The Nature and Enforceability of Smart Contracts in the Metaverse: A Legal Analysis and Implementation Challenges

1. Dorna Hakimelahi*: Department of Private Law, Zarg.C., Islamic Azad University, Zarghan, Iran

*Correspondence: d.hakimelahi@iau.ir

Abstract

Smart contracts, as one of the most significant achievements of blockchain technology, possess transformative potential in the formation, execution, and supervision of contractual relationships. By relying on self-executing code, these contracts enable the elimination of intermediaries, cost reduction, and enhanced transparency, and they play a fundamental role in environments such as the metaverse. Nevertheless, their digital nature and reliance on programming algorithms have generated extensive legal challenges in terms of acceptance and enforcement. The most significant of these challenges include difficulties in translating legal concepts into code, the lack of sufficient flexibility to modify or amend contractual terms, the complexity of determining liability in cases of algorithmic errors, and the incompatibility of such contracts with traditional dispute resolution mechanisms. Furthermore, the cross-border execution of smart contracts raises critical issues concerning judicial jurisdiction and conflict of laws, given the decentralized and non-territorial nature of blockchain technology. Concerns related to cybersecurity and the protection of privacy are also identified as major obstacles to the development of these contracts. Despite these challenges, legal and technological analyses indicate that, provided appropriate legal frameworks are articulated and effective supervisory mechanisms are established, smart contracts have the capacity to function as valid and efficient substitutes for, or complements to, traditional contracts. By examining the nature, legal status, and implementation challenges of smart contracts, this article emphasizes the necessity of revising existing regulations and aligning legal systems with emerging technological developments.

Keywords: Smart contracts, blockchain, contract interpretation, legal liability, metaverse.

Received: 07 October 2025
Revised: 01 February 2026
Accepted: 08 February 2026
Initial Publication 10 February 2026
Final Publication 01 July 2026

Citation: Hakimelahi, D. (2026). The Nature and Enforceability of Smart Contracts in the Metaverse: A Legal Analysis and Implementation Challenges. *Legal Studies in Digital Age,* 5(3), 1-15.

1. Introduction

Technological developments of the twenty-first century have not only challenged traditional legal concepts but have also created new grounds for rethinking the foundations of legal relationships between natural and legal persons. One of the most significant of these developments is the emergence of smart contracts, which, by relying on blockchain technology and eliminating the need for traditional intermediaries, have introduced self-executing capability into the realm of modern contracting (Werbach & Cornell, 2017). At the same time, the concept of the metaverse has expanded as a multilayered digital space in which living, working, entertainment, and even governance are virtually reconstructed (Dizaji & Dizaji, 2023). The convergence of these two phenomena—smart contracts and the metaverse—has generated a new challenge at the intersection of technology, economics, and law.

As the metaverse moves toward the creation of self-governing virtual communities and complex digital interactions, the use of smart contracts to regulate relationships among users, organizations, and even governmental entities appears inevitable. Nevertheless, the fundamental issue remains that, despite advantages such as automated execution, the elimination of intermediaries, and a high degree of transparency, smart contracts in many legal systems continue to face ambiguities regarding legal validity, enforceability, judicial interpretation, and the identification of contracting parties (Janssen & Durovic, 2018).

Moreover, the dependence of these contracts on rigid coding logic and the absence of human elements such as good faith, equity, or flexibility in the performance of contractual obligations have led some scholars to question their efficiency and legal legitimacy (Mik, 2017). In the metaverse, where many activities are based on digital ownership, disintermediated interactions, and decentralized entities such as decentralized autonomous organizations (DAOs), smart contracts may serve an infrastructural role; however, they still require interpretation and support from traditional legal systems.

Jason Allen presents his view in response to criticisms raised by Pardolesi and his colleagues, stating: "Nothing prevents a single instrument, written in a formal language (i.e., code), from embodying both the contract itself and the automated mechanism for its performance" (Allen & Hunn, 2022).

Accordingly, not only are perspectives sharply divided, but there is also significant disagreement over terminology itself. The UK Jurisdiction Taskforce has defined smart legal contracts as "legally enforceable smart contracts that can give rise to legally binding obligations in accordance with their terms"; it therefore appears preferable to understand smart contracts as a combination of smart contract code and traditional legal language operating together, rather than as a contract consisting solely of computer code (Durovic & Janssen, 2018).

The Cenkus Law Office has expressed a different view, stating that a smart legal contract is "a specific application of this type of code (a smart contract)…used to form an organization…used to execute a program or may be used…to facilitate a legally binding agreement" (Cenkus, 2018).

By contrast, Jelena Madir has argued that smart contracts "functionally consist of pieces of smart contract code, but are critically situated under the umbrella of an overarching relationship that creates legally enforceable rights" (Madir, 2020).

Thus, although there is a strong emphasis on definitional clarity, such clarity is far from achieved, rendering the practical task of reaching consensus highly complex.

With respect to pure smart contracts—contracts written entirely in code—the situation is even more complex. "(Legal) smart contracts can, in principle, satisfy the requirements for contract formation, and their problems are not insurmountable" (Durovic & Janssen, 2018). It should be noted that, given the flexibility and adaptability of English contract law and its rules of formation, smart contracts are capable of forming legally valid contracts and may therefore genuinely be regarded as enforceable agreements.

This article adopts an interdisciplinary approach to elucidate the legal nature of smart contracts, examine their applications in the metaverse, identify existing limitations, and propose pathways for better alignment of this phenomenon with fundamental legal principles. To this end, theories such as transaction cost economics and core principles of contract law are employed in order to provide a theoretical–practical analysis of the current state and future prospects of smart contracts in the metaverse.

2. Smart Contracts

2.1. The Concept of Smart Contracts

It should be noted that there is no international legal framework specifically designed for blockchain technologies and smart contracts; however, this issue is clearly under consideration at the legal/regulatory level. As has been observed, "today everything is about blockchain brainstorming," and at the national/regional level—particularly in the United States—certain regulations have been enacted or are in the process of enactment (Tasca, 2015).

For example, the State of Arizona enacted a detailed statute (Arizona House Bill 2417) which expressly provides that (a) “a signature that is secured through blockchain technology is considered an electronic signature,” (b) “a record or contract that is secured through blockchain technology is considered an electronic record,” and (c) “smart contracts may exist in commerce; a contract relating to a transaction may not be denied legal effect, validity, or enforceability solely because that contract contains a smart contract term” (Catchlove, 2018).

