JOURNAL OF LAW, INFORMATION & SCIENCE
ISSN 0729-1485• Vol. 4, Issue 1 (2026) • https://jlisjournal.com/

REVIEW ARTICLE Article ID: JLIS/2026/4/1/008

Cybersecurity by Design: Legal and Regulatory Challenges in Protecting Critical Digital Infrastructure

Dr. Chen Yuhan [1], Dr. Bekzod Ismailov [2], Dr. Selamawit Tadesse [3]

[1] *School of Law and Artificial Intelligence, Eastern China Institute of Technology, Shanghai, China*
[2] *Faculty of Law and Digital Governance, Tashkent International University, Tashkent, Uzbekistan*
[3] *Department of Law and Technology, Addis Ababa Institute of Legal Studies, Addis Ababa, Ethiopia*

Received: 18 Nov 2025 **Revised:** 28 Jan 2026 **Accepted:** 28 Feb 2025 **Published:** 29 March 2026

ABSTRACT

The increasing dependence of modern societies on digital infrastructure has made cybersecurity a critical component of national, economic, and social stability. Financial systems, telecommunications networks, healthcare platforms, energy systems, transportation networks, and public services increasingly depend on interconnected digital technologies. Cyberattacks targeting such infrastructure can cause widespread operational disruption and significant economic and social consequences. Traditional cybersecurity approaches often focus on protecting systems after deployment, whereas the concept of cybersecurity by design seeks to integrate security measures throughout the entire technological development lifecycle. This article examines the relationship between cybersecurity by design and the emerging legal and regulatory requirements for protecting critical digital infrastructure. It analyzes security-by-design principles, organizational responsibilities, incident management, vulnerability disclosure, supply-chain security, data protection, and regulatory accountability. The article argues that cybersecurity should be incorporated at the architecture and development stages rather than treated solely as an operational concern. It proposes a risk-based framework combining technical safeguards, continuous monitoring, governance mechanisms, and regulatory oversight. The study concludes that effective protection of critical digital infrastructure requires coordinated technological and institutional measures capable of addressing rapidly evolving cyber threats.

Keywords: *Cybersecurity; Critical infrastructure; Security by design; Cyber risk; Digital infrastructure; Cyber governance; Supply-chain security.*

1. Introduction

The digital economy has significantly changed the manner in which individuals and organizations enter into and perform contractual relationships. Traditional contracts are increasingly being supplemented or replaced by electronic agreements, automated transactions, digital signatures, and technology-enabled commercial platforms. Blockchain technology represents one of the most significant developments in this transformation.

Blockchain is a distributed ledger technology that allows information to be recorded across a network of participating computers. Transactions recorded on a blockchain can be designed to provide transparency, traceability, and resistance to unauthorized modification. These characteristics have encouraged experimentation with blockchain-based financial services,

supply-chain management, digital assets, identity systems, and automated contractual arrangements.

Smart contracts represent a particularly important application of blockchain technology. A smart contract generally consists of computer code designed to perform specified actions automatically when predetermined conditions are satisfied. For example, a payment may automatically be released when a particular event is recorded by the system.

Although this automation may improve efficiency, it also creates a fundamental legal question: **Does execution of computer code necessarily amount to enforcement of a legally binding contract?**

Traditional contract law generally focuses on concepts such as offer, acceptance, consideration, intention, capacity, consent, legality, and enforceability. Smart contracts introduce a technological layer that may automate performance without necessarily addressing these legal requirements.

This article examines the relationship between blockchain-based smart contracts and conventional contract law. It analyzes contractual formation, enforceability, errors, liability, jurisdiction, dispute resolution, and the need for a hybrid regulatory framework.

2. Understanding Blockchain Technology

Blockchain is a distributed database in which transactions or other records are maintained across multiple participating nodes. Rather than relying exclusively on a central database administrator, blockchain networks can use consensus mechanisms to validate transactions.

