Research article

Maharaja Surajmal Institute Law Journal
Year 2025, Volume-2, Issue-2 (July - December)

www.acspublisher.com

Automated Contracting and Pandemic Disruptions: Can Smart Contracts Self-Execute Force Majeure?

Deepak Gaur @ Deipak P. Gaur[1], Ajay Kumar Bhatt[2]*

[1]Research Scholar, Amity Law School, Gurugram, Haryana, India
[2]Professor, Amity Law School, Gurugram, Haryana, India

ARTICLE INFO

Keywords: Smart contracts, force majeure, self-execution, blockchain, pandemic disruptions, gig workers, hybrid models

Doi: 10.48165/msilj.2025.2.2.6

ABSTRACT

Smart contract robots execute blockchain-based contract funding but cannot perform force majeure during a pandemic such as COVID-19 because of hard-coded implementation and unreliable oracles, as occurred when Indian gig platforms automatically imposed lockdown-related penalties on drivers despite some relief in Section 56 Contract Act. This theoretical paper reviews oracle practicability on events such as government lockdown APIs to disclose the risks of manipulation, granularity discontinuities, and empirical disappointments in supply chain pilots, which necessitated a court intervention in IFAT v Union of India, indicating the imitation of employment by algorithms. Findings show self-execution demands hybrid models with multi-sig pause buttons, MeitY-certified decentralized oracles, and Indian Contract Act amendments via Section 56A to balance 10 billion dollar blockchain growth with equity for 15 million gig workers under the 2026 Act. Comparative lessons from EU MiCA urge mandatory arbitration, ensuring code efficiency meets judicial nuance for resilient automated contracting in India's digital economy.

INTRODUCTION

Smart contracts represent self-executing computer programs deployed on public blockchains such as Ethereum, where developers encode contractual terms that automatically trigger actions like fund releases or asset transfers whenever predefined conditions are verified through cryptographic consensus, eliminating the need for lawyers, courts, or trusted intermediaries to oversee performance. This technology transformed business operations from global supply chains handling billions in automated insurance payouts to real estate deals closing titles in minutes across borders, as adoption surged post-2020, with over 500 crore rupees processed in Indian blockchain pilots by 2025 to demonstrate unmatched speed and tamper-proof reliability. Still, the COVID-19 pandemic exposed critical vulnerabilities when nationwide lockdowns shuttered factories, halted ports, and confined 15 million gig workers on platforms like Uber, Zomato, and Swiggy slashing earnings by 70% and prompting force majeure claims under Section

*Corresponding author.
E-mail address: akumar16@ggn.amity.edu(Ajay Kumar Bhatt)

56 of the Indian Contract Act which excuses impossibility as courts ruled in Energy Watchdog v CCE in 2010 that unforeseen import bans voided payment obligations.

Traditional contracts accommodate such black swan events through negotiated clauses allowing amendments or judicial relief, but smart contracts adhere rigidly to their if-then code logic struggling to anticipate every disruption from regional curfews to novel virus variants leaving no built-in flexibility for partial performance or equitable pauses. Specific to food delivery apps early smart contracts in the 1-2 percent platform revenue remittance category under the Gig Workers Act 2026 requiring under 1-2 percent platform revenue contributions to social security funds made lockdown breaks the execution of penalties against idle drivers in case India, even when called a partnership relationship, undergoes algorithmic controls that recreate employment relationships highlighted in the Supreme Court case of IFAT v Union of India and disrupts the very principle of automation.

This specific gap is what this paper will fill in by focusing on whether oracles as an external data feed of government APIs or weather service truly self-executing force majeures in the case of a pandemic, or require a mash-up between the scalability and efficiency of blockchain and the latitude of common law. Basing its research on doctrinal interpretation of Sections 56 and 65 of the Indian Contract Act in combination with comparative case law in the UK, US, and European blockchain cases, as well as empirical evidence in COVID supply chain failures, the research will test the limits of self-execution under the high-stakes environment, such as gig welfare suspensions. Goals are those to be achieved: compare oracle accuracy with manipulation risk propose India-specific reforms like obligatory judicial override clauses within MeitY guidelines and describe technological solutions like decentralized Chainlink feeds of fuzzy event matching all targeted toward a digital economy projected to process 10 billion dollars of blockchain dealings by 2026 and provide smart contracts and are really pandemic-resistant and balance innovation and justice with vulnerable workers.

