IFSA Publishing

Blockchain and Cryptocurrency

Published by IFSA Publishing, S. L., 2026
https://bc-ifsa-journal.com/

Determining Intent in Smart Contracts: Identification Paths and the Calibration of Interpretive Mechanisms

Rui LU

Southwest Minzu University, School of Law, 16 Section 4, South Yihuan Road, Jiangxi Street, Wuhou District, Chengdu, Sichuan 610041, P.R. China
Tel.: + 86 13738188957
E-mail: Delovely33@qq.com

Received: 25 Feb. 2926 /Revised: 14 Mar. 2026 /Accepted: 18 Mar. 2026 /Published: 23 Mar. 2026

Abstract: As blockchain-based smart contracts gain wider adoption, their nature as code-driven mechanisms for automated contract formation and performance underscores the need for legal regulation. Determining their legal character is essential: the 'code theory' overlooks the core element of party intent, whereas the 'contract theory' better captures their essence, making it more normatively sound. Accordingly, a contractual lens provides the logical foundation for regulating smart contracts. Drawing on civil law's focus on subjective intent and common law's objective approach, this article distinguishes between scenarios of sufficient and constrained manifestation of intent, arguing that parties' deliberate activation of triggering mechanisms can constitute valid contractual assent – even without traditional negotiation or natural language. However, execution risks – semantic distortion, linguistic limitations of code, and over-rigid automation – necessitate a balanced framework integrating technical refinement, legal safeguards, and interpretive flexibility to reconcile efficiency with fairness in digital commerce. This article substantially extends an earlier version presented at B2C'2025 by providing a concrete identification path for determining intent in smart contracts and proposing specific risk mitigation strategies for different contract types.

Keywords: Blockchain technology, Smart contracts, Contract theory, Contractual intent, Semantic interpretation, Risk mitigation, Legal regulation.

1. Introduction

The term ‘smart contract’ was first coined in 1994 by American computer scientist, legal scholar, and cryptographer Nick Szabo, who defined it as ‘a set of digitally specified commitments, including the agreements by which the parties will fulfil these commitments’ [1]. As a computerised transaction agreement [2], smart contracts currently rely on blockchain technology as their core technical foundation, aiming to facilitate, verify, or execute contract negotiations or fulfilment without third-party interference. [3] They rely on decentralised blockchain technology composed of encrypted hash links, automatically recording, judging, and executing pre-set conditions through a node network in a distributed ledger. Based on the characteristics of the blockchain distributed ledger and peer-to-peer network, blockchain smart contracts can automatically complete the establishment, transmission, and fulfilment of instructions without human intervention.

Due to the IF-THEN trigger mechanism, smart contracts have a highly simplified establishment model. By pre-setting and inputting the conditions agreed upon by the parties regarding contract terms and performance methods in code form into the system, once the trigger conditions are met, the program automatically ‘outputs’ the performance results, achieving the integration and automation of contract establishment and performance. Smart contracts are currently widely applied in finance (e.g., Bitcoin, Ethereum, and other token-based methods for securities clearing and settlement, collateral management, derivative contracts, etc. [4]), healthcare (pre-authorisation processes for specific medical procedures), and the Internet of Things (e.g., automatic

purchasing when the quantity of food in a refrigerator falls below a pre-set value). They are increasingly being used as transaction tools [5]. In this coded transaction mechanism, contract content is expressed in programming language rather than natural (human) language, and its enforcement mechanism is highly automated. Therefore, there has been ongoing academic debate that smart contracts weaken or even deprive parties of the ability to fully express their true intentions during contract formation. Moreover, due to the ambiguity of natural language and the precision of code language, issues such as semantic conversion distortion, language span limitations, and excessive semantic migration may arise during contract execution. Therefore, the key to addressing the current debate over the expression of intent in smart contracts lies in seeking a recognition and calibration path that respects the characteristics of blockchain technology while incorporating appropriate technical improvements and legal regulations, thereby achieving a seamless integration between smart contracts and traditional contract law rules to better promote their healthy development.

Building upon the theoretical distinction established in Section 3, this article makes four distinctive contributions to smart contract regulation. First, it develops a novel theoretical framework differentiating between scenarios of sufficient and constrained intent manifestation in smart contracts, demonstrating that deliberate activation of triggering mechanisms constitutes valid contractual assent even in the absence of traditional negotiation or natural language. Second, it introduces a structured analytical framework for reconciling technical and legal language, offering a systematic methodology to determine whether on-chain actions satisfy the legal threshold for intent expression. Third, it proposes a classification schema for smart contracts based on revocability and modification costs, providing actionable guidance for selecting context-appropriate contract types across transactional landscapes. Finally, it delineates targeted risk mitigation strategies that synthesize technical refinement, legal safeguards, and interpretive flexibility – thereby advancing a balanced regulatory paradigm for digital commerce.

2. The Mechanism for Establishing Smart Contracts and Their Contractual Nature

2.1. Differences Between Smart Contracts and Traditional Contract Formation Mechanisms

The widespread concern within the academic community that smart contracts may restrict or even deprive parties of their true intentions primarily stems from the high degree of automation and automatic execution inherent in smart contracts, as well as the significant differences between their technical characteristics and traditional contract formation mechanisms.

Smart contracts supported by blockchain technology possess three key features: tamper-proofing, distributed transactions, and automatic execution. These three features complement one another, forming a delicate balance that collectively establishes a smart contract mechanism for automatic formation and execution without human intervention. Among these, tamper-resistance primarily manifests in blockchain's reliance on cryptography and consensus-based mechanisms [6], and once deployed, it cannot be altered [7]; distributed transactions primarily involve blockchain systems that typically do not rely on a central repository [8] to achieve decentralised information management and execution mechanisms. However, it is their high degree of automation and automatic execution that are considered the core elements hindering parties from reaching a genuine expression of intent in smart contracts.

