E-ISSN : 2774 - 5783
Volume 7 No.1 2026

ALGORITHMIC GHARAR AND LEGAL CERTAINTY IN BLOCKCHAIN-BASED SMART CONTRACTS: A COMPARATIVE STUDY OF INDONESIAN LAW AND ISLAMIC BUSINESS LAW

Didi Sukardi[1], Achmad Otong Busthomi[2], dan Afif Muamar[3]
Universitas Islam Negeri Siber Syekh Nurjati Cirebon[1, 2, 3]
Email: achmadbusthomi@uinssc.ac.id[1], Busthomi@gmail.com[2], afif_muamar@syekhnurjati.ac.id[3]

Received :
02 January 2026
Accepted :
20 February 2026
Published :
25 March 2026

Keywords:
Algorithmic Gharar; Blockchain; Smart Contracts; Indonesian Law; Islamic Business Law; Governance

ABSTRCT

This article examines the legal certainty of blockchain-based smart contracts within Indonesia's dual framework of positive law and Islamic business law. It asks how Indonesian contract and electronic-transaction rules accommodate automated agreements, how automation reshapes gharar, and what governance safeguards are needed. The study employs normative-comparative legal research, using legislation, regulatory instruments, Sharia standards, and scholarship selected for relevance and authority. Materials were analysed through doctrinal interpretation, cross-jurisdictional comparison, and thematic mapping of uncertainty. The findings indicate that Indonesian law may recognize smart contracts through contract and electronic-transaction rules, but the framework remains fragmented. Automation can reduce opportunistic non-performance while relocating uncertainty to code opacity, oracle reliability, tokenized asset rights, and irreversible execution. The article conceptualizes "algorithmic gharar" as an analytical lens, not a fiqh category, and proposes a Sharia-Compliant Smart Contract Governance model combining readable legal terms, code and Sharia audits, accountable data governance, limited reversibility, and coordinated oversight.

INTRODUCTION

Blockchain has moved beyond an experimental technology and is increasingly relevant to digital financial infrastructure. In Indonesia, the regulatory landscape for digital financial assets has changed significantly following Law No. 4 of 2023 on Financial Sector Development and Strengthening, Government Regulation No. 49 of 2024, and the Financial Services Authority (Otoritas Jasa Keuangan, OJK) Regulation No. 27 of 2024, which became effective on 10 January 2025. OJK Regulation No. 23 of 2025 subsequently amended the 2024 framework and expanded aspects of the regulatory regime for digital financial assets and related derivatives (Fauzy, 2024). These measures establish a more defined supervisory framework for digital-asset trading, but they do not create a comprehensive, general law of smart contracts.

A smart contract is code deployed on a blockchain that automatically performs specified operations when predetermined conditions are met. The term can refer to executable software alone or to software that performs obligations arising from a legally binding agreement expressed in natural language. This distinction matters: code can

execute a transaction, but its execution does not by itself establish that the parties understood the agreement, that the underlying asset rights are valid, or that an unjust outcome can be remedied (Nugroho, 2020). The United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on Automated Contracting in 2024 to facilitate legal recognition of automated contracting while addressing attribution, unexpected outcomes, and disclosure.

The Indonesian context also involves the interaction of two normative frameworks. Indonesian positive law governs contract formation, electronic transactions, digital-asset trading, and consumer protection. Islamic business law additionally evaluates contractual clarity, the nature of the subject matter, the distribution of risk, and the avoidance of prohibited elements such as excessive gharar and maisir. A transaction may therefore be technically executable and potentially valid under general contract rules while remaining problematic from a Sharia perspective. Conversely, the use of blockchain does not automatically make a transaction impermissible; its legal and Sharia assessment depends on the contractual structure, rights represented, and risks allocated.

