

New Principles of Contracting in the Digital Sphere

Homci Miloud

Université Echahid Hamma Lakhdar d'Eloued

homci20@gmail.com

Bouaroudj khaoula

Université frères mentouri Constantine 1

khaoula.bouaroudj@umc.edu.dz

Received: 08/02/2026 Accepted: 13/04/2026 Published: 02/06/2026

Abstract

Contracts undergo various changes at the different stages through which they pass as a result of developments taking place around the world. Given the significant impact of technology on contracting, new contracts have emerged that are predominantly digital in their formation, creation and performance. However, it is not possible to enumerate all contracts associated with the digital sphere and those that use technology and electronic means.

Because digitalisation affects contracting, and as a result of the integration of technology with legislation, modern principles have emerged and been introduced into contracting. Contracting parties must therefore become familiar with these principles in order to ensure the proper completion of transactions, their confidentiality, and the integrity of the contracting process.

Keywords: Contract; digitisation; technology; artificial intelligence; encryption.

Introduction

Contracting today can no longer be adequately conducted through traditional methods or agreements confined by the limits of place and time. As the world moves rapidly towards the digital sphere, we find ourselves facing entirely new rules of the game, in which distances disappear and algorithms and artificial intelligence have become a third party in contemporary contracts. The challenge is no longer limited to drafting contractual clauses; it also extends to ensuring trust and security in a virtual environment whose features change every day.

The challenge is no longer confined to drafting clauses, but also concerns how trust and security can be ensured in a virtual environment whose features change daily.

This research paper does not examine digital contracts solely from the legal or technical perspective. Rather, it seeks to address the subject from the perspective of the use of contracts themselves, including the possibility of treating certain contracts as a system or programme, and the transformation that may result from this and affect contract formation, which combines law with the use of technology.

Accordingly, the importance of this research lies, first, in understanding these principles and, second, in identifying the contracts that possess a digital character. From this standpoint, we focus on the changing philosophy of legal obligations and on how the rights of contracting parties are regulated within this open digital space. In other words, we seek to understand these principles and identify the contracts characterised by their digital nature.

The digital age has imposed a new logic through which the philosophy of contracting has changed as a result of technology entering the contractual field. This has led to the emergence of digital contracts and prompts us to examine the subject through the following research problem:

Research problem: To what extent can the new principles strike a balance between digital contracts and the assurance of legal certainty for contracting parties through the new principles governing digital contracts?

To address this problem and divide the subject in a way that facilitates its study, we raise the following questions: What are digital contracts? Can these contracts incorporate modern principles?

To answer the research problem and the related questions, we adopt a descriptive and analytical approach to digital contracts, on the one hand, and to the modern principles introduced into these contracts, on the other. Accordingly, the study is organised into two sections. The first examines the principal contracts used in the digital sphere, while the second considers the principles that may have been introduced into contracting as a result of technological use.

Section One: Contracts Used in the Digital Sphere

The use of digitalisation in contracting is expanding across a wide range of contractual transactions. Contracts used in the digital sphere are therefore not a single type, but comprise different types. It is consequently necessary to examine the nature of these contracts and identify the principal differences between them.

First: The Nature of Digital Contracts

Digital contracts are characterised by their reliance on electronic means. This type of contract is performed, wholly or partially, through communication tools operating in the computer environment or through any device connected to the Internet, which provides access to the digital sphere.

Studying digital contracts highlights an important point: this type of contract cannot be exhaustively enumerated, because new types may emerge at any time. This is due to the rapid and unlimited development of technology and the possibility of integrating it into the legal sphere. Nevertheless, it is possible to discuss the

principal contracts that used digital technologies at the time this paper was written, some of which are listed below by way of example and not limitation.

1. Smart contracts

Smart contracts have emerged relatively recently through the use of technology to bring transactions closer together without requiring the contracting parties to travel or meet. A smart contract is a computer programme that automatically forms, performs or terminates a contract. It operates through what are known as algorithms and relies on blockchain technology. A series of events is programmed to trigger consequences as soon as precisely specified conditions and terms, represented by previously entered data, are met. The programmed action is then performed when the relevant event occurs. The initial condition of a smart contract may be the performance of another contract, and each event recorded on the network may trigger another event once a smart contract has been programmed for that purpose. The mechanism resembles a vending machine, which delivers a product after payment and returns any change. In this way, the transaction between the customer and the machine is completed. A smart contract is not limited to transactions with machines: it may operate between two natural persons or between a natural person and a legal person, such as a company, with a pre-programmed machine serving as the link between them. This is known as the use of electronic tools in contracting.