The automated nature of blockchain technology is manifested in the fact that, once all information is collected, if appropriate parameters meet the conditions (typically expressed as "IF" code), the ledger can act as an electronic agent to replace human involvement in approval and management [8] automatically outputs the results of code execution (typically in the form of "THEN"). Smart contracts operate within the blockchain environment, strictly following the code without requiring approval at each step [9] to produce results. For example, the simplest "IF-THEN" conditional statement: if A sends some cryptocurrency to B, then B will send digital assets to A; and a more complex statement: "if A transfers some cryptocurrency to B every month, then A's advertisement will be placed on website C and remain visible for the next month; if A does not transfer cryptocurrency, then the advertisement will be automatically removed" [10]. The above two "IF-THEN" conditional statements serve as typical examples of smart contract automatic input and output scenarios. Once the "IF" condition is met, the blockchain technology code supporting the smart contract will automatically output the "THEN" conclusion based on the established condition – this is the process by which smart contracts automatically execute based on input code instructions under the guidance of blockchain technology.

It is precisely this highly automated execution feature and capability that allows smart contracts to bypass the traditional "bargaining" process where contract parties must repeatedly negotiate and communicate to establish a contract text, and begin execution after both parties' sign and the contract takes effect. This means that the parties signing a smart contract do not exhibit the outward appearance of "negotiation" during the negotiation phase, thereby exposing the risk of smart contracts restricting the parties' expressions of intent. It is therefore not surprising that such concerns have arisen in academic circles.

2.2. The Essence of Smart Contracts

In the application and development of smart contracts, the blockchain-supported automated transaction and enforcement mechanisms have given rise to "Code Supremacy" [11] "Code is Law" [12] "Code is Contract" [4] and similar perspectives, which contend that smart contracts themselves no longer require the support of law or traditional contract theory, as the power of code alone is sufficient to complete transactions and achieve autonomy. Conversely, scholars and practitioners with legal backgrounds contend that contracts governed solely by code will inevitably become unmanageable. Such contracts cannot fully represent or support the entirety of a transactional "contract." Instead, smart legal contracts – incorporating legal elements and support, and prioritising contractual attributes and essence – [4] are key to steering smart contracts towards sound development. The debate over whether the essence of smart contracts lies in code or contract has persisted unabated within both academic and practical circles.

Adherents of the "Code is Law" perspective contend that smart contracts are essentially programmable code executed on the blockchain [13], which can be understood as event-driven transactional agreements but are not regarded as legally binding contracts [10]. For instance, Ethereum is a prominent smart contract blockchain platform employing the Ethereum Virtual Machine (EVM) to support a Turing-complete scripting language, enabling developers to create and deploy diverse decentralised applications. Each participating node within the network runs the EVM [13] to complete the block validation workflow. Leveraging blockchain's unmanned, automated characteristics, the entire process executes autonomously without involving natural language interactions in the traditional legal sense. Thus, as an autonomous execution mechanism built upon blockchain platforms – integrating cryptographic safeguards and consensus mechanisms – smart contracts fundamentally provide the technical foundation for constructing trustless yet verifiable execution environments. Consequently, some scholars define them as "automatically executed electronic instructions drafted in computer code" [14] "computer protocols" [15] "A system for automatically moving digital assets" [16] "Self-executing computer code" [17] and so forth. Consequently, the "code is law" perspective contends that smart contracts should be understood primarily as a set of code systems or software programs operating on the blockchain, whose core function lies in the automatic execution of predefined operations rather than the traditional construction of legally binding contract texts using natural language.

Adherents of the "contract theory" contend that smart contracts should be interpreted as a "novel form of contract." The white paper Smart Contracts and Distributed Ledger – A Legal Perspective notes that for legal practitioners, contracts typically imply a specific legal obligation relationship, Smart contracts embody this particular legal relationship through code [4] constituting an expression of contractual form and representing a new development in contracts based on automation and standardisation [18]. Furthermore, scholar Chai Zhenguo holds a similar perspective, arguing that smart contracts, as predetermined rules (code), require deployment on blockchain programs. These rules take the form of contracts defined by software, regulating behavioural content within digital spaces. In a certain sense, they represent the expression of traditional contracts within the context of digital entities' behavioural content. In other words, smart contracts resemble the codification of electronic textual contracts, possessing all characteristics of standardised contracts while reducing corresponding regulatory and enforcement costs [19]. Consequently, the "contract theory" perspective indicates that smart contracts may be understood as self-executing agreements possessing legal efficacy as electronic information, with their technical characteristics aiding in overcoming legal impediments to their use as contract formation tools [20]. Smart contracts retain the attributes of traditional contracts, albeit expressed in the form of code.

Having presented the two aforementioned differing perspectives on the nature of smart contracts, it becomes apparent that the core divergence lies in how one approaches and perceives the technical medium of the smart contract itself, as well as how one views the inherent meaning of contracts and law. Adherents of the "Code Doctrine" maintain that smart contracts are entirely synonymous with code. This perspective places significant emphasis on the technical characteristics of smart contracts and blockchain technology, equating the core function of automatic execution with the entirety of a contract's purpose. It interprets the parties' intentions as a specialised form of code, implicitly negating and seeking to replace the existing contractual legal framework. However, this view distorts smart contracts into tools that alienate the parties' will, contravening the fundamental principle of freedom of contract. Its one-sided emphasis on the role of computer technology also overlooks essential elements in contract formation, effectiveness, and interpretation during transactions. Its rejection of the existing contract law system fundamentally misinterprets social fairness and natural justice. In terms of consequences, if the "code theory" prevails, smart contracts may become tools for parties to circumvent legal norms through technological means by leveraging code autonomy. Certain scenarios requiring the maintenance of fairness and justice – such as standard form contracts and grossly unfair terms – would lack legal recourse [21]. Parties' rights may also be compromised [22].

By comparison, the 'contract theory' perspective addresses the shortcomings inherent in the aforementioned 'code theory'. With technological advancement and the evolution of transactional forms, the manifestation of contracts has long transcended the traditional paradigms of 'paper documents' and 'natural language'. If the determination of whether an

agreement constitutes a contract remains confined to formal linguistic expression and offline negotiation processes, it fails to account for the diversity of contractual practices in the digital age. In Prime Sight Ltd v Lavarello, Lord Justice Tolsom noted that parties are generally free to enter into contracts on any terms they choose [23]. When individuals can reach agreements on their own terms, this aligns with the spirit and essence of "freedom of contract" and falls within the scope of traditional contract law [24]. This process of contract formation is not constrained by any prescribed form under traditional law; it suffices that the parties' intentions constitute an extension of their freely expressed will to be encompassed within the scope of a contract recognised by contract law [25]. As scholars of Raz have noted, contracts may be realised through diverse forms [26]. These encompass English language texts, nods or handshakes [27] and electronic data messages [28]. Consequently, in the digital age, smart contracts generated, transmitted, received, and stored on blockchains in the form of data code should analogously possess equivalent legal effect. The intentions expressed by parties through code on-chain, such as "automatically transferring assets to the counterparty upon fulfilment of condition A," though not written in traditional language, rely upon mutually selected platforms, rules, and parameter settings. Their legal function is no different in essence from that of a contract signed on paper. As the law continually adapts to new technologies, smart contracts should not be excluded from the contractual framework due to their programmed, automated, and coded nature. Rather, they should be regarded as a natural extension of traditional contracts within the digital era.