The State of Vermont has also enacted a statute with detailed provisions regarding blockchain (Section 1913, Blockchain Enabling), addressing matters of authentication, admissibility, and presumptions. For instance, it provides that (a) “a fact or record verified through the valid application of blockchain technology is authentic,” (b) “the date and time of recording a fact or record established through such a blockchain is the date and time the fact or record was added to the blockchain,” and (c) “the person identified through such a blockchain as the person who recorded the record is the person who recorded the record,” while, in any event, “a presumption does not extend to the truth, validity, or legal status of the contents of the fact or record” (Tasca, 2015).

In practice, “both states chose to recognize legal effects for information placed on a blockchain or within a smart contract and explicitly incorporate it into the legal system. Moreover, this approach aligns with the recent reaction of certain market authorities stating that securities laws may apply to token sales conducted through initial coin offerings, effectively bringing them within regulation indirectly” (Jaccard, 2018).

Nevertheless, most jurisdictions worldwide still lack blockchain-specific regulations. This may be partly due to the complexity of these technologies and, more fundamentally, to the inability of modern legislative processes to keep pace with rapid technological evolution.

In addition, because blockchain is a (technologically neutral) tool, it appears more reasonable to regulate its uses rather than the technology itself, in order to avoid suppressing innovation.

Regarding the need for special regulation, it has been observed that “the growing interest in blockchain technology, independent of a VC scheme, by default raises fewer policy concerns, because the technology will be used in a closed system governed by regulated financial institutions” (Scheinert, 2016).

However, “although blockchain technology was initially designed to implement the business model of the Bitcoin currency, it now appears to be emerging as a promising means of achieving other objectives as well. Blockchain technology may find its way into mainstream financial markets. It may be used in a wide variety of applications in which data must be transferred without risk of corruption. The problem for blockchain technology may be that it first appeared in a sensitive and heavily supervised domain such as currencies, drawing regulators’ attention while it was still immature and before its potential was fully understood” (Scheinert, 2016).

Accordingly, regulation targeting virtual currencies may indirectly introduce rules relevant to blockchain technologies, and this may have negative implications for blockchain (Tasca, 2015).

Undoubtedly, these technologies are at the center of attention—for example, Bank of America has reportedly filed numerous blockchain-related patents (Scheinert, 2016), while a Patentscope search returned 449 results for “blockchain,” 184 results for “smart contract,” and 63 results for “smart contracts” (de Caria, 2019)—and, as a result, careful and calibrated steps are required.

At present, the legal status of smart contracts in many legal systems remains uncertain, and relatively limited legal scholarship addresses the issue directly (International Monetary, 2016). Although the absence of specific regulation does not necessarily imply disorder or non-regulability, this legal gap can generate confusion in their legal interpretation and enforcement. In practice, smart contracts may be conceptualized as software components designed through computer code that execute automatically upon the satisfaction of predefined conditions (Savelyev, 2017). Despite the lack of dedicated rules in many jurisdictions, general principles of contract law and existing doctrines may still be applied to such arrangements (Tasca, 2015).

With the development of distributed ledger technology (DLT), the groundwork has been laid for broader and more effective implementation of smart contracts. Although a smart contract can technically exist independently of DLT, leveraging DLT facilitates automated execution at a global scale and enables direct, disintermediated interaction between contracting parties.

By contrast with the physical mechanism of selling goods, parties in smart-contract settings can finalize performance conditions remotely and without physical presence simply by agreeing on code and deploying it on a DLT infrastructure. This approach can reduce frictions in value transfer processes and further enable the automation of cross-border transactions (Goldenfein & Leiter, 2018).

Nevertheless, no comprehensive and universally accepted legal definition of "smart contract" has yet been established. In some accounts, a smart contract is not treated as a legally binding agreement, but rather as code that merely automates predefined commercial processes without the need for judicial intervention. These arrangements—sometimes referred to as "smart contract code"—have generated challenges in terms of alignment with the traditional structure of contract law.

At the legislative level, certain U.S. states have enacted rules addressing smart contracts. However, the diversity—and at times inconsistency—of definitions across states creates the risk of a fragmented and ambiguous approach. This trend can lead to uncertainty in practice when courts and market actors attempt to interpret the nature of such contracts. For example, Arizona law offers a specific definition of smart contract that differs from other states' formulations, underscoring the need for regulatory coordination at both national and international levels (Catchlove, 2018).

As a result, although smart contracts—by virtue of their technological capabilities—have introduced fundamental changes in how legal agreements may be performed, the absence of coherent legal frameworks will continue to pose serious challenges for judicial interpretation and application.

"An event-driven program, with state, that runs on a distributed, decentralized, shared, and replicated ledger and that can take custody over and instruct transfer of assets on that ledger." (Catchlove, 2018)

The State of Tennessee amended and expanded this definition and defined a smart contract as: "an event-driven computer program that runs on an electronic, distributed, decentralized, shared, and replicated ledger and that is used to automate transactions, including, but not limited to, transactions that: (a) take custody over and instruct transfer of assets on that ledger; (b) create and distribute electronic assets; (c) synchronize information; or (d) manage identity and user access to software applications" (Jaccard, 2018).

The principal appeal of distributed ledger technology in blockchain, as the name indicates, lies in how data are recorded and shared. Blockchain is a comprehensive and transparent record-keeping system for all transactions carried out through its software, and this information is simultaneously available to all network users. The term "blockchain" derives from its structure: a chain of blocks, each block containing a set of transactions. This chain is continuously updated in real time with new information. For example, in the Bitcoin blockchain—one of the most widely known implementations—updates occur approximately every ten minutes. As a result, transactions are finalized within that window, value and ownership are transferred, and all users' copies of the ledger are updated (Tapscott & Tapscott, 2016).

Distributed ledgers are generally categorized into two broad types: permissioned and permissionless. A network such as Bitcoin is permissionless, meaning any person with internet access can create an account without restriction (Micheler, 2015). By contrast, permissioned ledgers allow access only to individuals who satisfy specific conditions and authentication requirements. Such ledgers have increasingly attracted commercial interest, particularly in contexts such as derivatives markets.

Security in these ledgers is maintained through cryptography and the use of public and private keys. However, this design also entails distinct risks—especially if a user's private key is lost or unlawfully disclosed. Whenever a transaction occurs—such as spending a unit of digital currency or transferring ownership—the event is automatically recorded by the software and appended to the ledger. Any attempt to spend the same unit again is rendered ineffective by the blockchain structure (Green, 2018).

