

PolyConnect: Trust Neutral Cross-chain Interoperability

Suchitra Morwadkar, Anagha Kulkarni, Sanika Kulkarni*

Department of Information Technology, Cummins College of Engineering for Women, Maharashtra, India. *Corresponding Author's Email: sanika.h.kulkarni@cumminscollege.in

Abstract

Blockchain networks rely on different forms of governance, consensus, data and execution, which makes it difficult to achieve secure cross-chain data exchange. Existing interoperability approaches often rely on intermediaries, protocol-specific mechanisms, or limited validation, leaving gaps in trust minimization, data integrity and protection against cross-chain attacks. This paper proposes PolyConnect, a security-centric interoperability framework for verifiable and trust-minimized data exchange across heterogeneous blockchain networks. PolyConnect uses a standardized JSON-based record representation and combines hash validation, digital signatures, zero-knowledge proofs and blockchain-state/replay validation to provide layered cross-chain verification. The framework was evaluated across private, consortium, public and hybrid blockchain configurations using workloads of 100, 500 and 1000 records, with ten independent trials for each configuration. Evaluation considered processing performance, heterogeneous data format processing, attack detection, security coverage and comparison with representative interoperability approaches. Across 14 predefined attack scenarios, the complete validation pipeline detected 12 scenarios, achieving an Attack Detection of 85.71%, while the Security Coverage Metric reached 87.5% across eight security categories. Data Fetch and Serialization Time remained below 1 second across the evaluated heterogeneous data categories. Performance analysis showed that processing time varied substantially with workload size and blockchain configuration. Comparative analysis further showed that PolyConnect reduces intermediary dependence and provides broader security coverage but introduces higher computational and deployment overhead. These findings position PolyConnect as a security-focused approach that prioritizes verifiability, auditability and trust minimization in heterogeneous blockchain interoperability.

Keywords: Auditability, Interoperability, Cross-chain Communication, Data Integrity.

Introduction

Blockchain networks operate with different governance models, consensus mechanisms, data structures and execution environments, creating a heterogeneous distributed-ledger ecosystem (1–4). This heterogeneity limits information and state exchange across independent networks and creates challenges in maintaining data consistency, integrity, auditability and verifiability during cross-chain communication (5–7). Interoperability therefore requires more than connectivity; it must also address differences in data representation, validation procedures, trust assumptions and execution environments. Existing studies have proposed several mechanisms to enable interoperability. Decentralized oracles support external data provisioning and aggregation (8), while relay-chain approaches such as Polkadot provide inter-network coordination (9). Protocol-level mechanisms such as Cosmos Inter-Blockchain Communication enable information exchange between compatible blockchain

environments (10). Other approaches, including bridges, multi-signature schemes, relayers and standardized messaging, address asset transfer, data exchange and cross-chain communication requirements (11, 12). These approaches demonstrate the feasibility of interoperability, but their architectural assumptions introduce different security and performance trade-offs. Oracle-based solutions may introduce dependency on data providers, bridges can expose custodial or validation-related attack surfaces and relay or messaging mechanisms may depend on specific validator or protocol assumptions (13–15). Existing research also identifies challenges in simultaneously maintaining decentralization, semantic consistency and security under adversarial conditions (13). These limitations indicate the need for interoperability mechanisms that can validate exchanged data independently across heterogeneous environments. Interoperability can be considered across

This is an Open Access article distributed under the terms of the Creative Commons Attribution CC BY license (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted reuse, distribution and reproduction in any medium, provided the original work is properly cited.

(Received 17th June 2026; Accepted 25th August 2026; Published 04th October 2026)

foundational, infrastructure, protocol, semantic and cognitive levels, ranging from network and consensus connectivity to cross-chain logic and

autonomous interaction. Table 1 summarizes these levels and their principal mechanisms and limitations.

Table 1: Blockchain Interoperability Levels

Level	Focus	Mechanisms	Goal	Limitations
Foundational	Consensus and network	Relay-chains, Polkadot, Cosmos	Common communication layer	Limited to native protocol
Infrastructure	Data and asset transfer	Oracles, bridges, multi-signature	Basic interoperability	Trust reliance
Protocol	Standardised messaging	Axelar, Layer Zero	Cross-chain security	Protocol dependent
Semantic	Cross-chain logic and shared state	Cross-chain applications, schema alignment	Unified multi-chain apps	Schema limitations
Cognitive	AI-driven interaction	AI trust models, self-verifying protocols	Autonomous interoperability	Still in research stage

Security remains a cross-cutting concern because interoperability architectures can expose bridges, validators, relayers, smart contracts, oracles and off-chain storage to attacks (14–16). Threats include message and off-chain data tampering, unauthorized operations, replay, resource

exhaustion, excessive data exposure, oracle manipulation, identity spoofing and inconsistent blockchain states (17). Table 2 maps these threats to the security categories addressed by PolyConnect.