Therefore, the content of smart contracts should be viewed through the lens of the 'contract theory'. When considering a vehicle for transactions and expressions of intent, the crucial factor lies not in whether the method of expression is traditional, but whether the final form of the 'contract' constitutes the 'union' and 'intersection' of the parties' mutual intentions [29]. Conversely, the solution to bridging the gap between smart contract codification and traditional contractual forms lies in legislatively recognising the contractual nature of smart contracts, establishing legally enforceable standards for code conversion and readability, and enhancing mechanisms for translating encoded information into human-semantically comprehensible textual expressions.

3. A Theoretical Distinction: Sufficient Versus Constrained Manifestation of Intent

Building on the established "contract theory," smart contracts should be recognised as a new type of intelligent contract that requires semantic conversion to bridge the gap between code and traditional contract forms [30]. In semantic conversion, the core issue is how to preserve the core features of blockchain technology – such as the automatic execution of smart contracts – without diminishing or distorting the expression of intent, while also ensuring that corresponding legal norms can be clearly applied. Therefore, drawing on the understanding of contractual intent in both the traditional civil law and common law systems, exploring how to adequately express the parties' intent in smart contracts, as well as how to collect and transform such intent within smart contracts, has become a priority issue that must be addressed under contractual regulations.

In response to this challenge, this article posits a critical theoretical distinction between scenarios of sufficient manifestation of intent and constrained manifestation of intent in the context of smart contracts. This distinction serves as the foundation for determining when parties' actions – particularly the deliberate activation of triggering mechanisms – can be deemed to constitute valid contractual assent, even in the absence of traditional negotiation or natural-language terms.

3.1. The Content of Expressions of Intent in Traditional Contract Law

In traditional contract law, the interpretation of contractual intent forms the core of both the theory and practice of contract law, whether in the civil law system or the common law system. The common and core content lies in seeking the true intentions of the parties to maintain transaction security and fairness.

In the civil law system, represented by Germany and France, contract law is deeply influenced by Roman law and places greater emphasis on exploring the "inner intentions" of the parties. Under this system, the validity of a contract is deemed to stem from the parties' free will, and the expression of intent is regarded as an act of externalising one's inner intentions. In his General Principles of German Civil Law, Larenz emphasises that the interpretation of an expression of intent should first seek to uncover the true intentions of the party making the declaration, rather than merely adhering to the literal meaning of the words. He notes that if the party making the declaration has made an error or reservation, their true intentions should take precedence [31]. Additionally, the principle of reliance is introduced as an important supplement to balance the relationship between the declarant's true intent and the reasonable reliance of the counterparty. That is, the declarant's expression gives the counterparty reason to believe that a certain meaning exists, as external behaviour is a means of inferring the parties' true intentions [32], even if the declarant's true intention is not so, the declarant may still be bound by their declaration. This principle is particularly important in maintaining transaction security and protecting the reasonable expectations of the other party in cases of inadequate contract negotiations or unclear declarations. The introduction of the reliance principle has enabled the civil law

system to incorporate certain elements of objective interpretation, but its underlying principle remains the respect for the inner intent of the parties.

In contrast, the common law system, represented by England and the United States, places greater emphasis on the external appearance and objective reasonableness of transactions, stressing the theory of objective expression of intent. It holds that the validity of a contract does not depend on the parties' "secret inner intent," but rather on how a "reasonable third party" would understand the parties' words and actions in a specific context. Lord Dilock explicitly stated in Gibson v Manchester City Council that the formation of a contract is not based on the convergence of the parties' subjective intentions but on an objective assessment of the offer and acceptance [33]. Similarly, the same objective standard of consideration is reflected in Lord Clark's judgment in the Supreme Court case of RTS Flexible Systems Ltd v Molkerei Alois Müller GmbH & Co, where he noted that the formation of an "agreement" does not depend on their subjective mindset, but rather on the consideration of the information conveyed between them through words or actions [34]. This objective approach aims to promote certainty and predictability in commercial transactions, avoiding disputes arising from the difficulty of ascertaining the parties' subjective intentions. In the case of Investors Compensation Scheme Ltd v West Bromwich Building Society, Lord Hoffman outlined five principles for contract interpretation, emphasising that interpretation should consider "all relevant background information" [35] i.e., the "context," and to determine what understanding a "reasonable person" would have of the parties' words and actions given that background information.

3.2. The Content of the Expression of Intent in a Smart Contract

Whether it be the traditional civil law principle of "respecting the parties' genuine intentions" or the common law approach of "inferring intent from objective conduct," both theories are founded upon conventional contract law frameworks. However, as an emerging contractual model, smart contracts present unresolved questions regarding how parties' intentions may be ascertained through semantic transformation. Beyond the "contract theory," scholars hold divergent views: some contend that the "automatic formation" and "automatic execution" inherent in smart contracts inherently constrain parties' expressions of intent; others argue that regardless of negotiation, the core purpose of contract formation lies in "reaching agreement," meaning parties possess a sufficient expression of intent when consensus is attained.

Adherents of the "inadequate expression of intent in smart contracts" view contend that smart contracts suffer from structural deficiencies in core elements of intent formation, making it difficult to satisfy traditional contract law's requirements for sufficiency of expression. Scholar Florian Gamper explicitly notes that compared to conventional contracts, smart contracts often lack comprehensive coverage of transactional details and the parties' expected discretionary freedom in wording – for instance, the term "reasonable" – whose code logic struggles to fully map the intricate allocation of rights and obligations within complex transactions. He further emphasised that the value of natural language in contract formation lies not only in conveying information but also in preserving parties' discretionary and interpretative space, whereas the precision demanded by code renders it ill-suited to accommodate such flexibility [27]. Moreover, Michèle Finck's research reveals that the automatic execution characteristic of smart contracts may conflict with the "persistence of genuine intent" in expressions of will. Under the EU data protection legal framework, data subjects should retain the right to withdraw consent at any time; however, the irreversibility of smart contracts may lead to a disconnect between "formal consent" and "substantive changes in intent" [17].

