# INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

 ISSN: 2582-6433

# DISCLAIMER

 ISSN: 2582-6433

# EDITORIAL TEAM

## EDITORS

### Dr. Samrat Datta

*Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board*

### *Dr. Namita Jain*

*Head & Associate Professor*

*School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.*

*Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019*

 ISSN: 2582-6433

# Mrs.S.Kalpana

Assistant professor of Law

*Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.*

# Avinash Kumar

*Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.*

 ISSN: 2582-6433

# ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

 ISSN: 2582-6433

# CONTRACT LAW IN THE DIGITAL AGE: AI, BLOCKCHAIN, AND THE FUTURE OF LEGAL CONSENT AND LIABILITY

AUTHORED BY - NIVEDITA RAJESH & SWETHA PRABHA K

*Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They run on blockchain platforms, ensuring that the contract is immutable and automatically enforced when predetermined conditions are met. However, it challenges traditional contract principles of intent, liability, and consent, requiring evolving legal frameworks for automated environments. This research paper examines the implications of AI and blockchain technologies for contract law within the context of cyber law, particularly regarding automated decision-making. It questions whether traditional notions of consent and intent are still relevant when AI is involved in contract formation. The paper analyzes the roles of various stakeholders, including developers and users, and explores the legal frameworks needed to address liability issues arising from these technologies. It also investigates how consumer protection laws can adapt to prevent cartel behavior during AI-driven contract negotiations. Furthermore, the paper evaluates how courts should interpret smart contracts executed via blockchain, emphasizing the need for a check against algorithmic bias and discrimination. Additionally, it highlights the principle of contra proferentem, which suggests that any ambiguity in contracts should be interpreted against the interests of the party that drafted them, reinforcing the need for clarity in AI-generated contracts. Lastly, the study calls for international harmonization of laws governing AI in contracts and underscores the importance of transparency.*

 ISSN: 2582-6433

# I. INTRODUCTION

In the digital age, the rise of Artificial Intelligence (AI) and blockchain technologies has brought about significant transformations in various fields, including contract law. Traditionally, contracts have been formed based on human consent, intent, and mutual agreement. However, the increasing use of AI and blockchain challenges these fundamental principles, as automated systems are now capable of making decisions and executing contracts without direct human involvement. This introduction sets the stage for a comprehensive exploration of how these technologies are reshaping the landscape of contract law and why new legal frameworks are necessary.

## Background

AI and blockchain have become integral to modern contractual practices. AI systems, ranging from simple algorithms to advanced machine learning models, are increasingly being used to negotiate, form, and execute contracts autonomously. For instance, AI-driven platforms can automate complex transactions in finance, supply chain management, and other sectors, making decisions based on vast amounts of data in real-time. On the other hand, blockchain technology facilitates the creation of smart contracts—self-executing agreements with the terms of the contract directly written into code. These contracts automatically enforce themselves when predefined conditions are met, reducing the need for intermediaries and enhancing transaction security.

Despite their advantages, these technologies introduce new complexities to contract law. Traditional contracts rely on the notions of consent and intent, usually expressed through negotiation and agreement between human parties. In AI-driven contracts, the "consent" is often automated, and the "intent" may be derived from an algorithm rather than a human actor. This raises fundamental questions about the validity and enforceability of such agreements.

## Scope and Objectives

This paper aims to explore the profound impact of AI and blockchain on traditional contract law. It seeks to analyze how these technologies challenge established legal concepts such as consent, intent, and liability. Specifically, it will delve into the role of AI in contract formation and execution, examining whether automated decision-making aligns with the principles of mutual agreement and informed consent. The paper will also investigate the legal status of smart contracts executed on blockchain platforms, questioning how courts should interpret

 ISSN: 2582-6433

these code-based agreements in light of traditional contract law.

Moreover, the paper will scrutinize the issue of liability in AI and blockchain-driven contracts. With AI systems making autonomous decisions, it becomes essential to determine who is liable for breaches or damages arising from these decisions. Is it the developers who programmed the AI, the users who employed it, or the AI itself? By examining these scenarios, the paper will highlight the need for new legal frameworks to allocate responsibility fairly and effectively.

## II. RESEARCH METHODOLOGY

### A. STATEMENT OF RESEARCH PROBLEM

The incorporation of Contra Proferentem principle to effectively address consent, intent, and liability issues in AI-driven smart contracts.

### B. RESEARCH OBJECTIVE

The objective of the paper is to explore the impact of AI and blockchain on traditional contract law and to analyze the challenges to consent and intent, examine liability frameworks, evaluate consumer protection in AI-driven contracts, and assess the role of international law in addressing ambiguities in automated agreements, where unclear terms may lead to unfair disadvantages for one party, necessitating a standard that favors interpretations against the party that drafted the contract.

### C. RESEARCH QUESTIONS

1. How do traditional notions of consent and intent apply in AI-driven contracts, particularly concerning liability distribution among developers, users, and other stakeholders?
2. In what ways should consumer protection laws evolve to safeguard against potential abuses in AI-driven contract negotiations?
3. How should courts interpret smart contracts executed on blockchain to ensure fair liability allocation and mitigate ambiguities against the interests of less informed parties?
4. How can international harmonization of AI regulations address liability issues in smart contracts to promote fairness and consistency across jurisdictions?

 ISSN: 2582-6433

D. SCOPE AND LIMITATION OF THE STUDY

This study focuses on the intersection of AI, blockchain, and contract law, examining challenges related to consent, intent, liability, and consumer protection in automated negotiations. It explores the roles of stakeholders and the implications of smart contracts on traditional legal principles, while also addressing the need for transparency and international harmonization of regulations.

