Passagens. Revista Internacional de História Política e Cultura Jurídica
Rio de Janeiro: vol. 17, nº 3, setembro-dezembro, 2025, p. 522-551.

https://doi.org/10.15175/w0ztm173

Articles

The legality of smart contract through the lens of Indian Contract Act

Rahul J. Nikam*
Sharda University, Uttar Pradesh, India

Abstract

Smart contracts, a revolutionary technology that offers a digital alternative to conventional contracts, are popular. Smart contracts also known as automated digital contracts are becoming common in various countries due to their efficiency and openness. Various national and global forums have agreed that smart contracts might alter contract enforcement and boost economic development in India. Given this, it's crucial to understand the Indian Contract Act, (ICA) 1872 stance on smart contracts. ICA requires testing smart contracts for contractual validity before entering the uncharted seas of autonomous and anonymous digital contracting. This experiment raises many issues, especially given the law's strict procedural structure. This article refutes the claim that smart contracts should be regulated by self-regulation. Rather author prefers a broad interpretation of substantive contractual law to harmonize smart contracts under the ICA, following common law's flexibility. It is shown that smart contracts are built on the same principles as common law contracts and deepen our research in the framework of Indian law and precedent. Similar approaches from other countries support this perspective. Although many legislations require change, it is believed that a smart contract law is not needed. The paper concludes by proposing solutions to the potential obstacles that may arise due to present approach.

Keywords: rule of law; artificial intelligence; black box; smart contract; traditional contract.

A legalidade dos contratos inteligentes sob a ótica da Lei de Contratos da Índia

Resumo

Contratos inteligentes, uma tecnologia revolucionária que oferece uma alternativa digital aos contratos convencionais, são populares. Contratos inteligentes, também conhecidos como contratos digitais automatizados, estão se tornando comuns em vários países devido à sua eficiência e abertura. Diversos fóruns nacionais e globais concordaram que contratos inteligentes podem alterar a execução de contratos e impulsionar o desenvolvimento econômico na Índia. Diante disso, é crucial compreender a posição da Lei de Contratos da Índia (ICA) de 1872 sobre contratos inteligentes. A ICA exige que os contratos inteligentes sejam testados quanto à validade contratual antes de se adentrar nos mares desconhecidos da contratação digital autônoma e anônima. Esse experimento levanta muitas questões, especialmente considerando a estrutura processual rigorosa da lei. Este artigo refuta a alegação de que contratos inteligentes devem ser regulados por autorregulamentação. Em vez disso, o autor prefere uma interpretação ampla do direito contratual substantivo para harmonizar os contratos inteligentes sob a ICA, seguindo a flexibilidade do direito consuetudinário. Demonstra-se que os contratos inteligentes são construídos com base nos mesmos princípios dos contratos de direito consuetudinário e aprofunda-se nossa pesquisa no contexto da legislação e dos precedentes indianos. Abordagens semelhantes de outros países corroboram essa perspectiva. Embora muitas legislações exijam

* LLM Degree in Corporate Laws in 2008 and a Ph.D. degree in IPR Protection to Outer Space Activities in 2012 from the NALSAR University of Law, Hyderabad, India. He is currently a Professor at Sharda School of Law, Sharda University, Uttar Pradesh, India. E-mail: rahulsnikam@gmail.com. https://orcid.org/0000-0001-7279-1399

Received on May 2, 2025 and approved for publication on August 7, 2025.

mudanças, acredita-se que uma lei de contratos inteligentes não seja necessária. O artigo conclui propondo soluções para os potenciais obstáculos que podem surgir devido à abordagem atual.

Palavras-chave: Estado de Direito; inteligência artificial; caixa-preta; contrato inteligente; contrato tradicional.

La legalidad de los contratos inteligentes desde la perspectiva de la Ley de Contratos de la India

Resumen

Los contratos inteligentes, una tecnología revolucionaria que ofrece una alternativa digital a los contratos convencionales, gozan de gran popularidad. También conocidos como contratos digitales automatizados, se están volviendo comunes en varios países debido a su eficiencia y transparencia. Diversos foros nacionales e internacionales han coincidido en que los contratos inteligentes podrían alterar la ejecución de los contratos e impulsar el desarrollo económico en la India. Por ello, es crucial comprender la postura de la Ley de Contratos de la India (ICA) de 1872 sobre los contratos inteligentes. La ICA exige comprobar la validez contractual de los contratos inteligentes antes de adentrarse en el inexplorado mundo de la contratación digital autónoma y anónima. Este experimento plantea numerosos problemas, especialmente dada la estricta estructura procesal de la ley. Este artículo refuta la afirmación de que los contratos inteligentes deberían regularse mediante la autorregulación. En cambio, el autor prefiere una interpretación amplia del derecho contractual sustantivo para armonizar los contratos inteligentes bajo la ICA, respetando la flexibilidad del derecho consuetudinario. Se demuestra que los contratos inteligentes se basan en los mismos principios que los contratos de derecho consuetudinario y profundiza nuestra investigación en el marco del derecho y la jurisprudencia de la India. Enfoques similares de otros países respaldan esta perspectiva. Si bien muchas legislaciones requieren cambios, se cree que no se necesita una ley de contratos inteligentes. El artículo concluye proponiendo soluciones a los posibles obstáculos que puedan surgir debido al enfoque actual.

Palabras clave: Estado de derecho; inteligencia artificial; caja negra; contrato inteligente; contrato tradicional.

La légalité des contrats intelligents au prisme de la loi indienne sur les contrats

Résumé

Les contrats intelligents, technologie révolutionnaire offrant une alternative numérique aux contrats conventionnels, sont très répandus. Aussi appelés contrats numériques automatisés, ils se généralisent dans de nombreux pays grâce à leur efficacité et à leur transparence. Plusieurs forums nationaux et internationaux s'accordent à dire que les contrats intelligents pourraient modifier l'exécution des contrats et stimuler le développement économique en Inde. Il est donc crucial de comprendre la position de la loi indienne sur les contrats (ICA) de 1872 sur les contrats intelligents. L'ICA exige de tester la validité contractuelle des contrats intelligents avant de s'engager dans les eaux inexplorées des contrats numériques autonomes et anonymes. Cette expérience soulève de nombreuses questions, notamment compte tenu de la structure procédurale stricte de la loi. Cet article réfute l'affirmation selon laquelle les contrats intelligents devraient être réglementés par l'autorégulation. L'auteur privilégie une interprétation large du droit contractuel substantiel afin d'harmoniser les contrats intelligents sous l'ICA, en s'appuyant sur la flexibilité de la common law. Il démontre que les contrats intelligents reposent sur les mêmes principes que les contrats de common law et approfondit nos recherches dans le cadre du droit et de la jurisprudence indiens. Des approches similaires adoptées dans d'autres pays étayent cette perspective. Bien que de nombreuses législations nécessitent des modifications, une loi sur les contrats intelligents semble superflue. L'article conclut en proposant des solutions aux obstacles potentiels liés à l'approche actuelle.

Mots-clés : État de droit ; intelligence artificielle ; boîte noire ; contrat intelligent ; contrat traditionnel.

Die Rechtmäßigkeit von Smart Contracts im indischen Vertragsgesetz

Zusammenfassung

Smart Contracts, eine revolutionäre Technologie, die eine digitale Alternative zu konventionellen Verträgen bietet, erfreuen sich großer Beliebtheit. Smart Contracts, auch als automatisierte digitale Verträge bekannt, erfreuen sich aufgrund ihrer Effizienz und Offenheit in vielen Ländern zunehmender Beliebtheit. Verschiedene nationale und globale Foren sind sich einig, dass Smart Contracts die Vertragsdurchsetzung verändern und die wirtschaftliche Entwicklung in Indien fördern könnten. Vor diesem Hintergrund ist es wichtig, die Haltung des indischen Vertragsgesetzes (ICA) von 1872 zu Smart Contracts zu verstehen. Das ICA schreibt vor, Smart Contracts auf ihre Vertragsgültigkeit zu prüfen, bevor sie in die unbekannten Gewässer autonomer und anonymer digitaler Vertragsgestaltung vordringen. Dieses Experiment wirft viele Fragen auf, insbesondere angesichts der strengen Verfahrensstruktur des Gesetzes. Dieser Artikel widerlegt die Behauptung, Smart Contracts sollten durch Selbstregulierung reguliert werden. Der Autor bevorzugt vielmehr eine breite Auslegung des materiellen Vertragsrechts, um Smart Contracts im Rahmen des ICA zu harmonisieren und dabei der Flexibilität des Common Law zu folgen. Es wird gezeigt, dass Smart Contracts auf denselben Prinzipien wie Common-Law-Verträge beruhen, und vertieft unsere Forschung im Rahmen des indischen Rechts und der Präzedenzfälle. Ähnliche Ansätze aus anderen Ländern stützen diese Perspektive. Obwohl viele Gesetze geändert werden müssen, ist man der Ansicht, dass ein Smart-Contract-Gesetz nicht erforderlich ist. Das Papier schlägt abschließend Lösungen für die potenziellen Hindernisse vor, die sich aus dem derzeitigen Ansatz ergeben könnten.

