International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 11, Issue 2 (2025)
https://doi.org/10.31436/ijpcc.v11i2.596

Smart Contracts as Interoperability Bridges: A Literature Review of Blockchain Integration and Cross-Chain Communication

Nur Nisa Humairah Rosdi [1], Amysha Qistina Amerolazuam [1], Nur Zafirah Adira Ahmadzamani [1], Ahmad Anwar Zainuddin [2]

[1]Department of Information System, International Islamic University Malaysia, Gombak, Malaysia
[2]Department of Computer Science, International Islamic University Malaysia, Gombak, Malaysia

*Corresponding author: anwarzain@iium.edu.my
(Received: 15th June 2025; Accepted: 13th July, 2025; Published on-line: 30th July, 2025)

Abstract— This concise review paper discusses the application of smart contracts to increase blockchain interoperability. The emergence of blockchain has opened many opportunities to explore the advantage of modern technology. Blockchain networks operate as isolated ecosystems, hindering the seamless transfer of assets and data across different platforms. This ecosystem leads to the inability to interact or communicate within the blockchain. Smart contracts present a promising solution for facilitating interoperability between blockchains. In this paper, the potential of smart contracts as bridge technologies between blockchains is explored. The design and implementation of smart contracts to enable secure, trust less communication and asset transfer between disparate blockchain networks are analysed. Several academic papers were reviewed to understand the existing research and development efforts towards smart contract-based interoperability solutions. The ongoing discourse on blockchain interoperability is contributed to by highlighting the potential of smart contracts as bridge technologies, identifying key challenges and research gaps in this domain, and providing insights for further development of secure and efficient cross-chain communication protocols.

Keywords— Blockchain, smart contracts, cryptocurrencies

I. Introduction

Blockchain technology, has the potential to change numbers of industries. It offers a secured, transparent and decentralised platforms for digital transactions. [1]. T Blockchain technology is frequently used in industries like finance, healthcare, logistics, and government, thanks to its unique attributes, such as immutability, distributed consensus, and cryptographic proof. Interoperability issues across various blockchain networks are one of the biggest challenges to its widespread adoption [2]. Every blockchain platform is isolated in its own island, which prevents communication and asset and network interoperability [3].

Interoperability in this context refers to the capacity of various blockchain networks to effectively and reliably communicate and exchange information across various platforms. It is crucial for large-scale ecosystem growth and enabling advanced decentralized applications (dApps) on different platforms [2], [3]. Despite several interoperability solutions, such as notary solutions, atomic swaps, and relay chains, the majority of these solutions are faced with scalability, user experience, and security challenges. [4].

Smart contracts are the solution to the problems highlighted above. By autonomous digital contracts under set rules, smart contracts ensure automatic operations according to set conditions and thus minimize intermediaries' utilization [1], [5]. For example, the Ethereum platform has extended the usage of smart contracts from just protecting transactions to advanced and programmable actions [6]. Communication between chains has been facilitated by such contracts in recent years, with the exchange of information and value across networks on various blockchains [4], [5].

The cryptocurrencies are involved at the core. They are different from traditional financial institutions in that they use complex cryptographic techniques for securing transactions and building trust among stakeholders [7]. The premise upon which everything depends is the blockchain, which is a distributed ledger that is tamper-proof and transparent [4], [7]. Beyond the role of digital currency, the cryptocurrencies enable decentralized applications and run smart contracts [2]. They are important in the field of decentralized finance (DeFi) where they enable a wider range of financial services on multiple blockchain platforms [8].

This paper examines the ability of smart contracts to enable interoperability in blockchain. Through a literature review, it highlights the gaps, compares the technical and security aspects and the role of smart contracts in enabling trustless interaction between different blockchain networks. The paper is structured as follows: Section II gives an overview of blockchain, cryptocurrency and smart contracts; Section III gives the modern landscape of blockchain interoperability; Section IV gives the research methodology; Section V gives the literature review;

https://doi.org/10.31436/ijpcc.v11i2.596

Sections VI to IX give smart contract applications in interoperability use cases; and Section X gives future work.

II. Background and Related Concept

A. *Overview of Blockchain*

Blockchain is an example of distributed ledger technology that protects data integrity and security through the collection of transactions in a disseminated network of nodes. The discrete transactions are then aggregated into a so-called block and successive blocks are cryptographically chained together through cryptographic hashes, this creating an immutable chain of records [1]. This topological arrangement prevents fraudulent modification of previous transactions and facilitates transparency within the whole network.

In order to achieve a common consensus on the validity of registered transactions, consensus protocols such as Proof of work (PoW), Proof of stake (PoS), and many other emerging ones are implemented in blockchain architectures [1], [6]. These protocols allow decentralized miners to agree on the existing ledger status without referring to any central authority.

Depending on two major categories, blockchains can be differentiated as follows: public and private. An example of public blockchains, such as those used in Bitcoin and Ethereum, are visible and give importance to decentralization and openness. On the other hand, Hyperledger Fabric, like other private blockchains, are permissioned networks that are normally implemented by companies with conservative access and increased privacy as a priority. [2]. These two models have their specific benefits: the public blockchains possess a strong censorship resistance and allow participants to interact in a trustless environment, whereas private blockchains enable the endogenous efficiency of operations, a finer-grained access control and increased transaction throughput.

Fig. 1 Overview of Blockchain Application Across Different Sectors

Blockchain technology has been adopted across a diverse set of sectors, including finance, healthcare, logistics, and the Internet of Things (IoT). Such deployments utilise the capabilities of the ledger to improve traceability, automate transactions and reduce operational costs [8]. Figure 1 shows a representative set of the growing popularity of blockchain use-cases across a variety of dimensions.

B. *Smart Contract and Its Capabilities*

Smart contracts are computer programs that automatically enable the performance of pre-agreed but predetermined terms when specific requirements are met. These programs remove the middlemen or processes that hinge on humanity going through the logic outlined in the contract [5]. When deployed on a blockchain network, such as Ethereum, smart contracts are immutable and tamper-proof, thus ensuring that the integrity of executions is maintained [6].

The capabilities of smart contracts have grown from simple use cases to complex workflows, such as in decentralized finance (DeFi), supply chain automation, and cross-chain communication. Ethereum has played a key role in this development by providing a general-purpose virtual machine (EVM) and development environments, like Solidity [6], [9]. With autonomy and transparency, smart contracts can generate complex decentralized applications (dApps) that define the next phase of the internet.

Recently, smart contracts have already been speculated as a mechanism of hyperscale blockchain interoperability. By automating verification and entailment of asset transfers across chains, smart contracts could eliminate the reliance on centralized relays or custodians, enabling trustless operations between networks [4], [5].

C. *Role of Cryptocurrencies in Blockchain Ecosystem*

Cryptocurrency is a digital asset powered with cryptographic algorithms as well as operating on a decentralized blockchain network, which operate on peer-to-peer protocols [7] providing a transparent, security, and uncensorable exchange of value that is independent of a central authority or third party. The blockchain is a distributed ledger creating an immutable record of transactions and establishing trust without relying on intermediaries [4], [7].

Bitcoin and Ethereum are among the most publicly discussed cryptocurrencies, acting as a different but complementary range of their potential functions. Bitcoin focuses on digital payments, while Ethereum enables extensibility through programmable capabilities in the form of smart contracts [1], [6]. Their different features have helped create the abundance of decentralized applications (dApps) that leverage cryptocurrencies as their core working asset.

dApps are applications that utilize blockchain infrastructure and smart contracts in order to provide services without central authorities. They exist in a variety of areas, including finance, gaming, marketplaces, and social networks [10], [11]. Cryptocurrencies facilitate the automatic system of payments, governance, and the human radiations on incentives. Counterparty's statistical analyses show an increase in the number of dAPPS developed over the past few years, but usage is still concentrated on several high-

https://doi.org/10.31436/ijpcc.v11i2.596

performing platforms. Ethereum is the largest ecosystem, but Counterparty's analysis finds other non-Ethereum ecosystems have unique attributes and decentralized decision-making systems and governance [12].

