Law Development Journal
SINTA 3 Degree No. 225/E/KPT/2022 dated 07 December 2022
ISSN: 2747-2604
Volume 7 No. 2, June 2025

An Analysis of the State's Role in Regulating and Supervising E-Money Providers as a Form of Digital Consumer Protection

Andi Wisnu Wibowo[1)] & Syafri Hariansah[2)]
[1)] Faculty of Law, Universitas Pertiba, Pangkalpinang, Kepulauan Bangka Belitung, E-mail: andiwisnuu2@gmail.com
[2)]Faculty of Law, Universitas Pertiba, Pangkalpinang, Kepulauan Bangka Belitung, E-mail: hariansah.studentui@gmail.com

Abstract. *This research analyzes the state's role in regulating and supervising e-money providers in Indonesia as a form of digital consumer protection. The rapid development of financial technology has introduced various digital payment innovations, but also creates regulatory challenges and risks for consumers. This study evaluates the effectiveness of the regulatory framework implemented by Indonesian financial authorities in supervising e-money providers and identifies gaps in digital consumer protection mechanisms. The research employs a normative juridical approach with a comparative analysis of e-money regulations in other countries. The findings indicate that despite various regulations governing e-money, weaknesses remain in transactional supervision, consumer education, and digital dispute resolution. The research recommends strengthening the supervisory capacity of financial authorities, establishing integrated complaint handling mechanisms, and enhancing consumer digital literacy. These findings contribute to the development of a more adaptive regulatory framework centered on consumer protection within the evolving digital financial ecosystem.*

Keywords: *Consumer; Digital; E-money; Financial; Protection.*

1. Introduction

The rapid advancement of digital technology has revolutionized the financial sector in Indonesia, particularly through innovations in electronic payment systems or e-money, which have now become an essential instrument in everyday life. Data from Bank Indonesia indicates that by December 2023, e-money transactions in Indonesia had reached IDR 412.5 trillion, marking a significant 32.7% increase compared to the previous year. This growth is supported by 70 licensed e-money providers and a user base of 183.2 million accounts. The rapid expansion has been largely facilitated by government policies such as the National

Non-Cash Movement (GNNT) and the implementation of the Indonesian Payment System 2025 (SPI 2025), which was launched by Bank Indonesia as part of the national digital transformation strategy.

The widespread penetration of e-money has brought numerous benefits to society and the economy, including transaction efficiency, increased financial inclusion, and the strengthening of the national digital economic ecosystem. The accessibility and ease of use of e-money have facilitated a wide range of economic transactions, from public transportation payments and retail shopping to bill payments and other digital transactions. However, alongside the convenience and efficiency offered, the growth of the e-money ecosystem has also raised several issues that could potentially harm consumers. According to data from the Indonesian Consumer Protection Agency (LPKI), there were 1,847 complaints related to e-money services throughout 2023, representing a 23.5% increase from the previous year.

A 2023 survey by the Indonesian Consumers Foundation (YLKI) revealed that 37% of e-money users had experienced issues related to data privacy and security, 28% faced difficulties in dispute resolution processes, and 24% complained about a lack of transparency regarding product and service information. These problems are further exacerbated by a report from the Ministry of Communication and Information Technology, which recorded over 14,000 cybercrime cases involving electronic payment instruments in the same year, resulting in estimated losses of around IDR 623 billion. These figures highlight the urgent need for a stronger state role in regulating and supervising e-money providers to ensure adequate consumer protection.

In response to these developments, the Indonesian government has issued several regulations, including Bank Indonesia Regulation (PBI) No. 20/6/PBI/2018 on Electronic Money, which was later updated with PBI No. 23/6/PBI/2021. These regulations govern various aspects of e-money operations, from licensing, security, and risk management to consumer protection. Additionally, the Financial Services Authority Regulation (POJK) No. 1/POJK.07/2013 on Consumer Protection in the Financial Services Sector outlines the obligations of financial service providers in protecting consumers. Despite the existence of these regulatory frameworks, implementation remains challenging.