Schlüsselwörter: Rechtsstaatlichkeit; Künstliche Intelligenz; Blackbox; Smart Contract; Traditioneller Vertrag.

从《印度合同法》视角看智能合约的合法性

摘要

智能合约是一项革命性的技术，它为传统合约提供了数字化替代方案，目前正日益普及。智能合约，又称自动化数字合约，因其高效性和开放性，在各国日益普及。国内和国际论坛都一致认为，智能合约可能会改变合约执行方式，并促进印度的经济发展。有鉴于此，理解1872年的《印度合同法》（ICA）对理解印度司法界当前所持有的针对智能合约的立场至关重要。ICA要求在进入数字合约这个未知领域之前，人们必须对智能合约的有效性进行测试。在尝试执行智能合约的过程中，出现了许多问题，尤其是在ICA 严格的程序结构下。本文驳斥了智能合约应通过它的自我监管进行监管的说法。作者倾向于对传统的合同法进行广义解释，以协调《印度合同法》(ICA)框架下的智能合约，同时参照普通法的灵活性。本研究表明，智能合约建立在与普通法合同相同的原则之上，并深化了我们在印度法律和案例框架下的研究。其他国家的针对数字合约采用的类似方式也支持这一观点。尽管许多立法需要修改，但我们认为制定单独的智能合约法并非必要。最后，针对现有方式 （对传统的合同法进行广义解释)可能带来的潜在问题，本文提出了一些解决方案。

关键词：法制；法治；人工智能；黑箱；智能合约；传统合约

Introduction

It is inevitable that the law will be significantly influenced by the rapid advancement of technology. This is exemplified by the multifaceted impact that Artificial Intelligence has had on the current understanding of law. An example of a recent transition that can be comprehended is the recent increase in the popularity of smart contracts in the global market. A bilateral or multilateral contract automatically enforced without human intervention is called a smart contract. In 1994, Nick Szabo introduced the term “smart contract,” which refers to a bilateral or multilateral agreement whose terms are automatically enforced without human intervention. He characterizes smart contracts as a collection of digital promises that are formed between parties and are executed and enforced through digital procedures that are encoded within the contract. This terminology is a result of the advanced and superior functionality of these contracts in comparison to traditional contracts. A smart contract endeavors to reduce individual discretionary and government involvement in the contract by delegating the carry-out of contractual terms to a computer. Execution is possible by converting “human-readable” contract clauses into “machine-readable” code. For example, A debt contract for a car that locks its ignition if the conditions are not satisfied is a smart contract. An internal software in the car digitally validates that the contract conditions have been met in this contract. Thus, a code is included in a blockchain, which is a decentralized database that peer-to-peer network users may verify. A smart contract’s fundamental operation is the deployment of predetermined contractual terms in the form of coding on a blockchain platform. Because it operates entirely automatically, human interaction is not necessary.

A smart contract’s commercial explorations are driven by its advantages over a regular contract, including speed, efficiency, and cost. The smart contracts “Propy” (Ventura, 2020), which is based on real estate, and “Fizzy” (Clement, 2019), which is based on insurance, demonstrate the many business opportunities that this revolutionary technology offers. But the fact that smart contracts are self-executing has sparked debate in the legal community about their regulation and legality. The unwillingness of legal experts to acknowledge it as a “contract” in *stricto sensu* suggests something about this. They contend that standard contractual law cannot apply to smart contracts, in contrast to regular contracts. Although some academics have advocated for smart contracts to self-regulate, the author argues opposing this laissez-faire stance and instead suggests harmonizing current contract rules with the emerging smart contract regime. This would give smart contracts authority from the government and also let the law crack down on smart contracts with unfair terms or that help with illegal activities like money laundering and stealing private encryption keys, etc.

The main reason why there might be problems with control is that a standard contract is very different from an automatic smart contract. They both try to make sure that people follow through on their rights and obligations under contracts, but they do so in very different ways and with very different ideas. An intelligent contract is composed of machine-readable code that follows the structure of an “if this, then that” diagram. It then automatically carries out its terms, acting as a “proxy performer” of the parties’ contractual duties. Furthermore, a smart contract is integrated with the blockchain architecture, making cryptocurrency considerations legitimate contractual consideration. Therefore, in order for the usage of a smart contract to be considered acceptable consideration, cryptocurrency assets like Bitcoin would need to be used. Because of this automaticity and the fact that smart contract transactions are carried out using crypto-assets, there may be some legal repercussions, most notably about the commission of crimes. Theft of private encryption keys and the untraceable selling of private papers are examples of such crimes. Smart contracts may serve as an easy way for illicit contracts, like hit contracts, to operate as they provide smooth, untraceable transactions between two untrustworthy parties. In the present paper, the author explores the need to regulate smart contracts and makes the case that implementing them under the purview of the Indian Contract Act, of 1872 (ICA) would significantly enhance the procedures that underpin business dealings.

Legal material and methods

The article strives to examine the need to govern smart contracts by arguing that brining smart contracts into practice under the regime of Indian Contract Act, 1872 will substantially assist in improving processes underlying commercial transactions. The article provides a short supplementary study on the legality of cryptocurrencies and provide a concise explanation of the theoretical foundations of smart contracts. It analyses smart contract Jurisprudence and justifies the regulation of smart contracts based on economic and analogy literature to support the regulation of smart contracts. By claiming that smart contracts may be implemented within the Indian Contract Act without requiring significant changes, sets a new standard for scholarship in Indian contract law. Then it highlights several real-world challenges in smart contract regulation, and tries to provide general methods to address these challenges. In the conclusion article suggests interpreting current Indian contract law to support the legitimacy of smart contracts and offers the best answers to the issues that arise as a result of strategy discussed in the present article.

Result and Discussion

1. Discovering Smart Contracts

It would be imprudent to talk about smart contracts without first examining the idea behind blockchain technology, which drives them. The fundamental component of blockchain technology is a “chain” of “blocks,” which is a kind of data structure. These blocks constitute a ledger since they are linked to one another digitally and contain data. A distinct cryptographic hash code that identifies the next block in the chain is included with every block along with data. Each user on the network has a copy of the blockchain, and each modification to a block requires validation by all other users. To provide an example, consider a cryptocurrency that operates on the blockchain. When a transaction is made, the specifics of the transaction are entered into a block and verified by all network users. Because blockchain transactions are dispersed, they are transparent and certain.

Given this context, an agreement between participants via machine-readable code is called a smart contract. This code is included in a decentralized blockchain, which, in response to predefined “trigger events”, automatically triggers the smart contract. As a result, the smart contract’s terms are written in an “if-then” fashion, meaning that it will automatically carry out a certain action if the trigger event occurs. Because a smart contract relies on blockchain technology, digital assets based on the blockchain network like cryptocurrencies must be deployed. To put the preceding debt contract example in perspective with this explanation, a smart contract would be programmed to only permit the starting of the car if it has recorded the receipt of bitcoin equivalent to the debt contract’s conditions.

Smart contracts, which were pioneered in the early 1990s, only became commercially viable following the introduction of current decentralized platforms like Ethereum, which executes smart contracts. Users may design smart contract parameters in ‘Solidity’ using bitcoin on Ethereum. For example, flight delay insurance from AXA is an Ethereum smart contract. This insurance company ran “Fizzy”, an automated insurance contract platform. These contracts would automatically payout bitcoin insurance if a flight was delayed more than two hours. Steller, NEO, EOS, and Hyperledger are among decentralized smart contract systems that have emerged recently. They each provide unique traits and functionalities in the smart contract matrix and demonstrate how smart contracts may be tailored to match contracting parties’ demands.

Some of the intrinsic properties of a blockchain are inherited by smart contracts. Consequently, smart contracts are immutable, meaning that they cannot be altered after they have been established. Distributed smart contracts need all blockchain network users to confirm their activities. This greatly decreases deceit. For example, a “kick-starter” smart contract raises funding for a particular project. Once the project’s patrons deposit cryptocurrency into the smart contract, the money is automatically disbursed to the project creator upon the target amount being reached. The funds are redeposited into the patrons’ accounts if the objective is not achieved within the designated time frame. The intermediary third party is not required to be trusted by either the project creator or the patrons; however, the blockchain network’s users must verify any transaction due to its distributed nature. Smart contracts thereby enable transactions among non-trusting parties, and contracting users frequently employ pseudonyms when engaging in transactions through smart contracts.

