Journal of Law & Social Studies (JLSS)
Volume 7, Issue 4, pp 289-305
www.advancelrf.org

When Code Becomes Contract: An Analysis of Smart Legal Contract Formation under Pakistani Law

Waqas Rafiq
(Corresponding Author)
Ph.D. Law Scholar, University Gillani Law College, Bahauddin Zakariya University, Multan
Email: waqas.rafiq@pugc.edu.pk

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

Abstract

Smart contracts are software applications deployed on distributed ledger technologies, such as blockchain, that restructure the manner in which transactions are executed. Where such applications are employed to record and perform legally enforceable obligations, they operate as "smart legal contracts". Their automatic execution framework has altered conventional processes of contract formation and performance. When code performs contractual functions, smart legal contracts emerge as a novel mode of agreement formation under contract law. This paper tests whether smart legal contracts meet Pakistan's statutory formation requirements under the Contract Act, 1872 and the Electronic Transactions Ordinance, 2002. The study applies black-letter analysis, deductive legal reasoning and analogy under a doctrinal research design to evaluate whether established principles of Pakistani contract law are capable of regulating smart legal contracts.It fills a gap in existing legal scholarship by analysing the automated blockchain-enabled agreements under Pakistani case law and statutory commentary. This study offers observations relevant to harmonising legal doctrine with technological developments and strengthening confidence of the stakeholders in the responsiveness of the Pakistani legal system to contemporary digital challenges. The analysis concludes that smart legal contracts fall within the category of electronic contracts with prevailing rules on contract formation remain applicable in the blockchain environment. The enactment of specialised regulatory provisions governing contract formation in this area appears unnecessary.

Keywords: Blockchain, Distributed Ledger Technology, Legal Validity, Pakistan, Smart Contract, Smart Legal Contract.

Introduction

Smart contracts are self-executing computer programs deployed on distributed ledgers such as blockchain. In legal and commercial settings, they have brought changes how parties form, perform, and record transactions. Their use is not limited to cryptocurrency transactions but also spans a range of financial and commercial activities. One such use is the deployment of these systems as computational tools for recording and performing legal agreements, generally described as smart legal contracts (SLCs). Pakistan has begun a policy shift toward digital systems, with particular attention to blockchain technology and digital assets. The Digital Nation Pakistan Act 2025 and the establishment of the Pakistan Virtual Assets Regulatory Authority represent an important policy move in Pakistan's digital development by regulating and integrating digital financial instruments, including cryptocurrencies and virtual tokens, within the national financial system (Kiani, 2025). A further step in this digital transformation will be the integration of SLCs within the digital economy enabling the use of blockchain-based programmability tokens that represent digital assets as a medium of exchange (Kirillova et al., 2019, p. 293).

DOI: 10.52279/jlss.07.04.289305

Legal certainty is essential for the adoption of innovative digital instruments such as smart contracts and blockchains at commercial scales by mitigating the risks and cultivating the necessary assurance for the enterprises to allocate their resources towards innovative infrastructures. The legal framework of Pakistan has not address the regulatory aspects of smart legal contracts due to the lack of dedicated law and judicial interpretation. The Contract Act, 1872 and the Electronic Transaction Ordinance, 2002 only laid down the principles for traditional contracts and electronic transactions. They do not tackle the novel features of SLCs such as automated performance or the codification of contract terms. The lack of specific laws has created uncertainty about their legal validity and calls for their assessment under the Pakistani contract law.

This study analyse application of existing legal principles regarding contracts formation to SLCs and provide information that may influence future legislation and judicial rulings. This paper explains the concept of SLCs by discussing their characteristics and classifications. It then evaluates SLCs with respect to contract formation elements under Pakistani law to assess their fulfillment. The paper finally synthesise its main findings and recommends a clear course of action.

Embedding Code in Contracts

The Original Conception: Szabo's Smart Contracts

Nick Szabo introduced "smart contracts" to describe an automated protocol designed to perform contractual obligations (Szabo, 1994). He argued these digital protocols would improve on paper contracts by embedding provisions in hardware and software to automate performance and reduce human intervention (Szabo, 1997). He acknowledged the protocol's limits, noting it could only handle a narrow set of contract functions such as "payment terms, liens, confidentiality, and even enforcement." He expected the protocol could fulfil the legal role of enforcing contracts by reducing breaches and removing the need for "trusted intermediaries" through built-in economic safeguards that would impose financial penalties on parties who tried to break the terms. Thus he proposed bypassing conventional legal procedures, a stance that aligns with techno-libertarian principles (Allen & Hunn, 2022, p. 6).

When Szabo proposed this concept, available communication networks could not support automated protocols. Blockchain technology made those protocols technically feasible. Although blockchain began as Bitcoin's protocol in 2009 (Nakamoto, 2008), platforms such as Ethereum (Buterin, 2014) now enable reliable integration and execution of smart contracts.

Blockchain Fundamentals

A blockchain is a distributed ledger that keeps track of transactions by sending and synchronising data between nodes on a peer-to-peer network (World Bank, 2017, p. 1). The system uses cryptography and algorithms to create and verify a growing, append-only database made up of chained "transaction blocks" that together act as a ledger. Blockchain technology has key features that show its design and operational advantages over conventional centralised systems:

Decentralisation

Blockchain is a decentralised technology that runs without any central controlling authority. The system works peer-to-peer: each participant keeps a copy of the decentralised ledger on their computer (Werbach & Cornell, 2017, pp. 325–327). Network participants validate each new transaction block, and every member of the network can access it. Nodes agree on an event's validity by following agreed rules rather than by decision of a single actor (Finck, 2018, p. 20). This creates trust through transparency, and improves security by avoiding reliance on a single centralised server.

Immutability

Blockchain primarily distinguishes itself through a design that resists unauthorized tampering. By sequencing data in linked blocks and employing hashing and asymmetric encryption, the system builds its security features (Bashir, 2017, p. 47). This specific structure consequently prevents any single party from altering the ledger. These features further guarantee non-repudiation by providing undeniable evidence that an event occurred at a particular time and place.

