



<https://doi.org/10.62585/ilhr.v4i1.132>

Journal of International Law & Human Rights 	Volume and Issues Obtainable at Centeriir.org Journal of International Law & Human Rights ISSN (Print): 3007-0120 ISSN (Online): 3007-0139 Volume 4, No.1, 2025 Journal Homepage: http://journals.centeriir.org/index.php/jilhr	 Center of Innovation in Interdisciplinary Research
---	--	--

Enforcing Code: Doctrinal and Practical Remedies for Smart Legal Contracts in Pakistan

Waqas Rafiq¹

Muhammad Bilal²

¹Ph.D. Law Scholar, University Gillani Law College, Bahauddin Zakariya University, Multan. Lecturer, Department of Law, University of the Punjab, Gujranwala Campus, Punjab. Email: waqas.rafiq@pugc.edu.pk

²Associate Professor/Principal University Gillani Law College, Bahauddin Zakariya University, Multan. Email: mbilal@bzu.edu.pk

ABSTRACT

Smart legal contracts, which are self-executing programs encoded on blockchain technology, fundamentally transform the formation, performance, and enforcement of contractual agreements by automating obligations in an immutable and decentralized environment. This study critically examines the extent to which Pakistan's existing contract law framework—primarily governed by the Contract Act, 1872—can effectively address disputes arising throughout the entire lifecycle of smart legal contracts, from their initial formation and validity to their automated execution and potential termination. Employing doctrinal legal research and deductive reasoning, the paper systematically evaluates the applicability and limitations of traditional contractual remedies—including damages, specific performance, rescission, rectification, restitution, and termination—in the context of blockchain's technical characteristics, such as immutability, irreversibility of transactions, and the absence of intermediary control. The analysis reveals that while the deterministic and tamper-proof nature of blockchain poses significant challenges to conventional judicial intervention (particularly in cases requiring alteration or reversal of executed code), many disputes remain amenable to resolution under existing Pakistani law, provided courts recognize the dual nature of smart legal contracts as both code and legally binding agreements. Ultimately, it concludes that a balanced combination of carefully designed smart contract architecture (incorporating contingency logic and upgradeability features) and flexible, technology-aware judicial remedies can bridge the gap between blockchain's rigidity and the equitable demands of contract law, thereby ensuring access to meaningful justice in Pakistan's evolving digital economy.



© 2025 The Authors. Published by [Center of Innovation in Interdisciplinary Research \(CIIR\)](#).
This is an Open Access Article under the Creative Common Attribution Non-Commercial 4.0


Article History: Received: 02-05-2025

Accepted: 11-09-2025

Published: 30-11-2025

Keywords: Blockchain, Damages, Rectification, Remedy, Rescission, Restitution, Smart Legal

Corresponding Author's Email: mbilal@bzu.edu.pk

 <https://doi.org/10.62585/ilhr.v4i1.132>

Introduction

A smart legal contract serves as a legal agreement that uses a self-executing programme called a smart contract deployed on a blockchain. It can automatically monitor, execute, and enforce legal obligations. Some scholars contend that these technologies could reshape contract doctrine and commercial practice (Compagnucci et al., 2021, p. 1). Expected advantages include reduced reliance on intermediaries, faster and cheaper verification and enforcement, and lower transaction costs. Because blockchains record transactions in protocol-governed and tamper-evident ledgers often described as immutable and irreversible, these features make smart legal contracts especially attractive for commercial use. The defining feature of automaticity, which entails the elimination of human discretion from performance (UK Jurisdiction Taskforce, 2019, para 135), underpins claims that smart legal contracts deliver “guaranteed” performance (Durovic & Janssen, 2019, p. 71) and undermines the relevancy of established legal remedies (Cutts, 2019, p. 392), since a properly coded contract will carry out its programmed obligations immediately upon the satisfaction of specified conditions.

However, it has been observed that blockchain technology does not always ensure desired contractual performance (Poncibò & DiMatteo, 2019, p. 124). Just like traditional contracts smart legal contracts are susceptible to breach, since code can be faulty through programming errors, may be inconsistent with the intentions of the parties, untrustworthy oracles may supply false external inputs, or blockchain may be subject to unexpected operational failures (Bomprezzi, 2021, pp. 169–171). Additionally, contracts may be rendered void or voidable due to the defects like absence of free consent, lack of consideration, illegality, incapacity and frustration. Consequently, smart legal contracts remain vulnerable to contractual infirmities and breakdowns familiar in contract law, which supplies a range of ex post protections where agreements are defective or fail. Automaticity, however, creates distinct legal problems. The code will run even if there are issues that may invalidate the contract, as it cannot decline or defer performance (Green & Sanitt, 2020, p. 191). The conflict between the assurance of automated certainty and the traditional grounds for invalidity and non-performance raises the question: whether and how established legal remedies can function effectively when contractual obligations are embodied in self-executing and immutable code.

This article analyses various remedies provided by contract law that can be employed to tackle the issues encountered at each phase of the lifecycle a smart legal contract, from its formation to performance. Agreements established on blockchain technology must provide ways for effective relief just as traditional contracts that are subject to rescission, termination, or enforcement through various remedies such as rectification, damages, restitution, or specific performance. The primary challenge lies in determining how traditional remedies can be incorporated into immutable and self-executing smart contract codes, which are not easily reversible after execution, where on-chain assets may have been transferred irreversibly, and where the computational logic complicates the potential for judicial intervention. However, the significance of remedies under contract law is predicated on the premise that, irrespective of the extent of self-enforcement mechanisms in smart legal contracts the parties will retain the capacity to pursue redress through judicial forums (Janssen & Durovic, 2018, p. 767). There is a lack of comprehensive study about the applicability of these remedies within the automated framework of smart legal contracts as governed by Pakistani law. This emphasises the imperative to evaluate the applicability of contract law remedies for smart legal contracts in the framework of Pakistani law, particularly in relation to the basic objective of contract law to enable ex post resolution of conflicts over contracts.

The article commences by analysing whether and how erroneously coded terms can be corrected through rectification so that the recorded instrument accurately reflects the parties’ common intention. Next, it examines rescission and restitution, assessing mechanisms for returning tokenised assets or restoring value where contracts are void or voidable. The discussion then proceeds how to quantify damages for breach

of contract, how to invoke termination in cases of repudiation, and whether specific performance is possible. The conclusion recommends a hybrid approach combining ex-ante technical safeguards through pre-deployed escape routes in code with pragmatic adaptive judicial orders to make sure that substantive justice is served in settings of automated performance.

