ISSLP

Original Research

Challenges in Ascertaining Common Intention in the Interpretation of Contracts Concluded through Algorithmic Systems: The Conflict between Subjective and Objective Will in Light of the Principles of Contract Law

Elaheh. Alfooneh[1*], Shahin. Shahed Mofarred[1], Seyed Mostafa. Hashemi[2]

[1] MA Student, Department of Private Law, Yas.C., Islamic Azad University, Yasuj, Iran
[2] Department of Law, Yas.C., Islamic Azad University, Yasuj, Iran

*** Corresponding author email address**: elaalfone4148@gmail.com

Received: 2026-05-06 **Revised:** 2026-10-18 **Accepted:** 2026-10-25 **Initial Publish:** 2026-10-29 **Final Publish:** 2027-01-01

The increasing use of algorithmic systems in contract formation has challenged traditional assumptions concerning contractual intention, consent, and interpretation. In conventional contracts, the legal analysis of common intention generally proceeds from the relationship between the parties' internal will and their outward manifestations. In algorithmically concluded contracts, however, this relationship becomes more complex because the decisive human act may occur at the stage of designing, configuring, or authorizing the system, while the specific contractual manifestation may later be generated automatically without contemporaneous human awareness. This article examines the challenges involved in ascertaining common intention where the subjective will of a contracting party diverges from the objective manifestation produced by an algorithmic system. Using a descriptive-analytical legal method, the study evaluates the adequacy of subjective and objective theories of contractual interpretation in technologically mediated transactions and analyzes the significance of prior authorization, algorithmic parameters, contractual purpose, technological error, reasonable reliance, good faith, and risk allocation. The analysis demonstrates that neither a purely subjective nor a purely objective approach provides a satisfactory basis for interpreting algorithmic contracts. Excessive emphasis on internal intention can undermine transactional security, while strict adherence to algorithmic outputs may bind parties to results that fall outside the scope of their legally attributable will. The article therefore proposes an integrated interpretive approach in which common intention is treated as a legally attributable construct rather than merely a contemporaneous psychological state. Under this approach, courts should consider the scope of authority granted to the system, the foreseeability of the disputed output, technical records, prior dealings, the counterparty's reasonable reliance, and the visibility of any technological anomaly. Such a framework preserves the foundational principles of contractual autonomy while adapting them to the realities of automated and algorithmically mediated contracting.

Keywords: *Algorithmic Contracts; Common Intention; Contract Interpretation; Subjective Will; Objective Will; Smart Contracts; Autonomy of Will; Algorithmic Decision-Making*

How to cite this article:
Alfooneh, E., Shahed Mofarred, S., & Hashemi, S. M. (2027). Challenges in Ascertaining Common Intention in the Interpretation of Contracts Concluded through Algorithmic Systems: The Conflict between Subjective and Objective Will in Light of the Principles of Contract Law. *Interdisciplinary Studies in Society, Law, and Politics, 6*(1), 1-19. https://doi.org/10.61838/kman.isslp.612

1. Introduction

The transformation of contractual relations through digital technologies has progressively displaced many elements that were traditionally associated with the personal formation, expression, and interpretation of contractual intention. Whereas the classical image of a

© 2027 The authors. Published by KMAN Publication Inc. (KMANPUB). This is an open access article under the terms of the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

contract presupposes two or more legally competent actors who negotiate, exchange declarations, assess the meaning of the terms presented to them, and ultimately manifest assent through identifiable expressions of will, contemporary commercial transactions increasingly take place through software systems capable of selecting contractual counterparts, determining prices, generating contractual conditions, responding to market information, and concluding transactions without contemporaneous human intervention. The legal significance of this transformation is not confined to questions concerning electronic form, evidentiary reliability, or the technical validity of automated transactions. It affects a more fundamental premise of contract law: the assumption that contractual obligations can ultimately be traced to a legally meaningful intention attributable to the parties. Traditional contract doctrine has long treated intention and consent as foundational elements through which private persons voluntarily create binding legal relations, although the precise doctrinal relationship between inward intention, outward expression, consent, and enforceability differs among legal systems (Kaviani, 2025). The principle of autonomy of will historically provides the normative foundation for allowing individuals to determine whether to contract, with whom to contract, and on what terms, subject to mandatory legal limits and considerations of public order (Sacco, 2007). Even where modern legal systems restrict contractual freedom in order to protect weaker parties or regulate specific transactions, the concept of legally attributable will continues to provide a central explanation for why contractual promises generate obligations (Ben Saadia, 2022). Algorithmic contracting complicates this structure because the operative manifestation of contractual choice may emerge from computational processes that were designed or authorized by a person at an earlier stage but that subsequently operate according to variables, optimization mechanisms, or adaptive processes that may not correspond precisely to the person's actual subjective intention at the moment when a specific transaction is concluded.

The problem becomes particularly significant when courts or other adjudicative institutions must interpret a contract concluded through an algorithmic system. Contract interpretation is not limited to determining the semantic meaning of words appearing in a document. Its deeper function is to identify the legally relevant meaning of the parties' agreement by examining the relationship between their expressed terms, their conduct, the circumstances surrounding formation, commercial expectations, applicable usages, and the common intention that can reasonably be attributed to the transaction. Traditional approaches to contract interpretation frequently oscillate between subjective and objective theories. A subjective approach emphasizes the parties' actual internal understanding and seeks, insofar as legally possible, to reconstruct their true common intention rather than confining interpretation to the literal meaning of contractual expressions. An objective approach instead gives greater weight to the meaning that a reasonable person would attribute to the parties' words and conduct, especially where their internal states are inaccessible, divergent, or incapable of proof. General contract doctrine has therefore long confronted the tension between inward will and outward manifestation, and legal systems have developed various techniques for allocating the risk of discrepancies between what a party internally intended and what that party objectively appeared to communicate (Willmott et al., 2005). The emergence of algorithmic systems does not create this tension from nothing, but it intensifies it because the distance between internal human intention and external contractual manifestation may be structurally embedded in the technological mechanism through which the contract is generated.

Smart contracts and related forms of algorithmic contracting illustrate this difficulty particularly clearly. In some transactions, software merely performs ministerial functions that have been fully determined by the parties in advance. In others, algorithms make choices among alternative contractual possibilities based on market variables, programmed preferences, user data, predictive models, or automated optimization. The stronger the decisional autonomy of the system, the more difficult it becomes to treat each individual output as the direct expression of a specific contemporaneous human intention. Legal analysis of smart contracts has therefore increasingly questioned whether traditional doctrines of intention can be transposed without modification into algorithmically generated transactions (Pasban & Sadeghi, 2023). The issue is not necessarily

whether software itself possesses legal intention, because contractual capacity remains attributed to legal persons rather than technological artifacts. The more difficult question is whether, and according to what criteria, the output of an algorithm can be attributed to the person who deployed, configured, authorized, or benefited from it. Scholarship concerning the semantics of smart contracts has emphasized that computational execution may obscure the distinction between what parties legally intend and what software technically performs, particularly where code operationalizes only one aspect of the broader contractual relationship (Hacker, 2021). An algorithm may execute a transaction perfectly according to its code and nevertheless produce a legal result that conflicts with what one or both parties subjectively expected.

Iranian private law, like many civil-law systems influenced by a voluntarist conception of contract, assigns substantial importance to intention and consent. The distinction between intention as the decisive element through which a legal act is created and consent as the free acceptance of that legal act is especially relevant when assessing contracts generated by automated systems (Kaviani, 2025). Electronic contracting has already required jurists to reconsider how intention and consent can be manifested through technological interfaces and automated communications (Paknejad, 2023). Smart-contract scholarship has further demonstrated that a person may intentionally activate a technological mechanism while lacking a specific conscious intention regarding every individual result produced by that mechanism (Shafi'i, 2020). Consequently, the interpretive task becomes increasingly complex when the algorithmic output is disputed. A court may be required to distinguish between the intention to employ an algorithm, the intention embodied in the parameters initially selected by the user, the intention inferable from the broader commercial purpose of the transaction, and the specific contractual manifestation generated by the software. These forms of intention may coincide, but they may also diverge.

