Journal of Applied Informatics and Computing (JAIC)
Vol.10, No.4, August 2026, pp. 3220~3227
e-ISSN: 2548-6861

Risk Management and Sharia Compliance in Crypto Staking: A Systematic Literature Review

Maulana Asykari Muhammad [1]*, Fitroh [2]*, Rinda Hesti Kusumaningtyas [3]*
* Sistem Informasi, Fakultas Sains dan Teknologi, UIN Syarif Hidayatullah Jakarta, Indonesia
maulana.asykari22@mhs.uinjkt.ac.id [1], fitroh@uinjkt.ac.id [2], rinda.hesti@uinjkt.ac.id [3]

Article Info

Article history:

Received 2026-06-08
Revised 2026-07-24
Accepted 2026-08-07

Keyword:

Crypto Staking,
Decentralized Finance,
Enterprise Architecture,
Risk Management,
Sharia Compliance.

ABSTRACT

The adoption of Decentralized Finance (DeFi) introduces multidimensional risks that challenge institutional stability and Sharia jurisprudential standards. Existing studies often isolate technical security measures from theological compliance, creating a gap in governing digital assets under Sharia principles. This study aims to systematically review the intersection of technical risk mitigation and Sharia compliance in crypto-asset mechanisms. A Systematic Literature Review (SLR) was conducted following the PRISMA guidelines, analyzing 32 peer-reviewed articles published between 2023 and 2025. The synthesis reveals that technological and operational vulnerabilities in smart contracts induce elements of Gharar or uncertainty and Maysir or speculation, which conflict with the Maqasid al-Shariah objective of Hifzul Mal or protection of wealth. To bridge the gap between cryptographic protocols and Fiqh Muamalah or Islamic commercial law, this review identifies Enterprise Architecture (EA), specifically the TOGAF Architecture Development Method (ADM), as a structural integration framework. EA functions as a governance framework that systematically maps Sharia constraints directly into executable IT control layers. Specifically, the Business Architecture layer enforces contract validity, the Information Systems Architecture layer standardizes auditable data flows, and the Technology Architecture layer secures the consensus mechanics. The findings conclude that future research must transition from conceptual reviews to empirical implementations, particularly by designing Sharia-compliant enterprise architectures for post-Merge Ethereum staking protocols.

I. INTRODUCTION

The global financial ecosystem is currently undergoing a transformation driven by the rise of Decentralized Finance and blockchain-based asset validation mechanisms. As described by Arnone, these disruptive financial technologies offer computational efficiency and peer-to-peer economic inclusivity [1]. However, this rapid growth introduces a complex paradigm of multidimensional risks that threaten institutional and retail stability. Decentralized networks are inherently exposed to critical technical vulnerabilities, ranging from protocol-level smart contract exploits to infrastructure dependencies [2]. This problem underscores the direct significance of developing risk management frameworks, as traditional centralized security measures are inadequate to address modern, distributed cyber threats [3].

Within this decentralized landscape, the structural evolution of core blockchain protocols has expanded validation mechanisms. As outlined by Maulana et al., the transition of the Ethereum protocol to a staking-based validation model introduces specific design trade-offs and distinct trust assumptions regarding the validator set [4]. Following this architectural shift, staking operates through several separate models rather than a monolithic process [5]. Direct Proof-of-Stake or solo staking requires validators to lock native assets to secure the network, which aligns closely with the Islamic concept of *Ujrah* or wages for services. Conversely, liquid staking issues derivative tokens representing the locked assets, introducing secondary market

speculation that may trigger *Maysir* or gambling. Furthermore, delegated staking and custodial staking involve transferring asset control to intermediaries, raising concerns regarding contractual ambiguity and *Gharar* or excessive uncertainty [5], [6]. Therefore, evaluating Sharia compliance requires an understanding of these specific architectural differences.

In the domain of faith-based digital finance, navigating these technical challenges requires strict alignment with theological mandates. As elucidated by Asyiqin, a significant regulatory gap and information asymmetry exist among Muslim participants engaging with digital assets [7]. Previous Systematic Literature Reviews (SLRs) have predominantly focused either on the purely theological debate of cryptocurrency permissibility or exclusively on technical cybersecurity. To address this gap, the primary objective of this review is to investigate how Enterprise Architecture (EA), specifically the TOGAF Architecture Development Method (ADM), can be implemented to integrate technical risk mitigation with Sharia compliance. EA serves as a structural bridge, translating normative Islamic ethics into logical business rules and secure application architectures [8], [9].

To achieve an objective synthesis of this landscape, this study adopts a structured SLR using the PRISMA framework. This method is utilized for its ability to ensure transparency, qualitative data reduction, and deduplication across literature databases [10], [11]. The screening methodology is directed toward addressing three fundamental research questions: (RQ1) How does the current literature map the multidimensional risks inherent in DeFi staking ecosystems? (RQ2) What parameters are utilized to evaluate Sharia compliance within digital asset mechanisms? and (RQ3) How can EA be implemented as a structural framework to integrate technical risk mitigation with theological requirements? The remainder of this paper details the methodology (Section II), presents the thematic discussion answering each research question (Section III), and outlines the conclusions alongside prospective trajectories for future investigation (Section IV).

II. METHODS

The PRISMA methodology was structured into four primary stages: defining the research questions, conducting the literature search, assessing the quality of the selected papers, and extracting the data for synthesis.

