DOI: https://doi.org/10.36719/2706-6185/48/127-143

Baylar Suleymanli
University of Silesia
Master student
https://orcid.org/0009-0006-1893-7020
baylar.suleymanli@mail.ru

Regulatory Frameworks and Government Approaches to Blockchain (Smart Contracts): European Union, Great Britain, USA, China, and Comparative Insights

Abstract

This paper analyzes the regulatory frameworks and government policies regarding blockchain and smart contracts in the four of the world's biggest jurisdictions: the European Union, the United Kingdom, the United States of America and China. As blockchain technology, particularly smart contracts, transition from experimental applications to legal and commercial use, the need for regulatory clarity has become paramount. The study begins by outlining the technical and legal character of smart contracts and tracing a spectrum of models of incorporation into traditional contractual forms. It then examines the approach to the law of smart contracts in each jurisdiction, ranging from the EU's harmonization and codification under MiCA and the Data Act, to the UK's common law-based development, the US's patchwork state-level experimentation, and China's centralized and policy-driven legal enforcement. Through comparative visualizations like radar charts, stacked bar graphs, and heatmaps, the paper finds divergent levels of institutional support, crypto integration, consumer protection, and legal certainty. The findings show that even though every jurisdiction resonates with unique regulatory philosophies, they also reflect complementary models of blockchain governance. The article ends with a reemphasis on the need for global cooperation and standardization to enable the secure, efficient, and legally binding application of blockchain technology in international business and governance.

Keywords: *Blockchain regulation, smart contracts, Aİ Data Act, MiCA, USA legal fragmentation, China BSN, comparative analysis*

Bəylər Süleymanlı
Sileziya Universiteti
magistrant
https://orcid.org/0009-0006-1893-7020
baylar.suleymanli@mail.ru

Blokçeynə (Ağıllı Müqavilələr) dair Tənzimləyici Çərçivələr və Hökumət Yanaşmaları: Avropa İttifaqı, Böyük Britaniya, ABŞ, Çin və Müqayisəli Baxışlar

Xülasə

Bu məqalədə dünyanın dörd ən böyük yurisdiksiyasında, Avropa İttifaqı, Birləşmiş Krallıq, Amerika Birləşmiş Ştatları və Çində blokçeyn və ağıllı müqavilələrə dair normativ-hüquqi çərçivələr və dövlət siyasətləri təhlil olunur. Blokçeyn texnologiyası, xüsusilə ağıllı müqavilələr, eksperimental tətbiqlərdən hüquqi və kommersiya məqsədli istifadəyə keçdikcə, normativ aydınlığa ehtiyac daha da aktuallaşır. Tədqiqat ağıllı müqavilələrin texniki və hüquqi mahiyyətini ümumiləşdirir və onların ənənəvi müqavilə formalarına müxtəlif inteqrasiya modellərini izah edir.

Daha sonra hər bir yurisdiksiyada ağıllı müqavilələrin hüquqi tənzimlənməsinə yanaşmalar Aİ-də MiCA və Data Act vasitəsilə harmonizasiya və kodifikasiya yolu, Birləşmiş Krallıqda ümumi hüquqa əsaslanan inkişaf prosesi, ABŞ-da ştatlar səviyyəsində parçalayıcı eksperimentlər və Çində mərkəzləşdirilmiş, siyasət yönümlü hüquqi tətbiq araşdırılır. Radar diaqramları, qrafik sütunlar və istilik xəritələri kimi müqayisəli vizuallaşdırmalar vasitəsilə tədqiqat müxtəlif səviyyələrdə institusional dəstək, kripto inteqrasiyası, istehlakçı hüquqlarının qorunması və hüquqi müəyyənlik olduğunu üzə çıxarır. Nəticələr göstərir ki, hər bir yurisdiksiya unikal tənzimləmə fəlsəfəsi ilə səciyyələnsə də, onlar eyni zamanda bir-birini tamamlayan blokçeyn idarəetməsi modellərini əks etdirir. Məqalə beynəlxalq biznes və idarəetmədə blokçeyn texnologiyasının təhlükəsiz, səmərəli və hüquqi cəhətdən bağlayıcı tətbiqi üçün qlobal əməkdaşlıq və standartlaşdırma zərurətini bir daha vurğulamaqla tamamlanır.

Açar sözlər: *Blokçeyn tənzimlənməsi, ağıllı müqavilələr, Aİ Data Act, MiCA, ABŞ hüquqi parçalanma, Çin BSN, müqayisəli təhlil*

Introduction

The current stage of society's digitalization requires not only applied developments with a purely practical focus, but also serious theoretical research that synthesizes practice and enriches legal doctrine. Legal science plays a significant role in addressing this challenge, as the concept of the rule of law obliges us to "saturate" all phenomena with legal content, to frame them within a legal structure, and to ensure they reflect a system for protecting fundamental rights.

The difficulty of treating technologies as subjects of legal reflection lies in the fact that they cannot be considered traditional objects that merely receive external regulation. The logic of applying digital technologies often requires users to adapt to them—to a certain extent, to submit to them. This indicates a profound feedback effect of technology on the state itself as the primary producer of law. The development of computer science led to the emergence of distributed ledger technology, which, in turn, became the foundation for the evolution of smart contracts in their most widely understood form.

Blockchain technology is a system for organizing a distributed database. One of its main advantages is that it functions as a public digital ledger, where every user action is visible to their counterparties and transactions cannot be altered or reversed retrospectively. Blockchain also enables online payments, helps optimize costs, allows for real-time verification of customer or transaction data, supports the registration of deals, and maintains transaction records.

Research

Although blockchain is not yet widely used in commercial operations, many large companies are actively testing its capabilities. In particular, the technology enables the creation of automated "smart contracts"—computer programs that come into effect once specific conditions are met. When parties enter into such a contract, its execution begins automatically and without direct involvement, which is undeniably another major advantage of this technology.

Blockchain technologies, in the form of smart contracts, enable decentralized legal contract automation without intermediaries. With accelerating adoption, regulatory clarity is now a prerequisite for innovation and investment. Divergent international approaches result from variations in legal traditions, policy preferences, and political institutions.

1. Smart Contracts

Smart contracts are digital agreements that can operate autonomously, allowing parties to transparently and conflict-free transfer digital and physical assets as well as other valuables (Hewa et al., 2021). Nick Szabo is considered the author of the smart contract concept. In 1994, he defined a smart contract as a computer protocol that independently executes transactions and controls their performance using mathematical algorithms. Satoshi Nakamoto also substantiated the idea of the smart contract in 2008 in the article *"Bitcoin: A Peer-to-Peer Electronic Cash System"* (Nakamoto, 2008). The number of bitcoins in circulation and the authority to create and transfer bitcoins are

tracked and controlled by a distributed database that runs on smart contract software. According to Nick Szabo, just as vending machines replaced human vendors, smart contracts are capable of displacing intermediaries in various industries.