Also, smart contracts are not human-readable languages; rather, they are inherently digital entities represented as machine-readable code. From a judicial perspective, this is extremely problematic since the majority of judges lack the technical skills necessary to understand and comprehend code, which is especially troublesome in the Indian setting.

Thus, author use a hybrid paradigm, akin to Ricardian contracts, to solve this issue. In this model, a human-readable contract is added to the code. Thus, the hybrid mechanisms would comprise readable by machines and executable code and a document that resembled a contract but stated the smart contract's terms and conditions. This article will investigate smart contracts utilizing this hybrid model as a factual matrix and argue they are superior than conventional ones.

2. *Is a Smart Contract a Contract: Theory and Practice*

Smart contracts have self-executing capabilities, wherein the included code adheres to a predetermined purpose. This automaticity is sometimes used as support for the claim that these contracts and the customary dispute-resolution procedure cannot be reconciled. Some researchers think that since smart contracts are inherently self-enforcing, they need to be categorized under a certain "self-help" mechanism. Thus, a smart contract's execution is guaranteed, eliminating the need for court involvement. Despite the existence of this mechanism, it is contended that self-enforcement does not conflict with state regulation and does not replace the therapeutic process offered by remedies like injunctions, damages for breach of contract, etc. This section of the paper aims to defend state regulation from both a theoretical and practical standpoint, focusing on the legal context in which smart contracts may be used.

2.1. Existing Theories and Smart Contract Situating AI Realization

Due to advanced technology, smart contracts are more time and money efficient than regular contracts.[3] Since it is complex and has self-enforcing characteristics, academics contend that smart contracts operate independently of the law by providing an effective replacement for the traditional governance structure. On the other hand, it is argued that permitting such unrestrained self-execution will raise total expenses and reduce economic efficiency. In support of this claim, author draws on the normative framework offered by legal and economic theories, specifically citing the Economic Contract Theory and the Incomplete Contract Theory. These theories clarify how transaction cost economics supports the enforcement of smart contracts by the state, thereby fostering contractual efficiency. Let's compare the effectiveness aspect of smart contracts in the self-enforcement and state-enforcement paradigms using these two theories as a benchmark.

2.1.1. Theory of Economic Contracts Existing

Similar to regular contracts, smart contracts include the basic, abstract elements of contracting, such as offer, acceptance, consideration, consent from both parties, and legal purpose. The effectiveness of a contract is one such characteristic. The foundation of economic contract theory is the concept of efficiency, which links a contract's enforceability to its overall effectiveness. This efficiency may be attained in a contractual framework via mutual confidence and collaboration between contracting parties, which in turn offers a means of fostering "Pareto Efficiency". An enforceable contract may guarantee Pareto Efficiency for all parties in a business context by either enforcing contractual performance or correcting any violation by going to court. Since contracts are based on conditions that both parties have agreed upon, any advantages resulting from them should be protected so that neither party gains an unfair advantage over the other or suffers a negative outcome from one of the other's actions. Within the framework of the Economic Contract Theory, it is often said that the capacity of a contract to be legally enforced allows contracting parties to resolve underlying Pareto-inefficiencies or reach a Pareto-efficient solution.

Therefore, the current interpretation of smart contracts as self-executing contracts that fall beyond the purview of court enforcement serves to reduce their overall economic efficiency. Arguments in favor of self-regulation often hail the former as a productive substitute for judicial involvement (Vatiero, 2022). But this approach ignores the crucial role that court enforcement plays in transaction cost economics: According to these transaction costs, outside intervention is preferred in order to ascertain contractual rights, provide suitable remedies, and take into consideration any obstacles to agreement implementation. If there is no legal enforceability, these aspects remain unresolved, and depending just on the contract's automated execution might result in extra transaction costs.

An example of a contract that extends into an unforeseen occurrence, like a pandemic or hurricane, makes this point quite clear (Tjong Tjin Tai, 2018). As was previously said, a situation like this might result in contract irritation or make performance dependent since smart contracts only work within the parameters of their code. This increases the cost of the transaction for one or both parties. Increases in the price of certain raw supplies, transportation, etc., might result from a cyclone. Such outcomes may only be fought by cancelling the contract, since smart contracts are immutable. It is utterly impossible to factor in even the most unlikely events when creating a smart contract; the only way to account for unforeseen events is to use legal enforcement. While there may be additional expenses associated with litigation, it is still the only practical way to address events of the most unforeseen obstacles in contracts.

2.1.2. The Theory of Incomplete Contracts

Another argument in favor of regulating smart contracts is the Incomplete Contract Theory put out by Oliver D. Hart and Holmström (Hart, 1986). According to this idea, which was developed by Hart, real-world contracts are often poorly drafted and leave open terms that the parties must negotiate if and when unanticipated circumstances arise. This ambiguity is essentially unavoidable, but it also presents a risk in that it might lead to opportunistic actions by the parties to the contract who want to take advantage of this ambiguity. As a result, different interpretations arise, with each side promoting its own viewpoint. Renegotiation or lawsuits are often used to resolve this issue. Therefore, the argument for incomplete contracts is based on the increased transaction costs associated with ending a contract rather than renegotiating it, as well as the resulting decrease in efficiency. As previously said, there are two possible methods to remedy an incomplete contract: either by court intervention or through renegotiation between the parties. The "hold-up problem," a phenomenon whereby one side holds up the other because of its greater bargaining strength, forces unfairness in the contract, is the consequence of renegotiation. As a result, it is often advised that parties to an incomplete contract rely on the legal system to provide the missing pieces when time comes for enforcement. The Incomplete Contract Theory has been included into smart contracts by Szabo in forming and safeguarding relationships on public networks. Szabo contends that it would be too expensive in terms of mental, cognitive, and literary resources to factor in every possible outcome in an agreement. This may be lessened by excluding certain possibilities from smart contracts, leaving them unfinished. He supports ex-ante procedures of renegotiation among parties whenever such events arise in order to close the ensuing interpretational gap. Nonetheless, it is contended that the contractual parties must rely on the courts to close any gaps in the agreement in order to guarantee the effectiveness of incomplete contracts. Contractual efficiency is restored by the courts by addressing any gaps in the agreement, offering suitable interpretation in cases of ambiguity, and giving sufficient remedies. By assuring the fulfillment of the contract in accordance with the parties' intentions and appropriately paying damages for non-performance, this method guarantees that the effectiveness of a contract is maintained. Any argument in favor of smart contract self-regulation strips them of their effectiveness as self-regulation only ensures ex-ante contractual compliance and lacks the flexibility to handle unforeseen circumstances in court (Hsiao, 2017). As a result, it is believed that state regulation of partial smart contracts promotes economic efficiency by allowing courts to interpret the remaining information.

2.2. Analogical Justifications

Smart contracts need state regulation, as shown by a comparison with similar technology advancements that have been incorporated into the law. In this context, the vending machine is a frequently used illustration. An automatic vending machine works on the basis of a basic mechanical contract, in which a binding agreement is made between the parties upon receipt of the goods and the acceptance of the coin. It is important to remember that a contract made via a vending machine is enforceable by law. In Thornton v. Shoe Lane Parking (England, 1970), Lord Denning held that when a consumer inserts a coin into a vending machine to accept an offer made by the machine's owner, a legally enforceable contract is formed. This example comes from Szabo's dependence on the vending machine to explain his concept of smart contracts. According to his conceptualization, smart contracts would work and operate similarly to vending machines. While smart contracts and vending machines have similar fundamental functions, their link with blockchain gives them significantly more adaptable and economically beneficial capabilities. An algorithmic contract is another kind of contract that is comparable to a smart contract.

Contracts determined by computer algorithms are known as algorithmic contracts, which are enforceable in a court of law. Amazon's pricing strategy, which sets prices by sellers using computer algorithms, is one example of such a contract. Even with their inherent drawbacks, algorithmic contracts are nevertheless subject to laws governing electronic transactions. The Securities and Exchange Board of India is responsible for overseeing algorithmic trading. Furthermore, the Reserve Bank of India's Electronic Trading Platforms (Reserve Bank) Directions, 2018 regulate algorithmic trading that is carried out by the Electronic Trading Platforms. By treating electronic signatures and records as equal to manual records, US information technology law also recognizes algorithmic contracts. Smart contracts are considered a sophisticated kind of algorithmic contract due to their high degree of automation.

