Access to Justice in Eastern Europe
ISSN 2663-0575 (Print)
ISSN 2663-0583 (Online)
http://ajee-journal.com

Research Article

BLOCKCHAIN AND SMART PUBLIC PROCUREMENT CONTRACTS: A COMPARATIVE LEGAL ANALYSIS OF DIGITAL TRANSFORMATION IN THE PUBLIC SECTOR

Mohammed Abdelsalam, Alaa Abouahmed, Abdallah Shatat Adham Hashish and Enas AlQodsi*

DOI:
https://doi.org/10.33327/AJEE-18-8.4-a000137

Date of submission: 12 Aug 2025
Date of acceptance: 04 Oct 2025
Publication: 18 Nov 2025

Disclaimer:
The authors declare that the opinions and views expressed in this manuscript are free from any influence of any organization.

Copyright:
© 2025 Mohammed Abdelsalam, Alaa Abouahmed, Abdallah Shatat, Adham Hashish and Enas AlQodsi

ABSTRACT

Background. *The rapid advancement of digital technologies has introduced blockchain as a potential tool in public procurement contracts within the public sector. Smart contracts, particularly within civil law frameworks, have gained legislative recognition in jurisdictions such as France and several U.S. states. This development raises important questions about integrating blockchain-based smart contracts into governmental procurement systems, with a view to enhancing procedural transparency and operational efficiency, while acknowledging the limitations and dependencies on institutional frameworks.*

The central issue lies in clarifying the legal and technical implications of blockchain-based smart procurement contracts. The research examines their potential to streamline public procurement management and improve procedural efficiency, while recognising the need for legal safeguards that maintain administrative law principles and accommodate institutional constraints.

Methods. *This study adopts a comparative analytical approach, examining relevant legal provisions, technical requirements, and administrative practices across multiple jurisdictions. Various blockchain models—public, private, hybrid, and consortium—are evaluated for their suitability in procurement processes. Legislative experiences regulating smart contracts are analysed to extract best practices and inform a cautious framework for public sector adoption.*

Results and Conclusions. *The analysis indicates that blockchain-based smart procurement contracts may reduce bureaucratic delays and minimise human errors, while providing immutable records that can support accountability. However, successful implementation requires legal and institutional adjustments to address enforceability, liability allocation, interoperability, and data protection. A practical model illustrating each operational step—from drafting to automated execution—is proposed, emphasising feasibility and legal compliance rather than assuming transformative effects. The study highlights the necessity of tailored legislation, standardised protocols, and targeted training for public officials to support the cautious integration of blockchain in public procurement contracting. These measures aim to guide the legally informed and context-sensitive adoption of smart contracts, contributing to sustainable digital transformation in public sector governance.*

1 INTRODUCTION

The accelerated integration of blockchain technologies into public sector operations has generated extensive scholarly discourse, particularly regarding their application in smart contracts. While numerous prior studies have explored the technical foundations and general legal implications of blockchain in administrative contexts, there remains a significant gap in understanding how different legal systems[1]—particularly within civil law jurisdictions—can adapt blockchain-based smart administrative contracts to public procurement frameworks without compromising essential principles of administrative law.[2]

This research directly addresses that gap by systematically examining the interplay between blockchain's technical features—decentralisation, immutability, and transparency—and the procedural safeguards embedded in administrative contract law, such as equality between bidders, procedural transparency, and the protection of public interest. It is important to emphasise that blockchain is not a panacea for institutional or administrative shortcomings;

1 Ibrahim Kamel Al Shawabkeh and Mouaid Alqudah, 'Independent Regulatory Bodies in the Jordanian Legal System: An Evaluative Review' (2023) 9(2) *International Journal of Public Law and Policy* 188. doi:10.1504/IJPLAP.2023.130014.

2 Illinois Public Act 101-0514 'Blockchain Technology Act' (2020) <https://www.ilga.gov/legislation/publicacts/101/101-0514.htm> accessed 4 October 2025; Ibrahim Kamel Al-Shawabkeh, 'Legal Guarantees for Objective Performance Evaluation of the Federal Public Employee in the UAE Legislation' (2020) 10(3) Lawyer Quarterly 217; Ibrahim Kamel Al Shawabkeh and Mouaid Alqudah, 'Independent Regulatory Bodies in the Jordanian Legal System: An Evaluative Review' (2023) 9 International Journal of Public Law and Policy 188. doi:10.1504/IJPLAP.2023.130014.

© 2025 Mohammed Abdelsalam, Alaa Abouahmed, Abdallah Shatat, Adham Hashish and Enas AlQodsi. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

its effectiveness relies on robust legal frameworks, sound administrative practices, and appropriate oversight mechanisms.

Unlike existing studies that largely focus on either technical or legal analysis, this work integrates both dimensions to assess feasibility, legal risks, and adaptability within diverse civil law systems. The study recognises that implementing blockchain in public contracts involves complex legal, institutional, and political challenges that must be carefully managed, rather than assuming a straightforward technological solution. The novelty of this study lies in its comparative evaluation of legislative and regulatory approaches across multiple jurisdictions, including those with advanced blockchain legislation (such as France and selected U.S. states), and its adaptation of best practices for MENA-region civil law systems, where scholarly attention remains limited despite growing governmental interest in digital transformation. This comparative perspective enables the identification of legal mechanisms that can balance blockchain innovation with existing administrative norms while maintaining enforceability, accountability, and procedural integrity.

Furthermore, the study outlines a cautious operational approach for blockchain-based smart administrative contracts, detailing the stages from drafting and compliance verification to automated execution and post-contract audit. This approach illustrates potential integration pathways while acknowledging institutional, legal, and practical constraints.

By combining doctrinal analysis with a pragmatic operational framework, the research provides insights into how blockchain could be integrated effectively yet cautiously within public contracting processes. In doing so, it bridges theoretical and practical perspectives, offering guidance for legislators, regulators, and procurement authorities, without overstating the technology's transformative power.

2 METHODOLOGY

This study adopts a **comparative qualitative legal research methodology**, integrating doctrinal analysis with a practical operational framework. It examines legal provisions, legislative initiatives, and regulatory frameworks governing smart contracts and blockchain applications in public procurement across multiple jurisdictions, with a focus on civil law systems such as France and selected MENA countries, while drawing comparative insights from U.S. states that have enacted smart contract legislation. Doctrinal analysis was applied to statutory texts, administrative law principles, and judicial interpretations to evaluate the compatibility of blockchain features—such as automation, decentralisation, and immutability—with core administrative safeguards, including transparency, accountability, and equality among bidders.

The study further evaluates different blockchain models (public, private, hybrid, and consortium) for their suitability in procurement processes, considering technical aspects such as interoperability, data protection, and auditability. Legislative case studies were

analysed to extract best practices and inform a cautious framework for operational integration. Finally, the research develops a practical model mapping each stage of blockchain-based procurement—from drafting and compliance verification to automated execution and post-contract audit—highlighting legal feasibility and operational considerations. This methodology allows for a context-sensitive, comparative evaluation of blockchain's potential in public procurement, balancing innovation with legal and institutional constraints.

3 THE CONCEPT OF BLOCKCHAIN TECHNOLOGY

Recent studies have continued to expand the legal and technological understanding of blockchain-based smart contracts, highlighting how liability structures within distributed ledger systems have evolved and emphasising the regulatory gaps that affect enforceability in public administration. These insights also underline blockchain's growing readiness for public-sector use, as well as the potential for misuse and criminal offences. Security and privacy challenges associated with blockchain have been addressed,[3] alongside another significant issue: the importance of interoperability and establishing clear standards for the performance and execution of smart contracts.[4]

Smart administrative contracts represent a qualitative shift in how contracts are concluded and executed within public administrations.[5] These contracts rely on intelligent software that automatically executes contractual terms using blockchain technology. Their ideal integration exemplifies the relationship between blockchain technology and smart contracts,[6] as blockchain provides the technical foundation for these contracts by offering a secure and transparent platform for recording and automatically executing agreed-upon terms.[7] This integration enhances trust among contracting parties and ensures the precise and transparent execution of contracts. The adoption of blockchain technology in smart

3 Enas Mohammed Al-Qodsi, Iyad Mohammad Jadalhaq and Mohammed El Hadi El-Maknouzi, 'The Place of UAE's Food Security in the National Legislation and its Role in Supporting Global Food Security' (2024) 10(1) Cogent Social Sciences 2319379. doi:10.1080/23311886.2024.2319379

4 Dirk A Zetzsche, Ross P Buckley and Douglas W Arner, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' (2018) 4 University of Illinois Law Review 1361; Rui Zhang, Rui Xue and Ling Liu, 'Security and Privacy on Blockchain' (*arXiv*, 16 August 2019) arXiv:1903.07602v2 [cs.CR] <https://arxiv.org/abs/1903.07602> accessed 4 October 2025.

5 Enas Mohammed Alqodsi and Leila Arenova, 'Smart Contracts in Contract Law as an Auxiliary Tool or a Promising Substitute for Traditional Contracts' (2024) 16(3) Journal of Legal Affairs and Dispute Resolution in Engineering and Construction. doi:10.1061/JLADAH.LADR-1132.

6 Konstantinos Christidis and Michael Devetsikiotis, 'Blockchains and Smart Contracts for the Internet of Things' (2016) 4 IEEE Access 2292. doi:10.1109/ACCESS.2016.2566339.

7 Don Tapscott and Alex Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World* (Penguin 2016).

© 2025 Mohammed Abdelsalam, Alaa Abouahmed, Abdallah Shatat, Adham Hashish and Enas AlQodsi. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

contracts not only improves the efficiency and flexibility of contractual procedures but also provides data protection and the integrity of legal and administrative processes.[8]

However, it is important to recognise that while blockchain can enhance transparency and automation, its effectiveness in public administration ultimately depends on legal safeguards, institutional oversight, and adherence to administrative law principles.