Scholars who maintain that "smart contracts satisfy the requirement of full expression of intent" contend that although smart contracts employ code language in place of traditional natural language, they nonetheless fulfil the legal requirement for full expression of intent regarding the core elements necessary for contract formation. This conclusion finds corroboration within the theoretical frameworks of both major legal systems. From the perspective of the civil law tradition, German law requires that contract formation be based on the "mutual declaration of intent" by both parties. This principal manifests in smart contracts through the jointly established confirmation mechanism within the code. Scholar Ferreira's research indicates that the pre-execution negotiation of terms and parameter confirmation in smart contracts constitutes a phase where parties reach identical expressions of intent regarding core rights and obligations, exhibiting homogeneity with traditional contractual negotiation processes [36]. Durovic and Janssen note that the technical characteristics of smart contracts merely alter the medium of expression, without changing the fundamental principle that "the attainment of mutual consent constitutes the core of a contract." The manual confirmation stage prior to code execution ensures the authenticity of the expressed intent [37].

From the perspective of the Anglo-American "objective conduct standard," the code operations of smart contracts fully map the elements required for traditional contract formation. At the offer stage, pre-set contractual terms (such as the use of funds and reward mechanisms in crowdfunding smart contracts) constitute a "clear statement of willingness to enter into a contract on those terms" if their content is definite and accessible to specific parties. This aligns with the core characteristic of an offer defined by scholar McKendrick: the inclusion of an intention to be bound upon acceptance [24]. The acceptance phase may be fulfilled through on-chain actions. As established in Carlill v Carbolic Smoke Ball Co,

acceptance need not be expressed verbally; consent demonstrated through conduct remains valid [38]. In smart contracts, the user's act of transferring assets to a liquidity pool constitutes unconditional acceptance of the offer, made with full knowledge of its terms. This aligns with the traditional contractual logic that "performance constitutes acceptance" [24]. The consideration element manifests as the exchange of value between asset transfer and project returns, fulfilling Furmston's core definition: "one party's act or promise as the exchange condition for the other party's promise" [39]. Consequently, smart contracts fully embody the core elements of manifestation of intent through code execution. Their formation logic remains fundamentally consistent with traditional contracts regarding "authenticity of manifestation" and "element completeness"; differences in technological medium do not affect the determination of sufficiency of manifestation.

In summary, the fundamental dispute in academia regarding the sufficiency of parties' expressions of intent in smart contracts centres on how to interpret the semantic conversion mechanism between code language and natural language, and whether it can effectively embody fundamental elements of traditional contract law such as offer, acceptance, and consideration. Furthermore, differing interpretations of the formation of expressions of intent across legal systems further influence the recognition of such expressions in smart contracts. Building upon the foregoing analysis, this article will further explore the theoretical and practical feasibility of establishing "sufficiency of expression of intent" in smart contracts within the contractual framework. This aims to provide foundational institutional analysis and normative guidance for constructing smart contracts under a reasonable system of technological and legal regulation.

4. Path for Determining the Meaning of Smart Contracts

In the process of entering into a smart contract, although the parties did not follow the traditional path of negotiation involving "offer and acceptance," the expressions of intent they made still possess authenticity and sufficiency, and are not, as some scholars claim, "limited in expression." In fact, whether assessed under the standards of the civil law system or the common law system, parties entering into smart contracts possess sufficient expressions of intent, which are realised through a technical method distinct from traditional paradigms but equally legally binding. However, in terms of contract interpretation, the parties' expressions of intent may face certain interpretative risks due to the semantic transformation from "natural language" to "code language" and back to "natural language." Therefore, the improvement of the expression of intent mechanism in smart contracts should be achieved through the synergistic effects of technological innovation and legal regulations to jointly mitigate potential legal risks, thereby constructing a more comprehensive smart contract ecosystem and ultimately achieving a dynamic balance between transaction security and contractual freedom.

4.1. Exploring the Expression of Intent in the Context of contract formation

As scholars Kevin Werbach and Nicolas Cornell have pointed out, while smart contracts use the formulation "if... occurs, you will receive Bitcoin," which differs from the traditional contract statement "I will pay you Bitcoin," this difference merely reflects the technical specificity of their implementation [40].

Conversely, the opposing view that "smart contracts lack sufficient expression of intent" must be addressed from both the core requirements of expression of intent and the logic of contract practice. The simplification or omission of negotiation procedures does not necessarily negate the sufficiency of expression of intent. From the perspective of contract law principles, the sufficiency of expression of intent depends on "clarity of content" and "authenticity of intent," rather than the formal completeness of the negotiation process. The widespread use of standardised clauses in traditional contracts has established a mature solution: when clauses are pre-set and the other party lacks negotiation space, the law ensures the authenticity of the expression of intent through the "duty of reasonable disclosure" and the "rule of explicit consent." This logic of "negotiation simplification" and "procedural supplementation" shares an essential commonality with the operational mechanism of smart contracts: while the pre-set code of smart contracts omits the traditional contract's clause-by-clause negotiation process, parties achieve "explicit consent" through actions such as parameter confirmation and digital signature authorisation. The core requirements of this process are fundamentally consistent with the efficacy supplementation rules of standard terms.

Moreover, the code characteristics of smart contracts determine their inherent nature of "technologically fixed intent." The pre-set and confirmation stages of the code do not represent a "lack of intent," but rather the precise externalisation of intent in a digital environment. Parties' review of the code logic and setting of key parameters (such as the subject matter of the transaction and performance conditions) prior to deploying the contract are, in essence, substantive confirmations of the contract content, which are fully equivalent to the intent logic of "signing constitutes acceptance of all terms" in traditional contracts. As long as the parties' acceptance of the final terms is genuine and explicit, the simplification or even omission of the negotiation process does not constitute a defect in validity.

