Indonesian Interdisciplinary Journal of Sharia Economics (IIJSE)
e-ISSN: 2621-606X
Vol. 9. No. 2 (2026)
Page: 16283-16301

AN ANALYSIS OF PERCEIVED CREDIBILITY AND SHARIA COMPLIANCE IN DIGITAL FINANCIAL APPLICATIONS

Muhamad Farid Al Fathdry [1]
Universitas Tazkia, Bogor, Indonesia
muhamadfaridalfathdry@gmail.com

Ries Wulandari[2]
Universitas Tazkia, Bogor, Indonesia
rieswulandari@tazkia.ac.id

Abstract

The digital transformation in the financial sector presents complex challenges regarding platform credibility and sharia compliance, particularly for service providers operating in a two-sided market ecosystem. This study aims to deconstruct provider perceptions regarding application credibility defined through cost transparency and security as well as sharia compliance, and how these factors influence adoption and retention decisions. Using the Analytic Network Process (ANP) method, this research synthesizes assessments from five experts (academics and practitioners) to map problem and solution priorities within the Indonesian Islamic digital finance ecosystem. The findings indicate that internal problems, specifically system security aspects (weight 0.466), are the primary priority, preceding cost transparency and sharia compliance. Conversely, the most effective solutions are external, where the publication of verified track records through independent audits and certifications (weight 0.652) is considered the most critical determinant for user retention sustainability. These results imply that a sharia label alone is insufficient; platform providers must invest in external validation mechanisms to overcome information asymmetry and build long-term trust.

Keywords: Digital Financial Applications, Analytic Network Process (ANP), Sharia Compliance, Platform Credibility, User Retention

INTRODUCTION

The rapid development of digital financial applications has fundamentally transformed the global financial ecosystem, moving from a traditional, institution-centric intermediation model to a decentralized, platform-based digital ecosystem. Digital financial platforms such as e-wallets, peer-to-peer financing, and payment aggregators now act as multi-sided marketplaces, connecting users, service providers, and regulators through algorithm-based infrastructure (Banna et al., 2021; Gomber et al., 2018). In Indonesia, the adoption of digital financial services has shown very significant growth, driven by high mobile device penetration, regulatory policy support, and the strategic role of micro, small, and medium enterprises (MSMEs) in the national digital economy (AFTECH, 2023).

While offering efficiency, scalability, and expanded financial inclusion, digital finance also presents new challenges related to risk governance, information asymmetry, and institutional legitimacy. These challenges are particularly pronounced in developing countries, where regulatory capacity, digital literacy, and trust infrastructure are still under development (Banna et al., 2021; Ozili, 2023). In the context of Islamic finance, this complexity is even greater because digital platforms are not only required to comply with formal regulations, but must also comply with the ethical and operational principles of Islamic law, such as the prohibition of usury, gharar, and unethical speculative practices (Oseni et al., 2019; Sudarwanto et al., 2024; Unal & Aysan, 2022).

The main challenge to the sustainability of digital financial platforms lies in the fragility of trust between platform providers and service partners, such as merchants or MSMEs. As two- or multi-sided marketplaces, platform sustainability depends heavily on the active participation and retention of supply-side partners (Parker et al., 2017). Partners' decisions to adopt and remain with a platform are not solely driven by economic incentives, but also by perceptions of the platform's credibility, which includes fee transparency, system security, governance fairness, and operational reliability (Ferilli et al., 2024). When fee structures are not transparent or safety claims are difficult to verify, a perception gap arises that increases uncertainty and undermines trust.

In the Islamic digital financial ecosystem, the relationship between trust and credibility is mediated by perceptions of Sharia compliance. Sharia compliance is not simply a formal legal status established through fatwas or supervision by the Sharia Supervisory Board, but rather a multidimensional, perceptual construct. This construct is shaped by the clarity of contracts (such as murabahah, ijarah, and wakalah), the effectiveness of Sharia governance, and the level of confidence in the automated decision-making systems used within digital platforms (Rabbani et al., 2020; Usman et al., 2021). Several recent studies have shown that perceptions of Sharia compliance significantly influence the adoption of Sharia-compliant digital financial services by MSMEs, particularly through the formation of trust and long-term commitment. However, heterogeneity in understanding Sharia contracts among industry players often leads to inconsistent assessments, raising doubts about the authenticity of Sharia practices on digital platforms.

Despite the continued growth of research on digital finance and Islamic fintech, several significant research gaps remain. First, most previous studies have focused on the end-user perspective (user-centric), while the dynamics of service providers (provider-centric), the backbone of the platform ecosystem, have received relatively little attention. Second, Sharia compliance is generally treated as a dichotomous variable (compliant or non-

compliant), whereas in practice, Sharia compliance exists along a spectrum of perceptions influenced by the quality of information disclosure and governance. Third, the dominant methodological approaches are cross-sectional and regression-based, thus failing to capture the interrelationships between factors and the complexity of trade-offs in shaping perceptions of credibility and compliance.

This study aims to fill this gap using the Analytic Network Process (ANP) approach. Specifically, this study aims to (1) identify and prioritize key issues that shape perceptions of credibility and sharia compliance among service provider partners; (2) analyze the influence of differences in understanding sharia contracts on the formation of trust; and (3) formulate the most effective solution strategies to increase long-term partner retention. The urgency of this research lies in the urgent need to formulate governance standards that can bridge technological innovation with the certainty of sharia compliance, thereby supporting the sustainability and legitimacy of the sharia digital financial ecosystem in developing countries, particularly Indonesia.

REVIEW OF LITERATURE

Digital Finance

Digital finance refers to all financial activities and services designed, delivered, and utilized through digital infrastructure and interfaces, primarily mobile devices, internet networks, and cloud computing. These services include payments and fund transfers, savings and investments, financing, and protection or insurance based on digital platforms. Digital financial operations rely on process automation, data integration, and the use of algorithms to improve accessibility, service speed, transaction accuracy, and cost efficiency, while expanding service reach to segments of society and businesses previously underserved by the formal financial system (Ozili, 2018).

In practice, the digital financial ecosystem encompasses various service models and channels, such as e-wallets, integrated QR code-based payment systems, mobile banking, neobanks, peer-to-peer (P2P) lending, robo-advisory services, and the use of application programming interfaces (APIs) that connect partners or merchants with platform providers. The digital nature of these services allows for lower transaction costs, reduced geographic barriers, and real-time monitoring of user behavior and business partner performance (AFTECH, 2023).

However, digital transformation in the financial sector also presents new challenges that are more complex than those faced by conventional services. These challenges include the need for data governance and privacy protection, cybersecurity, cost transparency, and compliance with dynamic and increasingly stringent regulations. Without adequate governance, the efficiency advantages of digital finance have the potential to create systemic risks and undermine stakeholder trust (Banna et al., 2021).

