Self-Executing Smart Contracts: Technical and Legal Aspects

العقود الذكية ذاتية الإبرام والتنفيذ: الجوانب التقنية والقانونية

BENSALEM Ahmed Abderrahman*
University Center of Illizi
bensalem.ahmed.abderrahman@cuillizi.dz

AHMED Abdulhameed Suleiman
Arab East Colleges, Kingdom of Saudi Arabia
aaSuleiman@arabeast.edu.sa

Date of Submission 02-04-2026 Date of Final Acceptance 18-05-2026 Date of Publication June 2026

Abstract:

Self-executing smart contracts represent a qualitative advancement in the field of digital transactions, blending advanced technological innovation with legal frameworks to ensure the automatic and transparent execution of agreements while minimizing the need for traditional intermediaries. This article initially addresses the jurisprudential and legislative foundations that contributed to defining these contracts and establishing their legal regulations, then reviews the technical stages of drafting, deploying, and operating them on blockchain networks, with reference to their practical applications in areas such as real estate contracts, smart waqf contracts, and smart insurance. It also discusses the main practical and legal challenges related to technical security and data protection, providing a comprehensive view of the nature of these contracts and their growing role in the contemporary digital economy.

Keywords: Smart Contracts; Automated Execution; Blockchain; Legal and Practical Challenges; Contract Automation; Data Protection; Security; Cybersecurity.

ملخص:

تمثل العقود الذكية ذاتية الإبرام والتنفيذ تطورًا نوعيًا في مجال المعاملات الرقمية، حيث تمزج بين الابتكار التقني المتقدم والأطر القانونية لضمان تنفيذ الاتفاقيات تلقائيًا وبشفافية عالية، مع الحد من الحاجة للوسطاء التقليديين، بحيث يتناول المقال في البداية الأسس الفقهية والتشريعية التي ساهمت في تعريف هذه العقود ووضع ضوابطها القانونية، ثم يستعرض المراحل التقنية لإبرامها ونشرها وتشغيلها على شبكات البلوك تشين، مع الإشارة إلى تطبيقاتها العملية في مجالات متنوعة مثل عقود العقارات، وعقود الوقف الذكي والتأمين الذكي، كما يناقش أبرز التحديات العملية والقانونية المرتبطة بالأمان التقني وحماية البيانات، موفرًا رؤية شاملة لطبيعة هذه العقود ودورها المتنامي في الاقتصاد الرقمي المعاصر.

الكلمات المفتاحية: العقود الذكية؛ التنفيذ الآلي؛ البلوك تشين؛ التحديات القانونية والعملية؛ أتمتة العقود؛ حماية البيانات؛ الأمن؛ الأمن السيبراني.

*** Corresponding Author: BENSALEM Ahmed Abderrahman**

Introduction:

Self-executing smart contracts represent one of the most significant digital innovations in recent decades. They are not merely technical tools but a transformative development in understanding contractual obligations and their execution. These contracts rely on blockchain networks to automatically record and enforce agreements once predetermined conditions are met, ensuring high precision in fulfilling obligations while minimizing risks associated with delays, human intervention, or fraud. They embody the convergence of law and technology, where traditional legal provisions are translated into executable code, enhancing transparency, trust between parties, and creating a new digital legal environment characterized by reliability and efficiency[1].

The significance of this subject lies in the fact that smart contracts constitute an advanced stage in the evolution of digital transactions, offering extensive possibilities for restructuring traditional legal and commercial systems, including finance, real estate, waqf, and insurance. They go beyond merely simplifying procedures or accelerating transactions, opening the door to innovative business models based on automated contract execution and precise monitoring of obligations. Furthermore, they provide legal and technical mechanisms for addressing disputes more efficiently and accurately, making the study and understanding of these contracts, their operational mechanisms, and their legal frameworks an urgent necessity for researchers and practitioners alike[2].

Despite the increasing adoption of self-executing smart contracts, their legal and technical nature remains a subject of extensive debate, as they represent a convergence point between digital innovation and traditional legal frameworks. This situation raises several fundamental challenges, foremost among them how to achieve a balance between legal and jurisprudential compliance while ensuring the technical effectiveness of contracts on blockchain networks, as well as addressing practical issues such as data security, technical reliability, and integration with external systems. Hence, the main research problem emerges: **how can self-executing smart contracts align with legal and jurisprudential frameworks and be practically implemented on blockchain networks, while ensuring the ability to overcome the associated legal and practical challenges?**

This study adopts a multi-dimensional analytical approach that integrates legal and technical analyses of the fundamental concepts of smart contracts. From a legal perspective, the study examines national and international jurisprudential and legislative texts related to smart contracts, alongside comparative analyses of experiences in the United States, France, Belarus, and Malta, to assess the degree of legal recognition and regulatory frameworks governing their use. From a technical perspective, a descriptive-analytical method was employed to detail the operational stages of smart contracts, from programming design to deployment on blockchain networks, and finally to self-execution and verification of obligations. Furthermore, the study analyzes practical applications of smart contracts in diverse fields, with particular emphasis on technical and legal challenges, including cybersecurity, data protection, reliability, and regulatory compliance, providing a comprehensive view of the operational and legal dimensions of self-executing smart contracts.

Section I: Jurisprudential and Legislative Attempts to Define Smart Self-Executing Contracts

In the context of rapid digital transformations[3], the concept of smart self-executing contracts has become a focal point of interest for both jurists and legislators. Accordingly, this section initially addresses the jurisprudential attempts to delineate the scope of these contracts, followed by legal efforts to recognize and regulate them, and then highlights the essential characteristics that distinguish smart contracts[4].

A) Jurisprudential and Legislative Attempts

1- Jurisprudential Attempts

Smart contracts represent one of the most prominent digital innovations of the modern era, constituting a natural evolution of information and communication technology, particularly in the context of blockchain technology. The emergence of these contracts was driven by the need to develop mechanisms for executing digital agreements based on automatic execution and transparency, independent of traditional intermediaries, which has captured the attention of both jurists and legislators[5].