First of all, it is important to note that the term "smart contract" can be defined both from a technical and a legal perspective. As noted by French researcher Gaëtan Guerlin, a distinction should be made between the program (the smart contract), which operates on a blockchain platform, and the traditional legal contract. As a result, the smart contract appears to be layered on top of the traditional civil-law agreement (Gaëtan, 2017, p. 512).

When there is a need to conclude a complex transaction involving a significant amount of money, we typically seek advice from a lawyer or notary, pay for their services, and then wait for the task to be completed and the contract terms to be fulfilled (Vatiero, 2023). Until the lawyer confirms that all the documents are properly executed, we cannot gain access to the funds or property. However, by placing a bitcoin in the ledger, one can instantly obtain a deed, contract, product, driver's license—anything stipulated by the smart contract.

Smart contracts act as a software intermediary between the consumer and the blockchain repository (Ferreira, 2021). They execute an algorithm necessary to provide a complex service upon the client's request, including actions such as status and identity verification and task completion. They allow users to store data in the blockchain repository and access it without the need for search. Access to the core structures of the blockchain repository is provided through a computer interface (Bandara et al., 2019).

The description of the terms and execution algorithm of smart contracts is written in a programming language and uses mathematical tools (such as public-key cryptography), which eliminates the grounds for discrepancies in the interpretation of the transaction terms.

Execution is also carried out automatically through the operation of pre-defined programs in a computer system, without the involvement of the parties, once specific conditions coded into the program are met. Records of obligations and completed transactions are stored with timestamping, cannot be altered by anyone, and are maintained in a distributed manner.

Experts from The Chamber of Digital Commerce identify several models for structuring a smart contract:

- **External model**: In this approach, the program code used by the parties does not replace the agreement itself but merely automates the performance of obligations under the contract.
- **Internal (or embedded) model**: This model involves formalizing the relationship between the parties in one of two ways. The code either fully replaces a natural language contract or serves as an integral part of such a contract.

In this context, researchers introduce two distinct terms: smart contract and legal smart contract.

A smart contract refers to computer code that, upon the occurrence of certain conditions or states, is capable of executing automatically in accordance with predefined functions. This code can be stored and processed on a distributed ledger and can record any resulting changes directly into it.

A legal smart contract, on the other hand, refers to contract terms that are both legally compliant and automated through programming code, forming a legally binding agreement between two or more parties.

A similar approach is reflected in a joint study by the International Swaps and Derivatives Association (ISDA) and Linklaters, where the terms legal smart contract and smart contract code are used to distinguish between the legal aspects of the agreement and the technological execution layer (ISDA Linklaters, 2017).

Thus, a smart contract as a technical phenomenon is essentially a piece of computer code. From the standpoint of technical sciences, a smart contract is a software code fragment designed to perform specific tasks when a pre-defined condition encoded in the program is met.

Regarding the legal nature of smart contracts, various perspectives are expressed in legal literature. The dominant group of researchers associates the concept of a smart contract exclusively with distributed ledger technologies, particularly blockchain platforms.

In the context of using blockchain platforms, a smart contract can be concluded in two ways:

- In the form of an application using an electronic signature, executed pursuant to a framework agreement established upon entry into the blockchain;
- Through a click-wrap agreement, where the terms are accepted by ticking the "Agree" box.

Interaction between the parties occurs in an electronic environment and is aimed at transferring a digital asset, which may include cryptocurrency (e.g., Bitcoin). In order to enable transactions to be executed via a smart contract, it is sometimes necessary that the asset subject to the agreement be linked to a virtual unit operated by the computer program.

To achieve this, material or immaterial assets must be "moved" into the virtual environment and represented in a digital form. These virtual units, used as conditional units of value, are called tokens.

There are several types of smart contracts, such as legal smart contracts and Ricardian contracts. Smart contracts can be used in various business processes, asset trading, and other types of transactions, with the specific details determined by the parties involved, depending on the level of cooperation and desired outcomes (Ji et al., 2023; Ante, 2021). Any event or situation—such as changes in financial market indicators or a user's GPS coordinates—can trigger the execution of a smart contract either by the parties themselves or on their behalf (Wang et al., 2023a). When the conditions of the computer program are met, it is executed automatically without human intervention. Communication between smart contract participants can be verified and securely transmitted in encrypted form (Kirli et al., 2022).

Currently, the most widely used platform for creating and executing smart contracts is Ethereum, although other blockchain-based cryptocurrencies like EOS, Neo, Tezos, Tron, Polkadot, and Algorand also support smart contract functionality (Liu et al., 2023). After the execution of a smart contract, each server in the network updates the record reflecting the current operational state of the network. Once uploaded to the blockchain and verified, the document cannot be altered. The issue of authenticity in international trade contracts can be effectively addressed through the immutable and distributed nature of blockchain (Wang et al., 2023b).

The Ethereum Virtual Machine (EVM) manages the execution of smart contracts on the Ethereum blockchain (Liu et al., 2022). Before a smart contract can be executed on a particular blockchain, a transaction fee, known as the “gas fee”, must be paid. The more complex the operations of the smart contract, the higher the gas fee. This mechanism is designed to protect the EVM from overload caused by overly complex or numerous smart contracts.

“Gas” can be metaphorically described as the driving force that powers the execution of Ethereum smart contracts. A shortage of gas can prevent the network from processing transactions. Each transaction incurs a gas fee, and its execution depends on how contracts are distributed across the network. A significant amount of computational resources is required to complete these transactions, and the complexity of the computation determines the amount of gas required.

Based on the positions presented, it can be concluded that the fulfillment of obligations by a party under a smart contract occurs upon the occurrence of certain conditions—some of which may depend on the will of the party, and some of which may not.

Regarding the question of whether a smart contract can be qualified as an adhesion contract, it is important to consider that the terms of a smart contract may be predefined and publicly accessible to all potential participants, as they are recorded in a publicly available blockchain. However, it should also be taken into account that some blockchain platforms are public, while others are private and allow participation only by certain individuals or companies.

In the latter case, the classification of a smart contract as an adhesion contract may differ: in a private platform, the typical features of an adhesion contract—such as the unilateral establishment of terms by one party—may not be present.

Referring to foreign practice, it is also evident that the definition of the nature of smart contracts is closely linked to their functioning within blockchain platforms.

