ISSLP
Interdisciplinary Studies in Society, Law and Politics

Original Research

Smart Contracts and Legal Enforceability: Decoding the Political Philosophy of Code as Law

Amina. Yusuf[1], Robert. Martinez[2*]

[1] Department of Law, University of Lagos, Lagos, Nigeria
[2] Department of Law, Yale University, New Haven, USA

*** Corresponding author email address**: robert.martinez@yale.edu

Received: 2025-02-12 **Revised:** 2025-03-10 **Accepted:** 2025-03-16 **Published:** 2025-04-01

ABSTRACT

To explore the legal and philosophical implications of smart contracts, with a focus on their enforceability and the political significance of the "code as law" paradigm. This study adopts a narrative review approach using a descriptive analytical method to examine the intersection of law, technology, and political theory. Sources were selected from academic databases published between 2020 and 2024, encompassing legal scholarship, computer science literature, and political philosophy. Thematic analysis was used to synthesize key ideas related to legal enforceability, algorithmic governance, and the transformation of legal subjectivity in coded systems. The review highlights significant tensions between traditional legal norms and the deterministic nature of smart contracts. While smart contracts offer advantages in terms of automation and efficiency, they also lack the capacity to address ambiguity, context, and moral judgment. These contracts challenge core principles of legal theory, including consent, due process, and equitable remedies. Jurisdictions differ in their responses, ranging from proactive legal recognition to cautious regulatory experimentation. Hybrid models of enforcement and reliance on oracles demonstrate emerging attempts to bridge the gap between code and law. Smart contracts represent a disruptive force in the legal domain, necessitating critical reflection on the philosophical and institutional foundations of modern legal systems. Their adoption must be guided by a commitment to justice, democratic governance, and interdisciplinary oversight to ensure that legal innovation aligns with human values and ethical responsibility.

Keywords: *Smart contracts, legal enforceability, code as law, digital sovereignty, algorithmic governance, political philosophy, legal theory, rule of law, blockchain regulation.*

How to cite this article:

Yusuf, A., & 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), 292-302. https://doi.org/10.61838/kman.isslp.4.2.25

1. Introduction

The emergence of blockchain technology has redefined foundational assumptions in a wide range of fields, from finance and supply chain management to governance and law. At the heart of this disruption lies the concept of smart contracts—self-executing code that operates on decentralized blockchain networks and enforces predefined rules without reliance on traditional intermediaries. Originally conceptualized in the 1990s, smart contracts have gained considerable traction only in recent years, particularly with the proliferation of blockchain platforms such as Ethereum. These platforms provide an infrastructure in which logic-based scripts can autonomously facilitate, verify, and enforce the performance of contractual obligations. As Abdullah and Goh explain, smart contracts transform the nature of agreements by embedding contractual terms into digital code that executes automatically when specific conditions are met, eliminating the need for centralized

authorities or legal enforcement mechanisms (Abdullah & Goh, 2022).

This development has prompted scholars to reassess the very role of law in regulating digital interactions. One of the most radical conceptual shifts introduced by smart contracts is the idea of "code as law," a phrase popularized by Lawrence Lessig but now deeply embedded in academic and policy discourses. This view suggests that technological artifacts, particularly software code, can operate as regulatory mechanisms in the same way as legal norms. Rather than relying on normative language subject to interpretation, smart contracts impose an automated regime of compliance based solely on logical conditions. As Papantoniou notes, this represents a departure from the flexibility and context-dependency of traditional legal interpretation toward a rigid, execution-driven framework where the code itself dictates permissible and impermissible actions (Papantoniou, 2020). This paradigm shift raises profound political and philosophical questions about the delegation of normative authority from human institutions to technological systems.

However, the rise of smart contracts has also surfaced a range of legal and philosophical challenges concerning their enforceability. The primary issue lies in reconciling the deterministic nature of code with the interpretive, discretionary essence of law. In conventional legal systems, contracts are subject to a variety of doctrines, such as unconscionability, impossibility, and good faith, which enable courts to adapt enforcement to specific circumstances. Smart contracts, by contrast, execute exactly as coded, without room for human judgment. Donn observes that this gap generates tension, particularly in cross-border and high-stakes transactions where the failure of a smart contract to consider external factors can produce unintended or inequitable outcomes (Donn, 2023). Additionally, since smart contracts often operate independently of legal language or jurisdictional grounding, it becomes difficult to determine the applicable law or the forum for dispute resolution should something go awry.

The problem is further exacerbated by the increasing abstraction of legal authority in digital spaces. While traditional contracts are embedded within institutional frameworks backed by courts and state power, smart contracts are often deployed in transnational environments governed by decentralized code. This poses a unique dilemma: how should legal systems respond to agreements that are designed to operate outside their jurisdictional boundaries? As Alikhani and Hamidi argue, legal systems face the difficult task of balancing innovation and control, ensuring that smart contracts do not evolve into a parallel system of private ordering immune from public accountability (Alikhani & Hamidi, 2021). This raises questions about legitimacy, transparency, and the capacity of law to adapt to technological transformations without losing its core normative functions.