The roots of smart contracts trace back to the mid-1990s when legal scholar and cryptographer Nick Szabo first introduced the concept, considering them as a set of digitally defined promises incorporating protocols that enable parties to execute them automatically. This idea quickly evolved to include complementary smart contracts, which aim to enhance rather than replace traditional contracts by providing them with greater digital enforceability and credibility. [6]

Szabo initially defined smart contracts as a: "computerized transaction protocol that executes the terms of a contract." Later, with technological advancements, he refined the definition to: "a set of digitally specified promises, including the protocols through which the parties execute these promises." [7]

Meanwhile, Vitalik Buterin, the founder of the Ethereum network, defined a smart contract as: "a mechanism involving digital assets and two or more parties, in which some or all parties place assets into it, and the assets are automatically redistributed among those parties according to a formula based on specific data that was not known at the time the contract was initiated."[8]

Some have defined smart contracts as: "computer codes operating on the blockchain that include a set of rules according to which the parties to the contract agree to interact with each other, and when the predefined rules are met, the agreement is executed automatically."[9]

Investopedia defines them as: "self-executing contracts programmed within a decentralized platform called blockchain." Meanwhile, Regis de Boise describes smart contracts as: "digital contracts based on blockchain technology where the obligations of each party under the contract can be controlled."[10]

Others define smart contracts as "digital contracts that allow conditions based on decentralized consensus, are self-enforcing, and tamper-proof, through automatic execution."[11]

It is notable that these definitions are relatively complex, mostly focusing on the description and operational mechanism of smart contracts. Consequently, an alternative definition has emerged based on the idea of complementary or supportive contracts. P. De Filippi defines smart contracts as: "software executed in a decentralized manner on the blockchain[12], whose functions are activated upon the fulfillment of predetermined conditions." He emphasizes that smart contracts do not replace traditional contracts but rather enhance them. This view is shared by Mansour Daoud, who considers smart contracts as the ideal complement to conventional contracts, supporting them and providing them with digital and societal strength.[13]

From a technical perspective, smart contracts differ significantly from traditional electronic contracts. The latter can be executed on any digital platform using computers, tablets, or the internet. In contrast, smart contracts are created and executed exclusively within blockchain technology using encrypted mathematical codes, known as algorithms, which define the rights and

obligations of the parties in an “if… then…” structure. This enables automatic execution once predefined events or conditions are met, without the need for intermediaries or human intervention, thereby enhancing transparency, security, and tamper-resistance.[14]

Despite the significant innovation that smart contracts offer, they initially faced considerable skepticism due to their digital and virtual nature. Many individuals and institutions were unfamiliar with how they operated, which limited their adoption. However, these contracts experienced a qualitative leap with the advent of Bitcoin in 2008, which allowed transactions to be recorded and documented on the blockchain network while using digital currency as payment, enabling parties to interact within a secure digital environment. In 2013, programmer Vitalik Buterin further advanced this concept by developing the Ethereum network, which provided new programming protocols allowing for more flexible smart contracts adaptable to user needs. It also enabled self-execution of contracts with mining mechanisms associated with new cryptocurrencies, such as Ether.

What distinguishes smart contracts is not merely their digital nature, but their intelligent and automated execution, where two or more parties interact within a decentralized platform, ensuring full traceability and direct monitoring of transactions without requiring a third party. These contracts provide protection against forgery and manipulation while reinforcing trust and credibility in the digital environment. From a jurisprudential perspective, these features have sparked debate regarding the nature of the contract and the binding obligations of the parties. Scholars are divided: some view smart contracts as an extension of traditional contracts and a means to enhance them, while others see them as an independent entity requiring clear legal framing suitable for the digital context in which they operate[15].

Therefore, it can be concluded that smart contracts represent an advanced model of self-executing digital contracts, combining technical programming with legal commitment. They offer a secure and transparent platform for parties to efficiently execute their agreements while upholding fundamental legal principles, including obligation, contractual character, and transparency. This makes smart contracts an effective tool in modern digital transactions and a genuine complement to traditional contracts in light of rapid digital developments.

B) Legislative Attempts

It is observed that U.S. legislation has been particularly proactive in establishing boundaries and regulations for blockchain technology and smart contracts. The Arizona House Bill 2417 of 2017, concerning blockchain networks and smart contracts, defined a smart contract as: "Smart contract means 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."[16]

Similarly, Tennessee’s SB1662, focusing on blockchain technology, adopted the same definition. The New York law NY A08780 of 2017, Ohio law SB300 of 2018, and Nebraska law NE LB 695 of 2018 also adopted comparable definitions for smart contracts.

In contrast, Belarus defined smart contracts through Decree No. 08 of 2017, related to the development of the digital economy, as: "A program code designed to operate on a distributed ledger (blockchain), or another distributed information system, for the purposes of automatically executing transactions or performing other legal acts."[17]

Regarding French legislation, it can be noted that the French Civil Code does not yet contain a specific definition of smart contracts, representing a noticeable gap in the direct legal framing of this emerging technology. Nevertheless, the French legislator has explicitly recognized blockchain technology as the essential technical component and core driver of smart contracts. This recognition was not merely a formal statement; many scholars have considered it an important step toward the gradual legal acknowledgment of smart contracts within the French legal framework, paving the way for their future legal application.

This approach was concretely reflected in Article 12-223 of the French Monetary and Financial Code[18], which emphasizes the use of blockchain technology in financial transactions, stating: "A shared electronic recording device allowing the documentation of issuance and transfer of financial securities in accordance with conditions determined by a decree issued by the Council of State." This illustrates a conscious legislative approach to integrating digital innovation with the traditional legal system. Consequently, while France has not yet defined smart contracts directly, it has established the foundational legal provisions enabling the use of this technology, providing legal safeguards and regulatory frameworks that ensure transaction integrity and transparency—reflecting an advanced understanding of blockchain's role in enhancing the legal and economic reliability of smart contracts.

Belarus also represents another example of advanced legislative practice. Through Decree No. 08 of 2017 on digital economy development, the Belarusian legislator defined smart contracts as: "program code designed to operate on a distributed ledger (blockchain), a distributed information system used for the purposes of automatically executing transactions or performing other legal acts." This definition demonstrates Belarus's intent to integrate smart contracts within the traditional legal framework while emphasizing automated transaction and legal act execution. It reflects an international trend toward unifying core smart contract concepts, including decentralization, automatic enforceability, and digital asset management, while maintaining a clear legal framework—a sophisticated understanding of their nature and role in the contemporary digital economy.

Moreover, the Maltese Parliament, on July 4, 2018, established three laws regulating blockchain technology and smart contracts, as well as related issues. These include the Malta Innovation Act, the Innovative Technology Arrangements and Services Act, and the Virtual Financial Assets Act[19].