It is also important to acknowledge that the technical advancement of contracting is not wholly original. Contracts based on interchange agreements have been formed using the Electronic Data Interchange ('EDI'), a kind of electronic contract that is equivalent to regular contracts under Indian law. These electronic agreements are legally binding because they have the essential elements of a "contract," such as mutual consent, communication, and quid pro quo. Additionally, common law courts have recognized electronic contracts; in fact, legislation certifying electronic contracts have been established in Australia, New Zealand, and the UK in order to preserve the United Nations Commission on International Trade Law's (or "UNCITRAL") Model Law on Electronic Commerce. UNCITRAL has, for the most part, made smart contracts more legally enforceable. In India, the Information Technology Act, 2000 (IT Act – India, 2000) grants legal force to electronic contracts. Electronic contracts are deemed legitimate by virtue of S.10-A of the IT Act. Furthermore, any discrepancy under any legislation in force, including the Benami Transaction Act 1988, that may render an online transaction voidable is eliminated by S. 81 of the IT Act.

Contract computerization is not a recent development. Vending machines, electronic data interchanges, and algorithmic contracts serve as examples of how parties who agree to a contract are nonetheless subject to the legal enforcement mechanism even in cases where the contract is computerized. On the basis of this, it is believed that smart contracts should be treated similarly under Indian law and be covered by the technologically adaptable legal framework. It should be stated, nevertheless, that the aforementioned parallel is only meant to apply to the application of contract law concepts. Some implementation issues related to jurisdiction, novation, judicial interpretation, etc. are brought forth by the unique functional properties of smart contracts. It is argued that while incorporating technological advancements in different forms of contracting—smart contracts being one such form—the flexibility and adaptability of the law is not compromised.

2.3. Relevance

Although they are still in the early stages of development, smart contracts have just lately been widely used. There are encouraging indications that its incorporation into regular business dealings might be advantageous for the economy. Recently, the Australian Society of Construction Law advocated using smart contracts to establish construction trusts that might assist in resolving payment and insolvency-related difficulties, thereby improving the structural efficiency of society as a whole. The financial industry is likewise where this technology may find its greatest uses. Let's us limit our discussion in this section to the two main segments of the Indian financial industry. First, the real estate industry, which is valued at a trillion dollars and is expected to account for more than 13% of the nation's GDP in the coming ten years. Secondly, the banking industry, which contributes significantly to the nation's economy and is valued at more than 15% of the GDP. These industries account for a considerable portion of the GDP, and author thinks that integrating them with smart contracts would accelerate their development. This is mainly because these institutions are so complex and bogged down in bureaucracy and complicated procedures that they provide a chance to streamline their operations using smart contracts.

3. *Indian Legal Regime and Smart Contracts*

This section differs significantly from current Indian research on smart contracts. Here, it is contended that smart contracts are essentially compliant with the legal system of the nation and make an effort to show how they relate to Indian law in two sub-sections. The first sub-section looks at smart contracts in relation to the Contract Act and shows how they satisfy the fundamental needs of a contract. But let's don't go so far as to say that smart contracts can be easily incorporated into Indian law; instead, in the second sub-section, it describes certain procedural challenges that result from harmonizing smart contracts with the ICA

3.1. Application of the ICA, 1872 On Smart Contracts

Technology-driven social developments have changed contract law's fundamentals—offer, acceptance, consideration, permission from both parties, and legal purpose. The courts' readiness to adapt to technology shows this. Due to their "substantial similarities" to traditional contracts, some electronic contracts are covered under contract law. Smart contracts' immutability, encrypted language, and anonymity or pseudo-anonymity differs from traditional contracts in application and enforcement.

It is important to highlight that Indian courts have not yet dealt with blockchain-based contracts of any kind. Therefore, there isn't any legally enforceable precedent on the matter. Because of this shortcoming, in support of present study of smart contracts English case law are used wherever necessary. Because of the common law foundations of both India and the UK and the significant overlap between English and Indian contract law, English contract jurisprudence has a significant impact on Indian law. As an example, a result that is based mostly on a common law analysis is valid in both India and the UK. Similarly, since recognized contracting concepts apply to smart contracts, it is contended that they must have contractual force within the confines of common law, drawing on the Taskforce's Report. Let us examine how these ideas may be applied to smart contracts based on the strength of this case. In subsequent paragraph's, firstly it provides a quick explanation of the fundamental workings of smart contracts as well as the purpose and justification for this examination. The next subsections examine the fundamental elements of a legally binding agreement, including offer, acceptance, consideration, mutual consent, and legal purpose, and how these relate to smart contracts. It is concluded from present analysis that smart contracts meet the requirements necessary to be enforceable under the present ICA.

3.1.1. Application of the ICA, 1872 On Smart Contracts

It's often maintained that using smart contracts instead of going to court to enforce one's contractual duties should discourage parties from doing so. Although India has not yet passed progressive smart contract laws, other common law countries have shown that smart contracts may be controlled by present contract law providing the core contractual principles are respected. The Taskforce's Report (United Kingdom, 2021) unequivocally states that smart contracts are legally equivalent to regular contracts since both may meet common law standards for contracts. It goes on to say that common law is flexible enough to keep up with technological changes, even with the technical complications that come with operating smart contracts.

Even without smart contract legality decisions, the Indian judiciary has ruled that an electronic contract is not inherently less legal than a mechanical one because it does not preclude the application of general contract law principles. Although there are some similarities between electronic contracts and smart contracts, it would be pointless to attempt to rigorously compare the two. A click-wrap agreement is an example of a traditional contract that is completed digitally. E-contracts are seen by UNCITRAL as being on par with conventional contracts, and according to S. 10-A of the IT Act, they are enforceable and legitimate under Indian law. Although smart contracts are often described as an advanced version of electronic contracts, their dependence on the blockchain and the need for cryptocurrency to be deployed as consideration set them apart from electronic contracts. Additionally, smart contracts are automatically executed and cannot be changed. However, in comparison to traditional contracting as envisioned under the ICA, electronic contracts are especially click-wrap agreements that present a procedural change. However, Indian law recognizes them since they follow the basic principles of contract such as offer, acceptance, consideration, mutual consent, and legal purpose. Despite their procedural problems, smart contracts that essentially follow these basic contracting concepts are contractually valid. Based on the courts' stance on electronic contracts, it is argued that smart contracts will be accepted if the basic principles of contract are followed.

Smart contracts are a technically advanced over electronic contracts, but the current legal system does not allow for them to be seen as an anomaly. It is to be understood that the machine-readable, self-executing code is subject to legal enforcement, not the other way around. A significant ruling in favor of the legal validity of self-executing automated contracts was made in the B2C2 Ltd v. Quoine Pte Ltd. SGHC(I) 03 (Singapore, 2019). A contract allowed B2C2 to trade on Quoine's bitcoin trading platform. In one transaction, the platform conducted numerous bitcoin exchange agreements at times the market rate. After discovering a technical issue, Quoine unilaterally undid it. The appellant claimed this conduct breached trust. Quione unilaterally terminating the transactions violated the contract, as determined by the Court of First Instance and affirmed by the Court of Appeal. Even while it did not rule on whether the arrangement constitutes a legal contract, the Court of Appeal made two important observations on smart contract. First, the court inferred that the automated trading platform agreement was lawful. Second, the majority decided against fundamentally modifying the law in favor of "meaningful adaptation" of the current legal framework to address evolving technological issues, with respect to the application of common law principles to automated technologies. Given that it offers extensive information on the contractual validity of automated contracts and their integration into conventional contract law, the ruling might have an effect on the regulation of smart contracts. While comparable conflicts have not yet surfaced in India, it is pertinent for the purposes of this study to consider how fundamental contract law concepts apply to automated platforms. Ensuring comprehensive regulatory compliance in a smart contract transaction is a significant task. The interaction of many laws during smart contract transactions creates a minefield of technological and legal issues. For example, a variety of laws, including contract law, property law, registration law, and taxes law, come into play when purchasing land using a smart contract. To elaborate in the registration context, the ease with which title may be transferred using smart contracts raises concerns about the central registration of asset transfers. This illustrates the possible difficulties in enforcing smart contract regulations under the ICA. In order to completely materialize a statutorily controlled smart contract transaction, it is necessary to address this problem.

According to the ICA, some essential components of a legitimate contract, such as the desire to establish legal relations and mutual consent, are determined by an objective test. It is contended that consenting to a smart contract that is represented by machine-readable code signifies a commitment to be bound by the terms of the contract under this objective test. Usually, the fulfillment of certain requirements determines if a contract exists. Offer, acceptance, communication, consideration, mutual consent, and legal purpose are the widely acknowledged elements required for the establishment of a contract under the ICA. All of these elements together make up a legally binding contract. Thus, these necessary components of contract-formation must be present for smart contracts to be recognized as contracts under the ICA.