Smart contracts are particularly flexible. They can access a rich set of instructions and store digital assets, thereby providing a degree of security for contracting parties.

2. Electronic contracts

Electronic contracts are a form of contracting in which dealings take place electronically as an alternative to direct physical dealings.¹ In this type of contract, offer and acceptance meet through an international communications network by means of which data are exchanged electronically for the purpose of creating contractual obligations.² Offer and acceptance meet on the Internet through various means of communication that activate and facilitate contact between contracting parties. The Internet shortens distances and breaks down borders, making these contracts cross-border in nature.

3. Artificial-intelligence contracts

Some consider artificial-intelligence contracts to be contracts concluded between a human being and a programmed machine, which has the ability to perceive, understand and process information previously entered through sensors. Others consider artificial-intelligence contracts, which rely on computer systems, to be a simulation of human intelligence through the imitation of behaviour, patterns of thought and decision-making. It is a field specifically designed to perform tasks that human beings ordinarily perform.³

Artificial intelligence is no longer confined to particular fields; it has also entered the field of contracting. Electronic tools can be connected with various supporting means to enable parties to communicate conveniently, in addition to the programmes with which those tools must be equipped.

4. Cyber contracts

This type of contract is performed, wholly or partially, through communication tools in the computer environment. It may be completed entirely by email in the case of proposals or agreements that are not contentious. It may also be copied using computer-based communication tools or other means, such as fax records and conversations recorded on paper. Common technologies used to conduct business include commercial web pages and email messages.

Cyber contracts differ from cybersecurity. The latter refers to a set of basic tools, security concepts and mechanisms, guiding principles, risk-management methods, business and training practices, good practices,

safeguards and technologies that may be used to protect electronic communications against any event that could compromise the availability, integrity or confidentiality of stored, processed or transmitted data.

Cybersecurity is characterised by the use of a set of tools, policies, concepts, security mechanisms, guiding principles, risk-management methods, business and training practices, good practices, safeguards and technologies that can protect electronic communications against any event that could affect the availability, integrity or confidentiality of stored, processed or transmitted data.

1. Insaf Ayyoub Al-Momani, "Smart Contracts: Their Concept, Advantages and Elements," International Islamic Fiqh Academy Conference, 24th Session, Organisation of Islamic Cooperation, Dubai, 2019, p. 17.
2. Ahmed Rebahi, "The Legal Nature of the Electronic Contract," The Academy for Social and Human Studies, Algeria, vol. 5, no. 10, June 2013, p. 97.
3. Zainab Dawoud Makki, "The Legal Challenges of Smart Contracts in Light of Blockchain Technology," Journal of the University of Jordanian Olive Tree for Legal Studies, Jordan, vol. 6, issue 2, 2025, p. 46.

The digital contracts mentioned above do not represent all digital contracts, since only some have been discussed. Moreover, digital contracts are innumerable: new types of contracts using technology and electronic means may emerge at any time. Nevertheless, it is possible to highlight certain differences between digital contracts.

Second: Principal Differences between Certain Digital Contracts

To avoid confusion among the various digital contracts, contracts that rely on digitalisation, or, more precisely, contracts into which digitalisation has been introduced, we consider it useful to identify some differences between these contracts and traditional contracts, since traditional contracts form the foundation of contractual principles, as follows:

1. The relationship between digital contracts and traditional contracts

Smart contracts and traditional contracts share a reliance on traditional principles, which form the foundation of every contract. No contract can dispense with classical principles, since they constitute the basis of contracting. Nevertheless, certain differences may arise from the contract-formation stage. Before any contract is concluded, the parties to the contractual relationship must agree on a set of conditions relating to the programmes and tools used in the digital contract.

It is also necessary to agree on the type of contract so that the parties' intentions are directed towards the same contract. A digital contract itself does not appear until the programme is activated. The type of contract plays an important role in determining how offer and acceptance are exchanged and what the contractual terms will be.

The discussion does not end with identifying some differences between digital and traditional contracts; we will also clarify certain differences among digital contracts themselves.