Overall, the legislative experiences of the United States, Europe, and Belarus represent advanced models for incorporating digital innovation within clear legal boundaries, providing a secure legal environment for investors and users, and enhancing parties' confidence in the legal effectiveness and reliability of smart contracts.[20]

Section II: Technical Stages of Smart Contract Formation and Their Operational Mechanisms

Smart contracts represent one of the most significant digital innovations of the past decade, sitting at the intersection of law and technology. They enable the creation of digital contracts that execute automatically once predetermined conditions are met, without the need for intermediaries, thus enhancing efficiency, security, and transparency in transactions. To understand how these contracts function, it is essential to examine the technical stages they undergo from creation to execution.

A) Software Design and Contract Condition Specification

The process of establishing a smart contract begins with software design, where legal and technical developers first define the conditions and obligations that the contract must fulfill. This stage involves:

Identifying the participating parties and specifying the rights and duties of each.
Drafting executable conditions using a specific programming language, such as Solidity on the Ethereum network, or other languages compatible with the blockchain platform employed.
Converting legal clauses into digital algorithms that can be processed automatically once the conditions are met.

This stage is arguably the most critical in bridging law and programming, requiring precise formulation to avoid loopholes that may affect execution or parties' rights.[21]

B) Deploying the Contract on the Blockchain

Once the contract is designed, the next step is deployment on the blockchain, a technical procedure that ensures the contract's decentralization and immutability. Key elements of this stage include:

Transforming the programmed contract into digital code suitable for uploading onto the blockchain.
Adding the contract to the blockchain network, where it is replicated across all nodes to ensure redundancy and prevent tampering.
Securing the contract against alteration or deletion using cryptographic techniques, such as SHA-256, making the stored data immutable post-deployment.

This procedure guarantees that the contract operates independently of any central authority and that all parties can verify the conditions and obligations without an intermediary, while enabling transparent and reliable tracking of all contract-related events.[22]

C) Automated Execution Upon Condition Fulfillment

The core feature of smart contracts is the self-enforcing execution of obligations once predefined conditions are met. This stage involves several technical components:

1- Event Monitoring: The smart contract is linked to specific events on the network, such as receipt of a financial payment or fulfillment of a condition in an external database (off-chain data).
Activation of programmed functions: Once a condition is satisfied, the contract executes programmed functions, such as transferring digital assets, issuing electronic documentation, or activating a party's rights.
2- Execution verification: The blockchain employs consensus protocols (e.g., Proof of Work or Proof of Stake) to ensure that all nodes on the network reach the same conclusion regarding contract execution, preventing manipulation or errors.

This stage makes smart contracts highly efficient, capable of handling thousands of operations simultaneously without human intervention, while reducing the risk of fraud or execution delays.

D) Integration with External Data Sources (Oracles)

In many cases, smart contracts rely on external data (off-chain), such as currency exchange rates, weather conditions, or election results. Oracles serve as bridges linking the smart contract to real-world data, ensuring the accuracy of information prior to execution. Key aspects include:

1- Reliable Oracles: Data provided must be accurate and verifiable, as it directly governs contract execution.
2- Data encryption: Ensures information cannot be tampered with before entering the network.
Multiple sources: Contracts may use multiple data sources to guarantee accuracy and increase reliability.

3- This technology allows smart contracts to operate in diverse economic and legal environments, including insurance, finance, and supply chain management.

E) Continuous Verification and Auditing

After deployment and activation, ongoing verification and auditing mechanisms are required to ensure execution integrity and protect the parties:

1- Legal compliance verification: Ensuring that programmed conditions comply with local and international laws.
2- Code auditing: Inspecting the code for bugs or vulnerabilities that could compromise execution.
3- Event and transaction logging: Every step of contract execution is recorded on the blockchain, providing a permanent ledger that can be referenced in potential disputes.

This stage adds an extra layer of legal and technical security, reaffirming the role of smart contracts as reliable instruments for executing digital agreements.

(Prepared by the researcher).

The diagram illustrates the practical stages of smart contracts, beginning with drafting the terms and converting them into digital algorithms, followed by deploying the contract on the blockchain network to ensure decentralization and immutability.
It proceeds to self-execution once pre-defined conditions are met, integrates external data sources via Oracles to ensure data accuracy, and concludes with continuous verification and auditing to guarantee execution integrity and safeguard the parties involved.
This comprehensive framework demonstrates how smart contracts provide a secure and transparent environment, combining technical efficiency with legal compliance, making them an effective tool for enhancing trust and reliability in modern digital transactions .

Section III: Section III: Practical Applications of Self-Executing Smart Contracts

Self-executing smart contracts have moved beyond theoretical concepts to practical implementation in various sectors, demonstrating their potential to automate transactions and enforce agreements efficiently. This section provides an overview of real-world applications, illustrating how these contracts are applied in areas such as real estate, movable asset sales, Islamic endowments (waqf), leasing, and insurance, while highlighting the technological and legal mechanisms that enable their operation[23].

A) Real Estate Sale Contract

In the current era, it is possible to convert ownership of real estate, movable assets, services, or benefits into encrypted programmatic codes using blockchain technology. Consequently, the transfer of traditional or digital ownership between a seller and a buyer can be envisioned through these encrypted codes. Some experts consider this form of ownership transfer as a natural evolution from conventional ownership to intelligent digital ownership[24].

Let us assume that Seller "A" owns a house and has a digital wallet on the blockchain, while Buyer "B" wishes to purchase the house and also possesses a similar digital wallet. After both parties agree on the essential terms of the smart sale contract, with Seller "A" formally proving ownership of the property and Buyer "B" demonstrating financial capacity to pay the price in cryptocurrency, it is agreed that the property ownership will be transferred immediately upon full receipt of the payment by Seller "A" in their digital wallet.

The technical and legal steps to execute such a smart real estate contract can be outlined as follows:

1- Contract Creation: The terms and conditions of the smart sale contract are coded using a programming language such as Solidity. The encrypted code incorporates all the conditions agreed upon by the parties.
2- Digital Wallet Addresses: The blockchain addresses of both the seller and the buyer are defined.
3- Price and Cryptocurrency Specification: The property price and the type of cryptocurrency for payment are determined.
4- Payment Deposit: The buyer deposits the agreed amount into an escrow account on the blockchain. The funds remain locked until the technology verifies that all contractual conditions have been fulfilled.
5- Self-Verification of Payment: The contract activates its function to confirm that the buyer has paid the full amount.
6- Ownership Transfer: The contract triggers the transfer of property ownership and the associated documents on the blockchain.
7- Reversion Clause: In case the buyer fails to pay the amount by the agreed deadline, ownership is automatically reverted to the seller.
8- Digital Signatures: Both parties digitally sign the contract using their private keys registered on the blockchain.
9-Automatic Verification and Execution: The blockchain monitors the payment status, and once the seller’s wallet confirms full receipt, the contract automatically executes the ownership transfer and registers it in the buyer’s name.
10- Smart Contract Deployment: After completing all the previous steps, the smart contract is deployed and distributed across all blockchain users. From this point, the contract acquires absolute evidentiary validity and cannot be modified through conventional methods.