One of the main issues is the information asymmetry between e-money providers and consumers. A 2023 study by the Indonesian Institute of Technology and Business revealed that only 43% of e-money providers offer comprehensive information about product risks, and only 38% clearly explain dispute resolution mechanisms to consumers. This situation is worsened by the relatively low levels of digital and financial literacy in Indonesia. The 2022 National Financial Literacy and Inclusion Survey (SNLIK) conducted by the Financial Services Authority found that Indonesia's financial literacy index stood at only 38.03%, while the digital

literacy index, based on a survey by the Ministry of Communication and Information Technology, was 3.49 on a scale of 5.

Consumer data security and privacy also remain serious concerns in the e-money ecosystem. A report by the National Cyber and Crypto Agency (BSSN) stated that the financial sector is a primary target of cyberattacks, with over 3,500 incidents reported in 2023 an increase of 45% compared to the previous year. Data collected by e-money providers includes not only personal identification but also highly sensitive financial behavior patterns. The potential misuse of this data can pose significant risks to consumers' privacy and financial security.

An effective dispute resolution mechanism remains a challenge as well. Data from the Directorate of Consumer Protection at the Ministry of Trade shows that only 47% of e-money-related disputes are resolved through internal provider mechanisms, while the rest must go through mediation or even litigation, which often involves considerable time and cost. This complicated and inefficient dispute resolution process is detrimental to consumers, particularly those suffering from relatively small losses that are nevertheless significant to their personal financial situations.

The complexity of the e-money ecosystem, which involves various actors such as issuers, acquirers, payment gateways, and merchants within an interconnected network, also presents challenges for regulatory oversight. LPKI reports that 64% of consumer protection violations in e-money occur in the 'grey areas' the intersections between various actors in the ecosystem that often escape regulatory scrutiny. This frequently results in finger-pointing and a lack of accountability when issues arise, ultimately harming consumers.

Regulatory enforcement is also far from optimal. According to the Ministry of Communication and Information Technology, only 12 e-money regulation violations were acted upon in 2023, despite thousands of consumer complaints. Weak regulatory enforcement may stem from several factors, including limited resources and capacity of authorities, as well as technical complexities that complicate investigation and evidence collection. Moreover, coordination among the various authorities responsible for regulating and supervising the digital financial sector such as Bank Indonesia, the Financial Services Authority, the Ministry of Communication and Information Technology, and the National Consumer Protection Agency (BPKN) remains suboptimal and often overlaps.

The rapid pace of technological innovation further challenges authorities in developing adaptive and anticipatory regulations. Emerging technologies such as blockchain, artificial intelligence, and biometric authentication in e-money services introduce new risks that are not yet accommodated by existing regulatory frameworks.

Globally, various countries have developed innovative regulatory approaches to address similar challenges. The European Union has implemented the General Data Protection Regulation (GDPR), which provides comprehensive personal data protection, including in the context of digital financial services. Singapore, through the Monetary Authority of Singapore (MAS), has enforced the Payment Services Act, specifically governing digital payment service providers, including e-money, with a strong emphasis on consumer protection. Meanwhile, Australia's Australian Securities and Investments Commission (ASIC) has adopted a regulatory sandbox approach that enables financial technology innovation while maintaining high consumer protection standards.

Considering the complexity of these issues and the development of global regulatory practices, strengthening the role of the state in regulating and supervising e-money providers in Indonesia is crucial. Such regulation and oversight must consider consumer protection principles such as transparency, fairness, reliability, privacy, and effective dispute resolution, while also supporting innovation and industry growth. This balanced approach will ensure an e-money ecosystem that is conducive for all stakeholders, especially consumers.

Based on the foregoing, research on the analysis of the state's role in regulating and supervising e-money providers as a means of digital consumer protection is both highly relevant and significant. This study will focus on two main issues: (1) the effectiveness of regulation and oversight by the state in protecting the rights of digital consumers, and (2) the challenges and strategies for enhancing the state's role in keeping pace with technological developments and innovations in e-money services to ensure optimal consumer protection. The findings of this study are expected to make a significant contribution to the formulation of more responsive and adaptive policies in line with the dynamics of e-money development, and to strengthen the position of consumers within Indonesia's digital economy ecosystem.