Optimisation of Operational Performance

Blockchain handles intensive data processing while bypassing the expensive hardware overhauls standard to client-server models (De Filippi & Wright, 2018, p. 17). By mirroring datasets across multiple nodes, the system lowers costs and improves overall efficiency.

Classifying Blockchain Systems

Scholars generally divide blockchains into public or private types, alongside the distinction between permissioned and permissionless frameworks (European Law Institute, 2023, p. 23; Schrepel, 2021, p. 21). Public blockchains achieve maximum transparency by exposing every transaction to all network participants. Private blockchains, by contrast, limit access to transaction data to a designated group of authorized users. They are further differentiated on the basis who has the right to submit transactions and validate new blocks. In permissionless settings, any anonymous user can act as a node to initiate transactions, add blocks, or update the ledger. Permissioned networks instead restrict node operations and block creation to a select group of approved participants. Generally, a central administrator governs network entry based on set criteria and enforces system rules (World Bank, 2017, p. 11). Furthermore, these two models provide differing degrees of data immutability. Altering a permissionless ledger requires a majority of nodes to reach a collective consensus. The addition of nodes into the network result in the expanding number of ledger replicas and further complicate the potential for malicious collusion among participants (Eenmaa-Dimitrieva & Schmidt-Kessen, 2017, p. 11). Anonymity of participants makes it even tougher to work together to change the ledger. On the other side, permissioned blockchains work as closed systems where a small group of known validators has more control. This form makes it easy to update rules, reverse transactions, and make other changes to the ledger (Finck, 2018, p. 21).

Smart Contract: A misleading term

The phrase "smart contract" is not accurate. It means that a legal contract has been made, which is not necessarily true. On its own, a smart contract does not meet the legal requirements for a binding contract. It is just a deterministic program that runs on a blockchain when its specified conditions are satisfied (Lyons et al., 2019, p. 22). While smart contracts can encode self-executing agreements relevant to contract law, they are also used across many sectors, including asset tokenisation and automated supply chains. Despite performing functions that resemble traditional agreements, smart contracts do not always satisfy the formal standards for a binding contract (Allen & Hunn, 2022, p. 4).

Smart Legal Contract

To resolve this conceptual confusion, the term “smart legal contract” now identifies code specifically tailored to articulate and enforce binding legal obligations (Stark, 2016). This analysis views an SLC as a binding agreement in which a computer program, the smart contract, specifies and executes some or all obligations automatically and independently of human oversight (UK Law Commission, 2021, para 1.2).

Key Attributes of Smart Legal Contracts

SLCs rely on blockchain technology for deployment and gain additional functional features (Lyons et al., 2019, p. 22).

Automation

Automaticity serves as the defining characteristic of an SLC. Smart contracts carry out set instructions with absolute consistency due to their deterministic nature. Upon receiving input data, the program independently processes the information to fulfill obligations for the promisee. Consequently, the code discharges obligations without the risk of human hesitation or refusal, as it lacks the capacity to default (Green & Sanitt, 2020, p. 191). That operation delivers dependable enforcement once the triggering conditions are met.

Digital Character

Because SLCs operate automatically, contractual obligations must be expressed in code. This approach suits obligations based on conditional logic (if X, then Y), which aligns with the Boolean logic used in programming (ISDA & Linklaters, 2017, p. 11). SLCs exist only in electronic form because their subject matter and execution environment are digital, including cryptocurrencies and tokenised assets recorded on a blockchain (Savelyev, 2017, p. 124).

Non-repudiation

The decentralisation and tamper-resistant properties of blockchain help in ensuring that no single entity controls the network. Thus, parties are prevented from disrupting or altering a smart contract's execution (Savelyev, 2017, pp. 126–127). Moreover, blockchain's value lies in solving the double-spending problem by ensuring a digital asset cannot be spent more than once to multiple recipients (World Bank, 2017, p. 2). Distributed governance strengthens a contract's integrity and operational security, promotes trust by making performance certain, and increases efficiency by removing intermediaries and their costs.

Self-enforcement

Before blockchain, one of the parties had to rely on their counterpart's digital system to uphold electronic agreement. Blockchain removes the need for trust by operating as a peer-to-peer network in which each participant holds and runs the same code, producing results that are effectively indisputable (McKinney et al., 2018, p. 318). Consequently, no party can override the code's logic, and when that logic encodes contractual terms, the parties need not take additional steps to secure performance.

Typologies of Smart Legal Contracts

Distinguishing between different types of contractual clauses is essential, as some terms are neither suitable for independent automation nor appropriate for such a transition (Clack et al., 2017, p. 5; ISDA & Linklaters, 2017, p. 10). Scholars therefore categorize contract terms into operational and non-operational types. Operational clauses govern contract execution by defining duties that can be measured objectively and expressed through conditional logic. An illustrative example of such a paradigm can be found in the programming of a SLC to facilitate the release of escrow payments contingent upon the confirmation of delivery (Schrepel, 2021, p. 17). In contrast, non-operational provisions pertain to issues that defy codification, including choice-of-law and jurisdiction clauses, as well as obligations that necessitate human judgement, such as 'best efforts' or standards of reasonableness (Mik, 2017, p. 294). The SLCs have been put into three main groups based on the role that the code plays: 'external', 'hybrid' and 'solely code'(European Law Institute, 2023, pp. 24–27; UK Jurisdiction Taskforce, 2019, para 142; UK Law Commission, 2021, para 2.51).

In its external form, a legal contract exists off-chain alongside a code that resides on-chain. The code just serves as a tool to implement the rights and duties specified in the legal contract, for example, daily collateral flows (ISDA & Linklaters, 2017, p. 14). The code operates in a subordinate capacity to the legal contract, reflecting a hierarchical relationship in which the natural language document takes precedence. Thus, in instances a conflict arises between the code's execution and the contractual prose, the latter shall prevail.

Hybrid form merge traditional text and computer code into a single document by splitting obligations between natural language and executable scripts. A single contractual provision can also be expressed at the same time in both code and natural language. This format uses blockchain automation without losing legal precision by integrating machine-executable code with human-readable language (Verstappen, 2023, p.4). Since the parties agree to the SLC's terms through ordinary off-chain communications, whether in prose or code, the contract forms off-chain. If the natural-language and coded terms diverge, a legal issue arises over which version controls.