A. Research Questions (RQ)

To systematically bridge the gap between technical blockchain operations and Islamic commercial jurisprudence (*Fiqh Muamalah*), this review formulated three core research questions. Table I describe the Research Questions.

TABLE I
RESEARCH QUESTIONS

ID	Questions
RQ1	How does the current literature map the multidimensional risks (technological, operational, financial) inherent in DeFi staking ecosystems?
RQ2	What parameters are utilized to evaluate Sharia compliance (e.g., Hifzul Mal, Gharar, Ju'alah) within digital asset mechanisms?
RQ3	How can Enterprise Architecture (specifically TOGAF ADM) be implemented as a structural framework to integrate technical risk mitigation with theological requirements?

B. Search Strategy and Data Sources

A comprehensive literature search was conducted across major academic databases, including Google Scholar and Scopus thru Publish or Perish. Table II outlines the identified literature according to the queried databases.

TABLE II.
LITERATURES AND DATABASES

Keywords	Scopus	Google Scholar	Total
"Risk Management framework" AND "Decentralized Finance" OR "Staking"	7	278	285
"Sharia compliance" AND "Cryptocurrency"	6	567	573
"Enterprise Architecture" AND "Blockchain adoption" OR "TOGAF framework"	20	723	743

C. Inclusion/Exclusion Criteria and Quality Assessment (QA)

The initial database search found 1,601 records. To ensure the integrity and academic rigor of the synthesized data, the study applied strict inclusion and exclusion criteria. Table III explained the inclusion criteria required articles to be peer-reviewed.

TABLE III
EXCLUSION AND INCLUSION CRITERIA

Exclusion	Inclusion
Published before or after (2023-2025)	Published within (2023-2025)
Written in languages other than English	Written in English
Publications without full-text accessibility	Open access publications (full-text freely available).
Non-peer-reviewed materials, book chapters, opinion pieces, whitepapers, or general review articles	Peer-reviewed academic journal articles and conference proceedings.

Furthermore, as described in Table IV, articles were evaluated against three Quality Assessment (QA) criteria. Only papers

that positively satisfied all four QA criteria were selected for the final review.

TABLE IV
QUALITY ASSESSMENT

ID	Descriptions
QA1	Is the article published in a peer-reviewed academic journal or conference proceeding?
QA2	Does the study explicitly address at least one of the core domains: DeFi risk management, Sharia compliance in cryptocurrency, or Enterprise Architecture modelling?
QA3	Does the research present a clear methodological framework, conceptual model, or verifiable empirical findings?

D. Data Extraction and Synthesis

Following the PRISMA flow which involved removing duplicates, screening titles and abstracts, and assessing full texts for eligibility [11]. the selection process narrowed the initial 1601 records down to 32 core literatures. These 32 selected papers were then extracted and mapped into a structured thematic synthesis to directly answer the defined research questions. The entire selection process is visually documented in the PRISMA Flow Diagram (Figure 1).

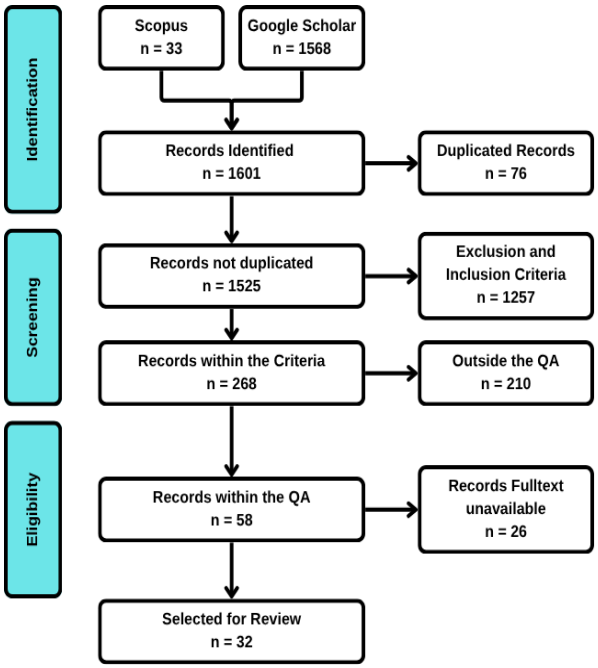

Figure 1. PRISMA Flow

III. RESULTS AND DISCUSSIONS

A. Characteristics and Thematic Clustering of the Selected Literature

To comprehend the evolution of the research landscape, an analysis of the broader publication trend was initially observed. As illustrated in Figure 2, the publication distribution across the three primary thematic domains demonstrates a consistent upward trajectory from 2021 to 2025. Specifically, research exploring Islamic Jurisprudence and Sharia Compliance experienced the sharpest increase, peaking at 322 general publications by 2025. Similarly, studies focusing on DeFi & Risk Management and Enterprise Architecture & IT Governance showed steady year-over-year growth. This trend underscores the growing academic interest in the intersection of digital assets and structural IT governance.