3.1.2. Acceptance and Offer

Under S. 2(a) of the ICA, an offer or proposal is a clear indication of the willingness to engage into a legally binding contract with the other party to get approval. An offer must meet these requirements to be accepted. Its conditions must be clear and communicated to the offeree. The legal relationship must be established. It must seek approval from the offeree. According to S. 2(b), acceptance means full and unambiguous approval to the offer. The objective intention test determines acceptance, leaving it to the parties' discretion. A unilateral contract may come from a performance-accepted offer. Notifying acceptance is as important as knowing the ICA compliant offer. Remember that English law recognizes automated contract offers and acceptances. Accepting an offer becomes a commitment, which, with reflection, becomes an agreement.

It to be noted that data transfer offer and acceptance is lawful. Data communications ideas are lawful under the IT Act to protect electronic contracts. The IT Act, S.10-A, states that using electronic communication for entering into a contract does not invalidate it. As supported by the 2005 UN Convention on the Use of Electronic Communication in International Contracts (UECIC) and the UNCITRAL Model Law on Electronic Commerce (MLEC). Article 11 of the MLEC states that data communications' legality, validity, and enforceability cannot be questioned. UECIC focuses on using electronic communications to create or execute contracts between parties with different locations. Article 12 of the convention states that automated message system exchanges are legal without human intervention.

Let us try to determine if a smart contract satisfies the requirements of a legitimate offer and acceptance based on the aforementioned legal basis. An offer is provided in machine-readable code with agreement terms and thus Codes indicate an intent to sign a contract. By publishing a smart contract on a blockchain network, it is essentially making a legitimate offer. It is assumed that users intending to establish a legal obligation do so when they view the code and consent to the rights and duties it encompasses. Because of this, a smart contract may clearly demonstrate the existence of a legitimate offer as long as it satisfies three requirements: (a) it must be clear; (b) it must be put on a platform; and (c) it must represent the intention to engage into a legal partnership.

The offeree's eagerness to accept the blockchain-published offer is important for acceptance. It is important to remember that the parties retain the freedom to determine what conditions constitute a valid acceptance. Any method allowed by this can be considered valid acceptance, including sending in the required information and documents, completing an action like inserting money into a vending machine, or just clicking the “I Agree” button. Smart contracts may be accepted by signing the offer via a distributed ledger with private cryptography keys or adding digital assets like bitcoin to the blockchain.

Recognizing the presence of valid acceptance is permitted by the fact that the parties signed the agreement using a private cryptography key. Given that the offeree can read and comprehend the offer’s terms, acceptance in the case of a hybrid smart contract is adequately indicated. Furthermore, regardless of the manner in which the offer and acceptance are conveyed, there is a strong presumption in a commercial transaction that the parties intend to establish legal relations. Utilizing an individual’s private cryptographic key to validate a transaction or shift assets is a reasonable assumption that demonstrates acceptance to the offer’s terms. A legitimate acceptance of the offer is therefore shown by the expression of this willingness to be bound. In addition, it is assumed that the smart contract is indeterminate and so infinite until a timeframe is specified. Thus, the parties’ independent engagement with the smart contract proves that an offer and an acceptance exist. The methods and concepts of offer and acceptance are thus similar to those of a standard contract, regardless of the contractual format.

3.1.3. Consideration

Agreements must be made from promises. S.2(d) defines consideration as an act, abstinence, or previous act or abstinence at offer as a prerequisite of a legal contract. It is seen as a gain, profit, or interest for the promisee, or as a loss, damage, or disadvantage for the promisor. A consideration must be worth something in the eyes of the law. The parties shall decide what is reasonable in their own discretion as consideration; whatever may appear small to one party does not lose legal significance. But it needs to convey the offer’s or want. The law of contracts and the sale of products have distinct definitions of consideration; the latter restricts consideration to monetary worth alone, so excluding barter exchanges. This role is comparable in India and the United Kingdom.

Nonetheless, ICA does not recognize this kind of limitation. In the event that the promisee does not get a commensurate advantage, even a clear harm to the promisor may qualify as legitimate consideration. In law, what matters is the content, not the format of the consideration. The mutuality and reciprocity of transaction are the main points of emphasis. The legal concept Quid pro quo is based on the exchange of value, not the quality of consideration. Determining the legitimacy of consideration, for instance, is a factual inquiry. When analyzing the issue to be taken into account in the context of smart contracts, the Taskforce's Report is relevant. According to the Taskforce, a smart contract's consideration may be determined by looking at its behavior or code. Smart contracts' promises with value transaction conditions are reasonable legitimate consideration. For example, a legal consideration arrangement would be one in which the buyer's account would be debited by a predetermined sum upon the shipment of certain products. The compensation for flight delays insured by AXA, which was covered at the beginning of this article, may serve as another real-world example of legitimate consideration under smart contracts. Therefore, a legitimate consideration is created when an automated transfer is subject to the normal premium being paid. Under the ICA, smart contracts that include these kinds of provisions may be rendered legally binding. The aforementioned analysis makes it clear that the ICA does not impose restrictions on the kind or method of consideration, in contrast to the Sale of Goods Act's viewpoint. Furthermore, the legislation does not prohibit the use of cryptocurrencies as consideration, as was covered in earlier part of article. As a result, under the ICA, payment in the form of bitcoin is acceptable.

3.1.4. Legal Intention

The foundational element of a legally enforceable contract is the existence of legal purpose. It is contended that parties' intentions to be legally bound by a contract may be represented using smart contracts. An objective process is used to determine *animus contrahendi*, or the intention to contract. It is crucial to remember that a transaction's commercial character creates an assumption that there was legal purpose. The concept in question was shown in the Edwards v. Skyways case (England, 1964), when the court deemed intent to engage into legal contacts even in the lack of a domestic or social contractual arrangement based on previous commercial agreements. In addition, the courts have deduced purpose from the parties' actions. In India, a comparable method for determining the parties' intentions has been approved. It goes without saying that each instance is unique and that determining such an intention depends on a number of elements, one of which is the possibility of being aware of the legal provisions of the contract.

When determining the legal purpose to engage into a contract, the parties' will, is the primary factor that may be inferred from the specific facts and circumstances of each instance. For example, in sustaining the legality of click-wrap agreements, courts in a number of countries have emphasized the fundamental feature of free will, which is seen to be properly deducible from the ability to review the terms before to clicking “I Agree” button. Smart contracts may be used with similar ideas. The parties’ will continue to be the foundation of a contract notwithstanding their self-executing nature.

The aforementioned analysis makes it clear that in order for a smart contract to be legally enforceable, both parties must be able to demonstrate their desire to act legally. It claims that signing a smart contract with a private key shows your adherence to its conditions. The offeror disclosing the contract’s coded conditions on a decentralized platform to acquire approval and the offeree using a private cryptography key to sign or transfer assets indicate a credible commitment to maintain the agreement. The parties to a smart contract who have read it through and understood it completely may be legally obligated by it since they have indicated that they want to be bound by it. Furthermore, some academics believe that a smart contract’s acceptance of a business offer must result in a legal desire to contract via behavior. Their argument is that there is a presumption of a valid contract in a business setting is persuasive. Taking to its logical conclusion shows that a reasonable person would see a commercial smart contract acceptance as legally binding and enforceable. The conditions of the contract should ideally be sufficiently, clearly, and accurately specified in the code in order to enforce such a contract. Therefore, when a smart contract is used for business, it is enforceable between two parties since it expresses their desire to be governed by the *code de jure.*

3.1.5. Consent on both sides

According to the ICA, *consensus ad idem* is one of a contract’s fundamental components. The willingness of the parties to mutually commit to an agreement is a sign of their convergence of ideas. Real and genuine consent of the parties is required by ICA; moreover, it should not be vitiated by error, force, fraud, undue influence, or deception. The test used to ascertain this kind of consent is impartial. The parties’ awareness of the terms that were accessible to them at the time of contracting may be used to infer mutual agreement. For instance, in the event of an electronic contract, the parties will be bound by the explicit and unambiguous terms stated on the website, even in the event that the terms are entered into without the parties’ knowledge. As long as the court finds that the offeror acted reasonably in making sure the offeree could easily see the terms of the contract, actual awareness of the provisions is therefore not necessary. The conditions of the offer will not be enforceable if they are not obvious or if the offeree has not been reasonably informed of them. On the other hand, if constructive notice can be attributed to the offeree and there is fair notice, the simple fact that there is a language barrier would not impact the contract. This suggests that an offer must be made explicitly and the offeree must have enough time to accept it before mutual consent can be read into a contract.