Addressing the gap between code and normative legal systems has therefore become one of the most pressing challenges for legal scholars, technologists, and policymakers alike. As Musthafa and colleagues point out, smart contracts expose the limitations of existing legal doctrines while also highlighting the need for interdisciplinary frameworks capable of integrating legal reasoning with computational logic (Musthafa et al., 2024). This gap is not merely a technical issue but a deeply philosophical one that touches on the foundations of authority, trust, and human agency in digital governance. If left unaddressed, it risks allowing private actors to embed unaccountable forms of power into technological infrastructures that affect everyday life.

The objective of this review is to critically examine the conceptual, legal, and philosophical dimensions of smart contracts, with particular emphasis on the political implications of the “code as law” paradigm. Rather than providing a purely technical or jurisprudential account, this study aims to synthesize insights from law, political theory, and technology studies to offer a comprehensive understanding of how smart contracts challenge existing notions of enforceability and governance. Through a descriptive analytical method, the review maps key debates, emerging regulatory frameworks, and theoretical discourses, offering a grounded yet critical perspective on the future trajectory of code-based legal systems.

2. Methodology

This narrative review adopts a descriptive analytical method to examine the evolving intersection of smart contracts, legal enforceability, and the political philosophy encapsulated in the notion of "code as law." The aim is not to statistically quantify findings but to conceptually map, interpret, and synthesize diverse

scholarly perspectives, legal commentaries, and philosophical analyses published within the last five years, from 2020 to 2024. The descriptive approach enables a critical exploration of the normative, technical, and philosophical dimensions of the subject, helping to decode how digital contractual logic interacts with traditional jurisprudence and political governance structures. This method is particularly suited for interdisciplinary inquiries where complex, often abstract, constructs such as legal authority, technological determinism, and philosophical autonomy need to be discussed holistically and contextually.

In selecting materials, a rigorous literature review was conducted across a variety of scholarly databases including JSTOR, Scopus, Web of Science, HeinOnline, SSRN, and Google Scholar. Key search terms used in combinations included “smart contracts,” “legal enforceability,” “blockchain law,” “code is law,” “techno-legal philosophy,” “algorithmic governance,” and “automated legal instruments.” The search strategy focused on peer-reviewed journal articles, policy papers, legal case analyses, and interdisciplinary conference proceedings. The temporal frame for inclusion was set between 2020 and 2024 to ensure that the most recent debates and developments are reflected. Sources were included only if they engaged substantively with the theoretical, normative, or regulatory implications of smart contracts and not merely their technical implementations. Works from legal studies, philosophy of law, computer science (with legal implications), and political theory were prioritized, with special attention to the writings of contemporary theorists and jurists who have critically engaged with the idea of digital code supplanting or transforming traditional forms of legal governance.

The analytical process involved an interpretive reading of the selected texts, with a focus on thematic convergence, conceptual disagreements, and emerging legal-philosophical narratives. Recurring themes such as the rigidity of code versus the flexibility of human law, the replacement of legal intermediaries with decentralized code, and the philosophical implications of automating contractual consent were identified and developed into distinct sections within the article. Particular attention was given to cross-jurisdictional approaches to smart contract recognition and enforcement, as well as the broader ideological undercurrents—such as libertarianism, digital sovereignty, and techno-determinism—that shape the discourse around "code is law." Throughout the analysis, care was taken to contextualize the findings within ongoing academic debates and regulatory developments, thereby grounding philosophical reflections in real-world legal and technological transformations.

3. Conceptual Foundations

3.1. What Are Smart Contracts?

Smart contracts are self-executing programs that operate on blockchain networks, automatically enforcing terms and conditions defined by their code. These contracts do not require a third party to monitor or verify the performance of obligations, as the execution occurs automatically when predetermined conditions are met. According to Guo, smart contracts represent a hybrid between legal instruments and computational protocols, bridging the gap between intent and action through automation (Guo, 2023). The fundamental idea is to replicate the logic of traditional contracts—offer, acceptance, and performance—within a digital environment, thereby reducing the need for intermediaries and minimizing the risk of non-compliance.

Technically, smart contracts can be classified into several typologies based on complexity and functionality. Bohyer and Hayajneh distinguish between simple smart contracts, such as those that execute payments upon delivery, and complex ones that involve multi-party workflows, data inputs from external sources, or conditional branching logic (Bohyer & Hayajneh, 2023). The common features across these categories include automation, immutability, and trustless execution. Once deployed on a blockchain, the contract's terms are virtually immutable and tamper-proof, ensuring consistent behavior across all network nodes.

