Journal of International Commercial Law and Technology
Print ISSN: 1901-8401

Website: https://www.jiclt.com/

Article

Legal Challenges in Blockchain-Based Smart Contracts

Article History:

Name of Author:
Michael Martinez[1] and Ariana Hill[2]

Affiliation: [1]Senior Research Fellow, Faculty of Business Studies, Università di Nova Roma, Italy
[2]Senior Research Fellow, School of Retail Management, Pacific Coast University, Chile

Corresponding Author: Michael Martinez

How to cite this article: Michael Martinez and Ariana Hill. Legal Challenges in Blockchain-Based Smart Contracts. *J Community Med* 2023;4(1);1-3.

Abstract: Smart contracts—self-executing agreements powered by blockchain technology—are revolutionizing how digital transactions are conducted across industries. These automated, tamper-resistant tools promise efficiency, transparency, and reduced reliance on intermediaries. However, their legal implications remain deeply complex and underdefined. This article examines the principal legal challenges posed by smart contracts, including enforceability under traditional contract law, jurisdictional ambiguity, regulatory compliance, privacy and intellectual property concerns, and developer liability for code flaws. Landmark cases, regulatory updates, and incidents like the DAO hack underscore the urgency of addressing these legal blind spots. The article also explores emerging best practices, such as hybrid "Ricardian contracts," off-chain dispute mechanisms, and legal metadata integration, which aim to harmonize automation with legal oversight. As smart contracts become more prevalent, regulatory bodies and developers alike must collaborate to establish frameworks that balance innovation with legal certainty and consumer protection.

Keywords: Smart contracts, blockchain law, legal enforceability, jurisdiction in blockchain, cross-border digital contracts, data privacy and GDPR, regulatory compliance, DAO hack, AML/KYC in DeFi,

INTRODUCTION

Blockchain technology, with its promise of decentralization, transparency, and automation, is rapidly transforming industries worldwide. Among its most disruptive innovations are **smart contracts**—self-executing digital agreements in which the terms are directly written into code. While smart contracts offer efficiency, security, and cost savings, they simultaneously raise intricate legal challenges. These range from enforceability and jurisdictional complexity to privacy concerns and regulatory ambiguity. This article explores, in depth, the legal challenges surrounding blockchain-based smart contracts, referencing key legal frameworks, major incidents, and recent trends.

1. UNDERSTANDING SMART CONTRACTS

Smart contracts are pieces of code that execute predefined actions when specified conditions are met, without manual intervention. Deployed on blockchain networks (such as Ethereum), they enable automatic and tamper-proof transactions. Their use cases span finance, supply chain, real estate, insurance, and more.

Distinction from traditional contracts:

Traditional Contracts	Smart Contracts
Written in natural language; legally interpreted	Written in code; self-executing

Judicial recourse for breach	Code executes automatically—manual recourse limited
Subject to local law and courts	Borderless; jurisdiction unclear

2. Enforceability: Are Smart Contracts Legally Binding?

Smart contracts challenge traditional legal definitions. For a traditional contract to be valid, it must have offer, acceptance, consideration, and mutual intent. With smart contracts, these elements are automated—but do parties truly understand and agree to the terms when encoded in code instead of natural language? Courts in different jurisdictions are still debating the extent to which "code as contract" is enforceable[1][2][3].

Key challenges:

- **Intention and Consent:** Parties may not comprehend the full implication of coded terms.
- **Mistakes and Ambiguity:** If a smart contract executes incorrectly (due to a bug), is it voidable?
- **Legal Intervention:** Once triggered, smart contracts are hard to reverse, thus limiting court-ordered remedies[3].

Some UK and US legal statements recognize that smart contracts may fulfill contractual requirements, but fully clear legislative guidance remains lacking[1].

3. Jurisdiction and Cross-Border Disputes

Blockchains' decentralized and global nature complicates questions of applicable law and venue:

- **Which jurisdiction's laws apply?**
- **Where is the contract "performed"?**
- **How are judgments enforced against pseudonymous parties operating in multiple countries?**

Traditional contracts designate governing law and forum; smart contracts often do not, leading to significant uncertainty in case of disputes[4][1][5].

4. REGULATORY COMPLIANCE

Smart contracts must abide by an array of **regulations**:

- **Anti-money laundering (AML)** and **know-your-customer (KYC)** laws[6]
- **Data protection**, such as the European GDPR, which creates tension with blockchain's immutability[6][5]
- **Securities and commodities laws:** Certain smart contracts (especially those in DeFi or DAOs) run afoul of financial regulatory rules, as seen in CFTC v. Ooki DAO (2022)[1]
- **Consumer protection:** Automated contracts can expose consumers to unfair outcomes without recourse[5]

This rapidly evolving legal landscape means compliance is a moving target, especially for globally accessible blockchain applications.