Fintech Regulation in Indonesia

In Indonesia, fintech is regulated under a multi-authority regulatory framework involving the Financial Services Authority (OJK), Bank Indonesia (BI), and the Ministry of Communication and Information Technology (Kominfo). The OJK serves as the primary regulator for fintech companies operating in the non-payment system financial services sector, particularly technology-based funding and financing services. This regulatory framework begins with Regulation (POJK) Number 13/POJK.02/2018 concerning Digital

Financial Innovation in the Financial Services Sector, which serves as an umbrella regulation and introduces principles of governance, risk management, consumer protection, and a regulatory sandbox mechanism for testing fintech business models.

More specific regulations regarding digital financing are regulated through POJK Number 77/POJK.01/2016 concerning Information Technology-Based Lending and Borrowing Services and reinforced by POJK Number 10/POJK.05/2022 concerning Information Technology-Based Joint Funding Services, which emphasizes information transparency, risk mitigation, organizer accountability, and strengthening consumer protection, including for Sharia-based fintechs that are required to meet Sharia compliance requirements and supervision by the Sharia Supervisory Board.

On the other hand, Bank Indonesia has the authority to regulate and supervise fintech related to payment systems and monetary stability. BI regulations cover e-money, digital wallets, QRIS, payment gateways, and digital payment system infrastructure through Bank Indonesia Regulation (PBI) No. 18 of 2016 concerning the Implementation of Payment Transaction Processing and PBI No. 19/12/PBI/2017 concerning the Implementation of Financial Technology.

Through this policy, BI emphasizes the principles of interoperability, security, efficiency, and inclusivity, and implements a regulatory sandbox mechanism to test payment system innovations before widespread implementation. For partners and merchants, compliance with BI regulations ensures that transactions are conducted through a secure, reliable, and nationally integrated system, thereby reducing operational risk and increasing trust in fintech platforms.

The information technology and data protection aspects of the fintech ecosystem are regulated by the Ministry of Communication and Information Technology, primarily through Law (UU) Number 27 of 2022 concerning Personal Data Protection and Government Regulation (PP) Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. These regulations require fintech operators to ensure the security of electronic systems, responsible management of personal data, and protection of data subjects' rights. In practice, compliance with Kominfo regulations is the foundation of digital trust, as failure to protect data and systems can directly impact a platform's reputation and business sustainability.

Overall, the regulations of the Financial Services Authority (OJK), Bank Indonesia (BI), and the Ministry of Communication and Information Technology (Kominfo) form the baseline compliance that all fintech operators in Indonesia must meet. Compliance with these regulatory obligations is not only legal but also serves as a signal of credibility for partners and users. The transparency of financing costs and governance regulated by the OJK, the security and reliability of transactions guaranteed by Bank Indonesia, and the protection of data and electronic systems supervised by the Ministry of Communication and Information Technology collectively shape the perception of trust in fintech platforms. Therefore, fintech operators are required to implement a compliance-by-design and continuous compliance approach, integrating regulatory aspects, risk management, and Sharia compliance from the product design stage through operations, thereby demonstrating verifiable accountability and trust from all stakeholders.

RESEARCH METHOD

This study employs a mixed-methods approach, utilizing the Analytic Network Process (ANP) as the primary analytical instrument to structure the complexities of credibility perception and Sharia compliance in digital financial applications. The research was conducted utilizing secondary data from authoritative literature and primary data acquired through expert interviews. The initiation phase began with the construction of an initial model based on a literature review, which was subsequently validated through in-depth interviews with experts to comprehensively map problem and solution elements prior to their conversion into the ANP framework.

Data collection involved selected respondents classified into practitioner and academic categories to ensure preference accuracy from diverse perspectives. The instrument employed was a pairwise comparison questionnaire utilizing a ratio scale of 1 to 9, designed to measure respondent assessment weights regarding internal and external problem clusters as well as proposed solutions. Unlike linear hierarchical structures, this model accommodates interdependence and feedback relationships among elements, with data collection conducted separately for each respondent to maintain the purity of each expert's geometric preferences.

Table 1. List of Respondents

Respondents		
No.	**Name**	**Description**
1.	Thuba Jazil, M.Sc.(Fin).	Academician
2.	Aminah Nuriyah, S.E.I., M.E.	Academician
3.	Desi Rachmawati, S.Ak.	Practitioner
4.	Fardhia Dini	Practitioner
5.	Linna Dwi Laelasari	Practitioner

Table 2. Scale in ANP

Definition	Intensity of Importance	Explanation
Extreme Importance	9	The evidence favoring one activity over another is of the highest possible order of affirmation.
For compromizes between the above values	8	
Very Strong and Demonstrated	7	An activity is favored very strongly over another, it’s dominance demonstrated in practice
For compromizes between the above values	6	
Strong Importance	5	Experience and judgement strongly favor one activity over another
For compromizes between the above values	4	
Moderate Importance	3	Experience and judgement strongly favor one activity over another.

For compromizes between the above values	2	
Equal Importance	1	Two activity contribute equally to the objective.

Source: (Saaty & Vargas, 2006b)

Data processing was performed using Super Decisions software to synthesize the complex network structure. The aggregation of individual assessments into a group consensus was executed through the calculation of the Geometric Mean, while the level of convergence among respondents was tested using Kendall's Coefficient of Concordance (W). The resulting global priority values served as the basis for strategic formulation, wherein the validity of the results was supported by Rater Agreement measurements to ensure a high degree of stability and objectivity in the generated decisions.

Rater Agreement is defined as a statistical measure that reflects the level of convergence or agreement among respondents (R1...Rn) on the elements in a cluster (Saaty & Vargas, 2006a). The instrument used to measure this level of agreement is Kendall's Coefficient of Concordance (W), with a value range of $0 < W < 1$. According to Ascarya and Sakti (2022), a value of $W = 1$ indicates perfect agreement among respondents. Conversely, a value of W close to 0 indicates high divergence or disagreement in assessment.

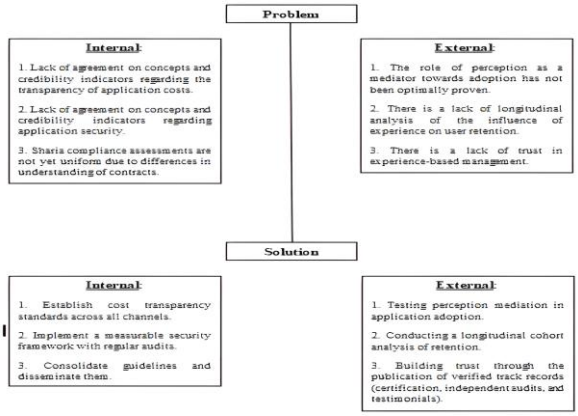
RESULTS AND DISCUSSION

Problem Decomposition

The problem decomposition stage was carried out to identify, analyze, and measure the complexity of the problem into several problem clusters in order to analyze the appropriate solutions to overcome the problems. The problem decomposition process in this study was carried out through a literature review based on previous research as well as national and international literature reviews, and through in-depth interviews to comprehensively map the elements of the problem.

In-depth interviews were conducted with expert respondents consisting of practitioners and academics who have expertise related to the digital financial application ecosystem. There were five expert respondents in this study, consisting of two academics and three practitioners who understand the issues of credibility and sharia compliance. Based on the results of these interviews and literature review, the author formulated the main issues related to the perception of credibility and sharia compliance in digital financial applications, which were then incorporated into the Analytic Network Process (ANP) framework.