Table 2: Interoperability Security Threats and Mitigations

Security Category	Threats	Affected Mechanisms	Existing Gaps	PolyConnect Mitigation
Data Integrity	Message tampering, off-chain tampering, double-spending	Cross-chain messages, bridges	Data alteration, inconsistent records	Hash verification, CID matching, IPFS
Authentication	Key compromise, multisig compromise	Keys, multisig, relayers	Key theft, unauthorized access	Digital-signature verification
Replay Prevention	Replay attacks	Signatures	Message reuse, duplicate execution	Unique IDs, timestamps
DoS Resilience	Resource exhaustion	Relayers, bridges, validators	Service disruption, processing delays	Lightweight metadata
Privacy Preservation	Cross-chain exposure, excessive sharing	Cross-chain records, metadata	Data disclosure, excessive sharing	Hash-based records, minimal metadata
Oracle Independence	Oracle manipulation	Oracles, off-chain providers	Centralized trust, data manipulation	Oracle-independent hash verification
Identity Verification	Sybil attacks, identity spoofing	Validators, relayers	Fake identities, unauthorized access	Public-key authentication
Consensus	Validator collusion, state	Validators, relayers	Collusion, conflicting	Independent hash +
Consistency	Inconsistency	Coordination	States	Signature Checks

Note: CID = Content Identifier, IPFS = Inter Planetary File System, DoS = Denial of Service.

The preceding limitations reveal a research gap in integrating heterogeneous data processing, security and validation mechanisms for interoperability across blockchain networks (18). Existing approaches generally address specific

communication, coordination, asset-transfer, or data-provisioning requirements, but do not consistently combine standardised data representation with layered cryptographic and blockchain-state validation while reducing

dependence on trusted intermediaries. This gap is particularly relevant when cross-chain exchange involves heterogeneous blockchain configurations and external data structures, where communication alone does not ensure consistent and verifiable data exchange.

The goal of this research is to develop PolyConnect to ensure secure data sharing between heterogeneous blockchain networks and assess its ability to provide trustless interoperability. The research also compares PolyConnect with representative interoperability approaches in terms of security coverage, performance, decentralisation, trust assumptions and deployment complexity. The novelty of PolyConnect lies in integrating record-centric interoperability, multi-level validation and trust-minimized cross-chain verification within a single framework. Unlike approaches primarily focused on asset transfer, messaging, or consensus coordination, PolyConnect combines standardised data representation with complementary cryptographic mechanisms, including Zero-Knowledge Proof (ZKP) based verification and blockchain-state validation and supports heterogeneous external data processing. Its evaluation jointly considers security coverage, attack detection, heterogeneous blockchain performance, data-format processing and comparative security and trust characteristics. Thus, PolyConnect addresses interoperability as an integrated data, security and cross-chain

verification problem rather than communication connectivity alone.

Methodology

Framework Architecture

PolyConnect aims to be a layered interoperability framework that allows for secure, chain-agnostic data exchange between different blockchains. The framework utilizes a record-centric interoperability design (19). Overall, there are four modules within the framework, each of which is responsible for different aspects of data exchange, validation and processing.

Record Layer

This layer specifies the standardized data representation that allows for the consistent interpretation of the records on different blockchains. This layer introduces data encoding in the form of a JSON based encoding that contains unique identifiers, system-level metadata and the application's specific data. Thus, the standardized JSON record is the input for the following processes, such as hashing, signing and storing in blockchains. This layer ensures semantic consistency across chains by abstracting data format differences and enforcing a particular data model. It decouples cross-chain metadata from domain-specific data, allowing disparate blockchains to validate and interpret records consistently. Figure 1 below shows the data schema used in PolyConnect.

```
{
  "recordId": "<Unique_Record_Identifier>",
  "recordType": "<Type_of_Record>",
  "actionType": "<created | updated | verified | transferred>",
  "metaRefs": {
    "issuerId": "<Originating_Entity>",
    "systemOrigin": "<Source_Blockchain_or_System>"
  },
  "payloadJson": {
    "entityGroupA": {
      "fieldA1": "<value>",
      "fieldA2": "<value>",
      ...
    },
    "entityGroupB": {
      "fieldB1": "<value>",
      "fieldB2": "<value>",
      ...
    },
    "entityGroupC": {
      "fieldC1": "<value>",
      "fieldC2": "<value>",
      ...
    }
  }
}
```

Figure 1: PolyConnect Standard Data Schema

The schema is generalized enough to allow application-specific data to be wrapped in a common header that attests to its cryptographic

authenticity and provenance, while retaining the ability to be processed and contextualized on different chains. Apart from standardization, the

Record Layer conducts an initial assessment of performance by recording the disk-write time when records are stored. This provides a preliminary performance metric before the data is transmitted across chains. Moreover, PolyConnect eliminates schema-level discrepancies that impede the process in most cases by standardizing the records at the initial stage.

Data Transfer and Proof Layer

This layer creates the standardised files for

transfer along with the cryptographic mechanisms necessary for authentication and verification. A SHA-256 digest is created for each file to aid in future verification processes (14–15). The payload is then saved using the IPFS (20), where the CID acts as its identifier. If the content is sensitive, then the system will generate a ZKP (21). The proof-generation process, depicted in Figure 2, is done by digitally signing the generated hash via the issuer and then linking it with the required metadata such as the CID, digital signature and timestamp.

