Smart Contracts and Contract Law Doctrine: Reconciling Self-Execution with Doctrines of Intent and Consent

1. Rafael González: Department of Public Law, Universidad Central de Venezuela, Caracas, Venezuela
2. Mariana Oliveira*: Department of Political Science, University of São Paulo, São Paulo, Brazil
3. Youssef El Amrani: Department of International Relations, Mohammed V University, Rabat, Morocco

***Correspondence: e-mail: mariana.oliveira@usp.br**

Abstract

Smart contracts represent one of the most transformative developments in contemporary private law, introducing automated, blockchain-based mechanisms that perform contractual obligations without human intervention. Their core features—self-execution, immutability, and reliance on coded logic—challenge foundational doctrines that have traditionally governed contract formation and enforcement. This narrative review examines the doctrinal tensions that arise when automated systems intersect with legal principles rooted in human intention, interpretive flexibility, and evaluative judgment. It explores how smart contracts complicate determinations of intent and consent, particularly when user interactions are interpreted as binding commitments despite limited understanding of the underlying code. The analysis highlights issues related to mistake, error, fairness, and interpretation, emphasizing that immutable execution can conflict with doctrines designed to prevent unjust outcomes. At the same time, the review identifies emerging mechanisms capable of harmonizing automation with legal doctrine. These include hybrid contract models that integrate natural language terms with executable code, layered architectures that separate legal and technical functions, reinterpretive approaches that reconceptualize intent as intent to automate, and standardization efforts that promote uniformity and predictability. Innovations in dispute resolution, including governance layers, reversible execution pathways, and both on-chain and off-chain adjudication systems, further support doctrinal compatibility. By synthesizing legal, technical, and regulatory perspectives, this review demonstrates that reconciliation is achievable when smart contracts are designed and interpreted through frameworks that respect both technological capabilities and the human-centered values of contract law. The findings suggest a path toward integrating automated performance into traditional legal systems while maintaining the substantive principles that ensure fairness, clarity, and legitimacy in contractual relationships.

Keywords: Smart contracts; blockchain; intent; consent; contract law; automation; doctrinal analysis; hybrid contracts; legal interpretation; digital contracting; private law.

Received: date: 13 November 2022
Revised: date: 17 December 2022
Accepted: date: 30 December 2022
Published: date: 01 January 2023

Citation: González, R., Oliveira, M., & El Amrani, Y. (2023). Smart Contracts and Contract Law Doctrine: Reconciling Self-Execution with Doctrines of Intent and Consent. *Legal Studies in Digital Age,* 2(1), 53-67.

1. Introduction

The rapid rise of blockchain-based smart contracts has transformed the landscape of private law by introducing automated, self-executing agreements that operate on decentralized infrastructures. As blockchain platforms gained prominence for their capacity to validate and enforce transactions without intermediaries, scholars began recognizing that these new contractual mechanisms depart substantially from traditional legal forms. In industries such as supply chain management, the increased reliance on blockchain systems for streamlining permissions and verification processes has highlighted both their disruptive potential and the distinct regulatory challenges they pose, particularly as empirical studies demonstrate significant user adoption driven by perceived reliability and transparency (Alazab et al., 2020). Similarly, the integration of automation within digital health systems has further illustrated the societal shift toward delegating transactional and decision-making authority to coded systems that minimize human discretion (Alanazi & Gay, 2020). These developments underscore the need to understand how self-executing tools operate not merely as technological innovations but as instruments capable of shaping norms within private law.

At the core of smart contract functionality lies the principle of self-execution, through which predefined conditions embedded in code automatically trigger outcomes once specified parameters are met. This embedded logic is strengthened by immutability, a defining characteristic of blockchain technology that ensures contractual terms remain unaltered once deployed. Commentators frequently emphasize that the rigid determinism of executable code challenges the long-standing assumption that contractual performance involves interpretive flexibility, making the oft-cited idea that “code is law” an especially contentious conceptual pivot in legal debates (Hunn, 2019). By minimizing discretionary judgment and enabling autonomous enforcement, smart contracts shift emphasis away from the interpretive traditions that have historically guided judicial evaluation of intent and performance. This transformation has also encouraged the growth of sophisticated architectures for managing digital permissions and record-keeping, as seen in blockchain frameworks designed to handle sensitive information and access rights (Farvin et al., 2023). As these systems develop, their technical precision becomes increasingly intertwined with normative questions about fairness, reasonableness, and enforceability.

Such technological advancements reveal deep doctrinal tensions surrounding the role of intent and consent in contractual formation. Classical contract doctrine assumes that parties intentionally bind themselves to specific obligations, with legal systems requiring demonstrable evidence of mutual assent. Scholars examining digital environments have raised concerns that automated execution lacks the nuance necessary to reflect a party’s subjective understanding or interpretive intentions, especially as individuals interacting with complex platforms may not fully grasp the legal consequences of triggering coded mechanisms (Lee, 2021). Civil law analyses similarly underscore the risks of relying exclusively on coded instructions to capture the breadth of parties’ legal commitments, noting that traditional legal interpretation often accounts for factors that fall outside the narrow precision of machine-readable terms (Kirillova & Эльдарович, 2023). Within this tension lies a broader dilemma: how to reconcile the machine-based execution of obligations with doctrines governing mistake, capacity, and unconscionability. These doctrines rely on human-centered evaluations that may not translate easily into deterministic code. Modern contract literature, particularly within technologically evolving sectors, illustrates that even when automation improves efficiency, it can simultaneously obscure how parties perceive obligations and risks (Bohyer & Hayajneh, 2023).