This mechanism introduces fundamental changes to the traditional concept of contracts. In conventional contracting, trust and cooperation between parties are vital. In blockchain-based contracts, however, all terms are transparently coded and visible to the parties. Once the specified conditions are satisfied, performance is executed automatically. This feature substantially reduces the need for mutual trust and, for that reason, these arrangements are sometimes described as "trustless contracts."

But what makes smart contracts so innovative? The answer is straightforward: apart from being digitally recorded and implemented through coding on a blockchain, these contracts do not differ radically in substance from traditional contracts.

Nevertheless, this technical feature enables smart contracts to offer significant advantages over their conventional counterparts. They are automated, autonomous, and executed without intermediaries (Dewey & Amuial, 2015).

Outside the United States, in 2017, Belarus was reportedly the first country to legislate smart contracts, defining them in a presidential decree as: "program code designed to operate on a distributed ledger for the purpose of automated execution of transactions or the performance of other legally significant actions" (Savelyev, 2017).

Notably, the decree establishes a reverse presumption that a person entering into a transaction using a smart contract is fully aware of the transaction's terms, including any flexible terms embedded in the smart contract.

However, for others, "smart contract" means a legal contract whose details are partially or fully represented or performed by software. In other words, a party's contractual obligations are fulfilled through the automated operation of software. In this chapter, references to "smart contracts" are intended to mean smart legal contracts, not smart contract code.

These distinctions between smart contract code and smart legal contracts can cause confusion in discussions of smart contracts, creating a risk that lawyers and computer scientists speak in parallel rather than engaging the same concept. However, rather than treating smart legal contracts and smart contract code as two separate concepts, the reality is that a relationship exists between them: for a smart legal contract to be performed, it must include one or more pieces of code designed to carry out specific tasks when predefined conditions are satisfied—namely, smart contract code. Accordingly, smart legal contracts are functionally composed of smart contract code components, but critically they exist under the umbrella of an overarching relationship that creates legally enforceable rights. As a result, every smart legal contract can be said to include one or more pieces of smart contract code, but not every piece of smart contract code constitutes a smart legal contract (International et al., 2017).

Given both core concepts and the emphasis on automation and enforceability, some authors have defined smart contracts as: "a smart contract is an automated and enforceable agreement. Automatable by computer, although some parts may require human input and control. Enforceable either by legal enforcement of rights and obligations or via tamper-proof execution of computer code" (Clack et al., 2017).

Put simply, a smart contract is an agreement whose performance is automated. This definition has the advantage of being sufficiently broad to cover both smart legal contracts and smart contract code. It captures what appears to be the core of virtually all understandings of smart contracts: automation and automated performance (and, by extension, enforceability) of a predefined conditional action.

In a similar approach, Clack and others have also defined smart contracts as follows: "a smart contract is an agreement whose performance is both automated and binding. Automated by computer, although some parts may require human input and supervision. Binding either through legal enforceability arising from rights and duties (contract law) or through tamper-resistant execution" (Nejat-Zadegan, 2022).

It is important to note, however, that smart contracts neither possess artificial intelligence nor are they capable of machine learning. They are designed to produce a specific outcome whenever a defined set of conditions is satisfied. For that reason, they are well-suited to "if this, then that" structures. Once a condition is met, the smart contract proceeds with the next step required for performance. For example, smart contracts are often considered ideal for parametric insurance, where payment is triggered upon the occurrence of a specified event. If a flight is delayed beyond a defined threshold or an earthquake of a specified magnitude occurs, payment can be made automatically rather than requiring the insured to undertake a lengthy claims process.

2.2. The Legal Nature of Smart Contracts

Although the term "smart contract," as noted, originated in the 1990s, there is still no precise definition of the concept. One of the most debated issues concerns the fundamental question of their legal significance. While the computer code of a smart contract may be regarded as a type of specific regulation—because its operational rules resemble legal effects—law and code remain two distinct systems that evolve autonomously within different normative and logical domains: the former regulates social relations, whereas the latter constitutes an information system (Szabo, 1996).

Not everything that is executable is necessarily legally significant. For example, a smart contract can be used to perform a non-contractual process, such as an online voting procedure, or to deliver a service such as paying cryptocurrency based on an agreement previously concluded off-chain. Conversely, it may constitute the contract itself—sometimes unilaterally and pre-defined by one party—or, where artificial-intelligence algorithms are employed, it may define, modify, or supplement the contractual content autonomously (Werbach & Cornell, 2017).

At the same time, the foregoing examples often concern the execution of clauses or limited, mechanical aspects, behind which there is—at minimum—human action by one party, performance under pre-existing contracts, or security measures deployed to protect contractual performance. With smart contracts, automation is, for the first time, capable of affecting not only clauses or modules but the entirety of the contract from formation to performance (Werbach & Cornell, 2017).

Conversely, not everything that is legally significant is executable. Certain contractual clauses cannot be programmed and performed through computer code because they are inherently open-textured or interpretive, such as fairness and good faith, due care and diligence, and similar standards (Mik, 2017).

Moreover, a computer code will not account for the possibility that the legal contract may be void unless it is instructed to do so. The system essentially operates according to its own rules and performs the contract in accordance with its algorithmic configuration, without regard to legal doctrines (Mik, 2017).

As a result, the phenomenon of smart contracts deployed on a distributed ledger such as blockchain is problematic, because divergences may arise between the legal system and the information-technology system, potentially leading to the performance of unlawful smart-contract outcomes (Werbach & Cornell, 2017).

There are serious disagreements regarding the nature of smart contracts. Some argue that the mere fact that a legal contract is an electronic contract—for example, a contract in PDF format or displayed on a computer screen as HTML—renders it a smart contract. This argument is incorrect in one respect, because such contracts do not inherently possess "smartness," and web protocols can generate "smart" pages independently of contractual automation. However, such pages may be "smart" if created using computational logic (such as fuzzy logic) and particular protocols. Others contend that smart contracts are a form of negotiated contract in the online environment, meaning a tool that electronically matches predetermined parameters accepted by the parties. Although that proposition may be partially accurate, it remains essential to recognize that the automation feature is what distinguishes smart contracts from other comparable arrangements (Rabbani Mousavian, 2021).

In this context, while some researchers propose distinctions among smart contracts, smart contract code, and smart legal contracts, others argue that smart contracts are independent of law. As computer scientists and economists have shown on multiple occasions, it is possible to discuss smart contracts without even addressing the question of their legal nature.