In solely coded SLCs the terms of the agreement are written and executed in source code without any natural-language counterpart. The source code can serve as the legal agreement, because it can manifest the parties' intent, govern their obligations, and record the resulting legal relationship (Tjin Tai, 2022, p. 210; Werbach & Cornell, 2017, p. 13). Accordingly, this form constitutes an on-chain method of contract formation when communications of proposal and its assent take place via the blockchain. Applications of SLCs expressed only in code are clear in the decentralised finance (DeFi) sector (Verstappen, 2023, p. 4).

Forming Smart Legal Contracts under Pakistani law

In Pakistan, contract formation under Section 10 of the Contract Act 1872 requires four elements: agreement, consent, capacity and consideration. Those same elements also apply to SLCs.

Agreement: Congruence of Proposal and its Reciprocal Acceptance

An agreement is formed by promises that act as consideration for each other (Contract Act, 1872 s. 2(e)). A proposal is an expression of the promisor's willingness to do or refrain from an act intended to obtain the promisee's assent (Contract Act, 1872 ss. 2(a)-(b)). Thus, an agreement arises from a proposal and its corresponding acceptance. The interchange of proposal and acceptance may be executed through either an affirmative act or a deliberate omission by the party making the proposal or the party accepting it, with the clear intention to convey such proposal or acceptance (Contract Act, 1872 s. 3).

The formation of a SLC may take place through both off-chain and on-chain mechanisms (Durovic & Janssen, 2019, p. 65). The formation of an on-chain contract can take place through a solely code SLC. In this scenario, the proposer transmits the code to the Ethereum. The promisee then accepts by interacting with it like sending requisite ethers as a payment. In contrast the formation of a SLC off-chain can take place either through external or hybrid forms, where parties negotiate and finalize the agreement using traditional methods such as in-person meetings or digital communications like email or websites before triggering the execution of the code on-chain (Bomprezzi, 2021, p. 129). Accordingly, off-chain SLCs give rise to no novel legal issues regarding exchange of proposal and its acceptance, being readily accommodated by existing doctrine, this section is confined to on-chain SLCs.

The uniqueness of the proposal

The proposal should encompass all requisite components to establish a legally binding contract; i.e., a proper proposal must possess the capability for acceptance (Soomro, 2015, p. 36). Contrarily, one encounters merely an invitation to treat, which serves as an enticement for another party to extend a proposal.

If a user uploads code to a blockchain that specifies transaction terms, treat that upload as a proposal rather than merely an invitation to treat (Durovic & Janssen, 2019, p. 67). Other participants can interact with and trigger the uploaded code's execution, which supports treating the upload as a valid proposal (Madir, 2018, p. 7). Existing common law, such as the principle that a functional automated parking machine ready to accept payment amounted to a proposal to enter the car park, reflect this rationale (*Thornton v Shoe Lane Parking Ltd*, 1971). By the same logic, deploying code that automatically transfers assets on payment can be seen as making a contractual proposal.

A proposal can be addressed to specific individuals or to a wider audience, including the public (*Carlill v Carbolic Smoke Ball Company*, 1893*)*. In the context of a public blockchain, code is accessible to all participants (Chamber of Digital Commerce, 2018, p. 17). Technically, if the code's execution is restricted to a particular blockchain address, the proposal may be deemed directed at a specific user. However, where the code is open to interaction from any participant, the proposal may be regarded as addressed to the public at large. Accordingly, SLCs are capable, in our view, of satisfying all the indicia of a valid proposal.

The particularity of acceptance

From a legal standpoint, acceptance must be absolute and unconditional, signifying the promisee's complete assent to all terms of the proposal (Contract Act, 1872 s. 7(1)). In the SLC framework, a promisee accepts the proposal once they authorize the transaction using their private key (Madir, 2018, p. 7). Any attempt to accept a proposal while varying its terms fails as a legal acceptance and functions instead as a counter-proposal (Soomro, 2015, p. 46). This act amounts to revocation of the initial proposal and assumes a fresh proposal. Thus, the role of the parties are reversed and now the original proposer has to accept this new proposal to form a contract. Blockchain's inherent immutability complicates this traditional legal exchange. After deployment, the code terms remain fixed and resistant to on-chain modification. Thus these proposals present a simple accept-or-reject choice and function unilaterally (Werbach & Cornell, 2017, p. 343). If the proposee wants to change the terms, they must deploy new code, which creates a fresh proposal and makes them the proposer.

The law generally requires standard communication of acceptance but it may also be inferred from conduct, such as performing the proposed conditions or accepting consideration (Contract Act, 1872 ss. 7(2) and 8). If a proposal is deployed in code, explicit natural-language communication of acceptance typically does not occur (Carron & Botteron, 2019, p. 127). Such digital proposals often include conditions precedent, where acceptance occurs by performance, for example, transferring a digital asset (e.g., currency, cryptocurrency, or tokenised offline asset) to the code (Raskin, 2016, p. 322). Where a proposal prescribes a mode of acceptance and the acceptor uses a different mode, the proposer may, within a reasonable time, insist on compliance. Otherwise, the acceptance is valid (Contract Act, 1872 s. 7(2)). With code, on-chain acceptance occurs only by the technical method specified in the code. Accordingly, solely coded SLCs allow for valid legal acceptance.

Timing of Contract Formation

The timing of contract formation is crucial. It determines when revocation becomes impossible and the parties become bound by their promises. A contract forms when a proposal is validly accepted (Soomro, 2015, p. 45). Determining this moment is straightforward in face-to-face or instantaneous exchanges, but it grows more complex when parties do not interact simultaneously and delays occur between proposal and acceptance. Law address these delays through the specific doctrines of dispatch, receipt, and actual notice to fix when a binding agreement forms (Christandl, 2018, pp. 324–326). Under the dispatch rule, acceptance takes effect when the acceptor sends it. By contrast, the receipt rule treats the contract as formed when the proposer receives the acceptance. Finally, the actual notice rule requires the proposer to be personally aware of the acceptance before the contract is binding.