From a regulatory perspective, the proliferation of smart contracts presents theoretical and practical challenges that legal systems are still attempting to navigate. The conceptual basis of rights and obligations becomes more complex when enforcement mechanisms operate independently of human intervention, raising questions about whether automated processes can adequately reflect legal status, relational expectations, or broader moral dimensions associated with consent (Butchart, 2021). In some jurisdictions, legal scholars have noted that the absence of clear statutory definitions hampers courts’ ability to classify smart contracts within existing doctrinal frameworks, especially when judicial reasoning must account for novel forms of evidence and machine-mediated performance (Nikzad & Sadiq, 2023). Policy research conducted within national legal systems, including reports assessing the technological and normative consequences of automating contracting processes, underscores the fragmented and often reactive nature of current regulatory efforts (Research Institute of Information Technology Law of the, 2023). The resulting uncertainty affects not only legislators and courts but also businesses that rely on predictable rules to evaluate contractual risk.

Despite extensive technological enthusiasm, significant gaps remain in legal scholarship regarding how smart contracts should be interpreted, validated, and remedied within traditional doctrinal categories. Some attempts to conceptualize standardized frameworks for smart contracting highlight the need for integrated models that align technical precision with legal interpretive practices (Vasiu, 2023). Likewise, foundational studies on the legal significance of contract formation stress that even in digital environments, doctrines governing entry into force, validity, and mutual agreement cannot be disregarded or replaced by mechanical execution (Suleymanli, 2023). Yet courts in multiple jurisdictions continue to struggle with disputes arising from flawed code, misaligned intentions, or ambiguous interactions between human-readable terms and executable logic. These unresolved issues demonstrate that while smart contracts present opportunities for efficiency and transparency, they simultaneously pose challenges that require careful doctrinal analysis.

The purpose of this narrative review is to explore these tensions by examining how smart contracts intersect with fundamental principles of contract law and to assess whether self-executing mechanisms can be reconciled with doctrines of intent, consent, and fairness. The contribution of this review lies in synthesizing legal, technical, and regulatory perspectives to clarify doctrinal implications and to provide a structured understanding of how automated contracting can coexist with the foundational values of private law.

2. Smart Contracts: Architecture, Functionality, and Legal Characteristics

The technical architecture of smart contracts is rooted in the decentralized infrastructure of blockchain systems, which allow for distributed verification, tamper resistance, and persistent storage. In these environments, every node contributes to validating transactions according to predefined consensus mechanisms, ensuring that once information is written onto the chain, it becomes practically immutable. This characteristic of permanence has been discussed extensively in studies examining blockchain-based frameworks for managing sensitive or high-stakes records, where the inability to retroactively alter terms or data enhances trust but simultaneously limits flexibility (Farvin et al., 2023). Blockchain's decentralized verification process eliminates the need for traditional intermediaries, and this shift fundamentally alters how contractual obligations are created, interpreted, and enforced. Research exploring how supply chain ecosystems incorporate blockchain technology shows that the infrastructure's transparency and distributed design reduce opportunities for manipulation while increasing accountability across actors that may previously have relied on hierarchical trust models (Alazab et al., 2020).

At the center of smart contract functionality is the notion of self-execution, through which coded instructions automatically trigger actions once predetermined conditions are met. This mechanism removes human discretion at the moment of enforcement, binding the parties to whatever outputs the programmed logic dictates. The deterministic nature of code means that the system enforces obligations with absolute consistency, a feature highlighted in early techno-legal analyses emphasizing how automation reshapes regulatory landscapes by embedding normative constraints directly into algorithmic structure (Hunn, 2019). Self-execution depends on accurate and reliable external data, often provided through oracles—software agents that deliver real-world information, such as market prices or shipment confirmations, into the blockchain environment. The reliance on oracles introduces both operational efficiency and systemic vulnerability, as the accuracy of execution depends on the oracle's integrity. This creates an environment perceived as trustless only in the narrow sense that parties need not trust each other, yet they must trust the technical mechanisms governing data input and execution. Scholars analyzing modern smart contract deployment across various industries emphasize that automation's success depends on the reliability of these informational gateways, particularly when complex contractual outcomes hinge on accurate data interpretation (Bohyer & Hayajneh, 2023).

Smart contracts can take several forms, including deterministic models in which the outcome is fixed and predictable, conditional models that rely on changing variables, and hybrid models that integrate natural language agreements with coded performance logic. Deterministic contracts function well in simple transactional exchanges where conditions and outcomes are fully foreseeable. By contrast, conditional smart contracts rely on dynamic variables, making them more aligned with commercial arrangements that depend on evolving external factors. Hybrid smart contracts are especially significant in modern legal analysis because they attempt to reconcile machine precision with human interpretive language. Legal research examining civil law support frameworks for smart contracts notes that hybrid models better accommodate judicial review, since they preserve a layer of human-readable text that can guide interpretive reasoning in the event of disputes (Kirillova & Эльдарович, 2023). Hybrid structures thus present a potential pathway toward aligning automated enforcement with traditional doctrines of contractual interpretation and intent.