The tension is further intensified by the economic function of automation. Parties use algorithmic systems precisely because automation reduces transaction costs, accelerates contracting, processes information at a scale beyond ordinary human capacities, and permits large numbers of transactions to be executed without repeated individual deliberation. Transaction-cost analysis demonstrates that contractual arrangements are deeply influenced by the costs associated with negotiating, monitoring, and enforcing exchanges (Williamson, 1979). Algorithmic contracting can dramatically reduce some of these costs, but the reduction in human participation at the formation stage may produce new interpretive costs when disputes arise. An individual who permits a trading system to enter hundreds of transactions according to predefined parameters may benefit from automation precisely because no human reviews each contract separately. It would therefore be conceptually artificial to insist that the individual possessed a fully formed subjective intention concerning every contractual term of every transaction. At the same time, it would be equally problematic to treat every algorithmic output as conclusively binding merely because it was technically generated by an authorized system. Such an approach could allow programming defects, corrupted data, unforeseen interactions, or machine-generated anomalies to determine legal obligations in circumstances where the result is fundamentally disconnected from the purpose for which the system was deployed.

The interpretive importance of this problem extends beyond smart contracts executed on distributed ledgers. Algorithmic contracting may occur through automated purchasing systems, dynamic-pricing software, high-frequency trading programs, digital marketplaces, insurance platforms, logistics systems, online advertising exchanges, automated procurement tools, and artificial-intelligence systems capable of generating or modifying contractual terms. The common characteristic is not any particular technological architecture but the existence of a computational intermediary between human decision-making and contractual manifestation. Prior analyses of intention in smart contracts have already identified the need to distinguish between the parties' juridical intention and the automatic technical implementation of contractual conditions (Shavand & Nasr, 2019). Similar concerns arise where the system does not merely execute predetermined terms but independently selects among available alternatives. The greater the algorithm's role in determining the content or occurrence of the

transaction, the greater the challenge of determining whether the objectively manifested agreement corresponds to the subjective will of the person to whom the system's conduct is attributed.

The principle of good faith also acquires particular significance in this context. Good faith functions in many legal systems as a mechanism for constraining opportunistic reliance on literal contractual language where such reliance would contradict the parties' legitimate expectations or the cooperative structure of their relationship (Tetley, 2004). In algorithmic contracting, however, good faith cannot simply resolve every discrepancy between subjective and objective intention. A counterparty that receives an apparently valid automated offer may have no knowledge of the other party's internal programming assumptions, system limitations, or undisclosed preferences. Protecting the internal intention of the algorithm user in every case could therefore undermine transactional security and reasonable reliance. Conversely, strict adherence to outward algorithmic manifestation could generate unjust outcomes where the counterparty knew or should have known that the system's output was anomalous or inconsistent with the surrounding circumstances. The interpretive challenge thus involves a balance between autonomy, reliance, good faith, commercial certainty, and the allocation of technological risk.

Against this background, the central objective of this article is to examine how common contractual intention should be ascertained when a contract has been concluded through an algorithmic system and the internal will of one or both parties diverges from the objective manifestation generated by that system. The analysis focuses on the tension between subjective and objective theories of contractual interpretation and asks whether traditional interpretive principles remain adequate when the contractual declaration is mediated, generated, or transformed by computational processes. Particular attention is devoted to the legal attribution of algorithmic outputs, the evidentiary reconstruction of intention, the significance of programming parameters and transaction records, the role of reasonable reliance, the treatment of algorithmic mistake, and the allocation of interpretive risk. The argument developed throughout the article is that algorithmic contracting does not justify abandoning the concept of common intention, but it requires a more differentiated understanding of where legally relevant intention is located. In this environment, intention cannot always be identified with the psychological state of a human actor at the exact moment of contractual conclusion. It must instead be reconstructed through an integrated analysis of prior authorization, technological configuration, contractual purpose, objective manifestations, counterparty reliance, and the foreseeability of the algorithmic outcome.

2. Theoretical and Legal Foundations of Common Intention in Contract Interpretation

Contractual interpretation occupies a distinctive position in private law because it mediates between autonomy and legal objectivity. On the one hand, contractual obligation is traditionally justified through the proposition that parties should be bound because they have voluntarily chosen to create a legal relationship. On the other hand, law cannot ordinarily inspect internal mental states directly and must therefore rely on external manifestations from which intention can be inferred. The interpretive process consequently transforms subjective will into a legally cognizable form. The principle of contractual freedom presupposes that the parties possess meaningful authority to structure their legal relations, yet this authority is neither unlimited nor purely psychological (Sacco, 2007). A party cannot generally escape an obligation merely by asserting that its undisclosed internal intention differed from the meaning reasonably conveyed by its conduct. The law therefore distinguishes between the internal formation of intention and its external legal manifestation, while attempting to preserve an appropriate relationship between the two.

The subjective theory of interpretation begins from the idea that contractual language is instrumental rather than ultimate. Words, signatures, electronic messages, and conduct are mechanisms through which parties communicate an agreement; they are not the agreement itself. Where the parties demonstrably shared a particular understanding, that common understanding may deserve priority over the ordinary or literal meaning of the language they used. This approach reflects the normative significance of autonomy because it seeks to enforce the agreement that the parties actually intended rather than an agreement artificially

constructed through detached linguistic analysis. The distinction between intention and consent is especially important in legal systems that conceptualize the juridical act as dependent upon a serious intention to create legal effects (Kaviani, 2025). The subjective approach accordingly regards interpretation as an inquiry into the parties' common juridical purpose, reconstructed through their declarations, negotiations, conduct, relationship, and surrounding circumstances.

Nevertheless, subjective interpretation faces significant evidentiary and institutional limitations. Mental states are private, recollections may be unreliable, and parties frequently develop self-serving accounts of their original intentions after disputes arise. Commercial transactions also involve situations in which the parties never formed a detailed shared understanding of every term. Standard-form agreements, complex financial transactions, and electronically generated contracts may contain provisions that no human participant has individually considered. For these reasons, objective interpretation protects both evidentiary reliability and transactional security. Contract law commonly gives legal effect to the reasonable meaning of manifestations because counterparties must be entitled to rely on what is communicated rather than on undisclosed reservations. General contract doctrine therefore places substantial weight on words, conduct, context, and reasonable expectations when identifying legally binding intention (Willmott et al., 2005). The objective approach is particularly important when the parties' subjective understandings differ or when no actual common intention can be established.

The conflict between internal and external will is therefore not simply a theoretical controversy between two abstract schools. It reflects competing values within contract law. Subjective interpretation promotes autonomy by respecting actual intention; objective interpretation promotes security by protecting reliance and predictability. The law must determine which party should bear the consequences when these values diverge. Restrictions on contractual freedom already demonstrate that private will is not treated as an absolute source of legal obligation (Safaei & Shomali, 2017). Mandatory rules, good faith requirements, consumer protection, public policy, and doctrines concerning unfair terms limit the extent to which expressed agreement can be treated as dispositive. At the same time, the existence of such restrictions presupposes a meaningful domain in which private will remains legally operative. The difficulty is therefore to determine when an outward manifestation should be treated as sufficiently attributable to a party even though it does not correspond perfectly to that party's subjective intention.