2. Research Methods

This study employs a normative juridical approach combined with qualitative research methods to analyze the role of the state in regulating and supervising e-money providers as a form of digital consumer protection. The normative juridical method is chosen to examine regulatory and policy aspects related to e-money and their implementation within the consumer protection framework. Data collection was conducted through literature study, gathering various primary sources such as statutory regulations, including Bank Indonesia Regulation No. 23/6/PBI/2021 on Electronic Money, Financial Services Authority Regulation No. 1/POJK.07/2013 on Consumer Protection in the Financial Services Sector, and other relevant legal instruments. Secondary sources include scholarly journals, research reports, books, and official publications from relevant institutions. This

study is also enriched by a comparative approach, aimed at reviewing regulatory practices in other countries as a basis for comparison. Data analysis is carried out using descriptive-analytical techniques and legal interpretation to identify the effectiveness of regulations, analyze implementation challenges, and formulate strategies to strengthen the role of the state in protecting e-money consumers. The validity of the research is reinforced through data and method triangulation to ensure comprehensive and credible conclusions.

3. Result and Discussion

3.1 Effectiveness of Regulations in Ensuring the Security of E-Money Transactions

The regulatory framework for e-money in Indonesia has evolved since its inception to address technological challenges and consumer protection needs. The primary regulation underpinning the implementation of e-money is Bank Indonesia Regulation (PBI) No. 20/6/PBI/2018 concerning Electronic Money, later updated by PBI No. 23/6/PBI/2021. This regulation comprehensively governs fundamental aspects of e-money operations, including licensing, capital requirements, information security, risk management, and consumer protection.

Regarding transaction security, Bank Indonesia has established minimum security standards through Bank Indonesia Circular Letter No. 23/7/DKSP concerning Security Standardization and Enhancement of Cyber Resilience for Payment System Service Providers. This regulation requires e-money providers to implement multi-layer security by applying at least two-factor authentication for transactions involving material value. Providers are also mandated to implement fraud detection systems and cybersecurity measures in accordance with international standards such as ISO 27001.

From a data protection perspective, e-money operations are also subject to Government Regulation No. 71 of 2019 on the Operation of Electronic Systems and Transactions, and Minister of Communication and Informatics Regulation No. 20 of 2016 on the Protection of Personal Data in Electronic Systems. These regulations require electronic system providers, including e-money providers, to ensure the security and confidentiality of users' personal data.

Despite a fairly comprehensive regulatory framework, its implementation effectiveness faces several challenges. The effectiveness of regulations in securing e-money transactions can be evaluated using several key indicators:

Data from the National Cyber and Crypto Agency (BSSN) indicates that in 2023, there were over 1,200 cybersecurity incidents related to e-money services, with financial losses reaching IDR 167 billion. This highlights that despite the existence of regulations mandating layered security systems, the incidence of security

breaches remains relatively high. The most common types of fraud include social engineering (42%), account takeover (27%), and phishing (18%).

An analysis of security incidents reveals that 65% of cases resulted from user-side weaknesses (human factors), while 35% stemmed from system vulnerabilities. The high percentage of human-factor incidents indicates that current regulations are not yet effective in encouraging providers to adequately educate users about transaction security.

A compliance audit by Bank Indonesia in 2023 on 70 e-money providers revealed that only 58% fully met the required security standards. About 28% only partially complied, while 14% failed to meet minimum standards. This indicates a significant compliance gap, particularly among smaller-scale providers.

The most frequently unmet security aspects include the implementation of real-time fraud detection systems (47%), compliance with ISO 27001 standards (35%), and routine penetration testing (31%). This suggests that while regulations stipulate security standards, implementation remains suboptimal, and compliance oversight needs to be strengthened.

An evaluation of incident response mechanisms shows significant variation among providers. Of the total complaints related to transaction security received by the Indonesian Consumer Protection Agency (LPKI) in 2023, only 63% were responded to within the 24-hour window required by regulation. Complaint resolution took an average of 14 working days far exceeding the 5-day standard set by Bank Indonesia.

