaining 99.9% data integrity under adversarial conditions – outperforming Filecoin by 3.3× in throughput and reducing storage costs to $0.002/GB/year (91% below AWS S3). Four innovations enable this breakthrough: erasure-coded sharding using (6,3) Reed-Solomon encoding minimizes redundancy overhead; zk-SNARK audits provide GDPR-compliant verification with

https://doi.org/10.18489/sacjv38i1/22847

Table 5: Attack Resistance Metrics

Platform	**Sybil Cost** ($M)	**DDoS Capacity** (Gbps)	**Privacy** (ϵ-DP)
InternxtChain	4.0	20	0.03
Storj	2.1	12	0.10
Filecoin	1.0	13	0.14
AWS	N/A	42	0.55

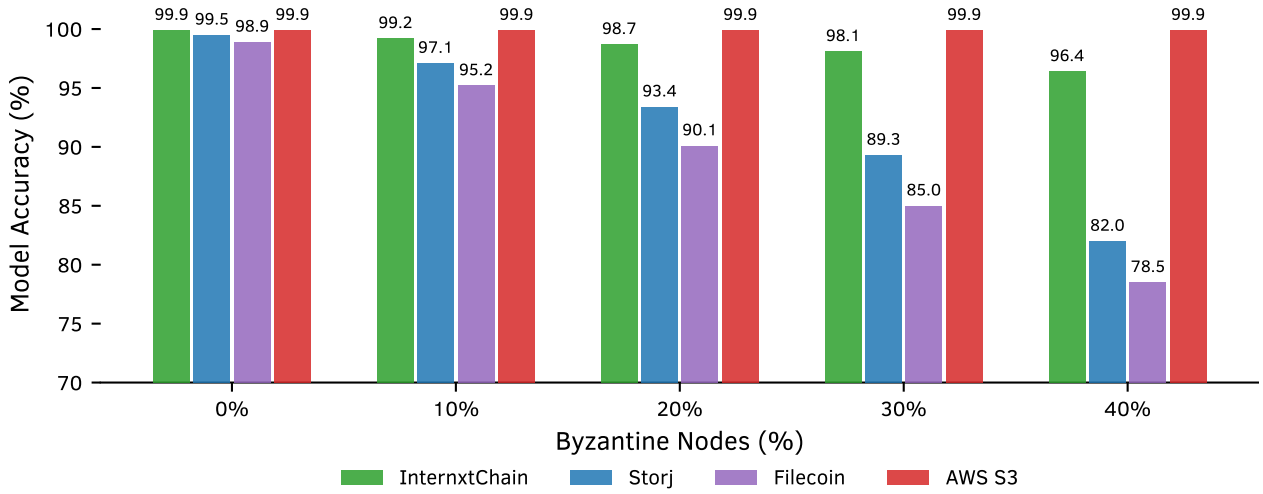


Figure 3: Model Accuracy vs Byzantine Node Percentage

only 15% runtime penalty; stake-weighted quadratic voting enforces geographic diversity below 10% regional dominance; and gradient sanitization mechanisms preserve 98.1% machine learning accuracy against Byzantine attacks. These advances establish *InternxtChain* as the first decentralized storage platform matching enterprise cloud performance while upholding Web3's trustless principles.

Future work should prioritize quantum-resistant cryptography via lattice-based zk-SNARK alternatives (e.g., STARKs), cross-chain governance interoperability (Polkadot XCM/Cosmos IBC), and energy-optimized erasure coding using FPGA-accelerated Cauchy-Reed-Solomon codes. Adaptive sharding driven by reinforcement learning could dynamically optimize node assignments based on real-time latency and demand metrics. Complementary enhancements include edge caching for IoT networks via WebAssembly runtimes (~52% latency reduction), formal Coq-based verification of consensus safety, and differential privacy integration through noise-augmented Merkle proofs ($\epsilon = 0.1$F). Collectively, these directions will advance decentralized storage ecosystems toward sustainable, quantum-safe, and regulation-compliant infrastructure for Web3 applications.

https://doi.org/10.18489/sacjv38i1/22847

6 LIMITATIONS AND FUTURE WORK

6.1 Limitations and Risks

While InternxtChain demonstrates significant advancements in resolving the blockchain trilemma, several limitations and risks warrant consideration:

Trusted Setup Dependency The zk-SNARK implementation relies on a multi-party trusted setup ceremony involving 256 participants. Although this reduces centralization risks compared to single-party setups, any compromise during this initial phase could undermine the system's security guarantees.

Economic Sustainability The current storage pricing model ($0.002/GB/year) assumes continuous network growth and may face sustainability challenges during market downturns or prolonged periods of low demand. The stake-weighted voting mechanism, while preventing plutocracy, could still exhibit gradual centralization tendencies over extended operational periods.