2. Smart contracts and artificial-intelligence contracts

Artificial intelligence can propose contracts that require precision. Its capabilities may exceed those of a human being and those of a simple robot programmed to conclude a contract on specified terms. It offers proposals suited to requirements, suggests contracts compatible with the offers sought and available, and may improve them. It can examine terms that fit the requested outcome and ensure precision in the offer. In this way, it reinforces the importance of obligations between the parties and of contractual terms, and can express these matters clearly.¹

From a technical perspective, artificial intelligence is a computer system capable of making choices independently, rather than choices specified by the person who developed or uses it. Artificial intelligence may

also compete with the human mind in selecting a contract and can execute instructions with a high degree of professionalism and in a logical, systematic manner. It can provide statistical solutions from which the best and most beneficial outcome may be selected, assess each case individually, and offer multiple solutions based on different forms of reasoning, together with an assessment of the applicability of legal provisions.

Smart contracts, by contrast, reduce many problems and ensure that an application operates as expected, since the contract code is stored on the underlying blockchain and can therefore be publicly examined. Artificial intelligence enables the automated, direct and public processing of contractual terms. This can be done even when thousands of network participants are present simultaneously. It may ensure the legitimacy of execution when performance results in a change of state—for example, a change in account balances. Such a change is subject to the consensus rules of the blockchain network and is reflected and protected by the underlying blockchain state.²

Artificial intelligence also promotes a culture of digital contracting. It can contribute to contracting by providing a correct understanding of the wording used and a logical analysis of the intended transaction. Artificial intelligence may be particularly helpful to parties using computers through the applications it offers, especially in relation to trading and automated participation in the conclusion of contracts.

1. Jeremy (Achour), “Contract Formation and Artificial Intelligence in French and English Law,” research dissertation in law, Master 2 in Contracts in French and European Law, Faculty of Law and Social Sciences, University of Poitiers, France, 2020/2021, p. 40.

2. Fabian Schär, “Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets,” Federal Reserve Bank of St. Louis Review, second quarter 2021, 103(2), p. 154, available at <https://doi.org/10.20955/r.103.153-74>.

Those who generally advocate the use of artificial intelligence argue that artificial-intelligence contracts are optimal for improving contracts, owing to their algorithms, high-performance analytics and effective use of big data associated with the digital computing environment. These features are absent from the classical contracting process. The use of these different technologies therefore has a significant effect on improving contracts and warrants further study. Programming companies seek to maximise the number of contracts concluded, often by supporting the parties and securing contractual content.¹

Artificial intelligence has been imposed on the digital system as a result of the growing use of technology in numerous fields, including the integration of technology and law. It has consequently affected contracting, making scholarly intervention necessary to examine whether artificial intelligence can coexist with traditional contract theory. This would enable legislators to enact legislation that accommodates the effects of artificial intelligence on traditional contract theory.

3. Distinguishing smart contracts from electronic contracts

Electronic contracts and smart contracts are both digital contracts. From a legal perspective, however, electronic contracts have been regulated by legislation in several jurisdictions. One example is French Law No. 2004-575 of 21 June 2004 on confidence in the digital economy, commonly known as the LCEN (Loi pour la confiance dans l'économie numérique). This law has undergone several amendments, particularly following the reform of contract law by Ordinance No. 2016-131 of 10 February 2016.

The Egyptian legislature regulated electronic contracting under Law No. 15 of 2004 concerning electronic signatures and the establishment of the Information Technology Industry Development Agency, dated 21 April 2004.

1. Law No. 18/05 of 10 May 2018 on electronic commerce, Official Gazette of the People's Democratic Republic of Algeria, no. 28, dated 16 May 2018.

2. Law No. 15/04 of 1 February 2015, laying down general rules relating to electronic signatures and certification, Official Gazette, no. 6, dated 10 February 2015.

3. Insaf Ayyoub Al-Momani, *op. cit.*, p. 17.

4. Al-Arabi Belhaj, *Sources of Obligations in Algerian Civil Law: Voluntary Sources—Contract and Unilateral Will, Part One*, Dar Houma, Algeria, 2nd ed., 2015/2016, p. 145.

Like these jurisdictions, the Algerian legislature has regulated electronic transactions through Law No. 18/05 on electronic commerce.¹ Before that, it addressed the possibility of verifying the digital exchange of documents through Law No. 15/04 on electronic signatures and certification.²

In contrast, smart contracts have not been regulated independently by a specific statute in the way electronic contracts have. The issue goes further, to whether this type of contract is recognised in the first place. Provisions that touch upon the subject concern only particular aspects of certain laws, and regulation has largely focused on blockchain, a technological system based on a chain of blocks that is important to smart contracts and digital contracts generally.