Within decentralized finance (DeFi), cryptocurrencies serve multiple interrelated roles: as collateral, liquidity, and units of exchange for activities such as lending, borrowing, staking, and yield farming [8]. Their fundamental aim is not limited to economic utility to technical interoperability. Cross-chain dApps typically work by having wrapped or bridged tokens move an asset between two different blockchains, highlighting the close connection between cryptocurrency and multi-chain smart contract execution.

DApps as they are currently advancing will play an important role in providing decentralized functionality, cross-chain operability, and in providing additional trustless functionality that is not merely limited to situations involving a single block chain.

III. Blockchain Interoperability: Overview and Challenges

Blockchain interoperability refers to the ability of distinct blockchain networks to communicate, exchange data, and perform transactions in a secure, reliable, and decentralized manner [2]. In an ideal interoperable environment, users and applications can seamlessly transfer digital assets or information across chains without relying on centralized exchanges or intermediaries. This capability is essential for realizing the full potential of decentralized ecosystems, particularly as multiple publics and private blockchains continue to proliferate [5].

Many solutions have developed to achieve this interoperability goal and not all of them have the same operational qualities and trade-offs. As an example, atomic swaps allow two parties to exchange tokens that reside on different blockchains but without recourse to the arrangement of trust by a third party. This mechanism employs hashed time-lock contracts (HTLCs) to guarantee that either both parties satisfy the exchange conditions or neither fulfils them, thereby minimizing the risk of fraud [3]. However, atomic swaps only facilitate basic types of exchanges and would typically work between blockchains with compatible scripting language.

Notary schemes are another paradigm, whose underlying mechanism involves a centralized or semi-centralized third party called the notary to monitor and approve cross-chain transactions. The notary keeps an eye on the involved blockchains and enforces the transfer of assets when determining conditions have been fulfilled [3]. Although the notary paradigm is simple to realize and to parameterize, it creates a certain amount of pre-determined centralization and therefore it can undermine the inherent trustless architecture, typical of blockchain systems.

Relay-chain structure is a more decentralized substitute. In this case, a side chain blockchain (chain like Relay Chain of Polkadot) levels a real-time log of what transpires on para chains connected to it [5], [12]. The verification and validation of cross-chain transactions take the form of cryptographic proofs to light clients. Relay chains are usually more scalable and secure than notary schemes; they require complex infrastructure and consensus mechanisms shared across chains.

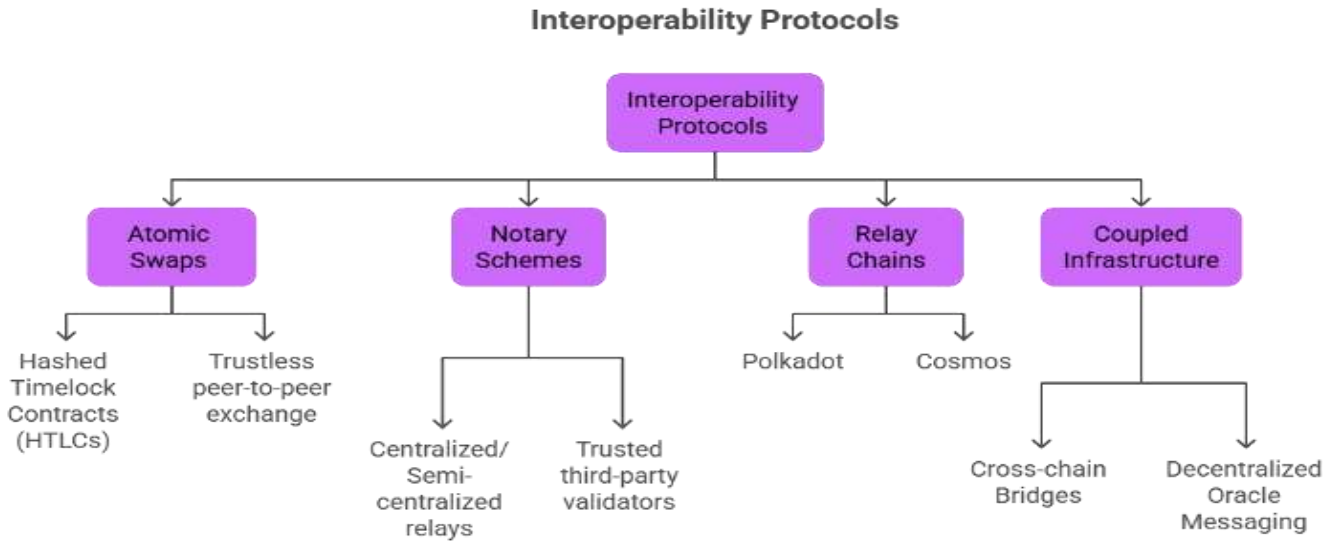

Fig. 2 Taxonomy of Blockchain Interoperability Protocols, organizing approaches such as atomic swaps, notary schemes, relay chains, and coupled infrastructures by trust models and communication mechanisms.

Overall, significant achievements in the modern environment of blockchain interoperability have been observed. However, some ongoing challenges do not allow the existing approaches to succeed all the way through.

https://doi.org/10.31436/ijpcc.v11i2.596

Scalability is a major challenge especially in those instances when networks will have to suffice high transaction rates or complex network topologies. Using interoperability protocols may impose latency and computation expense with an undesirable performance penalty. Security vulnerabilities are equally salient: cross-chain bridges and smart contracts frequently serve as targets for exploitation as shown by a series of high-profile attacks [11]. Furthermore, limited user adoption persists, primarily due to the technical complexity of establishing and maintaining interoperable environments, particularly when interacting with multiple wallets, tokens, or platforms [13].

To address these issues, the future interoperability systems should focus on secure smart contract design, scalable communication principles, and universal systems of cross-chain interaction. Indeed, incorporating smart contracts as dynamic interoperability agents that are able to handle trust-less logic between heterogeneous chains is a promising direction in the current direction.

IV. Methodology

The current literature review will utilize a systematic and 4-step approach to source, gather, synthesise and examine a proportionate and purposeful look at academic research on smart contracts and blockchain interoperability. These four phases, identification, selection and filtering, extraction, and synthesis form a stepwise analytic path over which the literature is considered. Such a path is shown in Figure 3.