One of the most notable early examples of a smart contract in action occurred in the autumn of 2016, when a $100,000 cheese and butter supply deal was executed between an Israeli producer, Ornua, and a Seychelles-based company. The buyer used a letter of credit for payment, facilitated by blockchain technology.

The goods were shipped by sea, and the containers were equipped with special geolocation sensors. As soon as the vessel entered the destination port, the sensors sent a signal to the blockchain system, indicating that the bank could release payment to the seller.

Thanks to blockchain, the entire transaction was completed in just 4 hours, compared to the usual 10 days under traditional conditions. Moreover, there was no need to exchange physical documents, and the risk of document forgery was completely eliminated.

It is also worth noting that smart contracts can be used for lending purposes. For example, one of the largest banking institutions in Spain, Banco Bilbao Vizcaya Argentaria (BBVA), issued a €75 million corporate loan using a smart contract on the Ethereum blockchain network. The use of distributed ledger technology (DLT) and smart contracts significantly reduces fraud risks and minimizes time-related transaction costs. This particular operation took only a few hours, whereas traditional mechanisms would typically require several days.

Another notable example is the German insurance company Allianz, which has implemented smart contracts to automate insurance payouts in the event of natural disasters. This use of blockchain-based automation improves efficiency, speeds up response time, and reduces administrative overhead in critical situations.

2. Legal İntegration of Smart Contracts

A smart contract can be integrated into a transaction in one of the following ways:

- **Fully in programming language** – the contract is written entirely in code, with no version in natural language.

This method is the least suitable for comprehensive transactions, as such contracts often include terms that do not require automation—such as choice of dispute resolution venue, representations, or warranties.

- **Duplication model** – the contract is written in programming code and also has a full copy in natural language. This ensures both machine-readability and legal clarity for human interpretation.

- **Hybrid model** – the contract is drafted in natural language, but some of its provisions are implemented and executed via code. This model is the most common in practice, as it combines legal expressiveness with the automation of specific clauses.

The most logical model today is the hybrid model, where part of the contract is written in natural language, and part is implemented as a smart contract.

For example, the algorithm may define the pricing mechanism and set triggers that initiate payment. Meanwhile, other provisions—such as dispute resolution procedures, representations and warranties, product descriptions, or force majeure clauses—are drafted in natural language.

Over time, another form of hybrid automation may gain popularity: one where natural language complements the code, rather than code being embedded into a paper contract. This approach is useful in cases where it is not feasible to codify all aspects of the agreement at an acceptable level of clarity.

Currently, such functionality is offered by the Corda blockchain developed by R3. In Corda, smart contracts include both a code-based component and a feature called Legal Prose—an embedded section of natural language text that provides legal context directly within the contract's framework.

When choosing the hybrid model for legally integrating a smart contract, the question arises: how to formally reflect the smart contract's terms within the main agreement. This reflection must affirm the genuine intent of the parties to be bound by its automated execution.

One option is to reference an external source in the agreement that contains the smart contract—such as a URL or address on a blockchain platform. An alternative approach is to duplicate the algorithm's logic in natural language within the contract.

Regardless of the method chosen, the natural language contract should ideally include the following elements:

- A statement that a specific part of the agreement is automated and executed via a program (smart contract), along with a description of the program's characteristics; this may include details on how the program interacts with the parties;
- An acknowledgment by the parties that they recognize the legal validity of such automated execution;
- A clause defining the precedence between the code and the natural language text in case of conflict;
- A mutual agreement to use electronic communication and to transfer assets via the smart contract system.

These provisions help ensure that the smart contract is properly embedded in the legal framework of the overall transaction, and that its execution reflects the parties' legal obligations.

In the hybrid model, the parties sign a natural language agreement that includes a reference to the smart contract. Additionally, a hash of this document can be stored in the distributed ledger, serving as a secure and immutable verification of the agreement's contents.

The smart contract itself can also be programmed to require signatures from specific participants. Before executing any actions, the program will prompt for and verify the required signatures from the designated parties.

Signature mechanisms vary across different blockchain platforms, depending on the underlying protocol and cryptographic framework. Some use basic public-private key encryption, while others incorporate multi-signature schemes, zero-knowledge proofs, or threshold signature systems to enhance security and enforce participation rules.

For example, on the Ethereum blockchain, a signature is generated by the user through their private key, which is created using the system's cryptographic protocol. Each transaction, including those involving smart contracts, is signed with this private key and then broadcast to the network for validation (Zhai et al., 2019).

In contrast, Hyperledger Fabric offers a more flexible approach. It allows users to upload and manage their own signing mechanisms (e.g., through hardware security modules or external cryptographic services). This is possible because Fabric is designed as a permissioned blockchain, giving organizations more control over identity management, access rights, and security protocols (Antwi et al., 2021).

Among those who need to understand the content of smart contracts are not only the contracting parties, but also regulatory authorities.

Currently, the law does not provide for any special procedures for presenting agreements involving smart contracts to regulatory bodies. As such, these contracts can be submitted in the usual manner, following standard document protocols.

In practice, there may be challenges in interpreting the logic embedded in a smart contract, as well as in assessing whether the algorithm truly reflects the intent of the parties and their actual relationship. However, the mere integration of a smart contract into a transaction does not obstruct the understanding of its legal substance.

At present, regulatory authorities have all the necessary means to obtain relevant information and to determine what the parties have agreed upon.

Nevertheless, it is important to remember that the use of smart contracts does not eliminate the obligation to prepare primary documentation in traditional form—such as invoices, shipping records, or other formal documents required for accounting and compliance purposes.

3. Smart Contracts in European Union

On April 11, 2018, for more comprehensive regulation, twenty-two European countries signed an agreement to establish the European Blockchain Partnership (EBP). This coalition includes nations such as the Netherlands, Germany, France, Norway, Spain, and others. The declaration states (Liakopoulos, 2024):

"In order to harness the opportunities of blockchain technologies and to avoid a fragmented approach, the signatories of this declaration agree to cooperate in creating a European Partnership for the development of blockchain infrastructure, which will help improve trustworthy and user-centric digital services within the Single Market."

The EU countries committed to sharing expertise and knowledge in both technical and regulatory domains, and to preparing for the launch of unified EU-wide applications that utilize distributed ledger technology (DLT) for use in both the public and private sectors.

According to Mariya Gabriel, the European Commissioner for Digital Economy and Society, blockchain represents an excellent opportunity for Europe and its member states to rethink their information systems, enhance user trust and personal data security, promote new business opportunities, and develop new areas of leadership for the benefit of citizens, public services, and business entities (Maslova, 2018).

