Human Interaction and Emerging Technologies (IHIET-AI), Vol. 201, 2026, 517–527
https://doi.org/10.54941/ahfe1007205

Assessing EU Consumer Protection Risks in AI-Driven Blockchain Tokenized Finance Through Smart Contract Design

Marta Urbane

Riga Stradiņš University, Dzirciema street 16. Riga, Latvia

ABSTRACT

Financial services based on blockchain tokenization increasingly rely on AI assisted smart contracts to structure consumer participation. Consumers engage in tokenized financial markets through interfaces and automated processes. This raises the question of whether EU consumer protection, based on transparency, fairness, and remedies and established at a time when written contracts between the consumer and the financial service provider prevailed, is applicable nowadays. In this paper, the author demonstrates how EU consumer law standards apply when contractual obligations are embedded within smart contract design and executed automatically. The focus lies on how information disclosure, imbalance between parties and access to remedy are shaped by smart contract design in AI driven tokenized financial services. Although regulatory challenges in tokenized finance have been widely discussed, the implications of smart contract design for the application of established EU consumer law standards have received less systematic attention, specifically in tokenized finance. The analysis is based on the doctrinal interpretation of the EU consumer protection rules and a close reading of the relevant case law of the Court. These standards are applied to a case study of AI assisted smart contracts used in blockchain based tokenized finance, treating smart contract design as part of the contractual arrangement rather than as a purely technical tool. The author shows that automated execution and technical irreversibility complicate informed decision making and weaken traditional mechanisms of judicial control. It concludes by outlining design related legal benchmarks that follow from EU consumer law and remain relevant for AI driven tokenized finance.

Keywords: EU consumer law, Blockchain tokenization, Smart contract design, Artificial intelligence

INTRODUCTION

AI driven digital infrastructures increasingly shape how individuals interact with financial markets. In recent years, blockchain based tokenization has expanded from experimental settings into consumer facing financial services. Tokenized finance restructures financial participation by relying on smart contracts that automate contractual performance and embed legal effects directly into technical systems. For consumers, the engagement with financial products occurs increasingly through interfaces, dashboards, and automated execution.

Received January 18, 2026; Revised March 1, 2026; Accepted March 10, 2026; Available online April 1, 2026

Within the EU, this development unfolds against a legal framework built on technology neutral consumer protection standards. EU consumer law aims to protect weaker parties by requiring transparent information, substantive fairness of contractual terms, and offering effective remedies (Namysłowska, 2025). These standards were developed at a time when contracts were easy to access and the meaning of their terms could be interpreted and reviewed by courts. The increasing reliance on AI assisted smart contracts in tokenized finance places pressure on these assumptions and raises questions about the continued effectiveness of EU consumer protection.

Smart contracts differ from traditional contractual instruments in both form and function. They translate contractual obligations into code and execute them automatically once predefined conditions are met. In tokenized financial services, AI tools often support contract design, risk assessment, and user interaction. This combination affects the way information is disclosed, the way consent is expressed, and how risks are allocated. Research has highlighted that smart contracts are not neutral technical tools, but embed normative choices that shape legal outcomes and power relations between parties (Schrepel, 2021).

Recent research has begun to explore consumer protection challenges arising from AI driven smart contracts. Scattarreggia shows that AI does not eliminate consumer protection risks but intensifies them by influencing disclosure practices and behavioural responses in automated contractual environments (Scattarreggia, 2025). At the regulatory level, Comegna highlights how AI and blockchain operate in legal silos, creating fragmentation that leaves consumer protection under enforced in technologically complex markets (Comegna, 2025). Although these contributions identify structural risks, fewer studies examine how existing EU consumer law standards apply to smart contract design in practice.

The EU consumer protection law offers a rich body of interpretative guidance through the case law of the Court of Justice of the European Union (Further - The Court). The Court has consistently emphasised that transparency requires consumers to understand the legal and economic consequences of contractual terms, not merely their formal availability (Kásler, C-26/13; Andriciuc, C-186/16). The Court has also stressed the need for effective judicial control of unfair terms and access to remedies (Aziz, C 415/11; Banco Español de Crédito C 618/10). These standards remain binding and form the core of consumer protection across sectors, notwithstanding the forms of contracts.

