INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW
An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 4 | Issue 3 | 2025 Art. 57

Contracting in the Age of Smart Contract

Vaishnavi P
Law Student, BA.LLB (Hons.)
Amity Law School, Amity University, Bengaluru

Dr. Shobha Yadav
Assistant Professor,
Amity Law School, Amity University, Bengaluru

Recommended Citation
Vaishnavi P and Dr. Shobha Yadav, *Contracting in the Age of Smart Contract*, 4 IJHRLR 813-830 (2025).
Available at www.humanrightlawreview.in/archives/.

Contracting in the Age of Smart Contract

Vaishnavi P
Law Student, BA.LLB (Hons.)
Amity Law School, Amity University, Bengaluru

Dr. Shobha Yadav
Assistant Professor,
Amity Law School, Amity University, Bengaluru

Manuscript Received	Manuscript Accepted	Manuscript Published
21 May 2025	28 May 2025	05 June 2025

ABSTRACT

The rise of blockchain technology and the integration of smart contracts have reshaped how parties engage in contractual relationships. Unlike traditional agreements grounded in legal language and judicial interpretation, smart contracts execute automatically upon satisfaction of coded terms. While these technological tools promise efficiency, security, and trustlessness, they also challenge classical legal frameworks. This paper explores the definition, legal validity, and enforceability of smart contracts in the Indian and global legal context. It delves into pertinent legislation, case laws, limitations, and the evolving role of legal professionals in a digital era. The objective is to provide a holistic understanding of how law can adapt to emerging technologies without compromising legal safeguards.

KEYWORDS

Smart Contracts, Blockchain, Contract Law, Legal Technology, Automation, Indian Contract Act, Enforceability, Code as Law, Legal Reform

INTRODUCTION

Contract law forms the bedrock of commercial interactions. As technology advances, traditional legal systems are constantly challenged to accommodate new modalities of agreement. Among these, smart contracts—self-executing agreements written in code and deployed on blockchain platforms—represent a paradigm shift. Originally conceptualized by cryptographer Nick Szabo, smart contracts enable transactions without intermediaries, governed entirely by pre-set digital rules. While the code may replicate the logic of traditional contracts, it raises questions

about consent, interpretation, enforcement, and jurisdiction.

This paper aims to analyze how contracting has evolved in the age of smart contracts, particularly in the Indian legal context, and identifies reforms required to make legal systems compatible with technological innovation.

UNDERSTANDING SMART CONTRACTS

A smart contract is a software protocol that digitally facilitates, verifies, or enforces a contract. They are deployed on blockchain platforms such as Ethereum and automatically execute actions when pre-defined conditions are met.

Key Features

- Reduces human error and manual processing.
- Code cannot be altered once deployed.
- All parties have access to the same data.
- Eliminates the need for intermediaries.

However, unlike traditional contracts, smart contracts often lack natural language expression, leading to ambiguity in interpretation and enforceability.

SMART CONTRACTS UNDER THE INDIAN CONTRACT ACT, 1872

To be enforceable under Indian law, a contract must fulfill the criteria under the Indian Contract Act, 1872, particularly:

- Section 2(h): A contract is an agreement enforceable by law.
- Section 10: Requires free consent, lawful consideration, lawful object, and competence of parties.
- Section 11: Addresses competency to contract.
- Section 13 & 14: Deal with consent and free will
- Section 23: Validity of the object of the agreement.

Although not explicitly codified in Indian law, smart contracts may fulfill these criteria if supported by mutual consent, consideration, and lawful purpose. However, questions arise regarding the understanding of code-based agreements by laypersons—can consent truly be free and informed if parties do not understand the language of execution?.