3.1. Jurisprudential Concept of Blockchain Technology

Blockchain can be understood as a ledger that exists simultaneously on many computers. This means that, unlike traditional ledgers, it is not stored in a single place or on a single computer. For instance, imagine a file containing specific data exists across an extensive network of computers. Furthermore, this file can be modified and data added to it on one of these computers. At the same time, all copies of the file are updated simultaneously across the entire network of computers. This means that all users of this extensive network of computers can see the updated information as soon as it is changed.

Therefore, one of the main features of blockchain technology is decentralisation, meaning no single person or organisation controls it. Its updates and maintenance are carried out by a network of users, each of whom has a copy of this ledger. The concept of "blocks" originated in the idea that information is organised into distinct blocks, each linked to the previous one. It is challenging to modify the information in one block without affecting the subsequent blocks.

As a result of decentralisation, another key feature of blockchain technology is trust and transparency. This is because every person in the network can access the same ledger simultaneously as all other users.[9]

Hence, blockchain technology can be understood as a digital notary public. While the traditional role of a notary is to verify transactions and parties and record them to prevent fraud, blockchain performs a similar function through a decentralised network of participants working simultaneously on a single ledger. This collective verification process makes fraud or manipulation extremely difficult, while also enhancing transparency and procedural reliability. Nevertheless, its effectiveness in public-sector operations ultimately depends on the surrounding institutional frameworks, legal safeguards, and administrative oversight.[10]

8 David Yermack, 'Corporate Governance and Blockchains' (2017) 21(1) Review of Finance 7. doi:10.1093/rof/rfw074.

9 Michel Curry, 'Blockchain Technology and the Legal Field' (*Moritz College of Law*, 2022) <https://moritzlaw.osu.edu/sites/default/files/2022> accessed 4 October 2025; Habiba Al Shamsi, 'Enhancing Digital Transactions with Blockchain Technology: Descriptive-Analytical Study' (2024) 7(3) Access to Justice in Eastern Europe 485. doi:10.33327/AJEE-18-7.3-a000322.

10 Tapscott D and Tapscott A (n 7); Yermack (n 8); Zetzsche, Buckley and Arner (n 4).

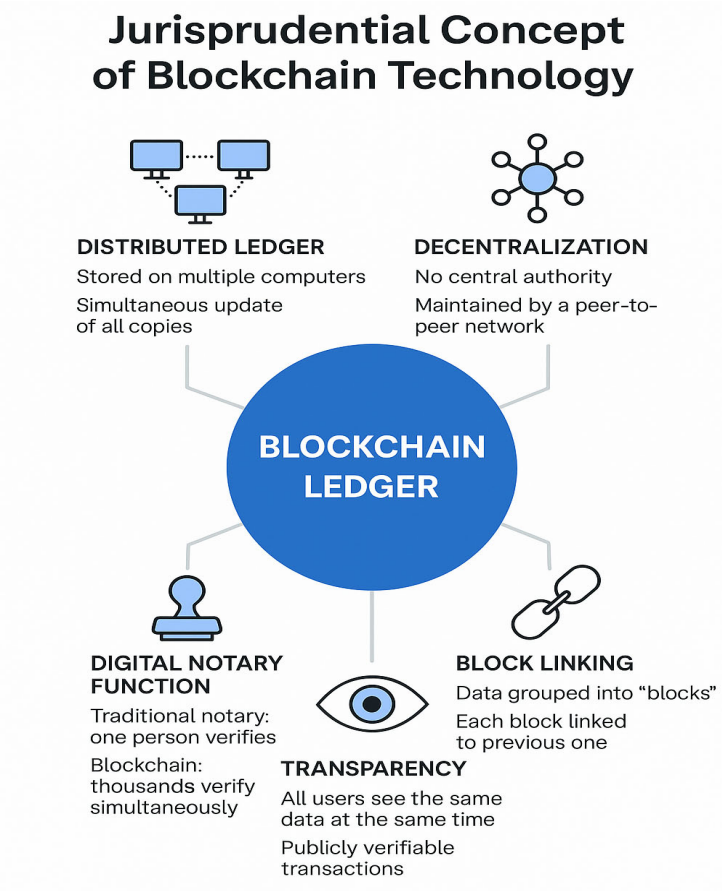

Figure 1. Key Components of Blockchain Technology from a Jurisprudential Perspective[11]

3.2. Legislative Approaches to Defining Blockchain Technology

According to the definitions provided by Forbes and IBM regarding blockchain technology, it is defined as "a shared, immediate, encrypted, and decentralised electronic ledger used to process and record financial transactions, contracts, physical assets, supply chain information, and more. The responsibility for managing this ledger is not assigned to any single person or entity; rather, it remains open to all participants, where every individual

11 Alan T Sherman and others, 'On the Origins and Variations of Blockchain Technologies' (*arXiv*, 15 October 2018) arXiv:1810.06130 [cs.CR] <https://arxiv.org/abs/1810.06130> accessed 4 October 2025.

© 2025 Mohammed Abdelsalam, Alaa Abouahmed, Abdallah Shatat, Adham Hashish and Enas AlQodsi. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

within the chain can access the details of every record—or block—and trace information across a secure network without the need for third-party verification."[12]

Moreover, several scholars have defined blockchain technology as a system for documenting all electronic steps, verifying and authenticating data and transactions, and storing them in an encrypted manner within private networks based on the peer-to-peer (P2P) principle.[13]

The Blockchain Technology Act (BTA), enacted by the State of Illinois in the United States and effective as of 1 January 2020, defines blockchain technology as "an electronic record created by a decentralised method by multiple parties to verify and store a digital record of transactions which is secured by the use of cryptographic hash technology of previous transaction information." This Act also defines "Electronic record" as "a record created, generated, sent, communicated, received, or stored by electronic means, including a blockchain or a smart contract." It also defines "Smart contract" as "a contract stored as an electronic record which is verified by the use of a blockchain."[14]

Blockchain technology is applied across financial transactions, smart administrative contracts, and asset transfers, potentially supporting transparency, security, and procedural efficiency, while recognising that these outcomes depend on institutional and legal safeguards. Such safeguards include a clear legislative framework (e.g., the Illinois Blockchain Technology Act, 2020), regulatory and administrative oversight, robust data protection, dispute-resolution mechanisms, and technical interoperability standards to ensure that smart contracts function reliably within existing public-sector processes. By emphasising these legal and institutional conditions, the paragraph acknowledges that blockchain alone cannot resolve governance, accountability, or procedural challenges in public administration, reflecting lessons from U.S. pilot implementations and mitigating the risk of technological determinism.[15]

This approach aligns with the definition provided by prominent legal scholars, who accurately describe blockchain as a decentralised digital system used to create an immutable and indelible ledger of transactions and data, secured through encryption technologies and managed in a distributed manner among multiple parties without the need for a central intermediary. This system aggregates information into sequentially and temporally linked blocks,[16] with each transaction being verified through majority consensus among network participants. Blockchain technology is utilised across a wide range of applications, including

12 Joseph J Bambara and others, *Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions* (McGraw Hill 2018); Stephanie Susnjara and Ian Smalley, 'What is Blockchain Technology?' (*IBM*, 2020) <https://www.ibm.com/topics/what-is-blockchain> accessed 4 October 2025.

13 Marcella Atzori, 'Blockchain Technology and Decentralized Governance: Is the State Still Necessary?' (2017) 6(1) Journal of Governance and Regulation 45. doi:10.22495/jgr_v6_i1_p5.

14 Illinois Public Act 101-0514 (n 2).

15 Tapscott D and Tapscott A (n 7); Yermack (n 8); Zetzsche, Buckley and Arner (n 4).

16 Emad Abdel Rahim Dahiyat, 'Towards New Recognition of Liability in the Digital World: Should we be More Creative?' (2011) 19(3) International Journal of Law and Information Technology 224. doi:10.1093/ijlit/ear006.

financial transactions, smart contracts, and asset transfers, providing high levels of transparency, security, and efficiency in the management of digital data and transactions.[17]

4 TYPES OF BLOCKCHAIN TECHNOLOGY

There are many different types of blockchain technology models, all of which depend on factors such as their degree of decentralisation, the privacy of transactions and data, the identity of participants, how consensus is reached, speed, energy consumption, transaction costs, and scalability.[18] To fully understand what this technology can offer, it is essential to distinguish between the various types of blockchain systems.

4.1. Public Blockchain

Public blockchains are open-source platforms that anyone in the world can access and utilise. Anyone can join the network by linking a digital wallet to the blockchain and connecting a personal device. This platform uses a peer-to-peer (P2P) system, meaning transactions occur directly between users without the involvement of intermediaries. This makes operations faster and more efficient. Anyone can join the network since there are no specific participation requirements. Bitcoin and Ethereum are two well-known public blockchain platforms primarily focused on the exchange and transfer of cryptocurrencies.[19]

These are decentralised networks that do not require permission to access. Accordingly, anyone can access them, view their contents, and contribute to them without needing anyone else's approval. This makes them transparent, as they are open to everyone. It should be noted that they are immutable and that users can remain anonymous, as they are not required to reveal their identities. As a result, some users may use pseudonyms, making monitoring difficult and raising concerns about compliance with anti-money laundering regulations and the prevention of evasion.[20] Additionally, there are challenges

17 Zetzsche, Buckley and Arner (n 4).

18 Fran Casino, Thomas K Dasaklis and Constantinos Patsakis, 'A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification, and Open Issues' (2019) 36 Telematics and Informatics 55. doi:10.1016/j.tele.2018.11.006.

19 Vitalik Buterin, *A Next-Generation Smart Contract and Decentralized Application Platform* (Ethereum White Paper, 2014) <https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum_Whitepaper_-_Buterin_2014.pdf> accessed 4 October 2025; Moatasem El-Gheriani and Adham Hashish, 'Harnessing the Crypto-Horse: Factors Affecting a Friendly Regulator of the Crypto-Industry: Dubai as a Test Case' (2025) 34(3) Information & Communications Technology Law 241. doi:10.1080/13600834.2025.2452718.

20 Ibrahim Kamel Al-Shawabkeh, 'Using the Tax to Reduce Environmental Pollution in the United Arab Emirates: Possibility and Challenges' in Enas Mohammed AlQodsi and Asma Khaleel Abdallah (eds), *Legal Frameworks and Educational Strategies for Sustainable Development* (IGI Global Scientific Publishing 2025) 1. doi:10.4018/979-8-3693-2987-0.ch001.