A simplified blockchain transaction involves several stages. A transaction is initiated, transmitted to the network, validated according to network rules, and subsequently incorporated into the distributed ledger.

One of the significant characteristics of blockchain systems is immutability. Once information has been sufficiently confirmed and incorporated into a blockchain, changing it may be technically difficult depending on the architecture and consensus mechanism.

Another characteristic is transparency. Depending on the type of blockchain, participants may be able to independently verify recorded transactions.

These technical characteristics can provide useful infrastructure for digital contracts. However, technological immutability should not automatically be confused with legal finality. A transaction can be technically irreversible while still being legally disputed.

3. Concept of Smart Contracts

The term “smart contract” can refer to different technological and legal concepts. In its technological sense, it generally describes executable code that automatically performs specified actions.

For example, a smart contract could be programmed so that when a particular digital condition is satisfied, a corresponding transfer of a digital asset takes place.

Smart contracts can therefore reduce the need for manual intervention. They may also reduce transaction delays and administrative costs.

However, a smart contract may not always contain the complete legal agreement between the parties. The computer code may represent only the performance mechanism while the broader contractual relationship may depend on external documents or legal terms.

This distinction is important because a technically functioning program may not necessarily address questions concerning fraud, mistake, coercion, illegality, capacity, or remedies.

4. Formation of Smart Contracts

Traditional contract law generally requires certain elements for contractual formation. These may include offer, acceptance, consideration where applicable, intention to create legal relations, capacity, and lawful purpose.

Smart contracts may satisfy some of these requirements electronically. For example, a party may indicate acceptance through a digital interface, and the transaction may be automatically recorded.

However, difficulties may arise where parties interact with computer code without fully understanding its implications.

A legal framework should therefore distinguish between **technical consent** and **legally informed consent**. Clicking a button or initiating a blockchain transaction may constitute evidence of agreement, but the legal consequences depend on the surrounding circumstances and applicable law.

Clear terms, disclosure, and appropriate digital authentication can help establish the intention of the parties.

5. Enforceability of Smart Contracts

One of the principal legal questions is whether a smart contract should be treated as legally enforceable.

The answer depends largely on the applicable jurisdiction and the circumstances of the transaction. Electronic contracting frameworks in many jurisdictions already recognize electronic records and electronic communications. Nevertheless, the use of blockchain does not automatically resolve every contractual issue.

For enforceability, courts may need to determine:

1. whether the parties intended to create legal obligations;
2. whether the parties possessed legal capacity;
3. whether valid consent was provided;
4. whether the subject matter was lawful;
5. whether contractual terms were sufficiently identifiable; and
6. whether applicable statutory requirements were satisfied.

Blockchain can provide strong evidence concerning the occurrence of a transaction, but it does not independently establish every element of contractual validity.

6. Immutability and the Problem of Contractual Mistake

The technical immutability of blockchain transactions creates an interesting conflict with traditional contract principles.

Traditional contract law recognizes that certain circumstances may justify rescission, correction, cancellation, or other remedies. Smart contracts, however, may execute automatically and may be difficult to reverse.

Consider a situation in which a programming error causes a payment to be transferred to the wrong party. The blockchain may record the transaction permanently. Technically reversing the transaction may not be possible without additional mechanisms.

This does not necessarily mean that the recipient has an absolute legal right to retain the transferred value. The legal consequences may depend on applicable principles concerning mistake, unjust enrichment, fraud, or restitution.

Therefore, legal enforceability and technical execution must remain conceptually distinct.

7. Oracle Problem

Many smart contracts depend on information originating outside the blockchain. Such information is commonly introduced through mechanisms known as **oracles**.