ENFORCEABILITY CHALLENGES

While smart contracts are legally binding in theory, several

hurdles exist:

1. **Consent and Interpretation**

Can parties be said to consent to what they do not understand? If a contract is written in Solidity (Ethereum's programming language), only coders might comprehend its terms. This poses a challenge to Section 13 of the Contract Act, which emphasizes meeting of minds**.**

2. **Mistake and Coercion**

Sections 20-22 of the Indian Contract Act deal with contracts made under mistake or misrepresentation. In smart contracts, bugs or coding errors could lead to serious financial consequences without recourse**.**

3. **Performance and Breach**

Smart contracts self-execute, but what happens in cases of force majeure, fraud, or partial performance? Since there is no centralized arbiter, such disputes may need to be resolved outside the code—contradicting the premise of automation.

LANDMARK PRECEDENTS

- **The DAO Hack (2016) – Unreported, Ethereum Blockchain**

This event wasn't litigated traditionally but sparked massive debate. A smart contract on Ethereum allowed a hacker to exploit a code vulnerability and siphon $50 million worth of Ether. The community decided to "hard fork" the blockchain to recover funds, illustrating that code is not always law, and human governance may override automated contracts.

- **State of Maharashtra v. Dr. Praful B. Desai (2003)**

Though not directly about smart contracts, this case by the Supreme Court of India accepted video conferencing as valid for legal procedures, showing judicial openness to technological advancement.

- **Trimex International FZE v. Vedanta Aluminium Ltd. (2010)**

The Supreme Court upheld an agreement formed over email, recognizing electronic communications as valid contracts under the Information Technology Act, 2000. This could be interpreted to extend to smart contracts if intention and

consent are present.

GLOBAL LEGAL PERSPECTIVES

- **United States**

The Uniform Electronic Transactions Act (UETA) and the Electronic Signatures in Global and National Commerce Act (E-SIGN) provide a framework for recognizing electronic contracts and signatures. States like Arizona and Nevada have passed laws explicitly recognizing blockchain-based records and smart contracts.

- **United Kingdom**

The UK Law Commission (2021) released a report stating that smart contracts can be interpreted and enforced using existing legal principles. They emphasized the importance of intent and ability to convert code into legal obligations.

- **European Union**

Under the eIDAS Regulation, electronic contracts and blockchain are being actively explored for cross-border commerce. However, uniform regulation on smart contracts is still in progress.

SMART CONTRACTS AND THE IT ACT, 2000 (INDIA)

- Section 10A of the IT Act recognizes the validity of electronic contracts formed through electronic means.
- Section 2(1)(ta) includes "digital signature" which could, in theory, be extended to blockchain-based identity verification.
- This gives a potential statutory basis for smart contracts under Indian law, though explicit reference to blockchain is still absent.

ETHICAL AND JURISDICTIONAL CONCERNS

- Lack of Consumer Protection: Contracts involving laypersons may exploit their lack of technical knowledge.
- Cross-Border Disputes: Blockchain operates globally, complicating jurisdiction and enforcement.
- Irrevocability: Once executed, smart contracts cannot be reversed easily, which may lead to inequitable outcomes.

THE FUTURE: HYBRID LEGAL-TECH CONTRACTS

An emerging solution is Ricardian Contracts—documents that

combine natural language (for human understanding) with code (for execution). This balances automation and interpretability. Lawyers must evolve to work alongside developers to ensure that digital agreements uphold legal principles.

Legal education and reform should include:

- Code literacy for lawyers
- Ethical AI and automation modules
- Smart contract auditing standards

LIMITS OF EXISTING LEGAL THEORIES OF SMART CONTRACTS

As discussed, smart contracts consist of "a set of promises, specified in digital form, including protocols within which the parties perform on these promises." In other words, smart contracts—embedded in a blockchain—can automatically receive and send assets and information. For smart contracts to work, parties' obligations should be well thought-out and ingrained in a self-executing code (e.g., if/then). Vending machines are the often-given analogy for smart contracts where parties' obligations are carefully pre-determined. All that is needed to trigger the contract is a dollar bill. Contracts are therefore simple and binary (e.g., if a dollar bill, then soda).