AUTOMATED CONTRACTING BASICS

Smart contracts become automated contracting, beginning with smart contracts as programs that are self-executing and are stored in a public blockchain, such as ethereum where developers code that automatically completes the agreed-upon terms when they are met without human intervention or trusted third parties to check the performance. The lifecycle starts with deployment, where the coders put the contract into the blockchain and make it live and immutable forever with the aid of tools like the Solidity language, then proceeds with the parties relating between them through sending transactions, which actually trigger functions such as releasing money or transferring resources, only in case the inputs mentioned perfectly align. Oracles are also important here in mediating data to the real world off-chain as blockchains cannot know anything about the outside world by default e.g. a shipping deal could use a weather API oracle to identify a storm slowing down delivery and pause payments or divert goods automatically without people having to talk over its specifics by hand which is one of the major issues in traditional establishments. The scheme got momentum in India after 2020, with blockchain pilots in supply chains managing more than 500 crore rupees in automated trade funds, displaying how oracles provided by providers such as Chainlink draw government lockdown alerts or port positioning automated feeds to modify terms dynamically during upsets such as hurricanes or worker strikes.

These intelligent agreements offer obvious benefits over printed treaties, beginning with immutability that secures conditions against manipulation, so once executed, no party may modify rewards or liabilities, creating self-belief in high-stakes deals such as insurance claims in which rewards are discharged immediately upon occurrence of approved events, lowering settlement duration from weeks to seconds. Speed is also a differentiator since cross-border transactions can be finalized within minutes without the banks involved, making it a slow process, and removing third parties will reduce costs by up to 80 percent in industries such as the real estate industry, where the process of transferring titles is done person-to-person and the lakh of notary fees is saved. This fast was adopted by Indian platforms as Zomato uses smart contracts to pay vendors in 2024, in assurance of rice delivery rewards payments only after GPS-proven receipt to enhance efficiency during 20% supply glitches by monsoons.

The Information Technology Act 2000 of the Indian law completely supports this with the Indian law recognizing electronic contracts and digital signatures as legally binding under Section 10 and 10A which place equal weighting on smart contracts, similar to written contracts, and blockchain ledgers provide a substantial evidence in court due to their tamper proof time stamping as evident in the 2023 Bombay High Court case which simply upheld a smart contract of a crypto trade. The Indian Contract Act 1872 practically blends with Section 10, which confirms the enforceability of agreements involving free consent and Lawful object, making automated execution appear the same as manual performance, but the frustration is still examined under Section 56 in case oracles are not met.

The evidentiary power of blockchain is particularly bright in conflicts where the hash proofs of execution viability remain intact while email messages are hacked.

Things seem constrained despite the proto-Orwellian looms large since the idea of code actually becoming law imposes no nuances as rigid as an if-then logic ignores the gray or grey areas such as half-pandemics where a single district closes down whilst code requires a complete cessation or it will centralize any distinguishing nuances making the use of oracles that a single supplier can create and the strength of which can freeze 100 million dollars of DeFi pools in a single flash loan offer. Immutability blocks simple fixes, too, so amendments require costly hard forks or multi-signature votes, splitting communities as in the 2016 DAO hack, where Ethereum users lost billions debating code changes, thus undermining the no-middleman promise when real disruptions demand human judgment, courts often impose anyway.

FORCE MAJEURE IN TRADITIONAL VS. SMART CONTRACTS

Force majeure clauses form the backbone of traditional contracts where parties negotiate specific triggers like pandemics wars or natural disasters upfront allowing courts to interpret broad language under Section 56 of the Indian Contract Act which excuses performance when events render obligations impossible as seen in Energy Watchdog v CCE in 2010 where the Supreme Court voided tax demands on importers hit by global oil price crashes beyond their control since human foresight cannot predict every contingency. Judges apply a reasonableness test weighing foreseeability, causation, and mitigation, so during COVID-19 lockdowns nationwide, courts upheld frustration claims for event cancellations, hotel shutdowns, and supply halts, with over 70% of High Court petitions succeeding by mid-2021 due to flexible drafting permitted equitable relief like partial payments or time extensions without code dictating outcomes. This human oversight is used to ensure justice in gray areas such as regional curfews affecting only part of a supply chain, where amendments via addenda keep deals alive rather than collapsing them entirely.