Electronic contracts are a form of contracting in which dealings take place electronically rather than through direct physical interaction.³ The same applies to smart contracts: both are forms of digital contracting. However, smart contracts are not classified as named contracts in the same way as electronic contracts, which have been addressed in legislative provisions.

As regards performance, electronic contracts—particularly where physical means are required—need a third party or, more precisely, rely on a third party to deliver products between the contracting parties. Smart contracts, by contrast, dispense entirely with a third party because they are wholly self-executing. This makes them a distinctive category of digital contracts.

In legal classification, electronic contracts do not constitute an independent family of contracts governed by a separate set of legal rules; they rely on the general provisions of the general theory of contract.⁴ The same applies to smart contracts, which are also subject to the general rules of contract theory implemented through a digitalisation protocol. Neither therefore constitutes an independent family of contracts. It should be noted that certain legal provisions attempt to regulate aspects of electronic contracts, with the scope of regulation varying from one legal system to another.

Both types represent developments in contracting through the digital environment. Electronic contracts constitute a qualitative leap in contracting, but this development did not stop there: it continued along another path, leading to smart contracts through deeper reliance on electronic technology in contracting. Smart contracts rely on encryption through blockchain, which is not found in electronic contracts, and use computer language at every stage, including performance.

These contracts provide examples of certain forms of digital contracting. They are illustrative only, because it is impossible to cover every digital contract, and the boundaries of the category have not been precisely defined. This is due to the continuing development of digital technology, which may give rise to new forms of digital contracts. This remarkable technological development has itself led to the emergence of new principles beyond the traditional principles already known. These are the subject of the second section.

Section Two: Modern Principles of Digital Contracts

Digital contracts may naturally be subject to new principles as a result of electronic transactions, which have both influenced and been influenced by these contracts. In particular, the means used are not equal in terms of the technologies available or the degree of control over technology. New principles have therefore emerged, which we divide into two categories: first, principles of a technological nature; and second, principles of a protective and preventive nature.

First: Principles of a Technological Nature

Principles of a technological nature have emerged from the use of technology and the range of electronic tools that, together, help optimise digitalisation. When combined with contracting, they have produced new principles, which are set out below.

1. The principle of technological neutrality

This is a new principle that was not previously recognised by traditional contract theory. It emerged alongside the new technologies introduced into contracting. The principle is reflected in the legal equality of all forms and means of communication, applied in a neutral manner and interpreted and applied without favouring one method over another, whether in drafting or interpretation. The aim is to preserve data across different smart devices.

The principle of technological neutrality represents legal equality among different forms and means of communication. It is interpreted and applied without discrimination between different methods, whether in their drafting or interpretation. This principle should be reinforced through specific legislation confirming that documents have equal legal value, whether they are on paper or on technological media, for evidentiary and proof purposes.

Technological neutrality should apply at every stage of contracting; it is not sufficient to apply it at one stage while ignoring the others. Nevertheless, particular stages, such as electronic signature, may receive specific attention.

2. The principle of electronic security

Digital contracts require the use of electronic technologies and appropriate security techniques to protect transactions and consumers' personal data. Attention must be paid to ensuring the integrity and security of these digital operations.

Electronic security enables contracting parties to avoid digital risks arising from unexpected malicious attacks, which may be caused by malware and viruses that damage smart digital technologies and programmes.

Digital security also protects networks, safeguards devices and programmes, and establishes technological trust among users.

What strengthens trust among parties using electronic devices in their dealings is electronic security, which inspires confidence through proactive preventive measures. These measures can counter digital extortion through firewalls that isolate digital systems and programmes from damage, while providing adequate data protection and ensuring that information can be transferred, stored and retrieved in its original form, even in the event of damage.