© 2025 Mohammed Abdelsalam, Alaa Abouahmed, Abdallah Shatat, Adham Hashish and Enas AlQodsi. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

in determining legal jurisdiction when court intervention is needed to resolve disputes arising from their use.

While public blockchains offer transparency, immutability, and operational efficiency, their adoption in public sector contracting is constrained by several factors. These include challenges in ensuring legal compliance, accountability, and procedural fairness, particularly in areas such as contract modification, force majeure, dispute resolution, and administrative discretion. Real-world pilot projects, such as blockchain-based government procurement trials in the United States and Europe, have demonstrated both potential benefits and limitations, highlighting the need for careful design, regulatory oversight, and technical feasibility assessment before full-scale implementation.

In the United States, pilot programs in defence and logistics are testing blockchain systems, though widespread adoption is not yet realised. For instance, Wyoming's Stable Token Commission launched a state-backed stable token on test networks in 2024, with full issuance planned for 2025. These initiatives indicate a growing interest in integrating blockchain into public sector operations, but also underscore the complexities involved in scaling such technologies. Similarly, in Europe, several countries have initiated blockchain projects aimed at enhancing transparency and efficiency in public services. However, many of these projects remain in pilot phases, with limited scalability and challenges in aligning with existing legal frameworks. These examples illustrate the cautious approach governments are taking towards blockchain adoption, emphasising the importance of addressing legal and technical challenges before full-scale implementation.[21]

4.2. Private Blockchain

Private blockchains are characterised by strict rules, unlike public ones that are open to everyone. They are controlled by a central authority or intermediary that determines who can access them and sets the rules for participation. This gives complete control over how the network operates and who can join. Banks, government agencies, and private companies

21 'Blockchain in Government Contracts: What You Need to Know' (*US Federal Contractor Registration*, 26 December 2024) <https://blogs.usfcr.com/blockchain-federal-contracting> accessed 3 October 2025; Emmanuel, 'Blockchain Use Cases in the Government and Public Sector' (*Tectum*, 21 March 2025) <https://tectum.io/blog/blockchain-use-cases-in-the-government-and-public-sector/> accessed 4 October 2025; 'Government Contracting and Blockchain: The Future of Federal Innovation' (*Government Contracting Digest*, 25 June 2025) <https://govcondigest.com/government-contracting-and-blockchain-the-future-of-federal-innovation/> accessed 3 October 2025; 'How the US Government Is Using Crypto, and Where It Could Go' (*US Federal Contractor Registration*, 20 June 2025) <https://blogs.usfcr.com/gov-crypto-projects> accessed 3 October 2025; Kostiantyn Tsentsura, 'How Governments Are Using Blockchain in 2025' (*Yellow.com*, 19 August 2025) <https://yellow.com/research/how-governments-are-using-blockchain-in-2025-from-digital-identity-to-cbdcs-and-voting> accessed 3 October 2025; Roopali Joshi, 'Use Cases of Blockchain in Government and Public Sector' (*A3Logics*, 23 October 2024) <https://www.a3logics.com/blog/blockchain-in-government/> accessed 3 October 2025.

often use private blockchains. Transactions in these networks are conducted securely within a closed, trusted environment, ensuring a high level of privacy and security. This could be significant, for example, when it comes to contracts conducted by health providers.[22]

As for private blockchains, they are networks affiliated with an entity or institution and are therefore controlled by that institution or entity. This also means access is controlled, so users must be authorised and granted permission to enter. The data within such blockchains is often protected by legal provisions related to data privacy. Generally, this type of blockchain is better positioned to comply with legal frameworks concerning data protection, transfer, and processing.

Private blockchains are characterised by strict rules, unlike public ones that are open to everyone. They are controlled by a central authority or intermediary that determines who can access them and sets the rules for participation. While these features provide privacy and operational control, they do not automatically ensure legal compliance, procedural fairness, or accountability in public sector applications. Banks, government agencies, and private companies often use private blockchains, but even in these controlled environments, challenges remain regarding contract modification, force majeure, dispute resolution, liability, and administrative discretion.

Private blockchain networks require ongoing monitoring and oversight to ensure adherence to data protection and other legal obligations; failure to do so could result in significant legal and administrative liabilities. Real-world pilot projects, such as internal blockchain-based contract management systems in European municipalities and select U.S. state agencies, have shown potential to streamline operations while maintaining confidentiality, yet these initiatives also highlight practical limitations, such as scalability, regulatory alignment, and the need for specialised training for officials.[23]

Furthermore, implementing private blockchains in governmental contexts involves financial, technical, and political considerations, including investment in infrastructure, integration with existing administrative systems, and alignment with local and national legislation. Therefore, while private blockchains offer controlled, secure, and efficient environments for contractual processes, their successful deployment in the public sector depends critically on robust legal frameworks, institutional safeguards, and ongoing administrative oversight.[24]

22 Ayman Mohamed Afify and others, 'Unveiling the Right to Health in Egypt: Exploring the Transformations and Challenges in Egyptian Constitutional Law and Policy' (2023) 12 Academic Journal of Interdisciplinary Studies 95. doi:10.36941/ajis-2023-0156.

23 Joshi (n 21); Emmanuel (n 21).

24 Blockchain in Government Contracts (n 21); Tsentsura (n 21).

© 2025 Mohammed Abdelsalam, Alaa Abouahmed, Abdallah Shatat, Adham Hashish and Enas AlQodsi. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

4.3. Hybrid Blockchain

Hybrid blockchains combine characteristics of both public and private networks. Some data is publicly accessible, while other data requires authorisation. This dual nature provides operational flexibility but also introduces legal and administrative challenges, particularly in public sector applications. Effectiveness depends on institutional frameworks, regulatory oversight, and the assignment of accountability to prevent misuse or legal violations.

Even in hybrid blockchains, challenges remain regarding contract modification, force majeure, dispute resolution, liability allocation, and administrative discretion. Real-world pilot projects have highlighted both opportunities and limitations: for example, the Dubai Land Department has implemented a hybrid blockchain for land registration, combining public access to certain records with restricted access to sensitive data. Similarly, some U.S. state agencies have experimented with hybrid blockchains to manage government contracts, demonstrating efficiency gains but also revealing practical limitations such as regulatory alignment, scalability, and staff training requirements.[25]

Implementation in governmental contexts also involves financial, technical, and political considerations, including infrastructure investment, integration with existing administrative systems, and compliance with national and local legislation. Therefore, while hybrid blockchains offer flexibility and potential operational improvements, their deployment in public-sector contracting must be carefully managed through robust legal frameworks, continuous monitoring, and clear governance structures.[26]

***Table* 1. Summary of Blockchain Technology Types**[27]

Type	Access	Control	Transparency	Privacy	Legal Considerations	Feasibility Implementation Challenges
Public Blockchain	Open to all	Decentralised	High	Anonymous Pseudonymous	Difficult to regulate; AML compliance; legal jurisdiction	Limited control; challenges with public procurement rules; accountability issues

25 Joshi (n 21).

26 Alaa Abouahmed, Ahmed Eldakak and Aliaa Zakaria, 'Using Electronic Auctions for Contracting in the UAE Federal Government Procurements' in Bahaaeddin AM Alareeni and Islam Elgedawy (eds), *Studies in Systems, Decision and Control* (Springer Cham 2023) 884. doi:10.1007/978-3-031-39158-3_82.

27 Jesse Anglen, 'Different Types of Blockchains: Public, Private, and Hybrid' (*Rapid Innovation*, 2025) <https://www.rapidinnovation.io/post/different-types-of-blockchains-public-private-and-hybrid> accessed 4 October 2025.

Private Blockchain	Restricted	Centralised	Limited to authorised participants	High	Easier compliance; data privacy; monitor liability	Requires oversight; regulatory alignment; specialised training; scalability issues
Hybrid Blockchain	Mixed: some public, some restricted	Mixed: some open, some centralised	Partial: public + private data	Depends on data classification	Requires adaptable legal frameworks; administrative safeguards; compliance monitoring	Complex implementation; regulatory alignment; technical and political hurdles; infrastructure investment; real-world pilot learning

5 THE CONCEPT OF SMART ADMINISTRATIVE CONTRACTS

There is currently no universally accepted definition of a smart contract. Various scholars and practitioners conceptualise smart contracts differently, with interpretations often shaped by their focus on the contractual processes, operational mechanisms, or anticipated outcomes. Despite the advantages of smart contracts, their adoption in administrative or public sector contracts is not without limitations. Legal recognition remains evolving, and ambiguities in jurisdiction, liability allocation, and contract modification pose significant challenges.[28] Furthermore, technical constraints, such as blockchain scalability, interoperability, and secure coding requirements, must be considered.[29] Therefore, while smart contracts can improve efficiency and transparency, they do not replace the need for careful legal oversight and risk management in public contracting processes.[30] Legal

28 Ahmad Ghandour and others, 'Legal Framework for Blockchain Contracts: An Analysis Under UAE Law' (*SSRN*, 14 December 2024) <https://ssrn.com/abstract=5056550> accessed 4 October 2025; Dalila Djamane, 'Smart Contracts: Global Perspectives and Legal Realities', pt 2 (*Daily Jus*, 6 August 2025) <https://dailyjus.com/legal-tech/2025/08/smart-contracts-global-perspectives-and-legal-realities-part-2> accessed 3 October 2025.

29 Irina Heaver, Alla Melnichenko and Zainab Kamran, 'Blockchain 2025 – UAE – Global Practice Guides' (*Chambers and Partners*, 12 June 2025) <https://practiceguides.chambers.com/practice-guides/blockchain-2025/uae> accessed 3 October 2025.