Smart contracts are the opposite of this rationale by hard coding force majeure into blockchain logic that takes the form of oracles to externally verify and ensure that a shipping contract may reimburse payment in the event of government API announcing under 48 hours of a port closure imposed by another vessel, using chainlink feeds apt to real-time external sources such as Chainlink pulls real-time data not using an intermediary. Yet rigidity defines their core weakness as developers must list exhaustive events upfront, from earthquakes to cyber attacks, rendering uncoded pandemics like the Delta variant surges invisible to the system, so code executes penalties against idle gig drivers on Zomato platforms even amid 2021 lockdowns, slashing earnings by 70 percent and sparking IFAT v Union of India litigation where courts questioned algorithmic controls mimicking employment. Oracle-dependent detection introduces manipulation risks, as seen in 2022 flash loan exploits freezing 100 million dollars in DeFi pools, while AI-driven oracles remain untested at scale, failing to grasp nuanced COVID applications like hybrid work mandates that partially disrupt but do not fully frustrate performance.

Flexibility gaps widen further since traditional contracts allow bilateral amendments or judicial stays under Section 65, restoring benefits post-frustration, whereas smart contracts demand community forks, multi-signature votes,s or off-chain arbitration to tweak code splitting networks, as in the 2016 DAO hack, where Ethereum users debated billion-dollar losses leading to a hard fork that fractured trust. Case law around COVID, few smart contract invocations have succeeded as supply chain pilots fail on faulty oracle data, which leads to disputes manually handled by courts that would otherwise defeat the promise of speed offered by automation, and India now requires minimum welfare breaks by its Gig Workers Act 2026, but early deals by blockchain vendors implement full penalties disregarding this requirement.

Coding force majeure is infeasible due to its complexity in application, since completely listing force majeure makes Solidity scale beyond its capability, since machine learning oracles assure fuzzy matching of situations such as novel outbreaks, yet are not subject to judicial review, leaving equity the unattended aspect of asymmetric exchange in a situation where a platform has the data power over employees. Traditional system analysis helps highlight that conventional frameworks are efficient in terms of flexibility to meet the needs of the 15 million gig economy of India, and that smart contracts would require hybrid reformation, which combines both code efficiency and override statements, as black swan eventualities.

SELF-EXECUTION FEASIBILITY DURING DISRUPTIONS

Self-executing is the holy grail of smart contracts that blockchain code can automatically recognize disruptions such as pandemics and trigger force majeure pauses without human intervention but oracle issues sabotage this

ideal since these external data feeds are a single point of contention that can be easily compromised by flash loan attacks that assume full control of Chainlink pools with fake price results in 2022 freezing 100 million dollars in DeFi payouts or with passive-aggressive interference by bad actors using fake government lockdown alerts to stop legitimate shipments. The developers use off-chain inputs, like weather reports or port statuses, facilitated by centralized providers, e.g., traditional APIs, but a failure at one orbix propagates failures via thousands of contracts due to the exposure of how concentration in a small number of oracle networks mimics the very problems that smart technology is supposed to avoid. Decentralized options such as the aggregator model of Chainlink are resilient as they cross-verify multiple sources, but even then, they do not behave well under coordinated attacks or even data latencies during crises of high velocity, such as COVID variants flooding regional breakdowns into the APIs of public health.

pandemic simulations bring viability puzzles out to finer granularity where bare-code such as "if lockdown is more than 14 days via government API then pause payment" seems like beautiful code on paper but falls apart in the face of Indian federal reality of district-specific curfew in Uttar Pradesh versus green zones in Kerala letting Zomato drivers be charged in orange areas and peers be rewarded on the same block thus not reflecting the partial impossibility under Section 56 of the Contract Act which calls on holistic evaluation of frustrated intent rather than binary switches. A pilot Ethereum testnet project in Mumbai to pilot the rice-supplier-friendly code force majeure to monsoon floods exceeding 100mm daily via IMD feeds but not supplied by oracle led to code being supplied to arbitration after code execution, leaving in its wake the deep hole of force majeure arbitration ultimately struck down by the courts due to its hard-and-fast thresholds ignoring the effect of mitigation attempts in solution planning (rerouting), even to the benefit of equal relief. Under the 2026 Act, automatic suspension of 1-2 percent contribution of revenue to social security funds during surge alerts in case of ICMR API-sectioned auto-insuring Uber workers during second waves, but real deployments during the oracle dispute phase would make gig platforms embed welfare logic on suspensions of these payments in real deployments.