This study's limitations concern establishing liability and accountability in smart contracts. As AI technologies evolve, clarifying responsibility among stakeholders—developers, users, and AI systems—becomes complex. Furthermore, the rapid pace of technological change and varying interpretations of contract law across jurisdictions may affect the relevance of its findings in various legal contexts.

E. RESEARCH METHODOLOGY

The research method opted for this paper is Qualitative Research Methodology. This type of research that aims to gather and analyse non-numerical data in order to gain an understanding of individuals' social reality, including understanding their attitudes, beliefs, and motivation. We have reviewed papers on assessing the impact of AI on contract law and exploring emerging legal challenges, smart contracts and its functioning and the legal applicability in India and liability concerns in smart contracts and also consumers' difficulty in negotiating with automated systems.

## III. AUTOMATED DECISION-MAKING AND CONSENT

In the traditional legal framework, consent is a central pillar of contract law, requiring an informed and voluntary agreement by all parties involved. However, AI-driven contracts are often formed through automated processes, where algorithms analyze data, predict outcomes, and make decisions without direct human intervention. For example, an AI system in a financial trading platform can autonomously enter into binding agreements based on market conditions without human oversight. This raises the question: Can actions taken by AI be seen as reflecting genuine consent?

When AI forms a contract, the traditional notion of consent becomes ambiguous. AI systems lack consciousness and cannot truly understand or consent to the terms of a contract. Instead, they operate based on pre-programmed rules and data inputs. The decision-making process is automated, and the AI's "consent" is essentially a proxy for the instructions given by its human

 ISSN: 2582-6433

creators or operators. This creates a dilemma in legal terms: Should the responsibility for consent lie with the individual who deployed the AI, or with the AI's developers who programmed its decision-making capabilities?

**Principle of Contra Proferentem**

Contra proferentem is a rule of contract interpretation that states an ambiguous contract term should be construed against the drafter of the contract. The term contra proferentem is derived from a Latin phrase meaning "*against the offeror*."[1] This rule is used to protect parties who are forced to agree to a contract without being able to negotiate the terms. It's often used in cases involving insurance companies that refuse to pay claims. The rule is derived from the Latin phrase verba chartarum fortius accipiuntur contra proferentem, which means "ambiguous words should be construed against the offeror".[2] The rationale behind this doctrine emanates from the fact that parties to the agreement are often not in equal position. One party dominates the execution of the agreement while the other party merely signs on the dotted line. Such contracts are mainly "standard form take it or leave it" contracts. A special case of the application of the principle of good faith to the situation with smart contracts may be the principle, *contra proferentem*, allowing that, in the case of unclear contract terms and the absence of establishing a valid common will of the parties, the condition is interpreted by the court in favor of the counterparty of the party that prepared the draft of the agreement.[3]

Contra proferentem is still a vital precaution even as blockchain and artificial intelligence (AI) technologies advance contracts. This idea aids in balancing the power between the companies or developers who create these self-executing contracts and the users who, in many cases, lack the technical know-how to fully comprehend the code's ramifications. In order to preserve fairness and shield customers from deceptive tactics or unforeseen liabilities, it guarantees that any ambiguity in the contract's automated execution will be handled in favor of the party with less power over its terms.

**The Concept of Intent in AI-Driven Contracts**

The issue of intent is similarly complex. Intent in contract law involves a conscious decision

[1] Contra proferentem, Legal Information Institute, https://www.law.cornell.edu/wex/contra_proferentem
[2] Julie Young, Contra proferentem rule: How it works and examples Investopedia, https://www.investopedia.com/terms/c/contra-proferentem-rule.asp
[3] Consumer protection in the light of Smart Contracts, https://edit.elte.hu/xmlui/bitstream/handle/10831/86291/ELJ_+2021_1_web-95-105.pdf?sequence=1

 ISSN: 2582-6433

by parties to enter into a legal relationship. In AI-driven contracts, determining whose intent is represented can be problematic. Is it the intent of the person who programmed the AI, the entity that owns and operates it, or does the AI act with a form of intent of its own?

For instance, consider an AI system that autonomously negotiates and finalizes a supply chain agreement. The AI's decisions are driven by its algorithms, which are designed to maximize efficiency or cost savings. However, if the AI agrees to terms that the human user would not have accepted had they been involved directly, whose intent does this agreement represent? This ambiguity challenges the foundational legal requirement of a "meeting of the minds," where all parties must have a mutual understanding of the contract terms.

Here, the contra proferentem principle may be useful in settling disagreements of this kind. A legal principle known as contra proferentem states that any ambiguity in a contract should be read against the party that drafted it. This principle could be used by the court to hold the party who "programmed" or deployed the AI accountable if the AI-driven contract contains provisions that one party later challenges because of ambiguity or unexpected terms. In this sense, if the AI's controllers are seen to be the ones who drafted the contract, then any ambiguity resulting from the AI's decision-making could be read against them. When it comes to addressing the power disparity that arises during contract discussions between AI and humans, the application of contra proferentem could be a significant legal weapon.

**AI as an Agent in Contractual Relationships**

One way to conceptualize the role of AI in contracts is to view it as an "agent" acting on behalf of a principal, such as the user or organization deploying the AI. Traditional agency law allows agents to enter into contracts on behalf of principals, with the principal typically bearing the responsibility for the agent's actions. However, applying agency law to AI introduces several complications. Unlike human agents, AI systems lack the capacity for independent moral judgment and subjective decision-making. They operate purely based on their programming and the data they process.