Rectification

Rectification is a specific remedy that has originated within the framework of English equity law. It is relevant in instances where a ‘written instrument’ does not accurately represent the agreement between the parties as a result of a mistake or misunderstanding (*Racal Group Services Ltd v Ashmore*, 1995, p. 1154). It is granted by the courts to amend a contract’s written terms so that they accurately represent the true intentions of the contracting parties or what the law, grounded in the objective principle, acknowledges as their mutual agreement (Chitty, 2023, para 5-057). Under Pakistani law, it is within the purview of a court to amend a written instrument representing the contract when it does not accurately reflect the intentions of the parties, provided that such discrepancies arise from a mutual mistake or fraudulent conduct (Specific Relief Act, 1877, s. 31). However, this remedy is discretionary in nature and does not affect the rights of third parties who engage in transactions for valuable consideration and in good faith. The modification in question does not affect the fundamental nature of the agreement, nor does it alter the legal rights and obligations. It merely serves to amend the written record of the agreement (*Kilcarne Holdings Ltd v Targetfollow (Birmingham) Ltd*, 2004, para 231).

The remedy of rectification holds significant importance for smart legal contracts. There may be errors in programming translation that hinder the code from accurately reflect the genuine intentions of the parties (Green, 2018, p. 249). However, its significance depends on the form of the smart legal contract under consideration. These are typically classified into three types based on the role played by the contract code: external, hybrid, and solely coded (European Law Institute, 2023, pp. 24–27; UK Jurisdiction Taskforce, 2019, para 142; UK Law Commission, 2021, para 2.51; Verstappen, 2024, p. 4). In the external model, a legally binding agreement remains a conventional natural-language contract. While code functions merely as an execution tool that performs some or all obligations without itself creating them. In hybrid contracts, certain obligations are expressed and enforced by code, while others remain in plain text. Both elements form part of the parties’ bargain. A solely coded contract incorporates the entire agreement into the source code without a separate natural-language instrument. Since this remedy aims to only amend the inaccurately documented provisions of a contract, it holds no relevance in external contracts. Therefore, the inability of the code to fulfil the provisions of the natural-language contract as agreed may give rise to a claim for breach only (UK Law Commission, 2021, para 5.5 footnote 359). On the other hand, in case of a hybrid or solely coded contract, wherein the code encapsulates the contractual stipulations, rectification becomes relevant as a remedy to amend inaccuracies in the recorded code to ensure that it corresponds with the true agreement of the parties.

The first ground for rectification is a mutual mistake, acknowledged as a ‘common mistake’ under English law, which prevents the written instrument evidencing contract from accurately expressing the parties’ actual shared intention (Chitty, 2023, para 5-001). In this case, the four prerequisites for rectification are: first, a common, continuing intention; second, an outward expression evidencing accord; third, that the common intention existed when the document was executed; and fourth, a mistake that prevented the instrument from reflecting that intention (*Swainland Builders Ltd v Freehold Properties Ltd*, 2002, para 33). “Common intention” refers to the parties’ actual mutually held intention at the time of formation and not merely coincident uncommunicated beliefs (*FSHC Group Holdings Ltd v GLAS Trust Corp Ltd*, 2019, para 176). While an “outward expression of accord” requires sufficient communication by which the parties have demonstrated that shared intention.

The fundamental premise underlying the law of rectification is that the parties engaged in the transaction aimed for a fair and conscientious agreement (Specific Relief Act, 1877, s. 32). Where the rectification of

a written instrument is under consideration, the court may investigate the instrument's intended meaning and its intended legal effects, rather than limiting itself to the question of what words the parties meant to use (Specific Relief Act, 1877, s. 33). Therefore, evidence of prior negotiations between parties and surrounding circumstances at the time of contract formation is admissible to prove the parties' common intention (*Chartbrook Ltd v Persimmon Homes Ltd*, 2009, paras 64-67). If the alleged common intention is clearly established through such evidence yet the document fails to record it, the court may amend the instrument to remove the said inconsistency (*FSHC Group Holdings Ltd v GLAS Trust Corp Ltd*, 2019). The underlying rationale is predicated on the principle that it contravenes the doctrine of good faith to permit a party to exploit a drafting mistake to enforce terms contrary to their shared intention.

Rectification for a mutual mistake about the parties' true shared intention can be an appropriate remedy for smart legal contracts (UK Law Commission, 2021, para 5.10). Because coders typically translate negotiated natural-language terms into executable code, there is a real risk that the resulting program may diverge from the parties' bargain (Green, 2018, p. 249). Traditional rules bar the use of evidence of purely subjective intentions when construing contractual language (*Chartbrook Ltd v Persimmon Homes Ltd*, 2009), so ordinary interpretive tools alone may not resolve conversion errors. Nonetheless, where it can be shown that the code misrecords the parties' common intention at the time of agreement, courts can intervene to rectify the coded terms and align the program with what the parties actually agreed.

The second ground for rectification arises where fraudulent conduct causes the written instrument to misstate the parties' true agreement. Fraud may be carried out by a contracting party, its agent, or by collusion and typically takes the form of deception through the means of false statements, deliberate concealment, promises without intent to perform, or other legally culpable acts (Contract Act, 1872, s. 17). In English law, these cases are classified as instances of unilateral mistake that is known to the other party, permitting rectification when the document does not record the parties' common intention (Chitty, 2023, paras 5-070 and 5-071). Even though older decisions required explicit proof of misrepresentation, fraud, or sharp practice, contemporary authorities emphasise that it is unjust for a party, cognisant of the other's mistakes, to enforce the instrument to its own advantage (*Thomas Bates & Son Ltd v Wyndham's (Lingerie) Ltd*, 1981, pp. 515 and 521).

The components of inaccurate suggestion and deliberate concealment may manifest in smart legal contracts. Suppose A and B negotiate agreed terms and record them in a non-binding memorandum, then implement those terms by a solely coded contract. Two permutations are possible. In the first, B's coder translates the memorandum into on-chain code but inadvertently embeds an incorrect pricing formula that benefits B. The error is discovered after deployment but before any execution or payment, and although B is informed of the mistake, B conceals it from A. B consequently presents a false assertion by omitting the disclosure of the mispricing. In the second, the parties jointly retain a developer who makes the same pricing-formula error. Later B's own coder detects the defect and, again, B withholds that knowledge from A. In this instance, the silence exhibited by B serves as a form of active concealment regarding a significant fact. In either case A may pursue rectification on the ground that the deployed code fails to accurately reflect the parties' actual agreement and that B's concealment, knowing the defect, amounts to fraud.