30 'DIFC Announces Enactment of New Digital Assets Law, New Law of Security and Related Amendments to Select Legislation' (*Dubai International Financial Centre (DIFC)*, 13 March 2024) <https://www.difc.com/whats-on/news/difc-announces-enactment-of-new-digital-assets-law---new-law-of-security-and-related-amendments> accessed 3 October 2025; 'UAE Cryptocurrency Regulations' (*Virtuzone*, 24 January 2025) <https://virtuzone.com/blog/uae-cryptocurrency/> accessed 3 October 2025.

© 2025 Mohammed Abdelsalam, Alaa Abouahmed, Abdallah Shatat, Adham Hashish and Enas AlQodsi. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

institutions still play a critical role in interpreting and enforcing contractual obligations that fall outside the scope of automated execution. In this regard, the legislature must adopt a specific definition following thorough and lengthy parliamentary debates and discussions with stakeholders.[31] A smart contract is an electronic agreement executed by two or more parties through a coded program. However, this program must operate within a blockchain network. Since the contract contains terms and rules, the program must include a set of predefined and mutually agreed-upon regulations and conditions. It is characterised by automatic execution once the conditions are met, without the need for intermediaries. The smart contract is characterised by decentralisation, self-verification, and immutability, ensuring the secure and reliable execution of agreed-upon obligations while enabling the programmed and transparent exchange of assets and funds.[32] This would increase competition among entities seeking to win and secure administrative contracts.[33]

***Table* 2. Comparison Between Traditional Contracts and Smart Contracts**[34]

Feature	Traditional Contracts	Smart Contracts	Legal / Practical Considerations
Form	Written or verbal agreement	Code executed on a blockchain	Smart contract code must comply with applicable legal standards; lack of uniform definition[35]
Execution	Manual, requires human intervention	Automatic, triggered by predefined conditions	Limited flexibility for unforeseen events; cannot easily adapt to force majeure or discretionary decisions[36]
Enforcement	Enforced by legal institutions	Enforced through blockchain consensus mechanisms	Ambiguous legal recognition; liability and dispute resolution still require oversight[37]
Intermediaries	Often requires third parties (e.g., lawyers, notaries, banks)	No intermediaries required	Third parties may still be needed for verification, legal advice, or regulatory compliance[38]

31 Tarek Abo El-Wafaa, Ahmed Khalil and Adham Hashish, 'Parliamentary Question: Insights from the Federal National Council in the UAE' (2024) 10(6) Heliyon e27671. doi:10.1016/j.heliyon.2024.e27671.

32 Kevin Werbach and Nicolas Cornell, 'Contracts Ex Machina' (2017) 67(2) Duke Law Journal 313.

33 Moatasem El-Gheriani and Adham Hashish, 'Egypt Amends its Competition Law to Establish a Pre-Merger Control System' (2023) 14(2) Journal of European Competition Law & Practice 106. doi:10.1093/jeclap/lpad014.

34 Yu Haizhe, Deng Xiaopengorcid and Zhang Na, 'To What Extent Can Smart Contracts Replace Traditional Contracts in Construction Projects?' (2023) 32(3) Engineering, Construction and Architectural Management 1393. doi:10.1108/ECAM-04-2023-0379.

35 Ghandour and others (n 28).

36 Djamane (n 28).

37 Heaver, Melnichenko and Kamran (n 29).

38 UAE Cryptocurrency Regulations (n 30).

Transparency	Private with limited accessibility	Transparent and verifiable on the blockchain	High transparency may conflict with data privacy regulations[39]
Security	Vulnerable to tampering or loss	Cryptographically secure and immutable	Security depends on correct coding; vulnerabilities may have irreversible consequences[40]
Cost and Time Efficiency	Potentially expensive and time-consuming	Lower cost and faster execution	Initial development and deployment costs can be high; maintenance required[41]
Flexibility in Modification	Can be renegotiated or modified	Difficult to modify once deployed	Legal amendments may require workarounds; immutability limits adaptability[42]
Jurisdiction and Legal Framework	Clearly defined and varies by jurisdiction	Ambiguous, with evolving legal recognition	Legal uncertainty may hinder adoption in government contracts[43]

6 TYPES OF SMART ADMINISTRATIVE CONTRACTS

Smart administrative contracts are categorised into two principal types: deterministic smart administrative contracts and non-deterministic smart administrative contracts, as detailed below:

6.1. Deterministic Smart Administrative Contracts

Deterministic smart administrative contracts rely entirely on information embedded within the blockchain network to execute their terms autonomously, without requiring external data sources. While this technological determinism can significantly improve operational efficiency and reduce human intervention, it also introduces critical limitations—particularly in public-sector contexts where unforeseen circumstances such as force majeure, contract modification, or discretionary administrative decisions are routine.[44] Such rigidity potentially undermines the rule of law and public sector accountability if there are no embedded legal mechanisms for judicial or arbitral oversight.[45]

39 Djamane (n 28).
40 Heaver, Melnichenko and Kamran (n 29).
41 DIFC (n 30).
42 Ghandour and others (n 28).
43 UAE Cryptocurrency Regulations (n 30).
44 Eric Tjong Tjin Tai, 'Force Majeure and Excuses in Smart Contracts' (2018) 26(6) European Review of Private Law 787.
45 Iyad Mohammad Jadalhaq and others, 'A Systematic Reviews and Meta-Analyses of Interruption of the Statute of Limitations for Civil Claims: A Comparative Study of Arab Legislations' (2023) 9(6) Heliyon e16756. doi:10.1016/j.heliyon.2023.e16756.

© 2025 Mohammed Abdelsalam, Alaa Abouahmed, Abdallah Shatat, Adham Hashish and Enas AlQodsi. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Empirical evidence from real-world deployments further illuminates these constraints. In Seoul's Yeongdeungpo District, a blockchain-based system for evaluating public tenders increased transparency but faced scalability challenges and stakeholder resistance, limiting broader adoption.[46] Meanwhile, Estonia has been a pioneer in legally recognising smart contracts in administrative systems—particularly in e-residency and healthcare records—but even there, legal clarity remains bounded by interoperability and regulatory education challenges.[47]

Given these realities, deterministic smart contracts should be viewed not as panaceas for governmental inefficiencies, but as targeted tools suitable for narrow, well-defined legal use cases. Their deployment must be integrated within robust legal and institutional architectures that preserve flexibility, oversight, and legitimacy in the public contracting process.

6.2. Non-deterministic Smart Administrative Contracts

In contrast, non-deterministic smart administrative contracts depend on external "oracles" to feed on-chain execution with off-chain data (e.g., macroeconomic indicators, FX rates for public finance, weather or logistics data) that trigger or qualify on-chain execution.[48] While this expands administrative use cases (e.g., index-linked payments or disaster-response procurement), it introduces the oracle problem: the legal and technical risks that arise when contract performance hinges on external data sources, raising questions about reliability, security, auditability, and liability allocation among contracting authorities, oracle providers, and vendors.[49] These risks are not hypothetical: market-manipulation cases exploiting price feeds (oracle/manipulation dynamics) have resulted in significant losses, underscoring the need for robust governance and dispute-resolution fallbacks rather than purely automated execution.[50]

From a legal-regulatory perspective, several jurisdictions have begun to frame smart-contract (and oracle) governance: the EU Data Act sets essential requirements for smart contracts used in data-sharing, including robustness, safe termination/kill-switch, and

46 'Seoul District Using Blockchain for Public Procurement' (*Ledger Insights*, 21 January 2019) <https://www.ledgerinsights.com/seoul-district-using-blockchain-for-public-procurement/> accessed 3 October 2025.

47 '*Estonia: Blockchain & Cryptocurrency Laws and Regulations 2025*' (***Global Legal Insights***, 25 October 2024) <https://www.globallegalinsights.com/practice-areas/blockchain-cryptocurrency-laws-and-regulations/estonia > accessed 4 October 2025; *Eesti Firma* (2025) <https://www.eestifirma.ee/en/> accessed 4 October 2025; *REI Systems* (2025) <https://www.reisystems.com/> accessed 4 October 2025.

48 Zhang, Xue and Liu (n 4).

49 Chanelle Duley and others, *The Oracle Problem and the Future of DeFi* (BIS Bulletin no 76, Bank for International Settlements 2023).

50 Jonathan Stempel, 'Trader Convicted of Mango Markets Fraud in First US Crypto Manipulation Case' (*Reuters*, 18 April 2024) <https://www.reuters.com/legal/trader-convicted-mango-markets-fraud-first-us-crypto-manipulation-case-2024-04-18/> accessed 3 October 2025.

logging—principles directly relevant to public-sector oracle use where erroneous feeds must be halted and reviewed.[51] In England & Wales, the Law Commission confirmed smart legal contracts are generally supportable under existing law, but parties must address interpretation, variation, and remediation—points that become pivotal when off-chain data controls on-chain performance.[52]

In the UAE, sectoral instruments provide a complementary framework: DIFC Digital Assets Law (No. 2 of 2024) recognises digital-asset arrangements and supports smart-contract-based operations within a clear property and control framework;[53] VARA's 2023 Regulations in Dubai introduce licensing, governance and risk-management duties over virtual-asset activities that would encompass oracle-dependent services;[54] and ADGM's 2023 DLT Foundations Regulations enable regulated structures (e.g., foundations/DAOs) to operate oracle networks or middleware with clearer accountability.[55] Privacy and data-governance constraints also apply: the UAE Federal Personal Data Protection Law (PDPL) 45/2021 sets principles for processing personal data (noting special rules/exclusions for government data), which is critical when oracle feeds include identifiable or sensitive information.[56]

For public procurement, non-deterministic designs should therefore: (i) document oracle governance (sources, decentralisation/multi-source aggregation, service-level remedies); (ii) embed safe-termination and human-in-the-loop review for contested feeds; (iii) allocate liability and dispute-resolution for faulty or manipulated data; and (iv) align with budgetary and stakeholder constraints, learning from EU public-sector blockchain pilots (EBSI) that emphasise interoperability and administrative oversight rather than full automation.[57] In short, non-deterministic contracts can solve narrow, well-specified administrative problems, but only when paired with explicit legal guardrails and operational controls on the oracle layer.[58]

51 EU Data Act (13 December 2023) art 36 <https://www.eu-data-act.com/Data_Act_Articles.html> accessed 4 October 2025.

52 Law Commission of England and Wales, *Smart Legal Contracts* (Law Comission 2021) <https://lawcom.gov.uk/project/smart-contracts/> accessed 4 October 2025.