Although smart contracts offer a heightened level of automation, their legal characteristics raise fundamental questions regarding how human intent is expressed, recorded, and enforced. The automatic execution of obligations can obscure whether parties genuinely understood the consequences of interacting with coded systems, particularly when the interface between user actions and machine logic lacks transparency. Research on digital interactions has shown that users often do not fully comprehend the technical or legal implications of the systems they engage with, suggesting a disconnect between actual consent and the consent presumed by automated processes (Lee, 2021). This absence of interpretive nuance clashes with longstanding legal doctrines requiring that contract formation reflect mutual assent, raising concerns about whether code can function as a legitimate proxy for subjective intention. In jurisdictions where doctrinal interpretation places weight on the meaning of declarations or the context surrounding an agreement, scholars caution that purely coded terms may fail to capture the complexity of human negotiation and communication (Suleymanli, 2023). These challenges become even more pronounced when considering parties with unequal technological literacy, which complicates assessments of voluntariness and fairness.

Irrevocability is another defining characteristic of smart contracts. Once deployed on a blockchain, the contract's code operates independently of the parties, and modification requires collective action or complex technical intervention. This autonomy has been praised for reducing opportunities for opportunistic behavior, yet it also removes the discretionary space that courts traditionally use to correct imbalances, interpret ambiguous clauses, or remedy mistakes. Legal researchers analyzing smart contracting frameworks observe that the lack of flexibility can inadvertently shift risks toward the party least capable of predicting technical failures or coding errors (Vasiu, 2023). The allocation of risk in non-modifiable systems places significant pressure on initial design stages, since errors embedded in code may execute without regard to equitable considerations or changed circumstances. Studies of national legal responses to smart contracting emphasize that these systems may require supplementary procedural safeguards to prevent disproportionate harm, particularly in sectors where individuals cannot reasonably anticipate the full implications of automated enforcement (Research Institute of Information Technology Law of the, 2023).

Interpretation remains one of the most persistent legal issues associated with smart contracts. When disputes arise, courts must determine whether to privilege the literal meaning of code or the context and purpose of the underlying agreement. Scholars examining legal systems where smart contracts are already in use have noted that the tension between natural language and executable code becomes especially visible when the two diverge, such as when human-readable terms fail to align perfectly with coded instructions (Nikzad & Sadiq, 2023). Because code operates with strict logic, it lacks the elasticity required to capture evolving intentions or unanticipated scenarios. As a result, interpreting a smart contract may require technical expertise that courts and litigants do not uniformly possess.

Despite these challenges, smart contracts are rapidly expanding across various sectors. In financial services, the automation of transactions supports faster settlement, reduced human error, and more transparent record-keeping. These features are particularly advantageous in high-volume environments where consistent performance is essential. In supply chain systems, blockchain contracts provide granular tracking of goods and automatic verification of delivery milestones, enhancing coordination among diverse commercial actors (Alazab et al., 2020). Digital asset markets rely heavily on smart contracts to facilitate token issuance, custody, and transfer, with coded mechanisms ensuring that asset ownership records remain consistent across a distributed network. Government digital services have also begun exploring smart contracts to streamline administrative functions, especially in areas where automated approvals or certifications can reduce bureaucratic delays. Studies examining emerging public-sector applications indicate that smart contracts hold significant potential for improving administrative transparency and reducing redundancy, provided legal frameworks evolve to accommodate their distinct operational characteristics (Binns, 2022).

Across these domains, the growth of smart contracts signals a foundational shift in how legal obligations are conceptualized and enforced. Their deployment illustrates both the promise of efficiency and the complexity of integrating automated tools into doctrinal structures that were historically designed around human judgment and interpretive flexibility. Understanding these characteristics is critical for evaluating how smart contracts can be reconciled with private law principles and for identifying the legal innovations necessary to support their continued adoption.

3. Doctrinal Foundations of Intent and Consent in Contract Law

The foundations of contract law rest heavily on the doctrines of intent and consent, both of which serve as benchmarks for determining whether parties genuinely undertook legally enforceable obligations. In classical doctrine, the intent to create legal relations is considered the first essential step in contract formation, and legal systems have historically assumed that agreements become binding only when parties demonstrate a deliberate commitment to be legally bound. Scholarship addressing modern contracting practices highlights that although many agreements occur through increasingly technological means, the legal requirement of intent persists as a doctrinal anchor by ensuring that contracts reflect interpersonal commitments rather than accidental interactions (Suleymanli, 2023). In traditional legal analysis, courts evaluate intent based on outward manifestations rather than subjective mental states, emphasizing actions, communications, and contextual behavior that reasonably signal contractual commitment. This requirement becomes even more critical in digital environments, where interactions mediated by interfaces or automated systems may blur distinctions between deliberate assent and incidental engagement.

Offer and acceptance constitute the next major doctrinal pillar. The mechanism by which a contract comes into being requires a clear and identifiable offer that communicates willingness to enter into a binding agreement under specific terms, followed by an acceptance that mirrors those terms. As legal thought has long emphasized, the congruence of offer and acceptance ensures that the contract formed is one that reflects mutual understanding rather than unilateral assumptions. In technology-mediated settings, however, the traditional symmetry between offer and acceptance can be disrupted, particularly when automated systems generate responses or actions that parties might mistakenly interpret as intentional. Research on digital interactions shows that users often encounter environments in which technological design obscures the legal implications of their conduct, raising questions about whether clicking a button or engaging with a coded process genuinely communicates acceptance of complex contractual obligations (Lee, 2021). These challenges underscore why courts continue to scrutinize the form and clarity of assent, especially when automated behavior replaces human communication.