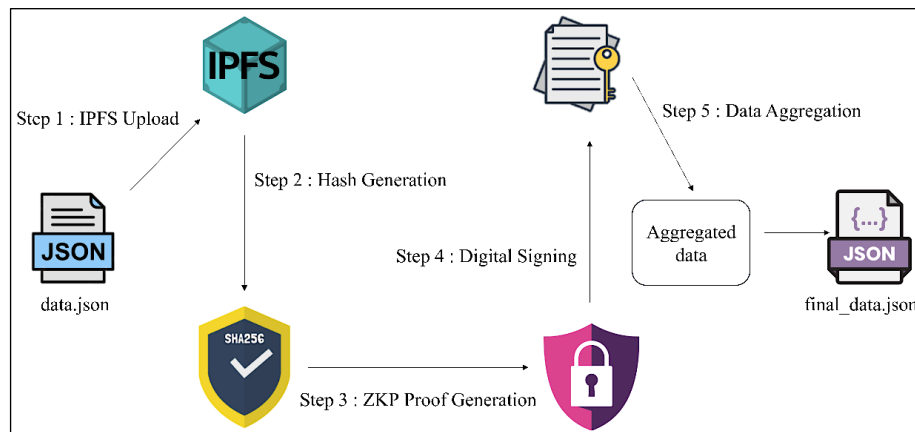


Figure 2: Data Transfer and Proof Generation

A major design goal of this layer is to maintain lightweight data structures to achieve the scalability of cross-chain communication. By doing so, this layer ensures integrity, immutability, authenticity and confidentiality of data with a reasonable overhead and a high degree of scalability for cross-chain data exchange.

Verification and Audit Layer

This layer is responsible for ensuring that any record received from another chain is trustworthy and tamper-proof by design. It cross-checks the hash value claimed by another chain with the freshly generated hash value of the received

payload to ensure data integrity throughout the transfer process. It authenticates the sender by checking the public key against the digital signature, thus ensuring that no one can impersonate the sender (22). The layer fetches the original file from IPFS using the CID and cross-references it with the metadata stored on chain to ensure accuracy. In case the submission contains privacy-preserving proof, it verifies the ZKP without disclosing the secret. The layer finally generates logs and metrics necessary for audit trails, compliance and post-event analysis. The Verification and Audit Workflow is depicted in Figure 3 below.

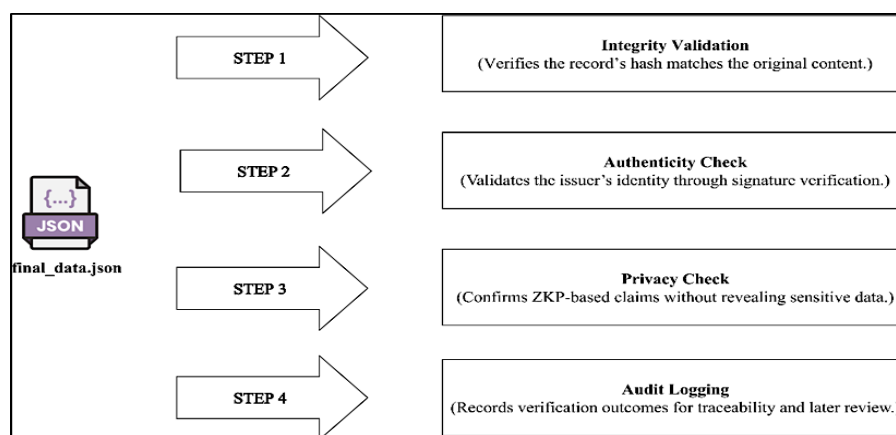


Figure 3: Verification and Audit Workflow

Blockchain Interaction Layer

This layer allows PolyConnect to interact with different blockchain platforms by designing pluggable handlers for hybrid, consortium, public and private blockchain networks (23). It transfers data by first loading metadata from the final json file into a particular ledger's transactional format using an appropriate handler and then writing it to

the ledger by invoking a chain code. By design, only the metadata is written into the blockchain, leaving room for each ledger to store a light verifiable reference of the original record. This approach provides PolyConnect with the flexibility to operate within heterogeneous trust domains and achieve full interoperability. Figure 4 below shows how the interaction layer works in detail.

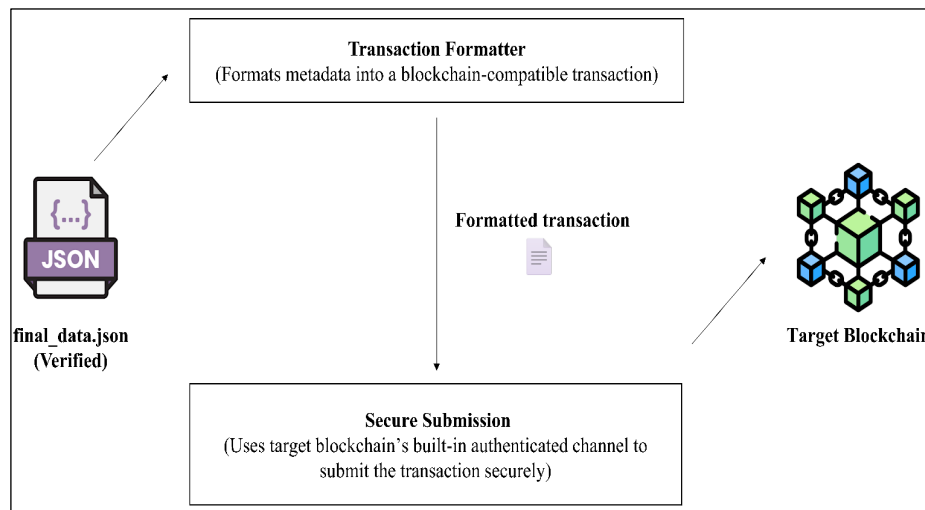


Figure 4: Blockchain Interaction Workflow

Figures 5 and 6 below represent the PolyConnect framework, which demonstrates the

cross-chain communication paradigm and internal processing flows.