The foregoing analysis indicates that, in theory, a court may rectify the code of a smart legal contract to reflect the parties' actual bargain. But in practical application, three serious obstacles emerge. First, a code deployed on a blockchain cannot be modified (Tech London Advocates, 2023, p. 122). This means that a remedy requiring an amendment of recorded terms may be technically infeasible (Herian, 2021, pp. 28–29). Second, on permissionless ledgers no single actor controls the ledger, and therefore no authority exists to implement a judicially ordered change. While a permissioned or consortium chain might permit enforcement of a court order, doing so would compromise the network's trust-minimising architecture (Paech, 2017, p. 1096). Taken together, these realities cast doubt on the practical applicability of

rectification to autonomous, self-executing code. Prima facie the remedy appears ill-suited where the operative terms are not readily susceptible to modification. Third, coding defects often emerge only after the contract has been executed. Unlike traditional rectification, which prevents further performance under a mistaken agreement, smart contracts self-execute on predefined triggers and commonly preclude timely judicial interruption. Once an automatic performance (for example, an asset transfer) has occurred, it may be impracticable to pause or reverse it. So rectification offers little practical relief, as claimants will usually need remedies that unwind the executed effects (Green, 2018, p. 251), practically leaving them with only the avenue of seeking damages against the recipient (Paech, 2017, p. 1096).

However, in spite of the code's execution, rectification can retain legal significance. Where a claimant who intended to seek rectification instead sues for damages because the code has already executed, the court must first construe the coded terms. If those terms are clear and the alleged erroneous provision is treated as part of the contract, a pure damages claim may fail. Yet rectification operates retrospectively and a successful order treats the contract as if the corrected terms had been in place from the outset (Mitchell et al., 2022, para 40-34). So any allegation of breach is measured against that corrected text (Hodge, 2015, para 1-70). Accordingly, a claimant can argue that the deployed smart contract, as executed on-chain, did not conform to the rectified terms and therefore amounted to defective performance. Furthermore, rectification continues to hold significance in the context of perpetual agreements characterised by recurring performance, as it serves to guarantee the accurate execution of obligations in the future (Green, 2018, p. 251). Rectification therefore remains useful both to secure correct future performance in ongoing arrangements and to ground claims for past performances that deviated from the rectified code.

Restitution

Restitution remedies unjust enrichment where an agreement is void or becomes void. It requires that any individual who has obtained any advantage pursuant to such an agreement must return it or provide compensation to the one providing it (Contract Act, 1872, s. 65). A void contract is treated as null ab initio and creates no enforceable rights or obligations (*The Chairman, District Scrutiny Committee v Sharif Ahmad Hashmi*, 1976), yet one party may nevertheless have conferred benefits under that nullity. Similarly, a voidable contract that is validly rescinded is treated as void from the outset and calls for restitution to restore the parties to their pre-contractual positions. In English law, restitution is developed as a distinct doctrine based on the principle that it is unjust for a party to keep a benefit acquired at the expense of another, and it operates to return benefits or award compensation where retention would be unjust (*Fibrosa Spolka Akcyjna v Fairbairn Lawson Combe Barbour Ltd*, 1943).

A claim for unjust enrichment turns on four issues: whether the defendant has received a benefit, whether that benefit was conferred at the claimant's expense, whether it would be unjust for the defendant to retain it, and whether any defence bar recovery (*Banque Financière de la Cité v Parc (Battersea) Ltd*, 1999, p. 227; *Muhammad Farooq v Javed Khan*, 2022, para 14). "Enrichment" denotes an objectively assessable gain, for example, receipt of money or property rights, or a negative benefit such as avoidance of an expense, provision of services, or discharge of a debt (Chitty, 2023, para 33-020). The claimant must show a corresponding loss resulting from the transfer. The purpose of restitution is to reverse the defendant's gain, where it would be inequitable for it to be retained (*Investment Trust Companies v Revenue and Customs Commissioners*, 2017, para 43).

The "unjust" element requires the claimant to show the benefit was conferred under circumstances the law treats as inequitable, commonly where the transfer was made by mistake or where the contractual basis for the transfer has failed (Chitty, 2023, para 33-016). A mistake arises when a party parts with a benefit believing a valid contract existed (*Brendon International Ltd v Water Plus Ltd*, 2023, para 107) and a failure of basis occurs where a transfer made pursuant to an apparently subsisting contract is undermined by the contract's nullity, so that retention of the benefit becomes unjust (Mitchell et al., 2022,

para 13-26). Where both parties have already exchanged benefits under a contract subsequently declared void, a claimant seeking restitution must make counter-restitution for any advantage received from the defendant to avoid unjust enrichment (Mitchell et al., 2022, para 31-01). If such reciprocal restoration is impossible, restitutionary relief will be denied.

The courts should encounter no novel doctrinal obstacle in the adjudication of restitution for nullified smart legal contracts, as the essential question remains the same: whether a party endured unjust enrichment to the detriment of another. In a Singapore case involving bitcoin-ether exchange transactions, the appellant contended that certain trading contracts were void for unilateral mistake and sought restitution for bitcoin transfers (*Quoine Pte Ltd v B2C2 Ltd*, 2020). The Court of Appeal acknowledged that the transfers constituted an enrichment at the appellant's expense but found that mistake was not established as to the counterparties and therefore the restitution claim failed (*Quoine Pte Ltd v B2C2 Ltd*, 2020, paras 133-135). However, the decision demonstrates that conventional restitutionary principles can be applied to smart legal contracts.

Rescission

Rescission is the remedy for voidable contracts (Contract Act, 1872, s. 64), whereby the aggrieved may either set aside or affirm the agreement for some vice or defect (*The Chairman, District Scrutiny Committee v Sharif Ahmad Hashmi*, 1976). Rescission treats the contract as void ab initio, reversing the transaction and reinstating the parties to their positions prior to the contract's formation. Traditionally, common-law courts required strict restitutio in integrum, refusing rescission unless the consequences of the contract could be completely undone (Chitty, 2023, para 10-135). For example, claims were denied where physical restoration was impossible after extraction of minerals (*Vigers v Pike*, 1842). Modern equity, however, adopts a more pragmatic approach and recognises that rescission is available where the court may secure "practical justice" (Chitty, 2023, para 10-136). Furthermore, the principle of restitutio in integrum is understood to require substantial instead of exact restoration. Where restoration in kind is impracticable, the court can often order monetary compensation equivalent to the value of benefits received (*Halpern v Halpern (No 2)*, 2007). Because most contractual benefits can be monetised, the impossibility of precise restoration now rarely bars rescission.

Rescission of a voidable contract under Pakistani law likewise turns on restitutio in integrum. It requires that a party who validly rescinds must restore any benefit obtained from the counterparty (Contract Act, 1872, s. 64). The law therefore give effect to the equitable requirement of complete restitution, and an agreement may be annulled only when the parties are capable of being returned to their positions prior to the contract (*Muhammad Sabir v Maj. (Rtd.) Muhammad Khalid Naeem Cheema*, 2010). Pakistani courts take a practical approach of restitutio in integrum, permitting monetary compensation where literal restoration is impracticable. Rescission is typically permissible provided that the advantage can be adequately assessed and compensated. If valuation or restitution is impossible, both restitution and rescission will be barred. The claimant must also account for any benefit they received by way of counter-restitution or by offsetting amounts due (*The Eastern Automobile Ltd v Tasdiq Hussain, I. F. S., Conservator of Forests*, 1959).