At the same time, recent financial regulation, including Regulation (EU) 2023/1114 on markets in crypto assets (MiCA Regulation), addresses risks linked to tokenized finance, but does not replace the application of general consumer law. Within the EU, tokenised financial services develop within an increasingly structured regulatory environment that seeks to balance innovation with investor and consumer protection, particularly following the adoption of MiCA Regulation (Jūrmalis et al., 2025). This creates a need to assess whether smart contract design in AI driven blockchain tokenized finance complies with established consumer protection standards. This article addresses this gap by examining how EU consumer protection standards operate when smart contract design determines contractual effects in AI driven blockchain tokenized finance. The analysis is grounded in doctrinal interpretation of EU consumer law, complemented by a close reading of the case law of the Court and relevant interdisciplinary literature, in order to assess how transparency, substantive fairness, and access to remedies operate when contractual obligations are embedded in AI-assisted smart contract design. By treating smart contracts as consumer interaction structures rather than purely technical instruments, the article connects EU consumer law doctrine with human interaction and system design, contributing to the broader discussion on legal safeguards in emerging technologies.

Human Factors Engineering involves understanding the need for comprehensive integration of human capabilities (cognitive, physical, sensory, and team dynamics) into a system design, beginning with conceptualization and continuing through system disposal. The primary concern for human factors engineering is the need to effectively integrate human capabilities with system interfaces to achieve optimal total system performance (use, operation, maintenance, support, and sustainment). Human factors engineering utilizes comprehensive task analyses to help define system functions and then allocates those functions to meet system requirements. The goal of HSI is to optimize total system performance, accommodating the characteristics of the user population that will operate, maintain, and support the system, and minimize life-cycle costs (Folds et al., 2008). HSI experts work within the Systems Engineering (SE) process to ensure that all human considerations are integrated throughout system design, development, fielding, sustainment, and retirement. The attention to human systems integration in system development programs drove hundreds of human-centered design improvements. Efforts were concentrated to maximize total system performance through improvements in human workload, ease of maintenance, and personnel safety which resulted in a cost avoidance of billions of dollars and prevention of hundreds of fatalities and disabling injuries for the system (Booher and Minninger, 2003).

METHODS

This study employs a qualitative narrative review alongside a descriptive analytical legal approach to analyse the interplay between smart contract design, AI-driven automation, and EU consumer protection regulation in blockchain-based tokenized financial services. In order to evaluate how established consumer protection standards function when contractual obligations are embedded in technical systems, the research aims to conceptually map, interpret, and synthesise doctrinal legal analysis, judicial reasoning, and interdisciplinary scholarship rather than statistically quantify empirical outcomes. This methodological choice reflects the normative nature of the research question, which concerns the interpretation and application of legal standards. The timeline for the analysis is from 2020 to 2025, as it is characterised by rapid expansion of tokenized finance, growing employment of AI-assisting smart contracts, as well as the important regulatory intervention at EU level. The timeline ensures that the study also reflects recent judicial developments, regulatory methods, and doctrinal debates in service to digital contracting and consumer protection.

The main academic and legal databases, such as JSTOR, Scopus, Web of Science, HeinOnline, SSRN, and Google Scholar, were used in an organised literature review process to choose sources. In addition, official EU legal sources were methodically reviewed, including the Court case law and EU legislative papers. "Smart contracts," "AI-driven contracts," "blockchain law," "tokenized finance," "EU consumer protection," "unfair terms," "transparency," "effective remedies," "code as law," and "algorithmic governance" were among the key search terms that were used in different combinations. Peer-reviewed journal articles, scholarly monographs, policy papers, legal commentary, and court rulings that significantly address the normative, regulatory, or doctrinal implications of smart contracts and automated contracting were the main emphasis of the search approach. The author only took into account materials that addressed consumer-facing applications or the legal implications of contractual automation. Research that was purely technical and had little impact on the law was excluded. Priority was given to work in EU consumer law, law and technology, financial regulation, and interdisciplinary legal scholarship. The chosen texts were interpreted as part of the analytical process, with special attention paid to thematic convergence, doctrinal conflicts, and the development of legal narratives. The transition from textual to architectural regulation, the conflict between automation and consumer comprehension, the effect of technical irreversibility on remedies, and the transfer of normative decisions from contract terms to system design are some of the key issues that have been identified. These themes were developed into distinct analytical sections that corresponded to transparency, substantive fairness, and access to effective remedies.