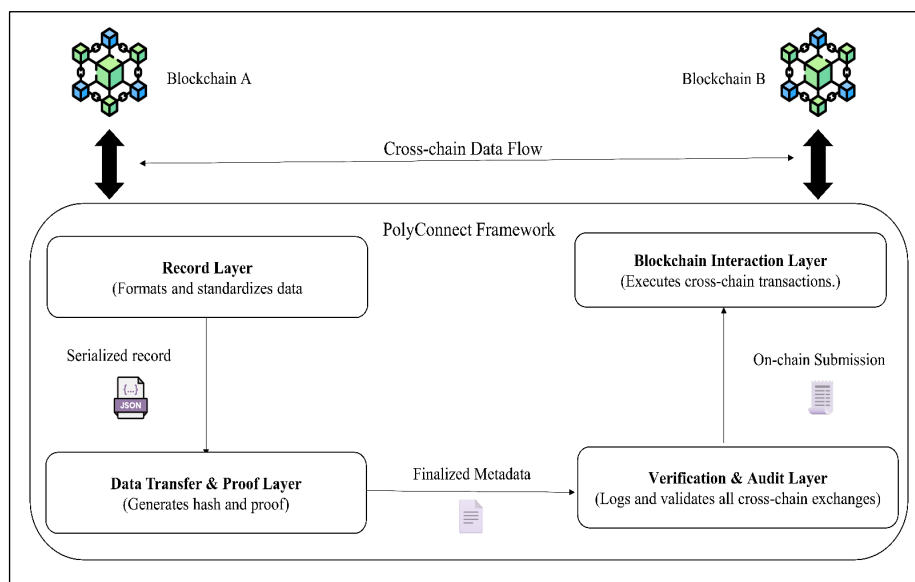


Figure 5: Overview of the Framework Workflow

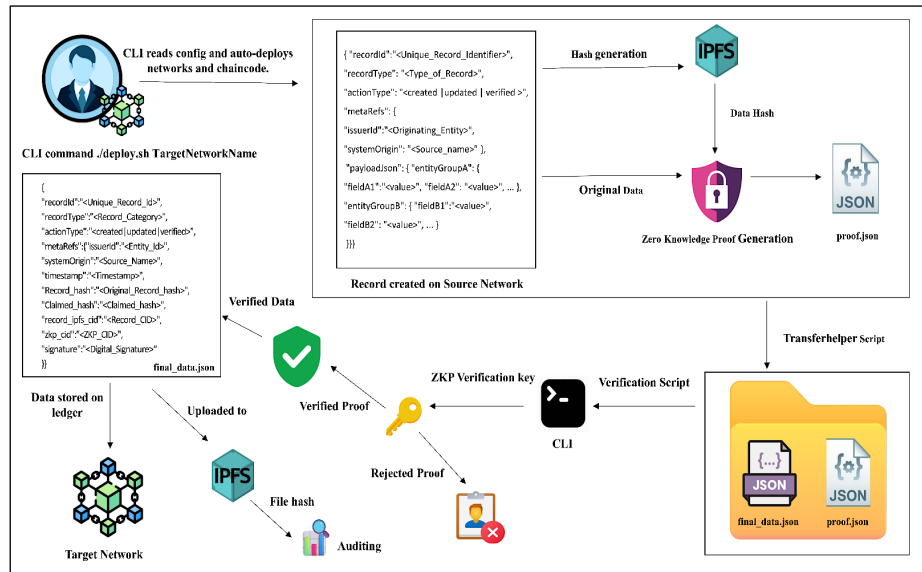


Figure 6: PolyConnect Internal Operational Workflow

Results

Evaluation Metrics

The proposed framework is evaluated for its computational and processing efficiency as well as its security features (24). This research considers

both traditional blockchain evaluation metrics and additional metrics relevant to cross-chain communication. Table 3 summarizes all evaluation measures considered in this research (25).

Table 3: Metric Definitions and Formulations

Metric	Description	Formula	Source
Total Processing Time	Total elapsed time for the complete workload	$TPT = t_{end} - t_{start}$	Standard metric
Throughput	Records processed per second	$TP = N / TPT$	Standard metric
Latency	Average transaction confirmation time	$Latency = t_{c,j} - t_{s,j}$	Standard metric
Data Fetch and Serialization Time	Time to fetch external data and format it for blockchain use	$DFST = T_f + T_s$	Proposed metric
Security Coverage Metric	Measures protection coverage against cross-chain security threats	$SCM = \frac{1}{N} \sum_{i=0}^N ci$	Proposed metric

Note: TP = Throughput, t_{end} = Timestamp when processing of the final record completes, t_{start} = Timestamp when processing begins, N = Number of records, j = Transaction, $t_{c,j}$ = Confirmation time, $t_{s,j}$ = Submission time, T_f = Data fetch time, T_s = Serialization time, ci = Binary coverage indicator for security category i.

Performance Evaluation

PolyConnect was evaluated across four blockchain network categories: Private, Public, Consortium and Hybrid, using workloads of 100, 500 and 1000 records (23, 24). Each configuration was evaluated through ten independent trials. Ten independent

trials were selected as a practical balance between obtaining reliable performance estimates and maintaining manageable experimental cost. The complete descriptive statistics for all network categories and workload sizes are presented in Table 4.