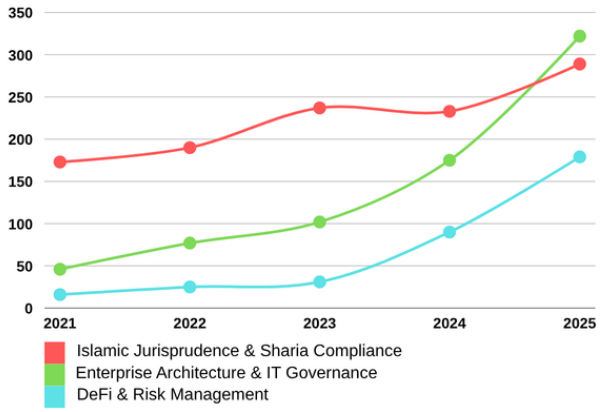

Figure 2. Trend of Literature Publications by Thematic Domain (2021-2025)

From this expanding pool of research, a final synthesis was conducted on 32 selected peer-reviewed articles following the PRISMA screening methodology. To ensure the findings capture contemporary advancements, particularly the architectural shift in Ethereum validation mechanisms. The inclusion criteria were strictly limited to the 2023–2025 timeframe. As visualized by Figure 3, the publication year distribution of the final selected literature heavily leans toward recent developments, with majority of the literatures published between 2024 and 2025.

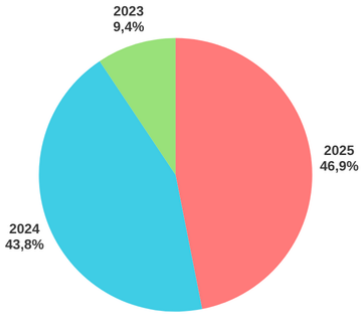

Figure 3. Literature Classification based on Years.

While the macro trends reveal a sharp increase in interdisciplinary interest, a critical analysis indicates a pronounced geographical bias within the selected literature. As illustrated in Figure 4, studies evaluating Sharia compliance and Fiqh adaptations are heavily concentrated within specific regions, predominantly Southeast Asia (specifically Indonesia and Malaysia) and the Middle East

(primarily the UAE, Bahrain, and Saudi Arabia). Conversely, foundational papers detailing technological architectures, smart contract security, and protocol-level vulnerabilities originate almost exclusively from Western research hubs or non-regional computer science repositories. This geographical concentration creates an academic asymmetry where the theological evaluation of decentralized assets is frequently conducted separately from the core engineering communities designing the protocols.

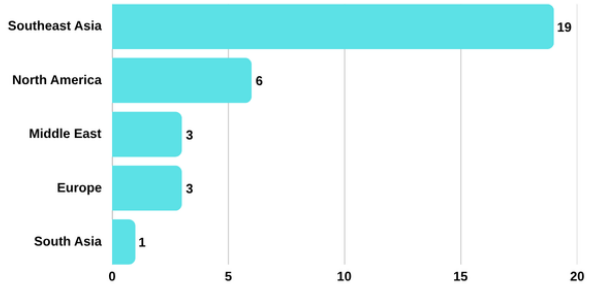

Figure 4. Geographical Distribution of the Selected Literature

Furthermore, the selected literature demonstrates a balanced integration of global technological frameworks and regional jurisprudential analyses. The distribution of the 32 articles across their respective thematic domains is detailed in Table V and visually represented in Figure 5. This categorization maps the current academic discourse into three primary pillars, providing a foundation for addressing the core research questions.

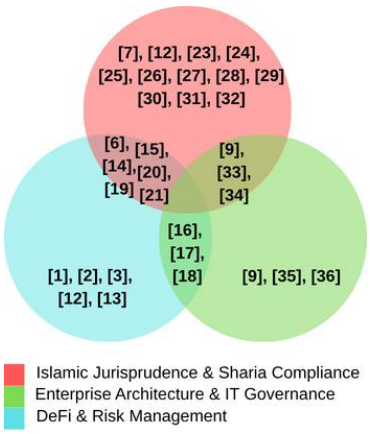

Figure 5. Literature Classification based on Domain.

TABLE V.
LITERATURES AND DATABASES

Domain	Literatures
DeFi & Risk Management	[1], [2], [3], [6], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21]
Islamic Jurisprudence & Sharia Compliance	[6], [7], [8], [14], [15], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28], [29], [30], [31], [32], [33], [34]
Enterprise Architecture & IT Governance	[8], [9], [16], [17], [18], [33], [34], [35], [36]

B. RQ1 How does the current literature map the multidimensional risks (technological, operational, financial) inherent in DeFi staking ecosystems?

Analysis of the synthesized literature reveals that the vulnerabilities in DeFi and crypto staking ecosystems manifest as a interconnected, multidimensional construct. As summarized in Table VI, current studies predominantly categorize these threats into three core dimensions: technological, operational, and financial.

TABLE VI.
MULTIDIMENSIONAL RISK MAPPING IN DEFI AND CRYPTO ECOSYSTEMS

Dimension	Identified Risks	Literatures
Technological	Smart contract vulnerabilities	[3], [6], [16], [17]
	Oracle manipulation	[16]
	51% attacks and network consensus threats	[3]
Operational	Validator and slashing risk	[18]
	Governance risk	[2], [36]
	Counterparty risk (third-party staking)	[2], [12]
Financial	Extreme price volatility	[2], [21], [29]
	Liquidity risk	[2]
	Market manipulation	[2], [24]

The literature identifies technological risks as the foundational vulnerabilities of decentralized infrastructures. Research from Alsadhan, highlights network-level threats in the cryptocurrency space, including 51% attacks, Sybil attacks, timejacking, and double-spending vulnerabilities [3]. Furthermore, as Amomo emphasize, that the reliance on autonomous, self-executing code exposes DeFi protocols to critical smart contract defects and oracle manipulations, which have historically resulted in cyber-exploits (e.g., the Poly Network and Euler Finance hacks) [16]. Agmar and Bashori note that the immutable nature of blockchain exacerbates these technological risks; because smart contracts execute automatically without human intervention, any anomaly or vulnerability in the underlying code cannot be easily reversed, frequently resulting in permanent asset loss [6].