A voidable contract remains operative until the entitled party elects to rescind; otherwise, he may either affirm the contract, thereby waiving rescission (*Messrs Balagamwalla Cotton Ginners and Pressing Factory v Messrs Akber Oil Mills*, 1965). Communication of rescission may be effected by notifying the other party or through conduct that plainly conveys the decision (Contract Act, 1872, ss. 3 and 66), such as commencing proceedings (Specific Relief Act, 1877, s. 35). Although the Contract Act does not prescribe immediate notice, the right to rescind can be lost by undue delay, including the expiration of three year limitation period (Limitation Act, 1908, First Schedule Article 114), the intervention of third-party rights, or where the defendant is prejudiced (Soomro, 2015, p. 280). Prejudice arises, for instance, where the plaintiff delays stopping receipt of benefits or restoring them, or where the plaintiff's conduct

has misled the defendant into taking further irreversible steps under the contract (*Messrs Balagamwalla Cotton Ginners and Pressing Factory v Messrs Akber Oil Mills*, 1965).

Where a smart legal contract is voidable, the aggrieved party retains the conventional right to rescind, and the usual doctrinal rules remain applicable. Practical impediments, however, flow from blockchain immutability and autonomous code execution. Once deployed the on-chain program runs without manual intervention and cannot readily be stopped (Durovic & Janssen, 2019, p. 73). Additionally, the rapidity of automated transactions increases the risk that an injured party will inadvertently waive the right to rescind or appear to have affirmed the contract before identifying the defect (Herian, 2021, p. 30). As a result, after partial or complete on-chain performance it is often extremely difficult in practice to unwind effects and restore the parties to their pre-contractual positions.

Compensatory Damages

Compensatory damages remain the primary contractual remedy, awarding the aggrieved party a sum of money equivalent to the financial harm attributable to the breach (Contract Act, 1872, s. 73). For smart legal contracts, it is probable that damages will serve as the primary remedy because technical and architectural constraints make other remedies difficult to implement (Green, 2018, p. 251; Paech, 2017, p. 1096). However, quantum assessment and enforcement cannot be fully automated (Tjin Tai, 2022, p. 221) and therefore require judicial determination and human execution (Pasa & DiMatteo, 2019, p. 355). The aim of such awards is to protect the claimant's expectation interest by placing him as nearly as possible in the position had the contract been performed (*Robinson v Harman*, 1848, p. 855), rather than to punish the breach (*Habib Bank Limited v Mehboob Rabbani*, 2023, para 11). Awards are therefore governed by the rules of foreseeability and mitigation (Contract Act, 1872, s. 73). Recovery is confined to those losses that naturally result from the contract breach or were anticipated by the parties at formation. Losses that do not fall within those categories are treated as too remote and therefore not recoverable (*A. Ismailjee & Sons v Pakistan*, 1986, para 12). Under the imputed-knowledge test, foreseeability is assessed by reference to what a reasonable person in the defendant's position would have foreseen. In practice, blockchain-specific risks (for example, coding errors, protocol bugs, oracle failures, or defective data feeds) are foreseeable risks that parties commonly assume (Giancaspro, 2017, p. 833), and the immutable on-chain record may assist claimants in proving foreseeability.

Pakistani law recognises general damages for ordinary, direct losses and special damages for atypical losses that must be pleaded and proved (*Mrs. Alia Tareen v Amanullah Khan*, 2005, para 10). When quantifying breach losses, courts assess whether the claimant took reasonable steps to mitigate (Contract Act, 1872, Explanation to s. 73) and will deny recovery for loss resulting from the claimant's own negligence (*Syed Ahmad Saeed Kirmani v Messrs Muslim Commercial Bank Ltd., Islamabad*, 1993). The duty does not require sacrificing personal welfare, reputation, commercial interests, or property (*Mehtab Din v Malik Fazal Hussain*, 1954). In an automated-performance setting, injured parties are expected to act quickly by engaging in substituting transactions or procuring identical off-chain performance in order to mitigate losses upon the discovery of a breach. A failure to undertake such measures will result in a reduction of recoverable damages. Temper resistant on-chain records may provide persuasive evidence of the claimant's efforts to mitigate loss.

Upon establishing entitlement to damages, the claimant must prove the quantum of loss (*Kamran Construction (Pvt) Ltd v Nazir Talib*, 2010, para 8), and the court will fix compensation on the available facts (*Qazi Dost Muhammad v Malik Dost Muhammad*, 1997). The judge selects the most appropriate valuation method by reference to the claimant's lost interest: restitution, reliance, or expectation (Soomro, 2015, p. 274). Restitution recovers any benefit the defendant has retained; reliance reimburses costs or harm sustained in anticipation of performance; expectation restores the profit or additional advantages the claimant could reasonably foresee (which may include resale profit when the defendant was aware of the anticipated resale) (*A. Ismailjee & Sons v Pakistan*, 1986; Chitty, 2023, para 30-022). Damages are

normally measured by the market price at the time performance was due (*Muhammad Sharif Sandhu v District Accounts Officer*, 2011, para 6), but if anticipatory breach is accepted, the assessment date becomes the moment of repudiation (*Ramgopal v Dhani Jadav Ji Bhatia*, 1928). Although some commentators question proof of loss in blockchain disputes (UK Law Commission, 2021, para 5.120), the ledger's immutable, timestamped records and token-transfer history often make it straightforward to establish the occurrence, timing and quantum of loss across restitution, reliance or expectation frameworks.

Parties frequently mitigate valuation uncertainty by agreeing on a fixed sum payable for breaches. The English law classified provisions of this nature into two distinct categories: realistic pre-estimates of loss (liquidated damages) enforceable by courts, and penalties, which are disproportionate sums intended to deter breach and that courts will not enforce (*Cavendish Square Holding BV v Talal El Makdessi*, 2015, para 32; *Jobson v Johnson*, 1989, p. 1040). Pakistani law, by contrast, does not adopt this formal distinction (*Province of West Pakistan v Messers Mistri Patel & Co*, 1969): an aggrieved party is entitled to "reasonable compensation" up to any amount the parties have stipulated (Contract Act, 1872, s. 74), and courts will examine whether actual loss exists before awarding the stipulated sum. The Supreme Court has affirmed contractual freedom to determine damages to avoid later disputes (*Messrs Khanzada Muhammad Abdul Haq Khan Khattak & Co. V WAPDA through Chairman WAPDA*, 1991, para 4), but it will withhold or reduce recovery where the sum bears no relation to demonstrable loss for instance, where retention of earnest money would be unconscionable (*Province of West Pakistan v Messers Mistri Patel & Co*, 1969). Consequently, agreed-sum provisions should be drafted carefully and with clear evidence that the stated figure corresponds to potential loss.