The doctrine of meeting of the minds—or consensus ad idem—further requires that parties share a mutual understanding regarding the essential terms of their agreement. Historically, this doctrine served to ensure that the subjective interpretations of parties aligned sufficiently to support valid contractual obligations, although modern jurisprudence often adopts an objective standard for determining whether such consensus exists. As legal scholars have noted in the context of digital contracting, the meeting-of-the-minds doctrine becomes especially strained when agreements involve coded logic or automated responses that may not reflect a party's interpretive expectations (Kirillova & Эльдарович, 2023). This raises important analytical questions about the extent to which human parties can be said to share meaning with machine-generated processes that operate according to fixed parameters rather than contextual interpretation.

Consent forms the final cornerstone of doctrinal analysis, and courts traditionally distinguish between express and implied consent. Express consent occurs when parties explicitly state their agreement, whether orally, in writing, or through clear affirmative actions. Implied consent arises from conduct, contextual behavior, or patterns of interaction that reasonably signal agreement. In technological environments, express consent often takes the form of digital signatures, electronic acknowledgements, or the activation of user-interface elements, whereas implied consent may arise through continued use of a platform or engagement with automated systems. Studies examining modern digital contracting practices highlight the risk that parties may not fully understand the scope or implications of the consent they provide, especially when interfaces are designed to simplify complex agreements into compressed or opaque interactive elements (Bohyer & Hayajneh, 2023). The distinction becomes increasingly significant in automated contracting systems, where express consent is often simulated through user interaction with coded triggers rather than through negotiated, comprehensible terms.

The reasonableness standard plays a critical role in interpreting intent and consent, anchoring contractual interpretation in what an objectively reasonable person would have understood in similar circumstances. This standard is especially important for evaluating conduct in digital environments, since courts cannot rely solely on subjective interpretations or sophisticated technical explanations. Research exploring legal responses to technological change indicates that the reasonableness standard operates as a protective mechanism, ensuring that parties are not unfairly bound by mechanisms they could not reasonably have understood or evaluated (Butchart, 2021). By grounding contractual interpretation in shared societal expectations, the reasonableness standard serves as a bridge between traditional legal doctrine and technologically mediated interactions that risk overwhelming naïve or inexperienced users.

Jurisdictional variations further complicate doctrinal analysis. In common law systems, the objective theory of intent dominates, holding that contractual intent is determined not by internal states but by outward expressions that a reasonable person would interpret as signifying agreement. This approach supports legal certainty by reducing the subjectivity inherent in assessing personal intention. Scholars addressing digital contracting emphasize that the objective theory becomes increasingly significant when interpreting interactions mediated by automated systems, since courts must evaluate actions rather than internal states (Binns, 2022). However, because automated systems may generate conduct that resembles assent without reflecting human intention, courts must carefully distinguish between actions attributable to the party and actions attributable to system design.

Civil law systems, by contrast, place greater emphasis on the will theory, which prioritizes parties' subjective intentions, evaluating declarations of intent to determine whether agreement exists. Analyses of civil law treatment of smart contracts note that declarations of intent remain central, even when agreements occur through coded processes, and that courts in these systems may look more closely at whether parties genuinely intended the legal consequences generated by automated logic (Kirillova & Эльдарович, 2023). This doctrinal orientation creates unique tensions when civil law principles encounter deterministic machine logic that does not account for evolving intent or contextual meaning. Legal scholarship within certain jurisdictions has raised concerns that automated systems may undermine the value placed on subjective will, especially when individuals lack technological expertise necessary to understand coded obligations (Nikzad & Sadiq, 2023).

International commercial law frameworks, including instruments such as the UNIDROIT Principles and the CISG, adopt a blended approach that emphasizes good faith, reasonableness, and the importance of contextual interpretation. Although these frameworks were not developed with blockchain or automation in mind, scholars analyzing their application to modern contracting technologies argue that their flexible interpretive standards could accommodate automated agreements by focusing on parties' behavior, communications, and expectations rather than exclusively on coded execution (Vasiu, 2023). This adaptability suggests that while traditional doctrinal categories may struggle with smart contracts, international commercial standards may offer a more resilient foundation for interpreting agreements that blend human intention with automated processes.

4. Doctrinal Tensions Between Smart Contracts and Contract Law

The tension between smart contracts and classical contract doctrine emerges most clearly in debates over whether code can genuinely express legal intent. Contract law traditionally relies on interpretive tools to determine whether parties meant to enter a binding legal relationship, but coded agreements collapse this doctrinal flexibility by embedding performance outcomes directly into machine instructions. Scholars examining techno-legal systems note that the rigidity of automated enforcement complicates the evaluation of intention because code can trigger obligations regardless of whether parties ever understood the legal meaning of their actions (Hunn, 2019). This rigidity means that the act of deploying or interacting with a smart contract may be treated as incontrovertible evidence of intent, even when the user's subjective or contextual understanding differs from the coded outcome. Legal analysis of digital contracting further suggests that technological systems often replace nuanced manifestations of intent with oversimplified signals, creating a gap between a party's internal state and the external actions interpreted by automated mechanisms (Lee, 2021). These doctrinal tensions become particularly visible when examining the difference between the intent to be legally bound and the intent merely to automate a process.