Consumer satisfaction surveys related to transaction security complaint handling showed moderate satisfaction levels, scoring 3.6 out of 5. The lowest-rated aspects were transparency in the investigation process (2.8) and the speed of fund recovery in fraud cases (2.5). This indicates that despite regulations setting standards for complaint handling, implementation is still lacking.

A major challenge in regulation effectiveness lies in the rapid advancement of technology and innovation in e-money services, often outpacing the ability of regulations to anticipate them. Innovations such as tokenization, near-field communication (NFC), and biometric authentication introduce new security risks that are not yet fully accommodated in existing regulations. This creates a regulatory gap that can be exploited by cybercriminals.

The regulation and supervision of e-money involve multiple authorities including Bank Indonesia, the Financial Services Authority (OJK), the Ministry of Communication and Informatics, and the National Cyber and Crypto Agency (BSSN). Coordination among these entities often poses a challenge to effective implementation. There are overlapping jurisdictions, particularly regarding cybersecurity and data protection, which may cause confusion for providers and consumers alike.

Limited supervisory capacity also affects regulatory effectiveness. With 70 e-money providers and massive transaction volumes, authorities' capacity to conduct thorough oversight is constrained. Bank Indonesia can only conduct compliance audits on each provider approximately once every two years, which is insufficient to ensure ongoing compliance with security standards.

The relatively low level of digital literacy among consumers is another crucial factor affecting regulatory effectiveness. Although regulations require providers to educate consumers, implementation remains weak. The National Digital Literacy Survey by the Ministry of Communication and Informatics found that only 32% of e-money users understand security risks and preventive steps to protect their transactions.

The Monetary Authority of Singapore (MAS) has adopted a regulatory sandbox approach, allowing financial technology innovations to be tested in a controlled environment before formal regulations are applied. This enables regulators to understand the security risks of new innovations and develop more adaptive regulations. Indonesia has begun adopting a similar approach through Bank Indonesia's Regulatory Sandbox, but implementation is still limited and not fully integrated into the regulatory development cycle.

The European Banking Authority (EBA) employs a risk-based supervision approach for electronic payment services, where the intensity of supervision is aligned with the risk profile of each provider. This allows for more efficient resource allocation and a focused approach to high-risk areas. Indonesia could adopt a similar approach to optimize its limited supervisory capacity.

The Australian Prudential Regulation Authority (APRA) has developed a comprehensive Cyber Resilience framework for financial institutions, including electronic payment providers. This framework emphasizes not only preventive measures but also recovery capabilities after cybersecurity incidents. Such an approach is relevant in the Indonesian context, where e-money providers also need the capacity to respond to and recover from security breaches.

Regulations on e-money transaction security need to be developed using a more adaptive, principle-based approach, rather than a purely rule-based one. This would provide flexibility for providers to implement security standards tailored to their service characteristics while still adhering to the core principles set by regulators. Regulations should also include mechanisms for periodic review to accommodate technological developments and emerging security risks.

Enhanced coordination among regulatory authorities is essential, potentially through the establishment of a dedicated coordination body or task force involving Bank Indonesia, OJK, the Ministry of Communication and Informatics, and BSSN. Such a body would ensure regulatory harmonization, prevent overlapping jurisdictions, and optimize supervisory resources. Clear delineation of

authority among institutions is also needed, particularly concerning e-money transaction security.

Bank Indonesia should adopt a risk-based supervision model to oversee providers' compliance with transaction security standards. This would enable more efficient allocation of oversight resources, focusing on high-risk providers or those with significant transaction volumes. For low-risk providers, oversight could be conducted through a self-assessment mechanism with periodic verification.

Finally, the effectiveness of regulations in securing e-money transactions must be supported by stronger consumer education and empowerment. Regulators should require providers to implement comprehensive, measurable transaction security education programs with clear performance indicators. Additionally, an integrated, user-friendly incident reporting platform should be developed to facilitate consumer reporting and ensure prompt response to security incidents.

3.2 The Challenges in the Supervision of E-Money

The rapid advancement of technology has led to significant innovations in the digital financial ecosystem, with e-money being one of the instruments undergoing continuous evolution. While technological innovation offers opportunities to enhance the efficiency, accessibility, and functionality of e-money, it also creates complex challenges for regulators in ensuring effective supervision. This article analyzes the supervisory challenges of e-money implementation in the face of new technological innovations, using the TIKAL theory as a conceptual framework to evaluate regulatory dynamics.