This is because, notwithstanding the term "contract," they are not necessarily perceived as a legal matter—at least within the blockchain discourse—such that both their legal character and their "smartness" have been contested.

From an information-technology perspective, the term "smart" has an operational meaning, indicating the use of algorithms and computer programs. By contrast, the term "contract" denotes that these instruments are used to perform obligations, exercise rights, or control assets on a distributed record (Szabo, 1996).

To clarify the difference between the information-technology phenomenon and the smart contract as a legal construct, some researchers suggest replacing the term "smart contract" with "smart legal contract," which more precisely indicates how associated legal contracts can be expressed and performed through software (Allen & Hunn, 2022).

The computer code constituting the basis of the smart contract is therefore essentially an infrastructure for contract formation and performance, much like a vending machine, a website, or an application that enables a user to accept contractual terms is an infrastructure (Surden, 2012).

The use of the term "smart" reflects the fact that smart contract code ensures that certain elements are executed automatically and in accordance with predefined conditions. A (legal) smart contract can, in practice, verify whether specific conditions have occurred and, if so, trigger a predefined action (Clack et al., 2017).

Accordingly, a smart contract in the legal sense—or a smart legal contract—is a contractual agreement that is structured and performed through IT code. Such an agreement entails the creation of legal obligations for the parties. Once the agreement is encoded and deployed, algorithms secure the performance of promises, unless judicial protection is invoked (Werbach & Cornell, 2017).

Therefore, while smart contracts are not automatically of legal significance merely because of their technical design, they do not operate in a legal vacuum. Where legal acts are concerned, law will ordinarily apply (Jones, 2019).

Ultimately, in such cases, the term can be understood in the manner originally proposed by Nick Szabo, which emphasizes the enhanced functionality of smart contracts relative to non-coded contracting without departing from legal analysis. On this view, smart contracts are "a set of promises, specified in digital form, including protocols within which the parties perform on these promises" (Szabo, 1996). The "smart" element does not imply that the use of artificial intelligence is required.

Similarly, other researchers have emphasized that smart contracts (a) are not merely digital contracts—many of which still depend on trusted authorities to achieve consensus and enforce outcomes—(b) do not entail artificial intelligence, regardless of what their name may suggest, and (c) do not "think" in the way a lawyer or an AI system might; rather, they automatically execute the lines of computer code for which they were programmed (Surden, 2012).

In light of the foregoing, a smart contract may be defined as an automated mechanism that performs its specified functions once particular predefined conditions are satisfied (Clack et al., 2017).

Legally, this constitutes the digital codification of a contract or parts of it. Its legal assessment therefore depends on the law applicable to the contract (Jones, 2019).

Although most smart contracts are also prepared in written or electronic form in natural language, the conclusion of the contract and its digital representation in a smart contract may occur simultaneously (Werbach & Cornell, 2017).

In this book, the analysis focuses on the smart contract from a legal perspective, addressing questions concerning the institution and the applicable contractual regulation.

For an agreement to be treated as legally binding and enforceable under common law, four basic elements are generally required: (1) offer, (2) acceptance, (3) consideration (exchange of value), and (4) the parties' intention to create legal relations. The legal system adopts a broad approach in this respect and treats any promise—regardless of form—as enforceable where these elements are satisfied and where factors such as duress or fraud have not vitiated consent (Jones, 2019).

From a practical standpoint, a contract is formed when the parties reach an agreement concerning the performance of future obligations, thereby creating rights and duties for all parties (Cutts, 2019).

One contested question in legal scholarship is whether smart contracts enjoy the same legal validity as traditional contracts. Although this question calls for a definitive and authoritative answer, it has in practice become a persistent point of debate among academics and practitioners.

Some researchers have attempted to overstate the power and status of smart contracts. For example, Savelyev advances a radical view that "smart contracts do not need a legal system to exist; rather, they can function without any overarching legal framework. In other words, on Savelyev's view, they constitute a technological substitute for the legal system as a whole" (Savelyev, 2017).

By contrast, some legal practitioners have expressed concern regarding the legal status of smart contracts because, unlike traditional contracts, they are not created through natural language but through computer data and encoded rules (Harley, 2017).

While this concern is understandable, this article supports the view that smart contracts should enjoy legal validity equivalent to traditional contracts, because "the data-oriented label simply indicates that the parties have agreed that part of the key contractual terms will be expressed in a form that is computer-processable" (Surden, 2012).

This argument is coherent because "from oral agreements to email correspondence, where the essential elements of contract are satisfied, all such arrangements may qualify as contracts in law" (Sklaroff, 2017).

The prevailing view rests on the assumption that the purpose of a traditional contract is to alter the rights and obligations of the parties. On this basis, smart contracts should be treated as contracts like any other, because they likewise operate as voluntary mechanisms for changing parties' rights and duties (Werbach & Cornell, 2017).

A legal statement by the UK Jurisdiction Taskforce further supports this position, arguing that smart contracts can be legally binding where they satisfy the common-law requirements for contract formation (Jones, 2019).

Sir Geoffrey Vos, a senior judge in the UK legal system, has stated that "a smart contract can be identified, interpreted, and enforced by applying established and orthodox principles of common law" (Vos, 2019). Despite the importance of this statement, it appears that a substantial part of the relevant legal literature has not sufficiently emphasized its status and implications. Some authors have treated this view merely as a theoretical comment lacking official authority, rather than as a persuasive legal interpretation.

A careful assessment of this position requires attention to the issuing body. The statement was published under the auspices of a UK legal taskforce comprising leading legal experts, government representatives, and senior members of the UK judiciary. This expert composition confers particular legal weight upon the statement, even if it is not formally binding.

The practical importance of this statement was also highlighted in the judgment of the High Court of England and Wales in AA v Persons Unknown (2019). In that case, Bryan J observed that the judicial members participating in the taskforce did not draft the statement in an official judicial capacity nor with the intention of issuing a binding decision, but acknowledged that the reasoning and conclusions articulated in it played an important role in shaping the court's judgment. This indicates that, while the statement lacks binding legal effect, it exerts significant influence as a matter of legal persuasion and its capacity to shape judicial reasoning.

Overall, it may be concluded that Sir Geoffrey Vos's position, and its implicit recognition in recent judicial reasoning, reflects a growing common-law tendency to accept and integrate smart contracts within the traditional framework of contract-law principles. At the same time, this trajectory will require continued theoretical engagement and the practical development of legal frameworks in this area.