Classical doctrine often resolves this problem through concepts such as mistake, misrepresentation, lack of consent, interpretation against the drafter, or protection of reasonable reliance. The exact doctrinal mechanism varies across legal systems, but the underlying structure is similar: the law assesses the seriousness of the discrepancy between internal intention and outward appearance, the behavior of the other party, and the extent to which the error should affect contractual validity or meaning. Freedom of will is itself subject to legal limitations where unregulated autonomy would produce inequitable or socially unacceptable results (Ben Saadia, 2022). Algorithmic contracting should therefore be situated within this broader doctrinal tradition rather than treated as an entirely separate legal universe. The novelty lies in the technological source and scale of the discrepancy, not in the basic existence of conflict between intention and manifestation.

Common intention is particularly difficult to identify where an algorithm intervenes because several potentially relevant levels of will may exist. The first is the party's general intention to participate in a category of transactions. A business may decide to purchase a certain commodity whenever market prices fall below a specified threshold. The second is the intention embodied in the software configuration. The user may select variables, thresholds, risk tolerances, or optimization objectives that determine when the system will transact. The third is the specific output generated by the algorithm in a particular case. The fourth is the legal meaning that an external observer would attribute to that output. These levels need not correspond. A person may have a general intention to buy only commercially usable goods but may configure an automated system that accidentally accepts a category of defective goods because of an incorrect parameter. The algorithmic output may objectively indicate an unconditional purchase even though the transaction conflicts with the user's broader commercial purpose.

This layered structure complicates the traditional idea that a declaration is simply an external expression of an internal intention. Electronic-contract scholarship has already recognized that intention and consent may be expressed through automated communications even where the person does not directly generate each message (Paknejad, 2023). Smart-contract analysis similarly demonstrates that the act of designing or activating a system can function as a prior manifestation of willingness to be bound by transactions produced according to specified conditions (Abdollahi, 2022). However, prior authorization cannot automatically answer every interpretive question because the scope of that authorization may itself be disputed. A party may authorize a system to transact within defined parameters without intending to assume the risk of every technically possible output. The interpretive task must therefore identify whether the contested transaction falls within the legally relevant scope of the authority conferred upon the system.

The distinction between contractual intention and technical execution is essential. Code translates certain conditions into computational instructions, but legal agreements often contain standards, qualifications, implied obligations, and contextual assumptions that cannot be fully represented through deterministic commands. Hacker argues that the semantics of smart contracts cannot be reduced to computational performance because legal intention and machine-readable execution operate at different normative levels (Hacker, 2021). A program may determine that a payment must be released when a data input satisfies a numerical condition, whereas the legal contract may presuppose that the underlying data is genuine, that performance has not been frustrated, or that the transaction has not been affected by fraud. The fact that software automatically executes a consequence does not necessarily establish that the parties legally intended that consequence under every circumstance in which the code produces it.

This distinction also affects the interpretation of imposed or non-negotiated terms. Digital systems frequently present parties with conditions that they do not negotiate individually and may not even read. The relationship between actual consent and formally manifested assent has therefore become increasingly significant in modern contracting (Karimi & Karimi, 2024). In algorithmic systems, the problem is amplified because terms may not merely be imposed by one contracting party but may be selected, ranked, modified, or generated by automated processes. If a system chooses among different contractual forms according to user data, the legal significance of that choice depends on whether the user can fairly be treated as having accepted the resulting terms. A purely subjective theory might conclude that no binding intention exists where the user lacked actual awareness of the specific term. A purely objective theory might treat activation of the system as sufficient assent to all generated conditions. Neither extreme provides a satisfactory solution for technologically mediated transactions.

Good faith offers one mechanism for moderating this conflict. Its relevance lies not only in preventing deliberate opportunism but also in defining the interpretive responsibilities of parties confronted with ambiguous or anomalous algorithmic outputs. Contractual good faith has traditionally operated as a standard requiring parties to exercise rights and interpret obligations in a manner consistent with the legitimate expectations generated by the contractual relationship (Tetley, 2004). If an algorithm produces a result so unusual that a reasonable counterparty would recognize the probability of error, strict reliance on the literal output may be inconsistent with good faith. Conversely, where the output falls squarely within the normal range of transactions and the counterparty has no reason to suspect an internal malfunction, good faith may support protection of objective reliance.

Economic considerations reinforce the need for a balanced approach. Contracting mechanisms exist partly to reduce the uncertainty and costs associated with exchange. Williamson's transaction-cost framework emphasizes that institutional arrangements must be evaluated according to the costs of organizing, monitoring, and enforcing transactions (Williamson, 1979). If every automated contract could be challenged whenever a user later asserted a different internal intention, the efficiency gains of algorithmic contracting would be substantially undermined. Counterparties would be required to investigate software architecture or internal business preferences before relying on apparently valid transactions. Yet the opposite rule, under which every output is irrevocably binding regardless of obvious malfunction or gross deviation

from authorized parameters, would impose excessive technological risk on system users and could discourage beneficial automation.

The theoretical foundation for interpreting algorithmic contracts should therefore remain anchored in the concept of legally attributable intention rather than psychological intention alone. What matters is not whether a human consciously contemplated the exact transaction at the instant it was formed, but whether the transaction can reasonably be connected to a chain of authorization and manifestation attributable to that person. Such attribution should include the initial decision to employ the system, the parameters selected, the foreseeable range of outputs, the surrounding contractual purpose, and the expectations reasonably created for the counterparty. This approach preserves the normative role of autonomy without requiring fictional claims about contemporaneous human cognition. It also preserves objective security by recognizing that outward manifestations remain essential evidence of intention.

Within this framework, common intention becomes a composite legal construct. It may sometimes correspond closely to an actual shared psychological understanding, particularly where the parties negotiated the system's operation in detail. In other situations, it may be reconstructed primarily through objective evidence concerning the architecture of the transaction, the system's authorized functions, established practices, and reasonable expectations. The law of smart contracts has already demonstrated that the search for intention must adapt to technological mediation rather than assuming that conventional doctrines can be applied mechanically (Rashvand & Naser, 2019). The central task is therefore not to choose permanently between subjective and objective theories, but to determine how the evidentiary and normative weight of each should vary according to the technological structure of the transaction.

3. Formation of Contractual Intention through Algorithmic Systems

The formation of contractual intention through algorithmic systems differs from conventional contracting primarily because decision-making is temporally and functionally separated from the moment at which the contractual manifestation occurs. In a traditional transaction, the act of expressing consent usually follows closely upon human deliberation. A person evaluates the proposed terms and then communicates assent through speech, writing, signature, conduct, or another legally recognized form. In algorithmic contracting, by contrast, the decisive human act may occur much earlier, when the system is designed, configured, activated, or authorized to operate. The subsequent contractual manifestation may then be produced automatically when particular conditions are satisfied. This temporal separation does not necessarily negate intention. Electronic-contract doctrine has long accepted that legal declarations may be generated through automated systems where the underlying use of the system is attributable to the person on whose behalf it operates (Paknejad, 2023). The difficulty lies in defining the extent to which initial authorization should control the legal interpretation of later outputs.

The simplest form of algorithmic contracting involves deterministic automation. A program may be instructed to accept every order meeting a fixed set of conditions, issue standardized contracts upon receipt of payment, or execute a transfer when a predetermined event occurs. In these cases, the algorithm resembles a sophisticated mechanical instrument. The human user has established the conditions in advance, and the software merely implements them. Attribution is relatively straightforward because the system's output is closely connected to the user's predetermined instructions. The use of automated mechanisms in smart contracts has therefore been defended as consistent with the principle of autonomy of will where the parties intentionally choose the technological mechanism through which their agreement will be formed or performed (Abdollahi, 2022). Nevertheless, even deterministic systems can generate interpretive disputes where the code fails to capture the parties' broader legal assumptions.