B) Movable Asset Sale Contract

One of the most prominent examples of smart sale contracts is the smart gold sale contracts that emerged in 2015 in Malaysia through the company Hello Gold. The company launched the first digital smart platform compliant with Islamic law (Shariah) for buying and selling physical gold digitally without direct human intervention[25].

The platform relies on automating complex financial operations, managing users' accounts with high precision, and executing fund transfers automatically once the pre-programmed conditions in the smart contract between the platform and its users are met. The company primarily uses Ethereum blockchain technology to ensure the highest levels of security and privacy in all transactions.

Smart contracts play a crucial role on the platform, as they handle account management and execute transfers automatically without the need for intermediaries, ensuring accuracy and speed in all transactions. These contracts also create "tokens," unique digital representations fully backed by physical gold. Blockchain users can verify that each token corresponds to a specific weight of real gold, with every transaction securely recorded on the blockchain.

Through this system, the platform provides instantaneous, secure, and fully digital services for buying, selling, and storing gold. It also allows users to withdraw invested funds at any time and facilitates the transfer of digital assets or gold balances between user accounts with ease and security.

C) Waqf (Endowment) Smart Contracts

Finterra Waqf Chain is among the pioneering companies specializing in the drafting and execution of smart Waqf (endowment) contracts. Founded in 2017 in Malaysia, the company has since expanded to several countries, including India, Singapore, Bahrain, the United Arab Emirates, and Saudi Arabia. It collaborates with the respective Ministries of Waqf in each country to invest Waqf funds in both profit-generating and non-profit projects, ensuring transparency and efficiency in resource management.

When an individual wishes to invest in a profitable Waqf project, they must log into the company's digital platform connected to blockchain technology and create a digital account and wallet. After verifying the accuracy of the provided information, the platform assigns the investor a credit rating and then presents all available Waqf projects, allowing the investor to make an informed smart investment decision.

Once the investor decides to commit a specific amount to a particular Waqf project, the funds are transferred to the platform's digital wallet, thereby executing the smart Waqf contract between the investor and the platform.

Regarding contract execution and profit distribution, the platform initially issues digital tokens representing the amounts contributed by each investor. These tokens are then automatically allocated according to each investor's share. Upon completion of the Waqf project, the revenues and profits are distributed automatically through the smart contract and blockchain technology, ensuring transparency, accuracy, and efficiency in managing Waqf funds and distributing benefits to investors in compliance with Shariah principles.

This application represents an advanced model for integrating digital technology with Islamic endowments. It enhances investment efficiency, automates processes, and ensures precise tracking of all funds and returns, reducing human errors and fostering trust among all parties involved.

D) Smart Lease Contract (Wethaq Platform)

The Wethaq Platform is a limited liability company officially recognized in the United Arab Emirates, Saudi Arabia, and the United Kingdom, providing it with a strong legal foundation to operate in both international and Islamic financial markets[26]. The platform is distinguished as the first private digital platform specializing in the implementation of smart contracts within Islamic financial markets, relying on automated legal procedures to ensure full compliance with financial and Shariah regulations.

The platform focuses on issuing automated smart lease contracts fully compliant with Islamic law, allowing for the complete management of contractual operations without direct human intervention while providing a high level of transparency and accuracy in financial transactions. Using smart contracts on the Wethaq Platform guarantees the automatic and reliable execution of all pre-agreed terms, such as rental entitlements, payment obligations, and performance guarantees, significantly reducing the legal and technical risks associated with traditional lease agreements.

The platform has notably expanded the use of smart contracts for advanced Islamic finance applications, including:

Issuance of Smart Sukuk: Traditional Sukuk are converted into digital, encrypted tokens on the blockchain, allowing their ownership and trading to be tracked transparently and securely, while enabling investors to access and verify transaction records in real time.

Smart Investment Management: Profit distribution, reinvestment of returns, and verification of legal and Shariah compliance can be executed automatically, reducing reliance on traditional intermediaries and enhancing portfolio management efficiency.

Legal Automation: Through smart contracts, Shariah and legal rules are directly embedded in the contract's code, ensuring that each clause is executed legally and financially, while eliminating human error or delays in implementation.[27]

The Wethaq Platform exemplifies an advanced stage in integrating financial technology with Shariah standards, combining digital security, transparency, and operational efficiency. It also provides a scalable foundation for a wide range of Islamic financial products, including crowdfunding, Islamic real estate finance, and digital Takaful (insurance). By leveraging blockchain technology, the platform ensures that every transaction is recorded on an immutable ledger, enhancing trust among all parties and reducing potential disputes.

E) Smart Insurance Contracts

In the insurance industry, smart contracts are transforming traditional operational models by automating processes that were previously manual, time-consuming, and prone to human error. A prominent example is Fizzy, a service launched by the French insurance company AXA, which leverages blockchain-based smart contracts to manage flight delay compensation claims efficiently.

Fizzy relies on the parametric insurance model, where compensation is triggered not by the conventional proof of loss but by the fulfillment of a predetermined parameter — in this case, a flight delay exceeding two hours. Upon verification of the triggering event, the smart contract automatically executes the agreed-upon compensation payment, transferring the funds directly to the insured party's digital account recorded on the blockchain. This execution occurs without manual intervention from the customer, the insurer, or any intermediary, thus minimizing administrative delays and operational overheads.

Moreover, blockchain-enabled smart contracts allow for transparent and auditable transactions, ensuring that all claim conditions and execution steps are permanently recorded in an immutable ledger. This transparency strengthens policyholder confidence and provides regulators with verifiable evidence of compliance with contractual obligations. Ethereum-based platforms have extended this model to multiple insurers, automating claims disbursement totaling approximately $18.9 million, demonstrating both scalability and reliability of smart contract applications in real-world insurance environments.