The concept of an "e-resident" first emerged in Estonia in 2014. People from around the world participated in a digital program, becoming digital residents and registering companies in Estonia. In contrast to this centralized model, a blockchain movement arose, aimed at decentralizing services. As a logical next step, Estonia's E-Residency Program was integrated with blockchain technology. Today, the E-Estonia program operates on the Ethereum blockchain.

Although the official preparation for launching Initial Coin Offerings (ICOs) in Estonia is still underway, the digital currency ESTcoin was created to add a new dimension and convenience to the e-residency program. Looking ahead, the e-residency ecosystem is expected to undergo further enhancements (Kim, 2023).

On March 14, 2023, the European Parliament approved new data control measures as part of a major legislative package on data privacy. The bill is aimed at addressing the protection of digital privacy without hindering innovation.

According to the new provision in the Data Act, all smart contracts are now required to include an "emergency kill switch." In the event of a security breach, IT professionals can use this kill switch method to immediately shut down the system. When a critical flaw or attack is detected, the kill switch embedded in the smart contract's code can either terminate the contract's execution immediately or suspend it, fix the issue, and restart the contract.

Legislation on smart contracts and the Internet of Things was approved by the European Parliament on March 14, 2023, as part of the Data Act, with an overwhelming majority (500 votes in favor and 23 against). The goal of this legislation is to promote the development of business models that foster the emergence of new industries and employment opportunities.

Article 30 of the Data Act outlines the core prerequisites related to smart contracts for data sharing (Casolari et al., 2023). Starting in 2024, corporations offering goods or services to consumers within the European Union must comply with the new rules. Although the content of the law has already been approved by the European Parliament, it is currently under final discussion. Once adopted, there will be a 12-month implementation period.

Implementation of the Data Act requires the establishment of effective termination mechanisms for smart contracts. These mechanisms may include internal functions that allow for the cancellation of the contract or issue a command to terminate it. The law demands a clear definition of the conditions that justify termination or suspension of a smart contract. In the IT domain, administrators frequently use a "kill switch" mechanism to shut down a device, network, or software in response to a security threat (Philip & Saravanaguru, 2022). In the context of smart contracts, this kill switch

should either terminate the contract or initiate a process of suspension, correction, and potential reactivation if a critical vulnerability or violation is detected (Chu et al., 2023).

The Data Act is a landmark initiative aimed at increasing data accessibility in line with EU principles and rules. It forms a core component of the European data strategy, significantly contributing to the digital transformation objectives outlined in the "Digital Decade" initiative.

Compliance with the core principles will be assessed by the developer or provider of the smart contract, who will be required to submit an EU declaration of conformity and bear responsibility for ensuring compliance with essential requirements. However, the exact interpretation of the term "responsibility" in this context remains ambiguous, and it is still unclear whether users of smart contracts will bear any civil liability. In cases of non-compliance with regulatory requirements, consequences will be determined by the legislation of the relevant EU member state.

4. Smart Contracts in the UK

As part of the UK government's "Innovate UK" program, the sale of Blockchain as a Service (BaaS) technology began on August 3, 2016. The UK's HM Revenue and Customs (HMRC) is exploring the potential of blockchain, along with other technical tools, to improve the tax, customs, and excise systems (Alexander, 2022).

In May 2016, the Parliamentary Office of Science and Technology (POST) published a brief report on financial technologies, focusing on four innovative areas, one of which was Distributed Ledger Technology (DLT). In January 2018, POST released a follow-up document titled "Areas of Interest," identifying DLT as a field that requires further research. The UK Department for Work and Pensions, in collaboration with the company GovCoin, conducted a study examining the potential of blockchain technology to enhance the welfare system (Hughes et al., 2018).

According to a report prepared by the UK Government Office for Science, several critical considerations and recommendations have been outlined regarding the legal and practical implementation of smart contracts. The report emphasizes the following key points:

- Smart contracts are contracts whose terms are written in programming code. This definition highlights that their enforceability and logic are embedded directly in code rather than in natural language.

- Criteria must be developed to determine the jurisdiction applicable to a smart contract. Given the cross-border nature of blockchain, clearly defining which legal system governs a smart contract is essential for dispute resolution and enforceability.

- Mechanisms should be developed to validate transactions without exposing their full content, and there is a need to establish legal regulation for data provided by oracles. Oracles, which deliver external data to blockchain systems, present a legal and technical vulnerability. The authenticity, reliability, and legal accountability of these data inputs must be addressed.

- Effective identification and authentication protocols must be implemented for both individuals and organizations. Ensuring that participants in smart contracts are properly identified is crucial for security, fraud prevention, and regulatory compliance.

- Security standards should be established for wallet providers. Digital wallets used to manage blockchain assets need to comply with robust cybersecurity standards to protect users from theft, hacking, or unauthorized access.

- In consumer-related smart contracts, the design should require minimal technical knowledge from the consumer. There should be a limited number of choices and configurations, and consumers must be given a clear understanding of the consequences of entering into an agreement via a programmatic algorithm.

In 2019, the UK Jurisdiction Taskforce (UKJT) concluded that the enforceability of smart contracts depends on the specific circumstances of each case. The Law Commission was tasked with evaluating the adequacy of existing legal frameworks in relation to smart contract governance, identifying legal ambiguities, and recommending new or updated legislation if necessary (Ferro et al., 2023).

However, despite ongoing legislative efforts, there remains a lack of research assessing the effectiveness of these regulatory measures (Blaszczyk, 2023).

According to the Thirteenth Program of Law Reform, issued under the direction of the Lord Chancellor, the Law Commission was tasked with conducting research and analysis in the field of legal smart contracts. In November 2019, the UK Jurisdiction Taskforce published an official statement on crypto-assets and smart contracts, affirming that smart contracts have the potential to create legally binding obligations that can be enforced according to their terms.

Following this, the Ministry of Justice requested the Law Commission to conduct a comprehensive review of the existing legal framework governing smart contracts. The Commission undertook further analysis to identify any legal gaps or uncertainties and determine whether additional research is necessary either now or in the future.

When legal disputes arise over smart contracts, courts rely on a specialized interpretive guidance, which states that the meaning of the code used in the contract should be assessed from the perspective of a rational programmer with relevant expertise, considering all contextual information available to the parties at the time the contract was formed. The Law Commission emphasized that even legally binding agreements composed entirely of code should be subject to legal interpretation, as there can be a discrepancy between the intended meaning of the code and its actual execution. This stems from the difference between the semantic interpretation of code and its practical application.

Incorporating code into the framework of legal interpretation may lead to challenges in understanding contractual intent. To address this, the Commission recommends using the standard legal test, which bases interpretation on the understanding of a reasonably informed expert in the relevant field (Durovic & Willett, 2023). This method is currently the dominant approach in contract interpretation.