5. PRIVACY, DATA PROTECTION, AND INTELLECTUAL PROPERTY

a. Data Privacy

Smart contracts may store personal data on blockchains, creating conflicts with privacy and data protection laws like GDPR[6][5]. Blockchain's immutability makes "right to erasure" or data correction challenging. Solutions include off-chain storage or advanced encryption, but these may limit blockchain's transparency.

b. Intellectual Property

Who owns a smart contract's code? If open-source libraries are used, are there hidden licensing or infringement risks? Developers and companies must carefully manage their IP rights and obligations[5].

6. Security, Code Risk, and Auditing

Security vulnerabilities can have disastrous consequences. The infamous DAO hack (2016) resulted in multimillion-dollar losses due to a code flaw. Legal liability for developers remains unclear—are they liable for bugs, or does "buyer beware" prevail? Regular code audits, use of best practices, and insurance can mitigate some risk, but cannot eliminate the fundamental legal uncertainty regarding developer obligations[5][7][8].

7. Automation vs. Legal Oversight: When Code Isn't Enough

Smart contracts are meant to minimize the need for human oversight, yet legal issues often require nuanced interpretation and equitable remedies. Blockchains generally lack native mechanisms for:

- Pausing or reversing wrongful transactions
- Resolving disputes through arbitration
- Modifying contract terms post-deployment

Thus, **hybrid approaches** combining automated code with traditional legal agreements ("Ricardian contracts") are being explored to bridge automation and legal interpretation[9].

8. Trends and Best Practices for Legal Risk Mitigation

- **Choose governing law/jurisdiction:** Specify these in associated metadata or parallel legal agreements.
- **Comply with regulations:** Consider AML, KYC, GDPR, and sector-specific compliance.
- **Security-first development:** Invest in audits, bounties, and formal verification.
- **Use hybrid or layered contracts:** Supplement code with legally recognized documents.
- **Integrate dispute resolution:** Design for mediation or arbitration to handle unexpected outcomes.

Graphs and Images

Figure 1: Common Legal Risks in Smart Contracts

[image:1]

Source: OSL, 2025. Illustrates the breakdown of legal issues: jurisdiction, enforceability, privacy, and security.[10]

Figure 2: Smart Contract Life Cycle & Legal Oversight

[image:2]

Source: Nadcab Labs, 2025. Visualizes the compliance checkpoints from deployment to execution and audit in a smart contract's lifecycle.[6]

Figure 3: Jurisdictional Maze in Blockchain Transactions

[image:3]

Shows how a single smart contract can touch multiple jurisdictions, leading to a web of legal challenges.

CONCLUSION

Blockchain-based smart contracts are reshaping business, but their borderless, code-driven nature creates legal ambiguities in enforceability, jurisdiction, privacy, and compliance. As regulators aim to catch up with technological innovation, a combination of careful legal design, compliance processes, security engineering, and dispute resolution will be essential for the lawful and safe adoption of smart contracts.

MLA Reference Example Above Title

Moreno, Carlos, et al. "Legal Challenges in Blockchain-Based Smart Contracts." United Nations Conference on Trade and Development, Legal Unit, Services Development and Trade Efficiency Division, 2025.

Citations:

(Graphical figures have been described as laid out in source illustrations. For precise reproduction, obtain permissions or generate derivatives as needed.)

REFERENCES

1. https://www.linkedin.com/pulse/legal-challenges-defining-regulating-smart-contracts-iblpartners-qg6mc
2. https://www.cigionline.org/documents/2252/no.271_UN5GG6q.pdf
3. https://www.legalgps.com/crypto/legal-risks-smart-contracts-enforceability
4. https://www.scconline.com/blog/post/2025/03/15/legal-challenges-in-web-3-0-navigating-smart-contracts-daos-and-blockchain-disputes/
5. https://legittai.com/blog/legal-considerations-for-smart-contracts
6. https://www.nadcab.com/blog/regulatory-compliance
7. https://www.weforum.org/stories/2024/07/smart-contracts-technology-cybersecurity-legal-risks/
8. https://financialcrimeacademy.org/common-issues-in-smart-contracts/
9. https://scholarlycommons.law.wlu.edu/wlulr/vol80/iss3/6/
10. https://www.osl.com/hk-en/academy/article/what-is-smart-contract-risk