However, the legal validity of smart contracts raises an additional layer of complexity that warrants closer attention. Unless smart contracts are recognized internationally, their performance may disrupt the application of private international law (Janssen & Durovic, 2018). Across legal systems, the requirements for contract formation differ; for example, a key distinction between civil-law and common-law systems is that common law requires "consideration" for an enforceable contract.

Accordingly, the legal validity of a smart contract depends on the extent to which the relevant jurisdiction is prepared to recognize and enforce it. This presents a major practical challenge because smart contracts are deployed on blockchain infrastructure that does not inherently recognize geographical borders. For that reason, the absence of coordinated international efforts toward legal recognition may prove problematic. In particular, it is difficult to predict what will occur in a private-international-law dispute if one jurisdiction treats a smart contract as lawful while another does not. Nevertheless, this should not prevent the conclusion that smart contracts ought to be accepted as legally binding contracts. It is therefore necessary to identify the characteristics that enable smart contracts to substitute for the traditional functions of contracts.

The inflexible nature of smart contracts must also be acknowledged. Smart contract code lacks certain essential human features that may impede parties' willingness to trust this form of contracting. Murray observed that smart contracts "seek to remove human elements such as contextualization and perhaps even empathy or a notion of 'justice' from interpretation and performance" (Murray, 2019). Machines cannot cultivate empathy, fairness, or justice; without such features, parties may refuse to engage in smart-contract arrangements. The force of law lies in judicial power to apply flexible legal standards while also considering surrounding circumstances such as the parties' situation and relationship. By contrast, machines are not equipped for such assessments because they are "rigid, determinate, and insulated from their commercial context" (Mik, 2017).

Similarly, machine learning has not yet reached a stage where it can reliably understand and apply natural language, remaining constrained to executing code. This limitation prompted Clack and colleagues to question whether smart contracts can address situations in which the parties have different understandings of the agreed terms (Clack et al., 2017). Where the meaning of a contractual term cannot be comprehended and the code is executed strictly, the smart contract's output may be undesirable because it "may differ from the parties' intentions" (Raskin, 2017). This inefficiency becomes more visible where the smart contract code is not written by the parties themselves. Mik, for example, argued that the coder may be unable to faithfully capture the parties' intentions, while the parties—who are not computer programmers—will be unable to review the code on their own (Mik, 2017).

As a result, machines will execute a smart contract even when the outcome is not desirable. Courts, by contrast, can evaluate the parties' intentions through legal knowledge and experience—something machines cannot do. This inevitably supports the view that smart contracts are inflexible self-executing instruments, whereas traditional contracts are more flexible (Janssen & Durovic, 2018).

This leads logically to the conclusion that opting for smart contracts requires "a trade-off between precision and certainty on the one hand, and ambiguity and flexibility on the other" (Mik, 2017). However, that trade-off is arguably unhelpful if one reflects further on the rigidity of smart contracts. Mik correctly acknowledged that "removing human judgment and automating choice may easily lead to a situation in which the contracting parties effectively lose the ability to choose whether and how to exercise their rights" (Mik, 2017). Parties to smart contracts may find themselves bound to an arrangement that does not generate the rights they intended. If parties take these concerns seriously when deciding whether to adopt smart contracts, they may revert to traditional contracting. Overall, this reinforces the conclusion that traditional methods have not been displaced by the emergence of smart contracts.

3. Smart Contracts in Metaverses

Smart contracts are digital arrangements that can be written in a blockchain structure using "if this, then that" code. These contracts refer to conditions that have been jointly defined in advance by the participants of a network, and once those conditions are satisfied, they are executed automatically. After deployment, the contracts require no further management unless the underlying conditions change. Accordingly, smart contracts can automate processes and eliminate intermediaries; once defined, there is no longer a need for direct negotiations over performance (Vo et al., 2021).

One potential application of smart contracts in metaverses is fundraising and project management. A proposed ecosystem integrating smart contracts enables stakeholders to participate in a project and monitor its progress. When a stakeholder contributes to a project via a smart contract, the stakeholder may track progress through a digital twin within the relevant metaverse environment. To access that metaverse, participants must prepare the required token and may do so through technologies such as augmented reality, virtual reality, or three-dimensional graphical spaces similar to computer games. Project progress updates are collected from IoT-based devices, BIM, and AI networks, all of which are integrated through a unified software interface and ultimately modeled (Moradi, 2022).

Multiple concepts have been proposed for integrating smart contracts into metaverses. Through smart contracts, "a novel blockchain-based framework for metaverse applications" can effectively manage and automate complex interactions between metaverse service providers and metaverse users. In particular, by virtue of smart-contract mechanisms, blockchain can manage and automate complex interactions among different entities in the metaverse, including interactions among service providers, users, and digital content creators (Nguyen et al., 2022). Meta-governance rules are executed automatically by smart contracts in "virtual companies and cities that operate in parallel with real companies and cities," and depending on operational outcomes, these governance rules are continuously adjusted to achieve the expected effect (Oppenlaender, 2022).

In practice, only a limited number of real-world use cases of smart contracts currently exist. Decentraland is a blockchain-based virtual world in which users can purchase, own, and develop parcels of digital land represented as non-fungible tokens on the Ethereum blockchain. Smart contracts enable decentralized governance on the platform and allow users to make collective decisions regarding its development and management. These contracts play a critical role in implementing community voting outcomes and ensuring that governance processes in the virtual world are transparent, tamper-resistant, and decentralized (Oppenlaender, 2022). They provide a trust-minimized mechanism through which users can collectively shape the development and management of the metaverse. In Decentraland, smart contracts also record ownership of valuable assets such as virtual land parcels and NFTs, producing an immutable and auditable ledger of property rights (Dowling, 2022). This function strengthens the security and authenticity of digital assets, which is essential in virtual environments where ownership and scarcity are foundational.

The CUHKSZ metaverse illustrates a broader deployment of smart contracts, using this technology to support core components of its ecosystem, including tokens, decentralized autonomous organizations, and its commercial system (Duan et al., 2021). Smart contracts here not only facilitate asset management but also enable the automation of complex interactions, thereby creating a more self-sustaining virtual environment. It can be observed that, to date, smart contracts have been used predominantly for governance and background operational functions in metaverses.