More complex systems introduce probabilistic, adaptive, or predictive decision-making. An algorithm may analyze market conditions, customer characteristics, risk profiles, previous transactions, or dynamically changing data before selecting the contractual response it considers optimal. In such cases, the user does not necessarily predetermine the exact content of every transaction. Instead, the user authorizes a method of decision-making. This resembles delegation, but the analogy is incomplete because the algorithm lacks legal personality and independent juridical intention. The acts

remain attributable, if at all, to the legal person who deploys the system. The central question becomes whether authorizing a decision-making process should be treated as equivalent to authorizing every reasonably foreseeable output produced by that process.

The distinction between intended method and intended result is therefore crucial. A trader may intentionally employ an algorithm that purchases securities when a set of indicators reaches specified values. The trader may not intend any particular purchase in advance, but the trader does intend that the system determine when purchases should occur according to the chosen methodology. This form of intention is structurally different from transaction-specific intention, yet it may be sufficient to justify contractual attribution. Scholarship on the intention of parties in smart contracts has recognized that contractual will may be expressed through the prior configuration and deployment of automated tools rather than through a separate psychological act accompanying each transaction (Shavand & Nasr, 2019). The legal significance of prior programming thus lies in its capacity to function as a standing manifestation of willingness to transact under defined conditions.

However, prior authorization cannot reasonably encompass unlimited outcomes. Every technological system operates within a field of expected and unexpected behavior. Software may produce anomalous outputs because of programming errors, corrupted data, adversarial manipulation, unanticipated market conditions, or interactions between multiple automated systems. The issue is therefore not merely whether the user activated the software but whether the disputed output falls within the risk that can fairly be attributed to that activation. Smart-contract interpretation has already highlighted the inadequacy of treating technical execution as conclusive proof of legal intention (Karimi, 2023). A computational result may be perfectly consistent with source code yet inconsistent with the purpose that the code was intended to serve.

The formation of contractual intention must therefore be analyzed through multiple layers of authorization. The first layer is institutional or organizational authorization: who decided that the system could be used for contractual purposes? The second concerns functional authority: what categories of transactions was the system authorized to conclude? The third concerns parameter authority: what limits were imposed concerning price, quantity, counterparty, timing, jurisdiction, or other legally relevant variables? The fourth concerns adaptation: was the system permitted to modify its decision rules on the basis of new data? The fifth concerns exceptional circumstances: were there safeguards designed to prevent transactions outside a normal commercial range? These layers help identify whether a disputed output represents an authorized manifestation of contractual will or a technological deviation from the user's legally relevant intention.

This analysis resembles familiar questions in agency law but cannot be reduced entirely to agency principles. An agent is a legal actor capable of receiving instructions, exercising judgment, and sometimes possessing knowledge that may be attributed to the principal. An algorithm lacks consciousness and legal personality. Its significance lies in the causal role it plays in producing legally operative manifestations. The legal system must therefore construct attribution through the conduct of the human or corporate actor responsible for deploying the system. The principle of autonomy supports this approach because a person who intentionally selects a technological mechanism should normally bear the legal consequences of outputs produced within the ordinary scope of that mechanism. At the same time, autonomy would be distorted if authorization of a system were treated as an irrevocable waiver of all protections against serious malfunction.

The difference between intention and consent also becomes particularly significant. A user may intend to employ a platform but may not freely consent to every term generated or imposed through it. Contemporary private-law scholarship has emphasized that intention and consent are related but not identical components of voluntary contractual commitment (Kaviani, 2025). This distinction matters where systems automatically incorporate standard conditions, modify prices, or present terms generated by artificial-intelligence models. If users are legally deemed to consent merely because they use the system, the objective manifestation may become detached from meaningful voluntariness. Legal analysis of imposed contractual terms likewise demonstrates that formal acceptance does not always resolve whether contractual consent is normatively sufficient (Karimi & Karimi, 2024).

The problem becomes even more difficult when both sides employ algorithms. In such transactions, no natural person may directly observe the moment of contract formation. One system may generate an offer, another may automatically evaluate and accept it, and the resulting agreement may be recorded and executed without direct human review. The common intention of the parties must then be reconstructed from the authorization structures surrounding both systems. The relevant evidence may include configuration settings, system logs, prior dealing, contractual protocols, platform rules, technical documentation, transaction thresholds, and the commercial purposes for which each algorithm was deployed. The traditional idea of a meeting of minds must therefore be reformulated as a legally attributable convergence of authorized manifestations.

The semantics of code complicates this reconstruction. Software instructions are precise in a computational sense, but computational precision does not necessarily correspond to legal completeness. Hacker's analysis of smart contracts emphasizes that contractual meaning cannot be identified exclusively with code because legal obligations often depend on standards and contextual considerations that cannot be fully captured by formal logic (Hacker, 2021). For example, a program may automatically release payment when a sensor records delivery, but the legal agreement may presuppose that the delivered goods conform to quality requirements. If the sensor confirms arrival while the goods are defective, the code's execution does not establish that the buyer intended to waive contractual remedies.

Algorithmic contracting also raises questions concerning contractual error. Classical mistake doctrine generally distinguishes between errors that are legally significant and those that remain at the risk of the mistaken party. In an algorithmic environment, the error may occur not in the party's conscious reasoning but in data entry, coding, model design, parameter selection, or system interaction. Smart-contract scholarship has identified ascertainment of intention as a major difficulty precisely because software-generated transactions may reflect technical error rather than genuine contractual preference (Shafi'i, 2020). The appropriate legal response depends on whether the error should be characterized as an internal mistake of the user, an objectively apparent anomaly, a defect in the technological intermediary, or a failure shared by both parties.

The allocation of technological risk must therefore play an important role. A party that chooses to rely on a sophisticated algorithm obtains efficiency benefits and should ordinarily bear some responsibility for maintaining and configuring that system. This resembles broader principles of contractual risk allocation, under which parties who control particular sources of risk may appropriately bear their consequences. Transaction-cost reasoning supports allocating responsibility in ways that encourage efficient prevention and monitoring (Williamson, 1979). If the algorithm user is best positioned to prevent configuration errors, imposing some risk on that user may create appropriate incentives. Yet a counterparty that knowingly exploits an obvious malfunction should not be able to invoke objective manifestation without qualification.

Good faith thus functions as an important boundary on technological attribution. If a party receives an algorithmic offer at a price so radically inconsistent with market conditions that error is obvious, enforcing the transaction solely on the basis of outward manifestation may conflict with reasonable commercial standards. Good faith principles traditionally limit opportunistic behavior and protect legitimate expectations in contractual relations (Tetley, 2004). The same logic can be adapted to algorithmic transactions. The objective appearance of agreement should carry substantial weight where reliance is reasonable, but its weight should diminish where the counterparty knew or should reasonably have known that the system's output did not correspond to genuine contractual authorization.

The formation of algorithmic contractual intention should therefore be understood through a doctrine of technologically mediated attribution. Such a doctrine would not treat software as an independent bearer of will. Instead, it would identify the circumstances under which computational outputs may legally count as manifestations of the user's intention. The most important factors include the scope of authorization, the predictability of the output, the user's control over system design, the existence of safeguards, the commercial context, prior transactions, the counterparty's knowledge, and the degree to which the output is consistent with the purpose for which the system was deployed. This framework allows legal

doctrine to preserve both the voluntarist foundation of contract and the practical realities of automated commerce.

