Selaparang: Journal of Law Studies
E-ISSN: 3124-4270 | Vol. 1 No. 2, 2026 | Pages 1-13
https://ojs.yahantara.com/index.php/SEJALS

Validity of Digital Contracts in Sharia FinTech Transactions: The Perspective of Islamic Economic Law and Indonesian Positive Law

Ibadurrahman[1]✉, Inayatul Mutmainnah[2], Muhammad Daffa Alfarizky[3]
(1) Universitas Indonesia Timur, Makassar, Indonesia
(2) Universitas Pepabri Makassar, Kota Makassar, Indonesia
(3) Institut Islam Negeri Pontianak, Kota Pontianak, Indonesia

Received: 31-01-2026 | Revised: 20-05-2026 | Accepted: 30-08-2026

Corresponding Author:
Ibadurrahman,
Universitas Indonesia Timur, Makassar, Indonesia, Jl. Rappocini Raya No. 171–174, Kecamatan Rappocini, Kota Makassar, Sulawesi Selatan, Indonesia
Email: jbadurrahman1990@gmail.com

ABSTRACT

The rapid development of financial technology (FinTech) in Indonesia has transformed financial transactions through the increasing use of digital contracts, raising legal questions regarding their validity under national law and Islamic principles. This study examines the legal status of digital contracts in Sharia-based FinTech, particularly concerning contractual consent, virtual contract formation, and personal data protection. Employing normative legal research through statutory, conceptual, and comparative approaches, the study analyzes Indonesian legislation, civil law provisions, and relevant DSN-MUI fatwas. The findings demonstrate that digital contracts are legally enforceable under Indonesian law when they satisfy contractual requirements and applicable electronic transaction regulations. From the perspective of Islamic law, virtual contractual assemblies can be accommodated through the concept of *majlis hukmi*, provided that mutual consent, contractual clarity, and the prohibition of *riba*, *gharar*, and *maysir* are maintained. Furthermore, personal data protection constitutes an essential element in safeguarding contractual integrity and supporting the objective of *hifz al-mal*.

Perkembangan teknologi finansial (*financial technology* atau FinTech) di Indonesia telah mengubah mekanisme transaksi keuangan melalui penggunaan kontrak digital, sekaligus menimbulkan persoalan hukum mengenai keabsahannya berdasarkan hukum nasional dan prinsip syariah. Penelitian ini bertujuan menganalisis kedudukan hukum kontrak digital dalam FinTech syariah, khususnya terkait persetujuan para pihak, pembentukan akad secara virtual, dan pelindungan data pribadi. Penelitian menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan komparatif melalui analisis peraturan perundang-undangan serta fatwa DSN-MUI yang relevan. Hasil penelitian menunjukkan bahwa kontrak digital memiliki kekuatan hukum mengikat apabila memenuhi persyaratan perjanjian dan ketentuan transaksi elektronik. Dalam perspektif hukum Islam, pembentukan akad secara virtual dapat diterima melalui konsep *majlis hukmi*, sepanjang memenuhi prinsip kerelaan, kejelasan akad, serta bebas dari *riba*, *gharar*, dan *maysir*. Pelindungan data pribadi juga menjadi unsur penting dalam menjaga integritas akad dan mewujudkan prinsip *hifz al-mal*.

Keywords: digital contracts, Indonesian positive law, Islamic economic law, Sharia FinTech

Introduction

The rapid development of financial technology (FinTech) across Southeast Asia, particularly in Indonesia, has fundamentally transformed economic interactions, financial transaction mechanisms, and the legal relationships underlying commercial activities. As the country with the world's largest Muslim population, Indonesia faces a distinctive challenge in developing a digital financial ecosystem that not only promotes economic efficiency but also

© 2026 The Author(s). Published by Yazri Harapan Nusantara, ID

This is an Open Access article distributed under the terms of the Creative Commons Attribution 4.0 International License (https://creativecommons.org/licenses/by/4.0/).

ensures compliance with Islamic legal principles (Mansurnoor, 2021). This transformation is reflected in the expanding utilization of information technology-based financing services, particularly peer-to-peer (P2P) financing, electronic payment systems, and digital investment platforms, which enable financial transactions to be conducted without physical meetings or conventional paper-based documentation (Arsyad & Basri, 2024). Within the context of Islamic financial technology, digital contracts have become fundamental legal instruments governing the formation of contractual relationships between fund providers (*shahibul mal*), platform operators, and financing recipients (*mudharib* or *mustahiq*). These contracts establish the rights, obligations, responsibilities, and allocation of risks among the parties involved in digital financial transactions (Sakti et al., 2026). Consequently, digital transformation has not merely altered the technical mechanisms through which financial transactions are conducted but has also generated new legal challenges concerning the legitimacy, enforceability, and Sharia compliance of contractual relationships in the digital environment. This development necessitates a comprehensive legal framework capable of accommodating technological innovation while preserving the substantive requirements of Islamic commercial law.