This distinction raises the question of whether AI can truly serve as a legal agent. Should AI be seen merely as an advanced tool, with full legal liability falling on the principal who uses it? Or should we consider a new category of legal agency specific to AI, which accounts for its unique characteristics? For example, if an AI system inadvertently enters into an unfavorable contract due to a flaw in its algorithm, should the user be held responsible, or does some liability

 ISSN: 2582-6433

rest with the developer who created the flawed system? These questions highlight the need for legal clarity regarding the status of AI in contractual relationships.

The principle of contra proferentem may also apply when an AI's decision leads to unclear or unfavorable contract terms. If a dispute arises over contract interpretation, the court could favor the party lacking control over the AI's programming or operation. This implies that the AI's owner or creator could be held accountable for negative interpretations if they failed to account for certain contingencies in the AI's design. In this way, contra proferentem could protect parties affected by AI-driven contracts who lack technical expertise or control over the AI's decisions.

**Implications for Contract Validity and Enforceability**

The involvement of AI in contract formation also impacts the validity and enforceability of contracts. Traditionally, contracts are valid when there is a clear agreement between parties, backed by a mutual understanding of the terms.[4] With AI-driven contracts, achieving this "meeting of the minds" becomes more complex. AI systems might make decisions leading to contracts that one of the human parties later disputes, claiming they did not fully consent or intend to enter into the agreement.

For example, an AI system might automatically renew a subscription service based on user behavior patterns without explicit approval for each renewal. If the user disputes the renewal, arguing they did not intend to continue the service, the question arises whether a valid contract exists. Courts and legal scholars must consider how to interpret such cases, potentially requiring a redefinition of contract law principles to accommodate the automated nature of AI systems.

Courts may favor the user, arguing they were unaware of certain terms due to the AI's opaque process, helping to balance power dynamics when contracts are created by AI without real-time human input. Contra proferentem could resolve ambiguity in favor of a disputing party, especially if AI-generated terms are unclear or overly complex for a layperson.

[4](PDF) is a 'smart contract' really a smart idea? insights from a legal perspective, https://www.researchgate.net/publication/317354410_Is_a_'smart_contract'_really_a_smart_idea_Insights_from_a_legal_perspective

 ISSN: 2582-6433

## *IV. BLOCKCHAIN AND SMART CONTRACTS*

Building on the discussion of AI's role in contract formation and execution, blockchain technology introduces another layer of complexity into the legal framework, particularly through the use of smart contracts. Blockchain, a decentralized and distributed ledger system, allows for the creation of immutable, self-executing agreements, commonly known as smart contracts. These contracts automatically enforce themselves when certain conditions are met, eliminating the need for intermediaries like lawyers or notaries. While this offers significant efficiency and security benefits, it also raises questions about how traditional legal concepts such as contract interpretation, flexibility, and enforceability should be applied to smart contracts.

### Understanding Smart Contracts

A smart contract is essentially a computer program that directly controls the transfer of digital assets or executes other predefined actions based on specific conditions coded within the contract. [5]For example, a smart contract on a blockchain platform could automatically release payment to a supplier once goods have been delivered and confirmed. The key advantage of smart contracts is that they are tamper-proof and self-executing, reducing the potential for human error or manipulation.

However, smart contracts are fundamentally different from traditional contracts. In a traditional contract, parties negotiate terms and retain some flexibility in their interpretation and enforcement. In contrast, smart contracts execute strictly according to the coded instructions, leaving little room for interpretation or adjustment once the contract is deployed. This raises important questions about how courts and legal systems should interpret and enforce smart contracts, especially when disputes arise.[6]

When AI-generated contract conditions are ambiguous or disadvantageous, Contra proferentem may be applicable. Courts might favor the party without control over the AI's programming by interpreting ambiguity against the AI's developer or owner. This safeguards those who get AI-driven contracts but lack the technical know-how to completely comprehend

[5] Law School Policy Review, Are smart contracts really smart? Law School Policy Review & Kautilya Society (2024), https://lawschoolpolicyreview.com/2024/01/13/are-smart-contracts-really-smart/

[6] (No date a) *Georgetownlawtechreview*. Available at: https://georgetownlawtechreview.org/wp-content/uploads/2017/05/Raskin-1-GEO.-L.-TECH.-REV.-305-.pdf

 ISSN: 2582-6433

the conditions of the agreement.

**Legal Interpretation of Smart Contracts**

One of the central challenges with smart contracts is their rigidity. Unlike traditional contracts, which can be amended or renegotiated based on changing circumstances, smart contracts automatically enforce the terms as written, with no room for human judgment or discretion. This poses a problem if unforeseen circumstances occur, or if one of the parties realizes that the contract contains an error. For instance, if a smart contract automatically transfers funds based on faulty data or a misunderstanding of the terms, how should courts resolve the dispute?[7] Courts traditionally interpret contracts by considering the intent of the parties and the circumstances surrounding the agreement. However, smart contracts complicate this process because they are expressed in code, not legal language. This leads to questions such as:

- Is the code itself the final expression of the parties' intent?
- Should courts interpret the code as they would any written contract, or do they need to consider the technical execution of the code and its alignment with the original agreement?

