IRSHAD Uzbek Journal of Law and Digital Policy |
Volume: 3, Issue: 1
2025

Smart Contracts in the Civil Law System: Problems of Legal Qualification

Pulatov Temurbek Gayratjon ugli
Tashkent State University of Law

Abstract

This article examines the legal qualification of smart contracts within civil law jurisdictions, emphasizing the challenges posed by automated, code-based agreements in systems traditionally grounded in codified statutes and doctrinal principles. By exploring current scholarly debates, legislative approaches, and judicial interpretations, this study highlights the tension between the self-executing nature of smart contracts and the requirement for consent, formality, and interpretation under civil codes. Drawing on a qualitative analysis of doctrinal writings, statutory frameworks, and case-based discussions, the paper identifies core issues of enforceability, liability, and consumer protection. Results reveal the need for a more coherent integration of legal theory and technological design, underscoring the role of hybrid solutions that blend human interpretation with automated execution. The discussion situates these findings in the broader trajectory of contract law modernization, concluding with recommendations for policymakers and practitioners regarding risk mitigation, technological design improvements, and harmonized regulatory standards.

Keywords: Smart Sontracts, Civil Law, Enforceability, Liability, Consumer Protection, Blockchain

APA Citation:

Pulatov, T. (2025). Smart Contracts in the Civil Law System: Problems of Legal Qualification. *Uzbek Journal of Law and Digital Policy, 3*(1), 155–181. https://doi.org/10.59022/ujldp.298

I. Introduction

The emergence of blockchain technology has introduced novel contracting mechanisms, commonly referred to as “smart contracts,” which automate contractual performance through self-executing code (Savelyev, 2016). While the term “smart contract” suggests a seamless fusion of legal and computational features, this convergence poses fundamental questions regarding how established civil law principles accommodate or resist such innovation (Mik, 2017). In civil law jurisdictions, contract validity, formation, and enforcement are typically governed by codified statutes, many of which contain formal requirements that may not align neatly with automated code-based execution (Isolino, 2019). For instance, real estate transactions or notarial acts might require a written instrument or specific documentation protocols that are not readily replicated by software logic (Fernández Carballo-Calero, 2020).

Consequently, this potential mismatch between code-driven processes and codified formalities generates uncertainty over whether and how a “smart contract” truly qualifies as a legally valid agreement. Despite the technological sophistication, civil law systems demand alignment with essential principles such as free will, consent, and clarity of obligations, highlighting the tension between self-enforcing contractual clauses and interpretative legal doctrines. As a result, the need to reconcile these conflicting imperatives underpins the central problem that this study seeks to address. The disparity between coded automation and codified law underscores the urgency of examining how civil law can adapt to or accommodate such novel contractual forms.

The lack of a universally accepted definition of “smart contract” exacerbates this complexity, with some commentators emphasizing its purely technical dimensions and others framing it as a novel legal instrument (Werbach & Cornell, 2017). Raskin (2017) notes that even the term “contract” can be misleading, as not all blockchain-based scripts necessarily constitute legally binding agreements under civil law. Nonetheless, the possibility that self-executing code might bypass key procedural or substantive safeguards has compelled courts, lawmakers, and scholars to reassess classical notions of offer, acceptance, and performance (Fairfield, 2014). Furthermore, regulatory bodies, such as the European Central Bank, have begun exploring how distributed ledger technologies intersect with existing financial and consumer protection regimes (Pinna & Ruttenberg, 2016). This broader institutional interest demonstrates that the problem extends beyond scholarly discourse, implicating market stability, consumer welfare, and overarching legal certainty (Albrecht, Lobet, & Trampe, 2019).

As a result, the crux of the problem is not merely the theoretical question of whether code can instantiate a contractual relationship, but rather how the operational realities of self-executing terms mesh with normative demands in civil law contexts

(Reyes, 2017). Resolving these issues is essential for ensuring that civil law frameworks remain relevant, robust, and capable of handling a rapidly evolving digital economy. Hence, this study's problem statement centers on the strategic integration of smart contracts into civil law systems without undermining foundational legal principles.

By focusing specifically on the challenges of legal qualification, this research highlights the friction points that arise when mandatory provisions, formality requirements, and interpretative doctrines encounter automated performance (Troiano, 2018). The tension is particularly acute in consumer transactions, where statutory safeguards exist to protect weaker parties from overreaching or exploitive conduct (Antognini, 2019). In purely automated environments, it becomes unclear how cooling-off periods, cancellation rights, or other protective measures can be operationalized if contract execution is triggered unconditionally by software code (Noto La Diega & Sappa, 2018). Moreover, liability allocation—especially in cases of code malfunction or unforeseen events—presents another layer of complexity that civil law jurisdictions must address (Zetzsche et al., 2018).

Collectively, these pressing concerns highlight the overarching research imperative: to provide a thorough, structured analysis of how civil law traditions might accommodate or adapt to the proliferating use of smart contracts. Therefore, this paper advances the discussion by seeking to clarify the conditions under which a smart contract may be recognized as legally valid and enforceable within civil law frameworks (Mik, 2017). Through a doctrinal and comparative lens, it aims to illuminate the evolving nexus between code, law, and regulatory policy. In doing so, this research sets the stage for broader conversations about the modernization of civil law in an era of ubiquitous digital innovation.

Over the past decade, scholarly interest in smart contracts has proliferated, leading to diverse conceptual, doctrinal, and empirical inquiries (Mik, 2017; Savelyev, 2016). Early discussions, such as Surden's notion of "computable contracts," contemplated how contractual terms could be structured for machine processing, foreshadowing the rise of blockchain-facilitated agreements. Building on this foundation, Werbach and Cornell (2017) examined "contracts ex machina," highlighting the inherent tension between automated performance and judicial interpretative practices that are deeply embedded in legal traditions, including civil law. Meanwhile, scholars like Raskin (2017) and Reyes (2017) have investigated the legitimacy and legality of smart contracts, arguing that self-execution may disrupt conventional contract doctrines, particularly those requiring evidence of a mutual intention to be bound.

Civil law-oriented research has notably emerged from jurisdictions like Italy (Filippi, 2020), Spain (Fernández Carballo-Calero, 2020), and France (Friedman & Tazi, 2019), each offering insights into how coded agreements can conform—or fail to conform—to mandatory form requirements, public policy constraints, and consumer

protection statutes. Collectively, this body of literature underscores the growing scholarly consensus that while smart contracts offer enhanced efficiency and transparency, their implementation must account for the unique structural features of civil law systems. In particular, the codified nature of civil law demands explicit statutory or doctrinal recognition if these technologies are to gain widespread acceptance. Hence, the literature sets the stage for identifying specific doctrinal conflicts and exploring potential resolutions.

Despite the surge in academic engagement, the literature reveals a pronounced gap in empirical analyses that examine actual case law or dispute resolutions concerning smart contracts in civil law jurisdictions (Fernández Carballo-Calero, 2020). Many studies remain theoretical, postulating how existing doctrines might apply to automated performance or speculating on the interpretations courts could adopt (Isolino, 2019). This theoretical orientation reflects the nascent stage of practical smart contract deployments, which remain limited in scope or confined to pilot projects. Nevertheless, the conceptual frameworks developed by scholars like Borges (2019) and Clack, Bakshi, and Braine (2016) have provided important foundations for understanding the ways in which distributed ledger technology could intersect with formal legal requirements, liability doctrines, and enforcement mechanisms.

Additionally, cross-jurisdictional studies, such as those by Noto La Diega and Sappa (2018), highlight common trends in EU civil law and underscore the need for a harmonized approach if the single market is to foster consistent smart contract regulation. The lack of direct judicial precedents remains a key challenge, as courts in many civil law countries have yet to issue definitive rulings that could clarify interpretative controversies (Savelyev, 2016). Consequently, scholars must rely heavily on analogical reasoning, extrapolating from existing doctrines to predict how a court might treat software code as a vehicle of contractual obligation. This reliance on theoretical constructs continues to shape the current literature, indicating a collective call for deeper empirical research and legal reform initiatives.