Operational risks in the DeFi ecosystem stem primarily from the absence of centralized intermediaries and regulatory ambiguities. Research from Roy et al. point out that the global crypto-asset landscape suffers from fragmented operational guidelines, making platforms susceptible to internal vulnerabilities, inadequate governance, and compliance failures [18]. Oben and Özdamlı, alongside Amomo, confirm that this lack of coherent oversight creates regulatory blind spots that advanced threat actors actively exploit for fraud and money laundering [2], [16]. From an end-user perspective, Abdel-Wahad et al. identify that the irreversible nature of transactions, coupled with the constant risk of private key loss and complex platform usability, significantly heightens the perceived threat vulnerability among retail investors, thereby hindering safe mainstream adoption [12].

Financial risks are tied to the speculative economic behavior of cryptocurrency markets. High price volatility and market manipulation as the primary threats to capital preservation in DeFi ecosystems [2]. The lack of underlying tangible assets makes these digital instruments susceptible to sudden market crashes. From an Islamic economic perspective, this financial instability is particularly problematic. Rahmadani and Fajar, Mohammed et al. argue that the erratic price fluctuations and speculative trading practices prevalent in decentralized platforms introduce elements of Gharar or excessive uncertainty and Maysir or gambling [21], [29]. The literature concludes that without robust mitigation frameworks, the financial risks inherent in DeFi staking directly contradict the fundamental Maqasid Shariah objective of Hifzul Mal (the protection of wealth).

C. RQ2 What parameters are utilized to evaluate Sharia compliance (e.g., Hifzul Mal, Gharar, Ju'alah) within digital asset mechanisms?

The evaluation of Sharia compliance within decentralized financial mechanisms relies on a set of established jurisprudential parameters. These parameters function as analytical filters to determine whether a digital asset or its underlying protocol is sharia compliant. Table VII categorizes those evaluative parameters into four primary constructs.

TABLE VII.
SHARIA COMPLIANCE PARAMETERS IN DIGITAL ASSET EVALUATION

Category	Identified Parameters	Literatures
Maqasid al-Shariah	Hifz al-Din (Protection of Faith)	[14], [15], [22]
	Hifz al-Nafs (Protection of Life)	[14]
	Hifz al-'Aql (Protection of Intellect)	[15]
	Hifz al-Mal (Protection of Wealth)	[7], [22], [27]
Prohibitive Elements (Harm Avoidance)	Gharar	[6], [24], [25], [29], [30]
	Maysir	[24], [29]
	Riba	[6], [23], [30]
Ontological Validity & Jurisdictional Fatwas	Mal Mutaqawwim & Sil'ah	[27], [28], [32]
	Strict prohibition approach	[25], [32]
	Adaptive regulatory sandbox approach	[28], [31]
Contractual Mechanisms & Instrument Comparison	Ju'alah & Ujrah (Validation rewards justification)	[21], [23], [30], [32]
	Integration with IT Governance/Smart Contracts	[8], [19], [26], [34]
	Comparison with digital Sukuk and Sharia banking	[20], [26], [33]

Current literature emphasizes that evaluating DeFi requires a comprehensive application of Maqasid al-Shariah, moving beyond the mere protection of wealth or *Hifzul Mal*. Asyiqin and Azizov et al. state that regulatory frameworks must ensure the technology serves the public interest without inflicting harm [7], [22]. Amir et al. incorporate *Hifz al-Nafs* and *Hifz al-Din*, arguing that financial protocols must not disrupt socioeconomic stability or violate faith-based ethical boundaries [14]. Furthermore, Yaqin et al. introduce the dimension of *Hifz al-'Aql*, highlighting that users must possess adequate digital literacy to make rational decisions rather than placing blind trust in automated algorithms [15].

The synthesis reveals a systematic correlation between specific technical vulnerabilities and the presence of Gharar and Maysir. The relationship is structural rather than merely conceptual. Agmar and Bashori, alongside Rani and Afandi, explain that smart contract vulnerabilities and unverified code create algorithmic Gharar [6], [30]. When code execution is opaque and susceptible to exploits, the contract lacks the clarity mandated by Islamic law. Regarding Maysir, Khaira et al. and Rahmadani and Fajar observe that the absence of underlying utility, particularly in liquid staking derivatives, transforms the ecosystem into a highly speculative environment [24], [29]. Findings from Junaidi et al. add that specific yield-generating models within decentralized exchanges often mimic Riba by guaranteeing fixed percentage returns without genuine risk-sharing [23].

The ontological classification of crypto assets as Mal Mutaqawwim or Sil'ah has led to significant divergence among global fatwa institutions. Munandar and Fahrurrozi and Wahid et al. highlight that major Indonesian Islamic organizations, including MUI, NU, and Muhammadiyah, adopt a strict prohibition approach [25], [32]. This perspective is influenced by the high volatility of the assets, the prevalence of fraud, and the lack of state monetary sovereignty. In contrast, Sidiq and Muliana and Mokodompis et al. document an adaptive approach in the Middle East, particularly in the UAE and Bahrain [28], [31]. These jurisdictions establish specific Sharia supervisory boards and regulatory sandboxes, allowing certain digital assets to be certified as compliant provided they pass technical and financial audits [27].