Automation is one of the defining characteristics of smart contracts. Through the use of conditional logic—typically structured as “if/then” statements—the contract autonomously determines whether its criteria have been satisfied and initiates the corresponding outcomes. For instance, if a buyer transfers a specific amount of cryptocurrency to a seller, the smart contract will automatically release the purchased asset or service. Budiyanto explains that this automation not only

increases efficiency but also reduces the risk of opportunistic behavior and disputes over non-performance (Budiyanto, 2023).

Real-world applications of smart contracts are already widespread and continue to grow. In the Ethereum blockchain, for example, smart contracts underpin decentralized finance (DeFi) protocols, non-fungible tokens (NFTs), and decentralized autonomous organizations (DAOs). In supply chain management, smart contracts facilitate real-time tracking and payment release upon verified delivery. Donn highlights the use of smart contracts in international trade, where automated escrow services can minimize transactional friction and enhance transparency across borders (Donn, 2023). In the insurance industry, parametric contracts automatically pay out when certain conditions—like rainfall levels or flight delays—are met, as noted by Almahasneh in her discussion on blockchain-based legal technologies (Almahasneh, 2024).

3.2. Legal Enforceability of Smart Contracts

Despite their technical sophistication, the enforceability of smart contracts in traditional legal systems remains contentious. Legal enforceability requires that a contract satisfy certain foundational principles, including offer, acceptance, consideration, and the intention to create legal relations. Chauhan points out that while smart contracts may technically fulfill the offer and acceptance requirements, determining mutual intention and valid consideration in machine-readable code can be problematic (Chauhan, 2020). Furthermore, in the absence of human-readable terms, it becomes difficult for courts to interpret the contractual meaning or assess whether consent was truly informed.

Jurisdictional recognition of smart contracts also varies significantly. In common law jurisdictions such as the United States, courts have begun to accept the validity of smart contracts under the principle that contracts formed by electronic means are legally binding if they meet traditional requirements. Atiyah and colleagues explore the challenges of enforcing such contracts in cross-jurisdictional transactions, emphasizing the need for legal clarity in environments where the governing law or forum for dispute resolution is ambiguous (Atiyah et al., 2024). In civil law systems, where legal formalism is more pronounced, courts may be less inclined to recognize the enforceability of contracts that lack traditional documentation or judicial oversight.

Some countries have started introducing legislation to regulate or acknowledge smart contracts within their legal systems. Onufreiciuc and Stănescu examine Romania's civil law framework and its cautious approach toward recognizing smart contracts, suggesting that while technical neutrality is maintained, the legal infrastructure is still adapting to accommodate these digital instruments (Onufreiciuc & Stănescu, 2021). Similarly, Nazarov highlights how crypto exchanges and decentralized applications pose new challenges for traditional contract law classifications, especially in environments that lack regulatory maturity (Nazarov, 2024).

Case studies from emerging jurisdictions and regulatory sandboxes provide further insight into this legal transition. For instance, the state of Arizona in the U.S. has enacted legislation explicitly recognizing smart contracts as legally enforceable, provided they comply with other statutory requirements. In contrast, the European Union has adopted a more measured approach, focusing on digital governance and consumer protection while exploring the role of smart contracts within the broader Digital Services Act framework. Berezina's comparative analysis reveals that while national laws are slowly evolving, the global legal system remains fragmented in its treatment of smart contracts (Berezina, 2021).

Ultimately, the legal enforceability of smart contracts hinges not only on their technological functionality but also on their ability to integrate with existing legal norms and procedural safeguards. As Baso and colleagues argue, the legitimacy of smart contracts will depend on whether they can uphold fundamental principles of justice, fairness, and accountability, rather than simply achieving mechanical execution (Baso et al., 2024). Without this integration, smart contracts risk operating in a legal vacuum, where the absence of recourse mechanisms could undermine both user confidence and systemic trust.

3.3. Code as Law: Philosophical and Political Origins

The notion that code could function as a form of law first gained serious traction through the work of Lawrence Lessig, whose foundational theory of "Code is Law" asserted that in digital spaces, software architecture

regulates behavior as effectively as legal norms do in the physical world. Lessig argued that while traditional legal systems govern through statutes enforced by state institutions, cyberspace is governed by code—written by developers who shape the parameters of permissible and impermissible action (Papantoniou, 2020). In this environment, code is not merely a technical instrument but a normative framework that determines user freedoms, restrictions, and capacities. As Zavyalova and colleagues note, the increasing sophistication of blockchain systems and smart contracts has only intensified this phenomenon, embedding normative rules directly into digital protocols rather than legislative texts (Zavyalova et al., 2019).

This transformation signals a broader shift toward technocratic governance, where decision-making authority is displaced from public deliberation and transferred to technical systems designed by private actors. Whereas democratic legal systems rely on participatory processes and judicial interpretation, code-based governance emphasizes efficiency, consistency, and automaticity. Donn critiques this shift, observing that technocratic logic tends to prioritize control and predictability over ethical reflection or democratic accountability (Donn, 2023). In the context of smart contracts, this translates into automated enforcement mechanisms that may lack nuance, fairness, or regard for social complexity. The technocratic orientation of code as law can therefore undermine the deliberative processes central to democratic legal orders, particularly when systems are designed without public input or institutional oversight.