The adoption of smart contracts in insurance not only accelerates the settlement process but also enhances risk management by reducing exposure to fraud, errors, and delays. From a legal perspective, smart contracts embed contractual obligations directly into code, ensuring enforceability while maintaining compliance with regulatory frameworks. Economically, this

innovation contributes to cost reduction, operational efficiency, and customer satisfaction, positioning smart contracts as a disruptive yet highly valuable tool in modern insurance practice.

Section IV: Practical and Legal Challenges of Self-Executing Smart Contracts.

Self-executing smart contracts represent an innovative model that integrates law and digital technology; however, they face a range of practical and legal challenges that may hinder their implementation and widespread adoption. This section aims to provide a general overview of these obstacles, highlighting their types and their impact on the effectiveness of smart contracts, whether from a technical, legal, or institutional perspective.

A) Security and Technical Reliability Challenges

Security and technical reliability remain among the most critical barriers to the widespread adoption of smart contracts. Smart contracts are executed on blockchain networks, which inherently rely on complex cryptographic protocols and decentralized consensus mechanisms. Any vulnerability in the underlying code—whether due to human error in programming, overlooked logical flaws, or malicious attacks—can result in substantial financial losses or the unintended execution of contractual terms. The decentralized nature of blockchain, while increasing transparency and reducing the need for intermediaries, also complicates error correction because once a contract is deployed, it is immutable.[28]

Moreover, as blockchain networks grow in size and complexity, the likelihood of unforeseen bugs or vulnerabilities rises. Smart contracts must also integrate seamlessly with external systems, such as traditional banking infrastructures, payment gateways, and financial platforms. Failure to achieve this integration can result in incomplete or inconsistent execution of obligations. To mitigate these risks, organizations must adopt rigorous testing protocols, including formal verification methods, security audits, and simulation-based stress testing, ensuring that smart contracts perform as intended under diverse scenarios.

B) Legal and Regulatory Challenges

Smart contracts challenge the very foundations of traditional legal frameworks. Many jurisdictions lack explicit legislation recognizing or regulating digital self-executing contracts, which introduces uncertainty regarding their enforceability. Critical issues include the evidentiary value of smart contracts in legal disputes, the allocation of liability in the event of contract failure, and the legal consequences of errors, omissions, or external attacks on the code. For example, if a bug in a smart contract leads to the unauthorized transfer of assets, questions arise about whether the parties are legally bound or if compensation can be claimed.

Cross-border transactions exacerbate these challenges. Smart contracts can operate seamlessly across multiple jurisdictions, raising complex questions regarding applicable law and jurisdictional authority. Additionally, contracts must comply with local legal regulations, financial rules, and, where applicable, Sharia law for Islamic finance contracts. Failing to account for these requirements may render a smart contract void, unenforceable, or subject to legal disputes. Consequently, legislators, regulators, and technologists must collaborate to create clear legal standards and frameworks that reconcile the decentralized, automated nature of smart contracts with established legal principles[29].

1- Personal Data Protection Law and Smart Contracts

From a high-level legal and regulatory perspective, self-executing smart contracts raise complex and unresolved challenges in relation to personal data protection, particularly within blockchain environments characterised by immutability, decentralisation, and permanent data replication. While these technical features enhance transparency and auditability, they may directly conflict with core principles enshrined in modern data protection regimes, including data

minimisation, purpose limitation, storage limitation, and the right to erasure ("right to be forgotten"). This structural tension requires a functional legal reconciliation between blockchain architecture and data protection compliance frameworks. Accordingly, any serious legal analysis of smart contracts must integrate the normative requirements of data protection law, particularly in light of the EU General Data Protection Regulation (GDPR), which establishes strict conditions for lawful processing of personal data in digital environments. The absence of a deletion mechanism in blockchain systems further intensifies the legal debate on whether immutable ledgers can be fully aligned with contemporary privacy standards, thereby necessitating hybrid compliance models such as off-chain storage or encryption-based anonymisation techniques.

2- Cybersecurity and Informatics Law in Smart Contract Systems

The operational deployment of self-executing smart contracts is inherently dependent on distributed digital infrastructures, rendering them highly exposed to cybersecurity threats such as code vulnerabilities, oracle manipulation, denial-of-service attacks, and unauthorized protocol interference. In this context, cybersecurity and informatics law constitute the primary normative framework for ensuring the resilience, integrity, and reliability of blockchain-based systems. These legal regimes do not merely address ex post liability but also establish ex ante preventive obligations concerning risk management, system security standards, and incident reporting mechanisms. Moreover, cybersecurity law introduces a structured liability framework for digital actors, including developers, platform operators, and service providers, thereby extending legal accountability to algorithmic environments. Consequently, the legal analysis of smart contracts must move beyond technical description to address critical issues of cyber-risk governance, digital forensics, and responsibility allocation in cases of system failure or malicious exploitation.

3-E-Commerce Law and the Legal Recognition of Smart Contracts

Within the digital economy, self-executing smart contracts represent a structural evolution of electronic contracting mechanisms, enabling automated execution, reduced transaction costs, and enhanced efficiency in online commercial exchanges. However, their legal validity and enforceability remain contingent upon the regulatory framework governing electronic commerce, which defines the essential conditions for contract formation, electronic authentication, and consumer protection. E-commerce law therefore serves as the doctrinal foundation for integrating blockchain-based agreements into the traditional legal order. Nevertheless, the automated and autonomous nature of smart contracts challenges conventional doctrines of consent, offer and acceptance, and contractual interpretation. This necessitates a reinterpretation of classical contract law principles in light of algorithmic execution systems, ensuring that legal certainty, consumer rights, and transactional fairness are preserved in digital environments governed by code rather than human intermediaries.

C) Data Protection and Privacy Challenges

While blockchain offers unparalleled transparency and traceability, it inherently conflicts with traditional data privacy standards. Smart contracts require access to participant data, which can include personal identifiers, financial information, or confidential business details. Because blockchain records are immutable and publicly accessible within the network, this raises significant risks regarding compliance with international privacy laws such as the European Union's General Data Protection Regulation (GDPR).