Table 4: Performance Statistics by Network and Workload

Records	Category	Mean TPT (s)	S _d	S _d ²	95% Ci (s)	C _v (%)
100	Private	12.33	0.40	0.16	12.04 - 12.61	3.24
100	Consortium	0.150	0.0044	<0.001	0.147 - 0.153	2.93
100	Public	26.01	0.85	0.72	25.40 - 26.61	3.25

100	Hybrid	26.06	1.07	1.14	25.30 - 26.83	4.10
500	Private	1114.96	19.42	377.01	1101.07 - 1128.85	1.74
500	Consortium	131.49	9.01	81.25	125.04 - 137.94	6.86
500	Public	140.45	3.36	11.31	138.04 - 142.85	2.40
500	Hybrid	80.55	5.19	26.97	76.84 - 84.27	6.45
1000	Private	7173.72	165.00	27223.94	7055.69 - 7291.75	2.30
1000	Consortium	2547.72	54.15	2932.11	2508.98 - 2586.45	2.13
1000	Public	607.21	7.43	55.25	601.89 - 612.53	1.22
1000	Hybrid	138.23	3.15	9.95	135.98 - 140.49	2.28

Note: S_d = Standard Deviation, S_d^2 = Variance, C_i = Confidence Interval, C_v = Coefficient of Variation, % = Percentage.

Across the evaluated workloads, the performance statistics show that PolyConnect can operate across all four blockchain configurations while exhibiting workload and configuration dependent processing behavior. Consortium provided the lowest processing time at 100 records, whereas Hybrid showed the most favorable scaling at 500 and 1000 records. Private exhibited a substantial increase in processing time as the workload increased, while Public showed comparatively steadier scaling. The relatively small standard deviations and confidence intervals across the trials indicate that the measured performance was generally stable within each configuration, with the coefficient of variation remaining low. Overall, the variation in performance reflects differences in the underlying blockchain processing characteristics and workload size, while the successful processing of all workloads through the same PolyConnect pipeline demonstrates its ability to handle heterogeneous blockchain environments effectively.

To formally assess whether TPT differed across network categories, a one-way ANOVA was performed separately for each workload using 10 independent trials per category. Significant differences were observed among the four network categories at all workload sizes: 100 records, $F(3,36) = 3064.78$, $p < 0.001$; 500 records, $F(3,36) = 20093.29$, $p < 0.001$; and 1000 records, $F(3,36) = 13655.26$, $p < 0.001$. These results confirm that the observed differences in TPT among network configurations were statistically significant at each workload size.

Heterogeneous Data Evaluation

PolyConnect was analyzed using datasets of different complexities that include basic JSON data to more complicated and time series data. There were four categories of datasets used as seen in Table 5. The DFST metric, described in Table 3, was used to evaluate data format processing performance.

Table 5: Heterogeneous Data Categories and DFST

Category	Key Characteristics	Complexity	DFST (sec)
Lightweight	Small JSON objects, few key-value pairs, no nesting	Low	0.74
Moderate	Shallow nesting, multiple fields, simple arrays	Medium	0.91
Complex	Deeply nested, hierarchical, heterogeneous fields	High	0.92
Time-Series	High-volume, sequential, timestamp-indexed	High	0.92

The results show that lightweight datasets required the lowest processing time, whereas datasets with greater structural complexity required higher processing time. The complex and time-series datasets showed similar DFST values, indicating comparable processing requirements under the evaluated conditions.

Security Evaluation

Security performance was evaluated against the 14 security threats identified in Table 2. The evaluation was performed layer by layer to examine the contribution of the proposed multi-level validation mechanism. For each configuration, the identified threats were assessed according to whether the enabled validation mechanisms could detect or mitigate the corresponding malicious or invalid condition. Table 6 presents the resulting layer-wise security performance.

Table 6: Ablation Analysis of Validation Layers

Architectural Layer	Mechanism Enabled	Detected Threats	Attack Detection (%)
L_2	Hash validation	3/14	21.42%
L_3	Digital-signature validation + ZKP	5/14	35.71%
L_4	Blockchain-state/replay validation	3/14	21.42%
$L_2 + L_3$	Hash + signature + ZKP	9/14	64.28%
$L_2 + L_3 + L_4$	Complete validation pipeline	12/14	85.71%

Note: L_2 = Layer Two, L_3 = Layer Three, L_4 = Layer Four.

The ablation results demonstrate that the validation layers provide complementary security rather than redundant checks. Hash validation ensures data integrity, digital signatures verify authenticity, ZKP validation strengthens proof verification and blockchain-state/replay validation ensures temporal and state consistency (21, 22). Thus, combining these layers addresses

distinct attack conditions that cannot be adequately covered by a single validation mechanism.

Security Coverage Evaluation

To provide an objective measure of security coverage, the SCM is defined as an unweighted binary coverage ratio over eight security categories listed in Table 2.

$$SCM = \frac{1}{N} \sum_{i=0}^N .ci \quad [1]$$

Where, $.ci \in \{0,1\}$ indicates whether a framework provides a documented and testable mechanism addressing security category i and $N=8$.

The eight categories represent the security dimensions used for SCM assessment as shown in Equation [1]. Equal weighting ($w_i=1$) is applied to all categories because no empirically validated severity hierarchy has been established among these dimensions, providing a transparent and reproducible baseline. For each framework, a category is assigned a binary value of 1 when a documented and testable security mechanism addresses that dimension and 0 otherwise. No partial or severity-based scoring is applied. The SCM is calculated as the proportion of covered categories among the eight predefined dimensions. A similar binary traceability criterion is uniformly used to evaluate all the frameworks based on the available security mechanisms and cited sources,

with the SCM scores presented in following table. A uniform denominator and a predetermined binary criterion ensure consistency across all the frameworks.

