IJCCL

Journal of Civil Criminal Law

E-ISSN: 3089-6878
P-ISSN: 3089-6886

Research Article

The Evolution of Contractual Liability in Smart Agreements: Legal Challenges of Blockchain-Based Transactions within Civil and Criminal Law Perspectives

H Muhamad Rezky Pahlawan MP[1*], Baharuddin Riqiey[2]

[1] Pamulang University, Indonesia; e-mail: rezkymustikaputra@gmail.com
[2] Narotama University, Indonesia; e-mail: baharuddin.riqiey@narotama.ac.id
* Corresponding Author: H Muhamad Rezky Pahlawan MP

Abstract: Background: The rapid development of blockchain technology and smart contracts has fundamentally transformed contractual relationships by shifting the role of human interpretation and enforcement toward automated, code-based, and decentralized systems. This transformation generates complex legal implications, particularly regarding the evolution of contractual liability, which is increasingly distributed and no longer centered on a single legal subject. **Objective:** This study aims to analyze the evolution of contractual liability in smart agreements and examine how such transformation affects the fundamental principles of traditional contract law within modern legal systems. **Methods:** This research employs a normative and conceptual legal approach, supported by an analysis of blockchain regulations across multiple jurisdictions, case studies of smart contract implementation, and a comparative legal analysis between civil law and common law systems, complemented by a multidisciplinary literature review. **Results:** The findings indicate that contractual liability in smart agreements has evolved from a centralized fault-based liability model to an algorithmic, distributed, and code-dependent liability structure within blockchain ecosystems. This evolution creates new legal challenges concerning the attribution of liability, legal certainty, and the limitation of judicial intervention in automated contractual arrangements. Furthermore, the study identifies a tension between technological efficiency and substantive legal justice, highlighting the need for adaptive legal frameworks capable of accommodating decentralized technologies while ensuring the protection of legal rights and accountability of involved parties.

Keywords: Blockchain; Contractual Liability; Decentralized Systems; Disruptive Technology; Smart Contracts

Received: July 16, 2025
Revised: September 10, 2025
Accepted: November 5, 2025
Published: December 31, 2025
Curr. Ver.: December 31, 2025

1. Introduction

The development of blockchain technology over the past decade has demonstrated a significant transformation, both technically and in terms of its legal and societal implications. Initially introduced as the underlying infrastructure for cryptocurrencies such as Bitcoin, blockchain functioned as a decentralized ledger system that enabled secure and transparent transactions without the need for a central authority. However, with the rapid advancement of digital technologies and the growing demand for trustworthy systems, blockchain has evolved into a foundational technology applied across various sectors, including finance, supply chain management, real estate, and public data governance. Its core characteristics decentralization, cryptographic security, and transparency have positioned blockchain as a viable solution to the persistent issue of trust deficits in digital transactions (Amla & Bhatia, 2025; Singh et al., 2024). Consequently, blockchain is no longer viewed merely as a technological innovation, but as a transformative paradigm shaping the digital economy.

One of the most groundbreaking innovations emerging from blockchain technology is the concept of smart contracts. These are digital contracts written in code that can automatically execute predefined actions once specific conditions are met. Unlike traditional contracts, which rely on intermediaries such as lawyers, notaries, or courts for validation and enforcement, smart contracts operate autonomously within the blockchain network. This automation significantly enhances efficiency, reduces transaction costs, minimizes human error, and ensures the immutability of contractual records (Banerjee & Saha, 2023; Shumyliak et al., 2023). As a result, smart contracts introduce a new model of contractual interaction that is faster, more reliable, and technologically driven.

The evolution of smart contracts has further led to the emergence of smart agreements, which integrate legal principles with algorithmic execution. Smart agreements represent a hybrid model in which contractual obligations are embedded within code while still reflecting the intent of the parties involved. In traditional legal frameworks, contract enforcement depends heavily on institutional mechanisms such as courts and dispute resolution systems. In contrast, smart agreements rely on deterministic code that automatically enforces contractual terms once predefined conditions are satisfied (Durovic & Willett, 2023; Upadhyay et al., 2021). This shift signifies a fundamental transformation in contractual relationships, where trust is transferred from legal institutions to technological systems.

However, this transformation also raises critical concerns regarding foundational principles of contract law, particularly party autonomy and contractual flexibility. In conventional contracts, parties retain the ability to renegotiate, interpret, or terminate agreements under specific circumstances, such as unforeseen events or force majeure. In contrast, smart agreements are inherently rigid, as their execution is strictly governed by pre-programmed code, leaving little room for human intervention once deployed. This rigidity may lead to outcomes that no longer reflect the original intent of the parties, thereby challenging principles of fairness and equity in contract law (van Eck, 2020; Werbach & Cornell, 2017). Therefore, a reassessment of traditional legal doctrines is necessary to accommodate this technological evolution.

In addition to civil law implications, smart contracts also pose significant challenges in terms of enforceability and liability. The immutable and irreversible nature of blockchain-based contracts means that once executed, they cannot easily be altered or revoked, even in cases of coding errors or unforeseen circumstances. This creates a legal dilemma, as traditional remedies such as contract rescission or judicial intervention may not be applicable in such contexts (Rizos, 2022; Sinitsyn et al., 2022). As a result, the gap between technological capabilities and existing legal frameworks becomes increasingly evident.

The issue of legal liability further complicates the use of smart contracts. In cases where financial loss occurs due to faulty code or system vulnerabilities, determining responsibility becomes challenging. Questions arise as to whether liability should be attributed to developers, users, or other stakeholders within the blockchain ecosystem. Moreover, the borderless nature of blockchain technology introduces jurisdictional complexities, as transactions may involve parties from multiple legal systems (Cinque, 2022; Jiménez, 2025). These challenges highlight the inadequacy of traditional legal approaches in addressing the multifaceted risks associated with smart contracts.