The distinction between intending to create a binding legal obligation and intending only to automate certain operational steps is central to doctrinal reconciliation. Parties may deploy smart contracts to ensure efficiency or verifiable performance without necessarily contemplating the broader legal consequences that accompany contractual formation. Studies analyzing contemporary applications of smart contracts emphasize that many users perceive automation primarily as a technological tool rather than a legal instrument, complicating judicial efforts to determine whether legally binding intent was present at the moment of deployment (Bohyer & Hayajneh, 2023). This problem is amplified when smart contracts are embedded into boilerplate templates offered by platforms or developers, since individuals interacting with such templates may neither negotiate nor fully understand the conditions encoded inside them. Research on standardized digital contracting underscores that templates often replicate terms without clarity, meaning that parties express only minimal or superficial assent to pre-existing coded conditions (Suleymanli, 2023). When courts must later determine intent, the machine-generated structure of such agreements limits opportunities to evaluate the contextual indicators that traditionally help establish contractual will.

Consent, the second major doctrinal pillar, faces equally substantial disruption in automated systems. In digital environments, consent frequently becomes a matter of interaction rather than understanding—users trigger events by clicking, sending tokens, or interacting with interfaces that may conceal the full extent of contractual consequences. Scholars studying digital ecosystems argue that this "consent by interaction" replaces "consent by comprehension," leading to a legal environment in which the mechanical gestures of participation are treated as conclusive evidence of voluntary agreement (Lee, 2021). This phenomenon becomes even more problematic when considering the information asymmetry between coders, who understand the technical architecture of the contract, and ordinary contracting parties, who may lack the expertise required to evaluate coded obligations. Empirical analyses of blockchain-based systems acknowledge that users often engage through simplified interfaces that fail to expose the underlying logic, contributing to an imbalance that undermines meaningful choice (Farvin et al., 2023). The asymmetry ensures that coders, or entities controlling smart contract templates, hold disproportionate power to shape the terms of the agreement.

Implied consent also takes on novel dimensions in automated environments. Because smart contracts execute automatically once certain triggers occur, courts may infer consent from actions that were not intended to communicate agreement. Legal studies examining the deployment of smart contracts in both public and private systems highlight that users may inadvertently activate legal consequences by performing routine interactions, such as sending tokens to an address or triggering an on-chain function (Kirillova & Эльдарович, 2023). This creates a doctrinal dilemma: should such interactions be treated as tacit acceptance of the coded terms, or should courts require evidence of informed understanding? Algorithmic opacity exacerbates these concerns. As systems grow more complex, the ability of users—let alone courts—to interpret coded logic diminishes, raising the question of whether any meaningful notion of informed consent can exist when contractual obligations are buried beneath layers of automation. Studies assessing public policy implications of smart contracts emphasize that opacity presents risks not only for private parties but also for legal institutions that rely on transparency to evaluate voluntariness and fairness (Research Institute of Information Technology Law of the, 2023).

Mistake doctrine represents another area where classical principles struggle to accommodate automated contracting. Traditional contract law distinguishes between unilateral and mutual mistakes and provides remedies when parties enter agreements under erroneous assumptions. Smart contracts, however, execute based on immutable code, meaning that once an error occurs—whether due to faulty logic, incorrect inputs, or misunderstandings—execution may proceed regardless of parties' intentions. Scholars focusing on immutable execution note that this rigidity stands in stark contrast to doctrines designed to prevent unjust enrichment or enforce equitable outcomes, as code lacks the capacity to account for contextual deviations (Hunn, 2019). Coding errors themselves introduce additional complexity. When developers embed flawed logic into a smart contract, the resulting behavior may diverge sharply from what the parties expected. Legal analysis of such scenarios questions whether parties should be held to unintended outcomes or whether liability should shift toward developers responsible for the faulty code (Nikzad & Sadiq, 2023). Disputes over unintended execution events—such as premature transfers of assets or automated penalties triggered by erroneous data—illustrate how doctrinal remedies must evolve to address machine-driven mistakes that traditional jurisprudence never contemplated.

Unconscionability and fairness concerns also intensify in technologically mediated contracting environments. Smart contracts often operate in contexts where users possess vastly unequal levels of technological literacy, and this disparity allows sophisticated actors to embed terms that disproportionately benefit them. Research into digital contracting acknowledges that individuals with limited technical knowledge may unknowingly enter agreements containing exploitative conditions simply because they lack the means to understand coded logic (Bohyer & Hayajneh, 2023). This inequality mirrors the concerns traditionally associated with adhesion contracts—agreements presented on a take-it-or-leave-it basis—but automation magnifies the risks by allowing unfair terms to enforce themselves automatically. Studies assessing the moral and structural aspects of automated systems highlight the danger that self-executing mechanisms can implement unfair obligations before users even have the opportunity to recognize or challenge them (Butchart, 2021). The speed and irreversibility of automated enforcement can therefore undermine the protective function of doctrines that historically acted as safeguards against coercion, exploitation, or imbalance.