A case law analysis of selected judgments from the Court was conducted to identify the assumptions of EU consumer law regarding consumer reasoning, contractual flexibility, and judicial oversight. Subsequently, the assumptions were contrasted with the functional attributes of AI-assisted smart contracts utilised in tokenized finance. This comparative study grounds the analysis in actual legislative and technical advancements rather than abstract categorisation, allowing an assessment of how automation and design decisions affect the practical execution of established consumer protection norms.

RESULTS

In earlier studies of the doctrinal approach, smart contracts were mainly characterised as technical instruments that exist outside the process of concluding a contract. According to this approach, a smart legal contract is a computerised transaction protocol that automatically performs the obligations agreed upon by the parties through traditional means, without itself creating a contract (Argelich Comelles, 2020). In this sense, the code is viewed as an external enforcement mechanism, and the code has legal significance only to the extent that it ensures the performance of the obligations. This understanding reflects a broader "code as law" debate, in which enforcement logic embedded in software is treated as normatively consequential rather than merely technical (Yusuf and Martinez, 2025). This approach is not appropriate in consumer-orientated blockchain finance. In practice, smart contracts often act as self-sufficient systems that execute all and only those rules that are embedded in their code. By making the terms of the contract verifiable, immutable, and automatically enforceable, they replace the possibility of voluntary non-performance with technical compliance. As a result, contracting practices are shifting from ex post judicial assessment to automated ex ante assessment, where legal and economic consequences stem directly from the system design (Borgogno, 2018). Recent research reflects a shift in approach, recognising that the design of a smart contract can partially formulate the content of the contract or, in some cases, act as the contract itself. Although the authors' opinions differ in relation to formal qualification, they are united by the conclusion that the incorporation of obligations, conditions, and sanctions into enforceable logic significantly transforms contractual relations. The transfer of normative choice from a legal text to the system architecture limits the flexibility of interpretation of contract norms and puts design at the forefront as the main source of contractual consequences (Durovic and Willett, 2023).

The EU consumer law addresses these conceptual differences by applying a functional approach. Instead of assessing whether code qualifies as a contractual term in the formal sense, the appropriate EU directives regulate the consequences of contractual obligations. Information obligations under Directive 2011/83/EU (Consumer rights directive), compliance requirements under Directive (EU) 2019/770 on contracts for the supply of digital content and digital services and Directive (EU) 2019/771 on contracts for the sale of goods, and the control of unfair terms under Directive 93/13/EEC on unfair terms in consumer contracts, apply in all cases where design choices determine the obligations, risks, or remedies of the consumer (European Law Institute, 2023). From a functional perspective, smart contract developers must comply with consumer protection requirements as if the code constituted the content of the contract, even if at a theoretical level the code is distinguished from traditional contract terms. This understanding aligns with broader EU consumer law scholarship on digital services, which recognises data flows and system architecture as constitutive elements of contractual performance rather than external technical layers (Efroni, 2020). At the same time, the lack of consistent case law in the field of smart contracts indicates that complete doctrinal clarity in judicial interpretation has not yet been achieved. Until such guidelines are established, EU consumer law rules provide the main framework for assessing the design of smart contracts based on their practical impact on consumer rights, rather than on their technical form.

Automation has transformed the transparency function of consumer contracts. In AI-driven smart contracts, key contractual consequences are often triggered by algorithmic input and executors automatically, to automated consumers who retain limited insight into the decision-making mechanism or the reasons for the occurrence of specific outcomes. This creates a structural compliance deficit. EU consumer protection regulation requires not only formal contract information, but also the ability of the average consumer to understand the legal and economic consequences of his or her obligations, as consistently emphasised by the Court (Kásler, C-26/13; Andriciuc, C-186/16). This standard is not met by providing access to the code or providing technical documentation. Research on automated and AI-driven contracting indicates that opacity is exacerbated when the decision-making logic is embedded in machine learning systems or in conditional code that cannot be meaningfully explained ex ante (Scattarreggia, 2025). Smart contract user interfaces often reduce complex risk assessments to simple prompts or binary choices to increase the cognitive load on the consumer and create the impression of informed consent. From a consumer protection perspective, non-compliance undermines the basic function of the threat as a protection mechanism against imbalance. As a result, automated enforcement does not eliminate information asymmetry, but transforms it by shifting opacity from contractual language to system design. Therefore, in EU consumer law, lack of certainty resulting from automation is considered legally significant, regardless of whether it arises from the text of the contract, the design of the interface, or the algorithmic logic embedded in the same contracts. This means that what matters is the consequences, not the form.