Comparative Evaluation

The comparative evaluation covers seven interoperability approaches, chosen to include major architectures adopted in blockchain interoperability. In contrast, PolyConnect was experimentally analysed based on its implementation and usage scenarios presented in this paper, while the performance and characteristics of the existing approaches were retrieved from the cited literature. The performance and efficiency characteristics of all evaluated approaches are reported in Table 7.

Table 7: Comparative Assessment of Selected Interoperability Approaches

Framework	Latency (sec)	Throughput (tx/s)	Scalability	Computational Overhead	References
Centralized Oracles	0.5–5	20–100	High (no consensus)	Low (no crypto checks)	(8)
Decentralised Oracles	5–30	5–20	Moderate (node aggregation)	Moderate (multi-node checks)	(8)
Notary/multi-signature Schemes	15–60	10–50	Moderate (quorum control)	Low (signature checks)	(11)
Cross-Chain Messaging Protocols	2–20	1–20	High (parallel routing)	Moderate (relay checks)	(1)

Asset and Data Transfer Bridges	30–600	1–15	Moderate (custodian step)	Moderate (custody checks)	(12, 14, 15)
HTLC/Atomic Swaps	600–3600	1–10	Low (cross chain checks)	Low (timelock checks)	(11)
Relay/Light-Client Mechanisms	600–3600	1–10	Moderate	High (light-client setup)	(9, 11, 26)
PolyConnect (proposed)	600–900	1–7	Moderate (multi-layer checks)	High (multi-layer crypto)	–

This comparison reveals the differences among the trust models, validation mechanisms, scalability and computational requirements. Trusted intermediary or semi-trusted intermediary based approaches typically involve less validation operations compared to the PolyConnect approach where validation is done using multi-layer

cryptographic and state-based verification. These differences arise from the different architectural and security requirements of the interoperability approaches assessed. Table 8 provides an analysis of existing approaches in terms of security coverage, decentralization, trust assumptions and deployment complexity.

Table 8: Security and Trust Comparison of Interoperability Approaches

Framework	SCM (%)	Decentralization	Trust Assumptions	Deployment Complexity	References
Centralized Oracles	25	Single operator	Trusts one operator's honesty	Low (single integration)	(8)
Decentralised Oracles	50	Committee-based	Trusts threshold, not one party	Moderate (node setup)	(8)
Notary / Multi-Signature Schemes	50	Notary quorum	Trusts quorum honesty	Low (quorum setup)	(11)
Cross-Chain Messaging Protocols	75	Validator/relayer set	Trusts relayer/validator honesty	High (relayer setup)	(1)
Asset and Data Transfer Bridges	37.5	Custodian controlled	Trusts bridge custodian	Moderate (custodian setup)	(12, 14, 15)
HTLC / Atomic Swaps	50	No intermediary	Cryptographic, trust-minimized	Moderate (timing setup)	(11)
Relay / Light-Client Mechanisms	75	No intermediary	Cryptographic, source-chain security	High (light-client setup)	(9, 11, 26)
PolyConnect (proposed)	87.5	No intermediary	Cryptographic verification, trust-minimized	High (handler setup)	–

The above comparison shows that approaches with less dependence on intermediaries and custodians offer better trust minimization via cryptographic or distributed verification methods. In comparison, those with more dependence on operators, committees, or custodians introduce additional trust assumptions.

PolyConnect falls under trust-minimized approach via cryptographic verification without an intermediary custodian and the increased architectural complexity in its deployment process is due to the security mechanisms incorporated into the framework.

Discussion

The findings indicate that PolyConnect adopts a secure approach for transferring data across chains. The findings also show that there is a trade-

off between improved validation and speed, which corresponds to the multi-level validation structure of the framework.

Performance and Scalability

The performance results indicate that the additional validation stages involved in PolyConnect lead to increased resource usage. The reduced throughput and increased latency in comparison to other approaches are due to the computational and verification requirements of the security mechanisms. The evaluation across diverse blockchain networks shown in Table 4 further indicates that performance varies with the characteristics of the specific blockchain environment. The variations show that performance across chains is affected by both the validation pipeline and the processing capabilities of the participating networks. The evaluation

across diverse data sources in Table 5 demonstrates that PolyConnect can process diverse records with relatively low data format processing overhead. The increase in processing time with greater data complexity indicates that serialization requirements are affected by the structure and volume of exchanged data. Thus, PolyConnect's performance should be considered in the context of both heterogeneous blockchain environments and data processing requirements involved in cross-chain operations.

Security and Validation

The ablation results show that the validation mechanisms provide complementary security coverage rather than redundant protection. Combining hash, signature, proof and state-based validation therefore improve the ability to address different attack conditions. The remaining undetected cases also identify limitations in handling acceptable timestamp variations and attacks involving already valid identities. Thus, PolyConnect should be considered a layered security mechanism rather than a complete defence against all attack classes. The SCM and Attack Detection percentage results provide complementary perspectives; the SCM measures security category coverage, whereas Attack Detection percentage measures experimentally detected attack scenarios. Their combined use provides a broader assessment of the framework's

security characteristics.

Comparative Analysis

The comparative analysis in Table 7 and Table 8 shows that interoperability approaches involve different trade-offs among security, performance, decentralisation, trust and deployment complexity. Approaches relying on centralized operators, custodians, or committees can reduce validation requirements but introduce additional trust dependencies (3, 11). In contrast, distributed and cryptographic approaches reduce intermediary dependence at the cost of additional verification. PolyConnect follows the latter model by combining cryptographic and blockchain-state verification without relying on a custodial intermediary. Therefore, it should not be interpreted as universally superior in performance, but as an approach that prioritizes security, auditability and trust minimization.