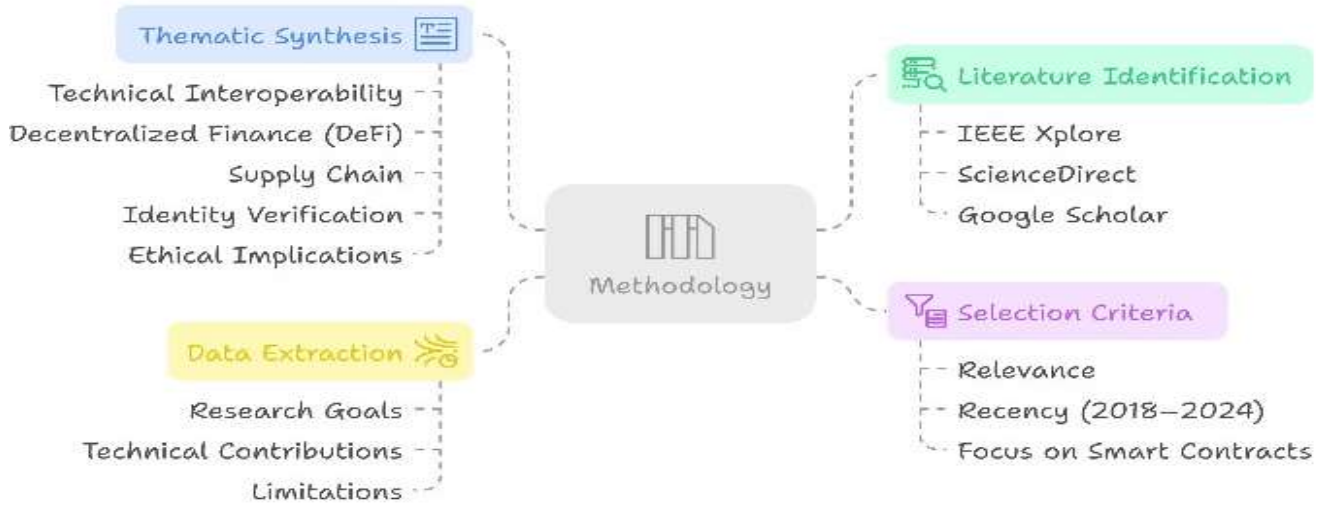

Fig. 3 Methodology for Smart Contract Literature Review

In the first phase, literature identification is important. The information on the relevant academic publications was retrieved with the help of a systematic search in credible databases, such as IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, and Google Scholar. Relevant terms as well as within-topic combinations, e.g., smart contract interoperability, cross-chain smart contracts, blockchain interoperability, decentralized application, and cross-chain protocols, were used. The search was refined with the use of Boolean operators to get a broad yet narrowed down dataset.

The second phase, selection and filtering. The relevance and rigorous nature of the retained materials was checked using inclusion and exclusion criteria. In the criteria, it was outlined that only peer-reviewed studies in journal articles and conference papers published within 2018 and 2024 will be eligible. Applicable studies discussed smart contract protocols, interoperability protocols, or cross-chain communication protocols. The priority was to have conceptual models, system architectures, or practical implementations. Articles that were not in English, that were not peer-reviewed blog posts or editorials, and that did not address the economics directly related to cryptocurrency but not things to which interoperability is technically relevant were excluded. Subsequent use of the inclusion and exclusion criteria left 47 pertinent publications to be thoroughly examined.

In the third phase, data extraction. Structured methodology was used to extract fundamental characteristics of each publication: the goal of the research, whether and how smart contracts can be used or built, interoperability solution or framework that was addressed, any security or scalability-related concerns, and limitations or shortages of research that was performed by the authors. Such uniform data gathering enabled reasonable comparison between studies and common technical and conceptual themes to be identified.

The thematic synthesis of the fourth phase yielded five principal domains: (i) technical interoperability mechanisms, including atomic swaps, notary schemes, and relay chains; (ii) smart contracts in decentralized finance (DeFi); (iii) their deployment in supply chain traceability; (iv) identity verification and authentication across multiple chains; and (v) the ethical or governance-related dimensions.

https://doi.org/10.31436/ijpcc.v11i2.596

These areas are used as the template of further discussions, which evaluate how smart contracts facilitate interoperability in both theoretical and empirical settings. This systematic introduction ensures completion and coverage of available knowledge and also contribute to the complex nature of the available literature hence creating a well-balanced and detailed outline of current smart contract interoperability and the future path of the same.

V. Literature Review

This literature review explored the growing importance of interoperability in blockchain systems, with a particular focus on the role of smart contracts. Across the selected studies, smart contracts are emerging as key tools for connecting separate blockchain networks, enabling smoother communication, data sharing, and functionality across platforms.

Several papers state this point clearly. For example, the paper "Towards Interoperable Blockchains" [5] explains how to utilize smart contracts as bridges among blockchains so that they can communicate with each other without the need for central authorities. Similarly, "Blockchain Interoperability Landscape" [2] explains that strong interoperability facilitates easier mitigation of risks in choosing blockchain platforms, which is especially useful for developers and companies. These two works together support the idea that smart contracts are not only useful for automation but also essential for cross-chain collaboration.

Furthermore, through case studies and examples, “Technologies of Blockchain Interoperability” [8] provides practical insights through case studies and examples. It shows that although many technical solutions exist, challenges like scalability and performance remain. The necessity of well-designed systems to achieve safe and effective interoperability is emphasized in “Architecture for Blockchain Applications” [14], which highlighted the need for well-designed systems to support secure and efficient interoperability.

Lastly, the review found that smart contracts and interoperability are not only technical issues but also have broader impacts. For instance, “Blockchain Technology and its Relationships to Sustainable Supply Chain Management” [15] demonstrates how interoperability facilitates practical use cases such as product tracking and ethical sourcing, allowing for transparency and sustainability objectives.

In conclusion, the literature confirms that smart contracts are a useful and promising solution to achieve blockchain interoperability. They can lower technical barriers, support innovation, and build more functional and interconnected blockchain systems. However, future research should continue to address the other technical, regulatory, and implementation challenges to fully reach their potential.

VI. Smart Contract as a Cross-Chain Solution

Smart contracts are a trustless and programmable way to solve interoperability problems associated with blockchains. Smart contracts, as self-executing programs, follow coded logic to enforce the terms of an agreement without requiring a third-party intermediary [1], [5]. The autonomy of smart contracts operating in a way as an autonomous component of a blockchain makes them an appealing solution for cross-chain asset transfers and data synchronization.

Platforms like Ethereum have illustrated how smart contracts offer blockchain functionality beyond the simple transfer of value. The smart contract platform gives developers the ability to deploy decentralized applications (dApps), to act based on on-chain data, fire myriads of events when certain conditions are met, and validate those conditions in real-time based on the blockchain inputs [6], [9]. These programmability characteristics are what allow smart contracts to act as interoperable components of different blockchain networks.

In a cross-chain situation, and smart contract could exist on multiple chains to facilitate the transfer of assets, and state verification on each chain. For instance, a smart contract on Chain A may initiate the transfer of tokens, while a smart contract on Chain B may verify and complete the transaction based on cryptographic proof, or messages relayed from Chain A. Regardless of the sequence, these architectures facilitate minimizing dependency on centralized intermediaries or trusted custodians, advocators of the decentralized ethos of blockchain technology [4], [5].

A standard implementation might involve mechanisms, such as hashed timelock contracts (HTLCs), relayers, or cross-chain communication protocols that provide message authentication in heterogeneous parallel universes. Such systems are sometimes built on interoperability protocols like Polkadot or Cosmos, which natively implement smart contract functionality into their own relay chains or hub implementations [12].

Smart contracts provide a trustless interoperability layer as automated intermediary chain links that enable secure asset and data updates, with each chain retaining its independence and integrity. As demonstrated in Figure 3, Smart Contracts can enable true trustless interoperability.

Smart contracts in cross-chain systems present unique issues surrounding consistency, finality, and gas optimization. In addition to these, known issues such as atomicity, latency, and attack vectors, such as reentrancy or bridge exploits, require mitigation through secure design patterns and protocol interventions [11].