3. Artificial-intelligence ethics as a modern principle

This is one of the most recent principles to accompany digitalisation and is closely linked to technology. In this context, UNESCO adopted its Recommendation on the Ethics of Artificial Intelligence on 23 November 2021. The Recommendation seeks to make AI ethics a normative instrument developed through a global approach based on international law and centred on human dignity and human rights, as well as gender equality, social and economic justice and development, physical and mental well-being, diversity, mutual dependence, and the reliance on, inclusion of and protection of the environment and ecosystems. It aims to provide important guidance for artificial-intelligence technologies.¹

The purpose of AI ethics is to create technology integrated with electronic tools and programmes that upholds values ordinarily associated with human beings, including gender equality, social and economic justice, and development. These values should be protected by international legislation and incorporated into technological

systems so that artificial intelligence is appropriately guided and its technologies are used responsibly and ethically.

1. Alexandra Bensamoun and Grégoire Loiseau, *Droit de l'intelligence artificielle*, 2nd ed., LGDJ, Lextenso, 2022, p. 19.

Second: Principles of a Protective and Technical Nature

Protective principles serve to impose prior oversight on programmes that may be used to organise contracting or electronic records, in order to preserve the information and data entered into them from damage. They constitute the first line of protection and prevent access to data by anyone who is not entitled to it. These principles include the following:

1. The use of electronic encryption

Encryption is a preventive process that may also be proactive. It is used to secure transactions and protect programmes against damage that may result from malicious software, as well as to remove such software before it causes information losses.

Electronic encryption is therefore a complex, varied and ongoing process intended to activate data-protection barriers against intrusion and security threats to digital programmes and devices.

Technically and practically, encryption is a branch of mathematics based on transforming data from an understandable form into symbols or signals that cannot be read or understood unless they are decrypted using decryption keys.²

From a technical perspective, encryption is a technique intended to alter content so that information does not leak and a message's contents are known only to the sender and recipient. In other words, it converts intelligible information into unintelligible information, which can be restored to its original state using the secret key with which it was encrypted. The aim is to preserve the confidentiality of information.¹

In terms of its use, encryption helps resist malicious software that may infiltrate systems and seize sensitive data or important records. Such interference may undermine the principle of equal opportunities and threaten the integrity of competitive processes.²

It is important to preserve data sustainability, protect it against breaches, and provide a secure digital environment capable of resisting malicious programmes that may destroy data stored in electronic programmes and devices.

1. Maryam Zan, "E-Commerce: Advantages and Risks," in the edited volume *Contracting in the Digital Space*, Arab Democratic Center for Strategic, Political and Economic Studies, Berlin, Germany, 2021, p. 132.

2. Fathallah Azzouz and Hassain Oumaria, "Cyber Challenges in Concluding Electronic Administrative Contracts," *Journal of Legal and Economic Studies*, vol. 8, no. 2, 2025, p. 756.

2. Cybersecurity

According to the European declaration, cybersecurity means "the ability of an information system to resist intrusion attempts or unexpected incidents targeting data".³ From another perspective, information security comprises a set of technical and administrative measures, including processes and mechanisms adopted to prevent unauthorised intervention for the purpose of espionage, intrusion or any improper use of electronic data held in a communications and information system.⁴

The United States Department of Defense, known as the Pentagon, has also considered cybersecurity to comprise all organisational measures necessary to ensure the protection of information in all its electronic and physical forms against various crimes, attacks, sabotage, espionage and incidents.¹

Some consider cybersecurity to be a set of tools, policies, security concepts, safeguards and guiding principles for addressing risks to information and its processing in order to protect the electronic environment.² It may also be understood as defensive means that enable hacking attempts to be detected and thwarted.³

The objective of cybersecurity is to protect against various cyberattacks intended to damage or disrupt the Internet through viruses or espionage attacks.⁴

1. Sebkhauoui Khaidja, "The Role of Cyber Security in Attaining the Sustainable Development Goals," *Review, Development and Human Resources Management*, vol. 11, issue 1, 2024, p. 614.

2. Samir Bara, "Cybersecurity in Algeria: Policies and Institutions," *Algerian Journal of Human Security*, University of Batna 1, Algeria, no. 4, 2017, p. 258.

3. Leila Ben Berghouth, *op. cit.*, p. 447.

4. Hatem Ben Azzouz and Halima Manani, "Cybersecurity and Cybercrime in Postmodern States: The United States of America as a Model," *Al-Risala Journal for Media Studies*, University of Tebessa, Algeria, vol. 6, no. 2, June 2022, p. 581.

3. Blockchain technology

Most digital contracts rely on blockchain technology, which is central to the development of these contracts, including, by way of example and not limitation, smart contracts.

