Smart Contracts and Legal Personality: Can Autonomous Code Bear Responsibility?

1. Andrei Ionescu: Department of Private Law, University of Bucharest, Bucharest, Romania
2. Michael Roberts*: Department of Political Science, Harvard University, Cambridge, USA
*****Correspondence: e-mail: michael.roberts@harvard.edu

Abstract

Smart contracts have evolved from basic automated scripts into increasingly autonomous systems capable of executing, modifying, and enforcing digital transactions without continuous human oversight. Their integration into decentralized blockchain networks challenges foundational legal concepts related to intention, agency, liability, and control. As these systems operate across jurisdictions, interact with off-chain data sources, and manage significant economic value, they expose gaps in existing legal doctrines that were built around human actors and centralized organizational structures. This narrative review synthesizes technological, doctrinal, and regulatory perspectives to examine whether autonomous smart-contract code can meaningfully bear legal responsibility. It analyzes how the architecture of blockchain networks, the nature of deterministic and adaptive smart contracts, and the dynamics of decentralized ecosystems complicate responsibility attribution. It further evaluates the suitability of classical liability doctrines—contract, tort, agency, and vicarious liability—and compares emerging models for the treatment of non-human actors such as AI systems and algorithmic agents. Global regulatory approaches are reviewed, including EU digital governance frameworks, U.S. federal and state-level developments, and proactive initiatives in jurisdictions such as Singapore, Switzerland, and the UAE. Emerging governance models involving mandatory oversight, code registration, insurance-based liability, and DAO legislation are assessed in light of their capacity to address the accountability gap created by decentralized automation. The review concludes that while smart contracts themselves cannot meaningfully possess legal personality, legal systems must develop new mechanisms to allocate responsibility among the human and institutional actors who design, deploy, and benefit from their operation. This adaptation is essential for ensuring fairness, transparency, and trust in an increasingly automated digital environment.

Keywords: Smart Contracts; Legal Responsibility; Blockchain Regulation; Autonomous Systems; DAO Governance; Algorithmic Accountability; Legal Personhood; Decentralized Technology

Received: date: 13 May 2023
Revised: date: 13 June 2023
Accepted: date: 27 June 2023
Published: date: 01 July 2023

Citation: Ionescu, A., & Roberts, M. (2023). Smart Contracts and Legal Personality: Can Autonomous Code Bear Responsibility?. *Legal Studies in Digital Age,* 2(3), 49-63.

1. Introduction

The rapid evolution of blockchain technologies has fundamentally reshaped the architecture of digital interaction, enabling a shift from centralized control to distributed mechanisms of trust in ways that challenge long-standing legal and institutional assumptions. Blockchains were initially introduced as infrastructures for secure and tamper-resistant recordkeeping, but they soon expanded into more complex frameworks capable of hosting self-executing agreements now known as smart contracts. Scholars emphasize that the transformative nature of these instruments lies in their capacity to encode legal or transactional logic directly into running code, allowing agreements to execute without intermediaries and often without subsequent human intervention (Graaf, 2019). In many jurisdictions, this shift signifies not merely a technological innovation but a deep alteration in the conceptual foundations of contractual obligations, because the execution of rights and duties becomes embedded in algorithmic processes rather than governed by human discretion (Ene, 2020). As the sophistication of these systems grows, the boundary between technological function and legal meaning becomes increasingly blurred, raising profound questions about whether smart contracts should be understood primarily as legal agreements, executable code, or hybrid constructs with unique doctrinal implications (Varbanova, 2023).

This transition from traditional digital agreements to self-executing and potentially autonomous systems introduces tensions that legal scholarship has only begun to unpack. Earlier forms of electronic contracting still hinged on identifiable human actors whose intention, consent, and liability were conceptually traceable through established legal doctrines. By contrast, smart contracts embed decision rules that can activate, modify, or terminate contractual relationships independent of continuous human direction. This automation is celebrated for reducing transaction costs and enhancing reliability, yet it also exposes participants to irreversible outcomes that unfold beyond human oversight, prompting concerns about the accountability mechanisms available when code behaves in unexpected ways (Sundell, 2023). Even when smart contracts operate exactly as written, the possibility of unintended consequences—such as unexpected interactions with oracles or vulnerabilities exploited through reentrancy attacks—creates a legal environment in which traditional fault-based reasoning becomes difficult to apply (Cohney & Hoffman, 2020). The problem is intensified when the code is deployed in decentralized environments that lack a single controlling entity, rendering questions of attribution and responsibility even more complex (Zykov, 2021).

The legal challenges surrounding responsibility become particularly significant when the automated execution of a smart contract produces harm that cannot easily be traced to a specific actor. Classical liability frameworks assume the presence of an agent whose actions or omissions can be evaluated under concepts such as negligence, breach of duty, or defective intention. However, such frameworks struggle when the operative "agent" is autonomous code executing deterministically across a decentralized network. Scholars argue that contract law is strained by the inability to evaluate machine logic for intention or consent in ways that align with human legal actors (Cvetković, 2020). Tort law similarly falters when determining foreseeability or reasonableness in contexts where the causal chain includes distributed validators, protocol designers, and unpredictable algorithmic triggers (Rizos, 2022). Agency law, which typically requires relationships of delegation or control, finds limited applicability when no party can intervene once the smart contract is deployed, thereby challenging conventional constructions of principal–agent responsibility (Onufreiciuc & Stănescu, 2021). These doctrinal deficiencies expose a growing accountability gap in which legal systems risk being unable to assign responsibility even when substantial economic harm has occurred.

The rise of scholarly discussions concerning electronic personhood, legal personality for autonomous systems, and algorithmic accountability reflects the broader uncertainty about how law should conceptualize entities that act without human supervision. Some commentators suggest that autonomous smart contracts may resemble certain limited forms of artificial agents whose behavior might be analogized to legal persons under specific regulatory models (Herian, 2022). Others argue that granting legal personality to non-sentient code would be excessively formalistic and potentially harmful, masking the roles of human designers, deployers, or users who benefit from the system's operation while avoiding responsibility (Bierć, 2019). Nonetheless, these debates highlight the fact that traditional legal subjectivity categories may be insufficient for emerging technologies that perform functions once strictly associated with humans. Discussions around algorithmic accountability further complicate the issue, as scholars explore how legal institutions can require explanations, auditability, or allocative responsibility when outcomes are generated through processes that are not fully interpretable by human observers (Ramos & Mannan, 2022). The question of whether smart contracts are merely tools or autonomous actors therefore lies at the center of ongoing doctrinal reevaluation.