Furthermore, the anonymity and pseudonymity inherent in blockchain systems create opportunities for the misuse of smart contracts in criminal activities. Studies have shown that malicious actors can exploit smart contracts to facilitate illegal activities such as money laundering, fraud, and covert collusion. The emergence of criminal smart contracts, which are deliberately designed to execute unlawful actions autonomously, underscores the potential risks associated with this technology (Ndiaye & Konate, 2021). This demonstrates that while smart contracts offer efficiency and innovation, they also present significant threats to legal order and public security.

In addition, technical vulnerabilities within smart contracts, such as coding bugs and security flaws, have been widely exploited by cybercriminals. These vulnerabilities can lead to substantial financial losses and are often difficult to remedy due to the immutable nature of blockchain systems. Empirical evidence indicates that attacks on smart contracts are becoming increasingly sophisticated, highlighting the need for robust security measures alongside legal regulation (Gritti et al., 2023; Zhang et al., 2019). Therefore, legal and technological safeguards must be developed concurrently to mitigate these risks.

Despite the growing academic and practical interest in blockchain and smart contracts, the integration of civil and criminal law in this domain remains underdeveloped. While traditional contract law continues to provide a foundational framework, its application to smart contracts is often unclear, particularly in terms of enforcement, evidence, and the protection of civil rights (Gliha & Marković, 2021; Yu et al., 2025). Additionally, the lack of harmonized global regulations further complicates the governance of blockchain-based transactions.

This regulatory gap underscores the need for an interdisciplinary approach that combines legal theory, technological expertise, and public policy. Without a comprehensive and adaptive legal framework, the misuse of smart contracts is likely to increase, potentially undermining fundamental principles of justice and human rights. Some studies have even identified cases of intentionally illicit smart contracts designed to evade legal scrutiny (Bejček, 2020; DiMatteo et al., 2019). Accordingly, the development of a coherent regulatory system is both urgent and necessary.

Based on the foregoing discussion, this study aims to analyze the evolution of contractual liability within smart agreements, particularly in the context of the intersection between civil and criminal law. It seeks to examine how traditional contract law principles can be adapted to regulate smart contracts and to identify the need for new regulatory frameworks capable of addressing emerging challenges. Ultimately, this research is expected to contribute to the development of a more adaptive, responsive, and just legal system in the digital era.

2. Literature Review

Contract Theory in Civil Law

Contract theory constitutes one of the fundamental pillars of civil law, governing the formation, interpretation, and enforcement of agreements between parties. As legal systems evolve in response to social, economic, and technological developments, contract theory has also undergone significant transformation. This section reviews key theoretical foundations and contemporary developments in contract law, focusing on its normative principles, conceptual frameworks, and practical implications within civil law systems.

Fundamental Principles of Contract Theory

At the core of traditional contract theory lies the principle of freedom of contract, which assumes that individuals possess the autonomy to determine the terms and conditions of their agreements without undue interference. This principle reflects a liberal legal philosophy that prioritizes individual will and consent as the basis of legal obligations. Closely related to this is the doctrine of pacta sunt servanda, which asserts that agreements that are lawfully concluded must be respected and performed in good faith. Together, these principles form the backbone of contractual relationships in civil law systems, ensuring legal certainty and predictability in private transactions (Ding, 2017; Fairgrieve, 2016).

However, modern contract law has increasingly recognized that absolute contractual freedom may lead to imbalances, particularly in situations involving unequal bargaining power. As a result, contemporary legal discourse emphasizes the need to balance autonomy with fairness and social justice. This shift reflects a broader understanding that contracts are not merely private arrangements but also social instruments that must align with public values and legal norms (Prabantarikso, 2024).

In addition, the principle of good faith (bona fide) has become a central element in civil law jurisdictions. Good faith operates both as a guiding principle in the formation and performance of contracts and as a corrective mechanism to prevent abuse of rights. It requires parties to act honestly, fairly, and reasonably in their contractual dealings. In European civil law, the concept of objective good faith has been further developed to include protections for third parties affected by contractual relationships, thereby expanding the scope of contractual responsibility beyond the immediate parties (Benli, 2020).

Normative and Conceptual Dimensions of Contract Theory

Contract theory can be broadly categorized into normative and instrumental approaches, each offering distinct perspectives on the purpose and function of contracts. Normative theories focus on moral and philosophical justifications for contractual obligations, emphasizing concepts such as promise-keeping, autonomy, and justice. These theories argue that contracts should be enforced because they represent voluntary commitments that individuals are morally bound to honor (Wibye, 2025).

In contrast, instrumental or economic approaches view contracts as tools for achieving efficiency and maximizing social welfare. From this perspective, the primary objective of contract law is to facilitate efficient allocation of resources and minimize transaction costs. Legal rules are therefore evaluated based on their ability to promote economic outcomes rather than moral considerations. While these approaches differ in their underlying assumptions, contemporary scholarship often integrates both perspectives to provide a more comprehensive understanding of contract law (Wibye, 2025).

The interplay between these approaches highlights the complexity of contract law as both a legal and social institution. It demonstrates that contract theory cannot be reduced to a single dimension but must be understood as a dynamic framework that accommodates multiple values, including fairness, efficiency, and legal certainty.

Protection of the Weaker Party

One of the most significant developments in modern contract law is the increasing emphasis on protecting weaker parties in contractual relationships. Traditional contract theory assumes that parties enter agreements on equal footing; however, in practice, disparities in knowledge, resources, and bargaining power often result in unfair outcomes. To address this issue, civil law systems have introduced various mechanisms to ensure substantive fairness.

For instance, legal frameworks in jurisdictions such as Jordan recognize the need for judicial or legislative intervention to restore contractual balance when one party is disproportionately disadvantaged. Courts may adjust contractual obligations or limit liability to prevent unjust enrichment or exploitation (Al-Sharida, 2024). Similarly, contemporary scholarship highlights the concept of contractual vulnerability, which underscores the importance of safeguarding individuals who are structurally disadvantaged in contractual negotiations (Khawaldeh et al., 2024).