The Contract Act adopts the postal rule from common law (*Adams v Lindsell*, 1818), applying the dispatch and actual-notice rules to fix when acceptance binds proposer and acceptor. Section 4 treats acceptance as binding on the proposer when it is dispatched and as binding on the acceptor when the proposer learns of it. The postal rule was designed to balance the proposer's power to revoke before contract completion with the need to protect the acceptor's interests (Peel, 2015, para 2-031).

The exchange of proposal and acceptance through email as electronic messages is similar to on-chain SLC execution transpired by the use of public-key infrastructure (R3 & Norton Rose Fulbright, 2016, p. 22). Blockchain-based proposals and acceptances thus qualify as electronic messages under existing legal standards. Thus, the rules for electronic contracts help determine when contract formation occurs on the blockchain.

In electronic contracting, traditional formation rules were adapted for digital use through UNCITRAL's adoption of the Model Law on Electronic Commerce (MLEC) in 1996. It is based on the principles of non-discrimination, technological neutrality, and functional equivalence to apply with paperless communication methods (Mukherjee, 2018). Pakistan followed this model and enacted the Electronic Transactions Ordinance (ETO) 2002 to legally recognise electronic documents, records and communications. The ETO is silent on the exact moment a contract is finalized, Section 15 establishes the rules for dispatch or receipt of messages. The time of receipt depends on whether the addressee has designated a specific computer system to receive the message. If a designated system exists, receipt transpires when the message enters that system. If the message is delivered to a different system owned by the addressee, it is considered received only upon retrieval i.e., actual notice. Where no system has been designated, receipt is deemed to occur once the communication enters any of the addressee's computer systems. These provisions along with Section 4 of the Contract Act treat acceptance as binding on the proposer when it is dispatched from the acceptor's computer system, and as binding on the acceptor when it arrives at the proposer's IT system. However, if the proposer has specified a particular IT system for receiving acceptances and the message reaches a different system under their control, it binds the acceptor only upon actual retrieval by the proposer.

Considering that the contract formation took place off-chain in external and hybrid forms, there exists no novel issue in ascertaining the timing of its formation. Consequently, in instances where the agreement is established offline, traditional regulations will govern, whereas in cases of online formation, the prevailing rules shall be interpreted to correspond with the electronic environment. Solely coded SLCs introduce a distinct method of contract formation through on-chain exchanges of proposal and acceptance. Applying the rules of dispatch and receipt to a blockchain requires identifying which specific technical acts meet these legal definitions. Effectiveness could occur either when a transaction is broadcast or when the network reaches consensus on its validity (Giancaspro, 2017, p. 830). One view suggests that dispatch occurs when an acceptor uses a private key to sign and transmit a transaction to the contract's address (Finocchiaro & Bomprezzi, 2020, p. 121). Receipt occurs when the validated transaction is accessible to the proposer after all nodes update their copies of the ledger. Under Pakistani law, acceptance may bind the proposer once the acceptance-transaction is recorded on the blockchain. The acceptor, however, becomes bound only after network consensus validates the transaction and routes it to the proposer.

Applying the postal rule adds unnecessary theoretical difficulty to determining exactly when a contract forms. While the postal rule suited the era of slow mail, it fails to account for how instant digital tools work today. Splitting liability between dispatch for one party and notice for the other creates contradictions that can threaten a contract's enforceability. We recommend that the legislature adopt a single receipt-based rule to determine contract formation.

Where acceptance is by conduct, the law treats performance of the proposal's terms or accepting the stated consideration as forming the contract (Contract Act, 1872 s. 8). Because solely coded SLCs are unilateral, acceptance occurs when a user sends tokens to the contract address, leaving the network's miners to carry out the remaining functions.This position finds support in the Common law (*Thornton v Shoe Lane Parking Ltd,* 1971), where the court held that acceptance occurred when the consumer inserted payment into the machine. Therefore, in our view the receipt rule becomes relevant here, and the solely code SLC is concluded when the proposer's address receive the requisite token.

Rules on Revocation

Revocation of proposal

A proposal can be withdrawn at any point before the acceptance has been effectively communicated to the proposer (Contract Act, 1872 s. 5). Therefore, in situations involving non-instantaneous communication, the revocation of proposal must be received by the acceptor before he initiate the transmission of acceptance to the proposer. A proposal may be revoked in four recognised ways: (i) through the communication of a revocation notice from the proposer to the other party; (ii) by the expiration of the time specified for acceptance in the proposal, or, if no time is specified, after a reasonable period has passed without acceptance being communicated; (iii) by the acceptor's failure to satisfy a condition precedent to acceptance; or (iv) by the death or insanity of the proposer, provided that the acceptor becomes aware of such death or insanity prior to acceptance (Contract Act, 1872 s. 6).

As established in the preceding discussion on the temporal dimensions of contract formation, the rules governing revocation of proposal and acceptance to off-chain formations do not involve any novelty. However, in the context of on-chain formation, the inherent immutability of blockchain architecture may operate as a substantive constraint on the proposer's capacity to effect revocation. The matter concerns how the technology operates, not the application of legal rule. In a permissionless blockchain, altering code after deployment is generally very difficult because of the system's structure. The code can still be deleted, however (Marino & Juels, 2016, p.158). Ethereum contracts, for example, use a self-destruct function to remove code and storage from the network (Chen et al., 2022). A proposer who triggers this function effectively issues a revocation notice as now code cannot be invoked and the proposal in it cannot be accepted. Accordingly, condition (i) can occur in on-chain SLCs.

Developers can design SLCs to bar users from executing code once a specific deadline passes (Meyer, 2020, p. 20). Since computer systems cannot interpret the legal concept of a 'reasonable time', this standard remains functionally useless for autonomous code (Giancaspro, 2017, p. 831). To prevent a proposal from lasting forever, the proposer should instead program a specific expiration date into the code. This approach allows on-chain SLCs to satisfy the requirements of case (ii). SLC code logic suggests that for case (iii) revocation happens implicitly because a condition precedent must be met before the code can run. That condition can require submitting a token that represents a native or off-chain asset, so no separate revocation mechanism needs to be coded into the contract.