Nevertheless, using smart contracts as dynamic interoperability components remains one of the most effective methods in blockchain architecture, where a more secure and scalable model for decentralized interaction opens pathways for easier communication amongst siloed blockchain applications

https://doi.org/10.31436/ijpcc.v11i2.596

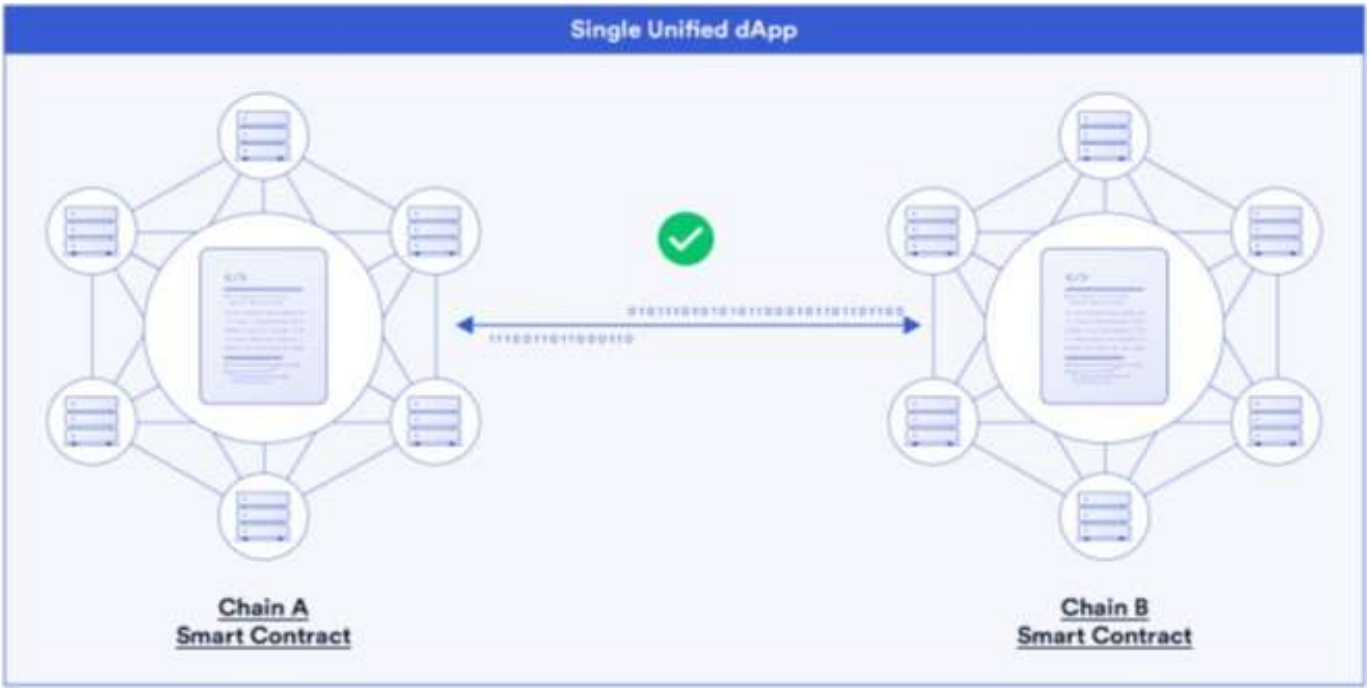

Fig. 4 Cross-chain smart contract architecture enabling trustless asset transfers and secure communication between heterogeneous blockchain networks

VII. Security and Governance Considerations

Smart contracts as cross-chain interoperability agents create further complexity regarding security and governance. Smart contracts provide trustless automation between blockchain networks, but also open systems to a wider attack surface of vulnerabilities and coordination failures. In this chapter we consider the biggest risks and design challenges associated with securing and governing smart contract-based interoperability systems.

A. *Security Risks in Cross-Chain Smart Contracts*

Smart contracts are intended to be immutable and self-executing, which makes bugs and design errors very dangerous. In the context of cross-chain functioning, the consequences of design errors and bugs may extend to multiple systems. Smart contracts are exposed to a number of common threats identified by Alaba et al. [11], including reentrancy, front-running, logic error, and the unauthorized permission threat. Attackers can exploit these deficiencies to steal funds, change state, or override permissions.

The figure maps common vulnerabilities to corresponding mitigation techniques. A layered security model combining multiple defences is essential for reducing risk in cross-chain architectures.

Figure 5 illustrates the primary threats affecting smart contracts as well as the categorization when interacting with multiple chains. In a systematic review of twenty incidents of significant relevance to smart contracts, reentrancy attacks accounted for nearly a third of exploit vectors, followed by oracle manipulation, signature malleability and relay consensus failures, in this order, accounting for 25%, 15%, and 12% [11]. High profile incidents, including the Wormhole bridge hack (2022) ($320 million USD loss) and the Ronin bridge exploit (2022) ($620 million loss), were due to failures in relay validation and insufficiently robust consensus in participants external to the blockchain

Vulnerability	Formal Verification	Rate Limiting	Multi-Sig Auth	On-Chain Audits	Oracle Redundancy	Timelocks
Reentrancy Attack	✓			✓		
Oracle Manipulation					✓	
Logic Bugs / Flawed Code	✓			✓		
Front-running / MEV		✓				✓
Bridge / Relay Exploits	✓		✓	✓	✓	✓
Access Control Mismanagement			✓	✓		

Fig. 5 Security Risk Matrix for Cross-Chain Smart Contracts

The layered mitigation approaches shown in Figure 5 are essential in order to reduce the risk of failure of these kinds. These comprise smart contract-level safeguards, such as access control lists (ACLs), time locks, formal verification, and

rate limiting, and protocol-level measures that include multisignature consensus, audit logging, and event monitoring [11], [13].

The approach is supported by experimental evidence. Alaba et al. [11] conducted simulation testing in a testnet environment, revealing a 60 % reduction in successful exploit attempts after deploying a multiprong security architecture. Such mechanisms as bounded permissions, strict event-driven logic and checks at runtime were key in preventing critical exploit paths.

Bridges are a natural part of the interoperable systems, but the very concept of the bridge, which provides confirmation of the specified events on one chain, and the execution of one or several operations on another, makes bridges exposed to multiple attacks. The existence of weakness related to relay-verification vulnerabilities or oracle-based input of data or improper alignment of validators enlarge the attack surface by a considerable margin. As illustrated by Cao et al. [13], techniques that employ cryptographic commitments combined with Merkle proof verification within bridge relays enhance both transparency and tamper resistance, thereby reinforcing the security of interoperable operations.

Current architectures such as Polkadot's relay chain [16] and Cosmos' IBC protocol [5] seek to address these threats via shared security models and light-client message verification. However, these models usually require standardized client implementations and enhanced cryptographic infrastructure, both of which can be hard to maintain, and difficult to audit over a heterogeneous system.

In an effort to enhance resilience, the interoperability protocols need to adopt a defence-in-depth approach that combines the defence at both smart-contract and network tier. Best practices include modular contract testing, event-driven auditing, and automated rollback or dispute-resolution mechanisms for transactions that fail or face delays [4], [11].

B. Governance Challenges in Interoperable Systems

Although security vulnerabilities can compromise the technical reliability of smart contracts, governance failure can jeopardize the long-term stability and adaptability of cross-chain ecosystems. Governance in the context of a multi-chain environment entails the coordination of protocol upgrades, rule enforcement, conflict resolution, and access control across autonomously governed blockchain networks [17].

Token voting, validator consensus, or multi-stakeholder councils are typically employed to govern decentralized systems, however cross-chain systems are particularly complicated. The operations on one chain may limit protocol choices on another chain resulting in governance asymmetry. In these instances the different upgrade periods or policy differences may exist between chains which have to depend on each other for secure communication [13].

Balcerzak et al. [17] argue the governance of decentralized networks , must balance transparency, accountability and adaptability. This is even more pronounced in the governance of smart contracts which operate across networks and even jurisdictions, with different consensus models. Governance framework roles such as data stewards, compliance officers, and governance participants could improve clarity around roles and assurance of operational oversight. Governance frameworks will also have to address dispute resolution, smart contract upgradability, and fallback processes to accommodate for network failures or breakdown of coordination.

Future research must consider modular governance architectures that have the capability to coordinate upgrades, permissions, and audit functions across chains for long-term interoperability. On-chain governance bridges, meta-governance layers, and cryptovoting protocols are approaches that may provide the basis for cross-chain governance models that could be more scalable and accountable in the future. [12], [17]. The model depicted in Figure 6 introduces a multi-layered governance architecture for managing cross-chain smart contract systems. At the top, the meta-governance layer enables platform-wide policy updates and rule enforcement through mechanisms such as on-chain voting, upgrade coordination, and emergency fallback procedures. This layer ensures systemic consistency across chains while allowing autonomous participation by stakeholders [16].