4. Smart Contracts in Light of Contract Law

"Smart contract" is a potentially misleading term. The term is used in connection with legally relevant contractual arrangements. When Nick Szabo theorized embedding contractual clauses in hardware and software "in such a way that breach becomes expensive," he spoke of "smart contracts" (Szabo, 1996). With the emergence of blockchain technology, this idea became practically implementable (Xu et al., 2019). Initially, blockchain technology was developed to exchange virtual currencies, and it then enabled the registration of digital assets more generally. More advanced blockchain applications allow deterministic computer programs to be deployed and executed automatically in accordance with predefined conditions (Xu et al., 2019). Blockchain technology therefore also enables the performance of contractual arrangements, and for this reason the relevant capability is commonly referred to as "smart contracts" (Mik, 2017).

Smart contracts are not necessarily contracts. A smart contract, in itself, is computer code that is capable of self-execution upon the occurrence of a specified condition. That code can be stored and processed on a blockchain, and any change to it is recorded on the blockchain (Earls et al., 2018). In theory, smart contracts can automate a wide range of actions. For example, a smart thermostat that adjusts the temperature inside a house according to predefined settings can be described as a smart contract. In such cases, smart contracts have no legal significance. They acquire legal meaning when they are used to automate actions or operations connected to legal rights. For example, a smart contract might issue an administrative license automatically once all licensing conditions are satisfied.

When smart contracts are used in the domain of contract law, some have suggested speaking instead of "smart legal contracts." Researchers commonly distinguish between smart legal contracts as contracts themselves and smart legal contracts as tools for performing existing agreements (Bomprezzi, 2020). The latter refers to using computer code to automate the performance of an agreement (in whole or in part) that is formed outside the blockchain, regardless of how that agreement was reached (Savelyev, 2017). Under this view, the smart contract is not the contract; rather, it is the instrument through which a contract is performed, and automated performance substitutes for performance by the obligor. The former view concerns whether an agreement can be expressed as lines of code and, in that case, whether smart legal contracts can constitute contracts (Werbach & Cornell, 2017). To answer this question, one must begin from the legal definition of contract (Bomprezzi, 2020).

A contract is a legally binding agreement between two or more parties (Bomprezzi, 2020). Accordingly, agreement is the core foundation of contract. Mutual assent is reached through the exchange of an offer and acceptance. Another essential requirement is the parties' intention for the contract to be legally binding, meaning that the offeror and offeree intended to enter into an agreement capable of producing legal effects within a legal system.

To achieve a "meeting of the minds" (offer and acceptance), both parties must manifest their intention in some manner. Under the principle of informality, absent mandatory form requirements, the parties are generally free to choose the form by which to conclude a contract. This principle supports concluding contracts electronically. A related international principle often invoked in this area is non-discrimination, meaning that legal effect should not be denied solely because the communication is in electronic form. Accordingly, contracts may also be expressed through computer code.

However, creating a smart legal contract does not automatically mean a contract has been concluded in the absence of a legally binding agreement. Therefore, smart legal contracts can be considered contracts only where a legally binding agreement exists. As noted in the literature, the fact that a smart contract is stored on a blockchain should not, by itself, be treated as proof of a party's consent to enter into a contract, because any person can deploy a smart contract to a blockchain in a way that purports to create obligations for arbitrary wallet holders (Waltl et al., 2018).

A meeting of the minds (offer and acceptance) can occur in various ways. Durovic and Janssen emphasize that smart legal contracts may be concluded either off-chain or on-chain (Durovic & Janssen, 2018). They explain the formation of on-chain contracts by reference to uploading a proposed contract in code language to a platform such as Ethereum and acceptance by a network participant who interacts with the deployed smart contract (for example, by making payment in Ether). In other words, a smart legal contract is formed on-chain when smart contract code is deployed to the blockchain, but only becomes an agreement when there is assent to its terms. Here, the smart contract together with the blockchain functions as the medium through which a user expresses contractual intent. If the intent of the user who deployed the smart contract corresponds with the intent of another user, a contract is formed and the smart contract becomes a smart legal contract. On-chain formation is especially significant because blockchain is a novel technology. In fact, smart contracts without blockchain have existed for years (Durovic & Janssen, 2018).

The following sections examine the relationship between contractual requirements and the formation of blockchain-based smart contracts. The aim of this analysis is to assess how rules of contract formation can be interpreted so that blockchain-based smart contracts can be situated within the framework of contract law.

5. Legal Challenges in Interpreting Smart Contracts

Despite the extensive potential of smart contracts, there are significant legal challenges in interpreting and enforcing them. One of the major challenges is determining the relevant conditions and how they are implemented. Unlike traditional contracts, which are typically drafted in human-readable legal language, smart contracts are executed as digital code that may be complex and difficult for non-specialists to understand. This can make accurate interpretation and correct performance challenging in some cases. In addition, when the parties require contextual interpretation or modifications to the agreed terms, legal problems arise because digital code executes automatically and lacks flexibility for revision or adjustment once deployed.

Moreover, because smart contracts rely on technologies such as blockchain, questions concerning transparency and responsibility also arise. For example, if a smart contract contains an execution error or is implemented incorrectly, identifying responsibility and providing remedies may be difficult because there is no central authority supervising these transactions (Green, 2018).

Smart contracts, as an innovation at the intersection of technology and law, despite their multiple advantages, face significant legal challenges that require careful attention and alignment with existing legal frameworks. These challenges typically arise in relation to interpretation, transparency, responsibility, legal validity, and dispute resolution. The following addresses some of the most important legal challenges in interpreting smart contracts:

5.1. Uncertainty of Legal Concepts in Programming Code

Smart contracts are commonly written as programming code that executes automatically based on specified conditions. However, one of the major challenges in interpreting these instruments is that many legal concepts present in traditional contracts (such as “acceptance,” “agreement,” “assignment,” “special conditions,” and similar constructs) are not defined in programming code in a simple or transparent manner. For example, standards such as “reasonable delay” or “reasonable measures” may be included in code, yet such concepts are difficult to operationalize in a deterministic execution environment and may lead to incorrect interpretation or misunderstanding in practice (Green, 2018).

5.2. The Need for Human Interpretation and Decision-Making in Complex Situations

Although smart contracts are executed automatically on the basis of algorithms, situations involving ambiguity or complexity in contractual conditions require human interpretation and legal assessment. For example, if one party claims that the contractual conditions should be interpreted differently from what is encoded in the software, dispute resolution will necessitate legal evaluation and careful interpretation of the contract. In traditional contracts, such interpretation is typically carried out by courts or judicial authorities; however, in the context of smart contracts, the absence of comparable institutional structures may generate serious challenges (Tapscott & Tapscott, 2016).