From a practical value perspective, insisting that smart contracts must reflect the "negotiation process" of traditional contracts not only contradicts the core efficiency requirements of digital transactions but also

ignores the innovative impact of technological characteristics on the form of expression of intent. The automatically executed terms of smart contracts, realised through code, are essentially a technological optimisation of traditional negotiation procedures rather than a negation of them. The immutability of their pre-set terms and confirmation actions actually provides stronger technological safeguards for the authenticity of the expression of intent. This form of expression of intent adapted to the digital ecosystem should be recognised inclusively by contract law, rather than being mechanically applied to the formal requirements of traditional transactions.

To summarise the comparative analysis above, Table 1 provides a clear framework illustrating how on-chain actions in smart contracts satisfy the core intent requirements of both major legal traditions.

Table 1. A Comparative Framework for Determining Intent in Smart Contracts.

Legal Tradition	Core Principle of Intent	Application to Smart Contracts	Justification/Example
Civil Law	Inner Intent / Reliance Principle	Explicit action as externalization of intent	Parties' joint confirmation of IF-THEN code logic is an external representation of their true, internal contractual intent. The act of deployment demonstrates a conscious choice.
Common Law	Objective Conduct	On-chain conduct as a verifiable sequence of legal acts	The series of transparent, immutable on-chain actions forms an objective record from which a rational observer can infer a clear intent to be bound by the agreement.

In summary, while the automated execution mechanism of smart contracts reduces the space for human intervention, it does not weaken the legal intent in the expression of behaviour. From the perspective of the "internal expression of intent" in the civil law system and the "objective behavioural assessment" standard in the common law system, it actually enhances external observers' ability to identify "contractual intent" and reduces interpretation disputes caused by linguistic ambiguity and semantic ambiguity in traditional contract formation. In some ways, it even enhances the clarity and certainty of the intent to form a contract, and can be argued to constitute sufficient expression of intent at the time of contract formation. From the general principles of contract law, the core of determining genuine intent lies in whether the act reflects a "legally binding intention," rather than the form of expression (written or oral). This intention is essentially the parties' right to make autonomous choices, i.e., the "intended legal effect" of the legal act. Such an act is typically the "expression" of this intent, i.e., the "manifestation of intent" [31]. As noted by scholar Atia, the pursuit of interests and reasonable reliance are sufficient to give rise to legal obligations [24]. This provides the basis for determining the validity of non-traditional form agreements.

From the perspective of the civil law system's principle of "respecting the parties' true intentions," smart contracts operate based on the parties' autonomous choices and explicit authorisation. The setting of "IF-THEN" execution conditions must first be jointly confirmed and agreed upon by both parties. In other words, smart contracts do not operate automatically out of thin air but are premised on the parties' explicit choices made after thorough consideration. When both parties make mutually consistent expressions of intent and jointly choose to automatically execute contract terms through triggering the "IF-THEN" mechanism, they have, in another form, expressed their joint acceptance of the constraints imposed by the content of their expressed "choice to have the smart contract execute the terms to achieve their intent." Without such explicit expressions of intent, the program itself cannot execute and will not produce any legal or factual binding effect. Therefore, the determination of intent should not be influenced by changes in form but should instead focus on the parties' genuine intent. Additionally, driven by technology, the objects of trust are undergoing subtle changes. Transactions are no longer based solely on trust in individuals but are increasingly based on trust in technology and its providers. In blockchain transactions, people choose to trust smart contracts and act according to their prescribed operational mechanisms. This is not only a form of technological trust but also institutional trust (institutional-based trust) [21]. Based on the principle of trust, both parties, aware of the automatic execution feature of smart contracts and with a consistent contractual purpose, adopt smart contracts to trigger an automatic fulfilment mechanism. This constitutes a reasonable trust in the automated execution mechanism and blockchain technology, thereby inferring their sufficient expression of intent. Therefore, under the civil law system, parties entering into smart contracts have a reasonable and sufficient expression of intent.

The "objective conduct standard" of the common law system provides the core framework for determining the intent of a smart contract: as long as the parties' conduct is sufficient for a rational third party with both legal and technical knowledge to reasonably infer their intent to be bound through objective evidence, the intent is deemed established. This standard was established in the core principle of

Smith v Hughes – the law focuses on the objective appearance of conduct rather than subjective, hidden intentions [41], and this logic applies equally to smart contract scenarios. During the formation of a smart contract, the sequence of parties' actions constitutes a recognisable trajectory of intent: invoking a standardised contract template (constituting an invitation to treat), setting key parameters for the subject matter of the transaction and performance conditions (constituting a definite offer), sending an execution instruction containing a digital signature to the blockchain system (constituting acceptance), and executing the blockchain smart contract code (constituting consideration). The temporal continuity and content certainty of these actions collectively form the objective appearance of "willingness to be bound by the contract." At this point, the "reasonable third party" should be defined as a professional with both contract law knowledge and blockchain technical expertise, who can determine through on-chain code whether the parties completed the operation with full knowledge that "code execution constitutes legal performance" – this aligns with the presumptive logic in traditional contracts that "signing constitutes acceptance of all terms of the text," but replaces "the ability to read and understand natural language text" with "the technical ability to interpret code logic" [42]. It is important to note that differences in the wording of smart contracts do not affect the substantive determination of the "objective behaviour" of the expression of intent.

4.2. Legal Risks and Regulatory Responses in Smart Contract Interpretation

4.2.1. Legal Risks

The ultimate purpose of establishing a smart contract is to fulfil the original objectives and intentions of the parties involved. However, due to the automated execution of smart contracts, which are not subject to any human intervention, unforeseen circumstances may arise during the execution process. In such cases, legal risks may arise in the interpretation of the contract, typically in the form of semantic distortion, language span limitations, and excessive semantic migration.

From the perspective of semantic distortion, this risk stems from the discrepancy between the code expression and the parties' true intentions under the automated execution mechanism of smart contracts. During the contract formation stage, if there is no effective mapping between the oral agreement and the coded terms, this may result in the execution outcome deviating from the parties' original intent. Typical scenarios include: smart contracts omitting core terms agreed upon in natural language, or code parameters differing substantially from oral commitments (e.g., in a gambling contract where a commitment to transfer a $200 prize is made, but the code is set to $20) [10]. Additionally, smart contracts may contain implicit terms not explicitly agreed upon by the parties, such as self-destruct conditions embedded in the code that result in the termination of rights without cause, even when the parties have not 45xternaliz an automatic termination clause [10]. Such discrepancies fundamentally stem from the inconsistency between the "expressive act" of intent and the "true inner intent" during contract execution, directly reducing the "precision of intent" in contract execution.