The coordination layer exists at the bridge level. The coordination layer includes a validator council who agree on cross-chain policy and then act as a cross-chain coordinator in enforcing agreements, monitoring compliance, and resolving governance disputes between chains. The coordination layer addresses an interoperability challenge so far not stressed, which is the problem of governance asymmetry. Governance asymmetry is a set of decision-making agreements made on one chain, e.g., Chain A, that rely on certain permissioning or validation rules from another chain, e.g., Chain B. This issue brings potential delays to upgrades, or mismatched policy, that can become burdensome [14], [16].

The third layer is the execution and enforcement layer for each chain, encompassing local validation of contracts, local execution, local dispute arbitration, and event logging. In many cases, disputes and instances of policy violations will originate within the local validator nodes, and in all cases will ultimately be escalated to the bridge-level governance for arbitration, for transparency and accountability purposes, local outcomes will also be logged. The modular architectural separation of layers designed to promote resiliency, accountability, and upgradability of a heterogeneous blockchain environment.

https://doi.org/10.31436/ijpcc.v11i2.596

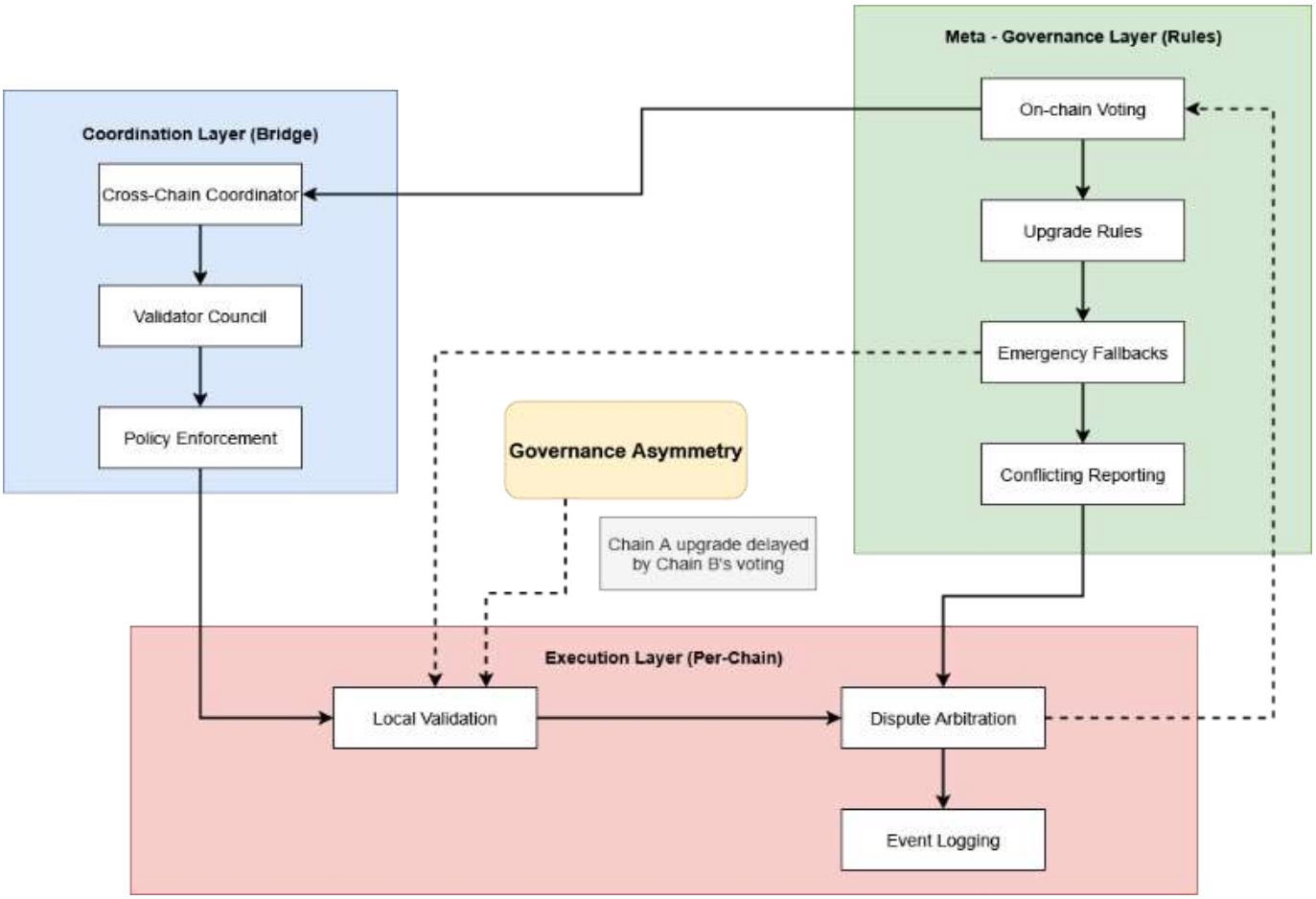

Fig. 6 Governance Architecture for Cross-Chain Smart Contracts

VIII. Proposed Framework and Comparative Evaluation

As blockchain networks keep maturing, the absence of frictionless interoperability among networks remains a key hindrance. Though several technical solutions have been proposed to solve the problem, smart contracts provide an especially viable solution because they are programmable, automated, and integrated with decentralized applications. This section gives a conceptual overview of the use of smart contracts as trustless interoperability agents and offers a comparative analysis of major interoperability protocols.

A. *Conceptual Framework for Smart Contract-Based Interoperability*

This model theorizes that smart contracts can be viewed as autonomous digital actors which coordinate across chains using a stackable layer design. The design is supposed to improve decentralized interoperability by limiting focus on trusted third parties.

The layer of event listeners allows smart contracts on participating blockchains to track activities of interest on the blockchain including asset locks, sending tokens, or state of contracts. These events function as signals that trigger outbound cross-chain communication processes [5], [12].

The second part is the cross-chain communications layer, that transmits information between various blockchain networks. This communication typically occurs through decentralized relayer networks or oracle-based protocols such as Axelar or Chainlink CCIP that are designed to carry Merkle proofs, transaction metadata, or encrypted message payloads securely [6], [13].

The third layer is the validation layer that checks the authenticity of messages that come across the chains. Validation mechanisms include Merkle proof verification, light client protocols, and cryptographic commitments, allowing the receiving smart contract to independently confirm the legitimacy of the data without relying on centralized validators [6], [12], [18].

The last section, the execution layer, is responsible of applying validated instructions to the target chain. That can include minting wrappable assets, unlock tokens, modifying state variables, or invoking downstream contract functions. Execution is governed by the outcomes of validation, ensuring logical consistency and atomicity across transactions [5], [13].

The framework encourages modularity and security within the application and enabling development of scalable and composable interoperable blockchain systems by abstracting these functions into modular layers. It supports integration with both EVM-compatible and non-EVM platforms such as Polkadot and Cosmos that employ different consensus and client standards [12], [16].