Within the staking mechanism, the block rewards earned by validators can theoretically be justified under the contracts of Ju'alah or Ujrah, as they represent compensation for securing the network [34]. However, Mohammed et al. caution that this validity is conditional upon the isolation of the protocol from illicit activities [21]. To contextualize this, the literature frequently compares crypto staking with established Islamic innovations, such as digital Sukuk or Sharia-compliant banking smart contracts [20], [26], [33]. Unlike digital Sukuk, which possesses clear underlying physical assets and centralized Sharia oversight, current decentralized staking lacks standardized institutional backing. As noted by James and Aisah et al., structured digital Islamic instruments utilize integrated IT governance and automated compliance auditing to ensure continuous adherence to ethical standards and structural features that are presently absent in native crypto staking protocols [8], [19].

D. RQ3 How can Enterprise Architecture (specifically TOGAF ADM) be implemented as a structural framework

to integrate technical risk mitigation with theological requirements?

Bridging the technical vulnerabilities of blockchain networks with the strict boundaries of Islamic jurisprudence requires a methodical structural blueprint. Out of the 32 reviewed articles, 11 studies specifically emphasize the necessity of IT governance, standardized architectures, and regulatory frameworks to mitigate decentralized risks. As outlined in Table VIII, the literature proposes various alternative approaches, such as the Governance, Risk, and Compliance (GRC) framework, the Crypto-asset Operational Risk Management (CORM) model, and the Cybersecurity and Regulatory Convergence Model (CRCM). To synthesize these fragmented models into a cohesive enterprise lifecycle, this study highlights the TOGAF Architecture Development Method (ADM) as the overarching integration framework.

TABLE VIII.
ENTERPRISE ARCHITECTURE IMPLEMENTATION FOR CRYPTO-ASSET GOVERNANCE

TOGAF ADM	Identified Strategies & Alternative Frameworks	Literatures
Architecture Vision & Business Architecture	Integration of GRC (Governance, Risk, Compliance) policies.	[8]
	Alignment of business logic with Fiqh Muamalah principles.	[28], [34]
Information Systems Architecture	Standardizing cross-chain interoperability protocols.	[35]
	Designing automated Sharia-compliant smart contract architectures.	[9], [26]
Technology Architecture & Requirement Management	Deployment of tamper-proof network infrastructure.	[17], [33]
	Application of alternative risk models (CORM and CRCM) for continuous vulnerability monitoring.	[16], [18], [36]

The initial phases of the TOGAF ADM require organizations to define their operational baseline before any technological development occurs. In the context of DeFi, this phase is utilized to embed theological and regulatory requirements directly into the business logic. As explained by Wardani, the implementation of blockchain-based systems in Islamic finance must begin with a clear alignment between institutional objectives and classical jurisprudential principles [34]. Supporting this structural approach, James asserts that integrating Governance, Risk, and Compliance (GRC) policies during the foundational architecture design ensures that compliance auditing becomes a core component of the business process rather than a secondary addition [8].

Moving into the data and application layers, the framework translates the predefined business rules into functional software models. As elucidated by Uppaluri, integrating decentralized finance into corporate structures requires a systematic approach to smart contract implementation, automated audit trails, and decentralized liquidity mechanisms [9]. To prevent isolated and fragmented systems, Anthony Jnr highlights the necessity of standardized application architectures that support cross-chain interoperability [35]. By mapping Sharia compliance rules onto these standardized digital protocols, developers can automate contract execution while ensuring that the data layer remains transparent and immutable.

The final implementation tier focuses on the physical infrastructure required to secure the ecosystem. As elaborated by Osilaja et al. and Fitria and Sari, establishing a tamper-proof technological architecture is critical for mitigating cyber threats and supporting the Sharia requirement for transaction transparency [17], [33]. Furthermore, managing the continuous evolution of these systems is a crucial aspect of EA requirement management. The literature provides several relevant alternative frameworks for this monitoring phase. As proposed by Roy et al. the CORM framework to systematically monitor network vulnerabilities, while Amomo introduces the CRCM model to align cybersecurity defenses with federal oversight [16], [18]. Finally, Simatupang and Indrayani stress that technological deployment must run parallel with institutional readiness, ensuring that the entire enterprise architecture remains legally and operationally viable throughout its lifecycle [36].

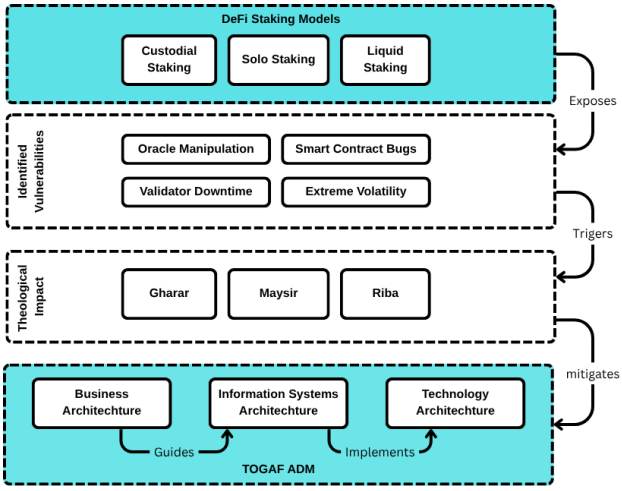

Figure 6. Conceptual Framework of Sharia-Compliant Enterprise Governance for Crypto Staking.