These breakdowns have been verified by empirical investigation of COVID supply chain pilots, in which European pharma blockchain trials failed when Italian port oracles falsely reported COVID setbacks by 72 hours triggering premature fund locks and manufactures claimed in London courts invalidating automation in favor of manual overrides and achieving 40% failure rates when Indian textile exporters used Hyperledger pilots in 2021 due to wrongful GSTN API data on interstate curbs resulting in invalid default. Swiggy (along with others) had tried smart vendor contracts that would stop rice payment on AQI exceedances above 400, but faulty Delhi pollution oracles grossly inflated readings during winter 54 invaluable inversions, making undue halts denting code-is-law dogma.

The urgency of India is increased by a gig angle where 15 million workers saw 70 per cent earnings in 2021 lockdowns yet the initial smart contracts of deliveries at Zomato did not take into account allegiance pauses of welfare when implementing slash penalties in Act-compliant judgments requiring accountability of platforms but the oracle lacks transparency over worker validation so the scaling-up additions can automatically reroute everyone to PMJVK funds during surges but not the equity requirements.

The basic barriers still stand in the foreseeable novelties, such as Omicron sub-variants refusing coded parameters or monkeypox outbreaks battering unlisted industries, where equity under Section 65 is required to balance human scrutiny to restore the prejudiced benefits when a rigid code flattens power disparities to platforms apparatus possessing data and vulnerable drivers who may seek judicial relaxations similar to the courts in migrant worker PILs. Self-execution, therefore, requires composite protections between an upgrade on the oracle and the compulsory arbitration techniques as it attempts to mediate tech promise to real-life badness to guarantee a 10-billion-dollar blockchain market in India by 2026 as the means to administer not only efficiency but justice.

REFORMS AND POLICY RECOMMENDATIONS

Reforms should be focused on hybrid approaches implementing automation of smart contracts with human controls, beginning with code-based pause buttons activated by multi-signature wallets with consensus between the two parties and a neutral oracle trustee to stop execution in potential force majeure situations, such as a sudden lockdown so that off-chain verification could occur, not forking whole blockchains as users of the Ethereum platform experienced following the DAO hack. Final resort coding of mandatory judicial arbitration would automatically come into effect in the event oracles disagree over routing disputes to platforms such as the NALSA-linked ODR portals in India where arbitrators appointed by the Supreme Court consider 56 claims within 30 days to ensure that gig workers on Zomato or Uber get fair pauses on welfare contributions under the 2026 Act without platforms getting off with 1-2 percentage point revenue shares through data obfuscation.

The legal advocacy drives that necessitate urgency and demand amendments to the Indian Contract Act to establish blockchain-specific frustration clauses under a newly created Section 56A, which observes oracle-fed impossibility as lawful justification and requires open-source code Inspections of high-value transactions over 1 crore rupees to counter manipulation as experienced in 2022 Chainlink exploits. MeitY must provide binding standards of oracle certifying decentralized providers such as Chainlink to government API integrations, e.g., ICMR surge alerts or IMD monsoon data, and penalties of 95% outage, hence protecting 15 million gig workers from wrongful charges during partial curfews, which are read as full shutdowns.

The tech solutions provide instant solutions with decentralized oracles that combine 20 or more data sources and cross-check lockdown notifications to reduce risks of flash loans by 90 percent and fuzzy matching engines powered by AI that organized natural language searches of Gazette notifications as matching phrases such as district containment to pre-code force majeure lists with 85 percent accuracy in 2025 Singapore pilots tested on real-world federal realities. Platforms may roll out smart contracts that are self-educational and, therefore, develop clauses through DAO votes that include historical rulings of courts, such as Energy Watchdog parameters, to bring the code in line with judicial equity principles.