The importance of legal certainty cannot be overstated. Notably, English law has been recognized as capable of incorporating smart contracts, ensuring legal protection for parties involved in international commercial agreements executed via digital technologies—provided these contracts fall under the jurisdiction of English law. The Law Commission's report also outlines key factors that contracting parties should consider, which is especially relevant for stakeholders in the decentralized finance (DeFi) sector.

5. Smart Contracts in the USA

The United States was one of the first countries where smart contracts became the subject of legislative initiatives. Several states have introduced or enacted laws recognizing the legal validity of blockchain-based contracts and digital signatures, laying the groundwork for the broader adoption of smart contracts in legal and commercial contexts. In the United States, the legislation of several states provides specific regulations governing relationships involving the conclusion and execution of smart contracts (Ferreira, 2021).

Arizona was an early leader in this area, legally recognizing the enforceability of signatures stored on the blockchain. Under Arizona law, smart contracts and blockchain-based signatures have the same legal status as traditional contracts and electronic signatures. According to Arizona law, a *smart contract* is defined as a program triggered by real-world events, operating within a distributed, decentralized, multi-user, and replicable ledger. The contract is capable of managing and transferring assets within this ledger environment.

In New York a bill has been introduced aiming to establish legal definitions relevant to blockchain technology. The proposal includes the incorporation of terms such as:

- “Blockchain technology”
- “Smart contracts”
- “Digital signatures stored on blockchain”

These definitions are to be added to New York’s technology law, providing a formal framework for the legal treatment of smart contracts.

In Florida, blockchain ledgers and smart contracts are legally recognized as valid methods for data storage, provided they do not violate existing laws and regulations. Key provisions include:

- A signature recorded on a blockchain qualifies as a valid electronic signature.
- If the parties agree to use blockchain for data storage, that source is deemed legally admissible.
- Notably, Florida law states (Plass, 2020):

"A contract shall not be denied legal effect or enforceability solely because an electronic record was used in its formation or because the contract contains terms recorded as a smart contract."

Tennessee has adopted clear recognition of blockchain-protected signatures, stating:

"A signature secured through blockchain technology is considered an electronic signature and constitutes a digital electronic signature."

Additionally: *"A record or contract that is secured using blockchain technology is considered an electronic record"* (Credle et al., 2025).

Tennessee also recognizes the legal validity of smart contracts or self-executing agreements, provided they activate upon the fulfillment of predefined conditions.

Furthermore, legislative initiatives related to smart contracts are actively being considered in other states, including Delaware, Nebraska, and Vermont.

Vermont is considering a bill that would allow blockchain records to be used as evidence in court. A blockchain record is considered authentic if it is supported by a written statement or certification that includes the date and time the record was entered or received. This initiative aims to enhance legal recognition and evidentiary value of blockchain data in judicial proceedings.

Nebraska has recognized the validity of using smart contracts in commercial transactions.

- The legislation explicitly states:

"A smart contract or a contract that contains a smart contract provision may be used in commerce. Such a contract shall not be denied legal effect, validity, or enforceability solely because it is a smart contract or contains a smart contract provision" (Plass, 2020).

However, a blockchain entry qualifies as a digital signature only if all parties to the agreement have expressly agreed to use such an electronic mechanism.

Delaware has proposed legislation to use blockchain for maintaining business entity records and to manage corporate records via smart contracts. The bill promotes the use of distributed ledger technology in corporate governance, enabling corporations to handle tasks such as shareholder records, board resolutions, and ownership structures more efficiently and transparently.

These efforts reflect a national trend toward formalizing the legal status of blockchain-based agreements and expanding their application across digital transactions and decentralized platforms. These state-level initiatives illustrate the decentralized legislative approach of the U.S., where individual jurisdictions tailor blockchain and smart contract laws to their economic, legal, and technological priorities. Together, they signal growing institutional acceptance of blockchain applications in law, commerce, and corporate governance.

6. Smart Contracts in China

China, which is actively digitizing its judicial system nationwide, has taken a leading position in the regulatory development of blockchain and smart contract technologies. The actions of the Chinese government appear more consistent and comprehensive compared to many other countries, reflecting a strategic and centralized approach to legal innovation.

A clear example of this can be seen in a landmark court case:

In January 2017, the Chinese media company Huatai Yimei filed a lawsuit against an IT firm from Shenzhen for intellectual property infringement. As part of its evidence, the plaintiff submitted blockchain records, having registered all of its digital content on a blockchain platform (De León & Santamaria, 2022).

The Hangzhou Internet Court ruled in favor of the plaintiff, recognizing the blockchain entries as valid legal evidence. This decision marked the first case in China's judicial practice where blockchain was accepted as proof in a copyright infringement dispute.

Since then, many Chinese legal experts have acknowledged blockchain as a "reliable, efficient, user-friendly, and cost-effective tool" for evidence preservation and rights protection. The case set a precedent and accelerated the formal integration of blockchain technology into China's legal infrastructure, particularly in areas such as digital copyright, contract enforcement, and online dispute resolution.

In June 2018, the Hangzhou Internet Court in China, which specializes in internet-related cases, issued a landmark ruling stating that data uploaded to a blockchain can be used as evidence in legal proceedings (Papagianneas, 2024).

To assess the reliability of electronic evidence stored on the blockchain, the court conducted a thorough examination of the integrity of the uploaded data. It concluded that:

- Electronic data preserved and protected by technical means, such as blockchain, must be evaluated and determined on a case-by-case basis.
- Courts should not reject technologies like blockchain or apply higher evidentiary standards simply because these tools are innovative or technically complex.
- At the same time, the standard of evaluation should not be lowered merely because blockchain is resistant to tampering or deletion.

The court emphasized that the transparency and immutability of blockchain make it particularly valuable not only for litigation evidence but also as a tool for protecting unregistered intellectual property rights.

Indeed, blockchain-based registration can document and make publicly accessible key details related to the creation of a work, such as the time of creation, rights holder's identity, and ownership chain. Furthermore, while it is typically difficult to distinguish between different copies of the same copyrighted work, the use of a unique cryptographic hash function enables tracking the individual distribution history of each copy via the blockchain.

In this way, blockchain presents itself as a promising tool to enhance the efficiency and transparency of the intellectual property market. However, the court acknowledged that significant tensions remain between the technical design of blockchain systems and their legal framework, which still needs further development and harmonization.

This regulation formally integrates blockchain evidence into the judicial process, reinforcing China's position as a global leader in legal and technological innovation in the digital era.