Figure 1. ANP Framework



This study divides the problems into four clusters, consisting of the “Internal Problems” cluster, the “External Problems” cluster, the “Internal Solutions” cluster, and the “External Solutions” cluster. Each cluster has three detailed problem nodes according to the cluster category and solution nodes offered according to the cluster category.

Cluster Identification

Problem Cluster

This cluster encompasses the issues formulated to investigate the dynamics of perceived credibility and Sharia compliance within digital financial applications. The problem formulation maps fundamental issues within the ecosystem (internal) as well as issues related to the perceptions and behaviors of users or providers (external). These problems are identified to comprehend the primary barriers to establishing trust and ensuring the sustainable adoption of Sharia-based applications.

A. Internal Problems

Internal problems refer to issues regarding the absence of standards, conceptual ambiguity, and technical-operational constraints inherent in the administration of digital financial applications. The specific issues within the Internal Problem Cluster are as follows:

1. Lack of conceptual consensus and credibility indicators regarding application cost transparency.

Cost transparency is a crucial element in building partner trust; however, there is currently no standardized consensus on how cost components should be disclosed. Frequently, cost information is presented in complex legal terminology or is obscured, rather than being presented as easily comprehensible information. This misalignment of concepts and indicators regarding cost transparency fosters information asymmetry between application administrators and providers, rendering credibility assessments biased and making cross-platform comparisons difficult (Farooq et al., 2020; Secinaro et al., 2025).

2. Lack of conceptual consensus and credibility indicators regarding application security.

Information security is a primary requirement in digital services, yet assessments of this aspect often rely solely on the platform's unilateral claims or limited interface experiences. The absence of widely agreed-upon standardized indicators such as mandatory publication of independent audits or uniform security incident reporting standards, creates uncertainty for providers in verifying the security of their data and operations (Arner et al., 2015; Lutfiah, 2024; Nurmara et al., 2023). This undermines the providers' ability to distinguish between genuinely secure platforms and those that are not.

3. Non-uniform assessment of Sharia compliance due to differing interpretations of contracts.

In the digital Islamic finance ecosystem, a major challenge lies in translating Sharia principles into automated processes, which often triggers differing interpretations regarding the validity of contracts (e.g., Murabahah, Ijarah, or Wakalah) . These differences in contract comprehension, coupled with variations in governance mechanisms and Sharia supervision, result in heterogeneous compliance assessments among providers (Lutfiah, 2024; Ramadhan, 2022; Sudarwanto et al., 2024). Consequently, Sharia compliance status is often perceived as ambiguous, sparking doubt regarding the validity of transactions conducted via the application.

B. External Problems

In the context of this research, external problems refer to gaps occurring outside the platform's technical control, specifically relating to user behavior dynamics, limitations in existing literature, and challenges in establishing market trust. The details of the External Problem Cluster are as follows:

1. Suboptimal empirical evidence of the role of perception as a mediator for adoption.

Previous studies on digital finance tend to focus on the direct relationship between technological features and usage decisions, or they treat Sharia compliance merely as a binary status (compliant/non-compliant). However, a provider's decision to adopt an application is not influenced solely by direct experience but is mediated by perceptual mechanisms specifically, how they interpret credibility and compliance. The lack of empirical evidence regarding how perceived credibility and perceived Sharia compliance function as mediators results in an incomplete understanding of adoption behavior, particularly on the supply side (providers/partners) (Hakim & Supriyanto, 2024).

2. Lack of longitudinal analysis on the influence of experience on user retention.

The majority of research in this field utilizes cross-sectional designs that capture phenomena at only a single point in time. This approach has limitations in explaining how user experience evolves into loyalty or long-term retention amidst a dynamic ecosystem. The absence of longitudinal analysis makes it difficult to map the stability of the influence of experience on users' decisions to continue using the application, despite retention being key to the sustainability of the platform ecosystem (Vives, 2019; Li et al., 2022; Ozili, 2023).

3. Lack of trust in management based on prior experience.

Trust is the primary foundation of the relationship between providers and platforms, yet it is often eroded by weak or ambiguous quality signals. In practice, there is a phenomenon of low provider trust in the integrity of application management both in terms of cost transparency and Sharia accountability based on their previous interaction experiences (Adnan et al., 2025; Ahmed et al., 2026; Hakim & Supriyanto, 2024). When perceived experience is inconsistent with platform claims, risk perception increases and trust in the administrator decreases, which ultimately impedes the growth of partner participation in the digital finance ecosystem.

Solution Cluster

This cluster contains solutions formulated to address the issues of perceived credibility and Sharia compliance in digital financial applications. The formulation involves mapping solutions to address problems originating from the internal application system and from external factors (user perception/environment). The solutions formulated in this study are as follows:

A. Internal Solutions

Internal solutions are derived from a literature review and in-depth interviews with experts (academics and practitioners) to address internal issues related to the lack of clear standards and governance described previously. The discussion of internal solutions is as follows:

1. Establishing cost transparency standards across all channels.

Cost transparency is a fundamental element in building platform credibility (Zulkarnaen et al., 2021). This solution emphasizes the importance of application administrators compiling and publishing a standardized cost structure, not merely as a legal footnote, but as easily accessible primary information. This standardization must include

details on fees, calculation formulas, and clear notifications regarding rate changes (change logs). Implementing transparency standards across all application communication channels aims to eliminate information asymmetry between providers and users. With honest disclosure and uniform standards, the information search cost for partners will decrease, and risk perceptions regarding hidden costs can be minimized. This aligns with Islamic business ethics principles that reject Gharar (uncertainty) in pricing and contracts (Laldin & Furqani, 2019).

2. Implementing a measurable security framework with routine audits.

To address doubts regarding data and operational security, the proposed solution is the implementation of a security framework based on international standards (such as ISO/IEC 27001), followed by routine audits by independent parties. Security must not merely be a unilateral claim but must be proven through valid assurance mechanisms, such as logging, audit trails, and transparent incident handling procedures ranging from detection to recovery. Application administrators need to utilize the results of these security and compliance audits as published signals of credibility for partners. In this way, security becomes a tangible indicator, allowing providers to distinguish credible platforms from non-credible ones, thereby increasing their confidence to adopt the service in the long term (Nurmara et al., 2023).

3. Unifying contract guidelines and disseminating them effectively.

Differences in understanding Sharia contracts in the digital realm often cause confusion and lower perceived compliance (Hasan et al., 2020). The solution to this problem is the unification of contract guidelines agreed upon by Sharia authorities and industry players, which are then massively disseminated to service providers. This unification encompasses the standardization of contract documentation, transaction flows, and Sharia boundaries within automation features. Application administrators must provide adequate education regarding why a contract (e.g., Murabahah or Wakalah) is valid for use in their digital context. With a unified guideline and effective dissemination, diverse interpretations can be minimized, thereby forming a solid perception of Sharia compliance in the minds of providers and service users (Rabbani et al., 2020; Unal & Aysan, 2022; Usman et al., 2021).