Blockchain is a chain of blocks. It is a large decentralised database that processes a growing and continuous set of records known as a blockchain. Each block is an independent unit within the chain that transfers data between blocks. Work is completed within the chain through this repeated process, enabling it to perform the required tasks, such as recording data or transferring ownership or funds.⁵

Another view is that blockchain is a technology comprising records that preserve transactions in sequential blocks. New transactions are added to the chain, and each transaction represents a particular operation carried out on the network. From another perspective, the blockchain structure is a neutral structure that cannot be controlled. It provides transparency, trust and security by relying on an open ledger accessible to all participants, who can view changes. No change can be made without the approval of all relevant parties, which increases trust among users.¹

The Blockchain Institute in France considers blockchain to be a secure and transparent technology for transferring and storing information without a controlling authority.²

The distributed database used by blockchain protects transactions. The ledger cannot easily be breached and its information manipulated because the database is distributed rather than centralised in a single location. An attacker would have to compromise all participants simultaneously, making manipulation difficult and changes to transactions correspondingly difficult.³

In general, blockchain technologies are among the modern technological innovations that have brought about a fundamental change in methods of contracting and managing digital transactions. Given the importance of blockchain in digital contracts, as well as the principles discussed above that have entered contracting without prior warning or permission, legislative intervention has become necessary to regulate these technologies and other related principles.

1. Amal Marzouk, "Blockchain Technology and Its Economic Applications," *Middle East Journal of Humanities and Cultural Studies*, Jordan, vol. 1, no. 5, 2021, p. 331.

2. Zainab Dawoud Makki, *op. cit.*, p. 51.

3. Amal Marzouk, *op. cit.*, p. 331.

4. Zainab Dawoud Makki, *op. cit.*, p. 50.

5. Zainab Dawoud Makki, *op. cit.*, p. 50.

Conclusion

In conclusion, the purpose of using technology in contracts appears to be to accelerate their performance, keep pace with development, introduce modern means into contracting, reduce errors by limiting human intervention, and benefit from the ease with which information can be signed, stored automatically and preserved securely, thereby facilitating later retrieval.

It is also important to keep pace with rapid technological progress and the race towards digitalisation in various fields, including contracting.

Although it is necessary to adapt to digital development in transactions, contracts cannot abandon traditional principles, on which they depend. This does not prevent the emergence of other modern methods or principles of contracting that were unknown in classical contracting. These principles accompany technological development and result from the intervention of digital tools in contracting.

In our view, some aspects of these principles appear to be independent of the parties' will and instead arise from the digital, electronic and technological tools used, such as the principle of technological neutrality.

Through this research paper, we have reached a number of findings that have contributed to enriching a subject that continues to develop and remains open to research from several perspectives.

Findings

The principal findings of this research paper are as follows:

- The introduction and use of electronic means in contracting is inevitable and has been imposed by the requirements of contractual life.
- The introduction of new contractual principles leads contracting parties to seek legal or digital security for their transactions.
- Contracting through technological environments and electronic means gives contracts an unlimited, cross-border character, allowing them to extend beyond the boundaries of a single State.
- Questions arise as to whether parties can be held liable for causes originating in the technological environment, the electronic means used in transactions, or digital tools. This has prompted a modern scholarly debate about whether liability can be attributed to devices or electronic means. The issue arises because the parties to a transaction or contract may seek to avoid liability for consequences resulting from the electronic means used in contracting.

Recommendations

We have also reached a number of recommendations that we hope will improve contracting through digital means and the integration of technology into law:

- Introduce stricter penalties for anyone who attempts to manipulate electronic data or develop malicious programmes for spying on, changing, transferring or falsifying data.
- Because technology-based contracts cross national borders, international legislation should be developed to regulate these transactions within a unified framework.
- Establish a mechanism that ensures a balance between the use of electronic means and the stability of transactions between contracting parties, without causing harm.

List of Sources and References

Legislation

1. Law No. 15/04 of 1 February 2015, laying down general rules relating to electronic signatures and certification, Official Gazette of the People's Democratic Republic of Algeria, no. 6, dated 10 February 2015.

2. Law No. 18/05 of 10 May 2018 on electronic commerce, Official Gazette of the People's Democratic Republic of Algeria, no. 28, dated 16 May 2018.