Automated enforcement transforms the exercise of substantive fairness. It reduces decision-making to pre-determined technical conditions, which exclude negotiation, change of opinion, or adjustment after the execution is triggered. In the smart contract environment, strict conditional logic replaces contextual evaluation with automatic results. These can disadvantage consumers even if no clause in the contract text appears manifestly unfair in itself. EU consumer law consistently links fairness to the protection of the weaker party. It requires that contract terms do not create a significant imbalance between the parties, as this is contrary to the principle of good faith, as explained by the Court in the cases as Aziz and Banco Español de Crédito (Aziz, C 415/11; Banco Español de Crédito C 618/10). Automated enforcement challenges this standard, as it eliminates the possibility of suspending enforcement, reviewing the terms, or exercising discretion at the moment when the imbalance becomes apparent. Legal research confirms that automation shifts the imbalance from contract language to system architecture, where design choices predetermine outcomes and redistribute risks to the detriment of consumers (Durovic and Willett, 2023; Borgogno, 2018). Thus, automation can create significant unfairness even without explicit unfair terms, and the development of smart contracts falls squarely within the scope of control of unfair contract terms under EU consumer law. The effectiveness of consumer remedies under EU law is directly threatened by the technical immutability of smart contracts. If enforcement is in fact irreversible, rights such as refusal, suspension of enforcement, or timely judicial intervention become formal. The Court has consistently emphasised that consumer protection must be effective in practice, not just in theory (Mostaza Claro, C-168/05; Aziz, C 415/11; Banco Español de Crédito C 618/10).

Smart contract architectures that do not provide for suspension, revocation, or human intervention violate this principle, preventing courts and consumers from restoring the legal balance after enforcement has begun. The EU legal framework makes this risk clearer. The MiCA Regulation requires the controllability of smart contracts, explicitly rejecting completely unstoppable enforcement. At the same time, the revised Directive (EU) 2024/2853 (Product liability directive) recognises software, including artificial intelligence systems and code, as products subject to strict liability for defects. In general, this approach confirms that the development of smart contracts gives rise to legal liability if it renders consumer remedies ineffective. This further strengthens the conclusion that the principle of effectiveness in EU consumer law cannot be ignored in the context of immutability.

Design vulnerabilities pose specific consumer protection risks. Technical flaws in the smart contract environment directly translate into market damage, especially when contracts coordinate token transfers, collateral management, or automated liquidation on a large scale. Analysis of smart contract transaction architectures shows that enforceable modules, such as transaction rules, allocation of rights and obligations, and sanction mechanisms, act as binding decision points. Logical errors in these modules can lead to incorrect asset allocation or losses in interconnected contracts (Liu et al., 2023). Legal research on smart contracts in the EU digital single market confirms this risk. The interdependence of contracts and certain vulnerabilities exacerbate the harm when malicious code is introduced into a consumer-facing environment (Schrepel, 2021). In AI-driven tokenized finance, the risks are even greater. Algorithmic outcomes dynamically initiate or modify contract execution. Consumers are exposed to systemic consequences that are difficult to predict or contain (Scattarreggia, 2025). These are not just technical shortcomings. They pose serious legal challenges. EU consumer protection is increasingly based on a preventive approach. Design choices are assessed according to their impact on the potential harm to the consumer. This approach is in line with recent regulatory trends, including the extension of product liability to software. Defective digital design is recognised as a cause of consumer harm. This means that the integration of design governance, testing, and controllability as elements of consumer protection must be emphasised.

The author concludes with a consolidation of the doctrinal findings by relating EU consumer protection standards to concrete features of smart contract design. Rather than treating transparency, fairness, and access to remedies as abstract points of reference, the results indicate how these requirements take shape within the technical structure of automated contractual systems. In AI-driven, blockchain-based financial services, contractual effects increasingly arise from design choices made ex ante, rendering the system architecture legally relevant for consumer protection.

Table 1 brings together these findings by mapping recurring smart contract design features with the consumer law standards they employ. Elements such as automated execution, interface-based consent mechanisms, technical irreversibility, and embedded enforcement do not operate only in support of contractual performance. In practice, they influence how obligations are triggered, how risks are allocated, and whether corrective mechanisms remain available once execution has occurred.

Table 1: EU consumer protection standards and smart contract design constraints.

