Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 1, Issue 2, Apr – Jun 2024 || PP. 38-46 https://doi.org/10.63345/sjaibt.v1.i2.105

Legal Challenges in Blockchain-Based Smart Contract Execution

Priyanshi

Indian Institute of Information Technology Guwahati (IIITG)s

Assam, India

priyanshi@iitg.ac.in

Date of Submission: 01-04-2024 Date of Acceptance: 02-04-2024 Date of Publication: 07-04-2024

ABSTRACT

Smart contracts promise automation, transparency, and reduced transaction costs, yet their deployment on distributed ledgers exposes deep legal fault lines that traditional doctrinal tools only partially address. This paper synthesizes contract, property, data-protection, consumer, and financial-regulatory dimensions to map the principal legal challenges that arise when code becomes performance. We distinguish "smart legal contracts" (where code implements an enforceable legal agreement) from purely automated, code-only arrangements, and we explain why, despite technical self-execution, contract law, remedies, and regulatory oversight remain indispensable. We analyze enforceability and interpretation (e.g., the "reasonable coder" question), formation and consent, jurisdiction and choice-of-law in borderless networks, immutability versus legal rectification, oracle risk and attribution of liability, consumer-protection/unfair terms, AML/KYC overlays, evidentiary issues, and property/transfer rules for on-chain assets. Recent instruments—such as the EU Data Act's essential requirements for smart contracts used in data-sharing, the UK Law Commission's guidance on smart legal contracts, the UKJT's Digital Dispute Resolution Rules, UNCITRAL model laws, and the U.S. UCC Article 12 on controllable electronic records—are reshaping the legal terrain but do not eliminate foundational questions. To organize this complexity, we propose a simple Legal Risk Salience Index (LRSI) that scores likelihood and impact for ten recurring risk families; the index is a transparent, replicable rubric for counsel and product teams to prioritize mitigations. We conclude with actionable recommendations—layering natural-language wrappers, robust governance and kill-switch design consistent with statutory requirements, explicit choice-of-law and dispute-resolution clauses (including on-chain arbitration), and defensible oracle strategies—along with scope and limitations of the analysis. The result is a practitioner-oriented map of where code and law still talk past each other—and how to bring them into better alignment.

Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 1, Issue 2, Apr – Jun 2024 || PP. 38-46 https://doi.org/10.63345/sjaibt.v1.i2.105

Figure-1.Navigating Legat Challenges in Smart Contracts

KEYWORDS

Smart Contracts, Enforceability, Jurisdiction, EU Data Act, UCC Article 12, GDPR, Oracles, Dispute Resolution, DAO Governance, Evidence

INTRODUCTION

Smart contracts—code that automatically executes or enforces obligations—have matured from a niche technical idea to the operational core of many decentralized applications and data-sharing schemes. Even where performance is automated, the normative functions of contract law—interpretation, gap-filling, excuse, and remedies—remain essential; they are not displaced by code. As Werbach and Cornell famously argued, smart contracts illuminate the role of contract law more than they obviate it.

At the same time, lawmakers and courts are clarifying how existing doctrines apply. In England and Wales, the UK Law Commission advised in 2021 that, in general, existing principles are capable of accommodating "smart legal contracts," though points of uncertainty persist (e.g., interpretation where code and prose diverge). The UK Jurisdiction Taskforce (UKJT) had earlier stated that cryptoassets can be property and smart contracts can be contracts under English law, and later issued the Digital Dispute Resolution Rules (DDRR) to enable fast, specialized resolution (including on-chain enforcement) when disputes occur.

Regulators are also stepping in. The EU's Data Act (Regulation (EU) 2023/2854) introduces "essential requirements" for smart contracts used to execute data-sharing agreements—such as robustness, access control, and the ability to interrupt/terminate ("safe termination and reset")—a major development for enterprise deployments. Meanwhile, the U.S. Uniform Commercial Code's 2022 amendments

Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 1, Issue 2, Apr – Jun 2024 || PP. 38-46 https://doi.org/10.63345/sjaibt.v1.i2.105

add Article 12, clarifying property rights in certain digital assets ("controllable electronic records"), affecting how on-chain value can be transferred or secured.