Smart contracts further take the automated feature of a vending machine further. In vending machines, only one party's performance is automated (i.e., the vending machine's). In smart contracts, however, both parties' performance of obligations is automated with no future obligations remaining to be executed. Moreover, in smart contracts, parties can even delegate the very conclusion of contracts to electronic agents and their obligations can be "synchronous," unlike the asynchronous relationship between a vending company and a consumer. In these limited contracts, therefore, there are only broken codes, not bargaining nor broken promises. Disputes can arise out of unforeseen coding errors or hacks. As a result, smart contracts include "occasional earthquakes" rather than "continual linguistic drift" that is inherent in traditional contracting.

In the last several decades, contract theory has focused on three paradigms for theorizing about the enforceability of contracts: promisor, promisee, and socio-economics surrounding the transaction. The bargain theory states that the promisor's manifested intention to create legal relations results in contractual obligations and is the basis of enforceability of contracts. This theory has also stressed the element of exchange in which only reciprocal promises are enforceable.

The reliance theory, on the other hand, shifts the focus onto the reliance made by the promisee as a result of a promise. Under this view, contracts are enforceable because people rely on the promises they receive. The last paradigm centers on the efficiency resulting from an exchange of promises (law-and-economics) or the shared public norms such as coordinating conduct (relational contract theory).

Legal scholars have debated the legal nature of smart contracts. Some believe smart contracts are neither smart nor contracts in part because parties may enter into legal obligations without "knowing it or intending to." This view is reinforced by the fact that smart contracts "are simply business rules encoded in software" and therefore are "not legally binding without contractual agreements." Some believe that smart contracts are contracts "at the conceptual level" but do not necessarily constitute exchange of promises per se.

Some point to the limited role of law in smart contracts because there is no entry point for legal intervention in these contracts. Others have categorized smart contracts based on the role of the algorithm. Depending on whether the algorithm is a gap-filler or a negotiator (tool or agent), the legal nature of such contracts differs. Some have criticized that smart contracts eliminate the social function of the act of contracting because the "technology of smart contracts neglects the fact that people use contracts as social resources to manage their relations."

Moreover, contracts are purported to be the main avenue for private lawmaking where individuals can solve their problems and regulate their behavior at the micro level. Such private lawmaking becomes automated and atomized with smart contracts. Smart contracts are also not reliant on third-party intermediaries or human agency for their execution.

The critique of smart contracts therefore comes from both legal and social angles. The skepticism towards smart contracts in law derives in large part from the nature of smart contracts that aim to resolve all issues ex ante and leave little to no room for corrective measures ex post. Smart contracts are entirely reliant on "ex ante formalizations, which can never match the flexibility of ex post human decision-making." In other words, it is the lack of human connection and decision-making that has in part sparked the skepticism about the legal and social nature of smart contracts.

These studies have largely focused on the immutability and automation of smart contracts while overlooking the distributed aspects of smart contracts. The distributed function enables new

methods of contract-making and resolution of disputes. This Part surveys the various approaches to the nature of smart contracts while providing fresh insights.

A. No Contract

Assent is a foundational requirement for contracts. Contract law requires mutual assent between parties or a "meeting of the minds." With the advancement of technology, it was this requirement that led some to believe that smart contracts are not contracts since they lack human assent. Moreover, along with the rapid progress of artificial intelligence (AI), AI can take over more aspects of contracting including bargaining, negotiation, and formation of contracts. This means lesser involvement of human agents and lesser relevance of consent.

Codes and algorithms can be expressions of assent, but it is the mutuality that can be a problem in smart contracts. This approach suggests that smart contracts are not enforceable because they do not satisfy the requirement of "manifestation of assent." In other words, lack of (apparent) assent forms the basis for doubting the contractual nature of smart contracts. The Restatement (Second) of Contracts provides that for a contract to be formed, each party should manifest assent with reference to manifestation of the other. This requirement casts doubt on the notion of assent in smart contracts where neither side of the bargain manifests assent in reference to the other side's offer. Simply put, as mentioned above, smart contracts resemble unilateral offers that cross each other and are not in reference or in response to another offer.

