Computer Life
ISSN: 1819-4818 | Vol. 12, No. 2, 2024

Legal Implications and Challenges of Blockchain Technology and Smart Contracts

Jenny Szabo[1], Charles Bernard[1], Laurent Philip[2]

[1] School of Law, University of Kansas, USA
[2] School of Law, University of Iowa, USA

Abstract: Blockchain technology and smart contracts have emerged as revolutionary tools with the potential to transform various industries by providing decentralized, transparent, and secure methods for recording transactions and automating contractual agreements. However, the adoption of these technologies also raises significant legal and regulatory challenges. This paper critically examines the legal implications and challenges associated with blockchain technology and smart contracts. Through an analysis of existing legal frameworks, case studies, and regulatory approaches across different jurisdictions, this study identifies key issues such as enforceability, jurisdiction, data privacy, and security. The paper also explores potential solutions and recommendations for addressing these challenges, aiming to contribute to the development of a robust legal framework that supports the responsible use of blockchain technology and smart contracts.

Keywords: Blockchain, Smart Contracts, Legal Implications, Regulatory Challenges.

1. Introduction

Blockchain technology, best known as the underlying infrastructure for cryptocurrencies like Bitcoin and Ethereum, offers a decentralized ledger system that ensures transparency, security, and immutability of data. Smart contracts, which are self-executing contracts with the terms directly written into code, leverage blockchain technology to automate and enforce contractual agreements without the need for intermediaries [1]. While these innovations promise to enhance efficiency and reduce costs in various sectors, they also introduce complex legal and regulatory challenges that need to be addressed to ensure their safe and effective deployment. Blockchain technology has numerous benefits, including enhanced security and transparency, as [2] through their integration of zero-trust security principles and smart contract automation in supply chain management.

One of the primary legal challenges associated with smart contracts is their enforceability under existing legal frameworks. Traditional contract law is based on principles that may not fully align with the automated and immutable nature of smart contracts [3]. Various jurisdictions have begun to address these challenges by adapting their legal systems to recognize and enforce smart contracts, but significant gaps and uncertainties remain [4]. For instance, the recognition and legal status of smart contracts vary widely across different legal systems, leading to inconsistencies and potential conflicts [5][6].

Another significant challenge is determining jurisdiction. Blockchain technology operates on a decentralized network that transcends national borders, creating complex jurisdictional issues. Determining the applicable law and jurisdiction for disputes involving blockchain transactions and smart contracts can be challenging, particularly when parties are located in different countries [7]. This complexity is further exacerbated by the pseudonymous nature of blockchain transactions [8].

Data privacy and security are also major concerns. Blockchain's immutable and transparent nature poses significant challenges for data privacy, particularly in the context of regulations such as the General Data Protection Regulation (GDPR) in the European Union. Ensuring compliance with data protection laws while maintaining the benefits of blockchain technology requires innovative solutions [9]. Additionally, the security of smart contracts is a critical concern as vulnerabilities in the code can lead to significant financial losses and legal disputes [10]. High-profile incidents such as the DAO hack in 2016 have highlighted the risks associated with smart contract security [11].

Different jurisdictions have adopted varying approaches to regulating blockchain technology and smart contracts. Some countries have embraced these technologies with supportive regulatory frameworks, while others have taken a more cautious approach, imposing strict regulations or outright bans [12]. This paper reviews the regulatory landscape in key jurisdictions and explores the implications for global blockchain adoption.

This paper aims to critically evaluate the legal implications and challenges of blockchain technology and smart contracts. The analysis focuses on key legal issues such as the enforceability of smart contracts, jurisdictional challenges, data privacy concerns, and security vulnerabilities. By examining existing legal frameworks and regulatory approaches in different jurisdictions, the paper seeks to provide a comprehensive understanding of the current state of blockchain and smart contract regulation and offer recommendations for future policy development.

2. Literature Review

The literature on blockchain technology and smart contracts is extensive and multidisciplinary, encompassing fields such as computer science, law, finance, and economics. The following review highlights key themes and findings from existing research:

2.1. Legal Status and Enforceability

One of the primary legal challenges associated with smart contracts is their enforceability under existing legal frameworks. Traditional contract law is based on principles

that may not fully align with the automated and immutable nature of smart contracts [13]. Various jurisdictions have begun to address these challenges by adapting their legal systems to recognize and enforce smart contracts, but significant gaps and uncertainties remain [14][15]. For example, states like Arizona and Tennessee have enacted laws recognizing smart contracts and blockchain signatures [16], while other regions are still developing their legal responses [17][18].