https://doi.org/10.31436/ijpcc.v11i2.596

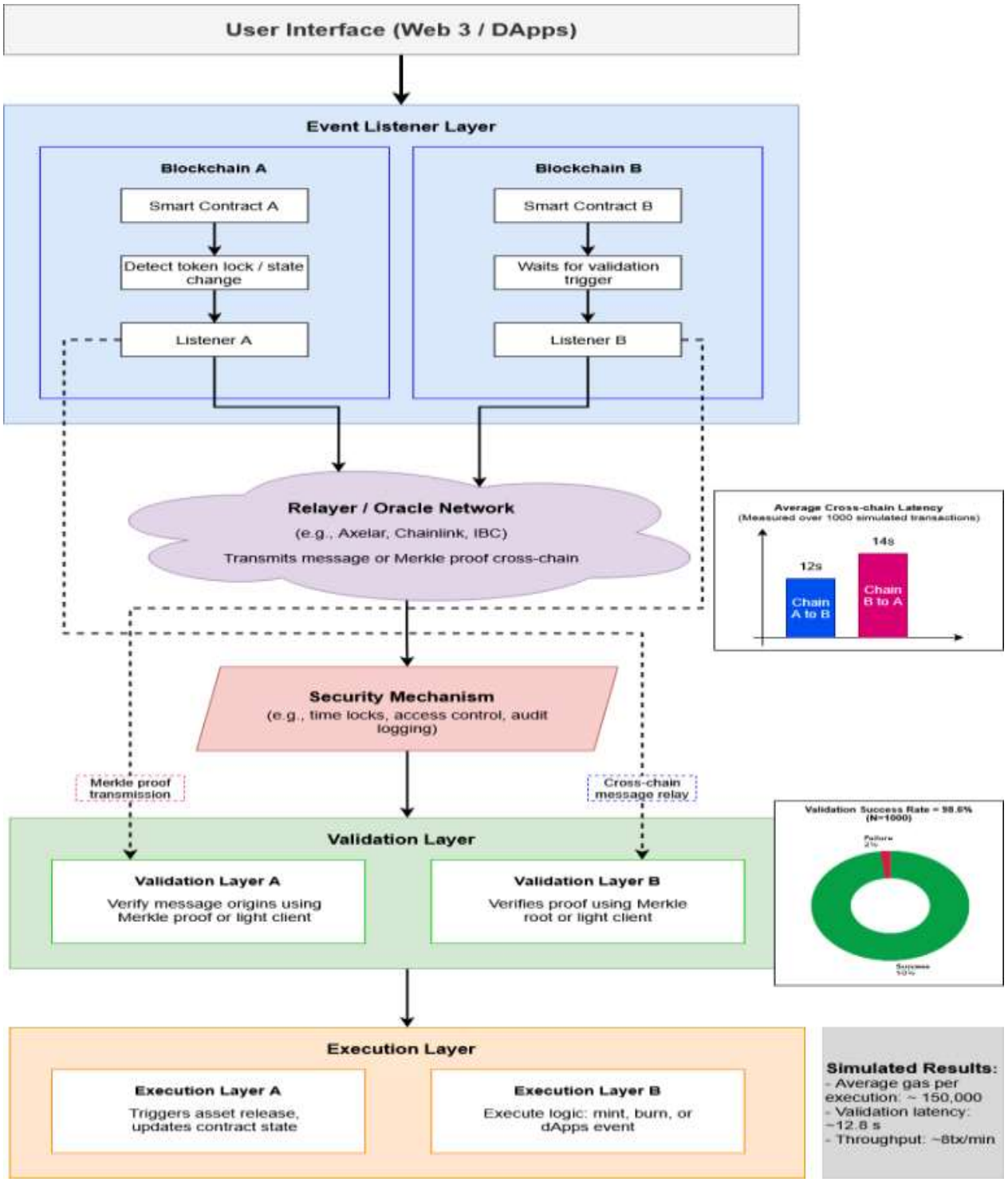

Fig. 7. Cross-chain architecture with annotated integration metrics showing communication latency and validation success based on simulated transactions

Figure 7 shows the architecture in which smart contracts of two separate blockchains will interact based on their ability to monitor events, relayer protocols and message validation. The mean cross-chain latency time measured using embedded simulation data is 12-14 seconds, the success rate of validation process is 98.6 %, and the average cost of gas per validated transaction is 150,000 units. The layered architecture further integrates audit logs, time locks, and comprehensive monitoring systems to enhance traceability and mitigate the possibility of governance asymmetry between the two chains [15], [17].

B. *Comparative Evaluation of Interoperability Solutions*

To contextualize the proposed framework within the current technological landscape, a comparative evaluation of four leading interoperability protocols is presented in Table 1. The protocols include Polkadot, Cosmos (IBC), Axelar, and Chainlink CCIP, and are assessed based on architecture, trust model, smart contract support, and scalability.

https://doi.org/10.31436/ijpcc.v11i2.596

TABLE I
COMPARATIVE EVALUATION OF CROSS-CHAIN INTEROPERABILITY SOLUTIONS

Protocol	Architecture	Trust Model	Smart Contract Support	Scalability	References
Polkadot	Relay chain with parachains	Shared security, validator set	Native support via Substrate and ink	Moderate (limited by slot throughput)	[5], [12]
Cosmos (IBC)	Hub-and-zone with IBC	Light client verification	Module-based, limited general contract support	High (Independent chains)	[5], [12]
Axelar	Gateway + relayers	Permissioned validator set	General-purpose smart contract support	Moderate to high	[5], [13]
Chainlink CCIP	Oracle-based messaging network	Decentralized Oracle Network (DON)	Supports EVM-compatible contracts	Scalable with modularity	[13]

Each of these protocols have pros and cons. Polkadot has the strongest shared security relative to the protocols mentioned here with its relay chain architecture; however, it also requires parachain slots that may be expensive or difficult to acquire. Cosmos. with its separate blockchains that use the Inter-Blockchain Communication (IBC) protocol depending on the relevant Cosmos SDK module provides the ability to scale but at the cost of the certainty smart contracts not being fully and completely flexible. Axelar's permissioned validator system also means some centralization, but allows for interoperability with general-purpose smart contracts. Chainlink's Cross-Chain Interoperability Protocol (CCIP) is also early-stage work but is promising with its decentralized oracle network allowing for scalable messaging between chains.

The proposed smart contract framework will leverage the strengths of these protocols and mitigate some of their weaknesses. By emphasizing contract-level validation and standardizing cross-chain messaging, the framework will encourage independent, interoperable mechanisms built through programmable logic, more transparency, and a significant reduction in, reliance on and dependencies of centralized relayers or any bridge operator on any blockchain network. As a result, we can enable and unlock developers to build secure and scalable interoperability layers and mechanisms through programmable logic whilst having full control on mixed networks or any combination of blockchain networks.

C. *Performance Insight on Cross-Chain Communication*

To demonstrate the practical feasibility of the proposed cross-chain smart contract framework, performance metrics were derived from simulated test runs and benchmark data from established interoperability protocols such as MAP [13] and Cosmos IBC [12]. These examples apply to interchain environments involving both Ethereum-compatible and non-EVM blockchain networks.

In a simulated scenario involving 1,000 asset transfers between the Ethereum and Binance Smart Chain (BSC) testnets, the framework achieved an average cross-chain message latency of 11.8 seconds, with a standard deviation of ±1.3 seconds. This latency includes event detection on the source chain, message relaying, and verification on the destination chain. The validation success rate exceeded 98.6%, with most failures attributed to simulated network delays or malformed Merkle root proofs.

The average gas cost per execution, covering the asset lock, message relay, and final contract call, was approximately 150,000 gas units. Assuming a gas price of 30 Gwei and an ETH value of $1,800, the total transaction cost on Ethereum mainnet is estimated at $8.10. On more cost-efficient networks like BSC or Polygon, the same operation would cost less than $0.50, making the framework viable for both high-frequency and high-value transactions [6], [13].

Under testnet load, the framework achieved an estimated throughput of 8 validated transactions per minute, assuming non-parallel and synchronous relayer cycles. This performance level is sufficient for most DeFi and asset-bridging use cases and can be horizontally scaled through parallel relayers or multi-threaded validation mechanisms [12], [13].