Interpretation represents perhaps the most profound site of doctrinal contention. The maxim "code is law," often invoked in technological discourse, suggests that coded instructions should be treated as definitive expressions of contractual obligations. However, courts traditionally rely on interpretive frameworks that account for ambiguity, context, and purpose. Scholars analyzing techno-legal disputes note that judicial institutions frequently lack the technical capacity to interpret code accurately, meaning that courts must depend on expert testimony or forensic analysis to understand the meaning embedded within automated logic (Binns, 2022). This dependence raises concerns about procedural fairness and accuracy, especially in complex disputes where coded behavior does not align with the contractual expectations of the parties. Interpretation becomes even more difficult in hybrid contracts containing both natural-language text and executable code. When the two components diverge, disputes arise over whether the coded instructions or the written terms should control. Studies examining civil law responses to such conflicts emphasize that declarations of intent may guide the interpretive outcome, even when coded logic points in a different direction (Kirillova & Эльдарович, 2023). In common law systems, courts may also confront limitations when applying rules such as the parol evidence doctrine, which traditionally restricts the use of extrinsic evidence but may conflict with the need to examine technical metadata or code repositories to determine the parties' obligations (Vasiu, 2023). Digital evidence therefore challenges long-standing evidentiary principles by introducing novel forms of proof whose interpretation requires combinatory legal and technical expertise.

These doctrinal tensions collectively illustrate that smart contracts do not simply represent a new mode of contracting but challenge the conceptual foundation of contract law itself. Their deterministic design and automated execution strain doctrines built on human intention, contextual interpretation, and equitable flexibility. As courts and legislatures grapple with these tensions, the need for coherent legal frameworks that reconcile automation with doctrinal principles becomes increasingly urgent.

5. Reconciling Smart Contracts with Doctrines of Intent and Consent

Efforts to reconcile smart contracts with the doctrinal requirements of intent and consent have increasingly focused on hybrid contractual models that combine natural language agreements with executable code. Scholars examining smart contract applications emphasize that human-readable terms remain essential for expressing the parties' legal intentions, even when automated execution handles operational tasks (Kirillova & Эльдарович, 2023). The combination of text and code allows parties to delineate which obligations are meant to be automated and which remain subject to traditional interpretation. This model appeals to courts because it provides contextual clues unavailable in purely coded systems, enabling judges to interpret ambiguous conduct using doctrinal tools such as reasonableness, declarations of intent, or established interpretive principles. Research on modernizing contractual processes across industries notes that hybrid structures enhance clarity by preserving a written record of expectations, thereby reducing disputes that arise from misalignment between human assumptions and coded behavior (Bohyer & Hayajneh, 2023). These hybrid systems also allow parties to embed fallback provisions that address contingencies outside the deterministic capabilities of code, supporting judicial intervention when necessary. Early judicial responses to such models suggest a gradual acceptance of mixed-format agreements, particularly in jurisdictions where courts increasingly encounter disputes involving blockchain-based transactions and require interpretive mechanisms beyond the rigidity of machine logic (Nikzad & Sadiq, 2023).

The development of layered contract architectures further supports reconciliation by separating the legal, technical, and governance functions of the agreement. In this structure, the legal layer articulates rights and obligations in natural language, serving as the authoritative reference for contractual interpretation. This layer reflects doctrines of assent and intent, ensuring that the written terms capture the parties' expectations in a form compatible with judicial reasoning. Scholars exploring blockchain-based systems note that human-readable provisions help mitigate the opacity of automation, providing transparency that users can understand without specialized technical knowledge (Farvin et al., 2023). The code layer, by contrast, translates certain obligations into machine-executable logic, enabling automated performance in ways that reduce error and increase transactional efficiency. Empirical studies examining blockchain adoption in supply chain and financial contexts highlight that the code layer improves reliability by eliminating opportunities for manipulation and minimizing reliance on intermediaries (Alazab et al., 2020). The governance layer supports mechanisms for dispute resolution, modification, and overrides, enabling actors to intervene when coded logic produces anomalous or unjust results. Policy research addressing national legal frameworks for smart contracts emphasizes that governance structures are critical for addressing unexpected behavior, whether due to oracle failures, coding mistakes, or evolving circumstances that coded instructions cannot anticipate (Research Institute of Information Technology Law of the, 2023). This three-layered architecture therefore provides a coherent model for integrating automated performance into frameworks that remain grounded in doctrinal principles.

Doctrinal reinterpretation also plays an important role in harmonizing smart contracts with traditional contract law. One emerging approach involves reframing intent as an "intent to automate," which acknowledges that when parties deploy smart contracts, their primary objective may be operational rather than legal. Legal analysis of digital transactions suggests that automated execution should not be assumed to reflect full contractual intent but should instead be understood as a deliberate choice to delegate performance to code (Suleymanli, 2023). This reframing treats the act of deploying or interacting with the smart contract as evidence of a narrower intention—namely, to carry out specific tasks under predetermined conditions—while leaving room for human interpretation of broader legal obligations. Similarly, courts may treat interaction with the system as a valid expression of consent, provided that the user's conduct reasonably reflects agreement under the circumstances. Studies addressing digital platforms indicate that outward actions, such as authorizing a blockchain transaction or triggering an automated function, can serve as manifestations of assent, much like clicking an "I agree" button in online contracting (Lee, 2021). However, such manifestations must be contextualized within an understanding of how technologically mediated interactions differ from traditional negotiations. This leads to a reinterpretation of the meeting-of-the-minds doctrine, which must now account for environments in which one party may act through coded logic rather than human communication. Scholars examining civil law and comparative doctrine emphasize that consensus may need to be understood as alignment between human intention and system-defined behavior rather than purely interpersonal understanding (Kirillova & Эльдарович, 2023).