Due to the challenges arising from the lack of explicit assent, the law moved towards agency theory and attribution. Most notably, the United States Uniform Computer Information Transaction Act (UCITA) provided that individuals are bound by the "operations of the electronic agent" even if such individuals are not "aware of or [have not] reviewed the agent's operations or the results of the operations." Under this theory, human agents provide a general assent to electronic agents even if human agents are not aware of the details of each transaction. This approach is also reflected in the Electronic Signature in Global and National Commerce Act (E-Sign Act), which provided that contracts formed as a result of electronic agents may not be denied legal effect so long as "the action of [the] electronic agent is legally attributable to the person to be bound."

B. Unilateral Contracts

A key feature of smart contracts is that parties do not exchange promises. The promises are in the form of offers that cross each other. In these types of contracts, one party puts a contract in the form of codes (smart) on a platform such as Ethereum. The smart contract therefore contains a set of unilaterally stipulated codes (conditions) that allow for the transfer of a digital asset or e-currency if those conditions are met. Pursuant to this approach, smart contracts are "interrelated unilateral contracts," by which each party presents its side of the bargain unilaterally.

Under this approach, performance of the conditions presented by the smart contract is key for the analysis of the contractual nature of the transaction. In a unilateral contract, the offeree can only accept the offer by performance rather than exchanging promises. The classic illustration of a unilateral contract is where the offeror states "I will give you $100 if you walk across the Brooklyn Bridge." In these types of contracts, contractual liability exists upon performance without the need for exchange or return of promise.

This feature has been the reason for judges adopting the unilateral contracts framework in instances where a promise given goes unreciprocated. For example, one study shows that judges have used the concept of unilateral contracts and found "promissory liability" of the employer in the context of employee benefits "without the necessity of finding a return promise by the employee."

The same analysis applies to the blockchain technology where initiators of smart contracts offer certain digital assets or crypto-currency if offerees perform by, for example, solving complex mathematical problems. Smart contracts therefore create a digital escrow where funds can only be released if certain conditions (performance) are satisfied by the offeree.

C. Agreement to Agree

Another theory of smart contracts rests on the notion that such contracts are agreements to agree. Smart contracts therefore simply invite further agreements and lack essential contractual terms. Although in most current forms of smart contracts important terms are specified due to simplicity (for example, if mining is completed first, the miner receives Bitcoin), this theory may be applied to more complex smart contracts. Under this approach, again, reliance is key and mutual assent is not necessary. The agreement to agree, or precontractual agreement, lies in the grey area between "full-

blown contracts" and "no obligation." More importantly, this framework can work well for smart contracting where each side puts forward its own set of conditions and, as discussed, parties dispatch cross offers.

Under this view, the inherent incompleteness of smart contracting stems from the fact that each party attaches different meanings to the obligations. The discord over the meanings and scope of the obligations, however, does not negate liability. In other words, liability should always arise from unilateral promises, but not necessarily from consensus and agreement.

The negotiations between parties fall into three categories. First, parties simply have engaged in preliminary negotiations. Second, the parties have agreed on all material terms and intend to memorialize this agreement in a formal document. Third, parties have negotiated and agreed on certain terms but left some terms open. In the first category, the party who did not benefit from the negotiations cannot recover any damages. In the second category, the contract is binding when the evidence supports a finding that the parties did not intend the formalization of their agreement to be essential. Under the third category, a prevailing rule is that parties should bargain in good faith over open terms, or else the refusing party will be responsible for the reliance expenditure.