When electronic contracts are made via websites, there are some issues that comes up. These online agreements, which are also known as adhesion contracts, make the assumption that website visitors are aware of the conditions even if they haven't read them. So "terms of use" are loosely browse-wrapped in a far-off area of the page, and this may lead to visitors being thought to have consented because accessing the website is tantamount to accepting the terms. Due to this dishonest technique, courts have ruled that conditions won't be binding on the offeree until the offeror can prove that enough notice was provided, even if they are near to contract-closing buttons.

The smart contracts are coded, making it hard to tell whether the offeror provided the offeree ample notice of the contract terms. In this sense, it is possible to ascertain if the need of mutual assent is included in the contract by looking back at the previous exchanges and/or communication that contributed to the agreement. Such communication may take the form of written, spoken, or electronic communications. Generally speaking, it is advised that the conditions of offer be sent via email or a "wrapper" contract and made accessible to the parties in a legible format in advance. Therefore, a hybrid contract might be very helpful in determining *consensus ad idem* (or not). These contracts have understandable language and may be used to verify agreement. The usage of private cryptography keys to conduct the transaction and the platform's unambiguous disclosure of the contract's conditions may further demonstrate mutual consent. This follows electronic commerce standards, which recognize electronic signatures as consent. In so far as the code is clear and understandable, the offeree has been provided notice of the terms and an opportunity to examine them, and the contract is entered into with clear notice of the terms, it can be assumed that the parties have understood and agreed upon the terms.

According to the ICA, a contract is formed when the aforementioned basic requirements are met. A legally enforceable contract is created when there is an offer, acceptance, consideration, *consensus ad idem*, and legal purpose. Thus, if smart contracts satisfy the ICA conditions for conventional contracts, their legal enforceability cannot be questioned. The legal precept that a contract's content supersedes its form is supported by this finding. Although a smart contract is often thought of as something different from a traditional legal agreement, it has many of the same important characteristics.

3.2. Application of the ICA, 1872 On Smart Contracts

The present study in the previous section proved that smart contracts are enforceable and legitimate under the ICA. In this section, let's see whether smart contract qualifies analysis by evaluating it in the context of certain procedural criteria, including those pertaining to authentication and record admission, among other things. The procedural aspects that shape the parameters of what constitutes a legally enforceable smart contract must be taken into account in any practical endeavor to fully incorporate smart contracts into the Indian legal system. In this sense, two notable pieces of law are the IT Act, 2000 and the Bhartiya Nyaya Sanhita 2023 (BNS), which establish the rules for electronic contracts. Below is a discussion of how these laws affect smart contracts.

3.2.1. Information Technology Act, 2000

The principal regulatory control over the electronic contract verification process is asserted by the IT Act. Under S.10-A of the Act, which states that using electronic records to express contract formation or communicate offers and acceptances does not render a contract unenforceable, electronic contracts are deemed legitimate. It is important to remember that data or information recorded on a block might be regarded as an electronic record since it is in electronic form. The aforementioned clause is by no means exclusive to India; laws along similar lines have been passed in China, the USA, the UK, and China.

When attempting to harmonize smart contracts with the IT Act, a number of operational problems arise. A matter of concern is to the need of cryptographic signature authentication in smart contracts, as mandated by S. 35 of the IT Act. According to the law, an electronic signature must be authenticated by a Certifying Authority (CA) authorized by the government. It is important to remember in this regard that digital signatures using cryptography are recognized by law as being comparable to handwritten signatures under the IT Act. An asymmetric pair of one private key and one public key, specific to a particular transaction, constitutes a digital signature, as per S. 3 as read with the Guidelines for Usage of Digital Signatures in e-Governance (India, 2010). The sender signs the electronic document using his private key, and the receiver uses his public key to validate the signature. Smart contracts validate their digital signatures using a specific "hash" key. However, in order for a digital signature to be considered legitimate, it must be properly validated by a CA in accordance with the IT Act. Even though smart contracts have the ability to automatically validate their cryptographic digital signature, the IT Act's authentication requirement presents an additional barrier to the seamless integration of smart contracts.

State verification is unnecessary since blockchain, the foundation of all smart contracts, is distributed and take cares of this legal aspect.

According to the UK Jurisdiction Taskforce's Report, if the legislation is interpreted with a purpose, it is possible to comply with the statutory regime's authentication criteria. The report suggests defining "electronic signature" broadly to include a wide range of novel methods for verifying the authenticity of an electronic document, such as the hash key signature of a smart contract. As an example of a very compelling approach to smart contract governance that may be replicated in Indian law, the Taskforce's Report holds that smart contracts satisfy the material conditions necessary for a valid signature. The IT Act has to be reconsidered in light of enforcement-related drawbacks in order to accommodate smart contracts.

3.2.2. Bhartiya Nyaya Sanhita (BNS) 2023

BNS has been quite adaptable to changes in technology. Notably, if certain requirements are met, electronic records may be admitted into court under S. 61 subject to the certain condition under S. 63. Electronic records may now produce legally binding contracts, electronic signatures are no longer illegal or inadmissible, and electronic records are now recognized as evidence.

Despite their groundbreaking technology, smart contracts have been questioned as credible proof. Integrating blockchain validation with the BNS, which requires digital signature authentication under S. 63 is challenging. Such authentication must be conducted in compliance with IT Act S. 35, which only recognizes authentication via a CA. Because of this procedural restriction, author relies on the Taskforce's Report to suggest re-examining the aforementioned clauses to allow for blockchain-based authentication. This way, a simple technicality won't prevent the execution of a smart contract that would otherwise be enforceable.

Another issue with the usual Indian method of valuing evidence is the coded nature of smart contacts. The inability of machine code to be read by the general public, including judges, is a significant barrier to understanding the smart contract itself, has already covered earlier. It may be possible to interpret coded phrases and determine their legal meaning by looking through previous letters and any supporting documentation. Additionally, parties may agree in advance in plain English, which may serve as the foundation for how the smart contract is interpreted. But in terms of allowing the smart contract's code itself to be admitted as key evidence, the courts would need some technical support in order to read and understand it. In this sense, to bridge the gap between the rigor of evidentiary law and the anonymity/pseudonymy of participants in a smart contract, courts and quasi-judicial agencies may need extra documented proof. In addition, the courts should think about assigning experts with standing to interpret the provisions of the agreement. Historically, amicus curiae have aided Indian courts on technical matters. However, standing experts must be able to read, interpret, and explain code as per the legal understanding to the court. In addition, their responsibilities and authority must be precisely defined to guarantee that they support the courts exclusively and do not unfairly influence their rulings. Numerous legal systems worldwide are progressing towards acknowledging proof that is grounded on blockchain technology. On this front, the US has been leading the way. Six US states—Vermont, Ohio, Tennessee, Wyoming, Arizona, and Nevada—have approved laws endowing blockchain recordings with the same evidential value as written documents. Because the blockchain is where smart contracts operate, these procedures are very important. They establish an important precedent that opens the door to affirming the evidence value of smart contracts by clearly recognizing the evidential value of Blockchain technology.

Thus, legally valid smart contracts as contracts will not materialize without procedural procedures to defend contractual parties' rights while limiting abuse. Although enacting a separate law governing smart contracts like to what the US does would accomplish this, author support changing specific sections of the current legislations wherever it is practical to do so in order to make room for smart contracts. For instance, in order to recognize cryptographically verified smart contracts as legitimate electronic records, changes to the IT Act and BNS requirements would be necessary. On the other hand, author think that the ICA provides a built-in regulatory framework that can enforce smart contracts in a manner akin to that of a conventional contract.

4. Regulatory Difficulties: An Unresolved Paradox

Given that the fundamental components of smart contracts may be governed by the ICA, it is clear from the above section that the status of smart contracts can generally be determined by using conventional ICA. But because of the smart contract's unique technical features, there are several obstacles to ICA regulation; two of them have been covered in-depth below

4.1. Territorial Jurisdiction Pinning

It is challenging for conventional legal provisions governing jurisdiction to accept smart contracts from the perspective of procedural law. The Code of Civil Procedure, 1908 (CPC) governs India and establishes jurisdiction in civil disputes. It specifies the proper authority that the petitioner(s) may contact since it incorporates the geographical and subject-matter aspects of such a dispute. A cursory study of the CPC, Ss.15–20 specifies these jurisdictional characteristics, and it becomes apparent that the nature of smart contracts and the idea of "cause of action" are incompatible.