Standardization efforts contribute additional pathways for reconciling smart contracts with legal doctrine. As blockchain adoption expands, industries and regulatory bodies increasingly seek uniform approaches that promote legal certainty, interoperability, and fairness. Analyses of smart contract governance frameworks argue that standardized models can reduce interpretive ambiguity by establishing widely recognized technical and legal specifications (Vasiu, 2023). International organizations, including standard-setting bodies and industry consortia, have begun developing frameworks that define the structure, safety requirements, and audit processes for smart contracts. Policymakers have also undertaken initiatives to adapt existing legal systems to blockchain-based contracting. Scholars examining national legal developments highlight amendments to commercial codes aimed at clarifying how automated transactions fit within established doctrines, including efforts to update statutory language governing offer, acceptance, and performance in automated contexts (Nikzad & Sadiq, 2023). In parallel, jurisdictions investigating distributed ledger technology propose model laws addressing contractual validity, evidentiary treatment of code, and recognition of digital signatures. These initiatives reflect a growing consensus that harmonized standards can support judicial interpretation and reduce the unpredictability associated with bespoke coded agreements.

Innovations in dispute resolution offer another means of addressing the doctrinal challenges posed by smart contracts. On-chain arbitration mechanisms have emerged as a tool for resolving disputes entirely within the blockchain environment, relying on decentralized adjudicators or algorithmic procedures to assess claims and determine remedies. Scholars assessing these systems note that they provide speed and efficiency but require robust governance safeguards to prevent bias, manipulation, or abuse (Binns, 2022). Off-chain remedies remain essential, particularly when disputes require interpretive analysis, equitable relief, or interventions beyond the technical scope of code. Legal studies recognize that traditional courts continue to play a crucial role in interpreting coded agreements and ensuring compliance with public policy (Kirillova & Эльдарович, 2023). Smart-contract modifiers, often referred to as "escape hatches," allow for human intervention in exceptional cases by enabling authorized parties to pause, amend, or reverse automated execution. These mechanisms address doctrinal concerns relating to mistake, unconscionability, and misaligned intent by providing pathways for correction when code does not reflect the parties' actual understanding. Policy research examining national approaches to blockchain systems underscores that reversibility frameworks are key components of trustworthy digital contracting, ensuring that automated processes do not operate beyond the bounds of legal fairness (Research Institute of Information Technology Law of the, 2023). Through these combined innovations, smart contracts can be reconciled with doctrines that demand human interpretive oversight, contextual evaluation, and equitable flexibility.

Together, hybrid models, layered architectures, doctrinal reinterpretations, standardization efforts, and dispute resolution innovations demonstrate that automation need not operate in isolation from legal principles. Instead, these approaches illustrate how smart contracts can evolve into legally interoperable instruments that harness technological efficiency while retaining the values embedded in the doctrines of intent and consent.

6. Conclusion

The evolution of smart contracts marks one of the most profound transformations in the modern law of obligations, challenging long-established doctrines that have guided courts, legislators, and legal practitioners for generations. As blockchain-based contracting systems increasingly shape commercial, financial, governmental, and private interactions, legal doctrine faces the difficult task of integrating automated enforcement mechanisms into a framework historically grounded in human judgment, interpretive flexibility, and evaluative reasoning. The analysis presented throughout this review demonstrates that smart contracts both illuminate and intensify foundational tensions surrounding intent, consent, mistake, fairness, and interpretation, forcing jurists to reconsider how these concepts function in environments where code takes over tasks once performed by human actors.

At the core of these tensions lies the question of how legal systems should conceptualize the nature of intent in a world where contractual performance may be executed without direct human intervention. Traditional doctrine has long required clear manifestations of intention to create legally binding obligations, yet automated systems blur the line between deliberate legal engagement and merely operational interaction. The distinction between intending to be legally bound and intending only to automate a process proves crucial to reconciling smart contracts with doctrinal expectations. This challenge becomes even more pronounced when considering that coded instructions are often designed, modified, or deployed by actors other than the contracting parties themselves. As technological systems continue to mediate contractual behavior, courts and legislators must determine how much weight to assign to the actions of machines and interfaces when evaluating the intentions of human participants.

Consent, the twin pillar of contractual validity, encounters equally significant pressures in automated environments. Smart contracts typically rely on user actions that trigger coded outcomes, but these actions may not reflect meaningful or informed consent. The shift from “consent by understanding” to “consent by interaction” demands a rethinking of how contractual assent is identified, authenticated, and validated. The risks are amplified by information asymmetries between technically sophisticated coders and ordinary users, as well as by the opacity inherent in algorithmic systems that conceal their internal logic from those interacting with them. The resulting environment invites profound doctrinal questions about the legitimacy of agreements formed through opaque or simplified interfaces and whether implied consent can truly stand in for informed, voluntary agreement in a technologically complex ecosystem.