Furthermore, contract law has expanded to include protections for third parties affected by contractual relationships. The doctrine of contracts with protective effects for third parties allows individuals who are not direct parties to a contract to claim damages if they suffer harm as a result of its performance. This development reflects a broader shift toward recognizing the social impact of contractual obligations and extending legal protection beyond traditional boundaries (Benli, 2020; Schroeter, 2017).

Economic Analysis and Efficiency in Contract Law

Economic analysis has become an influential approach in the study of contract law, particularly in assessing the efficiency of legal rules. One of the key concepts in this framework is the theory of efficient breach, which posits that breaching a contract may be economically justified if it results in a net gain for society. Under this theory, a party may choose to breach a contract if the benefits of doing so exceed the costs, provided that adequate compensation is paid to the non-breaching party (de Almeida Nunes, 2019).

This perspective challenges traditional notions of contractual obligation by suggesting that strict enforcement may not always lead to optimal outcomes. Instead, it advocates for a more flexible approach that considers the broader economic implications of contractual behavior. While controversial, the theory of efficient breach has contributed to a more nuanced understanding of contract law, particularly in commercial contexts where efficiency and profitability are key considerations.

Evolution of Contract Theory in Civil Law Systems

The evolution of contract theory in civil law systems has been significantly influenced by comparative legal developments and cross-jurisdictional borrowing. Civil law jurisdictions have increasingly incorporated concepts from common law, such as anticipatory breach, which allows a party to seek remedies before an actual breach occurs. Similarly, doctrines such as change of circumstances, rooted in German law, provide mechanisms for adapting contracts in response to unforeseen events (Schroeter, 2017).

Comparative studies also reveal fundamental differences between civil law and common law systems, particularly in concepts such as consideration and cause. While common law emphasizes the requirement of consideration as a basis for enforceability, civil law systems rely on the concept of cause and place greater emphasis on good faith and fairness. These differences highlight the diversity of legal traditions and the importance of contextualizing contract theory within specific legal frameworks (Fairgrieve, 2016).

Moreover, recent socio-legal approaches emphasize the embeddedness of contracts within broader social and institutional contexts. Contracts are no longer viewed solely as legal instruments but as social practices shaped by cultural norms, economic conditions, and institutional structures. This perspective underscores the need for a holistic understanding of contract law that integrates legal doctrine with social reality (Prabantarikso, 2024).

Smart Contracts, Blockchain Technology, and Legal Enforceability in Digital Transactions

Concept of Smart Contracts and Blockchain Technology

Blockchain technology has emerged as a foundational innovation in the digital era, fundamentally transforming how data and transactions are recorded, verified, and secured. Initially developed as the underlying infrastructure for cryptocurrencies such as Bitcoin, blockchain operates as a distributed ledger technology (DLT) that enables decentralized record-keeping without the need for a central authority. Each transaction is stored in a block and linked to previous blocks through cryptographic mechanisms, forming an immutable and tamper-resistant chain of data. This structure ensures transparency, traceability, and security, making blockchain particularly suitable for environments where trust among parties is limited (Dongfang & Wang, 2022; Singh et al., 2024). As a result, blockchain has been widely adopted across various sectors, including finance, healthcare, logistics, and digital identity management.

Building upon blockchain infrastructure, smart contracts represent a significant advancement in the automation of contractual relationships. Smart contracts are self-executing digital protocols in which the terms of the agreement are directly encoded into software programs deployed on blockchain networks. Once predefined conditions are met, these contracts automatically execute without requiring intermediaries such as lawyers or financial institutions. This automation enhances efficiency, reduces transaction costs, and minimizes the risks associated with human error and opportunistic behavior (Bhattacharya et al., 2023; Jesse, 2022). Furthermore, platforms such as Ethereum have played a crucial role in enabling the widespread development of smart contracts by providing programmable blockchain environments that support complex decentralized applications.

The application of smart contracts extends beyond financial transactions into diverse domains such as healthcare, Internet of Things (IoT), supply chain management, and digital identity systems. In healthcare, for instance, smart contracts can facilitate secure data sharing among stakeholders while maintaining patient privacy. In supply chains, they enable real-time tracking and automated verification of goods, thereby enhancing transparency and efficiency. Similarly, in IoT ecosystems, smart contracts can automate interactions between connected devices, creating more responsive and autonomous systems (Bhattacharya et al., 2023; Sharma et al., 2023). These wide-ranging applications demonstrate the transformative potential of smart contracts in modern digital infrastructures.

Despite these advantages, blockchain and smart contracts face several significant challenges that hinder their broader adoption. One of the primary issues is scalability, as blockchain networks often struggle to process large volumes of transactions efficiently. Additionally, high energy consumption associated with certain consensus mechanisms, such as proof-of-work, raises concerns regarding environmental sustainability. Another critical challenge lies in regulatory uncertainty, as existing legal frameworks are often ill-equipped to address the unique characteristics of decentralized technologies (Sharma et al., 2023; Singh et al., 2024). These challenges highlight the need for continued technological innovation and regulatory development.

Legal Enforceability in Digital Transactions

The integration of smart contracts into legal systems raises important questions regarding their enforceability in digital transactions. From a legal perspective, smart contracts possess several features that support their recognition as valid contractual instruments, including transparency, immutability, and traceability. Blockchain consensus mechanisms ensure that transactions are validated and recorded in a manner that is resistant to tampering, thereby enhancing the evidentiary value of smart contracts in legal proceedings (Kusber et al., 2020). Consequently, smart contracts have the potential to fulfill essential elements of a legally binding agreement, such as offer, acceptance, and intention to create legal relations.