A cause of action is by its very nature a physical notion that depends on geographical boundaries. For example, under S. 20(c) of the CPC, a violation of a contractual agreement in the city of Mumbai would give rise to a cause of action in Mumbai. Nonetheless, smart contracts are implemented using blockchain technology, which is not physically present in and of itself. Instead, the dispersed nodes within a public distributed blockchain may be located anywhere in the world, resulting in many legal claims in several countries. For example, a blockchain with nodes all across the nation may be used to negotiate a leasing agreement carried out by a smart contract within the jurisdiction of the city of Delhi. This would need dealing with several causes of action and tenancy rules. A blockchain may include nodes in various countries, this would be logistically difficult. Smart contracts provide anonymity, making it difficult to verify personal jurisdiction attributes like residency and physical presence. No matter if a smart contract was executed in India, the failure to establish jurisdiction poses legal issues that would make it difficult to enforce in court. First of all, state-to-state variations in the relevant legislation are possible in India; real estate regulations, for instance, might range significantly depending on the state in question. Without jurisdiction, it would be impossible to sue a smart contract for legal rights. Second, jurisdiction determines which court to file in. Thirdly, court fees vary by jurisdiction, making it difficult to evaluate a litigation to establish financial jurisdiction. The range of laws that may apply to a blockchain transactions or event and the worldwide distribution of nodes on the blockchain that aggravate cross-jurisdictional issues make jurisdiction identification crucial.

4.2. Cautions: About Security

A court may need to look at other circumstances in addition to the prerequisites that must be fulfilled for the establishment of a contract. These include elements like ability or competency, error, legality of agreement, etc. In this context, an analysis comprises a look into the parties' identities and the conditions of the contract. However, since smart contracts are based largely on a certain level of secrecy, this kind of investigation becomes difficult. Because smart contracts on public blockchains are pseudonymous, it is impossible to determine the identity of any party involved, which opens the door for illicit transactions. The anonymity provided by cryptocurrencies and blockchain makes it easier for "criminal smart contracts" to operate, which take use of smart contracts' inherent anonymity and lack of party responsibility to commit crimes repeatedly. Since cryptocurrencies are not regulated, there is no way for the government to find out who is who and what the public blockchain transaction was. Smart contracts allow for the conduct of physical crimes including contract murders, ransomware, and the theft of documents or digital security keys. The identity of the contracting parties is concealed by a public blockchain. To mass-manufacture phony certificates, for instance, a smart contract may be programmed to pay a reward for the transmission of the digital certificate key of an issuing authority. A person may implement such an agreement in the form of a smart contract, which would self-execute with little involvement from the criminal and make it far more difficult for law enforcement to follow and monitor illicit activities. In addition to being co-conspirators, the parties could also be victims of crimes. This results from the inability of a smart contract running on a public blockchain to track the identity of a user. An entity that would normally be prohibited might be able to sign harmful contracts for fictitious cloud services due to this absence of identity verification. Another problem that arises is bringing a party to court in the absence of any distinguishing features. It is not possible for the court or the party to gather information beyond the Blockchain Address of the user/party, hence it might be challenging to apply penalties against an anonymous organization.

4.3. Solutions for the Juridical Problems

As was shown in the preceding section, it is challenging to balance the technical reality of smart contracts with the procedural features of contract creation. Geographical jurisdiction is the most pressing issue. Section 20 of the CPC outlines three possible litigation venues: site of business, voluntary habitation, or location of action’s emergence. The anonymity that a public blockchain often ensures makes it difficult to determine the precise locations of the people making contact. Even a domestic blockchain inside national boundaries has nodes throughout the country, making them eligible for a cause of action under S. 20(c) of the CPC. Any smart contract dispute may be heard in any court in the country, undermining the legislative goal to limit the CPC’s exclusive territorial jurisdiction. Two solutions to this conundrum are given here. The first solution covers party autonomy in international commercial arbitration to accommodate smart contracts into present ICA. The second alternative suggests a major overhaul of procedural legislation to accommodate a smart contract-specific dispute resolution process. It is important to note that the two options listed below represent a significant divergence from India’s current procedural law and only serve to outline the general parameters of widely accepted approaches to the jurisdictional problems raised by smart contracts. Only once smart contracts become popular in India and raise difficulties unique to that nation can a comprehensive solution be conceived.

4.3.1. Autonomy of the Party

According to party autonomy, contracting parties should be allowed to pre-agree on the venue and legislation for resolving disputes. This basically indicates that any agreement reached by the parties on the jurisdiction of a dispute supersedes the conventional methods specified by the law to determine such jurisdiction.

Party autonomy has long been a cornerstone of private international law. The Rome I Regulation oversees all EU-foreign trade. Article 1 of this Regulation defines civil and commercial dispute contractual responsibilities. Thus, private international law jurisdiction covers smart contracts. Article 3 of the Regulation allows parties to present their contract to a forum selected in the contract, regardless of its geographic proximity to the contract matter. Several court opinions have concluded that in cross-border commercial transactions, the parties' choice determines jurisdiction and that an alternative technique should only be employed if it is not explicitly established.

The ICA, which does not in and of itself let parties to choose the law they choose to use, governs Indian law with regard to domestic transactions. But according to the judiciary's interpretation of S.28 of the ICA, parties may already subordinate courts' jurisdiction to one or more fora, provided that the fora have been granted this authority by the CPC. Suppose S. 20 of the CPC enables a contract dispute action to be brought in Mumbai, Delhi, or Bangaluru, the contract may require all associated litigation to be filed in Mumbai courts alone. Author suggests that the principal smart contract identify the forum of choice for the litigants; otherwise, the disagreement may be handled in any blockchain node country. It ensures anonymity, the system's foundation, as a core remedy in the blockchain network. In this spirit, it is not analyzed S. 20(a) and (b) of the CPC, which demand name disclosure, which negates one of smart contracts' main benefits. Each node's blockchain address may be used to determine its location without compromising anonymity. Smart contracts tend to be pseudo-anonymous, therefore anonymity does not hinder court enforcement. Additionally, the claimant may authenticate their identity by using the cryptographic key they signed the agreement with. Emerging technologies like Ethereum will enable party identification. The decentralized framework of blockchain-based smart contracts allows a single disagreement to lead to rival jurisdictional claims, notwithstanding the CPC's applicability. In order to restore the effectiveness of settling conflicts linked to smart contracts, party autonomy must intervene.

4.3.2. Dispersed Jurisdiction

As previously stated, distributed jurisdiction represents a significant shift from the nation's current conflict resolution legislation, requiring extensive substantive and procedural changes to be put into place. It is not a solution that can be used anytime soon and cannot be accommodated within India's conventional adversarial dispute settlement procedures. It only represents an emerging policy strategy that, should smart contracts become widely used as a viable substitute for conventional contracting, deserves careful thought. This model is used to start a discussion about smart contract solutions, however future policy approaches should be formed by smart contract practical reality and how it interacts with Indian legal processes. Currently, these empirical elements are lacking.

In distributed jurisdiction, blockchain-based anonymous judges resolve disputes. Blockchain service company "Aragon Network" (GitHub [2019?]), pioneered this idea. A group of peers who sit in judgment and write a verdict determine a matter, striking similarities to the jury system seen in American law. A more fitting comparison would be the contemporary Parliamentary Debate style, in which the judges choose the winning and losing teams based on the quality of their criticism, and the judgment is founded on the foundation of mutual trust.

A party puts a bond worth a certain amount of bitcoin and written reasons supporting his position whenever he wants to contest a contract that originated in the Aragon blockchain network. As a result, the defendant posts his bail and written arguments, which are then submitted to a panel of judges who are all anonymous and have posted bonds themselves. This panel's members are selected at random from among the blockchain network's users, and they won't communicate with one another throughout the case to preserve their anonymity. Thus, there is financial interest in the settlement process for both the parties and the arbiters. These bonds' value is used to pay for the blockchain's operational expenses; it is comparable to the "court fees" that a plaintiff must pay to have his or her case heard in any court of law. Each judge issues a ruling after giving careful regard to the written arguments presented by both sides and determines which party will get the case. Just as in a traditional court, the majority ruling determines the outcome of the case, and the judges get financial compensation according on whether or not they agreed with the majority. This should encourage judges to think critically about the issue at hand and make well-reasoned rulings. Since the judges remain nameless throughout the case, any possibility of panel collusion is eliminated. Additionally, this system pushes judges to support the majority as much as possible in order to enhance their “reputation.” These “respected” judges would serve on the panel in the event of an appeal, which would be entitled to a greater bond from the party making the appeal as well as higher compensation for the judges. Thus, this system ostensibly offers a venue for the impartial judges to settle conflicts, with judges in “higher courts” predicated on their track record as competent arbiters - akin to the theoretical foundations of the Indian judicial system. The present Aragon Network-style approach is based on the laissez-faire regulatory theory, where conflicts arising from smart contracts are settled without the need for government action. However, it is preferable that the state establish a dispute resolution network along similar lines, as smart contracts need to be governed by the state.