Parties may also seek to limit or exclude liability for breaches arising from code execution by inserting exclusion clauses in their natural-language agreements. If both parties agree to these clauses, they are enforceable (Mohan & Jain, 2020, pp. 597–598; *Provincial Government, NWFP (Now Government of West Pakistan) v M. K. Musafir*, 1965). However, courts interpret any ambiguity against the drafter under the principle of *contra proferentem* (*American Life Insurance Company (Pakistan) Limited V Agha Jan Ahmed*, 2011, para 12). This means that exclusionary language must be clear in order to work. In short, there is no fundamental doctrinal bar to awarding compensatory damages for breaches of smart legal contracts: agreed-sum and exclusion provisions remain available tools, and damages claims arising from on-chain performance can be litigated and enforced off-chain under established principles.

Termination

The right to terminate arises where the promisor repudiates by refusing or becoming incapable of performing the whole promise or where there is a breach of a condition, i.e., a term fundamental to the contract's primary object (Contract Act, 1872, s. 39; Specific Relief Act, 1877, ss. 12 and 60). Whether a term is a condition is a matter of contractual construction for the court, but a breach will be fundamental if it destroys the contract's essence or so substantially deprives the promisee of the expected benefit that continuation is unjustified (Soomro, 2015, p. 251). For example, a party's nonpayment of the price constitutes a contract repudiation, and the seller is justified in treating this as an anticipatory breach, thereby allowing for the termination of the contract and the pursuit of damages (*Bengal Oil Mills Ltd. V Dada Sons*, 1964, para 16). Parties can also establish or enhance termination rights through an express clause (*Pakistan Airline Pilots Association through Honorary General Secretary v Federation of Pakistan through Secretary for Ministry of Interior, Islamabad*, 2021, para 13). Termination discharges remaining obligations unless the parties agree otherwise (*Messrs A. C. Yusuf & Co. V Messrs K. B. H. M. Habibullah & Co.*, 1965, para 30), but it is not automatic. The innocent party is required to decide regarding the termination or affirmation of the contract. Affirmation keeps the contract alive, and in the absence of any clear election, the parties remain bound (*Karachi Water And Sewerage Board Through Authorised Representative v Messrs Karachi Electric Supply Corporation*, 2012, para 48).

The doctrinal rules governing termination apply equally to smart legal contracts in principle (Bomprezzi, 2021, pp. 209–210). In practice, however, blockchain immutability and autonomous code execution complicate relief. Once deployed, on-chain code typically runs to completion and cannot readily be stopped on a permissionless ledger, so termination does not necessarily prevent further automated performance (Meyer, 2020, p. 17). However, termination is feasible where obligations depend on off-chain acts, for example, oracle inputs or human performance, and an aggrieved party can withhold the requisite external inputs or refuse off-chain duties to halt further on-chain effects. Therefore, where performance spans the off-chain domain, post-deployment interventions remain a viable means of giving termination a practical effect.

Specific Performance

Specific performance constitutes an equitable remedy originating in English law, whereby a court can direct a contracting party to discharge positive obligations where damages are inadequate. Under Pakistani law courts may, at their discretion, award specific performance in instances where the quantification of damages proves difficult, such as in cases involving the original creations of a deceased artist; when financial compensation is evidently insufficient, as is often the case with the conveyance of immovable property; and when pragmatic challenges complicate the recovery of damages, exemplified by the enforcement of a promissory note that has been improperly endorsed by a party facing insolvency (Contract Act, 1872, s. 12). On the other hand, courts may refuse it where damages suffice, the terms lack sufficient clarity, the subject matter is destroyed, performance is rendered impossible, or the duty extends beyond specified temporal limits (Contract Act, 1872, s. 21). The applicant must show a readiness to perform and that the other party is unjustifiably refusing or delaying performance (*Messrs DW Pakistan (Private) Limited, Lahore v Begum Anisa Fazl-i-Mahmood*, 2023, para 6). The court must exercise its discretion on principled grounds, weighing unfair advantage to the plaintiff and hardship to the defendant (*Rao Abdul Rehman (Deceased) v Muhammad Afzal (Deceased)*, 2023, para 7).

Because self-executing code typically effects on-chain obligations automatically, courts seldom need to compel coded performance. Breaches of smart legal contracts frequently present as defective rather than total non-performance, making monetary compensation the more practical remedy (UK Law Commission, 2021, para 5.136). Where contractual obligations, however, extend into the off-chain environment, like supply of goods, customized services, or transmission of external data, specific performance continues to be applicable. If the unfulfilled duty is unique or damages are inadequate, a court may require completion of the off-chain act, subject to the traditional discretionary and substantive limits described above.

Interventions Post-Deployment

Doctrinally, conventional contract law remedies remain available against automated performance. However, their efficacy is limited by technical obstacles e.g., the difficulties of modifying deployed code, pausing or halting execution, and reversing on-chain transactions. The primary practical constraint is the immutable characteristic of blockchain. Accordingly, the utility of conventional remedies depends on the availability of technical or operational means of intervention.

Blockchain's Immutability

A blockchain is a distributed ledger consisting of sequentially linked blocks that record validated transactions and related metadata in an append-only, tamper-evident structure, secured by cryptographic primitives and maintained across network participants by consensus protocols (Bacon et al., 2018, pp. 4–5; World Bank, 2017, p. 1). Blockchain secures transactions by pairing cryptographic hash functions with asymmetric (public-key) cryptography, using matched public and private keys to authenticate transactions, prevent unauthorised access, and protect confidentiality (Bashir, 2017, pp. 154–155). By linking hashes, any unauthorised change to the underlying data immediately alters the corresponding hash and breaks the cryptographic links, which is the basis for describing blockchains as ‘immutable’. In

practice a record can only be rewritten if the network accepts a replacement chain, requiring validators (or an attacker controlling a majority of computational power or stake) to recompute block hashes, and the practical difficulty of doing so depends on the ledger's architecture and its consensus mechanism.