B. External Solutions

External solutions are strategic steps formulated to address challenges related to methodological aspects of research and the formation of public or market perception. These solutions aim to fill existing literature gaps and strengthen the trust ecosystem beyond the direct technical control of the application. The discussion of external solutions is as follows:

1. Testing perception mediation in application adoption.

This solution aims to empirically prove that application adoption decisions do not occur directly due to technological features alone, but through the user's cognitive assessment process. In this context, perceived credibility (related to transparency and security) and perceived Sharia compliance are positioned as mediating variables (Unal & Aysan, 2022). This testing is essential to validate that the existence of Sharia features or technical security is insufficient if it fails to form a positive perception in the user's mind. By proving this mediation role, application administrators and researchers can understand that technology investment must be accompanied by communication strategies capable of translating technical features into convincing psychological perceptions, which ultimately drive sustainable usage intention.

Vol. 9. No. 2 (2026)
Page: 16283-16301

2. Conducting longitudinal cohort analysis on retention.

To overcome the limitations of previous studies which are predominantly cross-sectional, this solution offers a longitudinal analysis approach. This approach monitors the same cohort of users over a specific period to observe the dynamics of changes in their perceptions and retention behavior. This analysis is necessary because trust and perceived compliance are not static conditions; both can fluctuate in line with application updates, changes in fee policies, or security incidents. By conducting cohort analysis over time, administrators can identify critical points where users begin to abandon the application and understand whether long-term usage experience strengthens or erodes the initial trust formed (Ahmed et al., 2026).

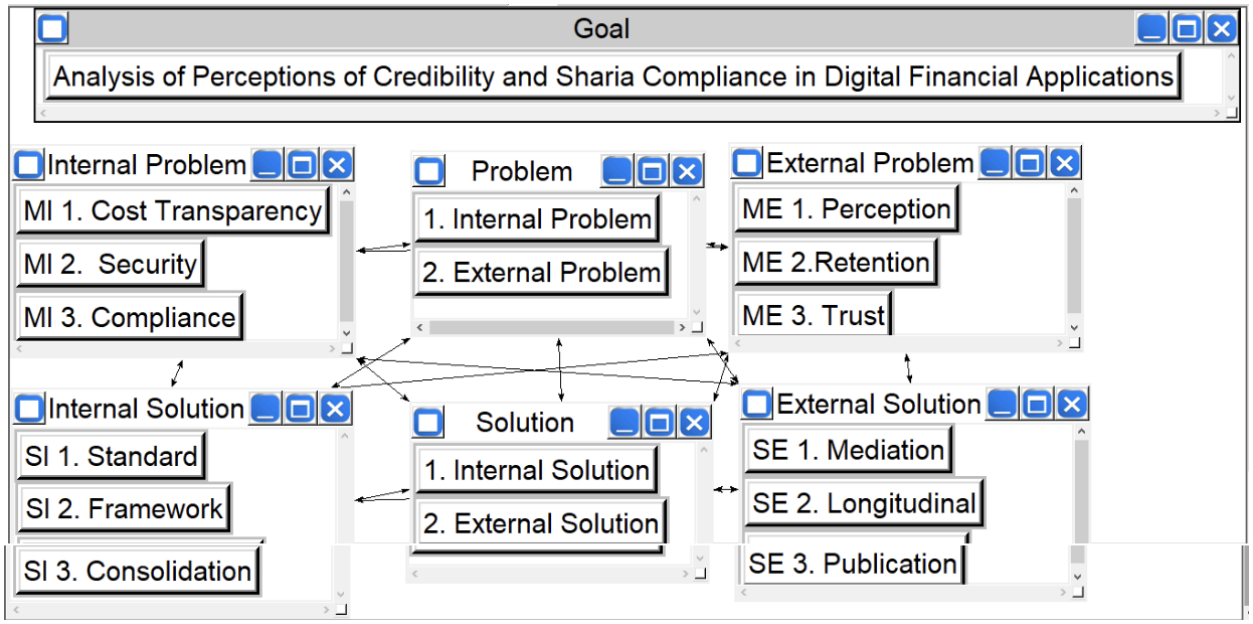
3. Enhancing trust through the publication of verified track records (certifications, independent audits, and testimonials).

This solution focuses on external mechanisms to reduce information asymmetry between application providers and users. Market trust can be significantly enhanced if the platform does not rely solely on internal claims but also presents quality signals verified by third parties. The publication of these track records includes international standard security certifications (such as ISO 27001), transparent independent Sharia audit reports, and authentic testimonials from partners who have joined. These signals serve as objective evidence helping users validate the platform's credibility and compliance without having to conduct their own audits, thereby lowering risk perception and accelerating the decision-making process to join the ecosystem (Czechowska & Paduszyńska, 2025; Ferilli et al., 2024; Secinaro et al., 2025).

ANP Network Model

The research on management issues regarding credibility and Sharia compliance in Indonesian digital Sharia finance applications is divided into four clusters in total: 3 Internal Problems, 3 External Problems, 3 Internal Solutions, and 3 External Solutions. Below is the ANP network image formed from this research:

Figure 2. ANP Network Model



Synthesis and Analysis

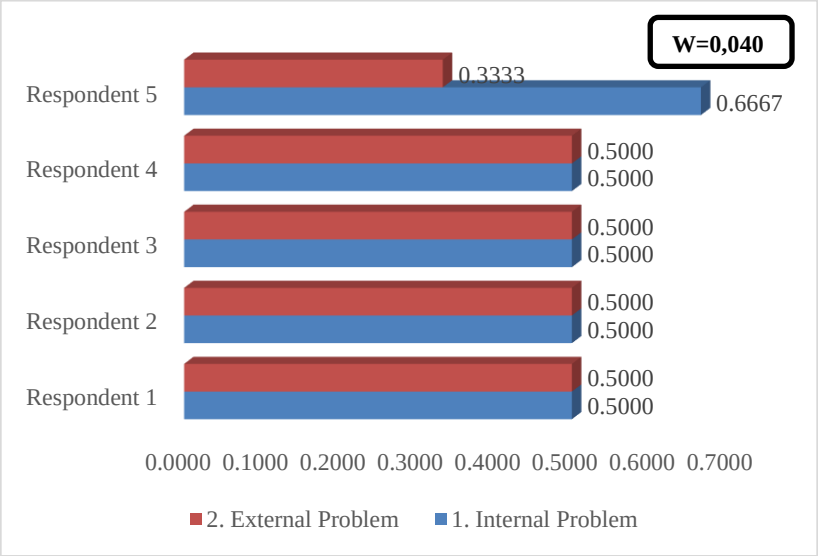
After conducting research through interviews and questionnaires with five respondents, consisting of three practitioners and two academics, the results were calculated using Super Decision and further processed in Microsoft Excel in the form of a geometric mean value, which shows the respondents' tendencies regarding internal problems, external problems, internal solutions, and external solutions as a whole. In addition, the results of these calculations produced a level of agreement or Rater Agreement value, as indicated by the Kendall's Coefficient of Concordance (W) value.