5. Managing Security Issues Through Third-Party Intervention

Ever since the digital behemoth Alibaba filed for a patent on the idea of third-party intervention, the idea has grown in favor. To put it simply, illicit smart contract transactions are identified by third-party involvement on the blockchain. The goal is to prevent criminal use of smart contracts by permitting outside action in situations when illicit activity is suspected. It should be emphasized that while public blockchain prevents users from being really identified, illegal smart contracts may be hampered by decentralization and the ensuing access to transactions via the blockchain because of the visibility and accessibility of the open-source code running on it. Furthermore, in addition to the two extremes i.e. Public Blockchain and Permissioned Blockchain and there is a third option known as Consortium Blockchain, which combines the efficiency and confidentiality of a permissioned blockchain with the advantages of a public blockchain’s decentralized regulation. Within a Consortium, a central authority uses a consensus-building process to verify the transaction and, more importantly, makes it possible for other parties to serve as intermediates, such as central administrators. Considering the appalling condition of cyber-security in India, any choice would necessitate the legislature taking extreme measures. The platform operators may adopt internal data security policies, monitor transactions on a regular basis, raise awareness among stakeholders, and other policy steps in the interim. Furthermore, “The Ring of Gyges,” one of the first publications to address the theoretical concept of illegal smart contracts, suggested involvement via trustee-based tracing, which entails giving trustees the authority to track transactions based on a user’s need to register. It suggests "trustee-neutralizable" smart contracts, which do not need user registration and allow certain sets of authorities to remove a contract based on predetermined criteria.

A bill called the Financial Technology Protection Act (United States, 2018), which was recently introduced in the US Congress, offers a potential remedy to the criminal use of smart contracts. It establishes procedures for looking into criminal and terrorist activity carried out through "new financial technologies," which includes digital currency. Based on this, it follows that allowing third parties to step in as trustees might lessen the growing criminalization of smart contracts that rely on the participants' anonymity. Furthermore, the integration of the virtual transaction with the real world would be facilitated by the involvement of a third-party authority. For example, obtaining an authorized certification is necessary to confirm that someone is the rightful owner of property or that they possess a public key. This means that by allowing other parties to intervene or encouraging a consortium blockchain, smart contracts that carry out illegal transactions may be marginalized.

Conclusion & Suggestions

The smart alternative to traditional contracting is not misfit. The ICA recognition of smart contracts is difficult. Smart contracts cannot be regulated laissez-faire at the cost of contractual parties. This article has identified these vices as routes for cyber theft, money laundering, and illegitimate contracts for physical offenses like hit contracts. Because these vices are bad for society, there has to be some kind of official control. This view is especially strong in light of present research, which shows that smart contracts may be subject to the same substantive law as traditional contracts. The advantages and potential of smart contracts much beyond the technological and legal obstacles that can be sufficiently resolved. Even though they are a more sophisticated and advanced kind of transaction, smart contracts include all the basic elements of conventional agreements, covenants, and records like an EDI transaction or a vending machine. Legally speaking, smart contracts satisfy the conditions necessary to be considered legitimate and may be governed similarly to conventional contracts.

Investigating the degree of its enforceability and the potential ramifications is the more difficult task. This, in author view, is based on a thorough examination of smart contracts that aims to understand their implications for legislation like the BNS, the IT Act, and the CPC from an implementation standpoint. Based on present analysis, it is believed that some procedural aspects of the law require reform, especially the decentralization of digital record licensing, the formulation of dispute resolution methods that take into account the distributed nature of smart contracts, and the appointment of standing experts by the courts to interpret and explain coded contracts, among other things.

As an outcome in theory, smart contracts are covered by the ICA and are thus not subject to further law. This paper, which restricts lawsuits by internally rectifying the deviations via self-execution, highlights the technological resilience of smart contracts in removing human participation. It highlights the incredible potential that smart contracts hold for the Indian economy, and as a result, it is also stressing the importance of learning from the legislative and judicial efforts of those jurisdictions that have worked to establish smart contracts as fully-functional legal agreements that can be enforced in court.

How to cite this article:

ABNT

NIKAM, Rahul J. The legality of smart contract through the lens of Indian Contract Act. *Passagens rev. int. hist. pol. e cult. jur.*, Niterói, v. 17, n. 3, p. 522-551, set.-dez. 2025. https://doi.org/10.15175/w0ztm173

APA

Nikam, R. J. (2025). The legality of smart contract through the lens of Indian Contract Act. *Passagens rev. int. hist. pol. e cult. jur.*, *17*(3), 522-551. https://doi.org/10.15175/w0ztm173

Editor responsible for the evaluation process:

Gizlene Neder

References

CLEMENT, Alexandre. fizzy by AXA: Ethereum Smart Contract in details. *Medium*, 24 May 2019. Available at: https://medium.com/@humanGamepad/fizzy-by-axa-ethereum-smart-contract-in-details-40e140a9c1c0. Accessed: 2 May 2025.

ENGLAND. Queen's Bench Division. Decision. Edwards v Skyways. Apr. 11, 1964. *All England Reporter*, 494. Available at: https://ipsaloquitur.com/contract-law/cases/edwards-v-skyways/. Accessed: May 2, 2025.

ENGLAND. Thornton v. Shoe Lane Parking Ltd. England and Wales Court of Appeal (Civil Division). Decision 1 QB 163. 18 Dec. 1970. *Wales Law Report*, 1. Available at: https://www.casemine.com/judgement/uk/5a8ff87860d03e7f57ec103b. Accessed: 2 May 2025.

GITHUB. *Aragon/whitepaper*: An opt-in digital jurisdiction for DAOs and sovereign individuals. [2019?]. Available at: https://github.com/aragon/whitepaper. Accessed: May 2, 2025.

HART, Oliver D. *The theory of contracts*. Cambridge, Ma: Dept. of Economics, Massachusetts Institute of Technology, 1986.

INDIA. Indian Contract Act, of 1872 (ICA). *Act No. 9 of 1872*, 25 Apr. 1872. Available at: https://www.indiacode.nic.in/bitstream/123456789/2187/2/A187209.pdf. Accessed: 12 Sept. 2025.

INDIA. The Information Technology Act, 2000 (IT Act). *India Code*, Jun 9, 2000. Available at: https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf. Accessed: Sept. 12, 2025.

INDIA. Ministry of Communications and Information Technology. Guidelines for Usage of Digital Signatures in e-Governance. Dec. 2010. Available at: http://bit.ly/4gro5f0. Accessed: Sept. 12, 2025.

INDIA. Ministry of Law and Justice. *The Bharatiya Nyaya Sanhita, 2023*. Nº 45 of 2023.Dec. 25, 2023. Available at: https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf. Accessed: Sept. 12, 2025.

HSIAO, Jerry I.-H. “Smart” contract on the blockchain-paradigm shift for contract law? *US-China Law Review*, v. 14, n. 10, 28 Oct. 2017. Available at: https://www.davidpublisher.com/index.php/Home/Article/index?id=34210.html. Accessed: 2 May 2025.

UNITED KINGDOM. Law Comission. *Smart legal contracts Advice to Government*. London: HH, 2021. Available at: http://bit.ly/46kup38. Accessed: May 2, 2025.

SINGAPORE. Singapore International Commercial Court. *B2C2 Ltd v Quoine Pte Ltd [2019] SGHC(I) 03*. Mar. 14, 2019. Available at: https://www.elitigation.sg/gd/gd/2019_SGHCI_3/pdf. Accessed: May 2, 2025.

TJONG TJIN TAI, Eric. Force Majeure and Excuses in Smart Contracts. *European Review of Private Law*, v. 26, n. 6, p. 787-804, 1 Dec. 2018. https://doi.org/10.54648/erpl2018055

UNITED STATES. Congress. H. REPT. 115-984 - *Financial Technology Protection Act*. Sept. 26, 2018. Available at: https://www.congress.gov/committee-report/115th-congress/house-report/984/1. Accessed: May 2, 2025.

VATIERO, Massimiliano. Smart Contracts vs Incomplete Contracts: A Transaction Cost Economics Viewpoint (September 25, 2018). *Computer Law & Security Review*, v. 46, 105710, September 2022. https://doi.org/10.2139/ssrn.3259958

VENTURA, Tim. Propy’s Mission to Transform the Real Estate Industry. *Medium*, 24 Jun. 2020. Available at: https://medium.com/@timventura/propys-mission-to-transform-the-real-estate-industry-c03b76d012ba. Accessed: 2 May 2025.