53 DIFC (n 30); DIFC Law No 2 of 2024 'Digital Assets Law' (1 March 2024) <https://www.difc.com/business/laws-and-regulations/legal-database?path=business&path=laws-and-regulations&path=legal-database&path=difc-laws> accessed 3 October 2025.

54 Virtual Assets Regulatory Authority (VARA), *Virtual Assets and Related Activities Regulations 2023* (VARA Dubai 2023).

55 'ADGM Introduces the Worlds First DLT Foundations Regime' (*Abu Dhabi Global Market (ADGM)*, 2 November 2023) <https://www.adgm.com/media/announcements/adgm-introduces-the-worlds-first-dlt-foundations-regime> accessed 3 October 2025.

56 Federal Decree-Law No 45 of 2021 'Concerning the Protection of Personal Data' [2021] Official Gazette 712 <https://uaelegislation.gov.ae/en/legislations/1972> accessed 3 October 2025.

57 'European Blockchain Services Infrastructure' (*European Commission*, 2025) <https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure> accessed 3 October 2025.

58 EU Data Act (n 51); Law Commission of England and Wales (n 52).

© 2025 Mohammed Abdelsalam, Alaa Abouahmed, Abdallah Shatat, Adham Hashish and Enas AlQodsi. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

7 CONTRACT LANGUAGE AND DOCUMENTATION

In traditional administrative contracts, the agreement is written in a natural language, such as Arabic or English, and documented through specialised authorities, including notaries or relevant administrative bodies. In contrast, in smart administrative contracts, the contract is drafted using coding languages. Programmers develop the coded contract to be automatically executed and documented on the blockchain platform. The contract is distributed across all network-connected devices in an encrypted form, ensuring it cannot be altered, damaged, or forged. Unlike traditional paper contracts, which may be prone to loss or damage, smart administrative contracts provide automatic, secure documentation without complex procedures or additional costs, thereby saving time and effort and better protecting the rights of the contracting parties.[59]

Because they are electronic, smart administrative contracts are converted into programmable code, eliminating the need for paper documents or intermediaries and thereby enhancing transparency and efficiency. Their conditional nature ensures the automatic, precise execution of terms, accelerating administrative procedures and reducing the need for human intervention. Self-verification strengthens trust among parties by automatically enforcing conditions without centralised supervision. Furthermore, the use of coding languages and automatic documentation protects contracts from damage or forgery compared to traditional paper contracts.[60]

Nevertheless, these advantages raise essential challenges. The use of coding languages may create a "language gap" between legal practitioners and programmers, limiting accessibility and hindering judicial oversight. Some comparative legislative experiences have begun to address this challenge. For example, the United Arab Emirates Federal Law No. 46 of 2021 on Electronic Transactions and Trust Services recognises the evidentiary value of electronic contracts. It provides a legal framework for digital signatures, [61] thereby facilitating their adoption in administrative contexts. Similarly, the European Union's Regulation (EU) No 910/2014 on electronic identification and trust services (eIDAS) establishes the legal validity of electronic documents and smart contracts across member states. These frameworks demonstrate a gradual recognition by legislators that, while smart contracts can replace traditional documentation methods, legal safeguards remain necessary to ensure transparency, accessibility, and effective dispute resolution.

59 Christopher D Clack, Vikram A Bakshi and Lee Braine, 'Smart Contract Templates: Foundations, Design Landscape and Research Directions' (*arXiv*, 15 March 2017) arXiv:1608.00771v3 [cs.CY] <https://arxiv.org/abs/1608.00771> accessed 3 October 2025.

60 Eliza Mik, 'Smart Contracts: Terminology, Technical Limitations and Real World Complexity' (2017) 9(2) Law, Innovation and Technology 269. doi:10.2139/ssrn.3038406.

61 Emad Abdel Rahim Dahiyat, 'The Legal Recognition of Electronic Signatures in Jordan: Some Remarks on the Electronic Transactions Law' (2011) 25(3) Arab Law Quarterly 297. doi:10.1163/157302511X568538.

8 MECHANISM OF SMART CONTRACTS OPERATION VIA BLOCKCHAIN TECHNOLOGY

To ensure the accurate application of smart contracts within the administrative contract lifecycle using blockchain technology, specific steps must be followed in alignment with the requirements of administrative agreements in terms of precision and reliability, as detailed below:

Step 1: Agreement on Terms

The first step involves determining the contractual terms, which means reaching a mutual agreement on the agreed-upon conditions. These might include, for example, the type of goods to be delivered, the payment timelines if delivery meets the required conditions, and the discount rates if the delivered goods fail to meet specific criteria. Naturally, these terms must be comprehensively identified, and each party's approval must be final after fulfilling all the internal approvals required for contracting on each side. This is particularly critical if an administrative agency seeks to enter into a contract and must meet all internal policy requirements to avoid any punitive measures from oversight authorities.[62]

The conditions vary and can cover various topics such as specifications of goods, delivery dates, price and amount of each payment instalment, and mechanisms for resolving disputes between the parties. The parties might also set a specific outcome for some disputes that may arise and leave other conflicts, which may require judges' discretion, to be resolved in court.

Moreover, this step is critical in administrative contracts under UAE law, particularly Federal Law No. 46 of 2021 on Electronic Transactions and Trust Services, which establishes the legal recognition of electronic agreements and sets requirements for internal approvals and auditability. Comparative experience, such as the UK Jurisdiction Taskforce (2019) statement on smart contracts, confirms that while blockchain automation can enhance efficiency, judicial oversight remains essential for disputes or modifications that cannot be encoded into the contract. These examples highlight that smart contracts must be implemented alongside clear legal and institutional frameworks to ensure enforceability, accountability, and protection of the public interest.

62 Gehad Mohamed AbdelAziz and Alaa Abouahmed, 'The Punitive Power of Independent Administrative Authorities: Focus on Financial and Tax Violations: A Comparative Study' (2024) 7(2) Access to Justice in Eastern Europe 301. doi:10.33327/AJEE-18-7.2-n000216; Abed Fayed, Aliaa Zakaria and Alaa Abouahmed, 'Innovations of Artificial Intelligence in Light of the Applicable Copyright Law: Realistic Solutions and Future Prospects. A Comparative Study of UAE, Egyptian, and French Laws' (2025) 8(1) Access to Justice in Eastern Europe 241. doi:10.33327/AJEE-18-8.1-a000116; Nicholas T Solosky and Diana Lyn Curtis Shutzer, 'Contractor Compliance and Internal Investigations: New Practical Strategies for Unpredictable Times' (2025) 60(4) The Procurement Lawyer 20.

© 2025 Mohammed Abdelsalam, Alaa Abouahmed, Abdallah Shatat, Adham Hashish and Enas AlQodsi. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Step 2: Conversion of Terms into Programming Code

The second step involves programming and encoding the terms agreed upon by the parties in the first step. This requires specialised software that relies on programming languages designed for smart contracts, which convert the contractual terms into encrypted programming code. This code outlines the rights and obligations of each party, detailing each obligation related to execution and linking them to the specific instructions for that execution. The aim is to monitor compliance during execution intelligently without human intervention. For example, a condition can be programmed so that if the delivered goods match the agreed-upon specifications, an automatic authorisation is issued to pay a specific portion of the contract value.

However, it is important to note that full automation cannot address all legal contingencies. Errors in programming or unforeseen circumstances (e.g., force majeure, disputes requiring judicial discretion) may still require human intervention. Under UAE Federal Law No. 46 of 2021 on Electronic Transactions and Trust Services, electronic agreements must comply with legal standards and include mechanisms for audit and verification. Similarly, the UK Jurisdiction Taskforce (2019) emphasised that smart contracts are enforceable under law, but parties should ensure that off-chain issues and coding errors do not compromise contractual obligations or rights.

Step 3: Deployment on a Blockchain Network

The third step involves uploading and deploying the smart contract onto a blockchain network that meets the specifications agreed upon by the parties. Naturally, this blockchain network must be licensed, meaning an authority has confirmed that it meets specific standards and has issued certification authorising the parties to use it.

Furthermore, the blockchain must be technically capable of interacting with the encrypted programming language in which the contract conditions were written. Each contracting party then receives keys and data that enable them to interact with the blockchain throughout the execution of the smart contract.

However, deployment does not eliminate legal accountability. Under UAE Federal Law No. 46 of 2021 on Electronic Transactions and Trust Services, parties remain responsible for compliance with contractual obligations and administrative approvals. Additionally, certification and licensing do not entirely prevent technical errors, security breaches, or unforeseen contingencies, which may require human intervention or corrective measures. Regulatory frameworks in jurisdictions such as ADGM and DIFC emphasise that smart contracts must include auditability, dispute-resolution mechanisms, and fail-safes to maintain legal and operational reliability.

Step 4: Automatic Execution upon Condition Fulfilment

This step refers to the network's ability to ensure that obligations are fulfilled and that corresponding obligations are executed. As previously explained, once goods that meet the conditions are delivered, the agreed payment amount is automatically transferred. This could also work in a different direction: if one party fails to perform their obligation, the agreed-upon terms may specify a sanction to be enforced, such as a penalty that the breaching party must pay.[63]

Nevertheless, automatic execution does not eliminate legal responsibility or the need for oversight. According to UAE Federal Law No. 46 of 2021 on Electronic Transactions and Trust Services, electronic agreements must comply with legal standards, allow for audit and verification, and maintain accountability of the contracting parties.[64] Errors in programming, unexpected contingencies, or inaccurate external data (e.g., from oracles) may still require human intervention or corrective measures.[65]

Transparent verification via immutable blockchain records enhances procedural efficiency, reduces time spent on monitoring compliance, and strengthens trust among parties. However, jurisdictions such as ADGM and DIFC emphasise that smart contracts must incorporate dispute-resolution mechanisms, fail-safes, and compliance checks to ensure enforceability and mitigate operational or legal risks.[66] Comparative studies further highlight that while smart contracts accelerate execution and reduce intermediaries, they cannot fully replace legal oversight in administrative contracts where human judgment, discretionary decisions, or unforeseen external events may affect outcomes.[67] Therefore, a hybrid approach combining automated execution with legal safeguards and auditability is recommended for public sector implementations.