In addition to these theoretical discussions, regulatory bodies and international organizations have begun issuing reports and guidelines that shape the scholarly narrative (Pinna & Ruttenberg, 2016). For instance, the European Blockchain Partnership and various national data protection agencies have produced guidance that indirectly influences how smart contracts must manage or protect personal data, especially under the General Data Protection Regulation (GDPR) (Zanfir-Fortuna & Husovec, 2019). Although such documents do not always specifically address civil law doctrines, they establish broader compliance parameters, thereby influencing the direction of scholarly debates around liability, data ownership, and privacy (Sillaber & Waltl, 2017). On a more general level, popular works like *Blockchain Revolution* by Tapscott and Tapscott (2016) have catalyzed public discourse around blockchain and smart contracts, stirring both optimism and concern about their disruptive potential.

This dissemination of information to non-expert audiences has also spurred

interest among policymakers, leading to increased demands for clarifying the legal status of self-executing agreements (Raskin, 2017). Summarizing these developments, the literature as a whole evidences a transitional phase in which academic scholarship, regulatory guidance, and nascent real-world deployments converge to demand a coherent, civil law-centric framework for assessing smart contracts. The body of existing work thus underscores the intricate balance between preserving established civil law principles and embracing innovations that promise efficiency gains and reduced transaction costs (Borges, 2019). This study aims to build upon that foundation by offering a structured approach to reconciling doctrinal imperatives with the distinctive features of smart contracts.

Despite the extensive theoretical discourse surrounding smart contracts, a clear research gap emerges in the realm of civil law-specific analysis, particularly regarding the intersection of mandatory norms, formality requirements, and consumer protection measures (Isolino, 2019). While significant contributions have been made by researchers examining common law frameworks, the codified nature of civil law demands a distinct analytical lens that accounts for legislatively enshrined principles (Savelyev, 2016). The existing literature often glosses over this distinction, leaving critical questions about how parties can prove consent, how notarial acts might be integrated, and how unconditional code execution can respect statutory cooling-off periods (Fernández Carballo-Calero, 2020).

This lacuna becomes more pronounced when considering high-stakes domains, such as real estate or secured transactions, where civil law typically imposes stringent documentation and authentication requirements (Filippi, 2020). Without addressing these areas, the research remains incomplete, providing only a partial roadmap for integrating smart contracts into daily commercial and consumer activities. Hence, the need to explore these intricacies within a civil law context underpins the motivation for the present study, which aims to fill the gap by analyzing both doctrinal perspectives and nascent practical developments.

Another aspect of the research gap pertains to the question of liability distribution, particularly in decentralized environments where no single entity assumes full responsibility for drafting, verifying, or maintaining the code (Zetzsche et al., 2018). Civil law doctrines on fault and negligence typically require identifiable parties who can be held accountable if contractual performance breaches statutory duties or harms another party (Troiano, 2018). By contrast, smart contracts deployed on public blockchains often involve multiple actors, including developers, platform providers, and end-users, complicating the apportionment of liability (Noto La Diega & Sappa, 2018).

The existing scholarship has acknowledged this complexity but rarely delves into the doctrinal intricacies of civil liability regimes or the ways in which courts might respond to a distributed network of contributors (Borges, 2019). This omission leaves a significant gap in understanding how civil law principles—especially those

dealing with cause-and-effect analyses and proximate causation—can be applied to code-based contract failures. The present study addresses this gap by examining doctrinal positions in various civil law jurisdictions and exploring emerging proposals for reconciling automated code execution with established liability norms.

Moreover, despite sporadic legislative proposals and regulatory experiments, there is a distinct shortage of systematic, cross-jurisdictional analysis of how civil law systems might coordinate their responses to smart contracts (Schouppe, 2019). (2) A handful of studies have compared EU and U.S. approaches, but few investigate the nuanced differences that can exist even among European civil law nations, each characterized by unique codifications and legal traditions (Raskin, 2017). This fragmentation of regulatory perspectives further accentuates the need for a unifying framework capable of guiding lawmakers, courts, and practitioners across diverse civil law contexts (Friedman & Tazi, 2019).

By synthesizing doctrinal insights from multiple jurisdictions, the present study offers a macro-level overview of the patterns and divergences shaping the legal qualification of smart contracts. This comparative lens is essential for policymakers seeking to harmonize legislation, particularly given the transnational nature of digital transactions (Pinna & Ruttenberg, 2016). Consequently, addressing the identified gap demands a nuanced exploration of how civil law systems can converge or diverge in regulating a technology that transcends geographical and jurisdictional boundaries.

The overarching aim of this article is to develop a comprehensive understanding of the legal qualification and enforceability of smart contracts in civil law jurisdictions, with a focus on doctrinal alignment and statutory adaptation (Savelyev, 2016). In particular, the study seeks to elucidate how foundational principles such as consent, form requirements, and consumer protection might be preserved or reinterpreted in the face of automated execution (Mik, 2017). By identifying key points of friction between code-based and statute-based contractual frameworks, the research aims to provide actionable insights that legislators, courts, and practitioners can use to navigate this evolving terrain (Isolino, 2019). Ultimately, the study aspires to move beyond theoretical speculation, proposing pathways for practical integration of smart contracts into civil law systems without eroding crucial legal safeguards (Troiano, 2018).

Through a comparative doctrinal lens, the analysis will examine multiple jurisdictions, highlighting instances where national laws or judicial interpretations have begun to acknowledge or incorporate blockchain-driven agreements (Fernández Carballo-Calero, 2020). This approach ensures that the objectives remain context-specific, avoiding one-size-fits-all solutions and underlining the diversity of civil law traditions. In so doing, the study aspires to fill existing gaps while stimulating future research on the intersection of civil law doctrine, technological innovation, and consumer welfare (Borges, 2019). Consequently, the aim and objective converge on offering a structured framework for reconciling innovation with established legal

fundamentals in civil law.

A second objective involves clarifying liability mechanisms, focusing on whether and how existing civil law doctrines can allocate responsibility when smart contracts malfunction or produce unintended outcomes (Zetzsche et al., 2018). This concern is especially salient given the decentralized nature of many blockchain platforms, where the identification of a single responsible party may be infeasible (Noto La Diega & Sappa, 2018). By evaluating scholarly proposals and emerging regulatory guidelines, the study aims to identify workable approaches that preserve fairness and predictability in liability disputes (Albrecht et al., 2019). Moreover, the objective extends to exploring whether recognized entities—such as developers, notaries, or "oracles" providing external data—might bear legal obligations under civil law frameworks (Troiano, 2018).

This clarificatory endeavor serves not only academics but also practitioners who must advise clients on risk mitigation strategies, indemnification clauses, and code audits (Karnitschnig & Pichonnaz, 2020). Through these analyses, the article seeks to contribute concrete proposals for bridging the conceptual gulf between self-executing performance and accountability principles enshrined in civil law (Reyes, 2017). As a result, liability emerges as a central point of inquiry, linked intimately with the overarching aim of harmonizing technological potential with codified legal doctrine. Addressing this objective ensures that the conversation extends beyond mere enforceability, encompassing the equitable distribution of risks and responsibilities in digitally mediated contracting.

Beyond enforceability and liability, the study's objectives include promoting legal clarity and fostering consumer trust in digital transactions (Antognini, 2019). In many civil law jurisdictions, consumer protection statutes form an integral part of contractual law, demanding transparency, fairness, and opportunities for redress (Fernández Carballo-Calero, 2020). Recognizing that blockchain technologies can obscure contractual terms or automate them in ways that consumers may not fully comprehend, the study aims to delineate how regulators and courts can safeguard user interests (Raskin, 2017). This objective extends to exploring the feasibility of mandatory disclosures, user-friendly interfaces, or standardized protocols that ensure consumer consent is both informed and voluntary (Mik, 2017).