4. Challenges in Ascertaining Common Intention in Algorithmically Concluded Contracts

The central interpretive difficulty in algorithmically concluded contracts arises from the possibility that the contractual manifestation generated by the system does not correspond to the internal intention of one or both parties. In conventional disputes, courts may examine negotiations, correspondence, conduct, prior dealings, and witness testimony to determine what the parties understood. In algorithmic contracting, these forms of evidence may remain relevant, but they are supplemented by technical evidence whose meaning may itself be contested. The interpretive inquiry may require examination of source code, system logs, user settings, data inputs, model parameters, decision rules, audit records, platform protocols, and the sequence of automated interactions preceding formation. The task is therefore not simply to discover a hidden psychological intention but to reconstruct a legally meaningful relationship between human authorization and machine-generated manifestation.

One major challenge is the absence of contemporaneous human awareness. A person may authorize a system to conduct transactions continuously without reviewing each output. If subjective intention is defined narrowly as a conscious mental state concerning a specific transaction, many algorithmic contracts would appear to lack intention altogether. Such a conclusion would be inconsistent with the practical reality of automated commerce and with existing legal acceptance of electronic transactions. The more defensible position is that the relevant intention may be formed at an earlier stage, when the user establishes the algorithm's authority. Studies of intention in smart contracts have accordingly emphasized the importance of prior authorization and technological configuration in identifying contractual will (Pasban & Sadeghi, 2023). The difficulty remains determining how far that prior intention extends.

A second challenge concerns the evidentiary status of algorithmic parameters. If a user configures a system to purchase goods within a specified price range, those parameters appear highly relevant to interpreting the user's intention. Yet parameters do not necessarily capture the full legal purpose of the transaction. They may be incomplete, incorrectly entered, technically transformed, or dynamically adjusted by the system. Furthermore, machine-learning systems may produce outputs through complex statistical relationships that cannot be translated into simple rules. The legal interpreter must therefore avoid treating code as a perfect representation of intention. Hacker's distinction between contractual semantics and computational implementation is particularly important here because technical execution may represent only a partial operationalization of the legal relationship (Hacker, 2021).

Opacity creates an additional problem. Some algorithmic systems are difficult to explain even for their developers, particularly where decisions emerge from complex models involving large numbers of variables. If neither party can fully explain why the system generated a particular contractual output, subjective reconstruction becomes highly uncertain. The interpretive process may then shift toward objective indicators such as the appearance of the transaction, established patterns of dealing, and the expectations reasonably generated for the counterparty. This shift does not necessarily abandon autonomy. Rather, it recognizes that where internal intention cannot be demonstrated with sufficient reliability, external manifestations must acquire greater legal weight. General contract doctrine similarly relies on objective interpretation where subjective states cannot be established with adequate certainty (Willmott et al., 2005).

The protection of reasonable reliance is especially important in this context. A counterparty interacting with an apparently authorized algorithm may have no practical means of determining whether its output perfectly corresponds to the system user's internal preferences. Requiring such investigation would undermine the efficiency of automated contracting. The law therefore has strong reasons to protect reliance where the output falls within the ordinary and foreseeable range of the system's operation. This approach is consistent with the broader principle that undisclosed internal reservations should not ordinarily defeat objectively manifested agreement. At the same time, reliance cannot be treated as reasonable where the circumstances strongly indicate error.

Algorithmic mistake illustrates this boundary. Suppose an automated pricing system mistakenly offers a product at one percent of its normal price because of a coding defect. If the counterparty immediately purchases an unusually large quantity after recognizing the probable error, the objective manifestation should not necessarily prevail. Good faith can provide a normative basis for refusing to protect opportunistic exploitation of obvious anomalies (Tetley, 2004). By contrast, if the price variation is commercially plausible and the counterparty has no reason to suspect malfunction, the system user's undisclosed internal intention may deserve less protection. The interpretive outcome should thus depend partly on the visibility and materiality of the discrepancy.

The doctrine of mistake in algorithmic transactions should distinguish among different sources of error. A data-entry mistake occurs where a human provides incorrect input. A programming mistake occurs where the software contains defective instructions. A model error occurs where the system makes an unexpected prediction or classification despite functioning technically as designed. A communication error occurs where the system transmits or receives information incorrectly. A strategic error occurs where the algorithm produces a commercially disadvantageous result because the user's chosen strategy was poor rather than because the system malfunctioned. These categories should not necessarily produce the same legal consequences. A party should ordinarily bear the consequences of a poor strategy because autonomy includes responsibility for choices. A catastrophic coding error that generates objectively absurd transactions presents a different case.

The distinction between intention and consent is again useful. A party may have intended to authorize a system but may not have consented in any meaningful sense to a transaction produced outside the contemplated range. Iranian legal analysis has treated intention and consent as fundamental but analytically distinct conditions of contractual will (Kaviani, 2025). In electronic contexts, scholars have similarly examined how these elements operate where contractual communication is automated (Paknejad, 2023). The challenge is to avoid collapsing all questions into binary validity. Many disputes do not require deciding whether a contract exists at all; they concern the interpretation of ambiguous terms, scope of obligations, or allocation of loss. In such cases, the discrepancy between internal and external will may influence interpretation without necessarily invalidating the transaction.

Another challenge concerns standardization. Algorithmic contracts frequently operate through predefined platforms with standardized terms. The user's freedom may be limited to selecting among available options or defining certain parameters. Restrictions on freedom of will are not unique to digital contracting; modern contract law has long recognized that bargaining power and mandatory rules constrain formal autonomy (Safaei & Shomali, 2017). In algorithmic systems, however, standardization may obscure whose intention is actually expressed. Platform designers may determine the legal architecture, users may select operational preferences, and algorithms may choose transaction-specific terms. The resulting contract may therefore reflect multiple layers of normative authorship.

The interpretation of imposed or automatically generated terms requires special caution. Research on contractual terms imposed upon parties emphasizes that formal acceptance does not always correspond to genuine substantive consent (Karimi & Karimi, 2024). Where an algorithm inserts a clause based on a user profile or automated risk assessment, the legal system should examine whether the clause was within the scope of what the party reasonably authorized. Objective manifestation remains relevant, particularly where the party had notice of the system's operation, but attribution should not become purely mechanical.

The role of contractual purpose also becomes more important as direct evidence of subjective intention decreases. Courts frequently interpret ambiguous terms in light of the economic and juridical purpose of the agreement. In algorithmic contracts, purpose can serve as a bridge between initial authorization and specific output. If a company deploys an automated procurement system solely to acquire materials needed for a defined production process, an anomalous transaction involving unrelated goods may be difficult to reconcile with the system's authorized purpose. Conversely, where the system is expressly designed to explore a broad range of opportunities, unusual outputs may still fall within the contemplated risk.

Prior course of dealing can similarly assist interpretation. If an algorithm has repeatedly concluded transactions within a consistent pattern and suddenly generates a radically different result, the departure may provide evidence that the output is anomalous. Conversely, a history of varied transactions may indicate that broad discretion was intentionally granted. Smart-contract scholarship has recognized that intention must often be reconstructed from the broader transactional environment rather than from the code alone (Rashvand & Naser, 2019). This approach is particularly persuasive because it treats algorithmic conduct as part of an ongoing relationship rather than as an isolated technical event.

The allocation of evidentiary burdens is also significant. A party seeking to avoid the apparent meaning of an algorithmic transaction on the basis of internal intention should ordinarily be required to provide persuasive evidence of the discrepancy. Otherwise, automated commerce would become vulnerable to opportunistic repudiation. Technical records may provide more reliable evidence than retrospective testimony. System logs can show parameter changes, authorization histories, error messages, or deviations from normal operation. However, the opposing party should also be permitted to demonstrate reasonable reliance and the absence of circumstances suggesting error.

The increasing complexity of algorithmic decision-making may require courts to rely on expert evidence. Yet expert testimony should not displace the legal character of the interpretive inquiry. Experts can explain how the system functioned, what data it processed, and whether an output was technically foreseeable, but the court must determine the legal significance of those facts. The question whether a transaction falls within legally attributable intention is normative, not merely technical. It requires balancing autonomy, security, reliance, good faith, and risk allocation.