Additionally, the integration of off-chain data through oracles introduces another layer of vulnerability. Incorrect, manipulated, or outdated data from external sources can trigger unintended contract execution. Protecting digital identities is also a major concern, particularly in cross-border transactions where reliable digital identification systems may not exist. As such, developers must implement advanced encryption techniques, secure multi-party computation, zero-knowledge

proofs, and decentralized identity solutions to ensure that private data is protected while maintaining the contract's integrity and enforceability.[30]

D) Cost and Institutional Adoption Challenges

Financial and organizational constraints are additional obstacles. Designing, deploying, and maintaining secure smart contracts requires substantial investment in technical expertise, software infrastructure, and ongoing monitoring. Organizations must bear costs associated with code audits, cybersecurity measures, and system integration. Furthermore, the adoption of smart contracts often faces resistance from institutions accustomed to traditional processes, due to concerns about digital reliability, loss of control, and unfamiliarity with decentralized execution mechanisms.

Overcoming these barriers requires not only technological solutions but also institutional education and cultural adaptation. Stakeholders must be informed about the efficiency, accuracy, and transparency advantages of smart contracts, while assurances must be provided regarding risk mitigation measures. Encouraging adoption may involve pilot programs, regulatory sandboxes, and public-private collaborations to validate the technology in real-world contexts. Broad acceptance is likely to hinge on the ability of organizations to demonstrate consistent reliability, legal compliance, and tangible benefits over conventional contract execution methods[31].

Conclusion:

Over the past decade, self-executing smart contracts have brought a radical transformation to the management of legal and financial transactions, as digital technology enables obligations to be executed automatically and with high precision, while minimizing human intervention and the need for intermediaries. This transformation represents a natural extension of the evolution of traditional contracts and reflects the capacity of digital innovation to reshape legal and economic frameworks in line with the demands of the digital era.

The study of the technical stages of these contracts, along with their practical applications in areas such as real estate sales, movable property transactions, smart insurance contracts, and Waqf (endowment) contracts, demonstrates that they provide an unprecedented level of transparency, security, and speed in fulfilling obligations. Furthermore, the blockchain-based nature of smart contracts ensures permanent documentation of transactions, enhancing trust between parties and reducing the likelihood of future disputes.

However, smart contracts cannot be regarded as a comprehensive solution without acknowledging the associated practical and legal challenges, which include network security, legal recognition, data protection, integration with traditional systems, and institutional adoption. This underscores the need to extract precise conclusions from this study and provide practical recommendations to overcome obstacles and maximize the benefits of this advanced technology in the future.

Results

The study reveals that self-executing smart contracts represent a fundamental shift in the concept of traditional contracts, both jurisprudentially and legally. Jurisprudential and legislative attempts have demonstrated the potential to adapt these contracts to Islamic law and national regulations, reflecting a serious effort to create a balanced legal framework between technological innovation and religious and legal requirements.

From a technical perspective, the stages of drafting and implementing smart contracts show that they rely on precise encrypted software, digital wallets, and blockchain technologies to ensure automatic execution of obligations, achieving unprecedented speed and efficiency in financial, real estate, and investment transactions.

Regarding practical applications—such as real estate sales, gold trading, smart insurance, and Waqf contracts—these contracts provide transparency, accuracy, and rapid execution, while reducing reliance on intermediaries and enabling permanent documentation on the blockchain, thus enhancing credibility and trust among parties.

However, the study of challenges indicates that smart contracts face technical, legal, regulatory, and privacy-related obstacles, as well as issues related to institutional adoption. There is an urgent need to develop advanced legal frameworks, robust security protocols, and reliable digital identity systems to ensure the long-term success of these contracts.

Recommendations

Based on the preceding results, the following practical recommendations can enhance the effectiveness of smart contracts:

1- Establish clear legal frameworks: Governments should enact explicit legislation recognizing smart contracts, defining parties' responsibilities and dispute resolution mechanisms in accordance with Islamic law and national regulations.

2- Enhance programming and digital infrastructure security: Implement independent code audits and regular security testing to prevent vulnerabilities that may affect contract execution.

3- Integrate with traditional systems: Connect smart contracts with banks, digital payment systems, and governmental authorities to ensure effective execution and legal compliance.

4- Develop reliable digital identity systems: Verify the identities of digital parties and ensure the security of personal and financial data in compliance with international data protection standards.

5- Promote awareness and training: Foster digital literacy among institutions and investors, highlighting the benefits of smart contracts and instructing on their safe and effective use.

Citations.

[1] - Gerardo Iuliano , Dario Di Nucci, Smart contract vulnerabilities, tools, and benchmarks: An updated systematic literature review, Journal of Systems and Software, June 2026, p3 , https://doi.org/10.1016/j.jss.2026.112788

[2] - ALqodsi, E. M., and L. Arenova. "Smart contracts in contract law as an auxiliary tool or a promising substitute for traditional contracts." J. Leg. Aff. Disput. Resolut. Eng. Constr. 16 (3).2024. 06524004. https://doi.org/10.1061/JLADAH.LADR-1132.

[3] - Farao, A., G. Paparis, S. Panda, E. Panaousis, A. Zarras, and C. Xenakis. "INCHAIN: A cyber insurance architecture with smart contracts and self-sovereign identity on top of blockchain." Int. J. Inf. Secur. 23 (1)2024. 347–371. https://doi.org/10.1007/s10207-023-00741-8.
See more about the 4th Industrial Revolution Braütigam & Klindt, "Industrie 4.0, das Internet der Dinge und das Recht" NHW 1137; European Law Institute (ELI) Principles on Blockchain Technology, Smart Contracts and Consumer Protection 2022.

[4] - Zinovyeva, Elizaveta and Reule, Raphael C. G. and Härdle, Wolfgang Karl, Understanding Smart Contracts: Hype or Hope? , March 15, 2021, Available at SSRN: https://ssrn.com/abstract=3804861 or http://dx.doi.org/10.2139/ssrn.3804861

[5] - Nonetheless, this does not mean that they are more economical in comparison to traditional contracts since the necessary technological equipment is quite expensive, while the electricity consumption, especially for solving the problem and verifying the transaction, is high (see Savelyev , p. 127; 2016. Temte , p. 92), while the drafting of a smart contract is not easy for a person, who must resort to a special engineer (see Lingwall & Mogallapu , p. 314 ff.; Temte (2019), p. 97; Pardolesi & Davola (2019), pp. 8-9; Müller & Seiler (2019), pp. 320-321; Junghöfer, p. 8). See also

Vatiero, "Smart Contacts vs Incomplete Contracts: A transaction cost economic viewpoint: Computer L & Security R, 1.2022.
Savelyev, p. 127 : Alexey Savelyev, dans ses travaux sur les aspects juridiques des smart contracts2016.