Additionally, the objective touches on potential legislative reforms, such as amendments to civil codes or the introduction of specialized statutes that address data privacy, disclaimers of liability, and mandatory conflict-resolution pathways in automated settings (Zanfir-Fortuna & Husovec, 2019). By aligning technological functionality with statutory mandates, the study's objectives underscore a commitment to consumer welfare as a core tenet of civil law. In sum, achieving these objectives contributes to a robust framework where smart contracts can thrive without undermining the social and protective dimensions that have historically guided civil law systems (Borges, 2019). Consequently, the research aims to facilitate a balanced

discourse in which innovation proceeds hand in hand with the preservation of foundational legal values.

Stemming from the above aim and objectives, the central research question is: *How can civil law jurisdictions reconcile the automated, code-driven features of smart contracts with the doctrinal requirements of consent, formality, and liability, while preserving essential consumer protection and interpretative safeguards?*

This question encapsulates the study's pursuit of both doctrinal alignment and practical feasibility, bridging the gap between academic theorizing and real-world legal processes (Savelyev, 2016). The question underscores the pivotal issue of identifying whether existing civil law principles are flexible enough to accommodate self-executing clauses or whether new legislation or doctrinal reinterpretations are indispensable (Isolino, 2019). By framing the inquiry in this way, the research acknowledges that smart contracts, while technologically advanced, cannot be analyzed in isolation from the socio-legal contexts in which they operate (Raskin, 2017).

Thus, the research question highlights the need for a multidimensional perspective that accounts for consumer rights, risk allocation, and the interpretative role of courts in bridging the gap between code and law (Werbach & Cornell, 2017). Addressing this question is essential for clarifying how automated agreements can be validly formed, enforced, and challenged in disputes, given the distinctive architecture of civil law. In doing so, it guides the entire study's structure, from the literature review to the proposed doctrinal frameworks. Ultimately, the research question serves as a unifying thread, tying together legal theory, policy considerations, and practical concerns.

Sub-questions arise from this overarching inquiry, beginning with whether smart contracts can fulfill formal requirements that traditionally necessitate written documents or notarized authentication (Fernández Carballo-Calero, 2020). Another sub-question involves determining how civil law principles governing consent—particularly the idea of "meeting of the minds"—map onto automated processes triggered by predefined if-then statements (Mik, 2017). Additionally, issues of liability distribution prompt further sub-questions: Who is responsible when code fails to execute properly, and how might courts assign fault or negligence when multiple contributors are involved (Zetzsche et al., 2018)? These sub-questions collectively deepen the inquiry, ensuring that the research does not remain at a generic level but instead probes specific doctrinal and practical complications (Isolino, 2019).

Such granularity is crucial for generating nuanced findings, particularly in areas where consumer protection and mandatory rules intersect with self-executing performance (Antognini, 2019). As a result, the sub-questions become integral to fully answering the primary research question, guiding the collection of data, the doctrinal analysis, and the interpretation of findings (Clack et al., 2016). By structuring the study around these focused queries, the research maintains a clear trajectory that

culminates in evidence-based conclusions. Hence, the questions together form a coherent framework for investigating the ramifications of automated contracting in civil law systems.

The research question and its sub-questions thus place a premium on interdisciplinary insights, recognizing that coding processes, economic rationales, and legal doctrines converge in smart contracts (Reyes, 2017). Civil law is not monolithic, and variations in legal culture, statutory design, and interpretative traditions demand a flexible analytical approach (Friedman & Tazi, 2019). Nonetheless, the unifying thread remains consistent: to determine how self-enforcing code can operate within a legal environment that places considerable weight on formalities, protective measures, and interpretative discretion (Werbach & Cornell, 2017). The research question thereby encourages a comparative lens, inviting the study to draw on examples from multiple civil law jurisdictions to demonstrate how they either converge or diverge in accommodating these innovations (Schouppe, 2019).

In turn, these comparative insights inform broader conclusions about whether a harmonized regulatory approach is possible—or even desirable—across civil law systems (Noto La Diega & Sappa, 2018). By systematically addressing the research question, the study aspires to offer both theoretical clarity and practical pathways for implementation, ensuring that civil law traditions are neither rendered obsolete nor unduly rigid in the face of technological progress (Savelyev, 2016). This structured inquiry culminates in a framework capable of guiding lawmakers, courts, and practitioners, weaving together doctrinal fidelity with technological potential (Isolino, 2019). Hence, the question serves as a strategic focal point, setting the stage for the subsequent methodological design, data collection, and analytical procedures outlined in this article.

The significance of this study lies in its potential to inform both theoretical discourse and policy-making on how civil law systems can adapt to the advent of smart contracts while preserving core doctrinal principles (Borges, 2019). Given the economic and social importance of contractual transactions, any legal uncertainty surrounding the enforceability or validity of code-based agreements could stifle innovation, hinder market efficiency, and potentially harm consumer interests (Antognini, 2019). By comprehensively analyzing doctrinal, statutory, and jurisprudential perspectives, the study offers a structured reference for lawmakers and legal practitioners seeking to reconcile new technologies with established legal norms (Mik, 2017). Moreover, it serves as a catalyst for further scholarly engagement by highlighting unresolved issues, thereby guiding future empirical research, pilot studies, and theoretical debates (Fernández Carballo-Calero, 2020).

At a broader level, the study underscores how civil law's codified nature can function as both an obstacle and a facilitator of technological adoption, depending on the adaptability of statutory mandates and interpretative flexibility (Clack et al., 2016). Consequently, the findings may significantly contribute to shaping a pragmatic yet

principled pathway for incorporating smart contracts into mainstream commercial and consumer settings, thus enhancing legal certainty and fostering trust in digital economies (Savelyev, 2016). As such, this research stands at the nexus of innovation and tradition, offering insights into the delicate balance required to integrate emerging technologies into longstanding legal frameworks. The significance thus extends beyond academic interest, impacting real-world contractual practices and regulatory strategies in multiple jurisdictions.

Another aspect of the study's significance involves addressing the broader question of legal harmonization across civil law systems, particularly within the European Union (Schouppe, 2019). While member states share certain foundational principles, their contract laws often differ in nuances that could impede cross-border usage of smart contracts (Friedman & Tazi, 2019). A well-founded doctrinal framework, grounded in this study's comparative insights, could inform EU-wide initiatives or directives that aim to standardize or at least coordinate legislative responses to automated contracting (Gatt, 2019). This harmonization would be particularly valuable for large-scale commercial applications, where blockchain-driven systems might transcend national boundaries, necessitating interoperability in both technical and legal senses (Pinna & Ruttenberg, 2016).

By highlighting these cross-jurisdictional complexities, the study underscores the importance of coordinated policy-making to prevent regulatory fragmentation and ensure a stable environment for blockchain-based innovation (Zanfir-Fortuna & Husovec, 2019). Consequently, the study's significance lies not only in deepening our understanding of civil law doctrines but also in shaping multilateral dialogues on how to approach automated contracting at a supra-national level (Werbach & Cornell, 2017). (7) This heightened awareness could facilitate new forms of legal cooperation, catalyzing policy alignment that benefits both businesses and consumers. (8) In this way, the study's findings have the potential to resonate well beyond the confines of individual jurisdictions.

Finally, by focusing on liability and consumer protection, the study holds significance for safeguarding individual users, who may otherwise be vulnerable in automated contractual environments (Troiano, 2018). The rapid execution triggered by software code can sometimes overshadow the user's ability to comprehend, contest, or negotiate contract terms, raising concerns about procedural and substantive fairness (Raskin, 2017). This study's attention to civil law doctrines of interpretation, good faith, and mandatory consumer rights is thus critical for ensuring that technology does not erode essential legal protections (Antognini, 2019). Additionally, clarifying how liability is distributed among developers, platform operators, and contractual parties addresses a core concern in decentralized systems, where identifying the "culpable party" is often more complex (Zetzsche et al., 2018).

By mapping existing doctrines to potential allocation scenarios, the study seeks to advance consumer confidence in automated transactions, thereby catalyzing broader

acceptance and usage of blockchain-based contracting (Albrecht et al., 2019). The significance thus transcends purely doctrinal considerations, touching upon the ethical and practical dimensions of law in the digital age. Overall, this multifaceted relevance—encompassing scholarly discourse, regulatory harmonization, and consumer welfare—positions the study as a vital reference for stakeholders grappling with the evolving intersection of technology and civil law (Mik, 2017). Ultimately, the research aims to ensure that innovation and legal tradition coexist in a manner that upholds justice, transparency, and efficiency.