The third category most resembles smart contracts. Smart contracts can only envision a limited world with a limited set of automated conditions. Inevitably, all contingencies cannot be determined ex ante. In such digital environments, however, parties cannot negotiate in good faith for open terms. This is consistent with the criticism of some law and economics scholars who stated that good faith negotiations are "deficient," and the law should only "protect the promisee's reliance interest if [t]his promisor deviated from an agreed investment" without the requirement for good faith negotiations.

Although courts have adopted a narrow approach to precontractual liability, this approach can also be helpful in understanding the nature of smart contracts. As mentioned, smart contracts are similar to a "pail of water on top of a door" that would inevitably and automatically drop once the door opens. This contract determines the main (automated) quid pro quo between parties. However, it leaves many contingencies out. What if the door does not open due to an external event or faulty codes? What if the code does not specify the contingency where multiple recipients complete the tasks simultaneously?

Smart contracts can fit the definition of a pre-contract because codes have not determined many contingencies of an agreement. In case of a fall-out, the party who relies on the code should be awarded the reliance damages (and not expectation interest).

The agreement-to-agree framework can also be helpful. However, as mentioned, precontractual liability is contested. Moreover, smart contracts, which currently only contain basic transaction formulas, do not have many essential elements left open to be determined (e.g., price of a commodity). Third, the theory of precontractual reliance rests on the idea of avoiding underinvestment in reliance. Whether this reliance incentive may work in the digital world where computers conduct transactions is unclear. As such, the agreement-to-agree framework, even though very helpful, may not capture the entirety of smart contracts.

As explained above, the existing contractual theories of smart contracts do not capture the nature of smart contracts nor do they fully explain their enforceability. Part III below argues for the reliance-based theory for smart contracts as the best theory to protect users.

RELIANCE AS THE BASIS FOR SMART CONTRACTS

Automation of contracts requires a new framework for analyzing contract law. The existing theories, as explained above, do not fully explain smart contracts. The prevailing bargain theory, which focuses on assent and mutuality, does not fully capture the intricacies of smart contracts and does not fully furnish a theory that can protect users. In this Part, the Article argues for a reliance-based theory of smart contracts that aims to protect users' reliance.

In section A, it provides an overview of promissory estoppel as the chief theory of reliance in contract law. In section B, it argues for the reliance-based theory of smart contracts that protects users' reliance.

- ***Reliance Theory Best Explains Smart Contracts***

Promissory estoppel is the reliance theory of promise enforcement. It is reflected in section 90 of the Restatement (Second) of Contracts. The consideration requirement under contract law dictates that only bargained-for promises form contracts. A promise is bargained for "if it is sought by the promisor in exchange for his promise and is given by the promisee in exchange for that promise." Promises that are

gratuitous and open-ended are not enforceable.

Pursuant to the promissory estoppel doctrine, however, promises that induce action or forbearance from the promisee can result in liability if, among others, the promisee reasonably relies on the promise to their detriment. Under promissory estoppel, an equitable remedy, contracts are binding if "injustice can be avoided only by enforcement of the promise." Promisee's detrimental reliance renders the promise binding and enforceable. This doctrine has introduced a reliance-based tort-like liability into contract law.

Scholars have debated the scope of promissory estoppel for many decades. Professor Jay Feinman summarized the debate by stressing the distinction between enforcement of a promise or protection of reliance as the two possible bases for promissory estoppel, while arguing for a third approach based on a relational theory of contract law. What is clear is that promissory estoppel of section 90 of the Restatement (Second) of Contracts made its way for courts to impose liability when the relationship is not contractual. As Professor Randy Barnett and Professor Mary Becker stated after analyzing the case law, "courts have… used promissory estoppel as a remedy for promissory or factual misrepresentation… on the basis of conventional tort or (possibly) contract doctrines." Promissory estoppel protects the reliance trust of promisees even if the bargain is deficient or lacking. This approach fits our increasingly automated contractual relationship as described below.