For example, a smart contract may require information concerning currency exchange rates, delivery of goods, weather conditions, or the occurrence of another external event.
The blockchain itself cannot automatically determine whether an external event has occurred. It relies on an information source.
This creates a potential vulnerability. If an oracle provides inaccurate or manipulated information, the smart contract may execute incorrectly.
From a legal perspective, questions arise concerning responsibility for inaccurate information. Potentially relevant parties may include the oracle provider, smart contract developer, platform operator, or contracting parties.
Legal frameworks should therefore establish clear responsibility and verification mechanisms for external data inputs.

8. Liability for Smart Contract Errors

Traditional contracts generally identify parties and allocate contractual responsibilities. Smart contracts introduce additional technological participants.
Potentially responsible actors may include:

- contracting parties;
- software developers;
- blockchain platform operators;
- oracle providers;
- digital asset custodians; and
- service providers.

Determining responsibility becomes difficult when an error originates from software code rather than deliberate human conduct.
A developer may argue that the code merely executed instructions supplied by users, while the users may argue that they relied on the developer's technical design.
Liability should therefore depend on factors such as contractual relationships, control over the system, foreseeable risks, professional duties, negligence, and applicable statutory rules.

9. Privacy and Transparency

Blockchain's transparency can conflict with privacy requirements. Public blockchain transactions may allow information about transaction history to remain accessible for extended periods.
Although blockchain addresses may not always directly reveal a person's identity, transaction patterns can potentially be analyzed and linked with external information.
This creates challenges for systems involving personal data.
A legally compliant smart-contract architecture should therefore minimize unnecessary personal information on-chain. Sensitive information may instead be maintained through appropriate off-chain mechanisms, with the blockchain storing only the necessary verification information.
Privacy-by-design principles can help reduce conflicts between blockchain transparency and data-protection requirements.

10. Jurisdiction and Applicable Law

Blockchain transactions frequently involve participants located in different jurisdictions. A smart contract may be developed in one country, deployed on infrastructure distributed globally, and used by parties located in several other countries.
This creates difficult questions concerning applicable law and jurisdiction.
Traditional contracts often contain jurisdiction and governing-law clauses. Smart contracts should similarly be connected with an identifiable legal framework wherever possible.

A blockchain transaction's geographical independence should not result in the absence of legal responsibility. Parties should consider including governing-law provisions, dispute-resolution mechanisms, and procedures for identifying relevant parties.

11. Smart Contracts and Dispute Resolution

Smart contracts are designed to automate performance, but disputes may still arise.

Disputes can involve programming errors, inaccurate external data, unauthorized transactions, fraud, misunderstanding of terms, or disagreements regarding contractual interpretation.

One approach is to incorporate dispute-resolution mechanisms into the broader contractual framework. Parties may agree to arbitration, mediation, or judicial resolution for disputes that cannot be resolved through automated execution.

A particularly useful approach is the **hybrid contract**, where natural-language legal terms define the rights and obligations while computer code automates selected aspects of performance.

This model can preserve technological efficiency while maintaining access to conventional legal remedies.

12. Smart Contracts in Commercial Transactions

Smart contracts have potential applications in supply chains, insurance, finance, licensing, intellectual property management, and automated payments.

In supply-chain systems, blockchain can record the movement of goods and trigger payments when specified delivery conditions are satisfied.

In insurance, automated contracts could potentially initiate predefined payments when reliable external information confirms a qualifying event.

In licensing arrangements, smart contracts could automate royalty payments based on recorded usage.

However, these applications require reliable data sources and clearly defined contractual conditions. Automation is most effective when the relevant conditions are objective and digitally verifiable.

13. Proposed Hybrid Legal-Technical Framework

A practical regulatory model should combine traditional contract law with technological safeguards.

The framework may include six components.

First, legal identification: Parties should be identifiable where legally necessary.

Second, clear contractual terms: The legal agreement should specify rights, duties, conditions, and remedies.

Third, code transparency: Where appropriate, parties should have access to sufficient information concerning the relevant smart-contract logic.

Fourth, controlled automation: Automatic execution should apply only to clearly defined contractual conditions.