It is essential to recognise the importance of transparent verification: each action taken by a party results in a record entered into the blockchain, which is immutable and simultaneously visible to the other authorised party. This achieves procedural efficiency and significantly reduces the time usually spent verifying each party's fulfilment of their contractual obligations.

63 Gehad Mohamed Abdelaziz and Adham Hashish, 'Using Sanctions in Enforcing Digital Markets Act in the EU' in Rim El Khoury and Nohade Nasrallah (eds), *Intelligent Systems, Business, and Innovation Research* (Springer Cham 2024) 775. doi:10.1007/978-3-031-36895-0_65.

64 Federal Decree-Law No 46 of 2021 'On Electronic Transactions and Trust Services' [2021] Official Gazette 712 <https://uaelegislation.gov.ae/en/legislations/1539> accessed 3 October 2025.

65 Zhang, Xue and Liu (n 4); Mik (n 60).

66 ADGM (n 55).

67 Clack, Bakshi and Braine (n 59); Fayed, Zakaria and Abouahmed (n 62).

© 2025 Mohammed Abdelsalam, Alaa Abouahmed, Abdallah Shatat, Adham Hashish and Enas AlQodsi. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

9 PRACTICAL APPLICATION OF A SMART ADMINISTRATIVE CONTRACT BASED ON BLOCKCHAIN TECHNOLOGY

A practical application can be illustrated through an administrative contract for the supply of equipment to a governmental facility, where the technical and administrative efficiency of utilising innovative contract technology via blockchain becomes evident. The process proceeds as follows:

Step 1: Agreement on Contractual Terms

The governmental party (the buyer) and the supplier (the seller) define the contractual terms, including details of the equipment supply—such as type, quantity, specifications, and delivery deadlines—as well as payment obligations. The governmental party may unilaterally draft the detailed terms based on specific administrative requirements and then send the contract electronically to the supplier. The supplier must review and approve the terms through the smart contract platform. This approval constitutes the "offer and acceptance" traditionally found in contract law but is now achieved through modern digital means, ensuring clarity of obligations and transparency in the contracting process.[68]

It is understood that all actions remain subject to applicable legal standards and administrative approvals.

Step 2: Coding the Agreed Terms

Once the terms are agreed upon, they are translated into programming code using a language specialised for smart contracts, such as Solidity. This process is crucial for incorporating the agreed-upon terms into the mechanism through which the contract will be enforced. The code specifies the conditions required for the contract's execution; for example, "If the equipment is delivered on the specified date, payment is automatically transferred to the supplier." This transformation renders the contract into a self-executing mechanism that eliminates the need for continuous human monitoring.[69]

Step 3: Deployment on a Blockchain Network

After coding, the contract is deployed on a blockchain network, such as Ethereum, which ensures that the contract cannot be altered or tampered with. The network's nodes verify the accuracy of the contract and confirm compliance with all technical and legal conditions.

68 Abdelaziz and Hashish (n 63); Max Raskin, 'The Law and Legality of Smart Contracts' (2017) 1(2) Georgetown Law Technology Review 305. doi:10.2139/ssrn.2842258; Iyad Mohammad Jadalhaq and Mohammed El Hadi El Maknouzi, 'Reading UAE Contract Law Through the Lens of Islamic Jurisprudence: A Case Study on the "Extraneous Cause' Exception in the UAE Civil Code" (2019) 19(2) Global Jurist 20180045. doi:10.1515/gj-2018-0045.

69 Clack, Bakshi and Braine (n 59).

The contract is then permanently stored on the blockchain, enhancing its security and transparency, making tampering practically impossible.[70]

Step 4: Automatic Execution Upon Fulfilment of Conditions

When the predetermined conditions are fulfilled—for instance, when the governmental party receives and inspects the equipment according to agreed-upon specifications—the network nodes verify the successful delivery. Upon confirmation, the smart contract automatically executes the corresponding obligation, such as transferring the agreed payment to the supplier. This automatic execution ensures precise and highly transparent fulfilment of commitments, reducing the likelihood of disputes or payment delays. In cases where the assets are physical, the settlement may occur off-chain. At the same time, documentation and follow-up remain on the blockchain network, thereby ensuring execution reliability and compliance with contractual terms.[71]

It is important to note that automatic execution of smart administrative contracts does not eliminate legal responsibility. Parties remain accountable for compliance with applicable legal standards and administrative approvals. In the UAE, this is governed by Federal Law No. 46 of 2021 on Electronic Transactions and Trust Services, which requires auditability and accountability for all electronic agreements.[72] Similarly, international frameworks, such as the UK Jurisdiction Taskforce (2019), recognise smart contracts legally but emphasise that human oversight may still be necessary in cases of coding errors, inaccurate oracle data, or unforeseen circumstances.

Operational limitations must also be considered: automatic execution may not cover force majeure events or other contingencies beyond the system's control. For contracts involving physical assets, settlements may occur off-chain while still being documented on the blockchain for transparency and auditability. Regulatory authorities like ADGM and DIFC recommend incorporating fail-safes, dispute-resolution mechanisms, and auditability features to ensure both legal enforceability and operational reliability.[73]

Comparative experiences from Europe, the United States, and Singapore show that while smart contracts improve efficiency and reduce intermediaries, human intervention remains essential for resolving complex disputes, addressing exceptional circumstances, and ensuring compliance with legal and administrative requirements.

70 Aaron Wright and Primavera De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (2015) 34 Social Science Research Network 41. doi:10.2139/ssrn.2580664.

71 Zhang, Xue and Liu (n 4).

72 Federal Decree-Law No 46 of 2021 (n 64).

73 ADGM (n 55); DIFC (n 30).

© 2025 Mohammed Abdelsalam, Alaa Abouahmed, Abdallah Shatat, Adham Hashish and Enas AlQodsi. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

10 CHALLENGES FACING SMART ADMINISTRATIVE CONTRACTS BASED ON BLOCKCHAIN TECHNOLOGY

While applying smart administrative contracts offers prominent administrative and legal advantages, several challenges persist.

10.1. Legal Challenges

The legal landscape for smart contracts faces several significant challenges, primarily due to the lack of a comprehensive, unified regulatory framework. Currently, no legislation explicitly governs all aspects of smart contracts, creating uncertainty about their legal recognition and enforceability. In the UAE, partial guidance is provided through Federal Law No. 46 of 2021 and the regulatory frameworks established by the Abu Dhabi Global Market (ADGM) and the Dubai International Financial Centre (DIFC), which aim to ensure that parties remain legally accountable despite the lack of a fully unified legal regime[74]. Another prominent challenge concerns issues of capacity and identity. Decentralised systems often struggle to verify participants' legal capacity to enter into contracts and confirm their identities.[75] To mitigate these risks, best practices now recommend incorporating robust Know Your Customer (KYC) and identity verification mechanisms to ensure that parties are legitimate and legally competent.[76] The interpretation of smart contracts further complicates their legal treatment. Since contractual obligations are encoded in programming languages, courts and administrators may face difficulties in translating these coded terms into enforceable legal obligations. Human intervention is often required, particularly in complex cases or situations involving force majeure and other exceptional circumstances.[77]

Relatedly, the inherent rigidity of smart contracts poses challenges in adapting to unforeseen events or changed circumstances. Because the contract logic is automated and deterministic, it may not accommodate deviations or contingencies without pre-coded exception mechanisms. [78] Off-chain intervention protocols and exception-handling measures are therefore recommended to maintain contractual compliance while ensuring fairness and practicality. [79]

74 ibid; Federal Decree-Law No 46 of 2021 (n 64).
75 Wright and De Filippi (n 70).
76 ADGM (n 55); DIFC (n 30); Federal Decree-Law No 46 of 2021 (n 64).
77 Raskin (n 68).
78 Kevin Werbach, 'Trust, But Verify: Why the Blockchain Needs the Law' (2018) 33(2) Berkeley Technology Law Journal 487.
79 UK Jurisdiction Taskforce, *Legal Statement on Cryptoassets and Smart Contracts* (LawTech Delivery Panel 2019) <https://technation.io/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf> accessed 3 October 2025.

Finally, state supervision and regulatory oversight remain areas of ambiguity. The integration of blockchain-based smart contracts into administrative and legal frameworks is still evolving, with regulatory authorities emphasising the need for auditability, fail-safe mechanisms, and dispute resolution procedures. These safeguards are essential to ensure that smart contracts operate reliably within the broader legal and institutional context.

10.2. Technical Challenges

Smart contracts and blockchain technologies face several interrelated technical challenges that may affect their functionality, scalability, and reliability. One of the primary limitations concerns storage capacity.[80] Current blockchain infrastructures, particularly public and hybrid models, may encounter scalability constraints and data storage issues as transaction volumes increase, which can impact performance and network efficiency.

Another critical issue is private key management. The security of blockchain systems depends on cryptographic keys, and the loss of a private key can result in permanent loss of access to the associated smart contract, raising concerns about reliability and risk management.

Interoperability and standardisation present additional obstacles. Diverse blockchain platforms often lack unified technical standards, complicating cross-network smart contract execution. International initiatives such as ISO/TC 307 and the EU Blockchain Observatory, are actively working to establish standardised protocols to enhance compatibility and ensure seamless interaction between different blockchain networks. Smart contracts that depend on external data sources, commonly referred to as oracles, also face challenges related to data reliability. If the information provided by oracles is inaccurate or delayed, the automated execution of contracts may produce unintended or incorrect outcomes. Moreover, the financial and operational feasibility of establishing and maintaining blockchain networks, particularly within governmental contexts, involves substantial investment, technical expertise, and political coordination. Implementing such systems requires careful planning to balance technological capability with institutional readiness. Comparative lessons from Europe, the United States, and Singapore demonstrate that, while smart contracts can enhance efficiency and reduce the need for intermediaries, human intervention remains indispensable. Complex disputes, exceptional circumstances, and legal or administrative compliance issues still require oversight, highlighting that blockchain is a tool for augmentation rather than a fully autonomous solution. [81]

80 Zhang, Xue and Liu (n 4).

81 Jamie Berryhill, Théo Bourgery and Angela Hanson, *Blockchains Unchained: Blockchain Technology and its Use in the Public Sector* (Working Papers on Public Governance no 28, OECD 2018); Wright and De Filippi (n 70).