[6] - Eliza Mik, Smart Contracts: A Requiem. Journal of Contract Law , Forthcoming. December 7, 2019. P3. Available at SSRN: https://ssrn.com/abstract=3499998 or http://dx.doi.org/10.2139/ssrn.3499998

[7] - Daoud, M. . Legal aspects of smart contract applications. Journal of Legal and Political Sciences, University of El Oued, Algeria,2021. 12(2), 36.

[8] - Lauslahti, Kristian, Mattila, Juri & Seppälä, Timo, "Smart Contracts – How Will Blockchain Technology Affect Contractual Practices?". ETLA Reports No 68.2017

[9] - Najiba Madawi.. Smart contracts and blockchain. Al-Mufakkir Journal for Legal and Political Studies, Djilali Bounaama University, Khemis Miliana – Algeria,2021. 4(2), 62.

[10] - Bayle Aurélie, Analyse prospective des smart contrats en droit français, Mémoire master II droit de la consommation et droit de la concurrence, faculté de droit et de science politique, Université de Montpellier, France 2016/2017, p40.

[11] - Issa, H. S. A. . The emergence of smart contracts in the blockchain era (pp. 6–7). Cairo: Al-Nahda Al-Arabia Publishing.2020.

[12] - De Filippi, P., & Wright, A. Blockchain and the Law: The Rule of Code.2018. Harvard University Press. Filippi, D., Primavera, & Hassan, S. Legal Implications of Blockchain: How Blockchains Enable Self-Executing Contracts. Harvard Journal of Law & Technology, 30, 723-773.

[13] - Daoud, M. The legal value of blockchain in evidence and its role in the scope of digital documentation of electronic transactions (p. 290). In Journal of Legal and Political Sciences, University of El Oued,2022 Algeria, 12(2).

[14] - Stazi, Smart Contracts and Comparative Law (Springer, 2021) (p. 81 ff.); Kipker, Birreck, Niewöhner & Schnorr, „Rechtliche und technische Rahmenbedingungen der „Smart Contracts"", 2020 MMR 509 (p. 510). According to World Economic Forum by 2027, 10% of the global gross domestic product (GDP) will be stored in blockchain-supported technologies, see Deep Shift Technology Tipping Points and Societal Impact (2015).

[15] - Regnath, Emanuel and Steinhorst, Sebastian "SmaCoNat: Smart Contracts in Natural Language", Forum on Specification & Design Languages (FDL),2018, IEEE Xplore, 5-16

[16] - It refers to an event-driven program that runs on a distributed, decentralized, shared, and replicated ledger, which is capable of taking custody of and instructing the transfer of values on that ledger.

[17] - Issa, H. S. A.The emergence of smart contracts in the blockchain era (p. 42). 2022. Cairo: Al-Nahda Al-Arabia Publishing.

[18] - Article L. 223-12 of the French Monetary and Financial Code provides that:
"…a shared electronic recording system allowing the authentication of these operations, under conditions, notably regarding security, defined by a decree of the Council of State."

[19] - For reference, these legislative texts are available at the following link (accessed on March 28, 2026, at 21:56):
http://www.justiceservices.gov.mt/downloaddocument.aspx?app=lom&itemid=12874811

[20] - Simon de Charentenay, Blockchain et Droit : Code is deeply Law, labase-lextenso, Gazette du Palais n°39, 2017, p.15.

[21] - Buchner, "Artificial Intelligence as a Challenge for the Law: The Example of "Doctor Algorithm"" 3 International Cybersecurity L Rev 181.2022. p. 182

[22] - Mustapha Mekki, Le contrat, objet des smart contracts (1er Partie), Dalloz p.410.

[23] - Ibba, G. "A smart contracts repository for top trending contracts." In Proc., 5th Int. Workshop on Emerging Trends in Software Engineering for Blockchain, edited by R. Tonelli, and M. Ortu,

17–20.2022. New York: Association for Computing Machinery. https://doi.org/10.1145/3528226.3528374.

[24] - Ballaji, N . Smart Contracts: Legal Implications in the Age of Automation. Beijing Law Review, 15, 1015-1032.2024. doi: 10.4236/blr.2024.153061.

[25] - Allen, J. G., & Hunn, P. Smart Legal Contracts: Computable Law in Theory and Practice.2022. Oxford University Press.

[26] - El Gendy, Amira El Sayed, Impact of the Use of Smart Contracts on the Efficiency of Islamic Banking Journal of Financial, Accounting and Administrative Studies, Volume 6, Volume 2 Larbi Ben M'hidi Oum El Bouaghi University - Laboratory of Finance, Accounting, Taxation and Insurance .

[27] - Atiyah, Ghassan Adhab, "Legitimacy of Smart Contracts from the Perspective of Islamic Law: A Case Study of Blockchain Transactions", Al-Istinbath: Jurnal Hukum Islam, Malaysia, Vol. 9. No. 1, 2024, 155 - 192.

[28] - Hervé Jacquemin, Alexandre Cassart, Blockchains and Smart Contracts in Law, Larcier Editions, 2020, p. 195.

[29] - Kaczmarek-Templin, B. “The smart contract—Problems with taking evidence in polish civil proceedings in the light of European regulations.” Bratislava Law Rev.2023. 7 (1): 65–76. https://doi.org/10.46282/blr.2023.7.1.308.

[30] - Verstraete, M. “The stakes of smart contracts.” Accessed October 12, 2024. https://heinonline.org/HOL/LandingPage?handle=hein.journals/luclj50&div=42&id=&page=.

[31] - Alaba, F., H. Sulaimon, M. Marisa, and O. Najeem. “Smart contracts security application and challenges: A review.” CCDS 5 (1): 15–412024.. https://doi.org/10.37256/ccds.5120243271.

Bibliography:

A- Books

1. Allen, J. G., & Hunn, P., *Smart Legal Contracts: Computable Law in Theory and Practice*, Oxford University Press, 2022.
2. De Filippi, Primavera & Wright, Aaron, *Blockchain and the Law: The Rule of Code*, Harvard University Press, 2018.
3. Issa, H. S. A., *The Emergence of Smart Contracts in the Blockchain Era*, Al-Nahda Al-Arabia Publishing, Cairo, 2020, pp. 6–7.
4. Jacquemin, Hervé & Cassart, Alexandre, *Blockchains and Smart Contracts in Law*, Larcier Editions, 2020.
5. Lauslahti, Kristian; Mattila, Juri & Seppälä, Timo, *Smart Contracts – How Will Blockchain Technology Affect Contractual Practices?*, ETLA Reports, No. 68, 2017.
6. Mekki, Mustapha, *Le contrat, objet des smart contracts (1ère Partie)*, Dalloz.
7. Simon de Charentenay, *Blockchain et Droit : Code is deeply Law*, Gazette du Palais, No. 39, Lextenso, 2017.
8. Stazi, Andrea, *Smart Contracts and Comparative Law*, Springer, 2021.