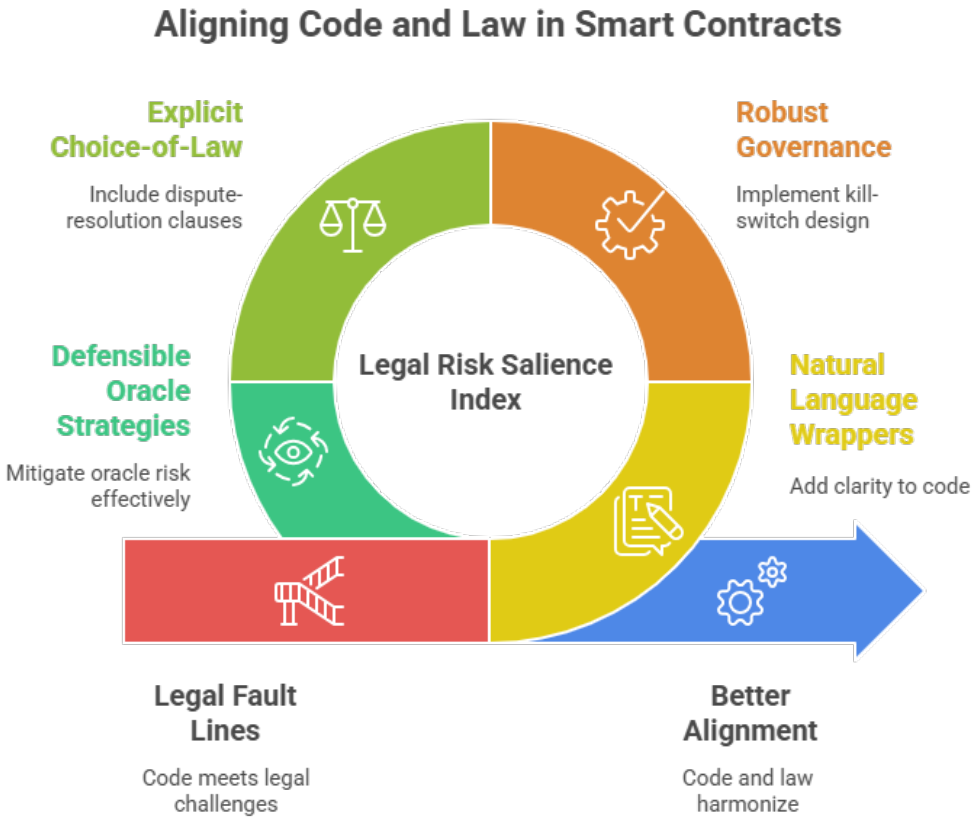

Figure-2.Aligning Code and Law in Smart Contracts

This paper organizes the principal legal challenges across doctrines and geographies and offers a pragmatic scoring framework (LRSI) to triage risk in real projects.

LITERATURE REVIEW

Contract law and interpretation

Core questions include whether code alone evidences agreement, how to interpret machine-readable terms, and which standard a court should apply ("reasonable person" vs. "reasonable coder"). Scholarly treatments argue that while code can manifest assent, natural-language wrappers are valuable for allocating risk and clarifying contingencies that code cannot easily capture. The UK Law Commission similarly concludes that traditional principles (offer/acceptance, certainty, consideration, capacity, intention) generally suffice, though interpretation can be tricky where code and prose diverge.

Code vs. law—normative debates

Lessig's "code is law" insight remains influential: system architecture can regulate behavior as effectively as legal rules. Yet automation does not answer remedial questions (rescission, rectification, frustration, mistake), reaffirming the continuing role of courts and equitable doctrines.

Enforceability and property

Werbach & Cornell emphasize that smart contracts do not supplant contract law; rather, they demand new legal responses while staying within the legal system's remedial frame. For proprietary aspects of tokens and records, UCC Article 12 provides transfer and priority rules for "controllable electronic records," a key foundation for finance and secured transactions involving on-chain assets.