© 2025 Mohammed Abdelsalam, Alaa Abouahmed, Abdallah Shatat, Adham Hashish and Enas AlQodsi. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

11 CONCLUSION

This study demonstrates that blockchain-based smart contracts, particularly in public procurement, offer transformative potential to enhance transparency, operational efficiency, and accountability in public sector contracting. By embedding contractual obligations into self-executing code and distributing immutable records across decentralised nodes, blockchain reduces procedural bottlenecks, minimises human error, and strengthens trust in administrative processes. These contracts improve speed, traceability, and procedural fairness, while upholding administrative law principles such as transparency, equality of bidders, and safeguarding public funds.

The comparative analysis highlights a significant gap in adapting blockchain contracting models to civil law jurisdictions in the MENA region. While advanced economies have begun regulating smart contracts for administrative purposes, judicial and administrative intervention remains essential to address exceptional circumstances and ensure compliance with local administrative law. Successful adoption, therefore, requires not only technological deployment but also institutional adaptation, legal safeguards, and human oversight to address liability, dispute resolution, and enforceability issues.

To overcome these challenges and enable successful implementation, governments should develop a hybrid regulatory-technical framework combining statutory provisions with mandatory technical standards, ensuring enforceability and interoperability across platforms, while explicitly addressing liability allocation, dispute resolution mechanisms, off-chain settlements, and compliance with UAE Federal Law No. 46 of 2021 and international smart contract guidelines.

Institutional capacity building and change management are essential to fostering trust in automation, reducing resistance among public officials, and encouraging collaboration across departments. Establishing a national blockchain infrastructure specifically for public procurement, with role-based access controls, audit trails, and integration with national identity systems, would create a secure, unified ecosystem. Pilot programs should begin with low-risk, high-volume procurement areas, gradually scaling to strategic projects, while incorporating real-time monitoring of compliance, error handling, and data validation.

This approach ensures that blockchain adoption aligns with a sustainable digital transformation strategy, reinforcing administrative law values, including equity, accountability, and protection of public interest, while providing clear guidance for policymakers, academics, and public procurement agencies.

REFERENCES

1. Abdelaziz GM and Abouahmed A, 'The Punitive Power of Independent Administrative Authorities: Focus on Financial and Tax Violations: A Comparative Study' (2024) 7(2) Access to Justice in Eastern Europe 301. doi:10.33327/AJEE-18-7.2-n000216
2. Abdelaziz GM and Hashish A, 'Using Sanctions in Enforcing Digital Markets Act in the EU' in El Khoury R and Nasrallah N (eds), *Intelligent Systems, Business, and Innovation Research* (Springer Cham 2024) 775. doi:10.1007/978-3-031-36895-0_65
3. Abouahmed A, Eldakak A and Zakaria A, 'Using Electronic Auctions for Contracting in the UAE Federal Government Procurements' in Alareeni BAM and Elgedawy I (eds), *Studies in Systems, Decision and Control* (Springer Cham 2023) 884. doi:10.1007/978-3-031-39158-3_82.
4. Afify AM and others, 'Unveiling the Right to Health in Egypt: Exploring the Transformations and Challenges in Egyptian Constitutional Law and Policy' (2023) 12 Academic Journal of Interdisciplinary Studies 95. doi:10.36941/ajis-2023-0156
5. Al Shamsi H, 'Enhancing Digital Transactions with Blockchain Technology: Descriptive-Analytical Study' (2024) 7(3) Access to Justice in Eastern Europe 485. doi:10.33327/AJEE-18-7.3-a000322
6. AlQodsi EM and Arenova L, 'Smart Contracts in Contract Law as an Auxiliary Tool or a Promising Substitute for Traditional Contracts' (2024) 16(3) Journal of Legal Affairs and Dispute Resolution in Engineering and Construction. doi:10.1061/JLADAH.LADR-1132
7. AlQodsi EM, Jadalhaq IM and El-Maknouzi MEH, 'The Place of UAE's Food Security in the National Legislation and its Role in Supporting Global Food Security' (2024) 10(1) Cogent Social Sciences 2319379. doi:10.1080/23311886.2024.2319379
8. Al-Shawabkeh IK, 'Legal Guarantees for Objective Performance Evaluation of the Federal Public Employee in the UAE Legislation' (2020) 10(3) Lawyer Quarterly 217
9. Al-Shawabkeh IK, 'Using the Tax to Reduce Environmental Pollution in the United Arab Emirates: Possibility and Challenges' in AlQodsi EM and Abdallah AK (eds), *Legal Frameworks and Educational Strategies for Sustainable Development* (IGI Global Scientific Publishing 2025) 1. doi:10.4018/979-8-3693-2987-0.ch001
10. Al-Shawabkeh IK and Alqudah M, 'Independent Regulatory Bodies in the Jordanian Legal System: An Evaluative Review' (2023) 9 International Journal of Public Law and Policy 188. doi:10.1504/IJPLAP.2023.130014
11. Anglen J, 'Different Types of Blockchains: Public, Private, and Hybrid' (*Rapid Innovation*, 2025) <https://www.rapidinnovation.io/post/different-types-of-blockchains-public-private-and-hybrid> accessed 4 October 2025

© 2025 Mohammed Abdelsalam, Alaa Abouahmed, Abdallah Shatat, Adham Hashish and Enas AlQodsi. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

12. Atzori M, 'Blockchain Technology and Decentralized Governance: Is the State Still Necessary?' (2017) 6(1) Journal of Governance and Regulation 45. doi:10.22495/jgr_v6_i1_p5

13. Bambara JJ and others, *Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions* (McGraw Hill 2018)

14. Berryhill J, Bourgery T and Hanson A, *Blockchains Unchained: Blockchain Technology and its Use in the Public Sector* (Working Papers on Public Governance no 28, OECD 2018)

15. Buterin Vi, *A Next-Generation Smart Contract and Decentralized Application Platform* (Ethereum White Paper, 2014)

16. Casino F, Dasaklis TK and Patsakis C, 'A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification, and Open Issues' (2019) 36 Telematics and Informatics 55. doi:10.1016/j.tele.2018.11.006

17. Christidis K and Devetsikiotis M, 'Blockchains and Smart Contracts for the Internet of Things' (2016) 4 IEEE Access 2292. doi:10.1109/ACCESS.2016.2566339

18. Clack CD, Bakshi VA and Braine L, 'Smart Contract Templates: Foundations, Design Landscape and Research Directions' (*arXiv*, 15 March 2017) arXiv:1608.00771v3 [cs.CY]

19. Curry M, 'Blockchain Technology and the Legal Field' (*Moritz College of Law*, 2022) <https://moritzlaw.osu.edu/sites/default/files/2022> accessed 4 October 2025

20. Dahiyat EAR, 'The Legal Recognition of Electronic Signatures in Jordan: Some Remarks on the Electronic Transactions Law' (2011) 25(3) Arab Law Quarterly 297. doi:10.1163/157302511X568538

21. Dahiyat EAR, 'Towards New Recognition of Liability in the Digital World: Should we be More Creative?' (2011) 19(3) International Journal of Law and Information Technology 224. doi:10.1093/ijlit/ear006

22. Djamane D, 'Smart Contracts: Global Perspectives and Legal Realities', pt 2 (*Daily Jus*, 6 August 2025) <https://dailyjus.com/legal-tech/2025/08/smart-contracts-global-perspectives-and-legal-realities-part-2> accessed 3 October 2025

23. Duley C and others, *The Oracle Problem and the Future of DeFi* (BIS Bulletin no 76, Bank for International Settlements 2023)

24. El-Gheriani M and Hashish A, 'Egypt Amends its Competition Law to Establish a Pre-Merger Control System' (2023) 14(2) Journal of European Competition Law & Practice 106. doi:10.1093/jeclap/lpad014

25. El-Gheriani M and Hashish A, 'Harnessing the Crypto-Horse: Factors Affecting a Friendly Regulator of the Crypto-Industry: Dubai as a Test Case' (2025) 34(3) Information & Communications Technology Law 241. doi:10.1080/13600834.2025.2452718

26. El-Wafaa TA, Khalil A and Hashish A, 'Parliamentary Question: Insights from the Federal National Council in the UAE' (2024) 10(6) Heliyon e27671. doi:10.1016/j.heliyon.2024.e27671

27. Fayed A, Zakaria A and Abouahmed A, 'Innovations of Artificial Intelligence in Light of the Applicable Copyright Law: Realistic Solutions and Future Prospects. A Comparative Study of UAE, Egyptian, and French Laws' (2025) 8(1) Access to Justice in Eastern Europe 241. doi:10.33327/AJEE-18-8.1-a000116

28. Ghandour A and others, 'Legal Framework for Blockchain Contracts: An Analysis Under UAE Law' (*SSRN*, 14 December 2024) <https://ssrn.com/abstract=5056550> accessed 4 October 2025

29. Heaver I, Melnichenko A and Kamran Z, 'Blockchain 2025 – UAE – Global Practice Guides' (*Chambers and Partners*, 12 June 2025) <https://practiceguides.chambers.com/practice-guides/blockchain-2025/uae> accessed 3 October 2025

30. Jadalhaq IM and El Maknouzi MEH, 'Reading UAE Contract Law Through the Lens of Islamic Jurisprudence: A Case Study on the "Extraneous Cause' Exception in the UAE Civil Code" (2019) 19(2) Global Jurist 20180045. doi:10.1515/gj-2018-0045

31. Jadalhaq IM and others, 'A Systematic Reviews and Meta-Analyses of Interruption of the Statute of Limitations for Civil Claims: A Comparative Study of Arab Legislations' (2023) 9(6) Heliyon e16756. doi:10.1016/j.heliyon.2023.e16756.