Smart Contract Design Feature	Consumer Law Standard Engaged	Consumer Risk Identified	Design Constraint Under EU Law
Automated execution	Substantive fairness	Binding outcomes without corrective space	Possibility to suspend or adjust execution
AI-based triggers	Transparency	Decision logic is difficult to understand	Explainability and traceability of triggers
Interface-based consent	Informed consent	Formal agreement without real understanding	Intelligible and non-deceptive interfaces
Technical irreversibility	Effectiveness of remedies	Remedies rendered impractical	Reversibility or equivalent redress
Embedded enforcement	Access to justice	Delayed or excluded review	Timely external intervention
Locked code design	Preventive consumer protection	Persistent defects and harm	Update and governance mechanisms

As Table 1 illustrates, conformity with EU consumer law cannot be reduced to compliance through information disclosure alone. What matters is whether the overall design of the contractual system allows consumers to grasp the implications of their commitments, prevents the emergence of structural imbalances, and preserves remedies that remain usable in practice. Seen from this perspective, EU consumer protection functions as a set of constraints that apply to the design of smart contracts in much the same way as they apply to contractual terms in more conventional settings. The synthesis offered here therefore situates smart contract design as a central point of regulatory compliance and captures the core result of the analysis, namely that established consumer law principles translate into operational requirements for AI-driven smart contracts in tokenized financial markets.

DISCUSSION

The results of the study allow the author to redefine smart contracts in the financial sector for consumers as legally functional artefacts whose design choices fulfil contractual functions. The code cannot be seen as a neutral layer of execution. EU law applies a functional procedure as well as consumers to consequences. If automation, interface design, or irreversibility determine what obligations arise, change, or are performed, these aspects fall within the scope of consumer protection. This interpretation is in line with the case law of the Court. Rights, justice, and remedies are assessed according to their practical impact, not their formal qualifications. This study demonstrates how a consequences-based approach is translated directly into design responsibility in AI-driven smart contracts.

The conclusions drawn limit bold "interpretations of "code is law"" that take autonomy, immutability, and self-execution as intrinsic values. EU consumer law does not reject automation in its essence, but subjects it to certain legal requirements to ensure fairness. The principle of transparency requires the intelligibility of legal and economic consequences, not just access to the code. In turn, the principle of fairness requires the elimination of structural imbalances, not just the absence of unfair formulations. The principle of effectiveness requires remedies that work in practice, not formal rights. Therefore, the author concludes that in the field of consumer finance, immutability and opacity are not neutral technical properties. They create legally significant risks. Such an approach positions EU law in contrast to techno-deterministic views and supports a consumer-orientated governance of automation (Durovic and Willett, 2023). The consumer should be at the centre of automation in the offer of AI-driven financial services.

The results also show increasing coherence between EU regulatory regimes. The MiCA Regulation requirement for the controllability of smart contracts in crypto-asset services rejects fully unstoppable enforcement and reinforces the consumer right to effective remedies. At the same time, the recast Product Liability Directive qualifies software, including artificial intelligence systems and embedded code, as products subject to a strict liability regime, including defective digital design in the preventive security framework. Overall, these instruments confirm the trend in EU law to consider system architecture as a point of legal liability. Consumer protection, financial regulation, and product liability converge here. Design choices that affect outcomes must comply with legal standards ex ante.

This analysis remains doctrinal and functional. The absence of settled case law by the Court directly addressing smart contracts means that some questions of classification and enforcement still wait for judicial resolution. However, existing consumer law principles provide a robust framework for evaluating effects. Future litigation will refine how transparency, fairness, and remedies apply to specific architectures, but the direction is clear: in AI-driven, blockchain-based consumer finance, smart contract design is not marginal - it is central to legal compliance.

CONCLUSION

In this article, the author argues that the design of a smart contract is the legally relevant content of the contract under EU consumer law. If automated execution, AI-based triggers, interface design, or technical irreversibility determine the emergence and performance of consumer obligations, these features fall within the scope of consumer protection. EU law is based on a functional approach that focuses on the consequences for the consumer, not on form. Conformity is assessed by how design choices affect transparency, fairness, and the practical availability of remedies.