To summarize the causal relationship between blockchain vulnerabilities, their theological implications, and the proposed structural solutions, this study constructs a conceptual framework. As illustrated in Figure 6, the framework maps how operational dynamics in staking models trigger elements of Gharar and Maysir, which affect the foundational pillars of Maqasid al-Shariah. Consequently, the framework applies the TOGAF ADM phases as a mitigation blueprint to integrate jurisprudential compliance into the business, information, and technology architectures of decentralized applications.

IV. CONCLUSION

This systematic literature review synthesizes 32 peer-reviewed articles published between 2023 and 2025 to examine the intersection of multidimensional risk management and Sharia compliance within decentralized financial ecosystems, specifically crypto staking mechanisms. The findings demonstrate that DeFi staking ecosystems are exposed to interconnected technological, operational, and financial vulnerabilities. Smart contract defects, oracle dependencies, regulatory fragmentation, and high asset volatility collectively threaten capital preservation. From a jurisprudential standpoint, these vulnerabilities introduce elements of Gharar and Maysir, which conflict with the Maqasid al-Shariah objective of Hifzul Mal. However, the analysis also reveals that a comprehensive Sharia evaluation extends beyond wealth protection alone. The reviewed literature identifies Hifz al-Din, Hifz al-Nafs, and Hifz al-'Aql as additional evaluative dimensions, indicating that DeFi protocols must also preserve faith-based ethical boundaries, socioeconomic stability, and user capacity for informed rational decision-making in automated environments. The review further reveals that the Sharia compliance status of crypto staking is not uniform across mechanisms. The literature distinguishes between direct Proof-of-Stake validation, liquid staking, and delegated or custodial staking, each carrying different risk profiles and jurisprudential implications. Validation rewards from direct staking can be justified under the contracts of Ju'alah or Ujrah, as they constitute compensation for network security services. However, liquid staking derivatives introduce secondary market speculation, while delegated staking raises concerns over contractual ambiguity due to intermediary involvement. These distinctions indicate that a blanket Sharia ruling on crypto staking is insufficient; compliance assessments must account for the specific architectural model employed.

Additionally, the synthesis documents a notable divergence among global fatwa institutions. Major Indonesian Islamic organizations such as MUI, NU, and Muhammadiyah adopt a prohibition-oriented stance driven by concerns over volatility, fraud, and monetary sovereignty. In contrast, jurisdictions in the UAE and Bahrain have adopted an adaptive regulatory sandbox approach, permitting certain digital assets to be certified as compliant following technical and financial audits. This jurisdictional variation underscores that the Sharia compliance of crypto staking remains a contested and context-dependent matter rather than a settled consensus.

To bridge the gap between technical security protocols and normative jurisprudential requirements, this review identifies Enterprise Architecture, specifically the TOGAF Architecture Development Method, as a practical integration framework. By utilizing a structured lifecycle approach, organizations can map Fiqh Muamalah requirements into business rules, application data parameters, and infrastructure tiers. The reviewed literature also identifies alternative models, including the GRC framework, CORM, and CRCM, which can complement the TOGAF ADM in continuous vulnerability monitoring and regulatory alignment. The findings carry implications for multiple stakeholders. Regulators may benefit from the proposed architectural approach to design audit mechanisms that accommodate both technical and theological compliance. Sharia advisory boards can use the identified parameters as structured evaluation criteria for digital asset certification. Blockchain protocol developers may consider embedding compliance checkpoints within smart contract design. Muslim investors are advised to distinguish between staking models, as the Sharia implications vary depending on the degree of intermediation, speculative exposure, and contractual transparency involved.

This study has several limitations. The review scope is restricted to English-language, peer-reviewed publications from 2023 to 2025, which may exclude relevant studies published in Arabic or Malay, as well as earlier foundational works. The narrow timeframe, while intentional to capture post-Merge Ethereum developments, increases the risk of publication bias on a rapidly evolving topic. The geographic concentration of the reviewed Islamic finance literature in Southeast Asia and the Middle East may limit the generalizability of the jurisprudential findings. Furthermore, the conclusion regarding TOGAF ADM as an integration framework is derived from conceptual synthesis rather than empirical validation on live staking protocols. Consequently, future research should transition from conceptual evaluations to empirical implementations. Specific areas requiring validation include the design of Sharia-compliant validator governance models, smart contract audit frameworks incorporating Fiqh parameters, and staking architectures based on the Wakalah contract structure. An immediate research direction is the development and testing of a comprehensive enterprise blueprint that applies the TOGAF ADM to post-Merge Ethereum staking protocols, enabling verifiable compliance enforcement within operational decentralized networks.

REFERENCES

[1] G. Arnone, "FinTech and Cryptocurrency: An Extensive Review of Developments, Advantages, Merits, Challenges, and Future Trajectories in the Financial Sector," *FMDB Transactions on Sustainable Technoprise Letters*, vol. 2, no. 4, pp. 212–226, 2024, doi: 10.69888/ftstpl.2024.000336.

[2] R. Oben and F. Özdamlı, "Decentralized Finance (DeFi): Benefits, Risks, and Risk Mitigation Strategies," *Istanbul Business Research*, vol. 0, no. 0, pp. 0–0, 2024, doi: 10.26650/ibr.2024.53.1426335.