A fundamental legal problem arises from the transition of contractual formation from conventional face-to-face interactions to electronic environments in which the contracting parties are not necessarily physically present in the same location. Within classical Islamic jurisprudence on commercial transactions (*fiqh muamalah*), the validity of a contract is closely associated with the concept of *majlis al-aqd*, referring to the contractual assembly or setting in which the agreement is established, as well as the principle of *an-taradhin*, which emphasizes the mutual consent and voluntary agreement of the contracting parties. These principles are essential to ensuring the authenticity of contractual consent, preventing uncertainty (*gharar*), and maintaining the legitimacy of commercial transactions (Zuhayli, 2002). However, contemporary FinTech transactions increasingly rely on electronic devices, digital applications, and online communication systems through which the offer (*ijab*) and acceptance (*qabul*) may occur remotely, asynchronously, and across different geographical locations. This transformation raises significant doctrinal questions concerning the interpretation of *majlis al-aqd* in virtual environments, the legal validity of electronically expressed contractual consent, and the extent to which digital communication can satisfy the substantive requirements of *sighat al-aqd*. Simultaneously, Indonesian positive law regulates contractual validity through the Indonesian Civil Code (*Kitab Undang-Undang Hukum Perdata* or KUHPerdata), while the recognition and legal consequences of electronic information, electronic documents, and electronic transactions are governed by Law No. 11 of 2008 concerning Electronic Information and Transactions (Electronic Information and Transactions Law or ITE Law). Accordingly, the legal implications of digital contracting extend beyond the transformation of contractual formalities and involve broader questions of legal certainty, evidentiary validity, and the harmonization of national legal provisions with Islamic commercial law principles.

The legal complexity of digital contracts is further intensified by the increasing utilization of electronic Know Your Customer (e-KYC) mechanisms, which involve the collection, processing, storage, and utilization of users' personal data. In digital financial transactions, personal information constitutes an essential component of identity verification, contractual authentication, risk mitigation, and the prevention of fraudulent activities. Nevertheless, the extensive processing of such information creates additional legal obligations concerning confidentiality, information security, transparency, and the accountability of digital platform operators. The enactment of Law No. 27 of 2022 concerning Personal Data Protection

(Personal Data Protection Law or PDP Law) establishes a stronger legal foundation for regulating the processing and protection of personal information in Indonesia, including within digital financial services (Putri Relina et al., 2025). From the perspective of Islamic commercial law, these issues can also be examined through the principle of *hifz al-mal*, which emphasizes the protection of wealth and economic interests as one of the fundamental objectives of Islamic law. Although personal data protection cannot be equated directly with the protection of wealth, the two concepts have important intersections in relation to financial security, the prevention of economic harm, and the preservation of transactional integrity. Unauthorized access to, misuse of, or disclosure of personal information may undermine users' financial interests, compromise contractual relationships, and diminish public confidence in digital financial services. Therefore, personal data protection should not be understood exclusively as a technical cybersecurity issue but also as an integral component of the legal governance of digital contracts, particularly in ensuring the legitimacy, security, and sustainability of Sharia-compliant financial transactions.

The significance of this research can also be understood in light of the growing academic interest in electronic contracting, digital financial governance, Islamic FinTech, and the regulation of technology-mediated commercial relationships. Previous legal scholarship has extensively addressed the general principles of electronic transactions, particularly contractual validity, the legal relationship between contracting parties, and consumer protection within digital commercial environments. Classical civil law perspectives, for instance, provide an important conceptual foundation for understanding the essential requirements of contractual validity, the legal consequences of agreements, and the rights and obligations arising from contractual relationships (Subekti, 2010). Meanwhile, studies concerning Islamic FinTech have increasingly emphasized the importance of contractual arrangements in ensuring that technology-based financial transactions comply with Islamic commercial principles, particularly regarding mutual consent, contractual clarity, and the allocation of responsibilities among the parties involved (Arsyad & Basri, 2024; Sakti et al., 2026). Contemporary Islamic jurisprudence has likewise highlighted the importance of interpreting classical contractual principles in response to technological developments and modern communication mechanisms without compromising the fundamental objectives of Sharia (Zuhayli, 2002). Nevertheless, these perspectives indicate the need for a more integrated examination of the relationship between electronic contractual validity under Indonesian positive law, the reconstruction of *majlis al-aqd* and *sighat ijab-qabul* within virtual environments, and the legal obligations associated with personal data protection in digital financial transactions. Thus, the examination of digital contracts in Islamic FinTech requires more than an isolated analysis of civil law or Islamic jurisprudence; it demands an interdisciplinary legal perspective that addresses the interaction between these regulatory and normative frameworks within a single contractual relationship.