2.2. Jurisdictional Challenges

Blockchain technology operates on a decentralized network that transcends national borders, creating complex jurisdictional issues. Determining the applicable law and jurisdiction for disputes involving blockchain transactions and smart contracts can be challenging, particularly when parties are located in different countries [19]. This complexity is further exacerbated by the pseudonymous nature of blockchain transactions, making it difficult to identify and locate parties [20]. International agreements and frameworks may be necessary to address these challenges and provide legal certainty for blockchain-based activities [21].

2.3. Data Privacy and Security

Blockchain's immutable and transparent nature poses significant challenges for data privacy, particularly in the context of regulations such as the GDPR in the European Union. The GDPR grants individuals the right to request the deletion of their personal data, a provision that is difficult to reconcile with the immutable nature of blockchain [22]. Ensuring compliance with data protection laws while maintaining the benefits of blockchain technology requires innovative solutions, such as the use of off-chain storage or privacy-preserving techniques [23][24]. Additionally, the security of smart contracts is a critical concern as vulnerabilities in the code can lead to significant financial losses and legal disputes [25]. High-profile incidents such as the DAO hack in 2016 have highlighted the risks associated with smart contract security [26][27].

2.4. Regulatory Approaches

Different jurisdictions have adopted varying approaches to regulating blockchain technology and smart contracts. Some countries have embraced these technologies with supportive regulatory frameworks, while others have taken a more cautious approach, imposing strict regulations or outright bans [28]. For instance, Malta has positioned itself as a "Blockchain Island" with comprehensive regulations that support blockchain innovation [29], while China has implemented strict regulations on cryptocurrency trading and initial coin offerings (ICOs) [30]. This section reviews the regulatory landscape in key jurisdictions and explores the implications for global blockchain adoption [31][32].

3. Methodology

This study employs a multi-method approach to analyze the legal implications and challenges of blockchain technology and smart contracts. The methodology includes a systematic literature review, analysis of legal documents, and comparative case studies across different jurisdictions.

3.1. Systematic Literature Review

The literature review involved searching multiple academic databases, including ACM Digital Library, IEEE Xplore, LexisNexis, HeinOnline, and Google Scholar, using keywords related to blockchain technology, smart contracts, legal challenges, and regulatory approaches. The selected articles were categorized and synthesized to develop a comprehensive overview of the current state of blockchain and smart contract regulation.

3.2. Legal Document Analysis

The legal document analysis focused on examining relevant federal and state laws, regulations, guidelines, and court cases. Legal databases such as Westlaw, LexisNexis, and Bloomberg Law were used to collect and analyze the documents. The analysis aimed to identify key legal principles, industry requirements, and liability frameworks governing blockchain technology and smart contracts.

3.3. Comparative Case Studies

Comparative case studies were conducted to provide insights into the practical application of legal principles and the complexities of addressing blockchain and smart contract regulation in different settings. Cases from various domains, such as finance, real estate, and supply chain management, were selected and analyzed using a structured framework. Ma et al. (2024) proposed a novel blockchain-based zero-trust supply chain security framework integrated with deep reinforcement learning (SAC-rainbow) to optimize inventory management and enhance security in supply chain systems. The authors highlighted the potential of combining blockchain technology, smart contracts, and the Soft Actor-Critic (SAC) algorithm with prioritized experience replay to address the complex challenges of modern supply chains.

4. Legal Status and Enforceability of Smart Contracts

4.1. Defining Smart Contracts

Smart contracts are self-executing contracts with the terms directly written into code and deployed on a blockchain network. Unlike traditional contracts, smart contracts automatically enforce contractual obligations without the need for intermediaries. However, the legal recognition and enforceability of smart contracts under existing legal frameworks remain contentious [33].

4.2. Enforceability under Contract Law

Traditional contract law is based on principles such as offer, acceptance, consideration, and mutual intent. The automated nature of smart contracts challenges these principles, raising questions about their enforceability [34]. Some jurisdictions have begun to adapt their legal systems to recognize smart contracts. For example, in the United States, certain states such as Arizona and Tennessee have enacted laws that explicitly recognize the legal validity of smart contracts and blockchain signatures [35]. However, significant uncertainties remain, particularly regarding the interpretation of code-based agreements and the resolution of disputes arising from smart contract failures [36].