However, the incorporation of smart contracts into traditional legal frameworks remains complex, particularly in cross-border contexts. Differences in national regulations create inconsistencies that can undermine legal certainty in international digital transactions. Comparative legal studies indicate that the lack of harmonized standards poses a significant barrier to the widespread adoption of smart contracts, as parties may face uncertainty

regarding applicable law and jurisdiction (Poncibò, 2021). This issue is further compounded by the decentralized nature of blockchain, which challenges conventional notions of territorial jurisdiction.

Another critical aspect of legal enforceability concerns the validity of electronic signatures in blockchain-based transactions. Digital signatures play a crucial role in verifying the identity of contracting parties and ensuring the authenticity of agreements. Research suggests that blockchain-based digital signatures may be functionally equivalent to handwritten signatures, provided that they meet certain legal and technical requirements (Dostov et al., 2023). Regulatory frameworks such as the European Union's eIDAS Regulation have established standards for electronic identification and trust services, thereby supporting the legal recognition of digital transactions. Nevertheless, the implementation of such frameworks varies across jurisdictions, leading to inconsistencies in legal recognition.

Consumer protection also represents a key concern in digital transactions involving smart contracts. The automated and irreversible nature of these contracts may expose consumers to risks, particularly in cases of coding errors or unfair contractual terms. Legal scholars emphasize the need for both preventive and corrective measures to safeguard consumer rights, including clear regulatory standards, dispute resolution mechanisms, and oversight by regulatory authorities (Risal, 2024; Septiningsih & Karimullah, 2024). Ensuring adequate consumer protection is essential for maintaining trust and fairness in digital markets.

In addition to regulatory challenges, the enforcement of smart contracts raises practical issues related to dispute resolution. Traditional judicial systems may be ill-equipped to handle disputes arising from blockchain-based transactions due to their technical complexity and cross-border nature. As a result, alternative mechanisms such as Online Dispute Resolution (ODR) have gained prominence as efficient tools for resolving disputes in the digital environment. ODR platforms enable parties to resolve conflicts remotely, often through automated or semi-automated processes, thereby reducing time and costs associated with litigation (Lozada & Talero, 2024). These mechanisms represent an important complement to existing legal systems in addressing the challenges of digital transactions.

Overall, the legal enforceability of smart contracts depends on the ability of legal systems to adapt to the unique characteristics of blockchain technology. While significant progress has been made in recognizing digital transactions, substantial gaps remain in terms of regulatory harmonization, consumer protection, and dispute resolution. Addressing these challenges requires an integrated approach that combines legal reform, technological innovation, and international cooperation.

Criminal Risks in Decentralized Systems

Decentralized systems, particularly those based on blockchain technology and decentralized applications (DApps), have transformed the digital landscape by offering enhanced transparency, security, and autonomy. These systems operate without centralized control, relying instead on distributed networks and cryptographic protocols to validate transactions. While such characteristics provide significant advantages, including resistance to censorship and improved data integrity, they also introduce complex criminal risks that challenge traditional law enforcement mechanisms. The anonymity and pseudonymity inherent in blockchain systems allow users to interact without revealing their real identities, creating opportunities for misuse in illicit activities (Bhardwaz et al., 2023).

One of the most prominent criminal risks in decentralized systems is the facilitation of illegal activities through anonymous infrastructures. For instance, ransomware-as-a-service (RaaS) has emerged as a sophisticated cybercrime model that leverages blockchain platforms such as Ethereum and decentralized storage systems like the InterPlanetary File System (IPFS). These technologies enable cybercriminals to deploy ransomware operations while maintaining anonymity and avoiding detection by authorities. The decentralized nature of these platforms makes it significantly more difficult to trace transactions and identify perpetrators, thereby complicating enforcement efforts (Karapapas et al., 2020). This phenomenon illustrates how decentralized technologies can be weaponized to support organized cybercrime.

Despite their decentralized architecture, many blockchain ecosystems still contain elements of centralization that introduce additional security vulnerabilities. Research indicates that components such as third-party scripts, centralized service providers, and privileged operations can create single points of failure within otherwise decentralized systems. These vulnerabilities may lead to privacy breaches, unauthorized access, and exploitation by malicious actors. The coexistence of decentralized and centralized elements creates a hybrid risk environment in which the perceived security of blockchain systems may be undermined

by hidden dependencies (Yan et al., 2023). Consequently, the security of decentralized systems must be assessed not only at the protocol level but also across the broader ecosystem.

Another significant concern relates to the vulnerabilities inherent in smart contracts, which are integral to many blockchain-based systems. Smart contracts are often susceptible to coding errors, flawed logic, and inadequate key management practices. These weaknesses can be exploited by attackers to manipulate contract execution, steal funds, or disrupt system operations. Additionally, threats such as 51% attacks where a single entity gains majority control over the network pose serious risks to the integrity and reliability of blockchain systems. Such vulnerabilities highlight the importance of robust security auditing and governance mechanisms in mitigating risks associated with decentralized technologies (Bhardwaz et al., 2023; Dhar et al., 2025).

Overall, while decentralized systems offer innovative solutions for digital transactions and data management, they simultaneously create new avenues for criminal activity. The combination of anonymity, technical complexity, and regulatory gaps makes these systems particularly attractive to cybercriminals. Addressing these risks requires a comprehensive understanding of both technological and legal dimensions, as well as coordinated efforts between stakeholders.

Legal Approaches to Disruptive Technologies

Disruptive technologies, including blockchain, artificial intelligence (AI), and neurotechnology, present significant challenges to traditional legal frameworks. These technologies evolve rapidly, often outpacing the ability of existing laws and regulations to adequately address their implications. As a result, there is a growing need for adaptive legal approaches that can effectively manage risks while fostering innovation. Scholars argue that conventional regulatory models, which tend to be rigid and reactive, are insufficient for governing technologies characterized by decentralization, automation, and cross-border functionality (Taeihagh, 2023).