II. Methodology

This study adopts a qualitative, doctrinal research design tailored to explore the legal qualification of smart contracts within civil law systems (Savelyev, 2016). Doctrinal research is particularly suited for dissecting codified statutes, legal commentaries, and jurisprudential interpretations, enabling a comprehensive examination of how law conceptualizes and regulates code-based agreements (Mik, 2017). The primary goal is to synthesize scholarly viewpoints, legislative texts, and emerging judicial precedents into a coherent framework that elucidates doctrinal adaptability or resistance to automated contracting (Borges, 2019). Unlike empirical legal studies that rely on quantitative data or case outcomes, doctrinal research provides a structured approach to analyzing the normative content of legal sources, identifying principles, and drawing out logical inferences (Werbach & Cornell, 2017).

This design aligns with the study's aim to clarify conceptual and doctrinal issues, focusing on the alignment of smart contracts with civil law's codified requirements for valid agreement formation and execution (Fernández Carballo-Calero, 2020). Additionally, the qualitative dimension allows for a nuanced exploration of interpretative debates, which are critical in civil law contexts where legislative provisions often leave room for jurisprudential reasoning (Raskin, 2017). Through this lens, the study prioritizes the theoretical and normative richness of legal texts, channeling these insights into an in-depth analysis of existing and potential legal frameworks. Consequently, the doctrinal research design is well-suited to address the central research question by systematically examining how civil law traditions can accommodate or adapt to smart contract technologies.

Within this doctrinal framework, the study employs a comparative approach, drawing on examples from multiple civil law jurisdictions—such as France, Italy, Spain, and Switzerland—to capture both shared principles and national idiosyncrasies (Filippi, 2020; Karnitschnig & Pichonnaz, 2020). This comparative dimension is essential because, while civil law systems share certain foundational concepts (e.g., the importance of codification, general contract law principles), substantive and procedural variations can yield different outcomes when applied to smart contracts (Schouppe, 2019). Therefore, the study design integrates cross-jurisdictional insights to identify whether smart contracts face similar doctrinal barriers or if some

jurisdictions have successfully crafted solutions that could serve as models (Isolino, 2019).

By analyzing a spectrum of national approaches, the research highlights patterns such as the acceptance of digital signatures as a proxy for written form, or the statutory codification of blockchain references within specific legislative acts (Gatt, 2019). This methodological choice ensures that findings are not overly dependent on one country's legal system, thereby increasing the relevance and applicability of the conclusions across a broader civil law landscape (Fernández Carballo-Calero, 2020). It also illuminates whether a harmonized EU-wide framework is feasible or whether cultural and legal heterogeneity might necessitate multiple parallel regulatory strategies (Zanfir-Fortuna & Husovec, 2019). Through comparative doctrinal analysis, this study can pinpoint specific points of divergence or convergence, offering a rich panorama of how civil law systems grapple with the phenomenon of self-executing contracts. In this way, the study design aspires to balance depth with breadth, ensuring that nuanced doctrinal interpretation aligns with a macro-level view of regional legal developments.

In addition to focusing on codified laws and legal scholarship, the study design incorporates an examination of regulatory documents, policy statements, and academic working papers, which often represent the cutting edge of scholarly discourse on blockchain and smart contracts (Clack et al., 2016; Pinna & Ruttenberg, 2016).By including these non-traditional sources, the design acknowledges that doctrinal law rarely evolves in a vacuum and is frequently shaped by policy discussions and technical white papers, particularly in rapidly changing domains like blockchain (Buterin, 2013). This expanded data set enables a more holistic view, capturing both the de jure and de facto realities of how smart contracts are discussed, perceived, and implemented (Tapscott & Tapscott, 2016). The qualitative analysis includes thematic coding of these sources to identify recurring motifs, such as enforceability challenges, liability allocation, consumer protection, and mandatory form requirements (Raskin, 2017).

By systematically organizing this information, the study is better positioned to compare the theoretical ideals of civil law with the practical constraints of code-based execution (Werbach & Cornell, 2017). Through iterative analysis, emerging patterns or contradictions can be cross-validated against leading doctrinal commentaries and any reported cases, ensuring that findings reflect both the normative aspirations of legal texts and the pragmatic considerations of technological design (Sillaber & Waltl, 2017). Ultimately, this multifaceted study design offers a robust scaffold for mapping the legal challenges associated with smart contracts in civil law contexts, bridging doctrinal rigour with contemporary policy discussions. The result is a methodological framework attuned to the intricacies of code-based contracting, providing clarity on points of overlap or tension between technological innovation and codified legal norms.

The sample for this study encompasses a diverse array of legal and scholarly materials, selected through a systematic review process aimed at capturing both foundational and cutting-edge perspectives on smart contracts in civil law (Mik, 2017). Primary legal sources include national civil codes, relevant statutes (e.g., consumer protection laws), and any published judicial opinions or administrative rulings that directly address—or incidentally comment on—smart contracts (Fernández Carballo-Calero, 2020). Secondary sources consist of peer-reviewed journal articles, law review essays, academic working papers, and authoritative treatises that provide doctrinal analyses, theoretical frameworks, or comparative insights (Savelyev, 2016).

Specific emphasis is placed on works published between 2012 and 2022, reflecting the period in which blockchain technology and smart contracts rose to prominence (Clack et al., 2016). This decade-long window ensures that the data set encapsulates the early conceptual discussions, the subsequent empirical or pilot experiences, and the emerging legislative or judicial responses to self-executing agreements (Werbach & Cornell, 2017). Additionally, the selection includes regulatory papers and industry reports from institutions such as the European Central Bank, capturing policy-level discourse on distributed ledger technologies (Pinna & Ruttenberg, 2016). By curating such a broad yet targeted sample, the research ensures a well-rounded view of how civil law systems conceive of and engage with smart contracts. This robust sample forms the foundation for the doctrinal and comparative analysis that follows.

Inclusion criteria required that each source explicitly discuss or implicate the role of smart contracts in civil law contexts, addressing issues like enforceability, consumer protection, or liability (Isolino, 2019). Studies focusing exclusively on common law jurisdictions were excluded, except where they offered clear comparative insights relevant to civil law, ensuring that the sample remained consistent with the study's core focus (Raskin, 2017). The review process also prioritized sources that offered empirical or case-based evidence, although such materials remain relatively scarce given the novelty of the technology (Troiano, 2018). To capture the most influential voices, high-impact academic journals and conferences—such as those dedicated to blockchain, fintech, or European private law—were systematically searched for relevant publications (Albrecht et al., 2019).

Additionally, references in seminal articles served as a snowballing technique to uncover further key texts, particularly those published in specialized law journals or edited academic volumes (Noto La Diega & Sappa, 2018). This multi-pronged approach ensured the comprehensiveness of the sample, capturing not only mainstream doctrinal perspectives but also niche or emerging scholarly arguments (Borges, 2019). By adhering to these inclusion and exclusion parameters, the data set offers a balanced representation of prominent theories, legal stances, and policy discussions pertaining to smart contracts in civil law. Consequently, the sample aligns

with the study's aim to dissect doctrinal nuances while reflecting the breadth of contemporary discourse.

After an initial compilation of potential sources, each document was reviewed for relevance, clarity, and depth of analysis regarding smart contracts and civil law doctrines (Fernández Carballo-Calero, 2020). Those that provided merely cursory mentions of blockchain or discussed unrelated technological applications were excluded to maintain a focused exploration of contract-specific issues (Savelyev, 2016). Materials that underwent peer review or came from reputable academic presses were prioritized, ensuring quality and credibility in the final selection (Mik, 2017). In total, the curated sample spans legislative texts from multiple jurisdictions, approximately 40 peer-reviewed articles or authoritative working papers, and a selection of policy documents that address or inform civil law approaches to automated contracting (Pinna & Ruttenberg, 2016; Zetzsche et al., 2018).