From a regulatory perspective, this finding is important for the convergence of EU regulatory frameworks on reliability by design. Consumer law standards, MiCA Regulation requirements on the controllability of smart contracts, and the revised Product Liability Directive's approach to software as a product all point to a shift from textual compliance to architectural compliance. For developers and service providers in the field of AI-driven blockchain finance, this means that legal compliance cannot be ensured by disclosure alone. Design decisions that ensure comprehensibility, reduce structural imbalances, and guarantee effective legal remedies are needed. At the same time, it can be noted that the analysis has limitations. As the Court has not yet developed a case law on smart contracts, there remains uncertainty about the application of consumer law principles to specific technical architectures. Therefore, future research should focus on the practical implementation of these standards. This includes design methodologies, audit mechanisms, and empirical, consumer-orientated evaluation of smart contract systems.

REFERENCES

Andriciuc, R.P. and Others v Banca Românească SA (C-186/16) EU:C:2017:703.

Argelich Comelles, C. (2020) "Smart contracts o "code is law": soluciones legales para la robotización contractual", CompSciRN: Other Robotics (Topic).

Aziz v Caixa d'Estalvis de Catalunya, Tarragona i Manresa (Catalunyacaixa) (C-415/11) EU:C:2013:164.

Banco Español de Crédito SA v Joaquín Calderón Camino (C-618/10) EU:C:2012:349.

Borgogno, O. (2018) 'Smart contracts as the (new) power of the powerless? The stakes for consumers', European Review of Private Law, Issue 6, pp. 885–902.

Comegna, V. (2025) "The persistence of the opposites: AI and blockchain for transparent and secure cross-regulatory compliance and enforcement cooperation test beds in the EU digital acquis", Journal of Law, Market & Innovation, 4(2), pp. 327–357.

Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on contracts for the supply of digital content and digital services, Official Journal L 136, 22.5.2019.

Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on contracts for the sale of goods, Official Journal L 136, 22.5.2019.

Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC, OJ L 2024/2853, 18.11.2024.

Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, Official Journal L 304, 22.11.2011

Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, Official Journal L 95, 21.4.1993.

Durovic, M. and Willett, C. (2023) "A legal framework for using smart contracts in consumer contracts: Machines as servants, not masters" Modern Law Review, 86(6), pp. 1390–1421.

Efroni, Z. (2020) 'Location data as contractual counter-performance: A consumer perspective on recent EU legislation', in Finck, M. et al. (eds.) Smart Urban Mobility. MPI Studies on Intellectual Property and Competition Law, vol. 29. Berlin: Springer, pp. 257–283. https://doi.org/10.1007/978-3-662-61920-9_13

European Law Institute (2023) "Interim report on EU consumer law and automated decision-making". Vienna: European Law Institute. Available at: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Interim_Report_on_EU_Consumer_Law_and_Automated_Decision-Making.pdf (Accessed: 18.01.2026).

Kásler, Káslerné Rábai v OTP Jelzálogbank Zrt (C-26/13) EU:C:2014:282.

Liu, Z., Feng, W., Zhang, Y. and Zhu, C. (2023) "Research on the architecture of transactional smart contracts based on blockchains", Electronics, 12(18), 3923. https://doi.org/10.3390/electronics120203923

Mostaza Claro, E.M. v Centro Móvil Milenium SL (C-168/05) EU:C:2006:675.

Namysłowska, M. (2025) 'The silent death of EU consumer law and its resilient revival: Reinventing consumer protection against unfair digital commercial practices', Journal of Consumer Policy, 48, pp. 317–336. https://doi.org/10.1007/s10603-025-09590-5

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets (MiCA), Official Journal L 150, 9.6.2023, pp. 40–205.

Scattarreggia, E. (2025) "AI-driven smart contracts: enhancing consumer protection or exacerbating consumer protection challenges?", Journal of Law, Market & Innovation, 4(3), pp. 607–636.

Schrepel, T. (2021) "Smart Contracts and the Digital Single Market Through the Lens of a 'Law + Technology' Approach", European Comission. Available at: https://op.europa.eu/en/publication-detail/-/publication/224da7da-1c18-11ec-b4fe-01aa75ed71a1/language-en# (Accessed:18.01.2026).

Schrepel, T. (2021) Smart contracts and the digital single market through the lens of a law + technology approach. Brussels: European Commission. Available at: https://ssrn.com/abstract=3947174 (Accessed: 18.01.2026).

Yusuf, A. and Martinez, R. (2025) 'Smart contracts and legal enforceability: Decoding the political philosophy of code as law', Interdisciplinary Studies in Society, Law, and Politics, 4(2), pp. 292–302. https://doi.org/10.61838/kman.isslp.4.2.25