A critical aspect of this debate involves distinguishing between automation and autonomy in code. Automation refers to the execution of predetermined instructions without deviation, while autonomy implies adaptive behavior or the ability to respond to external stimuli in ways not explicitly coded by human authors. Although many smart contracts function as automated scripts, a growing category interacts with dynamic data sources or incorporates logic that produces outcomes not entirely anticipated by developers. This is especially true when smart contracts integrate with oracles or operate within decentralized autonomous organizations (DAOs), where the contract's behavior reflects complex interactions among multiple layers of code and governance mechanisms (Ma, 2023). The ambiguity between these two modes of operation complicates legal analysis, because the more autonomous a system becomes, the less reasonable it is to attribute responsibility solely to the programmer or deployer. Yet, even automated systems can produce unintended effects if deployed into evolving blockchain ecosystems, thereby challenging assumptions that deterministic execution precludes unpredictability (Lisitsa & Zainutdinova, 2022). Understanding the degree of independence exhibited by different categories of smart contracts is thus essential for assessing their potential eligibility for legal responsibility.

At the global level, regulatory frameworks have not developed uniformly, resulting in fragmented approaches that reflect differing conceptualizations of smart contracts and their legal effects. Some jurisdictions treat smart contracts primarily as a technological implementation of pre-existing contractual doctrines, emphasizing the need to align code-based execution with traditional requirements of consent, offer, acceptance, and good faith (Marchenko & Dombrovska, 2021). Others adopt a more technologically driven approach, focusing on the functional capabilities of smart contracts without necessarily integrating them fully into established legal categories. For example, legislative analyses in multiple civil law systems have begun exploring whether smart contracts constitute a distinct class of digital agreements that require new regulatory principles (Michurin, 2023). Certain jurisdictions have enacted laws explicitly recognizing digital rights or blockchain-based transactions, thereby shaping the extent to which smart contracts may be enforced or interpreted in courts (Munawar, 2022). Meanwhile, comparative studies reveal that divergent doctrinal assumptions about contractual interpretation, error, and intention lead to inconsistent treatment of smart contracts across legal systems, underscoring the absence of an internationally coherent framework (Alfonso Delgado De Molina, 2022). These disparities highlight the urgency of developing clearer mechanisms to address disputes or failures arising from autonomous code.

The unresolved doctrinal challenges surrounding smart contracts demonstrate that legal systems must grapple not only with technological complexity but also with conceptual ambiguity. Many scholars note that the essence of the problem lies in the duality of smart contracts as both code and legal instrument, a dualism that complicates classification and interpretation (Klepikova et al., 2021). When a smart contract executes in a way that results in harm or an unexpected transfer of assets, courts must determine whether the legal significance lies in the intention encoded by the programmer, the understanding of the parties, the behavior of the algorithm, or the emergent effect of interactions across the blockchain network. Scholars examining the doctrinal tensions emphasize that legal systems are not yet equipped to resolve such issues consistently, particularly given the difficulty of interpreting code in light of legal norms (Sinitsyn et al., 2021). The literature also underscores that decentralized technologies disrupt established enforcement mechanisms by operating beyond national jurisdictions, creating challenges for conflict-of-laws analysis and raising questions about the applicability of traditional remedies such as rescission, restitution, or damages (Safarli, 2019). This doctrinal fragmentation reveals the need for analytical models capable of bridging technological structure and legal reasoning.

In light of these complexities, this narrative review aims to clarify the conceptual, doctrinal, and regulatory debates concerning the legal personality and responsibility of autonomous smart contracts. By synthesizing diverse strands of existing scholarship, the review evaluates competing interpretations of smart contract nature, surveys liability mechanisms within decentralized ecosystems, and analyzes proposals for governance or regulatory reform. Through descriptive analysis, it identifies gaps in current legal theories, interrogates the suitability of analogies to existing legal persons, and assesses whether alternative responsibility frameworks may be more coherent than extending legal personhood to autonomous code. The goal is to illuminate the structural challenges that arise when law interacts with decentralized automation and to provide a conceptual foundation for addressing harms that occur in environments lacking traditional oversight.

The guiding question that emerges from this inquiry is whether autonomous smart-contract code can bear legal responsibility, and if so, under what theoretical, doctrinal, or regulatory conditions this attribution might be justified.

2. Technological Foundations and Functional Autonomy in Smart Contracts

The technological foundations of smart contracts lie in the architecture of blockchain networks, whose structural features shape the degree to which code can operate independently from human oversight. Blockchains are designed as decentralized ledgers that distribute data storage and validation across numerous nodes, thereby eliminating reliance on a centralized authority and embedding trust directly into the protocol. Scholars emphasize that the decentralization of blockchains ensures that once a transaction or code execution is recorded, it becomes nearly impossible to modify without achieving consensus among a large number of participants, a characteristic closely tied to the immutability that makes smart contracts uniquely resistant to alteration after deployment (Graaf, 2019). This immutability is reinforced by consensus mechanisms, such as proof-of-work or proof-of-stake, which enable a distributed network of validators to agree on the accuracy of new blocks and the correct execution of code, creating a technical environment where execution is deterministic and resistant to tampering (Ene, 2020). The embedded consensus rules ensure that smart contracts execute precisely as written, producing a structure where technological reliability intersects with legal rigidity. This technical model introduces challenges when legal actors attempt to modify, suspend, or reverse the operations of a malfunctioning contract, because blockchain protocols offer no inherent means for intervention once code becomes part of the distributed ledger (Ramos & Mannan, 2022).

Within this architecture, smart contracts vary significantly in complexity, ranging from simple deterministic scripts to highly adaptive constructs capable of interacting with off-chain systems. The simplest type of smart contract functions as a deterministic script that executes predefined logic without considering external variables; its behavior is governed entirely by the inputs encoded at the time of its creation. Such contracts typically resemble conditional statements that activate only when specific criteria are met, and scholars note that they often mirror basic contractual obligations with minimal interpretive ambiguity (Safarli, 2019). As the technology developed, more sophisticated smart contracts emerged, incorporating condition-based logic capable of managing decentralized processes, particularly within decentralized autonomous organizations (DAOs). These DAO-governance contracts include complex voting mechanisms, dynamic asset allocation rules, and iterative functions that evolve as the organization's members interact with the system (Lisitsa & Zainutdinova, 2022). Their logic is not merely triggered by simple events but rather shaped by ongoing participation and multi-layered decision-making embedded in the algorithmic design.