Unlike formal deviations caused by semantic distortion, the risks associated with language span limitations focus on content loss during semantic conversion. This stems from the inherent structural and functional differences between code language and natural language, meaning that 45xternaliz languages interpreted by machines cannot adequately capture the abstract nature of legal principles or the flexibility of institutional rules [43]. The code requirements of smart contracts necessitate the conversion of natural language into conditional statements, meaning that all contract terms are translated into the form "if A, then B." This conversion barrier results in certain expressions of intent being unable to be 45xternalized through code [44]. For example, the "IF-THEN" mechanism struggles to translate terms like "reasonable care" and "best efforts," which depend on value judgements [42], thereby creating an "interpretation vacuum" in the contract content.

From the perspective of semantic over-translation, the rigidity of smart contract code may lead to expansive interpretations of the parties' intentions, where interpreters go beyond the literal meaning of the code and the parties' reliance interests to impose additional rights and obligations on the contract. A typical example is the mechanical expansion of "IF-THEN" logic. For example, a supply chain smart contract stipulates that "if goods are delivered 30 days late, 5 % of the payment will be automatically deducted." When the actual delay is 29 days, the interpreter may apply the deduction rule by analogy, citing the "absolute nature of code logic," while ignoring the flexible interpretation space for "reasonable time limits" in traditional contract law [42]. While this interpretation aligns with the formal logic of the code, it exceeds the parties' original intent of punishing malicious breaches rather than minor defects, constituting an excessive expansion of the parties' intentions.

4.2.2. Smart Contract Debugging Path Based on Risk Assessment

The existence of risk means that a more effective risk adjustment mechanism must be established. Only under more comprehensive technical debugging and legal regulation can smart contracts truly fulfil their functions of automatic execution and realisation of the rights and obligations of the parties, thereby promoting fairness and freedom in commercial transactions. There are adjustment paths that can be optimised and improved from a technical perspective,

a legal regulatory perspective, and the coordination between the two.

First, from a technical perspective, to reduce misinterpretation of parties' intentions and situations where execution does not align with parties' original intentions, blockchain software developers can create "permissioned" or private blockchain prototypes [45] add "permission" commands to the blockchain, allowing human intervention for modifications [46]. Additionally, after smart contracts are negotiated and written as programs, legal provisions can be incorporated into the runtime layer to validate the contracts. The purpose of this step is to verify the feasibility of the program from a technical perspective and detect any program vulnerabilities or code errors. The runtime layer dynamically verifies the static contract data of the contract layer. If any content violating legal provisions or the parties' intentions is detected, the contract program may be rolled back, updated, or self-destructed as necessary to ensure compliance with legal provisions and the parties' intentions [47].

Secondly, from the perspective of legal regulation, taking the civil law system as an example, protecting the parties' reliance interests has become a widely recognised important principle in modern civil law [31], which is more conducive to the freedom and fairness of transactions. Therefore, when smart contracts result in semantic distortion or language barriers due to technical limitations, even if the automatic execution mechanism of smart contracts renders misunderstood expressions of intent irreversible, corresponding legal provisions for smart contracts should be established based on the fundamental principles of modern civil law. This would respect and recognise the parties' original intent at the time of contract formation, thereby ensuring that parties have a reasonable expectation of reliance when entering into smart contracts. Additionally, the "safe harbour" rule established in the U.S. Digital Millennium Copyright Act of 1998 can be referenced. When unforeseen "contract interpretation" issues arise that result in damage to the parties' interests, the platform provider should also assume the role of "risk controller," immediately taking measures to prevent further damage to interests. Otherwise, the platform provider should bear joint liability for the expanded portion of the loss. This rule can also be combined with the "pre-review" rule, which involves conducting a formal review of the code for vulnerabilities at the outset of contract formation to reduce legal and transactional risks [46] The pre-review of the Wyndham Hotels booking smart contract by the U.S. Federal Trade Commission (FTC) is a typical example of this [48].

Finally, from the perspective of the interpretative mechanism for reconciling conflicts between technical and legal language, it is evident that when the semantic interpretation of a smart contract conflicts with the parties' intentions, a general rule must be established to clarify which party's terms take precedence when there is a conflict between natural language expressions and smart contract provisions [10]. From the perspective of the interpretation of the essence of the parties' intentions – drawing on the civil law system's emphasis on subjective will and the common law system's objective conduct standard – the parties' manifested intent should serve as the primary basis for interpreting their contractual assent, even in code-based agreements [49]. Therefore, the terms expressed in natural language in the contract or those implied by it should take precedence over the terms of the smart contract used. Furthermore, if there is a third-party interpretation of the contract, special rules should be established based on the principle of fairness to provide effective remedies for all parties to the contract, including third parties, to protect their rights from being infringed upon due to inconsistencies between the written terms of the contract and oral agreements [40]. Furthermore, beyond the priority of interpretation, at the level of smart contract types, they can be categorised into "strong smart contracts" with prohibitive costs for revocation and modification, and "weak smart contracts" that can be relatively easily modified after contract execution. Depending on the complexity of rights and obligations, a contract type can be selected based on the legal relationship at the time of contract formation. In more complex contracting scenarios, "weak smart contracts" can be chosen. When there are improper interpretations of the parties' intentions after the contract is automatically executed, the contract can be appropriately modified based on respecting the parties' intentions at the time of contracting [50].

By improving technology, refining legal rules, and resolving conflicts between technology and contracts, we can explore risk regulation pathways for the interpretation of smart contracts. This approach ensures automated efficiency while respecting the fairness and freedom of transactions, preventing technological means from eroding contract fairness and party rights, and fostering the harmonious coexistence of technology and legal principles to promote transaction circulation.

4.3. A Jurisdiction-Agnostic Framework for Verifying Contractual Intent in Smart Contracts

This article establishes a jurisdiction-agnostic interpretive pathway for intent verification in smart contracts, resolving the critical gap between technical execution and legal sufficiency. The mechanism operates through three sequentially integrated phases, each addressing a distinct dimension of contractual intent formation that transcends conventional negotiation paradigms.