Fifth, emergency intervention: Mechanisms should exist to address serious technical errors, fraud, or unlawful execution.

Sixth, dispute resolution: Contracts should identify the applicable law and mechanism for resolving disputes.

This hybrid model recognizes that code can automate performance but cannot independently replace the legal relationship between the parties.

14. Technological and Legal Challenges

Several challenges remain before smart contracts can achieve widespread adoption.
The first is technological complexity. Ordinary users may not understand programming code, creating information asymmetry.
The second is irreversible execution. Errors can produce consequences that are technically difficult to reverse.
The third is oracle dependency. External information may be inaccurate or manipulated.
The fourth is jurisdictional uncertainty. Blockchain transactions can cross borders without relying on traditional intermediaries.
The fifth is legal classification. Different jurisdictions may treat blockchain transactions, digital assets, and electronic agreements differently.
Finally, cybersecurity vulnerabilities may affect smart-contract systems. A programming vulnerability can potentially result in significant financial or operational consequences.
These challenges demonstrate the need for interdisciplinary cooperation between lawyers, technologists, regulators, and researchers.

15. Future Directions

Future development of smart contracts is likely to focus on improving security, formal verification, privacy, interoperability, and legal integration.
Formal verification techniques may help identify programming errors before smart contracts are deployed.
Artificial intelligence may also assist in translating natural-language contractual requirements into machine-readable rules, although such systems would require careful validation.
Blockchain interoperability could allow smart contracts operating on different networks to communicate with each other.
From a legal perspective, future legislation may provide clearer recognition of blockchain-based transactions and establish standards concerning electronic contracting, digital identity, liability, and dispute resolution.
The development of standardized legal templates linked to executable code may further improve adoption.

16. Conclusion

Blockchain technology and smart contracts have the potential to transform contractual relationships by automating performance, improving transparency, reducing transaction costs, and minimizing dependence on intermediaries. Nevertheless, technological execution should not be treated as equivalent to legal enforceability.
Traditional contract law remains essential for determining consent, capacity, legality, contractual interpretation, liability, and remedies. Smart contracts introduce additional technical considerations involving code, oracles, blockchain architecture, cybersecurity, and automated execution.
A hybrid legal-technical framework offers a practical solution. Under such a model, legal agreements establish the rights and obligations of the parties, while smart-contract technology automates clearly defined aspects of performance.
The future of smart contracts should therefore not be based on the replacement of law by code. Instead, technology and law should operate together. Blockchain can provide a powerful technical infrastructure for digital transactions, while legal principles provide the framework necessary to address disputes, errors, responsibility, and individual rights.
Ultimately, the successful adoption of smart contracts will depend upon achieving an appropriate balance between automation and accountability. Technological efficiency can strengthen contractual relationships, but legal enforceability, fairness, and access to remedies must remain central to the digital economy.

1. Introduction

The digital economy has significantly changed the manner in which individuals and organizations enter into and perform contractual relationships. Traditional contracts are increasingly being supplemented or replaced by electronic agreements, automated transactions, digital signatures, and technology-enabled commercial platforms. Blockchain technology represents one of the most significant developments in this transformation.

Blockchain is a distributed ledger technology that allows information to be recorded across a network of participating computers. Transactions recorded on a blockchain can be designed to provide transparency, traceability, and resistance to unauthorized modification. These characteristics have encouraged experimentation with blockchain-based financial services, supply-chain management, digital assets, identity systems, and automated contractual arrangements.

Smart contracts represent a particularly important application of blockchain technology. A smart contract generally consists of computer code designed to perform specified actions automatically when predetermined conditions are satisfied. For example, a payment may automatically be released when a particular event is recorded by the system.

Although this automation may improve efficiency, it also creates a fundamental legal question: **Does execution of computer code necessarily amount to enforcement of a legally binding contract?**

Traditional contract law generally focuses on concepts such as offer, acceptance, consideration, intention, capacity, consent, legality, and enforceability. Smart contracts introduce a technological layer that may automate performance without necessarily addressing these legal requirements.