At the heart of this shift lies a distinct ideology—one rooted in libertarian and cyber-anarchist visions of decentralized autonomy. The creators and proponents of blockchain technologies often advocate for a world where trust is encoded into protocols, and reliance on institutions is minimized. As Almahasneh explains, this worldview imagines law not as a product of collective will or social contract, but as an emergent property of cryptographic design and peer-to-peer consensus (Almahasneh, 2024). The ideology of code-based regulation thus challenges the legitimacy of traditional legal systems, proposing instead a model of self-regulation grounded in immutable code. Guo articulates this ideology as one of algorithmic objectivity, wherein computational systems are presumed to be impartial and incorruptible in ways human institutions are not (Guo, 2023).

However, the notion that algorithms can embody normative authority raises critical questions about legitimacy and accountability. Unlike legislatures or courts, software developers are not elected or subject to democratic checks. Yet, as Budiyanto observes, they wield significant power in determining how rules are designed, interpreted, and enforced within digital ecosystems (Budiyanto, 2023). This creates a new form of authority—algorithmic authority—where individuals are governed not by publicly debated laws, but by opaque systems of logic that they cannot question or contest. Berezina describes this dynamic as "rule by design," a form of governance where power is embedded into technical architecture rather than legal discourse (Berezina, 2021). In such a system, the boundaries of permissible behavior are predetermined by code and cannot be altered without modifying the underlying architecture, effectively eliminating the possibility for deliberative revision or legal challenge.

This entrenchment of power in digital systems has profound implications for how we conceive of law, citizenship, and sovereignty in the digital age. Sillanpää warns that the shift from legal to algorithmic governance risks transforming citizens into mere users of platforms, whose rights and obligations are dictated not by shared social norms but by the logic of systems designed elsewhere (Sillanpää, 2020). The political philosophy underpinning "code is law" therefore demands critical scrutiny. While it may offer efficiency and consistency, it also introduces new forms of exclusion, inequality, and domination—particularly when code reflects the biases, assumptions, or interests of its designers. Thus, understanding the philosophical and political origins of code as law is essential not only for grasping its legal implications but also for evaluating its compatibility with democratic ideals and social justice.

4. Tensions Between Legal Norms and Technical Code

The rapid proliferation of smart contracts and blockchain-based governance systems has exposed deep tensions between legal norms and technical code. At the most fundamental level, this tension can be understood as a conflict between the rule of law and the rule of code. In traditional legal systems, the rule of law entails a set of publicly promulgated, equally applied, and

interpretable norms, enforced by institutions bound by procedural fairness. In contrast, the rule of code involves deterministic execution based on logic written in programming languages, typically with no room for discretion or contextual understanding. As Dwivedi and colleagues emphasize, while code can enforce compliance, it lacks the interpretive capacity that legal systems rely on to balance competing interests or resolve ambiguity (Dwivedi et al., 2021).

Legal norms are inherently ambiguous, and this ambiguity serves a vital function. It allows judges to interpret rules flexibly, taking into account context, intent, and broader social values. By contrast, code must be precise and unambiguous to function properly, which limits its ability to adapt to novel or morally complex situations. Goh points out that this rigidity can be especially problematic in international contexts where differing legal traditions and cultural expectations require nuanced interpretation (Goh, 2022). The formalism of smart contracts may thus be incompatible with legal environments that prize interpretive judgment over mechanical application. Bohyer underscores this limitation, noting that once deployed, smart contracts are resistant to modification, making it difficult to correct errors, accommodate unforeseen changes, or respond to ethical concerns (Bohyer & Hayajneh, 2023).

One of the most pressing challenges is the absence of ex post justice mechanisms in pre-coded environments. Traditional legal systems allow for the retrospective evaluation of actions, enabling courts to issue remedies, assign liability, or adjust outcomes in light of new information. In contrast, smart contracts execute automatically and irreversibly, regardless of changed circumstances or unintended consequences. Nugraheni and colleagues argue that this creates a justice gap, where individuals may be bound by transactions that, while technically valid, are substantively unjust or coercive (Nugraheni et al., 2022). The inability to intervene or revise outcomes undermines core principles of fairness and accountability, which are central to modern legal systems.

These tensions become even more pronounced when considering fundamental rights such as due process and equity. Smart contracts do not provide opportunities for users to contest decisions, present evidence, or appeal outcomes. In conventional systems, due process ensures that legal subjects have access to procedures that safeguard their interests and enable redress. In algorithmic environments, however, decisions are often made and enforced without any transparency or human involvement. Nazarov warns that such systems can erode procedural safeguards, particularly when embedded in critical domains like finance, healthcare, or housing (Nazarov, 2024). Without avenues for contestation, users become subject to opaque processes that may reinforce inequality or discrimination.