32. Joshi R, 'Use Cases of Blockchain in Government and Public Sector' (*A3Logics*, 23 October 2024) <https://www.a3logics.com/blog/blockchain-in-government/> accessed 3 October 2025

33. Mik E, 'Smart Contracts: Terminology, Technical Limitations and Real World Complexity' (2017) 9(2) Law, Innovation and Technology 269. doi:10.2139/ssrn.3038406

34. Raskin M, 'The Law and Legality of Smart Contracts' (2017) 1(2) Georgetown Law Technology Review 305. doi:10.2139/ssrn.2842258

35. Sherman AT and others, 'On the Origins and Variations of Blockchain Technologies' (*arXiv*, 15 October 2018) arXiv:1810.06130 [cs.CR]

36. Solosky NT and Shutzer DLC, 'Contractor Compliance and Internal Investigations: New Practical Strategies for Unpredictable Times' (2025) 60(4) The Procurement Lawyer 20

37. Susnjara S and Smalley I, 'What is Blockchain Technology?' (*IBM*, 2020) <https://www.ibm.com/topics/what-is-blockchain> accessed 4 October 2025

38. Tapscott D and Tapscott A, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World* (Penguin 2016)

39. Tjong Tjin Tai E, 'Force Majeure and Excuses in Smart Contracts' (2018) 26(6) European Review of Private Law 787.

© 2025 Mohammed Abdelsalam, Alaa Abouahmed, Abdallah Shatat, Adham Hashish and Enas AlQodsi. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

40. Tsentsura K, 'How Governments Are Using Blockchain in 2025' (*Yellow.com*, 19 August 2025) <https://yellow.com/research/how-governments-are-using-blockchain-in-2025-from-digital-identity-to-cbdcs-and-voting> accessed 3 October 2025
41. Werbach K, 'Trust, But Verify: Why the Blockchain Needs the Law' (2018) 33(2) Berkeley Technology Law Journal 487
42. Werbach K and Cornell N, 'Contracts Ex Machina' (2017) 67(2) Duke Law Journal 313
43. Wright A and De Filippi P, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia' (2015) 34 Social Science Research Network 41. doi:10.2139/ssrn.2580664
44. Yermack D, 'Corporate Governance and Blockchains' (2017) 21(1) Review of Finance 7. doi:10.1093/rof/rfw074
45. Yu H, Deng X and Zhang N, 'To What Extent Can Smart Contracts Replace Traditional Contracts in Construction Projects?' (2023) 32(3) Engineering, Construction and Architectural Management 1393. doi:10.1108/ECAM-04-2023-0379
46. Zetzsche DA, Buckley RP and Arner DW, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' (2018) 4 University of Illinois Law Review 1361
47. Zhang R, Xue R and Liu L, 'Security and Privacy on Blockchain' (*arXiv*, 16 August 2019) arXiv:1903.07602v2 [cs.CR]

AUTHORS INFORMATION

Author contributions

All authors contributed to the conceptualization of the research and manuscript, including defining the study scope, designing the methodology, conducting analyses, and extracting results. They supervised the study. Additionally, all authors participated in drafting the manuscript and approved the final version.

Mohammed Abdelsalam
PhD, Associate Professor, Public Law Department, University College of Applied Science, Kingdom of Bahrain.
mohamed.abdelsalam@asu.edu.bh
https://orcid.org/0009-0005-3701-6393
Co-author, responsible for conceptualization, methodology, formal analyses, supervision, writing- original draft, writing- review and editing.

Alaa Abouahmed
PhD, Associate Professor, Public Law Department, United Arab Emirates University, United Arab Emirates.
alaa.m@uaeu.ac.ae
https://orcid.org/0000-0002-2276-260X
Co-author, responsible for conceptualization, methodology, formal analyses, supervision, writing- original draft, writing- review and editing.

Abdallah Shatat
Associate Professor of Management Information Systems, Bahrain Polytechnic, Kingdom of Bahrain
abdallah.shatat@polytechnic.bh
https://orcid.org/0000-0002-2605-6358
Co-author, responsible for conceptualization, methodology, formal analyses, supervision, writing- original draft, writing- review and editing.

Adham Hashish
PhD, assistant professor, Justice Diwan Law Firm
ahashish@gwmail.gwu.edu
https://orcid.org/0000-0002-2547-8284
Co-author, responsible for conceptualization, methodology, formal analyses, supervision, writing- original draft, writing- review and editing.

Enas AlQodsi*
PhD, Associate Professor, Private Law Department, United Arab Emirates University, United Arab Emirates.
enas.alqodsi@uaeu.ac.ae
https://orcid.org/0000-0003-4643-9660
Corresponding author, responsible for conceptualization, methodology, formal analyses, supervision, writing- original draft, writing- review and editing.

Competing interests: No competing interests were disclosed.

Disclaimer: The authors declare that the opinions and views expressed in this manuscript are free from any influence of any organization.

RIGHTS AND PERMISSIONS

Copyright: © 2025 Mohammed Abdelsalam, Alaa Abouahmed, Abdallah Shatat, Adham Hashish and Enas AlQodsi This is an open access article distributed under the terms of the Creative Commons Attribution License, (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

EDITORS

Managing editor – Mag. Bohdana Zahrebelna. **English Editor** – Julie Bold.
Ukrainian language Editor – Lilia Hartman.

ABOUT THIS ARTICLE

Cite this article
Abdelsalam M, Abouahmed A, Shatat A, Hashish A and AlQodsi E, 'Blockchain and Smart Public Procurement Contracts: A Comparative Legal Analysis of Digital Transformation in the Public Sector' (2025) 8(4) Access to Justice in Eastern Europe 242-74 <https://doi.org/10.33327/AJEE-18-8.4-a000137>

DOI: https://doi.org/10.33327/AJEE-18-8.4-a000137

Keywords: *Blockchain technology, smart contracts, public procurement, technical challenges, digital transformation, comparative law.*

DETAILS FOR PUBLICATION

Date of submission: 12 Aug 2025
Date of acceptance: 04 Oct 2025
Publication: 18 Nov 2025
Whether the manuscript was fast tracked? - No
Number of reviewer report submitted in first round: 2 reports
Number of revision rounds: 3 rounds: 2 major revisions and 1 minor revision

Technical tools were used in the editorial process:
Plagiarism checks - Turnitin from iThenticate https://www.turnitin.com/products/ithenticate/
Scholastica for Peer Review https://scholasticahq.com/law-reviews

AI DISCLOSURE STATEMENT

The authors declare that no artificial intelligence tools were used in the writing, translation, or editing of this manuscript. The research and the content of the article represent the authors' own original work. The corresponding author confirms that all co-authors complied with this declaration.

АНОТАЦІЯ УКРАЇНСЬКОЮ МОВОЮ

Дослідницька стаття

БЛОКЧЕЙН ТА СМАРТ-ДОГОВОРИ ПРО ДЕРЖАВНІ ЗАКУПІВЛІ: ПОРІВНЯЛЬНО-ПРАВОВИЙ АНАЛІЗ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ В ДЕРЖАВНОМУ СЕКТОРІ

Мохаммед Абдельсалам, Алаа Абуахмед, Абдалла Шатат Адхам Хашиш та Енас Аль-Кодсі*

АНОТАЦІЯ

Вступ. *Швидкий розвиток цифрових технологій представив блокчейн як потенційний інструмент у договорах про державні закупівлі в державному секторі. Смарт-договори, особливо в межах цивільного права, отримали законодавче визнання в таких юрисдикціях, як Франція та кілька штатів США. У цій статті порушено важливі питання щодо інтеграції смарт-договорів на основі блокчейну в державні системи закупівель з метою підвищення процедурної прозорості та операційної ефективності, водночас визнаючи обмеження та залежність від інституційних рамок.*

Головне питання полягає у з'ясуванні правових та технічних наслідків смарт-договорів про закупівлі на основі блокчейну. У дослідженні було з'ясовано їхній потенціал для оптимізації управління державними закупівлями та підвищення процедурної ефективності, водночас визнаючи необхідність правових гарантій, які підтримують принципи адміністративного права та враховують інституційні обмеження.

Методи. *Це дослідження використовує порівняльно-аналітичний підхід, розглядаючи відповідні правові положення, технічні вимоги та адміністративну практику в різних юрисдикціях. Різні моделі блокчейну — державні, приватні, гібридні та консорціальні — було розглянуто для того, щоб оцінити їхню результативність в процесах закупівель. Проаналізовано законодавчий досвід регулювання смарт-договорів, щоб виділити найкращі практики та сформувати обґрунтовану основу для впровадження в державному секторі.*

© 2025 Mohammed Abdelsalam, Alaa Abouahmed, Abdallah Shatat, Adham Hashish and Enas AlQodsi. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Результати та висновки. *Аналіз показує, що смарт-договори на основі блокчейну можуть зменшити бюрократичні затримки та мінімізувати людські помилки, водночас забезпечуючи незмінні записи, які можуть підтримувати підзвітність. Однак успішне впровадження вимагає правових та інституційних коригувань для вирішення питань щодо можливості забезпечити виконання, розподіл відповідальності, сумісність та захист даних. Запропоновано практичну модель, що ілюструє кожен операційний крок — від складання до автоматизованого виконання — з наголосом на доцільності та дотриманні законодавства, а не на передбачуваних трансформаційних ефектах. Дослідження підкреслює необхідність адаптованого законодавства, стандартизованих протоколів та цілеспрямованого навчання державних службовців для підтримки поступової інтеграції блокчейну в укладання договорів про державні закупівлі. Ці заходи спрямовані на керівництво юридично обґрунтованим та контекстно-залежним впровадженням смарт-договорів, сприяючи сталому цифровому перетворенню в управлінні державним сектором.*

Ключові слова: *технологія блокчейн, смарт-договори, державні закупівлі, технічні виклики, цифрова трансформація, порівняльне право.*