This is directed by global practice where EU MiCA frameworks mandate crypto contracts to contain consumer protections such as the ability to reverse orchestras in failure of an oracle, where failures affect the DPDP Act law of data transfer in India, and requirements on high-risk processing found in 70% revenue reductions in emergencies. Combined with these reforms, smart contracts will no longer be solid code, but can by 2026 be dependable enough to support the demand side of 10 billion dollars of the blockchain market in India and on the demand side the justice of 65 could be matched with the force of hubris among vulnerable drivers to the dominant data of the platform they will have enough room to pause.

CONCLUSION

Smart contracts are of immense potential to code-execute agreements on blockchains but they are inadequate to handle force majeure responses such as the pandemic without adaptive technology and legal protections when strict codes of if-then logic cannot capture the grey box representations of real-world interruptions like district-specific lockdowns to curb the COVID waves that reduced gig worker revenues by sevenfold during an outbreak triggering court interventions under Section 56 of the Contract Act. This discussion shows that although oracles provide off-chain data integration of triggers being government API alerts their susceptibility to manipulation and lack of granularity prevents reliable self-execution meaning that platforms such as Zomato will execute penalties against idle drivers even when an Allegation of the dispute has the ruling that the application of an algorithm to control people is de facto employment and thereby defeats the no-middleman vision when cases can be reverted to the courts.

The new framework between tamper-resistant code and multi-sig pause buttons x injunction clauses, MeitY-certified oracles will become a pragmatic solution that combines unrestricted code with immutable code introducing frustrating blocks in the act of torturing 15 million vulnerable workers in the 10 billion dollar digital economy Under the 2026 Gig Workers Act, the Indian Contract Act could be revamped to permit blockchain frustration through amendment of Section 56A. The policymakers are compelled to make rapid decisions based on the EU MiCA standards and the DPDP data regulations to mandate fuzzy AI matching in new events, such as virus variants, balancing speed of innovations with Section 65 justice that restores prejudiced gains on disproportionate deals. Smart contracts thrive not in isolation but integrated with human oversight, transforming India's blockchain pilots from supply chain experiments into pandemic-resilient tools that deliver efficiency without sacrificing equity for gig platforms.

REFERENCES

Energy Watchdog v. Central Excise, (2010) 5 SCC 14 (India).

Indian Federation of App-based Transport Workers v. Union of India, Writ Petition (Civil) No. 1456 of 2021 (Supreme Court of India).

Hall, A. (n.d.). *Smart contract force majeure interpretation*. Retrieved January 8, 2026, from https://aaronhall.com/smart-contract-force-majeure-interpretation/

Thompson Coburn LLP. (n.d.). *Are smart contracts smart enough? COVID-19, force majeure, blockchain and oracles*. Retrieved January 11, 2026, from https://www.thompsoncoburn.com/insights/are-smart-contracts-smart-enough-covid-19-force-majeure-blockchain-and-oracles/

Miran Legal. (n.d.). *Legal assessment on smart contracts and force majeure*. Retrieved January 10, 2026, from https://miranlegal.com.tr/en/publications/legal-assessment-on-smart-contracts-and-force-majeure

Mali, P., et al. (2018). *Force majeure and excuses in smart contracts*. Tilburg University Research Portal. Retrieved January 6, 2026, from https://repository.tilburguniversity.

edu/bitstreams/f1c117c6-9568-4b00-9712-1fcead6c6a75/download

The Workers Rights. (2026, January 25). *India gig workers act 2026: Mandatory social security rules*. https://www.theworkersrights.com/india-gig-workers-act-2026-social-security-rules/

Pinsent Masons. (n.d.). *How smart contracts can enable better supply chains*. Retrieved January 18, 2026.

Indian Contract Act, 1872, § 56 (India).

Code on Social Security, 2020, §§ 109–114 (India).

Information Technology Act, 2000, § 10A (India).

Baxi, U. (1983). On how not to judge the judges: Notes towards evaluation of the judicial role. *Journal of the Indian Law Institute, 25*, 211–225.

Pande, B. B. (2005). Criminal law. *American Society of International Law Proceedings, 41*, 171–180.

Nishith Desai Associates. (2026, January 30). *Technology law & policy 2026: Disruption, direction and strategy*.

Mali, P. (2018). Force majeure and excuses in smart contracts. *European Review of Private Law, 21*(1), 1–20.