Against this background, the research gap addressed in this article concerns the limited integration of doctrinal analyses examining the harmonization between Indonesian positive law governing digital contractual validity and the fundamental principles of Islamic contract formation, particularly within the operational context of FinTech transactions. Rather than treating digital contracts merely as technological adaptations of conventional agreements, this study investigates how the transformation of communication mechanisms affects the interpretation and fulfillment of the essential elements of Islamic contracts. Furthermore, personal data protection is examined as an integral dimension of contractual integrity, connecting national legal obligations with the broader objectives of Islamic legal protection. To

address this gap, the study focuses on three interrelated research questions: (1) How does Indonesian positive law regulate the validity and evidentiary force of digital contracts in FinTech transactions? (2) How does Islamic economic law conceptualize *majlis al-aqd* and the implementation of *ijab-qabul* (*sighat*) within virtual environments? and (3) What are the legal implications of personal data protection under the PDP Law in relation to the principle of *hifz al-mal*, contractual integrity, and the sustainability of digital financial transactions? These questions are examined through an analysis of relevant statutory provisions and DSN-MUI Fatwa No. 117/DSN-MUI/II/2018 concerning Information Technology-Based Financing Services Based on Sharia Principles. The fatwa provides an essential normative reference for evaluating the implementation of technology-based financing activities in accordance with Islamic commercial law. By bringing these three dimensions together, this research seeks to provide a more comprehensive understanding of the legal foundations governing digital contractual relationships within Indonesia's Sharia FinTech ecosystem.

Accordingly, this study positions the harmonization of digital contract law as a multidimensional legal issue involving civil law, electronic transaction regulations, personal data protection, and Islamic economic law. Employing a normative juridical approach, this research examines the relevant statutory provisions and Islamic legal principles to identify areas of convergence, potential regulatory inconsistencies, and the need for a more coherent legal construction of electronically executed contracts. Its principal contribution lies in developing an integrated analytical framework connecting the legal validity of digital contracts, the reinterpretation of *majlis al-aqd* and *ijab-qabul* within virtual environments, and personal data protection as an essential element in maintaining the integrity of Sharia-compliant financial transactions. Theoretically, this study is expected to enrich contemporary scholarship on Islamic economic law, particularly concerning the applicability and reinterpretation of classical contractual principles in response to technological innovation. Practically, its findings are expected to provide legal and regulatory insights for policymakers, Sharia FinTech platform operators, and other stakeholders in establishing contractual mechanisms that are legally valid, transparent, secure, and consistent with both Islamic principles and Indonesian legislation. Ultimately, the harmonization of these legal dimensions is expected not only to strengthen legal certainty but also to foster public trust, institutional accountability, and the sustainable development of Islamic financial services within an increasingly digital economic environment.

Methods

This study employs a normative legal research design (doctrinal legal research) by applying statutory, conceptual, and comparative legal approaches (Creswell & Creswell, 2018; Punch, 2014). The primary legal materials comprise the Indonesian Civil Code (Kitab Undang-Undang Hukum Perdata or KUHPerdata), particularly Article 1320 concerning the validity requirements of agreements; Law No. 11 of 2008 in conjunction with Law No. 1 of 2024 concerning Electronic Information and Transactions (ITE Law), particularly Articles 5 and 11, which regulate the legal recognition of electronic documents and the validity of electronic signatures; Law No. 27 of 2022 concerning Personal Data Protection (PDP Law); and DSN-MUI Fatwa No. 117/DSN-MUI/II/2018 concerning Information Technology-Based Financing Services Based on Sharia Principles. Secondary legal materials include legal textbooks, articles published in accredited scientific journals, and authoritative legal commentaries relevant to digital contracting and Islamic commercial law. The collected legal materials are examined through qualitative-prescriptive analysis by systematically interpreting and comparing statutory

provisions with the doctrinal principles of fiqh muamalah. This analytical process is intended to identify the legal compatibility, potential normative discrepancies, and regulatory implications arising from the implementation of digital contracts in Sharia FinTech transactions, ultimately providing a conceptual framework for harmonizing the validity of electronic agreements with Indonesian positive law and Islamic legal principles.