This iterative selection procedure culminated in a corpus that adequately represents the state of knowledge on smart contracts in civil law, capturing both established viewpoints and emergent discussions (Werbach & Cornell, 2017). Moreover, the final data set provides enough diversity to illuminate cross-jurisdictional themes and highlight areas where consensus or divergence is most pronounced (Friedman & Tazi, 2019). As such, the sample stands as a robust evidentiary base for subsequent doctrinal interpretation, comparative assessment, and legal synthesis (Isolino, 2019). Armed with this well-defined corpus, the study proceeds to the data collection and analysis methods that operationalize the comparative doctrinal approach.

Data collection in this doctrinal study involved systematically cataloging the relevant statutory provisions, case law excerpts, and scholarly arguments within a structured matrix, enabling thematic comparison across jurisdictions and topics (Mik, 2017). Each source was initially summarized, noting key themes such as enforceability, liability, form requirements, and consumer protection, followed by a closer examination of how these themes intersect with civil law principles (Savelyev, 2016). The process was facilitated by digital reference management tools, allowing for efficient cross-referencing and retrieval of sources, particularly when linking doctrinal arguments to specific statutory provisions or judicial comments (Troiano, 2018). To ensure consistency, a coding scheme was developed: documents were flagged for issues like "formality compliance," "interpretative tensions," "blockchain architecture," "consumer safeguards," and "liability allocation" (Isolino, 2019).

Coding enabled the identification of patterns and divergences, helping to reveal how certain jurisdictions might be more flexible about smart contract recognition or how specific scholars propose bridging code-based automation with classical contract doctrines (Raskin, 2017). By employing this systematic approach, the study avoided anecdotal or selective reliance on high-profile sources, instead basing conclusions on aggregated thematic evidence (Clack et al., 2016). This methodological rigor

strengthens the validity of subsequent findings, as each interpretative leap is grounded in a thorough review of multiple, thematically consistent sources (Werbach & Cornell, 2017). Overall, the structured data collection phase laid the groundwork for a robust analysis, ensuring that doctrinal inferences emerged from a carefully curated and meticulously indexed body of literature.

In parallel with coding textual sources, the study also tracked any references to actual or proposed legislative measures dealing specifically with smart contracts, such as pilot regulations, guidelines, or interpretative circulars issued by legal authorities (Gatt, 2019). This approach captured not only scholarly debate but also emerging real-world initiatives that could shape or clarify the legal status of automated agreements (Friedman & Tazi, 2019). For instance, certain jurisdictions have begun experimenting with "sandbox" environments for fintech solutions, potentially offering insights into how lawmakers might facilitate or restrict smart contract applications (Albrecht et al., 2019). By documenting these efforts, the study extends beyond purely academic discourse, reflecting the interplay between theoretical legal conceptions and the pragmatic steps taken by regulators or industry consortia (Pinna & Ruttenberg, 2016).

Where available, interviews or official statements from public consultations were also noted, although they were used mainly as supplementary data to confirm or refute scholarly assumptions (Zetzsche et al., 2018). This inclusive data collection strategy allows the study to provide a multi-faceted perspective, balancing doctrinal rigor with awareness of evolving legislative and industry practices (Fernández Carballo-Calero, 2020). Consequently, the resultant data set not only informs the study's doctrinal analysis but also anchors its discussion in the institutional realities of how smart contracts might be implemented or regulated (Mik, 2017). This dual-track approach ensures that the research remains cognizant of both theoretical ideals and on-the-ground developments in civil law contexts.

Finally, the data collection process concluded with a quality check, revisiting sources to ensure coherence and eliminating duplicates or tangential materials that did not substantially address the intersection of smart contracts and civil law (Isolino, 2019). Where discrepancies arose—for instance, conflicting interpretations about whether code could fulfill written requirements—priority was given to authoritative legal texts, peer-reviewed articles, or jurisprudential statements (Werbach & Cornell, 2017). The resultant data pool was then subjected to an iterative reading process, during which the coding scheme was refined to capture any overlooked nuances, such as the role of "oracle" services or multi-jurisdictional contracting scenarios (Borges, 2019). Feedback loops within this method allowed the study to remain agile, incorporating emerging commentary or newly published materials identified during the final stages of research (Schouppe, 2019).

By rigorously cross-verifying different types of evidence, the study minimized the risk of relying on isolated or outdated perspectives, thereby bolstering the

reliability of its doctrinal synthesis (Raskin, 2017). This meticulous approach ensures that the data collection methods align tightly with the research question, effectively capturing the multifarious ways civil law systems grapple with the legal qualification of smart contracts (Savelyev, 2016). Hence, the study emerges with a well-curated, thematically coded set of documents, primed for the analytical phase that follows in the subsequent sections. Taken together, the data collection methods constitute a structured, systematic pathway for assembling the diverse materials required for a comprehensive exploration of this technologically and legally intricate topic.

The analytical framework guiding this study centers on key civil law doctrines—formation, consent, formality, liability, and consumer protection—and how they intersect with the code-driven nature of smart contracts (Mik, 2017). For each doctrine, the framework examines whether and how self-executing features challenge or conform to statutory provisions, judicial interpretations, and scholarly commentaries (Isolino, 2019). Drawing inspiration from comparative law methodologies, the analysis identifies cross-jurisdictional commonalities, such as the recognition of electronic signatures, as well as divergences, such as mandatory notarization in certain jurisdictions (Fernández Carballo-Calero, 2020). This doctrinal lens is complemented by insights from policy analyses, capturing the influence of emerging regulations or sandbox programs designed to facilitate blockchain-based applications (Gatt, 2019).

Consequently, the analytical framework bridges traditional legal categories—like contractual defects, public policy limits, and obligations to act in good faith—with the technological specificities of automated code execution (Werbach & Cornell, 2017). Through this structured approach, the study delves into each doctrinal aspect with clarity, correlating code-based attributes like immutability and determinism with civil law concepts of interpretative flexibility and equitable remedies (Savelyev, 2016). By systematically aligning the features of smart contracts with legal categories, the framework facilitates a clear presentation of both conflict points and potential resolutions. Ultimately, the outcome is a cohesive, doctrine-by-doctrine mapping of where smart contracts may integrate smoothly and where reforms or interpretive innovations are most urgently needed.

A second layer of the framework involves liability allocation, particularly crucial in scenarios where automated performance results in unforeseen harm or breach of mandatory obligations (Troiano, 2018). Recognizing that civil law commonly imposes liability based on fault or negligence, the analysis investigates how code-related defects or failures might be attributed to different actors, including developers, deployers, or third-party oracle services (Noto La Diega & Sappa, 2018). The framework assesses whether existing liability doctrines, such as strict liability for defective products or professional negligence standards, could be analogously applied to code-based services (Zetzsche et al., 2018). This approach ensures that liability is not merely seen as a technical glitch but as a multi-faceted legal question implicating

duty of care, foreseeability, and risk assessment in automated transactions (Borges, 2019).

By synthesizing doctrinal insights with real-world practices—like platform audits or developer disclaimers—the framework highlights the interplay between classical legal principles and innovative contract architectures (Werbach & Cornell, 2017). Additionally, it investigates whether the decentralized character of certain blockchain networks complicates the identification of a singular accountable party, thus challenging established civil law paradigms that typically require a recognizable legal entity (Clack et al., 2016). This methodical scrutiny of liability doctrines underlines the complexities that smart contracts introduce, providing a structured basis for evaluating potential solutions or law reform proposals. Hence, the framework's dual focus on enforceability and liability ensures a holistic investigation of how civil law can accommodate self-executing contracts.