Rater Agreement and Geometric Mean Results

Rater Agreement and Geometric Mean Results for the Problem Cluster

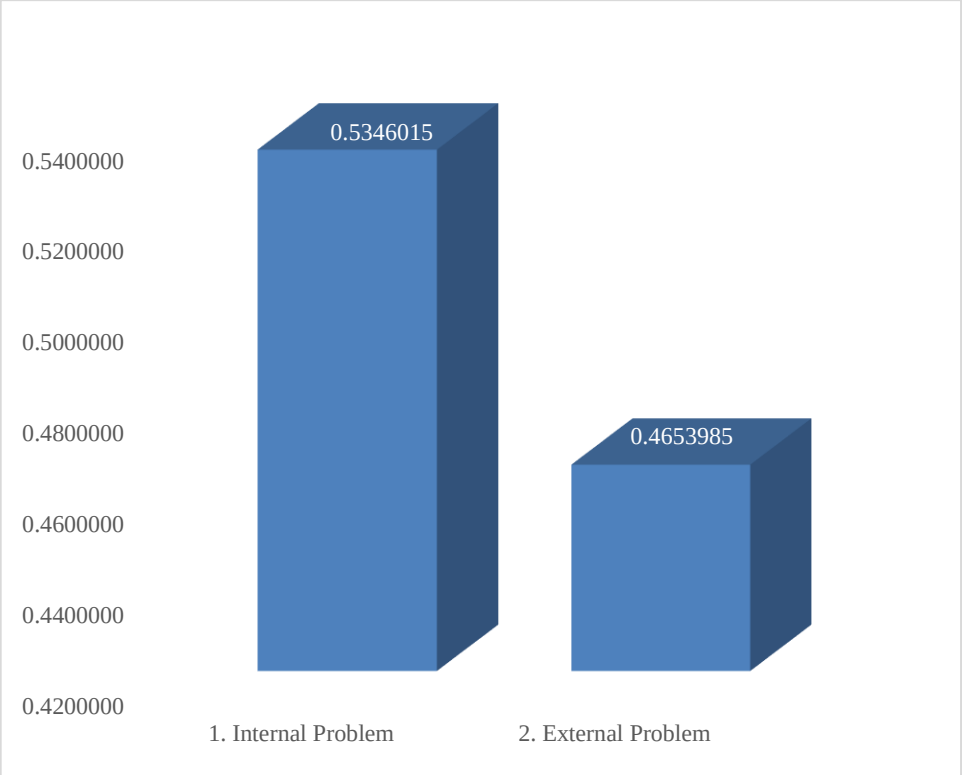
The Rater Agreement graph for the Problem Cluster indicates that the level of agreement among respondents regarding the assessment of internal and external problems remains very low, as evidenced by a Kendall's W coefficient of 0.040 (Figure 2). This value suggests that the respondents hold significantly divergent perceptions in determining problem priorities. Four respondents (Respondents 1–4) assigned equal weight to both internal and external problems (0.5000 each), implying that they view both categories as having equal urgency. However, Respondent 5 provided a differing assessment, assigning a higher weight to internal problems (0.6667) compared to external problems (0.3333). This disparity in assessment resulted in a decrease in the overall consensus level.

Figure 3. Rater Agreement Results for the Problem Cluster



The Geometric Mean graph for the Problem Cluster demonstrates that respondents prioritized internal problems over external problems (Figure 3). The geometric mean value for internal problems is 0.5346015, whereas for external problems it is 0.4653985. This difference indicates that, collectively, the respondents assess internal aspects as being more dominant and having a greater influence on the issues occurring within the research context. Although the respondent agreement level was previously low, the geometric mean results provide an aggregate view that internal problems such as the lack of cost transparency standards, inconsistency in security indicators, and differing interpretations of contracts (akad) are considered more significant than external factors. Consequently, the primary priority in problem resolution should focus on rectifying internal aspects before addressing external issues.

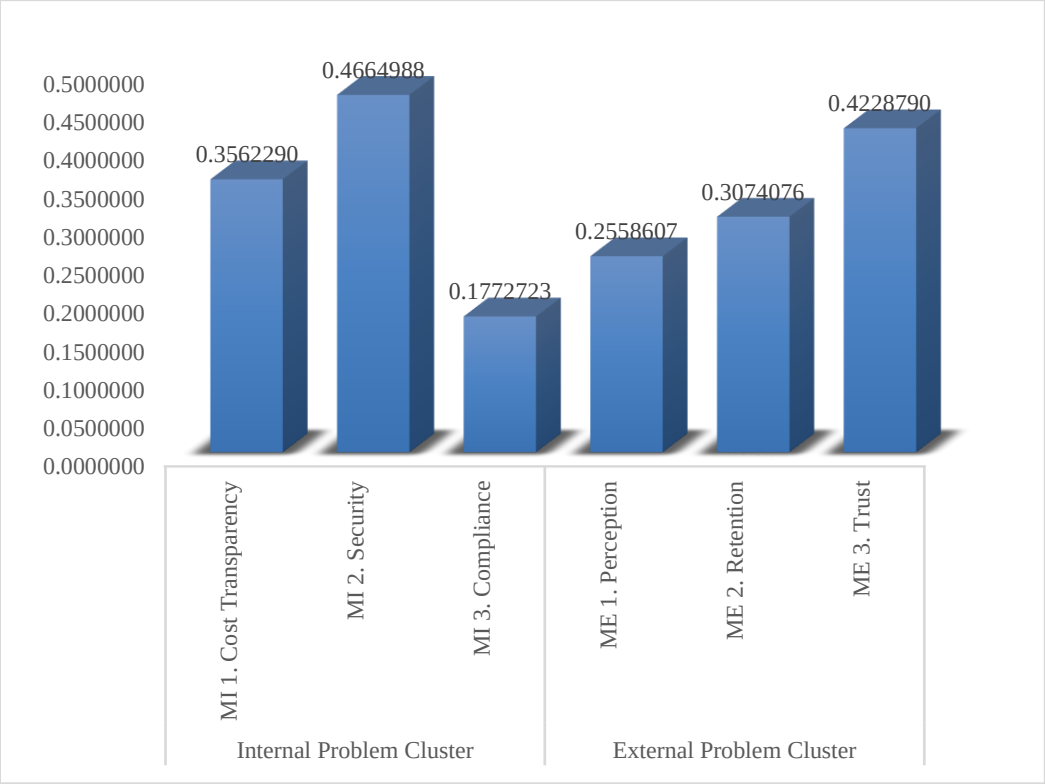
Figure 4. Geometric Mean Results for the Problem Cluster



The combined Geometric Mean results for the Problem Cluster reveal variations in the importance levels of each sub-problem within both internal and external categories (Figure 4). In the internal problem cluster, the sub-problem of application security obtained the highest score, becoming the top priority with a value of 0.4664988; this indicates that the security aspect is viewed as the most crucial issue by the respondents. Furthermore, application cost transparency ranks second with a value of 0.3562290, signaling that cost clarity and openness are also critical concerns, though not as strong as the security issue. Meanwhile, the sub-problem of Sharia compliance holds the lowest value at 0.1772723, suggesting that while this issue remains relevant, its priority level is relatively lower compared to the other two internal aspects.