Research on smart contracts has examined legal enforceability, technical limitations, regulation, and remedies (Drummer & Neumann, 2020; Ferreira, 2021; Giancaspro, 2017; Herian, 2021; Savelyev, 2017). More recent work has addressed consumer protection and the relationship between legal agreements and on-chain execution (Bassan & Rabitti, 2024; Durovic & Willett, 2023; Ferro et al., 2023; Nguyen, 2023). Research on Islamic finance has considered blockchain-enabled sukuk, digital trust, fintech development, and Sharia-related uncertainty (Alshater, Saba, Supriani, & Rabbani, 2022; Busari & Aminu, 2022; Chong, 2021; Fatin Hamamah, Vasavvi Acharjya, & Didi Sukardi, 2025; Khan et al., 2022). These strands provide a strong foundation, but they are not often integrated into a single governance analysis focused on Indonesia's evolving digital-asset framework.

This article addresses three questions: (1) to what extent can Indonesian contract and electronic-transaction law accommodate blockchain-based smart contracts; (2) how does automation relocate contractual uncertainty in ways relevant to gharar; and (3) what governance safeguards can connect legal certainty, consumer protection, and Sharia compliance? Its contribution is twofold. Conceptually, it uses "algorithmic gharar" as an analytical lens for uncertainty arising from code, external data, tokenized rights, and automated finality. Normatively, it proposes a Sharia-Compliant Smart Contract Governance (SCSCG) model. The term algorithmic gharar is not presented as a new category of Islamic jurisprudence, but as a contemporary application of established concerns about material contractual uncertainty.

METHOD

This article employs normative-comparative legal research based on library research. Its normative character lies in the interpretation of contract requirements, electronic-transaction rules, digital-asset regulations, and Sharia standards. Its comparative dimension considers international developments in automated contracting, particularly UNCITRAL's Model Law on Automated Contracting, alongside selected comparative legal scholarship (Efendi & Rijadi, 2022). A contextual socio-legal lens is used to situate the legal analysis within the institutional and market changes associated with digital-asset regulation. This lens is contextual rather than empirical: the study does not report interviews, surveys, field observations, or an original technical audit of a deployed smart contract.

Primary materials include the Indonesian Civil Code, Law No. 11 of 2008 on Electronic Information and Transactions as amended by Law No. 19 of 2016 and Law No. 1 of 2024, Government Regulation No. 71 of 2019, Law No. 4 of 2023, Government Regulation No. 49 of 2024, OJK Regulation No. 27 of 2024 as amended by OJK Regulation No. 23 of 2025, relevant implementing regulations, DSN-MUI Fatwa No. 117/DSN-MUI/II/2018, relevant AAOIFI Sharia

standards, and UNCITRAL's 2024 Model Law. Secondary materials comprise 20 peer-reviewed journal articles published in journals indexed in Scopus, selected purposively for their relevance to smart-contract enforceability, technical security, consumer protection, Islamic finance, and gharar. The selection is not presented as a systematic literature review; it is a focused doctrinal selection intended to support legal interpretation and conceptual synthesis.

The analysis proceeded in four stages. First, the study identified the legal bases through which an automated agreement may be assessed under Indonesian law (Efendi & Rijadi, 2022). Second, it compared those bases with selected international approaches to automated contracting and consumer protection. Third, it mapped recurring sources of technical and contractual uncertainty code opacity, oracle dependence, tokenized asset rights, and execution finality. Fourth, it assessed the implications of those uncertainties through the principles of gharar and maqāṣid al-sharīʿah, then synthesized the findings into a governance model. The method supports normative conclusions about legal design; it does not establish the actual frequency of these risks in Indonesian market practice

RESULT AND DISCUSSION

The Partial Recognition of Smart Contracts under Indonesian Law

Indonesian law can accommodate some smart-contract arrangements through existing legal principles, but this accommodation is partial rather than comprehensive. Article 1320 of the Indonesian Civil Code sets out the general requirements for a valid agreement, while Article 1338 establishes the binding force of agreements made in accordance with the law. The Electronic Information and Transactions Law, as amended, and Government Regulation No. 71 of 2019 provide a legal framework for electronic information, documents, systems, and transactions. These provisions may support the legal effectiveness of agreements formed or performed electronically, but they do not comprehensively resolve the distinct issues raised by executable code.