Another major evolutionary step in smart-contract functionality involves the incorporation of oracles, which serve as bridges between off-chain data and on-chain execution. Oracles provide smart contracts with real-time information, such as price feeds, weather data, or performance indicators, thereby expanding the contract's operational environment beyond purely internal blockchain events. Scholars observe that oracle dependence introduces a layer of unpredictability because the accuracy and integrity of external data sources can shape contract execution in ways not fully controlled by the original developers (Cohney & Hoffman, 2020). This reliance can cause smart contracts to behave differently than anticipated, particularly if the oracle is manipulated, fails to update, or provides incorrect information. More advanced smart contracts integrate algorithmic complexity, potentially including adaptive computation or machine learning components. Although machine learning is not yet a standard feature of most smart contracts due to computational constraints, experimental architectures demonstrate that models may be embedded in or referenced by contracts, thereby enabling systems that evolve based on data patterns rather than predefined logic (Ma, 2023). Such adaptive contracts challenge the presumption that smart contracts are deterministic and raise concerns about unforeseeable behavior emerging from algorithms learning or adjusting over time.

A key conceptual distinction in analyzing smart contract behavior involves differentiating automation from autonomy. Automation refers to the execution of tasks precisely as coded, without deviation, implying that the smart contract merely follows instructions predetermined by its authors. Autonomy, by contrast, implies a degree of independence, where the system may exhibit behaviors or outcomes not explicitly anticipated by the designers due to external interactions, emergent conditions, or internal adaptive logic. Scholars argue that many smart contracts still fall within the domain of automation, performing predictable tasks that mirror traditional conditional logic (Varbanova, 2023). However, the moment a contract interacts with external data sources, multi-contract ecosystems, or algorithmic components capable of state changes, it begins to resemble an autonomous system whose actions cannot be fully controlled or predicted by human actors (Sundell, 2023). Even deterministic contracts may display autonomy-like characteristics when deployed in decentralized environments where interactions with other contracts or protocols produce outcomes beyond the foresight of the creators, especially as the blockchain ecosystem continuously evolves (Klepikova et al., 2021).

The integration of machine learning into smart-contract ecosystems highlights the transition toward increased system autonomy. While blockchains are not optimized for computationally intensive models, hybrid architectures allow smart contracts to reference off-chain machine learning outputs or integrate with decentralized oracle networks that apply predictive analytics. As scholars point out, introducing learning algorithms into contractual structures creates inherent unpredictability because machine learning models evolve based on input data and may generate outputs unbeholden to deterministic coding logic (Michurin, 2023). This unpredictability complicates the accountability landscape, particularly when adaptive behavior leads to contract execution that cannot be explained solely through code review or deterministic logic tracing. Machine learning thereby magnifies the conceptual challenges that arise when attempting to understand or regulate systems whose internal operations may not be fully transparent or auditable, raising questions about whether and how legal frameworks can attribute responsibility to actions generated by evolving algorithms (Herian, 2022).

The technical vulnerabilities of smart contracts further illustrate the difference between intended execution and actual behavior in real-world deployment. High-profile exploits, such as the DAO hack, demonstrated how seemingly minor coding oversights can produce catastrophic consequences when embedded in decentralized and autonomous environments. Scholars highlight that reentrancy attacks, where a malicious contract repeatedly calls a vulnerable contract before previous executions are completed, exploit functional gaps that developers may not anticipate during design (Rizos, 2022). These vulnerabilities underscore that the deterministic nature of smart contracts represents both a strength and a weakness: the code executes exactly as written, even when the behavior enabled by the code was unintended or undesirable (Cvetković, 2020). Because smart contracts lack built-in mechanisms for halting, reversing, or correcting erroneous states, bugs can become permanently entrenched in the blockchain, thereby creating outcomes that neither developers nor users wanted but cannot remedy without network-level intervention (Zykov, 2021). The persistence of such vulnerabilities demonstrates that smart contract behavior is not merely a function of initial design but also deeply influenced by interactions with other contracts, network protocols, and user inputs.

The philosophical notion of "code as law," famously articulated in technology scholarship, intensifies the legal responsibility problem because it treats code as self-regulating and self-executing, thereby reducing—or effectively eliminating—the role of human interpretation in governing system behavior. Scholars argue that when code is conceptualized as law, the normative frameworks traditionally provided by legal systems are displaced by technological determinism, potentially rendering traditional enforcement mechanisms obsolete (Sundell, 2023). This conceptual shift becomes particularly problematic in contexts where smart contracts perform functions traditionally managed by legally accountable entities, because the absence of interpretability or flexibility means that disputes arising from code execution cannot be easily resolved through established legal doctrines. As the literature suggests, the code-as-law paradigm creates a landscape in which responsibility is embedded in technical architecture rather than in human actors, thereby raising questions about whether this paradigm effectively shields parties from responsibility or undermines fundamental principles of justice (Graaf, 2019).

The conditions under which smart contracts behave independently of human direction arise from the interplay between design constraints, network interactions, and external data dependencies. Once deployed, many smart contracts are immutable, meaning that developers or users cannot modify their behavior even when unforeseen circumstances emerge (Ene, 2020). When contracts rely on decentralized inputs or multi-contract ecosystems, their behavior may reflect emergent patterns rather than linear execution. For example, a smart contract governing a liquidity pool may adjust asset ratios automatically based on trades occurring across the network, without a human consciously directing those changes, thereby demonstrating functional autonomy (Lisitsa & Zainutdinova, 2022). Similarly, DAO-governed contracts may execute decisions based on collective voting mechanisms, where individual participants cannot control the final outcome of algorithmic execution (Marchenko & Dombrovska, 2021). These conditions illustrate that autonomy in smart contract systems often arises not from internal learning but from the decentralized, multi-agent environments in which they operate.

Developing an analytical framework for understanding operational responsibility versus legal responsibility requires distinguishing between what a smart contract does technically and how its actions should be interpreted legally. Operational responsibility refers to the technical causation underpinning contract behavior, which can be traced to coding logic, interactions with other protocols, or data inputs from oracles or users. Scholars note that technical attribution can often identify specific functions or events that triggered a given outcome, yet this operational clarity may not translate into legal responsibility when no identifiable human actor can be held accountable under existing doctrines (Cvetković, 2021). Legal responsibility, by contrast, requires frameworks capable of evaluating intention, foreseeability, fault, or norms of behavior—all of which are difficult to apply to autonomous or semi-autonomous code. Some argue that responsibility may need to be redistributed among developers, deployers, users, and network participants, depending on their respective roles in shaping contract behavior (Berezina, 2021). Others contend that new legal categories may be necessary to capture the distinct nature of algorithmic action, particularly when smart contracts perform roles similar to trustees, agents, or financial intermediaries without the capacity for human judgment (Baiesu & Ludmila, 2021). This analytical distinction underscores the central challenge in assigning responsibility within decentralized ecosystems: the technology produces predictable operational outcomes, but the law lacks mechanisms to evaluate those outcomes in terms of liability.