One promising approach to regulating disruptive technologies is the adoption of dynamic and collaborative regulatory frameworks. Regulatory sandboxes, for example, provide controlled environments in which new technologies can be tested under the supervision of regulatory authorities. This approach allows policymakers to better understand technological risks and develop appropriate legal responses without stifling innovation. In the context of artificial intelligence and blockchain, sandbox mechanisms enable iterative learning and regulatory experimentation, facilitating more effective governance (Badinszky, 2025). Such frameworks represent a shift toward more flexible and responsive regulatory strategies.

Another critical aspect of legal approaches to disruptive technologies involves the protection of fundamental rights, particularly in the digital age. Technologies such as blockchain and AI can have profound implications for privacy, data protection, and individual autonomy. The collection, processing, and storage of large volumes of data raise concerns about surveillance, misuse of personal information, and erosion of civil liberties. Legal scholars emphasize the need to integrate human rights considerations into the design and regulation of digital technologies, ensuring that technological advancement does not come at the expense of fundamental freedoms (Benlloch Domènech & Sarrión Esteve, 2022).

In addition to rights-based concerns, the governance of disruptive technologies must also address broader socio-economic and political dimensions. Legal frameworks should consider issues such as digital inequality, access to technology, and the distribution of risks and benefits among different stakeholders. A holistic approach to regulation requires collaboration between governments, industry actors, and civil society to develop inclusive and sustainable policies. This is particularly important in the context of decentralized systems, where traditional regulatory boundaries are blurred and enforcement mechanisms are less effective (Taeihagh, 2023).

Furthermore, legal responses to disruptive technologies must incorporate proactive cybersecurity strategies to mitigate emerging threats. As decentralized systems become more prevalent, ensuring their resilience against cyberattacks becomes a critical priority. Legal instruments should support the development of security standards, accountability mechanisms, and risk management frameworks that can adapt to evolving technological landscapes. By integrating legal and technical approaches, policymakers can enhance the security and reliability of digital ecosystems (Dhar et al., 2025).

In conclusion, the intersection of decentralized technologies and criminal risks necessitates a rethinking of traditional legal approaches. While blockchain and related technologies offer significant benefits, their misuse and associated risks require robust and adaptive regulatory frameworks. Effective governance must balance innovation with

accountability, ensuring that technological progress aligns with legal principles and societal values.

3. Research Method

This study adopts a normative and conceptual legal research approach to analyze the legal implications of blockchain technology and smart contracts within contemporary legal systems. The normative approach focuses on examining legal principles, doctrines, and statutory regulations governing contractual relationships, while the conceptual approach is used to explore theoretical frameworks related to decentralization, legal enforceability, and contractual liability in digital environments. By combining these approaches, the research seeks to understand how traditional legal doctrines can be interpreted and adapted to accommodate emerging technologies, particularly in the context of automated and self-executing agreements.

Furthermore, this research includes an analysis of blockchain regulations across multiple jurisdictions to identify regulatory patterns, inconsistencies, and gaps in the governance of decentralized systems. This analysis is complemented by a case study approach that examines the practical implementation of smart contracts in sectors such as finance, supply chain management, and digital services. Through these case studies, the research evaluates how smart contracts operate in real-world contexts, including their efficiency, potential risks, and legal challenges, especially in situations involving disputes, system vulnerabilities, or misuse of technology.

In addition, the study employs a comparative legal analysis to assess differences and similarities between legal frameworks, particularly within civil law and common law traditions, in addressing issues related to smart contracts. This comparative perspective focuses on aspects such as contract formation, interpretation, enforcement, and the role of judicial intervention. To support the analysis, the research is grounded in a multidisciplinary literature review, integrating insights from law, information technology, economics, and cybersecurity. This comprehensive methodological framework enables the study to provide a holistic and critical evaluation of legal responses to blockchain technology and to propose adaptive regulatory approaches aligned with technological developments.

4. Results and Discussion

The findings of this study demonstrate that blockchain technology and smart contracts have fundamentally reconfigured the architecture of contractual relations by shifting contractual execution from a human-centered interpretative system to an automated, code-driven enforcement mechanism. In this transformed environment, contractual obligations are no longer primarily mediated by judicial interpretation or discretionary enforcement, but by deterministic computational protocols embedded within decentralized networks. This shift represents a paradigmatic evolution in contract law, where trust is no longer institutionally mediated but technologically embedded, thereby altering the foundational logic of contractual accountability.

A key result of this transformation is the redefinition of contractual liability from a traditional fault-based model to an algorithmically mediated and distributed liability structure. In conventional legal systems, liability arises from identifiable human conduct, such as intent, negligence, or breach of contractual duty, and is ultimately assessed through judicial reasoning. However, in smart agreements, the execution of contractual obligations is pre-programmed, meaning that liability is no longer solely attributable to a single actor but is instead dispersed across multiple layers of the technological ecosystem. These layers include software developers, platform operators, node validators, and end-users. As a consequence, the study finds that contractual liability evolves into a fragmented construct in which responsibility becomes difficult to localize within traditional doctrinal categories.

The study further reveals that this evolution introduces a critical tension between deterministic execution and normative justice. While smart contracts ensure certainty and immutability in execution, they simultaneously eliminate the corrective function of judicial discretion, which in traditional contract law serves to mitigate unfair or unintended outcomes. This creates a structural limitation in which the principle of "code is law" may conflict with established legal doctrines such as good faith (bona fides), reasonableness, and equity. In several observed implementations, once a smart contract is deployed, its execution cannot be halted or modified without consensus or external intervention, even in cases of manifest error

or unjust enrichment. This rigidity highlights a fundamental misalignment between technological enforcement and legal normativity.