Finally, the analytical framework incorporates consumer protection as a distinct pillar, given the substantial role that mandatory consumer norms play in civil law systems (Antognini, 2019). The analysis gauges how these protections, including cooling-off periods, disclosure requirements, and prohibitions on unfair contract terms, might be upheld if contract execution is automated and irreversible once triggered by code (Fernández Carballo-Calero, 2020). By examining consumer law doctrines and legislative instruments, the framework highlights potential contradictions between the protective ethos of civil law and the automated finality of blockchain transactions (Raskin, 2017). This perspective enables an evaluation of whether existing remedies—such as contract rescission, damages, or injunctive relief—remain viable if key performance steps occur instantly and immutably (Mik, 2017).

Aligning these considerations with the liability layer, the framework explores whether consumer-facing platforms might bear additional obligations to offer user-friendly interfaces, dispute resolution options, or partial reversibility to comply with statutory mandates (Troiano, 2018). The goal is not only to identify points of tension but also to outline how hybrid approaches—where code is supplemented by legal controls—could reconcile the efficiency benefits of smart contracts with the protective policies central to civil law (Noto La Diega & Sappa, 2018). Through this integrative lens, the framework stands as a comprehensive model for assessing the full spectrum of contractual, liability, and consumer-related issues arising from blockchain-based agreements (Werbach & Cornell, 2017). In doing so, it sets the stage for the results and discussion sections, where concrete findings are presented and interpreted in light of the doctrinal and comparative analysis undertaken.

III. Results

Analysis of the coded materials reveals a gradual but discernible trend among civil law jurisdictions toward recognizing the potential validity of smart contracts,

provided they satisfy fundamental contractual requirements such as offer, acceptance, object, and cause (Savelyev, 2016). While no unified legislative framework exists, several jurisdictions have enacted or proposed amendments that acknowledge electronic or digital signatures as functional equivalents to traditional written forms, thus potentially enabling blockchain-based authentication (Filippi, 2020). In Switzerland, for example, legal provisions are interpreted flexibly, allowing "electronic signatures" to fulfill certain formality criteria, fostering an environment where self-executing contracts can gain legal traction (Karnitschnig & Pichonnaz, 2020).

By contrast, Spain's approach, though open to digital transactions, still emphasizes documentary formalities in specific domains—like real estate contracts—creating potential hurdles for purely code-driven agreements (Fernández Carballo-Calero, 2020). Scholarly commentary indicates that most civil law systems are adopting a technology-neutral stance, implying that nothing in principle precludes automated contractual clauses from being recognized as valid if they align with statutory mandates (Mik, 2017). However, critics note that automated code, lacking interpretative flexibility, may complicate the assessment of the parties' true intentions, a cornerstone of civil law contract theory (Werbach & Cornell, 2017).

Nevertheless, the results demonstrate that the recognition of smart contracts' legal validity does not automatically equate to their enforceability in all situations, particularly where public policy or mandatory consumer protections come into play (Antognini, 2019). Several authors emphasize that even if a smart contract meets basic formation requirements, its automated execution could violate statutory norms if it disregards cooling-off periods or other protective mechanisms (Noto La Diega & Sappa, 2018). Consequently, partial or hybrid frameworks have emerged, where contract code smart is supplemented by traditional legal agreements clarifying contingencies or dispute-resolution procedures (Raskin, 2017).

In Italy, proposals suggest integrating electronic notarial oversight, bridging code execution with a human legal intermediary for high-value or high-risk transactions (Isolino, 2019). While such measures provide a degree of certainty, they also diminish the purported efficiency gains of automation, indicating a tension between the desire for self-executing precision and the protective ethos embedded in civil law (Borges, 2019). Taken together, these findings reveal an evolving but incomplete consensus: civil law systems appear capable of legitimizing smart contracts under certain conditions, yet remain cautious about fully embracing code-driven finality without preserving established legal safeguards (Troiano, 2018).

The results further highlight critical enforceability issues, many of which arise from the discordance between the static execution of code and the dynamic interpretative processes traditionally employed by civil law courts (Mik, 2017). In numerous jurisdictions, formal written requirements—especially for transactions like property transfers or consumer credit agreements—pose a direct challenge to smart

contracts that lack a tangible document, signature, or notarization (Fernández Carballo-Calero, 2020).

Even in cases where digital equivalents are legally recognized, doubts persist about whether automated execution can be halted or revised if a statutory violation is detected post-deployment (Albrecht et al., 2019). Scholars point out that irreversible or immutable blockchain operations might contravene the equitable principles that allow courts to grant remedies like reformation or nullification based on vitiated consent (Werbach & Cornell, 2017). These tensions reveal that enforceability is not solely about meeting procedural formalities; it also concerns the capacity of code to accommodate the interpretative flexibility that civil law systems rely upon for equitable outcomes (Raskin, 2017). Thus, the legal enforceability of self-executing agreements remains conditionally recognized, hinging on whether automated processes can be paused or overridden to comply with mandatory norms.

Another enforceability concern relates to consumer protection statutes, which often require transparent disclosures, explicit consent, and the right to withdraw within specified periods (Antognini, 2019). If a smart contract automates performance immediately upon triggering conditions—without providing an opportunity for the consumer to reconsider—it could undermine these statutory entitlements (Noto La Diega & Sappa, 2018). In some jurisdictions, courts might refuse to enforce such agreements on public policy grounds, raising questions about how developers and merchants can design code that respects mandatory consumer rights (Troiano, 2018).

Proposed solutions include incorporating “escape hatches” or “time locks” within the code, allowing a buffer period for withdrawal before permanent execution occurs (Clack et al., 2016). Yet these design interventions may conflict with the idealized notion of trustless, fully automated transactions that originally motivated the development of smart contracts (Buterin, 2013). In sum, the results underscore that enforceability within civil law is contingent not only on satisfying formation and formality requirements but also on integrating protective elements that prevent the code’s self-executing logic from contravening fundamental legal principles (Savelyev, 2016).

With respect to liability, the results indicate that civil law doctrines often rest on identifying a party at fault or attributing negligence to a discernible individual or entity (Zetzsche et al., 2018). This structure becomes complicated in decentralized networks, where code is developed by multiple contributors, deployed by an anonymous party, or relies on data from external “oracles” (Noto La Diega & Sappa, 2018). Under classical civil law theory, fault-based liability presupposes a causal link between a party’s negligent act and the damage suffered, yet in a permissionless blockchain environment, establishing this chain of causation can be exceedingly complex (Borges, 2019).

Some scholars advocate an approach akin to product liability, treating smart contract code as a “product” subject to strict liability if proven defective (Troiano,

2018). However, critics of this analogy argue that software code lacks the tangible characteristics that typically underpin product liability doctrines, and distributing responsibility among multiple coders or auditors raises unresolved legal questions (Reyes, 2017). Overall, the findings suggest that liability frameworks in civil law remain underdeveloped for addressing the unique multi-actor nature of smart contract ecosystems.

Another critical aspect of liability involves the potential for automated execution to breach statutory duties, such as data protection rules or mandatory disclosures (Zanfir-Fortuna & Husovec, 2019). If a smart contract autonomously processes personal data or executes a transaction that violates privacy regulations, questions arise about who bears responsibility—the developer, the deploying entity, or the network as a whole (Sillaber & Waltl, 2017). The results demonstrate that civil law jurisdictions have yet to articulate cohesive doctrines addressing the accountability of decentralized systems, especially when no single entity exerts full control over the software (Savelyev, 2016).

Some legal scholars suggest imposing joint liability on all identifiable participants, but this approach could hinder technological experimentation and deter legitimate actors from participating in blockchain ventures (Noto La Diega & Sappa, 2018). Regulators in certain countries are exploring safe harbor provisions or limited liability frameworks aimed at encouraging innovation while mitigating catastrophic risks (Pinna & Ruttenberg, 2016). Nonetheless, the findings affirm that the question of liability in smart contract scenarios presents a persistent gap in civil law, necessitating further legislative and judicial guidance to balance efficiency, innovation, and protection.