These technological foundations reveal that smart contracts operate within a complex ecosystem where automation and autonomy intersect, shaped by the interplay of code, data, and decentralized network logic. As smart contracts become increasingly sophisticated and integrated into real-world systems, the question of how responsibility should be assigned becomes not only a technical matter but also a legal and philosophical one, grounded in how societies choose to conceptualize the actions of systems that operate without direct human control.

3. Legal Theories of Responsibility and the Problem of Non-Human Actors

The question of how responsibility should be assigned when the operative "actor" is non-human has long been a subject of legal inquiry, and the rise of autonomous smart contracts has reanimated debates across contract law, tort law, and agency theory. Classical liability doctrines were developed in eras when human action or organizational conduct could be identified as the source of legal effects. Contractual liability assumes that parties intentionally enter agreements, exchange manifestations of assent, and bear responsibility for breaches tied to obligations they deliberately undertook. This framework becomes difficult to apply when contractual performance is executed by code rather than human decision-making. Scholars examining digital contracting emphasize that while smart contracts may technically manifest offer and acceptance, the execution of their terms occurs without human discretion, thereby challenging the suitability of doctrines built around intention and voluntariness (Liu & Huang, 2019). Tort liability faces similar conceptual strain because negligence requires identifying a duty of care, a breach of that duty, causation, and damages, all of which presuppose a human—or at least an entity capable of acting unreasonably—behind the harmful behavior. In the context of automated systems, fault becomes difficult to assign when the behavior is the product of deterministic code rather than conscious choice (Cvetković, 2020). Strict liability may provide a partial pathway in contexts where harm results from inherently risky digital operations, but even this doctrine requires identifying a party responsible for introducing or managing the risk, a designation that becomes complex in decentralized systems (Rizos, 2022).

Agency and vicarious liability doctrines also struggle to accommodate autonomous code. Agency law presumes a relationship in which an agent acts on behalf of a principal and under the principal's control. Smart contracts, however, do not behave as traditional agents because no party has the ability to intervene or modify their actions once they are deployed to the blockchain. Scholars examining the legal nature of smart contracts caution that their autonomy undermines the possibility of applying agency principles, since control is relinquished at the moment of deployment and the code's execution is governed by network consensus rather than the will of a principal (Marchenko & Dombrovska, 2021). Similarly, vicarious liability depends on identifying a relationship between an actor and a responsible superior, such as an employer, but smart contracts complicate this inquiry because the individuals who write, deploy, or interact with code may not stand in legally recognizable hierarchical relationships (Sinitsyn et al., 2021). These doctrinal tensions reveal that the conceptual foundation of liability becomes unstable when behavior is generated by autonomous technical systems rather than by humans or legally constituted organizations.

Comparative legal analysis provides further insight into how systems historically treat non-human actors, demonstrating that legal personality is a flexible construct shaped by regulatory necessity rather than metaphysical assumptions. Corporations, for example, enjoy full legal personality, allowing them to own property, enter contracts, and be held liable even though they act through representatives. Scholars note that the legal system grants personhood to such entities as a functional tool that enables accountability and transactional reliability (Golecki, 2021). Similarly, vessels in maritime law have been treated as juridical persons capable of being sued in rem, a tradition that illustrates the willingness of legal institutions to assign personality for operational convenience rather than intrinsic qualities (Bierć, 2019). Even animals have occasionally been accorded limited legal standing in specific contexts, underscoring the fluidity of the concept. However, autonomous agents and AI systems occupy a more ambiguous terrain, because although they behave independently, they lack consciousness, moral agency, and institutional governance structures. Scholars studying AI regulation observe that while some legal systems have begun exploring frameworks for algorithmic agents, the absence of intentionality and the difficulty of assessing foreseeability complicate efforts to treat them analogously to corporations or other artificial persons (Herian, 2022). These comparisons show that while the law has dealt with non-human actors, extending legal responsibility to autonomous code introduces new conceptual complexities.

Debates surrounding electronic and algorithmic personhood gained traction as smart systems became more integrated into economic and social life. European discussions, particularly within the European Parliament, considered whether sophisticated AI systems should qualify for a form of "electronic personhood" that would allow them to bear limited liability. Scholars assessing these proposals note that they were heavily contested, with critics arguing that granting legal personality to non-conscious machines risks obscuring human responsibility while failing to provide meaningful accountability (Zenin et al., 2020). Other proposals focus on AI-specific liability models that would treat autonomous systems as risk-generating tools requiring insurance mechanisms or mandatory oversight, rather than granting them actual personhood. These models attempt to reconcile the operational independence of algorithms with the normative need for responsibility attribution, often emphasizing the obligations of developers, operators, or deployers to ensure safe system performance (Zykov, 2021). Critics of algorithmic personhood note that existing corporate models cannot be easily applied to autonomous tools because code lacks internal governance, ownership separation, or capacity for intentional wrongdoing, all of which are essential features of legal personality in traditional settings (Onufreiciuc & Stănescu, 2021). The personhood debate thus reflects deeper philosophical challenges about whether law should adapt to autonomous technologies or require that responsibility always remain anchored in human action.

A central obstacle in these debates is the challenge of interpreting intention, consent, malice, and foreseeability in systems where actions are generated by code rather than human decision-making. Intention has long served as a cornerstone of contractual and tort liability, yet code does not intend anything in the legal or moral sense. Scholars argue that while programmers may embed intentions into logic structures, the execution of code on decentralized networks involves interactions beyond their control, making it difficult to attribute the system's outcomes to a coherent human intention (Varbanova, 2023). Consent also becomes problematic when contractual terms are expressed in code that many users cannot read or fully understand, raising questions about whether agreement is meaningful when expressed through opaque computational logic (Liu & Huang, 2019). Malice is entirely inapplicable to code, yet harm may still occur through unintended functions or vulnerabilities. Foreseeability, a key condition for negligence, is equally complicated because interactions within blockchain ecosystems may generate outcomes that no programmer could reasonably anticipate, particularly when autonomous or adaptive features are present (Cohney & Hoffman, 2020). These conceptual gaps reveal how deeply classical doctrines depend on anthropocentric assumptions about cognition and volition.

The classification of smart contracts as tools, agents, or independent actors significantly influences how legal responsibility is conceptualized. Some scholars view smart contracts as mere tools, akin to automated vending machines, whose behavior is fully determined by human design and whose consequences should therefore be attributed to developers or deployers (Safarli, 2019). Others argue that in decentralized ecosystems, smart contracts operate more like agents because they carry out tasks on behalf of users or developers, interacting with other contracts and responding to external triggers in ways that resemble delegated authority (Klepikova et al., 2021). Still others suggest that smart contracts may function as independent actors within digital environments, particularly when integrated into DAOs or multi-contract systems that lack central control, raising the possibility that responsibility becomes diffuse or indeterminate (Lisitsa & Zainutdinova, 2022). These conceptualizations are complicated by the dual nature of smart contracts as both code and legal instrument, which makes them difficult to place within existing legal taxonomies.