Failure Handling and Recovery

PolyConnect incorporates mechanisms for dealing with failures in communication and transactions without compromising data integrity and avoiding duplicate entries. Verification takes place before blockchain submission, while controlled retransmission is done for temporary communication failures. Failure situations and their respective mechanisms are discussed in Table 9 (23).

Table 9: PolyConnect Failure Handling and Recovery

Failure Condition	Recovery Mechanism
Interrupted communication	Retry submission up to 3 times with a short delay, mark the record as failed if all attempts fail
Network partitioning	Mark the record as failed if the target network is unreachable, allow resubmission after recovery and reserve automatic resumption for future work
Incomplete transactions	Reject records that fail hash, digital-signature, or ZKP verification before blockchain submission
Validator failure	Rely on the target blockchain's native consensus mechanism for fault tolerance

Conclusion

This paper presented PolyConnect, a security-centric interoperability framework that facilitates verifiable and trust-minimized data exchange across heterogeneous distributed ledger environments. The experimental results demonstrate effective security coverage and attack detection, while the ablation analysis confirms that the validation mechanisms provide complementary protection. The evaluation across private, consortium, public and hybrid blockchain

configurations further show that processing performance depends on both workload size and network characteristics, indicating that no single blockchain configuration provides uniformly optimal performance. The heterogeneous data evaluation also demonstrates that PolyConnect can process diverse external data structures with relatively limited data format processing overhead. The comparative evaluation positions PolyConnect as a security-focused and trust-

minimized interoperability framework. Therefore, the results support PolyConnect as a framework that prioritizes security, verifiability and heterogeneous data interoperability rather than universal performance superiority. These findings are subject to several limitations. The evaluation was performed in a controlled testing environment. The comparative evaluation of existing interoperability approaches was literature based rather than a controlled head-to-head implementation. In addition, two predefined attack scenarios remained undetected, larger-scale workloads require further scalability evaluation and the DFST evaluation did not include dispersion-based statistical analysis. The current evaluation also did not assess ZKP performance on resource-constrained platforms or include systematic fault-injection testing. Future work will therefore focus on larger attack corpora, production scale evaluation, ZKP benchmarking on resource-constrained hardware and repeated DFST measurements with dispersion analysis. Further work will also investigate adaptive anomaly handling, decentralized oracle validation and resource-efficient implementation.

Abbreviations

CID: Content Identifier, DFST: Data Fetch and Serialization Time, IPFS: Inter Planetary File System, SCM: Security Coverage Metric, TPT: Total Processing Time, ZKP: Zero-Knowledge Proof.

Acknowledgement

MAN Truck & Bus India Pvt. Ltd. is sincerely thanked for its financial support of this research.

Author Contributions

Suchitra Morwadkar: Conceptualization, Supervision, Anagha Kulkarni: Verification, Investigation, Critical Evaluation, Sanika Kulkarni: Development of the Framework, Experimentations, Data Analysis, Visualization, Manuscript Preparation.

Conflict of Interest

No financial or non-financial conflicts of interest are associated with this research.

Data Availability

The datasets utilized for this research were sourced from freely accessible APIs. Additional data were also generated using the custom record generator to create a suitable multi-domain benchmark for testing purposes. Cross-chain verification and submission were implemented in the open-source blockchain frameworks

Hyperledger Fabric, Ethereum, Hyperledger Sawtooth and MultiChain. In all cases, the default consensus mechanisms were utilized and no changes were made to the inner workings of the base platforms. PolyConnect was implemented as an additional interoperability layer on top of the selected blockchain frameworks.

Declaration of Artificial Intelligence (AI) Assistance

Authors assert that this article has been prepared entirely by the authors without any use of AI. The authors take full responsibility for the content's originality, interpretation and accuracy.

Ethics Approval

Neither patients nor animals were included in this study, hence there was no need for ethical approval.

Funding

The authors sincerely acknowledge MAN Truck & Bus India Pvt. Ltd. for their financial contribution towards this research.

References

1. Li W, Liu Z, Chen J, Liu Z, He Q. Towards blockchain interoperability: a comprehensive survey on cross-chain solutions. *Blockchain Res Appl.* 2025;6(3):100286. doi: 10.1016/j.bcr.2025.100286
2. Yuan H, Fei S, Yan Z. Technologies of blockchain interoperability: a survey. *Digit Commun Netw.* 2025;11(1):210-224. doi: 10.1016/j.dcan.2023.07.008
3. Belchior R, Vasconcelos A, Guerreiro S, Correia M. A survey on blockchain interoperability: past, present and future trends. *ACM Comput Surv.* 2022;54(8):168. doi:10.1145/3471140
4. Khan S, Amin M, Azar A, Aslam S. Towards interoperable blockchains: a survey on the role of smart contracts in blockchain interoperability. *IEEE Access.* 2021; 9:118672-118691. doi:10.1109/ACCESS.2021.3106384
5. Amadi RS, Kayes ASM, Pardede E, Chowdhury MJM, Ahmed K. A comprehensive review of risk assessment frameworks in blockchain applications: research gaps and key lessons. *IEEE Access.* 2025; 13:131347-131377. doi:10.1109/ACCESS.2025.3590963
6. Jiang J, Zhang Y, Zhu Y, Dong X, Wang L, Xiang Y. DCIV: decentralized cross-chain data integrity verification with blockchain. *J King Saud Univ Comput Inf Sci.* 2022;34(10):7988-7999. doi: 10.1016/j.jksuci.2022.07.015
7. Eren H, Karaduman Ö, Gençoğlu MT. Security challenges and performance trade-offs in on-chain and off-chain blockchain storage: a comprehensive review. *Appl Sci.* 2025;15(6):3225.