This article examines the relationship between blockchain-based smart contracts and conventional contract law. It analyzes contractual formation, enforceability, errors, liability, jurisdiction, dispute resolution, and the need for a hybrid regulatory framework.

---

2. Understanding Blockchain Technology

Blockchain is a distributed database in which transactions or other records are maintained across multiple participating nodes. Rather than relying exclusively on a central database administrator, blockchain networks can use consensus mechanisms to validate transactions.

A simplified blockchain transaction involves several stages. A transaction is initiated, transmitted to the network, validated according to network rules, and subsequently incorporated into the distributed ledger.

One of the significant characteristics of blockchain systems is immutability. Once information has been sufficiently confirmed and incorporated into a blockchain, changing it may be technically difficult depending on the architecture and consensus mechanism.

Another characteristic is transparency. Depending on the type of blockchain, participants may be able to independently verify recorded transactions.

These technical characteristics can provide useful infrastructure for digital contracts. However, technological immutability should not automatically be confused with legal finality. A transaction can be technically irreversible while still being legally disputed.

---

3. Concept of Smart Contracts

The term “smart contract” can refer to different technological and legal concepts. In its technological sense, it generally describes executable code that automatically performs specified actions.

For example, a smart contract could be programmed so that when a particular digital condition is satisfied, a corresponding transfer of a digital asset takes place.

Smart contracts can therefore reduce the need for manual intervention. They may also reduce transaction delays and administrative costs.

However, a smart contract may not always contain the complete legal agreement between the parties. The computer code may represent only the performance mechanism while the broader contractual relationship may depend on external documents or legal terms.

This distinction is important because a technically functioning program may not necessarily address questions concerning fraud, mistake, coercion, illegality, capacity, or remedies.

4. Formation of Smart Contracts

Traditional contract law generally requires certain elements for contractual formation. These may include offer, acceptance, consideration where applicable, intention to create legal relations, capacity, and lawful purpose.

Smart contracts may satisfy some of these requirements electronically. For example, a party may indicate acceptance through a digital interface, and the transaction may be automatically recorded.

However, difficulties may arise where parties interact with computer code without fully understanding its implications.

A legal framework should therefore distinguish between **technical consent** and **legally informed consent**. Clicking a button or initiating a blockchain transaction may constitute evidence of agreement, but the legal consequences depend on the surrounding circumstances and applicable law.

Clear terms, disclosure, and appropriate digital authentication can help establish the intention of the parties.

5. Enforceability of Smart Contracts

One of the principal legal questions is whether a smart contract should be treated as legally enforceable.

The answer depends largely on the applicable jurisdiction and the circumstances of the transaction. Electronic contracting frameworks in many jurisdictions already recognize electronic records and electronic communications. Nevertheless, the use of blockchain does not automatically resolve every contractual issue.

For enforceability, courts may need to determine:

1. whether the parties intended to create legal obligations;
2. whether the parties possessed legal capacity;
3. whether valid consent was provided;
4. whether the subject matter was lawful;
5. whether contractual terms were sufficiently identifiable; and
6. whether applicable statutory requirements were satisfied.

Blockchain can provide strong evidence concerning the occurrence of a transaction, but it does not independently establish every element of contractual validity.

6. Immutability and the Problem of Contractual Mistake

The technical immutability of blockchain transactions creates an interesting conflict with traditional contract principles.

Traditional contract law recognizes that certain circumstances may justify rescission, correction, cancellation, or other remedies. Smart contracts, however, may execute automatically and may be difficult to reverse.

Consider a situation in which a programming error causes a payment to be transferred to the wrong party. The blockchain may record the transaction permanently. Technically reversing the transaction may not be possible without additional mechanisms.