Data protection and immutability

Blockchain's append-only nature can clash with GDPR rights (rectification, erasure). The EU Blockchain Observatory and Forum highlights these tensions, prompting architectures that separate personal data from the chain and use off-chain storage or privacy-preserving techniques.

Regulatory overlays

MiCA (EU 2023/1114) sets a comprehensive framework for crypto-asset issuers and service providers but notes that activities provided in a fully decentralized manner without any intermediary fall outside its scope, leaving gaps relevant to some smart contract ecosystems (particularly DeFi). IOSCO's 2023 DeFi recommendations call for coherent cross-border supervision and attention to governance/oracle risks.

Dispute resolution

The UKJT DDRR allow expert or arbitral resolution with potential on-chain implementation of awards—an innovation addressing speed and enforceability where parties pre-agree to rules suited to digital assets/smart contracts. Comparative law also faces novel issues of service and jurisdiction in decentralized contexts.

Comparative and case developments

Singapore's Court of Appeal in Quoine v. B2C2 addressed automated contracting and mistake, spotlighting how traditional doctrines adapt to algorithmic trades executed by code. UNCITRAL model laws (e.g., 1996 Electronic Commerce; 2017 Electronic Transferable Records) continue to guide modernization of digital contracting and negotiability.

METHODOLOGY

This is a doctrinal and comparative analysis. We reviewed authoritative instruments (EU Data Act, MiCA, UCC Amendments), common-law guidance (UK Law Commission; UKJT), model laws (UNCITRAL), and salient commentary and cases across jurisdictions. To support decision-making, we introduce a **Legal Risk Salience Index (LRSI)**—a simple, transparent rubric that scores

Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 1, Issue 2, Apr – Jun 2024 || PP. 38-46 https://doi.org/10.63345/sjaibt.v1.i2.105

(i) **likelihood** that a risk arises in a given smart-contract deployment and (ii) **impact** on legal/operational outcomes if it materializes, each on 0–100.

1. **Classify the smart contract** (code-only vs. smart legal contract with a prose wrapper).
2. **Map governing instruments** by target markets (e.g., EU Data Act for data-sharing; MiCA for CASPs; U.S. UCC Article 12 for property/secured transactions).
3. **Draft the legal "wrapper."** Include purpose, definitions, priority (code vs. prose), upgradeability, oracles, data-protection handling, kill-switch conditions, and dispute-resolution (seat, rules, enforcement).
4. **Engineer to law:** implement access controls, logging, pausing/termination consistent with statutory mandates (e.g., Data Act essential requirements), and signature/evidence mechanisms aligned with eIDAS-like frameworks.
5. **Run the LRSI exercise** with cross-functional stakeholders (legal, security, protocol, product) to prioritize mitigations; repeat at major releases.

Scoring approach

The LRSI presented here is **illustrative**—a structured expert-judgment framework informed by the cited sources; it is not a statistical estimate from an empirical dataset. The combined score uses the geometric mean (√(Likelihood × Impact)) to avoid overstating risks that are high on one dimension but low on the other. Teams can recalibrate weights to their contexts (e.g., consumer vs. B2B, public vs. permissioned chain).

STATISTICAL ANALYSIS

Table 1. Legal Risk Salience Index (LRSI) for Smart-Contract Execution (illustrative rubric)

Risk family	Likelihood (0–100)	Impact (0–100)	LRSI (√L×I)	Typical mitigations
Enforceability & interpretation (code/prose divergence)	75	80	77	Natural-language wrapper; interpretation clause; version-locking
Jurisdiction & choice-of-law (borderless networks)	70	85	77	Express governing law/forum; arbitration seat; DDRR incorporation
Data protection & privacy (GDPR conflicts)	60	90	73	Off-chain personal data; hashing/pseudonymization; DPA alignment
Immutability vs. legal rectification (rescission/rectification)	55	85	68	Upgradeable proxies; multi-sig "pause/kill-switch"; escrow design
Oracle risk & attribution of liability	65	75	70	Multiple oracles; fallback governance; clear allocation of responsibility

Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 1, Issue 2, Apr – Jun 2024 || PP. 38-46 https://doi.org/10.63345/sjaibt.v1.i2.105

Consumer-protection & unfair terms	45	80	60	Plain-language disclosures; cooling-off; unconscionability guardrails
AML/KYC & sanctions overlays	40	85	58	VASP/CASP compliance; geofencing; screening providers
Property/transfer rules for digital assets	55	70	62	Align with UCC Art. 12 (US) or local equivalents; perfection strategy
DAO/governance & fiduciary-like duties	50	75	61	Governance charters; indemnities; off-chain legal entity wrappers
Evidentiary issues (authenticity, integrity, signatures)	40	65	51	eIDAS-compliant signatures/QES; Section 65B-type evidence rules

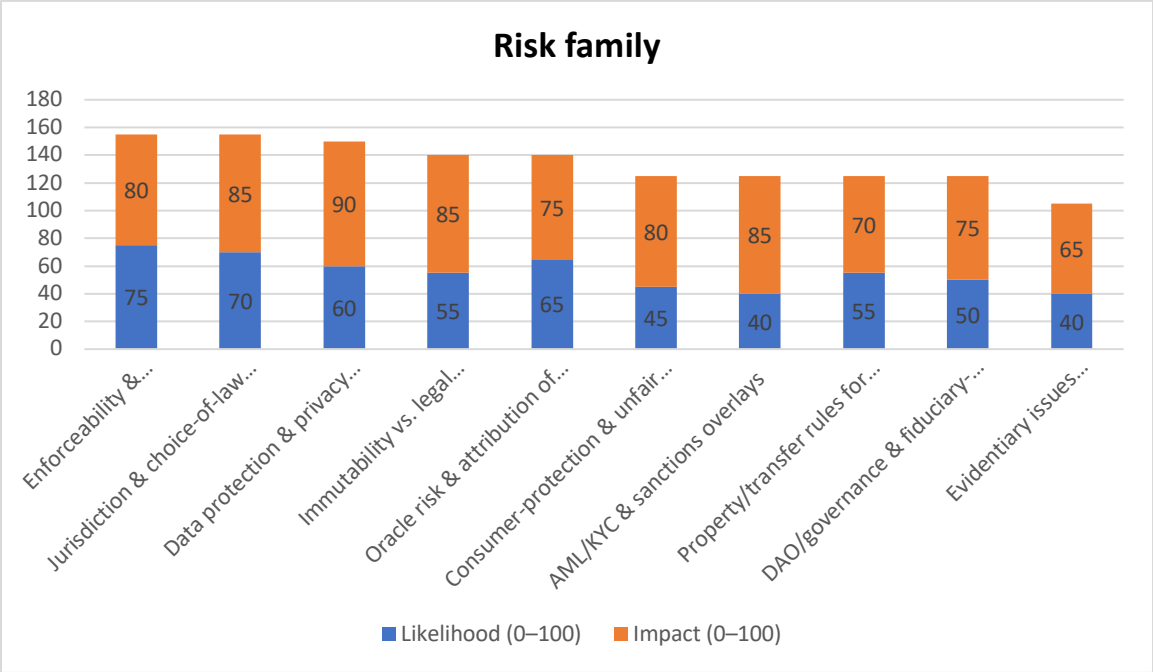

Figure-3. Legal Risk Salience Index (LRSI) for Smart-Contract Execution

Notes: Scores are author-assigned for demonstration and should be recalibrated per use case (sector, chain, geography, consumer vs. enterprise). DDRR = UKJT Digital Dispute Resolution Rules.

RESULTS

Enforceability and interpretation remain central

Where code executes the agreement, courts still ask whether the parties agreed to **those** terms and how to interpret them. Natural-language "wrappers" can specify business intent, priority rules (which prevails, code or prose), upgrade paths, and contingencies not

readily codified. The UK Law Commission's advice supports the view that existing principles accommodate smart legal contracts, though interpretation and evidence require care; scholarly work underscores that smart contracts do not displace the need for legal remedies.