From a comparative legal perspective, the study identifies divergent levels of adaptability between civil law and common law traditions. Civil law systems, grounded in codified norms and structured legal interpretation, face difficulties in classifying smart contracts within existing doctrinal frameworks, particularly regarding contractual formation and defect of consent in code-based agreements. Conversely, common law systems demonstrate greater interpretative flexibility, allowing courts to incrementally recognize novel forms of agreement; however, they still encounter doctrinal uncertainty in assigning liability for autonomous execution failures. Across both systems, the absence of a unified legal taxonomy for smart agreements contributes to regulatory ambiguity and inconsistent judicial responses.

The findings also indicate that cross-jurisdictional enforcement remains one of the most significant structural challenges in the governance of smart contracts. Because blockchain networks operate in a decentralized and borderless environment, traditional conflict-of-law principles such as territorial jurisdiction and choice of law become increasingly difficult to apply. This jurisdictional fragmentation leads to enforcement gaps, particularly in disputes involving parties from multiple legal systems. As a result, legal accountability becomes diluted in transnational blockchain transactions, further complicating the attribution of contractual liability.

In response to these challenges, the study identifies the emergence of adaptive regulatory instruments, particularly regulatory sandboxes, as a transitional governance mechanism. Regulatory sandboxes allow controlled experimentation with blockchain applications under supervisory oversight, enabling regulators to observe technological behavior while gradually developing legal standards. This approach reflects a shift from ex post regulation toward ex ante adaptive governance. However, the study also finds that sandbox mechanisms remain limited in addressing long-term issues of liability allocation, as they primarily focus on innovation facilitation rather than doctrinal reconstruction of contract law.

Another significant finding relates to the increasing prevalence of criminal exploitation within decentralized ecosystems. The anonymity and pseudonymity inherent in blockchain networks facilitate illicit activities such as ransomware attacks, fraud schemes, and illicit financial transfers. The emergence of ransomware-as-a-service models demonstrates how smart contract infrastructure can be repurposed for scalable criminal operations. In such contexts, the decentralization of responsibility also produces a "responsibility vacuum," where identifying legally accountable actors becomes increasingly complex. This directly reinforces the study's core finding regarding the diffusion of contractual liability in decentralized systems.

Technological vulnerabilities further complicate the legal landscape of smart contracts. The study finds that coding errors, inadequate security audits, and vulnerabilities in cryptographic key management constitute significant risk vectors that may lead to unintended contractual outcomes. Unlike traditional contractual breaches, these failures are not always attributable to intentional misconduct but may result from design flaws or systemic interactions within decentralized networks. This raises complex legal questions regarding whether liability should be assigned based on negligence in design, operational responsibility, or strict liability for deployed code. The absence of clear doctrinal guidance exacerbates uncertainty in legal accountability frameworks.

Finally, the study demonstrates that the evolution of smart agreements necessitates a reconceptualization of dispute resolution mechanisms. Traditional litigation models are often inadequate for addressing blockchain-based disputes due to their complexity, irreversibility of execution, and transnational nature. Consequently, alternative mechanisms such as Online Dispute Resolution (ODR) and blockchain-based arbitration systems are gaining relevance as supplementary enforcement structures. However, the study emphasizes that such mechanisms must be anchored in fundamental legal principles, including due process, transparency, and proportionality. Without such safeguards, technological efficiency risks undermining substantive justice.

In synthesis, the study confirms that contractual liability in smart agreements has evolved from a centralized, judge-mediated and fault-based system into a decentralized, algorithmically executed and structurally fragmented liability regime. This evolution reflects

not only a technological transformation but also a doctrinal challenge to the foundations of contract law. Accordingly, the legal system is compelled to develop hybrid regulatory models that integrate technological determinism with normative legal principles to ensure that innovation does not erode accountability, fairness, and legal certainty.

5. Comparison

The comparative analysis between traditional contract law and smart contract-based systems reveals a fundamental transformation in the conceptualization of contractual responsibility and enforcement mechanisms. In traditional legal frameworks, particularly within both civil law and common law traditions, contracts are grounded in human intent, interpretative flexibility, and judicial oversight. Liability is typically assigned based on fault principles, such as negligence, breach of duty, or failure to perform contractual obligations, and courts play a central role in interpreting contractual ambiguity and ensuring equitable outcomes. This structure allows for contextual reasoning, enabling legal systems to adapt contractual obligations to unforeseen circumstances and maintain normative fairness.

In contrast, smart contract systems operate on deterministic code executed within decentralized blockchain networks, where contractual performance is automated and self-enforcing. This shift eliminates the need for intermediaries and significantly reduces interpretative discretion, but simultaneously introduces rigidity in enforcement and fragmentation in liability attribution. While traditional systems centralize responsibility within identifiable legal subjects, smart contract ecosystems distribute responsibility across multiple technical actors, including developers, platform operators, and network validators. Consequently, the comparative findings highlight a structural shift from centralized, interpretive liability regimes to decentralized, algorithmically executed and diffused liability frameworks, creating significant doctrinal challenges for existing legal systems.

6. Conclusion

This study concludes that the evolution of smart agreements represents a profound transformation in the nature of contractual liability, shifting from a human-centered, fault-based legal model toward a decentralized and algorithmically enforced liability structure. In this new paradigm, contractual execution is no longer primarily governed by judicial interpretation or normative discretion but by immutable code embedded within blockchain systems. As a result, liability becomes increasingly fragmented and distributed across multiple actors within the technological ecosystem, thereby challenging the traditional legal assumption that responsibility must be traceable to a singular legal subject.

Furthermore, the study highlights that while smart contracts offer substantial benefits in terms of efficiency, transparency, and automation, they simultaneously generate new legal uncertainties related to fairness, enforceability, and dispute resolution. The absence of comprehensive regulatory harmonization and the rigidity of code-based execution create tensions between technological determinism and fundamental legal principles such as equity and due process. Therefore, the study emphasizes the need for adaptive legal frameworks that integrate technological innovation with normative legal safeguards, ensuring that the evolution of contract law in the digital era remains aligned with principles of accountability, justice, and legal certainty.