7. Comparative Insights

The European Union operates on a harmonized rules-based system and aims to harmonize member state laws into comprehensive legislation such as the Markets in Crypto-Assets Regulation (MiCA) and the Data Act. These legislations provide legal certainty for smart contracts, including requirements for kill switches and data access protocols, and promote innovation using regulatory sandboxes and the EU Blockchain Observatory.

In contrast, the United States possesses a fractured and case-based system. Legal recognition of smart contracts heavily depends on state actions (e.g., Tennessee, Arizona) since federal organizations like the SEC and CFTC implement blockchain applications differently. Though the U.S. enjoys high private sector innovation, regulatory unpredictability—most notably concerning crypto integration—contributes to the uncertainty and hinders legal foreseeability.

China has a centralized, policy-oriented system. Cryptocurrency is prohibited for public use, but blockchain and smart contracts are promoted in state-controlled domains like the Blockchain-based Service Network (BSN). Blockchain data have already been recognized by courts as evidence, and the government actively promotes blockchain for administrative and judicial applications, with high legal certainty maintained under tightly controlled limits.

The United Kingdom, with its common law background, is a principles-based and evolutionary strategy. Judicial finding and institutional contribution, like that of the UK Jurisdiction Taskforce and the Law Commission, are propelling legal certainty and have established the enforceability of smart contracts and explored their use in contract law. Innovate UK and the application of blockchain to

company governance (e.g., in Delaware-style initiatives) represent some of the rising institutional action (Table 1).

Table 1: Comparative Insights from Key Jurisdictions.

Feature/Region	EU	US	China	UK
Regulatory Style	Harmonized, rules-based	Fragmented, case-driven	Centralized, policy-driven	Principles-based, evolving through common law
Smart Contracts	Regulated under Data Act & eIDAS	Recognized under common law	Supported via BSN, tightly controlled	Recognized via UKJT guidance; enforceability confirmed by courts
Innovation Support	Sandboxes, EU Blockchain Observatory	Private sector-led	Government-driven	Government-backed initiatives (Innovate UK, Law Commission studies)
Crypto Integration	Legalized under MiCA	Ambiguous, agency-dependent	Prohibited for public use	Permitted under strict AML and FCA oversight
Legal Certainty	Increasing with MiCA and Data Act	Varies by state and agency	High, but innovation limited by state controls	Strengthening through case law and Law Commission clarification

Source: Author's own.

Figure 1 illustrates comparative radar chart for the mentioned countries' smart contract implementation.

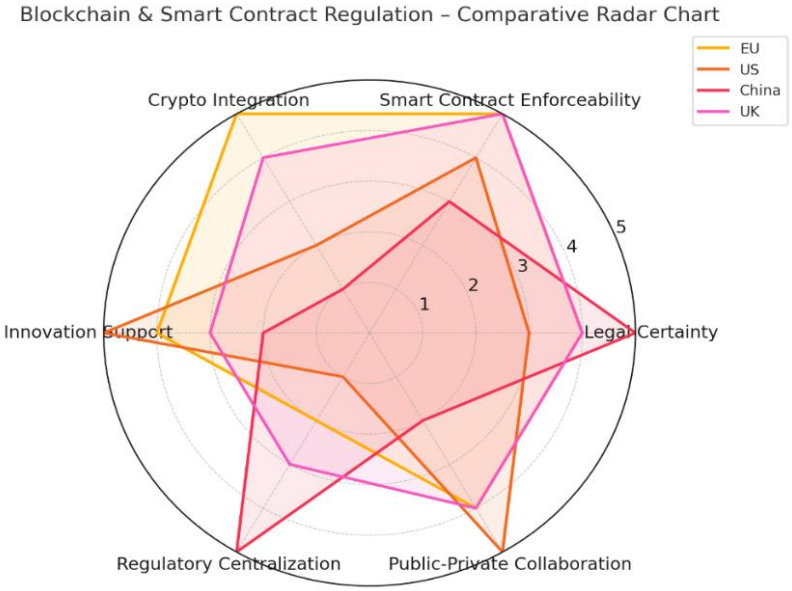

Figure 1: Blochchain and Smart Contract Regulation
Source: Author's own

This radar chart visually compares the regulatory landscapes of the EU, US, China, and the UK across six key dimensions of blockchain and smart contract governance. It can be observed from the chart that:

- The EU scores high on legal certainty and harmonized smart contract enforceability.
- The US excels in innovation support and public-private collaboration but is weaker in regulatory coherence.
- China has strong centralization and legal certainty but limited crypto integration and innovation freedom.
- The UK balances legal clarity with adaptable enforcement and strong collaboration, sitting between the EU and US models.

Figure 2 Presents legal and technical coverage of blockchain features.

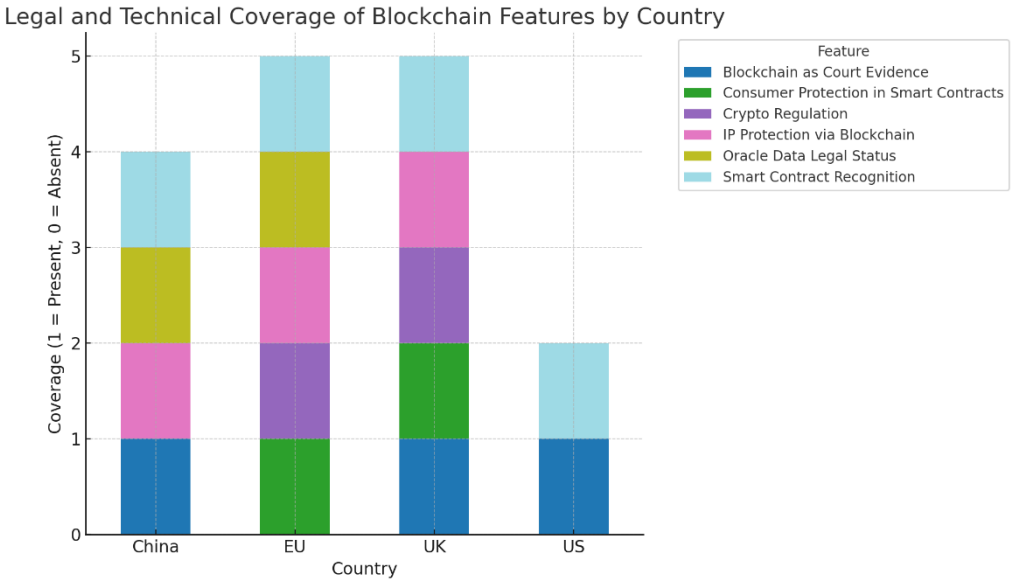

Figure 2: Legal and Technical Coverage of Blockchain Features by Country
Source: Author's own

The stacked bar graph shows considerable divergence in how the European Union, the United States, China, and the United Kingdom address the legal and technical aspects of blockchain adoption. The EU has a wide-ranging and forward-thinking approach, covering most key areas, including intellectual property protection, legal recognition of smart contracts, consumer protection, and regulation of oracles. This reflects the EU's style in developing a ordered and harmonized digital legal framework.