IV. Discussion

The findings illustrate that civil law jurisdictions are capable of recognizing the existence and, in some contexts, the validity of smart contracts, but they also highlight significant challenges to their seamless adoption (Savelyev, 2016). While technology-neutral statutes and flexible interpretations of form requirements provide a preliminary legal basis, the automated and immutable characteristics of smart contracts often clash with the core civil law doctrines of interpretative discretion and equitable remedies (Mik, 2017). Indeed, civil law's reliance on the examination of parties' subjective intentions and its capacity to annul or modify contracts upon discovering defects underscores the tension with code-based finality, where transactions can become irreversible almost instantly (Werbach & Cornell, 2017).

The results also illuminate that a strictly coded arrangement may fail to account for the complexity of real-world transactions, which frequently require renegotiation or equitable relief when circumstances change (Isolino, 2019). Consequently, while academic scholarship and limited legislative experiments display growing acceptance of smart contracts, their integration into mainstream practice remains heavily qualified

by the necessity to preserve fundamental civil law values (Schouppe, 2019). Thus, a core interpretative conclusion is that civil law traditions, while not inherently incompatible with smart contracts, demand cautious adaptation to ensure that automated performance does not override essential legal safeguards.

Another interpretative dimension pertains to enforceability and liability, which the results show to be deeply interconnected in automated contracting scenarios (Troiano, 2018). Enforceability hinges on meeting both formal requisites and substantive protective norms, rendering code-based clauses vulnerable to legal scrutiny if they unilaterally bypass consumer rights or public policy standards (Antognini, 2019). Meanwhile, liability allocation remains murky in decentralized environments, challenging classical civil law doctrines that presume an identifiable defendant (Zetzsche et al., 2018).

This complexity is not purely theoretical; real-world deployments reveal that code errors, oracle failures, and malicious hacks can produce significant financial losses, yet existing legal remedies may be inadequate or inapplicable (Noto La Diega & Sappa, 2018). Consequently, interpretative tensions arise between innovation-driven calls for limited liability or safe harbors and the civil law tradition of holding parties accountable based on fault or negligence (Borges, 2019). Taken together, these findings suggest that while the principle of pacta sunt servanda remains relevant, the mechanisms for ensuring accountability must evolve in tandem with the technology to maintain legal clarity and social legitimacy.

The results further underscore how consumer protection provisions—deeply engrained in many civil law systems—could serve as both a barrier and a catalyst for shaping smart contract design (Fernández Carballo-Calero, 2020). For instance, the mandatory inclusion of withdrawal periods or the prohibition of unfair contract terms might initially seem incompatible with automated, irreversible code (Antognini, 2019). Yet, this very tension has motivated developers to innovate solutions such as configurable “timeouts,” ensuring that vulnerable parties have a window in which to exercise statutory rights (Clack et al., 2016). In this sense, the need to respect consumer protections can drive creative technical adaptations that align code with the normative objectives of civil law, illustrating a form of constructive feedback loop between technology and legal principles (Mik, 2017).

Thus, interpreting the findings through a consumer lens reveals the potential for synergy between protective doctrines and code-driven efficiency, provided that lawmakers and developers collaborate to encode legal norms effectively (Troiano, 2018). Overall, the results suggest a nuanced picture: civil law’s structured doctrines and emphasis on fairness can coexist with smart contracts, so long as code is configured to uphold key protections and if interpretative flexibilities or override mechanisms remain available in exceptional cases.

Despite the breadth and depth of the data set, this study encounters inherent limitations due to the nascent stage of smart contract adoption and the relative scarcity

of definitive case law in civil law jurisdictions (Isolino, 2019). The reliance on doctrinal and theoretical sources means that certain conclusions may remain speculative until tested in courts, where judges must reconcile code-based execution with statutory provisions and established interpretative practices (Fernández Carballo-Calero, 2020). As a result, the study's insights, though robust in doctrinal analysis, cannot fully capture the practical realities and fluidities of actual dispute resolution processes, which may evolve rapidly once real-world controversies emerge (Savelyev, 2016).

Moreover, the comparative approach, while offering broad perspectives, also imposes constraints: not all civil law jurisdictions were examined, and legal nuances may differ substantially in regions beyond Europe, such as Latin America or Asia (Raskin, 2017). Hence, the conclusions drawn here may not universally apply to every civil law environment, necessitating further localized research (Troiano, 2018). Nonetheless, these limitations do not undermine the study's foundational aim, which is to illuminate key doctrinal challenges and potential pathways for reconciliation between smart contracts and civil law principles.

Another notable limitation is the rapid pace of technological development in the blockchain space, which can render certain legislative or scholarly discussions outdated relatively quickly (Clack et al., 2016). As new consensus mechanisms, privacy solutions, or cross-chain functionalities emerge, the assumptions underpinning current legal analyses may shift, leading to either more friction or easier integration with civil law norms (Mik, 2017). Consequently, some of the debates presented in this study might need re-evaluation in the near future, particularly if regulatory bodies impose stricter licensing requirements or if the technology evolves to address known vulnerabilities (Werbach & Cornell, 2017).

Additionally, the study does not engage in empirical testing—such as surveys or interviews with legal practitioners, developers, and end-users—that could yield valuable insights into actual perceptions and experiences with smart contracts (Reyes, 2017). Absent this empirical angle, the analysis remains primarily doctrinal, focusing on how laws and scholars interpret the phenomenon rather than how it manifests in practical, day-to-day operations (Noto La Diega & Sappa, 2018). Nevertheless, the theoretical and comparative framework presented here lays an essential groundwork for subsequent empirical studies, complementing the doctrinal perspective with real-world data.

A final limitation pertains to the assumption that civil law jurisdictions share enough commonalities to permit meaningful generalizations, which may overlook subtle yet important doctrinal divergences (Schouppe, 2019). While codification is a unifying feature, the specific structure, interpretative traditions, and levels of judicial discretion vary significantly among civil law countries (Friedman & Tazi, 2019). This diversity implies that the integration of smart contracts might proceed differently in each national context, influenced by social, economic, and political factors that a

broad comparative study cannot exhaustively capture (Zetzsche et al., 2018).

Moreover, certain jurisdictions may be guided by a tradition of strong consumer protection, while others prioritize economic freedom, leading to distinct regulatory outcomes (Antognini, 2019). Consequently, the findings should be viewed as indicative rather than prescriptive, offering a conceptual map rather than a definitive blueprint for all civil law systems (Mik, 2017). Despite these constraints, the study's doctrinal insights, coupled with comparative illustrations, serve as a valuable reference point, elucidating the core issues that any civil law jurisdiction is likely to face when grappling with the rise of smart contracts.

The study's findings align broadly with earlier scholarly works that emphasize the delicate balance between technological determinism and legal interpretative flexibility (Mik, 2017; Werbach & Cornell, 2017). In particular, Savelyev (2016) identified a similar tension between the code-centered finality of smart contracts and civil law's emphasis on shared intent and subjective interpretation, a conclusion mirrored in this study's results. Moreover, Raskin's (2017) inquiry into the legality of self-executing clauses resonates with the findings regarding enforceability hurdles, especially where consumer protection norms impose limitations on automated performance.

Beyond these general convergences, this article's comparative focus lends credence to Isolino's (2019) claim that certain jurisdictions—like Italy—are exploring hybrid solutions (e.g., digital notaries or partial automation) as a compromise that preserves key civil law protections. Similarly, Fernández Carballo-Calero (2020) and Filippi (2020) highlight the conditional acceptance of smart contracts in Spain and Italy, respectively, echoing this study's finding that enforceability remains subject to statutory compliance and formal requirements. Thus, the research corroborates and extends existing discussions by mapping cross-national variations and pinpointing specific statutory or doctrinal provisions that shape civil law responses to blockchain-based agreements.

In contrast to some earlier works that treat smart contracts primarily as a technical innovation with secondary legal implications, this study foregrounds the doctrinal challenges inherent in civil law systems (Savelyev, 2016). While authors like Buterin (2013) and Tapscott and Tapscott (2016) celebrate the transformative potential of blockchain, they devote comparatively less attention to the intricate statutory mandates and interpretative practices that civil law imposes on contract formation and enforcement. By prioritizing these doctrinal dimensions, this study delivers a more nuanced portrayal of how smart contracts intersect with legal codes designed to protect public order and weaker parties (Antognini, 2019).