For example, if a smart contract coded to automatically pay a contractor upon job completion fails to account for a scenario where the contractor does not complete the work to the agreed standard, how should a court intervene? Should the smart contract's automatic execution be halted, or should it be overridden by legal principles such as fairness or equity?

**Smart Contracts and the Traditional Elements of a Contract**

Smart contracts challenge the application of traditional legal principles like **offer, acceptance, and consideration**:

- **Offer and Acceptance**: In a smart contract, the terms are predetermined by the code, and the contract is executed automatically once the conditions are met. However, the lack of a traditional negotiation process raises the question of whether there is a true "offer" and "acceptance" in the legal sense, or whether the execution of the contract is simply a technical fulfillment of pre-programmed instructions.
- **Consideration**: The exchange of value (consideration) is a fundamental element of traditional contracts. In smart contracts, the transfer of assets or services happens

[7] Authors *et al.* (2019) *The enforceability of smart contracts in India*, *Contracts and Commercial Law - Corporate/Commercial Law - India*. Available at: https://www.mondaq.com/india/contracts-and-commercial-law/874892/the-enforceability-of-smart-contracts-in-india

 ISSN: 2582-6433

automatically, which fulfills the consideration requirement. However, if the coded terms do not reflect the true intentions or expectations of one party, disputes could arise about whether valid consideration was exchanged.[8]

**Enforceability and Dispute Resolution**

A major challenge with smart contracts is their enforceability, especially when disputes arise from unexpected outcomes. The immutable nature of blockchain makes it difficult to reverse executed contracts.[9] For example, if a smart contract erroneously transfers property ownership, traditional contract law offers remedies for fraud or misrepresentation, but smart contracts lack this flexibility. One proposed solution is hybrid contracts, which blend traditional legal language with smart contract code, allowing courts to resolve disputes based on the parties' original intent while leveraging blockchain's benefits. Courts may also need new standards to interpret smart contracts effectively.

**Smart Contracts and Jurisdictional Challenges**

Because blockchain networks are decentralized and often operate across national borders, smart contracts present significant jurisdictional challenges. For example, if a dispute arises from a smart contract executed on a blockchain that spans multiple countries, which legal system has the authority to resolve the dispute? Unlike traditional contracts, where jurisdiction is typically established based on the location of the parties or the nature of the transaction, blockchain-based smart contracts can complicate the determination of applicable law.

This lack of clarity creates a need for **international cooperation** and potentially new legal frameworks to address cross-border disputes arising from smart contracts. Regulatory bodies may need to develop harmonized rules or protocols to ensure that smart contracts are enforceable across different jurisdictions while protecting the rights of all parties involved.

***Liability in AI and Blockchain-Driven Contracts***

As AI and blockchain technologies continue to reshape contract formation and execution, one of the most significant legal challenges that arises is the issue of **liability**. When traditional contracts are breached, or when harm results from a contractual relationship, the responsible

[8] Briefing, I. (2022) *What are smart contracts and are they legal in India?*, *India Briefing News*. Available at: https://www.india-briefing.com/news/what-are-smart-contracts-and-are-they-legal-in-india-25343.html/

[9] Guest, Guest and Says:, V. (2017) *The legality of smart contracts in India*, *IndiaCorpLaw*. Available at: https://indiacorplaw.in/2017/12/legality-smart-contracts-india.html

 ISSN: 2582-6433

party is usually clear. However, with AI systems autonomously making decisions and blockchain smart contracts executing automatically, determining liability becomes more complex.[10] This section explores the potential liability of various stakeholders, including AI developers, users, and platform operators, and considers how legal frameworks might evolve to address these issues.

**Liability in AI-Driven Contracts**

In traditional contract law, liability typically falls on the party who breaches the agreement or causes harm. With AI-driven contracts, however, the question of who should be held responsible is less straightforward. Since AI systems make autonomous decisions, the liability for any errors or breaches could fall on multiple parties, depending on how the AI was used, designed, or maintained.

***Liability of Developers***

Developers who create AI systems play a central role in their functionality, and their work directly influences how AI behaves in contractual scenarios. If an AI system fails due to a coding error, leading to a breach of contract or other negative outcomes, one might argue that the developer should bear liability for the malfunction. This is particularly relevant in cases where AI systems contain defects or bugs that cause them to act in ways that deviate from the intended contractual obligations.

For instance, if an AI system used for financial trading inadvertently executes trades that violate a contract due to a programming flaw, should the developer be held liable for the damages? Current laws generally protect developers from liability under certain circumstances, particularly if they are not directly involved in the contract. However, as AI systems become more autonomous, there may be a need for stricter accountability mechanisms that address the role of developers in ensuring their systems function reliably in contractual settings.

***Liability of Users***

Users who deploy AI systems also face potential liability, especially when they rely on AI to make contractual decisions on their behalf. While the user may not have direct control over

[10] *Contract management blockchain use cases with AI-powered negotiations* (no date) *Legal Tech News & Contract Management Tips*. Available at: https://blog.lexcheck.com/contract-management-blockchain-use-cases-with-ai-powered-negotiations-lc

 ISSN: 2582-6433

every decision the AI makes, they are responsible for the outcomes that result from the AI's actions. For example, if a company uses an AI system to negotiate contracts and the AI agrees to unfavorable or illegal terms, the company may be held liable for the resulting breach, even though the AI acted autonomously.