The United States is patchier and more selective. While smart contract recognition and the admissibility of blockchain records into evidence in court are resolved in some states, other key areas like consumer protection and oracle data governance are undeveloped or nonexistent. The patchiness is in line with the US's decentralized regulatory framework, under which individual states do their own thing on blockchain policy.

China stands out in its judicial embrace of blockchain, especially in embracing it as legal evidence and in enabling IP protection through distributed ledgers. Nevertheless, despite such prowess, consumer protection and public crypto use rank limited, echoing the state's fixation on centralized control at the expense of innovation flexibility.

The United Kingdom presents a balanced profile. It has adopted legal norms recognizing blockchain as a method of IP protection, enforcement of smart contracts, and court evidence, and has also facilitated crypto regulation and consumer protection regimes. However, the legal handling of oracle data remains less advanced, indicating one direction in which regulatory elaboration can be focused going forward.

Overall, the chart evidences a spectrum of regulatory maturity, with the EU and UK showing broad and deep engagement, the US proceeding apace in pockets, and China at the forefront of centralized legal integration but with pinpoint constraints.

Figure 3 Illustrates regulatory intensity by feature and jurisdiction.

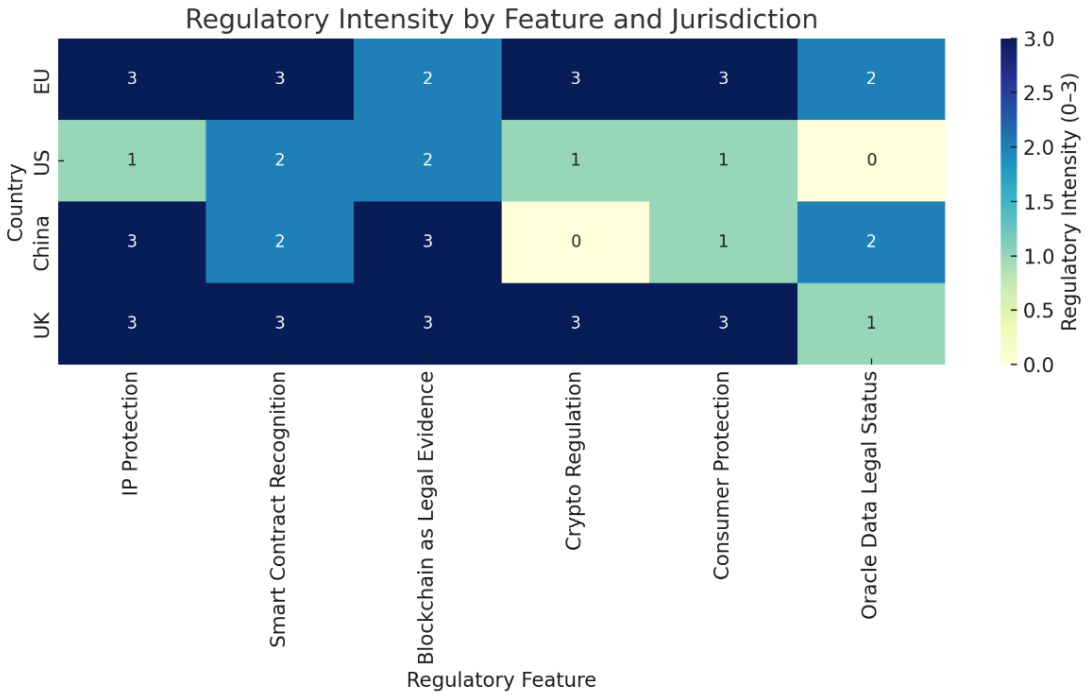

Figure 3: Regulatory Intensity by Feature and Jurisdiction
Source: Author's own

The heatmap in Figure 3 visually compares the regulatory intensity of blockchain-related features across the EU, US, China, and the UK on a scale from 0 (none) to 3 (high).

EU and UK show invariably high regulatory engagement across most dimensions, namely intellectual property protection, smart contract recognition, and consumer protection. This shows that they have robust institutional efforts to integrate blockchain within conventional legal frameworks.

The US is moderately advanced in the areas of smart contract recognition and admissibility of blockchain evidence but lags behind in consumer protection, crypto regulation, and legal certainty around oracle data. This echoes its decentralized, state-led legal evolution.

China performs highly in blockchain legal evidence and IP protection but less highly in crypto regulation and consumer-friendly legal support, consistent with its centralized but narrow scope blockchain approach.

The chart readily discloses the UK's and EU's evenhanded and forward-looking approach, China's strategic but constrained application, and the US's patchwork regulatory framework supported by fragmented jurisdictional authority.

Together, these jurisdictions present four different but complementary models of integrating blockchain and smart contracts into legal systems: the EU's codified uniformity, the U.S.'s decentralized experimentation, China's strategic centralization, and the UK's adaptive pragmatism.

Conclusion

Cross-regional analysis of smart contract regulation in the European Union, United Kingdom, United States and China demonstrates the emergence of four divergent yet linked models of legal

governance for the digital age. Each portrays more significant institutional philosophies, legal traditions and policy responses to the integration of blockchain technology.

The European Union is a harmonized and codified approach built on large legal documents such as the MiCA Regulation and Data Act to codify the standards for smart contracts, digital assets, and distributed ledger infrastructure. Its process is rooted in legal certainty, cross-border consistency, and promoting innovation through regulatory sandboxes and observatories.

The United States, in contrast, demonstrates a decentralized and fragmented regulatory environment where states like Arizona, Tennessee, and New York take the lead in legislation but federal consensus remains elusive. This patchwork model encourages rapid innovation and experimentation in some jurisdictions but undermines national consistency and legal certainty, notably in consumer protection and crypto regulation.

China offers the case of strategic centralization, where blockchain technologies like smart contracts are fully implemented within a highly controlled framework. Legal certainty is reflected in court recognition of blockchain evidence and institutional incorporation into administration systems. However, application scope remains restricted by a ban on public cryptocurrency use and central management over digital infrastructures.

The United Kingdom, with a common law heritage, illustrates a principles-based, evolutionary model of legal adaptation. Through research sponsored by government (e.g., UKJT and the Law Commission), judicial interpretation, and targeted regulatory guidance, the UK leaves private innovation room with the dignity of public guidance. It reaches a clear balance between legal enforceability and regulatory minimalism, thereby emerging as an adaptive jurisdiction for emerging digital contracting models.