In the external problem cluster, the sub-problem of user trust in management occupies the highest position or top priority with a value of 0.4228790 (Figure 4). This result illustrates that a lack of public trust serves as the primary challenge from the external side. Following this is the sub-problem of user retention with a value of 0.3074076, indicating that the sustainability of application usage remains an important issue to address. The perception sub-problem, with a value of 0.2558607, sits at the lowest position in the external cluster, illustrating that the role of perception as a mediator toward adoption is viewed as less significant compared to the aspects of trust and retention. Overall, these results indicate that security and trust are the two most prominent aspects among all analyzed sub-problems.

Figure 5. Combined Geometric Mean Results for the Problem Cluster

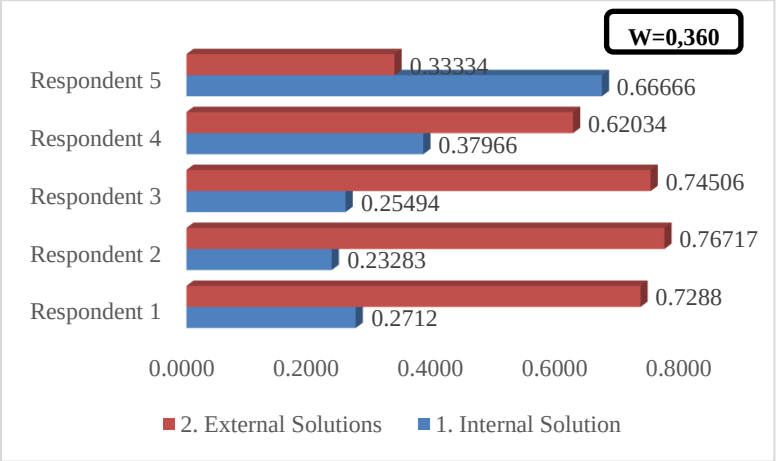


Rater Agreement and Geometric Mean Results for the Solution Cluster

The Rater Agreement graph for the Solution Cluster shows that the level of agreement among respondents falls into the moderate category, reflected by a Kendall's W coefficient of 0.360 (Figure 6). This value indicates a better tendency toward opinion alignment compared to the Problem Cluster, although it cannot yet be classified as high. In general, the majority of respondents assigned greater weight to external solutions compared to internal solutions, with a relatively consistent assessment pattern among respondents.

The graph shows that respondents 1 through 4 consistently placed external solutions as the dominant choice with weights exceeding 0.60, while weights for internal solutions ranged between 0.23 and 0.38. This pattern suggests that the majority of respondents perceive that challenges originating from outside the system—such as user perception, retention, and trust—require higher priority handling. However, an exception exists with Respondent 5, who assigned a higher weight to internal solutions (0.66666) compared to external solutions (0.33334). This difference in Respondent 5's assessment does not significantly affect the general trend because the other four respondents exhibited similar patterns. Overall, these results indicate that despite variations in opinion, particularly from one respondent, the majority of experts tend to agree that external solutions are more important to prioritize in the context of this research.

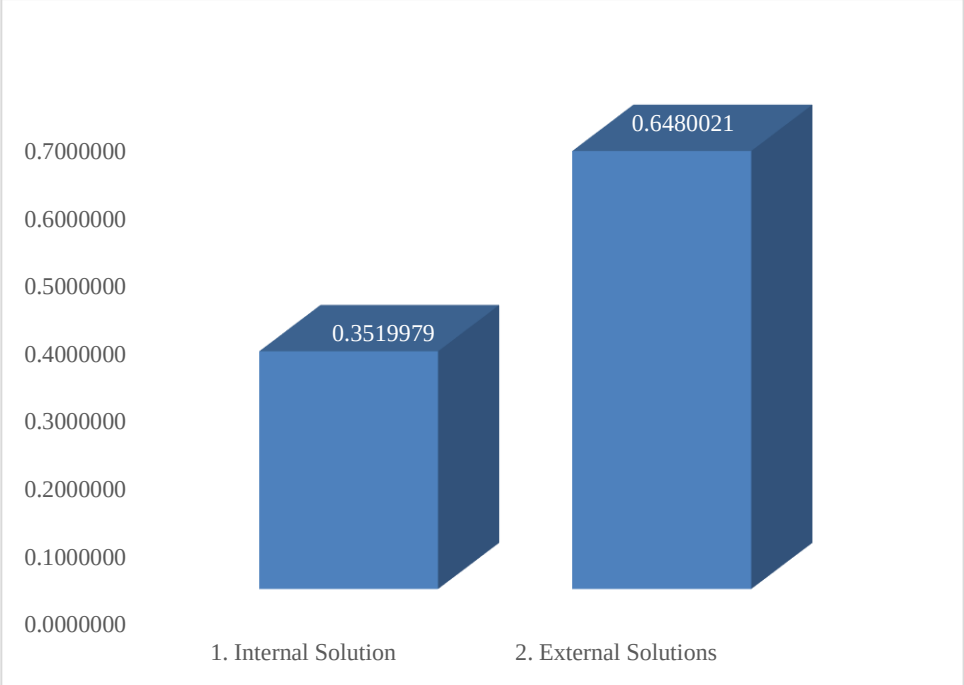
Figure 6. Rater Agreement Results for the Solution Cluster



The Geometric Mean results for the Solution Cluster indicate that respondents prioritize external solutions higher than internal solutions. The geometric mean value for external solutions reached 0.6480021, while internal solutions only obtained a value of 0.3519979 (Figure 6). This significant difference indicates that respondents view external improvements such as enhancing user perception, conducting longitudinal retention analysis, and strengthening credibility through the publication of verified track records as more strategic and urgent steps to address the identified problems.

The lower geometric mean value for internal solutions suggests that while improvements related to cost transparency, application security, and the unification of contract guidelines remain important, these aspects are considered less urgent compared to the need to build trust and improve user experience externally. Thus, these results provide direction that the problem-solving strategy should focus first on external aspects before strengthening internal aspects, especially in the context of strengthening adoption, retention, and user trust.