Result and Discussion

The Validity of Digital Contracts According to Indonesian Positive Law

Within the Indonesian civil law framework, the legal validity of digital contracts is fundamentally grounded in the general principles governing contractual obligations under the Indonesian Civil Code (*Kitab Undang-Undang Hukum Perdata* or KUHPerdata), particularly Article 1320. This provision establishes four cumulative legal requirements that determine whether an agreement may be recognized as legally valid: the mutual consent of the contracting parties, their legal capacity to enter into an agreement, the existence of a sufficiently determined contractual object, and the presence of a lawful cause. These requirements remain applicable regardless of whether an agreement is concluded through conventional face-to-face interactions or electronic communication systems. However, the emergence of financial technology (FinTech) introduces additional dimensions to their implementation, particularly because contractual relationships increasingly involve digital platforms as intermediaries facilitating the interaction between financing providers and recipients. Consequently, the application of Article 1320 must be understood in conjunction with the regulatory framework governing electronic transactions, particularly Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law), as amended by Law No. 1 of 2024, and Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE). These regulatory instruments provide the legal foundation for recognizing electronic agreements while establishing requirements concerning the reliability, security, and accountability of electronic systems through which contractual relationships are formed and administered.

The first requirement, namely mutual consent, concerns the existence of a genuine and legally recognizable expression of agreement between the parties. In digital financial transactions, the manifestation of consent is no longer necessarily demonstrated through handwritten signatures or direct verbal declarations. Instead, it may be expressed through various electronic mechanisms, including affirmative actions such as selecting an agreement confirmation option, accepting contractual terms through a click-wrap agreement, or executing a document using an electronic signature. Such mechanisms constitute legally relevant manifestations of contractual intention, provided that the identity of the consenting party and the authenticity of the expressed agreement can be established. Article 11 of the ITE Law recognizes the legal validity and binding consequences of electronic signatures when the applicable statutory requirements are fulfilled. These requirements include the ability to identify the signatory, indicate approval of the relevant electronic information, and ensure that the electronic signature and associated information retain their authenticity and integrity. Accordingly, the use of electronic consent mechanisms within FinTech applications may satisfy the consensual element prescribed under Article 1320 of the Civil Code. Nevertheless, the legal recognition of digital consent should not be interpreted as an unconditional validation of every electronic acceptance. The contracting process must also provide adequate information,

demonstrate the user's affirmative intention, and ensure that consent is not obtained through deception, coercion, or other circumstances that undermine the freedom of contractual will.

The second requirement concerns the legal capacity of the parties to undertake contractual obligations and assume the consequences arising from their agreements. In conventional contractual relationships, capacity is generally assessed through the legal identity and status of the individuals or legal entities entering into the agreement. Within the digital FinTech environment, however, the absence of direct physical interaction creates additional challenges in establishing the authenticity of users' identities and determining whether the individuals accessing a platform are legally entitled to perform the relevant legal acts. To address these concerns, financial technology providers increasingly employ Electronic Know Your Customer (e-KYC) procedures that integrate digital identity verification, personal identification data, biometric authentication, and facial recognition technologies. In certain implementations, the verification process involves matching the user's National Identification Number (*Nomor Induk Kependudukan* or NIK) and biometric information against population administration records managed by the Directorate General of Population and Civil Registration (Dukcapil). Such mechanisms are intended to reduce identity fraud, prevent unauthorized contractual participation, and strengthen the reliability of electronic identification. From a civil law perspective, e-KYC may serve as an important evidentiary and administrative instrument for establishing the identity of contracting parties. Nevertheless, identity authentication and legal capacity constitute two distinct legal questions. The successful verification of a person's identity does not automatically establish that the individual possesses the legal capacity required to enter into a particular agreement. Therefore, FinTech operators must ensure that identity verification is accompanied by appropriate assessments of legal eligibility and compliance with applicable contractual and regulatory requirements.

The third and fourth requirements under Article 1320 concern the certainty of the contractual object and the lawfulness of the underlying cause. Both requirements are particularly significant in digital financing arrangements because the parties generally establish their contractual relationships through standardized electronic documents and predetermined contractual provisions. The certainty of the contractual object requires the essential elements of the transaction to be sufficiently identifiable, transparent, and understandable to all parties. In Sharia-based FinTech financing, these elements may include the principal amount of financing, the nature and purpose of the transaction, the applicable financing or profit-sharing mechanism, the agreed margin where relevant, the duration of the financing arrangement, and the repayment schedule. Such information must be presented in a manner that enables users to understand the substance and potential consequences of their contractual commitments before providing consent. Meanwhile, the requirement of a lawful cause concerns the underlying legal purpose and substantive content of the agreement. Article 1337 of the Civil Code establishes that a cause is unlawful when it is prohibited by law or conflicts with morality or public order. Consequently, electronic contractual provisions must not merely satisfy formal requirements but must also contain lawful obligations and legitimate transactional purposes. In the context of Islamic financial services, this assessment further requires attention to the substantive compatibility of the financing arrangement with Sharia principles, particularly the prohibition of *riba*, *gharar*, and *maysir*. Thus, standardized electronic contracts should function not merely as administrative instruments but as transparent legal frameworks that ensure contractual certainty, legitimate purposes, and accountability throughout the financing relationship.