Together, these regimes provide four alternative models—the EU's centralized rule-making, the US's decentralized innovation, China's highly controlled integration, and the UK's dynamic legal development. If each finds its foundation in differing national priorities, they as a whole lend richness to world debate over how blockchain technology and smart contracts can coexist with legal norms, institutional arrangements, and democratic government. In the future, global conversation, mutual legal recognition, and technical standardization shall have vital roles to play in combining these models into a single global legal framework for decentralized digital systems.

References

1. Alexander, G. (2022). Blocking the gap: the potential for blockchain technology to secure VAT compliance. EC Tax Review, 31(3).
2. Ante, L. (2021). Smart contracts on the blockchain – A bibliometric analysis and review. Telematics and Informatics, 57, 101519.
3. Antwi, M., Adnane, A., Ahmad, F., Hussain, R., ur Rehman, M. H., & Kerrache, C. A. (2021). The case of HyperLedger Fabric as a blockchain solution for healthcare applications. Blockchain: Research and Applications, 2(1), 100012.
4. Bandara, E., Ng, W. K., Ranasinghe, N., & De Zoysa, K. (2019). Aplos: Smart Contracts made smart. In J. F. Ashish, Gh. R. Oliveira, P. L. Zhou (Eds.), Communications in Computer and Information Science (pp. 431–445).
5. Blaszczyk, M. (2023). Smart contracts, Lex cryptographia, and transnational contract theory. SSRN.
6. Casolari, F., Taddeo, M., Turillazzi, A., & Floridi, L. (2023). How to improve smart contracts in the European Union Data Act. Digital Society, 2(1).
7. Chu, H., Zhang, P., Dong, H., Xiao, Y., Shunhui, J., & Wenrui, L. (2023). A survey on smart contract vulnerabilities: Data sources, detection and repair. Information and Software Technology, 159(107221).

8. Credle, S., Harun, N. F., Johnson, G., Lawrence, J., Lawson, C., Hollern, J., ... & Tucker, D. (2025). Blockchain Research and Development Activities Sponsored by the US Department of Energy and Utility Sector. Energies (19961073), 18(3).
9. De León, I., & Santamaria, E. (2022). The Institutional Change of Intellectual Property Commercialization. In The Emerald Handbook of Entrepreneurship in Latin America (pp. 63-86). Emerald Publishing Limited.
10. Durovic, M., & Willett, C. (2023). A legal framework for using smart contracts in Consumer Contracts: Machines as servants, not masters. The Modern Law Review.
11. Ferreira, A. (2021). Regulating smart contracts: Legal revolution or simply evolution? Telecommunications Policy, 45(2), 102081.
12. Ferro, E., Saltarella, M., Rotondi, D., Giovanelli, M., Corrias, G., Moncada, R., Cavallaro, A., & Favenza, A. (2023). Digital assets rights management through smart legal contracts and smart contracts. Blockchain: Research and Applications, 4(3), 100142.
13. Gaëtan Guerlin. Considerations sur les smart contracts // Dalloz IP/IT. Droit de la propriete intellectuelle et du numerique. 2017. № 10. pp. 512—513.
14. Hewa, T., Ylianttila, M., & Liyanage, M. (2021). Survey on blockchain based smart contracts: Applications, opportunities and challenges. Journal of Network and Computer Applications, 177, 102857.
15. Hughes, E., Graham, L., Rowley, L., & Lowe, R. (2018, July 1). Unlocking blockchain: Embracing new technologies to drive efficiency and empower the citizen. The Journal of The British Blockchain Association, 1(1), 63–72.
16. Ji, B., Zhang, M., Xing, L., Li, X., Li, Ch., Han, C., & Wen, H. (2023). Research on optimal intelligent routing algorithm for IoV with machine learning and smart contract. Digital Communications and Networks, 9(1), 47–55.
17. Kim, N. (2023). National ID for public purpose. Georgetown Law Technology Review, 7(2).
18. Kirli, D., Couraud, B., Robu, V., & Salgado-Bravo, M. (2022). Smart contracts in energy systems: A systematic review of fundamental approaches and implementations. Renewable and Sustainable Energy Reviews, 158, 112013.
19. Liakopoulos, D. (2024). The future of European defence through blockchain as a way to integrate, fill gaps and address the crises of wars in a European context. Public Security and Public Order, (36), 124-134.
20. Liu, H., Fan, Y., Feng, L., & Wei, Z. (2023). Vulnerable smart contract function locating based on Multi-Relational Nested Graph Convolutional Network. Journal of Systems and Software, 204, 111775.
21. Liu, L., Wei-Tek, T., Zakirulm A., Hao, P., & Mingsheng, L. (2022). Blockchain-enabled fraud discovery through abnormal smart contract detection on Ethereum. Future Generation Computer Systems, 128, 158–166.
22. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. http://dx.doi.org/10.2139/ssrn.3440802
23. Natalia Maslova, C. M. A., & CTP, P. (2018). Blockchain: Disruption and opportunity. Strategic Finance, 100(1), 24-29.
24. Papagianneas, S. (2024). Smart courts, smart justice? automation and digitisation of courts in China. Asian Journal of Law and Society, 1, 27.
25. Philip, A., & Saravanaguru, R. (2022). Smart contract based digital evidence management framework over blockchain for vehicle accident investigation in IoV era. Journal of King Saud University – Computer and Information Sciences, 34(7), 4031–4046.
26. Plass, S. A. (2020). Federalizing Contract Law. Lewis & Clark L. Rev., 24, 191.
27. Smart Contracts and Distributed Ledger — A Legal Perspective // ISDA Linklaters. August 2017. pp. 4—5.

28. Vatiero, M. (2023). Smart contracts vs incomplete contracts: A transaction cost economics viewpoint. Computer Law & Security Review, 46, 105710.
29. Wang, L., Cheng, H., Zheng, Z., Yang, A., & Xu, M. (2023b). Temporal transaction information-aware Ponzi scheme detection for ethereum smart contracts. Engineering Applications of Artificial Intelligence, 126, Part C, 107022.
30. Wang, Y., Chen, X., Huang, Y., & Hao-Nan, Z. (2023a). An empirical study on real bug fixes from solidity smart contract projects. Journal of Systems and Software, 204, 111787.
31. Zhai, S., Yang, Y., Li, J., Qiu, C., & Zhao, J. (2019, February). Research on the Application of Cryptography on the Blockchain. In Journal of Physics: Conference Series (Vol. 1168, p. 032077). IOP Publishing.

Received: 31.03.2025
Accepted: 29.05.2025