Contractual freedom provides no simple answer because it supports arguments on both sides. A system user may invoke autonomy to argue that no obligation should arise beyond what was actually intended. A counterparty may invoke the same principle to argue that the user freely chose to transact through an automated mechanism and should therefore bear the consequences. Sacco's analysis of contractual freedom underscores that contractual will functions within a legal structure that determines when private choices deserve recognition (Sacco, 2007). Algorithmic contracting therefore requires the legal system to define the boundary between chosen technological delegation and unintended technological deviation.

Economic efficiency also supports a differentiated rule. Transaction-cost theory suggests that liability should, where possible, be allocated in a manner that reduces the overall costs of preventing, detecting, and resolving contractual errors (Williamson, 1979). A system operator may be best positioned to prevent programming defects, while a counterparty may be best positioned to avoid exploiting an obvious anomaly. The law should therefore encourage both technological diligence and commercially reasonable behavior. A rigid subjective rule would impose excessive verification costs on counterparties, while a rigid objective rule could create excessive exposure for system users.

The relationship between algorithmic interpretation and contractual liability must also be distinguished from questions of misconduct. A system may generate a disputed transaction without any intentional wrongdoing. Conversely, intentional or grossly negligent conduct may affect whether a party should be permitted to rely on contractual limitations or other protective doctrines. Contemporary legal scholarship concerning intentional and gross fault in contractual contexts illustrates the broader principle that the seriousness of conduct can influence the legal effect of contractual risk allocation (Shabahang et al., 2026). In algorithmic contracting, a party that knowingly deploys an unreliable system without safeguards may have a weaker claim to relief from adverse outputs than a party confronted with an unforeseeable technical anomaly.

A coherent interpretive framework should therefore reject both technological formalism and unrestricted subjectivism. Technological formalism would treat every output as definitive because it was generated by authorized code. Unrestricted subjectivism would allow parties to defeat objectively reasonable expectations through assertions of undisclosed intent. A more balanced approach should begin by identifying the scope of the system's authorization, then examine whether the disputed output was foreseeable within that scope, whether the counterparty reasonably relied on the manifestation, whether any discrepancy was apparent, whether the system's records support an alternative

interpretation, and whether enforcement would be consistent with good faith. The weight assigned to subjective and objective evidence should vary accordingly.

Where both parties actually shared a common understanding that differs from the literal algorithmic output, that shared understanding should generally prevail because the interpretive objective remains the enforcement of their real agreement. Where their internal understandings diverge, the law should give greater weight to objectively attributable manifestations. Where one party's system produces an abnormal result and the other party knew or should have known of the discrepancy, objective reliance deserves reduced protection. Where neither party could reasonably detect the problem and the output falls within the authorized risk of automation, the system user should ordinarily bear the consequences of having selected the technological mechanism.

The interpretive challenge is therefore ultimately one of attribution under conditions of technological mediation. The decisive question is not whether the algorithm possessed intention but whether the contractual manifestation can reasonably and normatively be attributed to the parties. This inquiry preserves the classical concern with common intention while adapting it to a context in which intention may be temporally displaced, technically encoded, partially delegated, and evidentially fragmented. The conflict between subjective and objective will remains central, but its resolution depends increasingly on technological context.

5. Toward an Integrated Framework for Interpreting Algorithmic Contracts

An adequate legal framework for interpreting contracts concluded through algorithmic systems must begin by recognizing that traditional interpretive doctrines remain relevant but require functional adaptation. The fundamental principles of contract law have developed precisely because parties' intentions are not always perfectly expressed. Ambiguous language, errors, incomplete agreements, standard terms, changes in circumstances, and divergent understandings have always required legal interpretation. Algorithmic systems introduce new factual mechanisms through which these familiar problems arise. The principal doctrinal mistake would therefore be to assume either that existing principles are wholly obsolete or that they can be applied without modification. The more appropriate approach is to preserve their normative foundations while adjusting the evidentiary and attributive criteria through which they operate.

The first principle should be that algorithmic output is presumptively attributable to the person who authorized the system when the output falls within the ordinary and reasonably foreseeable scope of that authorization. Such a presumption is necessary for transactional security. A party that intentionally deploys software to negotiate or conclude contracts creates an objective appearance that the system is authorized to perform those functions. The law of electronic contracting already supports the attribution of automated communications to the person on whose behalf the relevant system operates (Paknejad, 2023). Without such a principle, counterparties would be unable to rely on automated transactions and the commercial utility of algorithmic systems would be substantially reduced.

The presumption should not be irrebuttable. A system user should be permitted to demonstrate that a particular output resulted from a serious technological anomaly outside the scope of authorized risk. The strength of this claim should depend on the nature of the deviation, the foreseeability of the event, the user's diligence, and the counterparty's knowledge. Smart-contract scholarship concerning ascertainment of intention supports a contextual rather than purely formal approach to such disputes (Shafi'i, 2020). The inquiry should therefore distinguish between an unfavorable but authorized decision and an output that fundamentally exceeds the contemplated operation of the system.

The second principle should be that the scope of authorization must be reconstructed from both subjective and objective evidence. Internal instructions and configuration settings may reveal what the user intended the system to do, but these should not automatically override the manifestations presented to the counterparty. Conversely, outward appearance should not be treated as conclusive where technical records clearly demonstrate an obvious malfunction. The traditional tension between subjective and objective interpretation thus becomes a structured balancing

exercise rather than an exclusive choice between theories.

The third principle should concern the hierarchy of evidence. Direct evidence of a genuinely shared common intention should receive the greatest weight. If both parties understood that the algorithm was authorized to transact only within a certain range, a technical output outside that range should not ordinarily redefine their agreement. Where no shared subjective understanding can be established, objective evidence becomes more important. General principles of contract interpretation support reliance on reasonable meaning where actual common intention cannot be demonstrated (Willmott et al., 2005). In algorithmic transactions, objective evidence includes not only contractual language but also platform interfaces, technical documentation, transaction histories, user notifications, established practices, and system behavior.

The fourth principle should be technological transparency proportional to contractual risk. The law need not require parties to disclose source code in every transaction. Such a requirement would be commercially unrealistic and could undermine intellectual-property interests. However, where a party relies on a complex algorithm to generate contractual obligations, that party should maintain sufficient records to permit meaningful reconstruction of disputed transactions. The absence of audit trails should not automatically invalidate contracts, but it may affect evidentiary burdens. A party that controls the relevant system and fails to preserve basic records may reasonably bear the consequences of uncertainty concerning its operation.

The fifth principle should address automated errors through a differentiated doctrine of mistake. Not every unexpected algorithmic outcome should be legally characterized as mistake. Algorithms are often designed to make decisions that users themselves would not have predicted. The relevant distinction is between an output produced through the authorized operation of the system and an output caused by a defect or deviation that undermines attribution. The voluntarist foundations of contract require attention to whether the result can still reasonably be treated as an expression of the party's legally relevant intention (Kaviani, 2025). A commercially disadvantageous result is not necessarily a mistake; otherwise, automated decision-making would permit strategic repudiation whenever market conditions change.

The sixth principle should be protection of reasonable reliance. Where a counterparty receives a transaction that appears normal, conforms to established practices, and provides no indication of error, objective manifestation should carry substantial weight. This protects confidence in automated commerce. Yet the reliance principle must be moderated by good faith. A party that recognizes or deliberately exploits an apparent system malfunction should not receive the same protection as an innocent counterparty. Good faith provides a principled basis for distinguishing legitimate reliance from opportunistic behavior (Tetley, 2004).