B- Theses and Academic Dissertations

1. Bayle, Aurélie, *Analyse prospective des smart contrats en droit français*, Mémoire de Master II en droit de la consommation et droit de la concurrence, Faculté de droit et de science politique, Université de Montpellier, France, 2016/2017.

C- Scholarly Journal Articles

1. Alaba, F.; Sulaimon, H.; Marisa, M. & Najeem, O., “Smart Contracts Security Application and Challenges: A Review”, *CCDS*, Vol. 5, No. 1, 2024, pp. 15–41.

2. ALqodsi, E. M. & Arenova, L., "Smart Contracts in Contract Law as an Auxiliary Tool or a Promising Substitute for Traditional Contracts", *Journal of Legal Affairs and Dispute Resolution in Engineering and Construction*, Vol. 16, No. 3, 2024.
3. Atiyah, Ghassan Adhab, "Legitimacy of Smart Contracts from the Perspective of Islamic Law: A Case Study of Blockchain Transactions", *Al-Istinbath: Jurnal Hukum Islam*, Vol. 9, No. 1, Malaysia, 2024.
4. Ballaji, N., "Smart Contracts: Legal Implications in the Age of Automation", *Beijing Law Review*, Vol. 15, 2024, pp. 1015–1032.
5. Braütigam & Klindt, "Industrie 4.0, das Internet der Dinge und das Recht", *NHW*, p. 1137.
6. Buchner, Benedikt, "Artificial Intelligence as a Challenge for the Law: The Example of 'Doctor Algorithm'", *International Cybersecurity Law Review*, Vol. 3, 2022, pp. 181–190.
7. Daoud, M., "Legal Aspects of Smart Contract Applications", *Journal of Legal and Political Sciences*, University of El Oued, Algeria, 2021.
8. Daoud, M., "The Legal Value of Blockchain in Evidence and its Role in the Scope of Digital Documentation of Electronic Transactions", *Journal of Legal and Political Sciences*, University of El Oued, Algeria, 2022, p. 290.
9. El Gendy, Amira El Sayed, "Impact of the Use of Smart Contracts on the Efficiency of Islamic Banking", *Journal of Financial, Accounting and Administrative Studies*, Vol. 6, No. 2, Larbi Ben M'hidi University, Oum El Bouaghi, 2019.
10. European Law Institute (ELI), *Principles on Blockchain Technology, Smart Contracts and Consumer Protection*, 2022.
11. Farao, A.; Paparis, G.; Panda, S.; Panaousis, E.; Zarras, A. & Xenakis, C., "INCHAIN: A Cyber Insurance Architecture with Smart Contracts and Self-Sovereign Identity on Top of Blockchain", *International Journal of Information Security*, Vol. 23, No. 1, 2024, pp. 347–371.
12. Filippi, Primavera & Hassan, S., "Legal Implications of Blockchain: How Blockchains Enable Self-Executing Contracts", *Harvard Journal of Law & Technology*.
13. Ibba, G., "A Smart Contracts Repository for Top Trending Contracts", in *Proceedings of the 5th International Workshop on Emerging Trends in Software Engineering for Blockchain*, Association for Computing Machinery, New York, 2022, pp. 17–20.
14. Iuliano, Gerardo & Di Nucci, Dario, "Smart Contract Vulnerabilities, Tools, and Benchmarks: An Updated Systematic Literature Review", *Journal of Systems and Software*, June 2026.
15. Kaczmarek-Templin, B., "The Smart Contract—Problems with Taking Evidence in Polish Civil Proceedings in the Light of European Regulations", *Bratislava Law Review*, Vol. 7, No. 1, 2023, pp. 65–76.
16. Kipker, Dennis-Kenji; Birreck, Jan; Niewöhner, Jens & Schnorr, Thomas, "Rechtliche und technische Rahmenbedingungen der Smart Contracts", 2020.
17. Mik, Eliza, "Smart Contracts: A Requiem", *Journal of Contract Law*, forthcoming, December 7, 2019.
18. Najiba Madawi, "Smart Contracts and Blockchain", *Al-Mufakkir Journal for Legal and Political Studies*, Djilali Bounaama University, Khemis Miliana, Algeria, 2021.
19. Vatiero, Massimiliano, "Smart Contracts vs Incomplete Contracts: A Transaction Cost Economic Viewpoint", *Computer Law & Security Review*, 2022.
20. Zinovyeva, Elizaveta; Reule, Raphael C. G. & Härdle, Wolfgang Karl, "Understanding Smart Contracts: Hype or Hope?", March 15, 2021.

D- Electronic Resources and Websites

1. Ibba, G., "A Smart Contracts Repository for Top Trending Contracts", available at: https://doi.org/10.1145/3528226.3528374 (Accessed on March 28, 2026).
2. Iuliano, Gerardo & Di Nucci, Dario, "Smart Contract Vulnerabilities, Tools, and Benchmarks: An Updated Systematic Literature Review", available at: https://doi.org/10.1016/j.jss.2026.112788 (Accessed on March 28, 2026).
3. Kaczmarek-Templin, B., "The Smart Contract—Problems with Taking Evidence in Polish Civil Proceedings in the Light of European Regulations", available at: https://doi.org/10.46282/blr.2023.7.1.308 (Accessed on March 28, 2026).
4. Legislative texts available at: http://www.justiceservices.gov.mt/downloaddocument.aspx?app=lom&itemid=12874811 (Accessed on March 28, 2026, at 21:56).
5. Mik, Eliza, "Smart Contracts: A Requiem", available at SSRN: https://ssrn.com/abstract=3499998 or: http://dx.doi.org/10.2139/ssrn.3499998 (Accessed on March 28, 2026).
6. Zinovyeva, Elizaveta; Reule, Raphael C. G. & Härdle, Wolfgang Karl, "Understanding Smart Contracts: Hype or Hope?", available at SSRN: https://ssrn.com/abstract=3804861 or: http://dx.doi.org/10.2139/ssrn.3804861 (Accessed on March 28, 2026).