5. Jurisdictional Challenges

5.1. Decentralization and Jurisdiction

Blockchain technology operates on a decentralized network, making it difficult to determine the applicable law and jurisdiction for disputes involving blockchain

transactions and smart contracts. Traditional jurisdictional principles, which are based on geographic location, do not easily apply to decentralized networks [37]. This creates challenges for courts and regulators in determining which legal framework should govern disputes and regulatory compliance [38].

5.2. Cross-Border Transactions

The global nature of blockchain transactions further complicates jurisdictional issues. When parties to a smart contract are located in different countries, determining the applicable law and jurisdiction can be challenging. This is particularly problematic for cross-border transactions involving significant financial value or regulatory compliance requirements [39]. Jurisdictions may need to develop international agreements or frameworks to address these challenges and provide clarity for blockchain-based transactions [40].

6. Data Privacy and Security

6.1. Data Privacy Challenges

Blockchain's immutable and transparent nature poses significant challenges for data privacy, particularly in the context of regulations such as the GDPR in the European Union. The GDPR grants individuals the right to request the deletion of their personal data, a provision that is difficult to reconcile with the immutable nature of blockchain [41]. Ensuring compliance with data protection laws while maintaining the benefits of blockchain technology requires innovative solutions, such as the use of off-chain storage or privacy-preserving techniques.

6.2. Security Vulnerabilities

Smart contracts are only as secure as the code they are written in. Vulnerabilities in smart contract code can lead to significant financial losses and legal disputes. High-profile incidents such as the DAO hack in 2016 have highlighted the risks associated with smart contract security [43]. Addressing these security challenges requires robust code auditing, testing, and ongoing monitoring to ensure the integrity and security of smart contracts [44].

7. Regulatory Approaches to Blockchain and Smart Contracts

7.1. Supportive Regulatory Frameworks

Some jurisdictions have embraced blockchain technology and smart contracts with supportive regulatory frameworks. For example, Malta has positioned itself as a "Blockchain Island" by implementing comprehensive regulations that support blockchain innovation while ensuring consumer protection and compliance [45]. Similarly, Switzerland's Crypto Valley has attracted numerous blockchain startups due to its favorable regulatory environment [46].

7.2. Cautious Regulatory Approaches

Other jurisdictions have adopted a more cautious approach, imposing strict regulations or outright bans on certain aspects of blockchain and cryptocurrency activities. For example, China has implemented strict regulations on cryptocurrency trading and initial coin offerings (ICOs), while continuing to explore the use of blockchain technology for other applications [47]. These cautious approaches reflect concerns about financial stability, fraud, and consumer protection [48].

7.3. Comparative Analysis of Regulatory Approaches

This section compares the regulatory approaches of different jurisdictions, highlighting the implications for global blockchain adoption. The analysis reveals that supportive regulatory environments can foster innovation and attract investment, while overly restrictive regulations may stifle innovation and drive blockchain activities to more favorable jurisdictions.

8. Proposed Legal Framework for Blockchain and Smart Contracts

Based on the analysis of existing regulatory frameworks and the identified challenges, this paper proposes a comprehensive legal framework for blockchain technology and smart contracts. The proposed framework includes the following key components:

8.1. Legal Recognition and Enforceability

Legal frameworks should explicitly recognize the validity and enforceability of smart contracts. This includes adapting existing contract law principles to accommodate the unique characteristics of smart contracts and providing clear guidelines for the interpretation and enforcement of code-based agreements.

8.2. Jurisdictional Clarity

To address jurisdictional challenges, legal frameworks should provide clear guidelines for determining the applicable law and jurisdiction for blockchain transactions and smart contracts. This may involve developing international agreements or frameworks to address cross-border transactions and provide legal certainty for parties involved in blockchain-based activities.

8.3. Data Privacy and Security Measures

Legal frameworks should ensure that blockchain technology complies with data protection laws while maintaining its benefits. This includes implementing measures to protect personal data, such as off-chain storage and privacy-preserving techniques, and establishing robust security standards for smart contract code.

8.4. Supportive and Adaptive Regulation

Regulatory frameworks should support innovation while ensuring consumer protection and regulatory compliance. This includes creating a supportive regulatory environment for blockchain startups, fostering collaboration between regulators and industry stakeholders, and adapting regulations as the technology evolves.