The rigidity of smart contract execution additionally forces reconsideration of doctrines related to mistake and error. Traditional legal systems have long provided remedies when parties operate under incorrect assumptions, misunderstandings, or mutual misinterpretations. Yet smart contracts, designed to execute without discretion or evaluative capacity, treat coded instructions as absolute. This creates a tension between the immutability of blockchain-based performance and the equitable flexibility historically embedded in contract law to prevent injustice. As disputes emerge involving coding errors, unforeseen consequences, or unintended execution events, legal systems must grapple with the challenge of identifying appropriate remedies that account for both technological limitations and the enduring need for fairness in contractual relationships.

Concerns about unconscionability and fairness further underscore the limitations of automated contracting. The deterministic nature of smart contracts can allow unequal bargaining power, technological illiteracy, or unfair templates to produce results that contradict the normative foundations of private law. Automated enforcement of terms that would traditionally be considered oppressive or exploitative creates a risk that technological sophistication becomes a tool for bypassing the protective mechanisms doctrine was designed to uphold. These concerns reflect not only issues of individual justice but also broader questions about the integrity of legal systems tasked with promoting equitable outcomes.

Interpretation, arguably the most conceptually difficult area, reveals the sharpest divergence between the logic of code and the interpretive traditions of law. Courts must reconcile the precision and rigidity of machine-executable instructions with the ambiguity, nuance, and contextual richness that characterize human communication. Hybrid models and layered structures attempt to bridge this divide by preserving natural language text alongside executable logic, but even these innovations require courts to develop new methods for reading, understanding, and resolving conflicts between differing forms of contractual expression. The growing need for technical expertise within legal interpretation challenges long-standing evidentiary doctrines and raises important questions about the distribution of interpretive authority in technologically advanced systems.

Despite these tensions, the analysis also shows that smart contracts and traditional doctrine need not exist in opposition. Innovation in hybrid contract design, layered architectures, standardization initiatives, and dispute-resolution mechanisms demonstrates that automation can complement rather than replace doctrinal principles. By redefining intent in operational terms, contextualizing consent within technologically mediated actions, and incorporating reversibility or override mechanisms into automated systems, legal frameworks can preserve core doctrinal values while embracing the efficiencies offered by smart technology. Through thoughtful reinterpretation and calibrated adaptation, contract law can evolve to accommodate the new reality of automated performance without abandoning the human-centered foundations that give legal agreements their meaning.

Ultimately, the future of smart contracting depends on the development of legal principles that integrate technological innovation with longstanding doctrinal commitments. Achieving this balance requires a dual recognition: that automated systems offer unparalleled efficiency and precision, and that the legitimacy of private law rests on doctrines deeply rooted in human intention, fairness, and interpretive judgment. The challenge for courts, legislators, and legal theorists is to build frameworks that acknowledge the capabilities of code while ensuring that the values of contract law remain intact. With careful doctrinal adjustment and ongoing evaluation, smart contracts can become instruments that operate not only efficiently but also justly within the broader architecture of private law.

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

Alanazi, F., & Gay, V. (2020). E-Health for Diabetes Self Management in Saudi Arabia: Barriers and Solutions (Preprint). https://doi.org/10.2196/preprints.18085

Alazab, M., Alhyari, S., Awajan, A., & Abdallah, A. B. (2020). Blockchain Technology in Supply Chain Management: An Empirical Study of the Factors Affecting User Adoption/Acceptance. *Cluster Computing*, *24*(1), 83-101. https://doi.org/10.1007/s10586-020-03200-4

Binns, D. (2022). No Free Tickets. *M/C Journal*, *25*(2). https://doi.org/10.5204/mcj.2882

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

Butchart, L. (2021). On the Status of Rights. *Voices in Bioethics*, *7*. https://doi.org/10.52214/vib.v7i.8352

Farvin, S. F., Nithyashree, R., Sivanandhini, R., & Subasri, D. R. (2023). U-Medchain A Blockchain Based System for Medical Records Access and Permissions Management. *International Journal of Advanced Research in Science Communication and Technology*, 297-303. https://doi.org/10.48175/ijarsct-9133

Hunn, P. G. (2019). Smart Contractsas Techno-Legal Regulation. *Journal of Ict Standardization*, *7*(3), 269-286. https://doi.org/10.13052/jicts2245-800x.735

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

Lee, A. (2021). In the Shadow of Platforms. *M/C Journal*, *24*(2). https://doi.org/10.5204/mcj.2750

Nikzad, S., & Sadiq, A. R. (2023). Legal Analysis of Smart Contracts in the Iranian Legal System. *Quarterly Journal of Private Law Research*, *9*(36), 83-98.

Research Institute of Information Technology Law of the, J. (2023). *Policy Research Report on Smart Contracts and Their Legal Impacts in Iran*. Research Center of the Judiciary.

Suleymanli, O. (2023). Basic Terms for Conclusion and Entry Into Force of Contracts. *Scientific Work*, *17*(4), 81-87. https://doi.org/10.36719/2663-4619/89/81-87

Vasiu, I. (2023). Framework for Effective Smart Contracting. *Bratislava Law Review*, *7*(2), 107-122. https://doi.org/10.46282/blr.2023.7.2.511