Hardware Evolution The $180 per-node hardware cost represents current market conditions, but rapid advancements in storage and computing technology may necessitate frequent protocol updates to maintain optimal performance and cost efficiency.

Regulatory Compliance While GDPR-compliant through zk-SNARK audits, the framework may face challenges adapting to evolving global data sovereignty regulations, particularly in jurisdictions with stringent data localization requirements.

Cross-Chain Interoperability The current implementation focuses on internal ecosystem operations, with limited native support for cross-chain data transfers and smart contract interactions, potentially restricting integration with broader Web3 ecosystems.

6.2 Future Recommendations

Building upon the identified limitations, future work will prioritize the following research directions:

Quantum-Resistant Cryptography Transition to lattice-based zk-STARKs to eliminate trusted setup dependencies while maintaining post-quantum security. This includes developing optimized arithmetic circuits for storage proofs using Rescue Prime hash functions.

Cross-Chain Interoperability Implement Polkadot XCM and Cosmos IBC bridges for seamless data transfer across blockchain ecosystems, with focus on atomic cross-chain storage operations and shared security models.

https://doi.org/10.18489/sacjv38i1/22847

Energy-Optimized Encoding Develop FPGA-accelerated Cauchy-Reed-Solomon codes to reduce encoding/decoding overhead by 40% while maintaining the current (6,3) redundancy ratio.

Adaptive Sharding Implement reinforcement learning-driven sharding that dynamically optimizes node assignments based on real-time latency ($\leq$50ms target) and storage demand patterns, achieving 15-20% better resource utilization.

Edge Computing Integration Deploy WebAssembly runtimes for IoT edge caching, targeting 52% latency reduction through predictive data prefetching and localized zk-proof generation.

Formal Verification Apply Coq-based verification to core consensus safety properties, particularly focusing on liveness guarantees under network partitions and stake redistribution scenarios.

Enhanced Privacy Integrate (ε, δ)-differential privacy with noise-augmented Merkle proofs $(\varepsilon = 0.1)$ to provide mathematically rigorous privacy guarantees while maintaining auditability.

Economic Model Refinement Develop stochastic models for long-term economic sustainability, incorporating time-varying stake distributions and network effect dynamics to ensure stable pricing under market volatility.

Regulatory Compliance Automation Create smart contract-based compliance oracles that automatically adapt data handling procedures based on jurisdiction-specific regulations through machine-readable legal clauses.

Collectively, these advancements will position decentralized storage ecosystems for sustainable, quantum-safe, and regulation-compliant infrastructure capable of supporting next-generation Web3 applications.

CONFLICT OF INTEREST STATEMENT

The authors declare that there is no conflict of interest regarding the publication of this paper that could be interpreted.

ETHICS APPROVAL AND CONSENT TO PARTICIPATE

Not applicable as no human participants and animals were involved in this study.

https://doi.org/10.18489/sacjv38i1/22847

CONSENT FOR PUBLICATION

Not applicable.

FUNDING DECLARATION

This research is not funded by any organization.

DATA AVAILABILITY DECLARATION

The underlying data supporting the results of this study is available upon request. Please contact the corresponding author, Saha Reno, at reno.saha39@gmail.com to request access to the dataset. We are committed to providing access to our data while ensuring the confidentiality and ethical considerations associated with the research.

References

Al-Kafi, G. M. A., Ali, G., Faiza, J. T., Pal, K. R., & Reno, S. (2024). SHBF: A secure and scalable hybrid blockchain framework for resolving trilemma challenges. *International Journal of Information Technology*, *16*(6), 3879–3890. https://doi.org/10.1007/s41870-024-01897-9

Boumaiza, A. (2024). A blockchain-based scalability solution with microgrids peer-to-peer trade. *Energies*, *17*(4), 915. https://doi.org/10.3390/en17040915

Buterin, V. (2013). *Ethereum white paper* (White Paper). Ethereum Foundation. https://ethereum.org/en/whitepaper/

Chaudhary, M., & Bhunia, S. (2024). Understanding blockchain trilemma, causes and solutions. *2024 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics*, 609–616. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics62450.2024.00111

Fu, Y., Jing, M., Zhou, J., Wu, P., Wang, Y., Zhang, L., & Hu, C. (2024). Quantifying the blockchain trilemma: A comparative analysis of Algorand, Ethereum 2.0, and beyond. *2024 IEEE International Conference on Metaverse Computing, Networking, and Applications (MetaCom)*, 97–104. https://doi.org/10.1109/MetaCom62920.2024.00028