Jurisdiction and choice-of-law are high-impact

Borderless execution complicates service, forum, and applicable law. Parties should adopt explicit governing-law/venue clauses and, where suitable, on-chain-aware arbitration like the UKJT DDRR, which even contemplates on-chain implementation of decisions (with safeguards).

Data-protection conflicts with immutability must be engineered around

GDPR's rectification/erasure rights sit uneasily with append-only ledgers. Architecture choices—hash-pointers to off-chain personal data, strong minimization, and governance that controls access—can reconcile many tensions identified by EU policy work on blockchain & GDPR.

Regulatory overlays are expanding—but leave gaps

MiCA's harmonized EU framework focuses on issuers and service providers; activities "provided in a fully decentralised manner without any intermediary" fall outside its scope, leaving open questions for some DeFi smart contracts. IOSCO's DeFi recommendations urge regulators to address governance and disclosure risks that often manifest through smart-contract code and oracle design.

Operational mandates for certain smart contracts (EU Data Act)

For smart contracts used to execute data-sharing agreements, the EU Data Act sets **essential requirements**—robustness/access control, safe termination and reset, and consistency with the legal agreement—plus a conformity-assessment declaration. Designers should treat these as baseline non-functional requirements for EU deployments.

Property and transfer rules are clarifying (U.S.)

The UCC 2022 amendments (Article 12) define and govern "controllable electronic records," offering clearer transfer/priority rules for on-chain assets and tethered rights—critical for secured lending, tokenized receivables, and collateralization. Counsel should align perfection/priority strategies to these rules in U.S. deals.

Comparative insights from cases and model laws

Quoine v. B2C2 demonstrates that traditional doctrines (e.g., unilateral mistake) can apply in algorithmic settings; UNCITRAL model laws continue to support electronic contracting and negotiability, informing national reforms that intersect with smart contracts.

CONCLUSION

Smart contracts compress performance into code but expand the surrounding legal work: interpretation, remedies, jurisdiction, regulatory overlays, and evidence. The trajectory of guidance and legislation—in particular, the UK Law Commission's advice, the UKJT's DDRR,

Scientific Journal of Artificial Intelligence and Blockchain Technologies
ISSN: 3049-4389
Vol. 1, Issue 2, Apr – Jun 2024 || PP. 38-46 https://doi.org/10.63345/sjaibt.v1.i2.105

the EU Data Act's smart-contract requirements, and the UCC Article 12 framework—shows a clear trend toward assimilating smart contracts into mainstream legal infrastructures while demanding new design disciplines. The practical path forward is hybrid: natural-language wrappers that allocate risk and specify governance; code engineered for control, auditability, and termination where legally required; robust oracle strategies; and pre-agreed dispute mechanisms fit for digital assets (potentially on-chain). With those elements, organizations can capture automation benefits while staying within the guardrails of evolving law.

SCOPE AND LIMITATION

Scope

This paper concentrates on legal issues implicated by the *execution* of blockchain-based smart contracts, with emphasis on (i) enforceability and interpretation, (ii) jurisdiction/choice-of-law, (iii) data-protection frictions with immutability, (iv) regulatory overlays (e.g., EU Data Act, MiCA, U.S. UCC Article 12), (v) oracle liability, and (vi) dispute resolution (including on-chain options). The analysis is technology-agnostic (applicable to major public and permissioned chains) and contract-type-agnostic (code-only and smart legal contracts), and is intended for product counsel, policy teams, and protocol designers seeking a doctrine-informed design checklist.