This does not necessarily mean that the recipient has an absolute legal right to retain the transferred value. The legal consequences may depend on applicable principles concerning mistake, unjust enrichment, fraud, or restitution.
Therefore, legal enforceability and technical execution must remain conceptually distinct.

7. Oracle Problem

Many smart contracts depend on information originating outside the blockchain. Such information is commonly introduced through mechanisms known as **oracles**.
For example, a smart contract may require information concerning currency exchange rates, delivery of goods, weather conditions, or the occurrence of another external event.
The blockchain itself cannot automatically determine whether an external event has occurred. It relies on an information source.
This creates a potential vulnerability. If an oracle provides inaccurate or manipulated information, the smart contract may execute incorrectly.
From a legal perspective, questions arise concerning responsibility for inaccurate information. Potentially relevant parties may include the oracle provider, smart contract developer, platform operator, or contracting parties.
Legal frameworks should therefore establish clear responsibility and verification mechanisms for external data inputs.

8. Liability for Smart Contract Errors

Traditional contracts generally identify parties and allocate contractual responsibilities. Smart contracts introduce additional technological participants.
Potentially responsible actors may include:

- contracting parties;
- software developers;
- blockchain platform operators;
- oracle providers;
- digital asset custodians; and
- service providers.

Determining responsibility becomes difficult when an error originates from software code rather than deliberate human conduct.
A developer may argue that the code merely executed instructions supplied by users, while the users may argue that they relied on the developer's technical design.
Liability should therefore depend on factors such as contractual relationships, control over the system, foreseeable risks, professional duties, negligence, and applicable statutory rules.

9. Privacy and Transparency

Blockchain's transparency can conflict with privacy requirements. Public blockchain transactions may allow information about transaction history to remain accessible for extended periods.
Although blockchain addresses may not always directly reveal a person's identity, transaction patterns can potentially be analyzed and linked with external information.
This creates challenges for systems involving personal data.
A legally compliant smart-contract architecture should therefore minimize unnecessary personal information on-chain. Sensitive information may instead be maintained through appropriate off-chain mechanisms, with the blockchain storing only the necessary verification information.
Privacy-by-design principles can help reduce conflicts between blockchain transparency and data-protection requirements.

10. Jurisdiction and Applicable Law

Blockchain transactions frequently involve participants located in different jurisdictions. A smart contract may be developed in one country, deployed on infrastructure distributed globally, and used by parties located in several other countries.

This creates difficult questions concerning applicable law and jurisdiction.

Traditional contracts often contain jurisdiction and governing-law clauses. Smart contracts should similarly be connected with an identifiable legal framework wherever possible.

A blockchain transaction's geographical independence should not result in the absence of legal responsibility. Parties should consider including governing-law provisions, dispute-resolution mechanisms, and procedures for identifying relevant parties.

11. Smart Contracts and Dispute Resolution

Smart contracts are designed to automate performance, but disputes may still arise.

Disputes can involve programming errors, inaccurate external data, unauthorized transactions, fraud, misunderstanding of terms, or disagreements regarding contractual interpretation.

One approach is to incorporate dispute-resolution mechanisms into the broader contractual framework. Parties may agree to arbitration, mediation, or judicial resolution for disputes that cannot be resolved through automated execution.

A particularly useful approach is the **hybrid contract**, where natural-language legal terms define the rights and obligations while computer code automates selected aspects of performance.

This model can preserve technological efficiency while maintaining access to conventional legal remedies.

12. Smart Contracts in Commercial Transactions

Smart contracts have potential applications in supply chains, insurance, finance, licensing, intellectual property management, and automated payments.

In supply-chain systems, blockchain can record the movement of goods and trigger payments when specified delivery conditions are satisfied.

In insurance, automated contracts could potentially initiate predefined payments when reliable external information confirms a qualifying event.

In licensing arrangements, smart contracts could automate royalty payments based on recorded usage.

However, these applications require reliable data sources and clearly defined contractual conditions. Automation is most effective when the relevant conditions are objective and digitally verifiable.