Beyond the substantive requirements for contractual validity, the evidentiary status of digital contracts constitutes another essential dimension of legal certainty within Indonesia's electronic transaction framework. The recognition of electronic agreements would have limited practical significance if their contents, authenticity, and execution could not be established when disputes arise. In this regard, Article 5 paragraph (1) of the ITE Law expressly recognizes Electronic Information and/or Electronic Documents, including their printouts, as legally valid evidence. This provision provides an important legal basis for presenting digitally generated contractual records in judicial proceedings, including disputes arising from technology-based financial transactions. Electronic agreements, transaction histories, authentication records, electronic signatures, and other relevant digital documentation may therefore serve as evidentiary materials when their authenticity, integrity, accessibility, and legal relevance can be demonstrated. Nevertheless, the recognition of electronic information as valid evidence should be distinguished from the automatic attribution of perfect evidentiary force to every digital document. Its evidentiary weight depends on compliance with applicable legal requirements, the reliability of the electronic system, and the ability to establish that the submitted information has not been altered or manipulated. Accordingly, FinTech operators must maintain adequate electronic recordkeeping mechanisms, reliable authentication procedures, and appropriate system security to preserve the evidentiary integrity of digital contracts. These safeguards are essential not only for protecting the legal interests of contracting parties but also for ensuring that electronic agreements can provide an effective basis for resolving civil disputes within Indonesia's evolving digital financial ecosystem.

Table 1. Digital Contract Validity Framework Matrix

Legal Indicators	**Formal & Sharia Comparative Framework**
Legal Basis	KUHPerdata Pasal 1320 vs Fatwa DSN-MUI No. 117/2018
Form of Agreement	Certified Electronic Signatures (TTE) vs. Digital Ijab-Qabul (Declaration and Acceptance/ *Sighat*)
Identity Verification	e-KYC & Dukcapil vs. Legal Capacity (Ahliyah)
Substance of the Contract	A Lawful Basis (Causa) Free from Riba, Gharar, and Maysir

Analysis of Sharia Economic Law and the Concept of the Legal Council

From the perspective of Islamic Economic Law (*Fiqh Muamalah*), the legal permissibility of digital contracts is fundamentally grounded in the general jurisprudential maxim: *Al-ashlu fil-mu'amalat al-ibahah hatta yadulla ad-dalilu 'ala tahrimiha*, which establishes that all forms of commercial and transactional activities are presumptively permissible unless a valid Sharia argument demonstrates their prohibition. This principle provides a fundamental normative foundation for accommodating technological innovations within contemporary Islamic financial practices. Unlike acts of worship (*ibadah*), which are generally subject to specific textual prescriptions, commercial transactions (*muamalah*) allow a broader scope of adaptation in response to changing social, economic, and technological circumstances. Accordingly, the utilization of digital platforms, electronic documentation, and technology-mediated

communication does not inherently invalidate a contractual relationship under Islamic law. Rather, the legal assessment must focus on the substantive characteristics of the transaction, the fulfillment of contractual requirements, and the absence of elements prohibited by Sharia. In the context of Sharia-based FinTech, this jurisprudential principle provides the legal flexibility necessary to integrate digital transaction mechanisms into Islamic financial services while ensuring that technological developments remain consistent with the fundamental objectives and normative boundaries of Islamic commercial law.

The validity of a contract under Islamic jurisprudence is determined by the fulfillment of its essential elements (*arkan al-aqd*) and the corresponding legal conditions (*shurut al-aqd*). In general, the fundamental elements of a contractual relationship comprise the contracting parties (*al-aqidain*), the subject matter of the transaction (*ma'qud 'alaih*), and the contractual expression (*sighat*), which consists of an offer (*ijab*) and acceptance (*qabul*). Each element performs a distinct legal function in establishing the legitimacy and enforceability of an agreement. The contracting parties must possess the requisite legal competence (*ahliyah al-ada'*), meaning that they must have the capacity to undertake legally recognized acts in accordance with Islamic jurisprudential requirements, including the relevant standards concerning mental soundness and discernment (*tamyiz*). The subject matter must also be sufficiently identifiable, legally permissible, and capable of being delivered or implemented in accordance with the nature of the transaction. Meanwhile, the contractual expression must demonstrate a clear and mutually recognized intention to establish a binding legal relationship. Within the Sharia FinTech environment, these requirements are implemented through electronic identification, digital verification, standardized contractual documentation, and online consent mechanisms. Nevertheless, technological authentication should be understood as a means of establishing the identity and intention of the contracting parties rather than an automatic substitute for the substantive requirements of Islamic contractual capacity and validity.