Books

3. Al-Arabi Belhaj, *Sources of Obligations in Algerian Civil Law: Voluntary Sources—Contract and Unilateral Will*, Part One, Dar Houma, Algeria, 2nd ed., 2015/2016.

Scientific Articles

4. Ibrahim Khalil Khalifa Al-Balazi, "Cybersecurity: A Theoretical Reading of International Challenges and National Responses," *Academic Forum Journal (Humanities)*, Faculty of Sharia and Law, Ghat, Alasmarya Islamic University, Libya, vol. 9, no. 2, 2025, pp. 3053–3076.
5. Insaf Ayyoub Al-Momani, "Smart Contracts: Their Concept, Advantages and Elements," *International Islamic Fiqh Academy Conference, 24th Session, Organisation of Islamic Cooperation, Dubai*, 2019.
6. Samir Bara, "Cybersecurity in Algeria: Policies and Institutions," *Algerian Journal of Human Security*, University of Batna 1, Algeria, no. 4, 2017, pp. 255–280.
7. Hatem Ben Azzouz and Halima Manani, "Cybersecurity and Cybercrime in Postmodern States: The United States of America as a Model," *Al-Risala Journal for Media Studies*, University of Tebessa, Algeria, vol. 6, no. 2, June 2022, pp. 580–589.
8. Ahmed Rebahi, "The Legal Nature of the Electronic Contract," *The Academy for Social and Human Studies*, Algeria, vol. 5, no. 10, June 2013, pp. 96–105.
9. Zainab Dawoud Makki, "The Legal Challenges of Smart Contracts in Light of Blockchain Technology," *Journal of the University of Jordanian Olive Tree for Legal Studies*, Jordan, vol. 6, issue 2, 2025, pp. 36–59.
10. Amiroche Abane, "The Legal Regulation of Encryption as a Mechanism for Electronic Certification in Algerian and Comparative Legislation," *Journal of the Research Professor for Legal and Political Studies*, Faculty of Law and Political Science, University of M'sila, Algeria, vol. 7, no. 1, 2022, pp. 1234–1249.
11. Fathallah Azzouz and Hassain Oumaria, "Cyber Challenges in Concluding Electronic Administrative Contracts," *Journal of Legal and Economic Studies*, vol. 8, no. 2, 2025, pp. 759–773.
12. Leila Ben Berghouth, "Cybersecurity and the Protection of Digital Data Privacy in Algeria in the Age of Digital Transformation and Artificial Intelligence: Threats, Technologies, Challenges and Response Mechanisms," *International Journal of Social Communication*, Abdelhamid Ibn Badis University, Mostaganem, Algeria, vol. 10, no. 1, 2023, pp. 443–457.
13. Mohamed Yahya Ahmed Attia, "Smart Arbitration as a Mechanism for Resolving Disputes Arising from Contracts Concluded Using Blockchain Technology," *Journal of Jurisprudential and Legal Research*, Egypt, no. 36, April 2021.
14. Amal Marzouk, "Blockchain Technology and Its Economic Applications," *Middle East Journal of Humanities and Cultural Studies*, Jordan, vol. 1, no. 5, 2021, pp. 302–319.
15. Maryam Zan, "E-Commerce: Advantages and Risks," in the edited volume *Contracting in the Digital Space*, Arab Democratic Center for Strategic, Political and Economic Studies, Berlin, Germany, 2021.

References in Foreign Languages

16. Bensamoun, Alexandra, and Grégoire Loiseau. *Droit de l'intelligence artificielle*. 2nd ed. LGDJ, Lextenso, 2022.
17. Christodoulou, Hélène. "Les nouvelles technologies à l'origine de l'évolution contractuelle." *Communication – Commerce électronique*, Université Toulouse 1 Capitole, France, 2020, p. 4. Available at: <https://publications.ut-capitole.fr/>
18. Jeremy (Achour). "Formation du contrat et intelligence artificielle en droit français et anglais." Research dissertation in law, Master 2 in Contracts in French and European Law, Faculty of Law and Social Sciences, University of Poitiers, France, 2020/2021.

19. Schär, Fabian. "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets." Federal Reserve Bank of St. Louis Review, second quarter 2021, 103(2). Available at: <https://doi.org/10.20955/r.103.153-74>
20. Sebkhaoui, Khidja. "The Role of Cyber Security in Attaining the Sustainable Development Goals." Review, Development and Human Resources Management, vol. 11, issue 1, 2024.