The first issue is consent. A user may interact with a wallet, accept platform terms, or trigger a transaction through an application interface. However, the existence of a click or blockchain transaction does not necessarily establish informed consent to every consequence embedded in the code. Smart contracts may be difficult for non-specialists to understand, particularly where the legal agreement and the executable code are not aligned. The distinction between technical assent and meaningful legal consent is consistent with scholarship that identifies a persistent gap between legal requirements and technical implementation (Drummer & Neumann, 2020; Ferreira, 2021; Hamamah, 2020; Jaswant & Kale, 2022).

The second issue is attribution and legal capacity. A wallet address or cryptographic signature may help demonstrate control over a transaction, but it does not always identify the natural or legal person responsible for it. This problem is particularly significant in pseudonymous or permissionless environments. Where regulated intermediaries perform identity checks, attribution may be easier to establish; however, those controls do not automatically extend to every public blockchain transaction. Smart-contract governance should therefore record the relationship between account control, legal identity where required, authority to act, and the agreement being executed (Handayani, Syara, Garnita, & Fisailillah, 2023).

The third issue concerns the contractual object and the rights represented by a token. OJK Regulation No. 27 of 2024 and its amendment, OJK Regulation No. 23 of 2025, regulate the trading of digital financial assets, including crypto-assets and certain related instruments. They do not, by themselves, validate every underlying asset claim or every contractual arrangement encoded in software. A token may technically exist while the legal rights attached to it ownership, redemption, beneficial interest, or a claim against an issuer remain unclear. The legal treatment of a tokenized asset must therefore distinguish the

token as a digital record from the enforceable rights it purports to represent (Fauzy, 2024).

The fourth issue is remedy. Automated execution can reduce delays and opportunistic non-performance, but it may also execute a transaction based on faulty code, inaccurate data, or a disputed interpretation of the agreement. Legal enforceability should not be equated with technical irreversibility. Work on smart-contract remedies and consumer protection emphasizes that ordinary legal rights, including cancellation, conformity, and redress, may still need to operate alongside automated performance (Dewi, 2024; Durovic & Willett, 2023; Herian, 2021; Nguyen, 2023). The most defensible conclusion is therefore that smart contracts may be recognized through existing Indonesian law when applicable legal requirements are satisfied, but the legal consequences of code execution remain dependent on the surrounding agreement, evidence, asset rights, and available remedies. Existing Scholarship and the Remaining Research Gap.

Table 1 summarizes selected contributions from the literature and identifies the specific gap addressed by this article.

Study	Main contribution	Remaining issue for this article
Giancaspro (2017)	Examines the legal status and practical limitations of smart contracts.	Does not integrate Indonesian digital-asset regulation with Islamic business law.
Ferreira (2021)	Explains the movement from legal skepticism toward regulatory accommodation.	Does not develop a Sharia-based framework for algorithmic uncertainty.
Durovic and Willett (2023)	Shows why consumer rights and remedies must remain effective when contract performance is automated.	Focuses on consumer law rather than Indonesia's dual legal framework.
Busari and Aminu (2022)	Examines opportunities and challenges in using smart contracts for sukuk transactions.	Does not propose a general governance model for smart contracts.
Mohd Noh et al. (2025)	Reviews how gharar is understood in modern Islamic financial transactions.	Does not specifically map code, oracle, token-rights, and finality risks.
Bassan and Rabitti (2024)	Explores legal agreements and the possibility of contracting directly on blockchain.	Does not integrate the Indonesian regulatory context with Sharia compliance.

Source: Author's synthesis of the cited studies.

Algorithmic Gharar: The Relocation of Contractual Uncertainty

Gharar should not be understood as a prohibition of every risk or unknown future event. Commercial activity inevitably involves uncertainty. The relevant concern in Islamic commercial jurisprudence is material or excessive uncertainty that affects the clarity of the subject matter, the parties' obligations, or the fairness of the exchange. Recent review literature confirms that gharar analysis remains context-sensitive and must be applied to the nature and operation of the particular transaction (Mohd Noh, Nor Azelan, & Zulkepli, 2025). The question is therefore not whether a smart contract contains any uncertainty, but whether material uncertainty is concealed, inadequately allocated, or left without a fair mechanism for resolution.