The seventh principle should concern allocation of technological risk. Parties who choose algorithmic contracting should be presumed to accept ordinary risks inherent in the technology they employ. This does not mean assuming every conceivable risk. Rather, responsibility should correspond to control, foreseeability, and capacity for prevention. Transaction-cost theory supports assigning risks to the party best positioned to reduce or insure against them where such allocation lowers overall social costs (Williamson, 1979). A platform operator may therefore bear responsibility for defects in infrastructure, while a user may bear responsibility for erroneous parameters within its control.

The eighth principle should recognize contractual purpose as an interpretive anchor. Algorithmic outputs should not be examined in isolation from the transaction's commercial and juridical objective. Where the technical result is ambiguous, interpretation should favor a meaning consistent with the purpose reasonably attributable to the parties. This principle is especially valuable when code and legal language diverge. The semantics of smart contracts demonstrate that software execution cannot by itself capture the full normative content of contractual intention (Hacker, 2021). Contractual purpose thus helps integrate technical behavior into the broader legal relationship.

The ninth principle should address the role of standardized and imposed terms. Automated systems frequently operate within ecosystems where users accept platform conditions drafted by another party. Restrictions on autonomy and concerns about unfair terms therefore remain relevant (Safaei & Shomali,

2017). Where an algorithmic platform unilaterally determines the interpretive effect of technical outputs, courts should examine whether those provisions unfairly shift technological risks to parties who lack meaningful control. Formal assent should not automatically resolve this question.

The tenth principle should distinguish between interpretive disputes and validity disputes. A disagreement about the meaning of an algorithmic transaction does not necessarily imply that no contract exists. Courts should first determine whether the contested issue can be resolved through interpretation before resorting to doctrines of nullity, avoidance, or unenforceability. This distinction promotes stability and allows legal doctrine to respond proportionately. Smart-contract analysis has sometimes focused heavily on formation and validity, but many real disputes are better understood as questions concerning the scope of obligations (Karimi, 2023).

The eleventh principle should permit the use of technical evidence without allowing technical formalism to dominate legal reasoning. Source code, logs, and model documentation can illuminate the causal process that produced an output, but they do not independently determine legal meaning. The legal significance of a technical fact depends on principles of attribution, reliance, good faith, and contractual purpose. Courts should therefore distinguish between explaining how the algorithm behaved and deciding whether that behavior should legally bind the parties.

The twelfth principle should acknowledge different degrees of algorithmic autonomy. A deterministic script that executes fixed instructions should not necessarily be treated in the same manner as an adaptive system capable of generating novel contractual terms. The more open-ended the system's decisional authority, the more important it becomes to examine the scope of delegated discretion. A party that intentionally authorizes broad autonomous decision-making may reasonably bear a broader range of outcomes. Conversely, where the system is expected only to perform narrow ministerial tasks, an unexpected creative output may more readily fall outside the scope of authorization.

This framework also has implications for drafting. Parties employing algorithmic systems should define the legal relationship between code and contract. They may specify whether code merely performs the written agreement or whether certain machine-generated outputs are intended to have independent contractual significance. They may define error thresholds, suspension mechanisms, audit rights, notice procedures, and allocation of losses arising from technical malfunction. Such provisions cannot eliminate all interpretive disputes, but they can clarify the parties' common intention before problems arise.

The importance of ex ante clarification is reinforced by research concerning freedom of will and contractual limits. Autonomy functions most effectively where parties can understand the legal consequences of their choices (Ben Saadia, 2022). Algorithmic contracting should therefore be accompanied by transparency sufficient to enable meaningful authorization. A user need not understand every line of code, but the user should have a reasonable understanding of the categories of transactions the system may generate and the principal risks involved.

The framework also requires sensitivity to asymmetries between sophisticated and weaker parties. A large financial institution deploying proprietary trading algorithms should not be treated identically to an individual consumer interacting with an opaque automated platform. The normative force of autonomy depends partly on the reality of choice and information. Contract law has long recognized limits on freedom where bargaining conditions are structurally unequal (Safaei & Shomali, 2017). Algorithmic interpretation should therefore consider the institutional capacity of the parties to understand, control, and monitor the technological mechanism.

A final element concerns judicial methodology. Courts should approach algorithmic-contract disputes through a sequential inquiry. They should identify the contractual function of the system, determine the scope of human authorization, reconstruct the relevant objective manifestations, examine technical evidence of the system's operation, assess whether the disputed output was foreseeable, evaluate the counterparty's reliance, consider whether good faith limits either party's position, and then determine whether the result should be treated as attributable contractual intention. This methodology would provide greater analytical discipline than simply asking whether the computer "made a mistake."

Such an integrated approach preserves continuity with established contract principles while adapting them to technological realities. It recognizes that common intention remains a central interpretive ideal, but that intention in algorithmic contracting may be distributed across design decisions, parameters, institutional arrangements, automated outputs, and objective reliance. The result is neither the disappearance of contractual will nor the domination of code. It is a reconfiguration of how legal systems identify will when human decision-making is mediated by computational systems.

6. Conclusion

The increasing use of algorithmic systems in contractual formation requires a reconsideration of how contract law identifies and interprets common intention. The traditional model of contract assumes a relatively direct relationship between human deliberation, outward expression, and legal obligation. Algorithmic contracting weakens this temporal and functional connection because the human decision to authorize a transaction may occur long before the particular contract is generated. The system may subsequently select a counterparty, determine terms, calculate price, or execute performance without contemporaneous human awareness. This does not eliminate contractual intention, but it changes the manner in which intention must be legally reconstructed.

The central difficulty lies in the conflict between subjective and objective will. The person who deploys an algorithm may internally intend one category of transaction while the system objectively manifests another. A purely subjective approach would excessively undermine commercial certainty because counterparties could not safely rely on automated manifestations. A purely objective approach would create the opposite danger by treating every technical output as binding regardless of malfunction, error, or obvious departure from the purpose for which the system was authorized. Neither approach adequately responds to the structure of algorithmic transactions.

The appropriate solution is to treat common intention as a legally attributable construct rather than as a purely psychological phenomenon. The key inquiry should be whether the contested algorithmic output falls within the scope of authority that the contracting party reasonably conferred upon the system. This determination requires attention to the user's initial authorization, system parameters, commercial purpose, technological architecture, prior course of dealing, the foreseeability of the output, and the expectations generated for the counterparty. The relevant intention may therefore be located not at the precise moment of contractual conclusion but in the broader framework through which the system was empowered to act.

The distinction between authorizing a method and authorizing a specific result is particularly important. Algorithmic systems are often employed precisely because users do not wish or are unable to decide every transaction individually. A person may therefore intend that a system make decisions according to predefined or adaptive criteria without forming any contemporaneous intention concerning each output. Such delegation should generally be legally effective. However, it should not be interpreted as unconditional acceptance of every technically possible result. Outputs arising from serious defects, corrupted data, unauthorized parameter changes, or behavior radically outside the system's intended operational field may fall beyond the scope of attributable contractual intention.

Objective manifestation nevertheless remains indispensable. Contract law cannot function if parties are permitted to rely on private and undisclosed intentions whenever automated transactions become disadvantageous. Where an algorithm produces an apparently normal transaction within its authorized field of activity and the counterparty reasonably relies on that manifestation, the system user should generally bear the resulting contractual consequences. This allocation reflects the fact that the user voluntarily selected the technological mechanism and was ordinarily better positioned to control its operation.

At the same time, reasonable reliance must have limits. A counterparty should not receive full protection where the algorithmic output is manifestly abnormal, commercially irrational, or obviously the product of malfunction. The interpretive framework should distinguish innocent reliance from opportunistic exploitation. The visibility of the discrepancy between ordinary contractual conditions and the disputed output should therefore affect the weight assigned to objective manifestation.