The decentralization inherent in blockchain technology creates what many scholars identify as an "accountability gap," where the distribution of authority and control is so fragmented that no single actor can be held fully liable for harmful outcomes. Developers write the code but cannot modify it after deployment because immutability prevents unilateral intervention. Deployers initiate the contract on the blockchain, but once the system is running, they lack ongoing control, particularly when the contract interacts with external inputs or other network elements (Ene, 2020). Validators and network participants confirm transactions but typically lack intent or awareness of the specific operations being executed, thereby weakening arguments for their liability (Ramos & Mannan, 2022). Users may trigger contract functions, but their actions are limited to predefined interactions and often lack the ability to foresee complex downstream consequences. In some cases, the harm results from autonomous interactions among multiple contracts or from emergent conditions within the network, making it unclear whether anyone can be meaningfully identified as the responsible actor (Cvetković, 2021). This diffusion of responsibility raises the possibility of a legal vacuum in which harmful outcomes lack any legally accountable party.

Discussions about assigning responsibility to specific actors reveal the strengths and weaknesses of focusing on programmers, deployers, DAOs, network validators, or users. The programmer-focused model suggests that those who write the code should bear responsibility for vulnerabilities, errors, or harmful design features. Scholars who support this view argue that programmers occupy a role akin to product designers and thus should be responsible for foreseeable risks associated with their creations (Rizos, 2022). However, opponents note that immutability and decentralization mean developers often cannot correct problems post-deployment, weakening arguments that they retain control over the system once it becomes autonomous (Herian, 2022). Deployer-based responsibility focuses on the party who places the contract on the blockchain, but this model may unfairly attribute liability to actors who merely initiate code execution without fully understanding its technical complexities (Munawar, 2022). DAO-based responsibility models suggest that collective governance entities overseeing smart contracts should bear liability, but these organizations often lack legal recognition or clear internal structures, complicating enforcement (Marchenko & Dombrovska, 2021). Assigning responsibility to network participants is equally problematic because validators perform purely mechanical tasks without knowledge of contract content, making liability conceptually unsustainable (Berezina, 2021). User-based responsibility is limited because users interact only through predefined functions and cannot meaningfully influence underlying operations.

Some scholars even argue that in certain cases, the appropriate conclusion may be that no one is legally responsible, creating a responsibility vacuum. This outcome is troubling from a normative standpoint because legal systems generally seek to ensure that harms have remedies and that risks are assigned to actors capable of mitigating them (Baiesu & Ludmila, 2021). A model that allows harms to occur without accountability undermines foundational principles of justice and legal order, suggesting that existing frameworks must be adapted rather than abandoned.

Overall, the legal theories of responsibility currently available provide partial but insufficient tools for addressing harms arising from autonomous smart contract operations. Contract law struggles to accommodate systems that lack intention; tort law falters when foreseeability is undermined by algorithmic complexity; agency law fails when control dissipates across decentralized networks; and vicarious liability cannot apply without a clear organizational hierarchy. Comparative analyses show that while the law has successfully created artificial persons when needed for economic efficiency or social governance, extending such personhood to autonomous code remains a contested and philosophically fraught endeavor. The fragmentation of responsibility among programmers, deployers, platforms, validators, and users reveals a system that lacks a coherent mechanism for attributing liability. This synthesis of scholarly perspectives demonstrates both the promise and the limits of existing legal models, underscoring the need for conceptual and doctrinal innovation to address the accountability challenges posed by autonomous smart contracts.

4. Regulatory Approaches and Governance Frameworks for Autonomous Smart Contracts

Regulatory responses to autonomous smart contracts vary widely across jurisdictions, reflecting differing assumptions about the technological nature of blockchain systems, the appropriate reach of legal oversight, and the balance between innovation and risk mitigation. In the European Union, the regulatory architecture has begun to incorporate blockchain and automation into broader frameworks designed for digital markets. While the Markets in Crypto-Assets Regulation (MiCA) focuses primarily on crypto-assets and service providers, its underlying philosophy suggests a willingness to regulate not only financial intermediaries but also the infrastructures and automation mechanisms through which digital transactions occur. Scholars examining EU trends observe that the region increasingly attempts to integrate blockchain technologies into harmonized regulatory structures aimed at enhancing transparency and protecting users in digital markets (Berezina, 2021). The AI Act complements this landscape by addressing algorithmic behavior more directly, imposing obligations related to risk assessment, transparency, and oversight for high-risk AI systems. Although smart contracts are not explicitly classified as AI in current drafts, the Act's emphasis on explainability and human oversight resonates strongly with smart contract governance, particularly when contracts operate autonomously or influence financial or safety-critical environments. Additional EU instruments, such as the Digital Services Act, reinforce accountability mechanisms for automated decision-making processes, creating a layered regulatory context in which smart contracts may be indirectly regulated through broader digital governance rules (Herian, 2022).

In the United States, regulatory approaches are more fragmented due to the combination of federal and state authorities. Federal agencies such as the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) have taken active roles in policing blockchain-related activities, often viewing smart contracts through the lens of securities and commodities regulation. Scholars note that these agencies tend to apply traditional functional tests to determine whether smart contract–based transactions fall within their jurisdiction, meaning that the legal characterization of a digital instrument depends on the economic reality of the transaction rather than its technical form (Graaf, 2019). State-level legislation adds another layer of complexity: Wyoming has been especially proactive, enacting laws recognizing decentralized autonomous organizations (DAOs) as legal entities capable of owning property and entering contracts. These statutes impose certain governance structures and liability rules, such as requirements for registered agents and disclosures, thereby creating a bridge between blockchain-native forms of organization and traditional corporate law (Marchenko & Dombrovska, 2021). Similar developments have occurred in the Marshall Islands, where legislation creates DAO-based corporate forms with limited liability features. While these frameworks attempt to impose responsibility onto decentralized organizations, they do not directly resolve the accountability challenges posed by autonomous smart contracts themselves, which often function independently of organizational structures.