- ***Reliance Theory Can Help to Protect Users' Reliance***

As stated above, promissory estoppel furnishes a competing basis for enforcement of non-bargained-for promises. This Article argues that smart contracts are enforceable because the offeree has detrimentally relied on the set of conditions presented. There is doubt that conditions coded as smart contracts constitute a "promise" as discussed in contract law generally (and promissory estoppel). Smart contracts resemble a "pail of water on top of a door" that would inevitably and automatically drop once the door opens. Smart contracts set in motion unalterable conditions that can only be completed.

Despite such skepticism, the framework of promissory estoppel best fits smart contracting. On the one hand, the promisor should "reasonably expect" that the set of coded conditions are likely to induce actions (and even forbearance) within the platform. On the other hand, the promisee detrimentally relies on the codes (conditions) provided to attain

the promised reward or return.

Furthermore, the promissory estoppel approach has several advantages in framing smart contracts. First, the doctrine does not rely on mutuality of assent or exchange of promises. In fully-automated contracting with minimal human agent involvement, this doctrine can best explain the contractual nature of the transaction. Second, instead of the forward-looking feature of the bargain theory, it is backward-looking—aiming to remedy harms caused by reliance or misrepresentation. Third, the reliance-based approach is the "thinnest form of trust," where trust is only limited to the statements of another, in this case codes. Fourth, the reliance by the computer may be considered reasonable since it triggers the transfer only if it sees a match with another computer. Fifth, the doctrine of promissory estoppel arguably provides limited avenues for damages. The party who relies on the promise can claim reliance losses (as opposed to often more expansive expectation damages). In the digital world, contractual breaches occur largely due to incomplete or poor coding, not forward-looking promises that trigger expectations. Hence, awarding reliance losses—often awarded in tort cases—can be a more appropriate remedy. Moreover, due to automated and binary features of smart contracts, partial performances are rare. Equally, smart contracting presents few opportunity costs that justify expectation damages.

This view of smart contracts also avoids the problems legal scholars have faced with the issue of consent and assent in other new forms of contracting. In the last several years, consent has been the subject of debates in legal scholarship. Even though contract law is premised on the notion of consent, the importance of finding consent is diminishing due increasingly to cyber contracts and boilerplates. Scholars have discussed that true consent in this new age is amorphous and can be obtained by manipulation. This approach can be traced in the Uniform Electronic Transaction Act that stipulates that a contract "may be formed" even if "no individual was aware of or reviewed the electronic agents' actions."

This trend is notable in consumer contracts where the new draft restatement called for a "grand bargain" in which consent is exchanged for a more robust unconscionability doctrine. Recent behavioral law scholarship further shows that individuals have a formalistic view of contracts and often blame themselves for contractual harms even though they have not properly consented to the contractual terms and disclosures. Studies show that individuals find contracting a matter of formalizing an agreement rather than an assent. The

historical data from the Harvard Case Law Access Project also shows a sharp decline in recent years on the reference to the notion of consent in case law.

Against this background enters smart contracts and blockchain technology. The problem is more acute in blockchain technology where automation, anonymity, and synchronous transactions further isolate the notion of consent. The legal analysis of smart contracts, therefore, cannot be based on the notion of consent and mutual assent. As suggested above, it is the reliance on the technology of blockchain and codes that should lead the way for the legal analysis of smart contracts. As the recent hacks of blockchain show, it is the broken codes (or incomplete codes) that will be at the epicenter of contractual breach. The problem of mismatched codes—between what codes say they would do and what they actually do—is present in the context of initial coin offerings. Some of the intentional instances of mismatch are fraudulent. Most instances, however, are codes that are insufficient or can be manipulated.

With the exception of contract-as-reliance, all major contract theories require mutuality and bargain. The bargain theory requires intention or mutuality. The reliance theory, which is based on section 90 of the Restatement (Second) of Contracts on promissory estoppel, does not require a full quid-pro-quo bargain. It is aimed to protect reasonable reliance in the absence of a bargained-for exchange. Under this approach, the focus of contract enforceability shifts from manifestation or assent and consideration to the promisee's reliance and would create a distinct type of liability.