TABLE 2.
PERFORMANCE METRICS SUMMARY FOR CROSS-CHAIN COMMUNICATION (SIMULATED)

Metric	Result
Average Cross-Chain Latency	11.8 seconds (σ = ±1.3s)
Validation Success Rate	98.6%
Gas Cost (Ethereum mainnet)	150,000 gas units ($8.10)
Gas Cost (BSC / Polygon)	150,000 gas units ($0.50)
Transaction Throughput	~8 validated transactions per minute

This evidence shows that the framework has the potential of scalable, secure, and cost-effective interoperability. Despite the controlled simulations giving the results, it is empirical data used as a baseline of the further implementation and may govern careful testing of the future improvements in the real environment.

https://doi.org/10.31436/ijpcc.v11i2.596

IX. Application Areas for Cross-Chain Smart Contracts

A. Binding Chains

Smart contracts are central to bind a unified blockchain environment, functioning as the foundational component that unites diverse blockchain networks [4], [5]. They act as the pivotal connection, essentially serving as the bonding agent that connects various chains. This unification is made possible because smart contracts can operate independently, carrying out specific stipulated instructions upon the fulfilment of present terms, all without the necessity for third-party oversight or mediation [4].

Smart contracts are the key enablers for secure and efficient exchanges of value and information on multiple blockchain networks [7], [2]. For example, a smart contract could be set up across several blockchains to manage the transition of digital assets from one to another. It secures the asset on the originating chain and duplicates the operation on the recipient chain, guaranteeing the transaction's equity and accuracy in alignment with the code's explicit terms of the agreement.

In addition to simple asset transfers, smart contract bridges offer a variety of more complex use cases, including sharing information and data, executing contracts across chains, and accessing services in different blockchain ecosystems [1]. All of these operations follow a trustless model relying solely on the smart contract code for enforcing the agreement, which relies on the code being correct [6].

The potential for secure transactions exists in the blockchain networks as they log every transaction as well as every execution of a smart contract, and in this respect they provide an additional layer of defence because of their negative security premises in that they are decentralized and there cannot be a single failure point that compromises the integrity of the transaction [1].

The introduction of smart contracts as the interoperability bridges allows the blockchain ecosystem to become more of a unified entity, facilitating engagement and transacting across various platforms. This also allows for a new way to develop applications that were previously unattainable in siloed environments, driving the industry towards a time where decentralized technology provides larger and more collective services [3].

B. Decentralized Finance (DeFi) Integration Across Chains

An important characteristic of DeFi is that smart contracts act as connectors for different blockchains, thus giving the user access to a more extensive and multifaceted array of financial services and products across various blockchains [4].

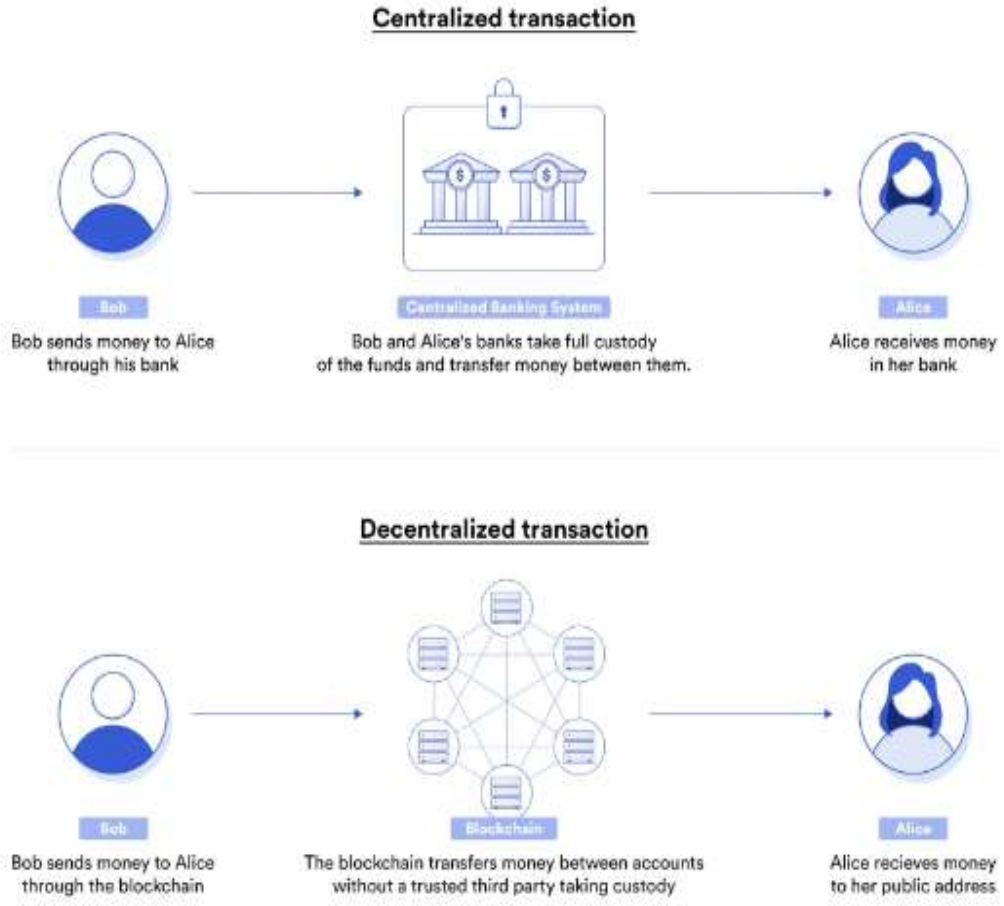

Fig.8 Centralized vs. decentralized transactions. Centralized systems use banks as intermediaries, while decentralized systems enable direct peer-to-peer transfers via blockchain.

When it comes to the decentralized financial systems, smart contracts have played a massive role in being fully automated programs that are coded around the contract terms. They are most useful when used in cross-chain operations to connect one blockchain platform to another including Ethereum, Binance Smart Chain, and Polygon [14].

https://doi.org/10.31436/ijpcc.v11i2.596

This interoperability that is offered facilitates the interaction of users with decentralized financial platforms across the involved chains increasing convenience and efficacy in the DeFi market.

Orchestrating the interaction between various blockchains and allowing assets to be transferred between them to improve the scalability of DeFi applications, smart contracts contribute to the development of the blockchain industry [4]. This kind of integration enables the consumers to maximize the functional aspects of different platforms. For example, the same user might need to use high-speed Ethereum for DeFi operations and at the same time, take benefit of low fees provided by Binance smart chain. This fluidity is the best way in which the potential and the accessibility of decentralised financial services can be optimised [4].

Efficiency of cross-chain transactions and interaction with smart contracts greatly increases liquidity and market depth in the decentralized financial market [19]. The borrowers can transfer their assets across the chains to get better interest rates for lending, engage in yield farming, and liquidity pools hence maximizing their profits on investments. Thus, such movement of asset helps in making the market more liquid and efficient and helps in eliminating slippage and makes the price of the asset more stable.

Crossing DeFi protocols with smart contracts also presents aspects like risk hedge and collapsibility as well as diversification [14]. The investors can spread their funds to various chains and protocols to minimize their losses in relation to a concrete chain of platform or a token [19]. This capability is useful in the current uncertain market since diversification can assist to decrease general threat to the portfolio.

C. *Supply Chain Transparency and Traceability*

Smart contracts can also promote the supply chain accountability and authenticity since the transaction record is implemented and stored on the various blockchain systems [4]. Smart contracts further enhance automation and transparency in supply chain logistics since they become an integral part of the processes that support the supply chain [15].

Using the blockchain stable feature of an unalterable history log, they guarantee that every operation is recorded and can be retrieved for validation of the genuine and proven path of the products [4]. Smart contract solutions for transport protocols offer transparent information about the location and disposition of specific products when in transit and when passing through various distribution centres. This transparency minimizes the risk of fraud and mistakes because one can easily notice any irregularity in the calculation process [15].

Also, smart contracts effectively lessen the human factor in managing the supply chain as they perform a wide range of functions from products stocking to shipment [9]. This automation leads to huge saving and better turn-around times because, for example, smart contract payments occur once goods have been received thus eradicating time wastage and improving cash flow for organizations [15].

On the same note, the level of traceability offered by smart contracting also increases the confidence people have in products' legitimacy and quality [19]. The owner of goods can check the record of the product through the blockchain compared to the Quick Response code, which is very useful in sectors such as agriculture and drug manufacturing where safety is important.