[3] A. A. Alsadhan, "Analyzing Cryptocurrency Security Risks: A Comprehensive Survey of Saudi Arabian Perspectives," *IET Inf. Secur.*, vol. 2025, no. 1, 2025, doi: 10.1049/ise2/5100339.

[4] E. Maulana, C. Avian, and D. D. Putra, "Blockchain Technology As A Digital Economic Enabler: A Comparative Analysis Of Decentralized Asset And Cryptocurrency Protocols (Bitcoin Vs. Ethereum)," *Proceeding of SINERGY*, vol. 1, no. 1, pp. 962–975, 2026.

[5] S. L. Furnari, "Staking Services: Taxonomy, Risks and Regulation," *Risks and Regulation (September 30, 2025)*, 2025.

[6] K. N. A. Agmar and Y. A. Bashori, "Analisis Kepatuhan Syariah (Shariah Compliance) terhadap Penggunaan Smart Contract,"

Jurnal Antologi Hukum, vol. 5, no. 1, pp. 120–134, 2025, doi: 10.21154/antologihukum.v5i1.4482.

[7] I. Z. Asyiqin, "Islamic Economic Law in the Digital Age: Navigating Global Challenges and Legal Adaptations," *Media Iuris*, vol. 8, no. 1, pp. 95–112, 2025, doi: 10.20473/mi.v8i1.61800.

[8] Ugoaghalam Uche James, "Blockchain Based Compliance Auditing For GRC Integration in Hybrid Cloud IT Governance Frameworks," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 10, no. 5, pp. 1100–1124, 2024, doi: 10.32628/cseit24113368.

[9] Prudhvi Uppaluri, "Integration of Blockchain-Based Decentralized Finance into Financial Planning and Analysis: A Framework for Corporate Finance Innovation," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 10, no. 6, pp. 2051–2060, 2024, doi: 10.32628/cseit2410612396.

[10] Z. S. Nugraha, M. A. Muhammad, and B. Waspodo, "The Use of Artificial Intelligence in Enhancing Customer Relationship Management (CRM): A Systematic Literature Review," *Jurnal Sisfokom (Sistem Informasi dan Komputer)*, vol. 14, no. 4, pp. 467–474, 2025, doi: 10.32736/sisfokom.v14i4.2454.

[11] M. S. Tsauri, "Human Vulnerabilities to Social Engineering Attacks: A Systematic Literature Review for Building a Human Firewall," *Journal of Applied Informatics and Computing*, vol. 9, no. 4, pp. 1127–1136, 2025, doi: 10.30871/jaic.v9i4.9585.

[12] R. Abdel-Wahad, A. Abdallah, C. El-Qutob, F. Yousef Omeish, and M. Yousef Abuhashesh, "Examining Blockchain Adoption: Insights From the Protection Motivation Theory," *Interdisciplinary Journal of Information, Knowledge, and Management*, vol. 20, p. 036, 2025, doi: 10.28945/5667.

[13] O. M. Olawoyin, "Blockchain Technology in Risk Management: Strengthening Cybersecurity and Financial Integrity," *International Journal of Research Publication and Reviews*, vol. 5, no. 10, pp. 2336–2348, 2024, doi: 10.55248/gengpi.5.1024.2829.

[14] M. F. Amir, S. Kadir, and S. Sumarlin, "Decentralized Finance and Its Maslahah: Shaping the Future of Financial Services in Indonesia," *Share: Jurnal Ekonomi dan Keuangan Islam*, vol. 13, no. 2, pp. 739–769, 2024, doi: 10.22373/share.v13i2.22857.

[15] Moh Ainul Yaqin, Siti Kamiliyah Adriani, and Nur Kholis, "Algorithmic Trust and Digital Gharar: A Maqāṣidiyyah Framework for Evaluating Blockchain in Islamic Trade Systems," *International Journal of Economics, Management and Accounting*, vol. 3, no. 1, pp. 79–90, 2025, doi: 10.61132/ijema.v3i1.1072.

[16] C. G. Amomo, "A cybersecurity and regulatory framework for mitigating fraud and illicit activity in cryptocurrency ecosystems," 2024, *researchgate.net*. doi: 10.30574/wjaets.2024.12.2.0294.

[17] Adeola Mercy Osilaja, Azeezat Raheem, and Enuma Edmund, "Enhancing software security with blockchain integration for decentralized and tamper-proof application architectures," *World Journal of Advanced Research and Reviews*, vol. 24, no. 3, pp. 2750–2767, 2024, doi: 10.30574/wjarr.2024.24.3.3977.

[18] D. Roy, A. Dubey, and D. Tiwary, "Conceptualizing an Institutional Framework to Mitigate Crypto-Assets' Operational Risk," 2024, *mdpi.com*. doi: 10.3390/jrfm17120550.

[19] N. Aisah, S. Z. J. Putri, and M. R. Hafizi, "Blockchain Technology Innovation As an Optimization of Transaction Security in Islamic Financial Institutions," *Journal of Central Banking Law and Institutions*, vol. 4, no. 1, pp. 23–48, 2025, doi: 10.21098/jcli.v4i1.265.

[20] M. Farhan, I. Imsar, and B. Dharma, "Analysis of Opportunities and Challenges of Blockchain Technology in the Islamic Banking Industry (Case Study on the Use of Smart Contracts)," *Jurnal Akuntansi, Keuangan, dan Manajemen*, vol. 5, no. 4, pp. 481–489, 2024, doi: 10.35912/jakman.v5i4.3488.