Automation can reduce some conventional sources of uncertainty, including delay, inconsistent performance, and discretionary non-performance. At the same time, it can relocate uncertainty to the technical architecture that governs execution. This article

uses the term algorithmic gharar for tha relocation. The term describes uncertainty tha may arise from the opacity or reliability of code and data, the legal status of tokenized rights, and the difficulty of correcting execution after an error. It is an analytical label, not a claim that classical fiqh recognizes a separate, newly established category of gharar.

Four sources are particularly relevant. First, code opacity and software defects may prevent a party from understanding the practical consequences of the agreement. Security research documents recurring vulnerabilities and the need for systematic code analysis before deployment (Rameder, di Angelo, & Salzer, 2022; Wang et al., 2021). Second, oracle dependence introduces external information such as prices, delivery status, or compliance data into an otherwise automated transaction. If the source, validation method, or responsibility for incorrect data is unclear, the parties may face risks that are not apparent from the contract text. Third, tokenized assets can obscure the difference between a digital token and the legal right it is intended to represent. Research on tokenized sukuk and digital-asset rights shows that technical execution must be connected to the underlying asset and its enforceable legal claims (Ferro et al., 2023; Khan et al., 2022). Fourth, execution finality may make an erroneous or unfair outcome difficult to reverse, even when a legal remedy is warranted (Herian, 2021; Mik, 2017).

Table 2. Sources of algorithmic gharar and corresponding governance responses

Source of uncertainty	Digital manifestation	Relevance to gharar analysis	Suggested response
Code opacity and defects	Users cannot readily interpret code; bugs or vulnerabilities may remain hidden.	A party may accept obligations without adequately understanding material consequences.	Readable master agreement, independent code audit, version control, and disclosure of material updates.
Oracle and data dependence	Execution depends on external prices, delivery confirmations, or third-party data.	Contract outcomes may depend on data that parties cannot inspect or control.	Verified data sources, redundancy, validation rules, audit trails, fallback procedures, and allocated liability.
Unclear tokenized rights	A token represents a claim whose legal basis, redemption rights, or ownership status may be uncertain.	The technical object is identifiable, but the underlying legal or Sharia rights may not be clear.	Asset classification, disclosure of off-chain rights, proof of title, and clear redemption/transfer terms.
Execution finality	An automatic transaction is difficult to pause or reverse after an error or fraudulent input.	A technically final outcome may preserve a materially unfair result without adequate remedy.	Narrow pause/override powers, independent review, dispute resolution, and proportionate restitution.

Source: Author's synthesis informed by Herian (2021), Mik (2017), Rameder et al. (2022), Wang et al. (2021), Ferro et al. (2023), and Mohd Noh et al. (2025).

Regulatory Fragmentation and the Need for Minimum Governance Standards

Indonesia's current framework is distributed across general contract law, electronic-transaction law, digital-asset regulation, and consumer-protection requirements. Each regime addresses a relevant part of the problem, but none provides a complete lifecycle framework for smart contracts covering formation, code-to-text consistency, data inputs, execution errors, and post-execution remedies. The result is a regulatory gap between the recognition of electronic transactions and the governance of automated contractual performance.

OJK Regulation No. 27 of 2024 provides a more defined framework for digital financial asset trading, while OJK Regulation No. 23 of 2025 adjusts and expands parts of that framework, including the treatment of digital financial assets and related derivatives (OJK, 2024a, 2025a). These rules are important for supervised market participants, yet they should not be read as a general endorsement of all smart contracts or of every asset represented by

a token. Likewise, UNCITRAL's Model Law on Automated Contracting is a comparative reference rather than directly applicable Indonesian law. It offers useful principles concerning recognition, attribution, automated outputs, disclosure, and unexpected outcomes.

The governance challenge is not solved by defining smart contracts as a new legal category alone. Regulation must also clarify the relationship between natural-language terms and executable code; require disclosure of material technical dependencies; assign responsibility for faulty inputs and code; and preserve proportionate remedies. The consumer-law literature warns against allowing automation to displace legally mandated protections simply because the system can execute without human intervention (Durovic & Willett, 2023; Nguyen, 2023). In Islamic finance, the same principle means that technical efficiency should not be treated as sufficient evidence of Sharia compliance. Studies of blockchain adoption and Islamic finance highlight potential gains in transparency and operational efficiency, but also the importance of institutional governance, user understanding, and regulatory clarity (Afifah, Abu-Hussin, & Zafar, 2025; Aisyah, Salwa, & Sunaryo, 2025; Alshater et al., 2022; Chong, 2021).