Technical evidence will play an increasingly important role in these disputes. System logs, configuration records, audit trails, transaction histories, and model documentation can help reconstruct whether the disputed output represented normal operation or technological deviation. However, technical evidence should inform rather than replace legal interpretation. The question of how software produced an outcome is different from the question of whether the resulting manifestation should legally bind the parties. The latter remains a normative inquiry governed by principles of autonomy, reliance, good faith, fairness, and risk allocation.

Algorithmic opacity also requires adjustments in evidentiary practice. A party that deploys a technologically complex system should maintain reasonable records of its operation where the system is used to create legally significant transactions. The inability to explain every computational process should not automatically deprive a transaction of legal effect, but the party controlling the system should not benefit from evidentiary uncertainty that could reasonably have been prevented through proper documentation. The preservation of reliable audit records can therefore become an important component of responsible algorithmic contracting.

The distinction between deterministic and adaptive systems should also influence interpretation. Where software merely executes predetermined commands, attribution is generally stronger because the link between human authorization and system output is direct. Where the system possesses broader adaptive or predictive capacity, the scope of authorization becomes more important. The law should ask whether the user intended to grant the system discretion to produce the type of result that occurred. The more extensive the delegated discretion, the broader the range of outputs that may reasonably be attributed to the user.

The interpretation of algorithmic contracts should also remain sensitive to differences in bargaining power and technological sophistication. A sophisticated corporate actor that designs and deploys its own algorithm can reasonably be expected to bear greater responsibility for its operation than a consumer interacting with an opaque digital platform. The language of autonomy should not obscure situations in which one party has little meaningful understanding or control over the technological system generating contractual terms.

A coherent legal approach should therefore adopt a graduated model. Where actual common intention can reliably be established, it should guide interpretation. Where common subjective intention cannot be demonstrated, objective manifestations should assume greater importance. Where objective manifestation conflicts with persuasive evidence of technological error, courts should assess foreseeability, control, reliance, and good faith. Where both parties could reasonably detect the anomaly, the legal consequences should reflect their respective conduct. Where neither could detect it, responsibility should generally be assigned to the party better positioned to manage the relevant technological risk.

The broader implication is that algorithmic contracting does not render classical contract law obsolete. Rather, it exposes assumptions that were previously less visible. Traditional doctrine often presumed that outward expression and inward intention were sufficiently connected to permit interpretation through familiar methods. Algorithmic systems reveal that this connection may be indirect, distributed, and temporally displaced. The task of modern contract law is therefore to reconstruct that connection without sacrificing either personal autonomy or transactional security.

The most defensible interpretive model is one in which contractual intention is understood as a continuum extending from human authorization to technological execution. Human intention determines the initial legal framework; software operates within that framework; objective manifestations communicate the resulting transaction to others; and legal interpretation determines whether the output remains within the scope of what can fairly be attributed to the parties. This approach avoids attributing independent legal will to machines while recognizing that modern contracting increasingly depends on technological intermediaries.

Accordingly, the conflict between subjective and objective will in algorithmically concluded contracts should not be resolved through categorical preference for one theory. The solution lies in a contextual synthesis. Subjective intention remains decisive when a genuine common understanding can be demonstrated. Objective manifestation becomes dominant where private intentions diverge or cannot be proven and reasonable

reliance has arisen. Technological evidence assists in determining whether the manifestation was properly attributable. Good faith limits opportunistic reliance on obvious errors. Risk-allocation principles determine who should bear the consequences of uncertainty where neither party acted improperly.

Through this integrated framework, contract law can preserve its foundational commitment to voluntary obligation while adapting to the realities of automated decision-making. The objective should not be to force algorithmic transactions into an outdated model of instantaneous human assent, nor to allow code to replace legal intention altogether. The more appropriate approach is to recognize that contractual will in the digital environment may be mediated, deferred, encoded, and operationalized through technology, but it remains ultimately grounded in legal attribution to human or organizational actors. The future of contract interpretation therefore depends on developing doctrinal tools capable of identifying that attribution with sufficient flexibility to protect autonomy, reliance, fairness, and commercial certainty simultaneously.

Authors' Contributions

Authors contributed equally to this article.

Declaration

In order to correct and improve the academic writing of our paper, we have used the language model ChatGPT.

Transparency Statement

Data are available for research purposes upon reasonable request to the corresponding author.

Acknowledgments

We would like to express our gratitude to all individuals helped us to do the project.

Declaration of Interest

The authors report no conflict of interest.

Funding

According to the authors, this article has no financial support.

Ethical Considerations

In this research, ethical standards including obtaining informed consent, ensuring privacy and confidentiality were observed.

References

Abdollahi, M. (2022). A Jurisprudential and Legal Study of Smart Contracts in Light of the Autonomy of Will. *Islamic Jurisprudence and Law Research Journal*(31).

Ben Saadia, M. (2022). *Restrictions on the Principle of Freedom of Will in the Field of Contracts* University of Mohamed Boudiaf, M'Sila].

Hacker, P. (2021). The semantics of smart contracts: Reconsidering intention in algorithmic contracting. *European Review of Private Law*, *29*(2), 175-210.

Karimi, H., & Karimi, A. (2024). Analysis of the Parties' Intention and Consent regarding Imposed Contractual Terms: A Comparative Study of Iranian and French Law. *Biannual Journal of Research and Development in Private Law*.

Karimi, S. (2023). Challenges in the interpretation of smart contracts and the role of parties' intention. *Comparative Law Research Quarterly*, *10*(4), 55-88.

Kaviani, F. (2025). *Distinguishing Intention and Consent as Fundamental Conditions of Will in Contracts: An Analysis of the Legal Effects of Nullity and Non-Enforceability in Imami Jurisprudence and Iranian Law* Ninth International Conference on Social Studies, Law, and Popular Culture,

Paknejad, F. (2023). A comparative study of the rules of intention and consent in electronic contracts in Iran and the European Union. *Private Law Research Quarterly*, *18*(1), 55-78.

Pasban, M., & Sadeghi, N. (2023). Examining the Role of Intention in Smart Contracts with Emphasis on the Iranian Legal System. *Private Law Research Quarterly*(41).

Rashvand, M., & Naser, M. (2019). The Intention of Contracting Parties in Smart Contracts. *Islamic Law Research Journal*(49).

Sacco, R. (2007). Contractual Freedom and Contractual Will. *International Review of Comparative Law*, *59*(4), 743-760.

Safaei, S. H., & Shomali, N. (2017). Countering the Unfairness of Contractual Terms from the Perspective of Restrictions on Freedom of Will in Jurisprudence and Positive Law. *Quarterly Journal of Jurisprudence and Foundations of Islamic Law*, *10*(3).

Shabahang, A., Badini, H., & Almasi, N. A. (2026). The Effect of Intentional or Gross Fault on the Contractual Limitation of the Multimodal Transport Operator's Liability under International Multimodal Transport Documents and Iranian Law. *Legal Studies in Digital Age*, *5*(4).

Shafi'i, A. (2020). A legal analysis of smart contracts and the issue of ascertaining intention. *Journal of Private Law Research*, *8*(3), 121-150.

Shavand, M., & Nasr, M. (2019). Intention of Parties in Smart Contracts. *Quarterly Journal of Islamic Law*, *17*(66), 85-110.

Tetley, W. (2004). Good faith in contract law: particularly in the contracts of arbitration and chartering. *Journal of Maritime Law & Commerce*, *35*(4).

Williamson, O. E. (1979). Transaction-Cost Economics: The Governance of Contractual Relations. *Journal of Law and Economics*, *22*(2), 233-261. https://doi.org/10.1086/466942

Willmott, L., Christensen, S., & Butler, D. (2005). *Contract Law*. Oxford University Press.