[21] M. O. Mohammed, M. C. El Amri, and A. M. Bakr, "Guiding Fiqh Analysis of Crypto Assets: A Proposed Framework," *Ahkam: Jurnal Ilmu Syariah*, vol. 24, no. 2, pp. 276–295, 2024, doi: 10.15408/ajis.v24i2.37346.

[22] E. Azizov, A. Azizov, A. Azizli, and A. A. Babayev, "A Maqasid al-Shariah Framework for Fintech and Digital Asset Regulation in Muslim Jurisdictions," *Journal of Islamic Law and Legal Studies*, vol. 2, no. 2, pp. 96–113, 2025, doi: 10.70063/jills.v2i2.119.

[23] M. A. Junaidi, R. Dewantara, and N. Chanifah, "Halal Certification of Cryptocurrency: A Framework for Strengthening Trust in Shariah-Compliant Digital Finance," *International Journal of Social Science and Religion (IJSSR)*, pp. 321–332, 2025, doi: 10.53639/ijssr.v6i3.382.

[24] H. Qiestha Khaira, A. Irawan, and M. Tamam, "Cryptocurrency in Islamic Economics: A Critical Analysis of Dogecoin's Compliance with Sharia Principles," *Al-Risalah Jurnal Ilmu Syariah dan Hukum*, vol. 25, no. 1, pp. 133–152, 2025, doi: 10.24252/al-risalah.vi.55707.

[25] M. Arif and A. M. Naim, "Controversies of cryptocurrency: Fatwa analysis from Muhammadiyah and NU," *Journal of Islamic Law on Digital Economy and Business*, vol. 1, no. 1, pp. 18–35, 2023, doi: 10.20885/jildeb.vol1.iss1.art2.

[26] H. Hermawan Adinugraha, S. M. Marier, R. Andrean, and H. H. Adinugraha, "An Islamic legal review of smart contract regulation in digital economic transactions: A comparative study between Indonesia and China," *Journal of Islamic Law on Digital Economy and Business*, vol. 1, no. 1, pp. 1–17, 2025, [Online]. Available: http://creativecommons.org/licences/by-sa/4.0/

[27] Z. Ahmad, M. N. Mokal, I. al- Amatullah, and M. N. A. Mafaz, "An Evaluation of Bitcoin From Shariah Perspective," *Review of Applied Management and Social Sciences*, vol. 6, no. 2, pp. 459–480, 2023, doi: 10.47067/ramss.v6i2.343.

[28] I. I. Mokodompis, R. P. Pedju, and A. A. Muhammad, "Integrating Islamic Law and Modern Regulation: Cryptocurrency as a Sharia-Compliant Digital Asset in Indonesia," *Antmind Review: Journal of Sharia and Legal Ethics*, vol. 1, no. 2, pp. 83–93, 2024, doi: 10.63077/r27rd104.

[29] N. M. P. Rahmadani and F. Fajar, "Aligning Cryptocurrencies With Islamic Law: Challenges, Ethical Concerns, and Regulatory Solutions," *Istinbath*, vol. 23, no. 2, pp. 366–383, 2024, doi: 10.20414/ijhi.v23i2.887.

[30] M. A. H. C. Rani and M. S. A. Afandi, "Cryptocurrency and Shariah: Analyzing the Implications of Islamic Jurisprudence on Bitcoin and its Ethical Framework," *International Journal of Research and Innovation in Social Science*, vol. 9, no. 10, pp. 1420–1431, 2025, doi: 10.47772/ijriss.2025.910000122.

[31] M. Yusuf Sidiq and S. Muliana, "Analysis of the Sharia-based crypto-asset regulatory framework in the United Arab Emirates (UAE) and Bahrain," *Journal of Islamic Law on Digital Economy and Business*, vol. 2025, no. 1, pp. 36–52, 2025, doi: 10.20885/jildeb.vol1.iss1.art3.

[32] N. A Wahid, D. Amanatillah, and C. D. Fitri, "From Fiqh to Finance: Assessing Bitcoin Status in Indonesian Monetary System," *Share: Jurnal Ekonomi dan Keuangan Islam*, vol. 12, no. 2, pp. 308–333, 2023, doi: 10.22373/share.v12i2.17762.

[33] Fitria and Dian Rahmita Sari, "Analysis of the Implementation of Blockchain Technology in Sharia Banking Transaction Transparency," *Morfai Journal*, vol. 5, no. 1, pp. 234–242, 2025, doi: 10.54443/morfai.v5i1.2564.

[34] R. E. K. Wardani, "Implementation of Blockchain-Based Smart Contracts in Islamic Finance," *Dalwa Islamic Economic Studies: Jurnal Ekonomi Syariah*, vol. 4, no. 2, pp. 130–152, 2025, doi: 10.38073/dies.v4i2.3760.

[35] B. Anthony Jnr, "Enhancing blockchain interoperability and intraoperability capabilities in collaborative enterprise-a standardized architecture perspective," *Enterp. Inf. Syst.*, vol. 18, no. 3, 2024, doi: 10.1080/17517575.2023.2296647.

[36] J. M. Simatupang and E. Indrayani, "Blockchain Adoption Readiness: Expert Perspectives on Policy, Implementation, and Governance in Indonesia," *Jurnal Bina Praja*, vol. 17, no. 3, 2025, doi: 10.21787/jbp.17.2025-2681.