A Sharia-Compliant Smart Contract Governance Model

To connect legal certainty, technical reliability, and Sharia compliance, this article proposes the Sharia-Compliant Smart Contract Governance (SCSCG) model. It treats a smart contract as a layered governance arrangement linking a legal agreement, executable code, external data, responsible institutions, and mechanisms for review and redress.

Governance pillar	Minimum controls	Legal and Sharia objective
1. Dual-form contracting	Maintain a human-readable master agreement and linked executable code; identify which terms prevail in a conflict; disclose material technical dependencies and the governing law.	Supports informed consent, interpretation, and clarity of rights and obligations.
2. Dual ex ante audit	Conduct independent code-security review and Sharia review before deployment; retain audit reports, version history, and records of material amendments.	Reduces preventable defects and evaluates the contract structure, object, risk allocation, and potential excessive gharar.
3. Oracle and data governance	Disclose data sources, validation methods, redundancy, fallback rules, data-update frequency, and responsibility for inaccurate inputs.	Makes external dependencies visible and allocates the risks arising from data quality.
4. Controlled reversibility and redress	Define limited pause or override triggers for material bugs, fraud, erroneous data, or binding dispute decisions; log all interventions and provide restitution procedures.	Preserves automation while avoiding absolute finality that blocks fair correction.
5. Coordinated oversight	Coordinate the responsibilities of regulated operators, OJK where applicable, Sharia supervisory bodies, auditors, and dispute-resolution institutions; maintain incident reporting and consumer complaint channels.	Connects financial regulation, consumer protection, technical accountability, and Sharia supervision.

The model does not assume that every smart contract requires the same level of control. Governance should be proportionate to the transaction's value, complexity, consumer impact, degree of decentralization, and reliance on external data. A simple low-value transaction may require limited disclosure and testing, whereas a regulated financial product or tokenized asset representing substantial property rights should be subject to

stronger audit, identity, asset-rights, and dispute-resolution requirements.

The model also avoids two extremes. Unrestricted human override can undermine predictability and invite opportunistic interference; absolute irreversibility can make the system unable to respond to fraud, bugs, or legally required remedies. Controlled reversibility should therefore be defined ex ante, limited to specified triggers, independently reviewable, and fully recorded. This approach is consistent with the broader literature's conclusion that technical automation does not remove the need for legal responsibility and remedies (Bassan & Rabitti, 2024; Ferreira, 2021; Herian, 2021).

Contributions, Policy Implications, and Limitations

The article makes three contributions. First, it updates the Indonesian legal discussion by considering the digital-asset regulatory framework established through Law No. 4 of 2023, Government Regulation No. 49 of 2024, OJK Regulation No. 27 of 2024, and its 2025 amendment. Second, it uses algorithmic gharar to identify uncertainty that may be obscured by executable code, external data, tokenized rights, and irreversible execution. Third, it develops the SCSCG model as a governance proposal that links legal and Sharia review with technical controls and remedies.

For policymakers, the priority should be minimum governance standards rather than an abstract prohibition or unconditional endorsement of the technology. Such standards could require a readable agreement linked to code, clear allocation of responsibility for oracle data, security testing proportionate to risk, transparent asset-rights disclosures, incident reporting, and access to dispute resolution. For regulated operators, the model provides a practical checklist for designing contracts that remain intelligible and accountable. For Sharia supervisors, it emphasizes that compliance assessment should examine the actual transaction structure and its technical dependencies, rather than rely solely on the label attached to a product.

The study has limitations. It is a doctrinal and conceptual analysis, not an empirical assessment of how Indonesian users, developers, regulators, or Sharia boards apply these safeguards in practice. It also does not test the code of any specific protocol or determine the Sharia status of a particular digital asset. Future research could conduct interviews with regulators and market participants, examine real-world tokenization products, and test the proposed governance model against specific contractual and technical designs.