With respect to case (iv), we doubt whether the rule applies to on-chain SLCs or whether the required conditions could realistically be contested in court. Typically, once an acceptor satisfies the condition precedent, the code executes automatically to finalize the transaction. Complications arise on breach where the promisee has died, become mentally incapacitated, or where a company has been dissolved. At that point, the claimant would have to file suit to recover damages for the breach. In our view, the legal representative of the proposer shall retain liability, contingent upon the acceptor's lack of awareness regarding any dissolution, mortality, or insanity prior to acceptance. Therefore, regarding solely code SLCs, we believe that the revocation of the proposal concerns how the technology operates, not the application of legal rule.

Revocation of acceptance

An acceptance can be revoked at any point before its communication is deemed complete with respect to the acceptor (Contract Act, 1872 s. 5). The Contract Act draws a clear distinction between the completion of communication of revocation vis-à-vis the party initiating the revocation and the party to whom it is directed. Pursuant to section 4, revocation is deemed complete as against the revoking party when it is dispatched beyond his control, and as against the recipient when it is received and comes to his knowledge. Therefore, in cases of non-instantaneous communication, the revocation of acceptance is effective only if it reaches the proposer before the acceptance itself is received by him.

Fast electronic communication has raised concerns about the possibility of rescinding acceptance (Bomprezzi, 2021, p. 90). Under the postal rule, the proposer's right to revoke ends at dispatch, whereas the acceptor's right ends the moment the proposer receives the acceptance (Fasciano, 1997, p. 975). On blockchain, it is unclear whether on-chain records can reliably show that a revocation occurred before a valid communication of acceptance. Legally, the revocation must be recorded on the proposer's node before the acceptance transaction to be valid. Because blockchains are normally immutable, on-chain revocation is difficult unless the code itself provides a revocation mechanism. If revocation is technically possible, the blockchain's chronological block structure, which provides a timestamped audit trail, could help verify which transaction actually came first.

The delay between an acceptor signing a transaction and its final validation on the blockchain might actually minimize the practical difficulties of revocation. Validators might include a transaction that nullifies the acceptance before they include the acceptance transaction. This sequence would render the acceptance validly revoked before it ever becomes binding. Thus, for solely coded SLCs, revocation of acceptance is determined by the technology's operational logic rather than by conventional legal rules.

Consent

Consensus ad idem is fundamental for contract formation in Pakistan. The Supreme Court held it as the basis of a meeting of minds and the evidence of parties' shared intention (*Farzand Ali v Khuda Bakhsh*, 2015). Under Section 13 of the Contract Act, consent only exists when parties agree upon the same thing in the same sense. "Same thing" means the same subject matter and "same sense" refers to the nature of the obligations or the context in which they apply. As Aftab Ahmed notes, no agreement is reached if the parties are preoccupied with different objects or interpret the contract's language differently, regardless of whether the confusion lies in the terms or the nature of the deal (Ahmed, 1987, p. 19). Ultimately, a contract does not form unless both parties share an identical understanding of its terms.

Courts assess consent by the objective reasonable-person standard (Wijayasriwardena, 2016, p. 4). This approach also places a stronger obligation on the drafting party to present the contract's terms in a form that people can readily understand. Solely coded and hybrid SLCs embodies contractual terms in programming code. Because most users cannot readily interpret programming code, the parties may struggle to confirm whether they genuinely agreed to the same terms (Carron & Botteron, 2019, p. 129; O'Shields, 2017, p. 186). The risk is greatest when one party alone drafts and deploys the coded SLC and the other simply accepts the pre-coded terms without negotiation.

Solely coded SLCs function like standard-form contracts because one party compile them, non-technical acceptors may not understand the terms, and blockchain design prevents counter proposals (Carron & Botteron, 2019, p. 129). Consumers in such weaker bargaining position become vulnerable and need additional legal protections. Specific rules apply to contracts made in the absence of negotiation and set out when the non-drafting party takes on legal responsibilities. Scholarly consensus holds that the drafter should take "reasonable steps" to inform the counterparty of the terms before or during contract formation (Jansen, 2018, pp. 277–278). Here, 'reasonable steps' means that the business must make the terms easy to find and written in language the consumer can understand.The rules established in the Contract Act regarding general contracts apply to standard-form contracts in Pakistan due to the lack of specific regulations for them. Additionally, existing case law has not directly addressed this issue. We suggest that, when presented with such cases, the courts would refer to current international standards for guidance.

In the realm of online contracts, standard-form contracts often take the form of 'wrap contracts', with click-wrap and browse-wrap as their predominant forms (Kim, 2013, pp. 2, 39–41). A 'click-wrap' contract presents the terms through a scrollable box or hyperlink, which the acceptor accepts by clicking the 'I agree' checkbox (Momberg, 2016, pp. 192–193, 204). On the contrary, a 'browse-wrap' contract lets users download digital material or access a website without clicking a specific checkbox or taking any other action. The provisions are available via hyperlinks marked 'terms of use' or 'legal terms'. The proposer must notify the proposee of the provisions before or during contract formation in both cases. Thus, the business must ensure that the other party understands the terms that they are agreeing to. Without these setups, in the case of browse-wrap agreements, the non-drafting party may not recognise their contractual nature due to the absence of any required affirmative action. Although, clicking a click-wrap box is not the same as signing, but it does indicate user engagement and therefore greater awareness.

This idea also fits solely code SLCs, which resemble wrap contracts because they use an atypical way of signalling acceptance (Finocchiaro & Bomprezzi, 2020, p. 123).Off-chain SLCs usually arise from face-to-face dealings or by the consumer accepting terms on the business' website. However, with hybrid SLCs, users may find the coded parts of the terms difficult to understand. For this reason, the proposer must explain the terms in plain language and take all steps needed to help the other party understand them. Where the drafter has fulfilled its disclosure duties, the consumer cannot evade the legal effects of a coded contract on account of absence of consent.