Other jurisdictions, particularly those with innovation-driven regulatory agendas such as Singapore, Switzerland, and the United Arab Emirates, have adopted more flexible or supportive approaches to blockchain governance. Singapore promotes regulatory sandboxes that allow blockchain developers to test autonomous financial tools under controlled oversight, a strategy that scholars highlight as a means of balancing innovation with public protection (Munawar, 2022). Switzerland's DLT Act provides legal clarity for token-based systems and envisions blockchain infrastructures as integral components of financial market regulation. Within this framework, responsibilities are more clearly assigned to operators and service providers, even in decentralized settings (Onufreiciuc & Stănescu, 2021). The UAE, particularly through the Dubai International Financial Centre (DIFC), has introduced forward-looking frameworks for digital assets, emphasizing flexibility and recognition of technologically mediated forms of contracting. These jurisdictions typically focus on building governance mechanisms around blockchain infrastructures rather than imposing personality on smart contracts themselves, thereby shaping accountability through institutional rather than technical frameworks (Lisitsa & Zainutdinova, 2022).

One significant development across several jurisdictions is the establishment of liability rules for blockchain-based corporate forms, particularly DAOs. Wyoming's DAO laws and the Marshall Islands' legislative frameworks attempt to address the governance and liability challenges inherent in decentralized systems by imposing structures that mirror corporate governance. These laws require DAOs to adopt operating agreements and clarify whether they function as member-managed or algorithmically managed entities, with different liability outcomes for each model. Scholars analyzing these developments note that algorithmically managed DAOs pose unique challenges because their governance logic depends entirely on autonomous code, thereby raising questions about whether liability should be assigned to members, developers, or the DAO entity itself (Cvetković, 2020). Similar issues arise in blockchain-based foundations, which may hold assets and execute decisions through automated logic. These regulatory experiments suggest that policymakers are willing to adapt corporate law to accommodate autonomous systems, yet significant uncertainty remains about how liability should be distributed when code executes actions unforeseeable or unintended by human actors (Baiesu & Ludmila, 2021).

Consumer protection is another domain in which regulatory frameworks struggle to keep pace with autonomous smart contracts. Traditional consumer protection law assumes that transactions can be rescinded, renegotiated, or voided under certain circumstances, yet the immutability of blockchain systems often eliminates these remedies. Scholars studying smart contract vulnerabilities emphasize that irreversible execution can leave consumers exposed to harm in cases of coding errors, oracle failures, or malicious exploitation (Rizos, 2022). Financial crime regulation adds further complexity: autonomous smart contracts can facilitate or inadvertently enable money laundering, fraud, or sanctions evasion, especially when integrated into decentralized finance (DeFi) systems that lack centralized oversight. Regulators in many jurisdictions increasingly require exchanges and service providers to implement know-your-customer (KYC) and anti-money-laundering (AML) mechanisms, but these controls do not directly govern the behavior of autonomous code once deployed on the blockchain (Ene, 2020). Data governance frameworks also intersect with smart contract regulation, particularly in contexts where contracts store or process personal data through immutable ledgers. The incompatibility between immutability and data erasure rights, such as those found in the EU's GDPR, poses unresolved legal contradictions (Berezina, 2021).

Auditability and explainability requirements have become central to emerging regulatory responses in light of the challenges autonomous systems pose. Smart contracts, especially those integrated with oracles or algorithmic logic, may behave in ways that are not readily understandable to regulators or users. Scholars argue that transparency obligations similar to those proposed in AI regulation may be necessary to ensure accountability in autonomous blockchain systems (Michurin, 2023). Some proposals require that smart contracts include audit trails, metadata documentation, or the capacity for third-party verification to facilitate dispute resolution or regulatory compliance. However, technical constraints complicate these aspirations: the very features that make blockchain secure—immutability and decentralization—make it difficult to implement after-the-fact transparency mechanisms. In addition, explainability remains a challenge when smart contract behavior emerges from complex interactions between multiple on-chain and off-chain components (Cohney & Hoffman, 2020). As a result, regulatory frameworks increasingly emphasize pre-deployment review, certification, or risk assessment as mechanisms for ensuring responsible behavior before code is activated.

The phenomenon of "regulatory bypass" further complicates governance, as smart contracts deployed on decentralized networks can operate across jurisdictions without regard to national borders. Scholars note that this transnational execution environment allows autonomous contracts to persist even when regulators attempt to prohibit certain activities, creating enforcement challenges that mirror those seen in cybercrime and peer-to-peer technologies (Zykov, 2021). The absence of a central authority means that regulators cannot easily compel modification or termination of harmful or unlawful contract behavior. Moreover, decentralized platforms can redeploy modified versions of prohibited contracts in new locations or under anonymous identities, thereby evading oversight. This environment challenges traditional regulatory assumptions grounded in territorial jurisdiction and centralized enforcement, prompting calls for cooperative international frameworks or technologically embedded compliance mechanisms (Herian, 2022).

In response to these challenges, scholars have proposed a variety of governance models intended to provide accountability while preserving the innovative potential of autonomous smart contracts. One widely discussed model involves mandatory human oversight, requiring a designated individual or entity to retain a "kill switch" or override capability. Proponents argue that this mechanism would ensure that harmful actions can be halted, thereby reducing risk and facilitating compliance with legal obligations (Varbanova, 2023). Critics, however, argue that such mechanisms undermine decentralization and could create new vulnerabilities by introducing single points of failure. Another proposed model centers on registration or licensing requirements for autonomous code, similar to mechanisms used in broadcasting, financial services, or pharmaceuticals. Under this model, developers would need to submit documentation or undergo technical review before deploying smart contracts, thereby creating a regulatory checkpoint that could prevent harmful deployments (Berezina, 2021). Insurance-based liability models represent another avenue, shifting responsibility from identifying at-fault actors to ensuring financial coverage for losses arising from autonomous contract behavior. This approach echoes historical strategies used in maritime and industrial regulation to manage risks associated with complex systems (Baiesu & Ludmila, 2021). Some proposals focus on developer or deployer responsibility frameworks, arguing that those who create or activate autonomous code should bear strict or semi-strict liability for risks that materialize post-deployment (Rizos, 2022). These proposals differ in their emphasis on innovation, control, and accountability, reflecting broader philosophical tensions about the proper role of law in regulating autonomous technologies.

A central normative question emerging from the literature concerns whether smart contracts should be granted some form of legal personhood. Proponents of legal personhood argue that treating autonomous code as a juridical entity could streamline liability allocation, allow contracts to hold assets or insurance, and create a coherent regulatory identity for decentralized systems (Golecki, 2021). Critics counter that legal personhood risks obscuring human responsibility, creating "empty shell" entities that lack governance, moral agency, or the internal structure necessary for meaningful accountability (Onufreiciuc & Stănescu, 2021). They argue that extending personhood to non-sentient code may produce more legal confusion than clarity, particularly when responsibility could instead be assigned to human actors involved in design, deployment, or governance processes. The debate reflects deeper concerns about whether the law should adapt to autonomous systems by creating new legal categories or whether responsibility should remain anchored in human behavior regardless of technological complexity (Zenin et al., 2020).