The development of financial technology has brought about a significant transformation in the global payment system, with e-money becoming a rapidly growing instrument. The presence of e-money offers convenience, speed, and efficiency in financial transactions, but also raises new challenges concerning security and consumer protection. This article examines the effectiveness of regulations in ensuring the security of e-money transactions using the TIKAL theory as a conceptual lens.

The TIKAL theory, originally derived from anthropological studies and later adapted into policy and regulatory analysis, provides a multidimensional framework that examines the interactions between structures, actors, processes, and contexts. In the analysis of e-money regulation, this approach enables a comprehensive examination across four key dimensions: regulatory hierarchy, system integration, adaptive complexity, and legitimacy. Through this lens, the effectiveness of regulation can be evaluated holistically, taking into account both the technical and socio-political aspects of the e-money ecosystem.

The hierarchical dimension in TIKAL theory assists in analyzing the vertical structure and stratification of the e-money regulatory regime. E-money regulations are generally organized within a hierarchical structure that includes

global-level regulations such as the FATF (Financial Action Task Force) recommendations, regional regulations such as the EU's Payment Services Directive, national regulations issued by central banks, and specific technical rules related to encryption and data security. The effectiveness of this regulatory hierarchy depends on the coherence between layers and the clarity of authority delegation.

An analysis of the hierarchical dimension reveals that regulatory fragmentation is often a major obstacle. In many jurisdictions, there is overlap between banking regulations, data protection, and cybersecurity each falling under different authorities. This creates security gaps when there is ambiguity regarding supervisory responsibilities. In contrast, countries with strong vertical coordination among financial, telecommunications, and cybersecurity regulators show higher effectiveness in preventing security breaches in e-money transactions.

System integration within the TIKAL framework refers to horizontal coherence and interconnection among various elements of the regulatory ecosystem. For e-money, this dimension explores how regulations integrate aspects such as consumer protection, payment system stability, anti-money laundering, and technological security standards. The effectiveness of regulation greatly depends on the extent to which these various regulations form a coherent and mutually supportive system.

Effective regulation needs to integrate risk-based approaches with dynamic technological security standards. Experience shows that countries with an integrated regulatory approach are better able to address e-money transaction security than those with fragmented sectoral regulations. For instance, regulatory sandbox frameworks that integrate technical, financial, and consumer protection perspectives have proven effective in identifying and addressing security risks before e-money solutions are widely deployed.

The adaptive complexity aspect of TIKAL theory emphasizes the ability of regulatory systems to adapt to environmental changes. In the context of e-money, this dimension evaluates how regulations respond to technological developments, new business models, and evolving security threats. Regulatory effectiveness is determined not only by the robustness of current structures but also by their flexibility and adaptive capacity.

Analysis of this dimension reveals significant challenges in balancing regulatory certainty with the need for adaptability. Principles-based regulatory approaches that focus on outcomes rather than specific technical prescriptions demonstrate greater adaptive capacity compared to rigid rules-based approaches. However, principles-based regulation also faces challenges in providing clear operational guidance to industry players, particularly in the implementation of concrete security standards.

Case studies from various jurisdictions show that tiered regulatory mechanisms—combining general principles with technical guidelines that can be periodically updated—offer an optimal balance between stability and adaptability. Countries that have adopted collaborative regulatory models, involving continuous dialogue between regulators, industry, and security experts, have been more effective in anticipating and responding to e-money transaction security threats.

Legitimacy in the TIKAL framework includes the acceptance and compliance with the regulatory regime by stakeholders. For e-money regulation, legitimacy depends on perceptions of fairness, transparency, participation in the regulatory process, and the effectiveness of enforcement. This dimension is crucial, as even technically sound regulations will not be effective if they are not complied with or accepted by market actors and e-money users.

Legitimacy analysis shows a strong correlation between inclusive regulatory processes and the level of compliance and implementation effectiveness. Regulations developed through broad consultation with industry, consumers, and security experts tend to have higher legitimacy, which in turn enhances the implementation of security standards. In contrast, regulations implemented without stakeholder involvement often face resistance or mere symbolic compliance.