Competency of Parties

An agreement to be enforceable under Pakistani law must be entered between competent persons. Section 11 of the Contract Act treats a person as competent if they are an adult, have sound mental capacity, and are not legally barred from making contracts. The absence of any of these qualities can invalidate the agreement and expose the other party to legal consequences. Pakistani case law treats a minor's agreement as void from the start and bars its ratification even after the minor becomes an adult (*Mehr Manzoor Hussain v Muhammad Nawaz*, 2010, [8]). The courts consistently hold that a minor cannot be held liable under a void contract (*The Chairman, District Scrutiny Committee v Sharif Ahmad Hashmi*, 1976). Even the doctrine of promissory estoppel does not apply in cases involving minors (*SherBaz Khan v Malkani Sahibzadi Tiwana,* 1996, [15]). Consequently, even when a minor fraudulently misrepresents himself as being of the age of majority to induce a counterparty to conclude an agreement, this does not prevent the minor from asserting his minority status to nullify the agreement (K*han Gul v Lakha Singh,* 1928, [11]). Furthermore, here the doctrine of unjust enrichment is also inapplicable, as minor is not required to repay advantages obtained under such an agreement. Comparably, any agreement by a person of unsound mind is void (Soomro, 2015, p. 98). The test for determining unsoundness of mind involves assessing whether a person lacks the capacity to comprehend the agreement and make a rational evaluation of its implications for their interests, which may be affected by factors such as a medical condition or inebriation (Contract Act, 1872 s. 12).

SLCs pose a problem for contractual capacity because there is no mechanism to confirm whether on-chain parties have the required legal competence (Hsiao, 2017, p. 693). This difficulty stems from the pseudonymity of permissionless blockchains, which do not reveal who is actually carrying out the transactions (Mik, 2017, p. 279). Consequently, persons who lack legal capacity like minors can still open accounts on permissionless blockchains and transact. An incompetent person can use or accept an SLC and later assert its invalidity to avoid the consequent legal obligations. This can harm the counterparty by hindering their right to obtain legal remedies. Pseudonymity and immutability on blockchain can also hinder the effectiveness of unjust-enrichment claims. It is difficult to identify a pseudonymous defendant. Restitution, requiring transaction reversal, is technically hard to achieve in SLCs unless the code itself allows the transaction to be reversed (Durovic & Janssen, 2019, p. 72).

Scholars have criticised Pakistani courts' approach of treating minors' agreements as void ab initio (Hussain & Fatima, 2024, p. 63). Minors are entering more types of contracts as they become more proficient with the technologies that support virtual transactions. They enter many online agreements to create email accounts, join social platforms, or use educational apps. Likewise, it is not unusual for young people to take part in SLCs for legitimate purposes. Declaring minors' contracts void ab initio can limit their access to lawful goods and services. This approach can cause problems because online platforms and permissionless blockchains generally cannot verify a user's legal competence.

The parties' pseudonymity can pose a problem only when the SLC is formalised on-chain in a permissionless setting. Off-chain agreements typically pose no identification problems because they arise in person or through a company's online platform. The party identity is likewise not an issue for on-chain contracts in permissioned settings because node identification is required to grant access (Sanz Bayón, 2019, p. 82).

A viable method for verifying identity and by extension, contractual capacity within permissionless blockchain environments may be derived from Section 13(1)(c) of the ETO, which provides that an electronic communication is attributable to its originator when transmitted through an information system configured by or on behalf of that individual to operate automatically. In the context of on-chain SLCs such attribution enables identification of the originator via a blockchain-anchored digital identity linked to a specific individual (Lapointe & Fishbane, 2019, pp. 54–55). Accordingly, even within permissionless frameworks, party identification may be feasible, particularly if legal obligations are imposed on blockchain service providers to screen users in advance for eligibility (Verstappen, 2023, p. 90). Therefore, in our opinion, the issue of cometency of contracting parties may be resolved through technical configurations of on-chain environment.

Consideration

The law generally requires that a binding agreement involve mutual benefit, as its formation rests on the reciprocal exchange of promises, each constituting consideration for the other (Contract Act, 1872 s. 2(e)). Accordingly, consideration is an essential element of a valid contract, and its absence renders an agreement void and unenforceable in law (Contract Act, 1872 ss. 10 and 25). The Supreme Court of Pakistan ruled that a pledge to perform for no consideration might possess ethical significance but does not create a contractual obligation or legal right and is therefore not enforceable (*Ch. Ghulam Rasool v Mrs. Nusrat Rasool,* 2008). However, exceptions to this rule exist, such as registered agreements based on natural love and affection among close relatives, promises to compensate for past voluntary acts, and written acknowledgments of time-barred debts (Contract Act, 1872 s. 25).

Consideration need not be a payment or something with an exact monetary value. It is an act, forbearance, or promise given at the promisor's request, may be past, present, or future and can be supplied by the promisee or even by a third party (Contract Act, 1872 s. 2(d)). Consequently, it encompasses any abstention, forbearance, detriment, or obligation that a promisee exhibits, endures, or assumes, which subsequently leads to an associated right, interest, advantage or profit for the promisee (*Hafeezullah Khan v Al-Haj Chaudhri Barkat Ali,* 1998). Moreover, consideration need not be adequate in value (Contract Act, 1872 s. 25 Explanation 2). The law prioritises the mutual and reciprocal nature of the exchange over its equivalence. Courts defer to the parties' autonomy in determining adequacy and will uphold consideration even if it is nominal (*Kulasekaraperumal v Pathakutty Thalevanar*, 1961, [9]).

In most instances, SLCs are expected to be concluded off-chain through external or hybrid forms that merge code with a natural language agreement, allowing traditional methods to assess consideration by examining reciprocal promises. Identifying consideration in on-chain SLCs is more difficult and demands a deeper legal analysis. Scholars disagree about whether solely code SLCs can satisfy the requirement of consideration. Some argue that because smart contracts lack the element of independent choice in their execution, they fail to form a mutual agreement of promises and thus lack valid consideration (Savelyev, 2017, pp. 128–130). This view overlooks the fact that delegating tasks to an automated system does not absolve a party of legal responsibility (Giancaspro, 2020, p. 37). Parties are legaly liable for their obligations whether they perform them personally or through code, as applied to automated electronic agreements.

Critics also contend that smart contracts lack valid consideration because they only automate transfers without personal commitments and do not exchange promises (Werbach & Cornell, 2017, pp.340–341). They do not change the legal relationship between parties and therefore are not real contracts. This argument is self-contradictory. The authors admit that even if smart contracts are not traditional promises, they still act as voluntary tools for parties to change their legal rights. They also accept that an agreement can be a contract even when no further acts are required, as in an executed contract.