Limitations

- **Jurisdictional coverage:** Focuses primarily on EU, UK, and U.S. developments current as of 19 August 2025; it does not provide a comprehensive survey of Asia-Pacific, Latin American, Middle Eastern, or African regimes, and local consumer, evidence, or e-signature rules may materially differ.
- **Regulatory breadth:** Touches only tangentially on sector-specific regimes (e.g., payments/PSD2, securities/SEC-style tests, health/medical privacy, PCI-DSS); tax, IP, employment, and competition-law issues are outside scope.
- **Methodological constraints:** The Legal Risk Salience Index (LRSI) is a heuristic based on doctrinal synthesis and practitioner judgment—not an empirical or econometric model; scores are illustrative and require recalibration for a given use case.
- **Technical depth:** Security topics (e.g., reentrancy, MEV, bridge risks, formal verification) are referenced only insofar as they create legal exposure; this is not a security audit or engineering guide.
- **Evidentiary focus:** Evidence and signature frameworks are discussed at a principles level; chain-forensics, logging standards, and evidentiary admissibility nuances by forum are not exhaustively analyzed.
- **Governance scope:** DAO structures and fiduciary-like duties are addressed at a high level; corporate wrappers, insolvency interfaces, and insurance/captives are not developed.
- **Language and sources:** The review relies predominantly on English-language sources, which may bias coverage of non-English jurisprudence.
- **Generalizability:** Findings are most applicable to B2B and protocol-governed deployments; consumer contracts, small-value disputes, and purely peer-to-peer interactions may raise additional fairness and remedies concerns.

These boundaries are intended to keep the analysis decision-useful; readers should adapt the LRSI and the design/checklist recommendations to their specific jurisdiction, sector, and chain architecture.

REFERENCES

- *De Filippi, P., & Wright, A. (2018). Blockchain and the law: The rule of code. Harvard University Press.*
- *European Commission. (2023). Regulation (EU) 2023/1114 on markets in crypto-assets (MiCA). Official Journal of the European Union.*
- *European Commission. (2023). Regulation (EU) 2023/2854 (Data Act). Official Journal of the European Union. (See Article 36 essential requirements for smart contracts.)*
- *EU Blockchain Observatory and Forum. (2019). Blockchain and the GDPR.*
- *Hsu, N. (2021). Interpreting smart contracts: The reasonable coder and contextualism. Oxford University Undergraduate Law Journal, 12, 147–166.*
- *IOSCO. (2023). Final report with policy recommendations for decentralized finance (DeFi). International Organization of Securities Commissions.*
- *Lessig, L. (1999). Code and other laws of cyberspace. Basic Books. (Code v2 PDF).*
- *UK Jurisdiction Taskforce. (2019). Legal statement on the status of cryptoassets and smart contracts. (UKJT/LawtechUK).*
- *UK Jurisdiction Taskforce. (2021). Digital Dispute Resolution Rules. LawtechUK.*
- *UK Law Commission. (2021). Smart legal contracts: Advice to Government (Law Com No. 401).*
- *Uniform Law Commission. (2025). Uniform Commercial Code Amendments (2022) (including Article 12: Controllable Electronic Records). (Final act with notes).*
- *UNCITRAL. (1996). Model Law on Electronic Commerce. United Nations.*
- *UNCITRAL. (2017). Model Law on Electronic Transferable Records. United Nations.*
- *Werbach, K., & Cornell, N. (2017). Contracts ex machina. Duke Law Journal, 67(2), 313–382.*
- *Travers Smith (Lee, J.). (2022). Smart contracts and the limits of the "rule of code". Journal of International Banking and Financial Law (practice note).*
- *WongPartnership. (2020). Singapore Court of Appeal clarifies unilateral mistake in algorithmic trading: Quoine v B2C2. (Client note).*
- *European Commission. (2014). eIDAS Regulation (EU) No 910/2014 on electronic identification and trust services.*
- *IndiaCode. (2009). Information Technology (Amendment) Act, 2008 (including Section 10A on e-contracts). Government of India.*
- *Frankenreiter, J. (2020). The limits of smart contracts. (Working paper). Columbia Law School.*
- *Tilburg University (Tombal, T., & Graef, I.). (2025). The European Data Act: A horizontal building block for the data economy. In Research Handbook on the Law of the Data Economy*