References

Al-Sharida, M. M. M. A. (2024). The Limits of Recompense in the Contractual Liability in Jordanian Civil Law. *Revista de Gestão Social e Ambiental*, *18*(4), e06462. https://doi.org/10.24857/rgsa.v18n4-111

Amla, M., & Bhatia, S. A. (2025). Unlocking Potential: An Analysis of Blockchain's Performance Impact on Business Transformation. In *Web 3.0 Unleashed: Transforming Industries and Building Ethical Frameworks* (pp. 125–145). https://doi.org/10.1108/978-1-83708-728-020251007

Badinszky, Á. (2025). Regulating the Most Disruptive Technology — Understanding Why {AI} Should Be Sandboxed. *ELTE Law Journal*, *2025*(1), 111–133. https://doi.org/10.54148/ELTELJ.2025.1.111

Banerjee, K., & Saha, S. (2023). A Comparative Study of Smart Contracts-Based Blockchain. In *Concepts, Technologies, Challenges, and the Future of Web 3* (pp. 289–306). https://doi.org/10.4018/978-1-6684-9919-1.ch015

Bejček, J. (2020). Smartly Illicit {Smart} Contracts Between the Effectiveness of the Contractual Agenda and the Coded Illegality, Especially in the Protection of Competition. *Pravnik*, *159*(5), 377–401.

Benli, E. (2020). Making {`The Principle of Honesty'} (Objective Good Faith) Measurable and Data-Driven Through the Theory of

{`Contract with the Effect of Third Party Protection'}: An Example from European Civil Law Countries. *Lawyer Quarterly*, *10*(2), 73–81.

Benlloch Domènech, C., & Sarrión Esteve, J. (2022). Fundamental Rights and Aporias of the Digital Age. *Cuestiones Constitucionales*, *46*, 3–28. https://doi.org/10.22201/iij.24484881e.2022.46.17046

Bhardwaz, S., Godha, R., Rani, S., & Mehta, A. R. (2023). *Exploring the Hazards of Embracing Decentralization in Blockchain*. https://doi.org/10.1109/GCITC60406.2023.10425880

Bhattacharya, A., Choudhury, T., & Sille, R. (2023). The Role of Smart Contracts and Blockchain Technology in Healthcare and Other Use Cases. In *Blockchain Applications in Healthcare: Innovations and Practices* (Vol. 1, pp. 189–206). https://doi.org/10.1002/9781394229512.ch10

Cinque, A. (2022). Smart Contract: Legal Nature and Contractual Remedies. *Osservatorio Del Diritto Civile e Commerciale*, *11*(2), 639–656. https://doi.org/10.4478/106124

de Almeida Nunes, R. M. (2019). The Efficient Breach of Contract: Perspectives of Enforcement in Brazilian Civil Law. *Civilistica.Com*, *8*(3).

Dhar, S., Kashyap, S., & Kumar, P. (2025). *Enhancing Cybersecurity in Blockchain: Legal Challenges and Solutions*. https://doi.org/10.4018/979-8-3373-2282-7.ch007

DiMatteo, L. A., Cannarsa, M., & Poncibò, C. (2019). *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*. Cambridge University Press. https://doi.org/10.1017/9781108592239

Ding, C. (2017). Perspectives on Chinese Contract Law: Performance and Breach. In *Chinese Contract Law: Civil and Common Law Perspectives* (pp. 301–322). https://doi.org/10.1017/9781316816912.013

Dongfang, J., & Wang, L. (2022). Research on Smart Contract Technology Based on Blockchain. *Proceedings of the 2022 International Conference on Artificial Intelligence in Everything (AIE 2022)*, 664–668. https://doi.org/10.1109/AIE57029.2022.00130

Dostov, V., Krivoruchko, S., Shust, P., & Titov, V. (2023). Are Digital Signatures in Blockchain Functionally Equivalent to Handwritten Signatures? In *Lecture Notes in Computer Science* (Vol. 14104, pp. 527–537). https://doi.org/10.1007/978-3-031-37105-9_35

Durovic, M., & Willett, C. (2023). A Legal Framework for Using Smart Contracts in Consumer Contracts: Machines as Servants, Not Masters. *Modern Law Review*, *86*(6), 1390–1421. https://doi.org/10.1111/1468-2230.12817

Fairgrieve, D. (2016). *Comparative Law in Practice: Contract Law in a Mid-Channel Jurisdiction*. Bloomsbury. https://doi.org/10.5040/9781782257240

Gliha, D., & Marković, S. (2021). Smart Contracts and the Evolution of a Legal Perspective on the Protection of Human Rights. In *Digital Technologies and the Law of Obligations* (pp. 166–180). https://doi.org/10.4324/9781003080596-12

Gritti, F., Ruaro, N., McLaughlin, R., Bose, P., Das, D., Grishchenko, I., Kruegel, C., & Vigna, G. (2023). Confusum Contractum: Confused Deputy Vulnerabilities in Ethereum Smart Contracts. *32nd USENIX Security Symposium (USENIX Security 2023)*, 1793–1810.