Equity, too, is compromised in systems governed solely by code. Human law allows for exceptions, equitable remedies, and context-sensitive judgments that ensure outcomes align with justice rather than formal compliance alone. Đurović and Lech highlight how smart contracts lack the capacity to consider mitigating factors or offer partial remedies, which can lead to harsh or disproportionate consequences (Đurović & Lech, 2019). This rigidity may benefit powerful actors who can shape or manipulate code in their favor, while leaving vulnerable populations without protection. As Matsushima and Noda argue, algorithmic enforcement mechanisms may optimize for efficiency but fail to account for the moral and social dimensions of legal relationships (Matsushima & Noda, 2020).

Moreover, the opacity of technical code exacerbates issues of accessibility and inclusion. Unlike legal language, which is intended to be publicly understood (albeit imperfectly), programming languages are intelligible only to a technical elite. Alikhani observes that this creates a new kind of legal asymmetry, where users are bound by rules they cannot read, interpret, or challenge (Alikhani & Hamidi, 2021). The result is a governance system where power is centralized not in institutions accountable to the public, but in the hands of developers and platform operators who control the infrastructure.

These contradictions underscore the need to reexamine the relationship between law and technology in light of the increasing reliance on code-based systems. While smart contracts offer significant advantages in terms of automation, efficiency, and trust minimization, they also raise complex normative questions that cannot be resolved through technical solutions alone. As Onufreiciuc and Stănescu assert, integrating smart contracts into legal systems requires more than regulatory recognition—it demands a fundamental

reconsideration of how values like justice, fairness, and accountability can be preserved in digital environments (Onufreiciuc & Stănescu, 2021). Bridging the gap between code and law is not simply a matter of translation but a philosophical and institutional endeavor that must be undertaken with care, transparency, and democratic engagement.

5. Implications for Legal Theory and Political Philosophy

The emergence of smart contracts has not only disrupted legal practice but has also provoked a significant rethinking of foundational assumptions in legal theory and political philosophy. Smart contracts, as autonomously executing digital agreements, represent more than a novel technical artifact—they signal a shift toward new forms of authority grounded in computation rather than jurisprudence. One of the most prominent theoretical implications is the rise of digital sovereignty, where individuals and communities seek to govern themselves through cryptographic tools rather than state-based legal structures. As Almahasneh explains, smart contracts are increasingly being viewed as instruments of self-regulation, empowering users to design and enforce rules autonomously without recourse to centralized legal authorities (Almahasneh, 2024). This reflects a broader aspiration toward digital sovereignty, where blockchain-based tools become the infrastructure for autonomous governance.

Digital sovereignty, as expressed through smart contracts, diverges sharply from traditional notions of state-centric legal sovereignty. In conventional frameworks, legal authority is derived from institutional legitimacy, constitutional procedures, and democratic deliberation. In contrast, smart contracts derive their authority from code and consensus protocols, creating decentralized regimes where enforcement is procedural and absolute. Kirillova emphasizes that this undermines the monopoly of state law by enabling transnational enforcement systems that operate independently of territorial jurisdictions (Kirillova & Эльдарович, 2023). These systems are not merely supplemental to legal regimes but actively compete with them, raising profound philosophical questions about the source and nature of legal normativity in a digitized world.

This condition has given rise to a new form of political organization often described as governance without government. Blockchain platforms host systems of rule-making, enforcement, and dispute resolution without traditional political institutions. This phenomenon, as Musthafa and colleagues argue, reflects the principles of crypto-anarchism—an ideological commitment to privacy, decentralization, and the minimization of state interference (Musthafa et al., 2024). At the same time, the hyper-automation and immutability of these systems evoke what might be called a digital Leviathan: a structure of total control enforced not by sovereign will but by unalterable code. Donn critiques this paradox, noting that while smart contracts promise liberation from bureaucratic inefficiencies, they also risk instituting systems of governance that are opaque, inflexible, and unaccountable (Donn, 2023).

This duality—the promise of freedom and the threat of domination—forces a reconfiguration of legal subjectivity in programmable environments. In traditional legal systems, the subject of law is an autonomous agent capable of moral reasoning and legal responsibility. Legal rules presuppose a subject who interprets, negotiates, and contests norms. In contrast, the subject of a smart contract is reduced to a node in a computational network, whose role is to trigger or respond to automated actions. Berezina highlights how this transformation diminishes the space for moral judgment and deliberative engagement, reducing legal relationships to input-output mechanisms governed by prewritten logic (Berezina, 2021). This reconceptualization challenges core liberal assumptions about the nature of personhood, responsibility, and agency within the legal order.