CONCLUSION

Blockchain-based smart contracts may be accommodated under Indonesian law through general contract principles and electronic-transaction rules, but the current framework does not provide a comprehensive regime for automated contractual performance. Regulation of digital financial asset trading strengthens market oversight, yet it does not automatically settle questions of consent, attribution, tokenized asset rights, code-to-text consistency, or remedies for erroneous execution.

From an Islamic business-law perspective, automation is not inherently prohibited. It can reduce some forms of opportunistic non-performance, but it may also relocate material uncertainty to code opacity, oracle reliability, unclear underlying rights, and execution finality. The term algorithmic gharar is used here as an analytical lens for these risks, not as a new category of fiqh.

The proposed SCSCG model combines dual-form contracting, independent code and Sharia audits, accountable oracle and data governance, controlled reversibility, and coordinated oversight. Its central principle is that technical execution should remain aligned with legally intelligible obligations, clear asset rights, fair risk allocation, and accessible remedies. Further empirical and product-specific research is needed to assess how these safeguards can be implemented in Indonesian practice.

REFERENCES

Afifah, K., Abu-Hussin, M. F., & Zafar, M. B. (2025). Transforming Islamic social finance: Determinants of blockchain technology

adoption for zakat payment. *Journal of Islamic Accounting and Business Research*. https://doi.org/10.1108/JIABR-08-2024-0283

Aisyah, Berliana, Salwa, Nur, & Sunaryo, Sidik. (2025). Keadilan dalam Perspektif Nilai-Nilai Pancasila : Relevansi dan Implementasinya dalam Sistem Hukum Indonesia. *Al Ilmu Sosial & Hukum Al-Zayn: Jurnal Ilmu Sosial & Hukum*, *3*(3), 1956–1964. https://doi.org/https://doi.org/10.61104/alz.v3i3.1513

Alshater, M. M., Saba, I., Supriani, I., & Rabbani, M. R. (2022). Fintech in Islamic finance literature: A review. *Heliyon*, *8*(9). https://doi.org/10.1016/j.heliyon.2022.e10385

Bassan, F., & Rabitti, M. (2024). From smart legal contracts to contracts on blockchain: An empirical investigation. *Computer Law & Security Review*, *55*. https://doi.org/10.1016/j.clsr.2024.106035

Busari, S. A., & Aminu, S. O. (2022). Application of blockchain information technology in Ṣukūk trade. *Journal of Islamic Accounting and Business Research*, *13*(1), 1–15. https://doi.org/10.1108/JIABR-10-2019-0197

Chong, F. H. L. (2021). Enhancing trust through digital Islamic finance and blockchain technology. *Qualitative Research in Financial Markets*, *13*(3), 328–341. https://doi.org/10.1108/QRFM-05-2020-0076

Dewi, Maftuhah; (2024). JURIDICAL ANALYSIS OF POACHING USING ASSEMBLED FIREARMS IN FOREST AREAS IN RELATION TO EMERGENCY LAW NUMBER 12 OF 1951 (STBL.1948.NO.17) (STUDY OF SPECIAL CRIMINAL DECISION: 115/PID.SUS/2019/PN.KNG). *FOCUS: Jurnal of Law*, *5*(1), 16–27.

Drummer, D., & Neumann, D. (2020). Is code law? Current legal and technical adoption issues and remedies for blockchain-enabled smart contracts. *Journal of Information Technology*, *35*(4), 337–360. https://doi.org/10.1177/0268396220924669

Durovic, M., & Willett, C. (2023). A legal framework for using smart contracts in consumer contracts: Machines as servants, not masters. *The Modern Law Review*, *86*(6), 1390–1421. https://doi.org/10.1111/1468-2230.12817

Efendi, Jonaedi, & Rijadi, Prasetijo. (2022). Metode Penelitian Hukum: Normatif dan Empiris. In *Kencana* (II). Jakarta.