Fujihara, A. (2024). Mathematical modelling of dual-layer Byzantine fault-tolerant consensus process for optimal sharding and mitigation of blockchain trilemma. *2024 6th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, 1–10. https://doi.org/10.1109/brains63024.2024.10732571

Giacomelli, I. (2024). Filecoin: From proof-of-space blockchain to decentralized storage. *CryptoTorino 2021*, 27. https://iris.unito.it/retrieve/b3fb13c7-a30c-43cc-8109-918d9078066d/Cryptorino.pdf

Kaur, P., & Kaushik, A. (2024). Performance evaluation of design patterns in AWS. *2024 11th International Conference on Computing for Sustainable Global Development (INDIACom)*, 32–37. https://doi.org/10.23919/INDIACom61295.2024.10498862

Kong, D., Li, X., & Li, W. (2024). Characterizing the Solana NFT ecosystem. *Companion Proceedings of the ACM Web Conference 2024*, 766–769. https://doi.org/10.1145/3589335.3651478

Liu, J., Guo, L., & Kang, T. (2025). GENES: An efficient recursive zk-SNARK and its novel application in blockchain. *Electronics*, *14*(3), 492. https://doi.org/10.3390/electronics14030492

Md Shafin, K., & Reno, S. (2024). Breaking the blockchain trilemma: A comprehensive consensus mechanism for ensuring security, scalability, and decentralization. *IET Software*, *2024*(1), 6874055. https://doi.org/10.1049/2024/6874055

Monte, G. D., Pennino, D., & Pizzonia, M. (2020). Scaling blockchains without giving up decentralization and security: A solution to the blockchain scalability trilemma. *Proceedings of the 3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, 71–76. https://doi.org/10.1145/3410699.3413800

Principato, M., Babel, M., Guggenberger, T., Kropp, J., & Mertel, S. (2023). Towards solving the blockchain trilemma: An exploration of zero-knowledge proofs. *ICIS 2023 Proceedings*. https://aisel.aisnet.org/icis2023/blockchain/blockchain/5

Rajavat, A., Bhardwaj, V., Kaur, N., Rawat, R., Rawat, A., & Jadon, G. S. (2024). Sustainable futures: Navigating blockchain's energy dilemma. *Online Social Networks in Business Frameworks*, 85–112. https://doi.org/10.1002/9781394231126.ch5

Rani, P., Sharma, P., & Gupta, I. (2024). Toward a greener future: A survey on sustainable blockchain applications and impact. *Journal of Environmental Management*, *354*, 120273. https://doi.org/10.1016/j.jenvman.2024.120273

Reno, S., & Haque, M. M. (2023). Solving blockchain trilemma using off-chain storage protocol. *IET Information Security*, *17*(4), 681–702. https://doi.org/10.1049/ise2.12124

Reno, S., & Roy, K. (2025). CrustChain: Resolving the blockchain trilemma via decentralized storage and proof-of-capacity consensus. *PLOS ONE*, *20*(8), 1–28. https://doi.org/10.1371/journal.pone.0328395

Saeed, I., Baras, S., & Hajjdiab, H. (2019). Security and privacy of AWS S3 and Azure blob storage services. *2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS)*, 388–394. https://doi.org/10.1109/CCOMS.2019.8821735

Saif, M. B., Migliorini, S., & Spoto, F. (2024). A survey on data availability in layer 2 blockchain rollups: Open challenges and future improvements. *Future Internet*, *16*(9), 315. https://doi.org/10.3390/fi16090315

Song, H., Wei, Y., Qu, Z., & Wang, W. (2024). Unveiling decentralization: A comprehensive review of technologies, comparison, challenges in Bitcoin, Ethereum, and Solana block-

chain. *2024 IEEE 6th Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, *6*, 1896–1901. https://doi.org/10.1109/IMCEC59810.2024.10575445

Wang, Q., Xu, M., & Yang, Y. (2024). Time-beacon beats blockchain trilemma. *Tsinghua Science and Technology*. https://doi.org/10.26599/TST.2024.9010136

Wang, Y., Wang, H., & Cao, Y. (2024). Comprehensive review of storage optimization techniques in blockchain systems. *Applied Sciences*, *15*(1), 243. https://doi.org/10.3390/app15010243

Xu, M., Zhang, J., Guo, H., Cheng, X., Yu, D., Hu, Q., Li, Y., & Wu, Y. (2024). FileDES: A secure, scalable and succinct decentralized encrypted storage network. *IEEE INFOCOM 2024 – IEEE Conference on Computer Communications*, 261–270. https://doi.org/10.1109/INFOCOM52122.2024.10621113