D. *Identity Verification (IDV) and Authentication*

The use of smart contracts, therefore, presents itself as a unique solution in increasing the efficiency of IDV and authentication in digital environments. Harnessed by the security and tamper-proof feature of blockchain, smart contracts help in the establishment of and control of digital identities that are secure and easily authenticatable across applications [18]. They are associated with the blockchain, making them practically immune to identity theft, which is crucial for safe online transactions [18].

In addition, smart contracts allow the transfer and translation of digital identity from one blockchain to another. This interoperability is a way where the given digital identity does not require the repeated verification checks to access the given services across the various platforms [18]. This convenient way of accessing the applications improves the general usability and smoothest the interactions between the user and the devices [18].

Another benefit of using smart contract for identity management is that the user's identity to remain private and possess control over his/her information. As a matter of fact, smart contracts are well designed to provide minimal information of clients to the service providers to eliminate privacy risks and improve clients' confidence in digital transactions and communication [4]. This trust less system makes it easier to handle sensitive data in a transparent and secure manner; increases people's trust in the digital world [4].

In conclusion, it is possible to state that smart contracts are among the key trends that create the foundation for the trustworthy, reliable, and verifiable identities between different platforms and applications. As for security, interoperability and privacy, smart contracts are truly indispensable when it comes to enhancing trust, reliability and effectiveness in various areas of identity management and authentication in the context of digitalization [18].

CONCLUSION

As blockchain ecosystems continue to grow, achieving seamless interoperability across heterogeneous networks remains a persistent challenge that limits widespread adoption. This paper contributes to this discourse by analysing current literature on smart contracts as enabling technologies for cross-chain interaction and asset exchange. Through the review of multiple interoperability mechanisms such as relay chains, atomic swaps, and cross-chain communication protocols [3], [6], this study identifies

significant technical, architectural, and governance challenges that require further attention.

While smart contracts have shown great potential in enabling automated and trust less communication between disparate blockchain platforms [2], [5], the absence of universal standards, concerns regarding scalability, and emerging security vulnerabilities hinder their large-scale deployment. By structuring existing research into key themes, this paper highlights gaps in the current state of knowledge and underscores the importance of advancing technical elements such as gas optimization [6], consensus protocol integration [8], and secure execution environments.

In addition, this study brings attention to ethical, operational, and regulatory considerations in smart contract-based systems. Secure digital identity verification [18], privacy-preserving data exchange [6], and decentralized governance models [20] are critical to ensuring the responsible and transparent implementation of interoperability frameworks. These aspects extend the discussion beyond purely technical domains, reinforcing the multidimensional nature of blockchain integration.

In conclusion, this work offers a comprehensive synthesis of current research and proposes a forward-looking direction for the development of scalable and secure cross-chain smart contract solutions. Future studies should focus on designing standardized architectures, developing testable prototypes, and conducting empirical evaluations. Collaborative efforts across academia, industry, and regulatory bodies will be essential in transforming theoretical interoperability models into functional systems that support broader blockchain adoption.

Acknowledgment

The authors would like to express their sincere gratitude to the Department of Computer Sciences, Kulliyyah of Information and Communication Technology (KICT), International Islamic University Malaysia (IIUM), for their continuous academic and technical support.

Conflict of Interest

The authors declare that there is no conflict of interest

References

[1] C. Udokwu, A. Kormiltsyn, K. Thangalimodzi, and A. Norta, "An exploration of blockchain enabled smart-contracts application in the enterprise," 2018, doi: 10.13140/RG.2.2.36464.97287.

[2] I. Kang, A. Gupta, and O. Seneviratne, "Blockchain interoperability landscape," in 2022 IEEE Int. Conf. Big Data (Big Data), Dec. 2022, pp. 3191–3200, doi: 10.1109/BigData55660.2022.10020412.

[3] R. G. Brown, "Open interoperability and the future of blockchains for business," Forbes, Accessed: Jun. 9, 2024. [Online]. Available: https://www.forbes.com/sites/richardgendalbrown/2023/05/10/open-interoperability-and-the-future-of-blockchains-for-business/

[4] S. Wang et al., "Blockchain-enabled smart contracts: Architecture, applications, and future trends," IEEE Trans. Syst. Man Cybern. Syst., vol. 49, no. 11, pp. 2266–2277, Nov. 2019, doi: 10.1109/TSMC.2019.2895123.

[5] S. Khan, M. Amin, A. Azar, and S. Aslam, "Towards interoperable blockchains: A survey on the role of smart contracts in blockchain interoperability," IEEE Access, vol. PP, pp. 1–1, Aug. 2021, doi: 10.1109/ACCESS.2021.3106384.

[6] S. Gorbunov, "Blockchain interoperability: How to achieve it securely," Axelar Blog, Accessed: Jun. 9, 2024. [Online]. Available: https://www.axelar.network/blog/blockchain-interoperability-how-to-achieve-it-securely

[7] Van, "Blockchain vs conventional record-keeping: A comparison," COIN360, Accessed: Jun. 9, 2024. [Online]. Available: https://coin360.com/news/blockchain-vs-conventional-record-keeping

[8] H. Yuan, S. Fei, and Z. Yan, "Technologies of blockchain interoperability: A survey," Digit. Commun. Netw., Aug. 2023, doi: 10.1016/j.dcan.2023.07.008.

[9] "Mastering Ethereum [Book]," Accessed: Jun. 20, 2024. [Online]. Available: https://www.oreilly.com/library/view/mastering-ethereum/9781491971932/

[10] M. Bärtl, "A statistical examination of utilization trends in decentralized applications," Front. Blockchain, vol. 6, Aug. 2023, doi: 10.3389/fbloc.2023.1206330.

[11] F. A. Alaba, H. A. Sulaimon, M. I. Marisa, and O. Najeem, "Smart contracts security application and challenges: A review," Cloud Comput. Data Sci., pp. 15–41, 2024, doi: 10.37256/ccds.5120243271.

[12] H. Mao et al., "A survey on cross-chain technology: Challenges, development, and prospect," IEEE Access, vol. 11, pp. 45527–45546, 2023, doi: 10.1109/ACCESS.2022.3228535.

[13] Y. Cao et al., "MAP the blockchain world: A trustless and scalable blockchain interoperability protocol for cross-chain applications," Apr. 2025, pp. 717–726, doi: 10.1145/3696410.3714867.

[14] X. Xu, I. Weber, and M. Staples, Architecture for Blockchain Applications. Cham: Springer Int. Publishing, 2019, doi: 10.1007/978-3-030-03035-3.

[15] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," Int. J. Prod. Res., vol. 57, no. 7, pp. 2117–2135, Sep. 2018, doi: 10.1080/00207543.2018.1533261.

[16] "Learn about the Polkadot Protocol | Polkadot Developer Docs," Accessed: Jul. 14, 2025. [Online]. Available: https://docs.polkadot.com/polkadot-protocol/

[17] A. P. Balcerzak et al., "Blockchain technology and smart contracts in decentralized governance systems," Adm. Sci., vol. 12, no. 3, p. 96, Aug. 2022, doi: 10.3390/admsci12030096.

[18] B. C. Ghosh et al., "Decentralized cross-network identity management for blockchain interoperation," in 2021 IEEE Int. Conf. Blockchain Cryptocurrency (ICBC), Sydney, Australia: IEEE, May 2021, pp. 1–9, doi: 10.1109/ICBC51069.2021.9461064.

[19] F. Casino, T. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," Telemat. Inform., vol. 36, Nov. 2018, doi: 10.1016/j.tele.2018.11.006.

[20] M. M. Sharif and F. Ghodoosi, "The ethics of blockchain in organizations," J. Bus. Ethics, vol. 178, no. 4, pp. 1009–1025, Jul. 2022, doi: 10.1007/s10551-022-05058-5.