Fatin Hamamah, Vasavvi Acharjya, & Didi Sukardi. (2025). Divorce and Children Sexual Deviant Behavior from the Perspective of Criminal Law and Sustainable Development Goals. *Unifikasi : Jurnal Ilmu Hukum*, *12*(01), 48–61. https://doi.org/10.25134/unifikasi.v12i01.789

Fauzy, Shanty D. (2024). Kegiatan Literasi Keuangan Oleh OJK Kepada Perempuan Di Riau Dilihat Dari Sudut Pandang Teori Transmisi Pesan John Locke. *Syntax Idea*, *6*(2), 508–525. https://doi.org/10.46799/syntax-idea.v6i2.2968

Ferreira, A. (2021). Regulating smart contracts: Legal revolution or simply evolution? *Telecommunications Policy*, *45*(2). https://doi.org/10.1016/j.telpol.2020.102081

Ferro, E., Saltarella, M., Rotondi, D., Giovanelli, M., Corrias, G., Moncada, R., Cavallaro, A., & Favenza, A. (2023). Digital assets rights management through smart legal contracts and smart contracts. *Blockchain: Research and Applications*, *4*(3). https://doi.org/10.1016/j.bcra.2023.100142

Giancaspro, M. (2017). Is a "smart contract" really a smart idea? Insights from a legal perspective. *Computer Law & Security Review*, *33*(6), 825–835. https://doi.org/10.1016/j.clsr.2017.05.007

Hamamah, Fatin. (2020). KEBIJAKAN HUKUM PIDANA DALAM UPAYA PENANGANAN ANAK YANG BERMASALAH DIKAITKAN DENGAN UNDANG-UNDANG NO. 23 TAHUN 2002 TENTANG PERLINDUNGAN ANAK. *Nature Microbiology*, *3*(1), 641. Retrieved from http://dx.doi.org/10.1038

Handayani, Intan, Syara, Salira Niti, Garnita, Sarassati, & Fisaililah, Laika. (2023). John Rawls: Filsafat Hukum. *Nusantara: Jurnal Pendidikan, Seni, Sains Dan Sosial Humaniora*, (September), 1–17. https://doi.org/10.11111/nusantara.xxxxxxx

Herian, R. (2021). Smart contracts: A remedial analysis. *Information & Communications Technology Law*, *30*(1), 17–34. https://doi.org/10.1080/13600834.2020.1807134

Jaswant, S., & Kale, P. (2022). Smart contracts and blockchain: Legal issues and implications for Indian contract law. *International Review of Law, Computers & Technology*, *36*(3), 312–329. https://doi.org/10.1080/13600869.2021.1999312

Khan, N., Kchouri, B., Yatoo, N. A., Kräussl, Z., Patel, A., & State, R. (2022). Tokenization of sukuk: Ethereum case study. *Global Finance Journal*, *51*. https://doi.org/10.1016/j.gfj.2020.100539

Mik, E. (2017). Smart contracts: Terminology, technical limitations and real world complexity. *Law, Innovation and Technology*,

9(2), 269–300. https://doi.org/10.1080/17579961.2017.1378468

Mohd Noh, M. S., Nor Azelan, S. H., & Zulkepli, M. I. S. (2025). A review on gharar dimension in modern Islamic finance transactions. *Journal of Islamic Accounting and Business Research*, *16*(5), 976–989. https://doi.org/10.1108/JIABR-01-2023-0006

Nguyen, S. T. (2023). Consumer protection against unfair contract terms in the age of smart contracts. *Federal Law Review*, *51*(4), 487–508. https://doi.org/10.1177/0067205X231205048

Nugroho, H. (2020). Postmodernisme dan krisis representasi hukum. *Law and Justice, 5(2)*. Retrieved from https://doi.org/10.0000/lawandjustice.520175

Rameder, H., di Angelo, M., & Salzer, G. (2022). Review of automated vulnerability analysis of smart contracts on Ethereum. *Frontiers in Blockchain*, *5*. https://doi.org/10.3389/fbloc.2022.814977

Savelyev, A. (2017). Contract law 2.0: "Smart" contracts as the beginning of the end of classic contract law. *Information & Communications Technology Law*, *26*(2), 116–134. https://doi.org/10.1080/13600834.2017.1301036

Wang, Y., He, J., Zhu, N., Yi, Y., Zhang, Q., Song, H., & Xue, R. (2021). Security enhancement technologies for smart contracts in the blockchain: A survey. *Transactions on Emerging Telecommunications Technologies*, *32*(12). https://doi.org/10.1002/ett.4341