- doi:10.3390/app15063225
8. Al-Breiki H, Rehman MHU, Salah K, Svetinovic D. Trustworthy blockchain oracles: review, comparison and open research challenges. *IEEE Access*. 2020; 8:85675-85685.
doi:10.1109/ACCESS.2020.2992698
 9. Robinson P. Survey of crosschain communications protocols. *Comput Netw*. 2021; 200:108488.
doi: 10.1016/j.comnet.2021.108488
 10. Peelam MS, Chaurasia BK, Sharma AK, Chamola V, Sikdar B. Unlocking the potential of interconnected blockchains: a comprehensive study of Cosmos blockchain interoperability. *IEEE Access*. 2024; 12:171753-171776.
doi:10.1109/ACCESS.2024.3497298
 11. Ren K, Ho NM, Loghin D, Nguyen TT, Ooi BC, Ta QT, Zhu F. Interoperability in blockchain: a survey. *IEEE Trans Knowl Data Eng*. 2023;35(12):12750-12769.
doi:10.1109/TKDE.2023.3275220
 12. Notland JS, Li J, Nowostawski M, Haro PH. SoK: cross-chain bridging architectural design flaws and mitigations. *Blockchain Res Appl*. 2026;7(1):100315.
doi: 10.1016/j.bcr.2025.100315
 13. Yin R, Yan Z, Liang X, Xie H, Wan Z. A survey on privacy preservation techniques for blockchain interoperability. *J Syst Archit*. 2023; 140:102892.
doi: 10.1016/j.sysarc.2023.102892
 14. Li N, Qi M, Xu Z, Zhu X, Zhou W, Wen S, Xiang Y. Blockchain cross-chain bridge security: challenges, solutions and future outlook. *Distrib Ledger Technol Res Pract*. 2025;4(1):8:1-34.
doi:10.1145/3696429.
 15. Mishra D, Phansalkar S. Blockchain security in focus: a comprehensive investigation into threats, smart contract security, cross-chain bridges and vulnerabilities detection tools and techniques. *IEEE Access*. 2025; 13:60643-60671.
doi:10.1109/ACCESS.2025.3556499
 16. Cheng L, Lv Z, Alfarraj O, Tolba A. Secure cross-chain interaction solution in multi-blockchain environment. *Heliyon*. 2024;10(7): e28861.
doi: 10.1016/j.heliyon.2024.e28861
 17. Xia P, Guo Y, Lin Z, Wu J, Duan P, He N, Wang K, Liu T, Yue Y, Xu G, Wang H. WalletRadar: towards automating the detection of vulnerabilities in browser-based cryptocurrency wallets. *Autom Softw Eng*. 2024;31(1):32.
doi:10.1007/s10515-024-00430-3
 18. Wang G, Wang Q, Chen S. Exploring blockchains interoperability: a systematic survey. *ACM Comput Surv*. 2023;55(13s):1-38.
doi:10.1145/3582882
 19. Sonkamble R, Bongale A, Phansalkar S, Dharrao D. A secure interoperable method for electronic health records exchange on cross platform blockchain network. *MethodsX*. 2024; 13:103002.
doi: 10.1016/j.mex.2024.103002
 20. Mandinyenya G, Malele V. Comparative security and performance evaluation of IPFS and Filecoin for off-chain blockchain storage. *Indones J Comput Sci*. 2025;14(4):4968.
doi:10.33022/ijcs.v14i4.4968
 21. Zhou L, Diro A, Saini A, Kaisar S, Hiep PC. Leveraging zero knowledge proofs for blockchain-based identity sharing: a survey of advancements, challenges and opportunities. *J Inf Secur Appl*. 2024; 80:103678.
doi: 10.1016/j.jisa.2023.103678
 22. Zhou Q, Zheng Y, Wei K, Chen M, Zeng Z. A multi-party functional signatures scheme for private blockchain. *Cryptography*. 2023;7(2):21.
doi:10.3390/cryptography7020021
 23. Lo NW, Chen CC, Huang JJ, Lee SC. Dynamic generation mechanism of virtual blockchain networks for cross-chain transactions. *Enterp Inf Syst*. 2025;19(5-6):623-648.
doi:10.1080/17517575.2025.2492723
 24. Rasoloveicy M, Haouari W, Fokaefs M. BlockCompass: a benchmarking platform for blockchain performance. *IEEE Trans Comput*. 2024;73(8):2111-2122.
doi:10.1109/TC.2024.3404103
 25. Fan S, Ghaemi S, Khazaei H, Musilek P. Performance evaluation of blockchain systems: a systematic survey. *IEEE Access*. 2020; 8:126927-126950.
doi:10.1109/ACCESS.2020.3006078
 26. Kim M, Kim Y. A practical gateway-based interoperability framework for blockchains in Web3. *IEEE Access*. 2025; 13:153542-153556.
doi:10.1109/ACCESS.2025.3604816

How to Cite: Morwadkar S, Kulkarni A, Kulkarni S. PolyConnect: Trust Neutral Cross-chain Interoperability. *Int Res J Multidiscip Scope*. 2026;7(4):237-248.
DOI: 10.47857/irjms.2026.v07i04.013459