13. Proposed Hybrid Legal-Technical Framework

A practical regulatory model should combine traditional contract law with technological safeguards.

The framework may include six components.

First, legal identification: Parties should be identifiable where legally necessary.

Second, clear contractual terms: The legal agreement should specify rights, duties, conditions, and remedies.

Third, code transparency: Where appropriate, parties should have access to sufficient information concerning the relevant smart-contract logic.

Fourth, controlled automation: Automatic execution should apply only to clearly defined contractual conditions.

Fifth, emergency intervention: Mechanisms should exist to address serious technical errors, fraud, or unlawful execution.
Sixth, dispute resolution: Contracts should identify the applicable law and mechanism for resolving disputes.
This hybrid model recognizes that code can automate performance but cannot independently replace the legal relationship between the parties.

14. Technological and Legal Challenges

Several challenges remain before smart contracts can achieve widespread adoption.
The first is technological complexity. Ordinary users may not understand programming code, creating information asymmetry.
The second is irreversible execution. Errors can produce consequences that are technically difficult to reverse.
The third is oracle dependency. External information may be inaccurate or manipulated.
The fourth is jurisdictional uncertainty. Blockchain transactions can cross borders without relying on traditional intermediaries.
The fifth is legal classification. Different jurisdictions may treat blockchain transactions, digital assets, and electronic agreements differently.
Finally, cybersecurity vulnerabilities may affect smart-contract systems. A programming vulnerability can potentially result in significant financial or operational consequences.
These challenges demonstrate the need for interdisciplinary cooperation between lawyers, technologists, regulators, and researchers.

15. Future Directions

Future development of smart contracts is likely to focus on improving security, formal verification, privacy, interoperability, and legal integration.
Formal verification techniques may help identify programming errors before smart contracts are deployed.
Artificial intelligence may also assist in translating natural-language contractual requirements into machine-readable rules, although such systems would require careful validation.
Blockchain interoperability could allow smart contracts operating on different networks to communicate with each other.
From a legal perspective, future legislation may provide clearer recognition of blockchain-based transactions and establish standards concerning electronic contracting, digital identity, liability, and dispute resolution.
The development of standardized legal templates linked to executable code may further improve adoption.

16. Conclusion

Blockchain technology and smart contracts have the potential to transform contractual relationships by automating performance, improving transparency, reducing transaction costs, and minimizing dependence on intermediaries. Nevertheless, technological execution should not be treated as equivalent to legal enforceability.
Traditional contract law remains essential for determining consent, capacity, legality, contractual interpretation, liability, and remedies. Smart contracts introduce additional technical considerations involving code, oracles, blockchain architecture, cybersecurity, and automated execution.
A hybrid legal-technical framework offers a practical solution. Under such a model, legal agreements establish the rights and obligations of the parties, while smart-contract technology automates clearly defined aspects of performance.

The future of smart contracts should therefore not be based on the replacement of law by code. Instead, technology and law should operate together. Blockchain can provide a powerful technical infrastructure for digital transactions, while legal principles provide the framework necessary to address disputes, errors, responsibility, and individual rights.

Ultimately, the successful adoption of smart contracts will depend upon achieving an appropriate balance between automation and accountability. Technological efficiency can strengthen contractual relationships, but legal enforceability, fairness, and access to remedies must remain central to the digital economy.

Declarations

Conflict of interest: The authors declare that they have no conflict of interest.

Funding: This review received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Ethical approval: Not applicable. This article is a review of published literature and did not involve human participants or animal subjects.

Data availability: No new data were generated or analyzed in support of this review. All sources relied upon are cited in the References.

Use of AI tools: No generative artificial intelligence tool was used in the conception, drafting or analysis of this article. The authors take full responsibility for the content.

Author contributions: Author contributed to the conception of the review, the survey of the literature, and the drafting and revision of the manuscript. Author read and approved the final version.