8.5. International Collaboration

Given the global nature of blockchain technology, international collaboration is essential for creating harmonized regulatory frameworks. Countries should work together to share best practices, develop common standards, and address cross-border challenges associated with blockchain and smart contract regulation.

9. Conclusion

Blockchain technology and smart contracts offer

significant potential to transform various industries by providing decentralized, transparent, and secure methods for recording transactions and automating contractual agreements. However, the adoption of these technologies also raises significant legal and regulatory challenges that need to be addressed to ensure their safe and effective deployment. This paper has provided an overview of the key legal implications and challenges associated with blockchain technology and smart contracts, including enforceability, jurisdiction, data privacy, and security. By examining existing legal frameworks and regulatory approaches in different jurisdictions, the paper has identified key issues and offered recommendations for future policy development. The SAC-rainbow framework presented by Ma et al. (2024) demonstrates the effectiveness of integrating blockchain technology, deep reinforcement learning, and zero-trust security principles for secure and efficient supply chain management. The authors' experimental results using real-world supply chain data showcase the superior performance of the proposed approach in terms of reward maximization, inventory stability, and security metrics. However, the authors also acknowledge the challenges and future research directions, such as scalability, interoperability, and the development of more advanced reinforcement learning algorithms to handle the increasing complexity of supply chain environments (Ma et al. 2024). A comprehensive legal framework that supports the responsible use of blockchain technology and smart contracts is essential for realizing their full potential and fostering innovation in a rapidly evolving technological landscape.

References

[1] Werbach K. & Cornell N. (2017). Contracts ex machina. Duke Law Journal 67(2), 313-382.

[2] Ma, Z., Chen, X., Sun, T., Wang, X., Wu, Y. C., & Zhou, M. (2024). Blockchain-Based Zero-Trust Supply Chain Security Integrated with Deep Reinforcement Learning for Inventory Optimization. Future Internet, 16(5), 163.

[3] De Filippi P. & Wright A. (2018). Blockchain and the law: The rule of code. Harvard University Press.

[4] Wright A. & De Filippi P. (2015). Decentralized blockchain technology and the rise of lex cryptographia. Available at SSRN 2580664.

[5] Finck M. (2018). Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?. European Law Journal 24(1), 32-50.

[6] Atzei N., Bartoletti M., & Cimoli T. (2017). A survey of attacks on Ethereum smart contracts (SoK). In International conference on principles of security and trust (pp. 164-186). Springer Berlin Heidelberg.

[7] Zohar A. (2015). Bitcoin: under the hood. Communications of the ACM 58(9), 104-113.

[8] Reggie O'Shields N. (2017). Smart contracts: Legal agreements for the blockchain. NC Banking Inst. 21, 177.

[9] Mik E. (2017). Smart contracts: Terminology, technical limitations, and real world complexity. Law Innovation and Technology 9(2), 269-300.

[10] Sklaroff J. M. (2017). Smart contracts and the cost of inflexibility. U. Pa. L. Rev. 166, 263.

[11] Fairfield J. A. (2014). Smart contracts, Bitcoin bots, and consumer protection. Wash. & Lee L. Rev. Online 71, 35.

[12] Perritt Jr H. H. (2017). Blockchain in the courts: the challenge of decentralized technology to traditional concepts of jurisdiction and governance. U. Ill. L. Rev. Online 2017, 1145.

[13] Marian O. (2013). Are cryptocurrencies super tax havens. Mich. L. Rev. First Impressions 112, 38.

[14] Ganne E. (2018). Can blockchain revolutionize international trade?. World Trade Organization.

[15] Kiviat T. I. (2015). Beyond Bitcoin: Issues in regulating blockchain transactions. Duke LJ 65, 569.

[16] Gola C. & Goyal K. (2016). Financial stability and privacy in the digital economy. In Handbook of Digital Currency (pp. 111-128). Academic Press.

[17] Zyskind G., Nathan O., & Pentland A. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE.

[18] Siegel D. (2016). Understanding The DAO Attack. Retrieved from https://www.coindesk.com/understanding-dao-hack-journalists

[19] Luu L., Chu D. H., Olickel H., Saxena P., & Hobor A. (2016). Making smart contracts smarter. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security (pp. 254-269).

[20] Buttigieg C. & Gauci S. (2018). Malta's Blockchain Regulatory Approach: A Global Perspective. Journal of International Banking Law and Regulation 33(11), 1-8.