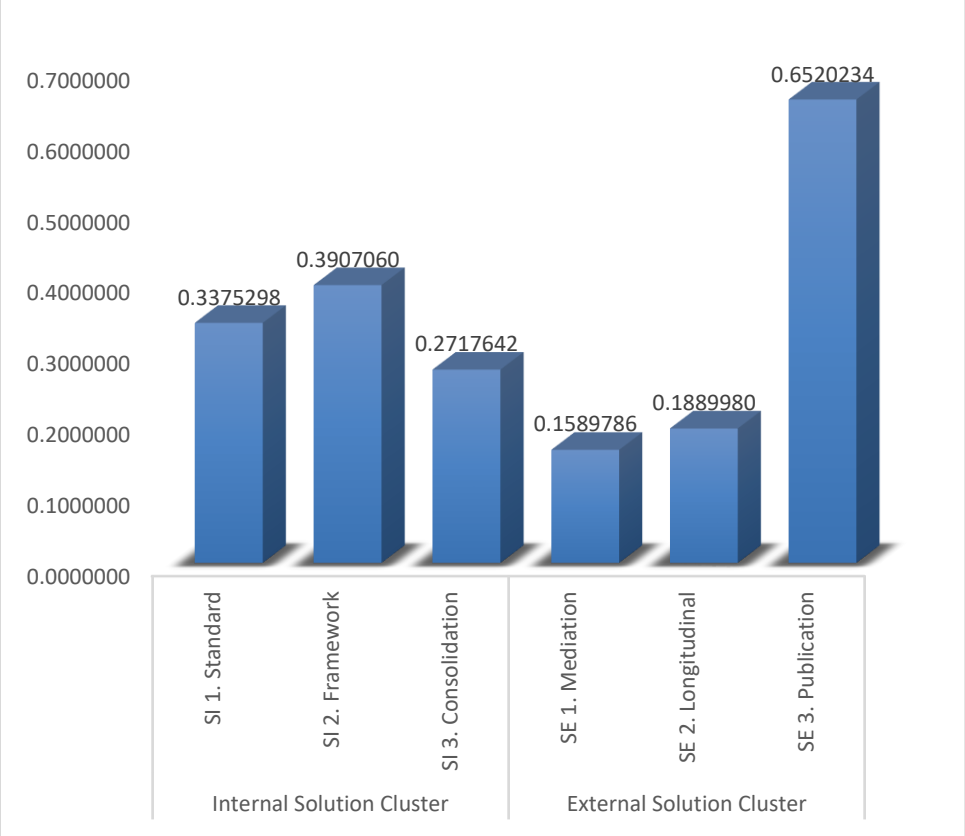
Figure 7. Geometric Mean Results for the Solution Cluster



The combined Geometric Mean results for the Solution Cluster reveal distinct priorities for each sub-solution within both the internal and external solution groups. In the internal solution cluster, the sub-solution of implementing a security framework (SI 2) occupies the highest position or top priority with a value of 0.3907060 (Figure 7). This value indicates that respondents assess the strengthening of the security framework as the most important internal step to prioritize. Furthermore, the establishment of cost transparency standards (SI 1) ranks second with a value of 0.3375298, showing that cost openness is also considered a crucial aspect, although its urgency is slightly below that of security. Meanwhile, the sub-solution of unification and socialization of contract guidelines (SI 3) has a value of 0.2717642, which is the lowest value among internal solutions. This indicates that while still relevant, its priority is not as great as the other two internal solutions.

In the external solution cluster, the publication of verified track records (SE 3) becomes the top priority with a value of 0.6520234, which is significantly higher than other external sub-solutions (Figure 7). This value indicates that increasing public trust through the publication of audit results, certifications, and testimonials is considered the most effective and urgent strategy to address external problems. The longitudinal sub-solution (SE 2) has a value of 0.1889980, showing a medium priority level, particularly regarding efforts to understand user retention behavior in the long term. Meanwhile, perception mediation (SE 1) occupies the lowest position in the external cluster with a value of 0.1589786, indicating that this aspect is considered important but not as critical as publication or longitudinal analysis.

Figure 8. Combined Geometric Mean Results for the Solution Cluster



CONCLUSION

Based on the Analytic Network Process (ANP) analysis, this study concludes that the perception of credibility in digital financial applications is predominantly influenced by the

internal problem cluster, with a weight of 0.5346015, surpassing external factors. Specifically, the Security sub-problem occupies the highest priority with a Geometric Mean value of 0.4664988, followed by Cost Transparency (0.3562290), while the Compliance aspect ranks lowest with a value of 0.1772723. Although significant divergence in opinion exists among experts indicated by a low Rater Agreement value (W=0.040), the synthesis of priorities demonstrates the dominance of External Solutions, with a value of 0.6480021. The strategy of Verified Track Record Publication, which encompasses certification and independent audits, emerges as the absolute priority with a value of 0.6520234, far exceeding the retention monitoring solution valued at 0.1889980.

Theoretically, these findings imply that the lack of clear security standards is perceived as a fundamental risk that impedes credibility more significantly than issues regarding the understanding of Sharia contracts; consequently, operational technical guarantees are deemed more urgent than compliance, which is currently viewed as secondary. The managerial implications assert that trust and long-term retention cannot be established solely through internal application features but must be mediated by third-party validation. Therefore, application developers are advised not only to focus on internal improvements but to aggressively pursue international standard certifications (such as ISO 27001) and audit transparency as primary quality signals to foster partner trust.

The primary limitation of this research lies in the utilization of the ANP method, which relies on assessments from a limited number of experts; thus, generalization to the broader user population warrants caution. For future research, it is recommended to conduct quantitative empirical testing to validate the alignment between expert perception and actual user behavior, as well as to perform in-depth qualitative studies to explore the causes of the polarization of views between practitioners and academics identified in this study. Furthermore, a longitudinal cohort approach is recommended to monitor the dynamics of user retention concurrent with updates to security policies and changes in cost structures over time.

REFERENCES

Adnan, M. F., Efendi, E. N., Asyraf Zamri, M. W., Ridwan, N., & Yusoff, Y. (2025). Factors Influencing User Retention and User Experience in Malaysian Fintech. *International Journal of Research and Innovation in Social Science*, *IX*(III), 3259–3272. https://doi.org/10.47772/IJRISS.2025.90300255

AFTECH. (2023). *Annual Members Survey 2022-2023*. https://fintech.id/id/knowledge-hub/aftech-annual-members-survey-20222023-bahasa-indonesia

Ahmed, W., Al-Sharafi, M. A., Raza, A., Al-Zaeemi, S. A. S., Al-Bashrawi, M. A., & Dwivedi, Y. K. (2026). A longitudinal big data approach to theorizing consumers' continuance intention to use loyalty apps. *Journal of Retailing and Consumer Services*, *88*, 104453. https://doi.org/10.1016/J.JRETCONSER.2025.104453

Arner, D. W., Barberis, J. N., & Buckley, R. P. (2015). The Evolution of Fintech: A New Post-Crisis Paradigm? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2676553

Ascarya, A., & Sakti, A. (2022). Designing micro-fintech models for Islamic micro financial institutions in Indonesia. *International Journal of Islamic and Middle Eastern*

Finance and Management, *15*(2), 236–254. https://doi.org/10.1108/IMEFM-05-2020-0233

Banna, H., Kabir Hassan, M., & Rashid, M. (2021). Fintech-based financial inclusion and bank risk-taking: Evidence from OIC countries. *Journal of International Financial Markets, Institutions and Money*, *75*, 101447. https://doi.org/10.1016/J.INTFIN.2021.101447

Czechowska, I. D., & Paduszyńska, M. (2025). The Role of Trust in Fintech Adoption and Development: Bibliometric Analysis. *Procedia Computer Science*, *270*, 2790–2798. https://doi.org/10.1016/J.PROCS.2025.09.401

Farooq, M. S., Khan, M., & Abid, A. (2020). A framework to make charity collection transparent and auditable using blockchain technology. *Computers and Electrical Engineering*, *83*. https://doi.org/10.1016/j.compeleceng.2020.106588