Despite significant progress, major gaps persist in global regulatory approaches to autonomous smart contracts. There is no consistent international framework governing liability, transparency, or consumer protection in decentralized ecosystems. Jurisdictions vary widely in their technological literacy, regulatory priorities, and philosophical orientations toward autonomy and responsibility. Scholars emphasize that many regulatory tools remain ill-suited to decentralized systems that challenge assumptions about control, authority, and intervention (Cvetković, 2021). The absence of clear dispute resolution mechanisms for smart contract failures leaves users vulnerable, while the incompatibility between immutability and legal remedies continues to undermine trust. Additionally, few jurisdictions have addressed the question of systemic risk arising from interconnected autonomous contracts, which may propagate failures across financial or logistical infrastructures.

Overall, the evolution of regulatory frameworks reveals both the promise and the limitations of current governance strategies. While jurisdictions experiment with innovative models such as DAO legislation, algorithmic oversight, and sandbox environments, deeper structural reforms are necessary to align legal accountability mechanisms with the technological realities of autonomous smart contracts. A coherent approach will require reconciling decentralization with regulatory authority, balancing innovation with risk management, and determining the appropriate role of human actors in systems increasingly shaped by autonomous logic.

5. Conclusion

The evolution of smart contracts from simple automated scripts into increasingly autonomous systems presents one of the most profound challenges modern legal frameworks have faced in the digital era. Their integration into decentralized blockchain networks disrupts long-standing assumptions about agency, intention, responsibility, and control. As smart contracts begin to operate with a level of independence from their creators and users, the law must grapple with the consequences of actions generated by systems that cannot think, intend, or understand but nonetheless create real-world effects, transfer assets, and sometimes cause harm. This challenge is not merely technical but conceptual: smart contracts force a reexamination of what it means to act, to decide, and to be responsible within a legal system that has historically centered humans and hierarchical organizations as the primary bearers of rights and duties.

Throughout this narrative review, an important theme emerges: smart contracts exist at the intersection of law and technology, and neither domain alone can fully account for their nature. Technologically, smart contracts are resistant to intervention, predictable yet capable of interacting in unpredictable ways, and situated within decentralized networks that dissolve traditional chains of authority. Legally, they blur the boundaries between tools and actors, between code and contract, and between deterministic execution and autonomous behavior. This duality creates conceptual friction, particularly when legal doctrines attempt to map human-centered categories such as intention, negligence, and agency onto systems that lack consciousness, volition, or flexibility.

Existing legal frameworks—contract, tort, agency, and corporate law—provide partial analogies but ultimately fail to accommodate the unique characteristics of autonomous smart contracts. Contract law struggles with unilateral execution and the absence of interpretive flexibility. Tort law falters when foreseeability becomes difficult to assess in decentralized and algorithmically complex environments. Agency law breaks down when no party retains control after deployment. Even the attribution models of corporate law, although more adaptable, cannot easily be extended to non-organizational entities that lack governance structures, internal decision-making processes, or stable legal identities.

Regulatory systems around the world have begun exploring solutions, yet global approaches remain fragmented. The European Union offers a structured regulatory vision built around transparency, accountability, and user protection, but it has not fully resolved how smart contracts fit within its AI and digital governance frameworks. The United States relies on functional tests and agency oversight, resulting in a patchwork of federal and state initiatives that provide clarity in some areas while leaving others unaddressed. Jurisdictions such as Singapore, Switzerland, and the UAE demonstrate how proactive regulation can support innovation, but even these advanced models must continually adapt as autonomous systems grow more complex and interconnected.

Attempts to regulate decentralized ecosystems face a fundamental paradox: the very features that make blockchain environments resistant to centralized abuse also make them resistant to centralized regulation. Immutability, decentralization, and pseudonymity create fertile ground for innovation but also restrict traditional forms of oversight and enforcement. This leads to an accountability gap in which developers, deployers, validators, and users each play roles in the operation of smart contracts, yet none of them neatly satisfy the conditions necessary for legal responsibility as currently understood. The possibility that some harmful outcomes might lack any legally identifiable responsible party represents a profound challenge for rule-of-law values and the legitimacy of digital governance systems.

To address these challenges, scholars and regulators have proposed several models, including mandatory human oversight, registration or certification requirements for autonomous code, insurance-based liability frameworks, and stronger responsibility assignments to developers or deployers. These proposals vary in feasibility and desirability. Some prioritize innovation and minimal intervention, while others emphasize safety, accountability, and risk distribution. Debates over granting legal personhood to smart contracts reflect even deeper divisions about how law should conceptualize autonomous systems: whether as tools whose risks must always be tied to human actors, as organizational analogues deserving their own legal identity, or as something entirely new that requires legal categories not yet developed.

A coherent future regulatory model must strike a careful balance. It must recognize the value of decentralization while ensuring mechanisms for accountability and redress. It must preserve opportunities for innovation while preventing harms that arise from opaque or uncontrollable automation. It must acknowledge the limitations of existing doctrines without prematurely adopting solutions—such as algorithmic personhood—that might generate more problems than they solve. Most importantly, it must maintain a commitment to fundamental legal principles: fairness, predictability, transparency, and the capacity to assign responsibility in a way that encourages both innovation and societal trust.

This narrative review demonstrates that smart contracts occupy a liminal space between technological autonomy and legal accountability. They challenge traditional legal assumptions, expose doctrinal gaps, and highlight the need for interdisciplinary approaches capable of bridging the divide between code and law. As smart-contract ecosystems expand—powering decentralized finance, supply chain automation, autonomous organizations, and future AI-driven infrastructures—the pressure on legal systems to adapt will only intensify. The question is not whether smart contracts will reshape legal responsibility, but how legal systems will choose to interpret, regulate, and integrate these autonomous digital actors.

Ultimately, the task ahead is one of conceptual clarity and regulatory creativity. Clear definitions of autonomy, responsibility, and control must guide legal analysis, while flexible regulatory frameworks must ensure accountability without suppressing beneficial innovation. The autonomous behavior of smart contracts does not eliminate the human element entirely, but it does complicate traditional responsibility models in ways that require thoughtful doctrinal evolution. As societies increasingly rely on autonomous digital systems, the law must evolve alongside them, ensuring that technological progress is supported by governance mechanisms that uphold justice, protect users, and sustain confidence in emerging digital infrastructures.