In permissionless networks, these actions are far more difficult to carry out (Bacon et al., 2018, pp. 38–39). Their open, pseudonymous architecture admits unknown validators, making coordinated manipulation difficult. Consensus mechanisms are deliberately resource-intensive and economically incentivize honest participation to deter bad actors. By contrast, permissioned ledgers, whether run by a known consortium of validators or a single governing party, can be amended more readily because participants are identified and the consensus process can be purpose-built. For this reason, blockchain is more accurately described as tamper-evident or unilaterally irreversible rather than absolutely immutable (Finck, 2018, p. 30; Rikken et al., 2017, p. 16). Smart-contract code is merely data recorded on the ledger, so the same technical dynamics that render blockchains effectively immutable apply to deployed contracts. On permissionless networks, it is therefore, as a practical matter, infeasible to halt or alter the live contract code, even where technical means might exist. In contrast, permissioned or consortium chains provide significantly more opportunities for authorised intervention or amendment.

Technical Solutions

Proposed technical interventions after a smart contract is uploaded fall into two broad categories: ledger-level intrusions and modifications made to the contract code itself. As noted earlier, reversing or halting execution is relatively straightforward in permissioned ledgers, where an administrator or a set of authorised validators can suspend or rollback transactions (Rikken et al., 2017, p. 16). By contrast, intervening on permissionless chains is costly and governance-heavy, although not impossible. The Ethereum DAO response via a hard fork demonstrates that community action can undo an attack (Cunningham, 2016, p. 238). However, persuading a majority of anonymous validators to accept changes is difficult in bilateral disputes. Consequently, direct ledger-level remedies on public chains tend to be impractical in practice, with the need to adopt remedial mechanisms built into the contract code itself. The interventions at the code level should allow suspension, amendment and reversal of on-chain execution, and to be effective, these capabilities must be incorporated at design time as dormant pathways (Sklaroff, 2017, pp. 291–292), that can be activated only to implement post-deployment remedies like rectification, rescission, or termination. Given the effective immutability of on-chain records, embedding such controls during drafting stage is essential, and contract code should be engineered to anticipate likely trigger events and to include the mechanisms necessary to respond when intervention becomes necessary.

Although a contract's code is immutably recorded once deployed, its runtime state, the contract's variables and callable functions, can be changed (Marino & Juels, 2016, p. 158). A common safeguard is to embed a "self-destruct" or kill switch which, when triggered, disables further execution and so effectively removes the contract's operative functionality (Schrepel, 2021, p. 38). Disabling a deployed contract by setting a terminal state does not erase its stored bytecode but can update the contract's state so its functions are no longer callable. This functional disabling of contract's code serves as an effective deletion that may prevent interference with subsequent remedial steps or the deployment of replacement contracts (Herian, 2021, p. 31). Law and policy are beginning to recognise these controls. For example, the EU Data Act 2023, specifically in Article 36(1)(b), mandates that operators of smart contracts implement mechanisms to halt ongoing transactions and incorporate internal functions that can terminate execution, thereby safeguarding against unintended performance. At the same time, blockchain architectures have grown more flexible. There are platforms like Cardano where off-chain code may drive on-chain scripts so that user input or external data can trigger pause or stop conditions (Seneviratne, 2024).

There are other technical routes too which facilitate precise modifications rather than the deactivation of an active contract. The particular functions or variables of a smart contract can be modified, removed, or extended at runtime by designing functions with controllable states using patterns such as modifiers and

enums, provided these controls are encoded at inception (Marino & Juels, 2016, pp. 162–164). Alternatively, modifications may be implemented through auxiliary or satellite contracts, wherein the principal contract assigns functionality to external contracts (through stored addresses or pointers), which can be substituted or enhanced to modify output without necessitating alterations to the original bytecode.

Even when intervention is technically feasible, considerable practical challenges emerge. Not only is it costly to encode every possible contingency into a contract code (Sklaroff, 2017, pp. 292–293), but it is also impractical because parties cannot predict all events that might affect performance, and trying to do so makes things too complicated (Tai, 2018, p. 798). Furthermore, the processes of termination and modification present both security vulnerabilities and economic risks. Hackers may exploit these vulnerabilities, if adequate protections are not implemented. Further, turning on a kill switch could temporarily or permanently deny users access to their assets (Seneviratne, 2024). For these reasons, any such mechanism must be protected by robust safeguards with procedures to restore operations and assets after intervention and transparent and equitable activation criteria to avoid inadvertent or improper destruction of value (Perez & Livshits, 2021). Moreover, granting powers to terminate contract codes creates a real risk of misuse (UK Law Commission, 2021, para 5.131). When a party attempts to prevent the execution of transactions that they deem unfavourable, they may pursue the option to terminate the contract, potentially leading to new forms of breach. Despite this risk, the absence of termination mechanisms may be worse, and wrongful shutdowns can still be remedied through orders for specific performance or awards of damages. Therefore, we believe that to minimise abuse, termination features must be engineered with robust safeguards and recovery mechanisms, and the authority to invoke them should sit with a neutral intermediary (for example, a court or arbitrator) rather than with private parties. Achieving that allocation of power would likely require legal or doctrinal reform, since current law leaves the election to rescind or terminate primarily with the aggrieved party.

Practical Solutions

If such embedded safeguards are lacking or ineffective, the courts can still pursue ‘practical justice’ by directing corrective on-chain measures that neutralise the effects of the original execution. One pragmatic route is to require the parties to record a corrective transaction or to agree on a revised version of the code and redeploy it (Bacon et al., 2018, p. 39; De Filippi & Wright, 2018, p. 85; Herian, 2021, p. 29). A subsequent on-chain transaction can neutralise an earlier transfer by creating a countervailing entry while leaving the original bytecode and history intact (Sanitt, 2023, p. 101). Although this technique is a technical rather than doctrinal undoing and may not amount to either rectification or rescission in the classical sense. It can operate as a practical novation or achieve the equivalent of specific performance by restoring the claimant’s substantive position. Where a platform is subject to central administration, a court may instead direct those administrators to suspend or reverse relevant transactions and restore benefits to effect relief even after on-chain execution.

However, such remedies ordinarily require either the parties’ cooperation or access to the promisor’s private key (Bacon et al., 2018, p. 39). Therefore, remedies that undo on-chain effects inevitably reintroduce the very inter-party trust that smart contracts were designed to eliminate. That problem is acute in permissionless, pseudonymous settings, where an innocent party or court may not know whom to approach to unwind a transaction (Meyer, 2020, p. 20). Alternatively, where restoration of the specific token or asset is impossible, courts can instead quantify the benefits conferred by the code and order monetary compensation to restore value, which would amount to a practical restitutionary remedy even if the precise asset cannot be returned (Yeo & Taylor, 2019, pp. 587–588). In short, technical and procedural workarounds can mitigate the rigidity of immutable, autonomous code, but effective judicial relief will often demand inventive and context-sensitive orders tailored to the ledger type, the pre-built contractual escape routes, and the extent of on-chain performance.