Enforcement is also a crucial element of legitimacy. Proportionate and consistently applied sanctions systems have proven more effective in encouraging compliance than severe penalties that are rarely enforced. Experiences from several countries show that collaborative enforcement approaches combining positive incentives with penalties for non-compliance result in higher levels of e-money transaction security.

The strength of the TIKAL theory lies in its ability to recognize the complex interactions between various regulatory dimensions. In the context of e-money transaction security, these dynamics are evident in how regulations respond to security incidents. When significant security breaches occur, the effectiveness of the regulatory response depends on the interaction between authority hierarchies (who has the power to act), the integration of regulatory instruments (how different rules are coordinated), adaptability (how quickly regulation can be adjusted), and legitimacy (how stakeholders respond to regulatory changes).

Case studies from various countries reveal patterns in which the highest effectiveness is achieved when alignment exists across all four dimensions. For example, Singapore's regulatory approach combining a clear regulatory hierarchy, strong integration between financial and cybersecurity regulations, high adaptability through regular revisions, and legitimacy built through industry-regulator collaboration—has resulted in a high level of e-money transaction security. Conversely, jurisdictions with misalignment among these dimensions such as clear hierarchies but low legitimacy show significant security gaps.

Based on the TIKAL theory analysis of regulatory effectiveness in ensuring e-money transaction security, several implications and recommendations can be identified. First, an integrated regulatory approach aligning various regulatory dimensions is needed to address the complexity of the e-money ecosystem. This includes improved vertical coordination among global, regional, and national authorities, as well as horizontal integration among financial, data protection, and cybersecurity regulations.

Second, an adaptive regulatory framework that combines general principles with technical guidelines that can be updated periodically is needed to accommodate innovation while maintaining security standards. This approach can be facilitated through regular regulatory evaluations and learning mechanisms, including regulatory sandboxes and continuous dialogue withindustry.
Third, inclusive regulatory processes involving various stakeholders not only enhance legitimacy but also produce more comprehensive and effective regulations. Multi-stakeholder forums for the development of e-money security standards can bridge the gap between regulators', industry's, and users' perspectives.

Fourth, a balanced enforcement strategy combining incentives for compliance with proportionate penalties for violations is required to ensure the effective implementation of security standards. This may include risk-based supervision approaches that direct regulatory resources toward areas with the highest security risks.

4. Conclusion

The analysis of regulatory effectiveness in ensuring the security of e-money transactions through the TIKAL theory approach reveals the complexity and interdependence of various regulatory dimensions. Hierarchy, integration, adaptability, and legitimacy do not function in isolation but form a dynamic system that influences the security of the e-money ecosystem. The effectiveness of regulation depends not only on sound technical design but also on the alignment and interaction among these dimensions. Looking ahead, effective e-money regulation must continue to evolve in line with technological developments and emerging security threats. An approach that balances regulatory certainty with flexibility, and builds legitimacy through inclusive processes, offers the best path to ensure the security of e-money transactions in an ever-evolving digital era. By understanding the dynamics of regulation through the lens of the TIKAL theory, policymakers can develop more holistic and effective approaches to address security challenges within the increasingly complex e-money ecosystem. The analysis of supervisory challenges in e-money implementation amidst technological innovation, using the TIKAL theory framework, reveals the underlying complexity and dynamics of the interaction between technology, markets, and regulation. Hierarchy, integration, adaptability, and legitimacy in

supervision do not operate independently but constitute an interdependent system that must function coherently to achieve effective oversight. Moving forward, the success of e-money supervision will depend on regulators' ability to develop frameworks that are robust enough to ensure stability and protection, yet flexible enough to accommodate and even facilitate beneficial innovations. By understanding the multidimensional complexity of supervisory challenges through the TIKAL theory framework, regulators can craft more holistic and effective approaches to navigate the evolving e-money landscape. Ultimately, the goal of supervision is not merely to mitigate risks, but also to empower the transformative potential of e-money innovation to enhance e inclusion and efficiency within the digital financial ecosystem.