The key legal question is whether users can be expected to fully understand and predict the actions of complex AI systems, particularly those that learn and evolve through machine learning algorithms. Should users be liable for actions taken by AI that were not reasonably foreseeable? Courts and lawmakers may need to establish clearer guidelines on the extent to which users are responsible for the behavior of the AI systems they employ.[11]

***Shared Liability***

In many cases, liability may be shared between developers and users. If an AI system malfunctions due to both a coding error and improper usage by the user, determining liability may involve a detailed investigation into the specific causes of the failure. Legal frameworks will need to evolve to address situations where multiple parties contributed to the breach or harm.[12]

For example, if a smart contract managed by an AI fails to execute properly because the developer's code did not account for certain variables and the user configured the system inappropriately, both parties may bear partial responsibility. Courts could apply principles of contributory or comparative negligence to allocate liability between the parties based on their respective roles in the failure.

***Product Liability and AI***

Another approach to AI liability is through the lens of product liability. If AI systems are treated as products, developers and manufacturers could be held liable under existing product liability laws. This would mean that if an AI system causes harm due to a defect or failure in its design or manufacturing, the party responsible for creating and distributing the AI could be liable for damages. However, applying product liability law to AI systems raises challenges, as the

[11] *Artificial Intelligence - who is liable when AI fails to perform?* (no date) *Artificial Intelligence – Who is liable when AI fails to perform? Insight | Technology, Media & Telecommunications | United Kingdom | International law firm CMS*. Available at: https://cms.law/en/gbr/publication/artificial-intelligence-who-is-liable-when-ai-fails-to-perform

[12] *Who is liable when the use of AI leads to harm?* (no date) *Wikborg Rein*. Available at: https://www.wr.no/en/news/who-is-liable-when-the-use-of-ai-leads-to-harm

 ISSN: 2582-6433

dynamic and evolving nature of AI may not fit neatly within traditional product categories.

Product liability law typically applies to physical goods, but AI systems are often intangible, consisting of software and algorithms that can change over time through updates and machine learning processes. [13]This raises the question of whether developers should be held liable for how their AI systems behave after they have been sold or deployed, especially if the AI continues to learn and adapt in ways that were not anticipated at the time of sale.[14]

***Platform Liability and Decentralization***

Blockchain's decentralized nature also complicates liability issues. Since there is no central authority or intermediary overseeing the execution of smart contracts, it is difficult to hold any single entity accountable when something goes wrong. Blockchain platforms typically provide the infrastructure for smart contracts but do not control or monitor individual transactions, which raises questions about their liability.

If a smart contract fails due to a flaw in the blockchain platform itself, could the platform operators be held liable? Given that many blockchain networks operate through decentralized consensus mechanisms, attributing liability to any one party is challenging. This could necessitate the development of new legal frameworks that address liability in decentralized environments, potentially involving collective responsibility or insurance mechanisms to cover damages.

***Algorithmic Bias and Discrimination in AI-Driven Contracts***

As AI systems increasingly take on roles in contract formation and decision-making, concerns about **algorithmic bias and** discrimination have emerged. AI systems, especially those utilizing machine learning algorithms, often rely on vast datasets to inform their decisions. However, these datasets can reflect societal biases, leading to discriminatory outcomes in AI-driven contracts. This section explores the risks of bias in AI, the legal implications of discrimination in contract law, and the potential safeguards that can be put in place to mitigate these risks.

[13] *The Artificial Intelligence Liability directive* (no date) *The Artificial Intelligence Liability Directive*. Available at: https://www.ai-liability-directive.com/

[14] Pallardy, R. (2024) *Ai is creating new forms of liability. how can it be managed?*, *InformationWeek*. Available at: https://www.informationweek.com/machine-learning-ai/ai-is-creating-new-forms-of-liability-how-can-it-be-managed-

 ISSN: 2582-6433

**The Problem of Algorithmic Bias**

Algorithmic bias occurs when an AI system systematically favors or disadvantages certain groups based on characteristics such as race, gender, or socioeconomic status. These biases often stem from the data used to train the AI system. For example, if an AI system used in contract negotiation or loan agreements is trained on historical data that reflects discriminatory practices (such as higher loan rejection rates for minority groups), the AI may replicate or even amplify these biases in its decision-making processes.[15]

AI does not have inherent intent or awareness, but it can perpetuate biases that exist in the data it processes. This is particularly concerning in contexts where AI systems are involved in contractual decisions, such as determining who is offered favorable terms in a commercial contract or deciding on pricing strategies in supply chains. If left unchecked, algorithmic bias could result in systemic discrimination, reinforcing social inequalities.[16]

**Discrimination in Contract Law**

Discrimination in contract law is generally prohibited by legal frameworks that protect individuals and groups from unfair treatment based on characteristics such as race, gender, age, religion, or disability. In the context of AI-driven contracts, there is a growing need to apply these anti-discrimination principles to automated systems.

For instance, an AI system used in employment contract negotiations might offer higher wages or better terms to male candidates compared to female candidates due to biased training data that reflects historical wage disparities. Such outcomes would violate anti-discrimination laws, even though the AI system itself lacks intent to discriminate. The question then becomes: Who is responsible for the discriminatory actions of the AI? Is it the company that deployed the AI, the developer who programmed it, or both?

Courts will need to grapple with these questions as AI becomes more embedded in the contract formation process. Traditional legal concepts of discrimination may need to be adapted to address the fact that AI systems can engage in discriminatory practices without human involvement or intent.