Conclusion

This paper assessed rectification, restitution, rescission, damages, termination and specific performance as applied to smart legal contracts and reached three interrelated conclusions. First, doctrinally traditional remedies remain available: rectification can address coding errors or deliberate miscoding; restitution answers void contracts via unjust-enrichment principles; rescission still applies to voidable agreements (subject to waiver or affirmation); termination is effective where future obligations depend on off-chain acts; and damages present no doctrinal obstacle because they are assessed and enforced off-chain. Second, practical enforcement is constrained by technical features such as effective immutability, a lack of a single point of control, and the irreversibility of on-chain transfers. So, remedies that require altering deployed code or reversing executed transactions are often impracticable on public ledgers. Third, these limits can be mitigated: private/consortium chains permit more direct intervention, network-level remedies (e.g., forks) remain possible but costly, and the more reliable solution is *ex-ante* engineering through kill switches, state controls, and upgradeable or satellite contracts. Where technical fixes are absent or insufficient, courts can still achieve practical justice by ordering corrective on-chain entries, novation, specific performance of off-chain duties, or monetary compensation to restore value. Ultimately, a mix of pre-coded safeguards and flexible judicial remedies preserves the operative availability of core contractual reliefs, the precise form of which depends on the ledger type, the contract's built-in alternatives, and the extent of on-chain performance.

References

A. Ismailjee & Sons v Pakistan, PLD 1986 SC 499 ____ (1986).

American Life Insurance Company (Pakistan) Limited V Agha Jan Ahmed, 350 CLD ____ (Karachi 2011).

Bacon, J., Michels, J. D., Millard, C., & Singh, J. (2018). Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralized Ledgers. *Richmond Journal of Law & Technology*, 25(1), 1–106.

Banque Financière de La Cité v Parc (Battersea) Ltd, 1 AC 221 (1999).

Bashir, I. (2017). *Mastering blockchain: Distributed ledgers, decentralization and smart contracts explained*. Packt.

Bengal Oil Mills Ltd. V Dada Sons, PLD 1964 (W. P.) Karachi 18 ____ (1964).

Bomprezzi, C. (2021). *Implications of Blockchain-Based Smart Contracts on Contract Law*. Nomos Verlag.

Brendon International Ltd v Water Plus Ltd, 1 WLR 1229 (2023).

Cavendish Square Holding BV v Talal El Makdessi, UKSC 67 (2015).

Chartbrook Ltd v Persimmon Homes Ltd, UKHL 38 (2009).

Chitty, J. (2023). *Chitty on contracts. Volume 1: General principles* (H. G. Beale, Ed.; 35th edn). Sweet & Maxwell.

Compagnucci, M. C., Fenwick, M., & Wrba, S. (Eds). (2021). Introduction: The Technology, Use-Cases and Law of Smart Contracts. In *Smart Contracts: Technological, Business and Legal Perspectives* (pp. 1–6). Hart Publishing. <https://doi.org/10.5040/9781509937059>

Contract Act (1872).

Cunningham, A. (2016). Decentralisation, Distrust & Fear of the Body—The Worrying Rise of Crypto-Law. *SCRIPTed: A Journal of Law, Technology and Society*, 13(3), 235–257.

Cutts, T. (2019). Smart Contracts and Consumers. *West Virginia Law Review*, 122(2), 389.

De Filippi, P., & Wright, A. (2018). *Blockchain and the law: The rule of code*. Harvard university press.

Durovic, M., & Janssen, A. (2019). Formation of Smart Contracts under Contract Law. In L. A. DiMatteo, M. Cannarsa, & C. Poncibò (Eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (pp. 61–79). Cambridge University Press. <https://doi.org/10.1017/9781108592239.004>

European Law Institute. (2023). *ELI Principles on Blockchain Technology, Smart Contracts and Consumer Protection*. European Law Institute.

Fibrosa Spolka Akcyjna v Fairbairn Lawson Combe Barbour Ltd, AC 32 (1943).

Finck, M. (2018). *Blockchain Regulation and Governance in Europe*. Cambridge University Press. <https://doi.org/10.1017/9781108609708>

FSHC Group Holdings Ltd v GLAS Trust Corp Ltd, EWCA Civ 1361 (2019).

Giancaspro, M. (2017). Is a ‘smart contract’ really a smart idea? Insights from a legal perspective. *Computer Law & Security Review*, 33(6), 825–835. <https://doi.org/10.1016/j.clsr.2017.05.007>

Green, S. (2018). Smart contracts, interpretation and rectification. *Lloyd’s Maritime and Commercial Law Quarterly*, 24, 234–251.

Green, S., & Sanitt, A. (2020). Smart Contracts. In P. S. Davies & M. Raczynska (Eds), *Contents of Commercial Contracts: Terms Affecting Freedoms* (1st edn). Hart Publishing.

Habib Bank Limited v Mehboob Rabbani, SCMR 1189 (2023).

Halpern v Halpern (No 2), EWCA Civ 291 (2007).

Herian, R. (2021). Smart contracts: A remedial analysis. *Information & Communications Technology Law*, 30(1), 17–34. <https://doi.org/10.1080/13600834.2020.1807134>

Hodge, D. (2015). *Rectification: The modern law and practice governing claims for rectification for mistake* (2nd edn). Sweet & Maxwell.

Investment Trust Companies v Revenue and Customs Commissioners, UKSC 29 (2017).

Janssen, A., & Durovic, M. (2018). The Formation of Blockchain-based Smart Contracts in the Light of Contract Law. *European Review of Private Law*, 26(Issue 6), 753–771. <https://doi.org/10.54648/ERPL2018053>

Jobson v Johnson, 1 WLR 1026 (1989).

Kamran Construction (Pvt) Ltd v Nazir Talib, SCMR 829 (2010).

Karachi Water And Sewerage Board Through Authorised Representative v Messrs Karachi Electric Supply Corporation, CLD 1225 (Sindh 2012).

Kilcarne Holdings Ltd v Targetfollow (Birmingham) Ltd, EWHC 2547 (Ch 2004).

Limitation Act (1908).

Marino, B., & Juels, A. (2016). Setting Standards for Altering and Undoing Smart Contracts. In J. J. Alferes, L. Bertossi, G. Governatori, P. Fodor, & D. Roman (Eds), *Rule Technologies. Research, Tools, and Applications* (pp. 151–166). Springer International Publishing. https://doi.org/10.1007/978-3-319-42019-6_10

Mehtab Din v Malik Fazal Hussain, PLD 1954 Lahore 451 ____ (1954).

Messrs A. C. Yusuf & Co. v Messrs K. B. H. M. Habibullah & Co., P L D 1965 (W. P.) Karachi 374 ____ (1965).