Jesse, N. (2022). "Cut Out the Middleman": Automating Business Processes with Blockchains and Smart Contracts. *IFAC-PapersOnLine*, *55*(39), 352–357. https://doi.org/10.1016/j.ifacol.2022.12.079

Jiménez, D. L. (2025). Commercial Transactions in the Digital Era: Navigating the Legal Complexities of Algorithmic Decision-Making. In *Transforming Corporate Social Responsibility and Business Ethics with AI* (pp. 139–174). https://doi.org/10.4018/979-8-3693-9894-4.ch005

Karapapas, C., Pittaras, I., Fotiou, N., & Polyzos, G. C. (2020). *Ransomware as a Service Using Smart Contracts and {IPFS}*. https://doi.org/10.1109/ICBC48266.2020.9169451

Khawaldeh, A. M., Al Masadeh, A. M., & Aldarawsheh, H. M. (2024). The Weaker Party in the Contractual Relationship. *Journal of Human Security*, *20*(1), 72–78. https://doi.org/10.12924/johs2024.20110

Kusber, T., Schwalm, S., Shamburger, K., & Korte, U. (2020). Criteria for Trustworthy Digital Transactions — Blockchain/DLT Between {eIDAS}, {GDPR}, Data and Evidence Preservation. *Lecture Notes in Informatics (LNI), Proceedings – Series of the Gesellschaft Für Informatik (GI)*, *P-305*, 49–60.

Lozada, N., & Talero, D. (2024). Electronic Enforcement in the Digital Era: Themis Without a Sword. *Uniform Law Review*, *29*(2), 204–220. https://doi.org/10.1093/ulr/unae030

Ndiaye, M., & Konate, P. K. (2021). Cryptocurrency Crime: Behaviors of Malicious Smart Contracts in Blockchain. *2021 International Symposium on Networks, Computers and Communications (ISNCC 2021)*. https://doi.org/10.1109/ISNCC52172.2021.9615702

Poncibò, C. (2021). The Digitalization of Contracts in International Trade and Finance: Comparative Law Perspectives on Smart Contracts. In *Digitalization and Firm Performance: Examining the Strategic Impact* (pp. 131–155). https://doi.org/10.1007/978-3-030-83360-2_6

Prabantarikso, R. M. (2024). Socio-Legal Review of Contracts: A Study of Social Embeddedness and Institutional Embeddedness in Contract Enforcement. *Mimbar Hukum*, *36*(2), 445–471. https://doi.org/10.22146/mh.v36i2.17201

Risal, A. (2024). Legal Protection for Debtors in Online Transactions: Evaluating Safeguards in E-Commerce. *Jurnal Hukum Bisnis Bonum Commune*, *7*(2), 176–187. https://doi.org/10.30996/jhbbc.v7i2.11656

Rizos, E. (2022). A Contract Law Approach for the Treatment of Smart Contracts' {Bugs}. *European Review of Private Law*, *30*(5), 775–802. https://doi.org/10.54648/erpl2022037

Schroeter, U. G. (2017). Anticipatory Breach, Change of Circumstances, and Third-Party Rights: A Civil Law Perspective. In *Chinese Contract Law: Civil and Common Law Perspectives* (pp. 323–350). https://doi.org/10.1017/9781316816912.014

Septiningsih, I., & Karimullah, S. S. (2024). Consumer Protection in the Digital Era: An Analysis of Consumer Protection in E-Commerce. *Nusantara: Journal of Law Studies*, *3*(2), 68–80. https://doi.org/10.5281/zenodo.17376951

Sharma, P., Jindal, R., & Borah, M. D. (2023). A Review of Smart Contract-Based Platforms, Applications, and Challenges. *Cluster Computing*, *26*(1), 395–421. https://doi.org/10.1007/s10586-021-03491-1

Shumyliak, L., Cibák, L., Ostapov, S., Salem, A.-B. M., & Skrypnyk, Y. (2023). Practical Implementation of Smart Contracts for Payment of Digital Goods. *CEUR Workshop Proceedings*, *3373*, 672–680.

Singh, J., Rani, S., & Kumar, P. (2024). Blockchain and Smart Contracts: Evolution, Challenges, and Future Directions. *2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS 2024)*. https://doi.org/10.1109/ICKECS61492.2024.10616652

Sinitsyn, S. A., Diakonova, M. O., & Chursina, T. I. (2022). Smart Contracts in the Digital Economy: Contractual Regulation and Dispute Resolution. In *Smart Innovation, Systems and Technologies* (Vol. 254, pp. 155–164). https://doi.org/10.1007/978-981-16-4621-8_13

Taeihagh, A. (2023). Addressing Policy Challenges of Disruptive Technologies. *Journal of Economic Policy Reform*, *26*(3), 239–249. https://doi.org/10.1080/17487870.2023.2238867

Upadhyay, K., Dantu, R., He, Y., Salau, A., & Badruddoja, S. (2021). Paradigm Shift from Paper Contracts to Smart Contracts. *Proceedings of the 2021 3rd IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA 2021)*, 261–268. https://doi.org/10.1109/TPSISA52974.2021.00029

van Eck, M. M. (2020). The Disruptive Force of Smart Contracts. In *Lecture Notes in Electrical Engineering* (Vol. 674, pp. 21–45). https://doi.org/10.1007/978-3-030-48230-5_2

Werbach, K., & Cornell, N. (2017). Contracts Ex Machina. *Duke Law Journal*, *67*(2), 313–382.

Wibye, J. V. (2025). Philosophical Methods in Contract Law. In *Research Methods for Contract Law and Scholarship* (pp. 90–114). https://doi.org/10.4337/9781035316472.00010

Yan, K., Zhang, J., Liu, X., Diao, W., & Guo, S. (2023). *Bad Apples: Understanding the Centralized Security Risks in Decentralized Ecosystems*. https://doi.org/10.1145/3543507.3583393

Yu, H., Deng, X., & Zhang, N. (2025). To What Extent Can Smart Contracts Replace Traditional Contracts in Construction Project? *Engineering, Construction and Architectural Management*, *32*(3), 1393–1410. https://doi.org/10.1108/ECAM-04-2023-0379

Zhang, L., Wang, Y., Li, F., Hu, Y., & Au, M. H. (2019). A Game-Theoretic Method Based on Q-Learning to Invalidate Criminal Smart Contracts. *Information Sciences*, *498*, 144–153. https://doi.org/10.1016/j.ins.2019.05.061