Ferilli, G. B., Altunbas, Y., Stefanelli, V., Palmieri, E., & Boscia, V. (2024). Fintech governance and performance: Implications for banking and financial stability. *Research in International Business and Finance*, *70*, 102349. https://doi.org/10.1016/J.RIBAF.2024.102349

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the Fintech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services. *Journal of Management Information Systems*, *35*(1), 220–265. https://doi.org/10.1080/07421222.2018.1440766

Hakim, M. A., & Supriyanto, A. (2024). Sharia Fintech and Gen Z: The Mediating Role of Perceived Usefulness. *Share: Jurnal Ekonomi Dan Keuangan Islam*, *13*(1), 322–346. https://doi.org/10.22373/SHARE.V13I1.22990

Hasan, R., Hassan, M. K., & Aliyu, S. (2020). Fintech and Islamic Finance: Literature Review and Research Agenda. *International Journal of Islamic Economics and Finance (IJIEF)*, *3*(1), 75–94. https://doi.org/10.18196/ijief.2122

Laldin, M. A., & Furqani, H. (2019). Fintech and Islamic finance: Setting the Sharī‘ah parameters. In *Fintech in Islamic Finance: Theory and Practice* (1st ed., pp. 113–119). Taylor and Francis. https://doi.org/10.4324/9781351025584-8/FINTECH-ISLAMIC-FINANCE-MOHAMAD-AKRAM-LALDIN-HAFAS-FURQANI

Lutfiah, I. N. (2024). Navigating Between Innovation and Compliance: The Challenges of Sharia Fintech Implementation in Indonesia’s Financial Ecosystem. *Demak Universal Journal of Islam and Sharia*, *2*(03), 211–220. https://doi.org/10.61455/deujis.v2i03.130

Nurmara, M. A. K., Hakim, M. N., Ardy, O. H. C., Jeffrey, R., Setiono, V. A., Kanigoro, B., & Irwansyah, E. (2023). A Review of Security in Financial Technology. *Procedia Computer Science*, *227*, 958–965. https://doi.org/10.1016/J.PROCS.2023.10.603

Oseni, U. A., Ali, S. N., Oseni, U. A., & Nazim Ali, S. (2019). Fintech in Islamic finance. In *Fintech In Islamic Finance* (Issue July). https://doi.org/10.4324/9781351025584-1

Ozili, P. K. (2018). Impact of digital finance on financial inclusion and stability. *Borsa Istanbul Review*, *18*(4), 329–340. https://doi.org/10.1016/J.BIR.2017.12.003

Parker, Geoffrey., Van Alstyne, Marshall., & Choudary, S. Paul. (2017). *Platform revolution : How networked markets are transforming the economy - and how to make them work for you*. W. W. Norton & Company.

PBI. (2017). Peraturan Bank Indonesia tentang Penyelenggaraan Teknologi Finansial. PBI No.19/12/PBI/2017. *Gubernur Bank Indonesia*.

Peraturan Bank Indonesia Nomor 18/40/PBI/2016 Tahun 2016 Tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran, Pub. L. No. 18/40/PBI/2016, Bank Indonesia (2016). https://peraturan.bpk.go.id/Details/135749/peraturan-bi-no-1840pbi2016-tahun-2016

Peraturan Pemerintah (PP) Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik, Pub. L. No. Nomor 71 Tahun 2019, Pemerintah Indonesia (2019). https://peraturan.bpk.go.id/Details/122030/pp-no-71-tahun-2019

POJK No, 77 2016 on Information Technology-Based Peer to Peer Lending Services, Pub. L. No. 77, OJK (2016). https://ojk.go.id/id/regulasi/Pages/POJK-tentang-Layanan-Pinjam-Meminjam-Uang-Berbasis-Teknologi-Informasi.aspx

POJK Nomor 13 /POJK.02/2018 Tentang Inovasi Keuangan Digital Di Sektor Jasa Keuangan (2018).

POJK Number 10 /POJK.05/2022 Concerning Information Technology-Based Joint Funding Services, Pub. L. No. No. 10, OJK 1 (2022). https://ojk.go.id/id/regulasi/Documents/Pages/Layanan-Pendanaan-Bersama-Berbasis-Teknologi-Informasi/POJK%2010%20-%2005%20-%202022.pdf

Rabbani, M. R., Khan, S., & Thalassinos, E. I. (2020). FinTech, Blockchain and Islamic Finance: An Extensive Literature Review. *International Journal of Economics & Business Administration (IJEBA)*, *VIII*(2), 65–86. https://ideas.repec.org/a/ers/ijebaa/vviiiy2020i2p65-86.html

Ramadhan, D. S. (2022). Financial Technology and Sharia Compliance Regulations in Islamic Banking in Indonesia. *Al-Arbah Journal of Islamic Finance and Banking*, *4*(2), 217–231. https://doi.org/10.21580/al-arbah.2022.4.2.15647

Saaty, T. L., & Vargas, L. (2006a). *Decision making with the analytic network process. Economic, political, social and technological applications with benefits, opportunities, costs and risks* (Vol. 95). Springer US. https://doi.org/10.1007/0-387-33987-6

Saaty, T. L., & Vargas, L. G. (2006b). Decision Making with the Analytic Network Process. In *Decision making with the analytic network process. Economic, political, social and technological applications with benefits, opportunities, costs and risks* (Vol. 195, Issue August, p. pp.1-26). Springer. https://doi.org/10.1007/978-1-4614-7279-7

Secinaro, S., Lanzalonga, F., Oppioli, M., & de Nuccio, E. (2025). The effects of disruptive technologies on accountability in fintech industry: Using bibliometric analysis to develop a research agenda. *Research in International Business and Finance*, *76*, 102816. https://doi.org/10.1016/J.RIBAF.2025.102816

Sudarwanto, A. S., Kharisma, D. B., & Cahyaningsih, D. T. (2024). Islamic crowdfunding and Shariah compliance regulation: problems and oversight. *Journal of Financial Crime*, *31*(4), 1022–1036. https://doi.org/10.1108/JFC-01-2023-0003/FULL/XML

Unal, I. M., & Aysan, A. F. (2022). Fintech, Digitalization, and Blockchain in Islamic Finance: Retrospective Investigation. *FinTech*, *1*(4), 388–398. https://doi.org/10.3390/fintech1040029

Undang-Undang (UU) Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi, Pub. L. No. No. 27 Tahun 2022, Pemerintah Indonesia (2022). https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Usman, H., Projo, N. W. K., Chairy, C., & Haque, M. G. (2021). The exploration role of Sharia compliance in technology acceptance model for e-banking (case: Islamic bank in Indonesia). *Journal of Islamic Marketing*, *13*(5), 1089–1110. https://doi.org/10.1108/JIMA-08-2020-0230

Zulkarnaen, D., Mukhlisin, M., & Eko Pramono, S. (2021). Can Blockchain Technology Improve Accountability and Transparency of Cash Waqf in Indonesia? *Journal of Economic Impact*, *3*(3), 158–166. https://doi.org/10.52223/jei3032105