The question of consent in this context becomes equally complex. In traditional legal theory, consent is a dynamic and contestable concept, subject to various legal tests and contextual evaluations. Consent is not merely a formal act but a substantive process, shaped by knowledge, intent, and freedom from coercion. Smart contracts, however, translate consent into an instantaneous action—usually a click or transaction—executed within an environment where the rules are embedded in inaccessible code. Budiyanto argues that such environments compromise meaningful consent, especially when users do not possess the technical expertise to understand the terms or consequences of their actions (Budiyanto, 2023). The irreversibility of smart contracts further complicates the notion of

withdrawing consent, making participation in these systems a form of de facto subjection rather than voluntary engagement.

Autonomy, too, is redefined in the world of coded transactions. While smart contracts appear to empower users by removing reliance on intermediaries, they simultaneously constrain autonomy by enforcing pre-coded outcomes with no room for human reconsideration. Papantoniou explains that this paradox creates a situation where autonomy is exercised only at the point of coding or deployment, after which all agency is surrendered to automated logic (Papantoniou, 2020). This raises philosophical concerns about whether such arrangements truly preserve the spirit of autonomy or merely simulate it within a tightly controlled framework. The capacity for reflection, renegotiation, and moral transformation—central to the human experience of law—is all but absent in systems that equate execution with legitimacy.

The implications for legal theory and political philosophy are thus profound. Smart contracts demand a rethinking of sovereignty, governance, subjectivity, consent, and autonomy. They challenge the boundaries between public and private law, between normativity and automation, and between freedom and control. As Nazarov argues, the rise of code-based regulation compels us to reimagine legal and political theory for an era where authority is no longer synonymous with human judgment, but with algorithmic execution (Nazarov, 2024). To respond adequately, scholars and institutions must engage with these technologies not only as regulatory tools but as transformative forces that reshape the very conditions of legal and political life.

6. Challenges and Critical Reflections

Despite their technological sophistication and potential for innovation, smart contracts are accompanied by a range of challenges that underscore the need for critical reflection. Chief among these are regulatory gaps and systemic risks that emerge from the intersection of law and code. Because smart contracts often operate across jurisdictions and outside traditional legal frameworks, they expose users to a host of vulnerabilities, including fraud, coercion, and discriminatory practices. As Goh points out, the absence of standardized legal recognition for smart contracts across countries creates ambiguity, particularly in cases where contractual disputes arise or where enforcement mechanisms fail (Goh, 2022). Fraud becomes especially difficult to address in smart contract systems, given their autonomous nature and the difficulty of reversing automated transactions once executed.

The potential for coercion is equally troubling. Smart contracts may bind individuals to agreements they do not fully understand or whose implications are hidden in technical complexity. Abdullah and Goh emphasize that in many cases, users are unaware of the risks associated with self-executing agreements, including the inability to modify terms or seek redress through conventional legal channels (Abdullah & Goh, 2022). Systemic bias also becomes embedded in these technologies when developers—consciously or unconsciously—encode assumptions or preferences that disadvantage certain groups. Chauhan argues that without oversight, smart contracts can replicate and amplify existing inequalities, functioning as "digital gatekeepers" that silently enforce discriminatory logic (Chauhan, 2020).

One of the most acute technical challenges in smart contract execution is the reliance on oracles—external data feeds that provide smart contracts with the information needed to trigger execution. Oracles serve as bridges between the blockchain and the real world, but they also represent single points of failure that undermine the decentralized ethos of smart contracts. Matsushima and Noda discuss how manipulation or malfunction of oracles can lead to catastrophic contract failures, especially in financial markets or insurance systems (Matsushima & Noda, 2020). The so-called "oracle problem" highlights the paradox of decentralized contracts depending on centralized data inputs, creating new vectors for error, fraud, and external influence.

In addition to technical risks, there is a critical need for interdisciplinary dialogue between law and technology. Legal scholars, developers, ethicists, and policymakers must collaborate to ensure that smart contracts evolve within a framework of accountability, transparency, and social responsibility. As Alikhani notes, the lack of such collaboration has resulted in a conceptual disconnect, where legal norms are retrofitted to technological systems rather than co-developed with them (Alikhani & Hamidi, 2021). Without sustained dialogue, there is a risk that smart contracts will become juridically isolated artifacts—legally enforceable in narrow terms but normatively alien to the broader legal tradition.

This interdisciplinary gap extends to institutions as well. Regulatory bodies often lack the technical expertise to assess or respond to the implications of smart contracts. Onufreiciuc and Stănescu point out that most legal institutions are still ill-equipped to handle disputes arising from blockchain-based agreements, leading to inconsistent rulings and unpredictable outcomes (Onufreiciuc & Stănescu, 2021). There is also a scarcity of case law, which inhibits the development of legal doctrines suited to address the unique features of smart contract environments. This further exacerbates legal uncertainty and discourages wider adoption in sectors that require stable and predictable legal frameworks.