5.3. Liability and Damages Arising from Faulty Execution

Another major legal challenge concerns liability and damages resulting from faulty execution or defects in smart contracts. If the code governing the execution of a smart contract contains errors or flaws—for instance, if an algorithm has been incorrectly programmed or a particular condition has been improperly evaluated—the contracting parties may encounter legal difficulties in seeking compensation for resulting losses. In such cases, the critical question is who bears responsibility for these errors: the programmer, the platform developer, or the contracting parties themselves? Moreover, because smart contracts are executed automatically, there is typically no opportunity to revise or amend the contractual terms during performance, which can give rise to serious legal problems (Green, 2018).

5.4. The Judiciary and Incompatibility with Traditional Legal Systems

One of the most significant challenges associated with smart contracts is their compatibility with traditional legal systems. In many jurisdictions, contracts must comply with specific legal requirements in order to be considered valid and enforceable. Given that smart contracts are generally executed automatically and, in most cases, without human intervention, judicial systems may find it difficult to assess their conformity with existing legal rules. In addition, judicial and legal institutions may face substantial obstacles in identifying and interpreting the terms of smart contracts, as these instruments rely primarily on programming code rather than human-readable legal language (Tapscott & Tapscott, 2016).

5.5. Privacy and Security

Another serious concern in the interpretation and implementation of smart contracts relates to privacy and data security. The information and data recorded and stored within smart contracts may contain sensitive details, potentially posing threats to the privacy of the contracting parties. Furthermore, the security of programming code and the blockchains on which smart contracts are executed represents a major issue. If such code is subject to cyberattacks or unauthorized interference, this may result in the destruction or alteration of contractual conditions, leading to complex legal consequences.

5.6. Issues Related to International Enforcement

In international transactions involving smart contracts, legal challenges may include questions of jurisdiction and compliance with the laws of different countries. Because smart contracts operate in a digital environment and are not overseen by any specific judicial or legal authority, determining which legal system has jurisdiction over disputes arising from such contracts can be difficult. In addition, national laws governing digital contracts and blockchain technology may vary considerably, creating further complications in the interpretation and enforcement of smart contracts across borders (Green, 2018).

In sum, although smart contracts have been introduced as an innovative mechanism for automating and facilitating contractual relationships, their code-based nature and reliance on blockchain technology expose them to significant legal challenges. The divergence between programming language and legal language, difficulties in interpreting legal concepts, the lack of flexibility in modifying contractual terms, uncertainty in allocating responsibility when errors occur, incompatibility with traditional legal systems, concerns regarding security and privacy, and the complexities associated with international enforcement all indicate that the use of smart contracts still requires clear legal frameworks, precise rules, and standardized mechanisms for dispute resolution. Accordingly, despite their considerable potential, the full development and acceptance of smart contracts remain contingent upon the alignment of law and technology and the establishment of appropriate legal infrastructures.

6. Conclusion

The transformations brought about by blockchain technology and smart contracts have fundamentally reshaped the traditional landscape of contractual relationships. By introducing mechanisms based on automation, transparency, the elimination of intermediaries, and the reduction of transaction costs, smart contracts have opened new horizons for digital interactions—particularly within the metaverse, where a new ecosystem of economic, social, and legal relations is emerging. Nevertheless, the analysis conducted in this study demonstrates that technological advancement alone, without the parallel adaptation and support of legal systems, cannot fully ensure the effective functioning of smart contracts.

First, the code-based nature of smart contracts means that many core concepts of contract law—such as the parties' mutual intent, good faith, flexibility, and the possibility of adjusting contractual terms—are either difficult to represent in code or subject to significant limitations. This misalignment between technical language and legal language increases the likelihood of disputes and complicates contractual interpretation. Second, the absence of mechanisms to modify or suspend the automatic execution of smart contracts, particularly in cases of algorithmic errors or changing circumstances of the parties, poses a serious challenge to ensuring contractual fairness and efficiency. In this context, the allocation of liability in the event of faulty execution—whether to programmers, platforms, or contracting parties—has emerged as one of the most contentious legal issues.

From the perspective of legal systems, it is evident that existing traditional frameworks are not yet fully equipped to address the technical and substantive characteristics of smart contracts. The lack of comprehensive national and international regulations, the limited development of judicial practice, and the absence of coordination among different legal systems constitute major obstacles to the cross-border enforcement of such contracts. Moreover, security concerns and privacy issues further underscore the need to rethink both technical and legal standards for data protection.

Despite these challenges, smart contracts possess significant potential to become a central component of many future digital interactions. Realizing this potential requires legal systems to recognize and accommodate this technology by developing adaptive foundations and establishing clear, standardized, and enforceable rules. Moving toward the development of "hybrid contract" models—where legal language and programming code operate alongside one another—may represent an important step in bridging the gap between law and technology.

Ultimately, smart contracts should be understood neither as a complete replacement for traditional contracts nor as purely technological tools. Rather, they represent a point of convergence between law and technology, and their success depends on achieving a balance between algorithmic precision and judicial flexibility. The future of smart contracts rests on constructive collaboration among legal scholars, technology experts, and legislative institutions—a collaboration that, if properly managed, has the potential to usher legal systems into a new era of efficiency, transparency, and justice.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all who helped us through this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

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

References

Allen, J. G., & Hunn, P. (2022). *Smart Legal Contracts: Computable Law in Theory and Practice*. Oxford University Press.

Bomprezzi, C. (2020). A Legal Analysis of the Use of Blockchain Technology for the Formation of Smart Legal Contracts. *MediaLaws*(2), 111-130. https://www.medialaws.eu/wp-content/uploads/2020/07/RDM_2_2020-Finocchiaro.pdf

Catchlove, P. (2018). Smart Contracts: A New Era of Contract Use. *Journal of International Law and Technology*, *2*(1), 2.