The central question guiding this review—whether autonomous smart-contract code can bear legal responsibility—ultimately leads to a broader inquiry about the future of law in an era of algorithmic governance. While smart contracts themselves cannot meaningfully hold intentions or duties, the legal system must still determine how responsibility flows through the networks of actors who design, deploy, maintain, and benefit from their operations. The solution will likely involve a combination of human oversight, institutional structures, technical safeguards, and new legal doctrines capable of capturing the unique nature of autonomous algorithmic action. As legal systems confront this challenge, their responses will shape not only the governance of smart contracts but the evolution of digital society itself.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all participants who participate in this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

Alfonso Delgado De Molina, R. (2022). Smart Contracts. 107-141. https://doi.org/10.1093/oso/9780192858467.003.0007

Baiesu, S., & Ludmila, B.-R. (2021). The Contract for the Benefit of a Third Person. Defining Aspects After the Modernization of the Civil Code of the Republic of Moldova. *National Law Journal*(1(243)), 133-141. https://doi.org/10.52388/1811-0770.2021.1(243).12

Berezina, E. A. (2021). Using a Smart Contract as a Legal Technology: National and Foreign Legislative Practice. *The Rule-of-Law State Theory and Practice*, *17*(1(63)), 97-118. https://doi.org/10.33184/pravgos-2021.1.7

Bierć, A. (2019). Towards Normatively Limited Judicial Sanction [Structured Discretion] as a Proportional Response to the Defectiveness of Legal Action (Contract) in Modern Legal Transactions. *Studia Prawnicze / the Legal Studies*, 7-36. https://doi.org/10.37232/sp.2019.4.1

Cohney, S., & Hoffman, D. A. (2020). Transactional Scripts in Contract Stacks. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3523515

Cvetković, P. (2020). Liability in the Context of Blockchain-Smart Contract Nexus: Introductory Considerations. *Zbornik Radova Pravnog Fakulteta Nis*, *59*(89), 83-100. https://doi.org/10.5937/zrpfn0-28637

Cvetković, P. (2021). Synthesis of the Legal Text and the Program Code: The Case of the Ricardian Contract. *Zbornik Radova Pravnog Fakulteta Nis*, *60*(90), 61-76. https://doi.org/10.5937/zrpfn0-29556

Ene, C. (2020). Smart Contracts - The New Form of the Legal Agreements. *Proceedings of the International Conference on Business Excellence*, *14*(1), 1206-1210. https://doi.org/10.2478/picbe-2020-0113

Golecki, M. J. (2021). The Limits of the Consensual Principle and the Structure of a Contract of Obligation in Italian Civil Law. *Nieruchomości Kwartalnik Ministerstwa Sprawiedliwości*, *Specjalne*(V), 295-309. https://doi.org/10.5604/01.3001.0015.5837

Graaf, d. (2019). From Old to New: From Internet to Smart Contracts and From People to Smart Contracts. *Computer Law & Security Review*, *35*(5), 105322. https://doi.org/10.1016/j.clsr.2019.04.005

Herian, R. (2022). Techno-Legal Supertoys. 246-268. https://doi.org/10.1093/oso/9780192858467.003.0012

Klepikova, O., Harahonych, O., & Antoshyna, I. (2021). Smart Contracts in the Context of Digitalization: The Legal Realities of World Experience. *Cuestiones Políticas*, *39*(70), 844-861. https://doi.org/10.46398/cuestpol.3970.51

Lisitsa, V., & Zainutdinova, E. (2022). Digital Rights and Their Use in a Smart Contract. *Juridical Science and Practice*, *18*(1), 29-38. https://doi.org/10.25205/2542-0410-2022-18-1-29-38

Liu, Y., & Huang, J. (2019). Legal Creation of Smart Contracts and the Legal Effects. *Journal of Physics Conference Series*, *1345*(4), 042033. https://doi.org/10.1088/1742-6596/1345/4/042033

Ma, A. (2023). Blockchain-Enabled Smart Legal Contracts. https://doi.org/10.5772/intechopen.109041

Marchenko, V., & Dombrovska, A. (2021). On Determining the Legal Nature of Smart Contracts. *170*. https://doi.org/10.2991/aebmr.k.210320.031

Michurin, I. (2023). Public Contract on the Internet and New Legislation on Digital Content. *University Scientific Notes*, 4-13. https://doi.org/10.37491/unz.95.1

Munawar, M. (2022). The Legality of Smart Contract in the Perspectives of Indonesian Law and Islamic Law. *Al-Istinbath Jurnal Hukum Islam*, *7*(1), 269. https://doi.org/10.29240/jhi.v7i1.4140

Onufreiciuc, R., & Stănescu, L.-E. (2021). Regulation of the Smart Contract in (Romanian) Civil Law. *European Journal of Law and Public Administration*, *8*(2), 95-111. https://doi.org/10.18662/eljpa/8.2/164

Ramos, S., & Mannan, M. (2022). Watch the Gap: Making Code More Intelligible to Users Without Sacrificing Decentralization? , 133-139. https://doi.org/10.1109/cbi54897.2022.10059

Rizos, E. (2022). A Contract Law Approach for the Treatment of Smart Contracts' 'Bugs'. *European Review of Private Law/Revue Européenne De Droit Privé/Europäische Zeitschrift Für Privatrecht*, *30*(Issue 5), 775-802. https://doi.org/10.54648/erpl2022037

Safarli, N. (2019). Smart Contract: The Concept, Legal Nature, Features of Conclusion and Execution. *Legal Concept*(4), 54-60. https://doi.org/10.15688/lc.jvolsu.2019.4.7

Sinitsyn, S., Diakonova, M. O., & Chursina, T. (2021). Smart-Contracts in the Digital Economy: Contractual Regulation and Dispute Resolution. *Digital Law Journal*, *2*(4), 40-50. https://doi.org/10.38044/2686-9136-2021-2-4-40-50

Sundell, V. (2023). Code Is Law: A Legal Justification of Irreversible Execution of Smart Contracts Through Consideration. https://doi.org/10.31219/osf.io/z9gma

Varbanova, G. (2023). Legal Nature of Smart Contracts: Contract or Program Code? *Journal of Digital Technologies and Law*, *1*(4), 1028-1041. https://doi.org/10.21202/jdtl.2023.44

Zenin, S., Kuteynikov, D. L., Izhaev, O., & Yapryntsev, I. M. (2020). Law Making in the Conditions of Algorithmization of Law. *Lex Russica*(7), 97-104. https://doi.org/10.17803/1729-5920.2020.164.7.097-104

Zykov, D. (2021). Blockchain and Other Technologies in the System of Traditional State and Legal Institutions. *Legal Concept*(3), 42-46. https://doi.org/10.15688/lc.jvolsu.2021.3.7