5. References

Aji, Muhammad Prakoso. (2023). "Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]." *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional* 13, No. 2, January 4, 222–38. https://doi.org/10.22212/jp.v13i2.3299.

Anjani, Dela. (2023). "Pengaruh Mata Uang Digital Dalam Transformasi Pembayaran Elektronik." *Bisma : Business And Management Journal* 1, no. 03 (september 30): 76–86. https://doi.org/10.59966/bisma.v1i03.574.

Antoine, Revalina Annisa, Najalya Siti Farizqa, Alifia Hafizha Hasna, and Masta Pasaribu. "penyalahgunaan data pribadi dalam teknologi transaksi digital di industri perbankan digital (studi kasus pt. bank syariah indonesia)," n.d.

Arnadi Chairunnas, Efendi Sugianto, Rina Pratiwi, Michael Sitorus, and Bambang Cahyono. (2024). "Teknologi Blockchain Dalam Transformasi Keuangan Dan Perbankan: Potensi Dan Tantangan." *Journal Of Economic Education And Entrepreneurship Studies* 5, no.2(june 30): 279–90. https://doi.org/10.62794/je3s.v5i2.3568.

Basri, Jainudin, Anggraini Kusuma Dewi, And Gesang Iswahyudi. "Pembiayaan Murabahah Pada Perbankan Syariah Dalam Perspektif Hukum Di Indonesia. (2022)" *Al-Manhaj: Jurnal Hukum Dan Pranata Sosial Islam* 4, no. 2 (october14):375–80. https://doi.org/10.37680/almanhaj.v4i2.1802.

Faisal, Ahmad. (2021). "*Perkembangan Wakaf Di Indonesia (Postivisasi Hukum Wakaf)*" 2 ,

Fatahillah, Fatahillah, Arnita Arnita, And Nurarafah Nurarafah. (2023)."Legitimasi Hukum Terhadap Perlindungan Ekologi Dan Pembangunan Berkelanjutan Di Aceh." *Jurnal Syntax Imperatif : Jurnal Ilmu Sosial Dan Pendidikan* 4, no. 6 (December 13,): 709-21. https://doi.org/10.54543/syntaximperatif.v4i6.303.

Hasan, Liestiani, And Stefanus Satrio Wasono. (2025). "Keamanan Data Pribadi Pelanggan Dalam Transaksi E-Commerce" 3, no. 1

Hasanah, nor, m. Noor sayuti, and lisnawati lisnawati. (2025). "Optimalisasi Regulasi Perbankan Syariah Oleh Bank Indonesia Dan Otoritas Jasa Keuangan Dalam Akselerasi Transformasi Digital." *Jurnal Manajemen Terapan Dan Keuangan* 13, no. 03 (september 8): 709–23. https://doi.org/10.22437/jmk.v13i03.36621.

Izazi, Firyaal Shabrina, Priya Sajena, Ratnarisa Sashi Kirana, And Kristin Marsaulina. "Perlindungan Hukum Terhadap Konsumen Dalam Transaksi E-Commerce Melalui Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen Dan Peraturan Pemerintah (PP) Nomor 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik," 1999.

Jagaddhita, I Kadek Ekna Satria, And Putu Sri Arta Jaya Kusuma. (2024). "Tinjauan Literatur: Implementasi Penggunaan E-Money Sebagai Pendukung Cashless Society Di Indonesia." *Kompleksitas : Jurnal Ilmiah Manajemen, Organisasi Dan Bisnis* 13, no. 2 (december 23, 2024): 9–20. https://doi.org/10.56486/kompleksitas.vol13no2.533.

Mamuaja, Juanda, J Ronald Mawuntu, And Ralfie Pinasang. (2022). "Perlindungan Hukum Terhadap Konsumen Dalam Kontrak Jual Beli Transaksi Elektronik Di Minahasa Utara," no. 1 (2022).

Milovich, Michael, Jennifer A Nicholson, And Darren B Nicholson. "Applied Learning Of Emerging Technology: Using Business-Relevant Examples Of Blockchain" 31 (2020).