In smart contracts, however, the manifestation of human intention occurs solely at the outset of entering the platform while human involvement, let alone mutuality of assent, is absent from each transaction. The socio-economics approach to contracting also requires an exchange of promises or societal norms. Neither of these elements can be found in an automated digital world. Smart contracts resemble the "truly discrete" exchange transaction hypothetical that Professor Macneil put forward in 1977. Such a transaction would be separated from all present, past, and future relations, and occur between "total strangers, brought together by chance (not by any common social structure)" while each party "would have to be completely sure of never again seeing or having anything else to do with the other."

LITERATURE REVIEW: ONLINE CONTRACTS

The emergence of the digital age has significantly transformed

traditional modes of contracting. Online contracts—ranging from e-commerce agreements to terms of service and smart contracts—have become a central concern for legal scholars, courts, and policymakers. This literature review explores major academic contributions, legal principles, and evolving debates surrounding online contracts.

1. **Nature and Formation of Online Contracts**

Scholars such as Kevin Werbach and Nicolas Cornell (2017) argue that the digitalization of contractual relationships challenges classical doctrines of contract law. In their influential work on smart contracts, they question whether these self-executing codes fulfill the requirements of offer, acceptance, and consideration. While they recognize the potential efficiency of automated agreements, they stress the importance of aligning them with existing legal norms.

Earlier works like *ProCD, Inc. v. Zeidenberg* (86 F.3d 1447, 7th Cir. 1996) laid the foundation for recognizing shrinkwrap and clickwrap contracts as legally binding, provided users had an opportunity to review the terms and explicitly consent. The legitimacy of online contract formation thus relies on clear mechanisms of notice and assent.

2. **Clickwrap, Browsewrap, and the Question of Consent**

Consent is a central theme in online contracting literature. Woodrow Hartzog (2011), in *The Clicks That Bind*, categorizes different online contract formats—such as clickwrap, browsewrap, and scrollwrap—and evaluates their enforceability. Courts, as Hartzog notes, have been more inclined to enforce clickwrap agreements (which require affirmative action) than browsewrap agreements (which rely on passive usage).

Cases like *Specht v. Netscape Communications Corp.* (306 F.3d 17) highlight judicial skepticism toward agreements where terms are not conspicuously presented or where the user is not required to actively indicate assent. Hartzog's work reveals a growing concern over how meaningful user consent really is in digital environments.

3. **Standard Form Contracts and Power Imbalances**

Margaret Jane Radin's book *Boilerplate* (2013) offers a critical view of standard form online contracts. She argues that the widespread use of non-negotiable, one-sided terms undermines traditional contract values such as mutuality and

voluntariness. These "contracts of adhesion" often deprive users of substantive rights, and courts rarely scrutinize them unless gross unconscionability is evident.

Nancy Kim, in her book *Wrap Contracts* (2013), expands on this by analyzing how modern contracting is often wrapped in interfaces designed to obscure key terms. She stresses the role of interface design in manipulating user consent and emphasizes the need for regulation to ensure transparency and fairness.

4. **Privacy, Data Protection, and Behavioral Economics**

The literature increasingly integrates insights from behavioral economics. Omri Ben-Shahar and Lior Strahilevitz (2016), in *Contracting for Privacy*, explain that users routinely agree to online terms without reading them, primarily because of cognitive overload and the illusion of choice. These findings challenge the traditional idea that consent equals fairness.

Legal scholars have begun to call for a shift from contract-based regulation to regulatory oversight for specific digital practices, especially where user data and privacy are involved.