[15] Engler, A. *et al.* (2023) *Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms, Brookings*. Available at: https://www.brookings.edu/articles/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/

[16] Ofori, D.A. (2023) *Navigating the AI and web3 revolution: Emerging frontiers in contract law, Revolutionizing Contract Law: The Impact of AI and Web3*. Available at: https://www.linkedin.com/pulse/navigating-ai-web3-revolution-emerging-frontiers-law-asare-ofori

 ISSN: 2582-6433

**Regulatory Frameworks for Addressing Bias in AI**

To address the risks of algorithmic bias in AI-driven contracts, there is a growing call for regulatory frameworks that ensure AI systems are fair, transparent, and accountable. Some key approaches include:

***Data Audits and Transparency***

One way to mitigate algorithmic bias is through regular **data audits**. By analyzing the data used to train AI systems, developers and users can identify potential biases and take corrective action before the AI is deployed. These audits should focus on ensuring that the data is representative of diverse populations and free from historical biases that could lead to discriminatory outcomes.

In addition, there is a need for greater **transparency** in how AI systems make decisions. In many cases, the decision-making process of AI is opaque, even to the people who design or use the systems. This is particularly true for AI systems that rely on deep learning, where the "black box" nature of the algorithms makes it difficult to understand how specific decisions are made. Ensuring that AI systems used in contractual processes are explainable and transparent can help prevent bias from influencing outcomes.

***Algorithmic Fairness Standards***

Governments and regulatory bodies are also exploring the creation of **algorithmic fairness standards** to ensure that AI systems operate without discrimination. These standards could include requirements for developers to test their AI systems for bias and to document the steps they have taken to address potential discriminatory outcomes. In some cases, algorithms could be required to meet certain fairness thresholds before they are allowed to be used in contract negotiations or other legal contexts.

For example, an AI system used in lending decisions could be required to demonstrate that it does not disproportionately reject loan applications from minority groups. Similarly, AI systems involved in hiring contracts could be tested to ensure that they do not favor one gender over another.

***Legal Recourse for Affected Parties***

When algorithmic bias leads to discriminatory outcomes in AI-driven contracts, affected

 ISSN: 2582-6433

parties must have access to **legal recourse**. This could involve giving individuals the right to challenge AI-driven decisions that they believe were discriminatory, much like they would challenge discriminatory actions taken by human decision-makers. However, this raises the issue of how individuals can effectively challenge AI decisions when the decision-making process is often opaque.

To facilitate legal challenges, courts may need to require AI developers and users to provide greater transparency regarding how the AI system arrived at its decisions. This could involve disclosing the data used to train the AI, the algorithms employed, and any fairness checks that were performed. By making this information available, individuals can better assess whether they were subject to discriminatory practices.

**Preventing Algorithmic Bias Through Human Oversight**

One of the most effective ways to prevent algorithmic bias in AI-driven contracts is through **human oversight**. AI systems should not be given complete autonomy in contractual decision-making, particularly in situations where bias could have significant negative consequences. By involving humans in the final decision-making process, organizations can ensure that AI-generated outcomes are reviewed for fairness and compliance with anti-discrimination laws.

The legal principle of contra proferentem can be a useful instrument for resolving the ambiguities and complexity of contracts based on blockchain technology and artificial intelligence. In cases where ambiguities occur in terms of agreements generated or executed by AI or smart contracts, contra proferentem could guarantee that the party in charge of the AI's deployment or design is held accountable for any ambiguities that may develop. By protecting users and other parties who lack technical knowledge or control over the AI's decision-making, this would uphold accountability and justice in the rapidly developing field of AI-driven contracts.

## V. INTERNATIONAL HARMONIZATION OF AI REGULATIONS

Given that AI systems and blockchain networks often operate across borders, there is a growing need for **international harmonization** of laws and regulations governing AI in contracts. Different countries have varying legal standards when it comes to anti-discrimination and data protection, which can lead to confusion and uneven outcomes when AI-driven contracts are used in global business transactions.

 ISSN: 2582-6433

For instance, an AI system used to negotiate contracts in multiple countries might comply with anti-discrimination laws in one jurisdiction but not in another. To address this, international organizations such as the United Nations or the European Union could work towards developing harmonized legal standards that ensure AI systems are fair and transparent, regardless of the jurisdiction in which they operate.

***International Harmonization of Law for Regulating AI in Contracts***

As AI technologies rapidly evolve and are adopted globally, the need for **international harmonization** of legal frameworks becomes critical. This section explores the challenges and opportunities presented by differing legal standards across jurisdictions and the necessity for cohesive regulations that address the unique aspects of AI in contract law.[17]

**Challenges of Jurisdictional Differences**

Different countries have varying approaches to AI regulation, resulting in a patchwork of laws that can complicate cross-border transactions.[18] This inconsistency can create uncertainty for businesses and consumers engaging with AI-driven contracts, particularly regarding liability, consumer protection, and data privacy.

1. **Diverse Legal Frameworks**: Nations may implement distinct legal standards regarding AI technologies, leading to challenges in enforcing contracts across borders. For instance, a smart contract executed in one jurisdiction may face legal scrutiny in another where the definitions of liability and consent differ significantly.
2. **Varying Approaches to Consumer Protection**: Consumer protection laws vary widely, impacting how AI systems interact with consumers. Some jurisdictions may prioritize strong protections against algorithmic bias and unfair practices, while others may have minimal regulations. This disparity can lead to consumer exploitation or discrimination in markets that cross borders.