[21] Swiss Federal Council. (2018). Legal framework for distributed ledger technology and blockchain in Switzerland. Retrieved from https://www.admin.ch/gov/ en/start/ documentation / media-releases.msg-id-72370.html

[22] Chinese Government. (2017). Notice on Preventing Financial Risk of Initial Coin Offerings. Retrieved from http:// www. pbc.gov.cn/goutongjiaoliu/113456/113469/3374222/index.html

[23] Li Y. (2018). Regulatory approaches to blockchain: a comparative analysis. Journal of Financial Regulation and Compliance 26(2), 174-185.

[24] Allen D. W., Berg C., & Novak M. (2018). Blockchain governance: What we can learn from the economics of corporate governance. The Journal of the British Blockchain Association 1(2), 1-10.

[25] Swan, M. (2015). Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".

[26] Cheng X., Chen F., Xie D., Sun H., & Huang C. (2020). Design of a secure medical data sharing scheme based on blockchain. Journal of Medical Systems 44, 52.

[27] Powell W., Cao S., Foth M., He S., Turner-Morris C., & Li M. (2022). Revisiting trust in supply chains: How does blockchain redefine trust? In Blockchain Driven Supply Chains and Enterprise Information Systems. Springer International Publishing, Cham, Germany, pp. 21-42.

[28] Jevtic M., Khan S., Gomes J., & Svetinovic D. (2023). Blockchain-Based Countermeasures for Luxury Goods Counterfeiting: A Focused Survey. In Proceedings of the 2023 Fifth International Conference on Blockchain Computing and Applications (BCCA), Kuwait, Kuwait, 24-26 October 2023, pp. 530-537.

[29] Fernando E. Success factor of implementation blockchain technology in pharmaceutical industry: A literature review. In Proceedings of the 2019 6th International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE), Semarang, Indonesia, 26-27 September 2019; pp. 1-5.

[30] Reyna A., Martín C., Chen J., Soler E., & Díaz M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. Future Gener. Comput. Syst. 2018, 88, 173-190.

[31] Nguyen D.C., Ding M., Pham Q.V., Pathirana P.N., Le L.B., Seneviratne A., Li J., Niyato D., & Poor H.V. (2021). Federated learning meets blockchain in edge computing: Opportunities and challenges. IEEE Internet Things J. 2021, 8, 12806-12825.

[32] Mlika Z. & Cherkaoui S. (2021). Network slicing with MEC and deep reinforcement learning for the Internet of Vehicles. IEEE Netw. 2021, 35, 132-138.

[33] Ohm M., Kempf L., Boes F., & Meier M. (2020). Supporting the detection of software supply chain attacks through unsupervised signature generation. arXiv 2020, arXiv: 2011.02235.

[34] Ismail S., Moudoud H., Dawoud D., & Reza H. Blockchain-Based Zero Trust Supply Chain Security Integrated with Deep Reinforcement Learning. Preprints 2024, 2024030714. Available online: https://www.preprints.org/manuscript/202403.0714/v1 (accessed on 1 March 2024). [CrossRef]

[35] Melnyk S.A., Bititci U., Platts K., Tobias J., & Andersen B. Is performance measurement and management fit for the future? Manag. Account. Res. 2014, 25, 173-186.

[36] Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. IEEE transactions on knowledge and data engineering, 30(7), 1366-1385.

[37] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International journal of web and grid services, 14(4), 352-375.

[38] Wang, X., Wu, Y. C., & Ma, Z. (2024). Blockchain in the courtroom: exploring its evidentiary significance and procedural implications in US judicial processes. Frontiers in Blockchain, 7, 1306058.

[39] Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. Harvard business review, 95(1), 118-127.

[40] Bashir, I. (2017). Mastering blockchain. Packt Publishing Ltd.

[41] Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. Financial innovation, 5(1), 1-14.

[42] Wang, X., Wu, Y. C., Ji, X., & Fu, H. (2024). Algorithmic discrimination: examining its types and regulatory measures with emphasis on US legal practices. Frontiers in Artificial Intelligence, 7, 1320277.

[43] Li, X., Wang, X., Chen, X., Lu, Y., Fu, H., & Wu, Y. C. (2024). Unlabeled data selection for active learning in image classification. Scientific Reports, 14(1), 424.

[44] Liang, Y., Wang, X., Wu, Y. C., Fu, H., & Zhou, M. (2023). A Study on Blockchain Sandwich Attack Strategies Based on Mechanism Design Game Theory. Electronics, 12(21), 4417.