4.3.1. Technical Intent Mapping as Contractual Foundation

The pathway commences with rigorous verification of the code's fidelity to pre-execution

intent. This requires demonstrable alignment between the smart contract's "IF-THEN" logic and documented prior agreements, alongside precise correspondence between coded parameters and expressly stated contractual terms. Crucially, this phase rejects semantic drift – a pervasive risk where code semantics diverge from human intent due to linguistic constraints – by mandating explicit linkage between on-chain conditions and off-chain negotiation records.

4.3.2. Jurisdictional Calibration of Intent Manifestation

The second phase dynamically adapts to legal system paradigms. In civil law jurisdictions, it evaluates whether parties' on-chain actions (e.g., deployment, parameterization) constitute conscious externalization of subjective intent, treating code activation as equivalent to signature. For common law systems, it applies an objective reasonable technologist test: whether a third party possessing relevant blockchain expertise would reasonably infer binding intent from the same actions. This dual-axis assessment resolves the "code theory vs. contract theory" impasse by grounding intent in actional context rather than linguistic formality.

4.3.3. Risk-Contextualized Contractual Validation

The final phase synthesizes transactional context with risk taxonomy to determine legal sufficiency. It requires: (i) verification that execution aligns with original intent (not merely code logic), (ii) identification of specific risk vectors (semantic distortion, language span limitations, or excessive semantic migration), and (iii) context-aware mitigation selection – such as mandatory pre-deployment audits for B2B contracts with high modification costs, versus dynamic consent protocols for consumer-facing smart contracts. This transforms risk assessment from a passive safeguard into an active determinant of contractual validity.

5. Conclusions

With the rapid development of the digital economy, smart contracts – an innovative fusion of blockchain technology and contractual mechanisms – are gradually expanding the operational logic of traditional contractual models. How to determine the true intent of the parties involved in the highly automated and decentralised operation mechanism of smart contracts has become an urgent issue that the field of contract law must address. This article, from the perspective of the "contract theory," examines the theoretical frameworks and criteria for determining intent in both the civil law system and the common law system. It argues that while smart contracts do not follow traditional negotiation pathways or natural language expression methods, they can still be deemed to constitute sufficient and clear contractual intent through the signing trigger mechanism, thereby meeting the legal requirements for sufficient intent.

However, smart contracts still face legal risks during execution due to semantic distortion caused by differences between natural language and technical language, language span limitations, and excessive semantic migration. These risks are particularly evident when there is a disconnect between the code language and the parties' true intentions, potentially leading to execution deviations and legal consequences. Therefore, while acknowledging the validity of smart contracts, efforts should be made from three aspects: technological improvements, legal regulations, and the coordination of technology and law, to establish a "technology-law-institution" synergistic and interactive adjustment pathway.

In summary, as an extension of the concept of contracts in the digital age, the regulatory framework for smart contracts should not be confined to technical logic or formalism. Instead, it should respect the characteristics of blockchain automation while grounding itself in the fundamental principle of party autonomy and the theoretical foundation of contract law. Through the mutual adaptation of technology and law, it should provide a legal framework to support the construction of an efficient and trustworthy digital transaction order. This approach not only addresses the challenge of contract recognition "beyond form" in the digital age but also provides a theoretical foundation and institutional insights for the universal application of smart contracts in the context of global governance, while also establishing a reasonable legal framework for the recognition and use of smart contracts to ensure the safety and freedom of commercial transactions.

References

[1]. N. Szabo, Smart contracts: Building blocks for digital markets, *Extropy: Journal of Transhumanist Thought*, Vol. 16, Issue 2, 1996.

[2]. N. Szabo, Smart contracts, https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

[3]. S. Bourque, S. F. L. Tsui, A lawyer's introduction to smart contracts, in Scientia Nobilitat: Reviewed Legal Studies (A. Tyc, Ed.), *Scientia Nobilitat*, 2014, pp. 4-23.

[4]. Smart contracts and distributed ledger – A legal perspective, Whitepaper, *European Union Blockchain Observatory and Forum*, 2019.

[5]. Q. F. Xia, Legal nature analysis of smart contracts, *Eastern Law Review*, Issue 6, 2022, pp. 33-43 (in Chinese).

[6]. M. Chevalier, From smart contract litigation to blockchain arbitration: A new decentralised approach leading towards the blockchain arbitral order, *Journal of International Dispute Settlement*, Vol. 12, Issue 4, 2021, pp. 558-584.

[7]. S. Y. Lin, L. Zhang, J. Li, et al., A survey of application research based on blockchain smart