The findings also diverge from purely optimistic accounts by highlighting how automated code can inadvertently bypass critical legal safeguards, thereby risking non-enforcement or liability (Noto La Diega & Sappa, 2018). This perspective aligns with the cautionary stance advocated by Clack et al. (2016), who stress the need for

standardized smart contract templates that integrate legal oversight rather than relying solely on code's self-executing character. Consequently, while acknowledging the advantages of automation—such as efficiency and reduced reliance on intermediaries—the study underscores the complexities civil law introduces, a viewpoint that some purely technical analyses overlook.

The present study also advances the conversation by emphasizing consumer protection as a driving factor shaping smart contract acceptance in civil law contexts (Fernández Carballo-Calero, 2020). Existing studies often reference consumer interests but rarely delve deeply into how mandatory norms, cooling-off periods, and disclosure rules might be systematically integrated into automated execution processes (Antognini, 2019). By systematically comparing jurisdictions, the study reiterates a theme found in Noto La Diega and Sappa (2018): that robust consumer protection can serve as an obstacle and a catalyst, compelling developers to encode protective features.

This emphasis further distinguishes the research from works focusing on corporate or financial applications, where consumer stakes are less central (Albrecht et al., 2019). Thus, while the findings share common ground with earlier scholarship in identifying key tension points—like interpretative rigidity or liability distribution—they extend the dialogue by detailing the specific ways consumer regulations might shape, limit, or encourage the design of smart contract systems (Troiano, 2018). Overall, this comparative doctrinal study supplements existing literature by offering both a macro-view of civil law's structural challenges and a micro-focus on consumer-centric issues, thereby refine our collective understanding of how smart contracts may be legally qualified and enforced.

Conclusion

It is evident that civil law systems, while initially seeming at odds with the automated and immutable nature of smart contracts, possess the doctrinal flexibility and legislative adaptability to accommodate such innovations under certain conditions. The key lies in ensuring that the foundational pillars of consent, formality, liability, and consumer protection are not undermined by self-executing code, a balance that may be achieved through hybrid approaches, code "escape hatches," or explicit statutory amendments. The research underscores that enforceability hinges on satisfying not only basic contract formation requirements but also mandatory norms that protect weaker parties and uphold public policy.

Furthermore, liability remains a contentious issue, especially in decentralized environments where the diffusion of responsibility complicates fault-based legal structures. However, emerging legislative experiments, scholarly proposals, and industry-led initiatives signal a growing willingness to harmonize code-driven transactions with the protective ethos embedded in civil law. Consequently, while significant doctrinal and practical hurdles persist, this study's findings reveal a

cautiously optimistic trajectory in which smart contracts and civil law can coexist, provided that deliberate and nuanced frameworks are developed to reconcile automation with legal tradition.

Ultimately, the ongoing evolution of blockchain technologies and the broadening array of smart contract applications make it imperative for civil law systems to offer clear, coherent guidance. The conclusions drawn here suggest that piecemeal solutions—be they judicial interpretations, private contractual stipulations, or limited legislative measures—must eventually converge into more comprehensive regulatory strategies that integrate doctrinal clarity with technological potential. By proactively engaging with these issues, lawmakers, courts, and developers can shape a future in which automated execution does not come at the cost of legal protection and interpretative justice.

In so doing, civil law can maintain its commitment to fairness and certainty while embracing the efficiency and transparency that smart contracts promise. The study thus provides a platform for future scholarly and practical endeavors, calling for empirical investigations, legislative experiments, and interdisciplinary collaborations to refine and apply the doctrinal insights presented. Through such sustained effort, civil law jurisdictions can rise to the challenge of a new technological epoch, harnessing the benefits of automation without sacrificing the fundamental values that have long anchored their legal systems.

Bibliography

AllahRakha, N. (2024). Cybersecurity regulations for protection and safeguarding digital assets (data) in today's worlds. Lex Scientia Law Review, 8(1), 405-432. https://doi.org/10.15294/lslr.v8i1.2081

Antognini, A. (2019). Smart contracts and consumer protection in civil law countries. *European Review of Private Law, 27*(5), 989–1012.

Borges, G. (2019). Smart contracts and the role of law. In P. Hacker, I. Lianos, G. Dimitropoulos, & S. Eich (Eds.), *Blockchains, smart contracts, decentralised autonomous organisations and the law* (pp. 91–107). Edward Elgar.

Buterin, V. (2013). A next-generation smart contract and decentralized application platform. *Ethereum White Paper*.

Clack, C. D., Bakshi, V. A., & Braine, L. (2016). Smart contract templates: Foundations, design landscape, and research directions. *arXiv preprint*, arXiv:1608.00771.

Fairfield, J. A. T. (2014). Smart contracts, Bitcoin bots, and consumer protection. *Washington & Lee Law Review Online, 71*, 35–50.

Fernández Carballo-Calero, M. (2020). Smart contracts and the Spanish legal system. *Revista de Derecho Civil, 7*(2), 153–177.

Filippi, G. (2020). Smart contracts in Italy: Legal issues and enforceability under civil law. *Contratto e Impresa, 36*, 251–269.

Friedman, S., & Tazi, T. (2019). Smart contracts as legal contracts in France: Form requirements and consent. *Revue Lamy Droit de l'Immatériel (RLDI), 160*, 29–39.

Gatt, J. (2019). Smart contracts and the digital single market legislation. *EUI MWP Working Paper*. European University Institute.

Ikigami, H. (2020). Smart contracts under Japanese civil law: Formation, validity, and future challenges. *Waseda Bulletin of Comparative Law, 41*, 63–82.

Isolino, M. F. (2019). Smart contracts e diritto privato: riflessioni sulla validità e l'efficacia delle clausole contrattuali automatizzate. *Diritto dell'Informazione e dell'Informatica, 2019*, 497–526.

Karnitschnig, S., & Pichonnaz, P. (2020). Smart contracts and their legal challenges in Swiss private law. *Revue de droit Suisse, 139*, 1325–1359.

Mik, E. (2017). Smart contracts: Terminology, technical limitations and real-world complexity. *Law, Innovation and Technology, 9*(2), 269–300.

Noto La Diega, G., & Sappa, C. (2018). Distributed ledger technologies and smart contracts: Legal implications for civil law. *European Review of Private Law, 26*(6), 805–832.

Pinna, A., & Ruttenberg, W. (2016). Distributed ledger technologies in securities post-trading: Revolution or evolution? *ECB Occasional Paper Series, 172*. European Central Bank.

Raskin, M. (2017). The law and legality of smart contracts. *Georgetown Law Technology Review, 1*, 304–341.

Reyes, C. L. (2017). Conceptualizing cryptolaw. *Nebraska Law Review, 96*(2), 384–445.

Savelyev, A. (2016). Contract law 2.0: "Smart" contracts as the beginning of the end of classic contract law. *Higher School of Economics Research Paper No. WP BRP 79/LAW/2016*.

Schouppe, T. (2019). Blockchain revolution without the 'chain'? Smart contracts and the corporate contracting process. *European Business Law Review, 30*(4), 571–598.

Sillaber, C., & Waltl, B. (2017). Life cycle of smart contracts in blockchain ecosystems. *Datenschutz und Datensicherheit – DuD, 41*(8), 497–500.

Surden, H. (2012). Computable contracts. *UC Davis Law Review, 46*, 629–700.

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world.* Portfolio.

Troiano, L. (2018). Smart contracts and civil liability. *Rivista di Diritto dei Media, 1*, 205–220.

Werbach, K., & Cornell, N. (2017). Contracts ex machina. *Duke Law Journal, 67*, 313–382.

Zanfir-Fortuna, G., & Husovec, M. (2019). EU data protection and automated contractual enforcement in smart contracts. *Masaryk University Journal of Law and Technology, 13*(2), 269–290.

Zetzsche, D. A., Buckley, R. P., & Arner, D. W. (2018). The distributed liability of distributed ledgers: Legal risks of blockchain. *University of Illinois Law Review, 2018*(4), 1361–1406.