In an SLC, consideration can be identified by examining the code or how it runs, and it turns on whether the parties exchange reciprocal promises or value (UK Jurisdiction Taskforce, 2019; Mik, 2017). When the parties deploy an SLC that transfers digital assets or tokenised goods or services for cryptocurrency, the exchange of value is clear. Since cryptoassets are now treated as property, on-chain SLCs should not be excluded from meeting consideration (UK Jurisdiction Taskforce, 2019, para 85). Moreover, given that cryptoassets are opined to be treated as property (UK Jurisdiction Taskforce, 2019, para 85), there is no compelling reason to exclude on-chain SLCs from satisfying the requirements of consideration. Commentators also say that on-chain SLCs function as unilateral contracts built on "if X, then Y" logic, with consideration supplied by performance (Durovic & Janssen, 2019, p. 70). For example, an insurance policy coded into the system can pay out automatically when a specified event occurs. Thus, the parties' exchange of rights and duties is built into the code and executed automatically by the SLC.

Conclusion

This study analysed validity of SLCs under the legal system of Pakistan. It shows that regardless of the terminology used, smart contracts are not binding in isolation. The legal basis still depends on the agreement between the parties. Because Boolean logic cannot encode every contractual term, the study identifies three distinct uses of smart contracts in forming SLCs. These contracts can be off-chain, where code only performs set obligations, or on-chain, where code both executes performance and expresses the parties' contractual intentions. This distinction makes it necessary to re-evaluate traditional contract formation rules to determine how SLCs can be integrated into Pakistan's contract law. Accordingly, the study examined formation prerequisites, starting with proposal and acceptance, their revocation and the exact time a contract forms. The study then considers the other formation elements: consent, capacity and consideration.

The study found that off-chain SLCs, whether structured as external or hybrid models, are formed when parties negotiate and finalise their agreements through traditional channels of communication, and do not introduce any novel legal challenges to the essential requirements for contract validity. Further, it is revealed that solely code SLCs operate as unilateral contracts, in which the smart contract itself embodies a proposal conditional upon a specified performance, such as the transfer of a digital asset to effect acceptance. Consequently, Pakistani contract law imposes no substantive obstacle to the concurrence of proposals and their acceptance in the formation of on-chain SLCs. On-chain SLCs qualify as contracts formed remotely and electronically through the exchange of electronic messages on blockchain. Moreover, regarding the timing of contract formation and revocation of proposal and acceptance, the challenge arises not from the technology itself but from the paradoxical nature of the outdated postal rule, which is unsuitable for today's rapid communication means and should be replaced by the receipt rule.

Regarding the element of consensus ad idem it is observed that as encoding contractual terms in a programming language, in both solely coded and hybrid formats, can obscure evidence of mutual assent, given that code is generally unintelligible to laypersons. Having noted parallels with standard-form wrap contracts and the significance of disclosure obligations, we are of the view that proposers must articulate code-defined terms in clear, plain language and secure the acceptor's full understanding to preclude any evasion of liability for lack of mutual assent. The pseudonymity of public permissionless blockchains raises doubts about the legitimacy of on-chain SLCs, especially where a party lacks legal capacity because real identities cannot be verified. This risk can be managed if blockchain service providers require identity checks and eligibility screening before allowing users to interact with the system. Consideration is satisfied in on-chain SLCs where digital assets or tokens are transferred for cryptocurrency, constituting a mutual exchange of value. This analysis shows that SLCs are essentially electronic contracts, and traditional contract law principles still apply to them. It is concluded that, at least in the context of contract formation, there is no necessity to establish new bespoke rules.

References

Adams v Lindsell, 1 ER 250 (1818).

Ahmed, A. (1987). Law of Contract and Agency in Pakistan. Aamir & Aasim Publications.

Allen, J. G., & Hunn, P. (2022). Editors' Introduction. In J. Allen & P. Hunn (Eds), Smart Legal Contracts: Computable Law in Theory and Practice (pp. 1–22). Oxford University Press. https://doi.org/10.1093/oso/9780192858467.003.0001

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

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

Buterin, V. (2014). Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform. https://ethereum.org/en/whitepaper/

Carlill v Carbolic Smoke Ball Company, 1 QB 256 (1893).

Carron, B., & Botteron, V. (2019). How smart can a contract be? In D. Kraus, T. Obrist, & O. Hari (Eds), Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law (pp. 101–143). Edward Elgar Publishing. https://doi.org/10.4337/9781788115131.00011

Ch. Ghulam Rasool v Mrs. Nusrat Rasool, PLD 2008 SC 146.

Chamber of Digital Commerce, S. C. A. (2018). Smart Contracts: Is the Law Ready? https://lowellmilkeninstitute.law.ucla.edu/wp-content/uploads/2018/08/Smart-Contracts-Whitepaper.pdf

Chen, J., Xia, X., Lo, D., & Grundy, J. (2022). Why Do Smart Contracts Self-Destruct? Investigating the Selfdestruct Function on Ethereum. ACM Transactions on Software Engineering and Methodology, 31(2), 1–37. https://doi.org/10.1145/3488245

Christandl, G. (2018). Formation of Contracts. In N. Jansen & R. Zimmermann, Commentaries on European Contract Laws (pp. 230–347). Oxford University Press. https://doi.org/10.1093/oso/9780198790693.003.0003

Clack, C. D., Bakshi, V. A., & Braine, L. (2017). Smart Contract Templates: Foundations, design landscape and research directions (No. arXiv:1608.00771). arXiv. http://arxiv.org/abs/1608.00771

Contract Act (1872).

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

Eenmaa-Dimitrieva, H., & Schmidt-Kessen, M. J. (2017). Regulation through code as a safeguard for implementing smart contracts in no-trust environments [Working Paper]. https://cadmus.eui.eu/handle/1814/47545

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

Farzand Ali v Khuda Bakhsh, PLD 2015 SC 187

Fasciano, P. (1997). Internet Electronic Mail: A Last Bastion for the Mailbox Rule. Hofstra Law Review, 25(3), 971–1003.