One of the most significant doctrinal challenges concerning digital contracts relates to the interpretation of the unity of the contractual assembly (*ittihad al-majlis*). In classical Islamic jurisprudence, the concept of *majlis al-aqd* is associated with the setting in which the offer and acceptance are exchanged, thereby establishing a coherent contractual process between the parties. Traditional interpretations frequently emphasize the continuity of the contractual interaction and, in certain contractual contexts, the physical presence of the parties within a common assembly. This requirement is intended to ensure that the acceptance genuinely corresponds to the offer and that the contractual intention of each party remains sufficiently clear throughout the formation of the agreement. However, the development of telecommunications and digital transaction systems has challenged the conventional understanding of physical presence as the principal indicator of contractual unity. Contemporary Islamic legal discussions, including the perspectives associated with Wahbah al-Zuhayli and the International Islamic Fiqh Academy (*Majma' al-Fiqh al-Islami*), provide a basis for examining the contractual assembly beyond its exclusively geographical dimension. Within this interpretative development, the concept of *majlis hukmi* offers a framework for understanding contractual interaction conducted through legally recognized electronic communication mechanisms. The essential consideration is therefore not necessarily the physical proximity of the parties, but whether the process of offer and acceptance maintains sufficient continuity, clarity, and legal certainty to establish a valid contractual relationship.

The application of *majlis hukmi* in digital transactions requires a careful assessment of the communication process through which the contractual offer and acceptance are exchanged. In electronic contracting, the offer may be communicated through a digital platform, while acceptance is expressed through an affirmative electronic response, such as selecting an agreement confirmation option or executing an electronic signature. The unity of the contractual assembly may consequently be assessed through the continuity of the communication process, the availability of the contractual offer, and the relationship between the offer and the subsequent acceptance. In synchronous transactions, this continuity may be established through real-time electronic communication, whereas asynchronous transactions require a more contextual examination of the validity period of the offer, the timing of acceptance, and the applicable contractual procedures. Acceptance must correspond to the essential terms of the offer and occur within the relevant period, without circumstances indicating withdrawal, rejection (*i'radh*), or the termination of the contractual interaction. Thus, the absence of physical co-presence does not necessarily constitute an obstacle to contractual validity, provided that the electronic mechanism preserves the substantive functions traditionally fulfilled by the contractual assembly. This interpretation demonstrates how Islamic commercial jurisprudence can accommodate technological developments without abandoning the fundamental requirements of mutual consent, contractual certainty, and the protection of the interests of the contracting parties.

The normative recognition of technology-based financing arrangements is further supported by DSN-MUI Fatwa No. 117/DSN-MUI/II/2018 concerning Information Technology-Based Financing Services Based on Sharia Principles. This fatwa establishes an important Islamic legal reference for the implementation of financial services facilitated by digital platforms, particularly in relation to the contractual relationships and operational mechanisms involved in Sharia-compliant financing. Its regulatory significance lies in recognizing the role of information technology in facilitating financing transactions while requiring the relevant parties and service providers to observe the applicable principles of Islamic commercial law. The framework accommodates various Sharia contractual arrangements, including *Murabahah*, *Mudharabah*, *Musyarakah*, *Ijarah*, and *Qardh*, according to the respective characteristics and legal requirements of each contract. The utilization of electronic documentation and digital communication mechanisms must therefore be assessed in relation to the substantive requirements of the underlying Sharia agreement rather than merely its technological form. Consequently, the fatwa provides a normative foundation for integrating digital contracting into Islamic financial services, while reinforcing the importance of transparency, mutual consent, contractual responsibility, and the avoidance of prohibited elements. In this respect, the development of digital contracts in Sharia FinTech represents not a departure from classical Islamic contractual principles, but an adaptation of their implementation to contemporary technological conditions, provided that the essential requirements and objectives of Sharia are consistently maintained.

Personal Data Protection and the Principles of Maqashid Syariah

The The enactment of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) represents a significant development in Indonesia's legal framework for regulating the collection, processing, storage, transfer, and utilization of personal information within digital financial services. For Financial Technology (FinTech) providers, particularly those operating under Sharia principles, the regulation establishes legal responsibilities to ensure that users'

personal data are processed lawfully, transparently, and securely. These responsibilities extend beyond obtaining consent during user registration and require appropriate organizational and technical safeguards to prevent unauthorized access, disclosure, alteration, loss, or misuse of personal information. In particular, Articles 35 and 36 of the PDP Law establish obligations concerning the security of personal data processing and the prevention of unauthorized access. The law also provides mechanisms for administrative sanctions under Article 57, including written warnings, temporary suspension of processing activities, deletion or destruction of personal data, and administrative fines. Furthermore, Articles 67 and 68 establish criminal liability for specified unlawful activities involving the acquisition, disclosure, use, or falsification of personal data. Consequently, inadequate data protection practices may expose FinTech operators to substantial legal consequences, depending on the nature and circumstances of the violation. These provisions demonstrate that personal data security constitutes an essential element of regulatory compliance and institutional accountability in Indonesia's digital financial ecosystem.