Another major concern is the potential overreach of technocratic power structures. Smart contracts concentrate considerable authority in the hands of developers, platform architects, and technical intermediaries, many of whom operate with minimal public oversight or ethical accountability. As Donn cautions, the unchecked power of these actors risks turning technical infrastructures into instruments of control, where legal rules are replaced by private governance models embedded in code (Donn, 2023). These technocratic systems may not be subject to democratic processes, leaving users vulnerable to opaque decision-making and unilateral rule changes.

This dynamic challenges the legitimacy of legal systems and the principle of rule of law itself. Berezina warns that if law becomes indistinguishable from code, and if governance is reduced to protocol execution, the capacity for critical engagement, contestation, and reform is diminished (Berezina, 2021). The result is a form of governance where authority is derived not from collective deliberation but from technical design, a condition that fundamentally alters the social contract between individuals and institutions.

In sum, while smart contracts offer new opportunities for efficiency and trustless transactions, they also raise urgent ethical, legal, and philosophical concerns. The risks of fraud, coercion, and systemic exclusion must be addressed through robust regulatory frameworks and inclusive design principles. The oracle problem underscores the need for technical resilience, while the concentration of power in technocratic hands necessitates institutional checks and balances. As Boranbay and Juchnevicius argue, the future of smart contracts must be guided not only by innovation but also by a commitment to justice, transparency, and human dignity (Boranbay & Juchnevicius, 2024). Only through sustained legal-tech dialogue and interdisciplinary collaboration can these goals be realized in a rapidly evolving digital landscape.

7. Conclusion

The integration of smart contracts into the legal and political landscape represents a paradigmatic shift that challenges long-standing assumptions about how legal relationships are formed, interpreted, and enforced. Unlike traditional contracts that are governed by state-backed legal systems and shaped through human deliberation, smart contracts operate within decentralized, automated ecosystems where code executes terms with precision and finality. This transformation not only introduces technical efficiencies but also demands a reconsideration of foundational legal principles such as consent, autonomy, due process, and equity. As programmable code increasingly substitutes for human judgment, the very nature of law is being reconfigured into something more deterministic, less flexible, and potentially less humane.

The philosophical implications of this shift are significant. The idea that "code is law" suggests a departure from institutional legitimacy toward algorithmic authority. While this may empower individuals in certain respects—particularly by reducing reliance on intermediaries—it also introduces new vulnerabilities. Smart contracts lack the ability to accommodate context, rectify injustice, or respond to unforeseen circumstances. They cannot assess motive, recognize coercion, or deliver equitable remedies. These limitations expose a critical tension between the aspirational neutrality of technology and the inherently interpretive, value-laden nature of legal reasoning.

Jurisdictions across the globe have begun to grapple with these issues, with some embracing smart contracts through legislation or regulatory frameworks, and others proceeding with caution. Still, legal recognition alone does not resolve the deeper concerns about enforceability, fairness, and democratic oversight. The hybrid approaches emerging in some jurisdictions—combining technical automation with legal dispute mechanisms—reflect an attempt to reconcile the promise of smart contracts with the normative commitments of the rule of law. These developments

underscore the need for legal systems to evolve without abandoning their ethical foundations.

Moreover, the rise of smart contracts poses institutional challenges that extend beyond technical implementation. Legal institutions must not only understand the technology but also shape its development through active engagement and oversight. Interdisciplinary collaboration between legal scholars, technologists, and policymakers is essential to ensuring that smart contracts serve human needs rather than override them. The future of legal innovation must be both technologically informed and ethically grounded.

At the heart of this conversation lies the question of what kind of legal future society wishes to build. If the law is to remain a tool for justice and inclusion, it must resist the temptation to equate automation with fairness or efficiency with legitimacy. Smart contracts may streamline transactions, but they cannot yet replicate the complexity of human judgment or the flexibility of equitable remedies. Therefore, their integration into legal systems must proceed with caution, critical reflection, and a steadfast commitment to democratic values.

In conclusion, while smart contracts offer revolutionary potential, their widespread adoption requires more than technological readiness. It requires a reimagining of legal theory, institutional reform, and a robust ethical framework. Only through such a comprehensive approach can the legal system accommodate innovation without sacrificing its foundational principles. As societies move further into the digital age, the challenge will be not just to regulate smart contracts, but to ensure they reflect the values and aspirations of a just legal order.

Authors' Contributions

Authors contributed equally to this article.

Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

Acknowledgments

We would like to express our gratitude to all individuals helped us to do the project.

Declaration of Interest

The authors report no conflict of interest.

Funding

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

Ethical Considerations

In this research, ethical standards including obtaining informed consent, ensuring privacy and confidentiality were observed.