Cenkus, L. (2018). Smart Contracts Explained: What They Are and Are They Legally Binding? https://cenkuslaw.com/smart-contracts-explained-legally-binding

Clack, C. D., Bakshi, V. A., & Braine, L. (2017). *Smart Contract Templates: Foundations, Design Landscape and Research Directions*. https://arxiv.org/pdf/1608.00771.pdf

Cutts, T. (2019). Smart Contracts and Consumers. *West Virginia Law Review*, *122*(2), 389-446. https://researchrepository.wvu.edu/wvlr/vol122/iss2/4

de Caria, R. (2019). Definitions of Smart Contracts. In L. A. DiMatteo, M. Cannarsa, & C. Poncibò (Eds.), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (pp. 19-36). Cambridge University Press. https://doi.org/10.1017/9781108592239.002

Dewey, J., & Amuial, S. (2015). What Is a Smart Contract? *Big Law Business*. https://bol.bna.com/what-is-a-smart-contract

Dizaji, A., & Dizaji, A. (2023). Metaverse and Its Legal Challenges. *Synesis*, *15*(1). https://seer.ucp.br/seer/index.php/synesis/article/download/2395/3402/9899

Dowling, M. (2022). Fertile LAND: Pricing Non-Fungible Tokens. *Finance Research Letters*, *44*, 102096. https://doi.org/10.1016/j.frl.2021.102096

Duan, Y., Yang, Y., & Liu, Y. (2021). Blockchain Technology in the Metaverse: Current Status and Future Opportunities. *Computer Networks*, *201*, 108-121.

Durovic, M., & Janssen, A. (2018). The Formation of Blockchain-Based Smart Contracts in the Light of Contract Law. *European Review of Private Law*, *26*(6), 753-772. https://doi.org/10.54648/ERPL2018053

Earls, J., Smith, M., & Smith, R. (2018). *Smart Contracts: Is the Law Ready?* (Smart Contracts Alliance, Chamber of Digital Commerce, Issue. https://lowellmilkeninstitute.law.ucla.edu/wp-content/uploads/2018/08/Smart-Contracts-Whitepaper.pdf

Goldenfein, J., & Leiter, A. (2018). Legal Engineering on the Blockchain: 'Smart Contracts' as Legal Conduct. *SSRN*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3176363

Green, S. (2018). It's Virtually Money. In S. Green & D. Fox (Eds.), *The Private Law Implications of Virtual Currencies*. Oxford University Press.

Harley, B. (2017). Are Smart Contracts Contracts? *Clifford Chance*. https://www.cliffordchance.com/briefings/2017/08/are_smart_contractscontracts.html

International Monetary, F. (2016). *Virtual Currencies and Beyond: Initial Considerations* [SDN/16/03](IMF Staff Discussion Note, Issue.

International, S., Derivatives, A., & Linklaters. (2017). *Whitepaper: Smart Contracts and Distributed Ledger – A Legal Perspective*.

Jaccard, G. (2018). Smart Contracts and the Role of Law. *Law and Technology Review*, *10*.

Janssen, A., & Durovic, M. (2018). Smart Contracts and the Regulation of Blockchain. *Journal of International Commercial Law and Technology*, *13*(2), 139-156.

Jones, L. (2019). *Introduction to Business Law* (5 ed.). Oxford University Press.

Madir, J. (2020). *FinTech: Law and Regulation*.

Micheler, E. (2015). Custody Chains and Asset Values: Why Crypto-Securities Are Worth Contemplating. *Cambridge Law Journal*, 505.

Mik, E. (2017). The Limitations of Smart Contracts: Flexibility and Judicial Intervention. *Journal of Law and Technology*, *15*(3), 101-115.

Moradi, A. (2022). *Metaverse Ubi Es? A Transaction Cost-Based Analysis of the State of the Art of Smart Contracts in the Metaverse*.

Murray, A. (2019). *Information Technology Law* (4 ed.). Oxford University Press.

Nejat-Zadegan, S. (2022). Smart Contracts (Concept, Elements, Features, and Functions). *Vekalat Dakhel Quarterly*, 32-51.

Nguyen, C. T., Hoang, D. T., Nguyen, D. N., & Dutkiewicz, E. (2022, 2022/06). MetaChain: A Novel Blockchain-Based Framework for Metaverse Applications. Proceedings of the 2022 IEEE 95th Vehicular Technology Conference (VTC2022-Spring),

Oppenlaender, J. (2022). The Perception of Smart Contracts for Governance of the Metaverse. Proceedings of the 25th International Academic Mindtrek Conference, https://doi.org/10.1145/3569219.3569300

Rabbani Mousavian, A. (2021). Rules Governing Smart Contracts in Imami Jurisprudence and Positive Law. *Islamic Jurisprudence and Law Research Quarterly*, *18*(66), 178-204.

Raskin, M. (2017). DAO and the Rise of Decentralized Autonomous Organizations. *Georgetown Law Technology Review*, *1*(1), 304-323.

Savelyev, A. (2017). *Contract Law 2.0: "Smart" Contracts as the Beginning of the End of Classic Contract Law* [WP BRP 71/LAW/2016](Higher School of Economics Working Paper, Issue.

Scheinert, C. (2016). *Virtual Currencies: Challenges Following Their Introduction* [PE 579.110](European Parliamentary Research Service, Issue. https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf

Sklaroff, J. M. (2017). Smart Contracts and the Cost of Inflexibility. *University of Pennsylvania Law Review*, *166*(1), 263-303.

Surden, H. (2012). Computable Contracts. *UC Davis Law Review*, *46*, 629-679. https://logic.stanford.edu/complaw/readings/computable_contracts.pdf

Szabo, N. (1996). Smart Contracts: Building Blocks for Digital Markets. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution*. Penguin.

Tasca, P. (2015). *Digital Currencies: Principles, Trends, Opportunities, and Risks* (ECUREX Research Working Paper, Issue.

Vo, A. T., Vo, K. T., Ha, Q. M., & Nguyen, D. C. (2021). Theoretical Background and Hypotheses Development on Smart Contracts and Distributed Ledger Technologies in Supply Chain Networks. *Operations Management Research*.

Vos, G. (2019). *Future Proofing for Commercial Lawyers in an Unpredictable World* (Annual COMBAR Lecture 2019, The Commercial Bar Association, Issue. https://www.judiciary.uk/wp-content/uploads/2019/11/COMBAR.lecture2019.final_.pdf

Waltl, B., Sillaber, C., Gallersdörfer, U., & Matthes, F. (2018). Blockchains and Smart Contracts: A Threat for the Legal Industry? In M. Janssen, Y. Charalabidis, & A. Zuiderwijk (Eds.), *Business Transformation through Blockchain: A Global Perspective* (pp. 287-315). Springer International Publishing. https://doi.org/10.1007/978-3-319-99058-3_11

Werbach, K., & Cornell, N. (2017). Contracts Ex Machina. *Duke Law Journal*, *67*(2), 313-382. https://scholarship.law.duke.edu/dlj/vol67/iss2/2

Xu, X., Weber, I., & Staples, M. (2019). *Architecture for Blockchain Applications*. Springer Cham. https://doi.org/10.1007/978-3-030-03035-3