**Opportunities for Harmonization**

The globalization of technology calls for cooperative efforts among nations to establish common standards that can govern AI's use in contracts. Several initiatives and frameworks

[17]Ofori, D.A. (2023) *Navigating the AI and web3 revolution: Emerging frontiers in contract law, Revolutionizing Contract Law: The Impact of AI and Web3*. Available at: https://www.linkedin.com/pulse/navigating-ai-web3-revolution-emerging-frontiers-law-asare-ofori

[18] Mistry, J. (2024) *Ai takes the Gavel: Contract laws' new sidekick in Automated Decision-making, SSRN*. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4786945

 ISSN: 2582-6433

can be explored:

1. **International Treaties and Agreements**: Countries can collaborate to create binding international treaties focused on AI regulation. These treaties can outline fundamental principles, such as fairness, transparency, and accountability in AI-driven contracts, providing a baseline for member states.
2. **Model Laws and Guidelines**: Organizations such as the **United Nations** or the **International Institute for the Unification of Private Law (UNIDROIT)** could develop model laws that countries can adopt or adapt to their legal systems. These model laws could address issues like liability in AI contracts, consumer protection, and dispute resolution.
3. **Cross-Border Regulatory Bodies**: Establishing international regulatory bodies focused on AI can facilitate cooperation and knowledge-sharing among countries. These bodies can help ensure that regulatory practices evolve alongside technology and that stakeholders have a platform to voice concerns.

Such harmonization efforts could include developing global standards for algorithmic fairness, transparency, and accountability, making it easier for businesses to deploy AI systems across borders while ensuring compliance with anti-discrimination laws.

## VI. CONSUMER PROTECTION AND AI-DRIVEN CONTRACT NEGOTIATION

As AI becomes more embedded in contract negotiations, particularly in the consumer space, new legal challenges emerge related to **consumer protection**. In AI-driven contract negotiations, consumers may face a power imbalance when interacting with automated systems, potentially leading to exploitation, unfair terms, or lack of transparency. This section examines how AI can create new risks in consumer contract negotiations, the legal frameworks that can protect consumers, and how laws might be adapted to address the specific issues posed by AI and blockchain technologies.[19]

### AI in Consumer Contracts: Risks and Challenges

AI systems are increasingly being used to negotiate contracts on behalf of businesses and consumers, especially in online transactions. For instance, AI can be employed to set dynamic

[19] *Artificial Intelligence (AI) act: Council gives final green light to the first worldwide rules on AI - Consilium*. Available at: https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/

 ISSN: 2582-6433

pricing, offer tailored contract terms, or even determine eligibility for services such as loans or insurance. While these technologies can increase efficiency and personalization, they also introduce risks for consumers, particularly in terms of **information asymmetry** and **power imbalances**.

***Information Asymmetry***

AI systems have access to vast amounts of data, allowing businesses to tailor contract terms and pricing to individual consumers. This could create significant **information asymmetry**, where the business has a deep understanding of the consumer's behavior, preferences, and willingness to pay, while the consumer lacks full knowledge of the AI's decision-making processes.

For example, an AI system might determine that a consumer is willing to pay a higher price for a product based on their browsing history or purchasing behavior, leading to **discriminatory pricing** practices. Similarly, AI could offer contract terms that benefit the business but disadvantage the consumer, without the consumer fully understanding the implications of those terms.

This information imbalance can undermine **informed consent**, a fundamental principle of contract law. For a contract to be valid, both parties must understand and agree to its terms. However, when AI systems are involved, consumers may not fully grasp how the terms were generated or the factors that influenced them, leading to questions about whether true consent was given.

***Lack of Transparency***

Another challenge is the **lack of transparency** in AI-driven negotiations. AI systems often operate as "black boxes," making decisions based on complex algorithms that are not easily understood by the average consumer. This lack of transparency can make it difficult for consumers to know whether they are being treated fairly, and it can prevent them from challenging unfair contract terms or practices.

For instance, if an AI system offers a consumer a contract with unfavorable terms, the consumer may not know how the AI arrived at those terms or whether the AI considered all relevant factors. This lack of clarity can erode trust and leave consumers vulnerable to exploitation.

 ISSN: 2582-6433

**Legal Frameworks for Consumer Protection**

To address these risks, legal frameworks must evolve to provide greater **consumer protection** in the context of AI-driven contracts. Traditional consumer protection laws, which are designed to protect individuals from unfair or deceptive practices, need to be adapted to account for the unique challenges posed by AI systems. Key areas of focus include ensuring fairness in contract terms, promoting transparency, and providing avenues for consumers to challenge AI-generated decisions.

***Ensuring Fairness in AI-Driven Contracts***

One of the primary concerns with AI-driven contracts is ensuring that the terms offered to consumers are **fair** and **non-exploitative**. Current consumer protection laws, such as those governing unfair contract terms, can be applied to AI-driven contracts, but additional safeguards may be necessary to ensure that AI systems do not take advantage of consumers' lack of knowledge or bargaining power.

For example, businesses using AI systems to negotiate contracts with consumers could be required to ensure that the terms are balanced and do not disproportionately benefit the business at the consumer's expense. Regulators could introduce rules that prevent AI systems from offering predatory terms, such as hidden fees or overly restrictive conditions, particularly in industries like insurance, finance, and e-commerce.

Furthermore, AI systems could be required to **explain** the reasoning behind their decisions, allowing consumers to better understand why certain terms were offered and whether they are fair. This could involve providing consumers with a clear, human-readable summary of the key factors that influenced the AI's decisions, helping to reduce the information asymmetry that currently exists.