From the perspective of Islamic Economic Law (*Fiqh Muamalah*), personal data protection should not be understood merely as a technical requirement or an administrative obligation imposed by national legislation. Rather, it represents an ethical and normative responsibility derived from the Islamic principle of *al-amanah*, which requires individuals and institutions to preserve and responsibly manage resources and information entrusted to them. When customers provide their personal information to Sharia FinTech platforms, they establish a relationship of trust that obliges service providers to utilize such information only for legitimate, disclosed, and mutually understood purposes. This responsibility is closely connected to the prohibition of betrayal (*khiyanah*) and deceptive conduct (*tadlis*), both of which undermine the ethical foundations of Islamic commercial relationships. The unauthorized distribution of customer information to third parties, particularly when used for intimidation, coercive debt collection, or other harmful purposes, represents a serious violation of these obligations. Such practices may also undermine the principle of mutual consent (*an-taradhin*), as articulated in QS. An-Nisa [4]: 29, which emphasizes that commercial transactions must be conducted through mutual agreement rather than wrongful appropriation or exploitation. Although this Quranic provision primarily addresses the legitimacy of economic transactions, its underlying ethical principle provides a relevant normative foundation for examining whether personal information is processed and utilized in ways that respect the rights, autonomy, and legitimate interests of customers.

The relationship between personal data protection and Islamic legal objectives can be further examined through the framework of *Maqasid al-Shariah*, particularly the preservation of wealth (*hifz al-mal*), life (*hifz al-nafs*), and human dignity and honor (*hifz al-'ird*). Personal information has become increasingly interconnected with individuals' financial security, social identity, reputation, and economic opportunities. Accordingly, its unauthorized disclosure or exploitation may generate consequences extending beyond the immediate violation of privacy, including financial losses, identity theft, reputational damage, psychological distress, and exposure to coercive practices. From this perspective, protecting personal data contributes to the preservation of wealth by preventing financial fraud and unauthorized transactions, while also safeguarding human dignity and personal security against harmful disclosure and exploitation. Suhendar and Ulum (2023), in their study of personal data protection in Sharia FinTech lending through Jasser Auda's systems approach to *Maqasid al-Shariah*, demonstrate that the protection of users' personal information is closely associated with justice, human

rights, and the ethical responsibilities of digital financial service providers. Similarly, Fauzi et al. (2026), examining personal data protection in digital payment services, emphasize the relevance of *hifz al-mal* and *amanah* in establishing the responsibility of digital service providers to safeguard customers' financial interests and personal information. These perspectives indicate that personal data protection is not an external consideration detached from Islamic financial principles but an integral dimension of the broader objectives of Sharia.

Recent scholarship further reinforces the argument that the governance of personal information in Islamic financial technology requires the integration of legal compliance, institutional accountability, and Sharia-based ethical standards. Miskam, Mohd Shahwahid, and Sholehuddin (2025), in their comparative examination of personal data protection within Sharia-compliant investment platforms, identify significant privacy, security, and governance challenges arising from the extensive use of personal and financial datasets in technology-driven investment services. Their analysis highlights the importance of combining personal data protection regulations with Sharia governance mechanisms to maintain investor confidence while supporting technological innovation. More recently, Sanusi et al. (2026) argue that personal information within Islamic FinTech social finance should be regarded as an entrusted responsibility rather than merely a digital asset subject to statutory protection. Their proposed Maqasid-based governance framework connects data privacy with institutional accountability, cybersecurity governance, justice (*'adl*), public welfare (*maslahah*), and the preservation of human dignity and wealth. These findings are consistent with the earlier analysis of Suhendar and Ulum (2023), although they also demonstrate that regulatory compliance alone may not sufficiently address the broader ethical dimensions of personal data governance. Nevertheless, these studies do not establish that every cybersecurity failure automatically constitutes a violation of Sharia or invalidates an underlying contract. Rather, the legal and ethical implications must be assessed according to the nature of the breach, the responsibilities of the data controller, the resulting harm, and the relevant contractual and regulatory obligations.