contract, *Wireless Networks*, Vol. 28, 2022, pp. 635-690.
[8]. Lowell Milken Institute for Business Law and Policy, Smart contracts: Is the law ready?, https://lowellmilkeninstitute.law.ucla.edu/wp-content/uploads/2018/08/Smart-Contracts-Whitepaper.pdf
[9]. M. C. Compagnucci, M. Fenwick, S. Wrbka (Eds.), Smart Contracts: Technological, Business and Legal Perspectives, *Hart Publishing*, Oxford, 2021.
[10]. N. Filatova, Smart contracts from the contract law perspective: Outlining new regulative strategies, *International Journal of Law and Information Technology*, Vol. 28, Issue 3, 2020, pp. 217-242.
[11]. P. De Filippi, A. Wright, Blockchain and the Law: The Rule of Code, *Harvard University Press*, Cambridge, 2018.
[12]. L. Lessig, Code 2.0: Law in the Networked Society (X. Li, W. W. Shen, Trans.), *Tsinghua University Press*, *Beijing*, 2018 (in Chinese).
[13]. H. Wang, J. Liu, J. Zhao, Blockchain smart contracts for decentralized matching of counterparties and automatic settlement of financial derivatives, *Blockchain: Research and Applications*, Vol. 6, Issue 4, 2025, 9.
[14]. Gibson v. Manchester City Council, [1979] UKHL 6, *UK*, 1979.
[15]. G. Governatori, F. Idelberger, Z. Milosevic, et al., On legal contracts, imperative and declarative smart contracts, and blockchain systems, *Artificial Intelligence and Law*, Vol. 26, Issue 4, 2018, pp. 377-407.
[16]. G. Wood, Ethereum: A secure decentralised generalised transaction ledger, Ethereum Project Yellow Paper, *Ethereum Foundation*, 2014.
[17]. M. Finck, Smart contracts as a form of solely automated processing under the GDPR, *International Data Privacy Law*, Vol. 9, Issue 2, 2019, pp. 78-94.
[18]. F. Lang, A new interpretation of contracts through smart contracts under blockchain technology, *Journal of Chongqing University (Social Sciences Edition)*, Vol. 27, Issue 5, 2021, pp. 169-182 (in Chinese).
[19]. Z. Chai, Contract law reflections on smart contracts under blockchain technology, *Guangdong Social Sciences*, Issue 4, 2019, pp. 240-241 (in Chinese).
[20]. E. A. Kirillova, V. V. Bogdan, I. B. Lagutin, et al., Legal status of smart contracts: Features, role, significance, *Jurídicas CUC*, Vol. 15, Issue 1, 2019, pp. 285-300.
[21]. Y. Wu, On the private law structure of smart contracts, *Jurist*, Issue 2, 2020, pp. 1-13 (in Chinese).
[22]. Q. Lin, Legal boundaries of smart contract code governance, *Hebei Jurisprudence*, Vol. 43, Issue 7, 2025, pp. 143-161 (in Chinese).
[23]. Cukurova Finance International Ltd v. Alfa Telecom Turkey Ltd, [2013] UKPC 22, [2014] AC 436, *UK*, 2013.
[24]. E. McKendrick, Contract Law (12th ed.), *Palgrave Macmillan*, London, 2020.
[25]. J. Gordley, Contract, property, and the will – The civil law and common law traditions, in The State and Freedom of Contract (H. Scheiber, Ed.), *Stanford University Press*, Stanford, 1998, pp. 79-83.
[26]. J. E. Penner, Voluntary obligations and the scope of the law of contract, *Legal Theory*, Vol. 2, Issue 4, 1996, pp. 325-357.
[27]. F. Gamper, A non-contractual approach to smart contracts, *International Journal of Law and Information Technology*, Vol. 31, Issue 3, 2023, pp. 231-252.
[28]. UNCITRAL, UNCITRAL Model Law on Electronic Commerce, https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce
[29]. L. Duguit, Traité de Droit Constitutionnel (3rd ed., Vol. 1), *Éditions de la Société Anonyme du Recueil Sirey*, *Paris*, 1927 (in French).
[30]. C. D. Clack, V. A. Bakshi, L. Braine, Smart contract templates: Foundations, design landscape and research directions, https://www.cs.ucl.ac.uk/fileadmin/UCL-CS/research/Research_Notes/Smart_Contract_Templates.pdf
[31]. K. Larenz, General Principles of German Civil Law, Vol. 1 (X. Wang, et al., Trans.), *China Law Press*, Beijing, 2003 (in Chinese).
[32]. M. Planiol, G. Ripert, Traité Élémentaire de Droit Civil, *Librairie générale de droit et de jurisprudence*, *Paris*, 1949 (in French).
[33]. SAGE, Formation of contracts: Gibson v. Manchester City Council, https://sk.sagepub.com/cases/formation-of-contracts-gibson-v-manchester-city-council
[34]. RTS Flexible Systems Ltd v. Molkerei Alois Müller GmbH & Co KG, [2010] UKSC 14, [2010] 1 WLR 753, 2010.
[35]. Stocznia Gdanska SA v. Latvian Shipping Co, [1998] 1 WLR 896, *UK*, 1998.
[36]. A. Ferreira, Regulating smart contracts: Legal revolution or simply evolution?, *Telecommunications Policy*, Vol. 45, Issue 2, 2021, pp. 1-16.
[37]. M. Durovic, A. Janssen, The formation of smart contracts and beyond: Shaking the fundamentals of contract law, in Smart Contracts and Blockchain Technology: The Role of Contract Law (M. Cannarsa, P. Sirena, et al., Eds.), *Cambridge University Press*, Cambridge, 2019, pp. 1-27.
[38]. Carlill v. Carbolic Smoke Ball Co, [1893] 1 QB 256, *UK*, 1893.
[39]. M. P. Furmston, Cheshire, Fifoot & Furmston's Law of Contract (16th ed.), *Oxford University Press*, Oxford, 2012.
[40]. K. Werbach, N. Cornell, Contracts ex machina, *Duke Law Journal*, Vol. 67, 2017, pp. 313-382.
[41]. Business Bliss Consultants FZE, Smith v. Hughes, https://www.lawteacher.net/cases/smith-v-hughes.php
[42]. H.-W. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, et al. (Eds.), Constitutional Challenges in the Algorithmic Society, *Cambridge University Press*, Cambridge, 2021.
[43]. L. Efimova, O. Sizemova, A. Chirkov, Smart contracts: Between freedom and strict legal regulation, *Information & Communications Technology Law*, Vol. 30, Issue 3, 2021, pp. 331-350.
[44]. Y. Ni, Civil law analysis, application, and implications of smart contracts under blockchain technology, *Journal of Chongqing University (Social Sciences Edition)*, Issue 3, 2019, pp. 178-190 (in Chinese).
[45]. M. N. Temte, Blockchain challenges traditional contract law: Just how smart are smart contracts?, *Wyoming Law Review*, Vol. 19, Issue 1, 2019, pp. 185-210.
[46]. L. Han, L. Cheng, Legal deconstruction and risk mitigation of blockchain smart contracts, *Learning and Practice*, Issue 3, 2022, pp. 54-62 (in Chinese).
[47]. X. D. Li, S. Y. Ma, Research on blockchain smart contracts under the contract section of the civil code,

Journal of Shanghai Normal University, Vol. 49, Issue 5, 2020, pp. 58-69 (in Chinese).
[48]. Federal Trade Commission v. Wyndham Hotels & Resorts, LLC, No. 14-3514 (3d Cir. 2015), *USA*, 2015.
[49]. R. Lu, Legal approaches to determining the expression of intent in smart contracts, in *Proceedings of the 4th Blockchain and Cryptocurrency Conference (B2C'25)*, 2025, pp. 97-99.
[50]. M. Raskin, The law and legality of smart contracts, *Georgetown Law Technology Review*, Vol. 1, Issue 1, 2017, pp. 305-341.