***Algorithmic Transparency***

Transparency is crucial for protecting consumers in AI-driven negotiations. **Algorithmic transparency** involves making the processes and decision-making criteria of AI systems more understandable and accessible to consumers. By requiring businesses to disclose how their AI systems operate, regulators can help ensure that consumers are not disadvantaged by hidden algorithms or opaque decision-making processes.

 ISSN: 2582-6433

For example, businesses using dynamic pricing algorithms could be required to disclose the factors that influence pricing decisions, such as market demand, consumer behavior, or time-sensitive factors. This would allow consumers to make more informed decisions and protect themselves from discriminatory or unfair pricing practices.

In addition to transparency about the AI's decision-making process, businesses could also be required to conduct **bias audits** on their AI systems. These audits would ensure that the AI is not unfairly discriminating against certain consumers based on characteristics such as race, gender, or socioeconomic status.

***Right to Challenge AI Decisions***

A key principle of consumer protection is the **right to challenge** unfair or exploitative practices. In the context of AI-driven contracts, consumers must have the ability to contest decisions made by AI systems, particularly if they believe those decisions were based on incorrect information or unfair biases.

One possible legal solution is to grant consumers a **right to explanation** and a **right to appeal** AI-generated decisions. For example, if an AI system denies a consumer a loan or offers unfavorable contract terms, the consumer should have the right to request a detailed explanation of how the decision was made and challenge the decision if they believe it was unfair. This would require businesses to provide more transparency in their AI systems and to ensure that there are human review processes in place to handle disputes.

Additionally, regulators could create **ombudsman** services or other independent bodies that consumers can turn to if they believe they have been treated unfairly by an AI system. These bodies could investigate complaints and provide consumers with a means of seeking redress.

***Preventing Cartel-Like Behavior in AI-Driven Negotiations***

One of the more novel risks associated with AI in contract negotiations is the potential for **collusion** or **cartel-like behavior**. AI systems, particularly in industries where businesses use similar technologies to set prices or negotiate terms, could inadvertently learn to collude with one another, leading to higher prices or less favorable contract terms for consumers.[20]

[20] Oecd (2021) *Competition and ai*, *OECD iLibrary*. Available at: https://www.oecd-ilibrary.org/finance-and-investment/oecd-business-and-finance-outlook-2021_3acbe1cd-en;jsessionid=x3V7mHQe2tRoTRScFNrwomcs2Kd-Fnuuq8fIfVa7.ip-10-240-5-95

 ISSN: 2582-6433

For instance, if multiple businesses in the same market use AI to set prices, there is a risk that these AI systems could identify patterns in each other's pricing strategies and adjust their prices accordingly, leading to a form of price-fixing. This would harm consumers by reducing competition and leading to higher costs.

To prevent such outcomes, regulators may need to develop new rules to govern how AI systems interact in the marketplace. This could include monitoring AI systems for signs of collusion or requiring businesses to implement safeguards that prevent their AI from engaging in cartel-like behavior. Additionally, competition authorities may need to adapt their enforcement strategies to account for the fact that AI systems can facilitate anti-competitive practices, even if there is no human intent behind the behavior.

In AI-driven consumer contract presentations, where knowledge asymmetry and a lack of transparency frequently leave consumers vulnerable, the contra proferentem principle can provide a useful defense. Given that consumers have no control over the AI's decision-making process, contra proferentem may be used to construe unclear or unjust terms produced by AI systems in the consumer's favor. By guaranteeing that any ambiguous clauses or deceptive contract terms are decided against the party having more control and comprehension of the AI, usually the business, this would assist alleviate the power imbalance.

## VII. SUGGESTIONS

***Navigating the Future of Contract Law in the Age of AI and Blockchain***

The rise of AI and blockchain technologies is reshaping contract law, necessitating a reevaluation of concepts like consent, intent, and liability. Clear guidelines are needed to establish responsibility in AI-driven contracts. Consumer protection laws must adapt to ensure transparency and fairness in automated negotiations. Additionally, international legal harmonization is crucial to facilitate cross-border transactions. Courts will need new frameworks to address the complexities of smart contracts, balancing automated execution with principles of equity and justice. Overall, a collaborative approach is essential to navigate this evolving legal landscape effectively.

 ISSN: 2582-6433

## VIII. CONCLUSION

In the future, the concept of contra proferentem can be extremely important in safeguarding parties with less control or knowledge of new technologies, as AI and blockchain continue to change contract law. Contra proferentem guarantees that conditions of contracts that are unclear or disadvantageous because of AI's decision-making are interpreted against the party who drafted or controlled the AI, usually to the advantage of the more vulnerable party. It is essential to have protections like contra proferentem in contract law as AI and blockchain become more integrated in order to preserve accountability, justice, and transparency in this changing legal environment.

The future of contract law in the age of AI and blockchain holds both promise and challenges. As these technologies evolve, so too must the legal frameworks that govern them. Policymakers, legal scholars, and industry stakeholders must collaborate to create adaptive, forward-thinking regulations that prioritize fairness, transparency, and accountability. To navigate this rapidly changing landscape, ongoing dialogue and interdisciplinary approaches will be essential. By embracing innovation while ensuring that core legal principles are upheld, society can harness the benefits of AI and blockchain technologies to enhance contractual relationships and foster trust in digital transactions. Ultimately, the successful integration of AI and blockchain into contract law will depend on our ability to balance technological advancement with ethical and legal considerations, ensuring that these powerful tools serve the interests of all parties involved.