References

Abdullah, J. A., & Goh, Y. (2022). Making Smart Contracts a Reality. 70-78. https://doi.org/10.1093/oso/9780192858467.003.0004

Alikhani, A., & Hamidi, H. R. (2021). Regulating Smart Contracts: An Efficient Integration Approach. *Intelligent Decision Technologies*, *15*(3), 397-404. https://doi.org/10.3233/idt-200180

Almahasneh, Y. (2024). The Legal Nature of Smart Contracts Programmed Using Blockchain Technology. *Ijlrs*, *3*(4), 8-31. https://doi.org/10.59992/ijlrs.2024.v3n4p1

Atiyah, G. A., Ibrahim, A. I., & Jasim, A. A. (2024). Enforcement of Smart Contracts in Cross-Jurisdictional Transactions. *International Journal of Law and Management*. https://doi.org/10.1108/ijlma-06-2024-0220

Baso, F., Yusuf, D. U., Djaoe, A. N. M., Iswandi, I., & Ramadhany, A. (2024). Overview of Smart Contract: Legality and Enforceability. *Dialogia Iuridica*, *16*(1), 096-111. https://doi.org/10.28932/di.v16i1.10024

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

Bohyer, K., & Hayajneh, T. (2023). Modernizing Contracts Across Industries: A Review of Smart Contract Applications and the Evolving Legal Landscape. *Icst Transactions on Scalable Information Systems*. https://doi.org/10.4108/eetsis.3299

Boranbay, S. S., & Juchnevicius, E. (2024). The Concept of a Smart Contract: Advantages and Current Situation of Legal Regulation in the Republic of Kazakhstan. *Bulletin of the Karaganda University "Law Series"*, *11529*(3), 100-112. https://doi.org/10.31489/2024l3/100-112

Budiyanto, A. E. (2023). Analisis Yuridis Penggunaan Smart Contract Dalam Perspektif Asas Kebebasan Berkontrak. *JSSR*, *1*(1), 815-827. https://doi.org/10.61722/jssr.v1i1.402

Chauhan, M. (2020). Smart Contracts and Smart Dispute Resolution. *International Journal of Online Dispute Resolution*, *7*(2), 149-183. https://doi.org/10.5553/ijodr/235250022020007002003

Donn, T. D. L. (2023). Smart Contracts and International Trade: European Legal Strategies for Managing Challenges. *Journal of Digital Technologies and Law*, *1*(4), 1042-1057. https://doi.org/10.21202/jdtl.2023.45

Đurović, M., & Lech, F. (2019). The Enforceability of Smart Contracts. *Revija Kopaonicke Skole Prirodnog Prava*, *1*(1), 73-94. https://doi.org/10.5937/rkspp1901073d

Dwivedi, V., Pattanaik, V., Deval, V., Dixit, A., Norta, A., & Draheim, D. (2021). Legally Enforceable Smart-Contract Languages. *Acm Computing Surveys*, *54*(5), 1-34. https://doi.org/10.1145/3453475

Goh, G. R. D. E. (2022). Smart Contract Disputes and Public Policy in the ASEAN+6 Region. *Digital Law Journal*, *3*(4), 32-70. https://doi.org/10.38044/2686-9136-2022-3-4-32-70

Guo, L. (2023). The Future of Civil Law: Legal Tech, Smart Contracts, and Automated Enforcement. *Science of Law Journal*, *2*(12). https://doi.org/10.23977/law.2023.021207

Kirillova, E., & Эльдарович, З. Т. (2023). Civil Law Support for Smart Contracts. https://doi.org/10.12737/2082660

Matsushima, H., & Noda, S. (2020). Mechanism Design With Blockchain Enforcement. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3554512

Musthafa, A. R., Putri, R. Y., Farizki, A. A., & Alma, S. A. (2024). Lex Cryptographia: Legal Extensions to Smart Contract Breaches and Governance in Blockchain Systems. *Jurnal Kajian Pembaruan Hukum*, *4*(2), 295. https://doi.org/10.19184/jkph.v4i2.53366

Nazarov, A. (2024). Legal Nature and Classification of Smart Contracts in Crypto Exchanges: Challenges to Traditional Contract Law. *Irshad J. Law and Policy*, *2*(9), 1-15. https://doi.org/10.59022/ijlp.224

Nugraheni, N., Mentari, N., & Shafira, B. (2022). The Study of Smart Contract in the Hara Platform Under the Law of Contract in Indonesia. *Scholars International Journal of Law Crime and Justice*, *5*(7), 273-285. https://doi.org/10.36348/sijlcj.2022.v05i07.005

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

Papantoniou, A. A. (2020). Smart Contracts in the New Era of Contract Law. *Digital Law Journal*, *1*(4), 8-24. https://doi.org/10.38044/2686-9136-2020-1-4-8-24

Sillanpää, T. M. (2020). Freedom to (Smart) Contract. *Ials Student Law Review*, 38-50. https://doi.org/10.14296/islr.v7i2.5203

Zavyalova, E. B., Shumskaia, E. I., & Shumskaia, A. I. (2019). Transactions in the Digital Age: Blockchain Technology and Smart Contracts. *Journal of Law and Administration*, *15*(3), 32-38. https://doi.org/10.24833/2073-8420-2019-3-52-32-38