5. **Jurisdiction, Enforceability, and Cross-border Disputes**

The global nature of the internet raises complex jurisdictional issues. Michael Geist (2001), in *Jurisdiction and the Internet*, explores the limits of applying territorial legal principles to cross-border online transactions. He emphasizes the need for international frameworks and mutual legal recognition to resolve disputes that arise from online contracting across jurisdictions.

6. **Indian Legal Framework on Online Contracts**

From an Indian perspective, scholars such as Dr. Rega Surya Rao examine the interplay between the Indian Contract Act, 1872 and the Information Technology Act, 2000. These laws jointly provide legal validity to electronic contracts and digital signatures. However, gaps remain in regulating user consent and addressing jurisdictional issues for cross-border e-commerce disputes. Indian courts have slowly begun interpreting online contracts, but jurisprudence remains limited.

CONCLUSION

Contracts are increasingly becoming digitized. In parallel, businesses are rapidly adopting digital contracts. Such digital

(smart) contracts operate as self-executing, self-enforcing, automated contracts in which parties involved are often anonymous. This trend is a departure from the traditional notion of contracts, whereby consent and forward-looking promises play a pivotal role in *ex ante* formation and *ex post* enforcement of contracts.

The legal nature of smart contracts remains shrouded in ambiguity. For example, terms and conditions of the platform, the underlying platform codes, and smart contract codes may be conflicting when it comes to parties' obligations and the binding nature of smart contracts.

Moreover, the possibility of hacks or code failures always exists. Given the new developments, this Article suggests that smart contracts should be analyzed through the lens of reliance-based contracting (similar to promissory estoppel or tort-based misrepresentation). Moreover, the reliance-based approach solves some of the problems posed by the consent-based approach in digital contracting.

Further, this Article analyzes the new efforts aimed at the resolution of disputes on the blockchain platform. It identifies key features of blockchain-based dispute resolution that have the capability of modifying contractual disputes and the very act of contracting.

The Article argues that blockchain-based dispute resolution results in seismic changes such as decentralized decision-making, network-based dispute resolution, and extrajudicial enforcement of decisions. More importantly, human connection and recognition can only be found in the dispute phase of contracting. This marks a shift from traditional contractual solidarity to digital solidarity.

REFERENCES

- Ben-Shahar, O., & Strahilevitz, L. (2016). *Contracting for privacy*. Journal of Legal Studies, 43(S2), S101–S123. https://doi.org/10.1086/677839

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

- Geist, M. (2001). *Is there a there there? Toward greater certainty for Internet jurisdiction.* Berkeley Technology Law Journal, 16(3), 1345–1406.

- Hartzog, W. (2011). The clicks that bind: Ways users "agree" to online terms of service. *St. John's Law Review, 81*(2), 401–463.
- Kim, N. S. (2013). *Wrap contracts: Foundations and ramifications*. Oxford University Press.
- Radin, M. J. (2013). *Boilerplate: The fine print, vanishing rights, and the rule of law*. Princeton University Press.
- Rao, R. S. (2018). *Cyber law and information technology*. Asia Law House.
- Restatement (Second) of Contracts § 90 (1981).
- Specht v. Netscape Communications Corp., 306 F.3d 17 (2d Cir. 2002).
- ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996).
- Uniform Electronic Transactions Act, U.S.C. § 7001 et seq. (1999).
- Barnett, R., & Becker, M. (1989). Beyond reliance: Promissory estoppel, contract formalities, and the synthesis of contract doctrine. *Columbia Law Review, 89*(4), 593–633. https://doi.org/10.2307/1122755
- Feinman, J. M. (1995). *Unmaking of contract law: The classical law of contracts in the modern legal system*. University of Chicago Press.
- Macneil, I. R. (1977). Contracts: Adjustment of long-term economic relations under classical, neoclassical, and relational contract law. *Northwestern University Law Review, 72*(6), 854–905.
- Becker, M. (1998). Reliance and contract doctrine. *Chicago-Kent Law Review, 74*(3), 875–898.