Messrs Balagamwalla Cotton Ginners and Pressing Factory v Messrs Akber Oil Mills, PLD 1965 (W. P.) Karachi 460 ____ (1965).

- Messrs DW Pakistan (Private) Limited, Lahore v Begum Anisa Fazl-i-Mahmood, SCMR 555 (2023).
Messrs Khanzada Muhammad Abdul Haq Khan Khattak & Co. v WAPDA through Chairman WAPDA, SCMR 1436 (1991).
- Meyer, O. (2020). Stopping the Unstoppable: Termination and Unwinding of Smart Contracts. *Journal of European Consumer and Market Law*, 9(1), 17–24.
- Mitchell, C., Mitchell, P., & Watterson, S. (Eds). (2022). *Goff & Jones on unjust enrichment* (10th edn). Sweet & Maxwell.
- Mohan, M. P. R., & Jain, A. (2020). Exclusion clauses under the Indian Contract Law: A need to account for unreasonableness. *NUJS Law Review*, 13, 593–629.
- Mrs. Alia Tareen v Amanullah Khan, PLD 2005 SC 99 ____ (2005).
- Muhammad Farooq v Javed Khan, P L D 2022 SC 73 ____ (2022).
- Muhammad Sabir v Maj. (Rtd.) Muhammad Khalid Naeem Cheema, CLC 1879 (Karachi 2010).
- Muhammad Sharif Sandhu v District Accounts Officer, SCMR 1287 (2011).
- Paech, P. (2017). The Governance of Blockchain Financial Networks. *The Modern Law Review*, 80(6), 1073–1110. <https://doi.org/10.1111/1468-2230.12303>
- Pakistan Airline Pilots Association through Honorary General Secretary v Federation of Pakistan through Secretary for Ministry of Interior, Islamabad, MLD 1059 (Sindh 2021).
- Pasa, B., & DiMatteo, L. A. (2019). Observations on the Impact of Technology on Contract Law. In L. A. DiMatteo, M. Cannarsa, & C. Poncibò (Eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (pp. 334–358). Cambridge University Press. <https://doi.org/10.1017/9781108592239.018>
- Perez, D., & Livshits, B. (2021). Smart Contract Vulnerabilities: Vulnerable Does Not Imply Exploited. *30th USENIX Security Symposium (USENIX Security 21)*, 1325–1341.
- Poncibò, C., & DiMatteo, L. A. (2019). Smart Contracts: Contractual and Noncontractual Remedies. In L. A. DiMatteo, M. Cannarsa, & C. Poncibò (Eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (pp. 118–140). Cambridge University Press. <https://doi.org/10.1017/9781108592239.007>
- Province of West Pakistan v Messers Mistri Patel & Co, PLD 1969 SC 80 ____ (1969).
- Provincial Government, NWFP (Now Government of West Pakistan) v M. K. Musafir, PLD 1965 SC 489 ____ (1965).
- Qazi Dost Muhammad v Malik Dost Muhammad, CLC 546 (Quetta 1997).
- Quoine Pte Ltd v B2C2 Ltd, SGCA(I) 02 (2020).

Racal Group Services Ltd v Ashmore, STC 1151 (1995).

Ramgopal v Dhani Jadav Ji Bhatia, AIR 1928 PC 200 ____ (1928).

Rao Abdul Rehman (Deceased) v Muhammad Afzal (Deceased), SCMR 815 (2023).

Rikken, O., Van Heukelom-Verhage, S., Mul, S., Boersma, J., Bijloo, I., Van Hecke, P., Rutjes, A., Stroucken, F., Linnemann, J., Terpoorten, H., & Reinder Nederhoed, R. (2017). *Smart contracts as a specific application of blockchain technology*. Smart Contract Working Group – Dutch Blockchain Coalition. <https://dutchblockchaincoalition.org/assets/images/default/Smart-Contracts-ENG-report.pdf>

Robinson v Harman, 1 Exch 850 (1848).

Sanitt, Dr. A. (2023). Remedies for Smart Legal Contracts. In B. Soyer, *Damages, Recoveries and Remedies in Shipping Law* (pp. 95–112). Informa Law from Routledge. <https://doi.org/10.4324/9781003376347-10>

Schrepel, T. (2021). *Smart contracts and the digital single market through the lens of a “law + technology” approach*. European Commission.

Seneviratne, O. (2024). The Feasibility of a Smart Contract “Kill Switch”. *arXiv Preprint arXiv:2407.10302*. <https://arxiv.org/html/2407.10302v1#bib.bib2>

Sklaroff, J. M. (2017). Smart Contracts and the Cost of Inflexibility. *University of Pennsylvania Law Review*, 166(1), 263–304.

Soomro, T. (2015). *The Contract law of Pakistan*. Oxford University Press.

Specific Relief Act (1877).

Swainland Builders Ltd v Freehold Properties Ltd, 2 E.G.L.R. 71 (2002).

Syed Ahmad Saeed Kirmani v Messrs Muslim Commercial Bank Ltd., Islamabad, SCMR 441 (1993).

Tai, E. T. T. (2018). Force majeure and excuses in smart contracts. *European Review of Private Law*, 26(6), 787–804.

Tech London Advocates. (2023). *Blockchain: Legal and regulatory guidance (third edition)*.

The Chairman, District Scrutiny Committee v Sharif Ahmad Hashmi, PLD 1976 SC 258 ____ (1976).

The Eastern Automobile Ltd v Tasdique Hussain, I. F. S., Conservator of Forests, PLD 1959 (W. P.) Lahore 681 ____ (1959).

Thomas Bates & Son Ltd v Wyndham’s (Lingerie) Ltd, 1 WLR 505 (1981).

Tjin Tai, E. T. (2022). Smart Contracts as Execution Instead of Expression. In J. Allen & P. Hunn (Eds), *Smart Legal Contracts: Computable Law in Theory and Practice* (pp. 205–224). Oxford University Press. <https://doi.org/10.1093/oso/9780192858467.003.0010>

UK Jurisdiction Taskforce. (2019). *Legal statement on cryptoassets and smart contracts*. The LawTech

Delivery Panel.

UK Law Commission. (2021). *Smart Legal Contracts: Advice to Government*. Law Com No 401.

Verstappen, J. (2024). A smart contract taxonomy. *Compact*. <https://www.compact.nl/pdf/C-2024-1-Verstappen.pdf>

Vigers v Pike, CL & Fin 562 (1842).

World Bank. (2017). *Distributed Ledger Technology (DLT) and Blockchain FinTech Note | No. 1*. <https://documents1.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf>

Yeo, N., & Taylor, A. (2019). Avoiding blockchain contracts. *Butterworths Journal of International Banking and Financial Law*, 34(9), 586–588.