Accordingly, the reliability of cybersecurity systems within Sharia FinTech platforms should be regarded as an essential supporting safeguard for maintaining the integrity, legitimacy, and sustainability of digital contractual relationships. Effective data governance requires more than the adoption of technological security measures; it also necessitates institutional policies governing data collection, purpose limitation, access authorization, retention, disclosure, and incident response. These measures should be implemented in accordance with the PDP Law while reflecting the ethical requirements of *amanah*, transparency, justice, and the prevention of harm (*darar*). Within the framework of *Maqasid al-Shariah*, cybersecurity can therefore be understood as an operational mechanism for realizing the objectives of protecting wealth, dignity, and personal security in digitally mediated financial relationships. Its position is best understood as a complementary condition supporting contractual integrity (*syarat takmili*), rather than an independent pillar of contract formation under classical Islamic jurisprudence. A digital agreement may satisfy the formal requirements of contractual validity, yet weaknesses in data protection can still undermine the trust, fairness, and practical security necessary for its proper implementation. Consequently, the integration of statutory data protection obligations and Sharia-based ethical governance is indispensable for establishing a digital financial environment that is not only legally compliant but also trustworthy, accountable, and consistent with the fundamental objectives of Islamic law.

Conclusion

Digital contracts on Sharia FinTech platforms have legal standing and are fully binding under both Indonesian positive law (Civil Code, ITE Law, PP PSTE, and PDP Law) and Sharia Economic Law (DSN-MUI Fatwa No. 117/2018). Formally, Electronic Signatures and digital documents are recognized as valid legal evidence. Under Sharia law, the absence of physical face-to-face contact is legally accommodated through the majlis hukmi doctrine without diminishing the essence of willingness (an-taradhin). This research recommendation requires regulators (OJK and BI) to tighten cyber audit supervision and ensure transparency of digital standard agreement clauses. Sharia FinTech providers are required to implement strict personal data protection standards to safeguard customer interests.

References

Arsyad, M., & Basri, A. (2024). Traditional and modern maritime economic systems in Indonesia. Historia: Jurnal Pendidik dan Peneliti Sejarah, 8(3), 563–576. https://doi.org/10.29408/fhs.v8i3.36587

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). SAGE Publications.

DSN-MUI. (2018). Fatwa DSN-MUI No. 117/DSN-MUI/II/2018 tentang Layanan Pembiayaan Berbasis Teknologi Informasi Berdasarkan Prinsip Syariah. Dewan Syariah Nasional Majelis Ulama Indonesia.

Fauzi, I. M., Nurfatwa, F., Sandiana, D. S. R., Anjani, R. D., Fawwaz, M. N., Latifa, M., & Wijaya, T. (2026). Tinjauan Maqashid Syariah terhadap Perlindungan Data Pribadi Nasabah Pada Digital Payment. https://doi.org/10.64994/silah.v3i1.78

Mansurnoor, A. (2021). Hukum Transaksi Digital Syariah di Indonesia. Rajawali Pers.

Miskam, S., Mohd Shahwahid, F., & Sholehuddin, N. (2025). Safeguarding Personal Data in Islamic Fintech: A Comparative Review of Shariah-Compliant Investment Platforms. Malaysian Journal of Information and Communication Technology, 10(2), 55–68. https://doi.org/10.53840/myjict10-2-234

Punch, K. F. (2014). Introduction to social research: Quantitative and qualitative approaches (3rd ed.). SAGE Publications.

Putri Relina, R., Sakti, A., & Tolapa, M. (2025). Digital regulatory dynamics in Indonesian financial technology. Geoforum, 158, 103892. https://doi.org/10.1016/j.geoforum.2024.103892

Republik Indonesia. (1945). Kitab Undang-Undang Hukum Perdata (KUHPerdata).

Republik Indonesia. (2008). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara RI Tahun 2008 No. 58.

Republik Indonesia. (2019). Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lembaran Negara RI Tahun 2022 No. 207.

Sakti, A., Arsyad, M., & Hasniah, H. (2026). Capital structure and legal protection in digital trade. Journal of Rural Studies, 112, 103120. https://doi.org/10.1016/j.jrurstud.2025.103120

Sanusi, S. W. S. A., Sholehuddin, N., Mohd Puad, N. A., Miskam, S., Robbani, H., Putranto, R. D., & Syam, R. (2026). Reconstructing Data Privacy Governance in Islamic Fintech Social

Finance in Malaysia and Indonesia through Maqasid al-Shariah. Journal of Muwafaqat, 9(2), 121–148. https://doi.org/10.53840/k77xzq93

Subekti, R. (2010). Hukum Perjanjian. Intermasa.

Suhendar, H., & Ulum, M. (2023). Perlindungan data pribadi penyelenggaraan fintech lending syariah: Analisis teori sistem Maqashid Syariah Jasser Auda. El Hisbah: Journal of Islamic Economic Law, 3(1). https://doi.org/10.28918/elhisbah.v3i1.918

Zuhayli, W. (2002). Al-Fiqh al-Islami wa Adillatuh. Dar al-Fikr.