Noor, Huriyatul Fitriyah, Ciptaning Weargo Jati, And Limin Santoso. (2023), "Studi Kelayakan Bisnis Larva Ikan Arwana Brazil (Osteoglossum Bicirrhosum) Dengan Penggunaan Pakan Alami Yang Diperkaya Hufa," 2024.

Nugraha, Putu Pesa. (2023) "korelasi ramalan joyoboyo pasar ilang kumandange terhadap pemasaran digital di era marketing 4.0 di indonesia." *bangun rekaprima* 9, no. 1 (april 30, 2023): 75. https://doi.org/10.32497/bangunrekaprima.v9i1.4475.

Nurhayati, Siti, Nurjamil, And Muhammad Haris Fadhillah. (2022) "Menakar Peluang Dan Tantangan Penyelesaian Sengketa Bisnis Fintech Syariah Melalui Laps." *Jurnal Tabarru': Islamic Banking And Finance* 5, No. 1 (February 9, 2022): 63–70. https://doi.org/10.25299/jtb.2022.vol5(1).8857.

Nurul Mujahidah, Kurniati, And Misbahuddin. (2024), "Responsibiltas Hukum Islam Terhadap Dinamika Perubahan Sosial." *AL-MUTSLA* 6, no. 1 (June 30, 2024): 89–109. https://doi.org/10.46870/jstain.v6i1.1017.

Ompusunggu, Sensia Gibsi, and Roy Valiant Salomo. "Analisis Pelaksanaan Sistem Pengendalian Intern Pemerintah di Indonesia," n.d.

Primadhany, Erry Fitrya. (2023), "Hukum Perlindungan Konsumen Dan Implikasinya Terhadap Hak Asasi Manusia Di Kabupaten Sukabumi: Studi Kasus Tentang Perlindungan Konsumen Pada Produk Pangan." *Jurnal*

Hukum Dan Ham Wara Sains 2, No. 06 (june 28, 2023): 492–500. https://doi.org/10.58812/jhhws.v2i6.444.

Purwoko, Dwi. (2023). "Kebijakan Pemerintah, Media, Dan Fatwa Mui Dalam Mendinamisasi Perkembangan Bank Syariah Di Indonesia" 10, no. 1 (2023).

Rahadiyan, Inda. (2022). "Perkembangan Financial Technology Di Indonesia Dan Tantangan Pengaturan Yang Dihadapi." *Mimbar Hukum* 34, no. 1 (june 30, 2022): 210–36. https://doi.org/10.22146/mh.v34i1.3451.

Roni Sahindra. (2022). "Pelaksanaan Hak Kekayaan Intelektual Dalam Kerangka Pembangunan Budaya Hukum (Diskursus Filosofis Keberadaan Hak Kekayaan Intelektual Di Indonesia)." *Journal Equitable* 7, No. 2 (November 30, 2022): 272–91. Https://Doi.Org/10.37859/Jeq.V7i2.4320.

Sebayang, Ekinia Karolin, Mahmud Mulyadi, And Mohammad Ekaputra. (2024). "Potensi Pemanfaatan Teknologi Artificial Intelligence Sebagai Produk Lembaga Peradilan Pidana Di Indonesia." *Locus Journal Of Academic Literature Review* 3, No. 4 (April 29, 2024): 317–28. Https://Doi.Org/10.56128/Ljoalr.V3i4.311.

Siregar, Fitri Yanni Dewi. (2023). "Aspek Hukum Penyederhanaan Perizinan Badan Usaha Di Bidang Lingkungan Hidup Dalam Undang-Undang Cipta Kerja," N.D.

Subagiya, Bahrum. (2023). "Eksplorasi Penelitian Pendidikan Agama Islam Melalui Kajian Literatur: Pemahaman Konseptual Dan Aplikasi Praktis,"

Suganda, Rangga. (2022) "Analisis Terhadap Peluang Dan Tantangan Perbankan Syariah Pada Era Digital," N.D. "Metode Pendekatan Yuridis Dalam Memahami Sistem Penyelesaian Sengketa Ekonomi Syariah." *Jurnal Ilmiah Ekonomi Islam* 8, No. 3 (October 31): 2859. Https://Doi.Org/10.29040/Jiei.V8i3.6485.