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

Finocchiaro, G., & Bomprezzi, C. (2020). A legal analysis of the use of blockchain technology for the formation of smart legal contracts. Media Laws, 2, 111–135.

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

Giancaspro, M. (2020). The consideration myth about smart contracts. ANU Journal of Law and Technology, 1(1), 35–44.

Green, S., & Sanitt, A. (2020). Smart Contracts. In P. S. Davies & M. Raczynska (Eds), Contents of commercial contracts: Terms affecting freedoms (pp. 191–210). Hart.

Hafeezullah Khan v Al-Haj Chaudhri Barkat Ali, PLD 1998 Karachi 274

Hsiao, J. I.-H. (2017). 'Smart' Contract on the Blockchain-Paradigm Shift for Contract Law? US-China Law Review, 14(10), 685–694.

Hussain, N., & Fatima, S. (2024). Capacity of Minor's Contracts under the Contract Act in Pakistan: A Critical Appraisal. Current Trends in Law and Society, 4(1), Article 1. https://doi.org/10.52131/ctls.2024.0401.0032

ISDA, & Linklaters. (2017). White Paper: Smart Contracts and Distributed Ledger – A Legal Perspective. https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf

Jansen, N. (2018). Art 2:104: Terms not Individually Negotiated. In N. Jansen & R. Zimmermann, Commentaries on European Contract Laws (pp. 272–280). Oxford University Press. https://doi.org/10.1093/oso/9780198790693.003.0003

Khan Gul v Lakha Singh, AIR 1928 Lah 609

Kiani, K. (2025, July 10). Authority to regulate crypto and digital assets formed. DAWN.COM. https://www.dawn.com/news/1923184

Kim, N. S. (2013). Wrap contracts: Foundations and ramifications. Oxford Univ. Press.

Kirillova, E. A., Bogdan, V. V., Lagutin, I. B., & Gorevoy, E. D. (2019). Legal status of smart contracts: Features, role, significance. JURÍDICAS CUC, 15(1), 285–300. https://doi.org/10.17981/juridcuc.15.1.2019.11

Kulasekaraperumal v Pathakutty Thalevanar, AIR 1961 MAD 405.

Lapointe, C., & Fishbane, L. (2019). The Blockchain Ethical Design Framework. Innovations: Technology, Governance, Globalization, 12(3–4), 50–71. https://doi.org/10.1162/inov_a_00275

Lyons, T., Courcelas, L., & Timsit, K. (2019). Legal and Regulatory Framework of Blockchains and Smart Contracts. European Union Blockchain Observatory and Forum. https://www.eublockchainforum.eu/sites/default/files/reports/report_legal_v1.0.pdf

Madir, J. (2018). Smart Contracts: (How) Do They Fit Under Existing Legal Frameworks? SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3301463

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

McKinney, S. A., Landy, R., & Wilka, R. (2018). Smart Contracts, Blockchain, and the Next Frontier of Transactional Law. Washington Journal of Law, Technology & Arts, 13(3), 313–347.

Mehr Manzoor Hussain v Muhammad Nawaz, SCMR 1042 (2010).

Meyer, O. (2020). Stopping the Unstoppable: Termination and Unwinding of Smart Contracts. Journal of European Consumer and Market Law, 9(1), 17–24.

Mik, E. (2017). Smart contracts: Terminology, technical limitations and real world complexity. Law, Innovation and Technology, 9(2), 269–300. https://doi.org/10.1080/17579961.2017.1378468

Momberg, R. (2016). Standard Terms and Transparency in Online Contracts. In A. De Franceschi (Ed.), European Contract Law and the Digital Single Market (1st edn, pp. 189–208). Intersentia. https://doi.org/10.1017/9781780685212.011

Mukherjee, A. (2018). Smart Contracts – Another Feather in UNCITRAL's Cap. Cornell International Law Journal Online, 6. https://cornellilj.org/2018/02/08/smart-contracts-another-feather-in-uncitrals-cap/

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/en/bitcoin-paper

O'Shields, R. (2017). Smart Contracts: Legal Agreements for the Blockchain. North Carolina Banking Institute, 21, 177–194.

Peel, E. (2015). Treitel: The law of contract (14th edn). Sweet & Maxwell : Thomson Reuters.

R3, N. R. F., & Norton Rose Fulbright. (2016). Can smart contracts be legally binding contracts? An R3 and Norton Rose Fulbright White Paper. https://engage.nortonrosefulbright.com/596/14051/uploads/r3-and-norton-rose-fulbright-white-paper-full-report-144581.pdf

Raskin, M. (2016). The Law and Legality of Smart Contracts. Georgetown Law Technology Review, 1(2), 305–341.

Sanz Bayón, P. (2019). Key Legal Issues Surrounding Smart Contract Applications. KLRI Journal of Law and Legislation, 9(1), 63–91. https://doi.org/10.2139/ssrn.3525778

Savelyev, A. (2017). Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law. Information & Communications Technology Law, 26(2), 116–134. https://doi.org/10.1080/13600834.2017.1301036

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

SherBaz Khan v Malkani Sahibzadi Tiwana, PLD 1996 Lah 483.

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

Stark, J. (2016, June 4). Making Sense of Blockchain Smart Contracts. https://www.coindesk.com/markets/2016/06/04/making-sense-of-blockchain-smart-contracts/

Szabo, N. (1994). Smart Contracts. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. First Monday, 2(9). https://doi.org/10.5210/fm.v2i9.548

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

Thornton v Shoe Lane Parking Ltd, 2 QB 163 (1971).

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 Contacts: Advice to Government. Law Com No 401.

Verstappen, J. (2023). Legal Agreements on Smart Contract Platforms in European Systems of Private Law. Springer International Publishing. https://doi.org/10.1007/978-3-031-35407-6

Werbach, K., & Cornell, N. (2017). Contracts Ex Machina. Duke Law Journal, 67(2), 313–382.

Wijayasriwardena, D. (2016). Consent in Online Contracts—Mindless or Mindful? (SSRN Scholarly Paper No. 2783793). Social Science Research Network. https://papers.ssrn.com/abstract=2783793

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